Research Open Access

The Syriac War from the Perspective of International Humanitarian Law

Karar Ali Maktoof
Wasit University - College of Law
karrara266@gmail.com

Abstract : During the last decade, the international community witnessed a widespread wave of computer hardware and information network technology that revolutionized the way we live our lives with, such as flexibility in obtaining information and the adoption of many basic services and infrastructures on them. However, every matter has its negative side as well as its positive side. Despite the tremendous development of the information revolution, it has at the same time made the international community face new risks associated with this development. Cyber attacks, whose effects are not limited to data in computers or systems but rather beyond that directly affects the real world, such as hacking computer systems to control air traffic, disrupting the work of nuclear power plants, and many negative effects that may lead to catastrophic accidents, and civilians are the main victims of such war. Since international humanitarian law seeks to protect civilians, legal experts have sought to examine the extent to which its rules can be applied to cyber wars.

International humanitarian law seeks to protect civilians from the scourge of armed conflicts and hostile attacks in particular. While recognizing the seriousness of these attacks and considering cyberspace as a field for such attacks, researchers and legal experts sought to analyze the rules of international humanitarian law to examine the extent to which its rules can be applied to attack the cyber wars that take place in the context of kinetic armed conflicts or outside its context. So the problem of our research , unlike the traditional military attacks that take place in the physical field, centers on cyber wars waged in a virtual field on the Internet with its double military-civilian use. Given that the rules and principles of international humanitarian law are applicable to all activities carried out by the parties during the armed conflict, the question arises about the extent to which the rules and principles of this law apply to cyber wars?

In order to answer this problem, the subject of this research is divided into two sections: the first is the definition of the nature of cyber war and the second is explaining its characteristics. In the first section, the possibility of applying the rules of international humanitarian law to cyber warfare is displayed, while in the second the practical challenges of applying the principles of war behavior to cyber wars is discussed.

Research Open Access

الحرب السيرانية في منظور القانون الدولي الانساني

م. كرار علي مكطوف

جامعة واسط– كلية القانون

karrara266@gmail.com

المقدمة : شهد المجتمع الدولي خلال العقد الأخير موجة انتشار واسعة لتكنولوجيا الأجهزة الحاسوبية والشبكة المعلوماتية التي أحدثت ثورة في الطريقة التي نعيش بها في حياتنا، كالمرونة في الحصول على المعلومات واعتماد العديد من الخدمات والبنى التحتية الأساسية عليهم. لكن لكل أمر جانبه السلبي كما هو جانبه الإيجابي، فعلى الرغم من التطور الهائل لثورة المعلومات، إلا أنها في ذات الوقت جعلت المجتمع الدولي يواجه مخاطر جديدة مرتبطة بهذا التطور، فقد ظهرت الحرول السيبرانية التي لا تقتصر آثارها على البيانات في أجهزة الكمبيوتر أو أنظمته، بل تتجاوز ذلك لتقوم بالتأثير بشكل مباشر على العالم الحقيقي كاختراق أنظمة الكمبيوتر للسيطرة على الحركة الجوية، وتعطيل عمل محطات الطاقة النووية والعديد من التأثيرات السلبية التي قد تؤدي إلى وقوع حوادث كارثية ويكون المدنيين هم الضحايا الرئيسين لمثل هذه الحروب. وبما أن القانون الدولي الإنساني يسعى لحماية المدنيين فقد سعى الخبراء القانونيين لبحث مدى إمكانية تطبيق قواعده على الحروب السيبرانية.

يسعى القانون الدولي الانساني إلى حماية المدنيين من ويلات النزاعات المسلحة والهجمات العدائية على وجه الخصوص هو القانون الدولي الإنساني، ومع الإقرار بخطورة هذه الهجمات واعتبار الفضاء السيبراني مجالاً لتلك الهجمات، سعى الباحثون والخبراء القانونيين إلى تحليل قواعد القانون الدولي الإنساني لبحث مدى إمكانية تطبيق قواعده على الهجمات السيبرانية التي تحصل في سياق النزاعات المسلحة الحركية أو خارج سياق النزاعات المسلحة الحركية ، لذا فان مشكلة بحثنا تتمحور في بخلاف الهجمات العسكرية التقليدية التي تتم في الميدان المادي، تشن حروب سيبرانية في ميدان افتراضي على شبكة الانترنت مع ما تتميز به من استخدام مزدوج عسكري – مدني. وعلى اعتبار أن قواعد ومبادئ القانون الدولي الإنساني واجبة التطبيق على كافة الأنشطة التي تقوم بها الأطراف أثناء النزاع المسلح، حيث تثور الإشكالية حول مدى إمكانية انطباق قواعد ومبادئ هذا القانون على الحروب السيبرانية ؟ ،

وللإجابة على هذه الاشكالية فقد قسمنا موضوع البحث الى.. مبحثين،المبحث الاول ماهية الحرب السيبرانية وتم تقسيمه على مطلبين الاول التعريف بالحرب السيبرانية والثاني وضحنا فيه خصائصها اما المبحث الثاني تناولنا فيه الحرب السيبرانية في ظل القانون الدولي الانساني،احتوى على مطلبين،الاول حول مدى امكانية تطبيق قواعد القانون الدولي الانساني على الحرب السيبرانية، اما في الثاني بحثنا فيه ،التحديات العملية لتطبيق مبادئ سلوكيات الحرب على الحروب السيبرانية .

المبحث الاول

ماهية الحرب السيبرانية

سوف ننطلق في تحديد مفهوم الحرب السيبرانية، بالإشارة إلى أن قواعد القانون الدولي الإنساني، وهي القواعد القانونية المنظمة للنزاعات المسلحة، لا تنطبق على كافة العمليات الالكترونية أو ما يطلق عليه حرب سيبرانية وفقاً لعمومية المصطلح، حيث يستخدم المصطلح في مجالات عدة تقع خارج نطاق النزاع المسلح وبالتالي خارج نطاق تطبيق قواعد القانون الدولي الإنساني،لذا سنتناول في هذا المبحثين مطلبين، المطلب الاول تعريف الهجمات السيبرانية،و المطلب الثاني: خصائص الحرب السيبرانية وبعض نماذجها

المطلب الاول : تعريف الهجمات السيبرانية : يحتم علينا تعريف مصطلح الهجمات السيبرانية التركيز على جانبين، الأول على السيبرانية في اللغة، فيما سيركز الثاني على الهجمات السيبرانية اصطلاحاً من خلال استعراض التعريفات التي أوردها الفقهاء والمتخصصين في هذا الجانب .

الفرع الاول :السيبرانية في اللغة : إن كلمة سيبرانية أو سايبر أو سيبراني تعتبر ترجمة حرفية لكلمة (Cyber) والمشتقة من كلمة (Cybernetics). وقد استخدم هذا المصطلح (Cybernetics) أكاديمياً لأول مرة من قبل عالم الرياضيات الأمريكي "نوربرت وينر" عام ١٩٤٨، في كتابه الشهير: "علم التحكم الآلي: أو التحكم والاتصال في الحيوان والآلة"، وذلك للإشارة إلى "آليات التنظيم الذاتي" [١] أما فيما يتصل بالبحث عن مصدر كلمة سايبر (cyber) في المعاجم اللغة العربية فنجد أنه لا يوجد مصطلح مقارب للسايبر (Cyber) إذ جاء معنى هذه الكلمة :

١. في قاموس المورد الحديث ب "الكمبيوتري" أو "عصري جدا" كما ورد معنى مصطلح (cybernetics) بأنه "علم الضبط" أو "علم التحكم الأوتوماتيكي".[٢]
٢. وجاء في قاموس المعاني بمعنى " تخيلي"[٣] أيضاً بالاطلاع على الوثائق الصادرة عن الأمم المتحدة الصادرة باللغة العربية، ومنشورات ومقالات اللجنة الدولية للصليب الأحمر، نجد أنها تستخدم مصطلح السيبرانية. ولهذه الأسباب مجتمعة قد استخدمنا مصطلح السيبرانية في بحثنا.

الفرع الثاني :الحرب السيبرانية اصطلاحاً : 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.[٤] وعلى الرغم من غياب إجماع واسع على تعريف محدد ودقيق لمفهوم الحرب السيبرانية، إلا أن ذلك لم يمنع الفقهاء كل في تخصصه من تقديم تعاريف للإحاطة بهذا المفهوم، ومن تلك التعاريف ما ذهب إليها خبراء ومختصين في القانون الدولي الإنساني ، وأولهم الأستاذ (SHIN) الذي عرف الحرب السيبرانية بأنها: "استخدام الطيف الالكتروني أو الكهرومغناطيسي لتخزين وتعديل وتبادل البيانات وجها لوجه مع أنظمة تحكم في بنى تحتية مرتبطة بها"[٥]

ويعرفها الأستاذ (Michae lN Schmitt)الحرب السيبرانية بانها: مجموعة من الاجراءات التي تتخذها الدولة للهجوم على نظم المعلومات بهدف الاضرار بها ،وفي الوقت نفسه للدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة[٦] ، كما عّرفها كل من الأستاذ "ريتشارد كلارك" و الأستاذ "روبرت كناكي" على أنها: " أعمال تقوم بها دولة تحاول من خلالها اختارق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضارر بالغة أو تعطيلها. وعرفها الأستاذ (Marco Roscini) بأنها: "تطويع الإمكانيات الالكترونية العسكرية لأجل التأثير في مواقع الكترونية أخرى وتعطيلها أو تدميرها سواء أكانت تقدم خدمات مدنية أو عسكرية[٧]. ويعتبر آخرون أن الحرب السيب ارنية هي:" امتداد للحروب التقليدية والمادية ، إذ يتألف جندها من المدنيين والعسكريين في آن واحد، كما أنها حرب أدمغة بالدرجة الأولى، كونها تستهدف في المقام الأول تدمير البنية العلمية والمعلوماتية للهدف، وتأخذ أشكالا عدة، كشكل الاتصالات بين الجيوش وقياداتها، وإضعاف شبكات النقل والإمدادات اللوجستية، وضرب المعلومات الاقتصادية، والعبث بالمحتوى التقني والرقمي وغيرها[٨].

ويرى بعض القانونيين أن أساليب عمل الحروب السيبرانية تتقارب من ناحية قانونية مع إشاعة الرعب والإرهاب، لذلك يمكن تعريف الحروب السيبرانية استنادا لهذه النظرة القانونية بأنها: نظام قائم على الرعب المنتشر في شبكة الإنترنت، والتي تهدف إلى تنفيذ العديد من الأعمال لترويع أمن الأفراد والجماعات والمؤسسات والدول، وإدخالهم في أزمات نفسية واقتصادية وسياسية واجتماعية ناتجة عما يعرف بالإرهاب الصامت ومن التعاريف الحديثة للحرب السيبرانية نذكر تعريف مجموعة الخبراء التابعين للناتو الوارد في القاعدة ٣٠من 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[٩]

المطلب الثاني: خصائص الحرب السيبرانية وبعض نماذجها : ارتأينا في هذا المطلب ان نوضح ابرز خصائصها ومن ثم نتعرف على بعض نماذجها على الصعيد الدولي وعلى النحو التالي:

الفرع الاول : خصائص الحرب السيبرانية : تتسم الحروب السيبرانية التي توجه من خلال الفضاء السيبراني بخصائص تميزها عن غيرها وهي :

١. الحرب السيبرانية هي ذات تقنية متطورة، عكست قمة التطور الذي وصلت إليه ثورة الحروب العادية[١٠].
٢. التكلفة المتدنية نسبياً للحرب السيبرانية، فلا تحتاج الدول إلى تخصيص ميزانيات ضخمة لإنتاج أسلحتها السيبرانية على خلاف الأسلحة المستخدمة في الحروب العنيفة التقليدية ذات الكلفة العالية جداً كحاملات الطائرات والمقاتلات المتطورة[١١]
٣. الحرب السيبرانية قد تحدث في أي وقت وبمدة قصيرة من الزمن، سواء في السلم، أو في الحرب العادية.

٤. يتمتع المقاتل بميزة واضحة في الحرب السيبرانية على المدافع، لأن هذه الحروب تتميز بالسرعة والمرونة والمراوغة، فمن غير المرجح أن تنجح عقلية التحصن لوحدها، لأن التحصين في هذا الاتجاه سيجعل الجانب الآخر عرضة لمزيد من محاولات الاختراق، وبالتالي المزيد من الضغط.
٥. لا تعرف الحرب السيبرانية الحدود الجغرافية فهي متنوعة ومتطورة بوسائلها المرتبطة بأكثر المجالات التقنية تطوراً وتغيراً في الحياة المعاصرة للدول، وهي علاوة على ذلك، غير محدودة الأهداف والنتائج، إذ قد تتعدى مخاطرها ميادين القتال التقليدية لتصل بدمارها إلى أكثر المواقع السيادية والحساسة تحصيناً وبعداً عن دائرة القتال.[١٢]
٦. صعوبة تحديد موقع وشخصية القائم بالهجمات السيبرانية ذات التأثير العالي؛ لكونها لا تترك أثر أو دليل على حصولها، إذ إن معظم الهجمات السيبرانية يتم اكتشافها بالصدفة، وبعد فترة طويل وبمساعدة المهارات الفنية عالية المستوى لاكتشاف مصدر الهجوم.
٧. كذلك تتميز الحرب السيبرانية بأن بها تدمير لا تصاحبه دماء وأشلاء بالضرورة، وبسبب انتشار الفضاء السيبراني وسهولة الوصول إليه يمكن أن يزيد عدد المهاجمين وكذلك توسع دائرة المواقع المستهدفة، ولتدور تلك الهجمات المتبادلة على نحو من الكر والفر ليعبر عن حالة صراع مطولة مرتبطة بالطبيعة المتنوعة للفضاء السيبراني[١٣]

الفرع الثاني : نماذج عن الحروب السيبرانية : شهدت العديد من الدول في السنوات الأخيرة الماضية إلى عدة هجمات وحروب سيبرانية، وتتنوع ما بين تدمير أنظمة إلكترونية لمنشآت حيوية عسكرية أو مدنية . وتعطيل أو إتلاف شبكات الدفاع العسكرية عن بعد، واختراق أو تعطيل أو تدمير شبكات القطاع العام والخاص، وتعطيل البنية التحتية للدول.لذا سنحاول بيان نموذجين وعلى النحو التالي:

اولاً : الهجوم السيبراني على المواقع النووية الإيرانية : حيث تم استهداف المفاعلات النووية الإيرانية بفيروس (Stuxnet)، الذي تم اكتشافه لأول مرة في جوان ٢٠١٠، والذي يعد الأخطر على صعيد الهجمات السيبرانية لمنشآت مدنية أو عسكرية على الإطلاق، إذ تعرضت المواقع النووية الإيرانية إلى أسلوب ومنهج يقوم على شقين: الأول باستهداف أجهزة الطرد المركزية وخروجها عن السيطرة من جهة، أما الثاني فبالتحايل على أجهزة التحكم والإيحاء لها[١٤]، أن عمليات تشغيل المنشأة النووية تعمل بصورة طبيعية، إلا أنها في الواقع معطلة. وأعلنت السلطات الإيرانية أن الفيروس قد أصاب حوالي ١٦٠٠٠ جهاز كمبيوتر وذلك بعد تعرضهم لهجوم في أكتوبر ٢٠١٠، وآخر في ابريل ٢٠١١، وتسبب في تعطيل حوالي ١٠٠٠ من أجهزة الطرد المركزي المفاعل النووي الإيراني في مدينة "ناتانز"، فضلا على تعطيل البرنامج النووي الإيراني لتخصيب اليورانيوم لمدة سنتين. واتهمت إيران الولايات المتحدة الأمريكية وإسرائيل بالوقوف وراء هذا الهجوم [١٥] وقد شكل استعمال هذا الفيروس نقلة نوعية في خطورة الحروب السيبرانية التي انتقلت من تدمير البيانات وسرقتها إلى تدمير المكونات المادية نفسها ونظم التشغيل

لقطاعات حيوية مثل الطاقة النووية وهو ما يفتح الباب أمام الكثير من التكهنات بأن مثل هذه الأسلحة المتطورة يمكن أن أمرا شائعا في المستقبل[١٦]

ثانيا : الهجوم السيبراني الروسي على اوكرانيا : ان الحرب السيبرانية جزء من الحرب الهجينة ويمكن أن يكون لها تأثير في الحرب الفعلية على الأرض. فتعطيل أو اختراق بيانات وزارات الدفاع قد يغير شيئا من الحرب، لكن نشر المعلومات الكاذبة قد يكون تأثيره أعظم بحسب خبراء .

حرب من نوع آخر اندلعت قبل الحرب الفعلية في أوكرانيا. قبل يوم من الغزو الروسي لأوكرانيا أصاب الشلل مواقع حكومية مهمة في العاصمة كييف، كذلك مقار الحكومة والبرلمان ووزارة الخارجية ومؤسسات الدولة الأخرى القراصنة استعملوا ما يطلق عليه بهجمات من نوع "DDos" (الحرمان الموزع من الخدمة)، حيث أغرقت الخوادم بطلبات غير مشروعة، من خلال تحميل البنية التحتية للخوادم بشكل مرتفع، ما أدى إلى توقفها عن العمل. أوكرانيا حملت موسكو مسؤولية الهجوم السيبراني. كما عثر المتخصصون على برامج تسمى "Wiper" (ماسح) وهو برامج ضار يمكنه حذف الكثير من البيانات من دون ملاحظة ذلك. مثل هذا الهجوم الروسي حدث في عام ٢٠١٧ على أوكرانيا ببرنامج ماسح "NotPetya" ، ما تسبب بأضرار اقتصادية كبيرة[١٧] ، حتى لحظة كتابة هذا البحث، ومع استمرار القتال الفعلي على الأرض في أوكرانيا، يظل الفضاء الإلكتروني على الأقل مسرحا ثانويا للحرب. وأوكرانيا الآن لا تقوم بتعبئة جيشها فقط، وإنما تعبئة خبراء تكنولوجيا المعلومات في البلاد أيضا. فحسب وكالة رويترز للأنباء، كانت الحكومة في كييف تبحث عن متطوعين قادرين على صد هجمات القراصنة الروس والتحضير لهجماتهم الخاصة على البنية التحتية لتكنولوجيا المعلومات الروسية المهمة ، لذا في في بعض الحالات يمكن أن يكون للهجمات الرقمية تأثير محدد للغاية على مسار الحرب الاعتيادية. لكن كلما زادت رقمنة الجيش، زادت نظريا مساحة الهجوم التي يوفرها. على سبيل المثال، حاول القراصنة الروس اختراق التطبيقات المستخدمة للسيطرة على سلاح المدفعية الأوكرانية. مع مثل هذا الإجراء، بحسب هيربيغ، يمكن للمرء على سبيل المثال الحصول على بيانات جغرافية من أجل قصف مواقع المدافع.[١٨] لذا فمن خلال ماتقدم يمكن للحروب السيبرانية والهجمات السيبرانية وقع كبير في الحروب العادية ويكون تدخلها امر حاسم للحرب الاعتيادية.

المبحث الثاني

الحرب السيبرانية في ظل القانون الدولي الانساني

وان 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 ، ومع التسليم بانطباق القانون الدولي الإنساني على الحروب السيبرانية، إلا أن ذلك لا يعني إنكار حقيقة وجود العديد من الإشكالات العملية لتطبيق مبادئ القانون الدولي الإنساني على الحروب السيبرانية، وتظهر هذه الإشكالات خاصة عند تطبيق مبادئ سلوكيات الحرب وهذا ما سنتناوله في هذا المبحث وعلى النحو التالي :

المطلب الأول : مدى امكانية تطبيق القانون الدولي الإنساني على الحروب السيبرانية : تعارضت الآراء الفقهية حول انطباق القانون الدولي الإنساني على الحروب السيبرانية من عدمه، فهناك من يرى أنه لا يمكن أن يطبق القانون الدولي الإنساني على تلك الحروب التي تحمل طبيعة خاصة، وتحتاج إلى نموذج قانوني جديد يتعامل معها وينظم استخدامها ، وهناك من يرى أنه يمكن تطبيق القانون الدولي الإنساني على الحروب السيبرانية عن طريق القياس والاجتهاد في المقارنة لذا سنحاول بيان ذلك في الفرعين الاتيين.

الفرع الأول : استحالة تطبيق القانون الدولي الإنساني على الحروب السيبرانية : تكمن خصوصية الفضاء الإلكتروني في عدم وجود دولة بإمكانها فرض سيطرتها وسيادتها الأحادية عليه، وهذا يؤدي إلى استخدامه بشكل قد يضر الإنسانية. وعلى هذا الأساس ظهر اتجاه فقهي سمي بالاتجاه الحر يرفض التعامل القانوني مع الإنترنت ويقضي بأن الإنترنت منطقة بلا قانون. ويعتبر أنصار هذا الاتجاه الذي يتزعمه بعض السياسيين الأمريكيين وعلماء التقنية، وتساندهم فئة قليلة من فقهاء القانون الدولي، أن الإنترنت مكان أو قارة أو فضاء مستقل في حد ذاته عن كل الفضاءات الأخرى بما فيها فضاؤنا المادي الملموس. وبالتالي لا يمكن إخضاعه حتى للقانون الدولي العام التقليدي، فهذا القانون لم ينجح لحد الآن بحكم الفضاء البحري أو الجوي الخارجيين[١٩] ، ويستند أنصار هذا الاتجاه على حجة أن الإنترنت عالم جديد لا يتفق والواقع المادي التقليدي. وعلى أساس ذلك، طرحوا سؤالا وجيها، هو إن سلمنا بضرورة إخضاع الإنترنت للقانون، فأي سلطة يكون بإمكانها السهر على فرض أحكامه في ظل استقلالية الشبكة وانفلاتها من مفهوم الخضوع؟ وأجابوا بانعدام السلطة القادرة على ذلك. وحتى إن وجد مثل هذا القانون، فإنها تبقى منطقة بلا قانون، لاستحالة إخضاعها للتدخل التنظيمي التقليدي للدول، كونها تتسم بطابع عالمي مفتوح، ويتعذر إخضاعها لقانون واحد لاشتراك كل الدول فيها [٢٠]. منظمة وفيما يتعلق بتطبيق أحكام القانون الدولي الإنساني على الحرب السيبرانية، فابتداء لا توجد أي قواعد قانونية في اتفاقيات القانون الدولي الإنساني تتعامل بشكل مباشر مع الهجمات السيبرانية، فهي غير في النزاعات المسلحة، إضافة إلى أن تطوير الهجمات السيبرانية حصل في فترة لاحقة على إعداد صكوك القانون الدولي الإنساني، كما أن القانون الدولي الإنساني وضعت قواعده لتنظيم وسائل وأساليب القتال ذات الطبيعة المتحركة التي تنتج عنها آثار مادية غير متوفرة في الهجمات السيبرانية، وبالتالي تكون هذه الأخيرة خارج نطاق القانون الدولي الإنساني لأنها ليست هجمات مسلحة[٢١]. ويبين أصحاب هذا الاتجاه أنه وعلى الرغم من أن مسمى الحرب يطلق على هجمات الكمبيوتر، فهو أيضا بحاجة إلى نظر، كون أن الحرب مفهوم يرتكز بالأساس على استخدام الجيوش النظامية، وكان يسبقها إعلان واضح لحالة الحرب وميدان قتال محدد. أما في هجمات الفضاء السيبراني، فإنها غير محددة المجال أو الأهداف كونها تنفذ عبر شبكات المعلومات والاتصال المتعدية للحدود الدولية، أو اعتمادها على أسلحة الكترونية جديدة تلاءم السياق التكنولوجي لعصر المعلومات، التي يتم توجيهها ضد المنشآت الحيوية أو وضعها عن طريق

العملاء لأجهزة الاستخبارات، وتجعل عملية استخدام هجمات الكمبيوتر من الناحية السياسية في أي صراع أقرب إلى توصيفها بالإرهاب عن كونها حرب، كما أن تحديد وتعريف الأسلحة المعلوماتية يثير مشكله كبيره في كيفية التعامل معها . ويضيف أصحاب هذا الرأي أن تطبيق المبادئ العامة في القانون الدولي الإنساني على الفضاء السيبراني تبدو غير واقعية، لأن وسائل وأساليب الحرب السيبرانية غير واضحة ومفهومة بشكل كاف، ولأنها تتم في سرية تامة. وتتسم كذلك هجمات الفضاء السيبراني بأنها استباقية ومن دون سابق إنذار، وأنها غير محددة المجال أو المدى، وتكون أهدافها غير محددة بخلاف الحرب التقليدية التي تكون أهدافها ومكانها محددين وتكون قوات الحرب السيبرانية غير معروفه وليست محددة في دولة سواء أكانت هدفا للحرب أو مشاركة فيها[٢٢]، حيث لا تصبح بالضرورة الدولة هي الهدف، وتكون الحرب السيبرانية متعددة الأوجه ومتشابكة مع غيرها، ومن تم تكون تفاعلاتها كبيرة فهي تتشابك مع الحرب الإعلامية وحرب الشبكات والاتصالات والحرب السياسية والسيكولوجية والحرب التكنولوجية والإرهاب [٢٣]

الفرع الثاني : خضوع الحروب السيبرانية للقانون الدولي الإنساني : يرى أنصار هذا الاتجاه عدم وجود فراغ قانوني في الفضاء السيبراني، واعتبار القواعد القانونية القائمة كافية وكفيلة لتنظيمه، والذي تشكل الإنترنت أحد وسائله الرئيسية، خاصة إذا علمنا أنه سبق تنظيم وسائل اتصال تشبهها مثل الهاتف والفاكس وغيرها من الوسائل الالكترونية. وعليه ينطبق القانون الدولي الإنساني بمبادئه وقواعده بصفة عامة على أي نزاع مسلح بما فيها الحروب السيبرانية، فإذا كنا نتفق بأن اتفاقيات القانون الدولي الإنساني لم تشر على وجه الخصوص للهجمات السيبرانية إلا أن هذه الحجة ليس لها أهمية تذكر، لأن شرط مارتينز وهو من المبادئ الراسخة في القانون الدولي الإنساني ينص صراحة على أنه عند وجود حالة لا تغطيها اتفاقية دولية "يظل المدنيون والمقاتلون تحت حماية وسلطة مبادئ القانون الدولي المستمد من التقاليد الراسخة، ومن مبادئ الإنسانية، وما يمليه الضمير العام"

وعلى هذا الأساس فإن كل ما يقع أثناء النزاع المسلح يخضع لمبادئ القانون الدولي الإنساني، وعليه لا وجود لفراغ قانوني بالنسبة للهجمات السيبرانية. كما أن قبول العرف الدولي كمصدر للقانون الدولي والمنصوص عليه في المادة ٣٨ من النظام الأساسي لمحكمة العدل الدولية يؤكد أيضا المغالطة التي وقع فيها من يرفضون[٢٤]انطباق القانون الدولي الإنساني على الهجمات السيبرانية اعتمادا على غياب نص قانوني معين أما بالنسبة للحجة التي ترتكز على حقيقة أن الهجمات السيبرانية يرجع تاريخها إلى ما بعد اعتماد المواثيق الدولية المشكلة للقانون الدولي الإنساني فإنها تنطوي على مغالطة أيضا، ذلك أن مثل هذا التبرير كان قد قدم إلى محكمة العدل الدولية في مسألة مدى مشروعية التهديد بالأسلحة النووية أو استخدامها سنة ١٩٩٦، ورفضت المحكمة في رأيها الاستشاري الاتجاه القائل بأنه نظرا لأن المبادئ والقواعد الإنسانية قد وضعت قبل اختراع الأسلحة النووية، فإن القانون الدولي الإنساني يكون غير منطبق عليها، واعتبرته رأيا تمثله أقلية بسيطة.

بينما أكدت أن رأي الغالبية العظمى من الدول والفقه وبدون أي شك، هو انطباق القانون الدولي الإنساني على الأسلحة النووية[٢٥]. ولأنه ليس هناك ما يدعو للتمييز بين الأسلحة النووية وأسلحة الحاسوب على الأقل من حيث التوقيت الذي استحدثت فيه بالنسبة لدخول المعايير الإنسانية ذات الصلة حيز التنفيذ، فإن نفس النتيجة تنطبق على الهجمات على شبكات الحاسوب أي التي تتم عبر الفضاء السيبراني [٢٦]وفي نفس السياق أشارت المادة ٣٦ من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لعام ١٩٤٩ المتعلق بحماية ضحايا النزاعات المسلحة الدولية لعام ١٩٧٧ 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" فوفقا لهذا النص إذا كيفنا الهجمات السيبرانية بأنها سلاح أو أسلوب من أساليب الحرب، فعلى الدول التحقق من مدى مشروعية استخدامها وفقا لقواعد هذا البروتوكول أو أية قاعدة أخرى من قواعد القانون الدولي، وهو ما يؤكد انطباق أحكام القانون الدولي الإنساني على الحرب السيبرانية. وهو ما سارت علية محكمة العدل الدولية في مسألة مدى مشروعية التهديد بالأسلحة النووية أو استخدامها، إذ أكدت في رأيها الاستشاري أن القانون الدولي الإنساني قد تطور ليأخذ بعين الاعتبار تغير الظروف، ولا يقتصر تطبيقه على أسلحة الماضي، وإنما ينطبق أيضا على استعمال الأسلحة الجديدة [٢٧].

وفيما يتعلق بحجة اعتبار أن الهجوم على شبكات الحاسوب ليس نزاعا مسلحا لغياب الأعمال العدائية التقليدية، ولأن وجود النزاع المسلح هو شرط لتطبيق القانون الدولي الإنساني، قد أصبحت مسألة نسبية في وقتنا الراهن، فنظرا للتقدم في وسائل وطرق الحرب، ولا سيما حرب المعلومات، فلا يكفي لتطبيق القانون الدولي الإنساني الاعتماد على معيار الفاعل فقط، بل يجب الاعتماد بدرجة أكبر على معيار آثار العمل. فلا أحد ينكر على سبيل المثال أن الحرب البيولوجية أو الكيميائية تخضع للقانون الدولي الإنساني على الرغم من أنها لا تتضمن استعمال أسلحة حركية. وعلى هذا الأساس فإن مبادئ القانون الدولي الإنساني تنطبق أينما تمت هجمات سيبرانية على دولة بشكل مكثف، فلا يمكن القبول بفرضية أن كل تصرف سيبراني ينشأ عنه قرصنة أو اختراق لبيانات الكترونية هو بمثابة أعمال عنف مسلح. كما يجب أن تهدف هذه الهجمات إلى إلحاق الأذى أو الوفاة للأفراد المدنيين أو إحداث أضرار بالبنى التحتية للدولة المستهدفة. وبهذا المقياس فالهجوم مثلا على شبكات الحاسوب الخاصة بنظام التحكم في مطار تابع لدولة معينة من قبل عملاء دولة أخرى يقتضي بداهة تطبيق أحكام القانون الدولي الإنساني على الرغم من عدم استخدام القوات المسلحة التقليدية [٢٨]

المطلب الثاني : التحديات العملية لتطبيق مبادئ سلوكيات الحرب على الحروب السيبرانية : إذا سلمنا بانطباق القانون الدولي الإنساني على الحروب السيبرانية، إلا أن ذلك لا يعني إنكار حقيقة الثغرات التي شهدتها طبيعة الحروب منذ اعتماد اتفاقيات جنيف لعام ١٩٤٩، حيث أصبحت وسائل وأساليب الحروب متطورة إلى درجة لم يكن يتصورها واضعي تلك الاتفاقيات، مما يؤدي إلى صعوبات عملية في إمكانية تطبيق مبادئ وقواعد القانون الدولي الإنساني على الحروب السيبرانية، وتظهر هذه الإشكالات خاصة عند تطبيق مبادئ سلوكيات الحرب المتمثلة أساسا في مبدأ الضرورة العسكرية ومبدأ التناسب ، ومبدأ التمييز والتي سنوضحها على ثلاث افرع وعلى النحو التالي:

الفرع الأول : مبدأ الضرورة العسكرية : يعد هذا المبدأ من أهم المبادئ الأساسية التي قام عليها القانون الدولي الإنساني، ويقصد بمبدأ الضرورة العسكرية بشكل عام التزام أطراف النزاع المسلح باستخدام القوة الضرورية لتحقيق هدف القتال الذي يتمثل في إخضاع العدو وتحقيق النصر عليه، فلا يمكن أن نتصور قيام حرب دون أن تكون هزيمة العدو والنصر عليه ضرورة عسكرية لدى قادة وجيوش الدولة الطرف في النزاع . ومن هنا نقول أن الهدف من الضرورة العسكرية هو كسب الحرب في حد ذاتها، ولكن وفق للقوانين المنظمة لها. ومن ثم فإن كل استخدام للقوة المسلحة يتجاوز تحقيق الهدف من القتال يصبح دون مسوغ من مسوغات الضرورة العسكرية يدخل في خانة العمل غير المشروع [٢٩]. وقد أخذت اتفاقيات جنيف لعام ١٩٤٩ بفكرة الضرورة العسكرية التي قد تمليها ظروف القتال، وجعلت منها مسوغا لبعض الانتهاكات الجسيمة لأحكامها، حيث أشارت هذه الاتفاقيات إلى أن تدمير الممتلكات أو الاستيلاء عليها على نطاق واسع يعد انتهاكا جسيما لهذه الاتفاقيات ما لم تبرره الضرورات الحربية[٣٠] ، كما أخذ البروتوكول الإضافي الثاني الملحق باتفاقيات جنيف لعام ١٩٤٩ المتعلق بحماية ضحايا النزاعات المسلحة غير الدولية لعام ١٩٧٧ بمبدأ الضرورة العسكرية، فقد أشارت المادة ١٥ منه إلى حظر مهاجمة المنشآت المحتوية على قوى خطرة حتى لو كانت أهدافا عسكرية، إذا كان من شأن ذلك أن يلحق خسائر فادحة بالسكان المدنيين، كما حظرت المادة ١٧ من البروتوكول ذاته الترحيل القسري للمدنيين ما لم تبرره الضرورات العسكرية الملحة. وتظهر إشكاليات تطبيق هذا المبدأ على الهجمات السيبرانية في صعوبة التمييز بين الأهداف العسكرية والمدنية والتي من الممكن أن تستهدف منشآت تقدم خدمة للقطاع العسكري وفي الوقت نفسه للمدنيين. كما أن الضرورات العملية في تطبيق مبدأ الضرورة العسكرية يصعب تطبيقها على الهجمات السيبرانية، فعلى سبيل المثال يمكن تحقيق الأهداف بأسر المقاتلين فقط دون قتلهم، فوجود المقاتل في ساحة القتال أفضل دائما في اتخاذ هكذا قرار والقدرة على التميز بين من يدعي الإصابة والذي قد يمثل تهديدا، وبالتالي يمكن استهدافه وقتله

وفقا لمبدأ الضرورة العسكرية، وبين من جرح جرحا بالغا حتى أنه لم يعد يمثل تهديدا، ذلك أن مبدأ الضرورة العسكرية يستلزم أن تكون القوة المستخدمة لا تتضمن عمليات الثأر، بالإضافة إلى عدم وجود بديل آخر للإجراءات أو التدابير المقرر استخدامها استنادا لمبدأ الضرورة[٣١].

الفرع الثاني : مبدأ التناسب يعد مبدأ التناسب : أحد المبادئ الجوهرية التي يجب تطبيقها أثناء النزاعات المسلحة سواء كانت دولية أم غير دولية لأنه يهدف إلى الحد أو التقليل من الخسائر وأوجه المعاناة المترتبة على العمليات العسكرية سواء بالنسبة للأشخاص أو الأشياء . ويعد هذا المبدأ من المسائل الدقيقة التي يصعب تحقيقها في بعض الأحيان أثناء القتال وإدارة العمليات الحربية، إذ يحظر القانون الدولي الإنساني الهجمات غير المتناسبة من أجل إنقاذ المدنيين والأعيان المدنية من آثار الحرب بقدر الامكان[٣٢]. ويعتمد مبدأ التناسب على تحقيق التوازن بين أمرين جوهريين، هما الميزة العسكرية المتوقعة من أعمال القتال من جانب والخسائر التي تلحقها هذه العمليات بالمدنيين والأعيان المدنية من جانب آخر، ويشترط في الميزة العسكرية أن تكون متوقعة وتتحقق عادة من خلال السيطرة على جزء من الإقليم أو تدمير القوات العسكرية للعدو أو إضعافها، كما يشترط فيها أن تكون ملموسة ومباشرة[٣٣]. وتظهر إشكاليات تطبيق هذا المبدأ على الهجمات السيبرانية في أن برمجة تلك العمليات الالكترونية لا يمكن في مقدورها تطبيق مبدأ التناسب، لاسيما إذا ما علمنا أن معادلة التناسب تعد معادلة صعبة ودقيقة حتى أثناء وإدارة العمليات الحربية التقليدية، فتحقيق المهمة القتالية وإحراز النصر هدف أساسي للقوات العسكرية، وتنفيذ القوانين وضبط التدمير وعدم إلحاق أضرار مفرطة بالخصم التزام قانوني واجب النفاذ، وبالتالي يحتاج إلى قائد عسكري متمكن يسوي ميزان هذه المعادلة، والأمر بدون شك يزداد تعقيدا إذا ما تعلق الأمر بالهجمات السيبرانية[٣٤] وهو ما أكده فقهاء القانون الدولي إذ يرى الأستاذ (Shin)أن مبدأ التناسب في استخدام القوة السيبرانية لا يزال غامضا ويحتاج إلى أجوبة أهمها كيف يمكن ضمان مبدأ التناسب في الرد على الهجمات السيبرانية. ويتفق الأستاذ (Rex)مع ما ذهب إليه الأستاذ (Shin) بقوله " :إذا تم توجيه هجمات سيبرانية ضد بني تحتية ثنائية الاستعمال)مدنية وعسكرية (وعن بعد، فلا يبدو أن المنفعة العسكرية ستكون واضحة، ما يجعل تطبيق مبدأ التناسب أثناء الهجمات السيبرانية أمرا في غاية الصعوبة[٣٥]".

الفرع الثالث : مبدأ التمييز يعتبر مبدأ التمييز : من أهم المبادئ التي جاء بها القانون الدولي الإنساني لضبط العمليات الحربية، ويتضمن هذا المبدأ تطبيقين أساسيين هما :ضرورة التمييز بين المقاتلين وغير المقاتلين في جميع الأوقات، وأن يتمتع المدنيين بالحصانة ضد الهجمات التي توجه إلى الأهداف العسكرية. وضرورة التمييز بين الأعيان المدنية والأعيان العسكرية، وأنه لا يجوز مهاجمة الأعيان المدنية بأي حال من الأحوال[٣٦]. وقد تم التطرق إلى مبدأ التمييز بصورة واضحة في المادة ٤٨ من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لعام ١٩٤٩ المتعلق بحماية ضحايا النزاعات المسلحة الدولية لعام ١٩٧٧ التي نصت على ما يلي " :تعمل أطراف النزاع على التمييز بين السكان المدنيين والمقاتلين وبين الأعيان المدنية والأهداف العسكرية، ومن ثم توجه عملياتها ضد الأهداف العسكرية دون غيرها، وذلك من أجل تأمين احترام وحماية السكان المدنيين والأعيان المدنية ."ويعد تطبيق مبدأ وجوب التمييز بين المقاتلين والمدنيين على الهجمات السيبرانية مسألة في غاية التعقيد –على

عكس الهجمات التقليدية–إذ سيكون المهاجم في الأغلب بعيدا عن المكان المستهدف من الهجوم ولمسافة قد تتجاوز المئات من الكيلومترات ، ما يعني أن التمييز بين المقاتلين والمدنيين هو أمر صعب إذا لم يكن مستحيلا[٣٧]. كما تصبح مسألة التمييز بين الأهداف المدنية والعسكرية في الهجمات السيبرانية صعبة، خاصة أن نظم الحواسيب العسكرية غالب ما تتصل بالنظم التجارية والمدنية وتعتمد عليها كليا أو جزئيا، بل وقد يكون هناك تداخل بين الاستخدامات المدنية والعسكرية بارتباطهما بشبكة واحدة ووسيط واحد هو الفضاء السيبراني، ومن ثم يكون من المستحيل شن هجوم سيبراني على بنى تحتية عسكرية وجعل آثارها تقتصر على هدف عسكري وحسب ودون الإضرار بالمدنيين والمنشآت المدنية[٣٨]. فعلى سبيل المثال عندما تتعرض الحواسيب الشبكات المعلوماتية التابعة لقوات عسكرية لدولة ما لهجمات سيبرانية، قد تجعل المدنيين عرضة لخطر الحرمان من الاحتياجات الأساسية مثل مياه الشرب والرعاية الطبية والكهرباء نظرا لاعتمادها على نفس الشبكات التي تم تدميرها.

الخاتمة

بعد اتمام البحث توصلت الباحثة الى عدد من النتائج والتوصيات :

اولاً :النتائج

١. الهجمات السيبرانية من المفاهيم الحديثة ١التي لا يوجد اتفاق دولي على تعريفها حتى يومنا هذا، ولكن على الرغم من ذلك لا تحدث في فراغ قانوني ويمكن الاستناد في ذلك إلى المادة٣٦ من البروتوكول الإضافي الأول لعام ١٩٧٧ وأيضاً لآراء وقرارات محكمة العدل الدولية كرأيها بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها.

٢. ان الفضاء السيبراني يشكل مجالاً دولياً جديداً يمثل امتداداً لنشاط الإنسان ذي الطابع المدني أو العسكري، ويوازي ما يقوم به الإنسان في المجالات والفضاءات الدولية الأخرى، كالمجال البري والبحري والجوي والفضاء الخارجي.

٣. تكمن الميزة النسبية للهجمات السيبرانية في انخفاض تكاليفها وسهولة اللجوء إليها إذا لا تتطلب حشوداً من المقاتلين العسكريين والآلاف من الأسلحة والوسائل كالنزاعات المسلحة الحركية التقليدية، بل يكفي لتنفيذها شخص أو مجموعة صغيرة ممن لديهم الخبرة والمهارة في التكنولوجيا السيبرانية وثغرات البرامج لاستخدامها ضد دولة أو دول أخرى، إلا أن هذه الميزة تتحول إلى مصدر قلق كبير إذا ما نظرنا إلى آثار هذه الهجمات وتبعاتها على السكان المدنيين والبيئة فيما لو تم تنفيذها على منشأة نووية أو مصادر الطاقة كشبكة الكهرباء والمياه.

٤. إجماع الفقهاء الدوليين على خضوع الهجمات السيبرانية التي تحدث في سياق النزاع المسلح الحركي للقانون الدولي الإنساني، إلا أن التحدي الأكبر هو تلك الهجمات التي تحدث خارج سياق النزاع

المسلح الحركي ومدى إمكانية عدها نزاع مسلح وإثبات نسبة الهجوم لدولة معينة وبالتالي إمكانية تطبيق القانون الدولي الإنساني عليها ايضاً

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.

ثانياً :التوصيات

١. العمل على تزويد الجيوش بتقنيات ومهارات التعامل مع التهديدات السيبرانية ويتم ذلك من خلال تعليم وتدريب المهندسين المعلوماتيين العاملين في القوات المسلحة، على اكتساب مهارات الأمن السيبراني من أجل أن يكونوا قادرين على تولي مسؤوليات حماية البنى التحتية الوطنية من تهديدات الهجمات السيبرانية القائمة حالياً وتلك المستقبلية.

٢. التواصل مع خبراء معلوماتيين وذلك لإيجاد برمجية معينة تقوم بفصل البنية التحتية والشبكات السيبرانية العسكرية عن المدنية وذلك لحماية السكان المدنيين من مخاطر الهجمات السيبرانية أهمية دور المجتمع الدولي في رفع الوعي بمخاطر الاستخدامات غير السليمة للتكنولوجيا، على الصحة والاقتصاد العالمي والأمن العالمي.

٣. تعزيز الحوار والتنسيق وتبادل المعلومات بين الدول والمنظمات الدولية والإقليمية في إطار مكافحة إساءة استخدام تكنولوجيا المعلومات والاتصالات. الدول النامية لتطوير وتحديث أمنها السيبراني والاستفادة من تجارب البلدان الأخرى

٤. أهمية سعي والخبرات الموجودة لديها وذلك كله في سبيل تحصين بنيتها الرقمية.

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 الصراعات والحروب.

المصادر :

اولاً:القران الكريم

ثانيا:المصادر العربية

١. أسامة صبري محمد، الحرب الالكترونية ومبدأ التمييز في القانون الدولي الإنساني، مجلة القانون للدراسات و البحوث القانونية، العدد ٧، ٢٠١٣م.

٢. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية،مفهومها والمسؤولية الدولية الناشئة عنها ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد ٤، ٢٠١٦م.

٣. إيهاب خليفة، الحرب السيبرانية، الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، العربي للنشر والتوزيع، القاهرة، ٢٠٢١م

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

٥. خالد روشو، الضرورة العسكرية في نطاق القانون الدولي الإنساني، رسالة دكتواره في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، ٢٠١٣م

٦. سعيد درويش، الحروب السيبارنية وأثرهاعلى حقوق الإنسان، دارسة على ضوء أحكام دليل "تالين "، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، المجلد ٥٤، العدد ٥، ٢٠١٧ م

٧. طالب حسن موسى، عمر محمود أعمر، الإنترنت قانونا، مجلة الشريعة والقانون، العدد ٣٧، ٢٠١٦م

٨. عمر محمود أعمر، "الحرب الإلكترونية في القانون الدولي الإنساني"، الشريعة والقانون، المجلد ٤٦، العدد ٣، ٢٠١٩م

٩. عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مكتبة الإسكندرية، وحدة الدارسات المستقبلية، مصر، ٢٠١٦.

١٠. علي عبد الرحيم ، العبودي ، هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين، المجلة العلمية الأكاديمية العراقية، العدد٥٧، جامعة بغداد، كلية العلوم السياسية، ٢٠١٩م.

١١. مصعب التجاني، "القانون الدولي الإنساني وحماية المدنيين خلال النزاعات المسلحة "نموذج الحالة السورية""، المركز الديمقارطي العربي للدارسات الاستراتيجية والسياسية والاقتصادية، برلين، ألمانيا، ٢٠١٩م

١٢. مايكل شميت، الحرب بواسطة شبكات الاتصال، الهجوم على شبكات الكمبيوتر)الحاسوب (والقانون في الحرب"، المجلة الدولية للصليب الأحمر،٢٠٠٢م

١٣. هاجر ختال، الوضع القانوني للحرب السيبرانية على ضوء قواعد القانون الدولي، مجلة التواصل في الاقتصاد والإدارة والقانون، المجلد ٢٥، العدد ٣، ٢٠١٩م

١٤. يحيى ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلد ٤، العدد ٤، ٢٠١٨م

١٥. يحيى مفرح الزهراني، الأبعاد الإستراتيجية والقانونية للحرب السيبرانية، مجلة البحوث والدراسات، العدد ٢٣، ٢٠١٧م

ثالثاً:الاتفاقيات

١. اتفاقيات جنيف الأولى والثانية والثالثة لعام ١٩٤٩على التوالي.

٢. لبروتوكول الإضافي الأول الملحق باتفاقيات جنيف لعام ١٩٤٩ المتعلق بحماية ضحايا النزاعات المسلحة الدولية لعام ١٩٩٧ م

رابعاً:المصادر الاجنبية

1-Le droit international humanitaire a évolué pour tenir compte des circonstances et son application ne se limite pas aux armements du passé ...». Paragraphe 85, CIJ Recueil 1996

خامساً : المواقع الالكترونية

١. فريدل تاوبه ، الحرب في أوكرانيا .. أي دور تلعبه الهجمات السيبرانية،مقال منشور في موقع قناة دوت فيلا عربي، ١ /٣ /٢٠٢٢/https://amp.dw.com/ar :

٢. خالد وليد محمود، كيف يمكن استخدام السلاح السيبراني في الأزمة الروسية الأوكرانية،مقال منشور في موقع قناة الجزيرة،٢١ /٢ /٢٠٢٢https://www.aljazeera.net :

٣. مقال منشور في موقع-https://www.icj-cij.org/public/files/case-related/95/095 :19960708-ADV-01-00-FR.pdf

٤. موقع الموسوعة الجزائرية للد ارسات السياسية والاستراتيجية، الحرب السيبرانية وتداعياتها على الأمن العالمي،تاريخ النشر،٢٠٢٠

٥. موقع https://www.politics-dz.com/ :

Microsoft Computer Dictionary, Fifth Edition, Microsoft Press, Washington,2002, p138, Available AT : https://cutt.ly/pkg9WxN

[٢] منير البعلبكي، رمزي منير، المورد الحديث، دار العلم للملايين، تيروت، ٢٠٠٩، ص٣٠٧

[٣] -موق قاموس المعاني، معنى كلمة سايبر: https://www.almaany.com/ar/dict/ar-en/cyber

[٤] أسامة صبري محمد، الحرب الالكترونية ومبدأ التمييز في القانون الدولي الإنساني، مجلة القانون للدراسات و البحوث القانونية، العدد ٧، ٢٠١٣، ص ٥

[٥] -أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية، مفهومها والمسؤولية الدولية الناشئة عنها ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد ٤، ٢٠١٦، ص ٦١٦

[٦] -يحيى ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلد ٤، العدد ٤، ٢٠١٨، ص ٨٤

[٧] -يحيى مفرح الزهراني، الأبعاد الإستراتيجية والقانونية للحرب السيبرانية، مجلة البحوث والدراسات، العدد ٢٣، ٢٠١٧،ص٢٣٥

[٨] حكيم غريب، صبرينة شرقي، تداعيات الحرب الإلكترونية على العلاقات الدولية،دراسة في الهجوم الإلكتروني على إيران (فيروس ستكنست") ، دفاتر السياسة والقانون،المجلد١٢،العدد٢٢، ٢٠٢٠ ،ص٢٦

[٩] –سعيد درويش، الحروب السيبارنية وأثرهاعلى حقوق الإنسان، دارسة على ضوء أحكام دليل "تالين" ، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، المجلد ٥٤، العدد ٥، ٢٠١٧ ، ص ١٨١

[١٠] موقع الموسوعة الجزائرية للد ارسات السياسية والاستراتيجية، الحرب السيبرانية وتداعياتها على الأمن العالمي، تاريخ النشر،٢٠٢٠

موقع : https://www.politics-dz.com/

[١١] المرجع السابق، نفس الموضوع

[١٢] علي عبد الرحيم، العبودي، هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين، المجلة العلمية الأكاديمية العراقية، العدد٥٧، جامعة بغداد، كلية العلوم السياسية، ٢٠١٩، ص ٨٩

[١٣] –علي عبد الرحيم، العبودي، المصدر السابق،ص١١٨

[١٤] أحمد عبيس نعمة الفتلاوي، مصدر سابق،ص٦٢٦

[١٥]إيهاب خليفة، الحرب السيبرانية، الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، العربي للنشر والتوزيع، القاهرة، ٢٠٢١، ص ٩١.

[١٦] حكيم غريب، صبرينة شرقي، تداعيات الحرب الإلكترونية على العلاقات الدولية، دراسة في الهجوم الإلكتروني على إيران (فيروس ستكنست) ، دفاتر السياسة والقانون، المجلد ١٢، العدد ٢، ٢٠٢٠،ص١٠١

[١٧] فريدل تاوبه، الحرب في أوكرانيا .. أي دور تلعبه الهجمات السيبرانية،مقال منشور في موقع قناة دوت فيلا عربي، ١ /٣ / ٢٠٢٢: https://amp.dw.com/ar

[١٨] خالد وليد محمود،كيف يمكن استخدام السلاح السيبراني في الأزمة الروسية الأوكرانية،مقال منشور في موقع قناة الجزيرة،٢١/ ٢/ ٢٠٢٢: https://www.aljazeera.net

[١٩] طالب حسن موسى، عمر محمود أعمر، الإنترنت قانونا، مجلة الشريعة والقانون، العدد ٣٧، ٢٠١٦، ص ٧-٨

[٢٠] طالب حسن موسى،مصدر سابق، ص ٨.

[٢١] أسامة صبري محمد، مصدر سابق، ص ٨

[٢٢] عمر محمود أعمر، "الحرب الإلكترونية في القانون الدولي الإنساني"، الشريعة والقانون، المجلد ٤٦، العدد ٣، ٢٠١٩، ص١٧٣

[٢٣] عمر محمود أعمر،المصدر السابق، ص ١٣٧

[٢٤] مايكل شميت، الحرب بواسطة شبكات الاتصال،الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب"، المجلة الدوليةللصليب الأحمر،٢٠٠٢،ص٩٠.

[٢٥] مايكل شميت، مصدر سابق،ص٩٠

[٢٦] مقال منشور في موقع:-https://www.icj-cij.org/public/files/case-related/95/095-19960708-ADV-01-00-FR.pdf

[٢٧] هاجر ختال، الوضع القانوني للحرب السيبرانية على ضوء قواعد القانون الدولي، مجلة التواصل في الاقتصاد والإدارة والقانون، المجلد ٢٥، العدد ٣، ٢٠١٩، ص ١٦٧

[٢٨] مايكل شميت، المصدر السابق، ص٩٤.

[٢٩] خالد روشو، الضرورة العسكرية في نطاق القانون الدولي الإنساني، رسالة دكتواره في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، ٢٠١٣ص ٨٣.

[٣٠] – المواد ٥١،٥٠، ١٧ من اتفاقيات جنيف الأولى والثانية والثالثة لعام ١٩٤٩على التوالي.

[٣١] –يحيى ياسين سعود، المصدر السابق، ص ٩٦

[٣٢] المادة (٥١/٥/ب) من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لعام ١٩٤٩ المتعلق بحماية ضحايا النازعات المسلحة الدولية لعام ١٩٩٧ بأنه: "الهجوم الذي يمكن أن يتوقع منه أن يسبب خسائر في أرواح المدنيين أو إصابة بهم أو أضرارا بالأعيان المدنية، أو أن يحدث خلطا بين هذه الخسائر والأضرار بشكل يفرط في تجاوز ما ينتظر أن يسفر عنه ذلك الهجوم من ميزة عسكرية ملموسة ومباشرة".

[٣٣] (٣)– مصعب التجاني، "القانون الدولي الإنساني وحماية المدنيين خلال الن ازعات المسلحة " نموذج الحالة السورية""، المركز الديمقارطي العربي للدارسات الاستراتيجية والسياسية والاقتصادية، برلين، ألمانيا، ٢٠١٩،ص٧٠

[٣٤] يحيى ياسين سعود، المصدر السابق، ص ٩٧

[٣٥] أحمد عبيس نعمة الفتلاوي، المصدر السابق، ص٦٣٨.

[٣٦] خالد روشو، المصدر السابق، ص ١٤٢.

[٣٧] أحمد عبيس نعمة الفتلاوي، المصدر السابق،ص٦٣٩

[٣٨] عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مكتبة الإسكندرية، وحدة الدارسات المستقبلية، مصر، ٢٠١٦، ص٩٦.