الحروب السيبرانية وأثرها على حقوق الإنسان: دراسة على ضوء أحكام دليل «تالين»

درويش سعيد
أستاذ مساعد (ب) ومحامي،
كلية الحقوق جامعة أمحمد بوقرة- بومرداس

مقدمة :

أدى التطور الكبير في الأسلحة ووسائل الحرب وما يترب عنها من خسائر فادحة في أرواح ومعدات الجيوش التقليدية، إضافة إلى التقدم المتسارع لتكنولوجيا الإعلام والاتصال وعلى رأسها تقنية الأنترنت وشبكات التواصل الاجتماعي العملاقة، وظهور ما يسمى بالمجتمعات والحكومات الإلكترونية، إلى بروز نوع جديد وغير مألوف من الحروب، يدعى «الحرب السيبرانية» (cyber war) أو (guerre cybernétique) أي الحرب الإلكترونية، حيث لجأت العديد من الدول في شكل سباق «تسلح إلكتروني» جديد،[1] إلى تطوير قدراتها القتالية في الفضاء السيبراني، لاسيما بعد الهجوم الإلكتروني الذي شنته روسيا ضد إستونيا عام 2007، والذي تسبب في شلل تام للدولة ومرافقها العسكرية والحكومية الحيوية، حيث أعتبر آنذاك أول هجوم إلكتروني تشنه دولة ضد دولة أخرى.

ثم توالى بعد ذلك لجوء الدول إلى الهجمات الإلكترونية، كتلك التي نفذتها روسيا أيضا عام 2008 ضد جورجيا، وهجوم كل من إسرائيل والولايات المتحدة الأمريكية سنة 2009 ضد منشأة « بوشهر» النووية الإيرانية بواسطة فيروس staxnet، الذي يسميه بعض العسكريون بالصاروخ الإلكتروني، وذلك نظرا للخصائص التدميرية المشتركة بينهما.

1 - قامت الجزائر أيضا في نهاية عام 2009، بتكوين أول دفعة «لإدارة الحرب الالكترونية» بمدرسة الإشارة بتيارت.

وبالرغم من التغيرات الجذرية التي طرأت على بنية الحرب الكلاسيكية، وطبيعتها القانونية المقسمة إلى نزاع مسلح دولي وآخر غير دولي، وأحيانا إلى حرب أهلية، إلا أن لجوء الدول إلى استخدام القوة الإلكترونية (electronic power)، في تزايد مستمر، وذلك لما توفره هذه الأخيرة من جهد ومال، كالتقليل من تكلفة الحروب والنزاعات المسلحة، نتيجة سهولة استخدام الأسلحة الإلكترونية، مثل الفيروسات وبرامج التجسس، وقرصنة المعلومات العسكرية والاستراتيجية.

فضلا عن تحقيق الأهداف المسطرة في ظرف وجيز، وكذا الدمار الهائل الذي تتسبب فيه تلك الأسلحة، حيث يرى البعض أن حجم الدمار الذي تلحقه الأسلحة «السيرانية» يضاهي الدمار الذي تحدثه أسلحة الدمار الشامل المعروفة، عن طريق ضرب البنية التحتية العسكرية الإلكترونية للدول، وشل كل مظاهر الحياة فيها، كمحطات الكهرباء والسدود والبنوك وسائر فروع الاقتصاد الأخرى.

ونتيجة لما سبق، تثور عدة تساؤلات حول مسألة حماية حقوق الإنسان ومن ثم المدنيين أثناء الحروب السيبرانية، وذلك بسبب كون ميدان هذا النوع من الحروب يختلف عن ميدان الحروب التقليدية، حيث التواجد المكثف للمدنيين على شبكة الأنترنت، وعلى اعتبار أن مستخدمي الفضاء السيبراني للأغراض العسكرية لا يقتصر فقط على الجيوش الإلكترونية، وإنما يتعدى ذلك إلى الأفراد العاديين كرواد الأنترنت من مستخدمي شبكات التواصل الاجتماعي.

كما تثور أيضا مسألة شرعية استهداف القراصنة الإلكترونيين، الذين يشنون هجمات ضد منشآت الدولة العسكرية، أو ضد شبكات الأنترنت التي تتحكم في تسيير الأعيان المدنية، كشبكات الكهرباء والسدود والمستشفيات...الخ، باعتبار أن تصرفهم يدخل ضمن «الإرهاب الإلكتروني».

ونظرا لقصور القانون الدولي في هذا المجال، نتيجة عدم وجود أي أساس قانوني يحكم اللجوء إلى الحرب الإلكترونية أو ينظم سير العمليات العدائية أثناءها، لذلك، تكمن أهمية هذا البحث في كونه يعالج موضوع حديث لا يزال في طور التبلور، لا سيما بعد استحداث صك قانوني يدعى دليل «تالين» (Manuel de Tallinn)، الذي أعدته

مجموعة من خبراء القانون الدولي بدعوة من حلف شمال الأطلسي «ناتو»، قصد دراسة مدى إمكانية تطبيق قواعد القانون الدولي الإنساني على الحروب السيبرانية.

وبالتالي، تهدف هذه الورقة البحثية إلى معالجة محتوى دليل «تالين» الذي يجيب على أهم النقاط الحساسة ذات الصلة بالحروب والهجمات الإلكترونية التي تنفذها الدول، أو تلك التي تقوم بها جهات فاعلة من دون الدول (Entités non étatiques)، كقواعد الاشتباك الإلكتروني وصفة المقاتل الإلكتروني، وإمكانية مراعاة مبادئ القانون الدولي الإنساني المعروفة كمبدأ التمييز مثلا، ومدى شرعية استهداف المقاتل الإلكتروني بالوسائل العسكرية المادية، كالطائرات العسكرية من دون طيار (armed drones).

ونظرا لتزايد تأثير التكنولوجيات الحديثة لاسيما الفضاء السيبراني على وضعية حقوق الإنسان ومن ثم الأمن الدولي، لذلك من الأهمية بمكان، تبيان موقف الأمم المتحدة أيضا وأجهزتها المختلفة ذات الصلة بحقوق الإنسان، إزاء لجوء الدول إلى الحروب السيبرانية، أو استخدام القوة الإلكترونية بذريعة الدفاع الشرعي عن النفس أو محاربة الإرهاب، وكذا رؤية ميثاق الأمم المتحدة لمسألة حفظ السلم والأمن الدوليين التي يمكن أن تثيرها تلك التهديدات[2]

ولمعالجة الموضوع وفق المنهج الاستقرائي الموائم لطبيعة البحث، نطرح الإشكالية التالية: ما مفهوم الحرب السيبرانية ؟ وفيم تتمثل آثارها على مسألة حقوق الإنسان؟ وما هو الأساس القانوني لحماية حقوق الإنسان في ظل هذه الحرب ؟ إن الإجابة عن التساؤلات المطروحة أعلاه، يقتضي إتباع الخطة التالية:

2 - في هذا السياق، صرحت السيدة «لويد لانجاميني» رئيسة مديرية الاتجار غير المشروع والجريمة المنظمة لدى مكتب الأمم المتحدة لمكافحة المخدرات والجريمة بأن: «هجمات الفضاء الإلكتروني أصبحت تشكل تهديدا حقيقيا لأمن الدول والأفراد»، حول هذه المسألة أنظر: مركز أنباء الأمم المتحدة، الأمم المتحدة وشركاؤها يركزون على جهود مكافحة جرائم الفضاء الإلكتروني، متاح على للرابط التالي: http://www.un.org/arabic/news/story.asp?NewsID=23351#.VztdkDWL-TIU، آخر زيارة للموقع بتاريخ: 12/04/2016، على الساعة 22 سا و32 د.

المبحث الأول: ماهية الحرب السيبرية

المطلب الأول: مفهوم الحرب السيبرية

المطلب الثاني: الطبيعة القانونية للحروب السيبيرية

المبحث الثاني: حقوق الإنسان خلال الحرب السيبرية

المطلب الأول: آثار الحرب السيبرية على حقوق الإنسان

المطلب الثاني: الأساس القانوني لحماية حقوق الإنسان خلال الحرب السيبرية

المبحث الأول: ماهية الحرب السيبرية

المطلب الأول: مفهوم الحرب السيبرية

الفرع الأول: تعريف الحرب السيبرية

لتعريف الحرب السيبرية، لابد من تعريف الفضاء السيبرانى، حيث عرفه قاموس أوكسفورد بأنه:" البيئة الافتراضية التي يتم عبرها اتمام عملية الاتصال عبر شبكات الكمبيوتر". و استنادا إلى هذا التعريف البسيط، يمكن اعتبار الحروب السيبرانية كشكل من أشكال الصراع ذات الأهداف السياسية، التي تقع داخل البيئة.[3]

وعلى الرغم من محاولات الخبراء و الدول والمنظمات الدولية إيجاد تعريف موحد للحرب السيبرانية، إلا أنه حتى الآن لم يتم الإستقرار على تعريف عام شامل لها، فبالنسبة للولايات المتحدة والناتو، يتم التركيز على الجانب الاقتصادي و المادي لأوجه الحرب السيبرانية، على عكس دول منظمة شنغهاي للتعاون التي تحاول الدفع بتعريف يتضمن أوجه السيادة الوطنية، والحفاظ على الحدود والهوية الثقافية للشعوب كأهداف للصراع في الفضاء السيبرانى.[4]

إلا أن تعريف مجموعة الخبراء التابعين للناتو في القاعدة 30 من دليل «تالين» (Manuel de Tallinn) المتعلق بتطبيقات القانون الدولي في مجالات الصراع والحروب السيبرانية ينص على أنها : " كل العمليات السيبرانية سواء كانت دفاعية أو هجومية، والتي يعتقد أنها قد تسبب إصابات أو وفيات للبشر، أو تلف وضرر للأشياء المادية".[5]

يبدو أن تعبير «الحرب السيبرانية» يُستخدم من قبل فئات عديدة من الناس للإشارة إلى أشياء مختلفة. ويُستخدَم المصطلح هنا للإشارة إلى وسائل وأساليب القتال

3 - محمد فخرالدين، حدود المجال الخامس – ما هى الحروب السيبرانية ؟، مؤتمر حروب الفضاء السيبراني، 15 /05 /2015، بحث متاح على الرابط التالي: https://seconf.wordpress.com/2015/05/15/، آخر زيارة للموقع بتاريخ: 12 /02 /2017، على الساعة: 18 سا و 5 د.

4 - نفس المرجع.

5 - نفس المرجع.

التي تتألف من عمليات في الفضاء الإلكتروني ترقى إلى مستوى النزاع المسلح أو تُجرى في سياقه، ضمن المعني المقصود في القانون الدولي الإنساني.[6]

كما يعرفها بعض الباحثين على أنها حرب جديدة تشهدها الدول الكبرى على مستوى دوائر القرار والشركات الضخمة. تَتَداخل فيها الأهداف العسكريَّة بالأهداف الاقتصاديَّة، أو ما يُعرَف بالتجسُّس الصناعي. ميدان هذه الحرب الشبكات العنكبوتيَّة التي باتَت تُسيطر على العالم الافتراضي، وجنودها هم خُبراء في علم الكمبيوتر والإنترنت، أذكياء في قدرتهم على اختراق الحواجز الأمنيَّة للمعلومات السريَّة لدى الخصم أو المُنافس، وقرصنتها.[7]

ولعلَّ أفضل تعريف مُبسَّط للحرب السيبرانيَّة هو ذلك الذي يَعتبرها مجموعة الأعمال العدائيَّة المُوجَّهة ضدَّ مُعطيات الدولة الإلكترونيَّة المُخزَّنة أو المُعالجة أو المُتبادلة من حاسوب إلى آخر بهدف كَشْفِها أو نَسْخِها أو تعديلها أو إتْلافِها أو عرقلة تدفُّقها (كالهجوم على أنظمة المُراقبة الجويَّة، وأنابيب نقل الغاز والبترول، والمفاعلات النوويَّة.[8]

الفرع الثاني: خصائص الحرب السيبرية

تثير الحرب السيبرية عدة صعوبات وإشكالات قانونية تجعل تطبيق القانون الدولي الإنساني أمرا صعبا، ومن أبرز هذه الإشكالات أن تشن الحرب السيبرية ضمن

6 - اللجنة الدولية للصليب الأحمر، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟ الأسئلة الشائعة، مقابلة مع السيد «لوران جيزيل» المستشار القانوني باللجنة الدولية للصليب الأحمر بتاريخ، 28 /06 /2013، متاحة على الرابط التالي: https://www.icrc.org/ara/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm، آخر زيارة للموقع بتاريخ 12 /02 /2017، على الساعة: 13 سا و54 د.

7 - طارق المجذوب، السَّايْبِر ساحة «خِفِيَّة» لحربٍ «ناعِمِة» قادِمة، الدفاع اللبناني، بحث متاح على الموقع التالي:
https://www.lebarmy.gov.lb/ar/content، آخر زيارة للموقع بتاريخ 16 /02 /2017، على الساعة: 22 سا و 01 د.

8 - نفس المرجع.

نزاع مسلح، أي ضرورة وجود نزاع مسلح سواء كان دولي أم غير دولي (conflit armé international ou non international)[9]، حيث أن الممارسة الدولية أثبتت أن الدول تنفذ الهجمات السيبرية بمعزل عن النزاع المسلح.

إضافة إلى ميدان المعركة، حيث تشن الحرب السيبرية في الفضاء السيبري الإلكتروني، الذي لا يعترف بالحدود الدولية، فبالرغم من أن القاعدة 21 من دليل «تالين» (Tallinn) الخاصة بالحدود الجغرافية، تنص على أن العمليات السيبرية تتم ضمن الحدود الجغرافية المنصوص عليها في القانون الدولي الإنساني، إلا أنه من الصعب تطبيق هذه القاعدة على أرض الواقع.

ونتيجة لذلك، فإن القتال بصورته الكلاسيكية، لا يمكن أن يجري إلا في مناطق معينة، ويميز بعض الفقهاء مثل (Oppenheim) في هذا الصدد، بين المنطقة الحربية (وهي المجال الذي يستطيع فيه المحاربون اعداد القتال وإنجازه)، وبين ساحة الحرب (وهي المكان الذي يجري فيه القتال فعليا).[10]

وعلاوة على ما سبق، وإجابة عن سؤال حول التحديات الأساسية التي تثيرها الحرب السيبرانية، أوضح المستشار القانوني للجنة الدولية للصليب الأحمر، بأنه يوجد فضاء إلكتروني واحد فقط تتقاسمه القوات المسلحة مع المستخدمين المدنيين، وكل شيء فيه متشابك ومترابط. وتتمثل التحديات الرئيسية في ضمان توجيه الهجمات ضد الأهداف العسكرية فقط، وتوخي الحرص بشكل مستمر لحقن دماء السكان المدنيين والبنية التحتية المدنية.[11]

كما تتميز الحرب السيبرية بنوعية الأسلحة التي يمكن استخدامها في القتال الإلكتروني، وفي هذا الصدد عرف دليل «تالين» (Tallinn) في القاعدة رقم 41 الأسلحة السيبرية، إذ صنف وسائل وطرق الحرب، بأنها تشمل من بين أمور أخرى: أسلحة

9 - تناول دليل «تالين» (Manuel de tallin) هذا التقسيم في القاعدتين 22 و23.

10 - شارل روسو، القانون الدولي العام، الأهلية للنشر والتوزيع، ترجمة شكر الله خليفة وعبد المحسن سعد، بيروت – لبنان، 1987، ص 347

11 - اللجنة الدولية للصليب الأحمر، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟ الأسئلة الشائعة، مرجع سابق.

وأساليب الحرب السيبرية الأخرى ذات الصلة، كالفيروسات والبرامج الخبيثة وأنظمة التجسس الإلكتروني...الخ. إضافة إلى مسألة المقاتل في الحرب الإلكترونية (Cyber-combattant)، وهل يمكن اعتبار القراصنة مقاتلين يمكن استهدافهم من قبل أطراف النزاع.

الفرع الثالث: الحرب السيبرية وشرط الهجوم الإلكتروني المسلح

يشترط في الحرب السبرية أن تتم عن طريق تنفيذ هجوم إلكتروني مسلح، ضمن وجود نزاع مسلح بمفهومه التقليدي، وهذا ما كرسته القاعدة 20 من دليل (Tallinn) المتعلقة بتطبيق قانون النزاع المسلح، حيث نصت على أن كل نشاط سيبري، ينبغي أن يخضع لقانون النزاعات المسلحة، لكنها اشترطت أن يتم ذلك في سياق نزاع مسلح، سواء كان دولي أو داخل الحدود الجغرافية للدولة، لذلك حددت القاعدة 26 من دليل «تالين» أعضاء القوات المسلحة، ونتيجة لذلك فإن المرتزقة في الفضاء الإلكتروني - حسب القاعدة 28 - لا يتمتعون بوضع المقاتل أو السجين.[12]

وتجدر الإشارة إلى غموض مفهوم الهجوم الإلكتروني المسلح وصعوبة تحديده من الناحية العملية، كما أن غموض مفهوم الهجوم هنا يؤدي إلى غموض الأهداف المشروعة أيضا، فالهجمات الإلكترونية تستهدف الشبكة الالكترونية العسكرية لجيش الدولة المعادية، لكن أحيانا يتم هذا الهجوم خارج النزاع المسلح ومن طرف أشخاص غرباء عن أطراف النزاع، ومن ثم تثور مسألة مشروعية الهدف في مثل هذه الحالة.

الفرع الرابع: الحرب السيبرية كنتيجة لتطور الحكومات والمجتمعات الإلكترونية

من أبرز العوامل التي أدت إلى ظهور الحرب السيبرية، هو التطور الكبير التي تشهده تكنولوجيا وسائل الاتصال[13]، والتي بدورها أفرزت مجتمعا جديدا يدعى بـ: المجتمع

12 - See The Tallinn Manual, 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

13 - أنظر على سبيل المثال: محمد سعادي، أثر التكنولوجيا المستحدثة على القانون الدولي العام، دار الجامعة الجديدة، 2014

الإلكتروني» نتيجة تأثير تقنية الأنترنت وشبكات التواصل الاجتماعي، وهذا ما أدى بالعديد من الدول إلى تبني التسيير الإداري الإلكتروني، أي «الحكومات الإلكترونية»، وهذا ما سهل للجميع من شن الهجمات عبر الفضاء الافتراضي، نظرا للانتشار الكبير لشبكة الأنترنت في العالم.

وقد زادت المصالح الاقتصادية للدول الكبرى والأطماع التوسعية والرغبة في الهيمنة على الدول الأخرى بوسائل غير تقليدية، إلى تبني الحرب السيبرية باعتبارها الوسيلة المثالية لتحقيق تلك الأهداف بأسهل وأسرع الطرق، مع تجنيبها الخسائر البشرية في صفوف القوات المسلحة التي لا غنى عنها في حالة الحرب الكلاسيكية التي تستخدم فيها وسائل الحرب الكلاسيكية كالجنود والطائرات والدبابات وغيرها.

المطلب الثاني: الطبيعة القانونية للحروب السيبرية

الفرع الأول: التعريف بدليل «تالين»

دليل «تالين»(Manuel de Tallinn)، هو وثيقة قانونية أعدها مجموعة من الخبراء تحت إشراف منظمة حلف شمال الأطلسي، (OTAN) وبمساللجنة الدولية للصليب الأحمر(CICR)، تتضمن قواعد القانون الدولي المطبقة أثناء الحروب السيبرية، يتكون من 95 قاعدة، حيث يعرف الحرب الإلكترونية أو الحرب السيبرية بأنها كل نشاط سيبري سواء كان هجومي أو دفاعي، يهدف إلى جرح أو قتل الأشخاص أو تخريب أو تدمير الممتلكات.[14]

ونظرا للماضي الطويل للجنة الدولية للصليب الأحمر في مجال القانون الدولي الإنساني، ولسمعتها واهتمامها أيضا بمجال الأسلحة، وتخوفها من التحديات التي أفرزتها التكنولوجيا العسكرية، لاسيما الأسلحة ذاتية التشغيل، لذلك كانت من بين المشاركين الفاعلين في إعداد دليل «تالين» (Manuel de Tallinn) عام 2013، والذي يعد الصك الدولي الوحيد الذي ينظم مثل هذه الهجمات

.

14 - The Tallinn Manual, Op. Cit.

الفرع الثاني: التكييف القانوني للحرب السيبرية وفقا لقواعد دليل «تالين»

نظرا لغموض الحرب السيبرية ليس من حيث مفهومها الذي يتداخل مع عدة مفاهيم أخرى كالحرب الإلكترونية وغرها، وإنما يمتد هذا الغموض حتى من الناحية الواقعية، إذ يشترط دليل «Tallinn» على سبيل المثال أن يتم هذا النوع من الحرب ضمن نزاع مسلح بمفهومه التقليدي، وهنا تثور عدة تساؤلات عن التكييف القانوني للهجمات السيبرية الأخرى التي تنفذها بعض الدول خارج وجود النزع المسلح، هل هو حرب سيبرية؟ أم جريمة إلكترونية دولية، أم شيء آخر؟. لذلك، تبرز مسألة صعوبة تكييف الهجمات السيبرية التي تشن بمعزل عن وجود نزاع مسلح، [15]

الفرع الثالث: الحرب السيبرية صورة من صور الجريمة الإلكترونية

تعدّت الهجمات السيبرانية وجهتها الأساسية، التي كانت تهدف إلى سرقة بيانات لتتمكن من سرقة أموال بطريقة سهلة وسلسة، وأصبحت ذات طابعٍ سياسي، تهدف إلى نشر الخوف والإرهاب في بعض الأحيان، أو إلى تثبيت القدرات في أحيانٍ أخرى.[16]

وبالتالي نَلمس يوما بعد يوم توجُّهًا دوليًا بارزًا نحو تجاوز عصر الجريمة الإلكترونيَّة (كعصابات الجريمة المُنظَّمة وقراصنة الكومبيوتر) إلى الإرهاب السيبراني وجرائم الإنترنت التي ترعاها دول شغوفة بجني أعظم الفوائد التجاريَّة أو العسكريَّة. ومن المُحتمل أنْ تتوسَّع الحرب السيبرانيَّة وتَتَجذَّر أكثر فأكثر، لاسيما بعد تطوُّر وسائل الاتصالات ووسائطها ساهَم في زَعْزَعَة الوظيفة التوجيهيَّة للدولة في كل ما يتعلَّق بالتحكُّم بالفضاء السيبراني.[17]

15 - حول هذه المسألة راجع: أحمد عبيس نعمة الفتليوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مقال منشور بمجلة المحقق الحلي، كلية الحقوق - جامعة الكوفة، 2016صر ص 16-15، متاح على الرابط التالي:
http://www.law.uokufa.edu.iq/staff/ahmedonn/files/researches

16 - إيهاب شوقي، الحرب السيبرانية...حرب المستقبل المفزعة، مرجع سابق.

17 - طارق المجذوب، السَّايْبِر ساحة «خِفِيَّة» لحربٍ «ناعِمة» قادِمة، مرجع سابق.

حيث أضحى مفهوم الحدود السياسيَّة والجغرافيَّة، وكذلك مفهوم السيادة ومفهوم الاستقلال عن الآخرين، من المفاهيم الغابِرة التي لا يُمكن الاعتداد بها. وبعد التحدِّي الاقتصادي والتحدِّي الرقمي، يُطالعنا التحدِّي الأمني. فالتطور التكنولوجي قلب مفهوم الأمن الوطني التقليدي رأسًا على عقب، لأنَّ وجود الفضاء السيبراني غيَّر من أنماط العلاقات الدولية وقواعد الحرب. وبنتيجة ذلك لم يَعُد للحدود حُرْمَة أو أهميَّة، ولم يَعُد خطر التدمير محليًّا يقتصر على أطراف النزاع، بل يُمكن أنْ يمتد إلى دول عَبَرت شبكاتها الوطنيَّة البرامج المعلوماتيَّة الخبيثة.[18]

الفرع الرابع: الحرب السيبرية والجيل السادس للحرب

يصنف البعض الطبيعة القانونية للحروب السيبرية ضمن الحروب «الذكية»، أو الجيل السادس من الحروب.[19] وذلك بعد تراجع الحروب الكلاسيكية لاسيما مع بداية الألفية الأولى من القرن الواحد والعشرين وبداية استخدام الطائرات العسكرية من دون طيار (Drones Armés) لضرب الجماعات المسلحة في نزاعات مسلحة لا تناظرية (Guerre asymétrique).

يتمثل الجيل الأول منه في الحروب التقليدية، والجيل الثاني هي حرب العصابات، أما الجيل الثالث فتتمثل في الضربات الاستباقية، وتتمحور حروب الجيل الرابع في الحرب على الارهاب، وصلا إلى الجيل الخامس الذي يستخدم التقنيات المؤامراتية التي تهدف الي إيجاد حكومة في الظل, أما الجيل السادس من الحروب فأول من أطلقته روسيا، وهي الحرب التي تدارعن بعد من خلال استخدام الأسلحة الذكية، وتهدف إلي تأليب المجتمع من خلال التجنيد الكامل لشبكات الإنترنت الذي يهدف الي هدم أركان الدولة وإفشالها.[20]

18 - نفس المرجع.

19 - أول من استخدم هذا المصطلح هو الجنرال الروسي (Vladimir Slipchenko)، وذلك في أعقاب حرب الخليج، للدلالة على الحروب الجديدة التي تستخدم وسائل تكنولوجية، كالفضاء الالكتروني الذي يتيح للمقاتلين من خوض الحرب عن بعد.

20 - حول هذه المسألة أنظر: هالة عصام الدين، أجيال الحروب، مقال منشور بجريد الأهرام، عدد46437، مؤرخ في 26/01/2014، متاح على الرابط التالي: http://www.ahram.org.eg/

لكن الأمر ليس بجديد، فبعد الانتهاء من عصر الحروب الكيميائية والفيزيائية دخل العالم في مرحلة التوظيف الذكي للتكنولوجيا، أو ما يطلق عليه بحروب الجيل السادس تفاديا للخسائر المادية والبشرية المباشرة، وتتخذ هذه الحروب أشكال عدة، فقد استطاعت الدول الغربية والمتقدمة تطوير آليات الجيل السادس من الحروب، بجيش من العلماء والباحثين في المجالات العلمية والمختلفة.[21] حتى صرنا في زمن الفاعلين الإلكترونيين (cyber actors)، والمقاتل السيبري (cyber combattants).

وحول خطورة هذا النوع من الحرب، أعلن قائد شعبة الاستخبارات العسكرية الإسرائيلية الجنرال، «أفيف كوخافي»، في المؤتمر السنوي لـ"مركز دراسات الأمن القومي" أن "حرب السايبر" باتت، في نظره، أهم من اكتشاف البارود. وأكد أن مجال حرب السايبر مازال في البداية، وأن هناك تطورات خطيرة تنتظره في المستقبل، مؤكدا على الطفرة التي أحدثتها حرب السايبر حيث كان يلزم في الماضي لجمع معلومات استخباراتية مثلاً عشرة أشخاص، أما الآن وبعد التطور في هذا المجال، يمكننا أن نقوم بتلك المهمة من خلال شخص واحد فقط.[22]

المبحث الثاني: حقوق الإنسان خلال الحرب السيبرية

المطلب الأول: آثار الحرب السيبرية على حقوق الإنسان

الفرع الأول: الآثار السلبية من خلال استهداف البنى التحتية الإلكترونية للأعيان المدنية

يشبه البعض حروب الفضاء «السيبراني» بأسلحة الدمار الجديدة، وذلك

News، آخر زيارة للموقع بتاريخ: 03/02/2017، على الساعة 13 سا و 18 د.

21 - مرفت بنت عبدالعزيز العريمي، الحروب الذكية ومستقبل شعوب العالم الثالث قراءات ومداولات، متاح على الرابط التالي:
http://www.raialyoum.com/?p=559609، آخر زيارة للموقع بتاريخ: 03/02/2017، على الساعة 15 سا و 43 د.

22 - إيهاب شوقي، الحرب السيبرانية...حرب المستقبل المفزعة، مرجع سابق.

لاعتبارات عدة، أهمها أن الفضاء «السيبراني» أصبح يستخدم في شتى مظاهر الحياة في الدولة، السياسية، الأمنية، الاقتصادية، والتجارية، كما أن البنى التحتية الإلكترونية المدنية غالبا ما ترتبط بنظيرتها العسكرية عن طريق شبكة الأنترنت.[23] فاستهداف نظم المواصلات إذن وشبكات الكهرباء والسدود والمستشفيات، والمنشآت الكيميائية أو النووية، من أهم الآثار السلبية التي تثيرها والهجمات «السيبرانية» وحروب الفضاء الإلكتروني (Cyber Attack أوAttaques Cybernétique)، وبالتالي فإن احتمال اختراق المنظومة الالكترونية للمفاعلات النووية قد يتسبب في كوارث مروعة بحيث يصعب التحكم في آثارها البشرية والبيئية.

كما أن سهولة ولوج شبكة الأنترنت وإتاحتها للجميع، يمكن للقراصنة أو الجهات الفاعلة من غير الدول (Entités non étatiques)، كالجماعات الإرهابية مثلا، أن تشن هجمات على دولة معينة، يمكن أن تتسبب في تدميرها اقتصاديا وعسكريا، لاسيما وأن الفضاء الالكتروني يتميز بكونه لا يعترف بتعداد الجيوش ولا بسيادة أو حدود الدول، فيمكن لشخص بسيط وبمفرده في أقصى مكان من الأرض، أن يشن هجوما مدمرا على دولة معينة.

وفي هذا الصدد، يساور اللجنة الدولية قلق بشأن الحرب السيبرانية بسبب ضعف الشبكات الالكترونية والتكلفة الإنسانية المحتملة من جراء الهجمات السيبرانية. فعندما تتعرض الحواسيب أو الشبكات التابعة لدولة ما لهجوم أو اختراق أو إعاقة، قد يجعل هذا الأمر المدنيين عرضة لخطر الحرمان من الاحتياجات الأساسية مثل مياه الشرب والرعاية الطبية والكهرباء. وإذا تعطلت أنظمة تحديد المواقع GPS عن العمل،

23 - حول هذه المسألة: راجع: تقرير اللجنة الدولية للصليب الأحمر عن القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، ورقة مقدمة أثناء أشغال المؤتمر الدولي الثاني والثلاثون للصليب الأحمر والهلال الأحمر بعنوان: (قوة الإنسانية) جنيف، سويسرا، 8 - 10 ديسمبر 2015، وثيقة رقم: IC/15xxx/32، متاح على شبكة الأنترنت على الرابط:
https://www.icrc.org/ar/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts آخر زيارة للموقع يوم 12/10/2016، على الساعة: 13 سا و 34 د

قد تحدث إصابات في صفوف المدنيين من خلال تعطيل عمليات إقلاع مروحيات الإنقاذ على سبيل المثال.[24]

الفرع الثاني: الآثار الإيجابية من خلال الحد من جرائم الحروب الكلاسيكية

من أبرز ايجابيات الحرب السيبرية، الأهداف غير البشرية للهجمات، وبالتالي تقلل من عدد الضحايا الذين، حيث يقدرعدد القتلى مثلا في الحربين العالميتين الأولى والثانية فقط بحوالي: 97 مليون قتيل، اي ما يعادل 6 % من سكان العالم آنذاك، إضافة إلى الجرحى والمرضى والمشردين واللاجئين، وكذا التدمير الذي يطال البنى التحتية والأعيان المدنية وغيرها....الخ.

لذلك، استهل ميثاق الأمم المتحدة في ديباجته بالإشارة إلى ضرورة إنقاذ البشرية من ويلاتها، حيث نصت القرة 2 من الديباجة على : «...أن ننقذ الأجيال المقبلة من ويلات الحرب التي في خلال جيل واحد جلبت على الإنسانية مرتين، أحزاناً يعجز عنها الوصف».

وفي هذا الصدد، أوضحت لائحة الجمعية العامة للأمم المتحدة رقم 70 /23 (2015)، الصادرة في 23 /12 /2015، المتضمنة للتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، من أن التطبيقات العسكرية للتطورات العلمية والتكنولوجية يمكن أن تسهم إسهاما كبيرا في تحسين وتطوير منظومات الأسلحة المتطورة، ولا سيما أسلحة الدمار الشامل. وبالتالي رفع مستوى التهديدات التي قد تمس بالأمن والسلم الدولي.

وفي إجابة عن سؤال حول إمكانية استخدام التكنولوجيا السيبرانية بشكل إيجابي أثناء النزاعات المسلحة، أجا المستشار القانوني اللجنة الدولية للصليب الأحمر (CICR)، بأن الأمر يقع على عاتق الدول أثناء سير العمليات الحربية، حيث تلتزم بتجنب الإصابات

24 - اللجنة الدولية للصليب الأحمر، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟ الأسئلة الشائعة، مرجع سابق.

العرضية في صفوف المدنيين[25] والإضرار بالبنية التحتية المدنية أو الحد منها على أقل تقدير. ودون التقليل من شأن التحديات، لا يمكن للمرء استبعاد إمكانية أن يؤدي التطور التكنولوجي في المستقبل إلى تطوير أسلحة سيبرانية من شأنها التسبب في إصابات وأضرار عرضية أقل من الأسلحة التقليدية في ظروف معينة، وذلك لتحقيق الميزة العسكرية نفسها.[26] علاوة على أنه يمكن استخدام الفضاء السيبري ورواده كشهود رقميين عن الجرائم التي يمكن ارتكابها في حق المدنيين.[27]

الفرع الثالث: الحرب السيبرية والجريمة الدولية

تعد الحرب السيبرية مجالا مناسبا لارتكاب الجريمة الدولية أو الحديث عنها، لكونها لا تعترف بالحدود الدولية، حيث من السهل ارتكاب أي جريمة دون مراعاة حدود الزمان والمكان. ولا الجهة التي تقف وراء الهجوم، من دول أو كيانات من غير دول، كالمنظمات الإرهابية أو القراصنة.

بيد أن مسألة تحديد هوية المهاجم في حالة الحرب السيبرية من أبرز العوائق القانونية التي تحول دون قيام المسؤولية الدولية، سواء أكانت جنائية أم مدنية، ولذلك نظرا لكون أغلب الهجمات السيبرية التي تم تنفيذها، كانت مجهولة المصدر، ومن ثم يثور تساؤل حول من يتحمل المسؤولية الجنائية؟ في حالة ارتكاب انتهاكات لحقوق الإنسان، والتي نص عليها دليل «تالين» (Manuel de Tallinn) في القاعدة 24.

ونتيجة لما سبق، يمكن تحديد القصد الجنائي للمهاجم، ففي حالة القرصان الإلكتروني على سبيل المثال، يمكن معرفة ما إذا كان تنفيذ الهجوم تم بدافع الفضول، أم له نوايا ودوافع عدوانية. لذلك تحذر اللجنة الدولية للصليب الأحمر من غموض

25 - تناول دليل «تالين» (Manuel de Tallinn) في القاعدة 29، والتي نصت على أن المدنيين يضلون تحت الحماية طالما لم يشاركوا في العمليات العدائية التي تتم في الفضاء السبيري.

26 - اللجنة الدولية للصليب الأحمر، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟ الأسئلة الشائعة، مرجع سابق.

27 - حول هذه المسألة، راجع على سبيل المثال: هند الحناوي، مبرمجون للحرب: تخيل مستقبل الصراع المسلح، مجلة حركة الصليب الأحمر والهلال الأحمر الدولي، العدد 1، 2014 ، ص 10

مفهوم الهجوم في مسألة الأسلحة المستخدمة في الفضاء السيبيراني، وذلك نظرا للآثار التي يرتبها هذا المفهوم، أبرزها مسألة إعلان الحرب (Indictio belli)، الذي يعد ضروريا في القانون الدولي الإنساني العرفي، خاصة عند اللجوء إلى الحرب او ما يعرف بـ: (Jus ad bellum)، إضافة إلى أهمية مفهوم المهاجم في تحديد المراكز القانونية لبعض أشخاص القانون الدول الأخرى، كالدول المحايدة والأحلاف العسكرية الحليفة أم المعادية...الخ.

كما أن معرفة هوية المهاجم تسمح بإمكانية متابعته عن الجرائم الجسيمة التي يخلفها الهجوم السيبري، سواء أمام القضاء الوطني أو أمام المحكمة الجنائية الدولية وفقا لنظام روما الأساسي لعام 1998، وذلك على أساس ارتكاب جرائم حرب أو جرائم ضد الإنسانية.[28] أو مخالفة أعراف الحرب بصفة عامة، وفي هذا الصدد يقول الأستاذ (Charles Rousseau)، بأن التصرف العادل في الحرب من بين الشروط الواجب استيفاءها في إطار نظرية الحرب العادلة.[29]

الفرع الرابع: المسؤولية الدولية عن الجرائم المرتكبة أثناء الحرب السيبرية

نص دليل «تالين» (Manuel d Tallinn) على المسؤولية القانونية للدولة عموما في القاعدة 6 منه، حيث حمل الدولة المسؤولية الدولية عن العمليات السيبرية المسندة لها، والتي تمثل انتهاكا لالتزاماتها الدولية، لاسيما العمليات السيبرية المنفذة انطلاقا من بناها التحتية السيبرية (القاعدة 7)، لكن ما يميز المسؤولية الدولية عن الجرائم

28 - لا سيما الفقرة 2 (ب) (20) من المادة 8 من نظام روما الأساسي للمحكمة الجنائية الدولية المعتمد في 17/07/1998، المتعلقة بجرائم الحرب، التي تنص على أن :» استخدام أسلحة أو قذائف أو مواد أو أساليب حربية تسبب بطبيعتها أضرارا زائدة أو آلاما لا لزوم لها، أو تكون عشوائية بطبيعتها بالمخالفة للقانون الدولي للمنازعات المسلحة، بشرط أن تكون هذه الأسلحة والقذائف والمواد والأساليب الحربية موضع حظر شامل وأن تدرج في مرفق لهذا النظام الأساسي، عن طريق تعديل يتفق والأحكام ذات الصلة الواردة في المادتين 121 ، 123».

29 - شارل روسو، مرجع سابق، ص 337، حول وجوب استجابة الأسلحة لقواعد حقوق الإنسان، أنظر:

-Stuart Casey-Maslen, Weapons under International Human Rights Law, Cambridge University Press (CUP), Cambridge, 2014

المرتكبة أثناء الحرب السيبرية هو غموض الأساس الذي يمكن أن تبنى عليه، أي هل تؤسس على نظرية المخاطر أم على أساس العمل غير المشروع، إضافة إلى تشتت المسؤولية الدولية عن مثل هذه الجرائم، إذ من الصعب أيضا – كما هو الحال بالنسبة للمسؤولية الجنائية – اسناد العمل العدائي لدولة معينة، وذلك نظرا للسرية التامة التي تنفذ بها هذه الهجمات.

فلقيام المسؤوليَّة الدوليَّة في هذا المجال، لابد من توفر 3 شروط رئيسية وهي: وجود ضرر، ناجِم عن عمل غير مشروع، ارتكبته دولة مُعيَّنة. وتنتفي المسؤوليَّة إذا كان الضرر نتيجة قوَّة قاهرة، أو خطأ ارتكبته الدولة التي أصابها الضرر، كما أن النشاط الناجم عن استخدام الفضاء السيبراني، والمُسبِّب للضرر، قد يكون مشروعًا، غير أنه لاعتبار استخدام هذا الفضاء عملاً مشروعًا، لا بد من توفر شروط أيضا.[30]

كما أن الجهة التي يمكن أن يرفع أمامها النزاع الذي يمكن أن يثور بمناسبة تنفيذ هجوم إلكتروني من طرف دولة معينة ضد دولة أخرى، هل هو مجلس الأمن الدولي (Conseil de Sécurité)، وفقا للقاعدة 18 من دليل «تالين» (Manuel de Tallinn)، الخاصة بمجلس الأمن الدولي، أو باعتباره الهيئة المختصة بالحفاظ على السلم والأمن الدوليين، أن المسألة تتعلق بشن حرب على دولة، أم أن محكمة العدل الدولية (Cour Internationale de Justice) هي الجهة المختصة دون غيرها بالنظر في هذا النزاع، على اعتبار أن المسألة تتعلق بترتيب المسؤولية الولية، والتعويض عن الأضرار التي تلحق بالدولة المضرورة.

المطلب الثاني: الأساس القانوني لحماية حقوق الإنسان خلال الحرب السيبرية

الفرع الأول: دليل «تالين» كصك وحيد منظم للحرب السيبرية

نظرا لقصور القانون الدولي في مجال الحرب السيبرية، نتيجة عدم وجود أي أساس قانوني ينظم اللجوء إلى الحرب الإلكترونية، أو ينظم سير العمليات العدائية

30 - طارق المجذوب، السَّايْبِر ساحة «خِفِيَّة» لحربٍ «ناعِمِة» قادِمة، مرجع سابق.

أثناءها، لذلك تم ابرام صك قانوني عام 2013 يدعى دليل « تالين» (Manuel de Tallinn)، الذي أعدته مجموعة من خبراء القانون الدولي بدعوة من حلف شمال الأطلسي «ناتو»، قصد دراسة مدى إمكانية تطبيق قواعد القانون الدولي الإنساني على الحروب السيبيرية، وذلك على إثر الهجوم الإلكتروني الشامل الذي شنته روسيا ضد إستونيا عام 2007. وقد نص الدليل في القاعدة 10 على مبدأ حظر استخدام القوة من طرف دولة ضد المنشئات السيبرية لدولة أخرى، ولذلك تكريسا لمبدأ حظر استخدام القوة المحرم دوليا. أما القاعدتين 13 و16 فقد تضمنتا على التوالي مسألتي الدفاع الشرعي عن النفس الفردي والجماعي، وذلك ردا على أي عدوان سيبري.

يتفق معدو دليل «تالين» (Manuel de Tallinn)، بأن قواعد القانون الدولي الإنساني تطبق أثناء الحروب السيبرية، إلى جانب اتفاقيات جنيف لعام 1949 وبروتوكولاتها الإضافية لعام 1977، لاسيما إذا شنت هذه الأخيرة ضمن نزاع مسلح، سواء كان دولي أم غير دولي (داخلي). بينما يرى البعض منهم بأن تطبيق القانون الدولي الإنساني على الحروب السيبرية، يكون في حالة ما إذا كان للهجوم أغراض عسكرية فقط، وليس مجرد أعمال قرصنة فقط ضد مواقع مدنية.

إلاَّ أنَّ عدم تنظيم استخدام الفضاء السيبري لا يعني تركه لمشيئة المُحاربين، فهناك أحكام عامَّة تفرضها قواعد الأخلاق ومبادئ الإنسانيَّة وتُطبَّق على أي عمليَّة حربيَّة. وهناك أيضًا نصوص مُدوَّنة بشأن الحرب الجويَّة والبريَّة والبحريَّة. تُلائم طبيعة الحرب السيبرانيَّة ويُمكن أنْ تُطبَّق عليها. واستنادًا إلى هذه الأحكام والنصوص نستطيع أنْ نتحدَّث عن القواعد المهمَّة لاستخدام الفضاء السيبري. فاللجوء إلى الفضاء السيبري لابُدَّ، إذًا، أنْ يكون مُتوافقًا، بدايةً، مع حق اللجوء إلى الحرب (أي الحالة التي يُسمح فيها للدولة باستعمال القوّة (Jus ad bellum)، كما يجب أنْ يكون استعمالها، بعد ذلك، مُستندًا إلى حقوق الإنسان والقانون الدولي الإنساني (أي القانون الذي يُنظِّم حالة الحرب).[31]

31 - نفس المرجع.

الفرع الثاني: قواعد القانون الدولي الإنساني

إضافة إلى قواعد دليل «Tallinn» المتعلقة بقواعد القانون الدولي المطبقة على الحروب السيبرية التي تشن أثناء النزاعات المسلحة، لابد من تطبيق أيضا قواعد ومبادئ القانون الدولي الإنسان، لاسيما العرفية منها، كشرط «مارتنز» (Clause de Martenz)، والمبادئ العرفية الأخرى، كمبدأ التمييز والتناسب والضرورة العسكرية.... الخ، على اعتبار أن تلك القواعد آمرة (Jus Cogens) أو ملزمة للجميع (Erga Omnes). والتي أدرجت مؤخرا ضمن قواعد دليل «Tallinn» الذي تضمن في القاعدة 20 مسألة تطبيق قانون النزاعات المسلحة على الحروب السيبرية، أما القاعدة 14 فقد خصصت للحديث عن مبدئي الضرورة والتناسب، كماحظر مثلا من خلال القاعدة 32 مهاجمة المدنيين، كما تضمنت القاعدة 37 حظر مهاجمة أغراض المدنيين من أعيان ومعدات... الخ.

كما تطبق أيضا المادة 3 المشتركة لاتفاقيات جنيف لعام 1949، إضافة لأحكام البروتوكولين الإضافيين الأول والثاني لعام 1977 المتعلقين على التوالي بحماية المدنيين أثناء النزاعات المسلحة الدولية، وحمايتهم أثناء النزاعات المسلحة غير الدولية.

زيادة على ما سبق، فإن تطبيق القانون الدولي الإنساني في الحرب السيبرية يهدف إلى الحد من استخدام هذه الأسلحة السيبرية عندما لا تكون مشروعة، فتقييم مشروعية الأسلحة الجديدة بصفة عامة يصب في مصلحة كافة الدول، حيث أنه يساعدها في ضمان توافق سلوك قواتها المسلحة مع الالتزامات الدولية. وتُلزم المادة 36 من البروتوكول الإضافي الأول لعام 1977، كل دولة من الدول الأطراف التحقق من امتثال أي أسلحة جديدة تقوم بنشرها، أو تدرس مسألة نشرها لقواعد القانون الدولي الإنساني، وهذه نقطة أخرى استحضرها دليل «تالين» على نحو مفيد.[32]

32 - اللجنة الدولية للصليب الأحمر، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟ الأسئلة الشائعة، مرجع سابق.

الفرع الثالث: قواعد القانون الدولي لحقوق الإنسان

القاعدة العامة هي أن تطبق القواعد الأساسية لحقوق الإنسان في جميع الحالات، من بينها الحرب السيبرية، كالحق في الحياة المكرس في جميع الصكوك الدولية لحقوق الإنسان أبرزها المادة 3 من الإعلان العالمي لحقوق الإنسان الصادر بتاريخ: 10 /12 /1948، والحق في الخصوصية والحياة الخاصة وفقا للمادة 12، [33] لاسيما وأن الهجمات السيبرية في الكثير من الأحيان تستهدف الحسابات الخاصة بالأفراد، كما حدث مع المترشحة السابقة للبيت الأبيض هيلاري كلينتون (Hillary Clinton) عام 2016، حيث تم استهداف بريدها الإلكتروني من طرف روسيا.

بالإضافة إلى حماية حقوق الانسان المدنية والسياسية، المكرسة في العهد الدولي الخاص بهذه الحقوق لعام 1966، حيث نصت الفقر 1 من المادة 6 على أن: « الحق في الحياة حق ملازم لكل إنسان. وعلى القانون أن يحمى هذا الحق، ولا يجوز حرمان أحد من حياته تعسفا» [34]وكذا حماية الجيل الثاني من حقوق الانسان وهي الحقوق الاقتصادية والاجتماعية والثقافية، التي تضمنها العهد الدولي المتعلق بالحقوق الاقتصادية والاجتماعية والثقافية لعام 1966، من خلال المادة 15، والذي نصت أيضا الفقرة 1 من المادة 5 منه على سبيل المثال على أنه: « ليس في هذا العهد أي حكم يجوز تأويله على نحو يفيد انطواءه على أي حق لأي دولة أو جماعة أو شخص بمباشرة أي نشاط أو القيام بأي فعل يهدف إلى إهدار أي من الحقوق أو الحريات المعترف بها في هذا العهد أو إلي فرض قيود عليها أوسع من تلك المنصوص عليها فيه».

33 - تنص المادة 3 من الإعلان العاملي لحقوق الإنسان على أن: « لكل فرد الحق في الحياة والحرية وسلامة شخصه»، أما المادة 12 فتنص على أنه:» لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات.»

34 - كما نصت الفقرة 1 من المادة 9 من نفس العهد على : « لكل فرد حق في الحرية وفى الأمان على شخصه، ....»، أما الفقرة 2 من المادة 5 فقد تضمنت: « لا يقبل فرض أي قيد أو أي تضييق على أي من حقوق الإنسان الأساسية المعترف أو النافذة في أي بلد تطبيقا لقوانين أو اتفاقيات أو أنظمة أو أعراف، بذريعة كون هذا العهد لا يعترف بها أو كون اعترافه بها في أضيق مدى»

الفرع الرابع: أحكام ميثاق الأمم المتحدة

يتضمن ميثاق الأمم المتحدة قواعد وأحكام عامة ذات الصلة بحماية حقوق الإنسان يمكن تطبيقها أثناء الحرب السيبرية، كمحتوى مبادئ ومقاصد الميثاق مثلا، التي تحظر استخدام القوة في العلاقات الدولية، [35] وحق الدول في الدفاع الشرعي عن النفس وفقا للمادة 51 في حالة العدوان، وباقي العمليات العدائية الأخرى، التي تستوجب اتخاذ تدابير المنع والقمع التي نص عليها الفصل السابع من الميثاق أي المواد (من 39 إلى 51)، وقد نص «دليل تالين» (Tallinn) على الإجراءات المضادة التي يمكن للدولة القيام بها ردا على هجوم سيبري لدولة أخرى في القاعدة 9.

بالإضافة إلى ضرورة احترام سيادة الدول، وما أصبح يعرف بـ:» الحدود الإلكترونية» أو « السيادة الإلكترونية» (la souveraineté cybernétique)، المنصوص عليها في القاعدة رقم 1 من دليل «تالين» (Manuel de Tallinn)، أي سلامة التي البنى التحتية السيبرية للدولة من الهجمات الإلكترونية، سواء من قبل الدول، أو حتى تلك التي تشن من طرف الكيانات من غير الدول (Entités non Etatiques).

فالتطوُّرات العلميَّة التي تَسمح باستخدام الفضاء السيبراني، وبعُبور شبكة الاتِّصالات الوطنيَّة أحيانًا، تَجعل من الصعب، عمليًا، مُمارسة السيادة الوطنيَّة على هذا المجال السيبراني، وإخضاعه أو إخضاع أيِّ جزء منه للتشريعات أو المُراقبة المحليَّة.[36]

كما أن الهجمات والحروب السيبرية أصبحت تهدد السلم والأمن الدوليين، من خلال المساس بـ«الأمن السيبري الدولي» المعتمد عليه في التجارة الدولية وفي العديد من مجالات العلاقات الدولية، لذلك من واجب المجتمع الدولي تفعيل أحكام ميثاق الأمم المتحدة ذات الصلة، بغية صيانة السلم والأمن الدولي. وفي هذا الصدد يرى المختصون

35 - تنص القرة 4 من المادة 2 من ميثاق الأمم المتحدة على أنه: «يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد «الأمم المتحدة»..»

36 - طارق المجذوب، السَّايْبِر ساحة «خِفِيَّة» لحربٍ «ناعِمة» قادِمة، مرجع سابق.

أن المعلومات في هذا العصر، توازي المال والذهب من حيث القيمة، لذلك يجب تأمينها بأفضل الطرق.[37]

ونتيجة لما سبق، حذرت الأمم المتحدة في مناسبات عدة المجتمع الدولي، من خطورة الحرب السيبرية ومن النتائج التي يمكن أن تتسبب فيها، وذلك من خلال لوائح الجمعية العامة رقم 61 /55 (2006)، المؤرخة في 06 /12 /2006، المتعلقة بدور العلم والتكنولوجيا في سياق الأمن الدولي ونزع السلاح، ولائحتها رقم 70/213 (2015)، المؤرخة في 22 /12 /2015، المتعلقة بتسخير العلم والتكنولوجيا والابتكار لأغراض التنمية.

37 - إيهاب شوقي، الحرب السيبرانية...حرب المستقبل المفزعة، مرجع سابق.

خاتمة:

في الختام نخلص إلى أن الحرب السيبرانية أو الإلكترونية ظهرت كنتيجة لتطور الوسائل التكنولوجيا المختلفة لاسيما وسائل الإعلام والاتصال، وكذا اعتماد العديد من دول العالم لنمط التسيير الإلكتروني أو ما يطلق عليه «بالحكومات الإلكترونية»، ما جعل الحرب السيبرانية تتسم بطابع خاص بالمقارنة بالحروب الكلاسيكية أو بنظرية النزاع المسلح، التي تقسم النزاعات المسلحة بصفة عامة، الى نزاعات مسلحة دولية وأخرى غير دولية.

وقد لجأت بعض الدول الكبرى إلى شن هجمات سيبرانية على البنى التحتية لدول تراها معادية، حيث تكبدت الدول المستهدفة خسائر مادية فادحة، إضافة إلى شن البنى التحتية الإلكترونية للأعيان المدنية الضرورية لحياة المدنيين.

ونظرا لخطورة هذا النوع من الحرب نتيجة سهولة شنها وآثارها الوخيمة على التمتع الكامل بحقوق الإنسان، لذلك تم الاتفاق في العاصمة الاستونية (Tallinn) على إعداد دليل «تالين» الخاص بتطبيق القانون الدولي على الحرب السيرانية، وبالرغم من أنه غير ملزم وأنه يشترط وجود نزاع مسلح لتطبيق القانون الدولي على هذا النمط الجديد من الحرب، إلا أنه يعد وثيقة مهمة تنظم هذا النوع من العمليات.

قائمة المراجع:

أولا: باللغة العربية:

- أحمد عبيس نعمة الفتليوي، الهجمات السيبرانية: مفهومها و المسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مقال منشور بمجلة المحقق الحلي، كلية الحقوق - جامعة الكوفة، 2016

- شارل روسو، القانون الدولي العام، الأهلية للنشر والتوزيع، ترجمة شكر الله خليفة وعبد المحسن سعد، بيروت – لبنان، 1987.

- محمد سعادي، أثر التكنولوجيا المستحدثة على القانون الدولي العام، دار الجامعة الجديدة، 2014

هند الحناوي، مبرمجون للحرب: تخيل مستقبل الصراع المسلح، مجلة حركة الصليب الأحمر والهلال الأحمر الدولي، العدد 1، 2014.

ثانيا: باللغات الأجنبية:

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

- Stuart Casey-Maslen, Weapons under International Human Rights Law, Cambridge University Press (CUP), Cambridge, 2014