Journal Of the Iraqia University (73-4) February (2025)

ISSN(Print): 1813-4521 OnIine ISSN:2663-7502
Journal Of the Iraqia University
available online at: https://www.mabdaa.edu.iq

مفهوم الهجمات السيبرانية وطبيعتها القانونية

هاشم حسين علي كاظم الحسون طالب دكتوراه في القانون الدولي العام

جامعة قم ، كلية القانون ، قم ، ايران

الاستاذ المشارك في القانون الدولي د. غلامعلى قاسمى

The concept of cyber attacks and their legal nature

hashimalhasoon1@gmail .com
g.ghasemi43@gmail.com
Hashim hussein ali kadhim alhasoon Dr. Gholamali Ghasemi
Phd student in public International Law… Associate Professor of International Law
Qum Univerzity , faculty of law , Com , Iran
… Qom University, Faculty of Law, Qom, Iran
hashimalhasoon1@gmail .com …
g.ghasemi43@gmail.comg.

Abstract

As a result of the emergence and development of cybercrimes, the methods in which amed conflicts take place have changed in recent years, as the field of modern battles has moved from the physical domain (classical wars) to a virtual domain technically called cyberspace, and the wars taking place in it are called cyber war, or cyber attacks,which can cause the total or partial destruction of the opponent's digital infrastructure,and cause disastrous effects on military and civilian facilities , and all aspects of life in them such as power stations , airports , banks , dams and all other branches of the economy , all of this without the need to enter into any real and phisycal clash with the opponent and without the need to bear the financial burdens and risks of armed confrontation that the attacker bears in the context of using conventional weapons ,and the difficulty of knowing the identity of the attacker and his ideological background and other characteristics that make these attacks extremely dangerous .**keywords:** cyber ,cyber attacks ,cyber war , legal nature , international law , international humanitarian law .

المستخلص

نتيجة نشوء وتطور الجرائم السيبرانية ، تغيرت الطرائق التي تجري فيها النزاعات المسلحة في السنوات الأخيرة ، إذ انتقل ميدان المعارك الحديثة من المجال المادي (الحروب الكلاسيكية) إلى مجال افتراضي يسمى اصطلاحاً الفضاء السيبراني "cyberspac" والحروب التي تجري فيه تسمى بالحرب السيبرانية "cyber war" ، أو الهجمات السيبرانية"cyber attacks" ، ومن شأنها إحداث تدمير كلي أو جزئي للبنية الرقمية التحتية للخصم ، وتتسبب بآثار فادحة على الأعيان العسكرية والمدنية ، وشل كل مظاهر الحياة فيها كمحطات الكهرباء والمطارات والبنوك والسدود وسائر فروع الإقتصاد الأخرى ذلك كله من دون الحاجة إلى الدخول في أي اشتباك حقيقي ومادي مع الخصم ومن دون الحاجة لتحمل أعباء مالية ومخاطر المواجهة المسلحة التي يتحملها المهاجم في إطار استخدام الأسلحة التقليدية ، وصعوبة معرفة هوية المهاجم والخلفية الآيديولوجية له وغيرها من الصفات التي تجعل من هذه الهجمات شديدة الخطورة**الكلمات المفتاحية:** السيبرانية ، الهجمات السيبرانية، الحرب السيبرانية، الطبيعة القانونية ، القانون الدولي، القانون الدولي الانساني .

المقدمة

بيان المسألة

دخلت التكنولوجيا والأنترنت في مختلف مجالات الحياة ، بل أصبح استخدامها ضرورة لا غنى عنها في جميع القطاعات الخاصة والعامة في تبادل المعلومات وتقديم الخدمات النوعية الكبيرة والتواصل بين البشرويعد هذا الجانب إيجابي وبحق ، لكن كان لهذا التطورجانب سلبي ووجه مظلم ، تمثل باستخدام تلك التقنيات والبرمجيات في استحداث نوع جديد من الإجرام ، أحدث نتائج بالغة الخطورة على الأفراد والمجتمعات وأمن المجتمع الدولي عامةً ، تمثلت بما يسمى الهجمات السيبرانية (Cyber attack) ، وبدأ يلوح شبح التهديد بالهجمات السيبرانية أكثر من أي وقت مضى ، فكلما زاد تطور ثورة المعلومات والتكنولوجيا تزايد معها التعرض للهجمات السيبرانية وإحداث دمارللبنى التحتية لدول تراها معادية لاسيما البنى التحتية للأعيان المدنية الضرورية لحياة المدنيين، ومن دون عناء ، بعد أن كان النظام التقليدي يعتمد على القوة العسكرية البشرية لمواجهة الدول الأخرى أو السيطرة عليها برا أو جوا أو بحرا ويكلفها الكثير من الخسائر البشرية والمادية .

أهمية البحث

تبرز أهمية هذا البحث من خلال إلقاء المزيد من الضوء على مفهوم الهجمات السيبرانية والتي شغلت حيزا كبيرا من الإهتمام في المحافل الدولية والأكاديمية معا ، وأصبحت هاجس العصر والذي جعل منها الموضوع المتصدرمن بقية المواضيع الأخرى والتي تدعى بالتحديات المعاصرة للقانون الدولي العام والقانون الدولي الإنساني والتكييف القانوني لها .

أهداف البحث

يهدف البحث إلى :

١. التعرف على مفهوم الهجمات السيبرانية ومالذي يميزها عن الحرب السيبرانية .

٢. الطبيعة القانونية للهجمات السيبرانية والتحديات الراهنة التي يواجها المختصون في القانون الدولي العام .

مشكلة البحث

إن مشكلة البحث تكمن في السؤال الآتي :

. ماهو مفهوم الهجمات السيبرانية وماهي طبيعتها القانونية وفقا للقانون الدولي العام والقانون الدولي الإنساني ؟

منهجية البحث

تم إعتماد المنهجين الوصفي و التحليلي للدراسة مفهوم الهجمات السيبرانية وطبيعتها القانونية

خطة البحث

تم تقسيم خطة البحث إلى مطلبين تناولنا في المطلب الأول إلى مفهوم الهجمات السيبرانية والذي قسم إلى فرعين تناولنا في الفرع الأول منه تعريف الهجمات السيبرانية واما الفرع الثاني تناولنا فيه التمييز بين الهجمات السيبرانية والحرب السيبرانية ، أما المطلب الثاني تناولنا فيه الطبيعة القانونية للهجمات السيبرانية والذي تم تقسيمه إلى فرعين تناولنا في الفرع الأول منه إلى الطبيعة وفق قواعد القانون الدولي العام ، والفرع الثاني تناولنا فيه الطبيعة القانونية وفق قواعد القانون الدولي الإنساني ، ثم ختمنا بحثنا بالإستنتاجات والتوصيات.

المطلب الأول مفهوم الهجمات السيبرانية

مع تحول الفضاء الإلكتروني إلى ساحة للتفاعلات الدولية ، برز العديد من الأنماط التوظيفية له ، سواء على صعيد الاستخدامات ذات الطبيعة المدنية أو العسكرية الأمر الذي جعل هذا الفضاء مجالا للصراعات المختلفة ، سواء للفاعلين من الدول أو غير الدول لحيازة أكبر قدر من النفوذ والتأثير السيبراني في هذا السياق ، وتبلورت ظاهرة "الهجمات السيبرانية"، التي إتسمت بخصائص مختلفة عن نظيراتها التقليدية ، من حيث طبيعة الأنشطة العدائية والفواعل والتأثيرات في بنية الأمن العالمي، وعبرت تلك الهجمات عن نمطين من القوة (الناعمة والصلبة) في عملية توظيف التفاعلات في الفضاء الإلكتروني، مما يعكس تنامي القدرات والتهديدات المتصاعدة لأمن البنية التحتية الكونية للمعلومات[1]فشهد العالم في السنوات الأخيرة سباق تسلح جديد وغير تقليدي ، يقوم على إنشاء وتطوير برامج تقنية متقدمة تستخدم لأغراض متنوعة في عالم افتراضي يسمى اصطلاحاً "السايبر" (Cyber) ، ويُقصد بالفضاء السايبر أو الفضاء السيبراني (Cyberspace): هو المجال الرقمي والإلكتروني الذي يمتد عبر مختلف خطوط وقنوات الاتصال المعدنية والبصرية والجوية في الأنترنت ، فهو الحيز المادي وغير المادي الذي يتكون أو ينشأ من جزء أو من مجموع الحواسيب ، وشبكات المعلومات المحوسبة ، وبرامج ومضامين ومعطيات مرور ورقابة والذين يستخدمون كل ذلك. ويُعرف أيضا بأنه مجال يتميز

باستخدام الإلكترونيات والطيف الكهرومغناطيسي لحفظ البيانات وتعديلها وتبادلها بواسطة أنظمة الشبكة والبنية التحتية المرتبطة بها[2]وللفضاء السيبراني خصائص عديدة في نطاق الحروب والنزاعات تستطيع الدولة أو الأفراد من خلالها توجيه هجمات بسرعة عالية ضد الأعداء الموجودين على مسافات بعيدة جداً دون تعريضهم للخطر، فأصبحت التهديدات السيبرانية من أهم التحديات التي يتوجب على الدول مواجهتها في العصر الحالي ، ومع تزايد الاعتماد على شبكة الإنترنت ، وخاصة في المجالات المرتبطة بالأمن القومي مثل الشبكات العسكرية والأمنية ، تزايد معها الحديث عن أهمية مواجهة هذه التهديدات ، وفي هذا السياق ظهر مفهوم الهجمات السيبرانية : وهي عبارة عن أعمال إلكترونية تقوم بها الدول أو الشركات التابعة لها ضد أنظمة وشبكات الكمبيوتر التابعة لدول أخرى لأغراض أمنية أو عسكرية[3].وعلى ضوء ما تقدم سوف نقوم بتقسيم هذا المطلب إلى فرعين نتناول في الفرع الأول منه تعريف الهجمات السيبرانية وفي الفرع الثاني سنتناول فيه التمييز بين الهجمات السيبرانية والحرب السيبرانية كالتالي :

الفرع الأول تعريف الهجمات السيبرانية

نظراً لحداثة مفهوم الهجمات السيبرانية ، لم يُحدد مفهومها بشكل واضح إلا مؤخراً فالهجمات السيبرانية مصطلح حديث ظهر في العقود الأخيرة نتيجة لثورة تكنولوجيا المعلومات ، ولم تكن الهجمات السيبرانية معروفة إلا في وقت قريب ، مما يشكل أحد أهم التحديات الراهنة التي يواجهها المختصون في القانون الدولي العام ، فيما يخص تحديد طبيعتها ، أو تعريفها تعريف موحد يمكن الاستدلال في ضوئه لتنظيم استخدامها بالحظر أو التقييد لمواجهة عواقبها الخطرة على الصعيد الإنساني ، 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[4].

تعريف الهجمات السيبرانية لغة :إنّ كلمة سيبرانية أو سايبر أو سيبراني تعتبر ترجمة حرفية لكلمة (Cyber) والمشتقة من كلمة (Cybernetics)، **و**عرف قاموس مصطلح الأمن المعلوماتي السيبرانية بقوله : هجوم سيبراني عبر الفضاء الالكتروني يهدف الى السيطرة على المواقع الالكترونية ، أو البنى المحمية الكترونياً لتعطيلها ، أو تدميرها أو الاضرار بها [5]ونجد في اللغة العربية أن مصطلح السيبرانية هو مصطلح مستخدم في اللغة الإنجليزية (Cyber) ، ولا يوجد مصطلح يناظره أو يقابله في اللغة العربية ، لهذا واجه المتخصصون في اللغة العربية صعوبات في اختيار مصطلح مقارب لمصطلح (Cyber) في اللغة الإنجليزية ، حتى إن بعض الترجمات العربية لهذا المصطلح كانت في أغلبها غير صائبة ، وهذا ما نجده في الترجمة غير الصائبة التي تناولت ترجمة عنوان: "إتفاقية أوروبا المتعلقة بالجريمة السيبرانية"، إذ تم ترجمتها إلى اللغة العربية "الاتفاقية المتعلقة بالجريمة الإلكترونية"[6].

تعريف الهجمات اصطلاحاً:أختلفت التعريفات التي تناولت مصطلح الهجمات السيبرانية على ضوء الاجتهادات الفقهية، والممارسات العملية الدولية،، فيعتبر جانب من الفقه إن الحرب السيبرانية هي امتداد للحروب التقليدية والمادية ، إذ يتألف جندها من المدنيين والعسكريين في آن واحد، كما إنها 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 الإقتصادية والعبث بالمحتوى التقني والرقمي وغيرها[7].ومن التعاريف الحديثة للهجمات السيبرانية نذكر تعريف مجموعة الخبراء 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 تتسب بإصابات أو وفيات للبشر، أو تلف وضرر للأشياء المادية[8] .

الفرع الثاني تمييز الهجمات السيبرانية عن الحرب السيبرانية

مع تشابه هذه الممارسات باعتبارها تتم إلكترونياً متماثلة أو مترادفة ، فلكل منها خصائص مميزة وقد يؤدي الخلط بينها إلى صعوبة أكاديمية ، تتمثل في عدم معالجته أو دراستها بشكل صحيح، وصعوبات عملية تتعلق بكيفية الرد المقبول قانوناً من جانب الدول على كل منها ، وكذلك صعوبات تشريعية ، حيث تقوم معظم الدول بتنظيم تلك العمليات وطنياً[9]عُرفت الحرب السيبرانية بأنها امتداد للسياسة من خلال إجراءات وأفعال ترتكب في فضاء السايبر بواسطة الدولة أو الأطراف الفاعلة من غير الدولة والتي تشكل تهديداً خطيراً لأمن البلاد أو تجري في استجابة لتهديد محتمل ضد أمن الدولة ، أو هي تلك الإجراءات التي تتخذها الأطراف في النزاع لكسب الميزة على خصومهم في فضاء السايبر باستخدام مختلف الأدوات التكنولوجية والأشخاص التقنيين ، وتحصل المزايا من خلال إتلاف أو تدمير أو تعطيل أو اغتصاب أنظمة الحاسوب للعدو (الهجمات

السيبرانية) أو من خلال الحصول على معلومات يرغب العدو في أن تبقى سرية (التجسس السيبراني أو الاستغلال لشبكات الحاسوب) ، وفي الواقع إن الحرب السيبرانية تهدف الى الإخلال بتوازن المعلومات والمعرفة لصالح القوات الصديقة ، لاسيما في غياب التوازن العسكري ، وعليه إن استخدام التفوق العلمي في الحرب السيبرانية سيغطي النقص في التجهيزات والقوات العسكرية وبالتالي يمكن تحقيق النصر فيه، وقد جاء تعريف الحرب السيبرانية في قاموس جامعة كامبريدج بأنها " أي نشاط يستخدم الإنترنت لمهاجمة الأجهزة الإلكترونية التابعة لدولة ما بقصد الإضرار بأشياء كأنظمة الإتصالات والنقل وموارد المياه والطاقة إن إستخدام الحرب السيبرانية قد يؤدي الى زعزعة استقرار الأنظمة المالية ، نظام الهاتف أو شبكة الكهرباء ، وقد يغير الأمن القومي بشكل جذري بسبب هجوم قد يأتي من أي مكان ، وفي تعريف أخر عرفت بأنها: الإستعمال الدفاعي أو الهجومي للمعلومات وأنظمتها بقصد تعريض عناصر المعلومات والعمليات القائمة على المعلومات ، والأنظمة المعلوماتية لشبكات الإنترنت التابعة للعدو في الفضاء السيبراني للخطر[10]وصعوبة التوصل ومعرفة مصدر الحرب السيبرانية تشكل عامل اختلاف آخر وذلك لتعدد الجهات الفاعلة في الفضاء السيبراني كالدول والمنظمات والجماعات الحكومية وغير الحكومية والإرهابيين والقراصنة وحتى الأفراد[11] .

المطلب الثاني الطبيعة القانونية للهجمات السيبرانية

تعد الهجمات السيبرانية ذات طبيعة خاصة ، نظراً للخطورة التي تتسبب بها هذه الهجمات على المستوى الدولي ، والخسائر المادية والبشرية التي تتسبب في إحداثها ، وتتميز هذه الهجمات بصعوبة اكتشافها ، فمرتكب الهجوم السيبراني يمكنه ارتكاب الهجمة في أماكن ودول وقارات مختلفة فهذه الهجمات عابرة للحدود، كذلك فإن قدرة مرتكب الهجمة السيبرانية على تدمير دليل الإدانة في أقل من الثانية الواحدة يشكل عاملاً إضافيًا في صعوبة اكتشاف الهجمات السيبرانية؛ وإذا ما تم اكتشافها فمن الصعب إثباتها فالهجمات السيبرانية تتم في إطار أو محيط غير تقليدي، حيث تقع خارج إطار الواقع المادي الملموس ، لتقوم أركانها في بيئة نظم الحاسوب والبيئة الرقمية المعلوماتية ، مما يجعل الأمور تزداد صعوبة وتعقيداً [12] كما تتمثل الطبيعة الخاصة للهجمات السيبرانية في قدرة الشبكات المعلوماتية على نقل وتبادل معلومات ذات طابع شخصي وعام في آن واحدمع ما يتبع ذلك من اعتداء على الخصوصية، وتعريض تلك البيانات والمعلومات لخطر الهجوم السيبراني عليها من خلال عمليات القرصنة والتسلل والاختراق السيبراني التي تهدف إلى التجسس على تلك البيانات والمعلومات أو اختلاسها وسرقتها أو إتلافها ومحوها وتدميرها؛ ويسهل ذلك توسع بنوك المعلومات بأنواعها التي لا حصر لها في وقتنا الحالي ، علاوة على توسع الأفراد والحكومات وكافة الكيانات والمنظمات والمؤسسات على مستوى العالم وسعيهم إلى ربط حواسيبهم بهذه الشبكات المذكورة؛ مما يجعل من هذه المعلومات غنيمة سهلة لمرتكبي الهجمات السيبرانية[13] فاللجوء المتزايد للدول إلى استخدام الهجمات السيبرانية في نزاعاتها ، جعل قواعد القانون الدولي بصدد اختبار حقيقي ومعقد حول مدى إمكانية تطبيق تلك القواعد الإنسانية الدولية التي قُننت قبل عقود من الزمن على الهجمات السيبرانية ، التي لم يتجاوز عمرها اكثر من عقد من الزمن[14]وبناء على ما سبق سنبحث مسألة الطبيعة القانونية للهجمات السيبرانية في فرعين ندرس في الفرع الاول طبيعة الهجمات السيبرانية وفق قواعد القانون الدولي العام ونخصص الفرع الثاني لدراسة طبيعة الهجمات السيبرانية وفق قواعد القانون الدولي الانساني.

الفرع الأول الطبيعة وفق قواعد القانون الدولي العام

لم ينظم القانون الدولي صراحة مسألة الهجمات السيبرانية سواء وقت السلم أو الحرب، وهذا راجع إلى الاستعمال الحديث نسبياً لشبكات الإنترنت ، بينما قواعد القانون الدولي التي تحكم العلاقات الدولية يرجع تاريخها إلى ما قبل وجود الفضاء السيبراني وبالتالي فقواعده قد لا تتلائم والتكنولوجيات الجديدة للحرب[15] ، غير أن الاستخدام الواسع للفضاء السيبراني كساحة صراع جديدة بين الدول يؤدي إلى مزيد من التهديدات للسلم والأمن الدوليين، وفي ظل غياب نصوص قانونية خاصة في القانون الدولي العام حول هذه الهجمات ، وازدياد التقنيات الرقمية المتطورة من فعالية وانتشار للجريمة السيبرانية ، لذلك تسعى غالبية أعضاء المجتمع الدولي إلى توضيح طبيعة هذه الهجمات من أجل إيجاد الأطر القانونية الكافية لمواجهتها ، سواء كانت تمثل أنشطة هجومية لإلحاق الضرر والأذى بأنظمة وشبكات معلومات الخصم ، أم كانت أنشطة دفاعية لحماية نظم معلومات الخاصة بالدولة المعتدى عليها، الأمر الذي يتطلب معرفة طبيعتها القانونية من أجل تسهيل سبل تجريمها والعقاب عليها[١٦]تشكل الهجمات السيبرانية تهديداً لأحد المبادئ الرئيسة في القانون الدولي ، وهو احترام سيادة الدول ، بوصفه واجباً أساسياً وهو واجب عدم التدخل ، الذي نصت عليه الفقرة (٤) من المادة الثانية من ميثاق الأمم المتحدة ، لما فيها من تسريب لمعلومات أمنية وسرية عن حكومات الدول، وقدد يتجاوز الأمر ذلك وربما يصل إلى الإضرار بالمدنيين؛ وبالخصوص عندما تسبب مثل هذه الهجمات قطعاً للخدمات الحيوية كالماء والكهرباء لذلك عرف القانون الدولي هذا الهجوم بأنّه: "عملية إلكترونية سواء أكانت هجومية أم دفاعي ، يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الإضرار بالمنشآت أو تدميرها [١٧].لهذا فإن وضع الهجمات السيبرانية في الإطار القانوني الدولي القائم على افتراض أنها مناسبة لهذا الغرض أمر صعب جداً؛ وذلك

بسبب الطبيعة الخاصة لها، والخصائص الفريدة من نوعها التي تتميز بها الهجمات السيبرانية، فضلاً عن وجود بيان قانوني رسمي ونهائي بشأن هذه المسألة، كل ذلك يجعل التساؤل قائماً حول أي أنموذج قانوني يجب أن يضم إطار الهجمات السيبرانية؟ والحق إن هذا التساؤل في حد ذاته مسألة نقاش كبيرة جداً ، ومحل اختلافات شائكة في مجال الحقوق القانونية والمسؤوليات التي تنتج عن تلك الهجمات[١٨].

الفرع الثاني الطبيعة وفق قواعد القانون الدولي الانساني

عرف القانون الدولي الإنساني مصطلح "الهجمات" بأنها أعمال عنف موجهة ضد عدو أو خصم سواء كانت هجومية أو دفاعية ، دون النظر إلى المنطقة التي يتم فيها تنفيذ تلك الأعمال، وهذا ما نص عليه البروتوكول الإضافي الأول لاتفاقيات جنيف لعام ١٩٧٧[١٩]، وبالتالي فان الهجمات السيبرانية موضوع البحث ، وبحسب التعريف السابق فهي لا تعتبر هجوماً لأن أعمال الهجمات السيبرانية هي عبارة عن القرصنة واختراق البيانات الإلكترونية ، حتى لو كانت موجهة للخصم بالهجوم أو الدفاع ، ولكن لا يمكن وصفها بأنها أعمال عنف ، وبالتالي وفقاً لبرتوكول ١٩٧٧ لا يمكن وصف الأنشطة السيبرانية بأنها هجمات عدائية ، ولكن لا يمكن النظر إلى المادة ٤٩ من البرتوكول المذكور، دون باقي أحكام البروتوكول ، الذي نص على القواعد الأساسية التي تحكم الهجمات في مواد أخرى ، والتي تنطبق إلى حد كبير مع الهجمات السيبرانية ، وعلى سبيل المثال ما نصت عليه المادة ٤٨ من البرتوكول ، والتي تفرض على المتنازعين التمييز بين المدنيين والمقاتلين وبين الأعيان المدنية والعسكرية ، أي تحظر شن أي نوع من الهجمات مهما كانت وسائلها وماهيتها[٢٠]وهذا ما أكدته القاعدة السابعة الواردة في القانون الدولي الإنساني التي تنص على ان يميز أطراف النزاع في جميع الأوقات بين الأعيان المدنية والأهداف العسكرية[٢١] ، وأيضاً ما أوردته المادة (٥١) في الفقرة الثانية بخصوص حظر الهجمات ضد السكان المدنيين الرامية أساسا الى نشر الرعب بينهم[٢٢]وبالتالي يتبين أن أعمال العنف تأخذ صورتين[٢٣]: الأولى أن تكون مباشرة وتؤدي بطبيعتها إلى إلحاق أذى مادي بالأعيان العسكرية والمدنية ، أو غير مباشرة أي تُلحق الأذى بعد وقوع الهجوم أيا كانت الوسيلة أو الطريقة.وفق ما تقدم فإن التركيز على آثار النشاط السيبراني وجسامته سيبين لنا إن وصف الهجوم متحقق فيه ، على سبيل المثال عندما تتعرض الحواسيب أو الشبكات في دولة ما للهجوم السيبراني ، فقد يؤدي ذلك الى حرمان المدنيين من الإحتياجات الأساسية كمياه الشرب والرعاية الطبية والكهرباء.ويمكن أن تتدخل النشاطات السيبرانية في تعطيل خدمات إنقاذ الأرواح كالمستشفيات أو أن تعطل البنى التحتية الحيوية مثل السدود والمفاعلات النووية وأنظمة التحكم في الطائرات ، وجراء كل هذا قد يتضرر مئات الآلاف من السكان[٢٤] فهذه النشاطات وعلى وفق جسامتها وآثارهاشهدت الأعوام الماضية إدخال تقنية واسعة من التكنولوجيا الحديثة إلى ساحة المعركة ، وأوجد الفضاء المعلوماتي ميداناً جديداً للقتال ومدى خضوع هذه العمليات الالكترونية الى القانون الدولي الإنساني ، وهل توجد قواعد قانونية في القانون الدولي النافذ قادرة على مواءمة التحديات التي يفرضها استخدام هذه الاسلحة الجديدة في النزاع المسلح الحديث والتي لا تتقاتل خلالها الجيوش النظامية أو فئات مسلحة تكون منظمة أخرى، لهذا تطرق العديد من فقهاء القانون الدولي إلى موضوع الحروب السيبرانية فطرحوا عدداً 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 .

الخاتمة

الإستنتاجات:

١. ليس من المستغرب أن يتربع اليوم موضوع الهجمات السيبرانية على قمة الدراسات القانونية ،إذ لايوجد إتفاق دولي لغاية الآن بشأن تعريف الهجمات السيبرانية لأنها من المفاهيم الحديثة ، مايؤدي إلى صعوبة تكييفها وتحديد مرتكب الجريمة.

٢. لابد من إحترام سيادة كل دولة ، حيث أصبح يعرف بـ "الحدود الأتكترونية" أوِ "السيادة الألكترونية" (la souverainete cybernetique)، المنصوص عليها في المادة رقم 1 من دليل تالين (وهو الصك الوحيد الذي عالج هذا الموضوع) ، أي سلامة البنى التحتية السيبرية للدولة من الهجمات الإلكترونية .

٣. نظرا للتطور السريع للهجمات والحروب السيبرانية وأصبحت تهدد السلم والأمن الدوليين ، من خلال المساس بالأمن السيبري المعتمد في التجارة الدولية وفي كل مجالات العلاقات الدولية، لذلك لابد من واجب المجتمع الدولي تفعيل أحكام ميثاق الأمم المتحدة المعنية بهذا الشأن .

٤. إن مايميز الحروب السيبرانية عن الحروب التقليدية هو في إنخفاض تكاليفها وسهولة اللجوء إليها إذ لا تتطلب جيشا من المقاتلين العسكريين وأسلحة ومعدات ، فقط إستخدام الأسلحة الألكترونية مثل الفيروسات وأسلحة التجسس ، وقرصنة معلومات عسكرية واستراتيجية .

٥. إن المهاجمين السيبرانيين غالبا مايستخدمون برامج تخفي مايؤدي إلى صعوبة الوصول إلى مصدر الهجوم ، لكن هذا لايعني هناك فراغ قانوني

تماما وإفلات المجرم من العقاب ، فيمكن الإستناد إلى آراء وقرارات محكمة العدل الدولية ، كرأيها بشأن مشروعية التهديد بالأسلحة النووية أو إستخدامها .

التوصيات :

١. نتيجة قصور القانون الدولي في هذا المجال وعدم وجود أساس قانوني يحكم استخدام الحرب الألكترونية ، أصبح من الضرورات الواجبة من قبل خبراء القانون تطوير القانون الدولي تزامنا مع التطور الكبير في تكنولوجيا المعلومات ومعالجة هذا القصور.

٢. إدخال موضوع الفضاء السيبراني والمخاطر التي تنتج عنه وتدريسه في ميدان جميع المؤسسات الأكاديمية وعلى المستوى الدولي ، وعلى المجتمع الدولي إتخاذ خطوات جدية بشأن مكافحة تلك الهجمات السيبرانية .

٣. الحفاظ على سرية المعلومات والبيانات والتصدي للهجمات السيبرانية من خلال إرساء بنية تحتية في مجال البرمجيات ، وفصل البنية التحتية والشبكات السيبرانية العسكرية عن المدنية وذلك لحماية السكان المدنيين من أي هجوم سيبراني معادي يحصل من الطرف الآخر .

قائمة المصادر والمراجع

أولا: الكتب.

١. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنا في ضوء التنظيم الدولي المعاصر، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، ٢٠١٨.

٢. بول روبنسون، قاموس الأمن الدولي، منشورات مركز الإمارات للدراسات والبحوث الإستراتيجية، أبوظبي، ٢٠٠٩.

٣. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجية الحديثة للجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، ١٩٩٢.

٤. حامد محمد علي البلداوي، الهجمات السيبرانية، (اضرارها واثارها ومواجهتها في قواعد القانون الدولي الانساني)، الطبعة الاولى، المركز العربي للدراسات والبحوث العلمية، القاهرة، ٢٠٢٤.

٥. خالد وليد محمود، الهجمات عبر الأنترنت ساحة الصراع الإلكتروني الجديدة، المركز العربي للأبحاث ودراسة السياسات، الدوحة، ٢٠١٣.

٦. سليم عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الأنترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، ٢٠١١.

٧. علي محمد كاظم الموسوي، المشاركة المباشرة في الهجمات السيبرانية، الطبعة الأولى، منشورات شركة المؤسسة الحديثة للكتاب، بيروت، ٢٠١٩.

ثانيا: الابحاث والمجلات.

١. أسامة صبري محمد ،الحرب الالكترونية ومبدأ التمييز في القانون الدولي الإنساني، مجلة القانون للدراسات والبحوث القانونية، العدد السابع، ٢٠١٣.

٢. جون – ماري هنكرتس و لويزدوز والد بك، القانون الدولي الإنساني العرفي اللجنة الدولية للصليب الأحمر ، المجلد الأول.

٣. حسام عبد الأمير خلف، البعد الجديد_ الخامس_ في النزاعات المسلحة القضاء الإلكتروني، مجلة كلية الحقوق العدد الاول، جامعة النهرين، العراق، ٢٠١٦.

٤. حكيم غريب، صبرينة شرقي، تداعيات الحرب الإلكترونية على العلاقات الدولية، دراسة في الهجوم الإلكتروني على إيران، (فيروس ستكنست)، دفاتر السياسة والقانون، المجلد الاول، العدد الثاني، ٢٠٢٠.

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

٦. عبد الصادق عادل، القوة الإلكترونية أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، مجلة السياسة الدولية، ٢٠١٥.

٧. عمر محمد أعمر ، الحرب الإلكترونية في القانون الدولي الإنساني، دراسات علوم الشريعة والقانون ١٣٦، المجلد ٤٦، العدد الثالث، ٢٠١٩.

٨. محمد السعيد رشدي، الإنترنت والجوانب القانونية لنظم المعلومات، بحث مقدم إلى مؤتمر الإعلام والقانون كلية الحقوق، جامعة حلوان، خلال الفترة من ٩-١٠ مارس ١٩٩٩.

٩. ياسر فيصل أمين، جرائم الإرهاب عبر الوسائل الإلكترونية "دراسة مقارنة" الجمعية المصرية للاقتصاد السياسي، مجلة مصر المعاصرة، بدون سنة نشر.

ثالثاً: الاتفاقيات الدولية.

١. البرتوكول الإضافي الأول لاتفاقيات جنيف لعام ١٩٧٧.

٢. اللجنة الدولية للصليب الاحمر، الملحقان" البروتوكولان الإضافيان الى إتفاقية جنيف المعقودة في ١٢ آب / اغسطس ١٩٤٩.

رابعاً: المواقع الالكترونية.

١. سند راهبردي بدافند سايبري كشور، سازمان بدافند غير عامل كشور، مركز بدافند سايبري كشور

٢. سور على الموقع الالكتروني التالي: http://d--padafand.farsp.ir/upload/96/att-pdf .

٣. الموقع الرسمي شركة نورتون التدرج المروع للجرائم الإلكترونية (٢٠١٢)، متوفر على الرابط الالكتروني التالي: .www.nowstatic.com

٤. لوران جيزيل، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية، اللجنة الدولية للصليب الاحمر، ٢٨/٦/٢٠١٣، متاح على الموقع الالكتروني التالي:https://www.ICrc.org.Cyber-warefare

خامساً: المراجع الاجنبية.

١. كاوه سيد مفيدي، جنك سايبري، سكيور تاركيت، مارس، ٢٠٠٤.

٢. قاسم ترابي، تكامل راهبرد ناتو در قبال جنگ سايبري دلايل، أبعاد و مؤلفة ها، تاريخ دريافت ١٤/٢/١٣٩٤ (٢٠١٥) فصلنامه مطالعات راهبردي سال هجدهم شماره اول بهار ١٣٩٤ (٢٠١٥)، شماره مسلسل ٦٧، تاريخ بذيرش ١٨/٤/١٣٩٤ (٢٠١٥).

3.Richard Kissel (2013), Glassory of Information Security Terms, National Institute of Standers and technology, U. s Department of Commerce.

4.U. S. Department of Defense (2010), Dictionary of Military and Associated Terms, Joint Publication 1-02, Nov. 8, (2010), as amended through Feb. 15, (2012).

هوامش البحث

(1) حامد محمد علي البلداوي، الهجمات السيبرانية، (اضرارها واثارها ومواجهتها في قواعد القانون الدولي الانساني)، الطبعة الاولى، المركز العربي للدراسات والبحوث العلمية، القاهرة، ٢٠٢٤، ص ٢١.

(2) خالد وليد محمود، الهجمات عبر الأنترنت ساحة الصراع الإلكتروني الجديدة، المركز العربي للأبحاث ودراسة السياسات، الدوحة، ٢٠١٣، ص ٤.

(3) سند راهبردي بدافند سايبري كشور، سازمان بدافند غير عامل كشور، مركز بدافند سايبري كشور ، ص ٢٤

سور على الموقع الالكتروني التالي: http://d--padafand.farsp.ir/upload/96/att-pdf .

(4) أسامة صبري محمد ،الحرب الالكترونية ومبدأ التمييز في القانون الدولي الإنساني، مجلة القانون للدراسات والبحوث القانونية، العدد السابع، ٢٠١٣، ص ٥.

(5)Richard Kissel (2013), Glassory of Information Security Terms, National Institute of Standers and technology, U. s Department of Commerce.

(6) عبد الصادق عادل، القوة الإلكترونية أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، مجلة السياسة الدولية، ٢٠١٥، ص ٢١٤.

(7) حكيم غريب، صبرينة شرقي، تداعيات الحرب الإلكترونية على العلاقات الدولية، دراسة في الهجوم الإلكتروني على إيران، (فيروس ستكنست)، دفاتر السياسة والقانون، المجلد الاول، العدد الثاني، ٢٠٢٠، ص٩٦.

(8) سعيد درويش، الحروب السيبرانية وأثرها على حقوق الإنسان، دراسة على ضوء أحكام دليل " تالين"، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، المجلد ٥٤، العدد الخامس، ٢٠١٧، ص ١٨١.

(٩) حسام عبد الأمير خلف، البعد الجديد_ الخامس_ في النزاعات المسلحة القضاء الإلكتروني، مجلة كلية الحقوق العدد الاول، جامعة النهرين، العراق، ٢٠١٦، ص ١٢٦.

(10) كاوه سيد مفيدي، جنك سايبري، سكيور تاركيت، مارس، ٢٠٠٤، ص ٧.

(11) قاسم ترابي، تكامل راهبرد ناتو در قبال جنگ سايبري دلايل، أبعاد و مؤلفة ها، تاريخ دريافت ١٤/٢/١٣٩٤ (٢٠١٥) فصلنامه مطالعات راهبردي سال هجدهم شماره اول بهار ١٣٩٤ (٢٠١٥)، شماره مسلسل ٦٧، تاريخ بذيرش ١٨/٤/١٣٩٤ (٢٠١٥)، ص ١٣٩.

(12) محمد السعيد رشدي، الإنترنت والجوانب القانونية لنظم المعلومات، بحث مقدم إلى مؤتمر الإعلام والقانون كلية الحقوق، جامعة حلوان، خلال الفترة من ٩-١٠ مارس ١٩٩٩ مشار إلى لدى: ياسر فيصل أمين، جرائم الإرهاب عبر الوسائل الإلكترونية "دراسة مقارنة" الجمعية المصرية للاقتصاد السياسي، مجلة مصر المعاصرة، بدون سنة نشر، ص٥١٦.

(13) جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجية الحديثة للجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، ١٩٩٢، ص ١١.

(14) علي محمد كاظم الموسوي، المشاركة المباشرة في الهجمات السيبرانية، الطبعة الأولى، منشورات شركة المؤسسة الحديثة للكتاب، بيروت، ٢٠١٩، ص ١٣.

(15) عمر محمد أعمر ، الحرب الإلكترونية في القانون الدولي الإنساني، دراسات علوم الشريعة والقانون ١٣٦، المجلد ٤٦، العدد الثالث، ٢٠١٩، ص ١٣٦.

(١٦) بول روبنسون، قاموس الأمن الدولي، منشورات مركز الإمارات للدراسات والبحوث الإستراتيجية، أبوظبي، ٢٠٠٩، ص ٨٥.

(١٧) ينظر في ذلك الموقع الرسمي شركة نورتون التدرج المروع للجرائم الإلكترونية (٢٠١٢)، متوفر على الرابط الالكتروني التالي: www.nowstatic.com.

(18)U. S. Department of Defense (2010), Dictionary of Military and Associated Terms, Joint Publication 1-02, Nov. 8, (2010), as amended through Feb. 15, (2012).

(١٩) ينظر في تفصيل ذلك نص المادة ٤٩ من البرتوكول الإضافي الأول لاتفاقيات جنيف لعام ١٩٧٧.

(٢٠) سليم عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الأنترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، ٢٠١١، ص ٢٥.

(٢١) جون – ماري هنكرتس و لويزدوز والد بك، القانون الدولي الإنساني العرفي اللجنة الدولية للصليب الأحمر ، المجلد الأول، ص ٢٣.

(٢٢) اللجنة الدولية للصليب الاحمر، الملحقان" البروتوكولان الإضافيان الى إتفاقية جنيف المعقودة في ١٢ آب / اغسطس ١٩٤٩، ص ٤٠.

(٢٣) أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنا في ضوء التنظيم الدولي المعاصر، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، ٢٠١٨، ص ٧.

(٢٤) لوران جيزيل، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية، اللجنة الدولية للصليب الاحمر، ٢٨/٦/٢٠١٣، متاح على الموقع الالكتروني التالي:https://www.ICrc.org.Cyber-warefare