الجمهوريَّة العربية السُّوريَّة
وزارة التعليم العالي والبحث العلمي
الجامعة الافتراضيّة السُّوريَّة
ماجستير التأهيل والتخصص
في القانون الدولي الإنساني

الهجمات السيبرانية في ضوء القانون الدولي الإنساني

بحث مقدم استكمالاً لمتطلبات نيل درجة ماجستير التأهيل والتخصص في القانون الدولي الإنساني

إعداد

نور أمير الموصلي

إشراف

الدكتورة إيمان يحيى حمدان

المُدرِّسة في ماجستير القانون الدولي الإنساني

الجامعة الافتراضيّة السُّوريَّة

2021

الهجمات السيبرانية في ضوء القانون الدولي الإنساني

Cyber-attacks in light of international humanitarian law

﴿مِنْ أَجْلِ ذَٰلِكَ كَتَبْنَا عَلَىٰ بَنِيٓ إِسْرَٰٓءِيلَ أَنَّهُۥ مَن قَتَلَ نَفْسًۢا بِغَيْرِ نَفْسٍ أَوْ فَسَادٍ فِى ٱلْأَرْضِ فَكَأَنَّمَا قَتَلَ ٱلنَّاسَ جَمِيعًا وَمَنْ أَحْيَاهَا فَكَأَنَّمَآ أَحْيَا ٱلنَّاسَ جَمِيعًا ۚ وَلَقَدْ جَآءَتْهُمْ رُسُلُنَا بِٱلْبَيِّنَٰتِ ثُمَّ إِنَّ كَثِيرًا مِّنْهُم بَعْدَ ذَٰلِكَ فِى ٱلْأَرْضِ لَمُسْرِفُونَ ﴿٣٢﴾

(سورة المائدة: الآية ٣٢)

الإهــداء

إلى من كانت أساس نجاحي في هذه الحياة

إلى كريمة النفس وينبوع العطاء

إلى أغلى إنسانة على قلبي

إلى الملاك العطوف والقلب الكبير

والدتي الحبيبة

حفظها الله وأطال في عمرها

إلى السند ومصدر القوة في حياتي

إلى من زرع في نفسي الطموح والسعي الدائم للتميز

إلى من كان لي خير صديق وحبيب

والدي الغالي

حفظه الله وأطال في عمره

إلى من شاركوني الحياة حلوها ومرها

إلى من استمد منهم قوتي وعزمي

إلى الضحكات التي لا تفارق حياتي

إخوتي

وفقهم وحفظهم الله

إلى رفاق الدرب الأوفياء

إلى من تعلمنا ودرسناً معاً

الأصدقاء، وزملاء الدراسة

شكر وتقدير

الحمد الله والشكر لله عز وجل أولاً وأخيراً الذي أعانني على إتمام هذا العمل المتواضع

ويسعدني أن أتقدم بالشكر والتقدير لحضرة الدكتور المحترم:

الدكتور ياسر حسن كلزي

على سعيه لافتتاح اختصاص الماجستير في القانون الدولي الإنساني ولرعايته وحرصه على تقديم العلم والمعرفة والفائدة لطلابه.

كما أتقدم بالشكر والتقدير والامتنان لحضرة الدكتورة المحترمة:

الدكتورة إيمان يحيى حمدان

على تكرمها وتفضلها بالإشراف على بحثي هذا، وما قدمته لي من توجيه ورعاية علمية مخلصة.

كما أتقدم بالشكر الجزيل للسادة الأفاضل أعضاء لجنة المناقشة لتفضلهم بمناقشة هذه الدراسة، وعلى القيمة العلمية المضافة من قبلهم إلى هذا البحث.

وكذلك أتوجه بالشكر لكافة أعضاء الهيئة التدريسية ورئاسة الجامعة الافتراضية السورية لكل ما قدموه لي ولزملائي خلال سنتين لنصل إلى مستوى إنجاز أبحاثنا بكفاءة وثقة.

ملخص البحث باللغة العربية

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 الحصـــول على المعلومات واعتماد العديد من الخدمات والبنى التحتية الأساسية عليهم.

لكن لكل أمر جانبه الســـلبي 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 الهجمات السيبرانية التي لا تقتصر آثارها على البيانات في أجهزة الكمبيوتر أو أنظمته، بل تتجاوز ذلك لتقوم بالتأثير بشـــكل مباشـــر على العالم الحقيقي كاختراق أنظمة الكمبيوتر للســـيطرة 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 الهجمات. وبما أن القانون الدولي الإنساني يسعى لحماية المدنيين فقد سعى الخبراء القانونيين لبحث مدى إمكانية تطبيق قواعده على الهجمات السيبرانية.

من أجل ذلك نسعى في هذا البحث إلى الإجابة على الإشكالية الأساسية وهي مدى إمكانية انطباق قواعد ومبادئ القانون الدولي الإنساني على الهجمات السيبرانية، من خلال فصلين، الأول يبحث الإطار النظري والقانوني للهجمات الســـيبرانية، بينما يتناول الثاني القانون الدولي الإنســـاني كإطار قانوني ناظم للهجمات السيبرانية، وأخيراً تحديد أهم النتائج والتوصيات التي توصلنا لها.

الكلمات المفتاحية: السيبرانية، الهجمات السيبرانية، الحرب السيبرانية، الفضاء السيبراني، القانون الدولي الإنساني.

Abstract

During the last decade, the international community has witnessed a widespread wave of computer and information network technology that has revolutionized the way we live in our lives, such as flexibility in obtaining information and the dependence of many basic services and infrastructure on them.

However, everything got both negative and positive side, despite the tremendous development of the information revolution, but at the same time it made the international community face new risks associated with this development, as cyber-attacks appeared that are not limited to the data in computers or systems, but rather It goes beyond that to directly affect the real world, such as penetrating computer systems to control air traffic, disrupting the operation of nuclear power plants and many negative effects that may lead to catastrophic accidents and civilians being the main victims of such attacks. As international humanitarian law seeks to protect civilians, legal experts sought to examine the applicability of its rules to cyber-attacks.

For this purpose, we seek in this research to answer the fundamental problem, which is the extent to which the rules and principles of international humanitarian law apply to cyber-attacks, through two chapters, the first examining the theoretical and legal framework for cyber-attacks, while the second deals with international humanitarian law as a legal framework regulating cyber-attacks, and finally Determine the most important findings and recommendations that we have reached.

Key words: cyber, cyber-attacks, cyber warfare, cyberspace, international humanitarian law.

خطة البحث

المقدمة

الفصل الأول: الإطار النظري والقانوني للهجمات السيبرانية

المبحث الأول: ماهية الهجمات السيبرانية

المطلب الأول: مفهوم الهجمات السيبرانية

المطلب الثاني: التأطير النظري للهجمات السيبرانية

المبحث الثاني: الجهود الدولية للتنظيم القانوني للهجمات السيبرانية

المطلب الأول: الجهود الدولية المباشرة للتنظيم القانوني للهجمات السيبرانية

المطلب الثاني: الجهود الدولية غير المباشرة للتنظيم القانوني للهجمات السيبرانية

الفصل الثاني: القانون الدولي الإنساني كإطار قانوني ناظم للهجمات السيبرانية

المبحث الأول: إمكانية انطباق القانون الدولي الإنساني على الهجمات السيبرانية

المطلب الأول: معايير تحديد الأهداف العسكرية المشروعة أثناء الهجمات السيبرانية في القانون الدولي الإنساني

المطلب الثاني: تطبيق المبادئ العامة في القانون الدولي الإنساني أثناء الهجمات السيبرانية

المبحث الثاني: تحديات انطباق القانون الدولي الإنساني على الهجمات السيبرانية

المطلب الأول: الهجمات السيبرانية في سياق النزاع المسلح

المطلب الثاني: الهجمات السيبرانية خارج سياق النزاع المسلح

الخاتمة

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، وتحكُّمهم في الأشياء المادية مثل المحولات الكهربائية والقطارات والمستشفيات والرادارات والمعاملات التجارية وأسواق الأوراق المالية.

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 الهجمات 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 يمسى بالهجمات 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 الهجمات السيبرانية إلى جانب الهجمات 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 الهجمات، 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 الهجمات 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 الهجمات 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 الهجمات.

وأبرز قانون دولي يسعى 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.

أولاً: إشكالية البحث

بخلاف الهجمات العسكرية التقليدية التي تتم في الميدان المادي، تشن الهجمات 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، تثور الإشكالية حول مدى إمكانية انطباق قواعد ومبادئ هذا القانون على الهجمات السيبرانية.

ثانياً: أسئلة البحث

وينطوي تحت السؤال الرئيس السابق عدة أسئلة فرعية هي:

١. ما المقصود بالهجمات السيبرانية؟

٢. ماهي طبيعة الهجمات السيبرانية وما الذي يميزها عن الحرب السيبرانية والجريمة السيبرانية؟

٣. ما هي أنواع الهجمات السيبرانية والآثار الناشئة عنها؟

٤. ما الجهود الدولية للتنظيم القانوني للهجمات السيبرانية؟

٥. ما مدى إمكانية انطباق القانون الدولي الإنساني على هذه الهجمات؟

٦. كيف سوف يتم تطبيق المبادئ العامة للقانون الدولي الإنساني أثناء الهجمات السيبرانية؟

٧. ما هي معايير تحديد الأهداف العسكرية المشروعة أثناء الهجمات السيبرانية في القانون الدولي الإنساني؟

ثالثاً: أهداف البحث

يهدف البحث إلى الإجابة على أسئلة البحث المذكورة آنفاً على وجه الخصوص:

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

٢. بيان الجهود الدولية للتنظيم القانوني للهجمات السيبرانية.

٣. توضيح معايير تحديد الأهداف العسكرية المشروعة أثناء الهجمات السيبرانية في القانون الدولي الإنساني.
٤. بيان إمكانية انطباق قواعد ومبادئ القانون الدولي الإنساني على الهجمات 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.
٥. استعراض حالات التطبيقية لهجمات سيبرانية حصلت في سياق النزاع المسلح وخارجه.

رابعاً: أهمية البحث

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

خامساً: الدراسات السابقة:

تعد الدراسات السابقة في هذا الموضوع قليلة نوعاً ما، نظراً لحداثة المصطلح، والاهتمام المتأخر به، لذلك سعينا البحث عن الدراسات التي تنطوي تحت هذا الموضوع، وقد تم ترتيبها من الأقدم للأحدث.

١) **الدراسة الأولى:** عنوانها ((المسؤولية الدولية الناشئة عن الهجمات السيبرانية))

إعداد الطالبة: زهراء عماد محمد كلنتر

رسالة ماجستير مقدمة إلى كلية الحقوق جامعة الكوفة عام ٢٠١٦.

أ) مضمون الدراسة

تناولت الدراسة الهجمات السيبرانية من حيث ماهيتها، وتطور الهجمات السيبرانية وطبيعتها وسياسة الدول وموقفها ونماذج عنها وفي القسم الثاني من الدراسة تناولت تكييف الهجمات السيبرانية والمسؤولية الدولية الناشئة عنها في ضوء أحكام القانون الدولي من خلال بيان تكييف الهجمات السيبرانية من ناحتين، الأولى في ظل مبدأ مسوغات الحرب (Jus ad Bellum) والثانية في ظل مبدأ سلوكيات الحرب (Jus in Bello)، وأيضاً تناولت الهجمات السيبرانية في ظل التنظيم الدولي

المعاصر، من حيث التنظيم القانوني بشأن المسؤولية الدولية، وبيان الجهود الدولية في تنظيم الهجمات السيبرانية.

ب) أوجه الاتفاق والاختلاف مع الدراسة الحالية

تتفق هذه الدراسة مع الدراسة الحالية في أنها تتناول ماهية الهجمات السيبرانية والجهود الدولية لتنظيمها ومدى انطباق مبادئ القانون الدولي الإنساني عليها، إلا أنها تختلف عن الدراسة الحالية في طريقة تناولها للموضوع حيث ركزت هذه الدراسة على ذكر خصائص الهجمات السيبرانية وأنواعها والآثار الناشئة عنها و بالإضافة لتحديد معايير الأهداف العسكرية المشروعة أثناء الهجمات السيبرانية، بالإضافة لذلك استعراض حالات تطبيقية لهجمات سيبرانية حصلت في سياق النزاع المسلح وخارجه وشرح كل حالة على حدى بالتفصيل ثم تقييم انطباق القانون الدولي الإنساني على هذه الحالات التطبيقية.

٢) الدراسة الثانية: عنوانها ((الهجمات السيبرانية على شبكات الحاسوب في ضوء القانون الدولي الإنساني))

إعداد الطالب: طلال محمد الحاج إبراهيم

رسالة دكتوراه مقدمة إلى كلية الحقوق جامعة دمشق عام ٢٠٢٠.

أ) مضمون الدراسة

تناولت الدراسة الفضاء السيبراني والهجمات السيبرانية من حيث الأهمية الاستراتيجية للفضاء السيبراني ومفهوم الهجمات السيبرانية وتداعيات هذه الهجمات على الأمن الدولي والنزاعات المسلحة، وأيضاً قانون النزاعات المسلحة من حيث الانطباق على الهجمات السيبرانية وذلك من خلال الحديث عن الهجمات السيبرانية والتحول في استخدام القوة في العلاقات الدولية، ومشروعية استخدام الهجمات السيبرانية في حالة النزاع المسلح، وفي القسم الثاني من الدراسة تناولت المشاركة المباشرة في الهجمات السيبرانية والجهود الدولية لمواجهتها من خلال بيان المسؤولية عن المشاركة المباشرة في الهجمات السيبرانية من ناحيتين ، الأولى التطرق للمسؤولية الدولية عن تصرفات المشارك المباشر في الهجمات السيبرانية و الثانية المسؤولية الجنائية عن المشاركة المباشرة وأهم الجهود الدولية المبذولة في تأمين الاستخدام السلمي للفضاء السيبراني.

ب) أوجه الاتفاق والاختلاف مع الدراسة الحالية

تتفق هذه الدراسة مع الدراسة الحالية في أنهما تنضويان تحت القانون نفسه وهو القانون الدولي الإنساني، إلا أنها هذه الدراسة سعت لتقييم مدى انطباق القانون الدولي الإنساني على حالات تطبيقية لهجمات سيبرانية حصلت سواء داخل سياق النزاع المسلح أو خارجه.

سادساً: منهج البحث

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

سابعاً: حدود البحث

١. **الحدود الموضوعية:** يعالج البحث موضوع الهجمات السبرانية في إطار القانون الدولي الإنساني فقط. بالتالي يخرج عن نطاقه مشروعية استخدام الهجمات السبرانية في ضوء أحكام ميثاق الأمم المتحدة الناظمة للجوء إلى القوة المسلحة، كما لا يتناول البحث موقف القانون الدولي لحقوق الإنسان من هذه الهجمات.
٢. **الحدود الزمانية:** الهجمات السيبرانية، هجمات حديثة ومتطورة، لا يمكن ضبطها بدقة، مع ذلك يمكن القول بأن حدود الموضوع ممتدة من حرب كوسوفو ١٩٩٩حتى عام ٢٠٢٠.
٣. **الحدود المكانية:** الهجمات السيبرانية تحصل في الفضاء السيبراني وهي في تزايد مستمر ومن الصعب حصرها بمكان واحد فالضرر قد يتعدى الهدف المقصود في بعض الحالات، لذلك فقد امتدت الحدود المكانية لهذا البحث لتشمل أكثر الدول وقعت فيها هجمات سيبرانية مثبتة إلى حد ما، كالولايات المتحدة الأمريكية، الجمهورية العربية السورية، الجمهورية الإسلامية الإيرانية، يوغسلافيا السابقة، جورجيا، واستونيا.

ثامناً: خطة البحث

قُسم البحث إلى فصلين، تناول الفصل الأول الإطار النظري والقانوني للهجمات السيبرانية، وجاء في مبحثين: الأول يبحث ماهية الهجمات السيبرانية، والثاني يعرض الهجود الدولية للتنظيم القانوني للهجمات السيبرانية.

أما الفصل الثاني يتناول القانون الدولي الإنساني كإطار قانوني ناظم للهجمات السيبرانية، وجاء في مبحثين: الأول يبحث إمكانية انطباق القانون الدولي الإنساني على الهجمات السيبرانية، والثاني يتناول تحديات انطباق القانون الدولي الإنساني على الهجمات السيبرانية.

الفصل الأول
الإطار النظري والقانوني للهجمات السيبرانية

تمهيد وتقسيم

وفقاً للدراســـات إن أي ظاهرة أو حدث لا ينمو ويزدهر إلا في ظل بيئة حاضـــنة وظروف مواتية تحفز على اتجاه داعم لها من التشجيع والمساندة المجتمعية، وهذا ما وجدته الشبكات الرقمية (الإنترنت) فعلاً من قبول واسع النطاق في كل أنحاء المعمورة، فمنذ نهايات القرن العشرين، عندما استخدم الانترنت بشــكل فعلي، بدأ العالم يشــهد تغيرات نوعية ســريعة لم يشــهدها قبل هذا التاريخ، خاصــة في مجال المعلومات والتكنولوجيا والاتصــالات، وقد أدى هذا التطور الكبير في تكنولوجيا المعلومات والاتصــالات خاصة في بداية القرن الحادي والعشرين، إلى خلق مجتمع وساحة افتراضية متكاملة ينشط في ظلها ليس الإنسان فحسب بل الدول ويؤثرون ويتأثرون بها.

نتيجة لذلك تركز الدول والمنظمات والشركات الكبرى بشكل كبير على الفضاء السيبراني، لتحقيق أهدافهم ومصــالحهم، وأصــبحت المواقع الإلكترونية والبرامج عبر الانترنت خاصــة تلك البرامج المتعلقة بالبنى التحتية للدول وسـيلة وأداة وهدف تسـعى إلى امتلاكهم واسـتغلالها هذه الدولة أو تلك لمصـلحتها الخاصة.

ولابد من الإشارة إلى أنه تكمن خصوصية الفضاء السيبراني في عدم وجود دولة بإمكانها فرض سيطرتها وسيادتها الأحادية عليه، مما أدى ذلك إلى استخدامه بشكل يضر الإنسانية، فظهرت الهجمات السيبرانية التي لم تكن معروفة إلا في وقت قريب وأصبحت من الأمور الرئيسية التي يتحتم على الدول مواجهتها في العصر الراهن بسبب ما يمكن أن تسببه هذه الهجمات من دمار هائل يمكن أن يمس الأمن القومي للدولة، حيث أدت تداعيات هذه الهجمات كأداة جديدة تســتخدم في الصــراع بين بعض الدول، وصعود فاعلين من غير الدول على الساحة الدولية، إلى نشوء جهود دولية تسعى لوضع تنظيم قانوني للهجمات السيبرانية.

وعليه أتناول الإطار النظري والقانوني للهجمات السيبرانية، في مبحثين:

المبحث الأول: ماهية الهجمات السيبرانية

المبحث الثاني: الهجود الدولية للتنظيم القانوني للهجمات السيبرانية

المبحث الأول
ماهية الهجمات السيبرانية

شـكلت الثورة الرقمية والمعلوماتية قفزة تكنولوجية، وأصـبح الفضـاء السـيبراني **(Cyberspace)** عنصـراً مؤثراً في النظام الدولي المعاصـر نظراً لما يحمله من أدوات تكنولوجية متطورة، حيث كشـف عن محاور جديدة وأضـاف مسـتويات كثيرة من التعقيد للعمليات العسـكرية، وبات أكثر تأثيراً في الحسـابات الاستراتيجية للدول، والدولة التي لا تملك التكنولوجيا السيبرانية المحصنة أمنياً سيتعرض فضاؤها السيبراني المتضـمن للأصـول والموارد والمعلومات والخدمات والبنية التحتية الحيوية، بما في ذلك الأمنية والعسكرية والمصرفية والتجارية والتعليمية والصحية والاقتصادية إلى الهجمات السيبرانية التي تسبب دمار هائل فيها. وأتناول فيما يلي ماهية هذه الهجمات، في مطلبين نبين في المطلب الأول مفهوم الهجمات السيبرانية، أما في المطلب الثاني التأطير النظري للهجمات السيبرانية.

المطلب الأول: مفهوم الهجمات السيبرانية

أمام الثورة الرقمية الحديثة التي أفرزت وجود فضاء سيبراني يقوم على أساس بنية عالمية لتكنولوجيا المعلومات والاتصـال، شـهد العالم سباقاً للتسـلح غير تقليدي من نوع جديد، يقوم على اسـتحداث وتطوير برامج تقنيه تستخدم في الفضاء السيبراني لأغراض عسكرية، حيث يتم توجيه هجمات بسرعة قصوى ضد أعداء يتواجدون على مسافة بعيدة جداً من دون تعرضـهم للخطر، سميت بمصـطلح الهجمات السيبرانية. وبناء على ذلك سـنتحدث في الفرع الأول عن تعريف الهجمات السـيبرانية، بينما الفرع الثاني سـنتطرق لطبيعة الهجمات السيبرانية.

الفرع الأول: التعريف بالهجمات السيبرانية

معظم التعاريف التي وردت بشـأن الهجمات السـيبرانية تشـترك في معنى متقارب وهو اسـتهداف مواقع إلكترونية أو نظام كمبيوتر أو جهاز كمبيوتر من خلال وسـائل اتصـال 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 المختصـون في القانون الدولي العام يقرون بأن المصـطلح يكتنفه الغموض والالتباس بسـبب عدم الاتفاق على تعريف محدد له، فمنهم

---

[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

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 الهجمات السيبرانية **(cyber attacks)** لأن مصطلح "الحرب" هو مصطلح غير محبذ في وقتنا الراهن على مستوى التنظيم القانوني الدولي، فيكون مصطلح "الهجمات السيبرانية" أكثر دلالة ومعنى، يتماشى مع مقتضيات القانون الدولي المعاصر.[١] وبالإضافة إلى ذلك فإن الهجمات 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 الهجمات السيبرانية من خلال أولاً بيان معناها لغةً واصطلاحاً وثانياً في بيان خصائصها.

أولاً_ الهجمات السيبرانية لغةً واصطلاحاً

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.

١. السيبرانية في اللغة

إن كلمة سيبرانية أو سايبر أو سيبراني تعتبر ترجمة حرفية لكلمة **(Cyber)** والمشتقة من كلمة **(Cybernetics)**[٢]. 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"[٣].

---

[١] 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

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

[3] 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

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".[١]

ب- وجاء في قاموس المعاني بمعنى " تخيلي"[٢].

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. الهجمات السيبرانية اصطلاحاً

إن مصطلح الهجمات 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[٣].

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 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

---

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

[٢] موقع قاموس المعاني، معنى كلمة سايبر، استرجعت بتاريخ٤/١٢/٢٠٢٠:
https://www.almaany.com/ar/dict/ar-en/cyber/

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

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)[١].

أما بالنسبة **للخبراء القانونيين في دليل تالين** فقد عرفوا الهجمات السيبرانية بأنها: عمليات سيبرانية، سواء كانت هجومية أو دفاعية، يهدف من خلالها التسبب بالإصابة أو وفاة لأشخاص أو الإضرار وتدمير الأهداف(الأعيان)[٢].

وعلى ضوء ما سبق يمكن القول أن الهجمات 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.

ثانياً_ خصائص الهجمات السيبرانية

تتسم الهجمات السيبرانية التي توجه من خلال الفضاء السيبراني بخصائص تميّزها عن غيرها من الهجمات العادية ومن أبرزها ما يلي

١. الهجمات السيبرانية هي هجمات تقنية متطورة، عكست قمة التطور الذي وصلت إليه ثورة المعلومات[٣].
٢. التكلفة المتدنية نسبياً للهجمات السيبرانية، فلا تحتاج الدول إلى تخصيص ميزانيات ضخمة لإنتاج أسلحتها السيبرانية على خلاف الأسلحة المستخدمة في النزاعات العنيفة التقليدية ذات الكلفة العالية جداً كحاملات الطائرات والمقاتلات المتطورة[٤].

---

[١] لين، هربرت: "النزاع السيبراني والقانون الدولي الإنساني"، مجلة اللجنة الدولية للصليب الأحمر، مجلد ٩٤(٨٨٦)، صيف٢٠١٢، ص ص ٥١٥-٥٣١، ص ٥١٩-٥١٨، متاح على الرابط:https://cutt.ly/RkoansD

[2] 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

[٣] موقع الموسوعة الجزائرية للدراسات السياسية والاستراتيجية، الحرب السيبرانية وتداعياتها على الأمن العالمي، استرجعت بتاريخ٢١/٤/ ٢٠٢٠م، متاح على الرابط: D3qG5hu/yl.ttuc//:sptth

[٤] المرجع السابق، نفس الموضع.

٣. الهجوم السيبراني قد يحدث في أي وقت وبمدة قصيرة من الزمن، سواء في السلم، أو في الحرب[١].
٤. يتمتع المهاجم بميزة واضحة في الهجمات السيبرانية على المدافع، لأن هذه الهجمات تتميز بالسرعة والمرونة والمراوغة، فمن غير المرجح أن تنجح عقلية التحصـــن لوحدها، لأن التحصـــين في هذا الاتجاه سيجعل الجانب الآخر عرضة لمزيد من محاولات الاختراق، وبالتالي المزيد من الضغط.
٥. لا تعرف الهجمات الســـيبرانية الحدود الجغرافية فهي متنوعة ومتطورة بوســـائلها المرتبطة بأكثر المجالات التقنية تطوراً وتغيراً في الحياة المعاصـــرة للدول، وهي علاوة على ذلك، غير محدودة الأهداف والنتائج، إذ قد تتعدى مخاطرها ميادين القتال التقليدية لتصـــل بدمارها إلى أكثر المواقع السيادية والحساسة تحصيناً وبعداً عن دائرة القتال.
٦. صعوبة تحديد موقع وشخصية القائم بالهجمات السيبرانية ذات التأثير العالي؛ لكونها لا تترك أثر أو دليل على حصـــولها، إذ إن معظم الهجمات الســـيبرانية يتم اكتشـــافها بالصـــدفة، وبعد فترة طويل وبمساعدة المهارات الفنية عالية المستوى لاكتشاف مصدر الهجوم.
٧. كذلك تتميز الهجمات السيبرانية بأن بها تدمير لا تصاحبه دماء وأشلاء بالضرورة، وبسبب انتشار الفضـاء السـيبراني وسـهولة الوصـول إليه يمكن أن يزيد عدد المهاجمين وكذلك توسـع دائرة المواقع المســتهدفة، ولتدور تلك الهجمات المتبادلة على نحو من الكر والفر ليعبر عن حالة صـــراع مطولة مرتبطة بالطبيعة المتنوعة للفضاء السيبراني[٢].

الفرع الثاني: طبيعة الهجمات السيبرانية

خلق تحديد طبيعة الهجمات السـيبرانية مشـاكل عملية وجدلاً بين الخبراء القانونيين، كما أنه بسـبب التطور التقني الحاصـل أدى ذلك إلى ظهور العديد من المصـطلحات والمفاهيم المتشـابهة مع بعضـها البعض في المجالات التقنية والمعلوماتية ولا سـيما في إطار المصـطلحات المشـتقة من السـايبر، لذلك وانطلاقاً من هذا سوف نبين في الفرع الأول الهجمات السيبرانية وسيلة أم أسلوب للقتال أما الفرع الثاني سوف نتحدث عن تمييز الهجمات السيبرانية عن الجرائم السيبرانية والحرب السيبرانية.

---

[١] المرجع السابق، نفس الموضع.

[٢] العبودي، علي عبد الرحيم: "هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين"، المجلة العلمية الأكاديمية العراقية، العدد ٥٧، جامعة بغداد، كلية العلوم السياسية، ٢٠١٩، ص ص ٨٩-١١٨، ص ٩٩-١٠٠-١٠١، متاح على الرابط: https://cutt.ly/XkokTen

أولاً_ الهجمات السيبرانية وسيلة أم أسلوب للقتال

استناداً إلى الإقرار العالمي بأن: "إن حق أطراف أي نزاع مسلح في اختيار أساليب ووسائل القتال ليس حقاً لا تقيده قيود"، إذاً إن التمييز بين "وسائل" و"أساليب" القتال مهم[١].وانطلاقاً من ذلك لابد من بيان الهجمات السيبرانية هي وسيلة أم أسلوب للقتال أم الاثنين معاً.

١. الهجمات السيبرانية وسيلة للقتال

إذا استخدمت الهجمات السيبرانية بذاتها للتسلل إلى أنظمة إلكترونية معدة للحماية أو تنظيم سير عمل منشآت حيوية للسيطرة عليها وتدميرها، فهنا تعد الهجمات السيبرانية وسيلة للقتال أي سلاحاً تهاجم به العدو[٢].

وإن من أهم الإشكاليات التي تواجه المجتمع الدولي في طريقة التعامل مع الهجمات السيبرانية هي ما يتعلق بالجدل حول إمكانية عد الأنشطة السيبرانية كسلاح وإمكانية خضوعها لقيود الاتفاقيات المعنية بالحد من التسلح إذ ذهب بعض الخبراء بعدم صحة وصف الهجمات السيبرانية بأنها "سلاحاً" لأنها تفتقد إلى الطاقة الحركية وبالتالي عدم خضوعها للتنظيمات الدولية المتعلقة باستخدام الأسلحة[٣]. وهذا مخالف للواقع إذ لا يشترط في الأسلحة احتواؤها على الطاقة الحركية وخير مثال على ذلك الأسلحة الكيميائية أو البيولوجية. فحقيقة السلاح هي في كل ما يمكن أن يحدث ضرراً جسدياً أو مادياً، ويستعمل لغرض الدفاع أو الهجوم أو التهديد[٤].

وقد أشارت اللجنة الدولية للصليب الأحمر عند حديثها عن الأسلحة السيبرانية أن تقييم مشروعية الأسلحة الجديدة يصب في مصلحة كافة الدول، حيث أنه يساعدها في ضمان توافق سلوك قواتها المسلحة مع الالتزامات الدولية. وبالإضافة لذلك تُلزم المادة ٣٦ من البروتوكول الإضافي الأول لعام

---

[١] ميلزر، نيلس: مقدمة شاملة القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر،٢٠١٦، ص ١٠١.

[٢] الفتلاوي، أحمد عبيس نعمة: الهجمات السيبرانية (دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر)، مرجع سابق، ص ٢١.

[٣] كلنتر، زهراء عماد محمد: المسؤولية الدولية الناشئة عن الهجمات السيبرانية، جامعة الكوفة-كلية القانون، جمهورية العراق، إشراف الدكتور: أحمد عبيس نعمة الفتلاوي،٢٠١٦م، ص ٣١.

[٤] شهاب، محمود إبراهيم عبد الرحمن: الأسلحة غير التقليدية في الفقه الإسلامي، الجامعة الإسلامية – عمادة الدراسات العليا، كلية الشريعة والقانون، قسم الفقه المقارن، غزة، إشراف الدكتور: زياد إبراهيم مقداد، ٢٠٠٧م، ص ٢، متاح على الرابط:
https://iugspace.iugaza.edu.ps/handle/20.500.12358/22293

١٩٧٧ كل دولة من الدول الأطراف التحقق من امتثال أي أسلحة جديدة تقوم بنشرها أو تدرس مسألة نشرها لقواعد القانون الدولي الإنساني، وهذه نقطة أخرى استحضرها دليل "تالين" على نحو مفيد[١].

٢. الهجمات السيبرانية أسلوب للقتال

إذا أسهمت الهجمات السيبرانية في توجيه العمليات وسهلت عمل القوة العسكرية التقليدية، فتعد أسلوب للقتال، كاستخدام الهجمات السيبرانية لإيقاف عمليات الاتصال في المطارات العسكرية والمدنية. ففي هذه الحالة، لم تستخدم الهجمات السيبرانية لتحقيق الهدف بنفسه بل لتمهيد الطريق أمام القوات العسكرية لتحقيق ميزة أو أفضلية عسكرية على العدو، فلذلك يمكن عدها أسلوب للقتال وإدراجها ضمن التخطيطات والتكتيكات العسكرية[٢].

ونستنتج من ذلك أن الهجمات السيبرانية تشكل وسيلة وأسلوب للقتال في الوقت نفسه، وذلك وفق الأهداف المستخدمة لتحقيقها. وقد طالبت اللجنة الدولية للصليب الأحمر الدول الأطراف في اتفاقيات جنيف أثناء المؤتمر الدولي الثامن والعشرين للصليب الأحمر والهلال الأحمر المنعقد عام ٢٠٠٣ بأن تخضع جميع الأسلحة الجديدة ووسائل وأساليب الحرب الجديدة "لاستعراض دقيق ومتعدد التخصصات" وذلك لضمان ألا يتخطى تطور التكنولوجيا الحماية القانونية المكفولة، ويعد استخدام الهجمات السيبرانية أثناء النزاعات المسلحة مثالاً جيداً على هذا التطور التكنولوجي السريع[٣].

ثانياً_ تمييز الهجمات السيبرانية عن الجرائم السيبرانية والحرب السيبرانية

لبيان الهجمات السيبرانية بشكل أوضح، من المهم التمييز بينها وبين الجرائم السيبرانية والحرب السيبرانية.

١. التمييز بين الهجمات السيبرانية والجرائم السيبرانية

تشترك الجرائم السيبرانية[٤] مع الهجمات السيبرانية في المجال التي تحدث فيه أي الفضاء السيبراني، إلا إنها تختلف عنها من ناحيتين:

---

[١] ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟، مقال منشور على موقع اللجنة الدولية الأحمر، استرجعت بتاريخ٤/١٢/٢٠٢٠م، متاح على الرابط:
https://www.icrc.org/ar/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm

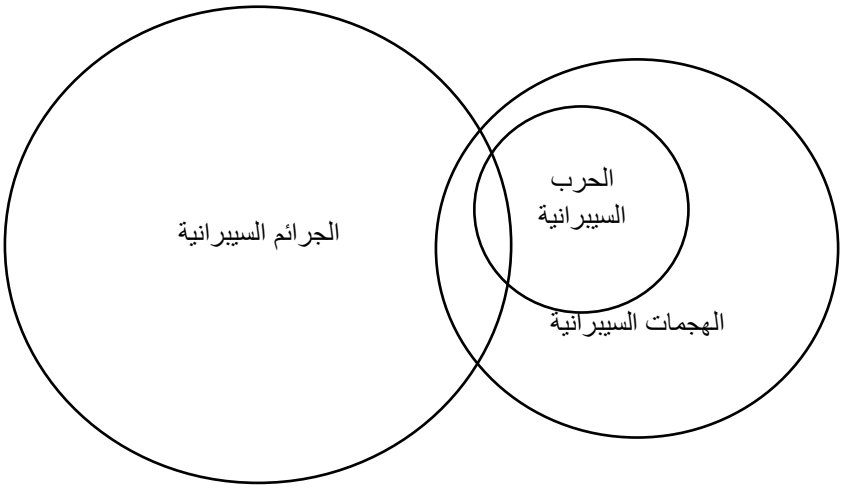
[٢] كلنتر، زهراء عماد محمد: المسؤولية الدولية الناشئة عن الهجمات السيبرانية، مرجع سابق، ص ٣٢.

[٣] ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟، مرجع سابق، نفس الرابط.

[٤] الجريمة السيبرانية لا يوجد لها تعريف معترف به عالمياً، بل هناك جوانب للجريمة السيبرانية معترف بها على نطاق واسع، وجاء في إرشادات الإسكوا للتشريعات السيبرانية (ESCWA) أن الجريمة السيبرانية تنقسم إلى نوعين أساسيين:

الناحية الأولى: بالنسبة للأشخاص غالباً ما يكون مرتكبي الجرائم السيبرانية هم الأفراد وتوجه ضد مؤسسات مالية أو شركات وحتى أفراد داخل أو خارج إقليم الدولة، بخلاف الهجمات التي تتم من قبل دول أو مجموعات حكومية أو غير حكومية ضد دولة أخرى(١).

الناحية الثانية: بالنسبة للأهداف غالباً ما يكون الهدف من الجرائم السيبرانية إثبات مهارة الفاعل تقنياً وقدرته على اختراق أجهزة الكمبيوتر أو بهدف التسلية والترفيه أو تحقيق مكاسب شخصية كسرقة المليكة الفكرية عن طريق شبكات الحاسب الآلي أو التسلل إلى أنظمة المصارف والتلاعب بأرقام الحسابات وتحويل الأموال دون الحاجة إلى تدمير وتعطيل شبكة الكمبيوتر المستهدفة (رغم أنه قد يعطلوها في بعض الحالات) وتكون هذه الأفعال مجرمة بموجب القانون الوطني، بخلاف الهجمات السيبرانية التي يستهدف مرتكبوها الأمن القومي والسياسي للدولة ويقوم هؤلاء بتخريب الشبكات التي تتحكم بالبنى التحتية الأساسية في الدولة وتدميرها بقصد إرباكها، وزعزعة النظام فيها لتحقيق أهداف أمنية أو عسكرية أو سياسية(٢).



النوع الأول: هو الذي يكون فيه الحاسوب أداة تنفذ بواسطتها الجريمة (كجرائم الاختلاس وانتحال الصفة والأفعال الإباحية)، وهي جرائم عادية والحاسوب هو مجرد الوسيلة التي سمحت بارتكابها.

النوع الثاني: هو الذي يكون فيه جهاز الحاسوب وشبكات الحواسيب وبرامجها موضوعاً للجريمة، أي أن الفعل الجرمي ارتكب على هذا الجهاز (مثل اختراق نظام أمان أو إرسال برنامج خبيث أو التعدي على اسم موقع على الانترنت مما يشكل جرماً يطال حقاً من حقوق الملكية الفكرية). وتشمل الجرائم السيبرانية مجموعة واسعة جداً من الأنشطة غير المشروعة مثل التعدي على البيانات المعلوماتية، وإساءة استعمال الأجهزة أو البرامج المعلوماتية، وجرائم التعدي على الملكية الفكرية للأعمال الرقمية، والجرائم التي تمس بالمعلومات الشخصية، وجرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية. انظر: إرشادات الإسكوا للتشريعات السيبرانية، مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية، بيروت، ٢٠١٢، ص١١٧-١١٨، متاح على الرابط: https://cutt.ly/DkoHsuQ

(١) كلنتر، زهراء عماد محمد: المسؤولية الدولية الناشئة عن الهجمات السيبرانية، مرجع سابق، ص ١٧.

(2) Hathaway, Oona A & Others: "The Law of Cyber-Attack", Article, California Law Review, 2012, PP817-886, p835, Available At: https://cutt.ly/Gko9ddj

إذاً إن النشـاط السـيبراني يتكون إما من جريمة سـيبرانية أو هجوم سـيبراني، إلا أنه من الممكن أن تكون الجريمة السيبرانية هي نفسها الهجوم السيبراني كما هو موضح في الشكل، وذلك عندما ترتكب جهة فاعلة غير حكومية عملاً غير قانوني عن طريق شـــبكة كمبيوتر، وتعطل شـــبكة الكمبيوتر، ويكون لها غرض ســـياســـي أو أمن قومي. على ســـبيل المثال، مجموعة افتراضـــية من الأفراد اخترقوا خادم وزارة الخارجية التابع للحكومة الأمريكية وقاموا بإغلاقه احتقاراً للحكومة الأمريكية. تقع هذه الحالة ضـــمن التداخل بين الجرائم السـيبرانية والهجمات السـيبرانية نظراً لأن جهة فاعلة من غير الدول قد ارتكبت عملاً غير قانوني عن طريق شبكة الكمبيوتر، لأغراض سياسية أو تتعلق بالأمن القومي، مما أدى إلى تعطيل شبكة الكمبيوتر[١].

ولا ترقى عواقب هذا العمل إلى مسـتوى الهجوم المسـلح أو تشـكل حرب سـيبرانية كما سـوف يتم شـرحه لاحقاً، وأيضـاً أن الدولة التي ترتكب هذا الفعل نفسـه لن تقع ضـمن هذا التداخل، نظراً لأن جهة فاعلة غير حكومية فقط هي التي يمكنها ارتكاب جريمة سيبرانية[٢].

٢. التمييز بين الهجمات السيبرانية والحرب السيبرانية

كما هو موضـح في الشكل، الحرب السيبرانية هي نوع أو جزء من الهجمات السيبرانية التي تحدث في أثناء نزاع مسـلح حركي أو التي تنتج آثار مادية تشـبه وتعادل آثار الهجمات المسـلحة التقليدية، بينما الهجمات السيبرانية هي كل نشاط سيبراني ضـار بالدول الأخرى سواء كان في وقت السلم أو في سياق نزاع مســـلح حركي وســـواء نتجت عنه آثار مادية جســـيمة في الأرواح أم الممتلكات أو لم يؤدي إلا إلى تشويش أنظمة الكمبيوتر فيها مادام كان ذلك لأغراض أمنية وعسكرية[٣].

ولابد من الإشارة إلى أن الحرب السيبرانية يمكن أن تشكل أيضاً هجوماً سيبرانياً وجرائم سيبرانية في ذات الوقت، كما هو موضـح في الشكل، حيث تشـتمل منطقة التقاطع بين الدوائر الثلاث على نوعين من الهجمات التي تنفذها جهة غير حكومية.

النوع الأول: تشمل الهجمات التي ترتكب عن طريق نظام أو شبكة كمبيوتر وتحدث في سياق نزاع مسلح قائم حركي وتعطل فيها وظيفة شـــبكة الكمبيوتر وذلك لأغراض ســـياســـية أو أمنية وطنية، وتنتهك فيها القانون المحلي.

---

(1) Ibid, p836.

(2) Ibid, p836.

(٣) كلنتر، زهراء عماد محمد: المسؤولية الدولية الناشئة عن الهجمات السيبرانية، مرجع سابق، ص١٩-٢٠.

النوع الثاني: تشمل الهجمات التي ترتكب عن طريق نظام أو شبكة كمبيوتر وتنتج آثاراً مكافئة لتلك التي تنتج عن هجوم مسلح تقليدي، وتعطل فيها وظيفة شبكة الكمبيوتر لأغراض سياسية أو أمنية وطنية، وتنتهك فيها القانون المحلي[١].

نستنتج أنه لكي نعد الهجوم بأنه هجوم سيبراني، يجب أن يتم من قبل جهات فاعلة تابعة للدولة أو من غير الدول، وأن يتضمن سلوكاً نشطاً، وأن يهدف إلى تعطيل وظيفة شبكة الكمبيوتر، وأن يكون له غرض سياسي أو أمن قومي. وبعض الهجمات السيبرانية هي أيضاً جرائم سيبرانية، ولكن ليست كل الجرائم السيبرانية هي هجمات سيبرانية. من ناحية أخرى، تلبي الحرب السيبرانية دائماً شروط الهجوم السيبراني. لكن ليست كل الهجمات السيبرانية هي حرب سيبرانية، فقط الهجمات السيبرانية التي لها آثار معادلة لتأثيرات "الهجوم المسلح" التقليدي، أو التي تحدث في سياق النزاع المسلح، هي التي ترقى إلى مستوى الحرب السيبرانية.

المطلب الثاني: التأطير النظري للهجمات السيبرانية

أصبحت الهجمات السيبرانية في هذا الزمن معقدة وخطيرة ولها أنواع متعددة وهي على نحو متزايد، وعندما وصلت أهدافها لمحاولة تدمير البنية التحتية لدول بأكملها، أصبح تطويرها في مقدمة أهداف الدول، فهي تعتبر قدرة ثانية لا تقل أهمية عن القدرة العسكرية وحتى النووية، إذ إن القدرة السيبرانية يمكنها اختراق المنشآت والقاذفات النووية والقواعد العسكرية وتعطيلها أو التحكم بها. لذلك سنبحث في الفرع الأول عن أنواع الهجمات السيبرانية أما الفرع الثاني فسنتناول الآثار الناشئة عن الهجمات السيبرانية.

الفرع الأول: أنواع الهجمات السيبرانية

أولاً_ هجوم الحرمان من الخدمة (Denial of service attacks) :

ومن اسمه، هدفه حرمان المستخدمين من خدمة معينة والتأثير عليها، ويطلق على أخطر أنواعه اسم **(DDOS _Distributed Denial of service)** حيث أن المهاجم يستغل في هذا الهجوم مجموعة من أجهزة الكمبيوتر لأشخاص لا يعرفهم ولكنه قام باستغلال ثغرات موجودة في أجهزتهم في أكثر من مكان ويقوم بمهاجمة سيرفر معين أو شبكة باستخدام هذه الأجهزة دون علم أصحابها[٢].

---

[1]Hathaway, Oona A. & Others: "The Law of Cyber-Attack", Op.cit, p836-837.

[٢] أنواع الهجمات السيبرانية وطريقة تنفيذ كل نوع منها، موقع كونكت للتقنية، استرجعت بتاريخ٤/١٢/٢٠٢٠م، متاح على الرابط:

https://cutt.ly/uh5Fys8

ثانياً_ الفايروسات (البرامج الخبيثة)

الفايروس **(virus)** هو برنامج مثل أي برنامج تطبيقي آخر، لكنه مصمم من قبل أحد المخربين لإحداث أكبر قدر ممكن من الضرر للنظام بعد ربطه بالبرامج الأخرى ولديه القدرة على تكرار نفسه حتى يبدو وكأنه يتوالد ذاتياً، وهذا يمنحه القدرة على استهداف البرامج الأخرى في الحاسب ومواقع أخرى في الذاكرة بهدف تدميرها، والفايروسات كما حددها التقرير الصادر عن المركز القومي للحاسبات في الولايات المتحدة الأمريكية، هي "برامج مهاجمة تصيب أنظمة الحاسب بأسلوب يماثل إلى حد كبير الفايروسات الحيوية التي تصيب الإنسان"، ويرجع الفضل في وضع أول تصور لفايروس معلوماتي إلى الدكتور " فريد كوهن " في الحلقة الدراسية التي ألقاها في الولايات المتحدة بجامعة كاليفورنيا حول آمن الحاسب الآلي عام ١٩٨٣.و أبرز خصائص الفايروسات بشكل عام تتجلى في قدرتها على الاختفاء، وقدرتها على الانتشار، وقدرتها على الاختراق، وقدرتها على التدمير[١].

ثالثاً_ برامج القنابل المعلوماتية

تعرف القنبلة المعلوماتية باسم **(الشفرة الموقوتة)**، وهي نوع من أنواع البرامج الخبيثة صغيرة الحجم يتم إدخالها بطرق غير قانونية وإخفائها مع البرامج الأخرى، وهذه البرامج من الناحية الشكلية ليست ملفاً كاملاً متكاملاً وإنما هي شفرة توضع ضمن مجموعة من الملفات وذلك بتقسيمها إلى أجزاء متفرقة هنا وهناك حتى لا يمكن التعرف عليها بحيث تتجمع فيما بينها بحسب الأمر المعطى لها في زمان ومكان معينين أو عند حدوث واقعة محددة، لذلك لا يمكن اكتشافها لأشهر أو سنوات، وهذه البرامج تستخدم لتدمير المعلومات والبيانات وتغيير برامج ومعلومات النظام، فضلاً عن غرضها الحمائي في حماية بعض برامج الملكية من خطر الهاكرز. وأكثر بروز لها يتجلى في الحملات الإعلانية كما هو الشأن في المجلات التي يوزع معها بعض الأقراص هدية تحتوي على بعض البرامج، فضلاً عن وجود هذه البرامج الخبيثة "القنابل" في عدد من مواقع الانترنت التي تتضمن مثل هذه البرامج، كما يمكن أن تظهر في بعض البرامج المؤجرة التي لا يفقد مالكها حقوق الملكية الواردة عليها، ففي هذه الأحوال إذ توقف المستأجر عن دفع القيمة الإيجارية المتفق عليها كان ذلك إخلالاً بالعقد المبرم بينهما مما يدفع بالمالك أن يرسل له قنبلة موقوتة أو هي قد تكون أصلاً موجودة في البرنامج المستأجر ومن ثم فإن المالك لا يرسل ما يوقف انفجارها[٢].

---

[١] الحسيني، عمار عباس: جرائم الحاسوب والانترنت (الجرائم المعلوماتية)، الطبعة الأولى، منشورات زين الحقوقية، بيروت(لبنان)،٢٠١٧، ص١٤٠_١٤١.

[٢] المرجع السابق، ص١٤٣_١٤٤.

رابعاً_ برامج الدودة

تعرف برامج الدودة بالبرامج التي تستفيد من الثغرات الموجودة في نظام تشغيل الكمبيوتر للانتقال من كمبيوتر إلى آخر، مما يؤدي إلى احتلال الشبكة بالكامل والتسبب في النهاية بآثار مدمرة، وبفضل الوصلات التي تربط الشبكات بعضها ببعض، يمكنهم الانتقال من شبكة إلى أخرى والتكاثر مثل البكتيريا في عملية النقل، ومن أهداف تلك البرامج شغل أكبر قدر ممكن من سعة الشبكة ومن ثم تقليل أو خفض كفاءتها، وقد تتعدى أهدافها لتبدأ بعد التكاثر والانتشار بالتخريب الفعلي للملفات والبرامج ونظم التشغيل وبروتوكولات الاتصال. وربما تكون أكثر الطرق وضوحاً لنشر هذه الديدان هي مرفقات البريد الالكتروني المصابة والتنزيلات التلقائية عند زيارة بعض مواقع الانترنت والتسلل عبر الثغرات الأمنية في أنظمة التشغيل أو برامج الحماية، ومن ناحية أخرى تتجلى أضرار هذه الديدان في أنها تتيح للمهاجم أن يستخدم الكمبيوتر المصاب لمهاجمة مواقع انترنت أو إرسال بريد إلكتروني أو تنزيل برامج ضارة إليه[١].

ويتضح من ذلك أن الهجمات السيبرانية لا تقتصر على نوع واحد، بل لها أنواع متعددة ومتجددة، وأعتقد في المستقبل سيكون هناك أنواع أخرى أكثر خطورة، لذلك لابد من السعي للحد منها.

الفرع الثاني: الآثار الناشئة عن الهجمات السيبرانية

ليس لآثار الهجمات السيبرانية حدود، فبإمكانها التسبب بانفجارات في مخازن الوقود والمحطات النووية وكافة المراكز الحيوية أو تعطيل وسائل النقل براً وبحراً وجواً أو تغيير مسار الرحلات، إضافة لتعطيل أنظمة الطاقة وقطع الكهرباء عن مدن بأكملها، وكذلك تعطيل أنظمة التحكم والتشويش على الصواريخ والطائرات وتغيير مسارها أو تعطيل أنظمة الدفاع أو حواسيب أمن المعلومات وتصل قدراتها لتعطيل أجهزة الاتصالات بكل أنواعها، ناهيك عن اختراق البنوك وسرقة الحسابات والتلاعب بالتحويلات[٢]وسوف نبين أهم الآثار الناشئة عن الهجمات السيبرانية في عدة مجالات فيما يلي.

أولاً_ الآثار الناشئة عن الهجمات السيبرانية في المجال العسكري

لقد لعبت التكنولوجيا دوراً مهماً في المجال العسكري، حيث تعتمد عليها معظم الأنظمة العسكرية اليوم، وتتمثل الميزة النسبية للتكنولوجيا في قدرتها على ربط الوحدات العسكرية معاً، لتسمح بتبادل المعلومات وتدفقها بسهولة، والسرعة في إعطاء الأوامر العسكرية، والقدرة على تدمير الأهداف عن بعد.

---

[١] المرجع السابق، ص١٤٥-١٤٦.

[٢] علاو، غيث: الهجمات السيبرانية.. أكبر من حرب نووية بوسائل إلكترونية، موقع متخصص في الشؤون الإيرانية، استرجعت بتاريخ٤/١٢/٢٠٢٠م: https://jadehiran.com/archives/16835

وقد تتحول هذه الميزة إلى نقطة ضعف، إن لم تكن الشبكة السيبرانية المستخدمة آمنة بدرجة كافية، فقد تؤدي الهجمات السيبرانية ضد الشبكات الخاصة بالمؤسسات الأمنية والعسكرية إلى السيطرة عليها، مما يؤدي إلى وقوع ضحايا في صفوف المقاتلين والمدنيين، وتهديد السلم والأمن الدوليين، وبالتالي إن الهجمات السيبرانية على المجال العسكري لها نفس النتائج الناجمة عن الاستخدام المادي للقوة العسكرية، والتي تتمثل في انهيار البنى التحتية للدولة، ووقوع وفيات بين العسكريين والمدنيين[١].

ثانياً_ الآثار الناشئة عن الهجمات السيبرانية في المجال الاقتصادي

أصبحت صناعة تكنولوجيا المعلومات والاتصالات مورداً اقتصادياً مهماً للكثير من الدول، حيث أسهمت ثورة تكنولوجيا المعلومات والاتصالات في جعل أصحاب القرار يتخذون قرارات استثمارية رشيدة وبالتالي ساهمت في زيادة معدلات التنمية الاقتصادية، ومن الأمثلة على استخدام التكنولوجيا في المجال الاقتصادي ما يلي: إعلانات المنتجات الجديدة، والأخبار الصحفية عنها، ومعلومات ترويجية حول مبيعات محددة وخاصة، وعرض دراسات السوق، وأبحاث العملاء، وجمع المعلومات الخاصة بخدمة العملاء، والتسويق الإلكتروني. فأي هجوم سيبراني على هذا المجال سوف يؤثر ويخلف العديد من الآثار السلبية وسيكون المدنيون عاطلين عن العمل وغير محميين، وستتعطل العمليات من منطقة إلى أخرى مسببة تدهوراً اقتصادياً على مستوى الدولة، ومثال على ذلك الاحتيال في تحويل الأموال بالوسائل السيبرانية وسرقة الأرصدة وتحويلها إلى أنشطة إجرامية[٢].

ثالثاً_ الآثار الناشئة عن الهجمات السيبرانية في المجال الصحي

أصبح استخدام أجهزة وبرامج الكمبيوتر في الوقت الحالي دوراً مهماً في تحسين جودة وكفاءة الرعاية الصحية وتقليل تكلفتها، ومن أهم ما تم تطويره فكرة السجلات الطبية الإلكترونية التي تشمل المعلومات الخاصة بالمريض والتاريخ الطبي والعلاجات السابقة، والأدوية المستخدمة سابقاً، وحالات الحساسية، والأعراض، ونتائج الأمراض المختلفة والاختبارات التشخيصية، وكذلك مواعيد زيارة الأطباء أو المستشفيات والعلاجات التي تلقاها المريض، وصور الأشعة التشخيصية والموافقات القانونية. ولقد أثرت التكنولوجيا الجديدة بشكل كبير على المجال الصحي، فظهر مفهوم الطب عن بعد الذي يهدف بشكل أساسي إلى تقديم الخدمات الطبية وخفض التكاليف بشكل أساسي في الدول الفقيرة أو المناطق الريفية بما يتماشى مع تلك المقدمة في المدن الكبرى والعواصم، وتقليل نفقات انتقال المريض والتواصل بين المريض

---

[١] خليفة، إيهاب: ما هو موقف ميثاق الأمم المتحدة من استخدام القوة السيبرانية في التفاعلات الدولية؟، موقع المستقبل للأبحاث والدراسات المتقدمة، استرجعت بتاريخ٤/١٢/٢٠٢٠م، متاح على الرابط: https://cutt.ly/rkpu3jQ

[٢] العتيبي، عبد الرحمن بجاد شارع: دور الأمن السيبراني في تعزيز الأمن الإنساني، جامعة نايف العربية للعلوم الأمنية– كلية العلوم الاستراتيجية (قسم الأمن الإنساني)، إشراف الدكتور: د. طارق محمد سليمان،٢٠١٧م، ص٦٢.

والطبيب وتقديم التشخيص ومتابعة حالة المريض إلكترونياً[١]. ويعد الهجوم السيبراني على هذه السجلات الطبية بمثابة خرقاً خطيراً للأمن السيبراني للرعاية الصحية، وبالتالي إحداث اضطراب كبير في المجال الصحي للدولة[٢].

رابعاً_ الآثار الناشئة عن الهجمات السيبرانية في المجال البيئي

لقد تم استخدام أنظمة الاستشعار عن بعد ونظم المعلومات الجغرافية في مجال الحفاظ على البيئة، حيث تسهل دراسة تلوث المياه والهواء وسطح الأرض من خلال صور الأقمار الصناعية بعد معالجتها بجهاز الكمبيوتر، في تحديد مصادر التلوث ومراقبة الامتداد الموضعي للتلوث، خاصة أثناء حدوث تلوث طارئ معين، بالإضافة إلى دراسة تركيز هذا التلوث، وسرعة جريانه وتدفقه، ومقدار تشتته أيضاً. وتستطيع أجهزة قياس الإشعاع متناهي القصر الدقيقة في الكشف عن تسرب النفط والبقع الزيتية. وفيما يتعلق بالكوارث الطبيعية، يمكن لصور الاستشعار عن بعد أن توفر معلومات دقيقة وسريعة عن مثل هذه الكوارث قبل أو أثناء حدوثها أو بعد حدوثها بوقت قصير، كالفيضانات والأعاصير، وحرائق الغابات، والكوارث والاندفاعات البركانية. يظهر جلياً أهمية التكنولوجيا في مجال حماية البيئة من التلوث والحد منه بأسرع وقت، وأي هجوم سيبراني على هذا المجال سوف يتسبب في الكثير من الدمار والأذى للنظام البيئي[٣].

ونستنتج أن آثار الهجمات السيبرانية على كل من المجالات العسكرية والاقتصادية والصحية والبيئية، خطيرة جداً وقد تؤدي إلى كوارث كبيرة خاصة إذا كانت نتائجها مماثلة للاستخدام المادي للقوة العسكرية، والتي تتمثل في انهيار البنى التحتية للدول، ووقوع وفيات بين العسكريين والمدنيين، وإحداث اضطراب كبير في المجال الصحي والأذى والدمار للنظام البيئي، لذا نؤكد مرة أخرى على ضرورة الحد من استخدام الهجمات السيبرانية.

---

[١] ملكية، طيب سليمان. عبد العزيز، فطيمة: "الطب عن بعد La tété-médecine: إبداع في الخدمات الطبية"، المؤتمر الدولي حول الإبداع والتغيير التنظيمي في المنظمات الحديثة: دراسة وتحليل تجارب وطنية ودولية، جامعة سعد دحلب البليدة (كلية العلوم الاقتصادية وعلوم التسيير)، الجزائر، ٢٠١١، ص ٦، متاح على الرابط: https://cutt.ly/1kpz44Y

[٢] العتيبي، عبد الرحمن بجاد شارع: دور الأمن السيبراني في تعزيز الأمن الإنساني، مرجع سابق، ص ٦٤.

[٣] العتيبي، عبد الرحمن بجاد شارع: دور الأمن السيبراني في تعزيز الأمن الإنساني، مرجع سابق، ص٦٥-٦٦.

المبحث الثاني

الجهود الدولية للتنظيم القانوني للهجمات السيبرانية

على الرغم من تزايد الهجمات السيبرانية والخطورة الناشئة عنها، إلا أن المجتمع الدولي يفتقر إلى إطار قانوني دولي شامل ينظمها، ومع ذلك فهو أمر لا يعني صحة القول بعدم وجود جهود دولية لتنظيم الهجمات السيبرانية بشكل مطلق، إذ هناك جهود تقدم بعض السبل التي يمكن توظيفها للسيطرة على هذا التهديد المتنامي. وأبرز هذه الجهود كانت من قبل المنظمات الدولية والإقليمية كالأمم المتحدة وحلف شمال الأطلسي والمجلس الأوروبي، وبالإضافة إلى ذلك هنالك تنظيمات دولية وإن كانت لا تتطرق إلى الهجمات السيبرانية بشكل مباشر، إلا أنها حاولت تنظيم الوسائل التي قد تستخدم في الهجوم السيبراني، ومن ثم يمكن تطبيقها على الهجمات السيبرانية الضارة كالتنظيمات الصادرة عن الاتحاد الدولي للاتصالات منذ عام ١٩٤٧ وقانون الطيران والبحار والفضاء. وانطلاقاً من هنا سوف نقسم هذا المطلب إلى فرعين، نبين بالأول الجهود الدولية المباشرة للتنظيم القانوني للهجمات السيبرانية، أما الثاني عن الجهود الدولية غير المباشر للتنظيم القانوني للهجمات السيبرانية.

المطلب الأول: الجهود الدولية المباشرة للتنظيم القانوني للهجمات السيبرانية

إن الاهتمام المتزايد لمعالجة الهجمات السيبرانية من خلال أطر قانونية مشتركة، جعل أغلب المنظمات الدولية تسعى إلى وضع تنظيم قانوني يحكم الهجمات السيبرانية وسوف نبين أبرز هذه الهجود فيما يلي.

الفرع الأول: الأمم المتحدة

لقد سعت الأمم المتحدة إلى تأمين سلامة استخدام التكنولوجيا، والشبكات المعلوماتية بشكل عام، وتشارك كلاً من الجمعية العامة ومجلس الأمن ومكتب مكافحة الإرهاب التابع للأمم المتحدة في مختلف المفاوضات لإيجاد توافق في الآراء من أجل وضع معايير توفر الحماية لشبكات الانترنت.[١]وسوف نبين ذلك فيما يلي.

---

[١] لبكي، جورج: "المعاهدات الدولية للإنترنت: حقائق وتحدّيات"، مجلة الدفاع الوطني، بيروت، العدد ٨٣، كانون الثاني ٢٠١٣، استرجعت بتاريخ٢٠٢٠/١٢/٢٥، متاح على الرابط:https://cutt.ly/nh5Hell

أولاً_ الجمعية العامة

١. القرارين ٥٥/٦٣ [١]و٥٦/١٢١[٢] اللذين يضعان الإطار القانوني بشأن " مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية".

٢. القرار ٥٧/٢٣٩ المتعلق ب " إنشاء ثقافة أمنية عالمية للفضاء الحاسوبي"[٣].

٣. القرار ٥٨/١٩٩ المتعلق ب "إرساء ثقافة عالمية لأمن الفضاء الحاسوبي وحماية الهياكل الأساسية الحيوية للمعلومات"[٤].

٤. القرار ٧٣/١٨٧ المتعلق ب " مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الجرمية"[٥].

٥. القرار ١٧٣/٧٤المتعلق ب " تعزيز المساعدة التقنية وبناء القدرات لتدعيم التدابير الوطنية والتعاون الدولي في مجال مكافحة الجريمة السيبرانية، بما يسمح تبادل المعلومات"[٦].

ويبدو أن الأمم المتحدة مستعدة للقيام بدور ريادي،[٧]فقد أعربت الدول الأعضاء للأمم المتحدة، في الاستعراض السادس للاستراتيجية العالمية لمكافحة الإرهاب في القرار ٧٢/٢٨٤ الصادر عن الجمعية العامة، عن قلقها إزاء تزايد استخدام الإرهابيين تكنولوجيا المعلومات والاتصالات، وبخاصة

---

(1) GA. Res. 55/63, UN. Doc. No, A/RES/55/63 (Jan, 22, 2001), Available At: https://undocs.org/ar/A/RES/55/63

(2) GA. Res. 56/121, UN. Doc. No, A/RES/56/121 (Jan, 23, 2002), Available At: https://undocs.org/ar/A/RES/56/121

(3) GA. Res. 57/239, UN. Doc. No, A/RES/57/239 (Jan, 31, 2003), Available At: https://undocs.org/ar/A/RES/57/239

(4) GA. Res. 58/199, UN. Doc. No, A/RES/58/199 (Jan, 30, 2004), Available At: https://undocs.org/ar/A/RES/58/199

(5) GA. Res. 73/187, UN. Doc. No, A/RES/73/187 (Jan, 14, 2019), Available At: https://undocs.org/ar/A/RES/73/187

(6) GA. Res. 74/173, UN. Doc. No, A/RES/74/173 (Jan, 7, 2020), Available At: https://undocs.org/ar/A/RES/74/173

(7)Wegener, Henning: "Hardnessing The Perils in Cyberspace: Who Is in Charge?", UNIDIR, 2007, P49, Available At: https://www.peacepalacelibrary.nl/ebooks/files/UNIDIR_pdf-art2646.pdf

شـبكة الإنترنت وغيرها من الوسـائط لارتكاب الأعمال الإرهابية أو التحريض عليها أو التجنيد لها أو تمويلها أو التخطيط لها[١].

ثانياً_ مجلس الأمن

١. القرار ٢٣٤١ (٢٠١٧)[٢]، الذي يهيب فيه الدول الأعضاء إلى "إنشاء أو تعزيز الشراكات الوطنية والإقليمية والدولية مع الجهات صاحبة المصلحة من القطاعين العام والخاص، حسب الاقتضاء، لتبادل المعلومات والخبرات من أجل منع الهجمات الإرهابية على الهياكل الأساسية الحيوية والحماية منها والتخفيف من آثارها والتحقيق فيها ومواجهتها والتعافي من أضرارها، وذلك بوسائل منها التدريب المشترك واستخدام أو إنشاء شبكات ملائمة للاتصال والإنذار في حالات الطوارئ، وأيضاً يسلم بأن جهود الحماية تتوزع على مسارات متعددة منها أمن الفضاء السيبراني".

٢. والقرار ٢٣٧٠(٢٠١٧)[٣]، الذي يحث فيه الدول الأعضاء على "العمل بصورة تعاونية لمنع الإرهابيين من حيازة الأسلحة، من خلال تكنولوجيات المعلومات والاتصالات، مع احترام حقوق الإنسان والحريات الأساسية والامتثال للالتزامات بموجب القانون الدولي".

ثالثاً_ مكتب مكافحة الإرهاب

لقد اتخذ مكتب الأمم المتحدة لمكافحة الإرهاب عدة مبادرات في مجال التكنولوجيات الجديدة منها برنامج أمن الفضاء الإلكتروني والذي يهدف إلى:

١. تعزيز قدرات الدول الأعضاء والمنظمات الخاصة على منع إساءة استعمال الإرهابيين والمتطرفين العنيفين التطورات التكنولوجية، والتصدي لخطر الهجمات السيبرانية التي تشنها الجهات الفاعلة الإرهابية على البنى التحتية الحيوية؛

٢. تطوير استخدام وسائط التواصل الاجتماعي لمكافحة الإرهاب والتطرف العنيف على الإنترنت، في ظل احترام حقوق الإنسان؛

---

(1) GA. Res. 72/284, UN. Doc. No, A/RES/72/284 (July, 2, 2018), Available At: https://undocs.org/ar/A/RES/72/284

(2) SC. Res. 2341, UN. Doc. No, S/RES/2341(2017) (February, 13, 2017), Available At: https://undocs.org/ar/S/RES/2341(2017)

(3) SC. Res. 2370, UN. Doc. No, S/RES/2370(2017) (August, 2, 2017), Available At: https://digitallibrary.un.org/record/1298189?ln=ar

٣. تخفيف آثار الهجمات السيبرانية واستعادة وإصلاح النظم المستهدفة، في حال حدوث تلك الهجمات.

وقد ألقى وكيل الأمين العام لمكتب الأمم المتحدة لمكافحة الإرهاب، فلاديمير فورونكوف كلمة بشأن مكافحة الإرهاب باستخدام التكنولوجيات الجديدة والناشئة، وأقتبس منه قوله: "يجب أن نوحِد صفوفنا الآن، وعلينا أن نفعل ذلك بسرعة، للتخفيف من هذا التهديد وضمان أن تظل التقنيات الجديدة قوة مسخّرة للخير وليس قوة للشر"[١].

الفرع الثاني: حلف شمال الأطلسي (الناتو)

أدت تداعيات الهجمات السيبرانية التي استهدفت البنية التحتية الرقمية لإستونيا عام ٢٠٠٧، وأيضاً الهجمات السيبرانية ضد جورجيا خلال نزاعها المسلح مع روسيا عام ٢٠٠٨، إلى سعي حلف شمال الأطلسي **(الناتو)** للتصدي للهجمات السيبرانية، فقد عمد إلى إنشاء مركز الدفاع الإلكتروني التعاوني للتميز. وفي الفترة ما بين سنتي ٢٠٠٩ و٢٠١٢، وبطلب من مركز الدفاع الإلكتروني التعاوني للتميز، قامت مجموعة من الخبراء والباحثين القانونيين بتقييم إمكانية تطبيق المبادئ القانونية على الهجمات السيبرانية[٢]، وتم تتويج هذه الجهود بنشر دليل يعرف باسم "دليل تالين" **(Manuel de Tallinn)** وهو وثيقة قانونية غير ملزمة، تنظم قواعد الاشتباك عبر الانترنت. وقد تم صدور إصدارين له:

- **الإصدار الأول عام ٢٠١٣** ويتكون من ٩٥ قاعدة قانونية ويركز على أشد الهجمات السيبرانية خطورة أي تلك الهجمات التي تنتهك حظر استخدام القوة في العلاقات الدولية، وتخول الدول ممارسة حق الدفاع عن النفس، و/أو الهجمات التي تحدث أثناء النزاع المسلح ويطبق عليها قواعد القانون الدولي الإنساني.

- **الإصدار الثاني عام ٢٠١٧** المعروف باسم **(Tallinn 2.0)**: ويتكون من ١٥٤ قاعدة قانونية، ويركز على الوضع القانوني لمختلف أنواع القرصنة والهجمات السيبرانية الأخرى التي تحدث يومياً خلال وقت السلم، والتي تقل عن عتبة استخدام القوة أو النزاع المسلح، ويتناول القضايا التي يصبح فيها الهجوم الرقمي انتهاكاً للقانون الدولي في الفضاء السيبراني[٣].

---

[١] أمن الفضاء الإلكتروني، موقع الأمم المتحدة، مكتب مكافحة الإرهاب، استرجعت بتاريخ ٢٠٢٠/١٢/٤م، متاح على الرابط: https://cutt.ly/AkpFX7U

[٢] السعبري، بهاء عدنان: عماد عبد خضير الزرفي، "انتقال التهديدات من الواقع إلى العالم الافتراضي"، مجلة جامعة بابل للعلوم الإنسانية، المجلد ٢٧، العدد٤، بغداد، ٢٠١٩، ص ص ٤٧٢-٤٨٧، ص٤٨٣، متاح على الرابط: https://cutt.ly/TkpGqEt

[٣] خليل، بشار: "ما هي الحرب السيبرانية؟ مستقبل مخيف للصراع الرقمي"، مجلة المعلوماتية، العدد ١٥٤، شهر آب، الجمعية السورية للمعلوماتية، ٢٠٢٠، متاح على الرابط:

ويقر الدليل بأن الهجمات السيبرانية وحدها قد تشكل نزاعات مسلحة تبعاً للظروف، لاسيما الآثار المدمرة لتلك الهجمات، وعلى الرغم من عدم إلزامية الدليل، فإنه وثيقة أخلاقية للدول الأعضاء في الحلف على الأقل، وينظم استخدامهم للهجمات السيبرانية خلال فترات النزاع المسلح [١].

ويوضح دليل تالين، القوانين الدولية التي يمكن تطبيقها على الحرب السيبرانية وهو يشتمل على كل من مبدأ حق اللجوء إلى الحرب **(Jus ad bellum)**، أي: القواعد الدولية التي تحكم وتنظم استخدام القوة من قبل الدول، ومبدأ سلوكيات الحرب **(Jus in bello)** أو قانون النزاعات المسلحة أو القانون الدولي الإنساني أي القواعد التي تنظم سلوك الأطراف المتنازعة في أثناء النزاع. كما إن دليل تالين لا يركز إلا على الهجمات السيبرانية في مواجهة هجمات سيبرانية أخرى، على سبيل المثال ينظم الهجوم السيبراني الذي يستهدف أنظمة القيادة أو السيطرة التابعة للعدو، ولا يشمل الغارة الجوية ضد مركز السيطرة السيبراني، كما يعالج هذا الدليل كلاً من النزاعات المسلحة الدولية وغير الدولية، ويجمع الفقهاء في ضوء دليل تالين، بأن النزاع المسلح الدولي يحصل متى ما قامت دولة ذات سيطرة كاملة **(Overall Control)** على مجموعة من الأفراد بتوجيه تلك المجموعة لتنفيذ هجمات سيبرانية ضد دولة أخرى. أما إذا كانت لا تملك إلا سيطرة فعالة **(Effective Control)** على تلك المجموعة فعندئذ تلك الهجمات لا تبلغ مستوى النزاع المسلح الدولي[٢].

الفرع الثالث: مجلس أوروبا

يعد مجلس أوروبا[٣]أول من اتخذ خطوات جدية ومباشرة لتنظيم جزء من الأمن السيبراني لأي منظمة دولية أو إقليمية أخرى، فقد قام بإنشاء اتفاقية بودابست المتعلقة بالجريمة السيبرانية وتعد هذه الاتفاقية أولى المعاهدات الدولية التي سعت إلى معالجة الجرائم السيبرانية من خلال تنسيق القوانين الوطنية، وزيادة التعاون بين الدول في محاربة الجرائم السيبرانية. وتمت في العاصمة المجرية بودابست في٢٠٠١/١١/٢٣، ويعد التوقيع على تلك المعاهدة الدولية الخطوة الأولى في مجال تكوين التضامن الدولي ضد تلك الجرائم التي تتم عبر شبكة الانترنت والاستخدام السيء لها[٤].

---

http://www.scs.org.sy/?q=scs/infomag/showarticlenode&id=853

[١] خليفة، إيهاب: القوة الإلكترونية كيف يمكن أن تدر الدول شؤونها غي عصر الانترنت" الولايات المتحدة الأمريكية نموذجاً"، الطبعة الأولى، العربي، القاهرة، ٢٠١٧، ص ١٦٦، متاح بشكل جزئي على الرابط:https://cutt.ly/2khoqnN

[٢] كلنتر، زهراء عماد محمد: المسؤولية الدولية الناشئة عن الهجمات السيبرانية، مرجع سابق، ص ١٠٥.

[٣] مجلس أوروبا هو منظمة دولية معنية بالدفاع عن حقوق الإنسان في القارة الأوروبية، موقعه الرسمي:
https://www.coe.int/en/web/portal/home

[٤] الزهراني، شيخة حسين: "التعاون الدولي في مواجهة الهجوم السيبراني"، مجلة جامعة الشارقة للعلوم القانونية، المجلد ١٧ العدد١، جامعة الشارقة–كلية القانون، الإمارات العربية المتحدة، حزيران ٢٠٢٠، ص ص ٧٤٠–٧٧٢، ص ٧٥٣–٧٥٤، متاح على الرابط:https://cutt.ly/JkpJyjF

أما بالنسبة للهجمات السيبرانية فيمكن القول إنها تتضمن الجرائم الواردة في اتفاقية بودابست التي تتعلق وتمس خصوصية وسلامة وتوافر بيانات ونظم الكمبيوتر لاسيما تلك المتعلقة بالنفاذ غير المشروع الكامل أو الجزئي إلى نظام كمبيوتر والتدخل في البيانات (وذلك عن طريق إتلافها، حذفها، إفسادها، تعديلها أو تدميرها)، والتدخل في النظام (وذلك عن طريق الإعاقة الخطيرة لاشتغال نظام الكومبيوتر عن طريق إدخال بيانات حاسوبية، إرسالها، إتلافها، حذفها، إفسادها، تغييرها أو تدميرها)[١]. وعلى سبيل المثال، تتطلب المادة ٢ من الاتفاقية أن تتبنى الدول " تدابير تشريعية وغيرها من التدابير لتجريم الأفعال الجنائية بموجب قانونهم المحلي، عند ارتكابها عمداً وبغير حق: النفاذ الكامل أو الجزئي إلى نظام كومبيوتر". ونستنتج أن الاتفاقية قد وضعت الإطار القانوني الدولي الأكثر تطوراً الذي ينظم الهجمات السيبرانية إلا أنها لا تتناول سوى جزء من التحدي العام. ومع ذلك، فإنها توفر نقطة انطلاق لتصميم إطار دولي شامل لتنظيم الهجمات السيبرانية غير القانونية[٢].

الفرع الرابع: مبادرات منظمة شنغهاي للتعاون (SCO)

اتخذت منظمة شنغهاي للتعاون،[٣]خطوات أولية مهمة نحو التعاون في مجال الأمن السيبراني ففي:

- عام ٢٠٠٦ وقع رؤساء الدول الأعضاء إعلاناً حول أمن المعلومات الدولية.

- عام ٢٠٠٩ تم صدور "إعلان يكاترينبورغ" وذلك في قمة منظمة شنغهاي للتعاون التي عقدت في يكاترينبورغ في روسيا وقد أظهرت المنظمة من خلاله التعاون والالتزام بهدف منع الحروب والهجمات السيبرانية،[٤] والحاجة الملحة للرد على التهديدات السيبرانية واعتبر أمن المعلومات على نفس أهمية السيادة الوطنية، والأمن الوطني، والاستقرار الاجتماعي والاقتصادي. حيث جاء في الفقرة السابعة: "تؤكد الدول الأعضاء في منظمة شنغهاي للتعاون على أهمية ضمان أمن المعلومات الدولي كأحد العناصر الرئيسية للنظام العام للأمن الدولي"[٥].

---

[١] مجلس أوروبا، الاتفاقية المتعلقة بالجريمة الالكترونية (بودابست)، مجموعة المعاهدات الأوروبية رقم ١٨٥، ٢٠٠١، المواد ٢،٤،٥، متاح على الرابط: https://cutt.ly/YkpJXmC

[2] Hathaway Oona A. & Others: "The Law of Cyber-Attack", op.cit, P864-863.

[٣] منظمة شنغهاي للتعاون: هي منظمة دولية حكومية دائمة، موقعها الرسمي: http://sectsco.org/

[4] Maonga, Sharon Kerubo: "A Case of Incapacity: The Interrogation of International Humanitarian Law as A Satisfactory Regulator of Cyber Warfare", Strathmore University, Strathmore Law School ,2017, P 40, Available at: https://cutt.ly/QjquA9H

[5] Shanghai Cooperation Organization, Yekaterinburg Declaration of The Heads of The Member States of The Shanghai Cooperation Organization, Consulate General of Uzbekistan In New York City (July 9, 2009), Available at: http://eng.sectsco.org/load/198293/

- عام ٢٠١١ تقدمت دول منظمة شـــنغهاي للتعاون بمشـــروع قرار للجمعية العامة للأمم المتحدة بشأن أمن المعلومات[١].

خلاصـــة القول، إن الجهود الدولية وإن كانت لا ترقى إلى مســتوى تنظيمي دولي شــامل، إلا أنها تظهر مدى الاهتمام الدولي المتزايد لوضـع أطر تنظيمية للتصـدي للهجمات السـيبرانية، وبالإضـافة لذلك تعد الخطوة الأولى نحو اتفاقية متعددة الأطراف تنظم اســتخدام هذه الهجمات وتقلل من آثارها الجســيمة على البشر.

المطلب الثاني: الجهود الدولية غير المباشرة للتنظيم القانوني للهجمات السيبرانية

فضـلاً عن الجهود الدولية السالفة الذكر، والتي تهدف إلى تنظيم الهجمات السيبرانية، هناك صكوك قانونية أخرى قد تنطبق بشـكل غير مباشـر على الهجمات السـيبرانية. وقد تم تشـكيل هذه النظم القانونية إلى حد كبير قبل ظهور الهجمات السيبرانية، وبالتالي فهي لا تنظم أو تحظر الهجمات السيبرانية صراحة. وبدلاً من ذلك، فإن هذه "الأطر المستندة إلى الوسائل" تنطبق على الهجمات السيبرانية، طالما أن الهجوم يستخدم الوسائل المعينة التي تنظمها الاتفاقية، وسوف نتطرق إلى أهم هذه النظم فيما يلي.

الفرع الأول: قانون الاتصالات

تم تنظيم قانون الاتصـــالات الدولي الحديث من قبل الاتحاد الدولي للاتصـــالات[٢]، ويعمل الاتحاد الدولي للاتصـالات على تحسـين ولوج المجتمعات في كل مكان إلى تكنولوجيا المعلومات والاتصـال بُغية تمكين الجميع من حق التواصـــل[٣]. ويمكن أن تطبق قواعده القانونية على الهجمات الســـيبرانية، حيث تسمح اتفاقية الاتحاد الدولي للاتصـالات للدول الأعضـاء بقطع أي اتصـالات سلكية أو لاسلكية التي قد تظهر بأنها قد تشكل خطراً على أمن أي دولة طرف في الاتفاقية،[٤] وعلاوة على ذلك، يحق للدول تعليق جميع خدمات الاتصـالات الدولية لمدة غير محدودة لأسباب تتعلق بالأمن الوطني، شريطة أن تقوم على الفور بإخطار الأمين العام للأمن المتحدة[٥]، كما لا يجوز لمحطات البث من دولة ما أن تتدخل بعمليات

---

(1) Kutnayeva, Nuria: "Cybersecurity in Central Asia", Unipath-Magazine, United States Central Command (CENTCOM), August 20 ,2015, Available At: https://cutt.ly/ijquJ7A

(٢) الاتحاد الدولي للاتصـــالات (ITU):هو وكالة متخصـــصـــة في مجال تكنولوجيات الاتصـــالات والمعلومات تابع للأمم المتحدة، الموقع الرسمي : https://www.itu.int/ar/Pages/default.aspx

(٣) الاتحاد الدولي للاتصالات، موقع الجزيرة، استرجعت بتاريخ٤/١٢/٢٠٢٠م، متاح على الرابط: https://cutt.ly/Wh5Hmoi

(4) Constitution of The International Telecommunication Union, Article 34.

(5) Ibid, Article 35.

بث دول أخرى[١]، وينبغي بالإضافة إلى ذلك، وضع جميع المحطات اللاسلكية وتشغيله بطريقة لا تتسبب بتداخلات ضارة للغير[٢].

وعلى الرغم من القيود المذكورة أعلاه، إلا أن اتفاقية الاتحاد الدولي للاتصالات لا تحظر على وجه التحديد استخدام الاتصالات للأغراض العسكرية، حيث تحتفظ الدول الأعضاء في الاتفاقية بحرية مطلقة فيما يتعلق باستخدام منشأتها الاتصالاتية العسكرية[٣]، ما دامت تتخذ جميع الخطوات اللازمة لمنع أي تدخل ضار[٤]، وقد تشمل عبارة "منع أي تدخل ضار" الهجمات السيبرانية.

الفرع الثاني: قانون الطيران

يحتوي قانون الطيران المدني على ثلاثة صكوك رئيسية يمكن أن تنطبق على الهجمات السيبرانية

أولاً_ اتفاقية شيكاغو لعام ١٩٤٤ للطيران المدني الدولي

حيث تتعهد الدول الأعضاء في الاتفاقية عند إصدار اللوائح الخاصة بطائراتها الحكومية بمراعاة سلامة ملاحة الطائرات المدنية[٥]، بالتالي الهجوم السيبراني الذي يستهدف الرحلات الجوية المدنية، إذا وجه من دولة ما ضد طائرات مدنية تابعة لدولة أخرى، يمكن أن يتعارض مع ضمانات هذه الاتفاقية بشأن سلامة ملاحة الطائرات المدنية. ومع ذلك، فإن الاتفاقية تسمح لدولة عضو بالانتقاص من التزامات الاتفاقية أثناء الحرب أو حالات الطوارئ الخاصة بالدولة، طالما أن الدولة تقوم بإخطار الحقيقة إلى المجلس [٦].

ثانياً_ اتفاقية مونتريال لعام ١٩٧١ لقمع الأعمال غير المشروعة ضد الطيران المدني

حددت الاتفاقية مجموعة من الأفعال غير المشروعة الموجهة ضد سلامة الطائرة والتي ترتكب عن قصد، فتجعلها غير صالحة للطيران أو من شأنها أن تعرض سلامتها للخطر في حالة الطيران[٧]. فالهجوم السيبراني الذي من شأنه أن يعرض سلامة الطائرة للخطر في حالة الطيران، على سبيل المثال: من خلال التدخل في نظام تشغيل الطائرة، أو تعريض سلامة الطائرة للخطر أثناء الطيران، على سبيل

---

(1) Ibid, Article 45.

(2) Ibid, Article 6.

(3) Ibid, Article 48(1).

(4) Ibid, Article 48(2).

(5) The 1944 Chicago Convention for International Civil Aviation, Article 3.

(6) Ibid, Article 89.

(7) The 1971 Montreal Convention for The Suppression of Unlawful Acts Against Civil Aviation, Article 1.

المثال، التدخل في اتصـــالات مراقبة الحركة الجوية أو جوانب أخرى من الملاحة الجوية. فإنه يدخل في نطاق هذه الاتفاقية، بينما إذا كان الهجوم السيبراني لا يجعل الطائرة غير قادرة على الطيران أو لا يعرض سلامتها للخطر أثناء الطيران فإن الاتفاقية لا تشمل أو تقييد مثل هذا الهجوم[١].

ثالثاً_ بروتوكول مونتريال لعام ١٩٨٨ لقمع أعمال العنف غير المشـــروعة في المطارات التي تخدم الطيران المدني الدولي

وســـع البروتوكول الإطار القانوني لقمع أعمال العنف غير المشـــروعة في المطارات التي تخدم الطيران المدني الدولي ليشـــمل أعمال العنف التي تعرض للخطر أو من المحتمل أن تعرض ســـلامة الأشـخاص في المطارات للخطر أو التي تعرض التشـغيل الآمن لمثل هذه المطارات للخطر[٢]. وبالتالي يحظر هذا البروتوكول أي هجمات ســـيبرانية يمكن أن تقوض الســـلامة في المطار الدولي، مثل العبث بقوائم حظر الطيران أو بيانات الركاب أو نظام شبكة الكمبيوتر في المطار[٣].

الفرع الثالث: قانون الفضاء الخارجي

يحتوي قانون الفضـــاء على قواعد قانونية قابلة للتطبيق على الهجمات الســـيبرانية، وينبع هذا الانطباق أساساً من حقيقة أن الشبكات العالمية، والجوانب الرئيسية لتكنولوجيا المعلومات الحديثة، تعتمد على منصـات فضـائية متعددة تدور حول الأرض من أجل دعم المحطات الأرضـية، وفضـلاً عن ذلك، تعتبر هذه المنصات الفضائية في غاية الأهمية للهجمات السيبرانية وذلك بسبب اعتبار هذه المنصات من العناصر الأكثر ضعفاً في نظام المعلومات لأنه يستحيل صد أي هجوم قد يقع عليها.

وبالإضافة إلى ذلك لأنها تمثل القوة الأكثر حيوية ومقدرة لأي دولة تريد القيام بالهجمات السيبرانية بشكل ناجح، وبالتالي ستكون هذه المنصـات الفضـائية مشتركة بالضـرورة في صـلب أي حرب سـيبرانية ســواء لعملية دفاعية أو هجومية. وبالتالي يمكن أن تندرج الهجمات الســيبرانية في إطار القواعد القانونية التي تنظم الأنشـطة في الفضـاء والتي صـيغت في معاهدة الفضـاء الخارجي منذ عام ١٩٦٧ والمعروفة رسميا باسم "معاهدة المبادئ المنظمة لأنشطة الدول في ميدان استكشاف واستخدام الفضاء الخارجي، بما في ذلك القمر والأجرام الســماوية الأخرى"، إذ تعد المبادئ المعتمدة في هذه المعاهدة ملزمة لكل المجتمع

---

[١] كلنتر، زهراء عماد محمد: المسؤولية الدولية الناشئة عن الهجمات السيبرانية، مرجع سابق، ص ١١٠.

[2] The 1988 Montreal Protocol for The Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Article 2.

[٣] كلنتر، زهراء عماد محمد المسؤولية الدولية الناشئة عن الهجمات السيبرانية، مرجع سابق، ص١١٠.

الدولي[١]. وكذلك تؤكد أنظمة الأقمار الصناعية كاتفاقية الاتصالات الفضائية لعام ١٩٧١ على "الغرض السلمي" في استخدام الأقمار الصناعية، ولكن على الرغم من أن هذه التنظيمات، لها دور جزئي في تنظيم الهجمات السيبرانية إلا أنها غير كافية[٢].

الفرع الرابع: قانون البحار

تحتوي اتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢ على عدة قواعد قانونية يمكن أن تنطبق بشكل ثانوي على أنشطة الهجمات السيبرانية، فقد نصت الاتفاقية على حق المرور البريء للسفن طالما أنشطتها لا تضر بالسلام وحسن النظام وأمن الدولة الساحلية، وقد عددت الأنشطة المحظورة مثل أي نشاط يهدف إلى جمع المعلومات للمساس بأمن أو دفاع الدولة الساحلية، أو نشر المعلومات والإشاعات بهدف التأثير على أمن أو دفاع الدولة الساحلية، أو أي نشاط يهدف إلى التدخل في أنظمة الاتصالات أو المرافق أو المنشآت الأخرى التابعة للدولة الساحلية[٣]. وبالتالي قد تؤدي هذه الأنشطة المحظورة إلى منع الهجمات السيبرانية التي تستخدم أنظمة الاتصالات والكمبيوتر الموجودة على متن السفن في البحار[٤].

إن القوانين الدولية هذه سواء التي تنظم الاتصالات أو الطيران أو الفضاء أو البحار وإن كانت تنطبق على الهجمات السيبرانية بشكل جزئي في نطاق اختصاص كل منها، إلا أنها لا تقدم آلية كاملة ومتماسكة للتصدي للهجمات السيبرانية، علاوة على ذلك، حتى لو تم أخذها ككل فإنها لا تقدم سوى مجموعة مختلطة من الأنظمة التي تترك العديد من الهجمات السيبرانية الضارة دون معالجة، فالطبيعة الفريدة للهجمات السيبرانية وتغيير كل عناصر النزاع في الفضاء السيبراني من ميدان ومقاتلين وأدوات وأساليب وأهداف تتطلب تنظيماً شاملاً واتفاقاً دولياً ينظم هذه الهجمات السيبرانية.

---

[١] نعوس، مصطفى: "حقوق والتزامات الدول في الحرب المعلوماتية"، مجلة دراسات علوم الشريعة والقانون، المجلد ٤٠، ملحق ١، الجامعة الأردنية، ٢٠١٣، ص ص ٧٨٤-٨٠٠، ص ٧٨٨-٧٨٩، متاح على الرابط: https://cutt.ly/PkpCkzb

[٢] كلنتر، زهراء عماد محمد: المسؤولية الدولية الناشئة عن الهجمات السيبرانية، مرجع سابق، ص ١١١.

[٣] اتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢، المادة ١٩.

[٤] كلنتر، زهراء عماد محمد: المسؤولية الدولية الناشئة عن الهجمات السيبرانية، مرجع سابق، ص ١١٢.

الفصل الثاني
القانون الدولي الإنساني كإطار قانوني ناظم للهجمات السيبرانية

تمهيد وتقسيم

بسبب اللجوء المتزايد للدول لاستخدام الهجمات السيبرانية في سياق النزاعات المسلحة أو خارج سياقها، جعل هذا الأمر قواعد ومبادئ القانون الدولي الإنساني أمام اختبار حقيقي ومعقد يدور حول مدى إمكانية تطبيق تلك القواعد الدولية التي قننت قبل عقود من الزمن على الهجمات السيبرانية. إلا أنه عند التعمق بقواعد القانون الدولي الإنساني نجد وبشكل واضح إلى أنه تم تبني التطورات الحديثة التي قد تحدث في وسائل وأساليب القتال في المستقبل، في المادة ٣٦ من البروتوكول الإضافي الأول لعام ١٩٧٧ حيث أقرت تلك المادة حقيقة إن أي نشاط عسكري معين يرتبط بوسائل وأساليب الحرب لم يتم تنظيمه بشكل دقيق لا يعني ذلك أنه يمكن استخدامه بدون أي قواعد. وبناء على ذلك فإن الأشكال الحديثة للهجمات السيبرانية التي لم يتم تضمينها في استخدامات الأسلحة التقليدية في الاتفاقيات الدولية، ترتبط بالقانون الدولي الإنساني وتخضع له كأي سلاح جديد عندما يتم استخدامه في النزاع المسلح. بالإضافة إلى ذلك إحدى القواعد الأساسية للقانون الدولي الإنساني تقر بأن:

"إن حق أطراف أي نزاع مسلح في اختيار أساليب ووسائل القتال ليس حقاً لا تقيده قيود "[١]

وأيضاً يمكن الرجوع إلى شرط مارتنز[٢] كأساس لتفسير معاهدات القانون الدولي الإنساني كلما وجدت الشكوك حول معنى بعض الأحكام الواردة فيه. واستناداً إلى هذه القاعدة، فإن كل ما يقع أثناء

---

[١] البروتوكول الإضافي الأول عام ١٩٧٧، المادة ٣٥، فقرة١.

[٢] شرط مارتنز، تمت تسميته بهذا الاسم نسبة إلى البروفسور فيودور فيودوروفيتش مارتنز، المندوب الروسي في عام ١٨٩٩ لدى مؤتمر لاهاي للسلام، وقد ذكر مارتنز ذلك الشرط بعد ما فشل المندوبون في مؤتمر السلام في الاتفاق على مسألة مركز المدنيين الذين يشهرون السلاح ضد قوات الاحتلال، حيث كانت الدول العسكرية الكبرى ترى أنه يجب أن يعامل هؤلاء المدنيون بوصفهم جنوداً غير نظاميين يخضعون لعقوبة الإعدام، في حين أن الدول الصغيرة رأت أنه يجب معاملتهم بوصفهم محاربين نظاميين، ونتيجة لذلك الخلاف قام مارتنز بطرح رأيه الذي أصبح يعرف بشرط مارتنز والذي جاء فيه :

"يظل المدنيون والمقاتلون تحت حماية وسلطان مبادئ القانون الدولي كما استقر بها العرف ومبادئ الإنسانية وما يمليه الضمير العام".

وقد ورد في ديباجة اتفاقية لاهاي لعام ١٨٩٩وعام ١٩٠٧ بشأن قوانين وأعراف الحرب البرية، بالإضافة لذلك تم النص عليه في اتفاقيات جنيف الأربع لعام ١٩٤٩ (في المادة ٦٣ من الاتفاقية الأولى، والمادة ٦٢ من الاتفاقية الثانية، والمادة ١٤٢ من الاتفاقية الثالثة، والمادة ١٥٨ من الاتفاقية الرابعة)، وكذلك تم النص عليه في البروتوكول الإضافي الأول لعام

المنازعات يخضع لمبادئ القانون الدولي الإنساني، مما يعني عدم خلو الهجمات السيبرانية من القانون أثناء النزاع المسلح. وتؤيد ذلك محكمة العدل الدولية في رأيها الاستشاري بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها، حيث أشارت إلى أن مبادئ وقواعد القانون الدولي الإنساني المستقرة تنطبق" على جميع أشكال الحروب وعلى جميع أنواع الأسلحة بما في ذلك تلك المستقبلية". فالمبادئ والقواعد الإنسانية قد وضعت قبل الأسلحة النووية، ومع ذلك فإنه لا يوجد شك بانطباق القانون الدولي الإنساني على الأسلحة النووية، وليس هناك ما يدعو للتمييز بين الأسلحة النووية والهجمات السيبرانية، من حيث الزمن الذي استحدثت فيه مما يعني إمكانية تطبيق القانون الدولي الإنساني عليها.

وبهذا الخصوص بين المستشار القانوني للجنة الدولية للصليب الأحمر **(Cordula Dorego)** أن الإطار القانوني الدولي الإنساني القائم يطبق على الهجمات" السيبرانية" ويجب احترامه، وقد تم تفنيد مزاعم من يعدون خلو الفضاء السيبراني من القوانين وعدم انطباق القانون الدولي الإنساني على الهجمات السيبرانية بقوله : إن هذه ليست المرة الأولى التي يحدث فيها تطوير وتغير في التكنولوجيا المستخدمة، وقد تعامل معها القانون الدولي الإنساني أو قانون النزاعات المسلحة، بمعنى أن القانون القائم قادر على التعامل مع هذه التطورات الجديدة دون الحاجة إلى إشعار أو وضع قواعد قانونية خاصة بالفضاء السيبراني[١].

وعليه أتناول فيما يلي القانون الدولي الإنساني كإطار قانوني ناظم للهجمات السيبرانية، وفق التقسيم الآتي:

المبحث الأول: إمكانية انطباق القانون الدولي الإنساني على الهجمات السيبرانية

المبحث الثاني: تحديات انطباق القانون الدولي الإنساني على الهجمات السيبرانية

١٩٧٧ في المادة (م١/ف٢)، وفي الديباجة البروتوكول الثاني، وأخيراً نصت عليه ديباجة اتفاقية حظر أو تقييد استعمال أسلحة تقليدية معينة يمكن اعتبارها مفرطة الضرر أو عشوائية الأثر لعام ١٩٨٠. ولابد من الإشارة إلى أن شرط مارتنز يسري على جميع أطراف النزاع سواء كانت طرفاً في الاتفاقيات التي تضمنها الشرط أم ليست كذلك وهذا يرجع إلى طبيعته العرفية والإنسانية. انظر: سعود، آيات محمد: شرط مارتينز في القانون الدولي الإنساني، موقع الحوار المتمدن، استرجعت بتاريخ ٢٠٢١/٢/، متاح على الرابط: https://www.ahewar.org/debat/show.art.asp?aid=591797

[١] أعمر، عمر محمود: "الحرب الإلكترونية في القانون الدولي الإنساني"، مجلة دراسات، علوم الشريعة والقانون، الجامعة الأردنية، الأردن، المجلد ٤٦، عدد ٣، ٢٠١٩، ص ص ١٣٤-١٥٥، ص ١٣٨، متاح على الرابط: https://cutt.ly/lkpBGCp

المبحث الأول

إمكانية انطباق القانون الدولي الإنساني على الهجمات السيبرانية

على الرغم من أن الهجمات 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 الهجمات 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 الهجمات السيبرانية. وبناء على ذلك سنبين في المطلب الأول معايير تحديد الأهداف العسكرية المشروعة أثناء الهجمات السيبرانية في القانون الدولي الإنساني، أما المطلب الثاني فسنتحدث عن تطبيق المبادئ العامة في القانون الدولي الإنساني أثناء الهجمات السيبرانية.

المطلب الأول: معايير تحديد الأهداف العسكرية المشروعة أثناء الهجمات السيبرانية في القانون الدولي الإنساني

شهدت نهايات القرن الثامن عشر وبدايات القرن التاسع عشر استقرار التفرقة بين المقاتلين وغير المقاتلين، وخير دليل على ذلك ما قاله المفكر الفرنسي الشهير "جان جاك روسو" في كتابه "العقد الاجتماعي" بالآتي (..." إن الحرب ليست علاقة بين إنسان وإنسان وإنما علاقة بين دولة ودولة، والأفراد ليسوا أعداء إلا بصفة عرضية لا كأفراد أو مواطنين، ولكن كجنود وعداؤهم ليس على أساس أنهم ينتمون إلى الطرف المحارب بل كمدافعين عنه..."[١].

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 الهجمات السيبرانية يفقدوا الحماية التي يتمتعوا بها ويصبحون أهدافاً مشروعة. وسوف نبين ذلك فيما يلي.

---

[١] روسو، جان جاك: العقد الاجتماعي، مؤسسة هنداوي للتعليم والثقافة، القاهرة،٢٠١٣م، ص ٣٣، متاح على الرابط: https://cutt.ly/WkpNp5Y

الفرع الأول: الأشخاص والأعيان المشروع استهدافهم أثناء الهجمات السيبرانية

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

أولاً_ الهجمات 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 الناشـئة عن مبادئ التمييز والتناسـب والاحتياط التي توفر حماية عامة للمدنيين والأعيان المدنية تنطبق فقط على العمليات العسـكرية التي تشـمل "هجمات" على النحو المحدد في القانون الدولي الإنساني. وتعرف الهجمات 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"[١].

و من وجهة نظر اللجنة الدولية، العمليات السـيبرانية التي تنفذ بواسـطة الفيروسـات والديدان الحاسوبية وسائر الوسائل الأخرى وتلحق أضراراَ بدينة 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 المنصـوص عليه في القانون الدولي الإنسـاني، على سبيل المثال وفاة المرضى في وحدات العناية المركزة نتيجة لعملية سيبرانية ضد شبكة الكهرباء مما تسـبب بقطع إمداد المسـتشـفى بالتيار الكهربائي. إذاً من المتفق عليه على نطاق واسـع أن العمليات السيبرانية التي يتوقع منها أن تسبب وفاة أو إصابة أو ضرراً مادياً تشكل هجمات بموجب القانون الدولي الإنساني [٢].

ويدعى أحياناً بأن الهجمات السـيبرانية لا تندرج في نطاق تعريف "الهجوم" ما دامت لا تتسـبب في أضـرار بدنية أو عندما يكون في الإمكان التخلص من الآثار الناجمة عنها. وإذا كان المراد بهذا الادعاء تسـويغ اعتبار الهجوم على ممتلكات مدنية عملاً قانونياً في هذه الحالات، فإن اللجنة الدولية ترى أنه

---

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

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

ادعاء باطل لا أساس له بموجب القانون الدولي الإنساني. فلا يجوز، بموجب القانون الدولي الإنساني توجيه الهجمات إلا إلى الأهداف العسكرية ولا يجوز الهجوم على الأهداف المدنية [١].

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 [٢]. 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 [٣]. 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)**[٤]، وجيش التحرير الشعبي الصيني لديه قسم أو فريق سيبراني يسمى "الجيش الأزرق"[٥]، ودولة النرويج لديها **(Cyberforsvaret)** أي الدفاع السيبراني الذي يقوم بإنشاء وتشغيل وحماية أنظمة اتصالات القوات المسلحة والبنية التحتية الرقمية[٦].

---

[١] تقرير اللجنة الدولية للصليب الأحمر للمؤتمر الدولي الحادي والثلاثون للصليب الأحمر والهلال الأحمر، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، جنيف، سويسرا،٢٠١١، الوثيقة:31IC/11/5.1.2 ، ص ٤٣-٤٢.

[٢] 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

[3]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

[٤] موقع القيادة السيبرانية للجيش الأمريكي، استرجعت بتاريخ٢٠٢١/١/٣١، متاح على الرابط: https://www.arcyber.army.mil/

[٥] الصين: "جيش أزرق" لحماية شبكات " الجيش الأحمر"، موقع BBC NEWS، استرجعت بتاريخ٢٠٢١/١/٣١، متاح على الرابط: https://www.bbc.com/arabic/scienceandtech/2011/06/110531_china_blue_army

[٦] موقع Cyberforsvaret الدفاع السيبراني النرويجي، استرجعت بتاريخ٢٠٢١/١/٣١، متاح على الرابط: https://www.forsvaret.no/

وقد سعى تالين إلى تحديد من هم "أعضاء القوات المسلحة" الذين يتمتعون بحقهم في الحصول على حصانة المقاتل ومركز أسير الحرب [١].

يمكن القول في رأينا، يشكل الأشخاص الذين يملكون أجهزة وبرامج سيبرانية بصفة منتظمة كمقاتلين تحت 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 الهجمات 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 [٢].

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[٣]. 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[٤].

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

---

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

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

[٣] 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

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

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 الهجمات المضادة [١].

ومن ناحية القدرة على الانخراط في عنف شديد بما فيه الكفاية، إذا أفضت الهجمات 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 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[٢].

ثالثاً_ الأعيان المشروع استهدافها أثناء الهجمات السيبرانية

يوضح دليل تالين أن الهجمات 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] 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

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

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[١].

المعيار الثاني: بحكم "موقعه": يشير الموقع عادة إلى منطقة جغرافية ذات أهمية عسكرية خاصة وفي حديثنا على سبيل المثال: إن عنوان **(IP)**أو **(كتلة عناوينIP)** 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 [٢] 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[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 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[٤]. 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 [٥].

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

---

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

(٢) 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)، استرجعت بتاريخ٢٠٢١/٢/١٣، متاح على الرابط: https://cutt.ly/5kCk8TQ

(3) Ibid, comment (7) on Rule (38).

(4) Ibid, comment (8) on Rule (38).

(5) Ibid, comment (10) on Rule (38).

تفيد بأن أحد أطراف النزاع على وشك شراء أجهزة أو برامج كمبيوتر معينة لأغراض عسكرية، فإن هذه العناصر تصبح على الفور أهدافاً عسكرية[١].

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[٢].

٢. الأعيان ذات الاستخدام المزدوج

نقصد بذلك الأعيان المدنية التي تستخدم لأغراض عسكرية في نفس الوقت، نتيجة لذلك تصبح هدفاً عسكرياً طوال هذا الاستخدام[٣]، 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.[٤]بالتالي تشكل الهجمات السيبرانية تحديات فريدة في هذا 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[٥]. 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

---

(1) Schmitt, Michael (gen ed) :Tallinn Manual on the International Law Applicable to Cyber Warfare, op.cit, comment (11) on Rule (38).

(2) Ibid, comment (18) on Rule (38).

(٣) ميلزر، نيلس: مقدمة شاملة القانون الدولي الإنساني، مرجع سابق، ص٨٩.

(4) Schmitt, Michael (gen ed) :Tallinn Manual on the International Law Applicable to Cyber Warfare, op.cit, comment (2) on Rule (39).

(5) Ibid, comment (3) on Rule (39).

أجهزة التوجيه أو الأقمار الاصـــطناعية التي تعتمد عليها هذه النظم، دائماً بحقيقة أن هذه المســـارات تستخدم لنقل معلومات عسكرية وهي من ثم تصنف كأهداف عسكرية[١].

إلا أنه هناك بعض البيانات المدنية تتعلق بأعيان معينة تتمتع بحماية خاصـــة بموجب القانون الدولي الإنســـاني[٢] وهي الأعيان والمواد التي لا غنى عنها لبقاء الســـكان المدنيين، والأعيان الطبية، والأشغال الهندسية والمنشآت التي تحوي على مواد وقوى وطاقات خطرة والبيئة الطبيعية، والأعيان الثقافية وأماكن العبادة[٣]، فالالتزام باحترام وحماية هذه الأعيان الخاصـــة يفترض بأنه يشـــمل حماية البيانات الخاصة بهذه الأعيان أيضاً[٤].

فالهجوم السيبراني الذي استهدف المستشفى التابع لجامعة هاينرش هاينه في مدينة دوسلدورف في شـهر أيلول/ ٢٠٢٠، وتسـبب بشـكل غير مباشـر في وفاة مريضـة. كان الهدف منه في الأصـل 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 الشـرطة من التواصـل مع الهاكرز وإبلاغهم بأن هجومهم يعيق أنشـطة المسـتشـفى، سـلموا إلى السلطات مفتاحاً إلكترونياً يتيح معالجة المشكلة واستئناف المعلومات التي طالها الهجوم[٥].

بالتالي إن مثل هذا الهجوم الذي اسـتهدف المسـتشـفى، من المسـتحيل القول إن المسـتشـفى كانت تسـتخدم لأغراض عسـكرية حتى يتم اسـتهدافها، ومن ناحية أخرى يسـتدعي 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[٦].

---

[١] دوريجي، كوردولا: "لا تقترب من حدود فضـــائي الإلكتروني: الحرب الإلكترونية والقانون الدولي الإنســـاني وحماية المدنيين"، مرجع سابق، ص ٥٦٤.

[٢] حمدان، إيمان: التكنولوجيا الجديدة والقانون الدولي الإنســاني (الحرب الســيبرانية)، دراســات معقمة في القانون الدولي الإنساني، الماجستير في القانون الدولي الإنساني، الجامعة الافتراضية السورية، دمشق(سوريا)،٢٠٢٠م، ص٩.

[٣] كلزي، ياســر: النظرية العامة في القانون الدولي الإنســاني، ماجســتير القانون الدولي الإنســاني، الجامعة الافتراضــية السورية، دمشق(سوريا)،٢٠٢٠، ص١٠٢.

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

[٥] وفاة مريضة جراء هجوم سيبراني على مستشفى ألماني، موقع RTonline، استرجعت بتاريخ٢٠٢٠/١٢/٤، متاح على الرابط:

https://cutt.ly/1h5Jy0u

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

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"[١]. 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"[٢].

الفرع الثاني: المدنيون الذين يشاركون مباشرة في الهجمات السيبرانية

يتأثر المدنيون بصورة أو بأخرى، بعواقب النزاعات المسلحة، ولا يحتاج الأمر إلى تحليل أو دراسة للاعتراف بما تسببه الحروب من خسائر في صفوف المدنيين. وإذا كان من البديهي أن هؤلاء يجب أن يبقوا خارج دائرة المعارك، فإن النزاعات المعاصرة كالهجمات السيبرانية تتجه إلى عكس ذلك[٣]. فقد يشارك المدنيون مشاركة مباشرة في الهجمات السيبرانية، وأعرض فيما يلي مدلول الأشخاص المدنيون، ومن ثم مفهوم المشاركة المباشرة في الهجمات السيبرانية.

أولاً_ مدلول الأشخاص المدنيين

برأينا يعد مدلول الأشخاص المدنيين واحد لا يختلف سواء كانت هذه الهجمات هي هجمات عدائية حركية بالمعنى التقليدي، أم هجمات سيبرانية، ولذلك أعرض فيما يلي مدلول الأشخاص المدنيين كما وضحته قواعد القانون الدولي الإنساني.

بداية عرفت المادة ٥٠ (١) من البروتوكول الإضافي الأول المدنيون بأنهم الأشخاص الذين لا ينتمون إلى القوات المسلحة على المعنى المبين في الاتفاقية الثالثة، المادة ٤(أ) ٣،٢،١و٦ والمادة ٤٣ من البروتوكول الأول.[٤]

ونصت الاتفاقية الرابعة على أنها تحمي "الأشخاص الذين يجدون أنفسهم في لحظة ما وبأي شكل كان، في حالة قيام نزاع مسلح أو حالة احتلال، تحت سلطة طرف في النزاع ليسوا من رعاياه أو دولة

---

[1]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

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

[٣] شهاب، مفيد: دراسات في القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر، بدون تاريخ نشر، ص ١٢١.

[٤] البروتوكول الإضافي الأول لعام ١٩٧٧، المادة ٥٠(١).

احتلال ليسوا من رعاياها"[١]. وهكذا، فإن الجنسية هي المعيار المميز، لكن يمكن تصور وجود أشخاص بدون جنسية "تحت سلطة طرف في النزاع"، وباعتبارهم من غير رعايا أطراف النزاع فإن الاتفاقية الرابعة تطبق عليهم أيضاً، رغم أنها لا تذكر ذلك صراحة.

ويشمل مفهوم" الأشخاص المدنيين" جميع الأشخاص المدنيين، كما وضحت ذلك المادة ٥٠(٢) من البروتوكول الإضافي الأول، وفي حالة الشك، تكون قرنية الصفة المدنية هي الأولى بالاتباع، حسب الجملة الأخيرة من الفقرة الأولى من المادة نفسها، ولا يجرد السكان المدنيون من تلك الصفة بسبب وجود أشخاص منعزلين بينهم لا يستجيبون لشروط تعريف المدنيين، كما جاء في الفقرة الثالثة من المادة المذكورة.

ولابد من الإشارة إلى القاعدة ٥ من قواعد القانون الدولي الإنساني العرفي والتي تطبق في النزاعات المسلحة الدولية وغير ذات الطابع الدولي، حيث جاء فيها:

" المدنيون أشخاص لا ينتمون إلى القوات المسلحة. ويشمل مصطلح " السكان المدنيون" جميع الأشخاص المدنيين".

إذاً يجب النظر إلى مفهوم المدنيين على أساس التأويل الواسع، وداخل الإطار العام للمدنيين خصص القانون الدولي الإنساني مزيداً من العناية لفئات محددة كالنساء والأطفال واللاجئين وعديمي الجنسية والصحافيين، وليس ذلك بسبب انتفاء صفتهم المدنية وإنما تحسباً لما ينالهم من أعمال وتجاوزات أثناء النزاعات المسلحة[٢].

ثانياً_ تحديد مفهوم المشاركة المباشرة في الهجمات السيبرانية

بداية لقد استخرج مفهوم المشاركة المباشرة في العمليات العدائية من الجملة المستخدمة في المادة الثالثة المشتركة من اتفاقيات جنيف الأربع، بعبارة "الذين لا يشتركون مباشرة في الأعمال العدائية"[٣]. ومن المتفق عليه أن مشاركة المقاتلين في العمليات العدائية هي أمر مفترض فيهم لا حاجة لإثباتها، فإن العكس هو الصحيح فيما يخص المدنيين الذين يُفترض فيهم أنهم من غير المشاركين في مثل تلك العمليات إلى أن يثبت العكس. وبهذا المعنى فإن مفهوم المشاركة المباشرة في العمليات العدائية يشير إلى: **"أعمال محددة يقوم بها الأفراد كجزء من سير العمليات العدائية بين الأطراف في نزاع مسلح"**[٤].

---

[١] اتفاقية جنيف الرابعة، المادة ٤، فقرة ١.

[٢] شهاب، مفيد، دراسات في القانون الدولي الإنساني، مرجع سابق، ص ١٢٢-١٣٢.

[٣] ميلزر، نيلس: دليل التفسيري لمفهوم المشاركة المباشرة في العمليات العدائية بموجب القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر،٢٠١٠، ص ٤١-٤٢-٤٣.

[٤]طوزان، أحمد: قانون النزاعات المسلحة، ماجستير القانون الدولي الإنساني، الجامعة الافتراضية السورية، دمشق(سوريا)،٢٠٢٠، ص ٧٨.

ويتطلب القانون الدولي الإنساني لإضفاء وصف المشاركة المباشرة على شخص من المدنيين، توافر ثلاثة شروط الوصول إلى حد حصول الضرر والارتباط بالعمل الحربي والعلاقة السببية بينهما. وفي إطار الأعمال التحضيرية للهجمات السيبرانية، غالباً ما يتم تصميم وبرمجة الأسلحة السيبرانية بصورة خاصة لتنفيذها على أهداف معينة ومحددة مسبقاً، مما يجعل من جميع هذه الأفعال بصورة واضحة، مشاركة مباشرة في الهجمات السيبرانية التي يترتب عليها فقدان الحماية من الهجمات المباشرة وآثار القتال، فضلاً عن العقاب الذي يمكن أن يتعرض له المدني المشارك مشاركة مباشرة في الأعمال العدائية السيبرانية عن طريق تصميم وبرمجة الفيروسات والأسلحة السيبرانية وفق القانون الوطني [١]. بالإضافة إلى ذلك إن القانون الدولي الإنساني لا يمنع أي شخص من أن يحمل السلاح في نزاع مسلح وأن يصبح "مقاتلاً محروماً من الامتيازات"، إلا أنه وبكل بساطة يلزم كل من يقوم بهذا، بالامتثال لقواعده التي تحكم سير العمليات العدائية [٢]. ويمكن قياس هذا الأمر على الهجمات السيبرانية إلا أنه ما يعنيه حمل السلاح في الهجمات السيبرانية هو أمر غير واضح كما ذكرنا سابقاً.

ولا بد من الإشارة أنه تحت توجيهات حديثة من اللجنة الدولية للصليب الأحمر، يمكن استهداف المدنيين الذين يتبنون مهمة قتالية مستمرة، فالمبرمج الذي يعمل مع المخابرات العسكرية بتعديل الكود لتنفيذ مقاصد الهجوم، حتى لحظة الهجوم. يمكن تصور أفعال مثل هذا المدني "وظيفة مستمرة تتضمن التحضير أو التنفيذ أو القيادة لأعمال أو عمليات ترقى إلى المشاركة المباشرة في الأعمال العدائية". نتيجة لذلك، قد يُنظر إلى المدنيين المتورطين في الهجمات السيبرانية على أنهم يؤدون مهام قد تغير وضعهم بموجب قانون الدولي الإنساني، مما يجعلهم أهدافًا مشروعة[٣].

ولقد اتفق غالبية الخبراء الدوليين في دليل تالين على غرار قواعد القانون الدولي الإنساني أن المدنيين يحتفظون بوضع المدنيين حتى لو شاركوا بشكل مباشر في الأعمال العدائية السيبرانية ولكنهم يصبحون معرضين للاستهداف. على سبيل المثال، إذا كان هنالك نزاع مسلح دولي يقوم فيه قراصنة وطنيون مدنيون بشكل مستقل بعمليات هجومية سيبرانية ضد قوات العدو، قد يتم استهداف هؤلاء الأفراد بشكل قانوني[٤].

---

[١] الموسوي، علي محمد كاظم: "المشاركة المباشرة للهبة الجماعية في الهجمات السيبرانية"، مجلة كلية الحقوق، جامعة النهرين، الدكتور حيدر أدهم الطائي، بغداد، ٢٠١٩، ص ص ٢٥-٥٨، ص ١٥، متاح على الرابط: https://cutt.ly/Skgb1y7

[٢] ميلزر، نيلس: مقدمة شاملة القانون الدولي الإنساني، مرجع سابق، ص ١٦٦-١٦٥.

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

[4] Schmitt, Michael (gen ed) :Tallinn Manual on the International Law Applicable to Cyber Warfare, op.cit, Comment (3) On Rule (29)

المطلب الثاني: تطبيق المبادئ العامة في القانون الدولي الإنســـاني أثناء الهجمات السيبرانية

تخضع الهجمات السيبرانية التي تنفذ في إطار نزاع مسلح لقواعد القانون الدولي الإنساني، لا سيما القواعد التي تحكم سير العمليات العدائية، وكما جاء في تقرير اللجنة الدولية للصليب الأحمر عام ٢٠١١ يجب أن يتوافق توظيف الهجمات الســـيبرانية في إطار النزاع المســـلح مع جميع مبادئ القانون الدولي الإنساني وقواعده، كما هو الحال مع أي سلاح أو وسيلة أو أسلوب حرب آخر، جديداً كان أم قديماً. وما يؤيد ذلك ما أشـــارت إليه محكمة العدل الدولية إن: "مبادئ وقواعد القانون الدولي الإنســـاني المنطبق في النزاع المسلح، تنطبق على جميع أشكال الحروب وعلى جميع أنواع الأسلحة بما في ذلك تلك المستقبلية ". لذا فإن نقل مبادئ القانون الإنساني الدولي إلى استخدامها في الهجمات السيبرانية، على الرغم من كونها سلاحاً جديداً للحرب، ليس ممكناً فحسب، بل مناسباً أيضاً.

وبالنظر إلى ما سبق إن اتخاذ القرار باستخدام الهجمات السيبرانية من قبل طرف في النزاع يجب عليه مراعاة عدد من المبادئ العامة التي تضـــمن تحقيق متطلبات المشـــروعية في ذلك القرار ونتائجه. وتتوزع هذه المبادئ بحســـبان المرحلة التي ينبغي مراعاتها فيها بين مبادئ تتعلق بالتحضـــير لاســـتخدام الهجمات السيبرانية وأخرى ترافق استخدامها في ميدان العمليات العدائية. وسنبين ذلك فيما يلي.

الفرع الأول: المبادئ المتعلقة بالتحضير لاستخدام الهجمات السيبرانية

تبدأ التحضـيرات لاسـتخدام الهجمات السـيبرانية بالتمييز بين ما يمكن اسـتهدافه من الأشـخاص أو الأعيان، ومالا يجوز اســـتهدافه، ومن ثم اتخاذ كل ما يلزم من الاحتياطات لتجنب وقوع أي انتهاك أو خرق لقواعد القانون الدولي الإنســـاني وصـــولاً لتلافي الآثار غير المرغوب فيها التي تخلفها الهجمات السيبرانية في جانب المدنيين والأعيان المدنية. وسنبين ذلك فيما يلي.

أولاً_ مبدأ التمييز بين المشروع والمحظور أثناء الهجمات السيبرانية

يجب أن يكون مبدأ التمييز في قلب النزاعات المســـلحة الحديثة، لأنه أســـاس المبادئ الرئيســـية المتعلقة بمسـألة الاسـتهداف القانوني، وقد تم النص عليه في البروتوكول الإضـافي الأول لعام ١٩٧٧[١]، والقانون الدولي الإنساني العرفي[٢]، بالتالي ينطبق مبدأ التمييز في صياغته وتفسيره على نطاق واسع ولا يقتصـــر على أنواع معينـة من الأســـلحـة أو وســـائل الحرب، فهو قـابـل للتطبيق على الهجمـات

---

[١] البرتوكول الإضافي الأول لعام ١٩٧٧، المادة (٤٨).

[٢] هنكرتس، جون–ماري ودوزوالد–بك، لويز: القانون الدولي الإنســـاني العرفي (المجلد الأول/القواعد)، اللجنة الدولية للصليب الأحمر،٢٠١٦، القاعدة رقم ١، ص ٣–٥.

السيبرانية.[١]ويقتضي ضمان احترام هذا المبدأ أثناء التحضير لاستخدام الهجمات السيبرانية التمييز بين المقاتلين وغير المقاتلين من جهة، وبين الأعيان العسكرية وتلك المدنية من جهة أخرى.

١. التمييز بين المقاتلين السيبرانيين وغير المقاتلين السيبرانيين

وردت الإشارة إلى مبدأ التمييز بين المقاتلين والمدنيين لأول مرة في متن إعلان سان بطرسبورغ لعام ١٨٦٨ عندما نص على أن: "الهدف المشروع الوحيد الذي يتعين على الدول أن تسعى إلى تحقيقه أثناء الحرب هو إضعاف القوات العسكرية للعدو"[٢]. وقد جرى تقنين هذا المبدأ في البروتوكول الإضافي الأول المشار إليه أعلاه، وأيضاً تطالب المادة ٥١ من البروتوكول الإضافي الأول بضمان الحماية العامة للمدنيين المهاجمين من الأخطار الناشئة عن العمليات العسكرية، أما بالنسبة للمدنيين الذين يشاركون بشكل مباشر في الأعمال العدائية فإنهم لا يتمتعون بالحماية بحكم المشاركة، كما أشرنا سابقاً. والجدير بالذكر أن النظام الأساسي للمحكمة الجنائية الدولية نص على هذا المبدأ حيث اعتبر أن تعمد توجيه هجمات ضد السكان المدنيين بصفتهم هذه، أو ضد أفراد مدنيين لا يشاركون مباشرة في الاعمال الحربية على أنه جريمة حرب[٣].

والغرض الأساسي من مبدأ التمييز هو لضمان استهداف أطراف النزاع للمقاتلين وليس المدنيين، ولتحديد ما إذا كانت الهجمات السيبرانية تميز بشكل صحيح بين المقاتلين السيبرانيين والمدنيين، يجب على المرء أن يفهم أين يكمن الفرق بين الاثنين كما وضحنا سابقاً. ومع ذلك، قد يكون من المستحيل عملياً التمييز بين مقاتل سيبراني أو فرد آخر مستهدف قانونياً لسببين رئيسيين:

السبب الأول: قد يكون من الصعب للغاية، إن لم يكن من المستحيل، تحديد ما إذا كان المدني على علم بأن جهاز شبكة الكمبيوتر الخاص به يشارك في هجوم سيبراني.

---

[1]Lülf, Charlotte: Modern Technologies and Targeting Under International Humanitarian Law, Working Paper, Vol.3, No3, IFHV, Ruhr University Bochum, Germany,2013, P7, Available At: https://cutt.ly/sksxM79

[٢]طوزان، أحمد: قانون النزاعات المسلحة، مرجع سابق، ص ٨٩.

[٣] نظام روما الأساسي للمحكمة الجنائية الدولية، المادة (٨)، الفقرة (٢)، ١٩٩٨م، متاح على الرابط: https://www.icrc.org/ar/doc/resources/documents/misc/6e7ec5.htm

وبناء على ذلك لا يمكن أن يصبح الأفراد، الذين تساهم أجهزتهم الشبكية الحاسوبية في الهجمات السيبرانية دون علم مالكهم، خاضعين للاستهداف القانوني [1]. فالمهاجم السيبراني في هذه الحالة هو الذي يقوم بإجبار المدني على المشاركة في النزاع. على سبيل المثال، عندما يخترق مهاجم سيبراني أجهزة كمبيوتر مدنية لدمجها في شبكة الروبوتات ومن ثم يهاجم خصماً. هناك نوعان من الانتهاكات المتضمنة:

أ- المهاجم السيبراني يهاجم بشكل غير قانوني أجهزة الكمبيوتر المدنية ببرامج ضارة تجبر الكمبيوتر على الاستجابة على أمر المهاجمين السيبرانيين. والجدير بالذكر أن الدولة المستهدفة يمكن أن ترد بهجوم مضاد متناسب يؤثر على أجهزة الكمبيوتر المخترقة. في هذه الحالة، يكون المهاجم السيبراني الأصلي مسؤولاً عن الضرر اللاحق للممتلكات المدنية بسبب الحالة المستهدفة.

ب- المهاجم السيبراني يجبر المدنيين بشكل غير قانوني على المشاركة المباشرة في الأعمال العدائية، وذلك من خلال صنع سلاح سيبراني يتكون من أجهزتهم الحاسوبية، هذا هو المعادل السيبراني لـ "الدرع البشري"[2]. ولا يمكن للدولة التي يتم تنفيذ هجوم سيبراني عبر شبكاتها الحاسوبية المدنية، أن تخضع للمساءلة عن الهجمات؛ ما لم يثبت أنه تم ذلك عن علم قادتها [3].

السبب الثاني: لم يتم اعتبار المهندسين المدنيين ومصممي الأسلحة الآخرين أفراداً مستهدفين بشكل قانوني لأن دورهم كان ضئيلاً بالفعل مقارنة بالقادة العسكريين بما في ذلك المهندسين العسكريين والجنرالات.

ومع ذلك، يبدو أن دور مهندسي البرمجيات المدنيين أكثر أهمية بشكل ملحوظ في سياق الحرب السيبرانية، خاصة أنه بمجرد إطلاق هجوم سيبراني على شبكة الكمبيوتر، لم يعد هناك حاجة إلى مزيد من الإجراءات غالباً، نظراً لأن مساره وإجراءاته تمت برمجته تلقائياً من قبلهم. فيمكن بسهولة إساءة استخدام ميزة الحرب السيبرانية هذه من قبل السلطات الرسمية للدولة، والتي يمكن أن تنكر أي صلة بجماعة مدنية تدعي صراحة مسؤوليتها عن هجوم. لذلك، من الممكن أن تحتوي المعاهدة السيبرانية الجديدة على أحكام من شأنها أن تأخذ في الاعتبار مشاركة جميع المدنيين بنشاط وعن علم في الهجمات السيبرانية بما في ذلك إعدادها وتنظيمها، كأفراد مستهدفين بشكل قانوني[4].

---

(1)Knopová, Eva: New IHL Framework for Cyber Warfare, Faculty of Law (Department of International Law), Charles University in Prague, Thesis Supervisor: Dr. Martin Faix,2016, P55-56, Available At: https://cutt.ly/8ksnQdZ

(2)Gervais, Michael: "Cyber Attacks and The Laws of War", op.cit, P567.

(3)Knopová, Eva: New IHL Framework for Cyber Warfare, op.cit, P56.

(4) Ibid, loc.cit.

٢. التمييز بين الأعيان العسكرية والأعيان المدنية

يعد التمييز بين الأعيان العسكرية والمدنية في إطار الإعداد لاستخدام الهجمات السيبرانية أثناء العمليات العدائية، مكملاً للتمييز بين المقاتلين والمدنيين، ومحكوماً بذات القواعد القانونية تقريباً. ونقر بأنه تكمن صعوبة الهجمات السيبرانية، في عدم وجود خط محدد وواضح بين الأعيان العسكرية والمدنية. ولتحديد ما إذا كانت الهجمات السيبرانية تفي بمتطلبات التمييز، يجب على المهاجم السيبراني أن يحدد:

أ- ما إذا كان الهجوم يميز بشكل كافٍ بين الأعيان المدنية والعسكرية، مع الأخذ في الاعتبار الاستخدام المزدوج لمعظم البنية التحتية للإنترنت؛

ب-ما إذا كانت الهجمات السيبرانية تتم بشكل عشوائي [١].

وقد تم الإشارة إلى الهجمات العشوائية المحظورة في المادة (٤٣،٥٠،٤٩) من دليل تالين، وتستند هاتان القاعدان إلى المادة ٥١ (٤) من البروتوكول الإضافي الأول، القاعدتين (١١ و١٢) من القانون الدولي الإنساني العرفي.

ويتم تقييم ما إذا كان الهجوم عشوائياً على أساس كل حالة على حدة، وتشمل العوامل التي يجب مراعاتها ما يلي:

- طبيعة النظام الذي يتم إدخال البرامج الضارة فيه أو المعرضة للخطر؛
- طبيعة أسلوب أو وسائل الحرب السيبرانية المستخدمة؛
- مدى وجودة التخطيط؛
- وأي دليل على اللامبالاة من جانب المشغل السيبراني في التخطيط للهجوم أو الموافقة عليه أو تنفيذه [٢].

ومن ناحية أخرى لا يمكن اعتبار العملية السيبراني على الأعيان المدنية هجوماً مسلحاً إلا إذا كان له آثار خطيرة تهدد الصحة على مواطني الدولة، فمن غير الواقعي أن نتوقع أن يوافق المجتمع الدولي على أن الهجوم على برنامج البورصة يعتبر هجوماً مسلحاً على الرغم من النطاق الواسع للأضرار الجسيمة المحتملة التي قد يتسبب فيها، بما في ذلك فقدان الوظائف بشكل كبير وما يترتب على ذلك من تهديدات لبقاء الكثيرين المدنيين. ومع ذلك، حتى فريق الخبراء الدولي انقسم حول هذه القضية: "بعض الخبراء لم يكونوا مستعدين لتسميته هجوم على بورصة نيويورك مثلاً بهجوم مسلح لأنهم لم يقتنعوا بأن

---

(1)Gervais, Michael: "Cyber Attacks and The Laws of War", op.cit, p33.

(2) Schmitt, Michael (gen ed) :Tallinn Manual on the International Law Applicable to Cyber Warfare, op.cit, comment (6) on Rule (49).

مجرد الخسارة المالية تشكل ضرراً، بينما شدد آخرون على الآثار الكارثية التي قد يحدثها مثل هذا الانهيار، وبالتالي يعتبرونها كافية لوصف العملية الإلكترونية على أنها هجوم مسلح وبالتالي، هناك حاجة إلى وضع تنظيم قانوني واضح من قبل المجتمع الدولي [١].

ثانياً_ مبدأ الاحتياط لتجنب المحظورات أثناء الهجمات السيبرانية

يقع على عاتق القائد العسكري الذي يتولى التخطيط لعمل عدائي أن يسعى لاتخاذ تدابير وقائية يحتاط بها من الوقوع في أي خلل يشكل انتهاكاً لقواعد قانون الدولي الإنساني الواجب التقيد بها واحترامها، وبذلك يعد المقدمة المنطقية لتحقيق التزاماته المترتبة عليه أثناء استخدام القوة[٢]، وقد تم النص على هذا المبدأ ضمن نصوص البرتوكول الإضافي الأول لعام ١٩٧٧تحت عنوان "التدابير الوقائية" التي ورد تفصيلها في نص المادتين ٥٧و٥٨منه. في حين لم يتضمن البرتوكول الإضافي الثاني مثل هذا التقنين ليظل تطبيق مبدأ الاحتياط "التدابير الوقائية" في النزاعات المسلحة غير ذات الطابع الدولي محكوماً بالقانون الدولي الإنساني العرفي (القاعدة ١٥).

وقد فرضت قابلية استخدام الفضاء السيبراني لمثل تلك الأنشطة العدائية بعض التعقيدات بخصوص الإجراء الاحتياطي الواجب اتخاذه قبل شن الهجمات السيبرانية والإجراء الاحتياطي الواجب اتخاذه لتلافي آثار هذه الهجمات[٣]، إلا أن دليل تالين الذي اعتمد في قواعده على قواعد القانون الدولي الإنساني تطرق لأهم الاحتياطات والتقديرات التي يجب أخذها بالحسبان عند تنفيذ الهجمات السيبرانية، وسنبينها من خلال نوعين من الاحتياطات فيما يلي:

١. **الاحتياطات الواجب اتخاذها قبل شن الهجمات السيبرانية**

أ- **الرعاية المستمرة:** أي أنه في أثناء العمليات العدائية التي تنطوي على هجمات سيبرانية، ينبغي أن تتخذ الرعاية المستمرة لتجنب الأضرار بالسكان المدنيين والأعيان المدنية[٤].

---

(1)Knopová, Eva: New IHL Framework for Cyber Warfare, op.cit, p56-57.

(٢) طوزان، أحمد: قانون النزاعات المسلحة، مرجع سابق، ص ٩١.

(٣) الصادق، عادل عبد: الإرهاب الإلكتروني القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة، مركز الأهرام للدراسات السياسية والاستراتيجية، الطبعة الثانية، القاهرة،٢٠٠٩، ص ٢٨٣، متاح على الرابط: https://cutt.ly/SksQ7Xl

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

ب- **التحقق من الأهداف:** ينبغي على أولئك الذين يخططون أو يصدرون الأمر بالهجوم السيبراني، اتخاذ جميع الاحتياطات الممكنة لكيلا يكون المدنيون، والأعيان المدنية والأشخاص الذين يتمتعون بحماية خاصة موضع للهجمات السيبرانية[١].

ج- **اختيار الوسائل والأساليب المستخدمة في الهجوم:** ينبغي على أولئك الذين يخططون أو يصدرون الأمر بالهجوم السيبراني اتخاذ جميع الاحتياطات المستطاعة عند اختيار وسائل الحرب وأساليبها المستخدمة في هذا الهجوم، وذلك بهدف التجنب أو على الأقل التقليل من الإصابات العرضية في صفوف المدنيين، أو التسبب بفقدانهم للحياة أو التلف والتدمير للممتلكات المدنية[٢].

د- **الاحتياطات الواجب اتخاذها لتحقق التناسب:** ينبغي على أولئك الذين يخططون أو يصدرون الأمر بالهجمات، الامتناع عن اتخاذ القرار بشأن تنفيذ أي هجوم سيبراني يتوقع منه أن يسبب خسائر عرضية في أرواح المدنيين أو تؤدي إلى إصابتهم أو إلحاق الأضرار بالأعيان المدنية، أو أن يحدث خلط نتيجة ذلك تكون نتائجه مفرطة مقارنة بالميزة العسكرية المرتقبة من الهجوم[٣].

هـ- **اختيار الأهداف:** أي أنه عندما يكون الخيار ممكناً بين عدة أهداف عسكرية ممكنة (مشروعة)، تحقق ميزة عسكرية مماثلة، فينبغي توجيه الهجمات السيبرانية إلى تلك الأهداف التي يتوقع منها أن تسبب خطراً أقل على أرواح المدنيين والاعيان المدنية[٤].

و- **إلغاء الهجوم أو إيقافه:** يجب على من يتخذ قرار الموافقة أو تنفيذ الهجمات السيبرانية، إلغاء أو تعليق الهجوم إذا اتضح ما يلي:

- الهدف ليس هدفاً عسكرياً أو أنه مشمول بحماية خاصة؛ أو
- من الممكن أن يسبب الهجوم، بصورة مباشرة أو غير مباشرة، خسائر عرضية في أرواح المدنيين، وإصابة المدنيين، أو الإضرار بالأعيان المدنية، أو المزيج من ذلك، والتي قد تكون مفرطة بالنسبة للميزة العسكرية الملموسة والمباشرة المتوقعة من الهجوم[٥].

---

(1) Ibid, Rule (53).

(2) Ibid, Rule (54).

(3) Ibid, Rule (55).

(4) Ibid, Rule (56).

(5) Ibid, Rule (57).

ز- **التحذيرات:** ينبغي أن يوجه إنذار مسبق فعال بشأن الهجمات السيبرانية التي قد تؤثر على السكان المدنيين، مالم تمنع الظروف ذلك[١].

٢. الاحتياطات الواجب اتخاذها لتلافي آثار الهجمات السيبرانية

يعد هذا الالتزام واجباً قانونياً ذو طبيعة عرفية بالنسبة للنزاعات المسلحة الدولية وغير ذات الطابع الدولي، وذلك بالاستناد إلى نص القاعدة ٢٢ من القانون الدولي الإنساني العرفي[٢]، وتمت الإشارة إليه في القاعدة ٥٩ من دليل تالين.

ومن الأمثلة على مبدأ الاحتياط: القيام بعزل البنى التحتية الالكترونية العسكرية عن المدنية، وفصل الحاسوب التي تعتمد عليها البنى التحتية الأساسية عن شبكة الانترنت، وعدم استخدام شبكة الاتصالات المدنية للأغراض العسكرية، ودعم البيانات المدنية الرقمية بنسخ احتياطية، واستخدام الإجراءات المضادة لفيروسات الحاسوب لحماية النظم المدنية، والقيام بتوزيع البرمجيات الواقية، ومراقبة النظم والشبكات الإلكترونية، وتطوير قدرات رد الفعل لمنع التسلل من قبل الخصم للنظم الإلكترونية المدنية[٣].

علاوة على ذلك، إن طبيعة التقنية السيبرانية المختارة تحدد أيضاً ما إذا كان يمكن الوفاء بالالتزام، فمن الممكن تعطيل الهجمات إذا تم تصنيف الهدف بشكل خاطئ، فقط إذا كان المهاجم قادراً على التحكم في السلاح أو الوسيلة المنتشرة، إلا أنه وعلى سبيل المثال: إذا تم استخدام برنامج الدودة، التي تقوم بتكرار نفسها دون مزيد من التحكم في الشخص الذي أطلقها للاستهداف يكون من الصعب إيقافها بسبب الطبيعة التقنية لها، فلا يمكن الالتزام بالالتزام، مما يؤدي إلى انتهاك القانون الدولي الإنساني[٤]. إلا أنه إذا تم تطويرها لتفوق كفاءة البشر، قد يكون لها القدرة على الامتثال لقواعد القانون الدولي الإنساني بشكل أفضل[٥].

---

(1) Ibid, Rule (58).

(٢) هنكرتس، جون-ماري ودوزوالد-بك لويز: القانون الدولي الإنساني العرفي (المجلد الأول/القواعد)، مرجع سابق، ص٦١.

(3) Schmitt, Michael (gen ed) :Tallinn Manual on the International Law Applicable to Cyber Warfare, op.cit, comment (1-9) on Rule (59).

(4)Lülf, Charlotte: Modern Technologies and Targeting Under International Humanitarian Law, op.cit, p44.

(٥) سعود، يحيى ياسين: " الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني"، المجلة القانونية (مجلة متخصصة في الدراسات والبحوث القانونية)، جامعة يحي فارس، الجزائر، ٢٠١٨، ص ص ٧٩-١٠٨، ص ٩٩، متاح على الرابط: https://cutt.ly/QksE4ii

الفرع الثاني: المبادئ التي تحكم استخدام الهجمات السيبرانية أثناء العمليات العدائية

يعمد أطراف أي نزاع مسلح لاستخدام القوة أو الهجمات السيبرانية على وجه الخصوص وفقاً لأولوية رئيسة هي إنهاء أو على الأقل إضعاف القدرة العسكرية للطرف الآخر لأقصى حد ممكن، إلا أن القانون الدولي الإنساني وبوصفه القانون الذي وجد أصلاً لترشيد استخدام القوة وليس لمنع استخدامها، وضبط هذا الاستخدام بمبدأين اثنين من المبادئ الأساسية التي ينبغي أن تظل موضوع احترام من قبل جميع أطراف النزاع، وهما: مبدأ التناسب بين الضرر والميزة العسكرية المباشرة ومبدأ الضرورة العسكرية.

أولاً_ مبدأ التناسب بين الضرر والميزة العسكرية المباشرة

يعني هذا المبدأ أن الميزة العسكرية التي تحصل عليها عملية معينة يجب أن تفوق الضرر الذي يلحق بالمدنيين والأعيان المدنية من جراء ذلك الإجراء، وقد تم التعبير عنه في متن المادة ٥٧ (البند الثاني/الفقرة أ/ثالثاً، والبند الثالث) والمادة ٥٢ من البروتوكول الإضافي الأول لعام ١٩٧٧، وإلى جانب الطابع التعاهدي البارز لهذا المبدأ يبرز طابعه العرفي الذي يؤكد وجوده كقاعدة أصلية من قواعد القانون الدولي الإنساني العرفي، وبالتالي انطباقه على النزاعات المسلحة الدولية وغير ذات الطابع الدولي على حد سواء[١].

وكما هو الحال مع جميع أنواع الأسلحة الأخرى المستخدمة في النزاعات المسلحة، يجب أن تمتثل الهجمات السيبرانية لمبدأ التناسب[٢]. فتبنى دليل تالين الذي اعتمد في قواعده على قواعد القانون الدولي الإنساني كما ذكرنا سابقاً على هذا المبدأ في القاعدة ٥١، وتناول المواقف التي يتعرض فيها المدنيون أو الأعيان المدنية للأذى العرضي، أي أنهم ليسوا أهدافاً مقصودة للهجوم. كما وضح، بأن حقيقة تعرض المدنيين أو الأعيان المدنية للأذى أثناء هجوم سيبراني على هدف عسكري مشروع لا تجعل بالضرورة الهجوم المذكور غير قانوني في حد ذاته. بدلاً من ذلك، تعتمد مشروعية الهجوم الذي ينتج عنه أضرار جانبية، على العلاقة بين الضرر الذي يتوقع المهاجم بشكل معقول أن يتسبب فيه بشكل عرضي للمدنيين والأعيان المدنية والميزة العسكرية التي يتوقعها نتيجة للهجوم. وعلى سبيل المثال: إن الهجوم السيبراني على نظام تحديد المواقع العالمي **(GPS)**هو نظام ثنائي الاستخدام وبالتالي فهو هدف قانوني. ومع ذلك، من المرجح أن يؤدي حرمان المستخدمين المدنيين من المعلومات الأساسية مثل البيانات الملاحية إلى إلحاق الضرر بالسفن التجارية والطائرات المدنية التي تعتمد على توجيهات نظام تحديد المواقع

---

[١] هنكرتس، جون-ماري ودوزوالد-بك لويز: القانون الدولي الإنساني العرفي (المجلد الأول/القواعد)، مرجع سابق، القاعدة رقم ١٤، ص ٤١-٤٣.

[2]Lülf, Charlotte: Modern Technologies and Targeting Under International Humanitarian Law, op.cit, p43.

العالمي، فإذا كان هذا الضـــرر المتوقع مفرطًا مقارنة بالميزة العســـكرية المتوقعة للعملية، فســـيتم حظر العملية وسيعتبر هذا الهجوم غير شرعي ومنتهكاً لمبدأ التناسب[١].

ومن ناحية أخرى قد تتسـبب الهجمات السـيبرانية في حدوث إزعاج أو تهيج أو توتر أو خوف، فلا تعتبر مثل هذه العواقب أضـراراً جانبية لأنها لا ترقى إلى "خسارة في أرواح المدنيين، أو إصـابة المدنيين، أو الأضـــرار التي تلحق بـالأعيان المدنيـة"، فلا ينبغي أخذ هذه الآثار في الاعتبار عند تطبيق هذه القاعدة[٢].

وبالنظر إلى مخاطر الهجمات السـيبرانية من المرجح جداً أن يتم انتهاك مبدأ التناسـب في تفسـيره التقليدي بسـبب الترابط بين الأنظمة المدنية والعسـكرية والآثار التي لا يمكن السـيطرة عليها على البنى التحتية المدنية[٣]، وفي سبيل الحد من هذه المخاطر والانتهاكات، قد نرى تغييرات في الأنظمة والشبكات من أجل فصل الشبكات المدنية عن الشبكات العسكرية من أجل تسهيل الوصول إلى مثل هذه الفروق في أوقات الحرب أو الأزمات[٤].

ثانياً_ مبدأ الضرورة العسكرية

ورد أول تعريف لمبدأ الضـــرورة العســـكرية في قانون ليبر عام ١٨٦٣ التي عرفها بأنها: "التدابير التي لا غنى عنها لتأمين انتهاء الحرب"[٥]. وتم الإشـــارة لهذا المبدأ في اتفاقية لاهاي الخاصـــة باحترام قوانين وأعراف الحرب البرية لعام ١٩٠٧ في المواد (٤٣و٥٤و ٢٣/ز). ويعتبر انتهاك مبدأ الضـــرورة العســكرية "جريمة حرب" في نظام روما الأســاســي للمحكمة الجنائية الدولية[٦]. وفي ذات الشــأن تمت الإشـــارة لمبدأ الضـــرورة العســـكرية في المواد٥٢/٢و ٥٤/٢و ٦٢/١و ٧١/٣و٦٧/٤ من البروتوكول الإضـافي الأول الملحق باتفاقيات جنيف الأربع لعام ١٩٤٩ والمتعلق بحماية ضـحايا النزاعات المسـلحة الدولية. وبالاطلاع على المواد السـابقة نسـتنتج، أن مبدأ الضـــرورة العســكرية، يتيح مهاجمة الأهداف

---

(1) Schmitt, Michael (gen ed) :Tallinn Manual on the International Law Applicable to Cyber Warfare, op.cit, comment (4) on Rule (51).

(2) Ibid, Comment (5) On Rule (51).

(3) Lülf, Charlotte: Modern Technologies and Targeting Under International Humanitarian Law, op.cit, P43.

(4) Andress, Jason. Winterfeld, Steve: Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, 1st Edition, Elsevier, USA,2011, P234, Available At: http://index-of.es/Hack/Cyber%20Warfare.pdf

(٥) أعمر، عمر محمود: "الحرب الإلكترونية في القانون الدولي الإنساني"، مرجع سابق، ص ١٤١.

(٦) نظام روما الأساسي للمحكمة الجنائية الدولية، مرجع سابق، القاعدة ٨(٢/أ/٤).

العسكرية كخيار ضروري بالمرتبة الأولى، إلا أن ذلك لا يمنع كضرورة من مهاجمة أعيان مدنية، إذا كانت تسهم بطريقة غير مباشرة في تحقيق ميزة عسكرية أكيدة. وقد تم تحديد شروط معينة في القانون الدولي الإنساني يمكن بموجبها اللجوء لمبدأ الضرورة العسكرية وهي ما يلي:

- أن يكون هذا التجاوز مؤقتاً ومرتبطاً بمدة قيام هذه الضرورة.
- أن يكون على أهداف محددة.
- أن يكون الغرض منها تحقيق ميزة عسكرية أكيدة.
- أن يتم مراعاة القانون الدولي الإنساني.

وبالنسبة لدليل تالين الذي استوحى قواعده من القانون الدولي الإنساني أشار إلى أنه في الحالات التي يكون الخيار ممكناً بين عدة أهداف عسكرية للحصول على ميزة عسكرية مماثلة، فالهدف الذي يتم اختياره للهجوم السيبراني، هو ذلك الهدف الذي يتوقع منه أن يسبب خطر أقل على المدنيين والأعيان المدنية، إما في حالة وجود العديد من الأهداف إلا أن أحداها تحقق ميزة عسكرية أكثر من مثيلاتها، ففي هذه الحالة من حق المهاجم توجيه الهجمات السيبرانية المباشرة ضد الهدف العسكري الذي يحقق أكثر ميزة عسكرية ممكنة في إطار النزاع المسلح، وهنا يجب أن ينظر بشأن الهجمات السيبرانية إلى الضرر الذي يلحق بالمنشآت والبنية التحتية المهمة بالنسبة للمدنيين، فضلاً عما يسببه للمدنيين من حرمان في وظائف وخدمات هذه المنشآت تطبيقاً لمبدأ الضرورة العسكرية[١].

واستناداً إلى ما سبق يمكن القول إن اللجوء إلى الهجمات السيبرانية يجب أن يكون ضرورياً لتحقيق الهدف العسكري المشروع، وأما مسألة تحديد الأهداف والمنشآت العسكرية في الفضاء السيبراني فتثير تحدياً واسعاً أمام المجتمع الدولي، وذلك لأن المنشآت التي تقدم خدمة للجهد العسكري هي في الوقت نفسه تخدم القطاع المدني، فيجب إذا على المقاتل السيبراني تحديد كل حالة على حدة، أي أنه في كل حالة، يجب على المقاتل السيبراني أن يقرر بشكل قاطع أن الهجوم السيبراني يوفر ميزة عسكرية لتحقيق هدف عسكري[٢]. وقد أشار إلى هذا التحدي ريكس هيوز **(Rex Hughes)** مدير شبكة الابتكار السايبري في جامعة كامبردج بالقول: "إن الهجمات الرقمية تنشئ تحدياً واضحاً أمام تطبيق مبدأ الضرورة العسكرية ولحل هذه المعضلة لابد من تضافر الجهود بين خبراء القانون الدولي ومهندسي الصناعات الإلكترونية لتحديد ما يمكن أن يوصف بهدف...."[٣].

---

[١] سعود، يحيى ياسين: "الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني"، مرجع سابق، ص٩٤.

[2] Gervais, Michael: "Cyber Attacks and The Laws of War", op.cit, P33.

[3] Hughes, Rex: "A Treaty for Cyber Space", International Affairs (Royal Institute of International Affairs 1944-), Vol. 86, No. 2, UK, 2010, pp. 523-541, p537, Available AT: https://academic.oup.com/ia/article/86/2/523/2326362

المبحث الثاني

تحديات انطباق القانون الدولي الإنساني على الهجمات السيبرانية

يواجه انطباق القانون الدولي الإنساني على الهجمات السيبرانية تحديات عدة، فلا يتضمن القانون الدولي الإنساني على أي قواعد صريحة بشأن الهجمات السيبرانية في الفضاء السيبراني، والسبب في ذلك هو أنها لا تكون هذه الهجمات حركية، أي ليست هجمات مسلحة بالمعنى التقليدي. إلا أنه وبالنظر إلى الهدف الأساسي للقانون الدولي الإنساني المتمثل بحماية المدنيين من ويلات الحرب، يصبح القانون الدولي الإنساني منطبقاً، وتندرج تلك الهجمات ضمن قواعده إذا كان هدف الهجمات السيبرانية هو تعريض الأشخاص المحميين وممتلكاتهم للخطر أو المخاطرة بحدوث ذلك، ولكن يبقى التحدي في مقدرة القانون الدولي الإنساني على تنظيم أساليب ووسائل الحرب الجديدة.

فأي سلاح لم يتم ذكره في أي اتفاقية لا يعني بالضرورة إباحة استخدامه، ويعد المثال الواضح للحظر الوقائي الوحيد هو ما ورد في البروتوكول الرابع لاتفاقية الأسلحة التقليدية لعام ١٩٨٠ الخاص بحظر استخدام أسلحة الليزر المعمية والذي ألحق باتفاقية عام ١٩٩٥م، فهذا السلاح تم تحريمه بمجرد بدء التجارب عليه، وقبل وضعه موضع الاستخدام العسكري الفعلي. لكن هذا المثال لا يمكن تعميمه؛ لأن معظم التجارب على الأسلحة الجديدة تعتبر أسراراً عسكرية، وبالتالي من النادر التعرف على آثار تلك الأسلحة. ومن ثم يأخذ تحريم استخدام سلاح معين حيزاً من الجهد والوقت والنيات الحسنة، وهذا ما قد لا يتوافر.

وبالإضافة إلى ذلك تم التركيز في اتفاقيات جنيف الأربع لعام ١٩٤٩ على حماية الأشخاص في حالة النزاعات المسلحة دون الإشارة إلى الهجمات السيبرانية، ودون الإشارة إلى استخدام أسلحة معينة. إلا أنه تعد البروتوكولات الإضافية أكثر ملاءمة لتقديم موقفها من استخدام الهجمات السيبرانية، كما أشرنا سابقاً المادة ٣٦ و٣٥ الفقرة ١ من البروتوكول الإضافي الأول لعام ١٩٧٧ بالإضافة لشرط مارتينز والرأي الاستشاري لمحكمة العدل الدولية بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها كلها تدل على أن القانون الدولي الإنساني قابل للانطباق على الهجمات السيبرانية التي تحدث في سياق النزاع المسلح، إلا إن الهجوم السيبراني إذا لم يحدث في سياق نزاع مسلح ولكن آثاره وتداعياته تنشئ هذا النزاع المسلح فيمكن انطباق القانون الدولي الإنساني عليه، ولكن بالمقابل إذا كانت آثاره لا تصل إلى نفس تأثير الهجوم العسكري الفعلي، لا يمكن انطباق القانون الدولي الإنساني عليه، بل يخضع للقانون الدولي لحقوق الإنسان وللقوانين الجنائية الوطنية. واستناداً لما سبق سوف نقسم هذا المبحث إلى مطلبين،

نستعرض في الأول الهجمات السيبرانية في سياق النزاع المسلح، أما الثاني الهجمات السيبرانية خارج سياق النزاع المسلح.

المطلب الأول: الهجمات السيبرانية في سياق النزاع المسلح

من المتفق عليه أن القانون الدولي الإنساني ينطبق على الهجمات السيبرانية التي تحدث في سياق نزاع مسلح قائم بالفعل. فيجب على الدول أن تحترم قواعد القانون الدولي الإنساني عندما تشن هجمات سيبرانية في إطار نزاع مسلح، بغض النظر عما إذا كان الفضاء السيبراني معترفاً به كميدان قتال اصطناعي جديد، يضاف إلى الميادين الطبيعية للحرب المتمثلة بالبر والجو والبحر والفضاء الخارجي ويرتبط بجميع هذه الميادين الطبيعية، أم لم يعتبر ميداناً للحرب في حد ذاته [١]. لذلك يجب أن تمتثل وسائل وأساليب الحرب القائمة على التكنولوجيا السيبرانية، عند استخدامها في نزاع مسلح من قبل أو لصالح أو نيابة عن أحد أطراف النزاع القائم لقواعد ومبادئ القانون الدولي الإنساني، كما هو الحال مع أي سلاح جديد أو أسلوب جديد لتنفيذ العمليات. كما أوضحت ذلك المادة ٣٦ من البروتوكول الإضافي الأول التي تُلزم الدول بفحص شرعية الوسائل والأساليب الحالية والمستقبلية للقتال في إطار القانون الدولي الإنساني القائم، مما يؤكد انطباق القانون الدولي الإنساني على هذه الوسائل والأساليب. وبالمثل تنص المادة ٤٩ منه على أن قواعد هذا البروتوكول تنطبق على الحروب البرية وعلى جميع أنواع الحروب الأخرى التي قد تضر المدنيين على البر، وهذا ينطبق على الحرب السيبرانية والتي تخاض ولو جزئياً من بنية تحتية أساسية موجودة على البر وتوجه ضد أهداف على البر، وتنطوي على مخاطر تؤدي إلى إلحاق الأذى بالمدنيين على البر [٢]. وعلينا ألا نستغرب عند قولنا بأن هناك حالات حصل فيها هجمات سيبرانية في سياق نزاع مسلح قائم بالفعل. وبالإضافة إلى ذلك يحقق تقييم انطباق القانون الدولي الإنساني على الهجمات السيبرانية في مصلحة كافة الدول، حيث أنه يساعدها في ضمان توافق سلوك قواتها المسلحة مع المبادئ والاتفاقيات الدولية. وعليه سوف نقسم هذا المطلب إلى فرعين، نبين في الفرع الأول الحالات التطبيقية للهجمات السيبرانية في سياق النزاع المسلح، أما الفرع الثاني سنتناول تقييم انطباق القانون الدولي الإنساني على الهجمات السيبرانية في سياق النزاع المسلح.

---

[١] اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، ورقة موقف اللجنة الدولية للصليب الأحمر، تشرين الثاني ٢٠١٩، ص٢٦.

[٢] حمدان، إيمان: التكنولوجيا الجديدة والقانون الدولي الإنساني (الحرب السيبرانية)، مرجع سابق، ص ٥.

الفرع الأول: حالات تطبيقية للهجمات السيبرانية في سياق النزاع المسلح

قد تحدث الهجمات السيبرانية في ساحة موازية لحرب تقليدية أو نزاع مسلح دائر على الأرض، ويكون ذلك تعبيراً عن حدة النزاع القائم بين الأطراف، كما قد يمهد لعمل عسكري، هنا تدور الحروب السيبرانية عن طريق اختراق المواقع الإلكترونية، وتخريبها، وشن حرب معلوماتية وتجسسية ضد الخصوم. "ويستمد هذا النوع من الحروب السيبرانية شدته من قوة أطرافه، وارتباطها بعمل عسكري تقليدي، خاصة في ظل بعض التقديرات التي تشير إلى أن تكلفة هذه الحروب قد تشكل الربع من إنفاق نظيراتها التقليدية، بما يمكن تمويل حملة حربية كاملة عبر الانترنت بتكلفة دبابة"[١]، وتاريخياً نجد حالات تطبيقية لهذه الحروب السيبرانية في حرب كوسوفو عام ١٩٩٩، حيث استهدفت الهجمات السيبرانية تعطيل شبكة الاتصالات للخصوم، وأيضا برزت خلال الجمهورية العربية السورية والكيان الصهيوني عام ٢٠٠٧، وكذلك بين روسيا وجورجيا في عام ٢٠٠٨[٢]. وسوف تتم دراسة هذه الحالات التطبيقية فيما يلي.

أولاً_ حرب كوسوفو عام ١٩٩٩

المكان: منطقة كوسوفو وتقع في وسط منطقة البلقان، جنوب شرق أوروبا.

الزمان: ٢٨ شباط ١٩٩٨-١١حزيران١٩٩٩.

سبب وأحداث الحرب: قامت جمهورية يوغسلافيا السابقة (تتألف من جمهوريتي الجبل الأسود وصربيا) بالسيطرة على كوسوفو، نتيجة لذلك نشب نزاع مسلح بين جماعة متمردة ألبانية كوسوفية معروفة باسم "جيش تحرير كوسوفو" وبين قوات المسلحة اليوغسلافية وكانت هذه الجماعة مدعومة من حلف شمال الأطلسي الناتو. وجاء أول اشتباك عسكري كبير لحلف الناتو في أعقاب النمو الهائل للويب خلال التسعينيات، فمثلما كانت فيتنام أول حرب تلفزيونية في العالم، كانت كوسوفو أول حرب واسعة النطاق على الإنترنت [٣].

---

[١] الصادق، عادل عبد: الهجمات السيبرانية: أنماط وتحديات جديدة للأمن العالمي، موقع الموسوعة الجزائرية للدراسات السياسية والاستراتيجية، استرجعت بتاريخ٢٣/١/٢٠٢١، متاح على الرابط: https://cutt.ly/TjCJhVt

[٢] تغري، موسى بن: "الحرب السيبرانية والقانون الدولي الإنساني"، مجلة الاجتهاد القضائي، المجلد١٢، عدد خاص (العدد التسلسلي٢٢)، جامعة محمد خيضر بسكرة، الجزائر، نيسان، ٢٠٢٠، ص ص ١٩٩-٢١٨، ص ٢٠٥-٢٠٤، متاح على الرابط:

https://www.asjp.cerist.dz/en/article/112730

[3]Geers, Kenneth: Strategic Cyber Security, NATO Cooperative Cyber Defence Centre Of Excellence, Tallinn, Estonia, June 2011, P 81, Available At:

https://www.law.upenn.edu/institutes/cerl/conferences/cyberwar/papers/reading/Geers.pdf

خلال الهجمات الأولى لحلف الأطلسي على يوغسلافيا السابقة عام ١٩٩٩، حدث شيء غريب أدى إلى توقف الاتصالات، لم تُشاهد قنابل أو صواريخ في المجال الجوي، ولم يسمع أي صوت، إلا أن تفاصيله وضحت بعد فترة من إعلان وزارة الدفاع الأمريكية أن سلاحاً جديداً استخدم في أول الحرب لخلع الرئيس سلوبودان ميلوسيفيتش. وتم اختبار هذا الهجوم السيبراني المميز والجديد نوعياً لأول مرة في ساحة معركة حقيقة، وقد صمم الهجوم السيبراني في تلك الفترة لاستهداف شبكة الاتصالات وتعطيلها ما يؤدي تلقائياً لتوقف شبكات الجيش، وهذا ما حصل مع الجيش اليوغسلافي الذي تعطل نظام الكومبيوتر الأساسي لديه نتيجة ما أسماه الإعلام اليوغسلافي بصاعقة كهربائية دخلت شبكة الاتصالات وانتشرت في كل نقطة تتصل بها ومن ضمنها الكمبيوترات العسكرية، مما أدى إلى توقف نظم الكمبيوتر الخاصة بالدفاع الجوي، التي كانت مهمتها استهداف طائرات حلف الأطلسي بالصواريخ.

وأيضاً أدى الهجوم السيبراني إلى توقف الشبكة الهاتف الرئيسية في يوغسلافيا، مما دفع القيادة الصربية في بلجراد (عاصمة صربيا) إلى الاتصال بقواتها عن طريق الخلوي حيث تم رصد المكالمات ومراقبتها، والتجسس عليها من قبل مركز أيشيلون الأمريكي للتنصت والمراقبة الموجودة في أوروبا، وكانت مراقبة الاتصالات الخلوية أسهل لأن عدد حملة الهاتف المحمول في يوغسلافيا يومها كان يقتصر على أركان النظام الحاكم ورجال الأعمال، مما جعل عدد الهواتف المطلوب التنصت عليها محدوداً.

وخلال العمليات العسكرية والهجمات السيبرانية التي شنتها قوات حلف شمال الأطلسي ضد الصرب، استغلت الولايات المتحدة الأمريكية الهجوم السيبراني الذي عطل نظم الكمبيوتر الخاصة بالدفاع الجوي، وقصفت طائراتها الحربية محطات الكهرباء الصربية بقنبلة إلكترونية أدت إلى إغراق معظم أراضي يوغسلافيا السابقة في الظلام، وقد ألقتها طائرة أمريكية من طراز **(F117)** المعروفة باسم **(الشبح)** على خمس محطات طاقة صربية وعلى ارتفاع معين انفجرت القنبلة وخرجت منها ملفات سلكية خاصة انتشرت في الجو كشبكة واسعة فوق خطوط الضغط العالي فعطلتها، وأدى ذلك إلى اشتعال النيران في المحطات، وتوقفت مراكز توزيع الطاقة اليوغسلافية عن العمل. وتوجد داخل القنبلة **(CBU94)** عدة قنابل أخرى تنطلق من داخلها في الجو، وكل واحدة منها مزودة بمظلة صغيرة، ثم تخرج من هذ القنابل أيضاً ملفات مصنوعة من الرصاص الكربوني هي التي تكون الشبكة الإلكترونية عند اقترابها من الأرض بحيث تصيب محطات الطاقة الكهربائية بالدمار، وقد تأثرت الحياة المدنية أيضاً نتيجة لتوقف محطات الطاقة الكهربائية عن العمل [١].

---

[١] إبراهيم، طلال محمد الحاج: لهجمات السيبرانية على شبكات الحاسوب في ضوء القانون الدولي الإنساني، جامعة دمشق (كليه الحقوق –قسم القانون الدولي)، دمشق(سوريا)، إشراف الدكتورة مايا الدباس،٢٠٢٠، ص٨٤–٨٥.

وبدأت العديد من مجموعات الهاكرز الموالية للصرب (أو المعادية للغرب)، مثل "اليد السوداء"، في مهاجمة البنية التحتية للإنترنت لحلف الناتو، وكان هدفهم المعلن هو تعطيل العمليات العسكرية للناتو، إلا أنه من غير المعروف ما إذا كان أي من الهاكرز قد عمل بشكل مباشر مع الجيش اليوغوسلافي [١]. وقد أدى ذلك الهجوم السيبراني، من بين أمور كثيرة إلى غلق حساب البريد الإلكتروني للحلف لعدة أيام أمام الزوار الخارجيين والعطل المتكرر لموقع حلف الناتو. إلا أنه في ذلك الوقت كان يعتبر الهجوم السيبراني مجرد حملة لمنع معلومات الناتو. واعتبرت الهجمات السيبرانية، على أنها تهديد، ولكنها ذات نطاق محدود التدمير، مما تطلب في ذلك الوقت استجابات تقنية محدودة مع جهود معلوماتية بسيطة [٢].

وفي النزاع المسلح ذاته، وبعد استهداف طيران حلف شمال الأطلسي للسفارة الصينية في بلغراد، قام عدد من القراصنة الصينيين، وكردة فعل بمهاجمة مواقع إلكترونية رسمية تابعة للولايات المتحدة الأمريكية، وبالذات الموقع الإلكتروني للبيت الأبيض، نجم عنها الاستحواذ على الآلاف من البيانات الرقمية، المصنفة آنذاك بأنها عالية السرية [٣].

ثانياً_ الهجوم السيبراني من قبل الكيان الصهيوني على الجمهورية العربية السورية عام ٢٠٠٧

المكان: منطقة الكُبر بمحافظة دير الزور، شرقي الجمهورية العربية السورية.

الزمان: ٦ أيلول عام ٢٠٠٧.

سبب وأحداث الحرب: الجمهورية العربية السورية في حالة حرب مع الكيان الصهيوني منذ عام ١٩٤٨، وبتاريخ ٢١ آذار ٢٠١٨ اعترف جيش الكيان الصهيوني رسمياً بتدمير ما يشتبه أنه مفاعل نووي سوري في ضربة جوية عام ٢٠٠٧ قائلاً: "إن الضربة الجوية أزالت تهديداً كبيراً على إسرائيل والمنطقة وكانت "رسالة" إلى آخرين"[٤].

ففي السادس من أيلول عام٢٠٠٧ قصفت طائرات صهيونية من نوع (**Eagle F15**) و (**Falcon F16**) منشأة في منطقة "الكُبر بمحافظة دير الزور"، شمال شرق الجمهورية العربية السورية يقال أنها

---

[1]Geers, Kenneth: Strategic Cyber Security, op.cit, p 82.

[٢] التهديدات الجديدة: الأبعاد الإلكترونية، موقع مجلة الناتو، استرجعت بتاريخ٢٠٢١/١/١٢م، متاح على الرابط:
https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/AR/index.htm

[٣] الفتلاوي، أحمد عبيس نعمة: الهجمات السيبرانية (دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر)، مرجع سابق، ص ٣٠-٣١.

[٤] إسرائيل تعترف رسميا بتدمير مفاعل نووي سوري في ٢٠٠٧، موقع DW، استرجعت بتاريخ٢٠٢١/١/١٢، متاح على الرابط:
https://cutt.ly/9jbBBEj

كانت منشـــأة نووية من تصـــميم كوريا الشـــمالية تم بناؤها لمعالجة البلوتونيوم[١]، وقد اســـتطاعت تلك الطائرات تفادي كشفها بواسطة أنظمة الدفاع الجوي السوري، بسبب الاستخدام المزعوم لبرنامج سوتر من قبل الكيان الصـهيوني ضـد رادار الدفاع الجوي السـوري، مما سـمح للكيان الصـهيوني برؤية ما تراه أجهزة الاســتشــعار، ثم تولي البرنامج منصــب مســؤول أنظمة الدفاع الجوي الســوري ليتمكن من التلاعب بالمستشعرات، لكي لا تتمكن أنظمة الدفاع الجوي السوري من رؤية الطائرات المقتربة، ونتيجة لذلك ظلت طائرات الكيان الصــهيوني المســتخدمة في الهجوم غير مكتشــفة وتمكنت من تجاوز نظام الدفاع الجوي السـوري وقصـفت المنشـأة المشـتبه بها دون عوائق. وفي الواقع لا يزال من غير الواضـح بالضـبط كيفية عمل نظام **(Suter)**[٢]، لكن من المحتمل أنه جرى استغلال النبضات الضوئية والكهربائية الصادرة من الرادارات السورية لإرسال رسائل مكتوبة باللغة الرقمية الثنائية المكونة من رقمي "**1**" و"**0**" لغرض التحكم فيما تراه تلك الرادارات، فبدلاً من التشويش عليها تم التحكم فيما تراه.

ثالثاً_ الهجمات السيبرانية بين روسيا – جورجيا ٢٠٠٨

المكان: منطقة أوسيتيا الجنوبية وتقع وسط جورجيا من ناحية الشمال.

الزمان: من ٧ إلى ١٦ آب ٢٠٠٨.

سبب وأحداث الحرب: أعلنت أوسيتيا الجنوبية استقلالها عن جورجيا في عام ١٩٩١، لكنها ظلت معترف بها عموماً من قبل المجتمع الدولي كجزء لا يتجزأ من جورجيا. وفي أب ٢٠٠٨، اندلع نزاع مســـلح بين الاتحاد الروسـي وجورجيا حول أوسـيتيا الجنوبية، وبالتحديد بتاريخ ٧ آب ٢٠٠٨، شـنت القوات الجورجية هجوماً مفاجئاً على الانفصـاليين في أوسـيتيا الجنوبية، وأشـارت روسـيا إلى الالتزامات الوطنية بحماية المواطن الروسي في الخارج، وفي ٨ آب، ردت بعمليات عسكرية في الأراضي الجورجية. إلا أنه قبل بدء الغزو الروســي، كانت الهجمات الســيبرانية تُشــن بالفعل ضــد عدد كبير من المواقع الحكومية الجورجية وتكثف الهجوم السيبراني بمجرد بدء الأعمال العدائية المفتوحة بين روسيا وجورجيا، إلا أنه على الرغم من انتهاء العمليات العسكرية باتفاق وقف إطلاق النار في ١٢ آب، إلا أن الهجمات السيبرانية استمرت طوال

---

[1]Schreier, Fred: "On Cyberwarfare", Working Paper No. 7, DCAF Horizon, Geneva,2015, P110, Available At:
https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf

[2]Futte, Andrew: "Cyber Threats and Nuclear Weapons: New Questions for Command and Control, Security and Strategy", Occasional Paper, Royal United Services Institute for Defence and Security Studies, UK, July 2016, p31, Available at:
https://rusi.org/sites/default/files/cyber_threats_and_nuclear_combined.1.pdf

بقية الشهر[١]، ومن نتائج هذه الهجمات السيبرانية توقف شبكة الانترنت الجورجية عن العمل, وأصبح موقع الرئيس الجورجي غير متاح، وعندما أصبح متاحاً لاحقاً، تم اختراقه ووضع صورة الزعيم النازي أدولف هتلر، وفي الوقت نفسه، توقفت مواقع العديد من الوزارات والجهات الحكومية وتعرض أكبر بنك تجاري في جورجيا للهجوم، وتم تشويه المواقع العامة على الإنترنت، وتم توزيع قائمة بعناوين البريد الإلكتروني للسياسيين الجورجيين لإرسال رسائل غير مرغوب فيها[٢].

وقد حد هذا الهجوم الإلكتروني بنجاح وفعالية من قدرة الحكومة الجورجية على التواصل مع مواطنيها وكذلك المتعاطفين معها حول العالم. ويمكن القول إن الهجوم السيبراني كان على مرحلتين: أولاً، في الأيام التي سبقت الغزو التقليدي للقوات الروسية، عانت البنية التحتية الإلكترونية الجورجية من هجمات **(DDOS)** واسعة النطاق، مما أدى إلى تعطيل المواقع الحكومية الجورجية. بينما استمرت المرحلة الأولى، تزامنت المرحلة الثانية مع بدء الغزو الروسي التقليدي والبنية التحتية الاقتصادية المستهدفة مثل البنوك ووسائل الإعلام، مما حد من قدرة الحكومة الجورجية على نشر المعلومات لمواطنيها [٣].

ولم تكن معظم هذه الهجمات تدار من قبل القيادة العسكرية الروسية كما قد يتبادر إلى الذهن، بل الكثير منها تم الإعداد له علناً بين المتعاطفين مع روسيا من قراصنة الانترنت الروس أو ما يسمون" بالهاكرز Hackers"، فقد تنادوا تحت شعارات مثل " قف مع بلدك يا أخي"، أو " من أجل حماية روسيا والدفاع عنها"، أو ما شابه ذلك من شعارات [٤].

---

(1)Tikk, E &Others International Cyber Incidents: Legal Considerations, Cooperative Cyber Defence Centre Of Excellence, Tallinn, Estonia, 2010, P67-68, Available At: https://scholar.google.com/citations?user=8xfcsb8AAAAJ&hl=en

(2) Ibid, loc.cit.

(3) Bell, Cameron H.: "Cyber Warfare and International Law: The Need for Clarity", Towson University Journal of International Affairs, VOL. LI, NO.2, Spring 2018, PP 21-43, P30, Available At: https://cutt.ly/tkdz7dI

(٤) الصادق، عادل عبد: أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، سلسة أوراق العدد ٢٣، وحدة الدارسات المستقبلة مكتبة الإسكندرية، مصر(القاهرة)، ٢٠١٦، ص ٢٢٦، متاح على الرابط: https://cutt.ly/ekdbrXW

الفرع الثاني: تقييم انطباق القانون الدولي الإنساني على الهجمات السيبرانية في سياق النزاع المسلح

يخضع النزاع المسلح لقواعد ومبادئ القانون الدولي الإنساني من لحظة نشوء النزاع المسلح بين الطرفين، أما بالنسبة للهجمات السيبرانية التي تجري في سياق نزاع مسلح وتكون مرتبطة به، ينبغي ألا يثار أي جدل إزاء الرأي القائل بأن الهجمات السيبرانية حين تنفذ في سياق نزاع مسلح دائر، فإنها تخضع لقواعد القانون الدولي الإنساني ذاتها التي يخضع لها النزاع، ولتقييم انطباق القانون الدولي الإنساني على الحالات التطبيقية سالفة الذكر لابد من تقييمها تبعاً للمبادئ الرئيسية للقانون الدولي الإنساني.

أولاً_ تقييم انطباق القانون الدولي الإنساني على الهجمات السيبرانية في حرب كوسوفو عام ١٩٩٩

يكيّف النزاع المسلح بين الاتحاد الروسي ويوغسلافيا بأنه نزاع مسلح دولي، بالتالي انطباق قواعد القانون الدولي الإنساني عليه، ومن المتفق عليه أن الهجمات السيبرانية التي تجري في سياق نزاع مسلح قائم بالفعل يطبق عليها القانون الدولي الإنساني. ولكن لابد أيضاً من إسناد الهجوم وتحليل فيما إذا كانت الهجمات السيبرانية وصلت إلى حد استخدام القوة المسلحة وتسببت في أضرار مادية للممتلكات أو فقدان للأرواح أو إصابة للأشخاص؟ حتى نقول إنها وصلت إلى وصف النزاع المسلح الدولي وبالتالي يتم تطبيق القانون الدولي الإنساني عليها، سوف نبيين ذلك في كل حالة على حدة.

الحالة الأولى: الهجوم السيبراني من قبل حلف شمال الأطلسي(الناتو) على يوغسلافيا

يعد الهجوم السيبراني الذي تم من قبل الاتحاد الروسي أسلوب من أساليب القتال، فقد استغلت الولايات المتحدة هذا الهجوم من ناحيتين في رأينا:

الناحية الأولى: أدى الهجوم السيبراني إلى قطع الاتصالات، بالتحديد إلى قطع شبكة الهاتف الرئيسية مما أتاح للولايات المتحدة الأمريكية فرصة التجسس ومراقبة الاتصالات الخلوية التي كان يقتصر حامليها في تلك الفترة على أركان النظام الحاكم ورجال الأعمال، مما جعل عدد الهواتف المطلوب التنصت عليها محدوداً، إلا أن فعل التجسس ومراقبة الاتصالات في حد ذاته لا يسبب ضرر فعلي ولا يدخل في نطاق القانون الدولي الإنساني.

أما بالنسبة للناحية الثانية: أدى الهجوم السيبراني إلى توقف الشبكة الرئيسية في يوغسلافيا وتعطيل الكمبيوترات العسكرية وتوقف نظم الكمبيوتر الخاصة بالدفاع الجوي، التي كانت مهمتها استهداف طائرات حلف شمال الأطلسي بالصواريخ، واستغلت الولايات المتحدة الأمريكية هذا التعطيل وأرسلت طائرات حربية من نوع **(F117)** التي استهدفت خمس محطات طاقة صربية مما أدى إلى اشتعال النيران وتوقفت مراكز توزيع الطاقة عن العمل، إذا هذا الضرر المادي يدخل في نطاق استخدام الأعمال العدائية مما يؤدي إلى تطبيق قواعد القانون الدولي الإنساني وهي اتفاقيات جنيف الأربع لعام ١٩٤٩ والبروتوكول

الإضـــافي الأول لعام ١٩٧٧ والقانون الدولي الإنســـاني العرفي وبالإضـــافة لقانون حقوق الإنســـان وأي التزامات إضافية يتفق عليها أطراف النزاع باتفاقيات خاصة، ولتقييم انطباق القانون الدولي الإنساني على هذا الهجوم ينبغي تقييمه تبعاً للمبادئ الرئيسية للقانون الدولي الإنساني فيما يلي:

مبدأ التناسب بين الضرر والميزة العسكرية الأكيدة: يجب أن يكون المقصود من الهجوم على نظام أو شبكة تكنولوجيا معلومات الخصم أن يؤدي إلى تحقيق ميزة عسكرية أكيدة. لقد أدى الهجوم السيبراني إلى توقف الشـبكة الرئيسـية في يوغسـلافيا وتعطيل الكمبيوترات العسـكرية وتوقف نظم الكمبيوتر الخاصـة بالدفاع الجوي، التي كانت مهمتها اسـتهداف طائرات حلف الأطلسـي بالصـواريخ، واسـتغلت الولايات المتحدة الأمريكية هذا التعطيل وأرسـلت طائرات حربية من نوع **(F117)** التي اسـتهدفت خمس محطات طاقة صـربية مما أدى إلى اشـتعال النيران وتوقفت مراكز توزيع الطاقة عن العمل. فيمكن القول ان الميزة العسكرية من هذا الهجوم السـيبراني تحققت، إلا إن الضـرر الذي لحق بالمدنيين يتجاوز الميزة العسـكرية فقد تأثرت الحياة المدنية أيضاً نتيجة لتوقف محطات الطاقة الكهربائية عن العمل.

مبدأ التمييز بين المقاتلين وغير المقاتلين: كان الهجوم السـيبراني موجه إلى أنظمة الكمبيوتر بالتالي لم يكن هناك اسـتهداف للمقاتلين أو غير المقاتلين بشـكل خاص، وبناء على ذلك لم يكن هناك ضـرورة لتطبيق هذا المبدأ.

مبدأ التمييز بين الأعيان العسـكرية والأعيان المدنية: لقد تم اسـتهداف شـبكة الاتصـالات إلا أن هذه العين يمكن اعتبارها عين عسكرية تسهم مساهمة فعالة في العمل العسكري لأن أدى ذلك لتوقف شبكات الجيش اليوغسـلافي وتعطيل الكومبيوترات العسـكرية، وتوقف أنظمة الكومبيوتر الخاصـة بالدفاع الجوي، التي كانت مهمتها اسـتهداف طائرات حلف الأطلسـي بالصـواريخ. وكذلك تم اسـتهداف محطات الكهرباء الصـربية إلا أنه هذه العين هي أعيان مزدوجة كونها ذات اسـتخدامين عسـكري ومدني فهذه العين يمكن اعتبارها عين عسكرية تسهم مساهمة فعالة في العمل العسكري إلا أنه بالمقابل لقد لحق ضرر بالأعيان المدنية جراء هذا الاستهداف.

مبدأ الضـرورة العسـكرية: لقد أدى هذا الهجوم السـيبراني إلى توقف نظم الكومبيوتر الخاصـة بالدفاع الجوي، التي كانت مهمتها استهداف طائرات حلف الأطلسي بالصواريخ.

مبدأ الاحتياط لتجنب المحظورات: لم يتم مراعاة مبدأ الاحتياط لأن الهجوم قد سـبب أضـرار للأعيان المدنية نتائجه مفرطة مقارنة بالميزة العسكرية المرتقبة من الهجوم.

الحالة الثانية: الهجوم السيبراني من قبل مجموعات الهاكرز الموالية للصرب على حلف شمال الأطلسي (الناتو)

لابد بداية من إسناد الهجوم السيبراني، لقد تم من قبل مجموعات الهاكرز ومن غير المعروف ما إذا كان الجيش اليوغسلافي عمل بشكل مباشر مع هذه المجموعات، ولو فرضنا جدلاً أنه الجيش اليوغسلافي كان يعمل معهم، هل وصل الهجوم السيبراني إلى حد استخدام القوة المسلحة لكي يطبق عليها القانون الدولي الإنساني؟ أدى الهجوم السيبراني إلى تعطيل موقع حلف الناتو وإغلاق حساب البريد الإلكتروني لعدة أيام أمام الزوار، فغاية الهجوم السيبراني هو مجرد حملة لحجب معلومات الناتو وإعاقة الوصول إلى الموقع، إذاً لا ضرر فعلي يذكر، لا يوجد تدمير مادي أو إزهاق للأرواح، فلا يمكن وصفها بأنها تندرج تحت نزاع مسلح دولي وبالتالي لا يمكن تطبيق القانون الدولي الإنساني عليها، يمكن أن يطبق القانون الدولي لحقوق الإنسان فضلاً عن القانون المحلي للدولة المعنية.

الحالة الثالث: الهجوم السيبراني من قبل عدد من الهاكرز الصينيين على الولايات المتحدة الأمريكية

لابد أيضاً من إسناد الهجوم السيبراني وفي بيان ما إذا كان هناك استخدام للقوة المسلحة حتى يتم تضمينه تحت مظلة النزاع المسلح الدولي وبالتالي تطبيق القانون الدولي الإنساني عليهم. بالنسبة لإسناد الهجوم السيبراني قد تم من قبل عدد من الهاكرز الصينيين، وبالنسبة لاستخدام الأعمال العدائية، فالهجوم السيبراني لما يتسبب بضرر أو بتدمير للأعيان المدنية أو إزهاق للأرواح، فقط حصلوا أو سرقوا بيانات رقمية سرية، فلا يمكن وصفها بأنها تندرج تحت نزاع مسلح دولي وبالتالي لا يمكن تطبيق القانون الدولي الإنساني عليها، يمكن أن يطبق القانون الدولي لحقوق الإنسان فضلاً عن القانون المحلي للدولة المعنية.

ثانياً_ تقييم انطباق القانون الدولي الإنساني على حالة الهجوم السيبراني من قبل الكيان الصهيوني على الجمهورية العربية السورية عام ٢٠٠٧

ذكرنا سابقاً بأن الجمهورية العربية السورية والكيان الصهيوني في حالة إعلان حرب منذ عام ١٩٤٨ وبالتالي يوجد نزاع مسلح دولي، والهجوم السيبراني الذي حدث عام ٢٠٠٧هو أسلوب من أساليب القتال، لابد من إسناد الهجوم وتحليل فيما إذا كانت الهجمات السيبرانية وصلت إلى حد استخدام القوة المسلحة وتسببت في أضرار مادية للممتلكات أو فقدان للأرواح أو إصابة للأشخاص؟ حتى نقول إنها وصلت إلى وصف النزاع المسلح الدولي وبالتالي يتم تطبيق القانون الدولي الإنساني عليها، سوف نبيين ذلك فيما يلي.

بالنسبة إلى إسناد الهجوم السيبراني: في تاريخ ٢١آذار ٢٠١٨م اعترف الجيش الإسرائيلي رسميا بتدمير ما يشتبه أنه مفاعل نووي سوري في ضربة جوية عام ٢٠٠٧.أما بالنسبة للأضرار فقد تسبب

الهجوم السيبراني بأضرار مادية وذلك بتدمير المنشأة التي يشتبه بأنها منشأة نووية. وبالتالي يطبق على هذا الهجوم السيبراني قواعد القانون الدولي الإنساني وهي اتفاقيات جنيف الأربع لعام ١٩٤٩ والبروتوكول الإضافي الأول لعام ١٩٧٧ والقانون الدولي الإنساني العرفي وبالإضافة لقانون الدولي لحقوق الإنسان وأي التزامات إضافية يتفق عليها أطراف النزاع باتفاقيات خاصة، وسنقيم انطباق مبادئ القانون الدولي الإنساني فيما يلي.

مبدأ التناسب بين الضرر والميزة العسكرية الأكيدة: يجب أن يكون المقصود من الهجوم على نظام أو شبكة تكنولوجيا معلومات الخصم أن يؤدي إلى تحقيق ميزة عسكرية أكيدة. الهجوم السيبراني عن طريق استخدام برنامج سوتر أثر سلباً على رادار الدفاع الجوي السوري ونتيجة لذلك ظلت طائرات الكيان الصهيوني المستخدمة في الهجوم غير مكتشفة وتمكنت من تجاوز نظام الدفاع الجوي السوري وقصف المنشأة المشتبه بها دون عوائق وتحقيق الميزة العسكرية، فالضرر كان فقط على رادار الدفاع الجوي السوري والميزة العسكرية هي استهداف المنشأة ولولا هذا الهجوم السيبراني لتمكن الدفاع الجوي السوري من التصدي لهذه الطائرات وإحباط العملية.

مبدأ التمييز بين المقاتلين وغير المقاتلين: كان الهجوم السيبراني موجه إلى أنظمة الكمبيوتر بالتالي لم يكن هناك استهداف للمقاتلين أو غير المقاتلين بشكل خاص، وبناء على ذلك لم يكن هناك ضرورة لتطبيق هذا المبدأ.

مبدأ التمييز بين الأعيان العسكرية والأعيان المدنية: لقد تم استخدام برنامج سوتر من قبل الكيان الصهيوني ضد رادار الدفاع الجوي السوري فقط. أي أنه تم استخدامه فقط ضد أعيان عسكرية ولم يستخدم على أعيان مدنية.

مبدأ الضرورة العسكرية: لقد تم استخدام برنامج سوتر لهدف استهداف المنشأة خوفاً من أن يكون في منطقة الشرق الأوسط منشأة نووية في سوريا تهدد وجود أمريكا والكيان الصهيوني لذلك تم استهدافها، إلا أنه في الحقيقة ليست هناك ضرورية عسكرية لأنه لم يكن هناك معلومات أكيدة على أنها منشأة نووية وحتى لو كانت منشأة نووية فإن سوريا لم تقم بأي عمل عدائي باستخدام هذه المنشأة.

مبدأ الاحتياط لتجنب المحظورات: نظراً لأن استخدام برنامج سوتر كان فقط يستهدف رادار الدفاع الجوي السوري فيمكن القول إن مبدأ الاحتياط كان معمول به.

ثالثاً_ تقييم انطباق القانون الدولي الإنساني على الهجمات السيبرانية بين روسيا – جورجيا ٢٠٠٨

هناك هجمات سيبرانية حدثت قبل وأثناء العمليات العدائية الحركية التقليدية، وهناك عدد من التساؤلات تتبادر إلى الذهن متى بدأ بالضبط النزاع المسلح الدولي؟ هل بدأ بالهجمات السيبرانية التي حدثت قبل بدء العمليات العدائية الحركية؟ أما بدأ بالهجمات سيبرانية التي حدثت مع العمليات الحركية التقليدية؟ لأن تاريخ البدء هو ما يطبق عليه القانون الدولي الإنساني. وللإجابة عن هذه التساؤلات سوف نحلل الهجمات السيبرانية التي حدثت قبل بدء العمليات الحركية والهجمات السيبرانية التي حدثت أثناء العمليات الحركية فيما يلي.

١. الهجمات السيبرانية التي حدثت قبل بدء العمليات العدائية الحركية التقليدية

لبيان فيما إذا كانت الهجمات السيبرانية تشكل نزاع مسلح دولي وبالتالي يطبق عليها القانون الدولي الإنساني لابد من تحليل هذه الهجمات من ناحيتين.

الناحية الأولى: إسناد الهجوم السيبراني، هل كان الاتحاد الروسي وراء هذه الهجمات السيبرانية أم الهاكرز أم الجماعات مسلحة؟ لحد الآن لا يوجد دليل قاطع من كان وراء الهجمات السيبرانية التي حدثت قبل العمليات الحركية.

الناحية الثانية: هل الهجمات السيبرانية وصلت إلى حد استخدام القوة المسلحة وتسببت في أضرار مادية للممتلكات أو فقدان للأرواح أو إصابة للأشخاص؟ وبرأينا أنها لم تصل إلى حد النزاع المسلح لأنه لا يمكن اعتبار تشويه المواقع الحكومية أو أي مواقع أخرى على أنه يعزز العمليات العسكرية الروسية أو أن هناك ضرورة عسكرية لها، فمن المسلم به أن الهدف من الهجمات السيبرانية كان مجرد تعزيز شرعية الغزو الروسي الذي يبدو أنه يندرج ضمن مفهوم الحرب الدعائية التي لا يغطيها القانون الدولي الإنساني.

ونستنتج من ذلك أن الهجمات السيبرانية قبل بدء العمليات العدائية الحركية لا تندرج تحت مظلة القانون الدولي الإنساني، ولكن يمكن تطبيق القانون الدولي لحقوق الإنساني، فضلاً عن القانون المحلي للدولة.

٢. الهجمات السيبرانية التي حدثت أثناء العمليات العدائية الحركية التقليدية

لابد من الإشارة أن العمليات العدائية الحركية التقليدية التي حدثت بين الاتحاد الروسي وجورجيا هي نزاع مسلح دولي يطبق عليها القانون الدولي الإنساني حتماً. ومن المتفق عليه أن الهجمات السيبرانية التي تجري في سياق نزاع مسلح قائم بالفعل يطبق عليها القانون الدولي الإنساني. ولكن لابد أيضاً من إسناد الهجوم وتحليل فيما إذا كانت الهجمات السيبرانية وصلت إلى حد استخدام القوة المسلحة وتسببت

في أضرار مادية للممتلكات أو فقدان للأرواح أو إصابة للأشخاص؟ حتى نقول إنها وصلت إلى وصف النزاع المسلح الدولي وبالتالي يتم تطبيق القانون الدولي الإنساني عليها، سوف نبيين ذلك فيما يلي.

إن الهجمات السيبرانية التي حدثت أثناء العمليات الحركية أي في الفترة التي تم إجراؤها بين ٨ آب ووقف إطلاق النار في ١٢ آب، لا يوجد دليل قاطع على من كان وراءها، ولكن من أجل الجدل سنفترض أن الاتحاد الروسي كان وراءها. في هذا الوضع الافتراضي، سنجيب على التساؤل الثاني، لقد تم بسبب الهجمات السيبرانية إيقاف تشغيل موقع الرئيس، وتم جعله يظهر على أنه هتلر، وتعرض البنك ومواقع الويب الحكومية للهجوم السيبراني، بالإضافة إلى بوابات الأخبار، ونظراً لانخفاض الاعتماد الإجمالي للسكان الجورجيين على الخدمات عبر الإنترنت، فقد كان فقط ٧٪ من سكان جورجيا إمكانية الوصول إلى الإنترنت خلال ذلك الوقت وهو ما يشير بحد ذاته إلى أن مثل هذا المجتمع لا يعتمد على الإنترنت وطبيعة مواقع الويب التي تمت مهاجمتها ليست ضرورية للاستقرار الاقتصادي، فالضرر كان فقط على هذه المواقع المحدد، وتأثير الهجمات السيبرانية لم يكن خطيراً بما يكفي بحيث يصل إلى حد الضرر الاقتصادي الشديد أو المعاناة الإنسانية الكبيرة، كما أن لا شيء من هذه الأشياء خدم كهدف عسكري. لم يقدموا مساهمة فعالة في العمل العسكري، كما أن تعطيلهم لم ينتج عنه ميزة عسكرية أكيدة. وكان من الأمثل لأجل اعتبار الهجوم السيبراني له ميزة عسكرية ويؤثر سلباً على العمليات العسكرية لأحد الأطراف المتحاربة، أن يتوقع على سبيل المثال: محاولة تعطيل الاتصال والتنسيق بين القوات أو التدخل في نظام التحكم في الدفاع الجوي. ومع ذلك، لا يبدو أن أياً من هذه الافتراضات موجود في هذه الحالة. فلا يمكن افتراض أن القانون الدولي الإنساني قابل للتطبيق في الحالة الجورجية.

المطلب الثاني: الهجمات السيبرانية خارج سياق النزاع المسلح

لا يتم شن الهجمات السيبرانية بالضرورة في أثناء نزاع مسلح قائم بالفعل، بل نتيجة التطور التكنولوجي والاعتماد الشامل على أجهزة الحاسوب وشبكات الاتصالات، يمكن أن نجد لها مجال تطبيقي واسع في كل الأوقات، فقد تستخدم هذه الهجمات في أوقات السلم، كاستخدامها نتيجة توتر سياسي أو اقتصادي بين بلدين أو لانتهاج سياسة معينة غير محبذة من قبل دولة أخرى أو لأسباب كثيرة أخرى. وقد تستهدف الهجمات السيبرانية البنى التحتية للمعلومات والانترنت أو توجه ضد البنى التحتية الحرجة المعتمدة على شبكات الحاسوب والانترنت في تشغيلها وعملها، وقد تستهدف القطاع الخاص من شركات ومصارف. وهناك إجماع بين المختصين في القانون الدولي الإنساني بأن الهجمات السيبرانية التي تتم خارج نزاع مسلح حركي قائم ليس من الشرط أن ينظمها القانون الدولي الإنساني، ويذهب إلى ذلك "لوران جيزيل" المستشار القانوني للجنة الدولية للصليب الأحمر بقوله: "لا يعني ذلك إن القانون الدولي الإنساني

ينطبق على كافة العمليات الإلكترونية أو كل ما يطلق عليه "الهجمات السيبرانية" في اللغة الشائعة، فالقانون الدولي الإنساني لا ينظم العمليات الإلكترونية التي تقع خارج سياق النزاع المسلح"[١].

لكن على الرغم من ذلك تجدر الإشارة إلى أن اتفاقيات جنيف لعام ١٩٤٩ استبدلت مصطلح "الحرب" المستخدم في اتفاقيات لاهاي بمصطلح "النزاع المسلح" من أجل توسيع النطاق المادي لتطبيق الاتفاقيات وجعل القانون الدولي الإنساني قابلاً للتطبيق بناء على تقييم واقعي لكل حالة. ووفقاً لدائرة الاستئناف التابعة للمحكمة الجنائية الدولية ليوغسلافيا السابقة في قضية تاديتش، لكي نكون أمام نزاع مسلح دولي يجب توافر عنصرين: (١) نزاع بين دولتين على الأقل؛ (٢) ولجوئهما إلى القوة المسلحة ضد بعضهما البعض. ولا يقصد باللجوء إلى القوة المسلحة أن تقوم الدولة باستخدام قواتها المسلحة، إنما اللجوء إلى الأعمال العدائية الحربية ضد دولة أخرى. وهذا ما تبناه دليل تالين، حيث نص على أنه" يوجد نزاع مسلح دولي عندما تكون هناك أعمال عدائية، والتي قد تشمل أو تقتصر على العمليات السيبرانية، التي تحدث بين دولتين أو أكثر"، حيث يقصد ب "الأعمال العدائية التطبيق الجماعي لوسائل وأساليب الحرب". ويعتمد تطبيق القانون الدولي الإنساني على الحالة الواقعية وليس على إدراك حالة النزاع المسلح من جانب الأطراف فيه[٢]، فإذا نفذ عملاء المخابرات المدنية بعمليات سيبرانية تصل إلى حد القوة المسلحة، وتسبب أو من المحتمل أن تتسبب في أضرار مادية للممتلكات أو فقدان الأرواح أو إصابة الأشخاص فقد يكون هناك نزاع مسلح، وإذا أمكن إثبات نسب الهجمات السيبرانية إلى دولة معينة لكان من الممكن انطباق القانون الدولي الإنساني كما لو تم تنفيذ الهجوم بوسائل حركية من ناحية أخرى، أما إذا كانت القوات المسلحة تشارك فقط في أنشطة تجسس أو أعمال شغب وتخريب دون التسبب بضرر مادي حقيقي، فلا يمكن القول بأنها ترقى إلى نزاع مسلح في غياب الأعمال العدائية المتزامنة. بالمقابل لو أن مثل هذا الهجوم السيبراني استهدف مثلاً شبكة الكهرباء الوطنية واستمر لفترة طويلة، مع تداعيات سلبية شديدة على توفير الخدمات الطبية والنقل والأسواق المالية والأمن فيمكن اعتبار مثل هذه الهجمات أعمال عدائية ترقى إلى استعمال القوة المسلحة، وإذا أمكن نسب هذه الهجمات السيبرانية لدولة معينة أو مجموعة مسلحة لأمكن انطباق القانون الدولي الإنساني عليها [٣]. وانطلاقاً من ذلك سوف نقسم هذا المطلب إلى فرعين، نبين في الأول الحالات التطبيقية للهجمات السيبرانية التي تحدث خارج سياق النزاع المسلح، أما الثاني سنتناول تقييم انطباق القانون الدولي الإنساني على هذه الهجمات السيبرانية.

---

[١] كلنتر، زهراء عماد محمد: المسؤولية الدولية الناشئة عن الهجمات السيبرانية، مرجع سابق، ص ٤٢-٤٤.

[٢] دوريجي، كودولار: "لا تقترب من حدود فضائي الإلكتروني: الحرب الإلكترونية والقانون الدولي الإنساني وحماية المدنيين"، مرجع سابق، ص ٥٤٣.

[٣] حمدان، إيمان: التكنولوجيا الجديدة والقانون الدولي الإنساني (الحرب السيبرانية)، مرجع سابق، ص ٦.

الفرع الأول: حالات تطبيقية للهجمات السيبرانية خارج سياق النزاع المسلح

قد تحدث الهجمات السيبرانية في ساحة منفردة وغير متوازية مع الأعمال العسكرية التقليدية، أي تحدث في حالة لا يكون فيها حرب تقليدية أو أي نزاع مسلح، ولكن هذه الهجمات السيبرانية إذا كانت ترقى إلى مستوى نزاع مسلح، وتسببت في أضرار مادية للممتلكات أو فقدان للأرواح أو إصابة الأشخاص وكان في الإمكان إثبات نسبة الهجمات السيبرانية إلى دولة معينة فعندئذ نطبق القانون الدولي الإنساني، أما إذا كان من الصعب إثبات نسبة الهجوم السيبراني إلى دولة معينة لا يمكن تطبيق القانون الدولي الإنساني عليها وعوضاً عن ذلك يمكن تطبيق القانون الدولي لحقوق الإنسان فضلاً عن القانون المحلي للدولة المعنية وتاريخياً نجد حالات تطبيقية لهجمات السيبرانية تحدث خارج سياق نزاع مسلح مثل الهجمات السيبرانية بين الصين والولايات المتحدة الأمريكية، وأيضا برزت خلال الهجوم السيبراني على استونيا عام ٢٠٠٧، وكذلك الهجوم السيبراني على المنشآت النووية الإيرانية، وسوف تتم دراسة هذه الحالات التطبيقية فيما يلي.

أولاً_ الهجمات السيبرانية بين الصين– الولايات المتحدة الأمريكية

المكان: الولايات المتحدة الأمريكية.

الزمان: لا يوجد تاريخ محدد معلن عنه لهذه الهجمات، ولكن يمكن القول من عام ٢٠٠٧ حتى يومنا الحالي.

سبب وأحداث الهجوم: منذ تأسيس جمهورية الصين الشعبية عام ١٩٤٩، اتسمت العلاقة بين الولايات المتحدة والصين بقدر كبير من الصراع والتحدي والريبة الاستراتيجية. وقد ازداد ثقل التوترات التي تفرق بين البلدين في السنوات الأخيرة. وللأسف، تنعكس هذه التوترات على الفضاء السيبراني بقدر ما تنعكس على العلاقات في العالم الفعلي. وفي الواقع، من بين جميع المجالات التي اضطربت فيها العلاقة بين الطرفين، كان مجال الفضاء الإلكتروني أكثرها إثارة للخلاف [١]. ومن الأمثلة الأكثر وضوحاً للهجمات السيبرانية بين الصين والولايات المتحدة الدالة على قدرة هذه الهجمات في التجسس والحصول على وثائق سرية حكومية وتجارية وعسكرية ما يلي:

- **عام ٢٠٠٧** ذكر بول ستراسمان **(Paul Strasmann)** الخبير الأمريكي في أمن المعلومات أن عدد ٧٣٥.٥٩٨ جهاز كمبيوتر في الولايات المتحدة قد تم محاولة كسر شفرتها من جانب المخابرات الصينية، وأشارت بعض التقارير أن شبكة تجسس على الشفرة يطلق عليها اسم **(Ghost Net)**

---

[١] هارولد، سكوت وارين وآخرون: التوصل إلى اتفاق مع الصين بشأن الفضاء الإلكتروني، مؤسسة (RANDA)، سانتا مونيكا، كاليفورنيا،٢٠١٦، ص ٤، متاح على الرابط: https://cutt.ly/PkdRw3m

تستخدم قواعد بيانات مقرها الصين، قد استطاعت الحصول على وثائق سرية حكومية وتجارية في ١٠٣ دولة، ولكن الحكومة الصينية نفت هذه البيانات [١].

- وفي كانون الأول ٢٠٠٩ وكانون الثاني ٢٠١٠ انطلق من الصين هجوم شفري عرفت باسم عملية أورورا **(Operation Aurora)** موجه ضد شركة جوجل وعشرين شركة أخرى، وقد وصفت شركة **(McAfee)** أن هذا الهجوم هو الأعلى نوعياً من حيث التقنية في ذاك الوقت [٢].
- وفي أيار ٢٠١٤ أدانت المحكمة الفيدرالية العليا الأمريكية خمسة ضباط جيش صينيين بارتكاب جرائم في مجال الشفرة وسرقة معلومات سرية ذات طبيعية تجارية. كما تضمنت لائحة الاتهام أنهم اخترقوا (٦) أجهزة كمبيوتر لشركات أمريكية وذلك لغاية سرقة معلومات سرية لصالح شركات صينية منافسة. وقالت الحكومة الصينية بأن هذه الاتهامات ملفقة وأن من شأنها الإضرار بالثقة بين الدولتين [٣].
- وفي تشرين الثاني ٢٠١٧ اتهمت وزارة العدل الأمريكية ثلاثة موظفين صينيين من شركة تكنولوجيا المعلومات **(Guangzhou Bo Yu Information Technology Company Limited)** باختراق شركات أمريكية تعمل داخل الولايات المتحدة منها **(Moodys Analytics)** **(Trimble Inc),(Siemens) (AG)**[٤].
- واتهم جيش التحرير الشعبي **(The Peoples Liberation Army) (PLA)** بالجاسوسية الاقتصادية من خلال سرقة خطط أعمال تجارية وتنصت على شركات **Westinghouse (Electric)** و**US Steel Corporation)** . وقد استطاعت المخابرات الصينية اختراق أجهزة كمبيوتر هيئات عسكرية أمريكية، وقام عملاؤها بسرقة معلومات عن نظام صواريخ باتريوت**(Patriot Missile System)** والطائرة المقاتلة **(F-35 Joint Strike Fighter)** والسفينة الحربية الجديدة **(Littoral)** وذلك في إطار عملية تطوير وتحديث التسليح الصيني[٥].

---

[١] الخولي، محمود إسماعيل: قضايا الخيانة والجاسوسية الجاسوسية والوعي الأمني، العربي، القاهرة، ٢٠١٩، ص١٥٣، متاح بشكل جزئي على الرابط: https://cutt.ly/NkdF1ow

[٢] المرجع السابق، ص ١٥٤.

[٣] المرجع السابق، نفس الموضع.

[٤] المرجع السابق، نفس الموضع.

[٥] المرجع السابق، ص١٥٥.

ثانياً_ الهجوم السيبراني على استونيا عام ٢٠٠٧

المكان: استونيا.

الزمان: عام ٢٠٠٧.

سـبب وأحداث الهجوم: تعد اسـتونيا من الدول المتقدمة في مجال تكنولوجيا الاتصـال والمعلومات حيث شهد ذلك القطاع نمواً منذ عام ٢٠٠٠ وفي عام ٢٠٠٧ أصبح ٥٢٪ من السكان يستطيعون الدخول إلى الانترنت وأصـبحت وزارة الدفاع الاسـتونية، بالإضـافة إلى العديد من الخدمات الحكومية ودفع الضـرائب وغيرها تعتمد على الفضاء السيبراني [١].

ومنذ استقلال جمهورية استونيا وعاصمتها تالين بعد تفكك الاتحاد السوفيتي سابقاً، ازداد التوتر بين السكان الأصليين لإستونيا وبين من استقر فيها وحمل جنسيتها من المواطنين ذوي الأصول الروسية، وفي شهر شباط ٢٠٠٧ أصدر المجلس التشريعي لإستونيا قانوناً يقضي بإزالة كل الأبنية التي أقيمت في الفترة التي كانت فيها إسـتونيا ضـمن دول الاتحاد السـوفييتي سـابقاً بما في ذلك التمثال البرونزي الضـخم في إحدى الميادين بوسط العاصمة الاستونية، وهو نصب تذكاري لجندي سوفييتي يمثل ذكرى مشاركة القوات السوفييتية في الحرب العالمية الثانية.

وبعد اعتراض الروس على ما اعتبروه تدنيساً لذكرى الأبطال السـوفييت الذين قضـوا نحبهم، استقر الأمر على قرار نقل التمثال إلى مقبرة تابعة للجيش، إلا أن هذا الإجراء كان أبعد ما يكون عن إخماد النزاع [٢]، فقد كانت نتيجة هذا القرار ليلتين من الاحتجاجات الجماهيرية وأعمال الشـــغب في إســـتونيا المعروفة باسم "الليلة البرونزية". ففي الأسابيع التي أعقبت الليلة البرونزية، تعرضت البنية التحتية الرقمية لإسـتونيا لهجوم إلكتروني هائل. اسـتخدم "الهاكرز" هجمات رفض الخدمة **(DDoS)** الهائلة لاسـتهداف خوادم الويب في إســـتونيا وإيقاف حركة مرور الويب، وشـــملت الأهداف [٣] الخدمات الحكومية اليومية والمواقع الإخبارية والمصـرفية والتجارة الإلكترونية. ولابد من الإشـارة أن هذا النوع من الهجمات السـيبرانية يثقل كاهل الشـبكات بالطلبات حتى تتعطل الشـبكة، مما يؤدي إلى "رفض" الوصـول إلى تلك الشـبكة أو الخدمة حتى يتوقف الهجوم [٤].

---

[١] الصادق، عادل عبد: أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مرجع سبق ذكره، ص٢٢٠.

[٢] إبراهيم، طلال محمد الحاج: مرجع سبق ذكره، ص٨٨-٨٧.

[3] Gervais, Michael: "Cyber Attacks and The Laws of War", op.cit, p13.

[4] Bell, Cameron H.: "Cyber Warfare and International Law: The Need for Clarity", op.cit, p27.

وعلى الرغم من تتبع السلطات الإستونية لبعض هجمات **(DDOS)** إلى عنوان مرتبط بالحكومة الروسية، إلا أن روسيا نفت أي مسؤولية رسمية عن الهجوم على إستونيا، مشيرة إلى أن الهجوم جاء من ناشطين خاصين موالين لروسيا، وأحدثت تلك الهجمات صدى واسعاً حيث أنه وللمرة الأولى واجهت "استونيا" هجوماً مباشراً، استهدف مواقع الانترنت الخاصة بالبنوك والوزارات والصحف وأجهزة الإعلام، مما أدى إلى عزل استونيا عن العالم الخارجي، وعن استخدام الوسائل التي تمكنها من الكشف عن أنها تتعرض للهجوم، وكانت تلك الضربات غير تمييزية. ومثل ذلك نقلة نوعية كبيرة في مجال استخدام شبكات الانترنت كمجال جديد للحرب غير التقليدية بطريقة متطورة ومعقدة لم يسبق لها مثيل، وتغيرت التكتيكات مع ظهور نقاط الضعف. وتم توجيه قنابل ذات حجم تصل إلى مئات من الميجا بايت إلى عنوان واحد، ثم لعنوان آخر، وهكذا. ولم تعلن أي دولة أو جماعة المسؤولية عن ذلك الهجوم ويدفع تعقد الهجوم للاعتقاد بأنه على الأقل يمثل جهوداً تتجاوز مهارات الأفراد أو الجريمة المنظمة ذاتها ويتطلب تعاوناً من قبل الدولة وشركة اتصالات ضخمة، ونظراً لأن استونيا تعد واحدة من أكثر الدول المتطورة في أنظمة اتصالاتها في أوروبا فقد تمكنت من اجتياز تلك الأزمة، ولكن دولاً أخرى كانت ستدفع ثمناً باهظاً إذا ما تعرضت لهجوم مشابه [١].

ثالثاً_ الهجوم السيبراني على المنشآت النووية الإيرانية

المكان: مدينة نطنز في محافظة أصفهان، جنوب العاصمة طهران.

الزمان: من نهاية عام ٢٠٠٩ إلى منتصف عام ٢٠١٠.

سبب وأحداث الهجوم السيبراني : أراد الرئيس بوش في عام ٢٠٠٦ إخراج البرنامج النووي الإيراني عن مساره أو إبطائه ومع ذلك، لم يرغب الرئيس بوش في شن غارات جوية على منشأة تخصيب اليورانيوم الإيرانية بدلاً من ذلك، سعى إلى خيار بين عدم القيام بأي شيء والهجوم الحركي، واستقر الأمر بهجوم سيبراني يستهدف أنظمة التحكم في الكمبيوتر في منشأة نطنز وبدأ العمل على تصميم فيروس ستاكسنت وتطويره من قبل الولايات المتحدة الأمريكية والكيان الصهيوني[٢]، وبعد تولي الرئاسة من قبل الرئيس أوباما، تعرضت إيران لهجوم سيبراني من قبل الولايات المتحدة الأمريكية وسلطة الاحتلال لمدة ٩ أشهر من نهاية عام ٢٠٠٩ إلى منتصف عام ٢٠١٠، وكانت الغاية من هذا الهجوم التسلل إلى أنظمة السيطرة

---

[١] الصادق، عادل عبد: أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مرجع سابق، ص٢٢١-٢٢٢.

[2]Wallace, David A. & Jacobs, Christopher: "Conflict Classification and Cyber Operations: Gaps, Ambiguities and Fault Lines", U. Pa. J. Int'l L, Penn Law: Legal Scholarship Repository, Vol. 40:3,2019, PP645-692, P655, Available At:
https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1985&context=jil

المستخدمة في أهم المنشآت النووية الإيرانية **(نطنز وبوشهر)** وتدميرها. وقد تم هذا الهجوم عن طريق فيروس **(Stuxnet)** الذي صمم لكي ينتشر بصورة سريعة مستهدفاً المنشآت النووية الإيرانية وبالأخص محطة نطنز لتخصيب اليورانيوم، ولكن دون التسبب بأضرار للمنشآت الأخرى. وبما أن محطة نطنز غير مرتبطة بشبكة الإنترنت، تم نشر وتسريب فيروس **(ستاكسنت)**، من خلال **(USB Flash Drive)** في الحواسيب عبر تعاون أمني أميركي إسرائيلي هولندي، ومع ذلك، لم تؤكد أي دولة من الدول المذكورة حتى الآن مشاركتها [١].

وعند دخول فيروس ستاكسنت لأي حاسوب يبدأ في البحث عن أنواع محددة من أنظمة التحكم لكي يهاجمها، وفي حالة عدم الكشف عن أي من الأنظمة التي برمج لاستهدافها يصبح **(Stuxnet)** غير فعال في الحاسوب ما عدا عملية نقل الفيروس للغير، أما عندما يكشف عن أي من الأنظمة التي برمج لاستهدافها، يقوم بإدخال أوامر وبرامج فاسدة لكي يغير الشفرات، ويعطي أوامر خاطئة وغير متوقعة. ولفيروس **(Stuxnet)** ثلاث وحدات أو أجزاء: الأولى: الوحدة التي تنفذ جميع الأعمال التخريبية والخبيثة، الثانية: الوحدة التي تنسخ الفيروس وتعمل على انتشاره، الثالثة: الوحدة التي تكون مسؤولة عن إخفاء الملفات والعمليات الخبيثة، وتعمل هذه الوحدات المكونة لهذا الفيروس كلها وفق نظام يعرف ب **(Zero-Day)**، ويعمل **(Stuxnet)** على مرحلتين: الأولى مرحلة السيطرة على نظام التحكم الموجود في أجهزة القيادة والسيطرة في المنشأة، واستخدام الحواسيب المربوطة بهذه الأنظمة للدخول في نظام"Scada"، والبحث عن شفرات موجودة فقط في أنظمة "Scada" الموجود في المحطات النووية الإيرانية، وتتم المرحلة الثانية بعد التحقق من ان الفيروس وصل للهدف المقصود، يبدأ بعمليات التخريب والتلاعب في أجهزة الطرد المركزية عن طريق زيادة السرعة والضغط وتقليلها في الأجهزة، إلى أن يتم تعطيلها وتخريبها. وصمم **(Stuxnet)** لكي يخدع المهندسين في غرفة السيطرة والتحكم عن طريق إرسال بيانات تتطابق مع عمل أجهزة الطرد المركزي الاعتيادية والسليمة، في حال لم تكن هي كذلك، ومنع أنظمة السلامة من توقيف العمليات غير الآمنة.

يمثل هذا الهجوم شكلاً جديداً وأكثر عدوانية من الهجمات السيبرانية السابقة، ليس فقط في التسبب بتعطيل ٣٠ ألف جهاز كمبيوتر للمنشآت الصناعية في إيران وحوالي ٤٥ ألف جهاز كمبيوتر حول العالم[٢]، والتسبب في إبطاء شبكة نظام المفاعلات النووية فحسب، بل أيضاً في التسبب بأضرار مادية حقيقية للمفاعلات النووية الإيرانية حيث تم تقييم الأضرار حوالي ١٠٠٠ جهاز طرد مركزي، وهي حقيقة

---

[١] الزاهد، مسعود: إيران.. حريق نطنز يعطل وحدة جديدة من أجهزة الطرد المركزي، الرابط الالكتروني لموقع قناة العربية، استرجعت بتاريخ٧/١/٢٠٢٠م: https://cutt.ly/Tjb5XH8

[٢] طهران تقر بإصابة بعض أجهزة الكمبيوتر الشخصية في بوشهر بفيروس، موقع BBC News، استرجعت بتاريخ٢٣/١/٢٠٢١، متاح على الرابط: https://cutt.ly/8jVinVm

تشير إلى أنه لا يكفي استخدام الوسائل المالية والتقنية لإصلاح الضرر فحسب، بل يحتاج أيضاً لوقت طويل وجهد بشري كبير، كما لو تم قصف أجهزة الطرد المركزي[1].

الفرع الثاني: تقييم انطباق القانون الدولي الإنساني على الهجمات السيبرانية خارج سياق النزاع المسلح

بالطبع لا يطبق القانون الدولي الإنساني خارج سياق النزاع المسلح، ولكن إذا حدث هجوم سيبراني سبب أو من المحتمل أن يسبب في أضرار مادية للممتلكات أو فقدان للأرواح أو إصابة للأشخاص يمكن أن ترقى هذه الهجمات السيبرانية إلى وصف نزاع مسلح، قياساً على الهجمات العدائية الحركية التي ترقى إلى نزاع مسلح ويطبق عليها القانون الدولي الإنساني. لذلك وانطلاقاً من هنا، سوف نقوم بتقييم الحالات السالفة الذكر ونرى هل بالإمكان أن ترقى تلك الهجمات السيبرانية إلى وصف نزاع مسلح دولي أم نزاع مسلح غير ذي طابع دولي وبالتالي انطباق القانون الدولي الإنساني ومبادئه عليها، أم مجرد أنها توترات واضطرابات وأعمال شغب وبالتالي لا ينطبق القانون الدولي الإنساني عليها.

ولبيان ذلك لابد من طرح هذه التساؤلات التالية:

١. هل يمكن إسناد الهجوم السيبراني إلى دولة أو إلى مجموعات مسلحة؟
٢. هل يمكن أن يتم وصف الهجوم السيبراني على أنه نزاع مسلح دولي أم نزاع مسلح غير طابع دولي أم أنه مجرد توترات وأعمال شغب؟

وسوف نقوم بطرح هذه التساؤلات على الحالات السالفة الذكر والإجابة عليها تبعاً لكل حالة على حدة.

أولاً_ تقييم انطباق القانون الدولي الإنساني على حالة الهجمات السيبرانية بين الصين والولايات المتحدة الأمريكية

كانت أصابع الاتهام توجه إلى الصين بسبب الهجمات السيبرانية التي كانت تحصل في الولايات المتحدة إلا أن الصين كان تنفي مثل هذه التهم ولم تعترف بها، وعلقت الحكومة الصينية بأن مثل هذه الاتهامات من شأنها الإضرار بالثقة بين الدولتين. أما بالنسبة لوصف أنه يوجد نزاع المسلح فإن الهجمات السيبرانية كانت غايتها فقط التجسس والحصول على معلومات سرية دون التسبب في أضرار مادية للممتلكات أو فقدان للأرواح أو إصابة الأشخاص، إذاً لا يمكن أن ترقى أعمال التجسس وسرقة المعلومات

---

[1] Linaki, Evangelia: Cyber Warfare and International Humanitarian Law: A Matter of Applicability, Journal of International Law of Peace and Armed Conflict (German Red Cross), Volume 27,4/2014, PP169-175, P175, Available At: https://cutt.ly/QkdZQQn

السرية إلى مستوى نزاع مسلح وبالتالي من غير الجائز تطبيق القانون الدولي الإنساني، عوضاً عن ذلك يمكن تطبيق القانون الدولي لحقوق الإنسان فضلاً عن القانون المحلي للدولة.

ثانياً_ تقييم انطباق القانون الدولي الإنساني على حالة الهجوم السيبراني على استونيا عام ٢٠٠٧

في الوضع الاستوني، لا يوجد دليل على أن الاتحاد الروسي كان وراء الهجمات، أو أنه سيطر على نشطاء القرصنة، لذلك لا يمكن أن يكون هناك نزاع مسلح دولي على هذا الأساس. ولكن من أجل الحجج سوف نفترض جدلاً أن هذه الهجمات نفذها الاتحاد الروسي، هل سيصلون إلى عتبة النزاع المسلح؟ من الواضح أنه تم إطلاق العمليات بقصد عدائي، لكن تشويه المواقع الحكومية وإرسال رسائل البريد الإلكتروني العشوائية لا ترقى إلى مستوى استعمال قوة مسلحة، فالعواقب كانت ضئيلة ولم يكن هناك ضرر جسدي أو تدمير مادي، وفي الغالب تسببت هذه الهجمات في إزعاج مؤقت نفسي، إذاً هذه الهجمات لم تصل إلى عتبة نزاع مسلح. ولكن في الحقيقة هناك بعض الحجج التي تفيد بأن هجمات DDoS على إستونيا ربما تكون قد ارتقت إلى مستوى "النزاع المسلح". ومن أهم هذه الحجج كثافة الهجمات وطول أمدها، لأن معظم هجمات **(DDoS)** بالعادة لا تدوم أكثر من بضعة أيام، لكن هذا الهجوم استمر عدة أسابيع، واستهدف القطاعين العام والخاص، بالنسبة لدولة مثل إستونيا تعتمد على الانترنت في تعاملاتها، فإن الهجمات السيبرانية المستمرة لمدة أسبوعين هي أكثر من مجرد إزعاج. وفي حال لم تكن إستونيا متطورة وماهرة في الدفاع عن نفسها كما ثبت، لكانت هجمات **(DDoS)** لعام ٢٠٠٧ أكثر تدميراً، ومع ذلك، فإن الأدلة المتاحة تتعارض مع مثل هذه الحجج [١]. ومنه نستنتج أنه لم تشكل الأعمال العدائية "التطبيق الجماعي لوسائل وأساليب الحرب" التي وقعت في إستونيا دليلاً كافياً للقول بأنه يوجد "نزاع مسلح". وبالتالي، لا يمكن وصف حادثة إستونيا على أنها نزاع مسلح دولي. وأيضا ليس نزاع مسلح غير ذي طابع دولي لأن حسب تعليق اللجنة الدولية للصليب الأحمر على المادة الثالثة المشتركة من اتفاقيات جنيف الأربعة إذا كانت الهجمات السيبرانية تقتصر فقط على إعاقة وظائف الانترنت أو استغلال الشبكات أو سرقة البيانات أو حذفها أو إتلافها، فمن غير المرجح الوصول إلى درجة شدة العنف التي تقتضي توافرها في القانون الدولي الإنساني.

وقد وصف أحد المعلقين على الهجمات السيبرانية التي حصلت في استونيا بأنها "أشبه بأعمال شغب سيبرانية أكثر من كونها هجوماً عسكرياً"[٢].

---

(1)Wallace ,David A & Jacobs, Christopher W: "Conflict Classification and Cyber Operations: Gaps, op.cit, P673.

(2)Gervais, Michael: "Cyber Attacks and The Laws of War", op.cit, P540.

إذاً إن هذه الهجمات السيبرانية لا ترقى إلى مستوى النزاع المسلح، وبالتالي لا يمكن تطبيق القانون الدولي الإنســاني عليها، إلا أن ذلك لا يعني وجود فراغ أو ثقب أســود في القانون الدولي، فيمكن تطبيق القانون الدولي لحقوق الإنسان فضلاً عن القانون المحلي للدولة في وقت السلم.

ثالثاً_ تقييم انطباق القانون الدولي الإنســاني على حالة الهجوم الســيبراني على المنشــآت النووية الإيرانية

على الرغم من عدم إعلان أي شـخص مسؤوليته على الهجوم السـيبراني الذي اسـتهدف المنشـآت النووية الإيرانية، إلا أن العديد من الأبحاث والدراسـات تقوم بنسـب هذا الهجوم للولايات المتحدة الأمريكية والكيان الصـهيوني خاصـة بسـبب ظهور اللغة العبرية في برمجة الفيروس، إلا أنه حتى يومنا هذا لم تقوم أي من الدولتين بالاعتراف علناً بتبني هذا الهجوم، لذلك، من الصـعب التحديد بشـكل قاطع ورسـمي من المســؤول عن الفيروس. ومع ذلك، بالنظر إلى تعقيد وتكلفة الهجوم، يبدو من المرجح أن تكون دولة متورطة، ونفترض جدلاً حسـب المعطيات أن الولايات المتحدة الأمريكية والكيان الصـهيوني هم كانوا وراء هذا الهجوم السيبراني.

وبالتالي إن الهجوم يعد نزاع مسـلح دولي سـيبراني حدث بشـكل مسـتقل عن الهجمات العسـكرية الحركية التقليدية ولعل غاية منفذ هذا الهجوم هو استخدامه لتجنب العملية العدائية على الأرض لكي يقوم بالالتفاف على القانون الدولي الإنســاني لكيلا تطبق قواعده ومبادئه عليه، لكن بما أنه نشــأ نزاع مســلح دولي فيطبق القانون الدولي الإنساني. وانطلاقا من ذلك سنقيم انطباق قواعد القانون الدولي الإنساني على هذا الهجوم فيما يلي:

مبدأ التناسب بين الضرر والميزة العسكرية الأكيدة: إن الضرر الذي لحق بالمدنيين جراء انتشار فيروس ستاكسنت هو ضئيل أو معدوم، مقارنة مع الميزة العسكرية الأكيدة فالغاية كانت من استهداف المفاعلات النووية الإيرانية هو لشـل قدرة إيران على إنتاج السـلاح النووي، فيمكن القول ان الميزة العسـكرية تحققت من خلال تدمير ١٠٠٠ جهاز طرد مركزي.

إلا أنـه لابد من الإشــــارة إلى أمر هام جداً وهو التقييد الموجود في المـادة ٥٦ من البرتوكول الإضافي الأول الذي جاء فيه:

"لا تكون الأشغال الهندسية والمنشآت التي تحوي قوى خطرة، ألا وهي السدود والجسور والمحطات النووية لتوليد الطاقة الكهربائية محلاً للهجوم، حتى لو كانت أهدافاً عسـكرية، إذا كان من شــأن مثل هذا الهجوم أن يتسبب في انطلاق قوى خطرة ترتب خسائر فادحة بين السكان المدنيين. كما لا يجوز تعريض الأهداف العسكرية الأخرى الواقعة عند هذه الأشـغال الهندسـية، أو المنشـآت أو على مقربة منها للهجوم،

إذا كان من شأن هذا الهجوم أن يتسبب في انطلاق قوى خطرة من الأشغال الهندسية أو المنشآت ترتب خسائر فادحة بين السكان المدنيين".

ويرد على هذا التقييد اســـتثناء ورد في الفقرة الثانية من المادة ٥٦ آنفة الذكر التي نصـــت تتوقف الحماية الخاصة ضد الهجوم المنصوص عليه في الفقرة الأولى في الحالات التالية:

أ) فيما يتعلق بالسدود أو الجسور، إذا استخدمت في غير استخداماتها العادية دعماً للعمليات العسكرية على نحو منتظم وهام ومباشـــر، وكان مثل هذا الهجوم هو الســـبيل الوحيد المســـتطاع لإنهاء ذلك الدعم.

ب) فيما يتعلق بالمحطات النووية لتوليد الكهرباء، إذا وفرت هذه المحطات الطاقة الكهربائية لدعم العمليات العســـكرية على نحو منتظم وهام ومباشـــر، وكان مثل هذا الهجوم هو الســـبيل الوحيد المستطاع لإنهاء ذلك الدعم.

ج) فيما يتعلق بالأهداف العسكرية الأخرى الواقعة عند هذه الأعمال الهندسية أو المنشآت أو على مقربة منها، إذا اســـتخدمت في دعم العمليات العســـكرية على نحو منتظم وهام ومباشـــر، وكان مثل هذا الهجوم هو السبيل الوحيد المستطاع لإنهاء ذلك الدعم.

إذاً إن مثل هذا الهجوم الســـيبراني على المفاعلات النووية الإيرانية حتى لو كان احتمال تعرض المدنيين إلى ضـرر ضـفيف يجب أن يكون محظور حسـب القيد المذكور في المادة ٥٦ بعدم اسـتهداف الأشغال الهندسية والمنشآت التي تحوي قوى خطرة مثل السدود والجسور والمحطات النووية لتوليد الطاقة الكهربائية حتى لو كانت أهدافاً عسكرية، أما بالنسبة للاستثناء على هذا القيد في الفقرة الثانية من المادة ٥٦ بأنه يمكن استهدافها إذا وفرت دعم للعميات العسكرية على نحو منتظم وهام ومباشر وكان مثل هذا الهجوم هو الســـبيل الوحيد المســـتطاع لإنهاء مثل هذا الدعم، فلم يكن هناك دعم للعمليات العســـكرية بالأصل حتى يتم استهدافها والاستفادة من هذا الاستثناء!.

مبدأ التمييز بين المقاتلين غير المقاتلين: كان الهجوم الســـيبراني موجه إلى أنظمة الكمبيوتر بالتالي لم يكن هناك اســـتهداف للمقاتلين أو غير المقاتلين بشـــكل خاص، وبناء على ذلك لم يكن هناك ضـــرورة لتطبيق هذا المبدأ.

مبدأ التمييز بين الأعيان العسـكرية والأعيان المدنية: اكتشـف الباحثون أنه على الرغم من أن الفيروس قد تم تصـميمه للانتشـار العشـوائي إلى حد ما داخل شـبكة، وسـبب في تعطيل ٣٠ ألف جهاز كمبيوتر للمنشـــآت الصـــناعية في إيران وحوالي ٤٥ ألف جهاز كمبيوتر حول العالم، إلا أن هذا التعطيل ليس جوهري، حيث أنه كان مبرمج لاستهداف أنظمة معين ولهدف عسكري محدد فقط وهي أنظمة المفاعلات

النووية الإيرانية التي تقوم بتخصيب اليورانيوم الذي يمكن استخدامه في صنع الأسلحة النووية فهذه العين يمكن اعتبارها عين عسكرية تسهم مساهمة فعالة في العمل العسكري.

مبدأ الضـــرورة العســـكرية: لقد تم اســـتهداف المفاعلات النووية الإيرانية لكي يتم منع إيران من إنتاج الأسلحة النووية، فاليورانيوم المخصب الذي يقوم بإنتاجه مفاعل نطنز هو مكون ضروري لإنتاج الأسلحة النووية.

مبدأ الاحتياط لتجنب المحظورات: لقد اتخذ المهاجم احتياطاته قبل الهجوم عن طريق تصـــميمه للفيروس بتقنية عالية وتحديد الهدف أو النظام الواجب اســـتهدافه، وتســـبب بأضـــرار فعلية فقط للمفاعلات النووية الإيرانية، ولم يكن **(Stuxnet)** مفرطاً نظراً لعدم حدوث أي ضرر جوهري لأجهزة الكمبيوتر المدنية [1].

---

(1) Richmond, Jeremy: "Evolving Battlefields: Does Stuxnet Demonstrate A Need for Modifications to The Law of Armed Conflict?", Fordham International Law Journal, Volume 35, Issue 3, Article 1, 2012, PP843-893, P856, Available At: https://core.ac.uk/download/pdf/144231051.pdf

الخاتمة

وهكذا نجد أن دراسة الهجمات السيبرانية تعد ضرورة ملحة نظراً لما يشهده عالمنا المعاصر من فرض الاستخدام السلبي للتقدم التكنولوجي، وأصبح هناك تأثير متبادل بين التقدم التكنولوجي وما يفرزه من تحديات وقدرة المجتمع الدولي والقانون الدولي الإنساني على وجه الخصوص على التكيّف معه، فيمكن للدول استغلال اتفاقيات القانون الدولي الإنساني بأنها قديمة ومر عليها الزمن وبالتالي يقوموا باستغلال هذه الناحية والقيام بهجمات سيبرانية دون وجود قواعد قانونية تنظمها ولكن كما وجدنا بأن الجهود الدولية تسعى إلى تنظيم الهجمات السيبرانية وضبطها وإن كانت تسير على نحو بطيء فإنها وإن دلت على شيء فإنها تدل على وعي المجتمع الدولي بخطورتها. وإن من أفضل ما تم التوصل إليه وعلى وجه السرعة في وقتنا الحالي هو انطباق الهجمات السيبرانية التي تحدث في سياق النزاع المسلح الحركي على القانون الدولي الإنساني. ولكن تبقى الهجمات السيبرانية التي تحدث خارج سياق النزاع المسلح تثير العديد من التساؤلات في مدى إمكانية نسب الهجوم لجهة معينة وفي عدها نزاع مسلح، وبالتالي إمكانية انطباق القانون الدولي الإنساني عليها يواجه العديد من الصعوبات ولا يزال هذا الأمر بحاجة إلى دراسة حثيثة من قبل الخبراء القانونيين.

وفي كل الأحوال، الهجمات السيبرانية لن تتوقف، ويجب على كل الدول، الاستعداد لمواجهة الخطر المحتمل مع التمسك بأمل ألا تحدث أي هجمات على البنى التحتية ذات التأثير المباشر على حياة المدنيين اليومية. وإذا لم يكن بالإمكان لمثل هذا الأمل أن يتحقق، فإن نفس البلدان التي تخطط لشن هجمات سيبرانية على البنى التحتية الحيوية هي ذاتها التي تخطط أيضاً لشن هجوم فعلي وحروب مادية. وقد سجل التاريخ تنفيذ مثل هذا السيناريو فعلياً في عدد من البلدان عبر العالم.

وإتماماً للفائدة فإنني أعرض في نهاية البحث لأهم النتائج التي توصلت إليها، وبعض التوصيات التي يمكن أن تسهم في زيادة الوعي بخطورة الهجمات السيبرانية وضرورة تنظيمها، وذلك لتحقيق الحماية المطلوبة للسكان المدنيين وأعيانهم المدنية بموجب القانون الدولي الإنساني.

أولاً- النتائج

١) الهجمات السيبرانية من المفاهيم الحديثة التي لا يوجد اتفاق دولي على تعريفها حتى يومنا هذا، ولكن على الرغم من ذلك لا تحدث في فراغ قانوني ويمكن الاستناد في ذلك إلى المادة ٣٦ من البروتوكول الإضافي الأول لعام ١٩٧٧ وأيضاً لآراء وقرارات محكمة العدل الدولية كرأيها بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها.

٢) جاء المجال الخامس وهو الفضاء السيبراني ليشكل 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.

٦) هناك جهود دولية بذلت في سبيل تنظيم الأنشطة السيبرانية كاتفاقية بودابست ودليل تالين والقرارات الصادرة عن الأمم المتحدة، وإن هناك قوانين وإن كانت سابقة لظهور الهجمات السيبرانية إلا إنها تنظم وسائل وأدوات قد تستخدم في تنفيذها مما يمكن الرجوع إليها، مع ذلك هذه الجهود لم ترق إلى مستوى تنظيم شامل لهذه الهجمات.

٧) أن التوسع في تفسير النصوص القانونية القائمة سيؤدي إلى خروجها من مضمونها ومحتواها.

٨) الإقرار بأنه تكمن صعوبة الهجمات السيبرانية من ناحيتين، الأولى في عدم وجود خط محدد وواضح بين الأعيان العسكرية والمدنية بسبب الاستخدام المزدوج لشبكة الانترنت، أما الثاني في صعوبة إثبات نسبة الهجوم السيبراني في حال تم تكييفه على أنه هجوم لدولة أو جهة معينة.

ثانياً- التوصيات

١) السعي لاعتماد اتفاقية دولية لتنظيم الهجمات السيبرانية وإن كنت أعتقد أن هذا الأمر بعيد المنال في الوقت الحالي وقد يستغرق وقت طويل من الزمن على غرار اتفاقية حظر الأسلحة النووية التي استغرق لدخولها حيز النفاذ في ٢٢يناير عام ٢٠٢١ حوالي ٧٥عام، وذلك بسبب تباين الآراء بين الدول وعزوف الدول من الانضمام إلى المعاهدات الدولية الملزمة، ولكن في حال كان هناك وعي من قبل المجتمع الدولي بخطورة هذه الهجمات هناك بصيص أمل باعتمادها، وأيضاً يمكن في الوقت الحالي وكحل سريع القيام بإصدار "بروتوكول إضافي رابع" ملحق باتفاقيات جنيف الأربع لعام ١٩٤٩ بغرض تنظيم الهجمات السيبرانية وتحريم استخدامها على البنى التحتية الحيوية التي يمكن أن تعرض حياة السكان المدنيين للخطر.

٢) 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.

٣) 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.

٤) أهمية دور المجتمع الدولي في رفع الوعي بمخاطر الاستخدامات غير السليمة للتكنولوجيا، على الصحة والاقتصاد العالمي والأمن العالمي.

٥) تعزيز الحوار والتنسيق وتبادل المعلومات بين الدول والمنظمات الدولية والإقليمية في إطار مكافحة إساءة استخدام تكنولوجيا المعلومات والاتصالات.

٦) أهمية سعي الدول النامية لتطوير وتحديث أمنها السيبراني والاستفادة من تجارب البلدان الأخرى والخبرات الموجودة لديها وذلك كله في سبيل تحصين بنيتها الرقمية.

٧) 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.

قائمة المصادر والمراجع

أولاً: المراجع العربية

١) الكتب العامة

الحسيني، عمار عباس: جرائم الحاسوب والانترنت (الجرائم المعلوماتية)، الطبعة الأولى، منشورات زين الحقوقية، بيروت(لبنان)،٢٠١٧.

خليفة، إيهاب: القوة الإلكترونية كيف يمكن أن تدير الدول شؤونها غي عصر الانترنت" الولايات المتحدة الأمريكية نموذجاً"، الطبعة الأولى، العربي، القاهرة، ٢٠١٧، متاح بشكل جزئي على الرابط: https://cutt.ly/2khoqnN

الخولي، محمود إسماعيل: قضايا الخيانة والجاسوسية الجاسوسية والوعي الأمني، العربي، القاهرة، ٢٠١٩، متاح بشكل جزئي على الرابط: https://cutt.ly/NkdF1ow

روسو، جان جاك: العقد الاجتماعي، مؤسسة هنداوي للتعليم والثقافة، القاهرة،٢٠١٣، متاح على الرابط: https://cutt.ly/WkpNp5Y

هارولد، سكوت وارين وآخرون: التوصل إلى اتفاق مع الصين بشأن الفضاء الإلكتروني، مؤسسة RANDA، سانتا مونيكا، كاليفورنيا،٢٠١٦، متاح على الرابط: https://cutt.ly/PkdRw3m

٢) الكتب القانونية

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)،٢٠٢٠.

الخن، محمد طارق: الجريمة المعلوماتية، الجامعة الافتراضية السورية (برنامج الإجازة في الحقوق)، دمشق (سوريا)، ٢٠١٢.

زور، جاسم: المرأة زمن الحرب بين الواقع وحماية القانون الدولي، الطبعة الأولى، منشورات زين الحقوقية، بيروت(لبنان)، ٢٠١٩.

شهاب، مفيد: دراسات في القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر، بدون تاريخ نشر.

الصادق، عادل عبد: أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، سلسة أوراق العدد ٢٣، وحدة الدارسات المستقبلة مكتبة الإسكندرية، مصر(القاهرة)، ٢٠١٦، متاح على الرابط: https://cutt.ly/ekdbrXW

الصادق، عادل عبد: الإرهاب الإلكتروني والقوة في العلاقات الدولية: نمط جديد وتحديات مختلفة، مركز الأهرام للدراسات السياسية والاستراتيجية، الطبعة الثانية، القاهرة،٢٠٠٩، متاح على الرابط: https://cutt.ly/SksQ7Xl

طوزان، أحمد: قانون النزاعات المسلحة، ماجستير القانون الدولي الإنساني، الجامعة الافتراضية السورية، دمشق(سوريا)،٢٠٢٠.

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

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

ميلزر، نيلس: دليل التفسيري لمفهوم المشاركة المباشرة في العمليات العدائية بموجب القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر،٢٠١٠.

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.

٣) رسائل الماجستير

شهاب، محمود إبراهيم عبد الرحمن: الأسلحة غير التقليدية في الفقه الإسلامي، الجامعة الإسلامية–عمادة الدراسات العليا كلية الشريعة والقانون، قسم الفقه المقارن، غزة، إشراف الدكتور: زياد إبراهيم مقداد، ٢٠٠٧، متاح على الرابط:
https://iugspace.iugaza.edu.ps/handle/20.500.12358/22293

العتيبي، عبد الرحمن بجاد شارع: دور الأمن السيبراني في تعزيز الأمن الإنساني، جامعة نايف العربية للعلوم الأمنية–كلية العلوم الاستراتيجية (قسم الأمن الإنساني)، إشراف الدكتور: د. طارق محمد سليمان،٢٠١٧.

كلنتر، عماد محمد: المسؤولية الدولية الناشئة عن الهجمات السيبرانية، جامعة الكوفة–كلية القانون، جمهورية العراق، إشراف الدكتور: أحمد عبيس نعمة الفتلاوي،٢٠١٦.

٤) الأطروحات الجامعية

إبراهيم، طلال محمد الحاج: الهجمات السيبرانية على شبكات الحاسوب في ضوء القانون الدولي الإنساني، جامعة دمشق (كليه الحقوق –قسم القانون الدولي)، دمشق(سوريا)، إشراف الدكتورة مايا الدباس،٢٠٢٠.

٥) وثائق وتقارير

إرشادات الإسكوا للتشريعات السيبرانية، مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية، بيروت، ٢٠١٢، متاح على الرابط: https://cutt.ly/DkoHsuQ

تقرير اللجنة الدولية للصليب الأحمر للمؤتمر الدولي الحادي والثلاثون للصليب الأحمر والهلال الأحمر، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، جنيف، سويسرا، الوثيقة: 31IC/11/5.1.2،٢٠١١.

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

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

ملكية، طيب سليمان. فطيمة، عبد العزيز: الطب عن بعد La tété–médecine: إبداع في الخدمات الطبية، المؤتمر الدولي حول الإبداع والتغيير التنظيمي في المنظمات الحديثة: دراسة وتحليل تجارب وطنية ودولية، جامعة سعد دحلب البليدة (كلية العلوم الاقتصادية وعلوم التسيير)، الجزائر، ٢٠١١، متاح على الرابط:https://cutt.ly/1kpz44Y

٦) المجلات العلمية المحكمة

أعمر، عمر محمود: "الحرب الإلكترونية في القانون الدولي الإنساني"، مجلة دراسات، علوم الشريعة والقانون، الجامعة الأردنية، الأردن، المجلد ٤٦، عدد ٣، ٢٠١٩، ص ص ١٣٤–١٥٥، متاح على الرابط: https://cutt.ly/lkpBGCp

تغري، موسى بن: " الحرب السيبرانية والقانون الدولي الإنساني"، مجلة الاجتهاد القضائي، المجلد١٢، عدد خاص (العدد التسلسلي٢٢)، جامعة محمد خيضر بسكرة، الجزائر، نيسان، ٢٠٢٠، ص ص ١٩٩–٢١٨، متاح على الرابط:
https://www.asjp.cerist.dz/en/article/112730

خليل، بشار: "ما هي الحرب السيبرانية؟ مستقبل مخيف للصراع الرقمي"، مجلة المعلوماتية، العدد ١٥٤ لشهر آب (أغسطس)، الجمعية السورية للمعلوماتية، ٢٠٢٠، متاح على الرابط:
http://www.scs.org.sy/?q=scs/infomag/showarticlenode&id=853

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، 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) صيف٢٠١٢، ص ص ٥٣٣-٥٧٨، متاح على الرابط: https://cutt.ly/Okp7S5Z

الزهراني، شيخة حسين: "التعاون الدولي في مواجهة الهجوم السيبراني"، مجلة جامعة الشارقة للعلوم القانونية، المجلد ١٧، العدد١، جامعة الشارقة-كلية القانون، الإمارات العربية المتحدة، حزيران ٢٠٢٠، ص ص ٧٤٠-٧٧٢، متاح على الرابط:https://cutt.ly/JkpJyjF

السعبري، بهاء عدنان: عماد عبد خضير الزرفي، "انتقال التهديدات من الواقع إلى العالم الافتراضي"، مجلة جامعة بابل للعلوم الإنسانية، المجلد ٢٧، العدد٤، بغداد، ٢٠١٩، ص ص ٤٧٢-٤٨٧، متاح على الرابط:https://cutt.ly/TkpGqEt

سعود، يحيى ياسين: "الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني"، المجلة القانونية (مجلة متخصصة في الدراسات والبحوث القانونية)، جامعة يحي فارس، الجزائر، ٢٠١٨، ص ص ٧٩-١٠٨، متاح على الرابط: https://cutt.ly/QksE4ii

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، متاح على الرابط:
https://www.asjp.cerist.dz/en/article/69268

العبودي، علي عبد الرحيم: "هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين"، المجلة العلمية الأكاديمية العراقية، العدد ٥٧، جامعة بغداد، كلية العلوم السياسية، ص ص ٨٩-١١٨، متاح على الرابط:https://cutt.ly/XkokTen

لبكي، جورج: "المعاهدات الدولية للإنترنت: حقائق وتحدّيات"، مجلة الدفاع الوطني، بيروت، العدد ٨٣، كانون الثاني ٢٠١٣، استرجعت بتاريخ٢٠٢٠/١٢/٢٥، متاح على الرابط:
https://cutt.ly/nh5Hell

لين، هربرت: "النزاع السيبراني والقانون الدولي الإنساني"، مجلة اللجنة الدولية للصليب الأحمر، مجلد ٩٤(٨٨٦)، صيف٢٠١٢، ص ص ٥١٥-٥٣١، متاح على الرابط: https://cutt.ly/RkoansD

الموسوي، علي محمد كاظم: "المشاركة المباشرة للهبة الجماعية في الهجمات السيبرانية"، مجلة كلية الحقوق، جامعة النهرين، الدكتور حيدر أدهم الطائي، بغداد، ٢٠١٩، ص ص ٢٥-٥٨، متاح على الرابط:https://cutt.ly/Skgb1y7

نعوس، مصطفى: "حقوق والتزامات الدول في الحرب المعلوماتية"، مجلة دراسات علوم الشريعة والقانون، المجلد ٤٠، ملحق ١، الجامعة الأردنية، ٢٠١٣، ص ص ٧٨٤-٨٠٠، متاح على الرابط: https://cutt.ly/PkpCkzb

٧) الاتفاقيات الدولية

اتفاقيات جنيف الأربع لعام ١٩٤٩ والبروتوكولين الإضافيين المحلقين لعام ١٩٧٧.

اتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢.

مجلس أوروبا، الاتفاقية المتعلقة بالجريمة الالكترونية (بودابست)، مجموعة المعاهدات الأوروبية رقم ١٨٥، ٢٠٠١، متاح على الرابط:https://cutt.ly/YkpJXmC

نظام روما الأساسي للمحكمة الجنائية الدولية، ١٩٩٨م، متاح على الرابط: https://www.icrc.org/ar/doc/resources/documents/misc/6e7ec5.htm

٨) قرارات الأمم المتحدة

أ- قرارات الجمعية العامة

GA. Res. 55/63, U. N. Doc. No, A/RES/55/63 (Jan, 22, 2001), Available At: https://undocs.org/ar/A/RES/55/63

GA. Res. 56/121, U. N. Doc. No, A/RES/56/121 (Jan, 23, 2002), Available At: https://undocs.org/ar/A/RES/56/121

GA. Res. 57/239, U. N. Doc. No, A/RES/57/239 (Jan, 31, 2003), Available At: https://undocs.org/ar/A/RES/57/239

GA. Res. 58/199, U. N. Doc. No, A/RES/58/199 (Jan, 30, 2004), Available At: https://undocs.org/ar/A/RES/58/199

GA. Res. 72/284, U. N. Doc. No, A/RES/72/284 (July, 2, 2018), Available At: https://undocs.org/ar/A/RES/72/284

GA. Res. 73/187, U. N. Doc. No, A/RES/73/187 (Jan, 14, 2019), Available At: https://undocs.org/ar/A/RES/73/187

GA. Res. 74/173, U. N. Doc. No, A/RES/74/173 (Jan, 7, 2020), Available At: https://undocs.org/ar/A/RES/74/173

ب-قرارات مجلس الأمن

SC. Res. 2341, U. N. Doc. No, S/RES/2341(2017) (February, 13, 2017), Available At: https://undocs.org/ar/S/RES/2341 (٢٠١٧)

SC. Res. 2370, U. N. Doc. No, S/RES/2370(2017) (August, 2, 2017), Available At: https://digitallibrary.un.org/record/1298189?ln=ar

٩) المعاجم:

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

ثانياً: المراجع الأجنبية

1- Dictionary

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

2- Books

Andress, Jason. Winterfeld Steve: Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, 1st Edition, Elsevier, USA,2011, Available At: http://index-of.es/Hack/Cyber%20Warfare.pdf

Geers, Kenneth: Strategic Cyber Security, NATO Cooperative Cyber Defence Centre Of Excellence, Tallinn, Estonia, June 2011, Available At: https://www.law.upenn.edu/institutes/cerl/conferences/cyberwar/papers/reading/Geers.pdf

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

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

3- Theses

Knopová, Eva: New IHL Framework for Cyber Warfare, Faculty of Law (Department of International Law), Charles University in Prague, Thesis Supervisor: Dr. Martin Faix,2016, Available At: https://cutt.ly/8ksnQdZ

Maonga, Sharon Kerubo: "A Case of Incapacity: The Interrogation of International Humanitarian Law as A Satisfactory Regulator of Cyber Warfare", Strathmore University, Strathmore Law School ,2017, Available At: https://cutt.ly/QjquA9H

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

4- Research:

Tikk, E & Others International Cyber Incidents: Legal Considerations, Cooperative Cyber Defence Centre Of Excellence, Tallinn, Estonia, 2010, Available At: https://scholar.google.com/citations?user=8xfcsb8AAAAJ&hl=en

Wegener, Henning: "Hardnessing The Perils In Cyberspace: Who Is In Charge?", UNIDIR, 2007, Available At: https://www.peacepalacelibrary.nl/ebooks/files/UNIDIR_pdf-art2646.pdf

5- Journals

Bell, Cameron H.: "Cyber Warfare and International Law: The Need for Clarity", Towson University Journal of International Affairs, VOL. LI, NO.2, Spring 2018, PP 21-43, Available At: https://cutt.ly/tkdz7dl

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

Hathaway, Oona A. & Others: "The Law of Cyber-Attack", Article, California Law Review, 2012, PP817-886, Available At: https://cutt.ly/Gko9ddj

Hughes, Rex: "A Treaty for Cyber Space", International Affairs (Royal Institute of International Affairs 1944-), Vol. 86, No. 2, UK, 2010, PP 523-541, Available AT: https://academic.oup.com/ia/article/86/2/523/2326362

Kutnayeva, Nuria: "Cybersecurity in Central Asia", Unipath-Magazine, United States Central Command (CENTCOM), August 20 ,2015, Available At: https://cutt.ly/ijquJ7A

Linaki, Evangelia: Cyber Warfare and International Humanitarian Law: A Matter of Applicability, Journal of International Law of Peace and Armed Conflict, Volume 27,4/2014, PP169-175, Available At: https://cutt.ly/QkdZQQn

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, Available At: https://cutt.ly/DksuNk5

Richmond, Jeremy: "Evolving Battlefields: Does Stuxnet Demonstrate A Need for Modifications to The Law of Armed Conflict?", Fordham International Law Journal, Volume 35, Issue 3, Article 1, 2012, PP843-893, Available At: https://core.ac.uk/download/pdf/144231051.pdf

Wallace, David A. & Jacobs, Christopher W.: " Conflict Classification And Cyber Operations: Gaps, Ambiguities And Fault Lines", U. Pa. J. Int'l L, Penn Law: Legal Scholarship Repository, Vol. 40:3,2019,PP645-692, Available At: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1985&context=jil

6- Working Paper:

Futte, Andrew: " Cyber Threats and Nuclear Weapons: New Questions for Command and Control, Security and Strategy", Occasional Paper, Royal United Services Institute for Defence And Security Studies, UK, July 2016, Available At: https://rusi.org/sites/default/files/cyber_threats_and_nuclear_combined.1.pdf

Lülf, Charlotte: Modern Technologies and Targeting Under International Humanitarian Law, Working Paper, Vol.3, No3, IFHV, Ruhr University Bochum, Germany,2013, Available At: https://cutt.ly/sksxM79

Schreier, Fred: "On Cyberwarfare", Working Paper No. 7, DCAF Horizon, Geneva, 2015, Available At: https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf

G- International agreements:

Constitution of The International Telecommunication Union.

Shanghai Cooperation Organization, Yekaterinburg Declaration of The Heads of The Member States of The Shanghai Cooperation Organization, Consulate General of Uzbekistan In New York City (July 9, 2009), Available At: http://eng.sectsco.org/load/198293/

The 1944 Chicago Convention for International Civil Aviation.

The 1971 Montreal Convention for The Suppression of Unlawful Acts Against Civil Aviation.

The 1988 Montreal Protocol for The Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation.

ثالثاً: المواقع

١) المواقع الرسمية

أمن الفضـــاء الإلكتروني، موقع الأمم المتحدة، مكتب مكافحة الإرهاب، اســـترجعت بتاريخ ٤/١٢/٢٠٢٠م، متاح على الرابط: https://cutt.ly/AkpFX7U

ما هي القيود التي يفرضـــها قانون الحرب على الهجمات الســـيبرانية؟، موقع اللجنة الدولية الأحمر، اســـتـــرجـــعـــت بـــتـــاريـــخ ٤/١٢/٢٠٢٠م، مـــتـــاح عـــلـــى الـــرابـــط: https://www.icrc.org/ar/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm

موقع الاتحاد الدولي للاتصالات (ITU): https://www.itu.int/ar/Pages/default.aspx

موقع القيادة السيبرانية للجيش الأمريكي، استرجعت بتاريخ٢٠٢١/١/٣١، متاح على الرابط: https://www.arcyber.army.mil/

موقع قاموس المعاني، استرجعت بتاريخ٢٠٢٠/١٢/٤: https://www.almaany.com/ar/dict/ar-en/cyber/

موقع مجلس أوروبا: https://www.coe.int/en/web/portal/home

موقع منظمة شنغهاي للتعاون: http://sectsco.org/

٢) المواقع الإخبارية

الاتحاد الدولي للاتصالات، موقع الجزيرة، استرجعت بتاريخ٢٠٢٠/١٢/٤م، متاح على الرابط: https://cutt.ly/Wh5Hmoi

إسرائيل تعترف رسميا بتدمير مفاعل نووي سوري في ٢٠٠٧، موقع DW، استرجعت بتاريخ٢٠٢١/١/١٢، متاح على الرابط: https://cutt.ly/9jbBBEj

أنواع الهجمات السيبرانية وطريقة تنفيذ كل نوع منها، موقع كونكت للتقنية، استرجعت بتاريخ٢٠٢٠/١٢/٤م، متاح على الرابط: https://cutt.ly/uh5Fys8

إيهاب خليفة، ما هو موقف ميثاق الأمم المتحدة من استخدام القوة السيبرانية في التفاعلات الدولية؟، موقع المستقبل للأبحاث والدراسات المتقدمة، استرجعت بتاريخ٢٠٢٠/١٢/٤م، متاح على الرابط: https://cutt.ly/rkpu3jQ

التهديدات الجديدة: الأبعاد الإلكترونية، موقع مجلة الناتو، استرجعت بتاريخ٢٠٢١/١/١٢م، متاح على الرابط: https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/AR/index.htm

الحرب السيبرانية وتداعياتها على الأمن العالمي، موقع الموسوعة الجزائرية للدراسات السياسية والاستراتيجية، استرجعت بتاريخ٢٠٢٠/١٢/٤م، متاح على الرابط: https://cutt.ly/uh5Gq3D

سعود، آيات محمد: شرط مارتينز في القانون الدولي الإنساني، موقع الحوار المتمدن، استرجعت بتاريخ٢٠٢١/٢/١٣، متاح على الرابط: https://www.ahewar.org/debat/show.art.asp?aid=591797

الشوابكة، مراد: ما هو نظام سكادا، موقع موضوع (أكبر موقع عربي بالعالم)، استرجعت بتاريخ٢٠٢١/٢/١٣، متاح على الرابط: https://cutt.ly/5kCk8TQ

الصـــين: "جيش أزرق" لحماية شـــبكات " الجيش الأحمر"، موقع BBC NEWS، اســـترجعت بتـــاريـــخ٢٠٢١/١/٣١، مـــتـــاح عـــلـــى الـــرابـــط: https://www.bbc.com/arabic/scienceandtech/2011/06/110531_china_blue_army

عادل عبد الصـــادق، الهجمات السـيبرانية: أنماط وتحديات جديدة للأمن العالمي، موقع الموسـوعة الجزائرية للدراسـات السياسـية والاسـتراتيجية، استرجعت بتاريخ٢٠٢١/١/٢٣، متاح على الرابط: https://cutt.ly/TjCJhVt

غيث علاو، الهجمات السـيبرانية.. أكبر من حرب نووية بوسـائل إلكترونية، موقع متخصـص في الشـــؤون الإيـــرانـــيـــة، اســـتـــرجـــعـــت بـــتـــاريـــخ٢٠٢٠/١٢/٤م: https://jadehiran.com/archives/16835

مسـعود الزاهد، إيران.. حريق نطنز يعطل وحدة جديدة من أجهزة الطرد المركزي، موقع قناة العربية، استرجعت بتاريخ٢٠٢٠/١/٧م، متاح على الرابط: https://cutt.ly/Tjb5XH8

موقع Cyberforsvaret الدفاع السـيبراني النرويجي، اسـترجعت بتاريخ٢٠٢١/١/٣١، متاح على الرابط: https://www.forsvaret.no/

وفاة مريضـــة جراء هجوم ســـيبراني على مســـتشـــفى ألماني، موقع RTonline، اســـترجعت بتاريخ٢٠٢٠/١٢/٤، متاح على الرابط:https://cutt.ly/1h5Jy0u

المحتويـــات

الموضوع	الصفحة
الإهداء	أ
شكر وتقدير	ب
ملخص البحث باللغة العربية	ج
Abstract	د
خطة البحث	ه
المقدمة	١
الفصل الأول: الإطار النظري والقانوني للهجمات السيبرانية	٦
المبحث الأول: ماهية الهجمات السيبرانية	٧
المطلب الأول: مفهوم الهجمات السيبرانية	٦
الفرع الأول: التعريف بالهجمات السيبرانية	٧
أولاً- الهجمات السيبرانية لغة واصطلاحاً	٨
١. السيبرانية في اللغة	٨
٢. الهجمات السيبرانية اصطلاحاً	٩
ثانياً- خصائص الهجمات السيبرانية	١٠
الفرع الثاني: طبيعة الهجمات السيبرانية	١١
أولاً- الهجمات السيبرانية وسيلة أم أسلوب للقتال	١٢
١. الهجمات السيبرانية وسيلة للقتال	١٢
٢. الهجمات السيبرانية أسلوب للقتال	١٣
ثانياً- تمييز الهجمات السيبرانية عن الجرائم السيبرانية والحرب السيبرانية	١٣
١. التمييز بين الهجمات السيبرانية والجرائم السيبرانية	١٣
٢. التمييز بين الهجمات السيبرانية والحرب السيبرانية	١٥
المطلب الثاني: التأطير النظري للهجمات السيبرانية	١٦
الفرع الأول: أنواع الهجمات السيبرانية	١٦

الفرع الثاني: الآثار الناشئة عن الهجمات السيبرانية	١٨
المبحث الثاني: الجهود الدولية للتنظيم القانوني للهجمات السيبرانية	٢١
المطلب الأول: الجهود الدولية المباشرة للتنظيم القانوني للهجمات السيبرانية	٢١
الفرع الأول: الأمم المتحدة	٢١
أولاً- الجمعية العامة	٢٢
ثانياً- مجلس الأمن	٢٣
ثالثاً- مكتب مكافحة الإرهاب	٢٣
الفرع الثاني: حلف شمال الأطلسي (الناتو)	٢٤
الفرع الثالث: مجلس أوروبا	٢٥
الفرع الرابع: مبادرات منظمة شنغهاي للتعاون (SCO)	٢٦
المطلب الثاني: الجهود الدولية غير المباشرة للتنظيم القانوني للهجمات السيبرانية	٢٧
الفرع الأول: قانون الاتصالات	٢٧
الفرع الثاني: قانون الطيران	٢٨
أولاً- اتفاقية شيكاغو لعام ١٩٤٤ للطيران المدني الدولي	٢٨
ثانياً- اتفاقية مونتريال لعام ١٩٧١ لقمع الأعمال غير المشروعة ضد الطيران المدني	٢٨
ثالثاً- بروتوكول مونتريال لعام ١٩٨٨ لقمع أعمال العنف غير المشـــروعة في المطارات التي تخدم الطيران المدني الدولي	٢٩
الفرع الثالث: قانون الفضاء الخارجي	٢٩
الفرع الرابع: قانون البحار	٣٠
الفصل الثاني: القانون الدولي الإنساني كإطار قانوني ناظم للهجمات السيبرانية	٣١
المبحث الأول: إمكانية انطباق القانون الدولي الإنساني على الهجمات السيبرانية	٣٣
المطلب الأول: معايير تحديد الأهداف العسكرية المشروعة أثناء الهجمات السيبرانية في القانون الدولي الإنساني	٣٣
الفرع الأول: الأشخاص والأعيان المشروع استهدافهم أثناء الهجمات السيبرانية	٣٤

أولاً– الهجمات السيبرانية بوصفها هجوم بموجب القانون الدولي الإنساني	٣٤
ثانياً– التعريف بمفهوم المقاتل السيبراني في القانون الدولي الإنساني	٣٥
ثالثاً– الأعيان المشروع استهدافها أثناء الهجمات السيبرانية	٣٧
١. المعنى العام للهدف العسكري	٣٧
٢. الأعيان ذات الاستخدام المزدوج	٣٩
الفرع الثاني: المدنيون الذين يشاركون مباشرة في الهجمات السيبرانية	٤١
أولاً– مدلول الأشخاص المدنيين	٤١
ثانياً– تحديد مفهوم المشاركة المباشرة في الهجمات السيبرانية	٤٢
المطلب الثاني: تطبيق المبادئ العامة في القانون الدولي الإنســـاني أثناء الهجمات السيبرانية	٤٤
الفرع الأول: المبادئ المتعلقة بالتحضير لاستخدام الهجمات السيبرانية	٤٤
أولاً– مبدأ التمييز بين المشروع والمحظور أثناء الهجمات السيبرانية	٤٤
١. التمييز بين المقاتلين السيبرانيين وغير المقاتلين السيبرانيين	٤٥
٢. التمييز بين الأعيان العسكرية والأعيان المدنية	٤٧
ثانياً– مبدأ الاحتياط لتجنب المحظورات أثناء الهجمات السيبرانية	٤٨
١. الاحتياطات الواجب اتخاذها قبل شن الهجمات السيبرانية	٤٨
٢. الاحتياطات الواجب اتخاذها لتلافي آثار الهجمات السيبرانية	٥٠
الفرع الثاني: المبادئ التي تحكم استخدام الهجمات السيبرانية أثناء العمليات العدائية	٥١
أولاً– مبدأ التناسب بين الضرر والميزة العسكرية المباشرة	٥١
ثانياً– مبدأ الضرورة العسكرية	٥٢
المبحث الثاني: تحديات انطباق القانون الدولي الإنساني على الهجمات السيبرانية	٥٤
المطلب الأول: الهجمات السيبرانية في سياق النزاع المسلح	٥٥
الفرع الأول: حالات تطبيقية للهجمات السيبرانية في سياق النزاع المسلح	٥٦
أولاً– حرب كوسوفو عام ١٩٩٩	٥٦
ثانياً– الهجوم السـيبراني من قبل الكيان الصـهيوني على الجمهورية العربية السـورية عام ٢٠٠٧	٥٨

ثالثاً– الهجمات السيبرانية بين روسيا – جورجيا ٢٠٠٨	٥٩
الفرع الثاني: تقييم انطباق القانون الدولي الإنساني على الهجمات السيبرانية في سياق النزاع المسلح	٦١
أولاً: تقييم انطباق القانون الدولي الإنساني على الهجمات السيبرانية في حرب كوسوفو عام ١٩٩٩	٦١
ثانياً: تقييم انطباق القانون الدولي الإنساني على حالة الهجوم السيبراني من قبل الكيان الصهيوني على الجمهورية العربية السورية عام ٢٠٠٧	٦٣
ثالثاً: تقييم انطباق القانون الدولي الإنساني على الهجمات السيبرانية بين روسيا – جورجيا ٢٠٠٨	٦٥
المطلب الثاني: الهجمات السيبرانية خارج سياق النزاع المسلح	٦٦
الفرع الأول: حالات تطبيقية للهجمات السيبرانية خارج سياق النزاع المسلح	٦٨
أولاً– الهجمات السيبرانية بين الصين– الولايات المتحدة الأمريكية	٦٨
ثانياً– الهجوم السيبراني على استونيا عام ٢٠٠٧	٧٠
ثالثاً– الهجوم السيبراني على المنشآت النووية الإيرانية	٧١
الفرع الثاني: تقييم انطباق القانون الدولي الإنساني على الهجمات السيبرانية خارج سياق النزاع المسلح	٧٣
أولاً– تقييم انطباق القانون الدولي الإنساني على حالة الهجمات السيبرانية بين الصين والولايات المتحدة الأمريكية	٧٣
ثانياً– تقييم انطباق القانون الدولي الإنساني على حالة الهجوم السيبراني على استونيا عام ٢٠٠٧	٧٤
ثالثاً– تقييم انطباق القانون الدولي الإنساني على حالة الهجوم السيبراني على المنشآت النووية الإيرانية	٧٥
الخاتمة	٧٨
أولاً– النتائج	٧٩
ثانياً– التوصيات	٨٠
قائمة المصادر والمراجع	٨١