مواجهة الحرب السيبرانية في قواعد القانون الدولي الانساني

م. د حامد محمد علي البلداوي

كلية الامام الجامعة / بلد

Confronting cyber warfare in the rules of international humanitarian law

M. Dr. Hamed Muhammad Ali Al-Baldawi

hamedali196666@gmail.com

المستخلص:

الحرب السيبرانية كأحدث شكل من أشكال الحروب القائمة بين الدول داخل الفضاء السيبراني، الذي أصبح مصدر تهديد فعلي لأمن الدول بصفة مشتركة ومنفردة، من خلال إتاحته لكل الأعمال العدائية ذات الطابع الإلكتروني ضد أي كان دون تمييز، بالإضافة إلى محاولات الجهود الدولية التي تسعى إلى إرساء قواعد تحقق وتحافظ على الأمن السيبراني العالمي,كذلك التطرق على أهم المبادئ في القانون الدولي الإنساني ومدى إمكانية تطبيقها على الحرب الإلكترونية. الكلمات ألافتتاحية: الحرب السيبرانية، الفضاء السيبراني, القانون الدولي الإنساني، الهجمات الإلكترونية.

Abstract:

Cyber war as the latest form of war between states within cyberspace, which has become a source of actual threat to the security of states jointly and individually, by allowing all hostilities of an electronic nature against anyone without discrimination, in addition to addressing international efforts that seek to establish Rules that achieve and maintain global cyber security, as well as shed light on the most important principles applicable in international humanitarian law and the extent to which they can be applied to electronic warfare

Keywords: cyber warfare, cyber space, international humanitarian law, cyber-attacks.

المقدمة :

مع التطور الكبير في تكنولوجيا الفضاء والاتصالت وزيادة الاعتماد عليها، ظهر ما يسمى بالهجمات السيبرانية التي تتم في الفضاء السيبراني، والتي يقوم بها مخترقي الشبكات سواء كانوا دول 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 الالكترونية الحساسة مثل المواقع العسكرية، حيث يقومون باختراقها بقصد الحصول على أسرار، أو وثائق أو نشر رسائل احتجاجية، أو حتى لجمع المال,وأصبحت الاختراقات السيبرانية من أهم المشاكل التي يواجهها اصحاب الاختصاص من فقهاء القانون الدولي الانساني, وذلك لصعوبة تحديد طبيعتها وعناصرها، وما يترتب على هذه الهجمات من تبعات المسؤولية المدنية الدولية والجنائية، خاصة وأن تلك الهجمات قد تلجأ إليها بعض الدول لأجل تحقيق مكاسب معينة، كالهيمنة على واقع النزاعات المسلحة، اضافة الى النتائج السلبية من التهديدات الإجرامية والإرهابية, التي قد تنتجها تلك الهجمات,من أجل الحصول على مزايا اقتصادية او سياسية,إذ أصبحت التكنولوجيا الحديثة جزء مهم من وسائل الحرب المعاصرة والتي تتم في الفضاء السيبراني وهو ما سمي بالحرب السيبرانية. يلاحظ ان المستجدات الحديثة في مجال التكنولوجيا, بأنّ الحرب السيبرانية تعدّ تحديا للمفاهيم السائدة حول الأمن القومي, ويتطلب إيلاء قضية الدفاع عن البنى التحتية الحيوية للدولة أهمية قصوى, لاسيما في مجالات الطاقة, والمياه, والحوسبة, والاتصالات, والمواصلات, والاقتصاد, في القطاعين المدني والأمني. وبناء عليه ينبغي إجراء التعديلات اللازمة على مفهوم الأمن القومي, وقد ازداد لجوء الدول إلى استخدام الحرب السيبرانية نظرا لما توفره هذه الأخيرة من جهد ومال، كالتقليل من تكلفة الحرب والنزاع المسلح، نتيجة سهولة استخدام الأسلحة السيبرانية مثل الفيروسات وبرامج التجسس، وقرصنة المعلومات العسكرية والإستراتيجية.أن أساليب عمل الحروب السيبرانية تتقارب من ناحية قانونية مع إشاعة الرعب والإرهاب، لذلك يمكن تعريف الحروب السيبرانية استنادا لذلك بأنها نظام قائم على الرعب المنتشر في شبكة الإنترنت، والتي تهدف إلى تنفيذ الأعمال لترويع أمن الأفراد والجماعات والمؤسسات والدول، وإدخالهم في أزمات اقتصادية ونفسية واجتماعية وسياسية ناتجة عن الارهاب السيبراني او ما يسمى بالارهاب الصامت, مما يعرض حياة المدنيين لخطورة الحرمان من الاحتياجات الاساسية مثل والرعاية الطبية, والكهرباء, ومياه الشرب, وغيرها, مما يتطلب موقف القانون الدولي الانساني بهذا الشأن من اجل حماية الفئات المشمولة وفق قواعد هذا القانون. وتتمحور الإشكالية في دراستنا حول مدى ملائمة القاعدة القانونية التقليدية الخاصة بالنزاع المسلح بموجب "القانون الدولي الإنساني" واستيعابها لفكرة الحرب السيبرانية ؟ وللإجابة على ذلك قسمنا موضوع الدراسة إلى **مطلبين** تناولنا في **المطلب الأول** دراسة مفهوم الحرب السيبرانية، وفي **المطلب الثاني** إلى تكييف الحرب السيبرانية وفقا للقانون الدولي الإنساني.

المطلب الأول دراسة مفهوم الحرب السيبرانية

أُطلق العديدمن المصطلحات والمفاهيم على الحرب السيبرانية,لذلك تم تمسميتها الحرب الافتراضية, أوالحرب الإلكترونية,أوالهجمات السيبرانيةعلى الحرب السيبرانية التي يتم من خلالها قيام القراصنة (Hackers)بمهاجمة الملفات والمواقع التي تخص الآخرين, كمهاجمة المواقع الإلكترونية للمنشآت المهمّة, (أومهاجمة الحواسيب التابعة للوحدات العسكرية أوالوحدات الاقتصادية لدول معيّنة؛بقصد تدميرها, والسيطرة عليها, والإضراربها)[1]ومايزيدفي إتساع التحدي الذي يواجهه المختصون في القانون الدولي العام والإنساني على وجه الخصوص، إنما يتجسد في الغموض التي إكتنفت مفهوم الجريمة السيبرانية, وعدم الاتفاق على تعريف محدد وأن ذلك ناتج عن حداثتها وغموضها وخلو بعض

التشريعات القانونية من تجريمها, وغيرها من الاسباب الأُخرى، يمكن الإستدلال في ضوئه لتنظيم استعمالها بالحظر أو التقييد لمواجهة عواقبها الخطرة على الصعيد الإنساني[٢] أضحى من الضروري الوقوف في **الفرع الاول** :على تعريف الحرب السيبرانية ,والتطرق إلى بعض النماذج للحروب السيبرانية **فرعا ثانيا** .

الفرع الاول : تعريف الحرب السيبرانية: ليس هناك إجماع واسع لتعريف واضح ومحدد لمفهوم الحرب السيبرانية حتى الآن، وتكمن المشكلة الأساسية في غياب هذا التعريف, إلى طبيعة القاعدة القانونية المتغيرة لمصطلحات متطورة ظهرت في الآونة الأخيرة في سياق النزاع المسلح، مثل الهجمات السيبرانية عن طريق الانترنيت.وعرفت كلمة السيبرانية،مشتقة من الكلمة اللاتينية سايبر (cyber) ومعناها افتراضي، والسايبر كلمة يجري استخدامها لوصف الفضاء الذي يضم الشبكات العنكبوتية المحوسبة، ومنظومات الاتصالات والمعلوماتية وأنظمة التحكم عن بعد. وتعني: كل ما يتعلق أو يرتبط بالحاسبات وتكنولوجيا المعلومات والواقع الافتراضي،ومنها اشتقت صفة السيبرانية وتعني علم التحكم الأوتوماتيكي، أو علم الضبط. و تعني(Cybernetics) أيضا القيادة أو التوجيه، والذي يعني علم الاتصالات وأنظمة التحكم الآلي في كل من الآلات والأشياء الحية [٣],ومن تلك التعاريف ما ذهب إليها خبراء ومختصين في القانون الدولي الإنساني، وأولهم الأستاذ(SHIN)الذي عرف الحرب السيبرانية بأنها:"استخدام الطيف الالكتروني أو الكهرومغناطيسي لتخزين وتعديل وتبادل البيانات وجها لوجه مع أنظمة تحكم في بنى تحتية مرتبطة بها" [٤] ويعتبر آخرون أن الهجمات السيبرانية هي:"استمرار 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 المعلوما ت الاقتصادية، والعبث بالمحتوى التقني والرقمي وغيرها"[٥]ومن التعاريف الحديثة للحرب السيبرانية نذكر تعريف مجموعة الفقهاء التابعين للناتو الوارد في القاعدة (٣٠) من دليل تالين المتعلق بتطبيقات القانون الدولي في مجالات الصراع والحروب السيبرانية ، 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"[٦]وتعرف (اللجنة الدولية للصليب الاحمر) هذه الحرب بانها "الافعال التي يتخذها أطراف النزاع, لتحقيق ميزة على خصومهم في الفضاء الالكتروني باستخدام أدوات تقنية مختلفة وتقنيات تعتمد على الطاقة البشرية من الناحية النظرية , يمكن تحقيق المزايا عن طريق اتلاف او تدمير او اعطاب او نهب انظمة الحاسوب لدى الخصم (الهجوم السيبراني), او بالحصول على معلومات يفضل الخصم أن تبقى سرية التجسس السيبراني او من خلال الاستغلال السيبراني[٧]أما الفقه العربي وبالرجوع إلى المختصين للغة العربية فيها، فنجد أن تحدياً واجهوه في إختيار مصطلح مقارب لمصطلح (Cyber) في اللغة الإنكليزية، ولا أدل على ذلك ما تطرقت له الترجمة الحرفية للغة العربية لعنوان إتفاقية (مجلس أوربا), المتعلقة بالهجمات السيبرانية بأن ترجمتها غير صائبة، إذْ تُرجمَ العنوان (Convention on Cybercrime) إلى اللغة العربية بأنهّ "الاتفاقية المتعلقة بالجريمة الإلكترونية"، ويعود السبب إلى عدم وجود اصطلاح مناظر له في اللغة العربية[٨] إذْ يتضح مما تقدم إن الترجمة للوثائق الصادرة من الأمم, المتحدة باللغة العربية استعملت اصطلاح "السيبرانية" بدل الإلكترونية، كالقرار المرقم (٢٣٩/ ٥٧) الذي صدر عن الجمعية العامة للأمم المتحدة بشأن "إنشاء ثقافة عالمية للأمن السيبراني"، والقرار رقم (١٩٩/ ٥٨) الصادر عن الجمعية العامة للأمم المتحدة، كذلك بشأن الدعوة للدول الأعضاء إلى التعاون وتعزيز ثقافة الأمن السيبراني,إنَّ سبب تسليط الضوء على مصطلح السيبرانية, في هذه الدراسة يعود إلى الاصطلاح الذي استعمله "نوربرت وينر" في كتابه وهو "Cybernetic"، ولعدم وجود اصطلاح, تم الاتفاق عليه في اللغة العربية من جانب، ولأن الوثائق الصادرة عن الأمم المتحدة باللغة العربية، استعملت مصطلح السيبرانية, نفسه من جانب أُخر[٩].ويؤيد الباحث التعريف الذي أشار إلى الهجمات السيبرانية بأنها: أي تصرف, سواء أكان دفاعيا أم هجوميا, يتوقع منه, وعلى نحو معقول, في التسبب بإصابة شخص, أو قتله, أو إلحاق أضرار مادية, أو دمار بالهدف المُهاجَم, إذ يعد هذا التعريف الأقرب والأشمل لمفهوم الحرب السيبرانية. وهو ما اشارت اليه مجموعة الخبراء التابعين للناتو, الوارد في القاعدة (٣٠) من دليل تالين المتعلق بتطبيقات القانون الدولي.

الفرع الثاني : نماذج للحروب السيبرانية: تعرضت العديد من الدول في السنوات الأخيرة الماضية إلى عدة هجمات سيبرانية، وتتنوع هذه الهجمات الخطيرة مابين تدمير أنظمة إلكترونية لمنشآت حيوية عسكرية أو مدنية, وتعطيل أو إتلاف شبكات الدفاع العسكرية عن بعد، واختراق أو تعطيل أو تدمير شبكات القطاع العام او الخاص، وتعطيل البنية التحتية للدول, ومن بين أكثر الهجمات التي وقعت على المستوى الدولي والتي يمكن إدراجها في سياق الحروب السيبراني وكما يلي :

اولا : الهجوم السيبراني على إستونيا: قامت الحكومة الاستونية بتاريخ ٢٠٠٧ م بنقل نصب تذكاري يعود الى ألحرب العالمية الثانية،الذي كان مخصص لتخليد الجيش الأحمر الروسي من وسط عاصمة استونيا "تالين" إلى مقبرة عسكرية خارجها، مما أدى إلى حدوث مظاهرات شعبية في المجتمع الإستوني الناطق بالروسية، والذي يمثل ما يقارب ٣٠ % 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 المدنيين من الحصول على خدمات أساسية عبر الانترنيت[١٠] . ووجهت إستونيا اتهاما رسميا لروسيا في ارتكابها هذه الهجمات السيبرانية، إذ اعتبرتها إستونيا بمثابةأعمال انتقامية بسبب قيامها بنقل النصب التذكاري المخلد للجيش الروسي خارج العاصمة تالين، وهو ما نفته روسيا[١١] وقد اعتبر العديد من الخبراء أن الحديث عن حرب سيبرانية ظل حديثا نظريا حتى تاريخ هذه الهجمات التي تعرضت لها إستونيا في ٢٠٠٧م والتي تعد أول حرب سيبرانية تم استخدام الفضاء السيبراني فيها لتدمير أهداف حيوية للعدو[١٢].

ثانيا: الهجوم السيبراني على المواقع النووية الإيرانية: تم استهداف المفاعلات النووية الإيرانية بفيروس (Stuxnet)[١٣]، الذي تم اكتشافه لأول مرة في٢٠١٠م، والذي يعد الأخطر والاكبر من الهجمات السيبرانية, لمنشآت عسكرية, أو مدنية على الإطلاق، إ ذ تعرضت المواقع النووية الإيرانية إلى أسلوب ومنهج يقوم على شقين: الأول باستهداف أجهزة الطرد المركزية وخروجها عن السيطرة من جهة، أما الثاني فبالتحايل على أجهزة التحكم والإيحاء لها، أن عمليات تشغيل المنشأة النووية تعمل بصور ة طبيعية، إلا أنها في الواقع معطلة[١٤] . وكان آخر الهجمات في ١٧ فبراير ٢٠١٢ م بعد اعلان الاجهزة الاستخبارية الإيرانية ,أن فيروس ستاكسنت قد ادى الى اصابة ما يقدر بستة عشر ألف جهاز كمبيوتر و,وذكرت إسرائيل أن هجمات ستاكسنت كانت حصيلة تعاون مع الولايات المتحدة للعمل على تعطيل المنشآت النووية ويمثل ذلك جزءا من منصة لإطلاق الفيروسات الخطرة، تم تطويرها عام ٢٠٠٧ م وتمت تجربته في إسرائيل[١٥]ومن جانب سياسي ايضا تعرضت ايران الى هجمات سبرانية اخرى, وذلك من خلال المواجهات بين إسرائيل والولايات المتحدة من جهة وأيران من جهة اخرى والتي تم استخدامها في تحريك القوه الناعمة داخل إيران بدعم الاحتجاجات في عام ٢٠٠٩م ، وتقديم دعم فني للمعارضة عقب الانتخابات الرئاسية، وفي نهاية ٢٠١١ م دشنت الولايات المتحدة "سفارة إلكترونية" لأعطاء الإيرانيين المعلومات حول التأشيرات عبر الإنترنت، والتواصل مع الطلاب الإيرانيين وهو ما يلائم عملية قطع العلاقات الدبلوماسية بين إيران والولايات المتحدة منذ ثلاثين عاما,وهو ما دعا إيران إلى غلق موقع السفارة الالكتروني وتجريم محاولة الدخول عليها على أنها تمثل تهديدا للأمن القومي لديها[١٦]وعلى هذا فيمكن اعتبار تحدي الأمن السيبراني أعلى تحديات الأمن القومي في هذا القرن ، مع الإشارة إلى أن المفهوم الحديث للأمن لا يقتصر فقط على الجوانب العسكرية، بل يواكب كل التهديدات والتحديات التي يمكن أن شكل حجر عثرة أمام الاقتصاد الرقمي وتدفق المعرفة، فقد أسقطت تكنولوجيا المعلومات والاتصالات مفهوم الحدود الجغرافية بين الدول مما يضع السيادة الوطنية في خطر، خاصة مع اختراق المواقع الرسمية الحكومية والتجسس المعلوماتي على هذه الدول.

المطلب الثاني تكييف الحرب السيبرانية وفقا للقانون الدولي الإنساني

شهدت الاعوام الماضية إدخال تقنية واسعة من التكنولوجيا الحديثة إلى ساحة المعركة, وأوجد الفضاء المعلوماتي ميدانا جديدا للقتال. ، ومدى خضوع هذه العمليات الالكترونية الى القانون الدولي الانساني، وهل توجد قواعد قانونية, في القانون الدولي النافذ, قادرة على مواءمة التحديات, التي يفرضها استخدام هذه "الاسلحة الجديدة"، في النزاع المسلح الحديث، التي لا يتقاتل خلالها الجيوش النظامية او فئات مسلحة تكون منظمة اخرى, تطرق العديد من فقهاء القانون الدولي إلى موضوع الحروب السيبرانية، فطرحوا عددا من الإشكاليات القانونية المتمحورة حول القانون الواجب التطبيق عليها . إن 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 المسألةسنتناول في هذا المطلب **عدم خضوع الهجمات السيبرانية لأحكام القانون الدولي الإنساني في الفرع الاول : وفي الفرع الثاني** سيتناول **: خضوع أحكام القانون الدولي الإنساني على الهجمات السيبرانية .**

الفرع الاول : عدم خضوع احكام القانون الدولي الإنساني على الهجمات السيبرانية :

تكمن خصوصية الفضاء الإلكتروني في عدم وجود دولة بإمكانها فرض السيطرة, والسيادة, الأحادية عليه، وبهذا يكون استخدامه بشكل يسبب اضرار بالإنسانية. وعلى هذا الأساس ظهر اتجاه فقهي سمي بالاتجاه الحر يرفض التعامل القانوني مع الإنترنت ويقضي بأن الإنترنت منطقة بلا قانون, لذلك اتجه جانب من الفقهاء القانونيين الأوروبي, والأمريكي, إلى اعتبار الفضاء الإلكتروني منطقة خاليه من القانون, وكل شيء

متاح، حيث يمكن لأي شخص امكانية العمل بأنشطة معاديه من دون قوانين أو ضبطاً للنفس. فقد قيل بأن كلمات المرور وألواح المفاتيح وأجهزة الحواسيب هي التي تشكل حدودا وفواصل بين العالمين، ولابد من الدخول إلى هذا العالم من خلال هذه،"فهذا العالم لايمكن أن تختص به دولة معينة، وبالتالي لا يمكن إنطباق القانون الدولي العام التقليدي، فهذا القانون لم يت نجاحه حتى الآن بحكم الفضاء البحري أو الجوي الخارجيين"[١٧]لذلك فإن أنصار الاتجاه الحر وهو رأي يرفض التعامل في القانون, مع الإنترنت، ويتزعمه بعض الساسة الأمريكيان وعلماء التقنيات, وتساندهم مجموعة قليلة من الفقهاء القانونين، يذهبون إلى القول: إن الإنترنت لايخضع الى القانون، والحجة في ذلك أن الإنترنت عالم حديث لا يتوافق مع واقع مادي تقليدي[١٨]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[١٩]وفيما يخص تطبيق أحكام القانون الدولي الإنساني, على الهجمات الإلكترونية، يذهب انصار هذا المذهب بأنه لا توجد فقرة قانونية بأي مادة في مواثيق القانون الدولي الإنساني, يمكنها معالجة الهجوم على الشبكات الحاسوبية, أو تتطرق الى حرب المعلومات أو العمليات المعلوماتية، كذلك لم توضع ضوابط للهجوم على الشبكات الحاسوبية, خلال النزاع المسلح، لان استخدام التكنولوجيا الحديثة للإنترنت هو حديث نسبياً، والقانون الدولي الإنساني القائم لايتلاءم مع أساليب الحرب الإلكترونية, إضافة إلى أن الاتفاقيات القائمة حالياً يعود تاريخها إلى قبل استخدام أو ظهور الاختراقات عبر شبكات الحاسوب[٢٠]وتتسم كذلك هجمات الفضاء السيبراني بأنها استباقية ومن دون سابق إنذار، وأنها غير محددة المجال أو المدى، وتكون أهدافها غير محددة بخلاف الحروب العادية التي تكون أهدافها ومكانها واضحين, 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 ثم تكون تفاعلاتها كبيرة فهي تتشابك مع الحرب الإعلامية وحرب الشبكات والاتصالات والحرب ذات البعد السياسي والسيكولوجي والحرب التكنولوجية والإرهاب[٢١] ويؤكد أصحاب هذا الراي حجتهم من أن عبارة الحروب الإلكترونية لم توجد في ميثاق الأمم المتحدة واتفاقيات جنيف, ولاهاي، ومعاهدة حلف شمال الأطلسي. ويستخدم ميثاق الأمم المتحدة ومعاهدة حلف شمال الأطلسي, على حد سواء مصطلحات مثل "السلامة الإقليمية"، و"استخدام القوة المسلحة"، "وعمل من جانب القوات الجوية أو البرية أو البحرية", "وهجوم مسلح"، وهي مصطلحات لا تنسجم مع مفهوم الحروب الإلكترونية, مما يضعها ظاهرياً خارج نطاق القانون الدولي[٢٢],وكما يبين النزاعان الإستواني والجورجي بصورة مثيرة لعواقب النزاع الإلكتروني والتشويش المحيط بجهود الرد الناجم, عن عدم اليقين بأن قواعد القانون الدولي التي من الممكن أن تطبق عليه، فعلى الرغم من جسامة الأضرار التي تلحقت بالبنية التحتية لهاتين الدولتين واستمرار الهجمات الإلكترونية لعدة أيام إلا أنها لم تعدّ بمثابة نزاع مسلح, .بالإضافة إلى أن المادة (٥١) من ميثاق الأمم المتحدة, بينت انه " ليس في هذا الميثاق ما يضعف أو ينتقص الحق الطبيعي للدول، فرادى أو جماعات, في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء الأمم المتحدة.... ",هذا النص يعطي للدولة الحق في الدفاع عن نفسها، عندما تواجه هجوما من قبل قوة مسلحة, أما في سياق الحرب السيبرانية فلا يعدّ الهجوم السيبراني نزاعا مسلحا, لأنه لا يتضمن استعمالا للقوة المسلحة ضد إقليم الدولة[٢٣]، ولا يوجد في معظم الحالات ما يثبت الأدوار التي قامت بها الدول في هذه النزاعات، وقد لا يصل الهجوم الإلكتروني من القوة لكي يمكن اعتباره هجوما مسلحا[٢٤]وبناءا على ذلك يمكن القول: إن القانون المعمول به حالياً لا يتماشى مع مستجدات العصر، لأنه وضع أساسا للتعامل مع النزاعات المسلحة التقليدية ولا ينطبق على الهجمات الإلكترونية، لأنه لا يعدّ نزاعاً مسلحاً لغياب الأعمال العدائية التقليدية , على الرغم من الحجج الواردة ضمن هذا الاتجاه، فإنه لا يمكن التسليم بوجود فراغ قانوني، فعند ظهور الثورة الصناعية الأولى لم يقل أحد بوجوب التخلي عن القوانين النافذة، وكذلك عند ظهور الطائرة كوسيلة نقل للبضائع والركاب، حيث كانت ظاهرة لايربطها أي شيء بالماضي، فهي تفقد اتصالها بالأرض وتكون محلقة في الجو بين السماء والأرض، وتحليقها يكون في الأجواءالإقليمية وأحيانا فيما وراءها، حيث لا سيادة ولا سيطرة لدولة على هذا الفضاء الخارجي. ومحكمة العدل الدولية في رأيها الاستشاري المتعلق بالتهديد باستخدام الأسلحة النووية ذهبت إلى القول: إن "المبادئ والقواعد الإنسانية قد وضعت قبل اختراع الأسلحة النووية"، ولكن هذا لا يمنع من تطبيق القانون الدولي الإنساني عليها، ولا يمكن التمسك بعدم انطباق القانون الإنساني على هذه الأسلحة بحجة أنها لم تكن معروفة عند وضع قواعده وهذا ما لايمنع من تطبيقه على الأسلحة النووية[٢٥].ونستنتج من ذلك أن الهجمات السيبرانية تشكل وسيلة وأسلوب للقتال في الوقت نفسه، وذلك وفق الأهداف المستخدمة لتحقيقها,وقد طالبت اللجنة الدولية للصليب لأحمر الدول المنضمة الى اتفاقيات جنيف أثناء المؤتمر الدولي الثامن

والعشرين, للصليب الأحمر والهلال الأحمر المقام عام ٢٠٠٣م بأن تخضع جميع الأسلحة الحديثة, ووسائل وأساليب الحرب الجديدة "لاستعراض دقيق ومتعدد التخصصات", حتى يتخطى تطور التكنولوجيا الحديثة الحماية القانونية المكفولة، ويعد استخدام الحروب السيبرانية أثناء النزاع المسلح مثالاً جيداً على هذا التطور التكنولوجي السريع"[٢٦]وبما أن المادة(٣٦) من الملحق "البروتوكول الأول الإضافي" لاتفاقيات جنيف تنص على أن: "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 محظوراً في جميع الأحوال أو في بعضها بمقتضى هذا الملحق "البروتوكول" أو أية قاعدة أخرى من قواعد القانون الدولي, التي يلتزم بها الطرف السامي المتعاقد", وفي ما يتعدى نطاق الالتزام المحدد الذي تفرضه هذه القاعدة على الدول الأطراف، تبين أن القاعدة العامة للقانون الدولي الإنساني, تنطبق على التكنولوجيا الحديثة, يجب على أطراف النزاعات أن تلتزم باتخاذ الاحتياطات اللازمة للحد من تأثير الحرب السيبرانية, ونتيجة لذلك، ويستحسن ان تكون نظم الحواسيب العسكرية منفصلة بما يكفي عن تلك الحواسيب المدنية، بغية حماية السكان المدنيين, من آثار الحرب االسيبرانية لذلك نؤكد لوجود حاجة إلى زيادة تحديث القانون الدولي الانساني يتوافق مع التطور التكنولوجي، أو أن آثارها الإنسانية أصبحت مفهومة على نحو أفضل. ويجب أن تقرر الدول والمنظمات الدولية ومنها منظمة الامم المتحدة خصوصا هذا الأمر في المستقبل. وفي غضون ذلك، من الضروري التشديد على أنه ما من فراغ قانوني في الفضاء السيبراني. وبعيداً عن ذلك، نواجه عدداً من الأسئلة حول كيفية تطبيق القانون الدولي الإنساني عملياً في المستقبل.

الفرع الثاني: خضوع أحكام القانون الدولي الإنساني على الحرب السيبرانية:

ويؤكد أنصار هذا الرأي إلى عدم الايمان بوجود فراغ قانوني في الفضاء الافتراضيCyberspace is not a “law-free" zone, واعتبار القواعد القانونية القائمة كافية لتنظيم الفضاء الإلكتروني، وانه يمكن تطبيقها على الفضائيات الحديثة, وسمي هذا الرأي بالمذهب القانوني. وإنه يمكن التعامل مع الإنترنت قانونا، خاصة سبق وأن تم تنظيم وسائل الاتصال التي تشبهها مثل الهاتف والمانتال في فرنسا والفاكس وغيرها من الاساليب الإلكترونية الحديثة, وما على فقهاء القانون سوى التعاون مع التقنين وخاصة أن العديد من المواد القانونية الموجودة تنطبق عليها[٢٧]. 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"[٢٨]وأما القول: إن الميثاق قد اشترط استخدام القوة وعدم اعتبار الهجوم" السيبراني "نزاعا مسلحا لأنه لا يتضمن استعمالا للقوة المسلحة، فميثاق الأمم المتحدة في المادة ٢ فقره (٤) حظر على الدول اللجوء إلى الحرب، أو التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي، أو الاستقلال السياسي لأي دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة، لكن الميثاق ترك تحديد المعنى الحقيقي لهذه القاعدة القانونية لمجلس الأمن الذي يقررها تبعا للظروف المحيطة بكل حالة على حدة، وهذا واضح من نص المادة ٣٩ من الميثاق التي تمنح مجلس الأمن سلطة تقرير الإجراءات القهرية، حيث إنّ هذا النص ورد بصورة غير ملزمة وذلك بسبب تمتع مجلس الأمن بصلاحيات تقرير ما إذا وقع تهديد للأمن والسلم الدوليين أو إخلال به أو كان وقع عملا من أعمال العدوان[٢٩] ، وقد يلجأ مجلس الأمن إلى اتخاذ هذه الإجراءات بصرف النظر عن نص المادة ٢ فقرة ٤ في حال رأى المجلس في موقف معين تهديدا للسلم، وذلك لعدم مخالفة هذا الإجراء لأحكام الميثاق أو لقواعد ومبادئ القانون الدولي[٣٠]، كل هذا يعني أن الفقرة الرابعة من المادة الثانية من ميثاق الأمم المتحدة والمواد ذات الصلة من الميثاق تنطبق على الهجمات الإلكترونية، ٤ من الميثاق. / بغض النظر عن نوع الأسلحة المستخدمة ويعدّ ذلك استخداما للقوة بالمعنى المقصود في المادة ٤/٢ من الميثاق.وفي نفس السياق أشارت المادة ٣٦ من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لعام ١٩٤٩م المتعلق بحماية ضحايا النزاعا ت المسلحة الدولية لعام ١٩٧٧ م 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"[٣١]بناءا على ذلك ينطبق هذا النص على الهجمات السيبرانية بأنها سلاح أو أسلوب من أساليب الحرب، فعلى الدول التأكد عن 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 السيبرانيةوعلى هذا 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. لقد أجمع الفقه الدولي على أن الهجمات الإلكترونية تعدّ حربا صحيحة عندما تكون أثارها على العالم المادي أثار مدمرة[٣٢]، "وإن استخدام القوة من خلال هذه الآلية الحديثة ضد دوله يشكل حق وطني للدولة المعتدى عليها للدفاع عن نفسها"[٣٣]وفي حالة نيكاراغوا مع الولايات المتحدة الأمريكية والمتعلقة بالأنشطة ذات الطابع العسكري وشبه العسكري في عام ١٩٨٦م،"بينت محكمة العدل الدولية أن المادة ٥١ لاتشير إلى أسلحة محددة وأن مفهوم الأسلحة ينطبق على أي استخدام للقوة" [٣٤]، وبغض النظر عن حقيقة أن الهجمات" السيبرانية لاتستخدم الأسلحة الحركية التقليدية، فإن ذلك لا يعني بالضرورة أنها لا يمكن أن تكون مسلحة, ويمكن اعتبار استخدام أي جهاز ينتج عنه خسائر كبيرة في الأرواح أو تدمير واسع للممتلكات مستوف لشروط الهجوم" المسلح"، ويدعم هذا الاستنتاج تأكيد مجلس الأمن على ذلك الحق في الدفاع عن النفس ردا على هجمات ١١ سبتمبر ٢٠٠١م على الولايات المتحدة[٣٥]إن الهجوم على شبكات الحاسوب إذا لم يحدث في سياق نزاع مسلح أو كانت أثاره لا تصل إلى نفس تأثير الهجوم العسكري الفعلي، لا ينطبق عليه القانون الدولي الإنساني، بل يخضع للقوانين الجنائية الداخلية[٣٦], فحسب هذا الرأي إن القانون الدولي الإنساني ينطبق على الحرب الإلسيبرانية على الرغم من عدم استخدام القوات المسلحة الفعلية ذلك عندما ينسب الفعل إلى دولة، وكانت نتائج هذا الهجوم على درجة عالية من الخطورة، بمعنى الأخذ بالنتائج المادية على ارض الواقع وليس بالأفعال العنيفة، مثل العمل الذي قد يستهدف التحكم بمركز الحاسوب والشبكات الوطنية لتوليد الطاقة، ومحولات الكهرباء ومرافق الأسلحة النووية بحيث تجعلها تُدمر نفسها من الناحية العملية، وكذلك التحكم بحركة الملاحة الجوية مما يؤدي إلى تصادم الطائرات[٣٧]، وينتج عن ذلك الأذى أو الوفاة أو إحداث التلف أو الدمار أو تكون هذه النتائج متوقعة، فإنه يعدّ هجوما مسلحا بالمعنى المقصود في القرار رقم (٣٣١٤), والصادر من الجمعية العامة للأمم المتحدة[٣٨], وعليه يمكن القول: إن أي هجوم"سيبراني"على دولة أو له عواقب في دولة أخرى هو بمثابة" هجوم مسلح "أو معادل له على الأقل عندما يستتبع دماراً كبيراً، أو خسائر في الأرواح البشرية وهذا ينسجم مع المعنى الوارد في ميثاق الأمم المتحدة ومعاهدة الناتو والقانون الدولي العام، وذلك لتمكين الدول من الدفاع الفردي والجماعي المشروع بواسطة الوسائل العسكرية[٣٩] 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 ١٩٤٩م ، حيث أصبحت وسائل وأساليب الحروب متطورة إلى درجة لم يكن يتصورها واضعي تلك الاتفاقيات, وعليه يجب معالجة تلك الثغرات مع التطور الحاصل في الحروب السيبرانية, وأيجاد سبل قانونية واضحة للتصدي لهذا النوع من عمليات الحرب الإلكترونية, و معالجة القانون القائم وجعله قادر على احتواء هذا النوع الجديد من الحروب.

الخاتمة :

النتائج:

١- الهجمات السيبرانية من المفاهيم الحديثة التي لايوجد اتفاق دولي على تعريفها حتى يومنا هذا، ولكن على الرغم من ذلك لا تحدث في فراغ قانوني ويمكن الاستناد في الك إلى المادة (٣٦) من البروتوكول الإضافي الأول لعام ١٩٧٧م.

٢-الحروب السيبرانية قد خرجت من فصول التصورات المستقبلية إلى الواقع والتطبيق، فقد أضحى الفضاء الرقمي ساحة اشتباك ما بين الدول، وهي في منحى تصاعدي مستمر من حيث تطور أساليبها وتهديداتها.

٣-بطئ الحركات التشريعية الدولية في الحد خطورة هذه الحروب، وفشل المجتمع الدولي في تنظيم إستخدامات الفضاء السيبراني بشكل سلمي.

٤-ان الدولة المعتدى عليها يكون لها الحق في استخدام القوة في الدفاع عن النفس وفقا للمادة (٥١) من ميثاق الامم المتحدة، بشرط ان يكون الرد على الهجوم السيبراني ضروريا لكي يكون الرد قانونيا ينطبق عليه صفة الدفاع الشرعي.

٥-لمعرفة مدى إمكانية انطباق قواعد ومبادئ القانون الدولي الإنساني على الهجمات السيبرانية التي تحدث في سياق نزاع مسلح حركي لابد من تكييف الهجوم السيبراني لمعرفة مدى انطباق مصطلح النزاع المسلح سواء الدولي أم غير الدولي عليها، ومن ثم يأتي دور تطبيق المبادئ وقواعد القانون الدولي الإنساني.

٦-ومن ثم ن تكاتف الجهود الدولية لإبرام اتفاقيات دولية تكون مهمتها الأساسية مواجهة المخاطر السيبرانية واحتوائها ومحاولة التخفيف منها.

التوصيات :

١-تعديل اتفاقيات جنيف لعام ١٩٤٩م والبرتوكولين المضافين اليها في عام ١٩٧٧م بغرض تحريم وتجريم الهجمات على البنية التحتية الحيوية التي يمكن أن تعطل الاتصالات الأساسية الدنيا وتعرض السكان المدنيين للخطر.

٢-تعديل ميثاق الأمم المتحدة لاستيعاب النزاع الإلكتروني وتحديد مفهوم النزاع المسلح وحالات الدفاع عن النفس ضد الهجمات السيبرانية, وعلى وجه الخصوص تعديل المادة ٤٢ من ميثاق الأمم المتحدة بما يسمح لمجلس الأمن باتخاذ التدابير اللازمة.

٣-وضع استراتيجيات التشريعات السيبرانية يكون قابلاً للتطبيق محلياً وعالمياً بالتوازي مع التدابير القانونية الوطنية والدولية المعتمدة.

٤-تعزيز الحوار والتنسيق المعلومات تين الدول والمنظمات الدولية والإقليمية في إطار مكافحة إساءة استخدام تكنولوجيا المعلومات والاتصالات.

٥-على الدول، خاصة العظمى والكبرى، أن تستغل التطور التكنولوجي في مجال الثورة المعلوماتية بما يخدم رفاه الدول بصورة عامة، والإنسان بصورة خاصة، بدل من تسخيرها في والحروب السيبرانية.

الهوامش:

١-خليفة إيهاب,القوة الإلكترونية وأبعاد التحول في خصائص القوة,مكتبة الإسكندرية, مصر,٢٠١٤م.

٢- منير البعلبكي , المورد: قاموس إنكليزي-عربي، دار العلم للملايين، بيروت, ٢٠٠٤م .

٣- أحمد عبيس نعمة الفتلاوي،الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر, مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد ٤، السنة ٨ ، ٢٠١٦م.

٤- حكيم غريب، صبرينة شرقي، تداعيات - الحرب الإلكترونية على العلاقات الدولية : د ا رسة في الهجوم الإلكتروني على إيران)فيروس ستكنست (، دفاتر السياسة والقانون، المجلد ١٢ ، العدد ٢ ، ٢٠٢٠م.

٥-سعيد درويش، "الحروب السيبرانية وأثرها على حقوق الإنسان: دراسة على ضوء أحكام دليل " تالين""، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، المجلد ٥٤ ، العدد ٥ ، ٢٠١٧م.

٦- علي حسين باكير, الحروب الالكترونية في القرن الواحد والعشرين, دون طبعة , مركز الجزيرة للدراسات, قطر, ٢٠١٠م.

٧- إيهاب خليفة،كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت، دار العربي للنشر والتوزيع،القاهرة، ٢٠١٧م.

٨- وستبي، جودي ر، دعوة إلى الاستقرار الجيوسيبراني، البحث عن السلام السيبراني، الناشر الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء، ٢٠١١م .

٩-توريه حمدون,الاستجابة الدولية للحرب السيبرانية، ، الناشر الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء، ٢٠١١م.

١٠-علوان عبدالكريم،الوسيط في القانون الدولي العام، دار الثقافة، عمان، ٢٠٠٦م.

١١-هينين ويجنر، مفهوم بشأن السلام السيبراني، البحث عن السلام السيبراني، ٢٠١١م.

الاتفاقيات والقرارات والمجلات والمنشورات والدراسات:

١- اتفاقيات جنيف الاربعة ١٩٤٩م, البروتوكول الاضافي الاول لعام ١٩٧٧م, المادة ٣٦.

٢ - قرارالجمعية العامة ٣٣١٤ مع تعريف العدوان المرفق به، في ١٤ كانون الأول /ديسمبر, ١٩٧٤م.

٣- مايكل ن شميت، الحرب بواسطة شبكات الاتصال: الهجوم على شبكاالمجلة الدولية للصليب الأحمر، مختارات من أعداد ٢٠٠٢ م.

٤-موسى طالب حسن، أعمر عمر محمود،الإنترنت قانونا، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة، العدد ٦٧.

٥-عادل عبد الصادق، أمريكا وتشكيل قيادة عسكرية في الفضاء الإلكتروني, هل بدأ الاستعداد لحروب المستقبل؟ تعلقيات مصرية، مركز الأهرام للدراسات , ٢٠٠٩ ، السياسية والاستراتيجية، العدد ١٣.

٦- مكتب الأمم المتحدة المعني بالمخدرات والجريمة: تقرير الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها، فيينا، ٢٠١٣، الوثيقة: UNODC/CCPCJ/EG.4/2013/2.

٧-ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟، مقال منشور على موقع اللجنة الدولية للصليب الأحمر، تمت الزيارة بتاريخ ٤ / ٩ / ٢٠٢٢ متاح على الرابط :

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

المصادر الاجنبية:

1- Oona' A.Hathway, Rebecca Crootof, Philip Levtiz, aley Nix, Aileen Nowlan, William Perdue and Julia Spiegel, "The Law of Cyber- Attack", California Law Review, 2012, p.7.
2-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. - Stuxnet est un ver qui ferait 3-partie d'un programme secret américain intitulé Olympic Games104. 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. .
-4- Lavenue,J.,(1996),Cyberspace ET Droit International: pour UN nouveau jus Communications:Revue. de la Recherche uridique–droit prospectif, p. 830. -.
5-Brown, D., (2006), Proposal for an international convention to regulate the use of information System in Armed Conflict, Harvard International Law review, Vol.47, p. 179.
6-Stahn, C., (2007),"Jus ad bellum', jus in Bello" jus pos bellum"? – Rrthing the Conception of the Law of Armed Force", The European Journal of International of International Law, 17(5) , p. 923,footnot,8.
7-la licéitéde la menace ou de l'emploi d'armes nucleaires, Rec. 1996, 241-242.
8-Koh, H., (2012), Cyberspace, Harvard International Law Journal, Online, volume 54, p.3.
9- Schmitt,M., (2012), Classification of Cyber Conflict. & Security Law, 17(2), P. 245–260.
10-Roscini, M., World Wide Warfare –Jus ad bellum and Use of Cyber Force, p. Cit. p. 115.
11-Green, J., (2015), Cyber warfare: a multidisciplinary analysis, (1st Edition), Routledge Studies in Conflict, Security and Technology, P. 126.
12- Messmer, E.,(2010), "Cyberattack Seen as Top Threat to Zap U.S. Power Grid," NetworkWorld, 2 June 2010 www.networkworld.com/news/2010/060210-nerc-cyberattack-power-grid.html.,-

هوامش البحث

[١] – خليفة إيهاب,القوة الإلكترونية وأبعاد التحول في خصائص القوة,مكتبة الإسكندرية, مصر,٢٠١٤م, ص٢٥.

2– Oona' A.Hathway, Rebecca Crootof, Philip Levtiz, aley Nix, Aileen Nowlan, William Perdue and Julia Spiegel, "The Law of Cyber– Attack", California Law

[٣] – منير البعلبكي , المورد: قاموس إنكليزي–عربي، دار العلم للملايين، بيروت, ٢٠٠٤م ,ص ٢٤.

[٤]– أحمد عبيس نعمة الفتلاوي،الهجمات السيبرانية مفهومها والمسؤولية الدولية ، السنة ٨ ، ٢٠١٦ ، ص ٦١٦ .

[٥] – حكيم غريب، صبرينة شرقي، تداعيات – الحرب الإلكترونية على العلاقات الدولية : د راسة في الهجوم الإلكتروني على إيران(فيروس ستكنست) ، دفاتر السياسة والقانون، المجلد 12 ، العدد 2 ، 2020 ، ص96 .

[٦] – سعيد درويش، "الحروب السيبرانية وأثرها على حقوق الإنسان: دراسة على ضوء أحكام دليل " تالين""، المجلة – الجزائرية للعلوم القانونية والاقتصادية والسياسية، المجلد ٥٤ ، العدد ٥ ، ٢٠١٧ ، ص ١٨١.

[٧] – د. علي حسين باكير , الحروب الالكترونية في القرن الواحد والعشرين , دون طبعة , مركز الجزيرة للدراسات, قطر , ٢٠١٠, ص٢٣.

[٨] – د. أحمد عبيس نعمة الفتلاوي: مصدر سابق، ص١٢.

[٩]– مكتب الأمم المتحدة المعني بالمخدرات والجريمة: "تقرير الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها"، فيينا، ٢٠١٣، الوثيقة: UNODC/CCPCJ/EG.4/2013/2.

10 – 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.

[11]– Evelyne AKOTO, Op.Cit, p. 14.

[١٢]– إيهاب خليفة، كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت،العربي للنشر والتوزيع،القاهرة، – ٢٠١٧ ، ص ٢١ .

13- – Stuxnet est un ver qui ferait partie d'un programme secret américain intitulé Olympic Games104. 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.

[١٤] – أحمد عبيس نعمة الفتلاوي، المرجع السابق، ص – ٦٢٦.

[١٥]– عادل عبد الصادق، أمريكا وتشكيل قيادة عسكرية في الفضاء الإلكتروني , هل بدأ الاستعداد لحروب المستقبل؟ ٢٠٠٩ ،العدد ١٣.

[١٦] – د/ عادل عبد الصادق، المرجع السابق , ٢٠١١م, ص٥٦.

[١٧]– موسى، طالب حسن، أعمر، عمر محمود،الإنترنت قانونا، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة، العدد ٦٧, ص٣٤٠.

-18-Lavenue,J.,(1996),Cyberspace ET Droit Internationalp. 830.

[١٩]– ب – حسن موسى، عمر محمود أعمر، "الإنترنت قانونا"، مرجع سابق, ص٨.

20 – Brown, D., (2006), Proposal for an international Vol.47, p. 179.

[٢١]– محمود أعمر،الحرب الإلكترونية في القانون الدولي الإنساني,مرجع سابق ص١٣٧.

[٢٢]– وستبي، جودي ر، دعوة إلى الاستقرار الجيوسيبراني، البحث عن السلام السيبراني، للعلماء، ٢٠١١م . ص ٦٤.

[٢٣]– توريه، حمدون , الاستجابة الدولية للحرب السيبرانية، البحث عن الامن السيبراني، ٢٠١١, ص٨٩.

[٢٤]– هناك من يدعي أن نص المادة ٢ فقره ٤ من ميثاق الأمم المتحدة ينطبق فقط على التهديد أو الاستخدام الفعلي للقوة المسلحة:

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

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

[٢٦]– ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟، مقال منشور على موقع اللجنة الدولية للصليب الأحمر، تمت الزيارة بتاريخ ٤ / ٩ / ٢٠٢٢ م، متاح على الرابط –https://www.icrc.org/ar/doc/resources/documents/faq/130628 cyber-warfare-q-and-a-eng.htm.

27- Koh, H., (2012), International Law in Cyberspace, Harvard International, volume 54, p.3.

[٢٨]– مايكل ن. شميت، "الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر (الحاسوب)والقانون أعداد ٢٠٠٢ م ، ص ٩.

[٢٩]– احمد عبيس نعمة الفتلاوي, الهجمات السيبرانية، المرجع السابق. ص٤٩.

[٣٠]– علوان، عبد الكريم ، الوسيط في القانون الدولي العام، دار الثقافة، عمان، ٢٠٠٦م , ص ٣٤.

[٣١]– اتفاقيات جنيف الاربعة ١٩٤٩م, البروتوكول الاضافي الاول لعام ١٩٧٧م, المادة ٣٦.

[٣٢]– وضع مايكل سميث:.Schmitt,M., (2012), Classification of Cyber Conflict Law, 17(2), P. 245-260

[٣٣]– في حال وقوع هجمات الكترونية من دولة فان الدولة المعتدى عليها الحق في الدفاع عن نفسها استناداً لنص المادة ٥١

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

36– Roscini, M., World Wide Warfare –Jus ad bellum and Use of Cyber Force, p. Cit. p. 115.

37-Green, J., (2015), Cyber warfare: a multidisciplinary analysis, (1st EditionP. 126.

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

[٣٨]– قرارالجمعية العامة ٣٣١٤ مع تعريف العدوان المرفق به، في ١٤ كانون الأول /ديسمبر, ١٩٧٤م.

[٣٩]– هينين ويجنر، مفهوم بشأن السلام السيبراني، البحث عن السلام السيبراني، البحث عن السلام السيبراني، الناشر الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء، ص٧ .