الهجمات السيبرانية بين مشروعيتها كوسيله للدفاع الشرعي وادانتها كاعتداء غير مشروع (دراسة تحليلية في ضوء القانون الدولي)

د/ محمد صلاح عبد اللاه ربيع
دكتوراة في القانون الدولي العام

الملخص باللغة العربية :

هذا البحث مخصص لمناقشة موضوع الهجمات السيبرانية بوصفه نوعاً جديداً من أنواع الجرائم، ولا يوجد تنظيم قانوني متكامل لهذا النوع من الجرائم داخلياً وعالمياً حتى الآن.

وتعتبر أنظمة الاتصالات والأنظمة الرقمية جزءاً أساسياً من حياة الأمم والأفراد في العصر الحالي، ولكن في الوقت نفسه تشكل تهديداً خطيراً على أمن الدول.

وهدف هذا البحث مناقشة موضوع الهجوم السيبراني كنوع جديد من الصراعات والنزاعات بين الدول وإظهار أهمية وخطورة الهجمات السيبرانية.

تركز الدراسة على الهجمات السيبرانية على الدول، وما يجب على الجهات الدولية الفاعلة أن تتبنى هذه الهجمات بشكل فعال ويجب أن تجد نظاماً قانونياً لها في القانون الدولي العام يسمح باستخدام حق الدفاع عن النفس في حالة وقوع هجوم إلكتروني دولي. إلا أنه لا يوجد حتى الآن أي مبرر قانوني يسمح بالدفاع عن النفس في هذا النوع من الهجمات أو البند القانوني الذي يعرض هذه الهجمات لعدوان غير مسلح وغير مباشر.

الكلمات المفتاحية: الهجمات السيبرانية، الهجوم السيبرانى، ماهية الهجمات السيبرانية، النظام القانوني للهجمات السيبرانية

Abstract:

Modern technologies of communication systems and digital systems are considered an essential part in the life of nations and individuals in the modern world, but at the same time these systems constitute a serious threat on the security of the states.

This study aimed at discussing the topic of cyber attacks as a new type of crime, and there is no integrated legal regulation for this type of crime, internally or globally, yet.

The study focuses on the inclusion of Cyber- attacks and Aggression against states, international actors must adopt these attacks effectively and they must find legal justification in the Public International Law Allows to use the right of self-defense in the event of an international cyber attack.

However, there is no legal justification until now that allows self- defense in this type of attacks or legal item that puts these attacks under unarmed and indirect aggression.

(ISSN: ٢٣٥٦ - ٩٤٩٢)

مقدمة :

يحتل موضوع الهجمات السيبرانية مرتبة متقدمة في الجهد القانوني وبالذات عند المؤسسات الدولية المتخصصة من جهة، ولقلة الأبحاث العربية والمصرية منها بالذات من جهة أخرى، دفعنا ذلك لاختياره ليكون موضوعاً لبحثنا هذا، معولين في إتمامها على تحليل أحكام القانون الدولي العام والجهود الدولية ذات الصلة بتنظيم استخدامها بالحظر أو التقييد، فضلاً عن أهم الاجتهادات القضائية والفقهية والتي تناولت موضوع الهجمات السيبرانية من زوايا مختلفة.

أن عدداً من الإشكاليات ستثار لدى البحث والتحليل في موضوع الدراسة من أهمها: ما هي السيبرانية وكيف نشأت؟ هل يمكن أن تصنف ضمن وسائل وطرائق القتال؟ وإذا كانت كذلك هل ستنطبق عليها أحكام الاتفاقيات الدولية والقواعد العرفية ذات الصلة بسير العمليات القتالية؟

ومن جانب آخر، نسأل كيف تعامل المجتمع الدولي مع مشكلة الفراغ القانوني الذي يشهده موضوع التنظيم الدولي للسيبرانية؟ وهل من بارقة أمل ببدء مفاوضات دولية متعددة الأطراف أو ثنائية تنهي الجدل حول شرعية اللجوء إليها في ضوء أحكام القانون الدولي الإنساني والقواعد العرفية المستقرة بين الأمم المتحضرة؟

وماذا لو استمر إخفاق المجتمع الدولي في التوصل إلى إبرام اتفاقية دولية تهتم بتنظيم الهجمات السيبرانية؟

فقد 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 والبنية التحتية الأساسية عليهم، وتحكمهم في الأشياء المادية مثل المحولات الكهربائية والقطارات والمستشفيات والرادارات والمعاملات التجارية وأسواق الأوارق 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) "كجيل 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 فلا 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 يسمى 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 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 أنظمهة الكمبيوتر بل تهدف إلى خلق تأثير في العالم الحقيقي، على سبيل المثال اختراق أنظمهة 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 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 والكهرياء ويكون المدنيين هم الضحايا الرئيسيين لهذه 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.

- **<u>أسباب اختيار موضوع البحث</u>**

تم اختيار موضوع هذا البحث بسبب التقدم التكنولوجي والتحول الرقمي التي تسعى أغلب دول العالم إلى إحراز تقدم فيه في مختلف المجالات، وفى المقابل هذا الهدف ظهر في المقابل ما يعرف بالهجمات السيبرانية كنوع من الحروب الإلكترونية بين الدول وبعضها البعض، ولكن ورغم النقاشات التي دارت حول هذا الموضوع ألا أنه لم تحدد ملامحه أو نظام قانوني يحكمه، لذلك تم إختيار هذا الموضوع ليكون محل بحث وتحديد النظام القانون المعمول به لمواجهة هذا النوع من الهجمات.

- **<u>منهج البحث</u>**

يعتمد البحث على المنهج التحليلى للنصوص القانونية الدولية والآراء الفقهية وأحكام القضاء الدولى والاستعانة بها بما يخدم البحث، وذلك لأهمية البحث العملية والعلمية.

(ISSN: ٢٣٥٦ - ٩٤٩٢)

وسوف نتناول موضوع الهجمات السيرانية من خلال المباحث الآتية:

المبحث الأول: مفهوم الهجمات السيبرانية

المبحث الثانى: تمييز الهجمات السيبرانية عما يتشابه معها والآثار المترتبة عليها

المبحث الثالث: موقف القانون الدولى من الهجمات السيبرانية ومكافحتها

المبحث الرابع: الجهود الدولية للتنظيم القانوني للهجمات السيبرانية

الفصل الأول

ماهية الهجمات السيبرانية

شكلت الثورة الرقمية والمعلوماتية قفزة تكنولوجية، وأصبح الفضاء السيبراني عنصراً مؤثراً في النظام الدولي المعاصر نظراً لما يحمله من أدوات تكنولوجية متطورة، حيث عن محاور جديدة وأضاف مستويات كثيرة من التعقيد للعمليات العسكريات أكثر تأثيراً في الحسابات الاستراتيجية للدول، والدولة التي لا تملك التكنولوجيا السيبرانية المحصنة أمنياً سيتعرض فضاؤها السيبراني المتضمن للأصول والموارد والمعلومات والخدمات والبنية التحتية الحيوية، بما في ذلك الأمنية والعسكرية والمصرفية والتجارية والتعليمية والصحية والاقتصادية إلى الهجمات السيبرانية التي تسبب دمار هائل فيها.

وسوف نتناول فيما يلي ماهية هذه الهجمات من خلال المباحث الآتية:

المبحث الأول: مفهوم الهجمات السيبرانية

المبحث الثانى: تمييز الهجمات السيبرانية عما يتشابه معها والآثار المترتبة عليها

المبحث الثالث: تكييف الهجمات السيبرانية وموقف القانون الدولى منها

المبحث الرابع: الجهود الدولية للتنظيم القانوني للهجمات السيبرانية

المبحث الأول

مفهوم الهجمات السيبرانية

المطلب الأول

مفهوم الهجمات السيبرانية وخصائصها

بسبب حداثة مصطلح الهجمات السيبرانية لم يتم الاتفاق على تعريف موحد جامع شامل لها بل تعدد التعريفات حول الهجمات السيبرانية وذلك على التفصيل التالى:

الفرع الأول

حداثة الهجمات السيبرانية

حاليا شهدت وسائل النزاعات المسلحة تطورا وثيقاً بما قدمته الخبرات البشرية من خدمات تقنية تهدف من خلالها إلى تحقيق أهداف معينة، وحماية المصالح الحيوية التي من أجلها قام النزاع المسلح، وعليه تعد تلك المصالح هي الاختبار العلمي لما وصل إليه التطور التقني من دخول الوسائل الحديثة للقتال، ومن خلال ظهور نوع جديد من وسائل القتال ألا وهي (الهجمات السيبرانية).

وتعمل هذه الهجمات على إتلاف أو تأخير الفعاليات الالكترونية وكذلك الاعتداء على المعلومات من خلال السيطرة عليها عبر اتصال الحواسيب بشبكة الانترنت خاصة كانت أم عامة. (١)

وأثناء النزاعات المسلحة تبرز أهمية استخدام تكنولوجيا المعلومات بين أطراف النزاع وقد تقوم الدولة بارتكاب الاعتداء بنفسها، أو عبر وكالة لأشخاص أو شركات نيابة عنها، والحافز هنا هو قلة تكاليف الاعتداء بالهجمات السيبرانية بالقياس إلى الهجمات التقليدية، كذلك صعوبة تحديد مسؤولية القائم بالهجوم، وأخيراً إبعاد المقاتلين عن خطر المواجهة المباشرة مع العدو.

والملاحظ أن وسائل النزاعات المسلحة أصبحت تأخذ أشكالاً مختلفة، فنجد أن النزاعات السيبرانية باتت تجري في الفضاء السيبراني وأن النتائج المتوخاة منها أصبحت ملموسة ويمكن ملاحظاتها في واقعنا من خلال استهداف البنية التحتية مدنية كانت أم عسكرية وشبكات الحماية الالكترونية في تلك المنشآت.(٢)

ويكاد يجمع القائمون على المؤسسات العسكرية في العالم أن من يمتلك تقنية عالية في حرب المعلوماتية هو من سيتفوق في أي نزاع سيبراني.

ومما لا شك فيه أن الهجمات السيبرانية تعد من أهم صور حروب المعلوماتية، والسبب في ذلك يعود إلى النسبة القليلة من الأضرار التي تسببها تلك الهجمات فضلا عن قلة تكاليفها.

ويرتبط ظهور الهجمات السيبرانية بالشبكة العنكبوتية (شبكة الانترنت) ارتباطاً وثيقاً من خلال السرعة في نقل المعلومات عن طريق حزم البيانات التي ترسل عبر الانترنت، وقد وصف البعض نشوء الهجمات السيبرانية بأنها تمثل انعكاساً للجيل الثالث في مجال الثورة التقنية والتي بدورها أسهمت في تغيير وتطوير حياة المجتمعات البشرية. (٣)

(١) علي محمد كاظم الموسوي، المشاركة المباشرة في الهجمات السيبرانية، المؤسسة الحديثة للكتاب، ط ١، ٢٠١٩، ص٣١
(٢) علي محمد كاظم الموسوي، المشاركة المباشرة في الهجمات السيبرانية، المرجع السابق، ص٣٣
(٣) رياض مهدي عبد الكاظم، وألاء طالب خلف، المعلوماتية والحرب الحديثة، دراسة حالة الحرب الأمريكية على العراق عام ٢٠٠٣، مجلة للعلوم الإنسانية، المجلد ١١، العدد ٢٩، ٢٠١٥، ص ١٨٢

(ISSN: ٢٣٥٦ - ٩٤٩٢)

وفي إطار ذلك التطور بدأ الاهتمام الدولي بالسعي إلى تحقيق السبق في تطوير مجالها الأمني والعسكري في العقد العاشر من القرن الماضي وفي حينها أطلق عليها الحرب السيبرانية الباردة.

وتلجأ الدول المتقدمة إلى استخدام الهجمات السيبرانية لتحقيق أهداف عسكرية محددة، بهدف الهيمنة على واقع النزاع المسلح وبأقل خسائر فلا حاجة لوجود أطراف متحاربة في ميدان المعركة أثناء تنفيذ تلك الهجمات فضلا عن الطابع الوقائي الذي تحمله الهجمات السيبرانية ضد أهدافها، وبعبارة اخرى انتقلت ساحات القتال من مجالها المادي إلى المجال الافتراضي ذي الآثار المادية والمعنوية. (٤)

الفرع الثانى

تعريف الهجمات السيبرانية

لم يتفق الفقه الدولي على تعريف قانوني أو تقني للهجمات السيبرانية وطبيعتها، وعلى ذلك ذهب البعض إلى تعريف الهجمات السيبرانية بأنه " مصطلح حديث نوعا ما، ينطوي على التسلل الى مواقع الكترونية غير مرخص بالدخول اليها، بهدف تعطيل أو اتلاف البيانات المتوفرة أو الاستحواذ عليها، وهو فعل دولة، عرفه شميت schmitt بأنه مجموعة من الإجراءات التي تتخذها الدولة على نظم المعلومات المعادية بهدف التأثير والاضرار بها، أو للدفاع عن نظم المعلومات الخاصة بها. (٥)

وقد عرفها البروفسور (فيورتس) أستاذ قسم الكيمياء في جامعة تكساس للتكنولوجيا بالقول "هجوم عبر الانترنت يقوم على التسلل إلى مواقع الكترونية غير مرخص بالدخول إليها بهدف تعطيل البيانات المتوفرة أو إتلافها أو الاستحواذ عليها وهي عبارة عن سلسلة هجمات إلكترونية تقوم بها دولة ضد أخرى". (٦) ومن جانب آخر توصف الهجمات السيبرانية بأنها أحدى أساليب حرب المعلومات التي تعتمد على السلاح المعلوماتي.

فيما يرى مايكل شميت أنها:"عمليات لإيقاع الفوضى في المعلومات الموجودة في أجهزة الحاسوب أو شبكات الحاسوب أو الأجهزة أو الشبكات نفسها أو نفيها أو الانتقاص من شأنها أو تدميرها، وجوهر هذه الهجمات – بغض النظر عن الإطار الذي تجري فيه –هو بالاعتماد على سيل من البيانات الالكترونية لتنفيذ الهجوم، ويمكن أن تصل الهجمات إلى مستوى حرب المعلومات، كذلك

(٤) د/ احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: فهو مفهومها المسؤولية الدواية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلبي للعلوم القانونية والسياسية، كلية القانون جامعة بابل، العدد الرابع، السنة الثامنة، ٢٠١٦، ص ٦٢٢، وأيضاً لنفس المؤلف، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، منشورات زين الحقوقية، لبنان، الطبعة الأولى، ٢٠١٨، ص١٦

(٥) أحمد عبيس نعمة الفتلاوي، الهجمات السبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، منشورات زين الحقوقية، بيروت لبنان، الطبعة الأولى، ٢٠١٨، ص ٣٦".

(٦) د/ أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية، دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، المرجع السابق، ص ١٦

يمكن اللجوء إليها وقت السلم"، والملاحظ على تعريف أعلاه أنه اقتصر على نتائج الهجمات وأهدافها على شبكات أنظمة الحاسوب والمعلومات التي يتم تخزينها فيها. (٧)

وتذهب المستشارة القانونية في اللجنة الدولية للصليب الأحمر كوردولا دورغ إلى أن الهجمات السيبرانية ما هي إلا "عمليات تشن ضد أو عبر حاسوب أو نظام حاسوب من خلال تدفق البيانات، وقد تهدف هذه العمليات إلى تحقيق أغراض مختلفة تضم على سبيل المثال اختراق نظام معين وجمع أو نقل أو تدمير أو تغيير أو تشفير البيانات أو إجراء تعديل للعمليات التي يتحكم بها جهاز الحاسب الآلي المخترق أو التلاعب بها ويمكن اعتبار هذه العمليات في بعض الظروف، هجمات بحسب التعريف الوارد في القانون الدولي الإنساني"، والملاحظ أن ما أوردته المستشارة جاء بناء على نص الفقرة (٢) من المادة (٤٩) من البروتوكول الإضافي الأول لعام ١٩٧٧. (٨)

ويرى جانب أخر من الفقه بأن الهجمات السيبرانية تقوم على استخدام لأنشطة الكترونية متعددة بهدف إضعاف أو تدمير أنشطة الحاسوب أو افسادها أو إرسال المعلومات من خلالها، أثناء استخدام شبكات الحاسوب التابعة للخصم، كما أن الهجوم السيبراني يمكن استخدامه في منع المستخدمين من اختراق الحاسوب، وفي استخدام آخر فإن الهجوم السيبراني يساهم في تدمير الآلات التي يتحكم فيها الحاسوب الآلي،(٩) وقد وصفها البعض الآخر أنها " قيام دولة أو كيانات من غير الدول بشن هجوم الكتروني في إطار متبادل، أو من قبل طرف واحد". (١٠)

وتعرف الهجمات السيبرانية وفق ما تبنته القيادة الاستراتيجية الامريكية عام ٢٠٠٧ بأنّه تطويع عمليات نظام الكمبيوتر بهدف منع الخصم من الاستخدام الفعال لها فضلاً عن التسلل الى نأظمة المعلومات وشبكات الاتصال بهدف جمع البيانات التي تحتويها وحيازتها وتحليلها، وعرَّفته شميت (Schmitt) المتخصص في القانون الدولي الإنساني بأنه الهجوم السيبراني هو أي تصرف الكتروني دفاعي كان أو هجومي يتوقع منه وعلى نحو معقول في التسبب بجرح او قتل شخص او الحاق اضرار مادية او دمار بالهدف المهاجم.(١١)

(٧) سراب ثامر أحمد، الهجمات على شبكات الحاسوب في القانون الدولي الإنساني، أطروحة دكتوراه، كلية الحقوق، جامعة النهرين، ٢٠١٥، ص ٨٠، وكذلك د/ عبد الله عبد الكريم على أحمد، الهجمات السيبرانية في ضوء القانون الدولى، بحث منشور في المجلة االمصرية للقانون الدولى، المجلد ٧٧٧، سنة ٢٠٢١، ص٧

(٨) نصت الفقرة (٢) من المادة (٤٩) من البروتوكول الاضافي الاول لعام ١٩٧٧ على أنه "تنطبق أحكام هذا الحق للحق ((البروتوكول)) المتعلقة بالهجمات كافة على الهجمات في أي إقليم تشن منه بما في ذلك الاقليم الوطني لأحد أطراف النزاع والواقع تحت سيطرة الخصم".

(٩) هربرت لين، النزاع السيبراني والقانون الدولي الإنساني، مختارات من المجلة الدولية للصليب الاحمر، المجلد (٩٤) العدد (٨٨٦)، ٢٠١٢، ص ٥١٨

(١٠) د/ عادل عبد الصادق، أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي، السياسة الدولية، القاهرة، ٢٠١١، ص ١٧

(١١) احمد عبيس نعمة الفتاوي، زهراء عماد مجيد، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، المجلد ١، العدد ٤٤، آذار، جامعة الكوفة – كلية القانون، ٢٠٢٠، ص ٥١ -٥٢

(ISSN: ٢٣٥٦ - ٩٤٩٢)

ويعرف (Mattew C.Waxman) الهجمات السيبرانية بأنها الجهود الرامية الى تغيير، تعطيل او تدمير أنظمة الحاسوب او الشبكات أو المعلومات او البرامج الموجودة عليها، والأضرار التي تسببها هذه الهجمات يمكن انْ تصيب شبكة الحاسوب او المرافق المادية او الأشخاص وتتراوح اضرار الهجمات السيبرانية من القرصنة الخبيثة وتشويه مواقع الانترنت الى دمار واسع النطاق للبنية التحتية العسكرية والمدنية المرتبطة بتلك الشبكات. (١٢)

كما جاء في دليل تالين أن الهجمات السبرانية هي "عمليات الكترونية سواء كانت هجومية أو دفاعية من المتوقع بشكل معقول أن تتسبب في إصابة الأشخاص أو موتهم أو الحاق الضرر أو تدمير الأشياء". (١٣)

ومن خلال ما تقدم يمكن تعريف الهجمات السيبرانية أنها: العمليات العدائية التي تستهدف شبكات الحاسوب والمنشآت المرتبطة بها لغرض تحقيق إصابات وأضرار مادية في المعلومات المخزنة في الحواسيب والبنية التحتية من خلال استخدام الفضاء السيبراني وتنفيذ الهجمات داخله، وقد تصل إلى الموت أو التدمير الكلي للبنية التحتية، وباختصار هي هجوم يقوم على التغلغل ومن ثم السيطرة وأخيراً التحكم عن بعد لتتحول الأوامر الرقمية إلى نشاط مادي لأجل التعطيل أو التدمير في الهدف أو العين المدنية المستهدفة من الهجوم شريطة ان تكون محمية أو مفعلة بواسطة برنامج الكتروني.

وعلى ذلك نلاحظ إهمال هذه التعاريف دور العنصر البشري الذي يعد الأساس لتنفيذ هذه الهجمات، كما تقاربت في تركيزها على الوسيلة الالكترونية والهدف أو المحل الالكتروني (حواسيب وكل ما يتصل بها) أيضا ركزت في مجملها على الأثار والأضرار التي تنتج عن هذه الهجمات، واتسع التعريف الذي قدمه الخبراء في دليل تالين ليشمل الهجمات السبرانية الدفاعية والهجومية في رغبة من الفقه في احتواء أكبر قدر من الوقائع بمفهوم الهجمات السبرانية.

(١٢) حيدر أدهم الطائي، علي محمد كاظم، المشاركة المباشرة للهبة الجماعية في الهجمات السيبرانية، مجلة كلية الحقوق، المجلد ٢١، العدد ٢، جامعة النهرين، ٢٠١٩، ص ٣٠

(١٣) دليل تالين، جهد أكاديمى مميز لمجموعة من الخبراء في القانون الدولى والمسائل التكنولوجية المعاصرة عن يحيي ياسين مسعود، الحرب السيبرانية في ضوء قواعد القانون الدولى الإنسانى، المجلة القانونية، المجلد ٤، ٢٠١٨، ص٩٤

الفرع الثالث

خصائص الهجمات السيبرانية

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

١- الهجمات السيبرانية هي هجمهات تقنية متطورة، عكست قمة التطور الذي وصلت إليه ثورة المعلومات، فهى تعكس التطور الحاصل في مجال البرمجيات والحواسيب والاتصالات.

٢- التكلفة المتدنية نسبياً للهجمات السيبرانية، مقارنة مع الميزانيات الضخمة التي تخصص لإنتاج أسلحة تقليدية كالغواصات والمقاتلات المتطورة، 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.(١٤)

٣- الهجوم السيبراني قد يحدث في أي وقت وبمدة قصيرة من الزمن، سواء في السلم، أو في الحرب فهى هجمات خاطفة وسريعة.

٤- يتمتع المهاجم بميزة واضحة في الهجمات السيبرانية على المدافع، لأن هذه الهجمات تتميز بالسرعة والمرونة والمراوغة، فمن غير المرجح أن تنجح عقلية التحصن لوحدها، لأن التحصين في هذا الاتجاه سيجعل الجانب الآخر عرضة لمزيد من محاولات الاختراق، وبالتالي المزيد من الضغط.(١٥)

٥- لا تعرف الهجمات السيبرانية الحدود الجغرافية فهي متنوعة ومتطورة بوسائلها المرتبطة بأكثر المجالات التقنية تطوراً وتغيراً في الحياة المعاصرة للدول، وهي علاوة على ذلك، غير محدودة الأهداف والنتائج، إذ قد تتعدى مخاطرها ميادين القتال التقليدية لتصل بدمارها إلى أكثر المواقع السيادية والحساسة تحصيناً وبعداً عن دائرة القتال.

٦- صعوبة تحديد موقع وشخصية القائم بالهجمات السيبرانية ذات التأثير العالي لكونها لا تترك أثر أو دليل على حصولها، إذ إن معظم الهجمات السيبرانية يتم اكتشافها بالصدفة، وبعد فترة طويلة وبمساعدة المهارات الفنية عالية المستوى لاكتشاف مصدر الهجوم. (١٦)

---

(١٤) نور أمير الموصلى، الهجمات السيبرانية في ضوء القانون الدولى الإنسانى، رسالة ماجستير في القانون الدولى الإنسانى، الجامعة الافتراضية السورية، ٢٠٢١، ص١٠، وكذلك لمى عبد الباقي محمود، اسراء نادر كيطان، المسؤولية الدولية عن الأضرار التي تحدثها الهجمات الالكترونية، عدد خاص لبحوث التدريسيين مع طلبة الدراسات العليا، الجزء الثاني، المجلد ٣٢، سبتمبر ٢٠٢١، ص٣٨٣

(١٥) نور أمير الموصلى، الهجمات السيبرانية في ضوء القانون الدولى الإنسانى، رسالة ماجستير في القانون الدولى الإنسانى، ٢٠٢١، ص١١

(١٦) لمى عبد الباقي محمود، اسراء نادر كيطان، المسؤولية الدولية عن الأضرار التي تحدثها الهجمات الالكترونية، المرجع السابق، ص٣٨٤

(ISSN: ٢٣٥٦ - ٩٤٩٢)

٧- لا حدودية من حيث النطاق الجغرافي وأيضا من حيث الأهداف والنتيجة فقد تتعدى الهدف المرصود الى مواقع سيادية وحساسة. (١٧)

٨- وتتميز الهجمات السيبرانية بأنها تدمير لا تصاحبه دماء وأشلاء بالضرورة، ويسبب انتشار الفضاء السيبراني وسهولة الوصول إليه يمكن أن يزيد عدد المهاجمين وكذلك توسع دائرة المواقع المستهدفة، ولتدور تلك الهجمات المتبادلة على نحو من الكر والفر ليعبر عن حالة صراع مطولة مرتبطة بالطبيعة المتنوعة للفضاء السيبراني. (١٨)

الفرع الرابع

طبيعة الهجمات السيبرانية

خلق تحديد طبيعة الهجمات السيبرانية مشاكل عملية وجدلاً بين الخبراء القانونيين، كما أنه بسبب التطور التقني الحاصل أدى الك إلى ظهور العديد من المصطلحات والمفاهيم المتشابهة مع بعضها البعض في المجالات التقنية والمعلوماتية ولا سيما في إطار المصطلحات المشتقة من السايبر، 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.

إذا ما استخدمت الهجمات السبرانية بذاتها للتسلل الى أنظمة الالكترونية معدة للحماية أو تنظيم سير عمل منشأة حيوية للسيطرة عليها وتدميرها كالهجوم الأمريكي الإسرائيلي على مفاعل نطنز عبر استخدام فيروس ستاكس نت في هذه الحالة يعد الهجوم السبراني وسيلة للقتال أي سلاح يهاجم به العدو، يخضع استعماله لقواعد القانون الدولي الإنساني.

أما إذا أسهم الهجوم السبراني في توجيه العمليات الحركية وتسهيل عمل القوة العسكرية التقليدية فتعد أسلوب قتال، على غرار الهجوم الذي سبق التدخل الإسرائيلي في مدينة دير الزور السورية سنة ٢٠٠٧، إذ تم تعطيل الرادارات السورية لتسهيل مرور الطائرات الإسرائيلية، أيضا الهجوم السبراني الذي سبق، التدخل الروسي في جورجيا عام ٢٠٠٨ وسواء استخدم الهجوم السبراني كوسيلة أم طريقة قتال أو الاثنين في الوقت ذاته فيجب ألا يتعارض مع أحكام قواعد القانون الدولي بأي شكل من الأشكال. (١٩)

---

(١٧) أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، المرجع السابق، ص٢١.

(١٨) على عبد الرحيم العبودى، "هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين"، المجلة العلمية الأكاديمية العراقية، العدد (٥٧)، جامعة بغداد، كلية العلوم السياسية، ٢٠١٩، ص ٨٩ -١١٨، ص ٩٩ -١٠٠ -١٠١

(١٩) أحمد عبيس نعمة الفتلاوي، الهجمات السبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلبي للعلوم القانونية والسياسية، ع الرابع، س الثامنة ٢٠١٦، ص ٦١٩

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،(٢٠) 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 سيرعمل منشأت حيوية للسيطرة عليها وتدميرها، فهنا تعد الهجمات السيبرانية وسيلة للقتال أي سلاحاً تهاجم به العدو. (٢١)

وإن من أهم الإشكاليات التي تواجه المجتمع الدولي في طريقة التعامل مع الهجمات السهيبرانية 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. (٢٢)

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.(٢٣)

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 تلزم المادة ٣٦ من البروتوكول الإضافي الأول لعام ١٩٧٧ كل دولة من الدول الأطراف التحقق من امتثال أي أسلحة جديدة تقوم بنشرها أو تدرس نشرها لقواعد القانون الدولى الإنسانى. (٢٤)

---

(٢٠) نيلس ميلزر، مقدمة شاملة القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر، ٢٠١٦، ص١٠١
(٢١) أحمد عبيس نعمة الفتلاوى، الهجمات السيبرانية "دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر"، ص٢١
(٢٢) زهراء عماد محمد: المسئولية الدولية الناشئة عن الهجمات السيبرانية، جامعة الكوفة-كلية القانون، جمهورية العراق، إشراف الدكتور: أحمد عبيس نعمة الفتلاوي، ٢٠١٦ م، ص ٣١
(٢٣) محمود إبراهيم عبد الرحمن شهاب، الأسلحة غير التقليدية في الفقه الإسلامي، الجامعة الإسلامية، رسالة ماجستير، كلية الشريعة والقانون، غزة، ٢٠٠٧، ص٢
(٢٤) القيود التي يفرضها قانون الحرب على الهجمات السيبرانية، مقال منشور على موقع اللجنة الدولية للصليب الأحمر، على الموقع التالى:
https://www.icrc.org/ar/doc/resources/documents/faq/١٣٠٦٢٨-cyber-warfare-q-and-a-eng.htm

(ISSN: ٢٣٥٦ - ٩٤٩٢)

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. (٢٥)

ونستنتج من ذلك أن الهجمات السيبرانية تشكل وسيلة وأسلوب للقتال في الوقت نفسه، وذلك وفق الأهداف المستخدمة لتحقيقها. وقد جالبت 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. (٢٦)

المطلب الثانى

أنواع الهجمات السيبرانية وأمثلة عليها وتكييفها القانوني

الفرع الأول

أنواع الهجمات السيبرانية

أولاً: هجوم الحرمان من الخدمة

وهذا النوع يكون 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. (٢٧)

(٢٥) زهراء عماد محمد: المسئولية الدولية الناشئة عن الهجمات السيبرانية، المرجع السابق، ص ٣٢

(٢٦) نور أمير الموصلى، الهجمات السيبرانية في ضوء القانون الدولى الإنسانى، رسالة ماجستير في القانون الدولى الإنسانى، ٢٠٢١، ص١٣

(٢٧) نور أمير الموصلى، الهجمات السيبرانية في ضوء القانون الدولى الإنسانى، رسالة ماجستير في القانون الدولى الإنسانى، ٢٠٢١، ص١٦

ثانياً: الفايروسات (البرامج الخبيثة)

الفايروس 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 تهدف 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 الفضهل 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، وأبرز خصائص الفايروسات بشكل عام تتجلى في قدرتها على الاختفاء، وقدرتها على الانتشار، وقدرتها على الاختراق، وقدرتها على التدمير. [٢٨]

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 توضه 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، فضلا 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، فضهلاً 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 يوقب انفجارها.[٢٩]

(٢٨) عمار عباس الحسيني، جرائم الحاسب والانترنت (الجرائم المعلوماتية)، الطبعة الأولى، منشورات زين الحقوقية، بيروت لبنان، ٢٠١٧، ص١٤٠-١٤١

(٢٩) عمار عباس الحسيني، جرائم الحاسب والانترنت (الجرائم المعلوماتية)، الطبعة الأولى، منشورات زين الحقوقية، بيروت لبنان، ٢٠١٧، ص١٤٣-١٤٤

(ISSN: ٢٣٥٦ - ٩٤٩٢)

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، ويفضل 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 لنشهر 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.(٣٠)

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

الفرع الثانى

أمثلة على الهجمات السيبرانية

رغم حداثتها فإن الهجمات السيبرانية تتخذ صورتين قد تلجأ إلىهما أطراف النزاع المسلح وهما:

الصورة الأولى: الهجمات المرافقة للهجوم التقليدي

وفي هذه الصورة يلجأ أطراف النزاع إلى استخدام الهجمات السيبرانية جنباً إلى جنب مع الهجوم التقليدي (الحركي) بهدف تقديم الدعم اهذا النوع من الهجوم، وسنعمل على استعراض بعض الأمثلة على الهجمات السيبرانية التي تكون مرافقة للهجوم التقليدي وكما يأتي:

١- هجوم مدينة دير الزور السورية

وهو هجوم قام به سلاح الجو الإسرائيلي بتاريخ ٦/أيلول/عام ٢٠٠٧ مستهدفا تعطيل دفاعات الجو السورية في أثناء مهاجمة منشآت مشتبه بأنها تتضمن مفاعلاً نووياً في مدينة دير الزور السورية وقد كان هذا الهجوم بالتزامن مع هجوم جوي قامت به مقاتلات سلاح الجو الإسرائيلي، وبالتالي تمكنت هذه المقاتلات من تحقيق أهدافها بسهولة ودقة، وقد وصفت هذه الهجمات السيبرانية بأنها عالية الدقة لأنها منعت الدفاعات السورية من كشف موقع الطائرات المهاجمة وتعقب مساراتها.

(٣٠) مار عباس الحسيني، جرائم الحاسب والانترنت (الجرائم المعلوماتية)، المرجع السابق، ص١٤٥-١٤٦، ونفس المعنى نور أمير الموصلى، الهجمات السيبرانية في ضوء القانون الدولى الإنسانى، المرجع السابق، ص١٨

وبهذه الطريقة أثبتت الهجمات السيبرانية قدرتها على مواكبة الهجمات التقليدية بشكل تكاملي مما أدى إلى تحسين أداء القوات المهاجمة في الهجوم التقليدي.(٣١)

٢- النزاع المسلح الروسي الجورجي عام ٢٠٠٨

بعد إعلان استقلال بلدة (أوستيا) الجنوبية عن جورجيا في آب عام ٢٠٠٨ اندلع نزاع مسلح بين روسيا وجورجيا، وقبل بدايته بيوم واحد شنت روسيا هجوما سيبرانياً واسعاً استهدف البنية التحتية المرتبطة بشبكة الانترنت.

ونتج عن هذه الهجمات (ميزة عسكرية أكيدة) مشكوك في مشروعيتها للجيش الروسي، إذ أنها استهدفت عناصر اقتصاد الدولة الجورجية ومؤسساتها المالية والإعلامية، والبنى التحتية المهمة للاتصالات والمعلوماتية والتي سببت حالة من الذعر بين المواطنين.(٣٢)

ومن خلال ما تقدم يتبين لنا الفائدة المتوخاة من تزامن الهجمات السيبرانية مع الهجمات التقليدية والاسهام الكبير في تحقيق الأهداف المطلوبة دون أن تتمكن القوات المسلحة للدولة المستهدفة من كشف مصدر تلك الهجمات أو منعها.

الصورة الثانية: الهجمات المستقلة

تتخذ هذه الصورة من الهجمات شكلاً مغايراً عن الصورة الأولى المرافقة للهجوم التقليدي(الحركي)، إذ تستخدم الهجمات المستقلة في حالة عدم وجود نزاع مسلح معلن من خلال استهداف أهداف، أو بنى تحتية معينة يكون لها أثر اقتصادي أو سياسي، وسنحاول بيان أنواع هذه الهجمات وكما يأتي:

١- الهجمات الروسية على إستونيا

في عام ٢٠٠٧ وجهت روسيا الاتحادية هجوماً سيبرانياً استهدف تعطيل شبكات الاتصالات الالكترونية في إستونيا وكانت المواقع الرسمية الحساسة مثل موقع رئيس الوزراء ورئيس البرلمان هي الأكثر استهدافاً فضلا عن مواقع حكومية أخرى.

وقد لجأت روسيا إلى استخدام برنامج تعطيل الخدمات الالكترونية ضد مواقع الكترونية جورجيا من خلال سيل البيانات غير الضرورية التي يستخدمها القراصنة ومخترقي شبكات الحاسوب عن بعد بإرسالها وإغراق المواقع الالكترونية بالشكل الذي يعمل على تعطيل النظام وبالتالي يصعب من مهمة المستخدمين في الوصول إليه وهذا النوع يسمى (إيدز الانترنت)، إذ يتم انجاز المهمة دون أن تكسر

(٣١) د. احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: فهو مفهومها المسؤولية الدواية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق المحلي للعلوم القانونية والسياسية، كلية القانون جامعة بابل، العدد الرابع، السنة الثامنة، ٢٠١٦، ص ٦٢٤

(٣٢) حسام عبد الامير خلف، البعد الجديد-الخامس-في النزاعات المسلحة الفضاء الالكتروني، مجلة كلية الحقوق، جامعة النهرين، العدد (١)، ٢٠١٦، ص ١٢٦

(ISSN: ٢٣٥٦ - ٩٤٩٢)

كلمات المرور أو تسرق البيانات السرية، إنما هي مسألة إطلاق برنامج يؤدي إلى ازدحام المرور للمواقع الالكترونية ومنع المستخدمين من الوصول إليها.(٣٣)

وقد عدت إستونيا هذه الهجمات انتقامية كونها متزامنة مع قيامها بنقل النصب التذكاري الذي يخلد الجيش الروسي من العاصمة (تالين) إلى مكان مجهول.(٣٤)

٢- الصراع السيبراني الأمريكي الإيراني

رغم عدم وجود مواجهة عسكرية مباشرة وعلى نطاق واسع بين الولايات المتحدة وايران، إلا ان سبل المواجهة الخفية ولاسيما السيبرانية كانت ولا زالت الأبرز على نطاق العمليات العدائية، ففي عام ٢٠٠٩ تعرضت أنظمة السيطرة في المنشآت النووية الإيرانية إلى سلسلة من الهجمات السيبرانية استمرت لمدة تسعة أشهر بدء من عام ٢٠٠٩ وحتى منتصف عام ٢٠١٠ من خلال التسلل إلى منشآت (نطنز) و(بوشهر) باستخدام فايروس (Stuxnet) والذي صمم لاستهداف نظم التحكم والسيطرة وأجهزة الطرد المركزية بهدف التحكم عن بعد والعمل على خروجها عن السيطرة، من دون أي مؤشر غير طبيعي على عمل تلك الأجهزة.(٣٥)

واستمرت سلسلة الهجمات السيبرانية الأمريكية على الخوادم الإيرانية وكان آخرها الهجوم الذي تعرضت له إيران في شهر شباط من عام ٢٠٢٠، والذي أدى إلى انقطاع الانترنت بنسبة (٧٥٪) في عموم البلاد، وقد أشارت مؤسسة (نت بلوكس) التي تعنى بالأمن السيبراني أن البيانات الصادرة عن إيران كشفت عن تعطيل شبكات الاتصالات الإيرانية عدة ساعات وهو ما اضطرها إلى حجب شبكة الانترنت لتتمكن من صد الهجمات السيبرانية والحفاظ على أمن البنية التحتية والجدير بالذكر أن آخر هجوم تعرضت له منشأة (نطنز) الايرانية كان بتاريخ ٣٠ / حزيران عام ٢٠٢٠، تسبب في انفجار المنشأة دون حصول خسائر بشرية.(٣٦)

٣- الهجمات السيبرانية على قطاع الصحة

كغيره من البنى التحتية التي تعتمد على التشغيل والإدارة والتحكم الالكتروني، يمكن أن يتعرض القطاع الصحي إلى هجمات سيبرانية تستهدف أهدافاً حيوية، مع اختلاف الغرض من الهجوم، إذ

(٣٣) سراب ثامر أحمد، الهجمات على شبكات الحاسوب في القانون الدولي الإنساني، أطروحة دكتوراه، كلية الحقوق، جامعة النهرين، ٢٠١٥، ص ٨٣

(٣٤) د. احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها المسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلبي للعلوم القانونية، كلية القانون جامعة بابل، العدد الرابع، السنة الثامنة، ٢٠١٦، ص ٦٢٤

(٣٥) الفايروس في مجال الحاسبات هو برنامج يصمم لإحداث إرباك أو خراب في برمجيات الحاسوب، وباستطاعته أن يتكاثر ويعيد إنتاج نفسه باستعمال وحدات وتجهيزات وبرامج الحاسوب دون علم صاحب جهاز الحاسوب أو ستعمل شبكة الحاسوب ويزداد تأثيرها يوماً بعد يوم، ينظر في ذلك: مصطفى محمد موسى، السيرة الذاتية للفايروسات الالكترونية سلسة اللواء الامنية في مكافحة الجريمة الالكترونية، الكتاب الرابع ط ١، دار الكتب القانونية، مصر، ٢٠٠٨، ص٤٦

(٣٦) د/ أحمد عبيس نعمة الفتلاوى، د/ أزهر عبد الأمير الفتلاوى، المسؤولية الناشئة عن استخدام وسائل القتال الفتاكة في نشر الأوبئة "الهجمات السيبرانية مقابل جائحة كورونا"، مجلة الحقوق، العدد ٤١، ص٦٥

مع تطور التكنولوجيا الحديثة تحتاج المستشفيات وقطاعات الصحة الأخرى إلى مواكبة هذا التطور من خلال الاعتماد على الارتباط الرقمي بمراكز التشغيل والسيطرة من خلال شبكة الانترنت (مثل الاتصال بالمختبرات والمستشفيات الأخرى والمرضى وموردي الأدوية وغيرهم).

والسؤال الذي يمكن أن نطرحه هنا هو: هل يمكن نشر الفيروسات الفتاكة من خلال الهجمات السيبرانية على القطاعات الصحية والعلمية؟

للإجابة نقول إن مواكبة التطور الحاصل في مجالات التحكم والسيطرة الالكترونية أو ما يصطلح عليه ايضا بالأتمتة الالكترونية زاد من إمكانية استهداف القطاعات الصحية عن طريق استخدام الهجمات السيبرانية، بسبب وجود ثغرات في منظومة الحماية المعلوماتية في تلك القطاعات، باعتبارها تقدم خدمات عامة للمرضى والمحتاجين للرعاية الصحية، وهو ما يصب في تدهور القطاع الصحي والخدمات التي تقدمها، والاكثر من ذلك هو في امكانية استخدام الهجمات السيبرانية لأجل تعطيل خدمات صحية، فضلا عن التصدي للفايروسات الفتاكة بصورة مباشرة أو غير مباشرة ، على سبيل المثال الهجمات السيبرانية التي استهدفت الحصول على فدية من مستشفى في(هوليود) قيمتها (٣,٦) مليون دولار والتي أعاقت رعاية المرضى لعدة أيام، كذلك هجوم آخر في سنغافورة في عام ٢٠١٦ أصاب الأجهزة الطبية لأكثر من عشرة أشهر، إذ تم اختراق حساب مليون ونصف مستخدم من ضمنها ١٦,٠٠٠ وصفة طبية.[٣٧]

والملاحظ أن المستشفيات ليست وحدها التي قد تكون هدفاً للهجمات السيبرانية، فشركات الأدوية هي الأخرى تكون مستهدفة لسرقة الملكية الفكرية، لكن المنشآت الصحية الأكثر أهمية والتي تكون عرضة للاستهداف هي المنشآت العلمية المخصصة لإجراء البحوث العلمية وإنتاج وتهجين وتخزن الفيروسات وهي موضوع بحثنا.

إذ أنه من الممكن استهداف هذه المخازن بهجمات سيبرانية وإطلاق الفيروسات الفتاكة المخزنة فيها وبالتالي انتشارها، والتي من المحتمل أن تنتشر عن طريق الهواء وأية طريقة أخرى تساهم في انتشارها، وبالتالي التسبب في انتشار الأمراض والأوبئة.

وقد يرى منفذي الهجمات السيبرانية أن المستشفيات تكون أهدافاً سهلة ويمكن من خلالها تحقيق أهداف اقتصادية من خلال دفع الفدية كما أسلفنا.

(٣٧) د/ أحمد عبيس نعمة الفتلاوى، د/ أزهر عبد الأمير الفتلاوى، المسؤولية الناشئة عن استخدام وسائل القتال الفتاكة في نشر الأوبئة "الهجمات السيبرانية مقابل جائحة كورونا"، مجلة الحقوق، العدد ٤١، ص٦٦

(ISSN: ٢٣٥٦ - ٩٤٩٢)

وقد أشار أحد الخبراء في اجتماع اللجنة الدولية للصليب الأحمر أنه في أغلب الحالات قد لا تكون هنالك حاجة إلى شفرة خبيثة لتنفيذ الهجوم السيبراني يسبب ضعف حماية الأجهزة الطبية، وقد يكون انتاج تحديث يصمم للاصطدام بالأجهزة الحيوية، مثل أجهزة تنظيم ضربات القلب وغيرها.(٣٨)

وفي تصريح للسيدة "فيرونيك كريستوري" (وهي كبيرة مستشاري الحد من التسلح في اللجنة الدولية للصليب الأحمر) ضمن بيان ألقته أمام (الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي) بتاريخ ١٠ /ايلول/عام ٢٠١٩، إذ أكدت أن قطاع الرعاية الصحية قد يكون معرضاً للهجمات السيبرانية، كغيره من القطاعات الأخرى التي تمثل البنية التحتية للمنشآت الحيوية في أية دولة.

وقد أبدت اللجنة الدولية للصليب الأحمر قلقها في حال تعرضت البنى التحتية في قطاع الصحة للهجمات السيبرانية وما يمكن أن تسببه من الخسائر البشرية المحتملة.

ومن خلال ما تقدم يتبين أنه بالإمكان استهداف المنشآت الصحية والمراكز العلمية التي تم فيها تهجين وتخزين الفيروسات الفتاكة التي تتسبب بنشر الأمراض والأوبئة والسيطرة على المنافذ التي تسمح لها بالخروج والانتشار، وبذلك تساهم الهجمات السيبرانية في نشر تلك الفيروسات.(٣٩)

الفرع الثالث

التكييف القانوني للهجمات السيبرانية

يعد الإجرام السيبراني من بين أهم المسائل الجنائية التي باتت تلقى إهتماماً كبيراً، سواء على المستوى الوطني أو الدولي، وذلك نظراً لإنتشارها الكبير فضلاً عن آثارها الهائلة التي تصيب الدول وكذا الأفراد على حد سواء، وهذا نتيجة تطور المجتمعات الإلكترونية وكذا لجوء العديد من الدول إلى نمط التسيير الرقمي أو ما يسمى بالحكومات الإلكترونية، التي حلت محل التسيير الإداري التقليدي لشئون الدولة.

أولاً: التكييف القانوني للهجمات السيبرانية بين الدول

يعرف البعض الجريمة السيبرانية بكونها عبارة عن نشاط إجرامي، تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي.

لذلك ترى اللجنة الدولية للصليب الأحمر أنه ليس هناك أي فراغ قانوني فيما يتعلق بتنظيم الفضاء السيبراني ككل لكن وبالرغم من أنه ليس هناك من إجماع واسع على تعريف محدد ودقيق

(٣٨) د/ أحمد عبيس نعمة الفتلاوى، د/ أزهر عبد الأمير الفتلاوى، المسؤولية الناشئة عن استخدام وسائل القتال الفتاكة في نشر الأوبئة "الهجمات السيبرانية مقابل جائحة كورونا"، مجلة الحقوق، العدد ٤١، ص٦٧

(٣٩) د/ أحمد عبيس نعمة الفتلاوى، د/ أزهر عبد الأمير الفتلاوى، المسؤولية الناشئة عن استخدام وسائل القتال الفتاكة في نشر الأوبئة "الهجمات السيبرانية مقابل جائحة كورونا"، مجلة الحقوق، العدد ٤١، ص٦٧

لمفهوم الحرب السيبرانية، إلا أنه وعلى الرغم من ذلك، فقد إجتهد عدد من الخبراء كل في مجال تخصصه، لتقديم تعريف يحيط بهذا المفهوم، وفي مقدمتهم الأستاذين "ريتشارك كلارك"، و "روبرتكناكي".(٤٠)

ومن بين سمات الحرب السيبرانية:

أ- الطبيعة اللاتماثلية: أي عدم التكافؤ بين الأطراف المتحاربة من حيث العدة والعتاد، حيث يحتاج القائمون على الهجوم السيبراني بصورة أساسية لأجهزة كومبيوتر لشن هجماتهم السيبرانية ومن ثم فهم لا يحتاجون إلى أسلحة معقدة، مثل المقاتلات العسكرية أو حاملات الطائرات لتهديد مصالح القوى الكبرى في النظام الدولي مثل الولايات المتحدة، بل يمكن لحوالي عشرة مبرمجين مهاجمة البنية التحتية الأمريكية وتعطيلها، أو سرقة معلومات حيوية، أو إعاقة قدرتها على إستخدام الأسلحة.

ب- أفضلية الهجوم: يكون للطرف الذي يقوم بشن الهجوم السيبراني اليد العليا، ولذلك وصف البعض الحروب السيبرانية باعتبارها أشبه بحروب المناورات التي يتمتع فيها بالأفضلية الخصم الذي يمتلك مهارات السرعة والمرونة.(٤١)

ج- تصاعد التهديدات للبنية التحتية الحيوية: تتزايد تهديدات الحرب السيبرانية إذا ما تم إستهداف البنية التحتية الحيوية بعمليات تخريبية مثل محطات الكهرباء وأنابيب النفط والخطوط الجوية والسكك الحديدية والبنوك، إذ إن الأضرار المترتبة على ذلك قد تصل قيمتها مئات المليارات من الدولارات، وقد يترتب عليها سقوط آلاف الضحايا. (٤٢)

من الأمثلة على الهجمات السيبرانية التي تستهدف البنية التحتية، إتهام موسكو للولايات المتحدة بشن هجوم سيبراني من خلال هاكرز عسكريين تمكنوا من التسلل إلى أنظمة إلكترونية خاصة بشبكات الطاقة الكهربائية وباتصالات سلكية ولاسلكية روسية، إضافة إلى منظومة القيادة في الكرملين، والتي جعلوها مهيئة للتعررض لهجمات إلكترونية أمريكية عن طريق إستخدام سلاح إلكتروني سري.(٤٣)

يخلص المتمعن في التعاريف السابقة إلى أن الهجمات السيبرانية التي تشنها الدول ضد بعضها البعض، يمكن أن تصنف على أنها إجرام سيبراني ترعاه الدول، لا سيما تلك العمليات التي لا تنفذها

(٤٠) حول جهود الأستاذين "ريتشارك كلاركر" و "روبرتكناكي"، راجع: المجال الخامس...الحروب الإلكترونية في القرن ال ٢١، موقع الجزيرة للدراسات، متاح على الرابط التالي:
http://studies.aljazeera.net/issues/٢٠١٠/٢٠١١٧٢١٢٢٧٤٣٤٦٨٦٨.htm.

(٤١) عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، المركز العربي لأبحاث الفضاء الالكتروني، مصر، ٢٠١٨، ص٥٣

(٤٢) شادي عبد الوهاب منصور، حروب الجيل الخامس: أساليب التفجير من الداخل على الساحة الدولية، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة – مصر، ٢٠١٩، ص١٠١

(٤٣) يحي مفرح الزهراني، الأبعاد الإستراتيجية والقانونية للحرب السيبرانية، مجلة البحوث والدراسات، جامعة الوادي، العدد ٢٣، السنة ٢٠١٧، ص٢٤١

(ISSN: ٢٣٥٦ - ٩٤٩٢)

الدولة بنفسها أو عن طريق أحد موظفيها أو أعوانها، وإنما يشن من قبل أشخاص معنوية على سبيل المثال الشركات التجارية وغيرها.

على هذا الأساس نصت إتفاقية بودابست لعام ٢٠٠١، المتعلقة بالجريمة السيبرانية في المادة ١٢، على مسؤولية الأشخاص المعنوية، وعلى ضرورة أن تسن الدول الأطراف نصوص قانونية ترتب المسؤولية على من يرتكب أي جريمة سيبرانية.(٤٤)

وما يعاب على هذه الإتفاقية، وهذه المادة بالذات، أنها لم تحدد ما إذا كانت الدولة أو أحد فروعها معنيا بأحكامها، وهذا ما يستوجب استبعاد نصوصها وضرورة البحث عن نصوص قانونية يمكن تطبيقها على الهجمات السيبرانية التي تشنها الدول.(٤٥)

- **<u>الهجمات السيبرانية بين الدول حرب سيبرانية</u>**

تثير الهجمات السريبرانية بين الدول عدة مسائل حاسمة في سبيل تكييف تلك الهجمات تكييفاً قانونياً صحيحاً، بمعنى هل تعتبر جريمة أم حرباً سيبرانية؟، وبالتالي يستلزم التطرق إلى صفات المجرم المعلوماتي، وهل تنطبق تلك الصفات على الدول أم لا؟، وكذا الكشف عن مسائل أخرى ذات الصلة، كالدوافع التي تدفع الدول إلى اللجوء إلى هذا العمل الإجرامي، وكذا الأساليب التي تستعمل عند قيامها بهذه الجرائم.

نظراً لأهمية هذا المسعى، وخطورة الجريمة السيبرانية في مثل هذه المسائل التي تمس بالأمن القومي للدول من جهة، وللطبيعة القانونية المعقدة للجريمة المعلوماتية التي تقع بين الدول من جهة أخرى، لذلك تحتم على الدول والقانونيين البحث في هذه المسألة الشائكة، التي باتت تؤرق جميع الدول، والمتمثلة في الإعتداءات الدولية بإستخدام البرمجيات الخبيثة قصد تدمير المعطيات السيبرانية أو الشبكات الأخرى التي تسير البنية التحتية الكبرى للدول، كمحطات الكهرباء، والسدود...الخ.(٤٦)

تبنى في هذا الصدد، آخرون مصطلح الحرب السيبرانية، وهذا إستناداً إلى إيديولوجية أمنية أو عسكرية، تضع منهاجاً لتحقيق أهدافا على الصعيد الأمني أو العسكري تجاه (العدو المفترض) وهذا ما يطبع الهجمات السيبرانية بين الدول بميزة أساسية تتمثل في الشمولية.

---

(٤٤) شادي عبد الوهاب منصور، حروب الجيل الخامس: أساليب التفجير من الداخل على الساحة الدولية، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة – مصر، ٢٠١٩، ص١٠٢

(٤٥) لإطلاع أكثر، راجع: أحمد زهران، موسوعة نظم وأساليب الحرب الحديثة، الطبعة الأولى، مطابع الأهرام التجارية، مصر، ١٩٨٩، وراجع كذلك: حيدر رندة، السلاح السيبراني في حروب إسرائيل المستقبلية، مؤسسة الدراسات الفلسطينية، بيروت – لبنان، ٢٠١٨

(٤٦) يعد الأمن الإلكتروني للدولة جزء لا يتجزأ من أمنها القومي، لاسيما ما تعلق منه بأنظمة المعلومات الخاصة بالقطاعات الحساسة

في نفس السياق، عادة ما ينصب إهتمام المختصين في القانون الدولي الإنساني على وصف الوسيلة والأثرر، وبعبارة أخرى، التركيرز على وسيلة الهجوم وطريقة تنفيذها وما سينجم عنها من آثار، أكثر من التركيز على ما تحتويه وسائل وطرائق القتال ذاتها.(٤٧)

يؤيد هذا التوجه كل من توماس رد وبيتر ماكبورنى المختصان في القانون الدولي الانساني إذ ذهبا إلى تفضيل إصطلاح الهجوم السيبراني، بدلاً من الحرب السيبرانية على أساس أن الأخير أوسع نطاقا من الأول.(٤٨)

- **الهجمات السيبرانية بين الدول جريمة سيبرانية ذات طابع خاص**

يعتبر الأمن السيبراني أحد عناصر الأمن القومي غير التقليدية، وذلك لأن أحد مستخدمي الفضاء الإلكتروني بإمكانه أن يوقع خسائر فادحة بالطرف الآخر وأن يتسبب في شل البنية المعلوماتية والإتصالات الخاصة به، وهو ما يسبب خسائر عسكرية وإقتصادية فادحة، من خلال قطع أنظمة الإتصال بين الوحدات العسكرية وبعضها البعض، أو تضليل معلوماتها أو سرقة معلومات سرية.(٤٩)

قد تحدث الحرب السيبرانية ليس لأسباب عسكرية محضة بل لمجرد الخلاف السياسي، أو بهدف سرقة المعلومات الإستراتيجية لمعرفة فيما يفكر الخصم أو حتى سرقة تصميمات الأسلحة العسكرية والتقنيات التكنولوجية الحديثة، الأمر الذي دفع الولايات المتحردة إلى عقد إتفاقية مع الصين لعدم شن هجمات سيبرانية على البنية التحتية الأمريكية أو شركات القطاع الخاص في حالة السلم.(٥٠)

ما يجعل أيضا الهجمات السيبرانية بين الدول ذات طابع خاص تكييفها في كثير من الأحيان على أنها إرهاب سيبراني: حيث أصبح عديد من الدول حول العالم تعتمد على فكرة نشر وإستخدام التقنيات الذكية والجديدة، سواء داخل المؤسسات والهيئات أو بين الأفراد وداخل المجتمع وتمثل إتاحة مثل هذه التقنيات سلاحاً ذا حدين فكما يمكن إستخدامه في تحسين جودة حياة البشر داخل المدينة يمكن إستخدامه أيضاً في تهديد أمن الأفراد بالأمن القومي للدولة، لذلك نجد أن بعض الدول حظرت إستخدام بعض هذه التقنيات الحديثة مثل الطائرات من دون طيار وذلك تخوفاً من إستخدام الحركات الإرهابية لهذه التقنية في تنفيذ عمليات إرهابية عن بعد، ولذلك يمثل الإرهاب السيبراني خطراً على الأمن القومي من خلال توظيف التقنيات الذكية في تنفيذ عمليات إرهابية سيبرانية.(٥١)

(٤٧) أحمد عبيس نعمة الفتيلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلبي، كلية القانون، جامعة بابل، ٢٠١٥

(٤٨) يحي مفرح الزهراني، الأبعاد الإستراتيجية والقانونية للحرب السيبرانية، نفس المرجع، ص٢٤١

(٤٩) إيهاب خليفة، تأثير الثورة الصناعية الرابعة على الأمن القومي: مجتمع ما بعد المعلومات، د. ر. ط، العربي للنشر والتوزيع، القاهرة – مصر، ٢٠١٩، ص ١٣٦ وص ١١٥

(٥٠) إيهاب خليفة، تأثير الثورة الصناعية الرابعة على الأمن القومي: مجتمع ما بعد المعلومات، المرجع السابق، ص ١١٥

(٥١) إيهاب خليفة، تأثير الثورة الصناعية الرابعة على الأمن القومي: مجتمع ما بعد المعلومات، المرجع السابق، ص ١٢٣

(ISSN: ٢٣٥٦ - ٩٤٩٢)

إن ما يجعل الهجمات السيبرانية بين الدول جريمة سيبرانية ذات طابع خاص، هو تعدد طبيعة الفاعلين أو الأطراف التي يمكن أن تشن هذه الهجمات، حيث تختلف هذه الأطراف ما بين دول لمنظمات إجرامية، وكذا الأفراد من قراصنة الأنترنت، وهذا ما يجعل من تكييفها أمراً صعباً، حيث يمكن وصفها بالجريمة السيبرانية، كما يمكن في نفس الوقت أن تكيف على أساس أنها حرب سيبرانية، أو الوصيفين معا.

وبالتالي فإن أي هجوم سيبراني، يمكن أن يتم بمشاركة كل هؤلاء الفاعلين وهذا نتيجة للعلاقة الوطيدة التي يمكن أن تجمع بين التنظيمات الإجرامية والحرب السيبرانية، حيث يمكن لعناصر الجريمة المنظمة في الفضاء السيبراني، أن تكون طرفا في حرب سيبرانية ضد دولة معينة، كما يمكن أن تلجأ الدول إلى إستخدام هذه التنظيمات ضد دولة أخرى قصد التمويه، أو الجوسسة السيبرانية.

من ثم، تتضح خطورة التهديدات التي تشكلها الجريمة المنظمة على أمن الفضاء السيبراني للدول، ومن ثم على الأمن الدولي بصفة عامة، وهو الأمر الذي أشارت إلى أهميته تقارير دولية، حيث ذهبت إلى أن العالم بحاجة إلى مليون خبير أمني، للحد من الهجمات السيبرانية الشرسة، وقد جاءت تصريحات الرئيس الأمريكي باراك أوباما، مؤكدة معاناة الدول جراء هذه الحرب في الفضاء المفتوح، حيث أكد أن العالم يحتاج لقوانين جديدة لوقف الهجمات السيبرانية.(٥٢)

فيما صرح العضو الأسبق في مجلس النواب الروسي الدوما (نيكرولاي كوريانوفج) بالقول "في القريب العاجل ستحدث الكثير من النزاعات المسلحة، ولكن لا على أرض المعركة التقليدية، بل من عدد هائل من جنود المعلومات، والتي يمكن أن تحقق أهدافا أمنية وعسكرية أكثر بكثير مما يحقق الآلاف من الجنود المقاتلين في جهات القتال".(٥٣)

ثانياً: تكييف الهجمات السيبرانية وفقاً لأحكام القانون القانون الدولى العام

لم ينظم القانون الدولى صراحة مسألة الهجمات السيبرانية سواء وقت السلم، وهذا راجع إلى الاستخدام الحديث نسبياً لشبكات الإنترنت، بينما قواعد القانون الدولي التي تحكم العلاقات الدولية يرجع تاريخها إلى ما قبل وجود الفضاء السيبراني، وبالتالي فقواعده قد تتلاءم التكنولوجيات الجديدة للحرب، غير أن الاستخدام الواسع للفضاء السيبراني كساحة صراع جديدة بين الدول يؤدى إلى مزيد من التهديدات للسلم والأمن الدوليين، وفي ظل غياب نصوص قانونية خاصة في القانون الدولى العام

(٥٢) أحمد عبيس نعمة الفتيلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلبي، كلية القانون، جامعة بابل، ٢٠١٥

(٥٣) عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، المركز العربي لأبحاث الفضاء الالكتروني، مصر، ٢٠١٨، ص٥٣

حول هذه الهجمات، سنبحث مسألة تكييفها وفقاً للمبادئ الأساسية للقانون الدولى العام، وهى مبدأ السيادة ، ومبدأ حظر استخدام القوة أو التهديد باستخدامها.(٥٤)

أ- <u>الهجمات السيبرانية ومبدأ السيادة</u>

تعد الهجمات السيبرانية إحدى الوسائل الحديثة والأكثر استخداما لصم الصراعات بين الدول، نظر لسرعتها وسهولة استعمالها وقلة تكلفتها، بحيث يمكن لأي دولة أن تعطل المنشآت والبنى التحتية العسكرية والمدنية لدولة أخرى بالضغط على بعض الأزرار، ومن ثم إخضاعها دون استخدام الوسائل التقليدية للحرب. (٥٥)

وقد ارتبط مفهوم السيادة مع البدايات الأولى لنشأة الدولة بالمفهوم الحديث وتنظيم المجتمع الدولي، وتعد معاهدة وستاليا لسنة ١٦٤٨ أول صك دولي وضع الأسس لهذا المفهوم الذي عرف عدة تطورات للتكيف مع الأوضاع الجديدة الناتجة عن التطور الذي عرفه المجتمع الدولي في مختلف المجالات، فالسيادة تقليديا لها مدلول سياسي ويقصد بها السلطة العليا للدولة في الداخل واستقلالها عن غيرها في الخارج،(٥٦) أما من الناحية القانونية فالسيادة هي المصطلح الدولي الذي يدل على الأهلية القانونية للدولة باعتبارها صفة تتميز بها الدولة عن غيرها من أشخاص القانون الدولي،(٥٧) تسمح لها بممارسة اختصاصاتها على الصعيدين الداخلي والدولي على حد السواء،(٥٨) وبإدارة شؤونها دون تدخل من أي دولة أو دول أخرى في إطار أحكام القانون الدولي.(٥٩)

ويعد مبدأ السيادة حجر الزاوية للقانون الدولي خاصة قابليته لمسايرة التطورات الحاصلة في الحياة الدولية، وقد تم الاعتراف به وتكريسه في ميثاق الأمم المتحدة الذي نص على أن تقوم الهيئة على مبدأ المساواة في السيادة بين جميع أعضائها".(٦٠)

لم يعد مفهوم السيادة يقتصر على المفهوم السياسي التقليدي ولا حتى القانوني، بل تطور وتكيف مع التقدم التكنولوجي وظهور الفضاء السيبراني كمجال خامس إلى جانب المجال البري والبحري والجوي والفضاء الخارجي، فظهر مفهوم السيادة السيبرائية"، الذي يعني بسط الدولة سيطرتها وولايتها

(٥٤) عمر محمود أعمر، الحرب الإلكترونية في القانون الدولى الإنسانى، دراسات، علوم الشريعة والقانون، المجلد ٤٦، عدد ٣، ٢٠١٩، ص١٣٦

(٥٥) نور أمير الموصلى، الهجمات السيبرانية في ضوء القانون الدولى، بحث مقدم استكمالاً لمتطلبات نيل درجة ماجستير في القانون الدولى الإنسانى، الجامعة الافتراضية السورية، ٢٠٢١، ص١٨-٢٠

(٥٦) د/ محمد طلعت الغنيمي، الوسيط في قانون السلام، المعارف، الإسكندرية، ١٩٩٣، ص٣١٩-٣٢٢

(٥٧) د/ محمد طلعت الغنيمي، الوسيط في قانون السلام، مرجع سابق، ص٣١٩-٣٢٢

(٥٨) حازم محمد علتم، أصول القانون الدولي العام، القسم الثاني أشخاص القانون الدولي، دار النهضة العربية بالقاهرة، ٢٠٠١، ص٣٤٤-٣٤٥

(٥٩) المرجع نفسه، ص٣٤٧، نفس المعنى احمد وافي، الحماية الدولية لحقوق الإنسان ومبدأ السيادة، دار هومة الجزائر، ٢٠٠٥، ص٤٩

(٦٠) المادة ٢ الفقرة ١ من ميثاق الأمم المتحدة

(ISSN: ٢٣٥٦ - ٩٤٩٢)

القضائية على الفضاء الرقمي المتمثل بشبكة الإنترنت"، ومن ثم حماية أمنها القومي من مخاطر التهديدات الجديدة المرتبطة الفضاء السيبراني الذي لا يعرف حدودا جغرافية بين الدول.[٦١]

ويرتبط مفهوم السيادة السيبرانية ارتباطا وثيقا بمفهوم الأمن السيبراني باعتباره مجموع الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به، وسوء استغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتأمين حماية وسرية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني،[٦٢] وبالتالي أي هجوم تقوم به دولة ضد الشبكات الإلكترونية لدولة أخرى بغرض إحداث اضطرابات في عمل الأنشطة والمرافق العمومية والخاصة للدولة المستهدفة، والمساس بمصالحها "، يشكل انتهاكا لسيادتها.

وعرفه الاتحاد الدولي للاتصالات بأنه مجموع الأدوات والسياسات وضوابط الأمن والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب، وأفضل الممارسات وآليات الضمان والتكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرانية وأصول المؤسسات والمستعملين، وتشمل أصول المؤسسات والمستعملين أجهزة الحوسبة الموصولة بالشبكة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات، ومجموع المعلومات المنقولة أو المحفوظة في البيئة السيبرانية، فالأمن السيبراني هو الجهد المستمر لحماية شبكات وبيانات المؤسسات والأفراد من الاستخدام غير المصرح به أو أي أذى أو اختراق يلحق بالشبكة، غير أن مفهوم السيادة السيبرانية يختلف عن مفهوم الأمن السيبراني، حيث يهدف هذا الأخير إلى حماية البنية التحتية والعمليات المتصلة بالإنترنت، بينما تركز السيادة السيبرانية على المعلومات والمحتوى الذي توفره الإنترنت كامتداد طبيعي للسيادة الوطنية في الفضاء الإلكتروني.[٦٣]

لم تعد القوة العسكرية التهديد الوحيد للدول وللمجتمع الدولي، بل أصبح امتلاك الدول للقوة الإلكترونية يمثل أكبر تهديد لسيادة الدول المستهدفة سواء في المجال العسكري، أو الاقتصادي، أو الثقافي، أو السياسي خاصة في ظل الحكومة الإلكترونية، وذلك من خلال استهداف مختلف الأنظمة

(٦١) حسام جاسم محمد أحمد الدليمي، التطور والتكنولوجي وأثره في سيادة الدول، رسالة ماجستير، كلية القانون والعلوم السياسية، جامعة الانبار، العراق، ٢٠١٨، ص١١٤، وكذلك فاطمة بيرم، السيادة الوطنية في ظل الفضاء السيبراني والتحويلات الرقمية "الصين نموذجا"، المجلة الجزائرية للأمن الإنساني، العدد ١، ٢٠٢٠، ص٧٨٩

(٦٢) فاطمة بيرم، السيادة الوطنية في ظل الفضاء السيبراني والتحويلات الرقمية "الصين نموذجا"، المجلة الجزائرية للأمن الإنساني، العدد ١، ٢٠٢٠، ص٧٩٥

(٦٣) سميرة شريطة، السيادة السيبرانية في الصين بين متطلبات القوة وضروريات الأمن القومى، المجلة الجزائرية للأمن والتنمية، المجلد ٩، العدد ١٦، ٢٠٢٠، ٤٠٤

المعلوماتية للدول بغرض السيطرة أو تدمير البيانات والمنشآت المرتبطة بها بأكبر سرعة، وبأقل تكلفة وعبئاً من ناحية المسألة والتبعات.(٦٤)

تشكل الهجمات السيبرانية التي ترتكبها دول على البنى التحتية الرقمية والتقنيات والمحتويات الرقمية والاتصالات انتهاكا للسيادة المحيرانية للدولة المستهدفة، والتي تعد امتدادا لسيادتها الإقليمية على البنى التحتية السيبرائية التي تغطيها سيادتها الإقليمية، وعلى المنشآت العسكرية والاقتصادية والسياسية والثقافية والاجتماعية المرتبطة بهذا الفضاء، فالدولة لها حق سيادي في إدارة شبكة الانترنت الخاصة بها التي يجب أن تعمل بشكل مستقل ودون الخضوع لدول أخرى،(٦٥) وفي الرقابة على مختلف الهيئات والمؤسسات والمنشآت والأنشطة المتواجدة على إقليمها طبقا للقانون الدولي "،(٦٦) وأي مساس بالبنية التحتية الإلكترونية كشبكات الاتصال ومحطات توليد الطاقة وتزويد المواطنين بالحاجيات الأساسية، وغيرها هو انتهاك لسيادتها، بل أن مبدأ السيادة يفرض واجبا على الدول في منع استخدام البنية التحتية الإلكترونية التي تقع على إقليم الدولة وتخضع لسيطرتها في النشاطات التي تستهدف السيادة السيبرانية لدول أخرى، كما أن سيادة الدولة لا تكون على البنية التحتية الإلكترونية الموجودة على إقليمها فقط، وإنما تمتد إلى البنى التحتية التي هي تحت سيطرتها والموجودة على أقاليم دول أخرى.(٦٧)

يتضح من خلال ما سبق أن الهجمات السيبرانية التي تشنها دولة على الفضاء الاقتراضي لدولة أخرى هو مساس بأمنها السيبراني، وهو ما يشكل انتهاكا لسيادتها على مختلف المنشآت والأجهزة المرتبطة بهذا الفضاء التي تقع تحت سيطرتها، ومن ثم فهو عمل دولي غير مشروع، وبالتالي فحماية مختلف الأنشطة (التجارية، والمدنية، وغيرها) يشكل مفتاح للأمن الوطني في المستقبل.

ب- <u>الهجمات السيبرانية ومبدأ حظر استخدام القوة والتهديد باستخدامها</u>

تعد معاهدة وستفاليا في نظر كثير من الفقهاء بداية تشكل القانون الدولي التقليدي القائم على مبدأ المساواة في ممارسة السيادة المطلقة من غير قيد أو حد يحدها، وهو ما أدى إلى اندلاع عدة حروب كمظهر طبيعي لهذه العيادة وأداة لتنفيذ السياسة الوطنية، وخلق حالة من الفوضى واللاستقرار في العلاقات الدولية.(٦٨)

(٦٤) صلاح حيدر عبد الواحد، حروب الفضاء الإلكتروني، دراسة في مفهومها وخصائصها وسبل مواجهتها، رسالة ماجستير، كلية الآداب والعلوم، قسم العلوم السياسية، جامعة الشرق الأوسط، ٢٠٢١، ص٢٠

(٦٥) سميرة شريطة، السيادة السيبرانية في الصين بين متطلبات القوة وضروريات الأمن القومى، المجلة الجزائرية للأمن والتنمية، المجلد ٩، العدد ١٦، ٢٠٢٠، ٤٠٤

(٦٦) أحمد عبيس نعمة الفتلاوى، وزهراء عماد محمد، تكييف الهجمات السيبرانية في ضوء القانون الدولى، مجلة الكوفة للعلوم القانونية والسياسية، المجلد ٤٤، العدد ١، كلية القانون والعلوم السياسية، جامعة الكوفة، ٢٠٢٠، ص٥٧

(٦٧) على محمد كاظم الموسوى، المشاركة المباشرة في الهجملات السيبرانية، المؤسسة الحديثة للكتاب، لبنان، ٢٠١٩، ص٢

(٦٨) د/ عبد الواحد محمد الفار، القانون الدولى العام، دار النهضة العربية القاهرة، ١٩٩٤، ص٤٣١

(ISSN: ٢٣٥٦ - ٩٤٩٢)

ساهم اندلاع الحربين العالميتين وما نتج عنهما من ويلات ودمار على الإنسانية جمعاء في ترسيخ الاعتقاد بضرورة تحريم الحرب كوسيلة لتسوية النزاعات الدولية، ولهذا الغرض تم إنشاء منظمة الأمم المتحدة، حيث نص ميثاقها على حظر استخدام القوة والتهديد باستخدامها في العلاقات الدولية بأية طريقة تتنافى ومقاصد الأمم المتحدة المتمثلة في الحفاظ على السلم والأمن الدوليين " ، بحيث أصبح التدخل أو التهديد باستعمال القوة أو باستخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة مخالف للقانون الدولي باعتباره عملا غير مشروع ٣ باستثناء حالتين: حالة الدفاع عن النفس، وحالة تدخل مجلس الأمن الدولي للمحافظة على السلم والأمن الدولي تطبيقا لنص المادة ٤٢ من الميثاق.(٦٩)

ويتوافق تحريم اللجوء إلى القوة بقاعدة أخرى في الميثاق، وهي قاعدة عدم التدخل في الشؤون الداخلية أو الخارجية لدولة أخرى، ما أكدته محكمة العدل الدولية في عدة قضاياة، كما يكرس ويكمل مبدأ. جواز التدخل في سيادة الدولة على إقليمها، فالتدخل عمل غير مشروع دوليا لما فيه من اعتداء على سيادة واستقلال الدول، كما أنه يشكل اعتداء خطيرا على النظام العام الدولي في المجتمع المعاصر.(٧٠)

إن استعمال القوة أو التهديد باستعمالها يتنافى مع أهداف مقاصد الرامية إلى حفظ السلم والأمن الدوليين، وقد ورد في نص الفقرة ٤ من المادة ٢ من الميثاق مصطلح "القوة" دون اقترانه بأي مصطلح آخر، أي دون تحديد لنوع القوة المستعملة، حيث جاءت الفقرة مطلقة لتشمل كل أشكال القوة، وهذا بخلاف المواطن الأخرى لاستعمال المصطلح في الميثاق، أين يقترن بمصطلح "المسلحة" كما ورد في الديباجة والمادة ٤٤ من الميثاق، وبناء عليه، فإن مفهوم القوة لا ينحصر فقط بالقوة العسكرية، وإنما يشمل كل أنواع التهديد بغض النظر عن الوسيلة المستخدمة طالما أن النية عدائية،(٧١) بحيث يتخذ التدخل باستعمال القوة أو التهديد باستعمالها صورا مختلفة منها التدخل العسكري، أو التدخل المالي، أو التدخل بقصد التخريب، وقد يتخذ التدخل شكلا فرديا أو جماعيا، وقد يكون صريحا ومباشرا، أو خفياً ومقنعاً، كما يحدث في الهجمات السيبرانية.(٧٢)

أدت التطورات التكنولوجية في المجال الإلكتروني إلى ظهور عدة مفاهيم جديدة، منها مفهوم القوة السيبرانية"، حيث أصبح التفوق في المجال الإلكتروني عنصرا حيويا في تنفيذ عمليات ذات فعالية

(٦٩) المادة (٧/٢) من ميثاق الأمم المتحدة
(٧٠) أميرة حناشي، مبدأ السيادة في ظل التحولات الدولية الراهنة، رسالة ماجستير، كلية الحقوق، جامعة منتورى، قسنطينة، ٢٠٠٨، ص٩٠
(٧١) على فاضل على سليمان، حق الدفاع الشرعى على الهجمات السيبرانية، مجلة تكريت للحقوق، السنة ٤، المجلد ٤، العدد ٤، الجزء ١، ص٨
(٧٢) د/ أحمد محمد رفعت، القانون الدولى العام، مكتبة علاء الدين، الإسكندرية، ٢٠٠١، ص١٩٦

على الأرض وفي البحر والجو والفضاء الخارجي من خلال اعتماد القدرة القتالية في الفضاء الإلكتروني على نظم التحكم والسيطرة التكنولوجية،(٧٣) غير أنه يجب التمييز في هذا الإطار بين استخدام الهجمات السيبرانية التي لها نفس الأغراض العسكرية مع الهجمات التقليدية ، والمتمثلة أساسا في استهداف البنية التحتية العسكرية للدول، وأمن المعلومات العسكرية، وبين الهجمات السيبرانية الأخرى التي ليس لها هدف عسكري كالحرب الإعلامية، ونشر الإشاعات والتحويلات المالية بصورة غير شرعية، فوحدها القوة السيبرانية لأغراض عسكرية والتي لها نفس التداعيات الناجمة عن استخدام القوة العسكرية التقليدية من قتل على نطاق واسع، وتدمير للطبيعة وللبنية التحتية للدولة، وسرقة المعلومات والبيانات العسكرية والتلاعب بها، والسيطرة على الأنظمة العسكرية التي تدخل ضمن مفهوم الفقرة ٤ من المادة ٢ من ميثاق الأمم المتحدة.(٧٤)

إن معيار تكييف الهجمات السيبرانية وفقا للمادة ٤/٢ يتعلق بالآثار والأضرار الناتجة عنها وليس بالوسيلة المستعملة، وهو ما أكدت عليه محكمة العدل الدولية في رأيها الاستشاري حول مشروعية التهديد بالأسلحة النووية أو استخدامها، حيث خلصت المحكمة إلى أن القانون الواجب التطبيق على المسألة المعروضة عليها والذي له أكبر صلة مباشرة هو القانون المتصل باستعمال القوة والوارد في ميثاق الأمم المتحدة إلى جانب القانون الواجب التطبيق على النزاع المسلح، كما لاحظت المحكمة أن التطبيق الصحيح للقانون يكون من خلال الأخذ بعين الاعتبار الخصائص الفريدة للأسلحة النووية، ولا سيما قدرتها التسيرية، وقدرتها على التسبب في آلام الإنسانية لا حصر لها، وقدرتها على إيقاع الضرر بالأجيال المقبلة، ومن ثم أكدت بأنه ليس في تلك الأحكام ما يشير إلى أسلحة معينة، فالفقرة ٤ من المادة ٢ تحظر أي استعمال للقوة بصرف النظر عن الأسلحة المستخدمة، وبناء على هذا الرأي، أكنت بعض الدول أن تجاوز حد استخدام القوة لا يتوقف على الوسائل الرقمية المستخدمة، ولكن على آثار العملية السيبرانية"، ومن ثم فالعملية السيبرانية التي تنفذها دولة ضد دولة أخرى تنتهك حظر استخدام القوة إذا كانت آثارها مماثلة (أو تتجاوز) الآثار الناجمة عن استخدام الأسلحة التقليدية، وفي هذه الحالة تنطبق أحكام القانون الدولي الإنساني المتعلقة بحماية الأشخاص والأعيان أثناء النزاعات المسلحة.(٧٥)

(٧٣) يحيي ياسين سعود، الحرب السيبرانية في ضوء القانون االدولى الإنسانى، المجلة القانونية، المجلد القانونية، المجلد ٤، العدد ٤، كلية الحقوق، جامعة القاهرة، ص٨٧

(٧٤) محكمة العدل الدولية، مشروعية التهديد بالأسلحة النووية أو استخدامها، الرأي الاستشاري الصادر في ٨ جويلية ١٩٩٦، موجز الأحكام والفتاوى الصادرة عن محكمة العدل الدولية ١٩٩٢-١٩٩٦، منشورات الأمم المتحدة، نيويورك، ١٩٩٨، ص٢٠١٦، على الموقع www.icj-cij,org/a

(٧٥) التعليق على الفقرة ١ من شرح القاعدة ٦٩ من دليل "تالين" بشأن القانون الدولى المطبق على الحروب السيبرانية، أعد من قبل مجموعة من الخبراء الدوليين، ٢٠١٣، ترجمة محمد كاظم الموسوى، ٢٠١٧، على الموقع www.academia.edu

(ISSN: ٢٣٥٦ - ٩٤٩٢)

وبناء على ما سبق يدخل في مفهوم القوة الوارد في المادة ٢ الفقرة ٤ من ميثاق الأمم المتحدة، الهجمات السيبرانية واسعة النطاق ضد السكان المدنيين أثناء النزاعات المسلحة أو خارجها، كإغلاق أجهزة الكمبيوتر التي تتحكم في محطات المياه والسدود التي ينتج عنها الفيضانات في المناطق المأهولة بالسكان، وكذلك الحوادث الهندسية المميتة والمتعمدة، مثل المعلومات الخاطئة التي تغذيها أجهزة الكمبيوتر للطائرات، وانهيار في محطات الطاقة النووية وانطلاق المواد المشعة في المناطق ذات الكثافة السكانية العالية، التي تتسبب في آثار وخيمة على السكان المدنيين تتجاوز في شدتها آثار الحروب التقليدية، وقد اعتبر أن الهجمات الإلكترونية الخطرة تمثل هجوما مسلحا ، حتى ولو لم يكن هناك إصابات بالأشخاص مثل الهجمات التقليدية التي لا ينتج عنها إصابات أو خسائر في الممتلكات، ولا يوجد أي سبب للوصول إلى استنتاج مختلف فيما يتعلق بالهجمات السيبرانية ضد النظم المدنية، إذ من الصعب الإقرار بشرعية الهجمات السيبرانية فذلك لا يعفي الدول من مسؤولية التدخل وفقا للفقرة ٤ من المادة ٢ من ميثاق الأمم المتحدة، في حال أتت الهجمات السيرانية إلى آثار مادية ملموسة في الأعيان المدنية أو العسكرية.[٧٦]

بينت محكمة العدل الدولية في قضية نيكاراغوا ضد الولايات المتحدة الأمريكية والمتعلقة بالأنشطة العسكرية وشبه العسكرية في سنة ١٩٨٦، أن المادة ٥١ لا تشير إلى أسلحة محددة وأن مفهوم الأسلحة ينطبق على أي استخدام للقوة، وبغض النظر عن حقيقة أن الهجمات السيبرانية" لا تستخدم الأسلحة الحركية التقليدية فإن ذلك لا يعني بالضرورة أنها لا يمكن أن تكون مسلحة"، ويسكن اعتبار استخدام أي جهاز ينتج عنه خسائر كبيرة في الأرواح أو تدمير واسع للممتلكات مستوف لشروط الهجوم المسلح، ويدعم هذا الاستنتاج تأكيد مجلس الأمن على ذلك الحق في الدفاع عن النفس ردا على هجمات ١١ سبتمبر ٢٠٠١ على الولايات المتحدة".

وفي هذا الإطار فقد اعتبر حلف شمال الأطلسي الهجمات السيبرانية المتلاحقة التي تعرضت لها جمهورية استونيا سنة ٢٠٠٧ والتي أدت إلى تعطيل كامل لشبكات الاتصال الإلكترونية فيها، بمثابة هجوم مصلح يهدد دول الحلف جميعاً، وقد أكد الحلف أن أي هجوم سيبراني يؤدي إلى تطبيق البند الخامس من ميثاق الحلف الذي يعتبر أي عدوان على عضو في الحلف بمثابة عدوان على جميع أعضاء الحلف.

(٧٦) المؤتمر الدولى الثانى والثلاثون للصليب الأحمر والهلال الأحمر، جنيف سويسرا، ٨-١٠ ديسمبر ٢٠١٥، تقرير عن القانون الدولى الإنسانى وتحديات النزاعات المسلحة المعاصرة، وثيقة أعدتها اللجنة الدولية للصليب الأحمر، عمر محمد، الحرب الإلكترونية في القانون الدولى الإنسانى، مرجع سابق، ص١٣٩

كما ذكر دليل تالين الذي أعدته اللجنة الدولية التابعة لحلف شمال الأطلسي والمكونة من خبراء قانونيين وعسكريين سنة ٢٠١٣، أنه يمكن استخدام القوة العسكرية الحقيقية في حالة تم شن هجوم الكتروني على دولة وأدى هذا الهجوم لخسائر بالأرواح البشرية.(٧٧)

ثالثاً: تكييف الهجمات السيبرانية وفقاً للقانون الدولي الإنساني

يطبق القانون الدولي الإنساني أو ما يسميه العسكريون قانون الحرب، أو قانون النزاعات المسلحة على مجموع قواعد القانون الدولي التي تهدف إلى حماية ضحايا تلك النزاعات، وذلك من خلال تقييد خيار الأطراف في النزاع سواء بالنسبة لطرق أو وسائل أو أهداف المعارك في الميدان، فالقانون الدولي الإنساني الأعمال العدائية، ويهدف إلى حماية الأشخاص المتواجدين بين أيدي أطراف النزاع المسلح كالأسرى والمدنيين، كما يهدف إلى حماية الممتلكات من آثار النزاعات المسلحة التقليدية.

شهدت السنوات الأخيرة تطوراً ملحوظاً في اللجوء إلى تكنولوجيات الحرب الجديدة، خاصة منها الهجمات السيبرانية في سياق النزاعات المسلحة، وهو ما أدى بكثير من الباحثين إلى تكييفها على أنها نزاع مسلح يخضع لمبادئ القانون الدولي الإنساني.

أ- الهجمات السيبرانية بوصفها نزاع مسلح

يثير الموضوع محل البحث مسألة في غاية الأهمية، تتعلق بوصف الهجمات السيرانية كجزء من نزاع مسلح، فالقانون الدولي الإنساني هو مجموعة من القواعد القانونية التي تسعى للحد من آثار النزاعات المسلحة لأسباب إنسانية، وبالتالي فإن مجال انطباق القانون الدولي الإنساني هو النزاع المسلح.

بداية تشير إلى أن مسألة انطباق القانون الدولي الإنساني على الهجمات السيبراتية هي محل خلاف في النقاشات الجارية بتفويض من الأمم المتحدة بين أعضاء فريق العمل المفتوح العضوية الذي أنشأته الجمعية العامة والذي يمارس مهامه جنبا إلى جنب مع فريق الخبراء الحكوميين، وكلا الفريقين مكلف بمهام منها دراسة كيفية انطباق القانون الدولي الإنساني على استخدام الدول لتكنولوجيات المعلومات والاتصالات، وقد اتفقت الدول الأعضاء في فريق الخبراء الحكوميين عامي ٢٠١٣ و ٢٠١٥ على أن أحكام القانون الدولي، لاسيما ميثاق الأمم المتحدة، قابلة للتطبيق في بيئة تكنولوجيا المعلومات والاتصالات، وأشارت إلى المبادئ القانونية الدولية المعمول بها، بما في ذلك حسب الاقتضاء، مبادئ الإنسانية والضرورة والتناسب والتمييز ٥٥، بحيث يمكن أن تكون الهجمات السيبرانية جزء من حرب سيبرانية إذا ما استخدمت في إطار نزاع مسلح لتحقيق أهداف عسكرية.(٧٨)

(٧٧) أحمد عبيس نعمة الفتلاوى، وزهراء عماد محمد، تكييف الهجمات السيبرانية في ضوء القانون الدولى، مرجع سابق، ٦٢٤
(٧٨) يحيي ياسين سعود، الحرب السيبرانية في ضوء القانون االدولى الإنسانى، المجلة القانونية، المجلد القانونية، المجلد ٤، العدد ٤، كلية الحقوق، جامعة القاهرة، ص٨٥

(ISSN: ٢٣٥٦ - ٩٤٩٢)

إن عدم وجود نص صريح في القانون الدولي حول الهجمات السيبرانية، لا يعني عدم انطباق القواعد العامة لقانون لاهاي التي تنظم وسائل وأساليب الحرب بما فيها استخدام الأسلحة والقواعد العامة لقانون جنيف الحماية الفئات الضعيفة والأعيان المدنية أثناء النزاعات المسلحة على هذه الهجمات، حيث جاءت هذه القواعد لتشمل كافة التطورات ذات الصلة، ومن ثم ينطبق القانون الدولي الإنساني على الهجمات السيبرانية التي تشكل جزء من نزاع مسلح باستخدام الوسائل التقليدية للحرب وتكون متصلة به، كما ينطبق على العمليات السيبرانية التي تصل في حد ذاتها إلى مستوى النزاع المسلح من حيث الآثار الناجمة عنها في ظل غياب العمليات الحركية.(٧٩)

يعرف دليل "تالين" الهجوم السيبراني بموجب القانون الدولي الإنساني بوصفه عملية الكترونية سواء هجومية أو دفاعية يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الأضرار بأعيان أو تدميره، كما قد يشكل توقف أحد الأعيان عن العمل ضرراً مادياً، فالهجمات السيبرانية تشكل وسيلة وأسلوبا للقتال في الوقت نفسه، ومن ثم يمكن اعتبار الفيروسات والديدان الإلكترونية سلاحاً –مثل الأجهزة والمفاعلات النووية يستخدم لتنفيذ الاختراق أو الهجوم السيبراني ، وفي هذه الحالة يمكن تطبيق قواعد ومبادئ القانون الدولي الإنساني السارية على هذه الهجمات بوصفها حرب سيبرانية، وقد اعتبر الدليل · الهجوم الإلكتروني بمثابة استخدام للقوة إذا كان أثر هذا الهجوم عند مقارنته بالاستخدام الفعلي للقوة مساويا له، أو قريبا منه.(٨٠)

وتعتبر اللجنة الدولية أيضاً أن العملية التي تهدف إلى تعطيل عين ما حاسوب أو شبكة حاسوبية، على سبيل المثال تشكل هجوما بموجب القواعد بشأن إدارة العمليات العدائية، سواء تم تعطيل العين عن طريق وسائل حركية أو سيبرانية، فأي عملية تستهدف تعطيل أو ضرب البنية التحتية المدنية والعسكرية تخضع لقواعد القانون الدولي الإنساني بغض النظر عن الوسيلة المستخدمة في ذلك، فالعبرة بالنتائج المادية على الأرض وليس بالوسيلة المستعملة.(٨١)

ومن صور استخدام العمليات السيبرانية أثناء النزاعات المسلحة عمليات التجسس، وتحديد الأهداف والعمليات المعلوماتية الرامية إلى التأثير على معنويات العدو وإرادته إزاء القتال، وقطع نظم اتصالات العدو أو تضليلها أو التشويش عليها، وتعطيل محطات الرادار، والمنشآت النووية، ولعل أخطر الهجمات السيبرانية المرتكبة أثناء النزاعات المسلحة أو خارج سياق هذه النزاعات والتي لها آثار وخيمة على المدنيين، تلك الهجمات التي تستهدف البنى التحتية التي يستعملها المدنيون على

(٧٩) يحيي ياسين سعود، الحرب السيبرانية في ضوء القانون االدولى الإنسانى، المجلة القانونية، المجلد القانونية، المجلد ٤، العدد ٤، كلية الحقوق، جامعة القاهرة، ص٩٠، ص٣٠٢

(٨٠) نور أمير الموصلى، الهجمات السيبرانية في ضوء القانون الدولى الإنسانى، مرجع سابق، ص٢٠-٢١

(٨١) يحيي مفرح الزهرانى، الأبعاد الاستراتيجية والقانونية للحرب السيبرانية، مجلة البحوث والدراسات، العدد ٢٣، السنة ١٤، ٢٠١٧، ص٢٣٩

غرار محطات توليد الكهرباء، ونظم الرعاية الصحية، وبرامج المساعدة الإنسانية، ومخططات الإسعاف وتعد الهجمات السيبرانية المتبادلة حاليا بين كل من روسيا وأوكرانيا بالموازنة مع الحرب الدائرة بينهما على الأرض أكبر تهديد للأمن والسلام في العالم، وتحديا كبيرا للمجتمع الدولي ينذر بحرب سيبرانية عالمية.(٨٢)

وتجدر الإشارة إلى أن القانون الدولي الإنساني لا يضفي الشرعية على استخدام القوة سواء كانت حركية أو سيبرانية، فلا يجوز أن يفسر أي نص ورد في هذا الملحق "البروتوكول" أو في اتفاقيات جنيف لعام ١٩٤٩، على أنه يجيز أو يضفي الشرعية على أي عمل من أعمال العدوان أو أي استخدام للقوة يتعارض مع ميثاق الأمم المتحدة.(٨٣)

إن الأضرار الناجمة عن الهجمات السيبرانية كفيلة بأن تجعل الهجوم الإلكتروني يرتقي إلى مستوى الهجوم المسلح، فالوفيات والإصابات في صفوف الفئات المحمية الناجمة عن تعطيل أنظمة دعم الحياة التي يتحكم فيها جهاز الكومبيوتر، وانقطاع التيار الكهربائي بشكل كامل، وكذلك تعطيل أجهزة الكومبيوتر التي تتحكم في محطات المياه والسدود مما ينتج عنه فيضانات في المناطق المأهولة بالسكان دليل كاف لاعتبار الهجوم السيراني قوة وعدوان.(٨٤)

وبناء على ما سبق فإن الهجمات السيبرانية تعطل المصالح الإستراتيجية والحيوية للدول على الرغم من أنها لا يتم فيها احتلال الأراضي والغزو المباشر إلا أن أبعادها التدميرية وأضرارها تجعلها أشد من العدوان المسلح في بعض الأحيان، بحيث أنها تؤدي إلى حدوث ضحايا وكوارث إنسانية، وهو ما يطرح بشدة موضوع المسؤولية الدولية عن هذه الهجمات.

ب- <u>خضوع الهجمات السيبرانية لمبادئ القانون الدولي الإنساني</u>

يخضع استخدام وسائل الحرب الإلكترونية لنفس المبادئ التي تحكم سير الأعمال العدائية بالأسلحة التقليدية، باعتبار أن القانون الدولي الإنساني واسع بما فيه الكفاية ليساير التقدم الحاصل في التكنولوجيا، فمن أبرز مواطن قوة القانون الدولي الإنساني كما ذهبت إليه محكمة العدل الدولية – أنه وضع بطرق تجعله قليلا للتطبيق على كافة أشكال وأنواع الأسلحة بما فيها الأشكال والأنواع المستقبلية، فالقانون الدولي الإنساني يحد من العمليات السيبرانية أثناء النزاعات المسلحة مثلما يحد من استخدام أي أسلحة ووسائل وأساليب حرب أخرى جديدة كانت أو قديمة – أثناء نزاع مسلح ، حيث يمكن في هذا الإطار أن نشير إلى أنه تم تبني التطورات الحديثة التي قد تحدث في وسائل

(٨٢) المادة (٦٩) من دليل تالين
(٨٣) الفقرة ٢ من ديباجة البروتوكول الإضافى الأول لسنة ١٩٧٧ الملحق باتفاقيات جنيف لسنة ١٩٤٩
(٨٤) على فاضل على سليمان، حق الدفاع الشرعى على الهجمات السيبرانية، مجلة جامعة تكريت للحقوق، السنة ٤، المجلد ٤، العدد ٤، الجزء ١، ٢٠٢٠، ص٩

(ISSN: ٢٣٥٦ - ٩٤٩٢)

وأساليب القتال في المستقبل في المادة ٣٦ من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف الأربعة لعام ١٩٤٩ التي نصت على أن يلتزم أي طرف سام متعاقد عند دراسة أو تطوير أو اقتناء سلاح جديد أو أداة للحرب، أو إتباع أسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظورا في جميع الأحوال أو في بعضها بمقتضى أحكام هذا الملحق (البروتوكول) أو أية قاعدة أخرى من قواعد القانون الدولي الإنساني التي يلتزم بها الطرف السامي المتعاقد، وبناء على ذلك، تخضع الهجمات السيبرانية لمبادئ القانون الدولي الإنساني التي تحكم سير العمليات القتالية باعتبارها وسائل وأساليب حديثة للقتال عندما تستخدم في النزاعات المسلحة، مع استثناء الأجهزة والبنية التحتية التي تشكل أهداقا عسكرية من الحماية، ولكن حق أطراف النزاع في اختيار أساليب ووسائل القتال غير مطلق بل يخضع للقيود التي يفرضها القانون الدولي الإنساني وهو ما يعرف بمبدأ تقييد حق أطراف النزاع في اختيار الوسائل والأساليب التي يرغبون في استخدامها"، حتى لا يتم الإضرار بالمدنيين والأعيان المدنية، أما في حالة عدم وجود نزاع مسلح قائم فقد ترتقي الهجمات السيبرانية لتكون نزاعا مسلحا بالنظر إلى أثرها على حياة المدنيين ٧٠ ، ومن ثم تنطبق قواعد ومبادئ القانون الدولي الإنساني على الهجمات السيرانية التي تستهدف الأشخاص المتمتعين بحماية خاصة، والأعيان المدنية، باعتبارها ومحلة وأسلوب للحرب ما تنتج نفس الآثار الذي يمكن أن تنتج عن الأسلحة التقليدية من دمار وانقطاع الخدمات الحيوية والأضرار أو الإصابة أو الوفاة.(٨٥)

كما يمكن الاستناد إلى المبادئ الأساسية الأخرى للقول بخضوع الهجمات الصحيرانية للقانون الدولي الإنساني، ولعل أهم هذه العبادي: مبدأ التمييز بين المدنيين والمقاتلين ، وشرط مارتنز ٧٢، الذي يعتبر من قبيل القانون العرفي ، بحيث ورد في ديباجة اتفاقية لاهاي لعام ١٨٩٩، وفي صلب البروتوكول الإضافي الأول لعام ١٩٧٧، وفي ديباجة البروتوكول الثاني لعام ١٩٧٧، والذي جاء فيه: في معينة فيحالة عدم وجود قاعدة معينة القانون الاتفاقي، يظل المدنيون والمقاتلون تحت حماية وسلطان مبادئ القانون الدولي كما استقر بها العرف ومبادئ الإنسانية وما يمليه الضمير العام".(٨٦)

وقد أكدت محكمة العدل الدولية في رأيها الاستشاري الصادر بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها من جهة على شرط مارتنز" الذي لا يمكن الشك في استمرار وجوده وقابليته للتطبيق، وبأن هذا الشرط يعد وسيلة فعالة لمواجهة التطور السريع في التكنولوجيا العسكرية، ومن ثم فإن مبادئ القانون الدولي الإنساني تنطبق على جميع أشكال الحروب، وعلى جميع الأسلحة بما في ذلك تلك المستقبلية" التي لم يتمكن المجتمع الدولي من حظرها أو تقييد استخدامها، فمبادئ وقواعد

(٨٥) نور أمير الموصلى، الهجمات السيبرانية في ضوء القانون الدولى الإنسانى، مرجع سابق، ص٣١
(٨٦) يحيي مفرح الزهرانى، الأبعاد الاستراتيجية والقانونية للحرب السيبرانية، مجلة البحوث والدراسات، العدد ٢٣، السنة ١٤، ٢٠١٧، ص٢٤٢

القانون الدولي الإنساني قد وضعت قبل الأسلحة النووية، ومع ذلك لا يوجد شك حول الطباق القانون الدولي الإنساني على هذه الأسلحة الفتاكة، وعلى تقنيات أي أسلحة ناشئة ، وليس هناك ما يدعو التمييز بين الأسلحة النووية والهجمات السيبرانية، من حيث الزمن الذي استحدثت فيه ٧٥ ، ومن حيث الآثار المدمرة الناتجة علهما، بل أن آثار الهجمات السيبرانية قد تكون أكثر جسامة وأكثر ضرراً إذا استهدفت المحطات النووية على نطاق واسع، وهو ما جعل محكمة العدل الدولية تركز في رأيها على الطبيعة التدميرية للسلاح وعلى الأضرار اللاحقة بالبشرية الناتجة عن استخدامه بصرف النظر عن الوسيلة في حد ذاتها.(٨٧)

وبالتالي، فعدم وجود قواعد مكتوبة في القانون الدولي الإنساني خاصة بالهجمات السيبرانية لا يعني أنها مباحة طالما أنها تتعارض مع مبادئ الإنسانية وما يمليه الضمير العام باعتبارها مبادئ تقييدية، وهنا تظهر أهمية شرط" "مارتنز" باعتبارها جزء من الأهمية الجوهرية لمبادئ القانون الدولي الإنساني التي تقدم الحل بالاستقراء للحالات المستجدة وتسهم في سد ثغرات القانون وتساعد في تطوره مستقبلا بتبيان المسار الذي ينبغي إتباعه، وهي تمثل في هذا الإطار القانوني أبسط الأمس الإنسانية التي يمكن أن تطبق في كل زمان ومكان وتحت جميع الظروف ، فالقانون الدولي الإنساني تعامل مع التطورات والتغيرات السابقة في التكنولوجيا المستخدمة في النزاعات المسلحة، بمعنى أن القانون القائم قادر على التعامل مع هذه التطورات الجديدة دون الحاجة إلى إشعار أو وضع قواعد قانونية خاصة بالفضاء السيبرانى.(٨٨)

وقد أشارت محكمة العدل الدولية في رأيها الاستشاري حول مشروعية التهديد بالأسلحة النووية أو استخدامها بصورة ضمنية إلى انطباق مبادئ القانون الدولي الإنساني على الهجمات السيبرانية رغم اختلاف ميدانها عن باقي ميادين الحروب التقليدية الأخرى " بقولها عن مبادئ وقواعد القانون الدولي الإنساني المنطبق في النزاع المسلح تنطبق على كل أشكال الحرب وكل أنواع الأسلحة ... بما في ذلك تلك المستقبلية".(٨٩)

إن العمليات السيبرانية سواء ارتكبت في السلم أو في الحرب – شأنها شأن أي أسلحة أو وسائل أو أساليب حرب أخرى جديدة كانت أم قديمة، تخضع في تنظيمها للقانون الدولي الإنساني الذي يوفر شريحة إضافية من الحماية ضد آثار الأعمال العدائية، بحيث تتطليق مبادئ القانون الدولي الإنساني التي تحكم سير ووسائل الأعمال العدائية، بما فيها مبادئ التمييز والضرورة والتناسب على جميع

(٨٧) نور أمير الموصلى، الهجمات السيبرانية في ضوء القانون الدولى الإنسانى، مرجع سابق، ص٣٢
(٨٨) يحيي ياسين سعود، الحرب السيبرانية في ضوء القانون االدولى الإنسانى، المجلة القانونية، المجلد القانونية، المجلد ٤، العدد ٤، كلية الحقوق، جامعة القاهرة، ص٩١
(٨٩) يحيي مفرح الزهرانى، الأبعاد الاستراتيجية والقانونية للحرب السيبرانية، مجلة البحوث والدراسات، العدد ٢٣، السنة ١٤، ٢٠١٧، ص٢٤٢

(ISSN: ٢٣٥٦ - ٩٤٩٢)

العمليات العسكرية سواء كانت حركية أو ذات طابع سيبراني، فيجب على أطراف النزاع المسلح التمييز بين المدنيين والمقاتلين، وبين الأعيان المدنية والأهداف العسكرية ، ومن ثم يكون توجيه العمليات العسكرية نحو الأهداف العسكرية دون غيرها،(٩٠) وهذا ينطبق على جميع الأنشطة العسكرية سواء أكانت حركية أو سيبرانية، فالهجمات السيبرانية يجب أن تقتصر على الأعيان العسكرية، والأعيان ذات الاستخدام المزدوج الأعيان المدنية التي تستخدم لأغراض عسكرية في الوقت نفسه طوال هذا الاستخدام.(٩١)

ويجب على أطراف النزاع المسلح الموازنة بين الضرورة العسكرية والاعتبارات الإنسانية لتحقيق الميزة العسكرية بأقل تكلفة في الأرواح والأعيان،(٩٢) فيكون استخدام القوة بالقدر اللازم لتحقيق الهدف المقصود والمشروع من النزاع المسلح وهو إخضاع العدو بصورة كاملة أو جزئية وبأقل قدر ممكن من التضحية في الأرواح والموارد، وبالتالي يمنع في هذا الخصوص تدمير ممتلكات العدو أو حجزها، إلا إذا كانت ضرورات الحرب تقتضي حتماً هذا التدمير والحجز، ويرتبط بما سبق مراعاة مبدأ التناسب أي حظر الهجوم الذي قد يتوقع منه أو يسبب بصورة عرضية خسائر في أرواح المدنيين أو إصابات بينهم أو أضرار بالأعيان المدنية، أو قد يسبب مجموعة من هذه الخسائر والأضرار تكون مفرطة مقارنة بالميزة العسكرية التي يحققها ذلك الهجوم، وقد تضمن دليل "تالين" قاعدة تحظر الهجمات الإلكترونية التي قد تسبب خسائر كبيرة في الأرواح أو الأعيان مقارنة بالنتائج العسكرية التي تحققها تلك الهجمات، وتجدر الإشارة أن الهجمات السيبرانية على الأعيان ذات الاستخدام المزدوج تشكل تحديا للقانون الدولي الإنساني بالنظر إلى صعوبة التمييز بين الجزء من الشبكة الإلكترونية الذي يستخدم لأغراض عسكرية، والجزء الذي يستخدم لأغراض مدنية، وبالتالي تصبح الشبكة بأكملها هدفا عسكريا، وهو ما قد يترتب عنه أضرارا للسكان المدنيين في حالة المساس بالبنية التحتية المدنية التي لا غنى عنها لبقاء السكان المدنيين.(٩٣)

ويتمتع السكان المدنيون والأعيان المدنية، والأشياء التي لا غنى عنها لبقاء السكان المدنيين بحماية خاصة بموجب القانون الدولي الإنساني، بحيث تكفل مبادئ القانون الدولي الإنساني حماية قوية للبنية التحتية المدنية الحيوية ضد آثار الهجمات السيبرانية في أثناء النزاعات المسلحة، ويجب ألا تستخدم الأسلحة والهجمات العشوائية، وتحظر الهجمات غير المتناسبة، كما يجب على المتحاربين احترام وحماية الوحدات والمنشآت الطبية والعاملين فيها في جميع الأوقات، وبالتالي فإن

(٩٠) المادة (٤٨) من البروتوكول الإضافى الأول لعام ١٩٧٧ الملحق بإتفاقيات جنيف الأربعة لعام ١٩٤٩
(٩١) القاعدة ٣٩ من دليل تالين
(٩٢) المادة ٢/٥٢ من البروتوكول الإضافى لعام ١٩٧٧ الملحق بإتفاقيات جنيف الأربعة لعام ١٩٤٩
(٩٣) يحيي ياسين سعود، الحرب السيبرانية في ضوء القانون االدولى الإنسانى، المجلة القانونية، المجلد القانونية، المجلد ٤، العدد ٤، كلية الحقوق، جامعة القاهرة، ص٩٤

الهجمات السيبرانية ضد الأشخاص والأعيان المحمية أثناء النزاع المسلح تمثل في معظم الأحوال انتهاكا للقانون الدولي الإنساني، كما ينطبق القانون الدولي الإنساني على البيانات المدنية المتعلقة بالأعيان التي لا تتمتع بحماية خاصة، مثل بيانات الضرائب والسجلات المصرفية على أساس مبدأ تستع السكان المدنيين بحماية عامة من آثار الأعمال العدائية، وأي استثناء لهذه البيانات من الحماية التي يوفرها القانون الدولي الإنساني من شأنه أن يؤدي إلى ثغرة كبيرة في نظام هذه الحماية.(٩٤)

المبحث الثانى

تمييز الهجمات السيبرانية عما يتشابه معها والآثار المترتبة عليها

المطلب الأول

تمييز الهجمات السيبرانية عن المصطلحات المقاربة لها

بسبب حداثة مصطلح السيبرانية جاء مصاحباً لكل من هو جيد في مجال الصراع التكنولوجي فأصبح يطلق مصاحباً لكلمة أخرة ومن ذلك الهجمات السيبرانية، والجريمة السيبرانية، والحرب السيبرانية، والصراع السيبرانى، وغيرها من المصطلحات مما بوحي للبعض أن كل هذه المصطلحات تستخدم للتعبير والدلالة على معنى واحد، لذلك سوف نحاول وضع الحدود بين هذه المصطلحات للوقوف على معنى كلاً منها، وذلك على الوجه التالى:

أولاً: الحرب السيبرانية

اشتقت السيبرانية من الكلمة اللاتينية (cyber) ويقصد بها "افتراضي" أو "تخيُّلي" وتستخدم ضمن مجال الفضاء الذي يضم الشبكات العنكبوتية المحوسبة، ومنظومات الاتصال والمعلومات وأنظمة التحكم عن بعد وكل ما يتعلق بأنظمة الحواسيب وتكنلوجيا المعلومات والواقع الافتراضي، والسيبرانية هي: علم التحكم الأوتوماتيكي والقيادة والتوجيه عن بعد.(٩٥)

وجاء معنى كلمة سايبر (cyber) في قاموس المورد ب (الكمبيوتري) أو (عصري جدّاً)، وعند البحث عن مصطلح السايبر في القواميس نجد غالبية القواميس الإنجليزية بصورة عامة والعربية بصورة خاصة تفتقر لهذا المصطلح لحداثته، وان قاموس مايكروسوفت للحاسوب قد تناول هذا المصطلح وبأنه مشتق البادئة (cyber) وهو علم التحكم الآلي.(٩٦)

(٩٤) إيمان حمدان، التكنولوجيات الجديدة والقانون الدولى الإنسانى (الحرب السيبرانية)، ماجستير في القانون الدولى الإنسانى، الجامعة الافتراضية السورية، ٢٠٢٠، ص٩

(٩٥) أميرة عبد العظيم محمد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، عدد ٣٥، جزء ٣، كلية القانون، جامعة الامارات العربية، ٢٠٢٠، ص٣٧٨

(٩٦) حيدر ناظم عبد علي، رباب محمود عامر، التنظيم القانوني للهجمات السيبرانية على المنشآت ذات القوى الخطرة، مجلة الكوفة، العدد ٤،٧ جامعة الكوفة، ٢٠١٩، ص ١٠٩

(ISSN: ٢٣٥٦ - ٩٤٩٢)

إذ تعود بداية نشأة الحروب السيبرانية الى مرحلة الحرب الباردة فإن أول حرب سيبرانية وقعت كانت بين الولايات المتحدة الأمريكية والاتحاد السوفييتي في عام ١٩٨٢، إذ قام جهاز المخابرات السوفييتي (سابقاً) (KGB) بعملية تسمى (x Line) صممت لتساعد الاتحاد السوفياتي على سرقة تكنولوجيا المعلومات لكل أنشطة الغرب، إذ قامت المخابرات السوفييتية بتدريب جيش من العلماء على التسلل الى الشركات والوكالات لسرقة المعلومات مع تسرب المعلومات إلى وكالة المخابرات الامريكية (CIA) والتي قامت بدلاً من إلقاء القبض عليهم تركتهم يواصلون العمل ولكن مع امدادهم بمعلومات مغلوطة، وإذ حصل الجواسيس السوفييت على وثائق تتضمّن مخططات ولكن تتضمن خطأ بسيطاً في الشفرة مع استمرار السوفييت باستخدام المعلومات المغلوطة لبناء العمود الفقري لخطوط نقل الغاز الطبيعي والنفط القادم من سيبيريا، وبعد فترة قصيرة تسبب الخطأ المتعمّد في الشفرة في حدوث انفجار لخط الأنابيب وكان هذا الانفجار يعادل ثلث حجم انفجار القنبلة النووية في هيروشيما.(٩٧)

أما الحرب السيبرانية كإطار عام للمفهوم فإنها تُشَنّ ضد كيانات محددة بهدف تعطيلها والحفاظ على مجال المعلومات من أي اعتداء سيبراني من طرف الخصم باستخدام الوسائل التكنلوجية والمعلوماتية المتطورة.(٩٨)

وعرفت وزارة الدفاع الامريكية الحرب السيبرانية بأنها: توظيف القدرات السيبرانية حيث يكون الهدف الأساسي هو تحقيق الأهداف والآثار العسكرية في الفضاء السيبراني أو من خلاله، وهي أيضاً نشاط مماثل أو غير متماثل دفاعي كان أم هجومي على الشبكة الرقمية من قبل فواعل دولية أو غير دولية الغرض منها هو إلحاق الضرر بالبنى التحتية الحيوية والأنظمة العسكرية.(٩٩)

وإن الحرب السيبرانية ميدانها الفضاء االسيبراني وهي غير محدودة المجال وتكون غامضة الأهداف لأنّها تتحرك عبر شبكة المعلومات والاتصالات المتعدية للحدود الدولية فضلاً عن اعتمادها على أسلحة الكترونية ذكية ومتطورة تلائم طبيعة السباق الإلكتروني لعصر المعلومات، أو يتم توجيهها ضد المنشآت الحيوية أو دسها عن طريق عملاء لأجهزة الاستخبارات.(١٠٠)

---

(٩٧) (٣) الحروب السيبرانية – نتائج ملموسة لمعارك غير مرئية، الجندي، بتاريخ ٤/١/ ٢٠٢١، ص ١، الشبكة الدولية للمعلومات:
https//www.aljundi. Ae%d٨٪a٧٪٨٤٪d٩

(٩٨) Michael Robinson, Kevin jones, helge janicke, cyber war fare: issues and challenges, article in computer and security, Elsevier ,volume – ٤٩ -, march, united kingdom, ٢٠١٥, p – ٢٤ -

(٩٩) زينب شنوف، الحرب السيبرانية في العصر الرقمي: حروب ما بعد كلاوزفيتش، المجلة الجزائرية للأمن والتنمية، المجلد ٩، العدد ٢، يوليو، الجزائر، ٢٠٢٠، ص ٩١

(١٠٠) يحيى ياسين سعود، الحرب السيبرانية في ضوء القانون الدول الإنساني، المجلة القانونية (مجلة متخصصة في الدراسات والبحوث القانونية)، العدد ٤، جامعة القاهرة – كلية الحقوق – فرع الخرطوم، ٢٠١٨، ص ٦

وعليه فإن الفاعل الرئيسي في الحرب السيبرانية هي الدول، إذ بدأت بعض الدول الاستعداد لهذا النوع من الحروب إنشاء جيوش سيبرانية داخل صفوف القوات المسلحة للدول عن طريق إبرام الاتفاقات السياسية والعسكرية، إذ توصلت الولايات المتحدة الأمريكية والصين في عام ٢٠١٥ لاتفاق خاص بالحروب السيبرانية بعدم شن أي هجمة سيبرانية، وأعلن الاتحاد الأوروبي في عام ٢٠١٧ من أن شن أي هجمة سيبرانية من دولة عدائية على الاتحاد الأوروبي يعد (تصرف حرب) يجب التصدي له، رغم الهجمات السيبرانية بين الحين والآخر وإنكار كل طرف ذلك.(١٠١)

واستكمالاً لمفهوم الحرب السيبرانية فيعرفها كل من (ريتشارد كلارك) و (روبرت كناكي) بأنها: أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تدميرها، ويعرّفها (بولو شاكريان) على أنّها: استمرار او امتداد للسياسة عن طريق الاجراءات المتخذة في الفضاء السيبراني من دول أو فاعلين غير دوليين، إذ تشكل تهديداً خطيراً للأمن القومي.(١٠٢)

١- <u>التمييز بين الهجمات السيبرانية والحرب السيبرانية</u>

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

<u>الناحية الأولى</u>: 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.(١٠٣)

<u>الناحية الثانية</u>: بالنسبة للأهداف غالباً ما يكون الهدف من الجرائم السيبرانية إثبات مهارة الفاعل تقنياً وقدرته على اختراق أجهزة الكمبيوتر أو تهدف التسلية والترفيه أو تحقيق مكاسب شخصية كسرقة الملكية 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 فيبعض الحالات) وتكون هذه الأفعال مجرمة بموجب القانون الوطني، بخلاف الهجمات السيبرانية التي يسهتدف مرتكبوها الأمن القومي والسياسي للدولة ويقوم هؤلاء بتخريب الشبكات التي

(١٠١) إيهاب خليفة، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الامن القومي، العربي للنشر والتوزيع، ط ١، القاهرة، ٢٠١٩، ص ١١٤

(١٠٢) إسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، منشوارت جامعة الشهيد حمة لخضر بالوادي، المجلد ١٠، العدد ١، الجزائر، ٢٠١٩، ص ١٢

(١٠٣) زهراء عماد محمد: المسئولية الدولية الناشئة عن الهجمات السيبرانية، جامعة الكوفة-كلية القانون، جمهورية العراق، إشراف الدكتور: أحمد عبيس نعمة الفتلاوي، ٢٠١٦ م، ص١٧

(ISSN: ٢٣٥٦ - ٩٤٩٢)

تتحكم بالبنية التحتية الأساسية في الدولة وتدميرها بقصد إرباكها، وزعزعة النظام فيها لتحقيق أهداف أمنية أو عسكرية أو سياسية.(١٠٤)

فالحرب السيبرانية هي نوع أو جزء من الهجمات السيبرانية التي تحدث في أثناء نزاع مسلح حركي أو التي تنتج آثار مادية تشبه وتعادل آثار الهجمات المسلحة التقليدية، بينما الهجمات السيبرانية هي كل نشاط سيبراني ضههر بالدول الأخرى سواء كان في وقت السلم أو في سياق نزاع مسلح حركي وسواء نتجت عنه آثار مادية جسيمة في الأرواح أم الممتلكات أو لم يؤدي إلا إلى تشويش أنظمة الكمبيوتر فيها مادام كان ذلك لأغراض أمنية وعسكرية.

ولابد من الإشارة إلى أن الحرب السيبرانية يمكن أن تشكل أيضاً هجوماً سهيبرانياً وجرائم سيبرانية في ذات الوقت، ويمكن تقسيم الهجمات السيبرانية إلى 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 وتعطل فيها وظيفة شبكة الكمبيوتر وذلك لأغراض سياسية أو أمنية وطنية، وتنتهك فيها القانون المحلي.

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.(١٠٥)

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.

(١٠٤) نور أمير الموصلى، الهجمات السيبرانية في ضوء القانون الدولى الإنسانى، رسالة ماجستير في القانون الدولى الإنسانى، ٢٠٢١، ص١٤

(١٠٥) زهراء عماد محمد، المسئولية الدولية الناشئة عن الهجمات السيبرانية، جامعة الكوفة-كلية القانون، جمهورية العراق، إشراف الدكتور: أحمد عبيس نعمة الفتلاوي، ٢٠١٦ م، ص٢٠ وما بعدها

وتتميز الحرب السيبرانية بمجموعة من الخصائص وهي: (١٠٦)

١-هي حرب رقمية ذات تقنية متطورة، وإن قمة التطور الذي بلغته ثورة المعلومات وبوابتها الحاسبة الإلكترونية التي شكلت بدورها الأداة المحورية لهذا النوع من الحروب والميدان الرئيسي لها.

٢-حرب لا تناظرية: فلا تحتاج الدول الى تخصيص ميزانيات ضخمة لإنتاج أسلحتها أسوة بالأسلحة المستخدمة في النزاعات التقليدية ذات الكلفة العالية وأنها ذات تكلفة متدنية نسبةً للأدوات اللازمة لشنها.

٣-تمتع المهاجم بأفضلية واضحة في حروب الانترنت على المدافع؛ فالحروب السيبرانية تتميز بالسرعة والمرونة والمراوغة وفي بيئة مماثلة يتمتع بها المهاجم بأفضلية من الصعب جدّاً على عقلية التحصّن لوحدها أن تنجح.

٤-حرب هلامية الشكل والملمح: فهي متعددة بميادينها، متنوعة ومتطورة بوسائلها المرتبطة بأكثر المجالات التقنية تطوّراً وتبدلاً في الحياة المعاصرة للدول وهي تطال بتدميرها أكثر المواقع السيادية والحساسة تحصيناً وبعداً عن دائرة القتال.

٥-إن الحرب السيبرانية تمتاز: بقوة تدميرية لا تصاحبها دماء وأشلاء، إذ يتضمن التجسس ثم النسف لكن لا دخان ولا غبار فيتم التدمير بوابل من الفيروسات، كما ان انتشار الفضاء الالكتروني وسع دائرة استهداف المواقع بمستوياتها كافة.

ثانياً: الفضاء السيبراني (cyber space)

أصبح الفضاء السيبراني في الوقت الحاضر يمس جميع الأرواح وأصبح ضرورياً ويطلق عليه العالم الافتراضي لأنه غير موجود في الواقع المادي والناس في العالم الافتراضي يعيشون حياة افتراضية جنباً إلى جنب مع حياتهم الواقعية.

ويعرف الفضاء السيبراني بأنّه عالم افتراضي يتشارك مع عالمنا المادي يتأثر به ويؤثر فيه بشكل معقد، إذ تقوم العلاقة بين العالمين على نظرة تكاملية ويوصف بأنه الذراع الرابع للجيوش الحديثة الى جوار القوات البرية والجوية والبحرية.(١٠٧)

ويعرف أيضاً بأنه المستودع الكبير الذي تجري فيه جميع عمليات التواصل الالكتروني عبر شبكات الحواسب، وهو منظومة من العناصر المتفاعلة فيما بينها والمتكونة من أجهزة الكمبيوتر، أنظمة الشبكات والبرمجيات، حوسبة المعلومات، نقل وتخزين البيانات.(١٠٨)

(١٠٦) علي عبد الرحيم العبودي، هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين، مجلة قضايا سياسية، العدد ٥،٧ جامعة النهرين – كلية العلوم السياسية، ٢٠١٩، ص ٩٩ – ١٠١

(١٠٧) نورة شلوش، القرصنة الالكترونية في الفضاء السيبراني "التهديد المتصاعد لأمن الدول"، مجلة مركز بابل للدراسات الإنسانية، المجلد ٨، العدد، ٢ جامعة بابل، ٢٠١٨، ص ١٩٠

(١٠٨) محمد وائل القيسي، مستقبل الامن الاستراتيجي العالمي في ظل التحديات التكنو – معلوماتية والفضاء السيبراني، مجلة دراسات إقليمية، مركز الدراسات الإقليمية، السنة ١٤، العدد ٤،٤ نيسان، جامعة الموصل، ٢٠٢٠، ص ١٥٣ – ١٥٤

(ISSN: ٢٣٥٦ - ٩٤٩٢)

كما عرفته الوكالة الفرنسية لأمن أنظمة الإعلام (ANSSI) وهي وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي بأنّه فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية، وأنه لا يقتصر على شبكة الانترنت فقط وإنّما شبكات عالمية وخاصة أخرى مثل (Swift/ psth Gps/ AcARs).[١٠٩]

ثالثاً: الأمن السيبراني (cyber security)

إن الأمن السيبراني هو عبارة عن التقنيات الالكترونية المستخدمة لحفظ سلامة الشبكات والبرامج والبيانات من الوصول غير المصرح به. وإن الأمن السيبراني يهدف الى ضمان تحسين الأمن الذي من شأنه الدفاع عن المنظمات من التعرض لهجوم من قبل المتسللين عبر الشبكة العنكبوتية.

وهذا مرده إلى أن العالم أصبح أكثر ارتباطاً بواسطة الشبكات العنكبوتية لتنفيذ المعاملات العامة ويقوم الأمن السيبراني بالحفاظ عليها وعليه فإنّ الأمن السيبراني وفق ما يراه الكاتبان (Pekka Nettaanmaki) و (Martti Lento) في كتابهما:

(cyber security: Analytics, technology and Automation)

بأنه مجموعة من الإجراءات التي تتخذ في الدفاع ضد الهجمات السيبرانية (قراصنة الكمبيوتر) وعواقبها وتنفيذ التدابير المضادة المطلوبة.[١١٠]

رابعاً: القوة السيبرانية (cyber power)

تعرف القوة السيبرانية بأنّها القدرة على القيام بنشاط سيبراني مؤثر في الفضاء السيبراني، أو القدرة على استخدام الفضاء السيبراني لتحقيق مجموعة من الأهداف والتاثير على الأحداث وتعرف أيضاً على أنها الموارد البشرية والمادية المتاحة ضمن بيئة استراتيجية يمكن استخدامها لإحداث تأثير في الفضاء السيبراني او من خلاله.[١١١]

خامساً: الصراع السيبراني (cyber conflict)

تواجه الحكومات والمؤسسات الى هجمات مضادة من نوع آخر وهي الهجمات السيبرانية بسبب الارتباط الكبير بين دول العالم افتراضياً وضمن الفضاء السيبراني خاصة بعد ثورة المعلومات التي حفزت ذلك تدريجياً، وهذا يدخل في مفهوم الصراع السيبراني الذي هو تعارض بين دول ما ضمن

(١٠٩) تغريد صفاء، لبنى خميس مهدي، أثر السيبرانية في تطور القوة، مجلة حمورابي للدراسات، مركز حمورابي للبحوث والدراسات الاستراتيجية، العدد ٣٣ – ٣٤، السنة ٨، شتاء - ربيع، بغداد، ٢٠٢٠، ص ١٤٩

(١١٠) صلاح مهدي هادي الشمري، زيد محمد علي إسماعيل، الامن السيبراني كمرتكز جديد في الاستراتيجية العراقية، مجلة قضايا سياسية، السنة ١٢، العدد ٦٢، جامعة النهرين، كلية العلوم السياسية، ٢٠٢٠، ص ٢٧٧

(١١١) Robert "Jake" bebber, cyber power and cyber effectiveness: an analytic framework, comparative strategy an international journal, routledge, taylor & francis group, volume ٣٦, November ٥, ٢٠١٧, p ٤.

نطاق القدرات السيبرانية في الفضاء السيبراني من اجل تحقيق اهداف يسعى إليها أطراف الصراع.(١١٢)

سادساً: الدفاع السيبراني (cyber defence)

يعرف الدفاع السيبراني بأنه آلية دفاع لشبكة الكمبيوتر وتشمل الاستجابة للإجراءات الفعالة من اجل حماية البنى التحتية الحيوية فتأمين المعلومات والحفاظ عليها للمنظمات والهيئات الحكومية والشبكات الأخرى، ويركز الدفاع السيبراني على المنع والكشف، وتوفير الاستجابة في الوقت المناسب ضد الهجمات السيبرانية من اجل منع العبث بالبنى التحتية او المعلومات.(١١٣)

سابعاً: الردع السيبراني (cyber deterrence)

يعرف الردع السيبراني بأنّه التلصص الإعلامي والاستعراض التكنلوجي والمحاكاة الاستراتيجية لإنشاء صورة رقمية مفرطة لهيمنة دولة مّا سيبرانيّاً عبر نطاق الفضاء السيبراني لردع الخصم سيبرانياً.(١١٤)

ثامناً: الاستراتيجية السيبرانية (cyber strategy)

هي تطوير وتوظيف القدرات اللازمة للعمل في الفضاء السيبراني متكاملة مع المجالات العملياتية الأخرى لتحقيق او دعم تحقيق الأهداف عبر عناصر القوة الوطنية وتعتمد الاستراتيجية السيبرانية على مزيج منظم من الغايات، والوسائل، والطرق لتحقيق اهداف الامن العسكري والسياسي والاقتصادي والمعلوماتي والوطني الأوسع من خلال الاعتماد على القدرات السيبرانية وتوفير الموارد والتكاليف الواجب اتخاذها لمواجهة المخاطر خاصة السيبرانية.(١١٥)

المطلب الثانى

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 أنظمهة 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 لتعطيهل أجهزة الاتصالات بكهل أنواعها، ناهيك عن اختراق البنوك وسرقة الحسابات والتلاعب بالتحويلات.(١١٦)

(١١٢) Alexander kosenkov, cyber conflict a new global threat, future internet, mdpi, ٨, ٤٥, ٢٠١٦, p١.
(١١٣) Darko galinec, darko mozink and boris, I bid, p ٤.
(١١٤) Stefan soesanto and max smeets, cyber deterrence: the past, present and future, center for security studies (css), Switzerland, ٢٠٢١, p ٥.
(١١٥) زينب شنوف، الحرب السيبرانية في العصر الرقمي: حروب ما بعد كلاوزفيتش، مصدر سبق ذكره، ص٩٢
(١١٦) نور أمير الموصلى، الهجمات السيبرانية في ضوء القانون الدولى الإنسانى، رسالة ماجستير في القانون الدولى الإنسانى، ٢٠٢١، ص١٨

(ISSN: ٢٣٥٦ - ٩٤٩٢)

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.

وقد تتحول هذه الميزة إلى نقطة ضعف، إن لم تكن الشبكة السيبرانية المستخدمة آمنة تدرجة 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 البنية التحتية للدولة، ووقوع وفيات بين العسكريين والمدنيين.(١١٧)

ثانيا: 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 والطبيب وتقديم التشخيص ومتابعة حالة المريض إلكترونياً. ويعد الهجوم السيبراني على هذه السجلات الطبية بمثابة خرقاً خطيراً للأمن السيبراني للرعاية الصحية، وبالتالي إحداث اضطراب كبير في المجال الصحي للدولة.(١١٨)

(١١٧) نور أمير الموصلى، الهجمات السيبرانية في ضوء القانون الدولى الإنسانى، المرجع السابق، ص١٩

(١١٨) عبد الرحمن بجاد العتيبى، الأمن السيبرانى في تعزيز الأمن السيبرانى، جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية (قسم الأمن الإنسانى)، ٢٠١٧، ص٦٢-٦٤

ثالثا: 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، خاصهة 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 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.(١١٩)

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 البنية 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.

المبحث الثالث

موقف القانون الدولى من الهجمات السيبرانية ومكافحتها

المطلب الأول

موقف القانون الدولى من الهجمات الحرب السيبرانية

تجب الملاحظة ابتداء، أن الهجمات الحربية "السبيرانية إنما تتعلق فقط بعمليات تكنولوجيا المعلومات في أوقات النزاع المسلح، وتُستبعد الاعتداءات التي تقع في أوقات السلم، ذلك أن التهديدات التي يشكلها الفضاء السبيراني للأمن، والتي لا يمكن اعتبارها نزاعا مسلحا، ويمكن أن تدخل ضمن نطاق الجرائم الإلكترونية والعمليات الإلكترونية، والقرصنة الإلكترونية والتجسس الإلكتروني، أو عند الاقتضاء الإرهاب الإلكتروني، ينبغي أن لا تناقش مع الشروط التي تثيرها تساؤلات حول انطباق قانون النزاعات المسلحة. وعليه، سيتركز نقاشنا في هذا المطلب على أهم

(١١٩) عبد الرحمن العتيبى، الأمن السيبرانى في تعزيز الأمن السيبرانى، المرجع السابق، ص٦٥-٦٦

(ISSN: ٢٣٥٦ - ٩٤٩٢)

الإشكالات القانونية المتعلقة بطبيعة الهجمات الحربية السبيرانية والقيود المفروضة من منظور القانون الدولي.

الفرع الأول

طبيعة الهجمات الحربية السبيرانية والقيود المفروضة عليها من منظور القانون الدولي

١- علاقة الهجمات السبيرانية باستخدام القوة والدفاع الشرعي:

ثار جدل ونقاش واسع حول طبيعة الأعمال الهجومية والدفاعية السبيرانية التي أصبحت ترتبط بالإستراتيجية العسكرية من خلال القدرة على شن هجمات تعطيل الخدمة أو الخداع أو التدمير أو الاستغلال، وهو ما يفرض تحديات فيما يتعلق بمفهوم العدوان الذي يعني استخدام القوة المسلحة من قبل دولة ضد السيادة أو الوحدة الإقليمية أو الاستقلال السياسي لدولة أخرى أو أي شكل آخر يتعارض مع ميثاق الأمم المتحدة.(١٢٠)

الأمر الذي جعل فقهاء القانون الدولي يتساءلون حول ما إذا كان استخدام الهجمات السبيرانية أو التهديد باستخدامها يندرج تحت نطاق القوة العسكرية المحظورة بموجب المادة ٢ فقرة ٤ التي يتطلب الإخلال بها تفعيل الفصل السابع من ميثاق الأمم المتحدة، أم أنها خارج نطاق الحظر المقصود؟ وهل تصل قوة الهجوم الإلكتروني إلى عتبة الهجوم المسلح الذي يبرر إعمال حق الدفاع الشرعي عن النفس؟

أ- الواقع أنه هناك صعوبة في تفسير مصطلح "استخدام القوة" (use of force) لعدم وجود أي تعريف واضح له لا في ميثاق الأمم المتحدة، ولا في أي صك دولي آخر ذي صلة. ومن المقبول به على نطاق واسع أن جميع أشكال الأفعال العدائية محظورة بموجب ميثاق الأمم المتحدة. ويشمل الحظر الهجمات بالأسلحة التقليدية، غير أنه بالرجوع إلى المادة ٣٩ من الميثاق نجدها ألحقت فعل العدوان وربطته بتهديد السلم والإخلال به وعند الحديث عن مصطلح تهديد السلم في القانون الدولي قد يكون ذلك بعيدا نوعا ما عن الهجمات الإلكترونية الدولية لكن عند التعمق أكثر، نجد أن هناك روابط معينة تؤدي إلى كون الهجمات الإلكترونية تحدث إخلالا بالسلم والأمن الدوليين من خلال حدوث هجمة إلكترونية دولية معلنة الدولة أخرى، والأمر الخطير في ذلك أن مثل هذا النوع من الهجمات قد يهاجم المصالح الإستراتيجية والحيوية للدول كنظم الاتصالات، أو قطع خدمة الانترنت أو استخدام الدعاية وشن الحرب النفسية والتجسس والقرصنة وتدمير قواعد البيانات الخاصة بمنشأت مدنية عن طريق قصف فيروسات تلحق دماراً كبيراً في البنية التحتية الوطنية الهامة للدول المستهدفة.

(١٢٠) جمال العظامات، جريمة العدوان في الهجمات الإلكترونية في نطاق القانون الدولي العام، مجلة المنارة، العدد ٤، المجلد ٢١، ٢٠١٥، ص١٣

هذا من جهة ومن جهة أخرى؛ فإنه عند التركيز على الوسائل المستخدمة في هجوم الحرب السيبرانية نجدها تضاهي ما يتم استخدامه في الحروب التقليدية من حيث آثارها وتداعياتها، كما ينتج عنها قدر من القنابل الأسلحة والقصف والعدوان وغيرها من مظاهر استخدام القوة داخل الفضاء الإلكتروني، والذي يكون له تأثير مماثل للهجمات الحربية التقليدية.

والواقع أنه لا توجد سوابق تشير أن مجلس الأمن الدولي تصرف بموجب المواد ٣٨، ٣٩، ٤٠ من ميثاق الأمم المتحدة حيال هجمة إلكترونية دولية، كما أن المجلس لا يضع معيارا محدداً في تكييف ما يعرض عليه من وقائع، وهو يتمتع بسلطة تقديرية فيما يعتبر إخلالاً ومساساً بالسلم والأمن الدوليين.(١٢١)

ب- إذا كانت هجمات الحرب السبيرانية تعبيرا عن استخدام للقوة المسلحة، فإنها تخضع للفصل السابع من ميثاق الأمم المتحدة ومبدأ الدفاع الشرعي عن النفس، لكن محاولة تطبيق مبدأ الدفاع الشرعي عن النفس أثار نقاشات ورؤى مختلفة حول مدى الموائمة القانونية وتطبيقاتها على تلك الهجمات، لاسيما وأن الميثاق لم يتناول على وجه التحديد مفهوم الضربات الوقائية للدفاع عن النفس، فوفقا للتفسير المتشدد (الضيق) فإن حق الدفاع عن النفس يتم فقط من جانب الدول للرد على هجوم مسلح، وهناك من يرى أن ميثاق الأمم المتحدة لم يذكر ذلك صراحة باعتبار أن حق الدفاع الوقائي عن النفس يدخل ضمن العرف الدولي،(١٢٢)

كما يوجد تحدى خطير بشأن المواءمة بين الهجوم والرد عليه وشرط التناسب مع فعل الاعتداء الذي هو شرط من شروط الدفاع الشرعي في القانون الدولي حيث إن شبكات الكمبيوتر تسمح بأن تتعدى آثار الهجوم لأكثر من دولة، كما أن الرد يتعدى أيضا لأكثر من دولة دون معرفة أو تحديد مصدر الهجوم ومن ثم ينقلب الدفاع الشرعي إلى عدوان بالإضافة إلى إمكانية إحداث أضراراً لا مبرر لها، حيث يمكن أن يطال مرافق حيوية فرض لها القانون الدولي حماية أثناء النزاعات المسلحة.(١٢٣)

ولمزيداً من التفصيل سوف نناقش حق الدفاع الشرعي من خلال ميثاق الأمم المتحدة وذلك على التفصيل التالي :

(١٢١) د/ عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي المعاصر، سلسلة أوراق، العدد ٢٣، وحدة الدراسات المستقبلية مكتبة الإسكندرية، ٢٠١٦، ص١٠٨-١١٠
(١٢٢) د/ عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي المعاصر، المرجع السابق، ص١١٤-١١٥
(١٢٣) د/ عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي المعاصر، مرجع سابق، ص١١٣

(ISSN: ٢٣٥٦ - ٩٤٩٢)

- **القوة الناشئة عن الهجوم السيبراني، وحق الدولة المعتدى عليها في الرد وفقاً للمادة (٥١) من ميثاق الامم المتحدة**

نظراً لحساسية استخدام القوة في العلاقات الدولية، وكذلك تعقد الفضاء السيبراني الذي أصبح يشكل قلق كبير للمجتمع الدولي لخطورة الهجمات التي تشن من خلاله. حيث تعد ظاهرة الهجمات السيبرانية من الأساليب المستحدثة والمتطورة في نفس الوقت والتي لا تزال مثاراً للجدل لعدم وجود موقف واضح تجاهها حيث ينطبق القانون الدولي على الهجوم السيبراني إذا اعتبر هذا الهجوم قوة وفقاً لميثاق الأمم المتحدة، إلا ان فقهاء القانون الدولي قد اختلفوا في ذلك، كما ان حق الدولة في الرد على الهجوم السيبراني أمر في بالغ الأهمية لأنه يحدد الآثار القانونية المترتبة على هذا الهجوم.

- **ما مدى اعتبار الهجوم السيبراني استخداماً للقوة**

لا شك بأن الفضاء السيبراني قد غير من طبيعة الصراع الدولي، فالتطورات الكبيرة في وسائل التكنولوجيا والاتصالات سهلت على الدول شن الهجمات السيبرانية بوصفها (قوة) تمكنهم من تنفيذ هجمات إلكترونية لمنشآت حيوية عسكرية او مدنية، فقد أصبح بإمكانها تعطيل وتدمير البنة التحتية للدولة حيث بين المعهد الدولي للدراسات الاستراتيجية في لندن بأن الفضاء السيبراني سيشكل أحد أهم ميادين الصراع في المستقبل لما له من تأثيرات مباشرة على سيادة الدول. بالرغم من الاتفاقات التي أبرمت في هذا الشأن إلا ان الموقف الدولي من الهجمات السيبرانية مازال ليس بالمستوى المطلوب، بالرغم من أنه أصبح واقع يومي يهدد للسلم والأمن الدوليين فقد نصت المادة الثانية/ الفقرة الرابعة من ميثاق الامم المتحدة على "تمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة أو باستخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على وجه لا يتفق مع مقاصد الأمم المتحدة"،[١٢٤] بينت المادة اعلاه ان استعمال القوة أو التهديد بها ضد سيادة الدول يتنافى مع أهداف الميثاق التي تهدف الى حفظ الأمن والسلم الدوليين. كما ورد في نص المادة اعلاه مصطلح القوة من دون تحديد نوع القوة المستخدمة حيث جاءت مطلقة لتشمل كل اشكال القوة.

غالباً ما يصطحب لفظ (القوة) في ميثاق الأمم المتحدة مصطلح "المسلحة" التي ذكرت في الديباجة والمادة الرابعة والأربعون من الميثاق، إلا ان مصطلح "القوة" جاء في الفقرة الرابعة من المادة الثانية وحاده من دون مصطلح "المسلحة"، مما زاد الأمر تعقيداً حيا أدى الى اختلاف آراء الفقهاء بشأن المعنى المقصود للقوة. وبخصوص ذلك ظهر اتجاهين مختلفين فيما يتعلق بتفسير مصطلح القوة، حيث يرى الاتجاه الأول ان المقصود من القوة هي القوة العسكرية فقط، بينما يرى الاتجاه الثاني ان المقصود باالقوة ليس فقط القوة العسكرية بل المقصود هو أوسع من ذلك، حيث يشمل الضغط

(١٢٤) المادة الثانية/ الفقرة الرابعة من ميثاق الامم المتحدة

السياسي والاقتصادي الذي يعد تهديداً للاستقلال السياسي للدولة الذي يعادل التهديد العسكري من حيث الخطورة.(١٢٥)

الاتجاه الاول: يأخذ أنصار هذا الاتجاه بالتفسير الضيق للمادة الثانية/ الفقرة الرابعة الذي يقضي بان المقصود بالقوة هي القوة العسكرية فقط ويستندون في رأيهم الى أن المقصود من نص المادة اعلاه يجب ان يكون في حدود ديباجة الميثاق ونصوصه الأخرى ذات الصلة. ان المادة الثانية/ الفقرة الرابعة يجب ان تفسر على أنها تجسد المعنى الضيق للقوة المحصورة في القوة العسكرية أو المسلحة. كما ان المادة الرابعة والأربعون من الميثاق تنص على اعتبار ان مضمونها يقصد به القوة المسلحة. وأيضاً يستندون أنصار هذا الاتجاه على ان الاقتراح الذي قدم في مؤتمر سان فرانسيسكو من البرازيل لاعتبار إجراءات الضغط السياسي من قبيل الاستخدام غير المشروع للقوة إلا ان هذا المقترح جوبه بالرفض وفقاً لهذا الاتجاه لا يمكن اعتبار الهجوم السيبراني قوة لأنه لا يرقى الى مستوى الهجوم المسلح.

الاتجاه الثاني: ذهب أنصار هذا الاتجاه الى ان مفهوم القوة لا ينحصر فقط بالقوة العسكرية وإنما يشمل كل أنواع التهديد بغض النظر عن الوسيلة المستخدمة في التهديد طالما ان النية عدائية. حيث ان الفقرة الرابعة من المادة الثانية جاءت مرنة بالشكل الكافي لاستيعاب الهجوم السيبراني نتيجاة لآثار المتشابهة بالنسبة للقوة العسكرية التقليدية. لذلك فأن الكود الضار أو الفايروسات لها نفس خصائص السلاح التي يمكن ان تكون أداة للتخريب والتدمير كالسلاح الحركي. علاوة على ذلك، أوضحت محكمة العدل الدولية في الفتوى التي أصدرتها بشأن مشروعية استخدام الأسلحة النووية حيث ان الفقرة الرابعة من المادة الثانية من ميثاق الأمم المتحدة لا تشير الى أسالحة محددة، ومن ثم فأن هذه المادة تنطبق على اي استخدام للقوة بصرف النظر عن الوسائل المستخدمة.(١٢٦)

وفقاً لما ذكر اعلاه، فان الهجوم السيبراني عندما يصل الى مستوى استخدام القوة فليس من الضروري التطرق الى الوسيلة التي تم التنفيذ من خلالها (الوسائل الالكترونية)، حيث يتم التعامل على أنها قوة لها نتائج على الأرض بغض النظر عن الوسيلة المستخدمة. لذا ليس من الضروري ان يوجد سبب يجعل الأسلحة لها آثار متفجرة، كما ان الأسلحة البيولوجية والكيميائية ليست من الأسلحة الحركية ولكن يبدو ان محكمة العدل الدولية قد تعامل ت ضمناً على أنها استخدام للقوة. حيث كلما زاد فاعلية سلاح جديد مقارنة بالسلاح التقليدي زاد احتمال ان يكون استخداماً للقوة او هجوماً مسلحاً.

(١٢٥) د/ كمال الدين، النزاع المسلح والقانون الدولي العام، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، ط ١، ١٩٩٧، ص ٣١

(١٢٦) د/ مصطفى احمد ابو الوفا، المبادئ العامة في القانون الدولي المعاصر، إشراك للطباعة والنشر، مصر، ٢٠٠٦، ص ٢٦٠ وما بعدها

(ISSN: ٢٣٥٦ - ٩٤٩٢)

ليست تسمية الجهاز (الكومبيوتر) أو الوسيلة المستخدمة كافية لاعتباره قوة أو سلاحاً، بل أن القصد من الاستخدام هو التأثير الذي يعد نقطة الالتقاء ما بين الهجوم السيبراني والقوة العسكرية. حيث ان استخدام أي جهاز أو عدد من الأجهزة مما يؤدي الى خسائر كبيرة في الأرواح أو تدمير كبير للممتلكات ينبغي عده مستوفياً لشروط الهجوم المسلح.(١٢٧)

- **مدى إمكانية تطبيق المادة (٥١) من ميثاق الأمم المتحدة على الهجوم السيبراني**

لا تزال القوة عنوان العلاقات الدولية حيث كان استخدام القوة في شن الحروب أمراً مشروعاً وإحدى الوسائل المستخدمة من أجل فض النزاعات بين الدول. قبل ميثاق الأمم المتحد ة وميثاق عصبة الأمم كانت الدول تلجأ الى القوة لشن الهجوم لأن القوة تعتبر مظهراً من مظاهر سيادة الدول حيث استطاعت الجهود الدولية في عهد منظمة الامم المتحدة الى تغيير بعض القواعد التي كانت سائدة في عهد عصبة الامم والتي منها استخدام القوة، حيث بات الأصل حظر استخدام القوة في العلاقات الدولية والاستثناء هو استخدامها في حالة الدفاع الشرعي مع تقييدها بالعديد من القيود وفقاً للمادة (٥١) من ميثاق الامم المتحدة استناداً لهذه المادة فأن كل دولة تتعرض للعدوان يكون من حقها الرد باستخدام وسائل القوة اللازمة لمواجهة العدوان فقط، ولا يجوز لها ان تتعدى في ذلك. لذا فأن الدفاع الشرعي ليس حق مطلق للدول بل مقيد ببعض القيود فلا يمكن استخدامه إلا إذا كان مستوفياً لشروطه المنصوص عليها (٥١) من الميثاق.

أصبحت مسألة أمن الفضاء السيبراني من أولويات الأمن القومي للعديد من الدول التي تعتمد بشكل كبير على التكنولوجيا والاتصالات في إدارة شئونها الداخلية. كما أن حق الدولة المعتدى عليها في الرد على الهجوم السيبراني يجب ان لا يخرج عن أطار ميثاق الامم المتحدة والقانون الدولي الإنساني من حيث الضرورة والتناسب. يجب ان يستوفي رد الفعل في الدفاع عن النفس ضد الهجمات السيبرانية التي ترتقي الى مستوى الهجوم المسلح بمتطلبات الضرورة والتناسب الذي لم تشر اليه المادة (٥١) من ميثاق الأمم المتحدة بشكل واض ح، إلا ان الرأي الاستشاري بخصوص الأسلحة النووية عام ١٩٩٦ هو ان يتوفر في ممارسة الحق في الدفاع عن النفس شروط الضرورة والتناسب التي تعد قاعدة من قواعد القانون الدولي العرفي، حيث ان هذا الشرط المزدوج ينطبق على المادة (٥١) من الميثاق بغض النظر عن وسائل القوة المستخدمة.

كما ان مسألة الضرورة تُعد من الموضوعات الشائكة وصعبة التقييم، لكن تطبيقاً لهذا المبدأ يجب ان تكون القوة المستخدمة في الرد السبيل الوحي د لمواجهة الدولة المعتدية. كما يجب ان يكون الرد

(١٢٧) طالب خيره، مبدأ حظر استخدام القوة في العلاقات الدولية، كلية العلوم الإنسانية والاجتماعية، جامعة ابن خلدون، ٢٠٠٧، ص٩

على الهجوم السيبراني ضرورياً لكي يكون الرد قانونياً ينطبق عليه صفة الدفاع الشرعي ان حق الدولة المعتدى عليها في استعمال القوة للرد على الهجوم ان لا يكون هذا الحق مطلق وانما مقيد وفق المادة (٤٨) من الملحق الإضافي لاتفاقية جنيف التي حددت الأهداف التي من الممكن استهدافها من قبل الدولة المعتدى عليها وهي (الاهداف العسكرية). كما بينت اتفاقية لاهاي الرابعة ليس من حق الدولة المعتدى عليها استهداف أو تدمير ممتلكات المدنيين وإلا عد استهدافها انتهاك لأحكام اتفاقية لاهاي مما يشكل جريمة وفقاً لأحكام اتفاقية روما المنشئة للمحكمة الجنائية الدولية.(١٢٨)

أكدت الإدارة الامريكية على ان استخدام القوة في الدفاع عن النفس ضد أي هجوم سيبراني ينبغي ان يقتصر الرد على ما هو ضروري لمواجهة الهجوم، وكذلك ان يكون متناسباً مع الخطر الذي يواجه لأن هذا يعد جوهر الدفاع عن النفس. وكذلك أكدت محكمة العدل الدولية في العديد من المواقف على ان الدفاع عن النفس يجب ان يكون متناسباً مع الهجوم المسلح والضروري للرد عليه باعتبارها قاعدة رسخة في القانون الدولي العرفي التي غابت عن احكام ميثاق الامم المتحدة الخاصة في حق الدفاع عن النفس.

حيث يتوجب على الدولة التي تستخدم حقها في الدفاع عن النفس رداً على الهجوم السيبراني ان تلتزم بأحكام اتفاقية جنيف التي تمنع ان يتضرر السكان المدنيون وممتلكاتهم من جراء الأخطار الناجمة عن الهجوم المسلح. كما يجب ان لا تكون ممتلكات ومصالح المدنيين من بنوك ومستشفيات وكهرباء هدف للدولة صاحبة الحق في الرد لكي لا يكون حق استخدام القوة في الدفاع عن النفس من الدولة المعتدى عليها ذريعة لتدمير البنة التحتية للدولة المعتدية، حيث ان اي انتهاك لاتفاقية جنيف من قبل الدولة عند استعمالها حق الدفاع الشرعي ستكون مسؤولة عن هذا الانتهاك. لذلك فأن الدولة المعتدى عليها في حال استعمال حقها في مواجهة الهجوم السيبراني لم تراعي احكام اتفاقية جنيف واتفاقية لاهاي الرابعة سوف تتسبب في انتهاك احكامهما. لذلك فأن سوء استخدام القوة في الدفاع عن النفس قد يحول الدولة من صاحبة حق الى دولة مسؤولة عن الانتهاكات التي خلفها الهجوم المخالف للأحكام والأعراف الدولية، وعليه يجب ان يكون مبدأ التناسب حاضراً في كل الحالات لأنه يعد جوهر وروح القانون الدولي الإنساني.

كما ان السيادة تعد من المبادئ الجوهرية التي قام عليها ميثاق الامم المتحدة فقد نصت الفقرة الثانية من المادة الأولى بأن "تقوم الهيئة على مبدأ المساواة في السيادة بين جميع الأعضاء" فاذا ما تعرضت سيادة اي دولة للانتهاك جاز لها استعمال القوة من أجل الدفاع عن سيادتها، لذلك تشكل

(١٢٨) د/ محمد خليل موسى، استخدام القوة في القانون الدولي المعاصر، دار وائل للنشر، الأردن، ٢٠٠٤، ص ٩

(ISSN: ٢٣٥٦ - ٩٤٩٢)

الهجمات السيبرانية انتهاكاً واضحاً لسيادة الدولة مما يجيز لها استخدام القوة لوقف هذا الانتهاك الذي يعد الأخطر على سيادة الدولة.(١٢٩)

ومن أهم الأمثلة على ذلك الهجوم الالكتروني الذي تعرضت له مواقع الكترونية في استونيا عام ٢٠٠٧ الذي وصفه خبراء في أمن شبكات الكومبيوتر بأنه الأعنف في التأريخ، حيث استهدف البنية التحتية الإلكترونية بشكل كامل مما جعل استونيا معزولة عن العالم. وقد أكد خبراء في هذا المجال ان روسيا هي من تقف وراء هذا الهجوم المدمر، وكذلك الهجوم السيبراني الذي استهدف مفاعل النووي الايراني في عام ٢٠١٠، حيث اتهمت إيران الولايات المتحدة الامريكية واسرائيل بإرسال فيروساً الكترونياً أطلق عليه اسم (Stuxnet) الذي تسبب في تعطيل آلاف الحواسيب، كما استهدف أجهزة الطرد المركزي بهدف تعطيله، ومن ثم فأن هذه الأمثلة تؤكد على حجم الدمار الذي يخلفه الهجوم السيبراني الذي يستدعي الرد من الدولة المعتدى عليها استناداً لمبدأ حق الدفاع الشرعي المنصوص عليه في ميثاق الأمم المتحدة في نص المادة (٥١)، من أجل الحفاظ على وجودها ومنع خرق سيادتها التي تعد من أهم المبادئ الأساسية التي يقوم عليها مبدأ الاحترام المتبادل بين الدول.

٢- القيود التي يفرضها القانون الدولي للهجمات في إطار الحرب السيبرانية:

إذا كانت قواعد الحرب التقليدية لا تنطبق حرفياً على الحرب السيبرانية حسب اتفاقيات جنيف الأربع لعام ١٩٤٩ وبروتوكولاتها الإضافية، إلا أن التكنولوجية السيبرانية لم تولد في فراغ قانوني، ذلك أن تقريري ٢٠١٣ و ٢٠١٥ اللذين أعدتهما مجموعة الأمم المتحدة للخبراء الحكوميين بشأن "التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي" أكدا أن القانون الدولي، وبخاصة ميثاق الأمم المتحدة، ينطبق، وهو ما يؤدي بنا إلى القول بأن القانون الدولي الإنساني ينطبق على الحرب السبيرانية إذا كانت هناك حالة نزاع مسلح وتسببت هجمات إلكترونية في تدمير بنى تحتية الحقت ضرراً بالمدنيين كاضطراب أنظمة المواصلات أو المستشفيات أو وقوع خسائر في الأرواح البشرية. وفي رأيها الاستشاري بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها. أشارت محكمة العدل إلى أن مبادئ وقواعد القانون الدولي المطبق في النزاع المسلح تنطبق على جميع أشكال الحروب وعلى جميع أنواع الأسلحة، بما في ذلك المستقبلية.(١٣٠)

ويشير تقرير اللجنة الدولية للصليب الأحمر لسنة ٢٠١٥ المعنون باسم " تقرير عن القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة" : ... إن أي لجوء إلى القوة سواء كان سبيرانياً أو حركياً (مادياً) بحسب طبيعته يظل دائما محكوما بميثاق الأمم المتحدة وقانون اللجوء إلى الحرب،

(١٢٩) د/ عامر عبد الفتاح الجومرد، السيادة، مجلة الرافدين للحقوق، جامعة الموصل، العدد الاول، ١٩٩٦، ص ١٦٣
(١٣٠) إيهاب خليفة، القوة الإلكترونية: كيف يمكن أن تدير الدولة شؤونها في عصر الإنترنت، دار العربي للنشر والتوزيع، القاهرة، ٢٠١٧، ص١٦٥

وأن القيود موجودة بمقتضى القانون الدولي إذا ما لجأت أو عندما تلجأ الدول والجماعات المسلحة إلى اعتداءات سبيرانية أثناء نزاع مسلح.

ولعل الاستجابة الدولية الأهم والأبرز لمعالجة الهجمات السبيرانية وردت في إصدار ما يسمى "دليل تالين" الذي يبحث إمكانية تطبيق القانون الدولي على الفضاء السبيراني، حيث تناول هذا الدليل عددا من المفاهيم مثل الحصار السبيراني الهجمات المصحوبة باستخدام القوة. وهذه المفاهيم تخضع للقانون الدولي الإنساني سواء تم تطبيقها في البر أو الجو أو البحر ويقر الدليل بأن الهجمات الإلكترونية وحدها قد تشكل نزاعات مسلحة تبعا للظروف لاسيما الآثار المدمرة لتلك الهجمات وفي هذا الصدد عرّفت المادة ٣٠ من الإصدار الأول لهذا الدليل لعام ٢٠١٣ الهجوم السبيراني بأنه: عملية إلكترونية سواء هجومية أو دفاعية والتي من شأنها أن تسبب إصابة أو موت أشخاص أو إتلافا أو تدميرا لمنشآت.(١٣١)

وفي السياق ذاته تُطرح عدة إشكالات بشأن القيود والحدود التي يفرضها تطبيق بعض قواعد القانون الدولي الإنساني على الهجمات السبيرانية في إطار نزاع مسلح كقواعد التمييز وحظر الهجمات العشوائية والالتزام باتخاذ الاحتياطات.

أ- قاعدة التمييز وحظر الهجمات العشوائية: يقتضي القانون الدولي الإنساني التمييز بين المقاتلين وغير المقاتلين وبين المنشآت المدنية والعسكرية كما تحظر الهجمات العشوائية التي من شأنها أن تصيب الأهداف العسكرية والأشخاص المدنيين أو الأعيان المدنية دون تمييز، لكن في حرب الهجمات السبيرانية تصبح مسألة التفريق بين من يقاتل ومن لا يقاتل صعبة، حيث لا يوجد جرحى ولا أسرى، بل توجد مرافق وأنظمة لا تعمل أو دمار ذاتي مشابه للقصف والتدمير التقليدي، كما أن نظم الحواسيب العسكرية غالبا ما تتصل بالنظم التجارية والمدنية وتعتمد عليها كليا أو جزئيا، بل وقد يكون هناك تداخل بين الاستخدامات المدنية والعسكرية بارتباطهما بشبكة واحدة ووسيط واحد هو الفضاء السبيراني ، ومن ثم يكون من المستحيل شن هجوم سبيراني على بنية تحتية عسكرية، وجعل آثارها تقتصر على هدف عسكري وحسب.

ب- قاعدة الالتزام باتخاذ الاحتياطات توجب المادة ٧٥ من البرتوكول الإضافي لاتفاقيات جنيف ١٩٤٩ التزاما على الدول باتخاذ كل الإجراءات في شكل اختيار وسيلة وطريقة الهجوم، من أجل تفادي أو تخفيف الأضرار العرضية التي قد تلحق بالبنية التحتية المدنية أو من شأنها أن تؤذي

(١٣١) د/ عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي المعاصر، مرجع سابق، ص٩٦

(ISSN: ٢٣٥٦ - ٩٤٩٢)

المدنيين. وهنا يثار الإشكال حيث توجد صعوبة في ممارسة الهجوم نظرا لتشابك شبكات الاتصالات والمعلومات ويتعذر التمييز بين ما يعد أنظمة مدنية وعسكرية.(١٣٢)

الفرع الثاني

المسؤولية الدولية عن الهجمات الحربية السبيرانية

أصبحت الدراسات القانونية المتخصصة تبحث في إمكانية توجيه المسؤولية الدولية ضد دولة أو مجموعة من غير الدول تنسب إليهم تهم بارتكاب هجمات حربية سيبرانية، علما أن البند السادس من دليل تالين يُحَمّل المسؤولية القانونية للدول عن أنشطتها السبيرانية التي تخرق بموجبها أي التزام دولي.(١٣٣) وفي هذا السياق تطرح عدة إشكالات قانونية أهمها:

١ – كيفية التعامل مع الإسناد والمسؤولية

أ– تُطرح إشكالية تحديد المسؤولية خلف الهجمات الحربية السبيرانية بوصفها تحديا قانونيا، خاصة الدول التي تعاني من هجمات الفضاء السبيراني التي تصاحبها حالة من التوترات والصراعات الدولية ،العالية ومن ثَمَّ توجد صعوبة في تمييز ذلك الهجوم والتحقق منه. كما أنه حتى إذا أخذت الهجمات مجرد ردة فعل، فإنها قد لا تستطيع التمييز بين الأطراف، ومن ثم تصبح غير قانونية وذلك لعبور الشبكات الحدود الدولية، وإصابة أطراف محايدة، كما أن التحقيقات بشأن الهجمات السبيرانية قد تجمع بين المبادئ الأساسية لعمل أجهزة الاستخبارات بوصفها عملا طبيعيا ماديا وبين الإلكتروني العابر للشبكات والحدود الدولية، لكن المحققين في أجهزة الاستخبارات الدولية قد لا يستطيعون الولوج إلى دول أخرى؛ لأن ذلك يشكل مساسا وانتهاكا لسيادتها.(١٣٤)

ب– هناك إشكالية ثانية متفرعة عن الإشكالية الأولى وهي تحديد هوية المعتدي فجهل الهوية في الفضاء السبيراني قاعدة وليس استثناء، وينجم عن ذلك صعوبة في تحديد مسؤولية الهجوم ونسبته لطرف أو جهة معينة وبما أن القانون الدولي يقوم على توزيع المسؤوليات على طرف أو نزاع أو فرد، تنشأ صعوبات كبيرة، وبالتالي تظل العلاقة بين الهجمات السبيرانية وأحد النزاعات المسلحة من الصعب إثباتها. وتحديد ما إذا كانت تقوم المسؤولية الدولية في ظل عدم ثبوت هوية المهاجم.

٢ – مدى مسؤولية الدولة عن تصرفات الأفراد

لاشك أن هناك إجماعا بين الخبراء الدوليين أن القانون ينطبق على شبكة الإنترنت بما في ذلك القانون الدولي لمسؤولية الدولة ذلك فإسناد تصرف ما إلى دولة بموجب القانون الدولي يحتاج إلى

(١٣٢) د/ عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي المعاصر، مرجع سابق، ص١٠١
(١٣٣) د/ سعيد درويش، ماهية الحرب الإلكترونية في ضوء قواعد القانون الدولي، حوليات جامعة الجزائر، العدد ٢٩، ج٢، ٢٠١٦، ص١٢٧
(١٣٤) د/ عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي المعاصر، مرجع سابق، ص١٢٢

دليل واسع على سيطرة الدولة على القراصنة فوفقا لقواعد المسؤولية غير المباشرة في القانون الدولي. تعد الدولة مسؤولة عن الأفراد الذين يعملون تحت سيطرتها الفعلية حيث تسأل عن أفعال رعاياها بشرط تحقق السيطرة الكاملة والفعلية، وقد ناقش فقهاء القانون الدولي بشكل مستفيض طبيعة هذه السيطرة الفعلية على أرض الواقع، لكن محكمة العدل الدولية قضت بأن انتهاكات قانون النزاعات المسلحة من قبل الأفراد لا يمكن أن تُعزى إلى دولة إلا إذا كان يمكن إثبات أن هذه الدولة أعطت تعليمات أو أجبرت على القيام بعملية ما، ومن ثَمَّ فعلى الدولة الضحية أن تثبت أن الدولة العدو أمرت أو كانت لديها "سيطرة فعالة على كل جوانب الهجوم الإلكتروني وهذا ليس بالأمر السهل . كما أن هذه المسألة وغيرها مازالت محل بحث ونقاش؛ ذلك أن المساهمين في دليل "تالين يحاولون إيجاد توافق في الآراء حول كيفية تطبيق قانون مسؤولية الدولة لاستخدام الأفراد في الهجمات الحربية السيبرانية. كما يطالب الخبراء في القانون الدولي بتطوير قواعد المسؤولية الدولية حتى لا تقف عقبة في وجه من تصيبهم الأضرار المترتبة عن الهجمات الحربية السيبرانية من التعويض العادل، فالمفهوم التقليدي للمسؤولية لم يعد قادرا على التكيف والتلاؤم مع الآثار والأضرار التي تسببها هذه الهجمات، لأن الأضرار تظل خطيرة وشاملة، وإثباتها أمر صعب.(١٣٥)

المطلب الثانى

موقف القانون الدولي من الهجمات الإرهابية الإلكترونية

تطرح هجمات الإرهاب السيبراني كأحد أنماط الإرهاب الدولي المعاصر العديد من الإشكالات، حيث لم تعالج الأمم المتحدة حتى الآن أية حالة يمكن الاستناد إليها بشأن الهجمات الإرهابية الإلكترونية كي يتسنى إمكانية تعاطي القانوني الدولي معها فالقانون الدولي لم يُعْطِ تعريفا واضحا ومنهجا معينا للتعامل مع هذا النوع المستحدث من الهجمات، بالرغم من أن خطورتها تضاهي خطورة هجمات الحرب السيبرانية من حيث الآثار والأضرار الجسيمة التي يمكن أن تخلفها علما أن الإرهاب لا يميز بين الأشخاص والمؤسسات والأنظمة إلا أن الجهات الأكثر استهدافا للعمليات الإرهابية السيبرانية هي المنظمات والدول لذلك سنتطرق في هذا المطلب إلى الاتفاقية الأوروبية بودابست لسنة ٢٠٠١، وقرارات الأمم المتحدة الفرع الأول، ثم ضرورة التوجه إلى تبني إطار تشريعي دولي ملزم لمواجهة الهجمات الإرهابية السيبرانية (الفرع الثاني).

(١٣٥) طارق المجذوب، السايبر ساحة خفية حرب ناعمة قادمة، مجلة الدفاع الوطنى اللبناني، العدد ٨٩، ٢٠١٤، شركة ناشرون لتوزيع الصحف والمطبوعات، لبنان ، ص٣٢

(ISSN: ٢٣٥٦ - ٩٤٩٢)

الفرع الأول

اتفاقية بودابست لسنة ٢٠٠١ وقرارات الأمم المتحدة

أ- الاتفاقية الأوروبية بودابست لمكافحة الإجرام الإلكتروني لسنة ٢٠٠١ لقد دعت ثلاثون دولة إلى التوقيع على أول اتفاقية دولية لمكافحة الإجرام السبيراني في العاصمة المجرية بودابست عام ٢٠٠١ عقب الهجمات الإرهابية التي تعرضت لها الولايات المتحدة في ١١ سبتمبر من العام نفسه. وتعد هذه الاتفاقية بمثابة المصدر القانوني الدولي الأول لكل الاتفاقيات الدولية والإقليمية والتشريعات الوطنية ذات الصلة بالإرهاب الإلكتروني، ونظرا لأهميتها انضم إلها العديد من الدول خارج مجلس أوروبا كالولايات المتحدة الأمريكية واليابان وكندا، وجنوب إفريقيا، وفي سياق ربطها بموضوع الهجمات الإرهابية الإلكترونية، يتطرق نص الاتفاقية إلى تجريم الأفعال التي تمس سرية وسلامة الأنظمة المعلوماتية، كالدخول غير القانوني المتعمد (القرصنة) والاعتراض على سلامة البيانات، وعرقلة الاستخدام الشرعي لنظام المعلومات، وإساءة استخدام أجهزة الحاسوب. وتهدف الاتفاقية بالأساس إلى السعي لتحقيق وحدة التدابير التشريعية بين الدول الأوروبية والدول المنضمة من غير الدول الأوروبية والتأكيد على أهمية التعاون الإقليمي والدولي في ميدان مكافحة جرائم الكمبيوتر والإنترنت، وضرورة فعالية خطط العمل لمكافحة الأنشطة التي تستهدف سرية وسلامة وتوفر المعلومات وأنظمة وشبكات الكمبيوتر، بما في ذلك تحديد الإطار الموضوعي لهذه الأنشطة، والإطار الإجرائي المتصل بالتحقيق والتحري والمقاضاة، فالاتفاقية تشجع على الاحتفاظ بمعطيات الربط وتفتيش الأنظمة المعلوماتية، وكذا مصادرة المعلومات وهي تدعو أيضا إلى جمع معطيات الاتصال ومحترى البرقيات الإلكترونية في الوقت المناسب لمعرفة مصدر أي هجوم إرهابي محتمل.[١٣٦]

ب- قرارات الأمم المتحدة ذات الصلة بالإرهاب الإلكتروني: أدركت الأمم المتحدة أن الاستخدام الإرهابي لتكنولوجيا الاتصال والمعلومات يعمل على إنشاء مواقف تشكل تهديدا للسلم والأمن الدوليين لذلك توزع اهتمامها بموضوع الإرهاب بصورة عامة والإرهاب الإلكتروني بصورة خاصة من مستوى الإدانة والتحذير عبر القرارات المتفرقة الصادرة عن مجلس الأمن الدولي، مرورا بمستوى البناء القانوني لصيغ المواجهة وصولا إلى وضع الخطط والإستراتيجيات الشاملة لمواجهة مثل هذا النوع من الهجمات بالنظر إلى تطور وسائل الخطر الدولي، حيث أصدرت الجمعية العامة العديد من القرارات التي توضح مدى تصاعد الاهتمام العالمي باستخدام تكنولوجيا الاتصال والمعلومات استخداماً غير سلمي، كقرار الجمعية العامة المتخذ في الدورة ٥٥/ ٨٢ ديسمبر ٢٠٠٠ والدورة ٦٥/ ١٩ ديسمبر

(١٣٦) بلقاسم بن صابر، الهجمات السيبرانية ومواجهتها في ضوء القانون الدولى المعاصر، مجلة حقوق الإنسان والحريات العامة، العدد ٤، ٢٠١٧، ص٢٠٥

٢٠٠١ بشأن إرساء الأساس القانوني لمكافحة إساءة استعمال تكنولوجيا الاتصال والمعلومات في أعمال إجرامية، وقرارها المتخذ في الدورة ٨٧/ ٢٣٩ ديسمبر ٢٠٠٢ بشأن إرساء ثقافة عالمية للأمن الإلكتروني بوصفه من القرارات الهامة التي تستهدف العمل على حماية البنية التحتية الحيوية للمعلومات، وحث وتفعيل دور المنظمات الدولية ذات الصلة ودعوة الدول إلى وضع استراتيجيات للتقليل من حجم التعرض للهجمات والأخطار السيبرانية التي تشكل تهديدا للبنية التحتية الحيوية للمعلومات. وقبل ذلك كانت قد قدمت روسيا في ديسمبر ١٩٩٨ مقترحا للجمعية العامة يتضمن مسودة قرار حول " التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي" تم تبنيه بالإجماع من أجل دعوة كل الدول لإبلاغ الأمين العام للأمم المتحدة بوجهات نظرهم حول تحديد الأفكار الأساسية المرتبطة بقضايا أمن المعلومات والعمل على تطوير المبادئ والقواعد الدولية التي من شأنها دعم أمن نظم المعلومات والاتصالات، والمساعدة في مكافحة الاستخدام الإرهابي والإجرامي لها، وفي عام ٢٠٠١ وافق أعضاء الأمم المتحدة على قرار إنشاء "مجموعة الخبراء الحكوميين GGE" التي بدأت عملها ٢٠٠٣ بهدف مناقشة الأخطار القائمة المحتملة في مجال أمن المعلومات الدولي، والإجراءات الممكنة لوضع الأسس الدولية التي تهدف إلى تقوية أمن نظم الاتصالات والمعلومات العالمية وفي ٨ سبتمبر ٢٠٠٦ بذلت الجمعية العامة للأمم المتحدة جهودها بإقرار إستراتيجية عالمية موحدة لمكافحة الإرهاب، وكان الإرهاب الإلكتروني حاضرا في سياق هذه الإستراتيجية حيث أشارت الفقرة ١٢ – ١و٢ إلى ضرورة التنسيق والعمل والمساعدة مع الدول الأعضاء والمنظمات الدولية والإقليمية ودون الإقليمية المعنية لتحديد وتبادل أفضل الممارسات في مجال منع الهجمات الإرهابية الإلكترونية ضد الأهداف المعرضة للخطر بشكل خاص.(١٣٧)

الفرع الثاني

التوجه نحو تبني إطار تشريعي دولي ملزم لمواجهة الهجمات الإرهابية السبيرانية

يضفي البعد الدولي للهجمات الإرهابية السبيرانية تعقيداً في مواجهتها خاصة أمام عدم وجود إطار قانوني دولي واضح يعالج الظاهرة المستحدثة، وهذا يستلزم إما وجود قانون دولي جديد أو عقد اتفاقيات مكملة للاتفاقيات المتعلقة بالإرهاب الدولي. ونشير هنا أنه في عام ٢٠٠٠ صدرت مسودة اتفاق عالمي حول الجريمة والإرهاب الإلكتروني من جامعة استانفورد فيما عرف بخطة ستانفورد، وقد شملت الخطة العديد من النقاط حول هدف الوصول إلى تعاون أوسع في مقاومة الهجمات السبيرانية على اعتبار أن الإرهابيين والمجرمين يستغلون نقاط الضعف في القوانين الوطنية للدول وجمودها في

(١٣٧) بلقاسم بن صابر، الهجمات السيبرانية ومواجهتها في ضوء القانون الدولى المعاصر، مجلة حقوق الإنسان والحريات العامة، العدد ٤، ٢٠١٧، ص٢٠٦

(ISSN: ٢٣٥٦ - ٩٤٩٢)

مواجهة مثل هذه الهجمات، علما أن دليل تالين في البند ٢٦ نص على منع الهجمات الإرهابية الإلكترونية التي تهدف إلى ترويع المدنيين، إلا أن هذه التوجهات تظل تفتقد الطابع الإلزامي لعدم صياغتها في إطار اتفاقية دولية شاملة وملزمة، وهو الأمر الذي دعا إليه الخبراء والمتخصصون في القانون الدولي خلال أشغال "المؤتمر الدولي لتجريم الإرهاب الإلكتروني" المنعقد في ١٥ و ١٦ ماي ٢٠١٧ بالعاصمة الإماراتية أبوظبي بمشاركة الأمم المتحدة والذي توج بما سمي "إعلان أبوظبي" إلى إيجاد أرضية مشتركة لصياغة منظومة قوانين وتشريعات دولية تواجه هجمات الإرهاب الإلكتروني وفي هذا الصدد صرح المسؤول الأممي نيابة عن الأمين العام للأمم المتحدة السيد "جهانجير خان" بأنه:" أصبحت هناك حاجة ملحة لإدخال تعديلات قوية وفي الوقت ذاته مرنة في القانون الدولي تواكب الوتيرة السريعة في استخدام التقنيات الإلكترونية لمواجهة مثل هذه الهجمات الإرهابية".

ونرى من وجهة نظرنا؛ أنه في ظل غياب صك دولي خاص لمواجهة الهجمات الإرهابية السبيرانية أن السبيل الأفضل للتعامل معها على الأقل في الوقت الراهن هو النظر إليها على أنها فعل قريب من الحرب، نظرا لتداعياتها التي تشكل تهديدا خطيرا على أمن الدول والمجتمع الدولي ككل وهذا يتحتم على دول العالم تكثيف آلية التعاون الدولي لصدها من خلال تفعيل الأطر القانونية للتدخل في تتبع وضبط وتسليم منفذي هذه الهجمات والتعاون والتنسيق الدائم مع الأنتربول والعمل على إيجاد مؤسسات وأجهزة دولية مكلفة بتتبع ديناميكية الهجمات الإرهابية السبيرانية، إضافة إلى ابتكار جهاز متخصص على مستوى كل دولة مكلف بالرقابة الشاملة للهجمات السبيرانية التي يمكن أن تشن من قبل الجماعات الإرهابية.(١٣٨)

المطلب الثالث

القانون الواجب التطبيق على الهجمات السيبرانية بين الدول

الفرع الأول

إتفاقية بودابست لعام ٢٠٠١ المتعلقة بالجريمة السيبرانية

من أهم الآثار المترتبة على تكييف الهجمات السيبرانية التي تنفذها الدول ضد بعضها البعض، هو البحث على القانون الواجب التطبيق، فإضافة إلى الأساس القانوني الذي تم الإعتماد عليه في تحديد طبيعة الهجوم، ينبغي أيضاً تحديد القواعد التي تحكم هذه التصرفات، وباستقراء نصوص إتفاقية بودابست لعام ٢٠٠١ المتعلقة بالجريمة السيبرانية، يتضح لنا أنه يمكن تطبيق بعض موادها على هذه المسألة.

(١٣٨) د/ سعيد درويش، ماهية الحرب الإلكترونية في ضوء قواعد القانون الدولى، حوليات جامعة الجزائر، العدد ٢٩، ج٢، ٢٠١٦، ص١٢٩ وما بعدها

على ضوء ما سبق، أبرمت إتفاقية بودابست كما جاء في ديباجتها، نتيجة للتغييرات العميقة التي نجمت عن الظاهرة الرقمية، وعن التقارب الرقمي والعولمة المستمرة لشبكات الحاسوب، وكذا إدراكاً للدول الأطراف فيها بالمخاطر التي قد تنجم عن إستخدام شبكات الحاسوب والمعلومات السيبرانية، في إرتكاب أفعال جنائية، لاسيما وأن المكافحة الفعالة لجرائم الفضاء المعلوماتي، تستلزم مزيد من التعاون الدولي السريع والفعال في المسائل الجنائية.(١٣٩)

بالإضافة إلى إتفاقية الإتحاد الإفريقي المتعلقة بالجريمة السيبرانية وحماية المعطيات ذات الطابع الشخصي، المبرمة بتاريخ ٢٠١٤/٦/٢٧، تضمنت في فصلها الثالث المعنون بـ: حماية الأمن السيبراني ومكافحة الجريمة السيبرانية.

لكن ما يعاب أيضاً على الإتفاقيتين، أي إتفاقية بودابست وإتفاقية الاتحاد الإفريقي هو كونهما تتعلقان بالجريمة السيبرانية التي تنفذ من قبل الأفراد وضد الأفراد، دون أن تتطرقا بالتحديد إلى الهجمات السيبرانية التي تشنها الدول ضد بعضها البعض.

الفرع الثاني

أحكام دليل تالين لعام ٢٠١٣ الخاص بالحرب السيبرانية

إن إستبعاد قواعد إتفاقية بودابست من التطبيق في حالة الهجمات السيبرانية التي تقع بين الدول، يجعلنا نبحث عن أساس قانوني آخر يمكننا الإعتماد عليه في تحديد طبيعتها القانونية وكذا القواعد التي تحكم مثل هذه الجرائم، لاسيما وأنها عادة ما ترتكب من طرف دولة ضد دولة أخرى.

من أبرز هذه النصوص قواعد دليل تالين لعام ٢٠١٣، المتعلق بقواعد القانون الدولي المطبقة على الحروب السيبرانية، أعد هذا الدليل من مجموعة خبراء في القانون الدولي بدعوة من منظمة حلف شمال الأطلسي (OTAN)، وبحضور اللجنة الدولية للصليب الأحمر الدولي (CICR)، يتكون هذا الدليل الذي يعد الوثيقة القانونية الوحيدة التي تحكم مثل هذه الإعتداءات التي تتم بين الدول، من ٩٥ قاعدة إستمدت في مجملها من أحكام القانون الدولي المختلفة كميثاق الأمم المتحدة وقواعد القانون الدولي الإنساني...وغيرها.

يقدم دليل تالين رؤى مثيرة للإهتمام في هذا الصدد فهو يتمسك على سبيل المثال بالثنائية التقليدية للنزاعات المسلحة الدولية والنزاعات المسلحة غير الدولية، ويقرر بأن العمليات الإلكترونية وحدها قد تشكل نزاعات مسلحة تبعاً للظرروف–لا سيما الآثار المدمرة لتلك العمليات–ويقدم الدليل في

(١٣٩) د/ عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، المركز العربي لأبحاث الفضاء الالكتروني، مصر، ٢٠١٨، ص٥٥

(ISSN: ٢٣٥٦ - ٩٤٩٢)

هذا الصدد تعريفاً للهجوم السيبراني بموجب القانون الدولي الإنساني بوصفه عملية إلكترونية سواء هجومية أو دفاعية يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الإضرار بأعيان أو تدميرها.

جاء دليل تالين نظراً لقصور القانون الدولي في مجال الحرب السيبرانية، نتيجة عدم وجود أي أساس قانون ينظم اللجوء إلى هذا النوع من الحرب أو ينظم سير العمليات العدائية أثناءها، لذلك تم إبرامه كصك قانوني وحيد يمكن أن يلجأ إليه في مثل هذه الظروف.

لكن ما يعاب على هذا الصك هو تطبيق نصوصه فقط على الحالات التي تتم خلال نزاع مسلح تقليدي، وهذا ما كرسته القاعدة ٢٠ من الدليل، المتعلقة بتطبيق قانون النزاع المسلح، حيث نصت على أن كل نشاط سيبري، ينبغي أن يخضع لقانون النزاعات المسلحة، لكنها إشترطت أن يتم ذلك في سياق نزاع مسلح، سواء كان دولي أو داخل الحدود الجغرافية للدولة.

بالإضافة إلى كونه ليس ملزما، إذ لا يرقى إلى مستوى الإتفاقية الدولية، فضلاً عن معارضة بعض الدول لأحكامه كروسيا والصين، على إعتبار أنهما لم تشاركا في إعداده، وكما لم يتم مراعاة التمثيل العالمي للدول في إختيار الخبراء الذين أعدوه.

الفرع الثالث

قواعد القانون الدولي التي تحكم العلاقات بين الدول

تأتي في مقدمة هذه القواعد نصوص ميثاق الأمم المتحردة، لاسيما الأحكام المتعلقة بحظر إستخدام القوة في العلاقات الدولية وحظر اللجوء إلى العدوان (أحكام الفصل السابع من الميثاق، أي المواد من ٣٩ إلى ٥١)، وكذا واجب احترام سيادة الدول واستقلالها السياسي والإقليمي (مبادئ ومقاصد الأمم المتحدة)، بالإضافة إلى أحكام إتفاقية فيينا لقانون المعاهدات لعام ١٩٦٩ ...الخ.

جاءت أحكام قواعد دليل تالين الخاص بالقانون الدولي المطبق أثناء الحروب السيبرانية، موافقة لما نص عليه ميثاق الأمم المتحدة، وكذا الصكوك الدولية ذات الصلة فيما يخص إحترام سيادة الدول، حيث تضمنت القاعدة الأولى منه مسألة السيادة وذلك بقولها: تمارس الدولة رقابتها على المنشآت السيبرانية وجميع الأنشطة ذات الصلة في إطار سيادتها الإقليمية.

كما نصت القاعدة رقم ٢ المتعلقة بالإختصاص، بأن تمارس الدولة إختصاصها على الأشخاص الممارسين للأنشطة السيبرانية داخل إقليمها الوطني، بينما شددت القاعدة ٤ على أن أي تدخل لدولة ما، في المنشآت السيبرانية لدولة أخرى يعد خرقاً لسيادتها، وفي هذا السياق، جاءت القاعدة ٦ من الدليل، لتحذر من أن الدول تتحمل المسؤولية القانونية عن أنشطتها السيبرانية التي تخرق بموجبها أي إلتزام دولي.[١٤٠]

(١٤٠) المادة ٦ من دليل تالين

أكدت الجمعية العامة للأمم المتحدة، علاوة على ذلك، أن حقوق الأشخاص خارج الفضاء السيبراني، يجب أن تحظى بالحماية أيضا داخله، وهذا ما تضمنه تقرير المفوضة السامية من خلال إعتماد القرار ١٦٧/٦٨، حيث طلبت الجمعية العامة من المفوضة السامية لحقوق الإنسان إعداد تقرير عن الحق في الخصوصية في العصر الرقمي، إذ تناول التقرير بالبحث، وفقاً لنص القرار: حماية الحق في الخصوصية وتعزيزه في سياق المراقبة الداخلية والخارجية للاتصالات الرقمية أو اعتراضها وجمع البيانات الشخصية. حيث قدم التقرير إلى مجلس حقوق الإنسان في دورته السابعة والعشرين وإلى الجمعية العامة في دورتها التاسعة والستين.

ينطبق القانون الدولي الإنساني بمبادئه وقواعده بصفة عامة على أي نزاع مسلح، ويشمل ذلك وسائل الحرب المستخدمة ومكان النزاع أو الصراع المسلح، ولكن في حالة كون مكان النزاع هو الفضاء السيبراني والأجهزة المستخدمة ذات خواص حديثة ومتطورة فهل ينطبق عليها ذلك؟[١٤١]

إستثنت اللجنة الدولية للصليب الأحمر في تقريرها عام ٢٠١٥ عمليات التجسس من إنطباق القانون الدولي الإنساني عليها، ولكنها إستدركت على هامش التقرير أنه من الممكن أن يشملها القانون الدولي الإنساني إذا أدت إلى إختراقات تقود لأضرار مادية كبيرة، حيث أن أغلب العمليات السيبرانية تتم في بدايتها عن طيرق التجسس والحصول على الإذن بالدخول للبيانات، المستهدفة عن طريق إختراق ذلك الجهاز أما الإستثناء الثاني فيتعلق بتشويش الاتصالات اللاسلكية والبث التلفزيروني فلم يتم إعتباره من قبيل الهجوم الوارد في القانون الدولي الإنساني.[١٤٢]

المطلب الرابع

المسؤولية الناشئة عن الهجمات السيبرانية

يتنازع موضوع القواعد التي تنظم استخدام الهجمات السيبرانية في الفضاء السيبراني ومسألة خضوعها لقواعد القانون الدولي الإنساني من عدمه اتجاهان، الأول يرى أن هناك فراغاً قانونياً، وهذا يقود إلى عدم خضوع الهجمات السيبرانية لقواعد تنظم عملية استخدامها وإمكانية إسناد المسؤولية عن استخدامها فيما يرى اتجاه آخر عكس ذلك، ولمزيد من التفصيل في الموضوع سنبينها كما يأتي:

أولاً: مسألة الفراغ القانوني

يوصف الفضاء السيبراني بأنه فضاء مستقل بذاته ويختلف عن الفضاءات الأخرى، ومنها الفضاء المادي، وبناء على ذلك يذهب جانب من الفقه الإنكلوسكسوني إلى أن الفضاء السيبراني هو منطقة مباحة ولا قانون يحكمها، ويمكن لأي شخص القيام بأي نشاط حتى لو كان معادياً دون أن

(١٤١) يحي مفرح الزهراني، الأبعاد الإستراتيجية والقانونية للحرب السيبرانية، نفس المرجع، ص٢٤٢
(١٤٢) يحي مفرح الزهراني، الأبعاد الإستراتيجية والقانونية للحرب السيبرانية، نفس المرجع، ص٢٤٣

(ISSN: ٢٣٥٦ - ٩٤٩٢)

يخضع لأي قواعد، وقد بنيت هذه الفكرة على أن كلمات المرور وأجهزة الكومبيوتر هي التي تفصل الفضاء السيبراني عن العالم المادي، وهي لا يمكن أن تحدد بدولة معينة وعليه لا يمكن إخضاع الفضاء السيبراني حتى للقواعد الدولية التقليدية التي لم تنجح – بصورة كاملة – حتى الآن في حكم الفضاء الجوي الخارجي.

ويحتج أصحاب هذا الاتجاه بعدم وجود نص قانوني صريح في الاتفاقيات المتعلقة بالقانون الدولي الإنساني يحكم الهجمات السيبرانية على شبكات الحاسوب، وكذلك المثال في الهجمات السيبرانية؛ والسبب هو حداثة استخدام تكنولوجيات التحكم والسيطرة الالكترونية، وعدم تناسب قواعد القانون الدولي الإنساني مع وسائل وأساليب القتال الحديثة، فضلا عن أن ظهور الهجمات السيبرانية وهو حديث النشأة بالنسبة للفترة التي صيغت فيها قواعد القانون الدولي الإنساني.

الحجة الأخرى التي يحتج بها مؤيدي هذا الاتجاه هي أن عبارة (الحرب السيبرانية) لم ترد في اتفاقيات لاهاي أو جنيف أو حتى ميثاق الأمم المتحدة، بل جاءت مصطلحات أخرى مثل (استخدام القوة المسلحة) و (الهجوم المسلح)، واستشهد أصحاب هذا الاتجاه بالنزاع الروسي الإستوني والهجمات التي شنتها روسيا على جورجيا والتشويش الذي تعرضت له محاولات الرد على الهجمات بسبب عدم اليقين من انطباق القواعد الدولية على تلك الهجمات، وبالنتيجة لم توصف تلك الهجمات بأنها نزاع مسلح.(١٤٣)

والجدير بالذكر أن المادة الخامسة من ميثاق حلف شمال الأطلسي لعام ١٩٤٩ عدت أي هجوم أو عدوتن مسلح يستهدف أي طرف في الاتفاقية أنه عدوان على جميع أعضاء الحلف، وبالتالي فقد أعطت الحق لكل دولة في الاتفاقية في رد الاعتداء، استناداً على نص المادة (٥١) من ميثاق الأمم المتحدة.(١٤٤)

من خلال ما تقدم نجد أن القوانين والمعاهدات الدولية الحالية لم تتطرق إلى الهجمات السيبرانية بشكل مباشر؛ لأنها وضعت لتحكم النزاعات المسلحة التقليدية دون الهجمات السيبرانية.

ونرى أن الحجج التي ذكرها أصحاب هذا الاتجاه لا يمكن أن تكون كافية للاستناد إلى فكرة الفراغ القانوني، بدليل أنه عند ظهور تكنولوجيا جديدة لم تكن هناك مطالبات بالتخلي عن أي قواعد أو قوانين نافذة، وخير شاهد ودليل ما أفت به محكمة العدل الدولية في الرأي الاستشاري بشأن

(١٤٣) عمر محمود أعمر، الحرب الالكترونية في القانون الدولي الانساني، مجلة دراسات علوم الشريعة والقانون، تصدر عن الجامعة الاوربية، عمان، المجلد (٤٦)، العدد(٣)، سنة ٢٠١٩، ص ١٣٦

(١٤٤) نصت المادة (٥) من اتفاقية حلف شمال الأطلسي لعام ١٩٤٩ على أنه "يتفق الأطراف، على أن أي هجوم، أو عدوان مسلح ضد طرف منهم أو عدة أطراف في أوربا أو أمريكا الشمالية، يعد عدواناً عليهم جميعاً، وبناءً عليه فإنهم متفقون على أنه في حالة وقوع مثل هذا العدوان المسلح، فإن على كل طرف منهم، تنفيذاً لما جاء في المادة (٥١) من ميثاق الأمم المتحدة عن حق الدفاع الذاتي عن أنفسهم بشكل فردي أو جماعي. ينظر أيضاً: د. احمد عبيس نعمة الفتلاوي، مصدر سابق ص٦٣٤

التهديد باستخدام الأسلحة النووية بقولها (أن المبادئ والقواعد الإنسانية قد وضعت قبل اختراع الأسلحة النووية. وهذا بدوره لا يكون عائقاً أمام تطبيق قواعد القانون الدولي الإنساني، وبذلك لا يمكن القبول بفرضية الفراغ القانوني في مسألة الهجمات السيبرانية.(١٤٥)

ثانياً: إسناد المسؤولية

بينت القواعد العرفية والقواعد المدونة الدولية، المسؤولية التي يمكن إسنادها إلى دولة ما في حال صدر تصرف من مؤسساتها الرسمية على أن تكون تحت سيطرتها وقيادتها أو في حال دعمها أو توجيهها لكيانات من غير الدول كشركات امنية أو مجموعات مسلحة.

وفيما يخص الشطر الأخير من الفقرة أعلاه، وبالذات مسؤولية الدولة عن دعم الكيانات من غير الدول، فيمكن القول ان المجتمع الدولي ما زال بعيد عن الإجماع عليها، وبعبارة أخرى بيان الرابطة القانونية بين الأثر وهو الانتهاكات الجسيمة التي ترتكبها المجموعات المسلحة، والمؤثر ونقصد بذلك الدول المتهمة بالتدخل في التحريض أو المساعدة لارتكاب تلك الانتهاكات، ومن الأمثلة الأخرى على القضايا الدولية المعاصرة، والتي ما زال المجتمع الدولي يسعى إلى تنظيمها، ما نجده واضحاً في تحديد مسؤولية الدول تجاه دعم مجموعات مسلحة نفذت هجمات سيبرانية.(١٤٦)

وفي سياق المسؤولية الدولية الناشئة عن الهجمات السيبرانية، فالأمر يختلف بحسب الظروف التي يتم فيها استخدام الهجمات فلو استهدف هجوم سيبراني تعطيل وسائل الاتصالات العسكرية أو المدنية أثناء النزاع المسلح، نجد أن هذا الهجوم يخضع لأحكام القانون الدولي الإنساني لأنه يرتبط بتصرفات المقاتلين والطرق التي تدار بها العمليات العسكرية.

ويذهب أنصار هذا الاتجاه إلى رفض فكرة الفراغ القانوني في الفضاء السيبراني والاكتفاء بالقواعد القانونية النافذة لتنظيم مسألة استخدام الهجمات السيبرانية، وهذا الرأي أطلق عليه اسم (المذهب القانوني).(١٤٧)

إن مبادئ القانون الدولي الإنساني يمكن أن تنطبق على الهجمات السيبرانية التي تستهدف دولة ما، متى ما وصفت هذه الهجمات بأنها تهدف إلى إحداث الأضرار أو الوفاة وأنها متوقعة أو محتملة على قدر كبير من الواقعية، وعلى سبيل المثال فالهجوم على مطار دولي واختراق الحواسيب نفذه أشخاص تابعين إلى دولة أخرى، فإن هذا الهجوم حتماً سيؤدي إلى انطباق القانون الدولي (الإنساني).(١٤٨)

(١٤٥) عمر محمود أعمر، مصدر سابق، ص١٣٧
(١٤٦) عمر محمود أعمر، مصدر سابق، ص١٣٧
(١٤٧) عمر محمود أعمر، مصدر سابق، ص١٣٧
(١٤٨) مايكل شميت، الحرب بواسطة شبكات الاتصال، الهجوم على شبكات الكومبيوتر(الحاسوب) في الحرب منشورات المجلة الدولية للصليب الاحمر، ٢٠٠٢، ص٩٤

(ISSN: ٢٣٥٦ - ٩٤٩٢)

وفي مقابلة مع المستشار القانوني للجنة الدولية للصليب الأحمر (كوردولا دورغ) أكدت انطباق القانون الدولي الإنساني على الهجمات السيبرانية أثناء النزاعات المسلحة وأنه واجب الاحترام، وحسب رأي المستشار أعلاه فإن القانون الدولي الإنساني يدخل حيز التنفيذ إذا كانت الهجمات السيبرانية ضمن نزاع مسلح، ويستوي الحال فيما لو كان النزاع المسلح دولياً أم غير دولي، وأكدت على عدم وجود فراغ قانوني بخصوص الهجمات السيبرانية.

ومن خلال ما تقدم يتبين لنا أن انتهاك الهجمات السيبرانية للقواعد الدولية التعاهدية أو العرفية أثناء النزاع المسلح ينتج عنه إسناد المسؤولية الدولية وهذه المسؤولية تكون في إطار المبادئ المنظمة لسير العمليات العدائية.(١٤٩)

وفي إطار اسناد المسؤولية عن الهجمات السيبرانية نجد أن المادة (٥٢) من البروتوكول الإضافي الأول لعام ١٩٧٧ وصفت العين المدنية كل أمر مادي لا يعد هدفاً عسكرياً".(١٥٠)

أما المادة (٢/٥١) فقد حظرت الهجوم على الأشخاص المدنيين والأعيان المدنية بشكل مطلق، كذلك المادة (٥٢) من البروتوكول المذكور اعلاه.(١٥١)

كما بين البروتوكول الإضافي الأول أنه إذا كان الهجوم يستهدف إحداث أذى أو موت أو تلف أو دمار أو كان يتوقع ذلك من الهجوم فإن الأمر يفسر لصالح المدني ويكون الهجوم غير مشروع، والحال ذاته ينطبق على الهجمات السيبرانية.

ومثلما تتسبب الهجمات المحتملة على مفاعل نووي بدمار كبير وإطلاق الاشعاعات، فإن استخدام الهجمات السيبرانية لاستهداف البنى التحتية وقطاعات صحية تحتوي على فيروسات فتاكة قد يؤدي إلى انتشار تلك الفيروسات وبالتالي إلحاق الضرر بأرواح المدنيين، والإضرار بالبيئة بسبب الهجوم السيبراني.(١٥٢)

وفي أواخر شهر آذار / مارس قدم باحثون في اللجنة الدولية للصليب الأحمر مقترحاً بحظر الهجمات السيبرانية ضد المرافق الطبية أثناء انتشار الوباء، وبتاريخ ٢٢/أيار/ ٢٠٢٠ نظمت ورشة عمل افتراضية في جامعة أكسفورد برعاية مشتركة من الحكومة اليابانية ومعهد أكسفورد للأخلاق

(١٤٩) تشمل المبادئ الدولية المنظمة لسير العمليات العدائية كما يأتي:
١- مبدأ حق أطراف النزاع في اختيار وسائل وطرائق القتال ليس حقاً مطلقاً.
٢- مبدأ وجوب التمييز بين المدنيين والمقاتلين.
٣- مبدأ الضرورة العسكرية.
٤- مبدأ التناسب في استخدام القوة.
٥- شرط مارتينز.
(١٥٠) المادة (١٠/٥٢) من البروتوكول الإضافي الأول لعام ١٩٧٧
(١٥١) المادة (٤/٢/٨/أولاً) من نظام روما الأساسي لعام ١٩٩٨، كذلك المادة (٥٢)، من البروتوكول الأضافى الأول لعام ١٩٧٧
(١٥٢) المادة (٣/٣٥) بروتوكول، المادة (٢/٨/ب/رابعاً) من نظام روما الأساسي لعام ١٩٩٨

والقانون والنزاع المسلح في مدرسة (خلافاتنيك) الحكومية ومايكروسوفت لغرض مناقشة موضوع الهجمات السيبرانية على القطاعات الصحية، كما اقترحت استونيا بصفتها رئيساً للأمم المتحدة آنذاك، التخطيط لاجتماع المجلس لمناقشة سلوك الدولة المسؤول في الفضاء السيبراني ومناقشة الحماية القانونية الممنوحة للرعاية الصحية.

وقد أكد بيان أوكسفورد على ضرورة حماية القطاعات الصحية من الهجمات السيبرانية أثناء فترة الجائحة، وإبعاد هذه القطاعات عن النزاعات السيبرانية، كما أيد البيان دعوة اللجنة الدولية للصليب الأحمر لحماية المرافق الطبية والخدمات الطبية من أي نوع من أنواع الاستهداف السيبراني، وأن هذه الهجمات لا تحدث في فراغ معياري أو منطقة خالية من القانون.

وللتفصيل أكثر في موضوع إسناد المسؤولية إلى الدول أو الأفراد سنعمل على إدراج بعض السوابق القضائية والتي تمثل أساساً لذلك وكما يأتي:[١٥٣]

١- قضية الانشطة العسكرية وشبه العسكرية عام ١٩٨٦

في قضية الانشطة العسكرية أو شبه العسكرية في أو ضد نيكارغوا جاء في رأي محكمة العدل الدولية أنه"...أن معيار المسؤولية الدولية عن التصرفات الخاطئة، إنما يتجلى في قدرة الدولة للسيطرة على القوات شبه العسكرية...".

ومن خلال رأي المحكمة نجد أن المحكمة ذهبت إلى تكييف التدخل بقولها "وبما أنه ثبت للمحكمة دور الولايات المتحدة في تدريب وتسليح المجموعات المسلحة (الكونترا) في نيكاراغوا وتجهيزها بوسائل اتصال مفتوحة".

وقضت المحكمة بمسؤولية الولايات المتحدة عن التدخل بالشؤون الداخلية لدولة نيكاراغوا وتحمل تبعات التصرفات المخالفة للقانون الدولي العام.[١٥٤]

٢- قضية المدعي العام ضد تاديتش(Tadic) ، المحكمة الجنائية ليوغسلافيا السابقة

في هذه القضية تطرقت المحكمة الجنائية الدولية ليوغسلافيا السابقة إلى موضوع مسؤولية الدولة عن الانتهاكات التي ترتكبها الجماعات المسلحة المدعومة من قبلها، وفي هذه القضية نجد أن اهتمام المحكمة كان منصباً على معيار آخر وهو معيار السيطرة الكاملة فجاء في حكم المحكمة أنه".... كان للدولة دور في التنظيم والتنسيق، فضلاً عن تزويد المجموعة المسلحة بالدعم، ما يعني

(١٥٣) أحمد عبيس نعمة الفتلاوى، د/ أزهر عبد الأمير الفتلاوى، المسؤولية الناشئة عن استخدام وسائل القتال الفتاكة في نشر الأوبئة "الهجمات السيبرانية مقابل جائحة كورونا"، مجلة الحقوق، العدد ٤١، ص٧٤

(١٥٤) أحمد عبيس نعمة الفتلاوى، د/ أزهر عبد الأمير الفتلاوى، المسؤولية الناشئة عن استخدام وسائل القتال الفتاكة في نشر الأوبئة "الهجمات السيبرانية مقابل جائحة كورونا"، المرجع السابق، ص٧٥

(ISSN: ٢٣٥٦ - ٩٤٩٢)

أن لها السيطرة الكاملة عليها، وما يصدر عن المجموعات المسلحة، يعني أنه صادر عن الدولة نفسها".

٣- قضية البوسنة والهرسك ضد صربيا

قامت البوسنة برفع دعوى أمام محكمة العدل الدولية في قضية الإبادة الجماعية في جمهورية البوسنة عام ٢٠٠٧، بحجة أن صربيا دعمت قوات حرب البوسنة عند ارتكابها جريمة الإبادة الجماعية في البوسنة، وبعد إجراءات التحقيق والبحث من قبل المحكمة جاء قرارها بعدم وجود أية صلة بين صربيا وبين قوات صرب البوسنة وبذلك انتفت الحاجة إلى إسناد المسؤولية إلى صربيا.

من خلال قرار المحكمة أعلاه نجد أن المحكمة استبعدت معيار السيطرة الكاملة باعتبار أن قوات صرب البوسنة والجيش الصربي لا يعدان جهازين تابعين إلى جمهورية صربيا لا واقعاً ولا قانوناً، وأصدرت المحكمة قرارها بعد أن تحققت من عدم وجود العلاقة المطلوبة بين قوات صرب البوسنة والتي حددتها المادة (٨) من مشروع مسؤولية الدول السابق ذكرها.

ثم عادت المحكمة إلى إدانة صربيا بسبب انتهاك التزامها بمنع الإبادة الجماعية، استناداً إلى منع الإبادة الجماعية، كان ذلك في ضوء الإبادة التي، ارتكبتها القوات الصربية في منطقة (سربيبرنتشا) في تموز من عام ١٩٩٥.(١٥٥)

وأشارت المحكمة أن صربيا لم تمتثل لاتفاقية منع الإبادة الجماعية بعدم اتخاذ التدابير التحفظية التي أقرتها المحكمة في ٨ /نيسان غام ١٩٩٣ كون هذه التدابير هي من صلاحياتها.

ويرى: انطونيو كاسييزي أن تبني محكمة العدل الدولية لمعيار السيطرة الفعالة في قضية الإبادة الجماعية في البوسنة لعام ٢٠٠٧ أنه غير واقعي بقوله "... أنه معيار غير واقعي في الإثبات".(١٥٦)

ويذهب (ماركوف)، و(كرامر) وفي سياق مسؤولية الدول عن الهجمات السيبرانية إلى أنه "يمكن أن يكون معيار السيطرة الفعالة مجدياً في تحديد جزء من المسؤولية الدولية لا كلها ويعتمد ذلك في تبني اتفاقية دولية تشارك فيها كل من الولايات المتحدة، روسيا لتحديد المسؤولية الدولية الناشئة عن الهجمات السيبرانية".

أما القاضي (ستين جولبيرج) فيرى "إن عدم وجود محاكم دولية أو جنائية مختصة بملاحقة المسؤولين عن ارتكاب الجرائم الخطرة على المستوى العالمي يعني أن عدداً غير قليل من منفذي الهجمات السيبرانية سيكونون بمنأى عن العقاب".

---

(١٥٥) أحمد عبيس نعمة الفتلاوى، د/ أزهر عبد الأمير الفتلاوى، المسؤولية الناشئة عن استخدام وسائل القتال الفتاكة في نشر الأوبئة "الهجمات السيبرانية مقابل جائحة كورونا"، المرجع السابق، ص٧٥

(١٥٦) صادق باقر إبراهيم العلوي، المسؤولية الدولية الناشئة عن دعم المجموعات المسلحة، دراسة تحليلية، منشورات زين الحقوقية، لبنان، بيروت، ط ١، ٢٠١٨، ص ٩١

ومن خلال كل ما تقدم نجد أن مسألة إسناد المسؤولية الدولية عن الهجمات السيبرانية في سياق القواعد الأولية للقانون الدولي العام قد لا تحقق أهدافها؛ والسبب هو في صعوبة تحديد هوية المهاجم السيبراني، وبالتالي تزداد صعوبة مهمة الدولة المدعية في إثبات هوية المهاجم السيبراني، والعمل على اكمال ملاحقته قضائياً، وهذا بحد ذاتها يعد عائقاً أمام تحقيق أهداف القانون الدولي بكونه معنياً بتنظيم قواعد المسؤولية وتحريكها ضد مرتكبي انتهاكات القانون الدولي العام من جهة والقانون الدولي الانساني كقواعد ثانوية من جهة اخرى، وهذا يستتبع ايضاً تعقد اجراءات الملاحقة بناءً على المسؤولية الجنائية الفردية.(١٥٧)

وفي إطار اسناد المسؤولية عن الهجمات السيبرانية نجد أن البروتوكول الإضافي الأول قد بين الفئات التي يجب أن لا تستهدف بالهجمات من خلال المواد (٢/٥١، ١/٥٢، ٤/٥١، ٤٩)، أما المادة (١٠/٥٢) من البروتوكول الاضافي الاول لعام ١٩٧٧ وصفت العين المدنية أنها ما لا يعد هدفاً عسكرياً.(١٥٨)

أما المادة (٢/٥١) فقد حظرت الهجوم على الاشخاص المدنيين والاعيان المدنية بشكل مطلق، ما دامت غير مشاركة مباشرة في العمليات العدائية.

كما بين البروتوكول الإضافي الأول أنه إذا كان الهجوم يستهدف إحداث أذى أو موت أو تلف أو دمار أو كان يتوقع ذلك من الهجوم فإن الأمر يفسر لصالح المدني ويكون الهجوم محظوراً، والحال ذاته ينطبق على الهجمات السيبرانية.(١٥٩)

وفي قرار مجلس الامن (٢٢٨٦) لعام ٢٠١٦ أكد على حث أطراف النزاع المسلح لكفالة تمكين العاملين في المجال الإنساني والخدمات الطبية بشكل كامل وآمن وفوري دون أي عوائق للمرضى والاشخاص المحتاجين للمساعدة.

وفي السياق المتقدم، نجد أيضاً إدانة أعمال العنف والهجمات وأي تهديدات يمكن أن توجه ضد الموظفين في القطاع الصحي، الذين يعملون في المجال الإنساني وبالتحديد في المهام الطبية، كذلك وسائل نقلهم ومعداتهم، كما حث القرار أطراف النزاع على عدم استهداف المستشفيات والقطاعات الصحية وعده انتهاكا للقانون الدولي الإنساني الدولي.

ومثلما تتسبب الهجمات المحتملة على مفاعل نووي بدمار كبير وإطلاق الإشعاعات، فإن استخدام الهجمات السيبرانية لاستهداف البنية التحتية وقطاعات صحية تحتوي على فيروسات قاتلة

(١٥٧) د/ أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية، دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، منشورات زين الحقوقية، بيروت، لبنان، ط ١، سنة ٢٠١٨، ص ٣٤٥
(١٥٨) المواد (٢/٥١، ١/٥٢، ٤/٥١، ٤٩، ٥٢) من البروتوكول الإضافي الأول
(١٥٩) المادة (٤/٢/٨/أولاً) من نظام روما الأساسي لعام ١٩٩٨، كذلك المادة (٥٢)، من البروتوكول الأضافى الأول لعام ١٩٧٧

(ISSN: ٢٣٥٦ - ٩٤٩٢)

قد يؤدي إلى انتشار تلك الفيروسات وبالتالي إلحاق الضرر بأرواح المدنيين، والإضرار بالبيئة بسبب الهجوم السيبراني،(١٦٠) ففي أواخر شهر آذار من عام ٢٠٢٠ قدم باحثون في اللجنة الدولية للصليب الأحمر مقترحاً بحظر الهجمات السيبرانية ضد المرافق الطبية أثناء انتشار الوباء.

إن اثبات المسؤولية الدولية بالاستناد إلى معياري السيطرة الفعالة والسيطرة الكاملة إذا ما أسهمت الدول في دعم هجمات قامت بها مجموعات مسلحة بالطرق التقليدية سيكون اعقد إثباتاً فيما لو كان الأمر متعلقاً بالهجمات السيبرانية والتي تعد غير مادية، ولا يمكن اثباتها بسهولة لأنها تتخذ من الفضاء السيبراني مجالاً لها وهذا بحد ذاته يعد عقبة أمام تنظيم إسناد المسؤولية الدولية، وهذا يؤكد الحاجة إلى وضع اتفاقية دولية تحدد قواعد صريحة تحظر تقديم الدعم للمجموعات المسلحة، لتكون الاتفاقية سبيلاً للجوء إلى المحاكم الجنائية الدولية في ملاحقة مرتكبي الانتهاكات الجسيمة من خلال الهجمات السيبرانية.(١٦١)

ومن الجدير بالذكر أن الأساس الذي تقوم علىه المسؤولية الجنائية الدولية هو افتراض ارتكاب الأشخاص الفعل الضار أي أن الشخص لا يكون مسؤولاً عن أي أفعال لم يشارك في ارتكابها أو حتى لم يكن له دور ثانوي فىها.

وتأسيساً على ما تقدم فإن استهداف القطاعات الطبية والعلمية التي تحوي الفيروسات الفتاكة والتي تعتمد على شبكات الحاسوب في تخزين تلك الفيروسات بالهجمات السيبرانية بالشكل الذي يؤدي إلى فتح مخازن الفيروسات وانتشارها بأية طريقة للانتشار سيؤدي حتماً إلى أن تتحمل الجهة المستخدمة للهجمات السيبرانية سواءً كانت دولة أم أفراد المسؤولية عن الأضرار التي يحدثها انتشار تلك الفايروسات.(١٦٢)

المطلب الخامس

المسؤولية وفقاً للقانون الدولي لحقوق الانسان

تعد معاهدات حقوق الإنسان من أهم مصادر القانون الدولي لحقوق الإنسان، عامة كانت أم خاصة ويأتي إلزام قواعد هذه الاتفاقيات من إرادة الدول الأطراف بالتزامها ببنود تلك الاتفاقيات وعليه فإن أي انتهاك لها يوجب مساءلة الدولة المنتهكة.

(١٦٠) المادة (٣/٣٥) بروتوكول، المادة (٢/٨/ب/رابعاً) من نظام روما
(١٦١) د/ أحمد عبيس نعمة الفتلاوى، د/ أزهر عبد الأمير الفتلاوى، المسؤولية الناشئة عن استخدام وسائل القتال الفتاكة في نشر الأوبئة "الهجمات السيبرانية مقابل جائحة كورونا"، مجلة الحقوق، العدد ٤١، ص٧٧
(١٦٢) د/ أحمد عبيس نعمة الفتلاوى، د/ أزهر عبد الأمير الفتلاوى، المسؤولية الناشئة عن استخدام وسائل القتال الفتاكة في نشر الأوبئة، مرجع سابق، ص٧٨

وتؤدي قواعد القانون الدولي لحقوق الإنسان دوراً مهماً في توفير الحماية لبني البشر من خلال وضع حدود لا يمكن تجاوزها سلباً أم إيجاباً، لغرض تحقيق هدف واحد وهو حماية الإنسان وعدم الاعتداء على حياته أو كرامته، والعمل على صيانة حقوقه بالشكل الذي يوفر العيش الكريم.

لقد واجه العالم في هذه الفترة أزمة صحية غير مسبوقة تتمثل في جائحة كورونا، فمنذ فترة طويلة لم تتعرض البشرية الى اختبار صحي عالمي بهذه الحدة، وهذا بحد ذاته يتطلب استجابة على مختلف المستويات السياسية والاقتصادية والصحية والاجتماعية في سبيل إنقاذ حياة ملايين من البشر، ولأن الحق في الحياة هو أحد الحقوق المهمة التي قد تستهدفها الهجمات السيبرانية، إذ يعد من الحقوق التي ترتبط بالحريات والملازمة لكل فرد في المجتمع ومن غير الوارد الاستغناء عنه.

ويتمتع الحق في الحياة بطابع مطلق، أي أنه لم ينشأ بقانون وضعي، لأنه لصيق بالإنسان وجوهر نشأته، ويعد الحق في الحياة أحد أهم الحقوق المدنية التي أكدت عليها الشرائع السماوية والإعلانات الدولية ومنها الإعلان العالمي لحقوق الإنسان والعهد الدولي للحقوق المدنية والسياسية.

إن في الحق الحياة يعد أساساً لحقوق الإنسان الأخرى، لان وجود الإنسان مرتبطاً بها لكي يتمتع ويمارس الحقوق الأخرى، وما يميزه هو أن القانون الدولي لحقوق الإنسان عد خصيصة عدم القابلية للتعليق أو التوقف في أي ظرف تمر به الدولة تمييز للحق في الحياة عن غيره ولا يمكن حرمانه منه.

إن حماية الحق في الحياة هو واجب يقع على عاتق جميع الدول في سبيل توفير حماية الإنسان، وذلك من خلال معالجة التهديدات المباشرة لهذا الحق، وفي القطاعات الصحية يبذل المختصون جهوداً كبيرة في سبيل الوصول إلى نقطة المحافظة على الحق في الحياة، ولأن الحق في الصحة يرتبط ارتباطاً وثيقاً بالحق في الحياة سنتناولهما تباعاً في الصكوك والاتفاقيات الدولية.(١٦٣)

وفي إطار البحث حول الهجمات السيبرانية وتأثيرها على القطاعات الصحية والعلمية في انتهاك الحق في الصحة والحق في الحياة، نجد أن جميع الشرائع السماوية والتشريعات والأعراف تحظر انتهاك الحق في الحياة، فهي تسعى دائماً إلى توفير الحماية لهذا الحق وغيره من حقوق الإنسان الأخرى. وقد عد المفاوضون في العهد الدولي الخاص بالحقوق المدنية والسياسية أن الحق في الحياة يقف حائلاً أمام أي حالة تؤدي إلى فقدان الشخص لحياته، وكانوا يعدونه ذو معنى أخلاقي وقانوني، فهو يشمل التصرفات غير المشروعة والتي تبتعد عن تحقيق العدالة.

وبالعودة إلى الإعلانات والاتفاقيات الدولية نجد أن الحق في الصحة والحق في الحياة قد أخذا حيزاً مناسباً من النصوص الدولية وسنتناولها تباعاً وكما يأتي:

(١٦٣) المادة (١/٢) من الإتفاقية الأوروبية لحقوق الإنسان لعام ١٩٥٠، والمادة (١/٤) من الإتفاقية الامريكية لحقوق الإنسان لعام ١٩٦٩

(ISSN: ٢٣٥٦ - ٩٤٩٢)

أولاً: الإعلان العالمي لحقوق الإنسان لعام ١٩٤٨

بتاريخ العاشر من كانون الأول من عام ١٩٤٨ صدور الإعلان العالمي لحقوق الإنسان وأكدت المادة الثالثة منه على حماية الحق في الحياة، ولم تؤيد المادة أعلاه أي تفسير يؤدي إلى السماح بانتهاك الحق في الحياة، وهذا بحد ذاته دليل على أن المجتمع الدولي يشترك في الرأي القانوني الداعم لترسيخ الحق في الحياة وحمايته.(١٦٤)

وفي إطار الحق في الصحة نصت المادة (٢٥) من الإعلان العالمي لحقوق الإنسان لعام ١٩٤٨ على أنه ١- لكل شخص حق في مستوى معيشة يكفي لضمان الصحة والرفاهية له ولأسرته، وخاصة على صعيد المأكل والملبس والعناية الطبية وصعيد الخدمات الاجتماعية الضرورية، وله الحق فيما يأمن بع العوائل في حالات البطالة أو المرض أو العجز أو الترمل أو الشيخوخة أو غير ذلك من الظروف الخارجية عن إرادته والتي تفقده أسباب عيشه، من خلال النص أعلاه نجد أن المادة (٢٥)على حق الأشخاص بالتمتع بصحته ورفاهية اسرته، من ناحية العناية الطبية والخدمات الاجتماعية.(١٦٥)

ومن الجدير بالإشارة أن الاعلان العالمي لحقوق الإنسان وغيره من الإعلانات الدولية لا تملك تلك القوة الملزمة التي تتمتع بها الاتفاقيات الدولية بالمعنى الدقيق، كما أن أي إلزام لهذه الإعلانات لابد أن يكون عن طريق اتفاق بين أعضاء الأمم المتحدة لعقد اتفاقيات تخص حقوق الإنسان، كما أن المادة (٢٢) من الإعلان العالمي لحقوق الإنسان بينت أن من سبل الحفاظ على حقوق الإنسان هو تنظيمها في الدساتير الداخلية للدول.(١٦٦)

ومع ما تقدم ذكره، جرت الممارسة الدولية ولا سيما في الاجتهادات القضائية الدولية والوطنية، على عد القواعد المتضمنة في الاعلان العالمي، على انها قواعد عرفية لا يمكن التنازل عنها أو انتهاكها، إذ يظل الإعلان في كثير من الأحيان المرجع الرئيسي الذي يجب الاحتجاج به لشجب انتهاكات حقوق الإنسان.

وفي هذا الشأن اعتنق الاتحاد الأوروبي تمامًا أهمية الإعلان، واستخدمه لوضع المعايير في تشريعاته الداخلية والاتفاقيات الدولية وبالذات الاتفاقية الاوربية لحقوق الانسان لعام ١٩٥٠، وتوجيه سياسته الخارجية، وبالخصوص الحقوق التي لا خلاف عليها دولياً ومنها الحق في الصحة.

(١٦٤) المادة الثالثة من الإعلان العالمي لحقوق الإنسان لعام ١٩٤٨ على أنه "لكل فرد الحق في الحياة والحرية وسلامة شخصه"

(١٦٥) المادة (٢٥) من الإعلان العالمي لحقوق الإنسان لعام ١٩٤٨

(١٦٦) المادة (٢٢) من الإعلان العالمي لحقوق الإنسان

ثانياً: العهد الدولي للحقوق المدنية والسياسية لعام ١٩٦٦

جاءت المادة ٦/أولاً من العهد الدولي لتؤكد على الحق في الحياة وأهميته وأنه أحد الحقوق الأساسية التي يتمتع بها الإنسان ومن الواجب حمايته وعدم الحرمان منه بأي شكل من أشكال.(١٦٧)

كما أكدت التقارير التي قدمتها الدول الأطراف في الأمم المتحدة للجمعية العامة أن الحق في الحياة يعد أسمى حقوق الإنسان وأهمها وأنه لا يمكن أن يقييد بأي حال من الاحوال، وأن نص المادة أعلاه أشار إلى الحماية من الحرمان التعسفي للحق في الحياة، ما دعى الدول الأطراف لاتخاذ التدابر الممكنة في سبيل منع الحرمان من الحياة، ومنع حالات القتل التعسفي التي تتبعها الأجهزة التابعة للدول، وهذا يتم من خلال إصدار قوانين داخلية تحد من أي ظرف يمكن أن يكون سبباً في الحرمان من الحق في الحياة.

وقد أبدت اللجنة المعنية بحقوق الإنسان رأيها في أن يتم تفسير الحق في الحياة بمعناه الواسع وليس كما جاء في المادة السادسة من العهد الدولي المتعلق بالحقوق المدنية والسياسية، كما أكدت اللجنة في تعليقها عن ضرورة أن تعمل الدول على تفادي الاعمال التي تؤدي الى خسائر بشرية كبيرة.(١٦٨)

في نص المادة الثانية من العهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية أكدت على أن تسلك الدول الأطراف ما استطاعت من طرق لضمان تمتع الافراد بالحقوق التي بينها العهد الدولي وأبرزها هو تشريع القوانين الداخلية التي تضمن ذلك.(١٦٩)

وفي نفس السياق جاءت الفقرة الثانية من المادة الثانية من العهد الدولي الخاص بالحقوق المدنية والسياسية لعام ١٩٦٦.(١٧٠)

من خلال ما تقدم نجد أن الدول ملزمة بتشريع قوانين، تكون أكثر مواءمة مع الاتفاقيات الدولية والعمل على إلغاء أو تعديل النصوص الوطنية المخالفة لها.

والجدير بالذكر أن الميثاق الأفريقي لحقوق الإنسان والشعوب لعام ١٩٨١ تطرق أيضاً الى مسألة حماية الحق في الحياة وضرورة اتخاذ الدول الأطراف إجراءات تشريعية لكفالة واحترام حقوق الإنسان.(١٧١)

---

(١٦٧) نصت المادة (١/٦) من العهد الدولي للحقوق المدنية والسياسية لعام ١٩٦٦ على أنه "الحق في الحياة حق ملازم لكل إنسان وعلى القانون أن يحمي هذا الحق ولا يجوز حرمان أحد من حياته تعسفاً".

(١٦٨) تعليق اللجنة المعنية بحقوق الإنسان رقم (٣٦) في شهر تشرين الثاني لعام ٢٠١٨، ص١٨٠

(١٦٩) نصت المادة (٢) من العهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية على أنه "تتعهد كل دولة طرف في هذا العهد بأن تتخذ بمفردها أو عن طريق المساعدة والتعاون الدوليين ولاسيما على الصعيدين الاقتصادي والتقني وبأقصى ما تسمح به مواردها المتاحة ما يلزم من خطوات لضمان التمتع الفعلي التدريجي بالحقوق المعترف بها في هذا العهد سالكة الى ذلك جميع السبل المناسبة وخصوصاً سبيل اعتماد تدابير تشريعية".

(١٧٠) المادة (٢/٢) من العهد الدولي الخاص بالحقوق المدنية والسياسية لعام ١٩٦٦

(ISSN: ٢٣٥٦ - ٩٤٩٢)

أما بالنسبة للحق في الصحة فقد فسرت لجنة الحقوق الاقتصادية والاجتماعية والثقافية في المجلس الاقتصادي والاجتماعي للأمم المتحدة الحق في الرعاية الصحية بناءً على التعريف الذي جاءت به الفقرة الأولى من المادة الثانية عشرة من العهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية لعام ١٩٦٦ أنه "حق يشمل المقومات الاساسية للصحة كالحصول على الماء الصالح للشرب والتداوي المناسب، وتوفير الغذاء والأمن ولا يقتصر على تقديم الرعاية الصحية في وقتها فقط، أضف إلى ذلك مسألة التوعية الصحية في الإطار المجتمعي".

أما الفقرة الثانية من المادة أعلاه فقد أكدت على واجب الدول الاطراف في اتخاذ عدد من التدابير في سبيل تأمين ممارسة الحق في الرعاية الصحية بشكل كامل.

وفي إطار موضوع بحثنا حول الهجمات السيبرانية نجد أنه من الضروري بيان فرضيات استهداف القطاعات الصحية، وعلى النحو الآتي:

لا يمكن للهجمات السيبرانية ان تتسبب بنشر فايروسات فتاكة كوسيلة نقل، بقدر ما انها تؤدي غايات محددة تتسبب إما بجانب سلبي قائم على منع تطوير برامج لمكافحة الفايروسات ومنها كورونا على سبيل المثال، أو من خلال تصرف ايجابي وهو التلاعب ببيانات مختبرية تحتفظ بها المؤسسات الصحية لأجل التوصل إلى لقاحات.

إن مهاجمة مستشفى عن طريق السيبرانية وتعطيل برامج الطوارئ للحالات الحرجة، سيعني المساعدة بنشر الفيروس في تلك المستشفى ومن ثم انتقال العدوى سريعا في المنطقة أو المدينة بشكل متسارع.

إن مهاجمة بيانات المرضى والتلاعب بمحتواها، سيعني عدم القدرة على الاستجابة الواقعية لكل مريض ومن ثم وقوع سلسلة من الاصابات الفتاكة المؤدية إلى ارتفاع بنسب الوفيات بين المرضى.[١٧٢]

إن مهاجمة المختبرات العالمية المعنية بتطوير أو انتاج لقاحات ضد فايروس كورونا، سيعني، التشكيك بفاعلية هذه اللقاحات من جهة، أو بإنتاج لقاحات مزيفة لتطرح إلى المستفيدين منها بواسطة مافيات القطاع الصحي العالمي، وهذا ما حصل بالفعل، إذ اعلنت كل من شركة فايزر وبيونتك في العاشر من شهر ديسمبر ٢٠٢٠، عن تعرضهما إلى هجمات سيبرانية ادت إلى سرقة بيانات مهمة

(١٧١) د/ أحمد عبيس نعمة الفتلاوى، د/ أزهر عبد الأمير الفتلاوى، المسؤولية الناشئة عن استخدام وسائل القتال الفتاكة في نشر الأوبئة "الهجمات السيبرانية مقابل جائحة كورونا"، مجلة الحقوق، العدد ٤١، ص٨١

(١٧٢) د/ أحمد عبيس نعمة الفتلاوى، د/ أزهر عبد الأمير الفتلاوى، المسؤولية الناشئة عن استخدام وسائل القتال الفتاكة في نشر الأوبئة "الهجمات السيبرانية مقابل جائحة كورونا"، مجلة الحقوق، العدد ٤١، ص٨٢

حول اللقاحات التي توصلت إليهما الشركتان، ما استدعى تحركا من وكالة الادوية الأوربية للتحقيق بهذا الانتهاك الخطير.(١٧٣)

المبحث الخامس

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 هناك 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.(١٧٤) وسوف نبين ذلك فيما يلي:

(١٧٣) د/ أحمد عبيس نعمة الفتلاوى، د/ أزهر عبد الأمير الفتلاوى، المسؤولية الناشئة عن استخدام وسائل القتال الفتاكة في نشر الأوبئة "الهجمات السيبرانية مقابل جائحة كورونا"، مجلة الحقوق، العدد ٤١، ص٨٣

(١٧٤) نور أمير الموصلى، الهجمات السيبرانية في ضوء القانون الدولى الإنسانى، رسالة ماجستير في القانون الدولى الإنسانى، ٢٠٢١، ص٢١

(ISSN: ٢٣٥٦ - ٩٤٩٢)

أولاً: الجمعية العامة

١- القرارين ٦٣ / ٥٥ و١٢١ / ٥٦ اللذين يضعان الإطار القانوني بشأن " مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية".

٢- القرار ٢٣٩ / ٥٧ المتعلق ب "إنشاء ثقافة أمنية عالمية للفضاء الحاسوبي".

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

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

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

ويبدو أن الأمم المتحدة مستعدة للقيام بدور ريادي، فقد أعربت الدول الأعضاء للأمم المتحدة، في الاستعراض السادس للاستراتيجية العالمية لمكافحة الإرهاب في القرار ٢٨٤ / ٧٢ الصادر عن الجمعية العامة، عن قلقها إزاء تزايد استخدام الإرهابيين تكنولوجيا المعلومات والاتصالات، وبخاصة شبكة الإنترنت وغيرها من الوسائط لارتكاب الأعمال الإرهابية أو التحريض عليها أو التجنيد لها أو تمويلها أو التخطيط لها.[١٧٥]

ثانياً: مجلس الأمن

١- القرار ٢٣٤١ (٢٠١٧)، 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 من 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)، الذي يحث فيه الدول الأعضاء على "العمل بصورة تعاونية لمن الإرهابيين من حيازة الأسلحة، من خلال تكنولوجيات المعلومات والاتصالات، مع احترام حقوق الإنسان والحريات الأساسية والامتثال للالتزامات بموجب القانون الدولي".[١٧٦]

(١٧٥) نور أمير الموصلى، الهجمات السيبرانية في ضوء القانون الدولى الإنسانى، رسالة ماجستير في القانون الدولى الإنسانى، ٢٠٢١، ص٢٢

(١٧٦) نور أمير الموصلى، الهجمات السيبرانية في ضوء القانون الدولى الإنسانى، رسالة ماجستير في القانون الدولى الإنسانى، ٢٠٢١، ص٢٣

ثالثاً: مكتب مكافحة الإرهاب

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 من إساءة استعمال الإرهابيين والمتطرفين العنيفين التطورات التكنولوجية، والتصدي لخطر الهجمات السيبرانية التي تشنها الجهات الفاعلة الإرهابية على البنية التحتية الحيوية.

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

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 نوحد صفوفنا الآن، وعلينا أن نفعل ذلك بسرعة، للتخفيف من هذا التهديد وضمان أن تظل التقنيات الجديدة قوة مسخرة للخير وليس قوة للشر".[١٧٧]

الفرع الثانى

حلف شمال الأطلسي (الناتو)

أدت تداعيات الهجمات السيبرانية التي اسهتدفت البنية التحتية الرقمية لإستونيا عام ٢٠٠٧، أيضاً 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، ويطلب من مركز الدفاع الإلكتروني التعاوني للتميز، قامت مجموعة من الخبراء والباحثين القانونيين تتقييم إمكانية تطبيق المبادئ القانونية على الهجمات السيبرانية،[١٧٨] وتم تتويج هذه الجهود بنشر دليل يعرف باسم "دليل تالين" 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

(١٧٧) نور أمير الموصلى، الهجمات السيبرانية في ضوء القانون الدولى الإنسانى، رسالة ماجستير في القانون الدولى الإنسانى، ٢٠٢١، ص٢٣

(١٧٨) بهاء عدنان السعيرى، عماد عيد خضير، انتقال التهديدات من الواقع إلى العالم الافتراضي، مجلة جامعة بابل للعلوم الإنسانية، المجلد ٢٧، العدد ٤، ٢٠١٩، ص٤٨٣

(ISSN: ٢٣٥٦ - ٩٤٩٢)

حق الدفاع عن النفس، الهجمات التي تحدث أثناء النزاع المسلح ويطبق عليها قواعد القانون الدولي الإنساني.

الإصدار الثاني عام ٢٠١٧ المعروف باسم (Tallinn ٢.٠) 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.(١٧٩)

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.(١٨٠)

ويوضح دليل تالين، القوانين الدولية التي يمكن تطبيقها على الحرب السيبرانية وهو يشتمل على كل من مبدأ حق اللجوء إلى الحرب أي القواعد الدولية التي تحكم وتنظم استخدام القوة من قبل الدول، ومبدأ سلوكيات الحرب 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 على مجموعة من الأفراد بتوجيه تلك المجموعة لتنفيذ هجمات سيبرانية ضد دولة أخرى. أما إذا كانت لا تملك إلا سيطرة فعالة على تلك المجموعة فعندئذ تلك الهجمات لا تبلغ مستوى النزاع المسلح الدولي.(١٨١)

الفرع الثالث

مجلس أوروبا

يعد مجلس أوروبا أول من اتخذ خطوات جدية ومباشرة لتنظيم جزء من الأمن السيبراني لأي منظمة دولية أو إقليمية أخرى، فقد قام بإنشاء اتفاقية تودابست المتعلقة بالجريمة السيبرانية وتعد هذه الاتفاقية أولى المعاهدات الدولية التي سعت إلى معالجة الجرائم السيبرانية من خلال تنسيق القوانين

(١٧٩) بشار خليل، ما هي الحرب السيبرانية؟ مستقبل مخيف للصراع الرقمى، مجلة المعلوماتية، العدد ١٥٤، الجمعية السورية للمعلوماتية، ٢٠٢٠

(١٨٠) إيهاب خليفة، القوة الإلكترونية كيف يمكن أن تدر الدول شئونها في عصر الانترنت، الولايات االمتحدة نموذجاً، الطبعة الأولى، القاهرة، ٢٠١٧، ص١٦٦

(١٨١) زهراء عماد محمد، المسئولية الدولية الناشئة عن الهجمات السيبرانية، جامعة الكوفة-كلية القانون، جمهورية العراق، إشراف الدكتور: أحمد عبيس نعمة الفتلاوي، ٢٠١٦ م، ص٢٠ وما بعدها

الوطنية، وزيادة التعاون تين الدول في محاربة الجرائم السيبرانية. وتمت في العاصمة المجرية بودابست في ١/٢٣/ ٢٠٠١، ويعد التوقيع على تلك المعاهدة الدولية الخطوة الأولى في مجال تكوين التضامن الدولي ضد تلك الجرائم التي تتم عبر شبكة الانترنت والاستخدام السيء لها.(١٨٢)

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)، 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.(١٨٣)

الفرع الرابع

مبادرات منظمة شنغهاي للتعاون (SCO)

اتخذت منظمة شنغهاي للتعاون، 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 بكاترينبورغ" وذلك في قمة منظمة شهنغهاي للتعاون التي عقدت في بكهاترينبورغ في روسيا وقد أظهرت المنظمة من خلاله التعاون والالتزام تهدف من الحروب والهجمات السيبرانية، 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".

(١٨٢) شيخة حسين الزهرانى، التعاون الدولى في مواجهة الهجوم السيبرانى، مجلة الشارقة للعلوم القانونية، المجلد ١٧، العدد١، جامعة الشارقة، كلية القانون، الإمارات العربية المتحدة، ٢٠٢٠، ص٧٥٣-٧٥٤

(١٨٣) نور أمير الموصلى، الهجمات السيبرانية في ضوء القانون الدولى الإنسانى، رسالة ماجستير في القانون الدولى الإنسانى، ٢٠٢١، ص٢٦

(ISSN: ٢٣٥٦ - ٩٤٩٢)

– عام ٢٠١١ تقدمت دول منظمة شنغهاي للتعاون بمشروع قرر للجمعية العامة للأمم المتحدة بشأن أمن المعلومات.

خلاصة القول، إن الجهود الدولية وإن كانت لا ترقى إلى مستوى تنظيمي دولي شامل، إلا أنها تظهر مدى الاهتمام الدولي المتزايد لوضع أطر تنظيمية للتصدي للهجمات السيبرانية، وبالإضافة لذلك تعد الخطوة الأولى نحو اتفاقية متعددة الأطراف تنظم استخدام هذه الهجمات وتقلل من آثارها الجسيمة على البشر.(١٨٤)

المطلب الثانى

جهود الدول لمواجهة التهديدات السيبرانية

سوف نتطرق في هذا المبحث إلى مختلف الجهود الوطنية والدولية من أجل مواجهة التهديدات السيبرانية، سواء في الجانب التقني أو الجانب القانوني.

الفرع الأول

الجهود الوطنية لتأمين الفضاء السيبرانى

أولاً: بناء الجيوش السيبرانية:

كان للتطور السريع للتكنولوجيا، خاصة الحرب السيبرانية تحدياً لمفاهيم الأمن القومي، حيث أصبحت قضية الدفاع عن البنية القومية للمعلومات ذات أهمية قصوى، وعليه سعت معظم الدول إلى تشكيل جيوش سيبرانية ورصدت ميزانيات ضخمة للتطوير في مجال الهجوم والدفاع والحماية.

وحسب الوكالة الروسية للاستشارات الأمنية زيكوريون فإن الولايات المتحدة تنفق أكثر على أمن الفضاء السيبرانى أكثر من أي بلد آخر، فوزارة الدفاع لديها ميزانية سنوية تبلغ ٧ مليارات دولار للأمن السيبرانى، وعدد الموظفين القراصنة يبلغ أكثر من ٩٠٠٠ موظف، وتنفق كل من الصين والمملكة المتحدة سنويا ١.٥ مليار دولار و٤٥٠ مليون دولار، على التوالي.(١٨٥)

وخصصت كوريا الشمالية نحو ٢٠ % من المى ا زنية العسكرية للأمن السيبراني. ويحتل الجيش السيبرانى الروسي المرتبة الخامسة في العالم، حيث تظهر التقارير أن قوات الأمن السيبرانى الروسية وصلت إلى ١٠٠٠ موظف، وتنفق وزارة الدفاع الروسية حوالي ٣٠٠ مليون دولار سنويا على مثل هذه الأنشطة.

(١٨٤) نور أمير الموصلى، الهجمات السيبرانية في ضوء القانون الدولى الإنسانى، رسالة ماجستير في القانون الدولى الإنسانى، ٢٠٢١، ص٢٦

(١٨٥) سليم دحمانى، أثر التهديدات السيبرانية على الأمن القومى، رسالة ماجستير، جامعة محمد بوضياف، كلية الحقوق والعلوم السياسية، ٢٠١٨، ص٥١

ثانياً: تشكيل هيئات وطنية للأمن السيبراني:

بما أن التهديدات السيبرانية لا تفرق بين مدني وعسكري، سعت الدول إلى تشكيل هيئات متخصصة في الأمن السيبرانى، تكون مهمتها:

- إعداد الإستراتيجية الوطنية للأمن السيبرانى، والإشراف على تنفيذها.
- وضع السياسات وآليات الحوكمة والإرشادات المتعلقة بالأمن السيبرانى وتعميمه.
- وضع أطر إدارة المخاطر المتعلقة بالأمن السيبرانى.
- وضع أطر الاستجابة للحوادث والاختراقات.
- وضع السياسات والمعايير الوطنية للتشفير.
- رفع مستوى الوعي بالأمن السيبراني.

كما يحدد الاتحاد الدولي للاتصالات ITU خمسة معايير لتصنيف مستوى الأمن السيبراني للدول وهي كالتالي: معاير تشريعية، تقنية، تنظيمية، بناء القدرات، ومعيار التعاون.(١٨٦)

ثالثاً: التشريعات الوطنية للأمن السيبراني

سن العديد من دول العالم قوانين لمواجهة التهديدات السيبرانية، بعد أن ظهر جلياً مدى سرعة انتشارها وفداحة الخسائر الناتجة عنها، وأجمع أغلب هذه القوانين أن هذه التهديدات ما هي إلا تعدي على الآخرين وعلى الممتلكات العامة والأنظمة بواسطة استخدام التقنية، وخصص جزء كبير من هذه القوانين عقوبات رادعة.

هذا إضافة إلى أن معظم الدول الأوروبية والآسيوية، والعربية، وغيرها من دول العالم التي أضافت إلى قانونها الجزائي ملحقاً خاصاً لمكافحة الجريمة السيبرانية (مثل الجزائر)، وهناك ثلاث دول عربية فقط سنت قوانين مستقلة لمكافحة الجرائم السيبرانية، هي السعودية وعمان والإمارات العربية المتحدة، هذه الأخيرة التي تعتبر رائدة في المنطقة العربية في إصدار تشريعات الأمن السيبراني، حيث صدر قانون مكافحة الجرائم السيبرلنية عام ٢٠١٢، ثم تم تعديله في ٢٠١٦، وقد دعم بمجموعة من السياسات التنظيمية والمعايير التقنية لتمكين مستخدمي الفضاء السيبراني ومقدمي الخدمات من الحصول على الظروف الأمنية اللازمة لحماية النظم الحساسة والبنية التحتية والبيانات، فضلا عن حماية المستخدمين.(١٨٧)

(١٨٦) سليم دحماني، أثر التهديدات السيبرانية على الأمن القومى، رسالة ماجستير، جامعة محمد بوضياف، كلية الحقوق والعلوم السياسية، ٢٠١٨، ص٥٢

(١٨٧) حسن بن أحمد الشهري،"الإرهاب الالكتروني – حرب الشبكات"، المجلة العربية الدولية للمعلوماتية، ٢٠١٥، ص ١٩

(ISSN: ٢٣٥٦ - ٩٤٩٢)

الفرع الثاني

الجهود الدولية من أجل فضاء سيبراني سلمي

أولاً: الحد من سباق التسلح السيبراني

يلعب التسليح أهمية استراتيجية في توازن القوى على المستوى العالمي، في ظل بيئة يسودها الشك وعدم اليقين وقابلية تدمير المصالح الاستراتيجية بسرعة الضوء، وهو ما يحمل خطورة عسكرة الفضاء السيبراني، وبتبني عديد الدول استراتيجية الحرب السيبرانية كحرب للمستقبل، واعتبار أن النصر في المعركة حليف من يقدر على شل القوة والتشويش على المعلومة، لقد بدأ سباق تسلح خطير لتطوير الأسلحة السيبرانية، كانت بداية ظهوره (يعتبر المختصون هذه الاسلحة السيبرانية بدائية) في الصراع الروسي–الاستوني، والروسي–الجورجي، والتطور البارز مع فيروس "ستاكسنت" الموجه ضد البرنامج النووي الإيراني والذي يتهم بتطويره كل من اسرائيل والولايات المتحدة.(١٨٨)

واتجهت الدول لتعزيز قدراتها السيبرانية سواء في مجال الدفاع والردع أو الهجوم، بالإضافة الى حماية بنيتها القومية للمعلومات، وذلك من خلال السعي إلى امتلاك التكنولوجيا وأنظمة الحماية، والعمل على تحقيق التفوق التقني. وعليه، فإن المشكلة في سباق التسلح السيبرانى تكمن في تحديد ماهية تلك الأسلحة، ومن ثم لا يصبح لدى المجتمع الدولي القدرة على التدخل لاحتواء التقدم في مجال تلك الأسلحة.

وحسب جوزيف. س ناي أنه يمكننا أن نتعلم من تاريخ العصر النووي. وفي حين أن التكنولوجيات السيبرانية والنووية تختلف اختلافًا كبيراً، فإن العملية التي يتعلم المجتمع من خلالها التعامل مع تكنولوجيا شديدة التعطيل، وفى المجال السيبرانى اقترحت روسيا في عام ١٩٩٩، معاهدة للأمم المتحدة لحظر الأسلحة الإلكترونية والمعلوماتية (بما في ذلك الدعاية).

قاومت الولايات المتحدة ما اعتبرته محاولة للحد من القدرات الأمريكية، ولا تزال تعتبر هذه المعاهدة عامة مضللة لا يمكن التحقق منها، وبدلاً من ذلك اتفقت الولايات المتحدة وروسيا و١٣ دولة أخرى على أن يعين الأمين العام للأمم المتحدة مجموعة من الخبراء الحكوميين التي اجتمعت أولاً في عام ٢٠٠٤.

وقد أسفرت تلك المجموعة في البداية عن نتائج هزيلة، ولكن بحلول جوان ٢٠١٥ أصدرت تقريراً أقرته مجموعة العشرين، يقضي بوضع معايير مقترحة لبناء الثقة.

(١٨٨) د/ عادل عبد الصادق، أسلحة الفضاء الالكتروني في ضوء القانون الدولي، سلسلة أوراق، العدد ٢٣، مكتبة الاسكندرية، ٢٠١٦، ص٦٤

وعلى الرغم من صعوبة عملية الرقابة والتفتيش على الاسلحة السيبرانية، فإن السعي نحو الحد من انتشار هذه الاسلحة، يتطلب وجود إطار دولي تتشارك فيه العديد من الدول والجماعات عبر العالم، إلى جانب وجود الإطار القانوني الدولي الذي يحدد الالتزامات والواجبات لجميع الفاعلين.

إن أي اتفاق من شأنه تنظيم الاستخدام العسكري للفضاء السيبرانى، يجب أن يعمل على منع نشر الأسلحة السيبرانية في وقت السلم، والسماح بالجهود الجماعية للدول أو المنظمات لتجنب التأثير على الاستخدام المدني للفضاء السيبرانى.(١٨٩)

ثانياً: قانون تالين

نظراً لصعوبة الحد من سباق التسلح السيبراني، من جهة، وقصور القانون الدولي في هذا المجال، نتيجة عدم وجود أي أساس قانوني ينظم اللجوء إلى الحروب السيبرانية، من جهة أخرى، تم إبرام صك قانوني عام ٢٠١٣ يدعى "دليل تالين Tallin manaul"، الذي أعده مجموعة من خبراء القانون الدولي بدعوة من حلف شمال الأطلسي NATO، قصد دراسة مدى إمكانية تطبيق قواعد القانون الدولي الإنساني على الحروب السيبرانية، وذلك إثر الهجوم السيبراني الشامل الذي شنته روسيا ضد إستونيا عام ٢٠٠٧.

ويحتوي دليل "تالين" على ٩٥ قاعدة، وتتمثل تحدياته الرئيسية في ضمان توجيه الهجمات ضد الأهداف العسكرية فقط، وتوخي الحذر لحقن دماء المدنيين والبنية التحتية الضرورية لحياتهم، وهذا نتيجة وجود فضاء سيبراني واحد تتقاسمه القوات المسلحة والجيوش السيبرانية مع باقي المستخدمين المدنيين.(١٩٠)

ويجيب دليل "تالين" على أهم النقاط الحساسة ذات الصلة بالحروب والهجمات السيبرانية التي تنفذها الدول، أو تلك التي تقوم بها جهات فاعلة من دون الدول، كمفهوم النزاع المسلح في إطار الحرب السيبرانية، وكذا مفهوم الجيوش السيبرانية وكيفية ادارة الحرب السيبرانية من خلال قواعد الاشتباك السيبرانى، وصفة المقاتل السيبرانى إضافة الى امكانية مراعاة القانون الدولي الانساني المعروفة كمبدأ التمييز، ومدى شرعية استهداف المقاتل السيبرانى بالوسائل العسكرية المادية كالطائرات العسكرية بدون طيار.

ويقصر دليل "تالين" الهجوم السيبرانية على أنه "عملية إلكترونية سواء هجومية أو دفاعية يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الإضرار بأعيان أو تدميرها"، لكن لم يتفق الخبراء حول

(١٨٩) سليم دحمانى، أثر التهديدات السيبرانية على الأمن القومى، رسالة ماجستير، جامعة محمد بوضياف، كلية الحقوق والعلوم السياسية، ٢٠١٨، ص٥٥-٥٦

(١٩٠) سعيد درويش،"ماهية الحرب الالكترونية في ضوء قواعد القانون الدولي"، حوليات جامعة الجزائر ١، العدد ٢٩، ص١١٩

(ISSN: ٢٣٥٦ - ٩٤٩٢)

"الضرر"، فهو يتوقف على كل بلد أن يقرر حجم الضرر الكافي لتبرير خوض الحرب، وهذا ما يعرف بنظرية اللجوء إلى الحرب (Jus ad bellum)، بحيث يشترط أن تكون مبررة وعادلة، لكي يمكن إضفاء صفة المشروعية عليها.(١٩١)

ثالثاً: الاتفاقيات الإقليمية والدولية لأمن الفضاء السيبراني

تنسجم الاتفاقيات الإقليمية مع متطلبات مواكبة سرعة تطور التهديدات السيبرانية، ويسجل في هذا المجال، عدد من المبادرات نذكر منها:

- في عام ٢٠٠٢، وضعت مجموعة بلدان الكومنولث قانوناً نموذجياً لمكافحة الجريمة. السيبرانية، إضافة إلى قانون الإثبات الرقمي.
- في عام ٢٠٠٩، بادرت المجموعة الاقتصادية لغرب إفريقيا، إلى إقرار توصية لمكافحة الجريمة السيبرانية، تشكل الإطار القانوني لعمل الدول الأعضاء.
- جاءت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات عام ٢٠١١، لتعزيز التعاون بين الدول العربية لمكافحة الجرائم السيبرانية والحفاظ على أمنها وسلامة مجتمعاتها.
- وتعتبر اتفاقية بودابست ٢٠٠١ (الاتفاقية الأوروبية لمكافحة الجريمة السيبرانية)، خطوة رائدة على مستوى التعاون بين الدول، وهي الوحيدة من حيث المدى وحجم الدول المنضمة إليها، دخلت حيز التنفيذ عام ٢٠٠٤، وتعتبر أداة إقليمية ملزمة لمكافحة الجريمة السيبرانية، عبر تحقيق الانسجام بين القوانين الوطنية، وقد شددت على ضرورة تحسين تقنيات التحقيق والبحث، وزيادة التعاون بين الدول.(١٩٢)

أما على المستوى الدولي، فقد لعبت هيئة الأمم المتحدة عبر القرارات الصادرة عنها التي تدعم الأمن والسلامة في الفضاء السيبرانى، وتوعية الوعي العالمي بالأمن السيبرانى دوراً في جذب انتباه الدول الأعضاء إلى أهمية التحديات السيبرانية. ومن أهم القرارات الصادرة عن الهيئة:

- قرار صادر سنة ١٩٩٠، حول قانون جرائم المعلوماتية.
- قرار صادر سنة ١٩٩١، حول مكافحة الاستخدام الجرمي لتقنيات المعلومات والاتصالات.
- عام ٢٠٠١، إنشاء "مجموعة الخبراء الحكومية GGE، بدأت عملها في ٢٠٠٤، لمناقشة الأخطار القائمة والمحتملة في مجال أمن المعلومات، والإجراءات الممكنة لوضع الأسس الدولية التي تهدف إلى تقوية أمن نظم الاتصالات والمعلومات العالمية.

(١٩١) سعيد درويش،"ماهية الحرب الالكترونية في ضوء قواعد القانون الدولي"، حوليات جامعة الجزائر ١، العدد ٢٩، ص١٣٣

(١٩٢) منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربى للبحوث القانونية والقضائية، بيروت، ٢٠١٧، ص١٠٣-١٠٤

- في العام ٢٠٠٣، صدر قرار خاص حول الأمن السيبراني، ركز على القدرة على مكافحة الجريمة السيبرانية.
- في العام ٢٠١٠، صدر قرار حول الأمن السيبراني، وملحق حول ضرورة أن تلجأ الدول، لمعرفة مدى تناسب أطرها التشريعية وقدرتها على مكافحة الجريمة السيبرانية.(١٩٣)

كما بذلت جهود عدة، من قبل مجموعات عمل متخصصة، بدعم من الاتحاد الدولي للاتصالات، لإقرار مجموعة من المعايير والقواعد، التي تضمن الاستخدام السلمي للمجال السيبراني.

لكن تبقى هذه الجهود، والمقررات والتوصيات، بالرغم من قيمتها على المستوى الدولي، غير كافية ولا فاعلة، نظراً لعدم الزاميتها القانونية، ولعدم إتاحتها إمكانية العقاب، هذا عدا عن الهوة الرقمية بين الدول، التي تزرع الشك بدل الثقة، خاصة مع سيطرة الولايات المتحدة الأمريكية على الانترنت.

الخاتمة

تعتبر الهجمات السيبرانية من أحدث أنواه الجرائم الأكترونية الدولية، وهي الجانب السلبي للتطور التكنولوجى حيث أنها جريمة معلوماتية ترتبط بالحاسب الآلى، وتعتبر الهجمات السيبرانية واحدة من أهم التحديات التي تواجه دول العالم في الوقت الحالي، لما لها من آثار وتداعيات على الأمن القومى للدول، إلى جانب بث الفوضى والرعب لدى شعوب دول العالم فهذه الجريمة عابرة للحدود لا تقف عن دولة معينة وهذا من أخطر آثار هذه الجريمة.

وقد عزز وجود ما يسمى بالهجمات السيرانية، ضعف طبيعة شبكة المعلومات وقابليتها للاختراق واعتماد العديد من الخدمات والبنية التحتية الأساسية على التكنولوجيا والشبكة المعلوماتية وهذا ما جعل المجتمع الدولي يواجه مخاطر جديدة مرتبطة بهذا التطور التكنولوجى.

وتزداد مخاطر 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 ، ولذلك فإن الآثار المحتمل لمثل هذه الهجمات ستكون على درجة عالية من الخطورة والجسامة مما قد يؤدي إلى وقوع حوادث كارثية مثل تصادم بين الطائرات وإطلاق المواد السامة من المصانع الكيمياوية أو إنقطاع تشغيل البنية التحتية مثل الشبكات إمدادات المياه والكهرباء ويكون المدنيين هم الضحايا الرئيسيين لمثل هذه الهجمات.

(١٩٣) د/ عادل عبد الصادق، الإرهاب الالكتروني والقوة في العلاقات الدولية: نمط جديد وتحديات مختلفة، مركز الدراسات السياسية والاستراتيجية، القاهرة، ٢٠٠٩، ص٣٣٤

(ISSN: ٢٣٥٦ - ٩٤٩٢)

تناولنا في البحث الجوانب القانونية المختلفة لموضوع الهجمات السيبرانية بداية من التعرف على ماهية الهجمات السيبرانية ومفهومها وخصائصها وطبيعتها وأنواعها. وميزنا بين الهجمات السيبرانية وغيرها من المصطلحات التي تتشابه معها. وبينا موقف القانون الدولى من الهجمات السيبرانية، ومحاولات مكافحتها والجهود الدولية المبذولة في سيبل ذلك، كما خصص المبحث الأخير لبحث مدى إمكانية الدفاع الشرعة ضد هذه الهجمات تبين لنا ان الهجمات السيبرانية تثير العديد من الإشكالات أولها أنها من الصعب أن تنسب لشخص دولي معين وبالتالي يصعب تحديد المسئولية المترتبة عليها، ومن ناحية أخرى لا يوجد معيار محدد حول إمكانية الدفاع الشرعي لصد الهجمات السيبرانية فما زال الموضوع محل بحث ونقاش ولم تتضح معالم واضحة في هذا الموضوع.

وعلى ذلك يجب الاعتراف ان قواعد القانون الدولي رغم أنها قواعد آمرة ألا أنها ليست قواعد جامدة وعلى ذلك يجب أن تتطور لمواكبة التطور الحاصل على الصعيد الدولي، وهذا الأمر يستدعى بالضرورة إلى تغيير مفهوم القوة ليشمل القوة العسكرية والغير عسكرية، مع ضرورة التعاون بين دول العالم من خلال عقد اتفاقيات وبروتوكولات لتنظيم مكافحة الهجمات السيبرانية بصورة أكثر دقة ووضوح وفاعلية.

- **نتائج البحث**

توصلنا من خلال هذا البحث إلى عدة نتائج أهمها:

١- لا يزال مفهوم الهجمات السيبرانية محل خلاف بين الدول والمنظمات والفقهاء القانون الدولى.

٢- إن وضع الهجمات السيبرانية في الإطار القانوني الدولي لقائم، أمر صعب جداً؛ وذلك بسبب الطبيعة الخاصة لها، إضافة إلى عدم وجود بيان قانوني رسمي ونهائي متفق عليه بشأن هذه الظاهرة.

٣- أن التطور التكنولوجى أصبح له العديد من السلبيات على الأمن القومى للدول.

٤- عدم كفاية الجهود الدولية للحد ومكافحة الهجمات السيبرانية رغم الجهود الدولية والإقليمية لمكافحة هذه الظاهرة، وذلك من خلال المؤتمرات والاتفاقيات الدولية لمنع الجريمة السيبرانية، ومعاملة المجرمين السيبرانيين.

٥- إن هناك صعوبات ومعوقات تقف عائقاً في وجه المساعي والجهود الحثيثة في إيجاد آليات فاعلة بين الدول لمكافحة الجرائم السيبرانية.

٦- إن الجرائم السيبرانية -بوصفها جرائم عالمية عابرة للحدود-لا تتحقق مكافحتها إلا من خلال التعاون الدولي على المستوى الإجرائي الجنائي.

- **توصيات البحث**

بعد التوصل للنتائج السابقة نوصي بالآتى:

١-يجب على فقهاء القانون الاهتمام بدراسة موضوع الهجمات السيبرانية بشكل أكثر فاعلية لتنظيم مكافحتها ووضع نظام قانوني لذلك.

٢-يجب وضع تشريعات داخلية لمكافحة الهجمات السيبرانية لسد الفراغ التشريعي في مجال مكافحة الجريمة السيبرانية.

٣-عقد اتفاقيات دولية وبروتوكولات للتعاون في مجال الهجمات السيبرانية.

٤-عمل وحدات متكاملة في كل الدول لرصد الهجمات السيبرانية وتكون مرتبطة بوحدات داخل الأمم المتحدة لبيان المسئول عن الهجمات السيبرانية ومعاقبته.

قائمة المراجع

أولاً: الكتب القانونية

- أحمد زهران، موسوعة نظم وأساليب الحرب الحديثة، الطبعة الأولى، مطابع الأهرام التجارية، مصر، ١٩٨٩
- أحمد عبيس نعمة الفتلاوي، الهجمات السبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، منشورات زين الحقوقية، بيروت لبنان، الطبعة الأولى، ٢٠١٨
- احمد وافي، الحماية الدولية لحقوق الإنسان ومبدأ السيادة، دار هومة الجزائر، ٢٠٠٥
- د/ إيهاب خليفة

١- تأثير الثورة الصناعية الرابعة على الأمن القومي: مجتمع ما بعد المعلومات، د. ر. ط، العربي للنشر والتوزيع، القاهرة – مصر، ٢٠١٩

٢- القوة الإلكترونية: كيف يمكن أن تدير الدولة شؤونها في عصر الإنترنت، دار العربي للنشر والتوزيع، القاهرة، ٢٠١٧

- حازم محمد علتم، أصول القانون الدولي العام، القسم الثاني أشخاص القانون الدولي، دار النهضة العربية بالقاهرة، ٢٠٠١
- حيدر رندة، السلاح السيبراني في حروب إسرائيل المستقبلية، مؤسسة الدراسات الفلسطينية، بيروت – لبنان، ٢٠١٨
- شادي عبد الوهاب منصور، حروب الجيل الخامس: أساليب التفجير من الداخل على الساحة الدولية، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة – مصر، ٢٠١٩

(ISSN: ٢٣٥٦ - ٩٤٩٢)

- شريف عتلم ومحمد ماهر عبد الواحد،" موسوعة اتفاقيات القانون الدولي الإنساني، النصوص الرسمية للاتفاقيات والدول المصدقة عليها"، إصدار بعثة اللجنة الدولية للصليب الأحمر بالقاهرة، الطبعة السابعة٢٠٠٧

- صادق باقر إبراهيم العلوي، المسؤولية الدولية الناشئة عن دعم المجموعات المسلحة، دراسة تحليلية، منشورات زين الحقوقية، لبنان، بيروت، ط ١، ٢٠١٨

- د/ عادل عبد الصادق

١-الإرهاب الالكتروني والقوة في العلاقات الدولية: نمط جديد وتحديات مختلفة، مركز الدراسات السياسية والاستراتيجية، القاهرة، ٢٠٠٩

٢-أنماط الحرب السيبرانية وتداعياتها على الامن العالمي، مجلة السياسة الدولية، القاهرة، ٢٠١١

٣-أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، المركز العربي لأبحاث الفضاء الالكتروني، مصر، ٢٠١٨

- عبد الإلة النوايسة، جرائم تكنولوجيا المعلومات–شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية. الأردن: دار وائل للنشر والتوزيع، المجلد الأولى، عمان، ٢٠١٧

- د/ عبد العزيز بن غرم الله آل جار الله، جرائم الإنترنت وعقوباتها وفق نظام مكافحة الجرائم المعلوماتية السعودي دراسة مقارنة (ويليه آثار العولمة على مستخدمي الإنترنت)، دار الكتاب الجامعي، الرياض، الطبعة الأولى، ٢٠١٧م

- د/ عبد الفتاح حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت. مصر: دار الكتب القانونية، المحلة الكبرى، الطبعة الأولى ٢٠٠٧

- د/ عبد الفتاح مراد، شرح جرائم الكمبيوتر والانترنيت، دار الكتب والوثائق المصرية، دط، دت

- عبد الكريم علوان، الوسيط في القانون الدولي العام، دار الثقافة، عمان، ٢٠٠٦

- د/ عبد الله أحمد هلالي، الجوانب الموضوعية والإجرائية للجرائم المعلوماتية على ضوء اتفاقية بودابست ٢٠٠١، دار النهضة العربية، ٢٠٠١

- د/ عبد الواحد محمد الفار، القانون الدولى العام، دار النهضة العربية القاهرة، ١٩٩٤

- علي محمد كاظم الموسوي، المشاركة المباشرة في الهجمات السيبرانية، المؤسسة الحديثة للكتاب، ط ١، ٢٠١٩

- علي نعمة جواد الزرفي، الجريمة المعلوماتية الماسة بالحياة الخاصة دراسة مقارنة، المكتب الجامعي الحديث، بدون طبعة، ٢٠١٩

- عمار عباس الحسيني، جرائم الحاسب والانترنت (الجرائم المعلوماتية)، الطبعة الأولى، منشورات زين الحقوقية، بيروت لبنان، ٢٠١٧
- غانم مرضي الشمري، الجرائم المعلوماتية، الدار العلمية الدولية، عمان، الطبعة الأولى، ٢٠١٦م
- د/ كمال الدين، النزاع المسلح والقانون الدولي العام، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، ط ١، ١٩٩٧
- د/ محمد حافظ غانم،" المسؤولية الدولية: دراسة لأحكام القانون الدولي وتطبيقاتها التي تهم الدول العربية"، محاضرات معهد الدراسات العربية العالية، جامعة الدول العربية، القاهرة، ١٩٦٢
- د/ محمد حميد المزمومي، الوسيط في شرح نظام الإجراءات الجزائية السعودي، مركز النشر العلمي بجامعة الملك عبد العزيز، جدة، الطبعة الثانية، ٢٠١٩
- د/ محمد خليل موسى، استخدام القوة في القانون الدولي المعاصر، دار وائل للنشر، الأردن، ٢٠٠٤
- د/ محمد طلعت الغنيمي، الوسيط في قانون السلام، منشأة المعارف، الإسكندرية، ١٩٩٣
- محمود أحمد القرعان، الجرائم الإلكترونية، دار وائل للنشر والتوزيع، عمان، الطبعة الأولى، ٢٠١٧
- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية. الأردن: دار الثقافة للنشر والتوزيع، الإصدار الثاني، المجلد الأولى، عمان، ٢٠٠٩
- د/ محمود عمر محمود، الجرائم المعلوماتية والإلكترونية، خوارزم العلمية، الطبعة الأولى، ٢٠١٥م
- د/ مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت دار النهضة العربية ٢٠٠٠
- د/ مصطفى احمد ابو الوفا، المبادئ العامة في القانون الدولي المعاصر، إشراك للطباعة والنشر، مصر، ٢٠٠٦
- مصطفى محمد موسى، السيرة الذاتية للفايروسات الالكترونية سلسة اللواء الامنية في مكافحة الجريمة الالكترونية، الكتاب الرابع ط ١، دار الكتب القانونية، مصر، ٢٠٠٨
- د/ مفيد شهاب، دراسات في القانون الدولي الإنساني اللجنة الدولية للصليب الأحمر بدون تاريخ نشر
- د/ منير البعلبكي،" المورد: قاموس انكليزي –عربي"، دار العلم للملايين، بيروت، ٢٠٠٤
- ناصر حمودى، العقد الدولي الإلكتروني المبرم عبر الإنترنت، بدون دار نشر،٢٠١٢
- نعمان عطاء الله الهيني، قانون الحرب او القانون الدولي الانساني، دار مؤسسة رسلان للطباعة والنشر والتوزيع دمشق، ٢٠٠٨

ثانياً: الرسائل العلمية

أ- **رسائل الدكتوراة**

(ISSN: ٢٣٥٦ - ٩٤٩٢)

- أيمن عبد العزيز سلامة، المسؤولية الدولية عن ارتكاب جريمة الإبادة الجماعية، رسالة دكتوراه، كلية الحقوق جامعة الإسكندرية، ٢٠٠٥

- سراب ثامر أحمد، الهجمات على شبكات الحاسوب في القانون الدولي الإنساني، أطروحة دكتوراه، كلية الحقوق، جامعة النهرين، ٢٠١٥

ب- رسائل الماجستير

- أسامة مهمل، الإجرام السيبراني، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، ٢٠١٨/٢٠١٧

- أميرة حناشي، مبدأ السيادة في ظل التحولات الدولية الراهنة، رسالة ماجستير، كلية الحقوق، جامعة منتورى، قسنطينة، ٢٠٠٨

- إيمان حمدان، التكنولوجيات الجديدة والقانون الدولى الإنسانى (الحرب السيبرانية)، ماجستير في القانون الدولى الإنسانى، الجامعة الافتراضية السورية، ٢٠٢٠

- حسام جاسم محمد أحمد الدليمي، التطور والتكنولوجي وأثره في سيادة الدول، رسالة ماجستير، كلية القانون والعلوم السياسية، جامعة الانبار، العراق، ٢٠١٨

- سليم دحماني، أثر التهديدات السيبرانية على الأمن القومى، رسالة ماجستير، جامعة محمد بوضياف، كلية الحقوق والعلوم السياسية، ٢٠١٨

- صلاح حيدر عبد الواحد، حروب الفضاء الإلكترونى، دراسة في مفهومها وخصائصها وسبل مواجهتها، رسالة ماجستير، كلية الآداب والعلوم، قسم العلوم السياسية، جامعة الشرق الأوسط، ٢٠٢١

- طالب خيره، مبدأ حظر استخدام القوة في العلاقات الدولية، كلية العلوم الإنسانية والاجتماعية، جامعة ابن خلدون، ٢٠٠٧

- عبد الرحمن بجاد العتيبى، الأمن السيبرانى في تعزيز الأمن السيبرانى، جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية (قسم الأمن الإنسانى)، ٢٠١٧

- محمود إبراهيم عبد الرحمن شهاب، الأسلحة غير التقليدية في الفقه الإسلامي، الجامعة الإسلامية، رسالة ماجستير، كلية الشريعة والقانون، غزة، ٢٠٠٧

- نور أمير الموصلى، الهجمات السيبرانية في ضوء القانون الدولى الإنسانى، رسالة ماجستير في القانون الدولى الإنسانى، الجامعة الافتراضية السورية، ٢٠٢١

ثالثاً: المقالات والأبحاث القانونية

- د/ احمد عبيس نعمة الفتلاوي

١- الهجمات السيبرانية: فهو مفهومها المسؤولية الدواية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق المحلي للعلوم القانونية والسياسية، كلية القانون جامعة بابل، العدد الرابع، السنة الثامنة، ٢٠١٦

٢- احمد عبيس نعمة الفتاوي، زهراء عماد مجيد، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، المجلد ١، العدد ٤٤، آذار، جامعة الكوفة – كلية القانون، ٢٠٢٠

٣- د/ أحمد عبيس نعمة الفتلاوى، د/ أزهر عبد الأمير الفتلاوى، المسؤولية الناشئة عن استخدام وسائل القتال الفتاكة في نشر الأوبئة "الهجمات السيبرانية مقابل جائحة كورونا"، مجلة الحقوق، العدد ٤١

- إسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية ولسياسية، منشوارت جامعة الشهيد حمة لخضر بالوادي، المجلد ١٠، العدد ١، الجزائر، ٢٠١٩

- أميرة عبد العظيم محمد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد ٣٥، الجزء ٣، كلية القانون، جامعة الامارات العبرية المتحدة، ٢٠٢٠

- بشار خليل، ماهى الحرب السيبرانية؟ مستقبل مخيف للصراع الرقمى، مجلة المعلوماتية، العدد ١٥٤، الجمعية السورية للمعلوماتية، ٢٠٢٠

- بلقاسم بن صابر، الهجمات السيبرانية ومواجهتها في ضوء القانون الدولى المعاصر، مجلة حقوق الإنسان والحريات العامة، العدد ٤، ٢٠١٧

- بهاء عدنان السعيرى، عماد عيد خضير، انتقال التهديدات من الواقع إلى العالم الافتراضي، مجلة جامعة بابل للعلوم االإنسانية، المجلد ٢٧، العدد ٤، ٢٠١٩

- تغريد صفاء، لبنى خميس مهدي، أثر السيبرانية في تطور القوة، مجلة حمورابي للدراسات، مركز حمورابي للبحوث والدراسات الاستراتيجية، العدد ٣٣ – ٣٤، السنة ٨، شتاء –ربيع، بغداد، ٢٠٢٠

- جمال العظامات، جريمة العدوان في الهجمات الإلكترونية في نطاق القانون الدولي العام، مجلة المنارة، العدد ٤، المجلد ٢١، ٢٠١٥

- حسام عبد الامير خلف، البعد الجديد–الخامس–في النزاعات المسلحة الفضاء الالكتروني، مجلة كلية الحقوق، جامعة النهرين، العدد (١)، ٢٠١٦

- حسن بن أحمد الشهري،"الإرهاب الالكتروني – حرب الشبكات"، المجلة العربية الدولية للمعلوماتية، ٢٠١٥

- حمدون تورية، الاستجابة الدولية للحرب السيبرانية، البحث عن الامن السيبراني، الناشر الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء، ٢٠١١

(ISSN: ٢٣٥٦ - ٩٤٩٢)

- حيدر أدهم الطائي، علي محمد كاظم، المشاركة المباشرة للهبة الجماعية في الهجمات السيبرانية، مجلة كلية الحقوق، المجلد ٢١، العدد ٢، جامعة النهرين، ٢٠١٩

- حيدر كاضم عبد علي، مبدأ التمييز بين المدنيين والمقاتلين دراسة على ضوء القانون الدولي الانساني، مجلة الكلية الإسلامية الجامعة النجف، العدد ٢٢، ٢٠١٣

- حيدر ناظم عبد علي، رباب محمود عامر، التنظيم القانوني للهجمات السيبرانية على المنشآت ذات القوى الخطرة، مجلة الكوفة، العدد ٤،٧ جامعة الكوفة، ٢٠١٩

- روان بنت عطية الله الصحفي، الجرائم السبيرانية، بحث منشور في المجلة الإلكترونية الشاملة متعددة التخصصات، العدد الرابع والعشرون، شهر (٥)، ٢٠٢٠

- رياض مهدي عبد الكاظم، وألاء طالب خلف، المعلوماتية والحرب الحديثة، دراسة حالة الحرب الأمريكية على العراق عام ٢٠٠٣، مجلة للعلوم الإنسانية، المجلد (١١)، العدد (٢٩)، ٢٠١٥

- زينب شنوف، الحرب السيبرانية في العصر الرقمي: حروب ما بعد كلاوزفيتش، المجلة الجزائرية للأمن والتنمية، المجلد ٩، العدد ٢، يوليو، الجزائر، ٢٠٢٠

- د/ سعيد درويش، ماهية الحرب الإلكترونية في ضوء قواعد القانون الدولى، حوليات جامعة الجزائر، العدد ٢٩، ج٢، ٢٠١٦

- سمير بارة، الامن السيبراني في الجزائر السياسات والمؤسسات. المجلة الجزائرية للآمن الإنساني، العدد ٤، ٢٠١٧

- سميرة شريطة، السيادة السيبرانية في الصين بين متطلبات القوة وضروريات الأمن القومى، المجلة الجزائرية للأمن والتنمية، المجلد ٩، العدد ١٦، ٢٠٢٠

- شوبرب جيلالي، مراد فائزة، الآليات الدولية والوطنية لمكافحة الجريمة السيبرانية، مجلة الدراسات القانونية والسياسية، المجلد ٩، العدد ٢، ٢٠٢٣

- شيخة حسين الزهراني، التعاون الدولى في مواجهة الهجوم السيبرانى، مجلة الشارقة للعلوم القانونية، المجلد ١٧، العدد ١، جامعة الشارقة، كلية القانون، الإمارات العربية المتحدة، ٢٠٢٠

- صلاح مهدي هادي الشمري، زيد محمد علي إسماعيل، الامن السيبراني كمرتكز جديد في الاستراتيجية العراقية، مجلة قضايا سياسية، السنة ١٢، العدد ٦٢، جامعة النهرين، كلية العلوم السياسية، ٢٠٢٠

- صورية بورباية، التعاون الدولي في مكافحة الجريمة المعلوماتية، مجلة القانون الدولي للدراسات البحثية، العدد ٠١، ٢٠١٩

- طارق المجذوب، السايبر ساحة خفية حرب ناعمة قادمة، مجلة الدفاع الوطنى اللبناني، العدد ٨٩، ٢٠١٤

- طالب حسن موسي، عمر محمود أعمر، (٢٠١٦)، الإنترنت قانونا، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة، العدد السابع والستين

- د/ عادل عبد الصادق، القوة الالكترونية: اسلحة الانتشار الشامل في عصر الفضاء الالكتروني، مجلة السياسة الدولية، العدد ١٨٨، مؤسسة الأهرام، مصر، ٢٠١٢

- د/ عامر عبد الفتاح الجومرد، السيادة، مجلة الرافدين للحقوق، جامعة الموصل، العدد الاول، ١٩٩٦

- عبد الله بن عبدالعزيز بن فهد العجلان، الإرهاب الإلكترونى في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، القاهرة، ٢٠٠٠

- عطية إدريس، مكانة الأمن السيبراني في منظومة الامن الوطني الجزائري. مجلة مصداقية، المجلد ١، العدد ١، ٢٠١٩

- على عبد الرحيم العبودى، "هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين"، المجلة العلمية الأكاديمية العراقية، العدد (٥٧)، جامعة بغداد، كلية العلوم السياسية، ٢٠١٩

- على فاضل على سليمان، حق الدفاع الشرعى على الهجمات السيبرانية، مجلة تكريت للحقوق، السنة ٤، المجلد ٤، العدد ٤، الجزء ١

- علي محمد كاظم المشاركة المباشرة للهبة الجماعية في الهجمات السيبرانية مجلة كلية الحقوق جامعة النهرين بغداد، ٢٠١٩

- عمر محمود أعمر، الحرب الإلكترونية في القانون الدولى الإنسانى، دراسات، علوم الشريعة والقانون، المجلد ٤٦، عدد ٣، ٢٠١٩

- فاطمة بيرم، السيادة الوطنية في ظل الفضاء السيبراني والتحويلات الرقمية "الصين نموذجا"، المجلة الجزائرية للأمن الإنساني، العدد ١، ٢٠٢٠

- فايزة ميموني، تسليم المتهمين بين مقتضيات التعاون القضائي الدولي وحقوق الانسان مجلة الحقوق والعلوم الإنسانية، المجلد / ١٥ العدد ١

- قطاف سليمان، مواجهة الجرائم السيبرانية في ضوء الإتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية، المجلد ٥، العدد ٢، ٢٠٢٢

- كوردولا دويجي، لا تقترب من حدود فضائي الإلكتروني، الحرب الإلكترونية والقانون الدولي الإنساني وحماية المدنيين، المجلة الدولية للصليب الأحمر، مجلد ٩٤، (٨٨٦) صيف ٢٠١٨

- لمى عبد الباقي محمود، اسراء نادر كيطان، المسؤولية الدولية عن الأضرار التي تحدثها الهجمات الالكترونية، عدد خاص لبحوث التدريسيين مع طلبة الدراسات العليا، الجزء الثاني، سبتمبر ٢٠٢١

(ISSN: ٢٣٥٦ - ٩٤٩٢)

- ليندا شرابسة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الالكترونية. مجلة دراسات وأبحاث، المجلد ١، العدد ١، ٢٠٠٩

- مايكل شميت، الحرب بواسطة شبكات الاتصال، الهجوم على شبكات الكومبيوتر(الحاسوب) في الحرب منشورات المجلة الدولية للصليب الاحمر، ٢٠٠٢

- محمد وائل القيسي، مستقبل الامن الاستراتيجي العالمي في ظل التحديات التكنو – معلوماتية والفضاء السيبراني، مجلة دراسات إقليمية، مركز الدراسات الإقليمية، السنة ١٤، العدد ٤،٤ نيسان، جامعة الموصل، ٢٠٢٠

- مراد مشوش، الجهود الدولية لمكافحة الإجرام السيبرانى، مجلة الواحات للبحوث والدراسات، المجلد ١٢، العدد ٧٠٣، ٢٠١٩

- منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربى للبحوث القانونية والقضائية، بيروت، ٢٠١٧

- نورة شلوش، القرصنة الالكترونية في الفضاء السيبراني "التهديد المتصاعد لأمن الدول"، مجلة مركز بابل للدراسات الإنسانية، المجلد ٨، العدد، ٢ جامعة بابل، ٢٠١٨

- نيلس ميلزر، مقدمة شاملة القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر، ٢٠١٦

- هربرت لين، النزاع السيبراني والقانون الدولي الإنساني، مختارات من المجلة الدولية للصليب الاحمر، المجلد (٩٤) العدد (٨٨٦)، ٢٠١٢

- يحيي مفرح الزهراني، الأبعاد الإستراتيجية والقانونية للحرب السيبرانية، مجلة البحوث والدراسات، جامعة الوادي، العدد ٢٣، السنة ٢٠١٧

- يحيي ياسين سعود، الحرب السيبرانية في ضوء القانون االدولى الإنسانى، المجلة القانونية، المجلد القانونية، المجلد ٤، العدد ٤، كلية الحقوق، جامعة القاهرة، فرع الخرطوم، ٢٠١٨

- يحيي ياسين مسعود، الحرب السيبرانية في ضوء قواعد القانون الدولى الإنسانى، المجلة القانونية، المجلد ٤، ٢٠١٨

رابعاً: المعاهدات الدولية

- ميثاق الأمم المتحدة ١٩٤٥
- الإعلان العالمى لحقوق الإنسان لعام ١٩٤٨
- البروتوكول الإضافي الأول والثانى لعام ١٩٧٧ الملحق باتفاقيات جنيف لسنة ١٩٤٩
- اتفاقية حلف شمال الأطلسي لعام ١٩٤٩
- الإتفاقية الأوروبية لحقوق الإنسان لعام ١٩٥٠

- العهد الدولي للحقوق المدنية والسياسية لعام ١٩٦٦
- الإتفاقية الامريكية لحقوق الإنسان لعام ١٩٦٩
- نظام روما الأساسي لعام ١٩٩٨
- اتفاقية مجلس أوربا المتعلق بالجريمة الالكترونية"، مجموعة المعاهدات الأوروبية رقم ١٨٥، بودابست عام ٢٠٠١
- تقرير اللجنة الدولية للصليب الأحمر للمؤتمر الدولي الحادي والثلاثون للصليب الأحمر والهلال الأحمر، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة جنيف سويسرا، ٢٠١١، الوثيقة. ٢. ١. ٥/ ١١/ ٣١ ic,

خامساً: المراجع الأجنبية

*Alexander kosenkov, cyber conflict a new global threat, future internet, mdpi, ٨, ٤٥, ٢٠١٦

* Darko galinec, darko mozink and boris, I bid, p ٤

*Michael Robinson, Kevin jones, helge janicke, cyber war fare: issues and challenges, article in computer and security, Elsevier ,volume – ٤٩ -, march, united kingdom, ٢٠١٥

*Robert "Jake" bebber, cyber power and cyber effectiveness: an analytic framework, comparative strategy an international journal, routledge, taylor & francis group, volume ٣٦, November ٥, ٢٠١٧

* Stefan soesanto and max smeets, cyber deterrence: the past, present and future, center for security studies (css), Switzerland,٢٠٠٠.