التكييف القانوني لدور المدنيين في الهجمات السيبرانية

أ.م.د فاضل عبد الزهرة فاضل

معهد العلمين للدراســـات العليا

Assistant Professor Dr. Fadel Abdel Zahra Fadel

El Alamein Institute for Postgraduate Studies

Legal adaptation of the role of civilians in cyber attacks

الكلمات الافتتاحية :

الهجمات السيبرانية. القانون الدولي الأنساني .المدنيين.

Keywords :

Cyber attacks International humanitarian law . Civilians.

Abstract : Cyber attacks are one of the most prominent challenges facing the world today, as they pose a real threat to individuals, companies, and institutions alike. As technology develops, these attacks become more diverse and complex, requiring a deep understanding of their nature, mechanisms, and effects. The technical and technological developments that the world has witnessed recently have led to wars entering a new era. Wars are no longer limited to their traditional patterns, as they have become cross-border without moving military armies in a way that is difficult to control by closing or securing borders. Indeed, even the training that the military armies used to

adopt on the ground, in which the fighter trains in special camps, has become at the present time and may later become more virtual or digital training. Rather, it is sufficient to train people on how to hack electronically and attack cyberly without resorting to those camps.

الملخص:

تعد الهجمات السيبرانية من أبرز التحديات التي تواجه العالم اليوم، فهي تشكل تهديدًا حقيقيًا للأفراد والشركات والمؤسسات على حد سواء. ومع تطور التكنولوجيا، أصبحت هذه الهجمات أكثر تنوعًا وتعقيدًا، مما يتطلب فهماً عميقًا لطبيعتها وآلياتها وتأثيراتها. فقد أدت التطورات التقنيَّة والتكنولوجية التي شهدها العالم مؤخراً إلى دخول الحروب حِقبةً جديدة. فلم تعُد الحروب تقتصر على أنمطها التقليدية، إذ أنها باتت عابرة للحدود دون تحريك جيوش عسكرية على نحو يصعب السيطرة عليها بغلق الحدود أو تأمينها. بل حتى التدريبات التي كانت الجيوش العسكرية تعتمدها على أرض الواقع بأن يتدرب المقاتل في معسكرات خاصة أصبحت في وقتنا الحالي وربما تصبح فيما بعد وبشكل أكبر تدريباً افتراضياً أو رقمياً وإنما يكفي تدريب الأشخاص على كيفية الاختراق الإلكتروني والهجوم السيبراني دون اللجوء إلى تلك المعسكرات.

المقدمة:

دخل العالم اليوم عصراً جديداً في إطار التقدم العلمي والتكنلوجي في مختلف المجالات، وكان لدخول التكنلوجيا الحديثة في ميدان التكنلوجيا العسكرية ، دور كبير في ايجاد نوع جديد من الأسلحة لم يستخدم في كافة الحروب التقليدية عُرِفت اصطلاحًا بالسايبر *(cyber)*. ولم يكن القانون الدولي الإنساني واتفاقيات جنيف الاربعة لعام ١٩٤٩ التي نظمت اوضاع النزاعات المسلحة قد عرفت الهجمات السيبرانية او وضعت ضوابط لها لحداثتها ، ومن الملاحظ ان الهجمات السيبرانية تعد سلاحاً غير منظور سواء استخدمت لمهاجمة اهداف مدنية او استخدمت لاغراض عسكرية ، سواء ارتكبت من قبل دول او جماعات او افراد ، لتحقيق اقصى ضرر لمنشأت العدو . كما ان القانون الدولي الأنساني لم يصنف الهجمات السيبرانية بوصفها وسيلة قتال او سلاح وذلك لحداثة وتطور الهجمات السيبرانية ولقدم القانون الدولي الإنساني الذي سبق ظهورها. وما يميز الهجمات السيبرانية سرعتها الزمنية بالتنفيذ ،

وشدتها في احداث التاثير والضرر لمنشأت العدو التي قد تصل الى ايقاف كل منظومة الحياة ، كما انها لاتتطلب معدات او منظومة صواريخ او منشأت نووية ، بل من الممكن جدا استخدام حاسوب او مجموعة معدات من قبل شخص ما يكون غالبا مجهول الهوية لاحداث الضرر في المنشأت المهاجمة . وتعتبر الهجمات السيبرانية من أبرز التحديات التي تواجه العالم اليوم، فهي تشكل تهديدًا حقيقيًا للأفراد والشركات والمؤسسات على حد سواء. ومع تطور التكنولوجيا، أصبحت هذه الهجمات أكثر تنوعًا وتعقيدًا، مما يتطلب فهماً عميقًا لطبيعتها وآلياتها وتأثيراتها. فقد أدت التطورات التقنيَّة والتكنولوجية التي شهدها العالم مؤخراً إلى دخول الحروب حِقبةً جديدة. فلم تعُد الحروب تقتصر على أنمطها التقليدية، إذ أنها باتت عابرة للحدود دون تحريك جيوش عسكرية على نحو يصعب السيطرة عليها بغلق الحدود أو تأمينها. بل حتى التدريبات التي كانت الجيوش العسكرية تعتمدها على أرض الواقع بأن يتدرب المقاتل في معسكرات خاصة أصبحت في وقتنا الحالي وربما تصبح فيما بعد وبشكل أكبر تدريباً افتراضياً أو رقمياً وإنما يكفي تدريب الأشخاص على كيفية الاختراق الإلكتروني والهجوم السيبراني دون اللجوء إلى تلك المعسكرات. أن لجوء كافة الدول الى سلاح الهجمات السيبرانية جعل قواعد القانون الدولي الأنساني امام اختبار دقيق يتمثل في امكانية تطبيق قواعده ومبادئه على هكذا نوعية من الحروب ، وكيفية تحديد المسؤولية الجنائية والمدنية الدولية عن الدول والشركات والافراد الذين يشنون هذه الهجمات . وبالتالي، فإن التنظيم الفعال للعمليات السيبرانية أثناء النزاع المسلح هو مسألة تهمّ جميع الدول، بغض النظر عن مستوى تطورها التكنولوجي، أو قدراتها العسكرية السيبرانية، أو مشاركتها في النزاعات المسلحة.

أهمية البحث(research importance): تكمن اهمية البحث كون الهجمات السيبرانية تعد تطور نوعي حديث في ميدان النزاعات المسلحة ، وان استخدامها كسلاح فعال يتعدى اثار كافة الاسلحة التقليدية ، كون السلاح السيبراني قد يؤدي الى ايقاف كل متطلبات الحياة ، وتبرز اهمية الموضوع في صعوبة تحديد المسؤولية الناتجة عن شن الهجمات السيبرانية وخصوصاً انها تستخدم من قبل افراد مدنيين يعملون لحسابهم الخاص ، او يتم الاستعانة بهم من قبل الدولة او يعملون في شركات خاصة .

إشكالية الدراسة(The problem of the study): لقد اصبحت الهجمات السيبرانية من السبل المؤثرة في النزاعات الحديثة ، خصوصا بعد ان كانت الحروب التقليدية تعتمد على القوة

العسكرية البشرية ، كما الهجمات السيبرانية ابرزت اشكالية قانونية بعدم وجود اطار قانوني ينظمها ومن هذا المنطلق يمكن ان تثارجملة من التسأولات إهمها:

١_ مدى انطباق القانون الدولي الانساني على الهجمات السيبرانية؟

٢_ مدى مسؤولية الافراد والشركات الخاصة عن قيامهم بشن الهجمات السيبرانية ؟

٣_ هل يمكن اعتبار الافراد الذين قاموا بالهجمات السيبرانية مقاتلين شاركوا في الأعمال القتالية المباشرة ومن ثم يمكن استهدافهم؟

منهجية الدراسة(Study methodology): سيتم اعتماد المنهج الوصفي والتحليلي لتحليل نصوص الاتفاقيات والمعاهدات ومدى انطباقها على الهجمات السيبرانية . وبيان الاراء والتطبيقات بخصوص هذا الموضوع .

هيكلية البحث(Research structure): سنناقش موضوع التكييف القانوني لدور المدنيين في الهجمات السيبرانية عبر مبحثين ، نتناول في المبحث الاول (مفهوم الهجمات السيبرانية) وعبر مطلبين نناقش في المطلب الاول (تعريف الهجمات السيبرانية) وفي المطلب الثاني نتناول (انواع الهجمات السيبرانية) ، ونتناول في المبحث الثاني (التكييف القانوني للهجمات السيبرانية المرتكبة من المدنيين) وعبر مطلبين نناقش في المطلب الاول (انطباق القانون الدولي الانساني على الهجمات السيبرانية) وفي المطلب الثاني نتناول (مسؤولية المدنيين عن الهجمات السيبرانية) . المبحث الأول: مفهوم الهجمات السيبرانيّة: لقد احدثت الثورة المعلوماتية نقلة نوعية في مجال استخدام نظم الحاسوب والشبكات لادارة مرافق البنى التحتية البلاد ومرافقها الحيوية ، الا ان ان الملاحظ ان العصر الحديث شهد استخداماً موسعا للهجمات السيبرانية سواء المجهة منها لالحاق اثار في الاعيان المدنية والثقافية للعدو او شل القدرة العسكرية للعدو من خلال شن هجمات القرصنة او التصيد الاحتيالي او بث البرامج الضارة التي تعرض امن انظمة الكومبيوتر والشبكات والاجهزة الالكترونية العائدة للعدو للخطر. لقد شهد العالم عدة أجيال من الحروب لغاية تاريخه، ولكل جيل سماته من حيث أنواع الأسلحة المستخدمة، وطبيعة الخطط والتكتيكات والاستراتيجيات، وميادين المعارك وغيرها، بدءًا من الجيل الأول الذي كان يعتمد على حشد الجيوش واستخدام الأسلحة والمدافع البدائية، مرورًا بالجيل الثاني الذي يعتمد على القوة النارية من خلال حشد أكبر عدد من الجنود واستخدام المدرعات والأسلحة الآلية. ظهر الجيل الثالث من الحروب إبان الحرب العالمية الثانية (١٩٣٩-١٩٤٥)، إذ تميّز بالتطوّر الكبير للمدرعات والاعتماد على القوات الجوية وسرعة الحركة والمفاجأة. أما الجيل الرابع من الحروب، فيقوم على ضرب العدو من الداخل من خلال عمليات

التمرد والتشجيع على الحروب الأهلية والطائفية، ليصبح المجتمع هو السلاح المستخدم لتدمير نفسه، إلى أن وصلنا إلى الجيلَين الخامس والسادس اللذين يجمعان بين الوسائل والأساليب التقليدية وغير التقليدية كحروب المعلومات والحروب السيبرانية ، التي لم يعد معها سباق التسلح اصطلاحًا عسكريًا فقط يقوم على تكديس الطائرات أو المدافع أو الدبابات أو أسلحة الدمار الشامل ، بل يقوم على استحداث برامج إلكترونية مُعدة لأغراضٍ عسكرية وتطويرها تُعرف اختصارًا بالسايبر. وسنتناول في هذا المبحث مفهوم الهجمات السيبرانية من خلال مطلبين حيث سنناقش في المطلب الأول (تعريف الهجمات السيبرانية) وفي المطلب المطلب الثاني سوف نناقش (انواع الهجمات السيبرانية).

المطلب الأول: تعريف الهجمات السيبرانية: لقد اصبح الفضاء الالكتروني هو عنوان الحياة المعاصرة ، واصبح عنصراً مؤثراً في العلاقات الدولية ، لا بل حتى النزاعات الدولية وغير الدولية والتي شهدت لأول مرة استخدام سلاح الهجمات السيبرانية ، وهو تطور نوعي احدث تغيير في استراتيجيات وخطط الحروب التقليدية ، وبالنظر لحداثة الهجمات السيبرانية ، فقد واجه الخبراء والمختصين صعوبة في تحديد مفهوم جامع لها ، وسنناقش في هذا المطلب تعريف الهجمات السيبرنية لغة واصطلاحاً .

الفرع الأول: تعريف الهجمات السيبرانية لغة : أن أول من أطلق هذه تسمية الهجمات السيبرانية عالم الرياضيات نوربرت وينر (Norbert Weiner) في العام (١٩٤٨)، أثناء دراسته لموضوع القيادة والسيطرة والاتصال في عالم الحيوان، فضلًا عن حقل الهندسة الميكانيكية. أن كلمة سايبر(cyber) تعود جذورها لليونان ، والتي تعني القيادة والتحكم عن بعد ، وترجع إلى المصطلح (kybernetes) والذي ورد للمرة الأول في مؤلفات الخيال العلمي[١]. وبالرجوع إلى قواميس اللغة ، فلم تشر في الغالب إلى مصدر كلمة سايبر(Cyber) ، سوى ما وجدناه في قاموس (المورد) إذ يعرفها بالقول:" السيبرانية : هي علم الضبط ، ومصدرها ("Cybernetics) ، وهو مصدر يتطابق مع مفهوم الهجمات السيبرانية ، أي ضبط الأشياء عن بعد والسيطرة عليها[٢]. وقد تميز قاموس (المورد) عن غيره من قواميس اللغة العربية بنصه بشكل صريح على كلمة سايبر (cyber) ، إذ عرفها بالقول: (السيبرانية هي علم الضبط، ومصدرها (kybernetes)) ، وهذا التعريف يتوافق مع معنى الهجمات السيبرانية ، التي يتم ضبطها والتحكم بها عن بعد . والملاحظ : ان كافة كافة المصطلحات العسكرية اكدت على نطاق استخدام كلمة سايبر في المجال العسكري حصراً، ولم تذهب الى تعريفها او مناقشة جذورها . فقد عرفها قاموس المصطلحات العسكرية الأمريكية(الفعل الذي يستخدم عبر الشبكات

الالكترونية بغية السيطرة أو تعطيل برامج الكترونية أخرى). وبالعودة إلى المختصين في اللغة العربية نجدهم قد واجهوا صعوبات كبيرة في اختيار مصطلحات تقترب من مصطلح(cyber) بالانكليزية. بسبب عدم وجود مصطلح متفق عليه في اللغة العربية من جهة، ولأن الوثائق الصادرة عن الأمم المتحدة باللغة العربية، استخدمت مصطلح السيبرانية نفسه من جهة اخرى[٣]. أما قاموس مصطلحات الأمن المعلوماتي فعرفها: (هجوم من عبر الفضاء الالكتروني يهدف إلى السيطرة على مواقع الكترونية أو بنية محمية الكترونياً لتعطيلها أو تدميرها والسيطرة عليها) [٤].

الفرع الثاني : تعريف الهجمات السيبرانية إصطلاحاً : وفقاً لدليل تالين المطبّق على الحرب السيبرانية في العام ٢٠١٣، فقد عرّفت الهجمات السيبرانية بأنها: «عمليات سيبرانية، سواء أكانت هجومية أم دفاعية، والتي يهدف من خلالها بصورةٍ معقولة التسبب بالإصابة أو وفاة الأشخاص أو الأضرار أو تدمير الأعيان الأهداف»[٥]. كما عرّفها مايكل شميت على أنها: «مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نُظم المعلومات المعادية بهدف التأثير والإضرار بها، وفي الوقت نفسه للدفاع عن نُظم المعلومات الخاصة بالدولة المهاجمة»[٦]. فيما عرفه فيورتس(Fuertes) بالقول:" هجوم عبر الانترنت يقوم على التسلل إلى مواقع الكترونية غير مرخص بالدخول إليها، بهدف تعطيل أو إتلاف البيانات المتوفرة فيها أو الاستحواذ عليها، وهي عبارة

عن سلسلة هجمات الكترونية تقوم بها دولة ضد أخرى[٧].

كما عرفها شين(Shin) بالقول: " استخدام الطيف الالكتروني أو الكهرومغناطيسي لتخزين وتعديل وتبادل البيانات وجهاً لوجه مع أنظمة تحكم في بنى تحتية مرتبطة بها." ويعرف(Waxman.C Mattew) الهجمات السيبرانية بأنها الجهود الرامية الى تغيير، او تعطيل او تدمير أنظمة الحاسوب او الشبكات أو المعلومات او البرامج الموجودة عليها، والأضرار التي تسببها هذه الهجمات يمكن ان تصيب شبكة الحاسوب او المرافق المادية او الأشخاص ، وتتراوح اضرار الهجمات السيبرانية من القرصنة الخبيثة وتشويه مواقع الانترنت الى دمار واسع النطاق للبنية التحتية العسكرية والمدنية المرتبطة بتلك الشبكات[٨]. وقد عرفه روسيني (Roscini)بالقول:" الهجوم السيبراني، هو أي تصرف دفاعياً كان أم هجومياً، يتوقع منه و على نحو معقول في التسبب بجرح أو قتل شخص أو إلحاق أضرار مادية أو دمار بالهدف المباشر[٩]. ونرى: ان الهجوم حتى يمكن وصفه بهجوم سيبراني يجب ان تتوفر فيه جملة من الخصائص إهمها ان تكون أضراره واسعة النطاق، وأن تكون طويلة الأمد أي آثارها تستغرق

فترة زمنية، وأن تكون بغرضٍ، أي عملية استخدام هذا السلاح أو هذه الوسيلة من أجل أن يكون واسع النطاق وطويل الأمد. وتعرف الهجمات السيبرانية ايضاً بأنها " تلك الاجراءات التي تتخذها الأطراف في نزاع مسلح ، لكسب الميزة على خصومهم في الفضاء الالكتروني وتحصل مزايا من خلال اتلاف أو تدمير وتعطيل أو إختراق أنظمة الحاسوب للعدو أو الحصول على معلومات سرية متى كانت في إطار نزاع مسلح يصل إلى مستوى الحرب[١٠]. وفيما يتعلق باللجنة الدولية للصليب الأحمر فقد عرفت الهجوم السيبراني بأنه: استخدام انشطة متعمدة لتغيير أو افساد أو خداع او إضعاف أو تدمير أنظمة الحاسوب أو شبكات الحاسوب للخصم أو المعلومات أو البرامج المدرجة في هذه الأنظمة أو الشبكات أو التي ترسل من خلالها، وقد تؤثر هذه الأنشطة ايضاً في الكيانات المرتبطة في هذه الأنظمة والشبكات[١١]. ونرى : أنه يمكن ان نعرف الهجمات السيرانية بانها التي يمكن التحكم بها عن بعد ، والتي تشن من قبل الدولة او افرادها او بشركات خاصة يتم الاستعانة بها من الدولة بغية الحاق اضرار بالغة بالعدو، تستهدف سرقة المعلومات الحساسة للعدو ، وتعطيل خدماته الحيوية، وتدمير بناه التحتية ، من خلال اختراق المنظومة المعلوماتية للعدو .

المطلب الثاني: نشأة الهجمات السيبرانية وإنواعها : على الرغم من ان الهجمات السيبرانية حديثة العهد ، الا انها ارتبطت باحداث متسارعة مع عهد الثورة المعلوماتية ، كما تنوعت هذه الهجمات بأوجه عدة.

الفرع الأول : نشأة الهجمات السيبرانية : ارتبطت الهجمات السيبرانية بحدثين مهمين ، هما اكتشاف الكمبيوتر ، وظهور الانترنت ، الحدثان اللذان احدثا انقلاباً في تاريخ البشرية ، ودخلت معها البشرية عصراً جديد هو عصر الثورة المعلوماتية ، بعد عصر الثورة الصناعية والزراعية . لقد كان منتصف الخمسينات من القرن المنصرم هو الحدث التاريخي الاهم في تاريخ البشرية ، حيث دخل الكومبيوتر والانترنت في كافة مجالات الحياة الصناعية والتجارية والتعليمية والصحية ، بل ان استخدامهما من قبل ملايين الاشخاص تحول في سنوات الى استخدامها من مليارات الافراد في العالم ، وارتبط العالم في محيط فضائي افتراضي عبر الزمن . ولم تتوقف استخدامات الحواسيب والانترنت في المجالات المدنية بل استخدمت ايضاً في المجالات العسكرية ، سواء في الصناعات العسكرية او في برامج الاقمار الصناعية او في برامج التجسس والقرصنة العسكرية . ومنذ البداية لم تكن للهجمات السيبرانية صدى على المستوى الدولي، حيث اقتصرت هذه الهجمات على مهاجمة شركات الاتصالات والشركات المصرفية والمالية ، الا ان التسارع في مجال الهيمنة العسكرية من قبل الدول ادى الى

استخدامها سلاح جديد هو سلاح الهجمات السيبرانية ، وهذا ماحصل في سياق الحرب الباردة بين امريكا وروسيا حيث كان الطرفان يعترضان اتصالات البعض الاخر، ويتجسسان الكترونياً على بعضهما بغية الحصول على افضلية في الحرب التي كانت مرتقبة . وفي سياق الحرب الباردة فقد سجلت نماذج للهجمات السيبرانية بين البلدين ، عندما شنت الولايات المتحدة الامريكية هجوماً سيبرانياً عام ١٩٨٢ على انابيب النفط الروسية والذي نجم عنه انفجار كبير الحق مع خسائر بالغة ، وفي عام ١٩٩١ شنت القوات الامريكية في حرب الخليج الاولى هجوماً سيبرانياً ، حيث قامت باختراق منظومة الدفاع الجوي العراقية ، وتدمير شبكة الاتصالات العسكرية للقوات العراقية . وبين عامي ١٩٩٨ _ ٢٠٠٠ فقد تعرضت انظمة الاتصال الالكترونية لوكالة ناسا الامريكية الى هجوم سيبراني من قبل روسيا والذي أدى إلى الاستحواذ على الآلاف من الملفات المصنفة بأنها عالية السرية ، والمفارقة ان كل الاطراف كانت تنفي مسؤوليتها عن الهجمات السيبرانية. ومن الأمثلة الأخرى الهجوم الأميركي الإلكتروني على نظام الدفاع الجوي الصربي سنة ١٩٩٨ لاختراقه بهدف تسهيل قصف أهداف صربية . وكذلك الهجوم الذي يعتقد أن مصدره روسيا واستهدف إستونيا سنة ٢٠٠٧ وأدى إلى تعطيل كافة مواقع الويب الحكومية والخاصة ووسائل الإعلام عبر البلاد [١٢]. وفي عام ١٩٩٩ قام سلاح الجو التابع لحلف الشمال الأطلسي(NATO) ، بشن هجمات سيبرانية استهدفت شبكات الهاتف النقال في يوغسلافيا السابقة اثناء حرب كوسوفو. وفي النزاع المسلح ذاته، وبعد استهداف طيران حلف شمال الأطلسي للسفارة الصينية في بلغراد، قام عدد من القراصنة الصينيين - وكردة فعل - بمهاجمة مواقع الكترونية رسمية منتخبة تابعة للولايات المتحدة الأمريكية، وبالذات الموقع الالكتروني للبيت الأبيض ، نجم عنها الاستحواذ على الآلاف من البيانات الرقمية ، المصنفة – آنذاك - بأنها عالية السرية. وفي العام ٢٠٠٧، قام العدو الإسرائيلي بواسطة سلاحه الجوي بهجومٍ على موقع سوري يُشتبه بأنه مفاعل نووي، والذي تزامن معه قيام العدو الإسرائيلي بهجماتٍ سيبرانية على أجهزة الرادار والاتصال في وزارة الدفاع وباقي منظومات الاتصال في المطارات العسكرية والمدنية، أدت إلى تعطيلها عن العمل بالكامل[١٣]. وتعرضت أستونيا في العام ٢٠٠٧، إحدى جمهوريات الاتحاد السوفياتي السابق، إلى هجمات سيبرانية متلاحقة أدت إلى التعطيل الكامل لشبكات الاتصال فيها، شملت مواقع رسمية حساسة لرئيس الوزراء ورئيس البرلمان والوزراء الأستونيين. وقد وجّهت أستونيا الاتهام إلى روسيا الاتحادية باعتبار أن الهجمة السيبرانية التي قامت بها الأخيرة ليست إلا عملية انتقامية لما قامت به أستونيا بنقل نصب تذكاري يخلّد

الجيش الروسي من العاصمة تالين إلى مكان مجهول . والمثال الآخر على الهجمات السيبرانية هو النزاع الروسي الجورجي في العام ٢٠٠٨، والذي أدى إلى تعطل نظام الاتصال الإلكتروني (IT)للقوات الجورجية بالكامل قبل بدء العمليات القتالية بيومٍ واحد، وبخاصةٍ في إقليم أوسيتيا عقب إعلان انفصاله عن جورجيا، ما أضعف وسائل الدفاع الجوية الجورجية، فضلًا عن تعرّض وسائل الإعلام والبنى التحتية وأهمها قطاع المواصلات لهجماتٍ سيبرانية أيضًا [١٤]. وفي عامي ٢٠٠٩، ٢٠١٠، برزت الهجمات التي نفذتها الوحدة (٨٢١١) الاسرائيلية بالتعاون مع "وكالة الأمن القومي" الأمريكية، على المنشأة النووية الأيرانية في (نطنز) ، إذ تمكنت الوحدة من نشر فيروس حاسوبي يطلق عليه اسم "ستوكسنت(Stuxnet) "داخل المرفق. واستهدف الفيروس المستخدمة في تخصيب اليورانيوم، ما أدى إلى جعلها تتحرك بوتيرة خارجة عن نطاق السيطرة مما ادى بنهاية الى تكسرها ، وكانت هذه الأجهزة من طراز "سيمنز سي ١٠٠٠" وهي اجهزة متطورة ، واتجهت الاتهامات الايرانية الى الولايات المتحدة الامريكية واسرائيل[١٥] . وبسبب النزاع المستمر بين الهند وباكستان بشأن الاستحواذ على كشمير ، ومع نهاية عقد التسعينات من القرن الماضي ، برزت لاول مرة بين الطرفين شن هجمات الكترونية عبر الفضاء الالكتروني ، من خلال استهداف قاعدة البيانات. وفي عام ٢٠١٤ وبعد التدخل الروسي في شبه جزيرة القرم ، أعلنت شركة "روستك العسكرية الروسية" من تمكنها من الاستيلاء على طائرة امريكية نوع (MQ5B) بدون طيار من خلال هجمة سيبرانية كهرومغناطيسية استهدفت التشويش استهدفت التشويش على نظام الملاحة في الطائرة . ومن الملاحظ: انه من عام ٢٠٠٦ لغاية الان ، شنت امريكا وايران عشرات الهجمات السيبرانية استهدفت منشأت نووية ، والمنشأت العسكرية ، ومحطات للطاقة ، وحاملات نفط ، ومنشأت حيوية ، الحقت اضراراً بالطرفين بلغت مليارات الدولارات ، واعتمد الطرفان سياسة الامن السيبراني كاستراتيجية قومية لمكافحة الهجمات السيبرانية . وكان اخر هجمة سيبرانية تم تسجيلها في عام ٢٠٢٤ ، عندما شنت ايران واسرائيل هجمات سيبرانية متبادلة استهدفت منشأت حيوية وعسكرية مهمة . ونرى: ان الهجمات السيبرانية تمثل التطور الحديث في ميدان العمليات العسكرية ، وقد تكون هذه الهجمات ، واستخدام الروبورت المقاتل والطائرات المسيرة ، العنوان الجديد للنزاعات المسلحة ، والتي سوف يكون الاعتماد عليها بنسبة عالية في الصراعات الدولية القادمة بدلا من الاسلحة والجيوش التقليدية .

الفرع الثاني : انواع الهجمات السيبرانية وخصائصها : بعد عصر الثورة المعلوماتية ، فقد تنوعت الهجمات السيبرانية والبرامج التي تستخدمها وسوف نستعرض اهم انواع الهجمات السيبرانية .

١_ هجوم الحرمان من الخدمة ::(attacks service of Denial) . ومن اسمه، هدفه حرمان المستخدمين من خدمة معينة والتأثير عليها، ويطلق على أخطر أنواعه اسم (service of Denial Distributed _DDOS) حيث أن المهاجم يستهدف في هذا الهجوم مجموعة من أجهزة الكمبيوتر لاشخاص لايعرفهم ولكنه قام باستهداف الثغرات الموجودة في أجهزتهم في أكثر من مكان ، ويقوم بمهاجمة سيرفر معين أو شبكة واستخدام هذه الاجهزة دون علم أصحابها. والملاحظ ان هجوم رفض الخدمة (DoS) يؤدي إلى إغراق الخادم بحركة المرور، مما يجعل موقع الويب أو المورد غير متاح. أما هجوم رفض الخدمة الموزع (DDoS) هو هجوم DoSيستخدم أجهزة كمبيوتر أو أجهزة متعددة لإغراق مورد مستهدف. كلا النوعين من الهجمات يغمران الخادم أو تطبيق الويب بهدف مقاطعة الخدمات، ونظرًا لأن الخادم يتم غمره بمزيد من حزم (TCP / UDP) أكثر مما يمكنه معالجتها، فقد يتعطل، وقد تتلف البيانات، وقد يتم توجيه الموارد بشكل خاطئ أو حتى استنفادها لدرجة شل النظام[١٦].

٢_ الفايروسات الخبيثة فايروسات الحاسوب (viruses) : وهي برمجيات خبيثة صنعت قصداً من أجل تغيير خصائص الملفات التي تصيبها لتقوم بتنفيذ بعض الأوامر إما بالإزالة او التعديل او الحذف او التخريب هدفها الأساسي هو الحاق الضرر. هذا الفايروس مصمم لتكرار نفسه ذاتياً ويمنحه هذا الوصف استهداف البرامج الاخرى في الذاكرة لالحاق اقصى ضرر ممكن بالنظام بقصد تدميره. ويرجع الفضل في وضع أول تصور لفايروس معلوماتي إلى الدكتور " فريد كوهن " في الحلقة الدراسية التي ألقاها في االولايات المتحدة الامريكية بجامعة كاليفورنيا حول آمن الحاسب الألي عام ١٩٨٣ [١٧]. وابرز خصائص الفايروسات تتمثل بقدرتها على التغير السريع ، والاختراق الشامل ، والانتشار ، والاختفاء ، والتدمير الشامل للبرامج او الانظمة التي تستهدفها .

٣_ برامج الدودة (Software Worm): وهي برمجيات تستهدف انظمة التشغيل في الحاسب الالي ، لاحداث اضرار بالغة في الملفات ، وانظمة الاتصالات وبروتوكولات التشغيل ، والعمل على خفض شبكة الاتصالات وتقليل كفاءتها . والطرق المعروفة لانتشار هذه الديدان يكون من خلال ارسال روابط انترنت مصابة بالفايروسات ، او مرفقات مع الرسائل الالكترونية ،

واستهداف انظمة الحماية ، والتسللسل الفايروسي عبر انظمة الحواسيب وارسال البرامج الضارة لها مما يجدث اضراراً بالغة في انظمتها وذاكرتها .

٤_ أحصنة طروادة (horses Trojan): وهي برامج تستهدف اختراق اجهزة الحاسوب، من خلا بث شفرة في برامج ذات انتشار عالمي ، يستهدف سرقة بيانات اجهزة الحواسيب ، من خلال اضعاف اجهزة الدفاع والحماية لديها .

٥_ برامج القنابل المنطقية(Bombs Logic) : وهي برامج تستهدف الشبكة المعلوماتية للوقوف على معرفة الية تشغيل النظام لفترة زمنية منتظمة ، بغية استهدافه بقنابل فايروسية متتالية لازالة اوامر او سجلات تم تثبيتها في الشبكة المعلوماتية مسبقاً، والهدف الرئيسي من هذا الهجوم السيبراني هو التحكم بالشبكة المعلوماتية او اتلافها ، وتظهر هذه الفايروسات بشكل واضح في عدد من مواقع الانترنت والمواقع المؤجرة ، وميزتها الاساسية هي قدرتها على التخفي لاشهر او سنوات دون اكتشافها .

٦_ الفايروسات الالكترونية (viruses electronic) : من اهم الفايروسات الالكترونية التي تم اكتشافها في عام ٢٠٠٩ هو فايروس ستاكس نت(stuxnet) والذي احدث نقلة نوعية في الحروب السيبرانية ، ويعد اخطر الفايروسات الالكترونية الذي يستهدف تدمير المكونات المادية لنظم التشغيل ، بعد ان كانت كل الهجمات والحروب السيبرانية السابقة تستهدف تدمير بيانات الانظمة فقط دون تدمير مكوناتها المادية ، اضافة الى فايروس ستاكس نت (stuxnet) ، فقد تم اكتشاف فايروس دوكو(duqo) عام ٢٠١١ من قبل جامعة بودابست ، وفيروس فليم (flame) الذي تم اكتشافه في عام ٢٠١٢ بواسطة فريق الاستجابة والطوارئ الايراني وجامعة بودابست والذي يعد اخطر الفايروسات تدميراً. ووفقاً لما تقدم: فأن الهجمات السيبرانية تتميز عن الهجمات العادية ، بكونها تمثل التطور التكنلوجي للعصر الرابع من جيل المعلومات الرقمي ، كما انها تتسم بكلفتها المتدنية قياساً بالاسلحة التقليدية، كما انها تتميز بسرعتها ودقتها وقدرتها على الاختراق، وتتعدى مخاطرها ميادين القتال التقليدية لتصل الى كافة البنى التحتية والمواقع الحساسة مخترقة كافة الحدود الجغرافية ، كما تتميز بقدرتها على التخفي وصعوبة اكتشافها ومن هي الدولة او الشركة او الافراد الذين يكونون خلفها وبالتالي صعوبة تحديد المسؤولية ، كما تتميز بسهولة استخدامها وتوفرها على نطاق واسع ضمن الشبكة العنكبوتية .

المبحث الثاني: التكييف القانوني للهجمات السيبرانية المرتكبة من المدنيين : لقد مثل ظهور الانترنت ثورة للبشرية والذي تم استخدامه بكافة المجالات التجارية والاقتصادية والاكادمية

بل حتى العسكرية منها ، وزاد مستخدمي الشبكة المعلوماتية ليصل الى بلايين البشر ، وكان لاستخدام الانترت في المجال العسكري نقطة تحول لدخول الجيل الخامس من الحروب بعد ان كانت الحروب التقليدية تتركز في الجو والبحر والبر والفضاء الخارجي . فاصبح العالم يتوجه الى استخدام سلاح جديد يختلف عن اسلحة الحروب التقليدية ويختلف عن الجرائم الالكترونية التي تستهدف الشركات التجارية ، وبالتالي ظهرت العديد من الاشكاليات في تكييف الهجمات السيبرانية على المستوى الدولي وخصوصا مع عدم وجود اتفاقيات او معاهدات قانونية تنظمها . ويعد دليل تالين اول محاولة قانونية لتكييف الهجمات السيبرانية سواء كانت النزاعات دولية او غير دولية ، والدليل يؤكد ان الهجمات السيبرانية قد تؤدي الى نزاعات مسلحة طبقاً لطبيعتها التدميرية ، التي قد تستهدف افراد او قتل اشخاص او تلحق اضرار باعيان مدنية . وبالتالي يثار التسأول هنا عن التكييف القانوني لهذه الهجمات وخصوصا التي ترتكب من المدنيين، وهل هي وسيلة او اسلوب للقتال ، وماهي المسؤولية الدولية للمدنيين والدول والشركات الخاصة عن دورهم في شن هذه الهجمات سواء كانت النزاعات دولية وغير دولية . وسنناقش هذا الموضوع عبر مطلبين نناقش في المطلب الأول (انطباق القانون الدولي الانساني على الهجمات السيبرانية) ونناقش في المطلب الثاني (مسؤولية المدنيين عن الهجمات السيبرانية).

المطلب الأول: انطباق القانون الدولي الانساني على الهجمات السيبرانية : ان عملية تكييف الهجمات السيبرانية ومدى انطباق القانون الدولي الانساني عليها اثار جدلاً فقهياً وقانونياً ، كما يثير اشكالية في القواعد المتعلقة بحق اللجوء الى الحرب .

الفرع الأول : طبيعية الهجمات السيبرانية : ان الثورة المعلوماتية واستخدام الهجمات السيبرانية كسلاح اثار نقاشاً قانونياً ، في مدى اعتبار هذه الهجمات سلاح ام وسيلة للقتال ، وهل هو سلاح محظور لا يجوز استخدامه في النزاعات مثل بعض الاسلحة التقليدية المحظورة .

أولاً: الهجمات السيبرانية اسلوب للقتال : ان الهدف الاساسي للحرب الذي نظمه القانون الدولي الانساني في كافة النزاعات سواء كانت نزاعات دولية او غير دولية هو اضعاف القوة العسكرية للعدو وليس القضاء عليه او ابادته ، وبالتالي ضرورة تقييد استخدام القوة للحد من مخاطر الدمار الشامل . ان اختلاف موازين القوى بين الاطراف المتحاربة لايعني استخدام وسائل او تكتيكات يحظرها القانون الدولي الانساني ، لان ذلك سيؤدي الى صعوبة التمييز بين المدنيين والمقاتلين وصعوبة في تطبيق مبدأ التناسب والاحتياطات المستطاعة ، واختيار

الأهداف العسكرية وأساليب الحرب ، وخصوصاً في النزاعات الدولية وتحدّد اتفاقيات لاهاي لسنة ١٨٩٩ و١٩٠٧ بالإضافة إلى اتفاقيات جنيف لعام ١٩٤٩ والبروتوكولين الإضافيين لها لعام ١٩٧٧، الأحكام والقيود والمحظورات الرئيسية المتعلقة باستعمال العنف وأساليب الحرب المختلفة أثناء النزاعات المسلحة الدولية وغير الدولية[١٨]. والقانون الدولي الانساني يحظر الالام غير المبررة والدمار والعنف الشديد ، ويجب ان تكون الوسائل المستخدمة في القتال موجهة الى هدف عسكري وليس مدني ، وان تكون مبررة في استخدامها لوجود ضرورة عسكرية مباشرة ، وان تكون متناسبة بحيث تحقق الميزة العسكرية . وان تتخذ كافة الاحتياطات المتناسبة والضرورية للحد من الاضرار التي تلحق المدنيين من جراء استخدام هذه الوسائل . ومن وسائل الحرب المحظورة بموجب اتفاقيات القانون الدولي الانساني (الغدر، الذعر، تجويع المدنيين ، الأعمال الانتقامية الموجهة ضد أهداف غير عسكرية، الهجمات التي تهدف إلى إحداث أضرار بالبيئة الطبيعية ، الهجمات على الأعمال والمنشآت التي تضمّ قوى خطرة ، احتجاز الرهائن ، استخدام الدروع البشرية أو ترحيل السكان لصالح سير الأعمال العدائية). وتشمل الحرب السيبرانية أساليب للقتال تتألف من عمليات إلكترونية ترقى إلى مستوى النزاع المسلح، من خلال استخدامها في تحسين اداء العمليات العسكرية وتسهيل عمل القوة العسكرية التقليدية ، كاستخدام الهجمات السيبرانية لتمهيد الطريق امام القوات العسكرية ، من خلال قطع الاتصالات في المطارات العسكرية والمدنية للعدو لتحقيق ميزة في الهجوم ، ومن ثم يمكن اعتبارها اسلوبقتال وجزء من الخطط العسكرية للمعركة.

ثانياً: الهجمات السيبرانية وسيلة للقتال : لقد جاءت نصوص القانون الدولي الإنساني، منذ البداية، لتضع حداً للمعاناة التي تسببها النزاعات المسلحة. ولهذه الغاية، يحدد القانون الدولي الإنساني كلاً من سلوك المقاتلين وقواعد اختيار وسائل الحرب وأساليبها بما فيها الأسلحة. ولقد اكد القانون الدولي الانساني على حظر او استخدام اية اسلحة محظورة او التي تلحق الالام غير مبررة ، فقد ضمن اعلان سان بيتر سبرج الصادر عام ١٨٦٨ التزام على الدول بالامتناع المتبادل عن السماح لقواتها البرية أو البحرية – في حالة الحرب – استعمال أى قذيفة يقل وزنها عن(٤٠٠ جرام) وتكون متفجرة أو مشحونة بمواد قابلة للانفجار أو الاستعمال، كما اشارت اتفاقية لاهاي لعام ١٨٩٩ الى امتناع الدول عن استخدام الرصاص الذى ينتشر أو يتمدد بسهولة في جسم الإنسان ومنه الرصاص ذو الغشاء الصلب الخفيف أو القاطع (Dum- dum)، كما حظرت لائحة قوانين الحرب البرية ١٩٠٧إستخدام السم أو الأسلحة السامة، وكذلك حظر استخدام الأسلحة والقذائف والمواد التي من شأنها إحداث إصابات وآلام لا مبرر لها [١٩]. وفي

١٩٢٥، اعتمدت الحكومات بروتوكول جنيف الذي يحظر استعمال الغازات السامة ووسائل الحرب الجرثومية.كما تم حظر استخدام الاسلحة الكيمياوية بموجب اتفاقية عام ١٩٩٣ لحظر الأسلحة الكيميائية وتدميرها، وتم حظر الألغام المضادة للأفراد بموجب اتفاقية حظر استعمال وتخزين وإنتاج ونقل الألغام المضادة للأفراد وتدمير تلك الألغام لعام ١٩٩٧. وفي ٢٠٠٨، اعتمدت ١٠٧ دولة الاتفاقية المتعلقة بحظر استخدام الذخائر العنقودية. وفي عام ٢٠٢١ تم حظر استخدام الاسلحة النووية في النزاعات المسلحة[٢٠]. وبالنسبة للهجمات السيبرانية في حال استخدامها للتسلل لانظمة منشأة حيوية بغية السيطرة عليها وتدميرها ، فان هذه الهجمات تعد وسيلة للقتال اي سلاح يستخدم لمهاجمة منشأت العدو الحيوية . بالرغم بعدم امتلاكها القدرة الحركية كسلاح ، لكن المهم هنا الاضرار المباشرة التي تلحقها هذه الهجمات بالعدو. ومهما كانت الاسلحة المستخدمة في العمليات العسكرية سواء كانت تقليدية او هجمات سيبرانية ، فان القانون الدولي الانساني ينظم استخدامها حالها كحال اي وسيلة او اسلوب قتال سواء كانت تقليدية او معاصرة. والدول التي اعتمدت اتفاقيات القانون الدولي الانساني ، كانت تهدف الى تنظيم النزاعات الحالية والمستقبلية ، اذا ادرجت في هذه الاتفاقيات قواعد تهدف الى تطوير وسائل واساليب قتال جديدة على افتراض ان القانون الدولي الانساني سينطبق عليها في المستقبل . ونرى : ان الهجمات السيبرانية تعد وسيلة واسلوب للقتال في ان واحد وفقاً للهدف من استخدامها، ولكنها مقيدة بان تراعي مبادئ القانون الدولي الانساني ، وان لا تلحق اضراراً غير مبررة بالعدو . وهذا ماأكدته اللجنة الدولية للصليب الأحمر، حينما طالبت الدول المنضمة الى اتفاقيات جنيف أثناء المؤتمر الدولي الثامن والعشرين, للصليب الأحمر والهلال الأحمر المقام عام ٢٠٠٣، 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"[٢١].

الفرع الثاني: القانون الدولي الانساني والهجمات السيبرانية : اثارت الهجمات السيبرانية جدالاً في مدى انطباق القانون الدولي الانساني عليها ، خاصة ان مبادئ القانون الدولي الانساني لم تشر اليها حينما وضعت كمبادئ تحاول تنظيم النزاعات التقليدية. ان الفضاء الالكتروني الذي تنشط فيه الهجمات السيبرانية رغم اختلافه عن الفضاء الذي تجرى فيه الحروب التقليدية لايعني انه فضاء حر بدون ضوابط تنظمه او مبادئ يمكن تطبيقه عليه . وتكمن خصوصية الفضاء الإلكتروني في عدم وجود دولة بإمكانها فرض السيطرة, والسيادة,

الأحادية عليه ، وهنالك اراء فقهية ترفض التعامل مع فضاء الانترنت من خلال الضوابط القانونية باعتباره فضاء حر لايخضع للقانون او لسيادة دولة ما. وبالتالي فان كلمات المرور وألواح المفاتيح وأجهزة الحواسيب هي متاحة للكل ، وبالتالي فان االفضاء الالكتروني ، لايمكن أن تختص به دولة معينة، وبالتالي لا يمكن إنطباق القانون الدولي العام التقليدي على الهجمات السيبرانية التي تشن من خلال هذا الفضاء"[٢٢]. وفيما يخص تطبيق أحكام القانون الدولي الإنساني, على الهجمات الإلكترونية، فان انصار المذهب الحر يذهبون الى انه لايوجد في القانون الدولي الانساني اي فقرة تشير الى الهجمات السيبرانية ، او الى الحرب الالكترونية ، او الى الفضاء الالكتروني ، او الى المبادئ التي تحكم خوض الهجمات السيبرانية لا من قريب او بعيد ، كون استخدام الانترنت والحواسيب والهجمات السيبرانية هو حديث نسبياً ، قياساً الى تاريخ اتفاقيات القانون الدولي الانساني التي يعود تاريخها إلى قبل استخدام أو ظهور الاختراقات عبر شبكات الحاسوب[٢٣] ، وكون المدة التي تم بها تنظيم اتفاقيات لاهاي (١٨٩٩_١٩٠٧) ، واتفاقيات جنيف لعام ١٩٤٩ وبروتوكولها الاضافيين لعام ١٩٧٧، لم يذكر فيها على وجه الخصوص اي ذكر لمفهوم الهجمات السيبرانية[٢٤]. ونرى: ان القانون الدولي الانساني وفقاً لهذا الاراء لايمكن تطبيقه على الهجمات السيبرانية ، كون القانون الدولي الانساني يستخدم دوماً مصطلحات النزاعات المسلحة ، او القوة الاقليمية ، او السيادة الدولية ، او الهجوم المسلح ، وهذه المصطلحات تكون خارج مفهوم الحروب الالكترونية. وفي سياق الحرب السيبرانية فلا يعدّ الهجوم السيبراني نزاعا مسلحا، لأنه لا يتضمن استعمالا للقوة المسلحة ضد إقليم الدولة[٢٥]، 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 ، فعلى الرغم من جسامة الأضرار التي تلحقت بالبنية التحتية في النزاع الاستوني والجورجي واستمرار الهجمات الإلكترونية لعدة أيام إلا أنها لم تعدّ بمثابة نزاع مسلح [٢٦] . الا انه عند استعراض ميثاق الامم المتحدة فاننا نجد ان المادة (٥١) من الميثاق قد اباحت استخدام القوة المسلحة في حال تعرض الدولة الى هجوم او نزاع مسلح كونه يمثل حق في الدفاع عن نفسها، عندما تواجه هجوما من قبل قوة مسلحة ، حيث نصت " 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" . ووفقا لهذا الاجتهاد فإن للدولة الحق في الدفاع عن نفسها إزاء أي هجوم، بغض النظر عن شكله ووسيلته. وقد جاء اعلان وزارة الدفاع الأمريكيو (البنتاغون) في عام ٢٠١١ ، ليؤكد على هذا التوجه، إذ جاء فيه

بأن توجيه هجمات الكترونية ضد الولايات المتحدة الامريكية ، ومايلحقه من اضرار في المنشات الحيوية المدنية والعسكرية ، فان ذلك يعد حربا واعتداء يبرر استخدام القوة العسكرية ضده[٢٧]. وبالتالي يمكن اعتبار الهجوم السيبراني الذي تعرضت له استونيا عام ٢٠٠٧ ، والذي استهدف البنى التحتية والمنشأت الحيوية لها بأنه عدوان يخضع إلى مبدأ الحق في اللجوء إلى الحرب. وهناك رأي اخر يتحدث بامكانية انطباق القانون الدولي الانساني على الهجمات السيبرانية ، سواء التي تشن من قبل الافراد او الدول او الشركات الخاصة ، مستندين في رايهم في ان القانون الدولي الانساني ينظم خوض الحرب ، وبالتالي عندما تكون الهجمات السيبرانية عشوائية وتستهدف الاضرار بالغير والاعتداء عليه ، فهنا يمكن تطبيق مبادئ القانون الدولي الانساني التي تطبق في الحروب التقليدية، كالتمييز والتناسب والاحتياطات المستطاعة ايضاً على الهجمات السيبرانية . وعند مراجعة المادة(٣٦) البروتوكول الإضافي الأول لاتفاقيات جنيف لعام ١٩٤٩ التي 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". وبالتالي فان على الدول الالتزام بتنفيذ مضمون المادة المادة(٣٦) من البروتوكول الإضافي الأول على الهجمات السيبرانية كونها تعد من قبيل الاسلحة والوسائل الحديثة في الحروب المعاصرة . وقد اشارت محكمة العدل الدولية في فتواها التي عنونتها ب"مشروعية التهديد بالاسلحة النووية أو استخدامها"، حيث أشارت المحكمة بان القواعد والمبادئ الثابتة للقانون الدولي الانساني السارية في النزاعات المسلحة تنطبق "على كافة أشكال الحرب وعلى كافة أنواع الاسلحة بما في ذلك الهجمات السيبرانية"[٢٨] . وعلى الرغم من اتفاقيات القانون الدولي الانساني لم تشر الى الهجمات السيبرانية بصراحة ، اي انها غير مقننة ، فان ذلك لايعني عدم انطباق القانون الدولي الانساني عليها ، فوفقاً لدليل تالين الذي عده مجموعة من الخبراء ، وعلى الرغم من انه اول محاولة لتكييف الهجمات السيبرانية ، وعلى الرغم من عدم الزاميته ، فانه عرف الهجوم السيبراني ، بموجب, القانون الدولي الانساني بوصفه "عملية إلكترونية سواء أكانت هجومية، أم دفاعية يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الاضرار بأعيان او تدميرها. وبالتالي في حال ثبوت ان الهجمات السيبرانية قد تؤدي اثار اقتصادية وعسكرية ومدنية ، او يكون استخدامها لرد او شن عدوان فانها مشمولة باحكام المادة (٥١) والمادة (٢/٤) من ميثاق الامم المتحدة في حال اللجوء اليها. وعند مراجعة مبادئ القانون الدولي

الانساني المتمثلة بالضرورة العسكرية والتناسب والتمييز ، نجد انها اكدت على مبادئ مشتركة يمكن تطبيقهاعلى الهجمات السيبرانية ، واستنادا للضرورة العسكرية قانها تنشئ تحديا امام استخدامها في الهجمات الرقمية ، لصعوبة مايمكن اعتباره هدفاً عسكرياً ، وبالتالي فان عدم وجود معايير ثابتة لاستخدام التكنلوجيا العصرية لاهداف عسكرية ، يجوز من باب الضرورة العسكرية الرد على الهجمات السيبرانية في حال اللجوء اليها، وهذا ظهر جلياً في التصريحات الامريكية والروسية في استخدام الهجمات السيبرانية في حال تعرض المنشأت النووية واجهزة الاتصالات والمنشأت الحيوية الى هجمات سيبرانية من باب الضرورة العسكرية . وبالنسبة لمبدأ التناسب الذي اكد على ان الميزة العسكرية يجب ان تكون متناسبة مع الاضرار الجانبية التي تحصل اثناء الهجوم ، وعلى الرغم من صعوبة تطبيق هذا المبدأ في الفضاء الالكتروني ، الا ان مبدأ تالين اكد على حظر الهجمات العشوائية الالكترونية التي قد تلحق اضراراً بالغة في المدنيين والاعيان المدنية قد تكون مفرطة مقارنة بالميزة العسكرية المتوخاة من الهجوم. ولو حاولنا تطبيق مبدأ التناسب في السياق السيبراني، فإن المشكلة تكمن في تقدير هذا المبدأ في إطار سرعة الاستجابة من جهة، والطبيعة السرية للهجمات السيبرانية من جهة أخرى، والتي قد يكون من الصعب تحديد حجمها وآثارها، فضلاً عن ذلك وفيما يتعلق برد الفعل السيبراني، فيصعب حساب التناسب مسبقاً أيضا، بسبب ترابط أنظمة المعلومات[٢٩]. وبالنسبة لمبدأ التمييز ، الذي يؤكد على التمييز بين المدنيين والمقاتلين ، وبين التمييز بين الاهداف العسكرية والمدنية ، والذي اجاز لأطراف النزاع توجيه عملياتها ضدّ الأهداف العسكرية دون غيرها، وبالتالي، يحظر شنّ الهجمات العشوائية[٣٠]. وقد أكدت هذا المبدأ محكمة العدل الدولية بقولها انه يجب على كافة الاطراف توجيه هجماتها العسكرية ضد المقاتلين والاهداف العسكرية حصراً، وبالتالي في حال وجود هجوم سيبراني فان يجب ان يوجه للحواسيب والانظمة العسكرية للعدو باعتبارها اهداف عسكرية مشروعة يمكن مهاجمتنها ، ولايجوز توجيه الهجمات السيبرانية ضد حواسيب او انظمة معلوماتية مدنية قد تلحق عند استهدافها اضراراً بالمدنيين بصورة مباشرة[٣١]. ونرى : ان الاراء التي تنادي بعدم انطباق اقانون الدولي الانساني على الهجمات السيبرانية ، تجافي الحقيقة ، حتى لو سلمنا جدلاً ان اتفاقيات القانون الدولي الانساني لم تعالج او تقنن الهجمات السيبرانية ، الا ان هذا لايعني عدم تطبيقه عليها ، 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 . وبالتالي فان شرط مارتنز [٣٢]، يطبق على الهجمات السيبرانية حتى لو كانت غير مقننة وفق قواعد القانون الدولي الانساني، كما ان محكمة العدل الدولية في رأيها في مواجهة التهديد واستخدام الاسلحة النووية ، وضعت تفسيرات جديدة للقانون الدولي الانساني الهدف منها الزام الدول بعدم استخدام الاسلحة الفتاكة بحجة عدم وجود قيود قانونية تحظر استخدامها[٣٣] ، كا اكدت ان المبادئ السامية للقانون الدولي الانساني ، تبقى منطبقة على جميع الاسلحة الجديدة بما في ذلك الاسلحة النووية[٣٤] ، وبالتالي فان هذا المضمون ينطبق على الهجمات السيبرانية التي تعد من وسائل واساليب الحرب المعاصرة.

المطلب الثاني : التوصيف القانوني للمدنيين المشاركين في الهجمات السيبرانية : لقد افضت المتغيرات السريعة في مجال تكنلوجيا المعلومات ، ودخولها واستخدامها في كافة جوانب الحياة ، ومنها الاستخدامات العسكرية ، الى بروز هجمات جديدة تختلف عن الهجمات التقليدية سميت الهجمات السيبرانية استهدفت الشبكة الدولية للمعلومات. وتنوع اثرها على مرتكبي هذه الجرائم . وغالباً ماترتكب هذه الجرائم من مدنيين مختصين في الشبكة العنكوبتية ، يمتلكون قدرات فائقة في التسلل والاختراق ، يعملون لحسابهم الشخصي او في شركات خاصة او تقوم الدولة بتوظيفهم ، وبالتالي يطرح تسأول مهم ، هل يعد الاشخاص الذين يقومون بالهجمات السيبرانية مدنيون لايجوز استهدافهم ويجب توفير الحماية اللازمة لهم ؟ ام يعدون مقاتلين يمكن استهدافهم باعتبارهم يشاركون في الاعمال القتالية المباشرة ابان شنهم للهجمات السيبرانية ؟.

الفرع الأول : مفهوم المهاجم الالكتروني : تتميز الهجمات السيبرانية بأنها تتم بواسطة شخص أو أكثر باستخدام جهاز كمبيوتر مزوّد بعددٍ كبير من الفيروسات، ويتم إرسالها إلى الهدف المراد إلحاق الضرر به، ويمكن أن يكون الضرر ماديًا أو معنويًا. وعليه، فإن الهجمات السيبرانية ليست سلاحًا تقليديًا، ولا ترقى لأن تكون سلاح دمار شامل وذلك نظرًا للأضرار الناتجة عنها. لقد تعددت التسميات لمرتكبي الهجمات السيبرانية ، فقد تم توصيفهم (بالهكر) او(قراصنة المعلوماتية) او (المجرم الالكتروني) او (مجرم الانترنت) او مجرم التقنية . فالمجرم الالكتروني الذي يقوم بالهجوم السيبراني هو " المجرم الذي لديه القدرة على تحويل لغته الى لغة رقمية واستخدامها من خلال الشبكة المعلوماتية بالقيام بفعل او الامتناع عنه"[٣٥]. او هو كل شخص طبيعي او معنوي تتوفر لديه المعرفة التقنية والتي يستخدمها في الفضاء الالكتروني لشن هجمات سيبرانية[٣٦] ، او هو كل مجرم سلك التقنية في

استخدام جرائمه[٣٧]. اما مجرم الانترنت (Hacker) فهو غالبًا شخص ذو إمكانيات برمجية وتقنية عالية في التعامل مع البرامج والشبكات وبنية الحاسب[٣٨]، تعطيه القدرة على استغلال الثغرات الأمنية في البرامج والأنظمة والمواقع الإلكترونية، لأهداف مختلفة قد تكون السرقة، أو التشهير، أو التخريب، او سرقة البيانات، أو حتى العبث لإثبات كفائته العالية. وأطلقت كلمة (Hacker) أساسا على مجموعة من المبرمجين الأذكياء الذين كانوا يتحدون الأنظمة المختلفة ويحاولوا اقتحامها، وليس بالضرورة أن تكون في نيتهم ارتكاب جريمة أو حتى جنحة، ولكن نجاحهم في الاختراق يعتبر نجاحا لقدراتهم ومهارتهم. إلا أن القانون اعتبرهم دخلاء تمكنوا من دخول مكان افتراضي لا يجب دخوله[٣٩]. كما عرف مجرم الانترنت بانه " كل شخص ذو صلاحية وكفاءة واهلية تقنية تمنكه من الاختراق وشن الهجمات السيبرانية ، وارتكاب افعال تقنية عبر الفضاء الالكتروني ، لايستطيعون مباشرتها عامة الناس حتى لو كانت لديهم معرفة باستخدام الحواسيب والانترنت[٤٠] .

ويتميز مرتكب الهجمات السيبرانية سواء كان مجرما للهجمات الالكترونية او مجرما عبر الانترنت ، بالتخصص الدقيق ، والخبرة ، والقدرة على الاختراق ،والذكاء الخارق ، والقدرة على التخفي.

الفرع الثاني : التوصيف القانوني لمرتكب الهجمات السيبرانية : سواء كان مرتكب الهجمات السيبرانية (Hacker) او(قراصنة المعلوماتية) او (المجرم الالكتروني) او (مجرم الانترنت) او مجرم التقنية ، يعمل لحسابه الشخصي او لحساب دولة او شركة خاصة ، فهل يمكن اعتباره مدنيا عند قيامه بشن هجوم سيبراني في نزاع مسلح دولي او غير دولي ، وبالتالي عدم جواز استهدافه ، او يمكن اعتباره مقاتلا ، كون الهجمات السيبرانية التي يقوم بها تعد من الاعمال القتالية المباشرة وبالتالي يجوز استهدافه ؟. ولغرض الاجابة على هذا التسأول ، وعلى الرغم من الهجمات السيبرانية حديثة ، الا ان القانون الدولي الانساني وضع لنا معايير للتمييز بين المقاتلين والمدنيين. فالمقاتل أو المقاتلين هم "جميع الأشخاص الذين يحق لهم وفقاً لقواعد القانون الدولي مباشرة الأعمال القتالية وبالتالي هم وحدهم الذين يجوز توجيه الإعمال العدائية ضدهم، ما يجعلهم الوحيدين المسموح بقتلهم او جرحهم او أسرهم وذلك وفقآ للقيود التي يضعها القانون الذي يحكم العمليات القتالية"[٤١]. ومصطلح "مباشرة الأعمال القتالية" أو ما يسمى" بالمشاركة المباشرة[٤٢]"، فأنه يقصد به "أعمال محددة يقوم بها الأفراد كجزء من سير العمليات العدائية بين الأطراف في النزاع"[٤٣]. وأما مصطلح المدني فقد جاء البروتوكول الإضافي الأول في المادة (٥٠) ما يلي:"١..... اي شخص لا ينتمي إلى

فئة من فئات الأشخاص المشار إليها في البنود الأول والثاني والثالث والسادس من الفقرة (أ) من المادة الرابعة من الاتفاقية الثالثة والمادة (٤٣) من هذا الملحق" البروتوكول"، وإذا ثار الشك حول ما إذا كان الشخَص ما مدنياً أم غير مدني فإن ذلك الشخص يعد مدنياً". وعلى هذا يشير تعريف الشخص المدني إلى هؤلاء الذين يتمتعون بالحصانة ضد الهجمات المباشرة مالم يقوموا بدور مباشر في العمليات العدائية وعلى مدا الوقت الذي يقومون خلاله بهذا الدور[٤٤]. فلا يجوز للعدو توجيه الأعمال العدائية بصورة مباشرة أم غير مباشرة ضد المدنيين ويجب توفير ضمانات احترام حياتهم وممتلكاتهم ماداموا من جانبهم يقفون موقفاً سلبياً ولا يأتون ضد قوات العدو عملاً من الأعمال القتالية التي تضر بأفراد القوات المسلحة المعادية أو بمجهودها الحربية[٤٥]. ويحق للمدنيين المحميين احترام حياتهم وكرامتهم حقوقهم الشخصية ومعتقداتهم السياسية والدينية وغيرها، ويجب عدم تعرض هؤلاء للتعذيب أو المعاملة القاسية أو المهينة أو العقاب البدني، ويجب أن يكون هؤلاء محميين من جميع أعمال العنف أو الانتقام. لكن في حال قيام المدنيين بالمشاركة بالاعمال القتالية المباشرة الذي يقصد بها "أعمال محددة يقوم بها الأفراد كجزء من سير العمليات العدائية بين الأطراف في النزاع"[٤٦]، فأن الحماية المعززة لهم بموجب اتفاقيات القانون الدولي الانساني تسقط عنهم بقيامهم باعمال قتالية . ومن الملاحظ عدم وجود قاعدة مدونة أو عرفية، ضمن القانون الدولي الانساني، تحظر على المدنيين المشاركة المباشرة في الهجمات السيبرانية التي ترقى إلى العمليات العدائية، وفي حال المشاركة، فسيتغير الوضع القانوني وسيفقدون الحماية المخصصة لهم ويكونون عرضة للاستهداف طوال الوقت الذي يقومون بهذا الدور، وعلى حد سواء أكان النزاع المسلح دولي أم غير دولي[٤٧]. أن مراجعة النزاعات المسلحة المعاصرة، سيكشف عن أن المدنيين حاضرون ونشطون في ساحات القتال بشكل كبير، ويمكن تلخيص ذلك في دورين على وجه الخصوص: أولاً كمرتزقة أو أعضاء في شركات أمنية وعسكرية خاصة لتنفيذ عمليات عدائية سيبرانية هجومية ودفاعية، وثانيا كقراصنة (مدنيين) يقدمون مساهمات مماثلة[٤٨]. ونرى : ان الهجمات السيبرانية المرتكبة من قبل الاشخاص اذا تسببت بشكلٍ مباشر أو غير مباشر بقتلٍ أو جرح أو تدمير أو تعطيل كلي أو جزئي، تعد وسيلة قتال، أما إذا استُخدمت كجزءٍ من مخطط عسكري فتعد أسلوب قتال ، فاساس التمييز بين اعتبار الاشخاص الذين يقومون بالهجمات السيبرانية مدنيين او مقاتلين هو مبدأ المشاركة المباشرة في الاعمال العدائية ، فالمدني الذي يقوم باختراق اجهزة الحاسوب لمنشأة مدنية او قرصنة حسابات مصرفية او يقوم بالتسلسل على حسابات المستخدمين في الشبكة

العنكبوتية ، لايمكن اعتبار مايقوم به من قبيل الاعمال العدائية المباشرة ، وبالتالي يستمرون بحماية القانون الدولي الانساني باعتبارهم مدنيين ، لكن هذا الامر لايعفيهم من المسائلة الجنائية عما ارتكبوه من جرائم سيبرانية اضرت بالغير. لكن اذا كان مرتكب الهجمات السيبرانية (Hacker) او(قراصنة المعلوماتية) او (المجرم الالكتروني) او (مجرم الانترنت) او مجرم التقنية ، الذي يعمل لحسابه الشخصي او لحساب دولة او شركة خاصة ، ويشارك مشاركة مباشرة في العمليات العدائية ، ويقوم باعمال تؤثر سلباً في العمليات العسكرية أو في القدرة العسكرية لطرف من اطراف النزاع ، سواء في الهجوم أو في الدفاع، والتي يُتوقع منها أن تسبب إصابة أو وفاة للأشخاص أو إلحاق الضرر أو تدمير الأشياء، تعد بمثابة هجوم ومن قبيل الاعمال القتالية ، استناداً للبروتوكول الإضافي الأول لعام ١٩٧٧ الملحق باتفاقيات جنيف الأربعة لعام ١٩٤٩ الذي نص في الفقرة ١ من المادة ٤٩ بأن: «الهجوم هو أعمال العنف الهجومية أو الدفاعية ضد الخصم». لقد استخدم دليل تالين، معيارا أقل صرامة من معيار التوجيه التفسيري الذي قدمته اللجنة الدولية للصليب الاحمر في تبيان المقصود بالاعمال العدائية المباشرة التي ترتكب من قبل المدنيين، فالمدني الذي ينوي التسبب في ضرر كاف للتأثير على الخصم، سيعني فقدانه للحماية كمدني، بل أكثر من ذلك، إذ سينظر إليه على أنه مشارك مباشر بالاعمال العدائية ومن ثم يصبح من السهل استهدافهم[٤٩].

ونرى : ان المبدأ الاساسي في القانون الدولي الانساني انه يستمر بحماية مرتكبي الهجوم السيبراني اذا كان هذا الهجوم ليس من قبيل الاعمال العدائية المباشرة كونهم مدنيين ، لكن اذا كان مرتكبوا الهجمات السيبرانية شاركوا بشكل مباشر بالاعمال العدائية ، وقاموا بهجمات سيبرانية دعماً لطرف من اطراف النزاع على حساب طرف اخر ، فتسقط هنا عنهم حماية القانون الدولي الانساني الموجهة للمدنيين . وعلى الرغم من صعوبة التمييز بين المدنيين والمقاتلين الذي يقومون بشن هجمات سيبرانية ، الا ان الهجوم المرتكب من قبل المهاجم الالكتروني والتي تكون اثاره هي ذات تاثير اثار الهجوم العسكري الفعلي، وكان على درجة عالية من الخطورة ، كمثال استهداف المنشأت النووية ، والتحكم بحركة الملاحة الجوية والشبكات الوطنية لتوليد الطاقة ، **وينتج عنه اثار مدمرة بالخصم ، أو خسائر بالارواح البشرية [٥٠] ، فإنه يعدّ هجوما مسلحا [٥١]، والشخص الذ قام به يعد مشاركاً بالاعمال العدائية المباشرة وفق احكام القانون الدولي الانساني . ونرى: ان اعتبار الشخص الذي يشن الهجمات السيبرانية مشاركاً في الاعمال القتالية المباشرة ، انه يمكن ان يكون محل للهجوم من قبل**

احد اطراف النزاع ، وانه يعد اسيراً اذا سقط في قبضة العدو ، ويمكن مساءلته دولياً اذا كانت الهجمات السيبرانية التي قام بها تنطبق عليها اوصاف الجرائم الدولية الواردة في النظام الاساسي للمحكمة الجنائية الدولية ، ولايمكن له التذرع بكونه مدني ، او يعمل بشركة خاصة ، او تم استئجاره من قبل الدولة للقيام هذه الهجمات . فالتدخل الإلكتروني في شبكات الكمبيوتر العسكرية ، سواء من خلال الهجمات على شبكات الكمبيوتر أو استغلالها، وكذلك التنصت على المكالمات الهاتفية في القيادة العليا للخصم أو الإرسال التكتيكي، فضلاً عن استهداف المعلومات من أجل الهجوم، يمكن أن يكون كافيا لاعتبار شخص مدني مشاركا بشكل مباشر في الأعمال العدائية. ولابد من الاشارة هنا انه يمكن استهداف المدنيين الذين يتبنون شن هجمات سيبرانية مستمرة ، كالمبرمج الذي يعمل مع القوات العسكرية منذ لحظة تخطيط الهجوم الى حين تنفيذه ، او كانت وظائفهم مستمرة تتضمن التحضير والتنفيذ او اعمال قيادة ترقى الى شن هجمات قتالية مباشرة ، مما يغير وصفهم في اطار القانون الدولي الانساني من مدنيين مشمولين بالحماية الى مقاتلين يمكن استهدافهم ، باعتبارهم اهداف مشروعة[٥٢] . وهو ما نجده في الاجتهاد الذي ذهبت إليه المحكمة الجنائية الدولية ليوغسلافيا السابقة في قضية المدعي العام ضد فاتمير ليماج (Limaj Fatmir) ، فلقد ذهبت المحكمة بأن المسؤولية المباشرة عن أي جريمة ترتكب، إنما توجه ضد الشخص القائم بالتصرف المادي للجريمة سواء بالفعل أم بالامتناع. وبالقياس مع ما تقدم فان الهجمات السيبرانية فأن المسؤولية المباشرة وعلى وفق ما تقدم، تقتضي وجود أدلة دامغة بأن من استخدم برمجيات سيبرانية، كان يعي ومتوقع بأن الظروف المحيطة بالعملية الهجومية تصادف وعلى نحو أكيد وقوع انتهاكات جسيمة، ففي هذه الحالة يكون المستخدم مسؤولاً مسؤولية مباشرة، سواء أكان مسيطر على قرارات البرمجيات بنفسه، أم قام بتنشيط برمجيات ذاتية القرار[٥٣].

الخاتمة:(Conclusion).

لقد توصلنا من خلال بحثنا هذا الى جملة من النتائج والتوصيات نورها في الاتي:

النتائج:

١_ يعد مفهوم الهجمات السيبرانية من المواضيع الحديثة ، ولم يكن القانون الدولي الإنساني واتفاقيات جنيف الاربعة لعام ١٩٤٩ التي نظمت اوضاع النزاعات المسلحة قد عرفت الهجمات السيبرانية او وضعت ضوابط لها ، لكن هذا لايعني من عدم وجود ضوابط قانونية يمكن تطبيقها عليها.

٢_ لقد اصبح الفضاء الرقمي ساحة للقتال بين الاطراف المتنازعة ، بدلاً من ميادين القتال التقليدية ، مما ادى الى وجود سباق دولي للسيطرة على الاسلحة السيبرانية.

٣_ اظهرت النزاعات المسلحة المعاصرة صعوبة وضع اليات رادعة للحد من استخدام الهجمات السيبرانية .

٤_ ان المدنيين الذين يقومون بالهجمات السيبرانية لايمكن التذرع بكونهم مدنيين ، كونهم يشاركون من خلال هذه الهجمات باعمال عدائية مباشرة.

٥_ اجمع الفقهاء الدوليين بخضوع الهجمات السيبرانية للقانون الدولي وبالخصوص تطبيق دليل تالين وشرط مارتنز على هذه وبالتالي قيام المسؤولية الدولية الفردية للمدنيين عن هذه الهجمات.

٦_ جاء المجال الخامس للفضاء السيبراني ليشكل مجالا دوليا حديثا لممارسة نشاط الانسان في المجال العسكري والمدني يضاف الى المجالات الاربعة الفضاء الخارجي ، البر، البحر ، الجو.

التوصيات:

١_ تعديل اتفاقيات القانون الدولي الانساني بشكل يواكب التطورات المعاصرة للهجمات السيبرانية .

٢_ مطالبة الحكومات بتعزيز الامن السيبراني والتعاون على المستوى الدولي والاقليمي في مجال مكافحة الهجمات السيبرانية .

٣_ مطالبة الامم المتحدة بضرورة عقد اتفاقية دولية خاصة بالهجمات السيبرانية .

٤_ مطالبة الدول بحظر استخدام المدنيين في اطار تنفيذ الهجمات السيبرانية .

٥_ مطالبة الدول بادخال مفاهيم الهجمات السيبرانية والامن السيبراني في المناهج التعليمية للقانون الدولي الانساني.

المصادر والمراجع: (Sources).

الكتب:

١. أحمد عبيس الفتلاوي وقاسم محمد مهدي الغزي، الدليل إلى فهم الهجمات السيبرانية العدوانية ، منشورات زين الحقوقية ، بيروت ، لبنان، ٢٠٢٤.

٢. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، ط١، مكتبة زين الحقوقية والأدبية، بيروت، لبنان ، ٢٠١٨.

٣. اسامة احمد المناعسة، بلال محمد الزغبي ، جرائم الحاسب الالي والانترنت، ط١، دار وائل ، عمان ، الاردن ،٢٠١٠.
٤. اسماعيل عبد الرحمن، الأسس الأولية للقانون الإنساني الدولي- في القانون الدولي الإنساني- دليل التطبيق على الصعيد الوطني، إعداد نخبة من المتخصصين والخبراء، تقديم احمد فتحي سرور، بعثة اللجنة الدولية للصليب الأحمر، القاهرة، ٢٠٠٦.
٥. توريه، حمدون , الاستجابة الدولية للحرب السيبرانية، البحث عن الامن السيبراني، الناشر الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء، ٢٠١١.
٦. جوزيف س. ناي الابن، المنازعات الدولية: مقدمة للنظرية والتاريخ، ترجمة: أحمد أمين الجمل، ومجدي كامل (القاهرة: الجمعية المصرية لنشر المعرفة والثقافة العالمية، ١٩٩٧.
٧. زهراء محمد كلانتر ، الهجمات السيبرانية ومسؤولية الدول عنها ، إصدارات مركز البيدر للدراسات والتخطيط، العراق ، بغداد ، ٢٠١٥.
٨. عادل عبدالصادق، الفضاء الإلكتروني والعلاقات الدولية: دراسة في النظرية والتطبيق، المكتبة الأكاديمية، القاهرة ، ٢٠١٦.
٩. علي محمد كاظم الموسوي، المشاركة المباشرة في الهجمات السيبرانية، المؤسسة الحديثة للكتاب، لبنان، ٢٠١٩.
١٠. عمار عباس الحسيني، جرائم الحاسوب والانترنت (الجرائم المعلوماتية)، ط١، منشورات زين الحقوقية، بيروت ، ٢٠١٧.
١١. عمر محمد ابو بكر يونس،الجرائم الناشئة عن استخدام الانترنت، الاحكام الموضوعية والجوانب الاجرائية ، دار النهضة العربية ، القاهرة ،٢٠٢٤.
١٢. فرانسواز بوشيه سولنييه ، القاموس العملي للقانون الإنساني، دار العلم للملايين، لبنان ، ٢٠٠٦.
١٣. محمد نور فرحات، تاريخ القانون الدولي الإنساني والقانون الدولي لحقوق الإنسان- دراسات في القانون الدولي الإنساني، مكتبة زين الحقوقية ، لبنان ، ٢٠٢٠.
١٤. ميلزر نيلس، دليل التفسيري لمفهوم المشاركة المباشرة في العمليات العدائية بموجب القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر، ٢٠١٠.
١٥. هينين ويجنر، مفهوم بشأن السلام السيبراني، البحث عن السلام السيبراني، البحث عن السلام السيبراني، الناشر الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء، ٢٠١٩.
المجلات:

١. أحمد عبيس نعمة الفتلاوي وزهراء عماد محمد ، تكييف الهجمات السيبرانية في ضوء االقانون الدولي ، مجلة الكوفة للعلوم القانونية والسياسية ، المجلد (٤٤) العدد(١) ، كلية القانون والعلوم السياسية ، جامعة الكوفة ، الكوفة ، النجف ، ٢٠٢٠.

٢. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية، مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية ، العددالرابع/ السنة الثامنة ، ٢٠١٦.

٣. أشرف محمد عبدالله غرايبه، وسائل وأساليب القتال في إطار القانون الدولي الإنساني، مجلة البحوث القانونية والاقتصادية ، جامعة صحار، عمان ، المجلد ١١، العدد ٧٧ ، ٢٠٢١.

٤. بكوش محمد امين وهروال نبيلة هبة ، خصوصية المجرم الالكتروني _ مجرم الانترنت نموذجاً، العدد(١) المجلد(٧) ، مجلة البحوث والحقوق في العلوم السياسية ، جامعة تيارات ، الجزائر، ٢٠٢١.

٥. بن تغري موسى، الحرب السيبرانية والقانون الدولي الأنساني، مجلة الاجتهاد القضائي ، المجلد (١٢) العدد(٢٢) ، مخبر الاجتهاد القضائي على حركة التشريع، جامعة محمد خُضر ، بسكرة، الجزائر ، ٢٠٢٠.

٦. حامد محمد علي البلداوي ، مواجهة الحرب السيبرانية في قواعد القانون الدولي الانساني، مجلة الجامعة العراقية ، العدد ٥٧،ج٢، العراق ، بغداد ، ٢٠٢٣.

٧. سلافة طارق الشعلان ، تكييف استخدام الحرب الالكترونية قي النزاعات المسلحة، مجلة الكوفة للعلوم القانونية والسياسية ، المجلد (١) العدد(٢٦) ، كلية القانون القانون جامعة الكوفة ، الكوفة ، ٢٠١٦.

٨. سهام جليلي ، خصوصية المجرم الالكتروني ، مجلة المفكر ، العدد ١٥ ، كلية الحقوق والعلوم السياسية ، جامعة محمد خيضر، بسكرة ، الجزائر ، ٢٠١٧.

٩. شويرب جيلالي ، مفهوم الحروب السيبرانية والأمن السيبراني، مجلة الحقوق والحريات ، جامعة الدكتور يحيى فارس المدية ، كلية الحقوق والعلوم السياسية، المجلد ١١ ، العدد ١، الجزائر، ٢٠٢٣.

١٠. طلال ياسين العيسى وعدي محمد عناب ، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الإنسانية – المجلد ١٩ ، العدد١، ٢٠١٩.

١١. كرار عباس متعب فرج ، الحرب السيبرانية: دراسة في استراتيجية الهجمات السيبرانية بين الولايات المتحدة الامريكية وإيران، مجلة حمورابي للدراسات، جامعة كربلاء ، العدد ٤٠ ، ٢٠٢١.
١٢. مايكل ن. شميت، "الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر (الحاسوب)والقانون في الحرب"، المجلة الدولية للصليب الأحمر، مختارات من أعداد ٢٠٠٢.
١٣. موسى طالب حسن ، عمر محمود، الإنترنت قانونا، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة، العدد٦٧، ٢٠١٦.
١٤. ناجي محمد أسامة الشاذلي، الجوانب القانونية للحرب السيبرانية دراسة في اطار القانون الدولي الإنساني، مجلة روح القوانين، العدد ١٠٣، المجلد ٣٥، ج٢، جامعة طنطا، كلية الحقوق، مصر، ٢٠٢٣.
١٥. هربرت لين، النزاع السيبراني والقانون الدولي الأنساني، مجلة اللجنة الدولية للصليب الأحمر، مجلد ٩٤(٨٨٦)، ٢٠١٢.

الرسائل والاطاريح:

١. صالح حيدر عبدالواحد ، حروب الفضاء الألكتروني ، دراسة في مفهومها، رسالة ماجستير ، كلية الاداب والعـــــلوم، جامعة الشرق الأوسط ، ٢٠٢١.
٢. طوزان احمد ، قانون النزاعات المسلحة ، رسالة ماجستير، الجامعة الافتراضية السورية ، سوريا ، ٢٠٢٠.
٣. مصطفى بن عصام نعوس، التنظيم الدولي للأنترنيت، اطروحة دكتوراه مقدمة الى مجلس كلية الحقوق جامعة حلب، سوريا،٢٠١١.
٤. نور أمير الموصلي ، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، رسالة ماجستير ، الجامعة الافتراضية السورية ، دمشق ، ٢٠٢١ .

القرارات الدولية:

١. قرار الجمعية العامة للأمم المتحدة المرقم (٣٣١٤) في ١٤ كانون الأول /ديسمبر, ١٩٧٤.

المواقع الالكترونية:

1)Myriam Dunn, "The Cyberspace Dimension in Armed Conflict: Approaching a Complex Issue with Assistance of the Morphological Method", Information and Security: An International Journal7 (2001): 145-158, online earticle, http://procon.bg/system/files/07.08_Dunn.pdf

٢. سعيد عطا الله ، الهكر (Hacker). ما هو وما هي انواعه ، مقال متاح على الموقع الالكتروني:
https://www.arageek.com/l/%d9%85%d8%a7-%d9%87%d9%88-%d8%a7%d9%84%d9%87%d9%83%d8%b1
٣ .القانون الدولي الإنساني والسياسات بشأن الأسلحة ونزع السلاح ، مقال متاح على الموقع الالكتروني:
https://www.icrc.org/ar/law-and-policy/weapons-and-disarmament.
٤. إبرز أنواع الهجمات السيبرانية حتى عام ٢٠٢١، مقال متاح على الموقع الالكتروني:
https://www.rmg-sa.com/ .
٥. ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟، مقال منشور على موقع اللجنة الدولية للصليب الأحمر، متاح على الرابط:
https://www.icrc.org/ar/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm.

المصادر الأجنبية:

1)D.Brown, Proposal for an international convention to regulate the use of information System in Armed Conflict, Harvard International Law review, Vol.47.

2)H.P.Gasser, international humanitarian Law in Introduction, Henery Dunat Institute, 1993.

3)Hathaway, Oona A. & Others: "The Law of Cyber-Attack", Op.cit.

الهوامش

(١) أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، ط١، مكتبة زين الحقوقية والأدبية، بيروت، لبنان، ٢٠١٨، ص١١.

(٢) أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية، مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية ، العددالرابع/ السنة الثامنة ، ٢٠١٦، ص ٦١٤.

(٣) أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مصدر سابق ، ص ٦١٤.

(٤) ناجي محمد أسامة الشاذلي، الجوانب القانونية للحرب السيبرانية دراسة في اطار القانون الدولي الإنساني، مجلة روح القوانين، العدد ١٠٣، المجلد ٣٥، ج٢، جامعة طنطا، كلية الحقوق، مصر، ٢٠٢٣، ص ١٢٢٦.

(٥) علي محمد كاظم الموسوي، المشاركة المباشرة في الهجمات السيبرانية، المؤسسة الحديثة للكتاب، لبنان، ٢٠١٩، ص١٠٢.

(٦) عادل عبدالصادق، الفضاء الإلكتروني والعلاقات الدولية: دراسة في النظرية والتطبيق المكتبة الأكاديمية، القاهرة ، ٢٠١٦، ص ٢٢-٢٦.

٧( ) احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مصدر سابق ، ص ٦١٥.

٨( ) كرار عباس متعب فرج ، الحرب السيبرانية: دراسة في استراتيجية الهجمات السيبرانية بين الولايات المتحدة الامريكية وايران، مجلة حمورابي للدراسات، جامعة كربلاء ، العدد ٤٠ ، ٢٠٢١ ، ص٢٠٠.

٩( ) أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، مصدر سابق، ص١٦.

١٠( ) شويرب جيلالي ، مفهوم الحروب السيبرانية والأمن السيبراني، مجلة الحقوق والحريات ، جامعة الدكتور يحيى فارس المدية ، كلية الحقوق والعلوم السياسية، المجلد ١١ ، العدد ١، الجزائر، ٢٠٢٣ ، ص ١٦١.

١١( ) هربرت لين، النزاع السيبراني والقانون الدولي الأنساني، مجلة اللجنة الدولية للصليب الأحمر، مجلد ٩٤(٨٨٦)، ٢٠١٢، ص ٥١٨.

(١٢) Myriam Dunn, "The Cyberspace Dimension in Armed Conflict: Approaching a Complex Issue with Assistance of the Morphological Method", Information and Security: An International Journal7 (2001): 145-158, online earticle, http://procon.bg/system/files/07.08_Dunn.pdf

(١٣) عادل عبد الصادق، مصدر سابق ، ص ١٠-١٢.

(١٤) مصطفى بن عصام نعوس، التنظيم الدولي للأنترنيت، اطروحة دكتوراه مقدمة الى مجلس كلية الحقوق جامعة حلب، سوريا،٢٠١١، ص.١٩٤

١٥) صالح حيدر عبدالواحد ، حروب الفضاء الألكتروني ، دراسة في مفهومها، رسالة ماجستير ، كلية الاداب والعـــــلوم، جامعة الشرق الأوسط ، ٢٠٢١، ص ٢٦. وجوزيف س. ناي الابن، المنازعات الدولية: مقدمة للنظرية والتاريخ، ترجمة: أحمد أمين الجمل، ومجدي كامل (القاهرة: الجمعية المصرية لنشر المعرفة والثقافة العالمية، ١٩٩٧، ص ٨٢.

١٦) نور أمير الموصلي ، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، رسالة ماجستير ، الجامعة الافتراضية السورية ، دمشق ، ٢٠٢١ ، ص ١٦. و طلال ياسين العيسى وعدي محمد عناب ، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الإنسانية – المجلد ١٩ ، العددا، ٢٠١٩، ص ٨٦. وانظر ايضاً إبرز أنواع الهجمات السيبرانية حتى عام ٢٠٢١، مقال متاح على الموقع الالكتروني:
https://www.rmg-sa.com/ تاريخ الزيارة ٦/١/ ٢٠٢٤.

١٧) عمار عباس الحسيني، جرائم الحاسوب والانترنت (الجرائم المعلوماتية)، ط١، منشورات زين الحقوقية، بيروت ، ٢٠١٧، ص ١٤٠_١٤١.

١٨) فرانسواز بوشيه سولنييه ، القاموس العملي للقانون الإنساني، دار العلم للملايين، لبنان ، ٢٠٠٦، ص١٦٧.

١٩) أشرف محمد عبدالله غرايبه، وسائل وأساليب القتال في إطار القانون الدولي الإنساني، مجلة البحوث القانونية والاقتصادية ، جامعة صحار، عمان ، المجلد ١١، العدد ٧٧ ، ٢٠٢١، ص ٢٤٤-٣٣٤.

[٢٠] القانون الدولي الإنساني والسياسات بشأن الأسلحة ونزع السلاح ، مقال متاح على الموقع الالكتروني: https://www.icrc.org/ar/law-and-policy/weapons-and-disarmament تاريخ الزيارة ٢٠٢٤/٧/١.

[٢١] ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟، مقال منشور على موقع اللجنة الدولية للصليب الأحمر، متاح على الرابط: تاريخ الزيارة ٢ / ٧ / ٢٠٢٤ . https://www.icrc.org/ar/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm.

[٢٢] موسى طالب حسن ، عمر محمود، الإنترنت قانونا، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة، العدد ٦٧، ٢٠١٦، ص٣٤٠.

23)D.Brown, Proposal for an international convention to regulate the use of information System in Armed Conflict, Harvard International Law review, Vol.47, p. 179.

[٢٤] حامد محمد علي البلداوي ، مواجهة الحرب السيبرانية في قواعد القانون الدولي الانساني، مجلة الجامعة العراقية ، العدد ٥٧،ج٢، العراق ، بغداد ، ٢٠٢٣، ص٣٥٧. وانظر زهراء محمد كلانتر ، الهجمات السيبرانية ومسؤولية الدول عنها ، إصدارات مركز البيدر للدراسات والتخطيط، العراق ، بغداد ، ٢٠١٥ ، ص٩. وانظر: أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية، مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مصدر سابق ، ص٦٢٨.

[٢٥] توريه، حمدون , الاستجابة الدولية للحرب السيبرانية، البحث عن الامن السيبراني، الناشر الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء، ٢٠١١, ص٨٩.

[٢٦]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.

وانظر ايضاً: حامد محمد علي البلداوي ، مصدر سابق ، ص ٣٥٨.

[٢٧] صالح حيدر عبد الواحد ، مصدر سابق، ص٥٠.

[٢٨] القانون الدولي الانساني والعمليات السيبرانية خلال النزاعات المسلحة ، ورقة موقف اللجنة الدولية للصليب الاحمر ، ٢٠١٩ ، ص٤ ، متاح على الموقع الالكتروني : تاريخ الزيارة ٢٠٢٤/٧/١ https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl_and_cyber_operations_during_armed_conflict_ar.pdf.

[٢٩] أحمد عبيس الفتلاوي وقاسم محمد مهدي الغزي، الدليل إلى فهم الهجمات السيبرانية العدوانية ، منشورات زين الحقوقية ، بيروت ، لبنان، ٢٠٢٤، ص١٦٣.

[٣٠] أنظر: (البروتوكول الاضافي الاول لعام ١٩٧٧ المادة ٤٨) ، والقواعد(٧ و١١ - ١٣) من القانون الدولي الإنساني العرفي.

[٣١] بن تغري موسى، الحرب السيبرانية والقانون الدولي الأنساني، مجلة الاجتهاد القضائي ، المجلد (١٢) العدد(٢٢) ، مخبر الاجتهاد القضائي على حركة التشريع، جامعة محمد خُضر ، بسكرة، الجزائر ،٢٠٢٠ ، ص٢٠٩.

[٣٢] مايكل ن. شميت، "الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكمبيوتر (الحاسوب)والقانون في الحرب"، المجلة - الدولية للصليب الأحمر، مختارات من أعداد ٢٠٠٢ م ، ص ٩.

[٣٣] سلافة طارق الشعلان ، تكييف استخدام الحرب الالكترونية في النزاعات المسلحة، مجلة الكوفة للعلوم القانونية والسياسية ، المجلد (١) العدد(٢٦) ، كلية القانون القانون جامعة الكوفة ، الكوفة ، ٢٠١٦ ، ص٢٥.

[٣٤]) احمد عبيس نعمة الفتلاوي وزهراء عماد محمد ، تكييف الهجمات السيبرانية في ضوء االقانون الدولي ، مجلة الكوفة للعلوم القانونية والسياسية ، المجلد (٤٤) العدد(١) ، كلية القانون والعلوم السياسية ، جامعة الكوفة ، الكوفة ، النجف ، ٢٠٢٠، ص ٦٤.

[٣٥]) سهام جليلي ، خصوصية المجرم االلكتروني ، مجلة المفكر ، العدد ١٥ ، كلية الحقوق والعلوم السياسية ، جامعة محمد خيضر، بسكرة ، الجزائر ، ٢٠١٧، ص٤٠١.

[٣٦]) بكوش محمد امين وهروال نبيلة هبة ، خصوصية المجرم االلكتروني _ مجرم الانترنت نموذجاً، العدد(١) المجلد(٧) ، مجلة البحوث والحقوق في العلوم السياسية ، جامعة تيارات ، الجزائر، ٢٠٢١، ص٧٦.

[٣٧]) عمر محمد ابو بكر يونس،الجرائم الناشئة عن استخدام الانترنت، الاحكام الموضوعية والجوانب الاجرائية ، دار النهضة العربية ، القاهرة ،٢٠٢٤، ص٢٣٣.

[٣٨]) اسامة احمد المناعسة، بلال محمد الزغبي ، جرائم الحاسب االلي والانترنت، ط١، دار وائل ، عمان ، الاردن ،٢٠٠١، ص٨١.

[٣٩]) سعيد عطا الله ، الهكر Hacker.. ما هو وما هي انواعه ، مقال متاح على الموقع االلكتروني: تاريخ الزيارة ٤/ ٧ / ٢٠٢٤.
https://www.arageek.com/l/%d9%85%d8%a7-%d9%87%d9%88-%d8%a7%d9%84%d9%87%d9%83%d8%b1

[٤٠]) عمر محمد ابو بكر يونس، المصدر السابق ، ٢٣٧.

[٤١]) محمد نور فرحات، تاريخ القانون الدولي الإنساني والقانون الدولي لحقوق الإنسان- دراسات في القانون الدولي الإنساني، مكتبة زين الحقوقية ، لبنان ، ٢٠٢٠ ، ص ٨٤.

[٤٢]) ميلزر نيلس، دليل التفسيري لمفهوم المشاركة المباشرة في العمليات العدائية بموجب القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر،٢٠١٠، ص ٤١_٤٢. .

[٤٣]) اسماعيل عبد الرحمن، الأسس الأولية للقانون الإنساني الدولي- في القانون الدولي الإنساني- دليل التطبيق على الصعيد الوطني، إعداد نخبة من المتخصصين والخبراء، تقديم احمد فتحي سرور، بعثة اللجنة الدولية للصليب الأحمر، القاهرة، ٢٠٠٦، ص ٢١.

[٤٤]) H.P.Gasser, international humanitarian Law in Introduction, Henery Dunat Institute, 1993,P:53.

[٤٥]) ميلزر نيلس ، مصدر سابق ، ص ٤٢.

[٤٦]) اسماعيل عبد الرحمن ، مصدر سابق ، ص٢١. وانظر: طوزان احمد ، قانون النزاعات المسلحة ، رسالة ماجستير، الجامعة الافتراضية السورية ، سوريا ، ٢٠٢٠، ص٧٨.

[٤٧]) أحمد عبيس الفتلاوي وقاسم محمد مهدي الغزي، الدليل إلى فهم الهجمات السيبرانية العدوانية ، مصدر سابق ، ص٢٩٨.

[٤٨]) المصدر نفسه ، ص ٢٩٩.

[٤٩]) أحمد عبيس الفتلاوي وقاسم محمد مهدي الغزي، الدليل إلى فهم الهجمات السيبرانية العدوانية ، مصدر سابق ، ص٣٠٤.

[٥٠] هينين ويجنر، مفهوم بشأن السلام السيبراني، البحث عن السلام السيبراني، البحث عن السلام السيبراني، الناشر الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء،٢٠١٩، ص٧ .

[٥١] أنظر: قرار الجمعية العامة للأمم المتحدة المرقم (٣٣١٤) في ١٤ كانون الأول /ديسمبر, ١٩٧٤.

[٥٢]) Hathaway, Oona A. & Others: "The Law of Cyber-Attack", Op.cit, P40

[٥٣]) أحمد عبيس الفتلاوي وقاسم محمد مهدي الغزي، الدليل إلى فهم الهجمات السيبرانية العدوانية ، مصدر سابق ، ص٣٠٧.