مجلة العلوم الإنسانية العربية
المجلد (٥) العدد (٤)
الإصدار الثامن عشر
٢٠٢٤ (٢٢-١)

الآليات الدولية لحماية حقوق الإنسان من التهديدات السيبرانية

د. انتصار على صالح الورشفانى
محاضر، القانون الدستورى، جامعة طرابلس، كلية القانون.

نشر إلكترونياً بتاريخ: ١٥ اكتوبر ٢٠٢٤م

الملخص

تهدف الدراسة إلى تطوير فهم شامل للتهديدات السيبرانية التي تحدث في ساحة المعركة الافتراضية الحديثة وإظهار كيف يمكن تطبيق مبادئ وأنظمة القانون الإنساني الدولي على هذه التهديدات. وهذا مهم بشكل خاص لأن استخدام الفضاء الإلكتروني للعمليات العسكرية أدى إلى تعطيل قوانين الصراع المسلح. ومن المرجح أن تستهدف الهجمات السيبرانية المدنيين بدلاً من الأفراد العسكريين، مما يؤثر على السكان المدنيين بدلاً من القوات المسلحة. وتدور القضية الرئيسية حول مدى استخدام الآليات الدولية لحماية حقوق الإنسان من التهديدات السيبرانية. استخدم الباحث نهجًا تحليليًا وصفيًا استنتاجيًا ووجد أن التهديدات السيبرانية هي شكل حقيقي من أشكال الحرب في إطار القانون الإنساني الدولي، مما يتسبب في أضرار جسيمة ويتطلب تعريفًا عاجلاً لمناطق الحماية والضمانات للأفراد المتضررين.

الكلمات المفتاحية: العمليات العسكرية، الإلكترونيات، المدنيين، الهجمات السيبرانية.

Abstract

The study aims to develop a comprehensive understanding of the cyber threats that occur in the modern virtual battlefield and to demonstrate how international humanitarian law principles and regulations can be applied to these threats. This is particularly important because the use of cyberspace for military operations has disrupted the laws of armed conflict. Cyber-attacks are likely to target civilians rather than military personnel, impacting civilian populations rather than armed forces. The key issue revolves around the extent to which international mechanisms for safeguarding human rights from cyber threats are utilized. The researcher used a deductive descriptive analytical approach and found that cyber threats are a genuine form of warfare within international

humanitarian law, causing severe damage and requiring an urgent definition of protection areas and safeguards for affected individuals.
Keywords: Military operations, Electronics, Civilians, Cyber-attacks.

*** 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 برز الفضاء أو المجال السيبراني (Cyberspace) "كمجال خامس للحرب"، إلى جانب البر والبحر والجو والفضاء، وأبرز ما يميز هذا المجال كوسيلة لاستخدام القوة أو انطلاق التهديدات منه هو أنه غير محسوس وغير حركي، حيث أن استخدام هذا المجال من أجل إحداث خلل سواء بشكله الوظيفي أو التركيبي لا يتطلب نقلاً لقطع عسكرية من مكان إلى مكان آخر، إضافة إلى ذلك فإنه من غير الممكن التنبؤ بالموعد التي سيستخدم فيها هذا المجال من أجل إحداث ذلك الخلل.

وقد عزز وجود ما يمسي بالتهديدات السيبرانية، ضعف طبيعة شبكة المعلومات وقابليتها للاختراق بسبب الاعتماد المفرط على برامج الحماية المقدمة للجهاز، وعدم تغيير كلمات المرور، وتجاهل التحديثات والاتصالات العشوائية وتشغيل شبكات Wi-Fi العامة، بالإضافة لذلك طمع الدول الكبرى إلى استخدام التهديدات السيبرانية إلى جانب التهديدات العسكرية الحركية لزيادة تداعيات العمليات العسكرية على الخصم، ليس هذا فقط بل يؤدي غموض تحديد هوية مرتكب الهجوم السيبراني إلى رغبة الدول في اعتماد مثل هذه التهديدات، وبالإضافة لذلك يمكن العثور على الأسلحة السيبرانية من خلال الانترنت المظلم (Dark Web) وهذا الأمر له تداعيات خطيرة على المجتمع الإنساني ككل.

وتظهر المخاوف الإنسانية بشكل واضح عندما لا تقتصر آثار هذه التهديدات على البيانات في أجهزة الكمبيوتر، أو أنظمة الكمبيوتر بل تهدف إلى خلق تأثير في العالم الحقيقي، على سبيل المثال اختراق أنظمة الكمبيوتر للسيطرة على الحركة الجوية وخطوط أنابيب النفط ومحطات الطاقة النووية ومراقبة الحركة الجوية والبرية والبحرية والسدود، ولذلك فإن الآثار المحتمل لمثل هذه التهديدات ستكون على درجة عالية من الخطورة والجسامة مما قد تؤدي إلى وقوع حوادث كارثية مثل التصادم بين الطائرات، وإطلاق المواد السامة من المصانع الكيماوية أو انقطاع تشغيل البنية التحتية والحيوية مثل شبكات إمدادات المياه والكهرباء ويكون المدنيين هم الضحايا الرئيسيين لمثل هذه التهديدات.

وأبرز قانون دولي يسعى إلى حماية المدنيين من ويلات النزاعات المسلحة والتهديدات العدائية على وجه الخصوص هو القانون الدولي الإنساني، ومع الإقرار بخطورة هذه التهديدات واعتبار الفضاء السيبراني مجالاً لتلك

التهديدات، سعى الباحثون والخبراء القانونيين إلى تحليل قواعد القانون الدولي الإنساني لبحث مدى إمكانية تطبيق قواعده على التهديدات السيبرانية التي تحصل في سياق النزاعات المسلحة الحركية أو خارج سياق النزاعات المسلحة الحركية.

أولاً: إشكالية البحث وتساؤلاته

بخلاف التهديدات العسكرية التقليدية التي تتم في الميدان المادي، تشن التهديدات السيبرانية في ميدان افتراضي على شبكة الانترنت مع ما تتميز به من استخدام مزدوج عسكري- مدني. وعلى اعتبار أن قواعد ومبادئ القانون الدولي الإنساني، ومنذ صياغة اتفاقيات جنيف الأربعة لعام ١٩٤٩ وبروتوكوليها الملحقين لعام ١٩٧٧، واجبة التطبيق على كافة الأنشطة التي تقوم بها الأطراف أثناء النزاع المسلح، تتمثل الإشكالية حول مدى تطبيق الآليات الدولية لحماية حقوق الإنسان من التهديدات السيبرانية.

وينطوي تحت السؤال الرئيس السابق عدة أسئلة فرعية هي: -

١- ما المقصود بالتهديدات السيبرانية؟

٢- كيف يتم تطبيق المبادئ العامة للقانون الدولي الإنساني أثناء التهديدات السيبرانية؟

٣- ما هي معايير تالين والقدرات الوطنية والدولية في مواجهة التهديدات السيبرانية؟

ثانياً: أهداف البحث

يهدف البحث إلى: -

١- تكوين صورة واضحة المعالم عن التهديدات السيبرانية التي تدور في الميدان الافتراضي الجديد للقتال.

٢- بيان إمكانية انطباق قواعد ومبادئ القانون الدولي الإنساني على التهديدات السيبرانية، خاصة أن استخدام الفضاء السيبراني لشن العمليات العسكرية قلب قوانين النزاع المسلح رأساً على عقب، فالأهداف المقصودة بأي هجوم سيبراني ستكون على الأرجح مدنية لا عسكرية، وستؤثر على السكان المدنيين لا على القوات العسكرية.

٣- استعراض دليل تالين والقدرات الوطنية والدولية في مواجهة التهديدات السيبرانية.

ثالثاً: أهمية البحث

نظراً لتزايد التهديدات السيبرانية في الآونة الأخيرة وصعوبة تحديد الجهة التي صدرت عنها هذه التهديدات وعدم وجود أساس قانوني ينظمها، تكمن أهمية هذا البحث في كونه يعالج موضوع حديث لا يزال في طور التبلور ويسلط الضوء على مفهوم هذه التهديدات والتهديدات وطبيعتها الاستثنائية. بالإضافة لذلك يحلل قواعد ومبادئ القانون الدولي الإنساني لبحث إمكانية انطباقها على التهديدات السيبرانية، وتقييم هذا الانطباق على حالات تطبيقية لهجمات سيبرانية حصلت فعلاً.

رابعاً: منهج البحث

تستدعي طبيعة البحث وموضوعه اعتماد المنهج الوصفي التحليلي (الاستنباطي)، حيث يقوم البحث باستعراض ماهية التهديدات السيبرانية وتحليل قواعد ومبادئ القانون الدولي الإنساني في سبيل تقييم إمكانية تطبيقها على التهديدات السيبرانية.

*** ماهية التهديدات السيبرانية**

أمام الثورة الرقمية الحديثة التي أفرزت وجود فضاء سيبراني يقوم على أساس بنية عالمية لتكنولوجيا المعلومات والاتصال، شهد العالم سباقاً للتسلح غير تقليدي من نوع جديد، يقوم على استحداث وتطوير برامج تقنيه تستخدم في الفضاء السيبراني لأغراض عسكرية، حيث يتم توجيه هجمات بسرعة قصوى ضد أعداء يتواجدون على مسافة بعيدة جداً من دون تعرضهم للخطر، سميت بمصطلح التهديدات السيبرانية.

معظم التعاريف التي وردت بشأن التهديدات السيبرانية تشترك في معنى متقارب وهو استهداف مواقع إلكترونية أو نظام كمبيوتر أو جهاز كمبيوتر من خلال وسائل اتصال إلكترونية أخرى، مما يهدد سرية أو سلامة أو توفر المعلومات المخزنة عليه، وعادة ما تكون صادرة من مصدر مجهول إما يسرق أو يغير أو يدمر هدفاً محدداً عن طريق اختراق نظام حساس[1]، وإن كان المختصون في القانون الدولي العام يقرون بأن المصطلح يكتنفه الغموض والالتباس بسبب عدم الاتفاق على تعريف محدد له، فمنهم من تبنى مصطلح الفضاء السيبراني (cyber space) بالاستناد إلى المحيط الذي تجري فيه الاعتداءات السيبرانية، ومنهم من تبنى مصطلح الحرب السيبرانية (Cyber warfare) استناداً إلى إيديولوجية أمنية أو عسكرية ضد العدو المفترض، بينما فضل البعض الآخر مصطلح التهديدات السيبرانية (cyberattacks) لأن مصطلح "الحرب" هو مصطلح غير محبذ في وقتنا الراهن على مستوى التنظيم القانوني الدولي، فيكون مصطلح "التهديدات السيبرانية" أكثر دلالة ومعنى، يتماشى مع مقتضيات القانون الدولي المعاصر[2]، وبالإضافة إلى ذلك فإن التهديدات السيبرانية أوسع نطاقاً من الحرب السيبرانية، وقد تحدث خارج نطاق النزاعات المسلحة، فتكون سبباً لبدء النزاع المسلح أو تحدث في نطاق النزاعات المسلحة، فتشكل جزءاً من الحرب السيبرانية. وعليه سنتناول تعريف التهديدات السيبرانية من خلال أولاً بيان معناها لغةً واصطلاحاً وثانياً في بيان خصائصها.

أولاً– التهديدات السيبرانية لغةً واصطلاحاً

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

١– السيبرانية في اللغة: إن كلمة سيبرانية أو سايبر أو سيبراني تعتبر ترجمة حرفية لكلمة (Cyber) والمشتقة من كلمة

[1] Pande, Nihar Ranjan: Cyber Attacks and Counter Measures: User Perspective, (Post-Graduate Diploma in Cyber Security), Uttarakhand Open University, Haldwani 2016, P1,Available at: https://cutt.ly/9ki28jB

[2] صابر، بلقاسم بن: "الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر"، مجلة حقوق الإنسان والحريات العامة، العدد ٤، جامعة عبد الحميد بن باديس، الدكتور حيدرة محمد، الجزائر، ٢٠١٧، ص ص ١٨٤-٢١٥، ص ١٨٨، متاح على الرابط: https://www.asjp.cerist.dz/en/article/69268

(Cybernetics)[٣]. 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"[٤].

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: –

أ– في قاموس المورد الحديث ب "الكمبيوتري" أو "عصري جداً" كما ورد معنى مصطلح (cybernetics)بأنه "علم الضبط" أو "علم التحكم الأوتوماتيكي"[٥].

ب– وجاء في قاموس المعاني بمعنى "تخيلي"[٦]: 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.

٢– التهديدات السيبرانية اصطلاحاً: إن مصطلح التهديدات السيبرانية هو مصطلح حديث نسبياً، لذلك قد حاول العديد من الخبراء والفقهاء القانونيين وضع تعريف محدد له. وسنستعرض هذه التعاريف تبعاً لوجهات النظر التي يتبناها أصحابها.

فقد 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. فيما عرفه شمت (Schmitt)بالقول: مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نظم المعلومات المعادية بهدف التأثير والإضرار بها، وفي الوقت نفسه للدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة[٧].

وفيما يتعلق باللجنة الدولية للصليب الأحمر فقد عرفت الهجوم السيبراني بأنه: استخدام أنشطة متعمدة لتغيير أو إفساد أو خداع او إضعاف أو تدمير أنظمة الحاسوب أو شبكات الحاسوب للخصم أو المعلومات و/ أو البرامج المدرجة في هذه الأنظمة أو الشبكات أو التي ترسل من خلالها، وقد تؤثر هذه الأنشطة أيضاً في الكيانات المرتبطة

---

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

[4] Cybernetics or Control and Communication in The Animal and The Machine. See: Wiener, Norbert: Cybernetics or Control and Communication in The Animal and The Machine, M.I.T, Press, Second Edition, Cambridge, Massachusetts, 1948, Available At: https://cutt.ly/akhwlob

[٥] البعلبكي، منير. والبعلبكي، رمزي منير: المورد الحديث، دار العلم للملايين، بيروت، ٢٠٠٩، ص٣٠٧.

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

[٧] الفتلاوي، أحمد عبيس نعمة: الهجمات السيبرانية (دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر)، الطبعة الأولى، منشورات زين الحقوقية، بيروت(لبنان)، ٢٠١٨م، ص١٦.

بهذه الأنظمة والشبكات. وقد يستخدم الهجوم السيبراني في منع المستخدمين المرخص لهم من الولوج إلى حاسوب أو خدمة معلومات (هجوم الحرمان من الخدمة)، أو لتدمير الآلات التي يتحكم فيها الحاسوب (الغرض المزعوم للهجوم السيبراني بالفيروس ستوكسنت)، أو لتدمير أو تغيير بيانات حيوية (مثل الجداول الزمنية لاستخدام عمليات لوجستية عسكرية). ويُرجى ملاحظة أن الآثار المباشرة لهجوم سيبراني (الأضرار التي تصيب الحاسوب) قد تكون أقل أهمية من الآثار غير المباشرة (الأضرار التي تصيب النظام الذي يرتبط به الحاسوب)[٨].

أما بالنسبة للخبراء القانونيين في دليل تالين فقد عرفوا التهديدات السيبرانية بأنها: عمليات سيبرانية، سواء كانت هجومية أو دفاعية، يهدف من خلالها التسبب بالإصابة أو وفاة لأشخاص أو الإضرار وتدمير الأهداف (الأعيان)[٩].

وعلى ضوء ما سبق يمكن القول أن التهديدات السيبرانية في رأينا: هي عمليات سيبرانية تقوم بها الدولة أو مجموعات حكومية أو غير حكومية سواء كانت هجومية أو دفاعية، يهدف من خلالها التسبب بالإصابة أو وفاة لأشخاص أو الإضرار وتدمير الأهداف (الأعيان) ضد خصم معين، وذلك عن طريق الدخول قصداً بطريقة غير مشروعة إلى جهاز حاسوبي أو منظومة معلوماتية أو موقع إلكتروني على الانترنت، دون أن يكون له الحق أو يملك الصلاحية أو التصريح بالقيام بذلك والقيام بحذف البيانات أو تغييرها أو تشفيرها أو إعاقة أو المنع قصداً بأي وسيلة كانت الوصول إلى الخدمة أو تعطيلها أو توقيفها عن العمل أو الحد من قدرة صاحب الموقع على التحكم بموقعه، أو استخدام البرمجيات الخبيثة أيا كان نوعها وبأي وسيلة كانت، بقصد الإضرار بالأجهزة الحاسوبية أو المنظومات المعلوماتية أو الشبكة.

*** إمكانية انطباق القانون الدولي الإنساني على التهديدات السيبرانية**

على الرغم من أن التهديدات السيبرانية لم يكن لها وجود عند إبرام اتفاقيات جنيف الأربع لعام ١٩٤٩ والبروتوكولين الإضافيين لعام ١٩٧٧، إلا أن هناك اتفاق دولي واسع النطاق على أن القدرة على استخدام التهديدات السيبرانية حسب القانون الدولي الإنساني يجب ألا تقيم مقابل فكرة مثالية افتراضية بل يجب مقارنتها بالبشر، انطلاقاً من هذا يسعنا القول إن قواعد القانون الدولي الإنساني الاتفاقية التي تطبق على الأهداف العسكرية المشروعة، أغلبها أصبحت قواعد عرفية ومعترف بها من قبل الدول وبالتالي إمكانية تطبيقها على التهديدات السيبرانية. وبناء على ذلك سنبين في المطلب الأول معايير تحديد الأهداف العسكرية المشروعة أثناء التهديدات السيبرانية في القانون الدولي الإنساني، أما المطلب الثاني فسنتحدث عن تطبيق المبادئ العامة في القانون الدولي الإنساني أثناء التهديدات السيبرانية.

---

٨ لين، هربرت: "النزاع السيبراني والقانون الدولي الإنساني"، مجلة اللجنة الدولية للصليب الأحمر، مجلد ٩٤ (٨٨٦)، صيف ٢٠١٢، ص ص ٥١٥-٥٣١، ص ٥١٩-٥١٨، متاح على الرابط: https://cutt.ly/RkoansD

9 Schmitt, Michael (gen ed): Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, New York, First Published,2013, Available At: https://cutt.ly/tkofrbK

*** الأشخاص والأعيان المشروع استهدافهم أثناء التهديدات السيبرانية في القانون الدولي الإنساني**

إذاً يعد المقاتلين من الأهداف العسكرية المشروعة، بالإضافة لذلك يدخل في نطاق الاستهداف جميع الأعيان الثابتة والمتحركة التي تسهم مساهمة فعالة في العمليات العدائية التي يباشرها أحد الأطراف، وأيضاً إذا شارك المدنيون مشاركة مباشرة في التهديدات السيبرانية يفقدوا الحماية التي يتمتعوا بها ويصبحون أهدافاً مشروعة.

من البديهي القول إن فئة المقاتلين هم أول فئة مشروع استهدافها أثناء التهديدات السيبرانية، أما بالنسبة إلى الأعيان المشروع استهدافها أثناء التهديدات السيبرانية فهي التي تسهم مساهمة فعالة في العمل العسكري وينتج عنها ميزة عسكرية أكيدة وللحديث بالتفصيل عن الأشخاص والأعيان المشروع استهدافهم أثناء التهديدات السيبرانية، سنتطرق بالحديث بداية عن التهديدات السيبرانية بوصفها هجوم بموجب القانون الدولي الإنساني ثم نبين مفهوم المقاتل السيبراني في القانون الدولي الإنساني، وأخيراً نتحدث عن الأعيان المشروع استهدافها أثناء التهديدات السيبرانية فيما يلي:

أولاً– التهديدات السيبرانية بوصفها هجوم بموجب القانون الدولي الإنساني

يوفر القانون الدولي الإنساني حماية خاصة لبنية تحتية معينة، مثل الخدمات الطبية والأعيان التي لا غنى عنها لبقاء السكان المدنيين، بغض النظر عن نوع العملية التي تلحق بها الضرر. ومع ذلك، فإن معظم القواعد الناشئة عن مبادئ التمييز والتناسب والاحتياط التي توفر حماية عامة للمدنيين والأعيان المدنية تنطبق فقط على العمليات العسكرية التي تشمل "هجمات" على النحو المحدد في القانون الدولي الإنساني. وتعرف التهديدات على أنها أعمال العنف ضد الخصم، سواء تم القيام بها على سبيل الهجوم أو الدفاع وبغض النظر عن المنطقة التي تنفذ فيها مثل تلك الأعمال"[١٠].

ومن وجهة نظر اللجنة الدولية، العمليات السيبرانية التي تنفذ بواسطة الفيروسات والديدان الحاسوبية وسائر الوسائل الأخرى وتلحق أضراراً مادية بأشخاص أو أضراراً مادية بممتلكات أخرى غير البرامج أو البيانات الحاسوبية التي تعرضت للهجوم نتيجة الآثار المباشرة أو غير المباشرة (أو الارتدادية) المتوقعة للهجوم بأنها "أعمال عنف"، أي هجوم بالمعنى المنصوص عليه في القانون الدولي الإنساني، على سبيل المثال وفاة المرضى فى وحدات العناية المركزة نتيجة لعملية سيبرانية ضد شبكة الكهرباء مما تسبب بقطع إمداد المستشفى بالتيار الكهربائي. إذاً من المتفق عليه على نطاق واسع أن العمليات السيبرانية التي يتوقع منها أن تسبب وفاة أو إصابة أو ضرراً مادياً تشكل هجمات بموجب القانون الدولي الإنساني[١١].

ويدعى أحياناً بأن التهديدات السيبرانية لا تندرج في نطاق تعريف "الهجوم" ما دامت لا تتسبب في أضرار مادية أو عندما يكون في الإمكان التخلص من الآثار الناجمة عنها.

[١٠] البروتوكول الإضافي الأول لعام ١٩٧٧، المادة ٤٩.

[١١] اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، ورقة موقف اللجنة الدولية للصليب الأحمر، تشرين الثاني ٢٠١٩، ص ٧.

وإذا كان المراد بهذا الادعاء تسويغ اعتبار الهجوم على ممتلكات مدنية عملاً قانونياً في هذه الحالات، فإن اللجنة الدولية ترى أنه ادعاء باطل لا أساس له بموجب القانون الدولي الإنساني. فلا يجوز، بموجب القانون الدولي الإنساني توجيه التهديدات إلا إلى الأهداف العسكرية ولا يجوز الهجوم على الأهداف المدنية[١٢].

ثانياً– التعريف بمفهوم المقاتل السيبراني في القانون الدولي الإنساني

تعد من أهم المسائل الشائكة التي لم يجمع عليها شراح القانون الدولي في وقتنا الحالي هي مفهوم المقاتل السيبراني أي من هو الشخص الذي يمكنه أن يشترك في العمليات العدائية السيبرانية ويتمتع بوصف المقاتل[١٣]. ويعرف المقاتلون بصفة عامة بأنهم: "الأشخاص الذين يخولهم طرف في نزاع مسلح استخدام القوة، تنفيذاً للعمليات العدائية في ميدان النزاع". ولا بد من الإشارة إلى أنه يتطلب تعريف المقاتل الشرعي بموجب القانون الدولي الإنساني مستوى من مسؤولية المنظمة أو قيادة الدولة، وهذه السمات موجودة داخل الدول التي لديها قوات مسلحة لديها قدرات سيبرانية[١٤]. حيث أنشأت العديد من البلدان فروعاً أو وحدات سيبرانية خاصة بها داخل القوات المسلحة، على سبيل المثال لا الحصر، لدى الولايات المتحدة الأمريكية القيادة السيبرانية للجيش الأمريكي (U.S. Army Cyber Command)[١٥]، وجيش التحرير الشعبي الصيني لديه قسم أو فريق سيبراني يسمى "الجيش الأزرق"[١٦]، ودولة النرويج لديها (Cyberforsvaret) أي الدفاع السيبراني الذي يقوم بإنشاء وتشغيل وحماية أنظمة اتصالات القوات المسلحة والبنية التحتية الرقمية[١٧].

وقد سعى تالين إلى تحديد من هم أعضاء القوات المسلحة" الذين يتمتعون بحقهم في الحصول على حصانة المقاتل ومركز أسير الحرب[١٨].

يمكن القول في رأينا، يشكل الأشخاص الذين يملكون أجهزة وبرامج سيبرانية بصفة منتظمة كمقاتلين تحت

---

[١٢] تقرير اللجنة الدولية للصليب الأحمر للمؤتمر الدولي الحادي والثلاثون للصليب الأحمر والهلال الأحمر، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، جنيف، سويسرا، ٢٠١١، الوثيقة: C٣١/٥,١,٢/١١، ص ٤٣-٤٢.

[١٣] درويش، سعيد: ماهية الحرب الإلكترونية في ضوء قواعد القانون الدولي، مجلة العلوم القانونية والاقتصادية والسياسية، العدد ٢٩، الجزء الثاني، جامعة الجزائر-كلية الحقوق، ٢٠١٨، ص ص١١٧-١٣٧، ص١٢٤، متاح على الرابط: https://cutt.ly/2kpMulR

[14] Gervais, Michael: "Cyber Attacks and The Laws of War", Berkeley Journal of International Law, Volume 30, Issue 2, Article 6,2012, PP 525-579, P566, Available At:https://cutt.ly/mkp1eep

[١٥] موقع القيادة السيبرانية للجيش الأمريكي، متاح على الرابط: https://www.arcyber.army.mil

[١٦] الصين: "جيش أزرق" لحماية شبكات " الجيش الأحمر"، موقع BBC NEWS، متاح على الرابط: https://www.bbc.com/arabic/scienceandtech/2011/06/110531_china_blue_army

[١٧] موقع Cyberforsvaret الدفاع السيبراني النرويجي، استرجعت بتاريخ ٣١/١/٢٠٢١، متاح على الرابط: https://www.forsvaret.no/

[18] Schmitt, Michael (gen ed): Tallinn Manual on the International Law Applicable to Cyber Warfare, op.cit, Rule (26)

راية طرف في هجوم سيبراني أهدافاً مشروعة لنظرائهم في الطرف الآخر، فضلاً عن كونهم وبهذه الصفة هم من يقع على كاهلهم التقيد بالالتزامات التي تفرضها عليهم قواعد ومبادئ القانون الدولي الإنساني.

ولا بد من الإشارة إلى أن مفهوم الهبة الشعبية ينطبق على التهديدات السيبرانية فبقدر ما "يحمل نشطاء القرصنة الأسلحة علانية" ويستجيبون بشكل دفاعي، يمكن أن يندرجوا في فئة الهبة الجماعية، ويحصلون على وضع أسير الحرب، إلا أن ما يعنيه "حمل السلاح علانية" في الفضاء السيبراني غير محدد حتى الآن[١٩].

وبالنسبة للمجموعات المسلحة المنظمة سيبرانياً تطبق نفس المعايير الخاصة بالعنف الحركي بموجب القانون الدولي الإنساني عند تقدير وجود نزاع مسلح غير دولي ينطوي على هجمات سيبرانية، أي أنه يجب أن تكون هذه الجماعة منظمة ولديها القدرة على الانخراط في عنف شديد بما فيه الكفاية[٢٠].

فالجماعات المسلحة المنظمة افتراضياً على الرغم من صعوبة إثبات ما إذا كانت قد استوفت الحد الأدنى للتنظيم المطلوب حتى تصبح طرفا في نزاع مسلح غير ذي طابع دولي إلا أنه ليس من المستحيل تقدير ذلك، وبناء عليه يمكن أن تصبح طرفاً في النزاع[٢١].

وكما يقول مايكل شميت،" إن أعضاء المنظمات الافتراضية ربما لا يلتقون أبداً بل وربما لا يعرفون النشاط الفعلي لبعضهم البعض. ومع ذلك، فيمكن لهذه المجموعات أن تتصرف بطريقة منسقة ضد الحكومة (أو جماعة مسلحة منظمة)، وأن تتلقى أوامر من قيادة افتراضية، وأن تكون منظمة للغاية. فعلى سبيل المثال: من العناصر التي قد تكلف بها المجموعة تحديد نقاط الضعف في الأنظمة المستهدفة، وقد يكون العنصر الثاني هو تطوير برامج ضارة لاستغلال نقاط الضعف المذكورة، وقد يكون العنصر الثالث تنفيذ العمليات، وقد يكون العنصر الرابع الحفاظ على دفاعات سيبرانية ضد التهديدات المضادة[٢٢].

ومن ناحية القدرة على الانخراط في عنف شديد بما فيه الكفاية، إذا أفضت التهديدات السيبرانية إلى نفس العواقب العنيفة التي تقضي إليها العمليات الحركية، أي إذا استخدمت على سبيل المثال لفتح بوابات السدود أو التسبب في اصطدام الطائرات أو القطارات، فإنها تصل إلى درجة الحدة اللازمة لاعتبار الجماعة المسلحة المنظمة افتراضياً طرفاً في نزاع مسلح

[19] Gervais, Michael: "Cyber Attacks and The Laws of War", op.cit, loc.cit.

[٢٠] اللجنة الدولية للصليب الأحمر، تعليق اللجنة الدولية للصليب الأحمر على المادة الثالثة المشتركة، التعليق رقم ٤٣٦، منشورات اللجنة الدولية للصليب الأحمر، ص ٤١، متاح على الرابط:https://cutt.ly/Akp3Hqm

[٢١] اللجنة الدولية للصليب الأحمر، تعليق اللجنة الدولية للصليب الأحمر على المادة الثالثة المشتركة، التعليق رقم ٤٣٧، مرجع سبق ذكره، نفس الموضع.

[٢٢] دوريجي، كوردولا: "لا تقترب من حدود فضائي الإلكتروني: الحرب الإلكترونية والقانون الدولي الإنساني وحماية المدنيين"، المجلة الدولية للصليب الأحمر، مجلد ٩٤ (٨٨٦) صيف ٢٠١٢، ص ص ٥٣٣-٥٧٨، ص ٥٥١، متاح على الرابط: https://cutt.ly/Okp7S5Z

غير دولي. وفي المقابل إذا كانت تقتصر فقط على إعاقة وظائف الانترنت أو استغلال الشبكات أو سرقة البيانات أو حذفها أو إتلافها، فمن غير المرجح الوصول إلى درجة حدة العنف التي تقتضي توافرها في القانون الدولي الإنساني، وبالتالي لا تصبح طرف في النزاع المسلح غير ذي طابع دولي[٢٣].

ثالثاً– الأعيان المشروع استهدافها أثناء التهديدات السيبرانية

يوضح دليل تالين أن التهديدات السيبرانية على الحواسيب وشبكات الحاسوب والبنية التحتية السيبرانية، يجب أن تقتصر حصراً على الأهداف العسكرية، بينما لا يجوز أن تكون الأعيان المدنية هدفاً للهجوم السيبراني، وبالنسبة للأعيان المزدوجة بين العين العسكرية والعين المدنية تصبح هدف عسكري طوال هذا الاستخدام، وأعرض فيما يلي المعنى العام للهدف العسكري والأعيان المزدوجة.

١– المعنى العام للهدف العسكري يجب أن يستوفي الهدف شرطين لتصنيفه هدفاً عسكرياً

*** الشرط الأول**

يجب أن يسهم الهدف مساهمة فعالة في العمل العسكري للطرف المعادي، ويتم ذلك من خلال أحد هذه المعايير الأربعة: –

١– المعيار الأول: بحكم "طبيعته": وهي الصفة المتأصلة في الشيء وتشير عادةً إلى الأشياء التي هي في الأساس عسكرية، وتعتبر أجهزة الكمبيوتر العسكرية والبنية التحتية الإلكترونية العسكرية أمثلة نموذجية للأشياء التي تلبي معيار الطبيعة[٢٤].

٢– المعيار الثاني: بحكم "موقعه": يشير الموقع عادة إلى منطقة جغرافية ذات أهمية عسكرية خاصة وفي حديثنا على سبيل المثال: إن عنوان (IP)أو (كتلة عناوين IP) ليس موقعاً على الرغم من أنه مرتبط بالبنية التحتية السيبرانية التي قد تكون مؤهلة كهدف عسكري. فالمقصود ليس الاستخدام الفعلي لمنطقة ما، ولكن المقصود أنها تقدم مساهمة فعالة في العمل العسكري للعدو من خلال موقعها مما يجعلها هدفاً عسكرياً. على سبيل المثال، قد يتم استخدام عملية سيبرانية ضد نظام SCADA[25] لخزان ما لإطلاق المياه في منطقة يتوقع فيها وجود عمليات عسكرية للعدو، وبالتالي حرمان العدو من استخدامها، في هذه الحالة تكون مساحة الأرض هدفاً عسكرياً لما لها من فائدة عسكرية للعدو[٢٦].

٣– المعيار الثالث: بحكم "استخدامها": عندما يتم استخدام هدف أو منشأة مدنية لأغراض عسكرية، فإنها تصبح هدفاً عسكرياً من خلال معيار "الاستخدام"، على سبيل المثال: محطات التلفزيون أو الإذاعة المدنية التي تبث بانتظام معلومات

---

[٢٣] اللجنة الدولية للصليب الأحمر، تعليق اللجنة الدولية للصليب الأحمر على المادة الثالثة المشتركة، مرجع سابق، نفس الموضع.

[24] Schmitt, Michael (gen ed) :Tallinn Manual on the International Law Applicable to Cyber Warfare, op.cit, comment (6) on Rule (38).

[25] نظام (SCADA) أو (التحكم الإشرافي واكتساب البيانات) هو نظام مصمم خصيصاً لتشغيل البنية التحتية والتحكم فيها، مثل الكهرباء وأنظمة الطاقة النووية والاتصالات ومنشآت تخزين النفط. انظر: الشوابكة، مراد: ما هو نظام سكادا، موقع موضوع (أكبر موقع عربي بالعالم)، متاح على الرابط.https://cutt.ly/5kCk8TQ

[26] Ibid, comment (7) on Rule (38).

عسكرية. بالتالي إن استخدم أحد أطراف النزاع شبكة كمبيوتر مدنية معينة لأغراض عسكرية، تفقد الشبكة طابعها المدني وتصبح هدفا عسكريا. وحتى إذا استمرت الشبكة أيضاً في الاستخدام للأغراض المدنية فهي تبقى هدف عسكري[٢٧]. ولا بد من الإشارة إلى أنه يمكن للأعيان المدنية التي أصبحت أهدافاً عسكرية عن طريق الاستخدام، أن تعود إلى الوضع المدني إذا توقف الاستخدام العسكري بمجرد حدوث ذلك، يستعيدون حمايتهم من الهجوم[٢٨].

٤- المعيار الرابع: بحكم "الغرض": يشير إلى الاستخدام المستقبلي المزمع لشيء ما، أي أنه لا يتم استخدام العين حالياً لأغراض عسكرية، ولكن من المتوقع استخدامه في المستقبل، ويكتسب وضع الهدف العسكري بمجرد أن يتضح هذا الغرض، ولا يحتاج المهاجم إلى انتظار تحويله إلى هدف عسكري من خلال الاستخدام إذا كان الغرض قد تبلور بالفعل بدرجة كافية. على سبيل المثال، إذا توفرت معلومات موثوقة تفيد بأن أحد أطراف النزاع على وشك شراء أجهزة أو برامج كمبيوتر معينة لأغراض عسكرية، فإن هذه العناصر تصبح على الفور أهدافاً عسكرية[٢٩].

*** الشرط الثاني**

يجب أن يكون تدمير الهدف أو الاستيلاء عليه أو تعطيله يوفر للطرف المهاجم ميزة عسكرية أكيدة تشير "الميزة العسكرية" إلى تلك الميزة المتأتية من الهجوم، ويُقصد بمصطلح "الميزة العسكرية" استبعاد ميزة ليست عسكرية بطبيعتها، على وجه الخصوص، الميزة الاقتصادية أو السياسية أو النفسية.

على سبيل المثال، إن الهجوم السيبراني على قطاع عمل مدني، ظناً من قبل المهاجم أنه سيضعف بشكل عام الدولة المعادية، لن يؤدي بالضرورة إلى ميزة عسكرية بالمعنى المطلوب، حتى أنه لا يعد هدف عسكري لأنه لا يقدم مساهمة فعالة في العمل العسكري، فالتوصيف كهدف عسكري، يجب أن تكون الميزة العسكرية التي يحتمل أن تنتج واضحة[٣٠].

٢- الأعيان ذات الاستخدام المزدوج: نقصد بذلك الأعيان المدنية التي تستخدم لأغراض عسكرية في نفس الوقت، نتيجة لذلك تصبح هدفاً عسكرياً طوال هذا الاستخدام[٣١]، وقد تم ذكر هذه القاعدة في إطار المادة ٥٢(٢) من البرتوكول الإضافي الأول، والقاعدة ٣٩ من دليل تالين، ولا بد من الإشارة أن الهجوم على الأعيان ذات الاستخدام المزدوج تخضع لمبدأ التناسب وشرط اتخاذ الاحتياطات في الهجوم[٣٢]. بالتالي تشكل التهديدات السيبرانية تحديات فريدة في هذا

[27] Ibid, comment (8) on Rule (38).
[28] Ibid, comment (10) on Rule (38).
[29] Schmitt, Michael (gen ed) :Tallinn Manual on the International Law Applicable to Cyber Warfare, op.cit, comment (11) on Rule (38).
[30] Ibid, comment (18) on Rule (38).

[٣١] ميلزر، نيلس: مقدمة شاملة القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر، ٢٠١٦؛ هنكرتس، جون-ماري. ودوزوالد-بك، لويز: القانون الدولي الإنساني العرفي (المجلد الأول/القواعد)، اللجنة الدولية للصليب الأحمر، ٢٠١٦، ص٨٩.
[32] Schmitt, Michael (gen ed) :Tallinn Manual on the International Law Applicable to Cyber Warfare, op.cit, comment (2) on Rule (39).

الصدد، فالشبكة الالكترونية التي تُستخدم للأغراض العسكرية والمدنية، قد يكون من المستحيل معرفة أي جزء من الشبكة سيمر عبر الإرسالات العسكرية، وأي منها في الأجزاء المدنية، ففي مثل هذه الحالات، الشبكة بأكملها (أو على الأقل تلك الأجزاء التي من المحتمل بشكل معقول أن يكون الإرسال فيها) مؤهلة كهدف عسكري[٣٣]. وتثير العواقب الإنسانية المترتبة على هذه الحالة قلقاً بالغاً على حماية السكان المدنيين، ففي عالم يعتمد فيه قطاع كبير من البنية الأساسية المدنية، والاتصالات المدنية، والشؤون المالية والاقتصاد والتجارة والصحة على البنية الأساسية الإلكترونية الدولية، يصبح من السهل للغاية أن تقوم الأطراف بتدمير هذه البنية الأساسية، وسيبرر تعطيل الكابلات الرئيسية أو الشبكات أو أجهزة التوجيه أو الأقمار الاصطناعية التي تعتمد عليها هذه النظم، دائماً بحقيقة أن هذه المسارات تستخدم لنقل معلومات عسكرية وهي من ثم تصنف كأهداف عسكرية[٣٤].

إلا أنه هناك بعض البيانات المدنية تتعلق بأعيان معينة تتمتع بحماية خاصة بموجب القانون الدولي الإنساني[٣٥] وهي الأعيان والمواد التي لا غنى عنها لبقاء السكان المدنيين، والأعيان الطبية، والأشغال الهندسية والمنشآت التي تحوي على مواد وقوى وطاقات خطرة والبيئة الطبيعية، والأعيان الثقافية وأماكن العبادة[٣٦]، فالالتزام باحترام وحماية هذه الأعيان الخاصة يفترض بأنه يشمل حماية البيانات الخاصة بهذه الأعيان أيضاً[٣٧].

فالهجوم السيبراني الذي استهدف المستشفى التابع لجامعة هاينرش هاينه في مدينة دوسلدورف في شهر أيلول/ ٢٠٢٠، وتسبب بشكل غير مباشر في وفاة مريضة. كان الهدف منه في الأصل ابتزاز الجامعة إلا أنه أدى إلى انهيار الشبكة المعلوماتية السيبرانية الخاصة بمستشفى الجامعة، وأدى إلى عجز المستشفى عن مواصلة أنشطتها بصورة اعتيادية بسبب استمرار تعطل الشبكة السيبرانية لفترة طويلة، إلا أنه وبعد تمكن الشرطة من التواصل مع الهاكرز وإبلاغهم بأن هجومهم يعيق أنشطة المستشفى، سلموا إلى السلطات مفتاحاً إلكترونياً يتيح معالجة المشكلة واستئناف المعلومات التي طالها الهجوم[٣٨].

بالتالي إن مثل هذا الهجوم الذي استهدف المستشفى، من المستحيل القول إن المستشفى كانت تستخدم

[33] Ibid, comment (3) on Rule (39).

[٣٤] دوريجي، كوردولا: "لا تقترب من حدود فضائي الإلكتروني: الحرب الإلكترونية والقانون الدولي الإنساني وحماية المدنيين"، مرجع سابق، ص ٥٦٤.

[٣٥] حمدان، إيمان: التكنولوجيا الجديدة والقانون الدولي الإنساني (الحرب السيبرانية)، دراسات معقمة في القانون الدولي الإنساني، الماجستير في القانون الدولي الإنساني، الجامعة الافتراضية السورية، دمشق (سوريا)، ٢٠٢٠م، ص٩.

[٣٦] كلزي، ياسر: النظرية العامة في القانون الدولي الإنساني، ماجستير القانون الدولي الإنساني، الجامعة الافتراضية السورية، دمشق(سوريا)، ٢٠٢٠، ص ١٠٢.

[٣٧] حمدان، إيمان: التكنولوجيا الجديدة والقانون الدولي الإنساني (الحرب السيبرانية)، مرجع سابق، ص٩.

[٣٨] وفاة مريضة جراء هجوم سيبراني على مستشفى ألماني، موقع RTonline، متاح على الرابط: https://cutt.ly/1h5JyOu

لأغراض عسكرية حتى يتم استهدافها، ومن ناحية أخرى يستدعي إلى التفكير بأن ما هي الميزة العسكرية التي حققها. في هذا الصدد، يجب إيلاء اهتمام خاص لمتطلبات إجراء هجمات بطريقة مصممة لتقليل الضرر اللاحق بالسكان المدنيين والأعيان المدنية[٣٩].

هذا بالنسبة إلى البيانات المتعلقة بالأعيان التي تتمتع بالحماية الخاصة، وعلى الرغم من ذلك تم استهدافها، فماذا بالنسبة إلى البيانات المدنية الأساسية المتعلقة بالأعيان التي لا تتمتع بالحماية الخاصة مثل بيانات الأمن الاجتماعي والضرائب السجلات والحسابات المصرفية فمن المحتمل أن تفلت من الامتداد التنظيمي لقانون الدولي الإنساني، وبالتالي تتعارض مع المبدأ" أن السكان المدنيين يتمتعون بحماية عامة من آثار الأعمال العدائية"[٤٠]. وحسب رأي اللجنة الدولية للصليب الأحمر فإن "استثناء البيانات المدنية الأساسية من الحماية التي يوفرها القانون الدولي الإنساني للأعيان المدنية من شأنه أن يؤدي إلى ثغرة كبيرة في هذه الحماية"[٤١].

*** تطبيق المبادئ العامة في القانون الدولي الإنساني أثناء التهديدات السيبرانية**

ثمة حاجة ملحة للقيام بموائمة التهديدات السيبرانية مع القانون الدولي الإنساني، نظرا لأن أعمال الحرب السيبرانية ستسفر عن خرق أحكام عديدة في القوانين الحالية المسلحة أو أنها ستكون خارج نطاق هذه القوانين تماماً، فيجب احترام الأطر الكبرى والاتفاقية المهمة في هذا القانون، خاصة اتفاقيات جنيف لعام ١٩٤٩ والبروتوكول الإضافي الأول الخاص بحماية ضحايا المنازعات الدولية المسلحة (البروتوكول الأول)[٤٢]، واتفاقيات لاهاي (١٨٩٩ و١٩٠٧) الخاصة باحترام قوانين وأعراف الحرب البرية، ونظام روما الأساسي للمحكمة الجنائية الدولية.

كما ينبغي احترام مبادئ القانون الدولي الإنساني الممكن انطباقها على التهديدات السيبرانية، من خلال توفير قدر كاف من الحماية للبنية التحتية الحيوية لمنع أوجه التدمير، والأذى والمعاناة غير الضرورية، وضمان الحد الأدنى من الاتصالات الأساسية ذات الصلة بحماية المدنيين، حيث أن البنى التحتية الحيوية المحمية ستشمل البنى التي تدعم المستشفيات، والمرافق الطبية ومراكز دور العجزة، والنظم

[39] Schmitt, Michael (gen ed) :Tallinn Manual on the International Law Applicable to Cyber Warfare, op.cit, Rule (52)

[40] Mccormack, Tim: International Humanitarian Law and The Targeting of Date, Volume 94 ,International Law studies, U.S. Naval War College, United States, 2018, PP223-240, P227,Available At: https://cutt.ly/DksuNk5

[٤١] حمدان، إيمان: التكنولوجيا الجديدة والقانون الدولي الإنساني (الحرب السيبرانية)، مرجع سابق، ص٩.

[٤٢] جودي ر. وستبي، دعوة إلى الاستقرار الجيوسيبراني، الاتحاد الدولي للاتصالات، مقال منشور على الرابط الإلكتروني، جانفي ٢٠١١، ص ٦٥، الرابط الإلكتروني. https://www.itu.int/dms_pub/itu-s/opb/gen/S-.GEN-WFS.01-1-2011-MSW-A.docx

المالية، ونظم دعم الحياة والأجهزة الطبية الهامة، وسلاسل الإمداد، ووسائل النقل، ومرافق الأخبار ودور العبادة والمراكز الدينية، والمرافق التعليمية، والمسعفين، وأجهزة إنفاذ القانون، وليس المقصود بالقائمة المعروضة آنفاً أن تكون كاملة، بل أن تقدم أمثلة على أنواع النظم التي تساند المدنيين الأبرياء وتكون النظم والأجهزة المعلوماتية التي تحميها عرضة للهجمات الإلكترونية، بما في ذلك صغار الأطفال، والعجزة، والجرحى، والعجائز، ومن المفروض أن تساعد مساهمات الجهات المعنية الدبلوماسيين في رسم الحدود المقدسة للبنية التحتية الحيوية[٤٣].

فيجب على الطرف المسؤول عن هجوم سيبراني ما اتخاذ التدابير إلى أقصى قدر ممكن، من أجل تفادي أو تخفيف الضرر العرضي الذي يلحق بالبنية التحتية المدينة أو يؤذي المدنيين، وهذا سيتطلب التحقق من طبيعة النظم التي تتعرض للهجوم والأضرار المحتملة التي قد تنجم عن أحد التهديدات، وهذا يعني أيضاً أنه عندما يصبح جلياً أن هجوماً سيتسبب بإصابات أو أضرار مدنية عرضية، يجب إلغاؤه أو العدول عنه.

علاوة على ذلك، يجب على أطراف النزاع أن تلتزم باتخاذ الاحتياطات اللازمة من آثار التهديدات، ونتيجة لذلك، تكون نظم الحواسيب العسكرية منفصلة بما يكفي عن تلك المدنية، بغية حماية السكان المدنيين من آثار التهديدات العرضية والعشوائية، ويُمكن للاعتماد على نظم الحواسيب العسكرية والتوصيل بين نظم الحواسيب التي يديرها متعاقدون مدنيون وتُستخدم أيضاً لأغراض مدنية أن يثير القلق، وعلى صعيد آخر، قد تساهم تكنولوجيا المعلومات أيضاً في الحد من الأضرار العرضية التي تلحق بالمدنيين أو البنية التحتية المدنية، وعلى سبيل المثال، قد يلحق تعطيل خدمات معينة تُستخدم لأغراض عسكرية ومدنية أضراراً أقل مما يُلحق تدمير البنية التحتية تماماً، وفي هذه الحالات، يفرض مبدأ الاحتياط القابل للجدل التزاماً على الدول باختيار الوسائل الأقل ضرراً بغية تحقيق أهدافها العسكرية[٤٤].

لذا فإن الأذى والضرر الناجمين عن تدمير أو تعطيل نظم البنية التحتية الحيوية غير ضروريين وسيتسببان في معاناة ومصاعب جسيمة من النوع الذي هدفت قوانين النزاع المسلح إلى منعه، وفضلاً عن ذلك، ولأن هذه الشبكات تخدم أعداداً ضخمة من السكان، فإن الأذى والضرر المتأتيين من مثل هذا الهجوم سيكونان على نطاق واسع وغير متناسبين مع المزايا العسكرية المستخلصة، وبالتالي، من المهم للغاية أن توضح هذه المسألة في حالة السكان المدنيين، فحسبما يرى الشخص، من منظور ضيق أو منظور واسع، أنواع العمليات الإلكترونية التي تخضع للقواعد التي تحكم سير العمليات العدائية، يمكن أن تكون الأعمال التالية محظورة أو قانونية في سياق نزاع مسلح:-

١- تعطيل شبكة الكهرباء المدنية أو نظام لمعالجة المياه (دون إلحاق أضرار مادية بها).

[٤٣] البرتوكول الإضافي الثاني الملحق باتفاقيات جنيف والمتعلق بحماية ضحايا المنازعات المسلحة غير الدولية، ٨ حزيران/يونيه ١٩٧٧، تاريخ بدء النفاذ: ٧ كانون الأول/ديسمبر ١٩٧٨، الرابط الإلكتروني. https://www.legal-tools.org/doc/0453fb/pdf/

[٤٤] حمدون إ. توريه، الاستجابة الدولية للحرب السيبرانية، مقال إلكتروني ص ١٠٢، https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-MSW-A.docx

٢- توجيه هجوم يترتب عليه حرمان نظام مصرفي من خدمة الإنترنت مما يكون له تأثير كبير على قدرة عدة ملايين من عملاء المصرف على الحصول على الخدمات المصرفية.

٣- توجيه هجوم يترتب عليه الحرمان من الخدمات المقدمة عبر نظام خاص لحجز رحلات الطيران عبر الإنترنت من أجل التسبب في عدم تمكن السكان المدنيين من مغادرة مناطق النزاع.

٤- إغلاق شبكة الإنترنت وشبكات الهاتف المحمول في منطقة معينة من البلد لمنع الدعاية التي يطلقها الخصم[٤٥].

كما أنه على البلدان أن تحترم حياد البلدان الأخرى وألا تنقل أي نوع من التهديدات عبر بناها التحتية الحيوية وهذا يتسق هذا مع اتفاقيات لاهاي ١٨٩٩ و١٩٠٧ في المادة ٠٥ و١٣، التي تقيّد نقل القوات أو قوافل الإمدادات أو الذخائر عبر الأقاليم أو المياه المحايدة، وبالمستطاع تدمير العديد من البنى التحتية الحيوية، مثل الشبكات الكهربائية، من خلال فرط تحميل النظام، وهكذا فإن السماح للبلدان بشن التهديدات السيبرانية التي يمكن أن تعبر من خلال العديد من شبكات البلدان الأخرى دون علمها لا يتسق ببساطة مع تاريخ القوانين الدولية للنزاع المسلح والغاية منها، وسيتطلب هذا المبدأ المقترح الحصول على إذن من البلدان الأخرى قبل شن هجوم سيبراني، وبالتالي العمل كرادع ضد شن هجوم سيبراني[٤٦].

كما أن مبدأ التمييز يُلزم الدول بأن تميّز في جميع الأحوال بين المدنيين والمقاتلين وبين الأعيان المدنية والأهداف العسكرية، وهو مبدأ أساسي من مبادئ القانون الدولي الإنساني، على حد قول محكمة العدل الدولية، ولا يجوز توجيه التهديدات إلا نحو المقاتلين أو الأهداف العسكرية، ويعني هذا أنه عند تخطيط وتنفيذ العمليات الإلكترونية، فإن الأهداف المسموح بها فقط في إطار القانون الدولي الإنساني هي الأهداف العسكرية، مثل أجهزة الكمبيوتر أو النظم الحاسوبية التي تحقق مساهمة فعالة في العمليات العسكرية الملموسة، ولا يجوز توجيه التهديدات عبر الفضاء الإلكتروني نحو النظم الحاسوبية المستخدمة في منشآت مدنية بحتة[٤٧].

*** دليل تالين والقدرات الوطنية والدولية في مواجهة التهديدات السيبرانية**

في هذا المبحث سنتناول دليل تالين كأحد الأطر القانونية الجديدة لمواجهة التهديدات السيبرانية من خلال مجموعة القواعد والمبادئ المتفق عليها والتي تشكل الأرضية الحقيقة لبداية البحث عن السبل من أجل تطوير قواعد القانون الدولي الإنساني لتستوعب مثل هذه الحروب، وصولا إلى الحلول الموجودة لدى الدول أو المتفق عليها في القانون الدولي

[٤٥] كوردولا دروغيه المستشارة القانونية في اللجنة الدولية، ما من فراغ قانوني في الفضاء السيبراني، مقال منشور على موقع اللجنة الدولية للصليب الأحمر بتاريخ ١٦/٠٨/٢٠١١، الرابط الإلكتروني. https://www.icrc.org/ar/doc/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm

[٤٦] عمر محمود اعمر، الحرب الإلكترونية في القانون الدولي الإنساني، دراسات علوم الشريعة والقانون، المجلد ٤٦ عدد ٠٣، ٢٠١٩، الرابط الإلكتروني. https://journals.ju.edu.jo/DirasatLaw/article/viewFile/101907/10621?target =_ blank

[٤٧] جودي ر. وستبي، المرجع السابق، ص ٦٨.

والتي يمكن التقيد بها في حال حدوث حرب سيبراني، وهي مجالات بدأ التوافق حولها ووجب تطويرها كما سنرى.

*** دليل تالين بشأن التهديدات السيبرانية**

يعد دليل تالين المتعلق بالقانون الدولي المنطبق على عمليات حرب الفضاء الإلكتروني أو التهديدات السيبرانية المشار إليه باسم دليل تالين، هو الإجراء الأشمل الذي يسعى إلى تفسير قواعد القانون الدولي (الحق في الحرب وقانون الحرب)، في إطار الحرب الإلكترونية، وقد صاغ هذا الدليل مجموعة من الخبراء بناء على دعوة من مركز الامتياز التعاوني للدفاع عن الفضاء الإلكتروني التابع لمنظمة حلف شمال الأطلسي، وهو يقدم مجموعة مفيدة من القواعد التي تقترن بتعليق يعكس مختلف الآراء بشأن المسائل الشائكة التي تثيرها هذه التكنولوجيا الجديدة، وشاركت اللجنة الدولية للصليب الأحمر في مداولات مجموعة الخبراء بوصفها مراقبًا، إلا أنها لا توافق على جميع الآراء الواردة في الدليل[٤٨].

ويقدم دليل تالين رؤى مثيرة للاهتمام في هذا الصدد، فهو يتمسك على سبيل المثال بالثنائية التقليدية للنزاعات المسلحة الدولية والنزاعات المسلحة غير الدولية، ويقر بأن العمليات الإلكترونية وحدها قد تشكل نزاعات مسلحة تبعاً للظروف – لا سيما الآثار المدمرة لتلك العمليات–، ويقدم الدليل في هذا الصدد تعريفاً للهجوم السيبراني بموجب القانون الدولي الإنساني بوصفه "عملية إلكترونية سواء هجومية أو دفاعية يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الإضرار بأعيان أو تدميرها.

ويكمن صلب الموضوع مع ذلك في التفاصيل أي ما ينبغي أن يُفهم على أنه "ضرر" في العالم الالكتروني، وبعد مناقشات مكثفة، اتفق أغلب الخبراء على أنه علاوة على الضرر المادي فإن توقف أحد الأعيان عن العمل قد يشكل ضرراً أيضاً، وتتمثل وجهة نظر اللجنة الدولية للصليب الأحمر مع مبادئ دليل تالين في أنه إذا تعطل أحد الأعيان، فليس من المهم كيفية حدوث ذلك سواء بوسائل حركية أو عملية إلكترونية، وهذه القضية مهمة للغاية في الممارسة العملية حيث أن أي عملية إلكترونية تستهدف تعطيل شبكة مدنية خلاف ذلك، لن يشملها الحظر الذي يفرضه القانون الدولي الإنساني على الاستهداف المباشر للأشخاص المدنيين والأعيان المدنية[٤٩].

ويذكر الدليل أيضًا أن مبدأي الاحتياط والتناسب، يجب احترامهما في حال تعرضت شبكة الإنترنت أو أجزاء كبيرة منها للهجوم، ولكن على الرغم من أن هذا قد يبدو مطمئنًا للوهلة الأولى، فهو يترك إشكالية حول ما إذا كان من الممكن أو غير الممكن استهداف شبكة الإنترنت بالكامل، أو استهداف أجزاء منها إذا كانت تستخدم في الاتصالات العسكرية وكان تدميرها أو تعطيلها يوفر ميزة عسكرية أكيدة (مرة أخرى رهنًا بالتناسب والاحتياطات).

[٤٨] حماية الأشخاص المدنيين والسكان في وقت الحرب، المقتطف من القواعد الأساسية لاتفاقيات جنيف وبروتكولها، اللجنة الدولية للصليب الأحمر، ٣١ ديسمبر ١٩٨٨، www.icrc.org/web/eng/siteeng0.nsf/html/57JMJ.

[٤٩] كوردولا دوريجي، المرجع السابق، ص ٥٤١.

وينص دليل تالين بشأن مبدأ الاحتياط على أنه بالنظر إلى تعقد العمليات الإلكترونية، وارتفاع احتمالات الإضرار بالنظم المدنية، والفهم المحدود في بعض الأحيان لطبيعتها وتأثيرها لدى المسؤولين عن اعتماد العمليات الإلكترونية، ينبغي أن تتاح لمخططي المهام، حيثما أمكن، الاستعانة بالخبرة التقنية الموجودة لمساعدتهم في تحديد ما إذا كانت التدابير الاحتياطية الملائمة قد اتخذت، وإذا كانت الخبرة، ومن ثم القدرة على تقييم طبيعة الهجوم والخسائر والأضرار العرضية بين المدنيين، غير متاحة، فقد يتعين على المهاجم الامتناع عن الهجوم[٥٠].

*** الأساليب الوطنية والدولية المقترحة لمواجهة التهديدات السيبرانية**

على المستوى الوطني فإن معظم الحكومات تعترف بضرورة إعادة توزيع الموارد وإصلاح استراتيجيات الأمن الوطنية على بعض المستويات، وتبادر كثير من البلدان إلى زيادة التمويل وبحث الموارد التكتيكية والدبلوماسية لتعزيز أمنها السيبراني، مما يجعلها تصمم أسلحة سيبرانية هجومية وقدرات دفاعية أيضاً، وهي تعتبر الأسلحة السيبرانية بمثابة "مضاعِفات القوة" التي ينبغي استعمالها في المقام الأول بالاقتران مع الأعمال العسكرية الأكثر تقليدية من أجل تعزيز قدراتها الحربية بشكل كبير، ويمكن أن يشمل هذا النوع من التحويل تدريب الموظفين العسكريين (أو إعادة تدريبهم)، وتحديث خدمات الاستخبارات للتركيز على جمع المعلومات العلمية والتكنولوجية ذات الصلة وإجراء عمليات محاكاة للحرب السيبرانية والمناورات العسكرية مع إيلاء اهتمام خاص لتطبيقات تكنولوجيا المعلومات والاتصالات، كما قد يشمل إنشاء فرق حربية للإنترنت تكون مكرسة لتحقيق الأمن السيبراني، ويمكن دمجها في وكالات استخبارات الدول[٥١].

أما على المستوى الدولي فإنه نظراً لأن المعايير والصكوك القانونية الدولية الحالية غير مجهزة تجهيزاً كاملاً للتعامل مع التحديات الجديدة التي يطرحها الأمن السيبراني، يعتبر الحوار العالمي والتعاون من الأمور الضرورية بهذا الشأن، والطبيعة المتغيرة للتكنولوجيا ذاتها – مع تداخلات متزايدة بين السلطات القضائية الوطنية وتكنولوجيا المعلومات والاتصالات المرتبطة بها، والموارد والأنظمة على الخط – تجعل اعتماد استراتيجيات جديدة والتعاون الدولي يتسمان بأهمية أكثر لضمان السلام السيبراني[٥٢].

ومن الضروري أن تعمل البلدان على تنسيق أطرها القانونية لمكافحة الجرائم السيبرانية وتيسير التعاون الدولي، ويتعين على الدول أن تعمل في سبيل وضع إطار قانوني وتنظيمي مشترك، وإقامة نظام لتحديث هذه القوانين على أساس منتظم لمعالجة الطبيعة المتغيرة للتهديدات التي يتعرض لها الأمن، وقد دعت بعض المجموعات بالفعل إلى إصدار معايير دولية وقواعد سيبرانية كوسيلة لتحسين الأمن السيبراني على

[٥٠] ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية، اللجنة الدولية للصليب الأحمر، مقال منشور على موقع اللجنة بتاريخ ٢٨/٠٦/٢٠١٣، الرابط الإلكتروني .
https://www.icrc.org/ar/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm

[٥١] كوردولا دوريجي، المرجع السابق، ص ٥٧٤.

[٥٢] حمدون إ. توريه، الاستجابة الدولية للحرب السيبرانية، المرجع السابق، ص ١٠٥.

الصعيد الدولي، فيتعين لدى إصدار مبادئ توجيهية لتحقيق الأمن السيبراني بين الدول، النظر في الخصائص المميزة للفضاء السيبراني وأبرز التحديات التي تطرحها هذه السمات، وذلك من خلال وضع استراتيجيات من أجل تطوير نموذج للتشريعات المتعلقة بالجرائم السيبرانية يكون قابلاً للتطبيق والتنفيذ على الصعيد العالمي، ويساعد في فهم الجوانب القانونية للأمن السيبراني من أجل تنسيق الأطر القانونية لا سيما من خلال موارده المختلفة الخاصة بالتشريعات المتعلقة بالجرائم السيبرانية[٥٣].

*** الخاتمة**

من كل هذا نصل إلى أن التهديدات السيبرانية تعد حربا حقيقية بمفهوم النزاعات المسلحة في القانون الدولي الإنساني، لاعتمادها على التهديدات ولاستهدافها مجمل ما تستهدفه الحرب، كما أنها تلحق أضرارا قد تضاهي في جسامتها أضرار الحروب التقليدية، ما يظهر الحاجة العاجلة في الوقت الحاضر من حيث تحديد مجالات الحماية والأشخاص المحميين من أثار هذه التهديدات السيبرانية، ونوع هذه الحماية المقدمة لهذه الفئات المحمية.

كما أن القانون الدولي الإنساني يمكن في شكله الحالي أو بعد تطويره أن ينطبق على التهديدات السيبرانية بعد ضبط مدلولها ومجالاتها بشكل دقيق، خاصة أنه في الفضاء السيبراني كما أشار د. حمدون توريه، الذي تتسم كل دقيقة تمضي فيه بالأهمية، فإن الحل الواضح والأمثل يتمثل في تطوير اتفاقيات القانون الدولي الإنساني القائمة، وجعلها أكثر قابلية لتشمل كل أنواع التهديدات وكل أنواع المخاطر والأضرار الناتجة عن هذه التهديدات، خاصة أن إبرام معاهدات جديدة خاصة بالتهديدات السيبرانية فقط محفوفة بالمشكلات لتداخل هذه التهديدات مع الحروب التقليدية؛ كما أن هذه الاتفاقيات تتطلب مداولات مطولة متعددة الأطراف في مرحلة الصياغة، لتفتح بعدها للتوقيع، وبعد هذا يتعين على الأطراف الموقعة المصادقة على المعاهدة قبل أن تدخل حيز التنفيذ، بل وحتى عقب ذلك فإنها لن تكون سارية المفعول إلا بالنسبة إلى تلك البلدان التي صادقت عليها وطبقتها، وكل هذا يحتاج إلى وقت طويل، وهو ما سيكون في صالح الجهات الفاعلة والمجرمين السيبرانيين[٥٤].

ومن التوصيات المقترحة في هذا الشأن أن تضم البلدان القومية صفوفها، بمساهمة من الجهات المعنية، لإدخال التعديلات التالية على القوانين الدولية القائمة للنزاع المسلح:-

١- يجب على الدول التي تسعى لتطوير قدراتها الدفاعية في مجال التهديدات السيبرانية أن تجعل توسيع قدراتها العسكرية مرسوما مع الحدود الموضوعة لحماية ضحايا النزاعات المسلحة وضحايا الحرب السيبرانية، حيث تعترف بوجود مستوى جديد من "الحد الأدنى الجوهري من الخدمات" التي تحظى بالحماية من النزاع، وهذا الإجراء سيمنع التدمير والمعاناة بدون داع بين المشا ركين في النزاع، وسيؤدي إلى حماية البلدان الأخرى غير المشا ركة في هذه الحرب من الضرر، ووجود هذا

[٥٣] عادل عبد الصادق، الإرهاب الإلكتروني: القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة، القاهرة، مركز الدراسات السياسية والاستراتيجية، الطبعة الأولي، ٢٠٠٩، ص ١٥٦.

[٥٤] حمدون إ. توريه، الفضاء السيبراني وتهديد الحرب السيبرانية، المرجع السابق، ص ٦٩.

المستوى من الاستقرار السيبراني أمر حيوي، لكي لا تضيع فوائد الإنترنت في خضم قوى التكنولوجيا المدمرة.

٢- كما ينبغي تحديد المقصود بالسلامة الإقليمية المدرجة في ميثاق الأمم المتحدة لتشمل البنى التحتية الحيوية، والإتاحة والمنعة والسرية السيبرانية، وهي مفاهيم تحتاج إلى دقة تحديدها خاصة أن الحرب السيبرانية قد تكون أثارها أشمل وأعم.

٣- ينبغي إحداث تعديل جوهري على اتفاقيات لاهاي الخاصة بتنظيم وسائل وطرق التهديدات، بغرض تحريم استخدام القوات غير النظامية في القتال السيبراني وحظر نقل التهديدات السيبرانية عبر شبكات البلدان المحايدة تحت أي ظرف كان.

٤- ينبغي تعديل اتفاقيات جنيف بغرض تحريم التهديدات على البنية التحتية الحيوية التي يمكن أن تعطل الاتصالات الأساسية الدنيا وتعرض السكان المدنيين للخطر، خاصة أن تدمير الاتصالات قد يمس الأنظمة الصحية وأنظمة معالجة المياه وغيرها، وهي في النهاية ضرورية لبقاء السكان المدنيين أحياء.

٥- ينبغي أن يلتزم كل بلد بألا يكون الطرف الذي يبدأ بشن هجوم سيبراني على غيره من البلدان إلا في الحدود الضيقة والمسموح بها دفاعا عن النفس، تجنبا لانتشار هذه التهديدات إلى مجالات ودول ومنظمات، ويكون من الصعب التحكم في آثارها.

٦- كما يلتزم كل بلد بالتعاون مع غيره ضمن إطار دولي للتعاون لضمان الأمن في الفضاء السيبراني، وتطوير نظام الأمم المتحدة وقوات حفظ السلام ليستوعب مثل هذه التهديدات وهذه الحروب مستقبلا.

*** المراجع**

أولاً- المراجع العربية

البرتوكول الإضافي الثاني الملحق باتفاقيات جنيف والمتعلق بحماية ضحايا المنازعات المسلحة غير الدولية، ٨ حزيران/يونيه ١٩٧٧، تاريخ بدء النفاذ: ٧ كانون الأول/ديسمبر ١٩٧٨، الرابط الإلكتروني . https://www.legal-tools.org/doc/0453fb/pdf/

البعلبكي، منير. والبعلبكي، رمزي منير: المورد الحديث، دار العلم للملايين، بيروت، ٢٠٠٩، ص٣٠٧.

تقرير اللجنة الدولية للصليب الأحمر للمؤتمر الدولي الحادي والثلاثون للصليب الأحمر والهلال الأحمر، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، جنيف، سويسرا، ٢٠١١، الوثيقة: C٣١/٥,١,٢/١١، ص ٤٣-٤٢.

جودي ر. وستبي، دعوة إلى الاستقرار الجيوسيبراني، الاتحاد الدولي للاتصالات، مقال منشور على الرابط الإلكتروني، جانفي ٢٠١١، اطلع عليه بتاريخ ٢٠/٧/٢٠١٩، الرابط الإلكتروني. https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-.1-2011-MSW-A.docx

حماية الأشخاص المدنيين والسكان في وقت الحرب، المقتطف من القواعد الأساسية لاتفاقيات جنيف وبروتكوليها، اللجنة الدولية للصليب الأحمر، ٣١ ديسمبر ١٩٨٨،

www.icrc.org/web/eng/siteeng0
.nsf/html/57JMJV

حمدان، إيمان: التكنولوجيا الجديدة والقانون الدولي الإنساني (الحرب السيبرانية)، دراسات معقمة في القانون الدولي الإنساني، الماجستير في القانون الدولي الإنساني، الجامعة الافتراضية السورية، دمشق (سوريا)، ٢٠٢٠م، ص٩.

حمدون إ. توريه، الاستجابة الدولية للحرب السيبرانية، مقال إلكتروني ص ١٠٢، اطلع عليه بتاريخ
https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-MSW-A.docx

درويش، سعيد: ماهية الحرب الإلكترونية في ضوء قواعد القانون الدولي، مجلة العلوم القانونية والاقتصادية والسياسية، العدد ٢٩، الجزء الثاني، جامعة الجزائر– كلية الحقوق، ٢٠١٨، ص ص١١٧–١٣٧، ص١٢٤، متاح على الرابط :
https://cutt.ly/2kpMulR

دوريجي، كوردولا: "لا تقترب من حدود فضائي الإلكتروني: الحرب الإلكترونية والقانون الدولي الإنساني وحماية المدنيين"، المجلة الدولية للصليب الأحمر، مجلد ٩٤ (٨٨٦) صيف ٢٠١٢، ص ص ٥٣٣–٥٧٨، ص ٥٥١، متاح على الرابط :
https://cutt.ly/Okp7S5Z

صابر، بلقاسم بن: "التهديدات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر"، مجلة حقوق الإنسان والحريات العامة، العدد ٤، جامعة عبد الحميد بن باديس، الدكتور حيدرة محمد، الجزائر، ٢٠١٧، ص ١٨٤–٢١٥، ص ١٨٨، متاح على الرابط :
https://www.asjp.cerist.dz/en/article/69268

الصين: "جيش أزرق" لحماية شبكات " الجيش الأحمر"، موقعBBC NEWS ، استرجعت بتاريخ ٣١/٨/٢٠٢٤، متاح على الرابط :
https://www.bbc.com/arabic/scienceandtech/2011/06/110531_china_blue_army

عادل عبد الصادق، الإرهاب الإلكتروني: القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة، القاهرة، مركز الدراسات السياسية والاستراتيجية، الطبعة الأولي، ٢٠٠٩، ص ١٥٦.

عمر محمود اعمر، الحرب الإلكترونية في القانون الدولي الإنساني، دراسات علوم الشريعة والقانون، المجلد ٤٦ عدد ٠٣، ٢٠١٩، اطلع عليه بتاريخ ٦/٩/٢٠٢٤، الرابط الإلكتروني .
https://journals.ju.edu.jo/DirasatLaw/article/viewFile/101907/10621?target =_ blank

الفتلاوي، أحمد عبيس نعمة: التهديدات السيبرانية (دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر)، الطبعة الأولى، منشورات زين الحقوقية، بيروت(لبنان)، ٢٠١٨م، ص١٦.

كلزي، ياسر: النظرية العامة في القانون الدولي الإنساني، ماجستير القانون الدولي الإنساني، الجامعة الافتراضية السورية، دمشق(سوريا)، ٢٠٢٠، ص ١٠٢.

كوردولا دروغيه المستشارة القانونية في اللجنة الدولية، ما من فراغ قانوني في الفضاء السيبراني، مقال منشور على موقع اللجنة الدولية للصليب الأحمر بتاريخ ١٦/٠٨/٢٠١١، اطلع عليه بتاريخ ١/٩/٢٠٢٤، الرابط الإلكتروني . https://www.icrc.org/ar/doc/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm

اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، ورقة موقف اللجنة الدولية للصليب الأحمر، تشرين الثاني ٢٠١٩، ص ٧.

اللجنة الدولية للصليب الأحمر، تعليق اللجنة الدولية للصليب الأحمر على المادة الثالثة المشتركة، التعليق رقم ٤٣٦، منشورات اللجنة الدولية للصليب الأحمر، ص ٤١، متاح على الرابط:https://cutt.ly/Akp3Hqm

لين، هربرت: "النزاع السيبراني والقانون الدولي الإنساني"، مجلة اللجنة الدولية للصليب الأحمر، مجلد ٩٤ (٨٨٦)، صيف ٢٠١٢، ص ص ٥١٥-٥٣١، ص ٥١٨-٥١٩، متاح على الرابط : https://cutt.ly/RkoansD

ما هي القيود التي يفرضها قانون الحرب على التهديدات السيبرانية، اللجنة الدولية للصليب الأحمر، مقال منشور على موقع اللجنة بتاريخ ٢٨/٠٦/٢٠١٣، اطلع عليه بتاريخ ٣٠/٨/٢٠٢٤، الرابط الإلكتروني . https://www.icrc.org/ar/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm

موقع Cyberforsvaret الدفاع السيبراني النرويجي، استرجعت بتاريخ ٣١/٨/٢٠٢٤، متاح على الرابط: https://www.forsvaret.no/

موقع القيادة السيبرانية للجيش الأمريكي، استرجعت بتاريخ ٣١/٨/٢٠٢٤، متاح على الرابط : https://www.arcyber.army.mil

موقع قاموس المعاني، معنى كلمة سايبر، استرجعت بتاريخ ٤/٩/٢٠٢٤ : https://www.almaany.com/ar/dict/ar-en/cyber/

ميلزر، نيلس: مقدمة شاملة القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر، ٢٠١٦؛ هنكرتس، جون-ماري. ودوزوالد-بك، لويز: القانون الدولي الإنساني العرفي (المجلد الأول/القواعد)، اللجنة الدولية للصليب الأحمر، ٢٠١٦.

الشوابكة، مراد: ما هو نظام سكادا، موقع موضوع (أكبر موقع عربي بالعالم)، استرجعت بتاريخ٣/٩/٢٠٢٤، متاح على الرابطhttps://cutt.ly/5kCk8TQ.

وفاة مريضة جراء هجوم سيبراني على مستشفى ألماني، موقع RTonline، استرجعت بتاريخ ٤/٩/٢٠٢٤، متاح على الرابط : https://cutt.ly/1h5JyOu

ثانياً– المراجع الاجنبية

Cybernetics or Control and Communication in The Animal and The Machine. See: Wiener, Norbert: Cybernetics or Control and Communication in The Animal and The Machine, M.I.T, Press, Second Edition, Cambridge, Massachusetts, 1948, Available At: https://cutt.ly/akhwlob

Gervais, Michael: "Cyber Attacks and The Laws of War", Berkeley Journal of International Law, Volume 30, Issue 2, Article 6,2012, PP 525-579, P566, Available At:https://cutt.ly/mkp1eep

Mccormack, Tim: International Humanitarian Law and The Targeting of Date, Volume 94 ,International Law studies, U.S. Naval War College, United States, 2018, PP223-240, P227,Available At: https://cutt.ly/DksuNk5

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

Pande, Nihar Ranjan: Cyber Attacks and Counter Measures: User Perspective, (Post-Graduate Diploma in Cyber Security), Uttarakhand Open University, Haldwani 2016, P1,Available at: https://cutt.ly/9ki28jB

Schmitt, Michael (gen ed): Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, New York, First Published,2013, Available At :https://cutt.ly/tkofrbK