ماهية الحرب الإلكترونية في ضوء قواعد القانون الدولي

سعيد درويش: أستاذ مساعد"ب"
كلية الحقوق، جامعة الجزائر 1

ملخص:

تهدف هذه الورقة البحثية إلى معالجة محتوى دليل "تالين"، الذي يجيب على أهم النقاط الأساسية ذات الصلة بالحروب والهجمات الإلكترونية التي تنفذها الدول، أو تلك التي تقوم بها جهات فاعلة من دون الدول، وكذا مفهوم النزاع المسلح في إطار الحرب الإلكترونية، بالإضافة إلى مفهوم الجيوش الالكترونية وكيفية إدارة الحرب الالكترونية، من خلال التطرق لقواعد الاشتباك الإلكتروني فضلا عن صفة المقاتل الإلكتروني، وأخيرا ضرورة مراعاة مبادئ القانون الدولي الإنساني المعروفة كمبدأ التمييز مثلا، ومسألة شرعية استهداف المقاتل الإلكتروني بالوسائل العسكرية المادية، كالطائرات العسكرية من دون طيار وغيرها.

الكلمات المفتاحية: ماهية - الحرب الإلكترونية - في ضوء - قواعد - القانون الدولي.

Summary :

The purpose of this research, is to study the content of the "Tallinn" Handbook, which addresses the most challenging questions, including those related to the rules of international law applicable in electronic warfare, as well as cyber attacks carried out by States, non-state actors.

This research has also for objective, to highlight related terms, such as the notion of armed conflict in the context of electronic warfare, as a cyber-fighter, cyber-actor, and the need to respect the principles of International humanitarian law during cyber war armed conflict.

Keywords: concept - electronic warfare - in light of the rules - of international law.

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 السيبيرية" (cyber war) أو (guerre cybernétique) أي الحرب الإلكترونية، حيث لجأت العديد من الدول في شكل سباق "تسلح إلكتروني" جديد، إلى تطوير قدراتها القتالية في الفضاء السيبيراني، 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 (stuxnet)، الذي يسميه بعض العسكريون بالصاروخ الإلكتروني، وذلك نظرا للخصائص التدميرية المشتركة بينهما.

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 "السيبيرانية" 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 المفهوم الواسع والضيق للحرب الإلكترونية، وتكييفها القانوني الصحيح في إطار القانون الدولي، ومدى قابلية الحروب الإلكترونية للتقسيم التقليدي للنزاعات المسلحة. [1] وكذا مسألة حماية حقوق الإنسان ومن ثم المدنيين

أثناء الحروب الإلكترونية، 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 السيبيراني 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 بعض الأعيان المدنية الضرورية لحياة المدنيين، كشبكات الكهرباء والسدود، البنوك والمستشفيات...الخ، باعتبار أن تصرفهم يدخل ضمن ما يسمى بـ: "الإرهاب الإلكتروني".

ونظرا لقصور القانون الدولي في هذا المجال، نتيجة عدم وجود أي أساس قانوني ينظم اللجوء إلى الحرب الإلكترونية أو ينظم سير العمليات العدائية 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.

تكن أهمية الموضوع في كونه يواكب التطور التكنلوجي الذي بدأ يسيطر على أغلب مفاصل الحياة اليومية، والذي يرافقه تحول عمل الدول والحكومات إلى نمط الحوكمة الإلكترونية مما يجعل هذا النوع من الحروب يمثل خطرا قد يقود الى شل عمل الحكومات.[2]

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)، كمفهوم النزاع المسلح في إطار الحرب الإلكترونية، وكذا مفهوم الجيوش الالكترونية وكيفية إدارة الحرب الالكترونية من خلال التطرق لقواعد الاشتباك الإلكتروني وصفة المقاتل الإلكتروني، إضافة إلى إمكانية مراعاة مبادئ القانون الدولي الإنساني المعروفة كمبدأ التمييز مثلا، ومدى شرعية استهداف المقاتل الإلكتروني بالوسائل العسكرية المادية، كالطائرات العسكرية من دون طيار(drones armés) .

ونظرا لتزايد تأثير التكنولوجيات الحديثة لاسيما الفضاء السيبيراني على وضعية حقوق الإنسان ومن ثم الأمن الدولي، لذلك كان من الأهمية بمكان، تبيان موقف الأمم المتحدة أيضا وأجهزتها المختلفة ذات الصلة بحقوق الإنسان، إزاء لجوء الدول إلى الحروب السيبيرية، 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 التهديديات

ولمعالجة الموضوع وفق المنهج الاستقرائي الموائم لطبيعة البحث، نطرح الإشكالية التالية:

كيف عالج دليل تالين مسألة الحرب الإلكترونية ؟ وما مدى شرعية استخدام القوة الإلكترونية (cyber power) في إطار ميثاق الأمم المتحدة ؟ وفيم تتمثل آثار الحروب السيبيرية على مسألة حقوق الإنسان ؟

إن الإجابة عن التساؤلات المطروحة أعلاه، يقتضي إتباع الخطة التالية:

المبحث الأول: تطبيق قواعد القانون الدولي الإنساني على الحرب الإلكترونية.

المطلب الأول: دليل "تالين" كأساس قانوني للحرب الإلكترونية.

المطلب الثاني: الحرب الإلكترونية وتغيير المفهوم التقليدي للحرب.

المطلب الثالث: الصراعات الإلكترونية الدولية وغير الدولية.

المبحث الثاني: ميثاق الأمم المتحدة واستخدام القوة الإلكترونية (cyber power).

المطلب الأول: ميثاق الأمم المتحدة واللجوء إلى الحرب الإلكترونية (jus ad bellum)

المطلب الثاني: الصراعات الإلكترونية وأثرها على السلم والأمن الدوليين.

المطلب الثالث: جهود المجتمع الدولي في تقنين قواعد الحرب الإلكترونية.

المبحث الأول: تطبيق قواعد القانون الدولي الإنساني على الحرب الإلكترونية

المطلب الأول: دليل "تالين" كأساس قانوني للحرب الإلكترونية

الفرع الأول: مبدأ التمييز بين الفاعلين الإلكترونيين (cyber actors)

دليل "تالين"(Manuel de Tallinn)، هو وثيقة قانونية 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.[3] ومعنى ذلك أن الهجوم السيبري الذي يعتد به في إطار قواعد القانون الدولي هو ذلك الذي يتم خلال نزاع مسلح.

وفي هذا الصدد، تتمثل التحديات الرئيسية في ضمان توجيه الهجمات ضد الأهداف العسكرية فقط، وتوخي الحرص بشكل مستمر لحقن دماء السكان المدنيين والبنية التحتية الضرورية لحياتهم. وهذا نتيجة وجود فضاء إلكتروني واحد تتقاسمه القوات المسلحة والجيوش الإلكترونية مع باقي المستخدمين المدنيين.[4] ولا شك أن التحدي الأكبر يكمن في مسألة التمييز بين الفاعلين الإلكترونيين (cyber actors)، أي بين ما يسمى بالمقاتل السيبري (cyber combattants-)، وبين المستخدمين الآخرين.

علاوة على ذلك، يحظر القانون الدولي أن تكون الإصابات العرضية المحتملة في صفوف المدنيين مفرطة مقارنة بالميزة العسكرية المباشرة والمتوقعة من الهجوم السيبري. فإذا لم تُستوفى هذه الشروط، لا ينبغي شن الهجوم. ويشترط دليل (Manuel de Tallinn) أن تتضمن الأضرار العرضية آثارا مباشرة أو غير مباشرة، وأن أي آثار غير مباشرة (متوقعة) ينبغي أن تُدرج في تقييم التناسب أثناء عملية التخطيط للهجوم وتنفيذه، وهي نقطة ذات صلة كبيرة بالفضاء الإلكتروني. وتؤكد هذه التحديات على أهمية توخي الدول الحذر الشديد عند اللجوء إلى الهجمات السيبرية.[5] وهذا ما نصت عليه القاعدة 14 من الدليل الخاصة بالضرورة العسكرية والتناسب، حيث شددت على أن استخدام القوة عن طريق الفضاء السيبري من طرف دولة ما في إطار الدفاع الشرعي عن النفس، ينبغي أن يستجيب لمبدئي الضرورة العسكرية والتناسب.

كما أفردت قواعد دليل "تالين" حماية خاصة - في إطار مبدأ التمييز – لفئات معينة من المدنيين، كالفرق الطبية عن طريق حماية حواسيبهم من الاستهداف ضد أي هجوم إلكتروني، من خلال القاعدة 71، وكذا حماية معدات أفراد الأمم المتحدة، باعتبارهم

محايدين ويتولون مهام إنسانية (القاعدة 74). وضرورة اختيار الأهداف بدقة أثناء الهجوم (القاعدة 56).

الفرع الثاني: قواعد الاشتباك الإلكتروني واحترام القانون الدولي الإنساني

قواعد الاشتباك في الحرب الإلكترونية الرقمية لم تتبلور حتى الآن، لكن هناك تساؤلات مهمة ينبغي أن تجيب عنها قواعد دليل (Manuel de Tallinn)، لتحديد استراتيجيات الرد العسكري وكيفية التعامل مع العدو، تتمثل هذه التساؤلات في الجهة التي تقرر وتحدد إذا كان بلد ما يتعرض لهجوم إلكتروني، أم أنها محاولات قرصنة عادية، غايتها التسلية وسرقة الحسابات من بعض الهواة والعابثين، وكذا حدود السيادة الوطنية للدولة في الحرب الإلكترونية، وما إذا كان الهجوم على مواقع إلكترونية لجهات مدنية تتبع مؤسسات الدولة، يعتبر هجوماً إلكترونياً ينبغي الرد الفوري عليه.[6]

بالإضافة إلى نطاق وحجم الهجوم الإلكتروني وأهدافه، كيفية التدرج في الرد، الرد الدبلوماسي إذا كان الهجوم مغطى من قبل حكومة خارجية، أو الرد الالكتروني لتدمير منظومة السلطة والسيطرة التي تتحكم بالهجوم الالكتروني، أو الرد العسكري المباشر في حال احتمال خسائر في الأرواح، كيفية إدارة عملية التنسيق فيما بين الأجهزة المخولة بالرد في الدولة، كأجهزة المخابرات وقوات الدفاع الإلكتروني في الجيش، لتنفيذ عمليات الهجوم أو الدفاع الرقمية أو إيقاف العمليات، وكيفية التأكد من أن العمليات حققت أهدافها المرسومة.[7]

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 حتى في حالة ما إذا كان للهجوم أغراض عسكرية، وليس مجرد أعمال قرصنة فقط ضد مواقع مدنية.

ومن بين أهم قواعد القانون الدولي الإنساني في إطار قواعد الإشتبك، أنه يقع على عاتق الدول أثناء سير العمليات الحربية الالتزام بتجنب الإصابات العرضية في صفوف المدنيين، وكذا الإضرار بالبنية التحتية المدنية أو الحد منها على أقل تقدير. ودون التقليل من شأن التحديات التي تثيرها الحروب الإلكترونية، فإنه لا يمكن استبعاد إمكانية أن يؤدي

التطور التكنولوجي في المستقبل، إلى تطوير أسلحة سيبرية من شأنها التسبب في إصابات وأضرار عرضية أقل من الأسلحة التقليدية، وذلك قصد تحقيق الميزة العسكرية نفسها. و في هذا الصدد ستواصل اللجنة الدولية للصليب الأحمر باعتبارها آلية لتطبيق القانون الدولي الإنساني، رصد التطورات التي يمكن أن تقع في مجال استحداث هذا النوع من الأسلحة.[8]

الفرع الثالث: حماية المدنيين والأعيان المدنية أثناء الصراع الإلكتروني

يحظر دليل Tallinnمن خلال القاعدة 32 مهاجمة المدنيين، كما تضمنت القاعدة 37 حظر مهاجمة أغراض المدنيين من أعيان ومعدات...الخ.[9] وفي هذا السياق، يساور اللجنة الدولية للصليب الأحمر قلق بشأن الحرب السيبرية، وهذا بسبب ضعف الشبكات الإلكترونية وسهولة اختراقها، وكذا بالنظر للتكلفة الإنسانية المحتملة من جراء الهجمات السيبرية. فعندما تتعرض الحواسيب أو الشبكات التابعة لدولة ما لهجوم أو اختراق أو إعاقة، قد يعرض المدنيين للخطر، ويحرمهم من الاحتياجات الأساسية مثل مياه الشرب والرعاية الطبية والكهرباء. كما أن تعطل أنظمة تحديد المواقع (GPS) عن العمل في بعض الدول، قد تحدث إصابات في صفوف المدنيين من خلال تعطيل عمليات إقلاع مروحيات الإنقاذ.[10]

فضلا عن إمكانية أن تتعرض خلال الهجوم السيبري، السدود والمحطات النووية وأنظمة التحكم في الطائرات، نظراً لاعتمادها على الحواسيب المرتبطة بالشبكات. حيث تكون هذه الأخيرة متداخلة إلى درجة يجعل من الصعب الحد من آثار هجوم سيبري ضد جزء من المنظومة، دون الإضرار بالأجزاء الأخرى، أو تعطيل المنظومة بأكملها. ونتيجة لذلك قد تتضرر مصالح مئات الآلاف من الناس وصحتهم وحتى حياتهم. وتذكر اللجنة الدولية جميع أطراف النزاع بتوخي الحرص بشكل مستمر من أجل حقن دماء المدنيين، وهو أحد أهم الأدوار التي تقوم بها، فالحروب لها قواعد وحدود تنطبق أيضا على اللجوء إلى الحرب السيبرية، بنفس القدر في حالة استخدام البنادق والمدفعية والصواريخ.[11]

المطلب الثاني: الحرب الإلكترونية وتغيير المفهوم التقليدي للحرب

الفرع الأول: الفضاء السيبري وميدان المعركة الإلكترونية:

ينص دليل "تالين" في القاعدة 21 الخاصة بالحدود الحدود الجغرافية، بأن النشاط السيبري يخضع للحدود الجغرافية المنصوص عليها في القانون الدولي المطبق أثناء النزاع المسلح، وهذا بالرغم من الصعوبات التي تنطوي عليها الهجمات الإلكترونية التي تجرى في الفضاء الإلكتروني (الافتراضي)، حيث من الصعب أن تصمد الحدود أمام تلك الهجمات.

وفي هذا الاتجاه، يتمسك "الدليل" بالثنائية التقليدية للنزاعات المسلحة الدولية والنزاعات المسلحة غير الدولية، ويقر بأن العمليات الإلكترونية وحدها قد تشكل نزاعات مسلحة تبعاً للظروف، لا سيما بالنظر للآثار المدمرة لتلك العمليات. وقد ثار نقاشا حول مفهوم "الضرر" في العالم الإلكتروني أثناء إعداد الدليل. وبعد مناقشات مكثفة، اتفق أغلب الخبراء على أنه علاوة على الضرر المادي، فإن توقف أحد الأعيان عن العمل قد يشكل ضرراً أيضاً. وهو الرأي أيضا الذي تبنته اللجنة الدولية للصليب الأحمر، حينما أقرت بأنه ليس مهما في حالة تعطل أحد الأعيان، البحث عن كيفية حدوث ذلك، سواء بوسائل عسكرية مادية أو عملية إلكترونية. وهذه القضية مهمة للغاية في الممارسة العملية، حيث أن أي عملية إلكترونية تستهدف تعطيل شبكة مدنية، سيشملها الحظر الذي يفرضه القانون الدولي الإنساني على الاستهداف المباشر للأشخاص المدنيين والأعيان المدنية.[12] 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.

الفرع الثاني: صفة المقاتل في الحرب الالكترونية:

من بين المسائل الشائكة التي لم يجمع عليها شراح القانون الدولي، هي المسائل الضرورية لتطبيق قواعد القانون الدولي الإنساني على الحرب الإلكترونية، والمتمثلة في بعض المفاهيم كالمقاتل السيبري (Cyber-combattant) أي من هو الشخص الذي يمكنه أن يشترك في العمليات العدائية، وكذا مفهوم الاشتباك الإلكتروني، بالإضافة إلى صعوبة تحديد المدنيين ضمن الفاعلين السيبريين (Les acteurs cybernétiques).

وبالتالي، تثور عدة تساؤلات بهذا الخصوص، لا سيما حول متى يصبح القرصان محارباً، ومتى تدخل المناورات الملتوية أو عمليات التجسس في الفضاء السيبري ضمن خانة «الاعتداء المسلح»، ومتى تصبح البرمجيات الخبيثة سلاحاً؟ بحسب تصنيف القانون الدولي؟[13] 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.[14]

الفرع الثالث: الأسلحة الإلكترونية في الحروب السيبرية

تتميز أسلحة حروب الفضاء الإلكتروني بخصائص تدميرية فريدة، حتى قال أحدهم أنه: "لا أعرف على وجه التحديد السلاح الذي سيستخدمه الإنسان في الحرب العالمية الثالثة،

لكني أعلم أنه سيستخدم العصي والحجارة في الحرب العالمية الرابعة".[15] لذلك عالج دليل "تالين" هذه المسألة في القاعدة رقم 41، حين عرف وسائل وطرق الحرب، بأنها تشمل أسلحة الحرب السيبرية والأساليب السيبرية الأخرى ذات الصلة.

فهي إذن أسلحة غير ملموسة، تهدف في مجملها إلى تدمير قدرات الخصم، أو حرمان المدنيين من الخدمة، كالبرامج الخبيثة، والقنابل المنطقية، وبرامج الخداع والتجسس كأحصنة طروادة، والتلاعب الرقمي وانتهى الى بيان خصائص تلك الأسلحة، ومن بين الأمثلة على ذلك، الهجوم الكوري على شركة (SONNY)، وكذا الحرب التي استهدفت البنى التحتية في استونيا والتي كانت أغلبها موجهه من روسيا، بالإضافة إلى الحرب الروسية الجورجية التي تزامنت فيها كل من الهجمات الإلكترونية والهجمات العسكرية التقليدية، مما خلق فعالية تدمير مزدوجة، وأخيرا الحرب التي استهدفت محطة "ناتانز" لتخصيب اليورانيوم في ايران.[16] باستخدام فيروس يدعى (stuxnet) حيث يشبه في قوته التدميرية الصاروخ العادي، لذا سماه البعض بالصاروخ الإلكتروني.

المطلب الثالث: الصراعات الإلكترونية الدولية وغير الدولية

الفرع الأول: الجيوش الإلكترونية واختراق الحدود الافتراضية

نص المبدأ الأول الخاص بالسيادة على أن الدولة تمارس رقابتها على المنشآت السيبرية وجميع الأنشطة ذات الصلة في إطار سيادتها الإقليمية. لكن الممارسة العملية تؤكد خلاف ذلك، وهذا بالنظر إلى الفضاء السيبري الشاسع، والذي يعد بمثابة ساحة للمعركة، بحيث تضطر الجيوش الإلكترونية في سبيل تنفيذ عملياتها السيبرية، إلى تخطي كل الحدود جوية كانت، أو برية، أو بحرية، وهذا ما يثير تساؤلات عديدة حل العلاقة الموجودة بين هذا النوع من الجيوش، وضرورة احترام سيادة الدول ومن ثم القانون الدولي.

وفي هذا السياق، يعبّر بعض العسكريون عن مخاوفهم من توسيع نطاق الحرب الرقمية، حيث يرى "كارل شراينر" وهو عميد في أكاديمية قيادة الجيش الألماني في هامبورغ، وأحد الأشخاص الذين يؤكدون على ضرورة تحديد «قواعد أخلاقية» لساحة المعركة على الإنترنت، أن وجود معيار دولي لاستعمال الأسلحة الرقمية أمر أساسي. وبالتالي، يجب أن يعيد القادة العسكريون النظر بأهم مسألة متعلقة بالدفاع في الفضاء الإلكتروني وهي هوية المعتدي، الذي عادة ما يكون خلف الحدود، (transnational)، وفي هذا الاتجاه نص «دليل تالين» بأنه: «في معظم الحالات، يمكن تحديد مصدر الاعتداءات

على البيانات». لكن ولسوء الحظ، لا ينطبق هذا الحكم مع تجارب عدد من خبراء أمن تكنولوجيا المعلومات، الذين يرون عكس ذلك.[17]

تجدر الاشارة إلى أنه ومنذ شهر فبراير عام 2011، تشكلت ما يسمى بقيادة الحرب الالكترونية الحاسوبية في البنتاغون برئاسة الجنرال كيت ألكسندر الذي ترأس وكالة الأمن القومي في وقت سابق، وسيقع على عاتق القيادة الجديدة وفقاً للعقيدة الجديدة تحديد الخصوم الرئيسيين والهجمات الافتراضية المحتملة في الشبكات الحاسوبية العالمية.[18]

الفرع الثاني: الفضاء الإلكتروني وأسلحة الدمار الإلكترونية الشاملة

نظرا للترابط الشديد الذي يميز الفضاء السيبري، وارتباطه أيضا بباقي الشبكات والأنظمة الأخرى ذات الصلة، فإن أي استخدام للبرامج الخبيثة، أو الفيروسات الفتاكة، بكون له عواقب وخيمة على البنية التحتية الإلكترونية لأية دولة، حيث يمكن أن تشل كل مظاهر الحياة الاقتصادية والاجتماعية فيها، وهذا ما حدث بالفعل سنة 2007 في استونيا، حيث أرعب هذا السلوك الدول والجيوش على حد سواء، ومن ثم كان ذلك الهجوم سببا في إعداد دليل "تالين".

ونتيجة لما سبق، فإن الدمار الذي تسببه الأسلحة السيبرية يمكن أن يضاهي أسلحة الدمار الشامل، لذلك ينبغي التأكد من توافق الأسلحة الجديدة لقواعد القانون الدولي قبل استخدامها، وفي هذا الصدد تلزم المادة 36 من البروتوكول الإضافي الأول لعام 1977 من اتفاقيات جنيف، الدول الأطراف، التحقق من امتثال أي سلاح جديد لقواعد القانون الدولي الإنساني. وهذا أيضا صميم ما تطرق له دليل "تالين".

فقد طالبت الدول الأطراف في اتفاقيات جنيف أثناء المؤتمر الدولي الثامن والعشرين للصليب الأحمر والهلال الأحمر المنعقد عام 2003، بأن تخضع جميع الأسلحة الجديدة ووسائل وأساليب الحرب الجديدة "لاستعراض دقيق ومتعدد التخصصات"، وذلك لضمان ألا يتخطى تطور التكنولوجيا الحماية القانونية المكفولة. ويُعَد استخدام العمليات السيبرية أثناء النزاعات المسلحة مثالاً مناسبا على هذا التطور التكنولوجي السريع.[19]

الفرع الثالث: نحو سباق تسلح إلكتروني جديد

دفع التطور في مجال الفضاء الإلكتروني، إلى بروز ترسانة غير تقليدية لأسلحة إلكترونية (Cyber weapon) مختلفة، حيث تجري الولايات المتحدة سنويا محاكاة التعرض لحرب إلكترونية فيما يطلق عليها بعاصفة الحواسب، (cyber storm)، خصصت

500 مليون دولار في ميزانية عام 2012، لمواجهة التهديدات الإلكترونية، كما أعلنت عن جهود تصنيع لأسلحة إنترنت هجومية لمواجهة احتمال تعرضها لهجوم، وزادت من تمويل الأبحاث الإلكترونية من 120 مليون دولار إلى 208 ملايين دولار عام 2012.[20]

كما قامت إيران بتأسيس مقر الدفاع الإلكتروني في أكتوبر 2011، وأصبحت من ضمن الدول التي تملك منظومة دفاعية كاملة في مواجهة تهديدات الحرب الإلكترونية. وفي إسرائيل تم إنشاء وحدة خاصة تدعي "رام" لمواجهة حملات الغزو الإلكتروني والدفاع عن المواقع الاستراتيجية، وقامت اليابان بتطور فيروس لملاحقة وتعطيل مصادر الهجمات الإلكترونية التي تشن ضدها، وقامت الصين التي تعد أول دولة في العالم تنشئ وحدة خاصة بالحرب الإلكترونية بتطوير أسلحة نبض كهرومغناطيسية.[(21)] إضافة إلى الترسانة الإلكترونية لروسيا التي تعد رائدة في هذا المجال، حيث تعد أول دولة في العالم تشن حربا إلكترونية عامي 2007 و2008 ضد كل من استونيا وجورجيا.

المبحث الثاني: ميثاق الأمم المتحدة واستخدام القوة الإلكترونية (cyber power)

المطلب الأول: ميثاق الأمم المتحدة واللجوء إلى الحرب الإلكترونية (jus ad bellum)

الفرع الأول: مصير سيادة الدول في ظل الفضاء الإلكتروني

جاءت أحكام قواعد دليل (Tallinn) الخاص بالقانون الدولي المطبق أثناء الحروب السيبرية، موافقة لما نص عليه ميثاق الأمم المتحدة، وكذا الصكوك الدولية ذات الصلة فيما يخص احترام سيادة الدول، حيث تضمنت القاعدة الأولى منه مسألة السيادة وذلك بقولها: تمارس الدولة رقابتها على المنشآت السيبرية وجميع الأنشطة ذات الصلة في إطار سيادتها الإقليمية، كما نصت القاعدة رقم 2 المتعلقة بالاختصاص، بأن تمارس الدولة اختصاصها على الأشخاص الممارسين للأنشطة السيبرية داخل إقليمها الوطني، بينما شددت القاعدة 4 على أن أي تدخل لدولة ما، في المنشآت السيبرية لدولة أخرى يعد خرقا لسيادتها.[22] وفي هذا السياق، جاءت القاعدة 6 من الدليل، لتحذر من أن الدول تتحمل المسؤولية القانونية عن أنشطتها السيبرية التي تخرق بموجبها أي التزام دولي.

علاوة على ذلك، أكدت الجمعية العامة للأمم المتحدة أن حقوق الأشخاص خارج الفضاء الإلكتروني، يجب أن تحظى بالحماية أيضاً في الفضاء الإلكتروني. وهذا ما تضمنه تقرير المفوضة السامية من خلال اعتماد 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، وفقاً لنص القرار: "حماية الحق في الخصوصية وتعزيزه في سياق المراقبة الداخلية والخارجية للاتصالات الرقمية و/أو اعتراضها وجمع البيانات الشخصية." حيث قدّم التقرير إلى مجلس حقوق الإنسان في دورته السابعة والعشرين وإلى الجمعية العامة في دورتها التاسعة والستين.[23]

الفرع الثاني: الدفاع الشرعي عن النفس في إطار الحرب الإلكترونية

كانت المسألة الأكثر إثارة للجدل خلال الاجتماعات بمدينة" تالين" في استونيا، تتعلق بتوقيت الضربة الهجومية المبررة باعتبارها عملية استباقية للدفاع عن النفس ضد الاعتداءات الإلكترونية. فوفق العقيدة الراهنة، يجب أن يكون الاعتداء وشيكاً لاستعمال حق الدفاع عن النفس بشكل استباقي. لكن «دليل تالين» يبدو أكثر تساهلا في هذا المجال، فيعتبر أن الضربة الأولى تكون مبررة إذا كانت تعكس الفرصة الأخيرة لمواجهة التهديد، وذلك حتى لو كشف السلاح الرقمي عن أسوأ آثاره في مرحلة لاحقة.[24]

وحول هذه المسألة، تثور جملة من التساؤلات، حول ما إذا كانت الهجمات السيبرية تنتهك حظرا عاما على استخدام القوة وفقاً للمادة 2 (4) من ميثاق الأمم المتحدة، وهل يصل الهجوم الإلكتروني الى عتبة (الهجوم المسلح) الذي يؤدي إلى إعمال الحق في الدفاع عن النفس بموجب المادة 51 من ميثاق الأمم المتحدة. لكن دليل (Tallinn) أجاب بأن الهجمات الإلكترونية قد تؤدي بشكل قانوني إلى الحق في الدفاع عن النفس بموجب المادة 51، متى كان من شأنها أن تلحق دمارا كبيرا في البنية التحتية الوطنية الهامة للدولة المستهدفة.[25] وبالتالي نستنتج أن معدي الدليل اعتمدوا على المبادئ العامة التي نص عليها ميثاق الأمم المتحدة في هذا المجال، إضافة إلى قواعد القانون الدولي العرفي التي كرستها الممارسة الدولية.

الفرع الثالث: مدى مشروعية الرد على أي هجوم إلكتروني بالوسائل العسكرية

نص المبدأ 18 المتعلق بمجلس الأمن الدولي أن لمجلس الأمن الدولي أن يقرر وفقا للفصل السابع إن كان أي نشاط سيبري يمكنه أن يهدد الأمن الدولي أو أن يشكل عملا من أعمال العدوان، كما أجاز المبدأ 95 لمجلس الأمن الدولي أن يتحرك بموجب الفصل السابع من ميثاق الأمم المتحدة، في حالة الحرب السيبرية أيضا، لاسيما إذا خرقت دولة من الدول السلم والأمن الدوليين، أو لم تلتزم بواجب الحياد في أية حرب سيبرية.

وفي هذا الصدد، فإن المحامين العسكريون الأميركيون ممن شاركوا في إعداد قواعد دليل "تالين"، مصممون على أن الضرر الإلكتروني يمنح الحق بشن «اعتداء مسلح»، لاسيما وأن الحروب أصبحت تتدلع ضمن ساحات القتال الرقمية أيضاً، لذلك طرح خبراء القانون الدولي قواعد خاصة بالحرب الإلكترونية، لكن تتعدد الأسئلة العالقة، من بينها: هل من المناسب الرد على أي هجوم إلكتروني بالوسائل العسكرية مستقبلاً ؟ قد تكون القواعد التي جمعها خبراء القانون الدولي النافذون في الكتيّب، كفيلة بطمس الخطوط بين الحرب والسلم، وقد تسمح بشن اعتداء خطير على البيانات الرقمية، وقد يحتدم الصراع ويتحول سريعاً إلى حرب حقيقية بالقنابل والصواريخ. لأن القادة العسكريون يمكن أن يفسروه كدعوة لإطلاق أول ضربة استباقية في الحرب الإلكترونية.[26]

المطلب الثاني: الصراعات الإلكترونية وأثرها على السلم والأمن الدوليين

الفرع الأول: الإرهاب الإلكتروني وتداعياته على الأمن الدولي

يشعر البعض بالقلق من أن تمهد اقتراحات «دليل تالين» لتوسيع قواعد «الحرب على الإرهاب»، حيث أضاف معدّو الدليل دعوة الخبير الجيوستراتيجي الأميركي "جوزيف ناي" لأخذ تدابير وقائية ضد «النسخة الإلكترونية من اعتداءات 11 سبتمبر» إلى الكتيّب. يعني ذلك أنه باستطاعة الدول أن تعلن الحرب على مجموعات القراصنة المنظّمة، باستخدام طائرات قتالية بلا طيار مثلا ضدهم، وفي هذا السياق يحذر الخبير "كريس" من أن توسيع منطقة القتال لتشمل الحواسيب المحمولة التابعة لجماعة غير منظمة من الأفراد سيطرح «تهديداً حقيقيا على حقوق الإنسان».[27] على اعتبار أن ذلك يمكن أن يمس بخصوصية الأفراد وبياناتهم الشخصية، لاسيما أولئك الذين تجمعهم روابط وعلاقات ضمن شبكات التواصل الإجتماعي، وهذا بالرغم من أن القاعدة 36 من الدليل، منعت الهجمات الإرهابية التي تهدف إلى ترويع المدنيين. وفي هذا السياق صرحت السيدة "لويد لانجاميني" رئيسة مديرية الاتجار غير المشروع والجريمة المنظمة لدى مكتب الأمم المتحدة لمكافحة المخدرات والجريمة، على هامش مؤتمر الأمم المتحدة لمكافحة الجريمة المنعقد في الدوحة عام 2015 بأن: " جرائم الفضاء الإلكتروني أصبحت تشكل تهديدا حقيقيا لأمن الدول والأفراد" لذلك ركزت الأمم المتحدة جهودها بالتعاون مع وشركاءها لخلق عالم رقمي أكثر أمانا.[28]

الفرع الثاني: تطور المجتمعات الإلكترونية وتهديد الأمن الالكتروني

مع تطو المجمعات الإلكترونية تحت تأثير التقدم المذهل في وسائل الاتصال الرقمية، وظهور ما يسمى ب"الحكومات الإلكترونية"، أصبحت خطورة الجرائم الإلكترونية تكمن في كونها عابرة للحدود، إذ تكلف الاقتصاد العالمي سنويا مئات المليارات من الدولارات، حيث بات الفضاء الإلكتروني مكانا مثاليا للمجرمين اليائسون، وفي هذا الصدد صرح نائب الأمين العام للأمم المتحدة بأن التكنولوجيا "تصنع تقدما هائلا ضد الجوع والمرض، غير أنها تمكن أيضا للجريمة المنظمة، وتثير شبح الهجمات الإلكترونية التي تسبب الإعاقات " ومن أجل التصدي لهذه الجرائم، أنشأت الأمم المتحدة فريق خبراء حكومي دولي مفتوح العضوية لدراسة جرائم الأنترنت.[29] فمع التطور المستمر والمتسارع للفضاء السيبري، أصبحت الأجهزة الأمنية الدولية، تنشر بلاغات بحث على مواقع التواصل الاجتماعي، عن مجرمين مطلوبين، وهذا ما يعكس حجم شبكة الأنترنت، بحيث أصبحت عالما مستقلا بذاته.

الفرع الثالث: الجريمة المنظمة في الفضاء السيبري وعلاقتها بالحرب الإلكترونية

نظرا لسهولة استخدام الأفراد والفاعلين من غير الدول للفضاء الإلكتروني، أصبح هذا الأخير ملاذا آمنا على ما يبدو للمجرمين المحترفين من أجل قرصنة المواقع الإلكترونية بهدف الكسب غير المشروع، لذلك أفردت القاعدة 82 من دليل "تالين" حماية خاصة للممتلكات الثقافية، أو بغية تجنيد عناصر ضمن الشبكات الإرهابية، كما يفعل تنظيم "داعش"، أو ما تقوم به جماعة "الأنونيموس" الشهيرة (Anonymous)، أما عن العلاقة الوطيدة بين هذه التنظيمات الإجرامية والحرب الإلكترونية، فتكمن في أن عناصر الجريمة المنظمة على شبكة الأنترنت، يمكن أن تكون طرفا في حرب إلكترونية ضد دولة معينة، أي في نزاع مسلح داخلي، كما يمكن أن تلجأ الدول إلى استخدام هذه التنظيمات قصد التمويه، أو الجوسسة الإلكترونية.

بالتالي، تتضح خطورة التهديدات التي تشكلها الجريمة المنظمة على أمن الفضاء السيبري، ومن ثم على الأمن الدولي، وهو الأمر الذي أشارت إلى أهميته تقارير دولية، حيث قالت أن العالم بحاجة إلى مليون خبير أمني، للحد من الهجمات الإلكترونية الشرسة، وقد جاءت تصريحات الرئيس الأمريكي باراك أوباما، مؤكدة معاناة الدول الكبرى جراء هذه الحرب في الفضاء المفتوح، حيث أكد أن العالم يحتاج لقوانين جديدة لوقف القرصنة الإلكترونية.[30]

المطلب الثالث: جهود المجتمع الدولي في تقنين قواعد الحرب الإلكترونية

الفرع الأول: جهود المنظمات والهيئات الدولية

ساهمت بعض المنظمات الدولية في وضع قواعد القانون الدولي المطبقة على الحروب الإلكترونية التي تدور معاركها في الفضاء السيبري، ومن بين هذه المنظمات حلف شمال الأطلسي واللجنة الدولية للصليب الأحمر، التي عقدت عدة مؤتمرات وندوات دولية لدراسة مدى إمكانية تطبيق قواعد القانون الدولي الإنساني على الحروب والهجمات السيبرية، على غرار النزاعات المسلحة التقليدية.

وتتويجا لتلك الجهود، أعدت أول وثيقة في هذا الشأن تتمثل في دليل "تالين"، بدعوةٍ من منظمة بحثية تابعة لحلف الأطلسي في العاصمة الإستونية، تالين، عُقد اجتماع برئاسة محام عسكري أميركي له علاقات مع البنتاغون، حيث ناقش خلاله خبراء بارزون في مجال القانون الدولي قواعد الحروب المستقبلية.[31] وفي مقدمتها الحروب السيبرية التي تشنها الدول أو باقي الفاعلين الآخرين.

بدأ مصطلح الحرب ومنذ زمنٍ طويل يأخذ ألفاظاً مغايرة، أهمها ما ورد في اتفاقيات جنيف الأربعة لعام 1949، والتي درجت على لفظ النزاعات المسلحة أو (Armed Conflicts). حيث يتضمن هذا المصطلح في طياته أقل قدراً من العنف الذي يحمله مصطلح الهجوم المسلح (Armed Attack). فحتى وقتٍ ليس ببعيد، أثير النقاش حول إذا ما كان القانون الدولي الإنساني ينظم مسألة العمليات العسكرية عن طريق الإنترنت (Cyber-Operations)، لذلك، بدأت المنظمات الحكومية الدولية "" تعترف بأن القانون الدولي الإنساني ينظم مثل تلك العمليات بالفعل. حيث أن فريقاً من الخبراء الحكوميين اجتمع عام 2013 تحت رعاية الأمم المتحدة، وبحضور 15 ممثلٍ عن دولهم، مؤكدين على ذات الأمر. وما يؤكد هذا الموقف، هو ما اتخذه الاتحاد الأوروبي في قضية هجوم إلكتروني سنة 2013. وهو الموقف أيضا الذي تبناه حلف شمال الأطلسي (NATO) عام 2014، في تصريح قمة ويلز (Wales Summit Declaration).[32]

الفرع الثاني: موقف الفقه والقضاء الدوليين من الحرب الالكترونية

ساهم الفقه الدولي في تقنين قواعد الحرب الإلكترونية من خلال دليل "تالين"، حيث تمت كتابته من قبل حوالى 20 من فقهاء القانون والممارسين الآخرين من محامين وغيرهم، ويعد الدليل الوثيقة الوحيدة المعبرة عن تكيف القانون الدولي الحالي مع الحروب السيبرية. ومن بين النقاط التي أثارت جدلاً واسعا بين الفقهاء الذين ساهموا في إعداد الدليل، أن المدنيين غير محظورين من المشاركة في العمليات العدائية عبر الإنترنت، ولكنهم يفقدون حمايتهم من

الهجمات مع أول مشاركة لهم بها، ومعنى ذلك أن المدنيين بعيدين كل البعد عن الحروب السيبرية مالم يشاركوا فيها، فإن قاموا بخوضها يعتبرون وقتئذ أهدافا حربية مشروعة.[33] وهي نفس الأحكام التي تضمنتها اتفاقيات جنيف لعام 1949 وبروتوكولاتها الإضافية لعام 1977، وهذا ما يوحي بأن قواعد دليل (Tallinn)، أعدت بالاعتماد على قواعد القانون الدولي المعمول بها، لاسيما القانون الدولي الإنساني والعرفي، وكذا ميثاق الأمم المتحدة.

وتجدر الإشارة إلى أنه وبعد حادثة شركة "سوني" سنة 2014، احتدم النقاش ما بين الساسة والقانونيين والمثقفين، فيما إذا كان السلوك الذي قامت به كوريا الشمالية ضد الولايات المتحدة الأمريكية عن طريق الإنترنت، يشكل عملا حربياً، أو عملاً من أعمال الحرب (Acts of War). بمعنىً آخر، هل يمكن اعتبار هذه الأعمال من قبيل الهجوم المسلح (Armed Attack)، المذكور في ميثاق روما (Rome Statute) للمحكمة الجنائية الدولية، بما يخول – كنتيجة لذلك الهجوم – الدولة المعتدى عليها، أن تقمع وترد ذلك الهجوم بواسطة ما تمتلكه من قوة مماثلة، وعن طريق الإنترنت أيضاً، وذلك تحت غطاء ما يسمى قانوناً بحق الدفاع الشرعي (The Right to Self-Defence).[34]

الفرع الثالث: موقف اللجنة الدولية للصليب الأحمر

اضطلعت اللجنة الدولية بدور بارز في تقنين قواعد الحرب الإلكترونية، وذلك من خلال مساهمتها في اعداد دليل "تالين"، حيث انعكست مواقفها في الأحكام التي تضمنها، كما شاركت اللجنة بصفة مراقب في مناقشات الخبراء الذين صاغوا دليل "تالين"، قصد ضمان تبني قواعد القانون الدولي الإنساني السارية قدر الإمكان ضمن أحكامه، وتعزيز الحماية التي يوفرها هذا الفرع من القانون لضحايا النزاعات المسلحة في قواعد الدليل.[35]

ونتيجة لذلك، ترى اللجنة الدولية للصليب الأحمر أن الاعتداءات وحدها التي تسبب ضرراً جسدياً أو شخصياً، هي التي تُؤخَذ بعين الاعتبار على مستوى القانون الدولي. أما تعطّل الحاسوب أو فقدان البيانات فليس مبرراً كافياً لشن أي «اعتداء مسلح». لكن ماذا لو لم يسبب تعطل الحواسيب ضرراً جسدياً (كما يحصل في معظم الحالات)، بل أدى إلى خسائر مالية كبرى؟ المحامون العسكريون الأميركيون الذين شاركوا في مؤتمر "تالين" شددون على أن الضرر الاقتصادي يمنح الحق بإطلاق اعتداء مضاد إذا اعتُبر الضرر «كارثياً». في نهاية المطاف، يتوقف على كل بلد أن يقرر حجم الضرر الاقتصادي الكافي لتبرير خوض الحرب.[36] وهذا ما يعرف بنظرية اللجوء إلى الحرب (Jus ad bellum)، بحيث تشترط أن تكون مبررة وعادلة أيضا، لكي يمكن إضفاء صفة المشروعية عليها.

الخاتمة:

في الختام نخلص إلى القول بأن دليل تالين هو الوثيقة القانونية الوحيدة إلى حد الآن، التي تتضمن قواعد للقانون الدولي الإنساني التي تحكم مسألة اللجوء إلى الحرب الإلكترونية، وكذا مسألة جواز استهداف مستخدمي الفضاء السيبيري باعتبارهم مقاتلين، شريطة مراعاة قواعد الاشتباك الإلكتروني كمبدأ التمييز بين الفاعلين الإلكترونيين، وهذا بغية حماية المدنيين والأعيان المدنية أثناء الصراعات الإلكترونية والسيبيرية.

وفيما يتعلق بمدى شرعية استخدام القوة الإلكترونية (cyber power) في إطار ميثاق الأمم المتحدة، يحق للدول أن تلجأ إلى ذلك في حالة الدفاع الشرعي عن النفس في إطار الحرب الإلكترونية، وكذا في إطار محاربة الإرهاب الالكتروني خلال لصراعات الإلكترونية، وذلك نظرا للتأثير الخطير للهجمات السيبيرية الشاملة على الأمن الدولي، وبالتالي فإن الرد على أي هجوم إلكتروني بالوسائل العسكرية يعد مشروعا في إطار القواعد العامة لميثاق الأمم المتحدة.

أما عن آثار الحروب السيبيرية على مسألة حقوق الإنسان، فقد كفلها القانون الدولي من خلال قواعد دليل "تالين" الخاصة بحماية المدنيين من مستخدمي الفضاء السيبيري، سواء فيما يتعلق بحياتهم الخاصة، أو عن طريق حماية مصالحهم المادية من أي هجوم إلكتروني، والمرتبطة بالكثير من الأعيان المدنية التي تسير عن طريق شبكات الأنترنت.

الهوامش:

1 - نزاع مسلح دولي ونزاع مسلح غير دولي.

2 –**جامعة بغداد**، كلية القانون، فرع القانون الدولي يعقد ندوة (حروب الفضاء الالكترونية)، بتاريخ 2016/4/12، متاح على الرابط التالي: http://www.colaw.uobaghdad.edu.iq/ArticleShow.aspx?ID=1405، آخر زيارة للموقع يوم 2016/05/02 على الساعة: 22 سا و01 د.

3 – 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, p. 106

4 - **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: 2016/04/16، على الساعة: 16 سا و18 د.

5 – نفس المرجع.

6 - **صالح الدين زيدان**، طبول الحرب الرقمية ، *مجلة المسلح*، مقال منشور بتاريخ 2016/01/14، متاح على الرابط: http://www.almusallh.ly/ar/thoughts/633-vol-38–44، آخر زيارة للموقع بتاريخ: 2016/04/03، على الساعة 21 سا و44 د.

7 - نفس المرجع.

8- **إيهاب شوقي**، الحرب السيبرانية...حرب المستقبل المفزعة، *شبكة الأخبار* العربية ANN ، متاح على الرابط: http://www.anntv.tv/new/showsubject.aspx?id=101954#.VztrLTWLTIU ، آخر زيارة بتاريخ: 2016/05/06، على الساعة 22 سا و10 د.

9 - Tallinn Manual on the Jnternatonal Law applicable to Cyber Warfare, Op. cit, pp.113-125.

10 - **اللجنة الدولية للصليب الأحمر**، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية ؟، مرجع سبق ذكره.

11 – نفس المرجع.

12- **إيهاب شوقي**، الحرب السيبرانية...حرب المستقبل المفزعة، *شبكة الأخبار العربيةANN* ، مرجع سبق ذكره.

13- **صحيفة العرب**، الحرب الإلكترونية تتسف منطق الحرب التقليدية، نشر بتاريخ 2013/04/11، متاح على الرابط : http://www.alarab.co.uk/?p=27010، آخر زيارة للموقع يوم: 2016/04/12، على الساعة 23 سا و17 د

14 - See ; Tallinn Manual on the Jnternatonal Law applicable to Cyber Warfare, Op. cit, pp. 96-103.

15 - المقولة لألبير أينشتاين

16 - **جامعة بغداد**، كلية القانون، فرع القانون الدولي يعقد ندوة (حروب الفضاء الالكترونية)، مرجع سبق ذكره.

17 - **جريدة الجريدة**، قواعد جديدة وخطيرة للحرب الإلكترونية، بتاريخ 2013/04/10، متاح على الربط التالي :

http://www.aljarida.com/news/index/2012595844/، آخر زيارة للموقع: 2016/02/23، على الساعة 19 سا و20 د.

18 - اللمسات الأخيرة "لعقيدة الحرب الالكترونية" الأمريكية، 2013/02/5، متاح على الربط :http://arabic.sputniknews.com/arabic.ruvr.ru/2013_02_05/103686032. آخر زيارة للموقع: 2016/02/23، على الساعة 15 سا و55 د.

19 - **اللجنة الدولية للصليب الأحمر**، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية ؟، مرجع سبق ذكره.

20 - **مؤتمر حروب الفضاء السبرانى**، الفضاء الإلكتروني وأسلحة الانتشار الشامل بين الردع وسباق التسلح، 2015/05/15، متاح على الرابط التالي :https://seconf.wordpress.com/2015/05/15/، آخر زيارة للموقع يوم: 2016/04/16، على الساعة: 06 سا و58 د.

21 - نفس المرجع.

22 - Tallinn Manual on the Jnternatonal Law applicable to Cyber Warfare, Op. cit, pp.15-18.

23 - **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: 2016/04/16، على الساعة: 07 سا و 22 د.

24 - **جريدة الجريدة**، قواعد جديدة وخطيرة للحرب الإلكترونية، بتاريخ 2013/04/10، مرجع سبق ذكره.

25 - **جامعة بغداد**، كلية القانون، فرع القانون الدولي يعقد ندوة (حروب الفضاء الالكترونية)، مرجع سبق ذكره.

26 - **صحيفة العرب**، الحرب الإلكترونية تنسف منطق الحرب التقليدية، مرجع سبق ذكره.

27 - **جريدة الجريدة**، قواعد جديدة وخطيرة للحرب الإلكترونية، بتاريخ 2013/04/10، مرجع سبق ذكره.

28 - **الأمم المتحدة**، مركز أنباء الأمم المتحدة، الدوحة: الأمم المتحدة وشركاؤها يركزون على جهود مكافحة جرائم الفضاء الإلكتروني، 2015/04/17، متاح على الربط التالي :
http://www.un.org/arabic/news/story.asp?NewsID=23351#.VztdkDWLTIU، آخر زيارة للموقع يوم: 2016/04/12، على الساعة: 12 سا و 33 د.

29 - **الأمم المتحدة**، مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية، المنعقد في الدوحة 12-19 أفريل 2015، متاح على الرابط:

http://www.un.org/ar/events/crimecongress2015/cybercrime.shtml، آخر زيارة للموقع بوم: 2016/03/11، على الساعة 22 سا و05 د.

30 - **محمد محمود**، «الحرب الإلكترونية»، أشرس معارك الألفية الثالثة، مجلة كل الأسرة، ملحق الاسبوع السياسي، متاح على الرابط:

-: http://www.alkhaleej.ae/supplements/page/8e4a7054-318c-4242-adea-04a217c14923#sthash.Bs3r5p3h.dp، آخر زيارة للموقع يوم: 2016/04/10، على الساعة 23 سا و16

31- **إيهاب شوقي**، الحرب السيبرانية...حرب المستقبل المفزعة، *شبكة الأخبار العربية ANN*، مرجع سبق ذكره.

32 - **صحيفة العرب**، الحرب الإلكترونية تنسف منطق الحرب التقليدية، مرجع سبق ذكره.

33 - **محمد أبو على**، لكل فعل رد فعل حتى الحروب الإلكترونية، بتاريخ: 2013/04/02، متاح على الرابط http://techarabi.com/26310 :، آخر زيارة للموقع يوم: 2016/04/13، على الساعة 20 سا و00 د.

34 - **ماهر أسامة مسعود**، موقف القانون الدولي الإنساني من الهجوم عن طريق الإنترنت " Cyber War"، أمد للإعلام، متاح على الرابط:
https://www.amad.ps/ar/Details/80978، آخر زيارة للموقع بتاريخ 2016/05/12، على الساعة: 12 سا و10 د.

35 - **إيهاب شوقي**، الحرب السيبرانية...حرب المستقبل المفزعة، شبكة الأخبار العربية ANN ، مرجع سبق ذكره.

36 - **صحيفة العرب**، الحرب الإلكترونية تتسف منطق الحرب التقليدية، مرجع سبق ذكره.