الطبيعة القانونية للهجمات السيبرانية التي تقع بين الدول

The legal nature of cyber attacks that take place between states

منزر رابح[1] ، درويش سعيد[2]

[1] معهد الحقوق والعلوم السياسية المركز الجامعي تيبازة، rabah1609@yahoo.fr

[2] كلية الحقوق جامعة الجزائر 1، saidderouiche7@gmail.com

تاريخ الإرسال: 2020/05/28 تاريخ القبول: 2020/06/20 تاريخ النشر: 2021/11/30

ملخص:

تهدف هذه الدراسة إلى تبيان الطبيعة القانونية للهجمات السيبرانية التي تقع بين الدول، من حيث كونها إما جريمة سيبرانية تحكمها إتفاقية بودابست لعام 2001 المتعلقة بالجريمة السيبرانية، أم حرب سيبرانية تخضع لأحكام دليل تالين لعام 2013 الخاص بقواعد القانون الدولي المطبقة على الحروب السيبرانية التي تتم في إطار نزاع مسلح، أو عبارة عن جريمة دولية ذات طابع خاص تطبق عليها قواعد القانون الدولي العام الأخرى التي تحكم العلاقات بين الدول وفي مقدمتها ميثاق الأمم المتحدة، ومن ثم يمكن إثارة المسؤولية الدولية للدولة المعتدية على أساس أن هذا السلوك يعد صورة من صور العدوان الذي يحظره القانون الدولي.

كلمات مفتاحية: الطبيعة القانونية، الهجمات السيبرانية، المجرم السيبراني، تقع بين الدول.

Abstract: This study aims to demonstrate the legal nature of cyber-attacks, which take place between states, as well as whether cybercrime, governed by the 2001 Budapest Convention on cybercrime, or by the provisions of the Tallinn manual adopted in 2013, on international law applicable to cyber wars. Or by other rules of international law, in particular those governing relations between states, in particular the Charter of the United Nations, etc.

Keywords: The legal nature - cyber attacks - cybercriminal - takes place between states.

1- المؤلف المرسل: منزر رابح rabah1609@yahoo.fr

مقدمة:

يعد الإجرام السيبراني من بين أهم المسائل الجنائية التي باتت تلقى إهتماما كبيرا، سواء على المستوى الوطني أو الدولي، وذلك نظرا لإنتشارها الكبير فضلا 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 لشؤون الدولة.

لكن، إذا كان الإعتداء السيبراني الذي ينفذه الأشخاص العاديون ضد الأنظمة الحاسوبية داخل دولة معينة، يعد جريمة سيبرانية لا مراء فيها، فإن الأمر يختلف تماما في حالة ما إذا نفذ هذا الهجوم من قبل دولة ضد دولة أخرى، كالذي قامت به إسرائيل ضد إيران عام 2009، [1] أو ذلك الهجوم الذي نفذته روسيا ضد إستونيا عام 2007 وضد جورجيا عام 2008. حيث يرى البعض أن المسألة تعد حربا سيبرانية لا تختلف كثيرا عن الحرب الكلاسيكية المعروفة، إلا من حيت الوسائل المستخدمة وميدان إدارة المعارك وأشياء أخرى ذات صلة، كإعلان الحرب وغيرها، على إعتبار أن الحروب السيبرانية غالبا ما تنفذ بطريقة سرية ودون إعلان مسبق.

من ثم، من الأهمية بما كان، تبيان الحدود الفاصلة بين الجريمة السيبرانية والحرب السيبرانية، سواء من حيث التكييف القانوني للوقائع المؤدية للجريمتين، أو من حيث الأساس القانوني أو النظام القانوني الذي ينظمهما، فالجريمة السيبرانية التي ينفذها الأفراد داخل أو ضد الدولة يطبق عليها قانون تلك الدولة. ففي الجزائر مثلا يتم التصدي للجريمة السيبرانية من خلال نص القانون رقم 04-15، المؤرخ في: 2004/11/10، المتعلق بالحماية الجزائية للأنظمة المعلوماتية، وكذا القانون رقم 09-04، المؤرخ في: 2009/08/05، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

غير أن الإشكال الذي يثور هنا، يكمن فيما إذا نفذت هذه الجريمة من طرف دولة ضد دولة أخرى، إذ يصعب هنا إعمال القانون الداخلي للدولة، لأن المجرم السيبراني (cybercriminel) هنا مختلف تماما وغير مألوف، وبالتالي ينبغي البحث عن قواعد قانونية دولية كي تطبق على مثل هذه الهجمات، فالقانون الدولي إذن هو المختص للنظر فيها، نظرا لكون الفاعلين عبارة عن دول وليسوا أشخاص عاديين.

من هذا المنطلق، يسعى هذا البحث إلى تبيان الطبيعة القانونية للهجمات السيبرانية التي تنفذها الدول في ما بينها، حيث يبحث فيما إذا كانت تلك الهجمات مجرد جريمة سيبرانية أطرافها دول، أو أشخاص القانون الدولي الأخرى من كيانات من غير الدول (entités non étatiques)، كالمنظمات الدولية أو الشركات المتعددة الجنسيات وغيرها.

تتجلى أهمية هذه الدراسة في كونها تعالج مسألة التكييف القانوني للهجمات السيبرانية التي تقع بين الدول، من حيث كونها إما جريمة سيبرانية تحكمها إتفاقية بودابست لعام 2001 المتعلقة بالجريمة السيبرانية، أم هي حرب سيبرانية تخضع لأحكام دليل تالين لعام 2013، الخاص بقواعد القانون الدولي المطبقة على الحروب السيبرانية التي تتم في إطار نزاع مسلح، أو هي جريمة دولية ذات طابع خاص تطبق عليها قواعد القانون الدولي العام الأخرى التي تحكم العلاقات بين الدول، وفي مقدمتها ميثاق الأمم المتحدة، ومن ثم يمكن إثارة المسؤولية الدولية للدولة المعتدية على أساس أن هذا السلوك هو صورة من صور العدوان الذي يحظره القانون الدولي.

تأسيسا على ما سبق، تحاول هذه الورقة البحثية الإجابة عن التساؤل الجوهري التالي: **ماهو التكييف القانوني الصحيح للهجمات السيبرانية التي تقع بين الدول؟**

الإجابة عن هذا السؤال الجوهري يقتضي الإستعانة بالسؤالين الفرعيين التاليين:

- هل هي جريمة سيبرانية ذات طابع دولي أم أنها حرب سيبرانية
- ما هو القانون الواجب التطبيق على مثل هذه الهجمات ؟

تجدر الإشارة إلى أن معالجة الإشكالية المطروحة، سيكون وفق المنهج الإستقرائي الموائم لطبيعة الموضوع، المتمثلة في البحث عن الأسانيد القانونية التي تدعم وجهات النظر المختلفة، كما سيتم الإستعانة بالمنهج الوصفي قصد إستعراض السمات التي تميز كلا الجريمتين، وذلك من خلال الخطة التالية:

المبحث الأول : التكييف القانوني للهجمات السيبرانية بين الدول.

المطلب الأول: الهجمات السيبرانية بين الدول إجرام سيبراني.

المطلب الثاني: الهجمات السيبرانية بين الدول حرب سيبرانية.

المطلب الثالث: الهجمات السيبرانية بين الدول جريمة سيبرانية ذات طابع خاص.

المبحث الثاني: القانون الواجب التطبيق على الهجمات السيبرانية بين الدول.

المطلب الأول: إتفاقية بودابست لعام 2001 المتعلقة بالجريمة السيبرانية.

المطلب الثاني: أحكام دليل تالين لعام 2013 الخاص بالحرب السيبرانية.

المطلب الثالث: قواعد القانون الدولي التي تحكم العلاقات بين الدول.

1.المبحث الأول : التكييف القانوني للهجمات السيبرانية بين الدول.

1.1.المطلب الأول: الهجمات السيبرانية بين الدول إجرام سيبراني.

يعرف البعض الجريمة السيبرانية (cyber crime) بكونها عبارة عن نشاط إجرامي، تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي.[2] لذلك ترى اللجنة الدولية للصليب الأحمر أنه ليس هنالك أي فراغ قانوني فيما يتعلق بتنظيم الفضاء السيبراني ككل.[3]

لكن وبالرغم من أنه ليس هنالك من إجماع واسع على تعريف محدد ودقيق 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"**.[4] ، 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 [5]

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 إلى مئات المليارات من الدولارات، كما أنه قد يترتب عليها سقوط آلاف الضحايا. [6]

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 للتعرض لهجمات إلكترونية أمريكية عن طريق إستخدام سلاح إلكتروني سري[7].

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 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 (Budapest) لعام 2001 المتعلقة بالجريمة السيبرانية [8] في المادة 12، على مسؤولية الأشخاص المعنوية، وعلى ضرورة أن تسن الدول الأطراف نصوص قانونية ترتب المسؤولية على من يرتكب أي جريمة سيبرانية.

لكن ما يعاب على هذه الإتفاقية، وعلى هذه المادة بالذات، أنها لم تحدد ما إذا كانت الدولة أو أحد فروعها معنيا بأحكامها، وهذا ما يستوجب إستبعاد نصوصها وضرورة البحث عن نصوص قانونية يمكن تطبيقها على الهجمات السيبرانية التي تشنها الدول[9].

2.1.المطلب الثاني: الهجمات السيبرانية بين الدول حرب سيبرانية.

تثير الهجمات السيبرانية بين الدول عدة مسائل حاسمة في سبيل تكييف تلك الهجمات تكييفا قانونيا صحيحا، بمعنى هل تعتبر جريمة أم حربا 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.

نظرا لأهمية هذا المسعى، وخطورة الجريمة السيبرانية في مثل هذه المسائل التي تمس بالأمن القومي للدول[10] 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 البنى التحتية الكبرى للدول، كمحطات الكهرباء، والسدود...الخ.

تبنى في هذا الصدد، آخرون مصطلح الحرب السيبرانية (Cyber Warfare)، وهذا إستنادا إلى إيديولوجية أمنية أو عسكرية، تضع منهاجا لتحقيق أهدافا على الصعيد الأمني أو العسكري تجاه (العدو المفترض).[11] وهذا ما يطبع الهجمات السيبرانية بين الدول بميزة أساسية تتمثل في الشمولية.

في نفس السياق، عادة ما ينصب إهتمام المختصين في القانون الدولي الإنساني على وصف الوسيلة والأثر، وبعبارة أخرى، التركيز على وسيلة الهجوم وطريقة تنفيذها وما سينجم عنها من آثار[12]، أكثر من التركيز على ما تحتويه وسائل وطرائق القتال ذاتها[13].

يؤيد هذا التوجه كل من توماس رد (Thomas Rid) وبيتر ماكبورني(Peter Mcburney) المختصان في القانون الدولي الانساني إذ ذهبا إلى تفضيل إصطلاح الهجوم السيبراني، بدلا من الحرب السيبرانية على أساس أن الأخير أوسع نطاقا من الأول.[14]

3.1.المطلب الثالث: 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 والإتصالاتية 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 [15].

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 المتحدة إلى عقد إتفاقية مع الصين لعدم شن

هجمات سيبرانية على البنية التحتية الأمريكية أو شركات القطاع الخاص في حالة السلم [16].

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 سلاحا ذا حدين فكما يمكن إستخدامه في تحسين جودة حياة البشر داخل المدينة يمكن إستخدامه أيضا في تهديد أمن الأفراد بالأمن القومي للدولة، لذلك نجد أن بعض الدول حظرت إستخدام بعض هذه التقنيات الحديثة مثل الطائرات من دون طيار وذلك تخوفا من إستخدام الحركات الإرهابية لهذه التقنية في تنفيذ عمليات إرهابية عن بعد، ولذلك يمثل الإرهاب السيبراني خطرا على الأمن القومي من خلال توظيف التقنيات الذكية في تنفيذ عمليات إرهابية سيبرانية.[17]

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 أمرا صعبا، 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 (les acteurs)، 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 [18].

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.(19)

فيما صرح العضو الأسبق في مجلس النواب الروسي الدوما (نيكولاي كوريانوفج) Kuryanovich Nikolai 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.(20)

2. المبحث الثاني: القانون الواجب التطبيق على الهجمات السيبرانية بين الدول.

1.2. المطلب الأول: إتفاقية بودابست لعام 2001 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 أيضا تحديد القواعد التي تحكم هذه التصرفات. وباستقراء نصوص إتفاقية بودابست لعام 2001 المتعلقة بالجريمة السيبرانية، يتضح لنا أنه يمكن تطبيق بعض موادها على هذه المسألة.

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 إدراكا 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.[21]

بالإضافة إلى إتفاقية الإتحاد الإفريقي المتعلقة بالجريمة السيبرانية وحماية المعطيات ذات الطابع الشخصي، المبرمة بتاريخ: 2014/06/27، التي تضمنت في فصلها الثالث المعنون بـ: حماية الأمن السيبراني ومكافحة الجريمة السيبرانية.

لكن ما يعاب أيضا على الإتفاقيتين، أي إتفاقية بودابست(Budapest) وإتفاقية الاتحاد الإفريقي(union africaine) 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.

2.2. المطلب الثاني: أحكام دليل تالين لعام 2013 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 (le manuel de Tallinn) لعام 2013، 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 95 قاعدة إستمدت في مجملها من أحكام القانون الدولي المختلفة كميثاق الأمم المتحدة وقواعد القانون الدولي الإنساني...وغيرها [22].

يقدم "دليل تالين" رؤى مثيرة للإهتمام في هذا الصدد فهو يتمسك على سبيل المثال بالثنائية التقليدية للنزاعات المسلحة الدولية والنزاعات المسلحة غير الدولية، ويقر بأن العمليات الإلكترونية وحدها قد تشكل نزاعات مسلحة تبعا للظروف- لا سيما الآثار المدمرة لتلك العمليات- ويقدم الدليل في هذا الصدد تعريفا " 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 نظرا 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 20 من الدليل (manuel de Tallinn)، 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، فضلا 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.

3.2. المطلب الثالث: قواعد القانون الدولي التي تحكم العلاقات بين الدول.

تأتي في مقدمة هذه القواعد نصوص ميثاق الأمم المتحدة، لاسيما الأحكام المتعلقة بحظر إستخدام القوة في العلاقات الدولية وحظر اللجوء إلى العدوان

(أحكام الفصل السابع من الميثاق، أي المواد من 39 إلى 51)، وكذا واجب احترام سيادة الدول واستقلالها السياسي والإقليمي (مبادئ ومقاصد الأمم المتحدة). بالإضافة إلى أحكام إتفاقية فيينا لقانون المعاهدات لعام 1969...الخ.

جاءت أحكام قواعد دليل (Tallinn) 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.[23]

كما نصت القاعدة رقم 2 المتعلقة بالإختصاص، بأن تمارس الدولة إختصاصها على الأشخاص الممارسين للأنشطة السيبرانية داخل إقليمها الوطني، بينما شددت القاعدة 4 على أن أي تدخل لدولة ما، في المنشآت السيبرانية لدولة أخرى يعد خرقا لسيادتها، وفي هذا السياق، جاءت القاعدة 6 من الدليل، لتحذر من أن الدول تتحمل المسؤولية القانونية عن أنشطتها السيبرانية التي تخرق بموجبها أي إلتزام دولي.[24]

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 167/68، حيث طلبت الجمعية العامة من المفوضة السامية لحقوق الإنسان إعداد تقرير عن الحق في الخصوصية في العصر الرقمي، إذ تناول التقرير بالبحث، وفقا لنص القرار: "حماية الحق في الخصوصية وتعزيزه في سياق المراقبة الداخلية والخارجية للاتصالات الرقمية و/أو اعتراضها وجمع البيانات الشخصية." حيث قدَم التقرير إلى مجلس حقوق الإنسان في دورته السابعة والعشرين وإلى الجمعية العامة في دورتها التاسعة والستين.[25]

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؟ [26].

إستثنت اللجنة الدولية للصليب الأحمر في تقريرها عام 2015 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 طريق التجسس والحصل على الإذن بالدخول للبيانات، المستهدفة عن طريق إختراق ذلك الجهاز أما الإستثناء الثاني فيتعلق بتشويش الإتصالات اللاسلكية والبث التلفزيوني فلم يتم إعتباره من قبيل الهجوم الوارد في القانون الدولي الإنساني[27] .

الخاتمة:

تتحدى التكنولوجيات الحديثة المفاهيم القانونية القائمة، حيث تتدفق المعلومات والإتصالات بسهولة أكبر من جميع أنحاء العالم، ولم تعد الحدود عائقا أمام هذا التدفق، فضلا عن أن المجرمين ما فتئوا يتواجدون في أماكن غير تلك التي تنتج فيها أفعالهم آثارها، ومع ذلك، تظل القوانين الوطنية محصورة بشكل عام في إقليم معين لهذا، ينبغي أن يوفر القانون الدولي الحلول للمشاكل المطروحة، مما يستلزم إعتماد صكوك قانونية دولية ملائمة. وفي هذا الإطار، تهدف إتفاقية الجريمة الإلكترونية – بودابست 2001- إلى رفع هذا التحدي، مع إبلاء الإحترام الواجب لحقوق الإنسان في مجتمع المعلومات الجديد.

نخلص في الختام إلى أن الهجمات السيبرانية التي تقع بين الدول لها طبيعة قانونية خاصة، تحكمها قواعد القانون الدولي المتعلقة بتنظيم العلاقات بين الدول، كتلك التي تلزم الدول على إحترام سيادة الدول وتحرم إستخدام القوة في العلاقات الدولية وتحظر أي شكل من أشكال العدوان.

فضلا عن كون الجريمة السيبرانية لا يمكن أن تنطبق على مثل هذه الوقائع على إعتبار أن الدولة لا يمكن تجريمها جنائياعلى غرار باقي الأشخاص

الطبيعية والأشخاص المعنوية الأخرى كالشركات وغيرها، وبالتالي يستلزم البحث عن تكييف آخر.

كما لا يمكن أن نكيف هذا النوع من الهجمات بكونه حروب سيبرانية لأن قواعد القانون الدولي ذات الصلة (أحكام دليل تالين Manuel de Tallinn لعام 2013)، تشترط وجود نزاع مسلح تقليدي كي نستطيع تسمية هذه الهجمات بالحروب السيبرانية.

الهوامش:

1- تم هذا الهجوم بإستخدام فيروس(Stuxnet) ، الذي يسميه البعض بالصاروخ الإلكتروني للدلالة على الحرب السيبرانية، حول هذه المسألة، راجع على سبيل المثال:

2 -- Mostefa Chaouche, Croiserie aux vents du Web Editions Publibook, Paris, 2013.

حول هذه المسألة، راجع على سبيل المثال: **عبد الفتاح بيومي حجازي**، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر 2002.

3 - Comité international de la Croix-Rouge, Pas de vide juridique dans le cyberespace , Interview avec CordulaDroege, conseillère juridique au CICR, le 16-08-2011, Comité international de la Croix-Rouge, voir le lien, https ://www.icrc.org/fre/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm, dernière visite du site,23.02.2017 à 10 h et 03 minutes. **CordulaDroege** définit la cyber crime comme suit : « nous entendrons par guerre cybernétique, les moyens et méthodes de guerre qui s'appuient sur la technologie de l'information – ou cyber-technologie –, et qui sont utilisés dans le cadre d'un conflit armé au sens du droit international humanitaire, par opposition aux opérations militaires cinétiques traditionnelles »

4- حول جهود الأستاذين **"ريتشارك كلارك"** و**"روبرتكناكي"**، راجع: المجال الخامس.. الحروب الإلكترونية في القرن الـ21، موقع الجزيرة للدراسات، متاح على الرابط التالي: http://studies.aljazeera.net/issues/2010/2011721227434686 8.htm، آخر زيارة بتاريخ: 2015/10/25، على الساعة: 22:40.

الشأ ن: **عادل عبدالصادق**، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، المركز العربي لأبحاث الفضاء الالكتروني، مصر، 2018، ص 53.

5- شادي عبد الوهاب منصور، حروب الجيل الخامس: أساليب "التفجير من الداخل" على الساحة الدولية، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة – مصر، 2019، ص 101.

6- يحي مفرح الزهراني، الأبعاد الإستراتيجية والقانونية للحرب السيبرانية، مجلة البحوث والدراسات، جامعة الوادي، العدد 23، السنة 2017، ص ص 225-248، ص.241.

7- شادي عبد الوهاب منصور، نفس المرجع، ص 102.

8- Conseil de l'Europe, Convention sur la cybercriminalité, adopté à Budapest le 23.11.2001, voir le lien http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_fr.pdf, dernière visite du site, 09.02.2017 à 15 h et 33 minutes

9- للإطلاع أكثر، راجع: **أحمد زهران،** موسوعة نظم وأساليب الحرب الحديثة، الطبعة الأولى، مطابع الأهرام التجارية، مصر، 1989. وراجع كذلك: **حيدر رندة،** السلاح السيبراني في حروب إسرائيل المستقبليّة، مؤسسة الدراسات الفلسطينية، بيروت – لبنان، 2018.

10- يعد الأمن الإلكتروني للدولة جزء لا يتجزأ من أمنها القومي، لاسيما ما تعلق منه بأنظمة المعلومات الخاصة بالقطاعات الحساسة.

11 - Shin, Beomchul, The Cyber Warfare and the Right of Self – Defense: Legal
Perspectives and the Case of the United States, IFANS, Vol.19, No1, June 2011, p.104

نقلا عن**: أحمد عبيس نعمة الفتلاوي،** الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي، كلية القانون، جامعة بابل، 2015.
http://www.law.uokufa.edu.iq/staff/ahmedonn/files/researches/%D8%A8%D8%AD%D8%AB%20%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9.pdf

12- أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مرجع سابق، متاح على الرابط التالي:
http://www.law.uokufa.edu.iq/staff/ahmedonn/files/researches/%D8%A8%D8%AD%D8%AB%20%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9.pdf

13 - Thomas Rid and Peter Mcburney,"Cyber – Weapons", Routledge publisher, The RUSI Journal, February –March, 2012, Vol.157.NO.1.p.3.

نقلا عن: **أحمد عبيس نعمة الفتليوي**، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مرجع سابق.

14- يحي مفرح الزهراني، الأبعاد الإستراتيجية والقانونية للحرب السيبرانية، نفس المرجع، ص.241.، راجع كذلك: **جوناثان الفورد**، تأثير التكنولوجيا العسكرية الحديثة، مركز الدراسات العسكرية، ترجمة: بيطار جبرئيل، مركز الدراسات العسكرية، دمشق- سوريا، 1983.

15- إيهاب خليفة، تأثير الثورة الصناعية الرابعة على الأمن القومي: مجتمع ما بعد المعلومات، د. ر. ط،العربي للنشر والتوزيع، القاهرة – مصر، 2019، ص136 وص115، راجع كذلك في هذا الشأن: **مارك مازيتي**، حروب الظل، الحروب السرية الأمريكية الجديدة، ترجمة: أنطوان باسيل، الطبعة الثالثة، شركة المطبوعات، بيروت – لبنان، 2016.

16- إيهاب خليفة، نفس المرجع،ص123.

17- pour plus de détails, voir ; **Laura Baudin,** les Cyber - attaques dans les conflits armés : qualification juridique, imputabilité et moyens de réponse envisagés en droit international humanitaire, L'harmattan , Paris, 2014.

18- اللجنة الدولية للصليب الأحمر، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟ الأسئلة الشائعة، اللجنة الدولية للصليب الأحمر، بتاريخ 28-06-2013، متاح على الرابط التالي:

https://www.icrc.org/ara/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm، آخر زيارة للموقع يوم: 2017/03/16،على الساعة: 10 ساو 00 د. راجع كذلك في هذا الشأن:

Mamadou Mouth Bane, le Crime organisé dans le Sahel: l'utilisation du numérique et les politiques de prévention, éditions L'Harmattan, 2019.

19- Franz-Stefan Gady and Greg Austin," Russia, The United States, And Cyber Diplomacy Opening the Doors", The East West Institute, Printed in the United States,2010,p.1

- نقلا عن: **أحمد عبيس نعمة الفتليوي**، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مرجع سابق.

20- Conseil de l'Europe, préambule de la Convention sur la cybercriminalité, adopté à Budapest le 23.11.2001, voir le lien http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_fr.pdf, dernière visite du site, 09.02.2017 à 15 h et 33 minutes

21- للإطلاع أكثر، راجع:**عادل عبد الصادق،** أسلحة الفضاء الالكتروني في ضوء القانون الدولي الإنساني، المركز العربي لأبحاث الفضاء الالكتروني، مصر 2018، راجع كذلك: **محمد سعادي،** أثر التكنولوجيا المستحدثة على القانون الدولي العام، دار الجامعة الجديدة، الإسكندرية – مصر، 2014.

22- See The Tallinn Manual's Rule 30, North Atlantic Treaty Organization, Tallinn Manual on the Jnternatonal Law applicable to Cyber Warfare, NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, UK, 2013, pp.15-18

23- Idem.

24- الأمم المتحدة، الحق في الخصوصية في العصر الرقمي، الأمم المتحدة: حقوق الإنسان، مكتب المفوض السامي، متاح على الربط التالي:
http://www.ohchr.org/AR/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx، آخر زيارة للموقع يوم: 2017/03/11، على الساعة: 05 سا و26 د.

25- يحي مفرح الزهراني، الأبعاد الإستراتيجية والقانونية للحرب السيبرانية، المرجع السابق، ص.242.

26- يحي مفرح الزهراني، الأبعاد الإستراتيجية والقانونية للحرب السيبرانية، نفس المرجع، ص.242.

27- يحي مفرح الزهراني، الأبعاد الإستراتيجية والقانونية للحرب السيبرانية، نفس المرجع، ص.243.

قائمة المراجع:

أولا: المراجع باللغة العربية.

ا)- الكتب:

1- أحمد زهران، موسوعة نظم وأساليب الحرب الحديثة، الطبعة الأولى، مطابع الأهرام التجارية، مصر، 1989.

2- إيهاب خليفة، تأثير الثورة الصناعية الرابعة على الأمن القومي: مجتمع ما بعد المعلومات، د. ر. ط، العربي للنشر والتوزيع، القاهرة – مصر، 2019.

3- جوناثان الفورد، تأثير التكنولوجيا العسكرية الحديثة، مركز الدراسات العسكرية، ترجمة: بيطار جبرئيل، مركز الدراسات العسكرية، دمشق- سوريا، 1983.
4- حيدر رندة، السلاح السيبراني في حروب إسرائيل المستقبليّة، مؤسسة الدراسات الفلسطينية، بيروت – لبنان، 2018.
5- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، 2002.
6- شادي عبد الوهاب منصور، حروب الجيل الخامس: أساليب "التفجير من الداخل" على الساحة الدولية، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة – مصر، 2019.
7- محمد سعادي، أثر التكنولوجيا المستحدثة على القانون الدولي العام، دار الجامعة الجديدة، الإسكندرية – مصر، 2014.
8- مارك مازيتي، حروب الظل، الحروب السرية الأمريكية الجديدة، ترجمة: أنطوان باسيل، الطبعة الثالثة، شركة المطبوعات، بيروت – لبنان، 2016.
9- عادل عبد الصادق، أسلحة الفضاء الالكتروني في ضوء القانون الدولي الإنساني، المركز العربي لأبحاث الفضاء الالكتروني، مصر 2018.

II)- المقالات:

1-- يحي مفرح الزهراني، الأبعاد الإستراتيجية والقانونية للحرب السيبرانية، مجلة البحوث والدراسات، جامعة الوادي، العدد 23، السنة 2017، ص ص 225-248.

III)- الإتفاقيات والمواثيق والإعلانات الدولية

1- ميثاق الأمم المتحدة، المعتمد بتاريخ 22 جوان 1945.
2- إتفاقية بودابست المتعلقة بالجريمة الإلكترونية، مجلس أوروبا، مجموعة المعاهدات الأوروبية، رقم 185، المعتمدة بتاريخ 23 نوفمبر2001.
3- إتفاقية الإتحاد الإفريقي المتعلقة بالجريمة السيبرانية وحماية المعطيات ذات الطابع الشخصي، المبرمة بتاريخ 2014/06/27.

IV)- **القوانين والتشريعات الوطنية.**

1- قانون 04-15، مؤرخ في 27 رمضان عام 1425، الموافق 10 نوفمبر سنة 2004، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 جوان سنة 1966، والمتضمن قانون العقوبات، الجريدة الرسمية، العدد 71 بتاريخ 10 نوفمبر 2004، ص.8.

2- قانون 09-04، مؤرخ في 14 شعبان عام 1430 الموافق 5 أوت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47 بتاريخ 16 أوت 2009، ص.5.

V)- **المصادر الإلكترورنية.**

1- أحمد عبيس نعمة الفتليوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي، كلية القانون، جامعة بابل، 2015، متاح على الرابط التالي:
http://www.law.uokufa.edu.iq/staff/ahmedonn/files/researches/%D8%A8%D8%AD%D8%AB%20%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9.pdf

2- الأمم المتحدة، الحق في الخصوصية في العصر الرقمي، الأمم المتحدة: حقوق الإنسان، مكتب المفوض السامي، متاح على الربط التالي:
http://www.ohchr.org/AR/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx، آخر زيارة للموقع يوم: 2017/03/11، على الساعة: 05 ساو 26 د.

3- بدون إسم، المجال الخامس..الحروب الإلكترونية في القرن الـ21، موقع الجزيرة للدراسات، متاح على الرابط التالي: http://studies.aljazeera.net/issues/2010/20117212274346868.htm، آخر زيارة بتاريخ: 2015/10/25، على الساعة 22:40.

ثانيا: المراجع باللغة الأجنبية

I- **Ouvrages**

1- Laura Baudin, les Cyber - attaques dans les conflits armés : qualification juridique, imputabilité et moyens de réponse envisagés en droit international humanitaire, L'harmattan, Paris, 2014.

2- Mamadou Mouth Bane, le Crime organisé dans le Sahel: l'utilisation du numérique et les politiques de prévention, éditions L'Harmattan, 2019.

3- Franz-Stefan Gady and Greg Austin," Russia, The United States, And Cyber Diplomacy Opening the Doors", The East West Institute, Printed in the United States, 2010.

4- Mostefa Chaouche, Croiserie aux vents du Web Editions Publibook, Paris, 2013.

5- NATO, Tallinn Manual's Rule 30, North Atlantic Treaty Organization, Tallinn Manual on the Jnternatonal Law applicable to Cyber Warfare, NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, UK, 2013.

Perspectives and the Case of the United States, IFANS, Vol.19, No1, June 2011.

6- Shin, Beomchul," The Cyber Warfare and the Right of Self – Defense:Legal

7- Thomas Rid and Peter Mcburney,"Cyber – Weapons", Routledge publisher, The RUSI Journal, February –March, 2012, Vol.157.NO.1, 2012.

8- Comité international de la Croix-Rouge, Pas de vide juridique dans le cyberespace, Interview avec Cordula Droege, conseillère juridique au CICR, le 16-08-2011, Comité international de la Croix-Rouge, voir le lien, https ://www.icrc.org/fre/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm, dernière visite du site,23.02.2017 à 10 h et 03 minutes.

9- Conseil de l'Europe, Convention sur la cybercriminalité, adopté à Budapest le 23.11.2001, voir le lien http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_fr.pdf, dernière visite du site, 09.02.2017 à 15 h et 33 minutes.