موقف القانون الدولي من الهجمات الإلكترونية

Cyber from Law International of position The Attack

م.م. ليث ناجح حميد

جامعة الفلوجة / كلية القانون

المقـــدمـــة

في أبريل عام٢٠٠٧ تعرضت استونيا إلى اعتداء الإلكتروني ، أدى إلى تعطل جميع الأنظمة الالكترونية وخاصة الأنظمة البنكية ، وكذلك كل وسائل الاتصال الالكترونية، أن تأثير هذا الاعتداء كأن بمثابة الهجوم التقليدي على هذه الدولة، لذلك فإن استخدام التقنية الحديثة قد يكون لها نفس القوة والتأثير الذي تخلفه الأسلحة التقليدية كالصواريخ والأسلحة النووية المدمرة ،لأنهما يحملان نفس الهدف والغاية، وبعد التطور الهائل الذي حدث في التكنولوجيا والانترنت فإن قوانين الحروب عدلت لتشمل الاعتداءات التي تحصل نتيجة استخدام هذه التكنولوجيا في إدارة مرافق الدولة العامة والخاصة، لكن مع كل هذا الخطر الذي تثيره الهجمات الالكترونية فإنها لا تزال خارج دائرة ما يعرف بالنزاعات المسلحة لأن الهجوم الالكتروني له من الخصائص تجعله يستقل عن الهجوم التقليدي.

إن موضوع الاعتداء الالكتروني (**Cyber Attack**) أصبح من المواضيع المهمة والساخنة وخاصة بعد هجمات استونيا عام ٢٠٠٧، وأن الكثير من فقهاء

القانون الدولي بدؤوا يقارنون الاعتداء الالكتروني بالهجوم النووي (**unclear Weapons**) لما يخلفان من أثاراً تدمرية هائلة وخاصة في الدول المعتمدة على التكنولوجيا الحديثة في إدارة مرافقها.

لذا فإن هذا البحث سوف يناقش ماهية الهجوم الالكتروني وما هو القانون الذي يحكم أو يفرض الجزاءات على المعتدين دولا كانوا أم منظمات إرهابية (non-state Actors) وأخيراً سيتناول البحث حق الدولة المعتدى عليها برد الاعتداء طبقاً لنظرية الدفاع الشرعي أو الدفاع عن النفس.

أهمية الموضوع:

إن الهجوم الإلكتروني له أهمية بالغة في معرفة إبعاده ونطاقه وكذلك الطرق التعامل معه لأنه يؤسس لحروب ونزاعات دولية، كذلك أن الهجوم الالكتروني أصبح أحد الأسلحة الفتاكة التي تهدد امن الدول وسيادتها، إذ أصبحت الهجمات الالكترونية مستخدمة استخداما واسعا لما تحمله من تأثير على المواقع المستهدفة ؛ لأنها لا تقل حجم تأثيرها عن تأثير الأسلحة التقليدية كالأسلحة النووية والمدمرة، فإن من الضروري معرفة موقف القانون الدولي من الهجوم الالكتروني وكيف التعامل معه في حال وقعه.

أسباب اختيار الموضوع:

إن سبب اختيار موضوع البحث يكمن فيما يلي :

١-انتشار الهجمات الالكترونية في العالم، والتي وأصبحت تمثل تهديداً للسلم الدولي، وأثارت نزعات دولية تمس سيادة وامن والدول.

٢-إن فقهاء القانون الدولي لم يتفقوا على آلية واضحة وصورة واحدة من هذه الهجمات.

٣-آثار الهجمات الالكترونية لا تقل درجة قوته عن الهجوم المسلح لذا من الضروري مقارنته مع الهجوم المسلح المنصوص عليه في القانون الدولي بفرعيه المكتوب والعرفي للوصول إلى نتيجة واحدة بأن الهجمات الالكترونية محرمة دولياً.

مشكلة الدراسة:

تتجسد مشكلة الدراسة في السؤال الآتي: هل أن الهجوم الالكتروني يعتبر هجوماً مسلحاً يقع تحت طائلة ميثاق الأمم المتحدة ويعطي للدولة الحق في الدفاع الشرعي ؟ فالهجوم الالكتروني يثير إشكالية كبيرة لأن ميثاق الأمم المتحدة والقانون الدولي العرفي لم يتطرقا إليه وهناك من فقهاء القانون الدولي أنكر عنه الصفة المسلحة واعتبره هجوما لا يرقى إلى مرتبة الهجوم المسلح.

منهجية الدارسة:

إن المنهجية المعتمدة في هذه الدراسة هي المنهج التحليلي الوصفي لأحكام ميثاق الأمم المتحدة ومقارنتها مع بعض النصوص للوصول إلى نتيجة توضح موقف القانون الدولي من الهجوم الالكتروني وكيفية التعامل معه في حال حدوثه.

خطة البحث:

المطلب الأول: ماهية الهجوم الالكتروني.
المطلب الثاني: الهجمات الالكترونية باعتبارها قوة .
المطلب الثالث: الوضع القانوني للدولة المعتدية والمعتدى عليها .
المطلب الرابع: الرد على الهجوم الالكتروني.

المطلب الأول

ماهية الهجوم الالكتروني

Concept of Cyber-Attack

إن للهجوم الالكتروني مفهوم ومدلول يختلف عن الجرائم الالكترونية أو الاعتداءات الالكترونية الأخرى لذا سوف نتناول في هذا المطلب تعريف الهجوم

الالكتروني ونقارن بينه وبين الجرائم الالكترونية لاختلاف الهدف والغاية من خلال الفرعين الآتيين:

الفرع الأول: تعريف الهجوم الالكتروني (Definition of Cyber-Attack)

توجد بعض الصعوبات في إعطاء تعريف واضح ودقيق للهجوم الالكتروني بسبب اختلاف القوانين الوطنية والدولية في مواجهة هذه الجريمة أو الهجوم لأن أنشطة الفضاء الالكتروني (Cyber-Space) تشمل بعض الأنشطة التي لا يمكن اعتبارها ضمن دائرة النزاعات والاعتداءات الالكترونية، لكن الاتجاه الغالب عند فقهاء القانون الدولي والمتخصصون في مجال ((Computer Security) ركزوا على العواقب استخدام هذه الأنشطة الالكترونية[١] .

فيعُرف الهجوم الالكتروني على انه عبارة عن رسائل كاذبة يبعثها المهاجمون يسبب إغلاق مفاعل نووي أو انقطاع التيار الكهربائي يؤدي إلى تعطل أنظمة المراقبة الجوية والمطارات، وإضرار اقتصادية هائلة تتعلق بسوق الأسهم والأنظمة الإلكترونية في الدولة، أن الباحثون في مجال ((Computer Security) أكدوا بأن جميع هذه السيناريوهات الواردة في التعريف لا يمكن أن تحدث بصورة عرضية أو حادث طارئ ((cyber-incident) بل تُعد هجمات الالكترونية الغاية منها ضرب أهداف معينة في دولة ما، وعرفه المتخصص في مجال الأمن الحكومي الأمريكي البروفسور Richard A Clark بأنه أفعال صادرة عن دولة ما ضد أجهزة الكومبيوتر والشبكات التابعة لدولة أخرى الغرض منه تعطيل هذه الأنظمة أو خلق اضطراب الكتروني[٢] .

1-Scott J. Shackelford, From Nuclear War to Net War: Analogizing Cyber Attacks in International Law, Shackelford, P 218- 233.

2- Ian Traynor, Russia Accused of Unleashing Cyber war to Disable Estonia, GUARDIAN(LONDON), May 17, 2007. 1.

إن هذا التعريف يتفق مع ما ذهب إليه مدير الاستخبارات الأمريكية CIA بأن الهجوم الالكتروني هو محاولة متعمدة الغرض منها تدمير الشبكات الالكترونية لدولة ما، بعد عام ٢٠١١ تم أنشاء القيادة الالكترونية الأمريكية (United States Cyber Command)) ونشرت هذه القيادة تعريفاً خاصاً بالهجوم الالكتروني بأنه عمل عدائي باستخدام الكومبيوتر أو الشبكات والأنظمة ذات الصلة تهدف إلى تعطيل أو تدمير الأنظمة الالكترونية فلا يقتصر هذا التدمير على الأنظمة الالكترونية بل يهدف إلى تدمير البنى التحتية لهذه الأنظمة[١] .

لقد أنتقد هذه التعريف لأنه حدد الهجوم الالكتروني بالأعمال العدوانية (hostile acts) في حين أن الصفة الأساسية التي تميز الهجوم الالكتروني هي الهدف من الهجوم (Objective of the Attack) ، وبعد عام ٢٠١٢ اتفق معظم خبراء ((Computer Security) بأن الهجوم الالكتروني(Cyber–Attack) بأنه يتألف من أي عمل يهدف إلى تقويض شبكات الحاسوب لغرض سياسي أو وطني.

إن التعريف ميز الهجوم الإلكتروني عن الجريمة الإلكترونية لأن الكثير من التعاريف الخاصة بالهجوم الكتروني الموجودة في عالم ((Computer Sciences) لم تميز بينهما بل خلطت بين الجريمة والهجوم الالكتروني، ومن خلال هذا التعريف يجب التميز بين العناصر الأساسية المكونة للهجوم الالكتروني.

١–يجب أن يتألف من أي عمل: هذا يعني أن الهجوم الالكتروني يتألف من أي عمل من الإعمال الآتية وهي القرصنة والعدوى[٢].

٢– تقويض أو تدمير الوظائف الكومبيوتر أو الشبكات: يقصد به أن الهجوم الالكتروني يجب أن يكون هادفاً إلى تقويض أو تدمير شبكات الكومبيوتر وكذلك عمل

1–Pamela Hess, Pentagon Puts Hold on USAF Cyber Effort, ASSOCIATED PRESS, Aug. 13

2–France v. Turkey (the Lotus Case), PCIJ, 1927, PCIJ Reports, series A, No. 10

خلل في أنظمة التشغيل ومن الأمثلة استخدام الديدان أو الفيروسات أو ما يعرف حصان طروادة.

٣- نظام الكومبيوتر أو الشبكات: إن الهجوم الالكتروني يجب أن يهدف إلى تدمير أو تقويض نظام الكومبيوتر ونظام الشبكات، ويجب الإشارة هنا بأن المفهوم بالكومبيوتر يشمل (Cell Phone) وكل أنظمة التي تدار عبر شبكات الويب وشبكات الكومبيوتر ، ولا يقتصر على الحاسبات التقليدية Desktop and Laptop.

٤- لغرض سياسي أو لغرض الأمن الوطني: إن هذا الشرط يميز الهجوم الالكتروني عن غيره من الاعتداءات الالكترونية الأخرى سواء كأن هذا الغرض تابع لدولة أو لمنظمة إرهابية أخرى[١] .

الفرع الثاني: مقارنة الهجوم الالكتروني بالجريمة الالكترونية

Comparison between Cyber-Attack and Cyber-Crime

يخلط الكثير من المهتمون في هذا المجال بين الهجوم الالكتروني(Cyber-Attack) والجريمة الالكترونية (Cyber-crime) فتعرف الجريمة الالكترونية بأنها كأي مخالفة ترتكب ضد الإفراد أو الجامعات بدافع إجرامي كالتي تتعلق بالبنية التحتية لتكنولوجيا المعلومات، بما يؤدي إلى الوصول غير المشروع إلى هذه البيانات أو الاعتراض غير القانوني لها عن طريق نقلها من والى جهاز الحاسوب كإدخال بيانات خاطئة أو التلاعب بالبيانات أو العبث بها[٢] ، وفي الحقيقة إن الفرق بينهما واضح

1 -Amir Efrati& Siobhan Gorman, Google Mail Hack Is Blamed on China, WALL ST. J., June 2, 2011, at A1; Wyatt Andrews, China Google Hacker's Goal: Spying on U.S. Govt, CBs NEWS (June 2, 2011), http://m.cbsnews.com/fullstory.rbml?catid=20068474&feed_i videofeed=36 (last visited Apr. 19, 2017) Thom Shankar & Elisabeth 53 .

2- Bahrain Government, the Central management for combating the corruption

وجوهري، فالمعتدي في الهجوم الالكتروني يكون دولة أو منظمة إرهابية أو أي جهة أخرى بينما المعتدي في الجريمة لا يمكن أن يكون سوى منظمات إرهابية أو جهات قرصنة ... الخ ، فإن الجريمة الالكترونية لا يمكن أن ترتكبها دولة، والهجوم الالكتروني يكون ضمن اختصاص القانون الدولي لما يمثله من اعتداء خطير على سيادة الدولة بينما تكون الجريمة الالكترونية ضمن الاختصاص الوطني طبقاً لمبدأ إقليمه القانون[١] ، وأن أهم ما يميز الهجوم الالكتروني عن الجريمة الالكتروني: كون الهجوم الالكتروني يهدف إلى تقويض أو تدمير شبكات الويب والكومبيوتر بيمنها الهدف في الجريمة الالكترونية يكون مقتصراً على السرقة أو القرصنة، إن الهجوم الالكتروني لا يرتكب إلا لغرض سياسي أو لغرض الأمن الوطني وهذا لا نجده في الجريمة الالكترونية ترتكب دائما تحت غطاء المالي أو للحصول على منافع مالية أو نقدية.

المطلب الثاني

الهجمات الالكترونية باعتبارها قوة

force is Attack Cyber

إن الهجوم الالكتروني لا يكون تحت طائلة القانون الدولي إلا إذا اعتبر هذا الهجوم قوة تقع تحت طائلة ميثاق الأمم المتحدة، والمعاهدات الدولية المنظمة للنزاعات والعلاقات الدولية، وظهر الهجوم الالكتروني نتيجة التطور التكنولوجي الذي حصل في عالمنا، فالقوة الناتجة عنه تتطور من حيث النطاق والتأثير بتطور هذه التكنولوجيا فمن

http://www.acees.gov.bh/cyber-crime/the-concept-of-e-crime

1-Brian Krebs, Report: Russian Hacker Forums Fueled Georgia Cyber Attacks, WASH.

POST SECURITY FIX BLOG (Oct. 16, 2008, 3:15 PM),

http://voices.washingtonpost.com/securityfix/report_russian_hacker_forums_f.html /١٠/٢٠٠٨

المحتمل مستقبلاً إن تفوق القوة الناتجة من حيث التأثير والتدمير القوة الناتجة عن السلاح التقليدي.

الفرع الأول: الامتناع عن استخدام القوة والتدخل في الشؤون الداخلية للدول (Prohibition of use of force)

إن النظام القانوني الجديد الذي نص على منع استخدام القوة وأن هذا المنع تأطر في نص المادة الثانية الفقرة الرابعة من ميثاق الأمم المتحدة حيث نصت إلى أنه " تمتنع أعضاء الهيئة جميعا في علاقاتهم الدولية عن التهديد باستعمال القوة أو باستخدامها، ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على وجه لا يتفق مع مقاصد الأمم المتحدة" ، نصت هذه الفقرة على ضرورة الامتناع عن استخدام القوة أو التهديد باستخدامها ضد سيادة الدولة بأية طريقة تتنافى مع أهداف الأمم المتحدة المتمثلة في الحفاظ على السلم والأمن الدوليين، فاكتسب مبدأ تحريم استخدام القوة في العلاقات الدولية على القوة القانونية في مطلع القرن الماضي، فإن الفقرة تنطوي على تطور كبير في النظام القانون الدولي، حيث غدا استخدام القوة أو التهديد بها أمراً غير مقبول قانوناً[١] .

إن ما يلاحظ في نص المادة الثانية الفقرة الرابعة من الميثاق استخدم مصلح القوة (Force) وهو تعبير اشمل إذ أنه يغطي كل استعمالات القوة الموجهة ضد الاستقلال السياسي والوحدة الإقليمية، فالنص حرم كل إشكال القوة سواء كانت هذه القوة مباشرة أو غير مباشرة، ولكن أثُير تساؤلاً وجدلاً واسعاً حول علاقة الهجمات الالكترونية وعلاقاتها بنص المادة الثانية من ميثاق الأمم المتحدة.

1- Ian Traynor, Russia Accused of Unleashing Cyber war to Disable Estonia, GUARDIAN (May 16, 2007), http://www.guardian.co.uk/world/2007/may/17/topstories3.russia detailing the reactions by Estonian, EU, and NATO officials to a cyber-attack on Estonia.

إن الإجابة على هذا التساؤل لا بد من تحليل نص المادة الثانية للوصول إلى مفهوم دقيق لمعنى القوة، أن نص المادة الثانية الفقرة الرابعة جاء لينسجم مع الغرض الأساسي لمنظمة الأمم المتحدة وهو حماية الأمن والسلم الدوليين، لذلك فإن استخدام أو التهديد باستخدام أي القوة تهدد الأمن السلم الدوليين، وإن المنع في نص المادة الثانية الفقرة الرابعة جاء مطلقاً وشاملاً لكل إشكالها لأن واضعوا الميثاق لم يدر في خلدهم عند وضع الميثاق التطور الكبير في إشكال القوة الذي يشهده عالمنا اليوم، بل أن جل تفكيرهم كأن نحو القوة العسكرية أو القوة المسلحة ، لذلك فإن من الممكن التوسع في هذا المفهوم وإمكانية شموله للهجمات الالكترونية كصورة من صور القوة في العهد الحديث، وإن هذا التوسع في تفسير نص المادة لا يتعارض أو يتنافى مع اتفاقية فينا لقانون المعاهدات لسنة ١٩٦٩[١] .

إن ما ذهب إليه فقهاء القانون الدولي بأن نص المادة الثانية– الفقرة الرابعة جاءت كلمة قوة نكرة ومفردة إذ أنها جاءت في مواقع أخرى باسم القوة المسلحة، وعلى هذا الأساس فإن الميثاق استخدم مصطلحين القوة المسلحة والقوة بالتالي فإن كلا المصطلحين يعتبران خيارات لمجلس الأمن لرد هذا التهديد باعتباره ضد الأمن والسلم الدوليين، هذا الاختلاف في المصطلحات أدى إلى اختلاف فقهاء القانون الدولي والسياسية في المجتمع الدولي خلال الحرب الباردة بين من أيد التوسع في تفسير مفهوم القوة ويجب أن تشمل صور أخرى مثل الضغط والإكراه السياسي والاقتصادي، وكانوا أنصار هذا الرأي الدول الآسيوية والنامية هم من أيد هذا التوجه، إما أنصار الدولة الغربية فكانوا يؤيدون فكرة المفهوم الضيق للقوة ليشمل القوة المسلحة فقط ؛ لأن التطور التكنولوجي كأن في مصلحتهم[٢] .

1–Vienna Convention on Law of Treaties, Articles 30,31,32.

١–كمال حماد، النزاع المسلح والقانون الدولي العام، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت ، ط١ ، ١٩٩٧ ، ص٣١.

في عام (١٩٨٧) صدر قرار الجمعية العامة للأمم المتحدة الخاص بتعزيز تأثير المبادئ الخاصة بالامتناع عن استخدام القوة، حيث جاء هذا القرار متفقاً مع التوسع في نص المادة الثانية الفقرة الرابعة من الميثاق وجعلها محرمة حتى وإن اشتملت على ضغط أو أكراه سياسي.

إلا أن فقهاء القانون الدولي العام اختلفوا حول كيفية اعتبار الهجوم الالكتروني قوة تحت طائلة المادة الثانية الفقرة الرابعة من ميثاق الأمم المتحدة فذهبوا إلى اتجاهات مختلفة:

١-الاتجاه الأول: ذهب أنصار هذا الاتجاه بأن الهجوم الالكتروني يعتبر قوة محظورة ومحرمة، واعتمد أنصار هذا الاتجاه على نظرية Strict Liability Model أن هذه النظرية تعتبر من الهجوم الالكتروني قوة تحت طائلة المادة الثانية من الفقرة الرابعة إذا كأن موجها ضد البنى التحتية ويودي إلى تدميرها، انتقدت هذه النظرية ؛ لأن الهجوم الالكتروني لا يودي إلى تدمير البنى التحتية بل يقوم بتعطلها[١] .

٢-الاتجاه الثاني: قال أنصار هذا الاتجاه بأن العبرة بطريقة التوصيل (Method of Delivery) ، وأن الهجوم الالكتروني إذا استخدم سواء بطريقة الفيروس أو الدودة أو تسلل أدى إلى الوصول للغاية المنشودة من الهجوم يعتبر قوة محظورة قانوناً.

٣-الاتجاه الثالث: ذهب أنصار هذا الاتجاه إلى أن الهجوم الالكتروني يعتبر أداة مساوية للسلاح التقليدي إذا تم أدى إلى تعطيل أو تدمير أو خلق اضطراب في البنى التحتية في الدولة، حيث اعتمد أنصار هذا الاتجاه على نظرية Direct result of (Attack)، و اعتمدوا على النتيجة النهائية المستخلصة من هذا الهجوم بغض النظر عن طريقة استخدامه لكي يعتبر هذا الهجوم هجوماً محرماً وفق قواعد القانون الدولي

1-Ona A. Hathaway, The Law of Cyber Attack, Yala Law School, 2012, 843 .

العام ، وأن توجه المجتمع الدولي مع هذا الاتجاه الأخير في وصف الهجوم الالكتروني باعتباره قوة، فإن كل الأوصاف المادية التي تجب أن تتوفر بالقوة هي متوفرة بالهجوم الالكتروني[١].

الفرع الثاني : موقف الولايات المتحدة الأمريكية من مفهوم القوة

The position of US toward use of force

إن الولايات المتحدة لم تصرح بصفة صريحة ورسمية بأن الهجوم الالكتروني يعتبر قوة تندرج تحت طائلة المادة الثانية – الفقرة الرابعة من ميثاق الأمم المتحدة، لكن خبراء القانون الدولي والسياسية في الولايات المتحدة الأمريكية كأن لهم موقفاً أكثر وضوحاً ودقة من موقف الإدارة الرسمية، فذهب جانب منهم إلى أن الهجوم الالكتروني يجب أن يدخل ضمن الإطار القانوني لمفهوم القوة المنهي عنها في الميثاق وخلص بدراسة أعدها مجلس البحوث الوطنية الأمريكي وكانت نتائجها أن الهجوم الالكتروني يجب أن يعاقب عليه وفق القانون الدولي وينطبق عليه مفهوم المادة الثانية الفقرة الرابعة من الميثاق لأن تأثيره الهجوم الالكتروني على البنى التحتية للدولة لا يقل عن تأثير الهجوم العسكري المسلح وكلاهما يحملان نفس الغرض هو التعطيل أو تدمير[٢].

إلا أن فقهاء القانون الدولي والسياسة الدولية أكدوا بأن القوة لا تشمل سوى الهجوم الالكتروني الذي يهدف إلى تعطيل أو تدمير البنى التحتية لأجهزة الكومبيوتر وشبكات الاتصال وأنظمة الاتصال والخدمات الالكترونية، فلا يندرج تحت هذا المفهوم إعمال التجسس الالكتروني والتجنيد الالكتروني، وجمع المعلومات الاستخبارية والهجمات الوقائية التي تقوم بها الدولة للوصول إلى معلومات أمنية أو سياسية، لأن هذه الإعمال لا يصل حجم تأثيرها المدمر إلى التأثير الناتج عن استخدام القوة

1-Id(845)

٢-كمال حماد، مصدر سابق، ص ٣٤.

العسكرية أو القوة المسلحة حتى وأن اشتركت مع الهجوم الالكتروني بالباعث أو الدافع أو النية وهي لأغراض سياسية أو وطنية ولكن نتائجهما مختلفة[١].

إما عن المواقف الرسمية للمسئولين الأمريكيين فجاءت متوافقة مع الفقهاء القانونيين، حيث أكد الكثير منهم أن الهجوم الالكتروني يؤسس إلى قوة محظورة في القوانين الدولية بما فيها ميثاق الأمم المتحدة والقانون الدولي العرفي ففي عام ١٩٩٩ أصدرت وزارة الدفاع الأمريكية تقريراً مفصلا عن موقفها من الهجوم الالكتروني حيث أيدت فيه الموقف الأمريكي غير الرسمي بأن الهجوم الالكتروني يؤسس إلى قوة ضد سيادة الدولة وأمنها وسلامة أراضيها، وأنه وقوعه يؤسس لحالة الدفاع الشرعي المنصوص عليها في المادة ٥١ من ميثاق الأمم المتحدة باعتباره احد وسائل الرد وردع الدولة المعتدية[٢].

في عام ٢٠١٢ صرحت وزارة الخارجية الأمريكية في حال لو تعرضت الولايات المتحدة إلى هجوم الكتروني فإن الولايات المتحدة سوف ترد على هذه القوة لأنها لا تقل تهديداً عن الهجوم العسكري التقليدي، حيث كان لوزيرة الخارجية السابقة هيلاري كلينتون تصريحاً يحمل مدلولا بأن الهجوم الإلكتروني قوة تستوجب استخدام حق الدفاع الشرعي إذ قالت :

"States, terrorist and those who would act as their proxies must know that the United State will protect our network, those who engage in cyber-attack should face consequences and

1-Joshua Correll and Tracie Keesee, "Racial Bias in the Decision to Shoot?" The Police Chief, May 2009,

2- Matthew C. Waxman, Cyber-Attack and Use of Force: Back of the Future of Article 2(4), Yale Journal of International law Vol 36, 2013,P 430-437.

international condemnation in an interconnected world, an attack an one nation's network can be an attack on all"[1].

خلاصة لما تقدم فإن الإدارة الأمريكية مع المبدأ العام السائد لدى فقهاء القانون الدولي بأن الهجوم الالكتروني يعتبر قوة مستخدمة ممنوعة تحث ميثاق الأمم المتحدة والقانون الدولي العرفي ولكنها لم تصرح بذلك رسمياً دفعاً لأي حرج يحصل، وهذا أحد أساليب الإدارة الأمريكية المتبعة في السياسة الدولية والقانون الدولي.

المطلب الثالث

الوضع القانوني للدولة المعتدية والمعتدى عليها

defenser and Attacker of Status Legal

إن الوضع القانوني للدولة المعتدية والمعتدى عليها يُعد أمراً بالغ الأهمية لأنه يحدد الآثار القانونية المترتبة على هذا الهجوم، فالوضع يختلف باختلاف تأثير هذا الهجوم على الدولة المعتدى عليها وحجم الدمار الذي يخلفه، وكذلك حق الدفاع الشرعي لا يقوم إلا إذا تضررت الدولة المعتدى عليها وكانت هذه الإضرار مباشرة لأن الفقه القانوني الحديث يسير نحو المساواة بين السلاح التقليدي والهجوم الالكتروني، لذا فإن الآثار التي تترتب على كلتا الدولتين تكون نفسها التي تترتب عند استخدام الأسلحة التقليدية كالأسلحة النووية والتدميرية[٢].

1-Amnesty International, US: Rights for All, 1998. P 13, http://www.amnesty.org/en/library/info/ AMR51/035/1998/en.

2-Ryan Gabrielson, Ryann Grochowski Jones and Eric Sagara, "Deadly Force, in Black and White," ProPublica, October 10, 2014, http://www.propublica.org/article/deadly-force-in-black-and-white

الفرع الأول : حق الدولة في الدفاع عن نفسها وفق ميثاق الأمم المتحدة

the Right of state to use self defence

اختلف فقهاء القانون الدولي في مدى إمكانية اعتبار الهجوم الالكتروني هجوماً مسلحاً يستوجب قيام حالة الدفاع عن النفس، فذهب جانب من الفقه إلى اعتماد نظرية الوسيلة المستخدمة Instrument–based وقالوا بأن الهجوم الالكتروني وحدة لا يمكن أن يؤسس هجوماً مسلحاً يستوجب حالة الدفاع عن النفس وفق المادة الحادية وخمسون من ميثاق الأمم المتحدة، وأيدوا حجتهم بأن الهجوم الالكتروني لا يتوفر فيه الصفة الأساسية التي ترتبط بالسلاح التقليدي Physical Characteristics Traditionally associated with Military، وبعبارة أخرى أن المهاجمون الالكترونيين لا يستخدمون السلاح التقليدي المتعارف عليه الذي ينتج عنه القوة الحقيقية المدمرة، وقالوا أن الهجوم الالكتروني يكون هجوماً مسلحاً إذا استخدم المهاجمون أسلحة عسكرية تقليدية مثل تفجير أجهزة الكومبيوتر والشبكات واستندوا في حجتهم على المادة ٤١ من ميثاق الأمم المتحدة حيث اعتبرت الرسائل اللاسلكية وتعطيل أجهزة والراديو لاتصل إلى درجة القوة المسلحة[١]، وكذلك استندوا على قرار الجمعية العامة للأمم المتحدة الذي وضع قائمة بالأعمال التي تؤسس ما يسمى بالعدوان ولم يكن من بينها الهجوم الإلكتروني.

وذهب أنصار هذا النظرية في حججهم إلى أن حلف شمال الأطلسي (الناتو) عقد اتفاقية بين أطرافه وأكدوا على مبدأ الدفاع المشترك ضد الهجمات الالكترونية، ونصت المادة الرابعة من الاتفاقية على الدول التشاور فيما بينها إذا وقع هجوماً الكترونياً وأن هذا الهجوم لا يعتبر هجوماً مسلحاً وعلى الدول الأعضاء المساعدة فيما بينها تطبيقاً لنص المادة الخامسة من هذه الاتفاقية، ومن مميزات هذه النظرية هي سهولة تطبيقها ولا ويثار بشأنها أي صعوبة لأن استخدام الأسلحة التقليدية والقوة

١–د.حازم علتم ، قانون المنازعات المسلحة الدولية، ط١ ، القاهرة، ١٩٩٤، ص ١٩٩.

المسلحة هو أمراً سهلا لتحديد طبيعتهُ ونطاقهُ ضمن دائرة النزاعات المسلحة، لكن اغلب الفقه هجر هذه النظرية لما تثيره من تعدي واضح على سيادة وامن الدول والحكومات [١].

وذهب بعض فقهاء القانون الدولي إلى اعتماد نظرية الهدف الأساسي Target-based، فذهب أنصار هذه النظرية الى أن الهجوم الالكتروني يمكن أن يصنف هجوماً مسلحاً عندما يستهدف النظام الحاسوبي والأساسي في الدولة، فإن حق الدولة في استخدام حقها في الدفاع عن النفس ينشئْ عندما يكون هناك أذى كافي ووشيك يبرر استخدام هذا الحق، وقال أستاذ القانون الدولي Walter Sharp أحد مؤيدي هذه النظرية بأن الهجوم الالكتروني يؤسس هجوماً مسلحاً ويعطي الحق للدولة في الدفاع عن نفسها عندما تخترق دولة ما أو جهة ما الأنظمة الوطنية الحاسوبية بغض النظر إذا ما سبب هذا الخرق أذى أو تعطيل أو تدمير البنى التحتية للدولة، وقال أنصارها بأن هذه النظرية تؤدي إلى حماية الأنظمة الوطنية الحساسة وتعطي الحق باستخدام الدفاع الشرعي أو الدفاع عن النفس عندما يتم اختراقها، لكن اغلب الفقهاء لم يؤيدوا هذه النظرية لما تثيره من نزاعات مسلحة بين الدول بسبب حماية الأنظمة الحاسوبية في الدولة [٢]

وذهب معظم الفقهاء القانون الدولي العام إلى اعتماد نظرية جديدة سميت نظرية التأثير المباشر Affects-Based، حيث جمعت هذه النظرية بين النظرتين السالفتين، إذ اعتمدت على العلاقة السببية بين الفعل والضرر النهائي الناتج من الهجوم، فعلى سبيل المثال أن الهجوم الالكتروني على خطوط الجوية لدولة أو الهجوم على البورصات أو هجوم الذي حصل على استونيا يعتبر هجوما الكترونيا ويستوجب قيام

١-د.رياض الصمد، تطور الإحداث الدولية في القرن العشرين، المؤسسة الجامعية للدراسات والنشر، بيروت، ط١ ،١٩٩٩ ص ٨٨.

٢-محمد يونس الصائغ، حق استخدام الدفاع الشرعي وإباحة استخدام القوة في العلاقات الدولية، الرافدين للحقوق، ٢٠٠٧، ص ١٨٧- ١٩٠.

حق الدفاع عن النفس لأن الضرر النهائي أو تأثيرات هذا الهجوم كافية لقيام هذا الحق[١].

الفرع الثاني : تطبيق القانون الدولي الإنساني على المهاجمين

Apply International Humaintrin law of Cyber Attackers

عرفت الجنة الدولية للصليب الأحمر القانون الدولي الإنساني بأنه: (مجموعة من القواعد والضوابط هدفها الحد من تأثير النزاعات المسلحة، وحماية الأشخاص الذين لا يشاركون في القتال كالمدينين أو الذين لم يُعدوا طرفاً في القتال مثل الجنود المقاتلين، كما يرمي إلى الحد من الوسائل المستخدمة في الصراع أملا في التخفيف من الخسائر البشرية والمادية المترتبة على النزاع المسرح)[٢] ، من خلال هذا التعريف فإن القانون الدولي الإنساني ينظم النزاعات المسلحة، ويراعى حقوق المدنيين إثناء وبعد هذه النزاعات وأن إحكامه وقواعده توثر على مستوى العنف وطبيعة التهديد الواقع على المجتمع، وبعد الحروب التي حصلت في العالم أنصرف اهتمام القانون الدولي الإنساني إلى معايير التمييز مختلفة لإعطاء الوصف القانوني سليم لكل قضية أو نزاع وكانت هذه المعايير تنصب على أهم المسائل الجوهرية في القانون الدولي الإنساني وهي التمييز بين المقاتلين وغير المقاتلين –التمييز بين البنى التحتية المدنية والعسكرية ،وحظر استخدام الهجمات المسلحة غير مناسبة مع حجم الخطر المحتمل الوقوع.

إن لهذا التمييز أهمية بالغة ؛ لأن المقاتلين يجب أن يلتزموا بقوانين الحرب وقواعد اتفاقية جنيف الأربع، فإن بعض القواعد لا تنطبق على غير المقاتلين، فقد عرفت المادة ٤٤ من البرتوكول الجنود أو المقاتلين (بأن الجنود لا يتمتعون بوصف المقاتلين من خلال اللباس العسكري أو حمل الأسلحة والمعدات أو المشاركة العلنية في

1- Malcolm N. Shaw, International Public Law, Cambridge: Cambridge University Press, 2008.

2- The 1949 Geneva Conventions I-IV and Additional Protocol I & II 1977.

المعارك مراجعة المادة)، والسؤال الذي يثار في هذا الصدد هل ينطبق القانون الدولي الإنساني على المهاجمين الإلكترونين في حال تم إلقاء القبض عليهم؟ وإذا تم إلقاء القبض عليهم هل سوف يعاملون كأسرى حرب[١].

وقبل الخوض في إمكانية تطبيق القانون الدولي الإنساني على المهاجمين الإلكترونين لابد من إعطاء وصف قانوني واضح لمفهوم النزاع المسلح، فإن اتفاقية جنيف الأربع لم تعرف النزاع وكذلك الملحق بالاتفاقية لم تتطرق إلى مفهوم النزاع المسلح، ولكن المحكمة الجنائية في يوغسلافيا عرفت النزاع المسلح بأنه(هو النزاع الذي يحصل عندما يتم اللجوء إلى القوة المسلحة بين الدول أو بين قوات مسلحة أو بين السلطات الحكومية)[٢].

إن المهاجمين الإلكترونين على الأرجح يكون هجومهم الالكتروني موجهه ضد الدولة أو شبكات الكومبيوتر المدنية وبالتالي فالهجمات الالكترونية لا تكون على الغالب ضد المواقع العسكرية لقوات العدو، كذلك أن نطاق الهجوم الالكتروني يفوق حدود القانون الدولي الإنساني وأهدافه، وإن الأهداف العسكرية هي التي وحدها تكون عرضه للهجوم الالكتروني وأن البنى التحتية للدولة يجب أن تكون محصنة عن الهجوم المتعمد.

وفيما يخص بقضية استونيا التي تعتبر القضية الأهم في القانون الدولي العام خاصة بالهجوم الالكتروني، فإن هجوم استونيا استهدف البنى التحتية للدولة فضرب البنوك، والمطارات، والمحطات الفضائية، والخدمات الحكومية، بالتالي فمن غير المعقول أن يوصف هؤلاء بمقاتلين لأن أهدافهم ليست عسكرية بل كانت مدنية بحته، ولكن بعض فقهاء القانون الدولي العام احتج على ذلك واستندوا بأن NATOهاجم

1- Michael N. Schmitt et al., Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge: Cambridge University Press, 2013)

2- Scott J Shackeford 555.

محطات التلفزيون وبعض الخدمات الحكومية في كوسوفو لم يخرج هذا الهجوم عن دائرة النزاع المسلح المستهدف القوات العسكرية، ولكن اغلب فقهاء القانون الدولي انتقدوا هذا الرأي وقالوا أن التدخل الإنساني في كوسوفو مختلف لأن NATOاستهدف بعض البنى التحتية كأن لغرض إدارة المعارك وللسيطرة العسكرية[١].

علاوة على ذلك أن قانون الحرب يفرض مسؤولية كبيرة على الدولة في حال استخدام قوة كبيرة أو أسلحة مدمرة لا تتوافق مع حجم الخطر العسكري المحتمل أو الفشل بالخلط بين الأهداف العسكرية والمدنية،[٢] ، فإن المتوقع أن الهجوم الالكتروني يخلف بعض الخسائر في الأرواح والأموال المدنيين إثناء العمليات فعند مقارنة الهجوم التقليدي بالإلكتروني وخاصة في بعض الدول التي تحدث فيها هجمات الكترونية فإن هذه الهجمات استهدفت المنشآت المدنية وخلفت خسائر مادية كبيرة للدول والمدنيين، وأن الدول المعتدى عليها لم تهاجم أي قوات مسلحة لذا أن تطبيق القانون الدولي الإنساني على الهجوم الالكتروني غير قانوني ولا يوجد له أساس تشريعي[٣].

المطلب الرابع

الرد على الهجوم الالكتروني

Attack Cyber of Response the

إن الدولة المعتدى عليها التي تنوي الرد على الهجوم الالكتروني باستخدام القوة المسلحة يجب عليها ليس فقد الالتزام بقواعد ميثاق الأمم المتحدة والقانون الدولي العرفي، بل عليها الالتزام بقواعد القانون الدولي الإنساني وهي الضرورة والتناسب، وإن مبدأ حالة الضرورة هو من الأمور صعبة التقييم ولكن تطبيقاً لهذا المبدأ يجب أن تكون القوة المسلحة الحل الأخير لمواجهة الدولة المعتدية، فإن الرد على الهجوم الالكتروني

١-المواد(٤٨ -٤٩) من ملحق البرتوكول الأول من اتفاقية جنيف لسنة ١٩٥١.

٢-المادة(٥١) بروتوكول ١ من اتفاقية جنيف ١٩٥١.

٣- المادة (٥٠) من ملحق البروتوكول الأول من اتفاقية جنيف لسنة ١٩٥١.

يجب أن يكون ضرورياً حتى يكون هذا الرد قانونياً ينطبق عليه صفة الدفاع الشرعي ، وبالتالي على الدولة المعتدى عليها التي تنوي الرد أن تحسب المنفعة التي تكمن في هذا الهجوم العسكري مقابل الهجوم الالكتروني الذي تعرضت إليه أنظمتها والمنشآت التابعة لها[١]، فإن المادة (٤٨) من الملحق الإضافي في اتفاقية جنيف حددت الأهداف التي تستطيع الدولة استهدافها وهي الأهداف العسكرية حصراً، وكذلك فإن الاتفاقية لاهاي الرابعة منعت اي تدمير أو مصادرة لممتلكات المدنيين وبالتالي فإن انتهاك هذه القوانين يعتبر جريمة دولية معاقب عليها في اتفاقية روما المنشئة للمحكمة الجنائية الدولية[٢].

أما عن المبدأ الثاني الذي يسمى التناسب بين الاعتداء الذي حصل والقوة التي سوف تنتج عن الدفاع الشرعي هو من المبادئ التي نصت عليها اتفاقية جنيف في الملحق الإضافي حيث نصت الفقرة (١) منها يتمتع السكان المدنيون والأشخاص المدنيون بحماية عامة ضد الإخطار الناجمة عن العمليات المسلحة ويجب لإضفاء فعالية على هذه على هذه الحماية مراعاة القواعد التالية دوما وبالإضافة إلى القواعد الدولية الأخرى القابلة للتطبيق)[٣] ، ووفقاً لهذا المبدأ فإنه يحضر إي استخدام للقوة إذا نتج عن هذه القوة إي إصابات أو خسائر مادية أو بشرية في المواطنين المدنيين التابعين لدولة المعتدية، فإن الدولة المعتدى عليها تواجه تحدياً فريداً من نوعه في استخدام القوة لأن صانعوا قرار استخدام القوة كوسيلة للدفاع الشرعي يجب أن يضعوا مصالحهم في كفة ومصالح المدنيين التابعيين لدولة المعتدية في كفة أخرى، فإن فقهاء

1- Oren Gross, Cyber Responsibility to Protect Legal Obligation of States Directly Affected by Cyber Incident, Cornell International Law Journal, Vol.48, p 504-510

2-Micheal Gervais, Cyber Attack an Law of wars, Berkeley Journal of International law, Volume 30, 2012 p 560.

3-Article 51 of additional Protocol I of Geneva Convention of 1977 .

القانون الدولي قالوا من الصعب أحياناً تقييم حالة التناسب عندما تتعرض مصالح وأرواح المدنيين للخطر[١]، ولكن بعضهم من قال بأن أرواح ومصالح المدنيين تكون في خطر عندما يتسبب الهجوم الالكتروني بتعطيل الأنظمة في مشفى أو مطار، وبالتالي فإن مبدأ التناسب يجب أن يكون قائماً في كل الأحوال لأنه من المبادئ المتأصلة في القانون الدولي الإنساني الغرض منه تقليل حجم الخسائر المدنيين [٢].

1-131. Protocol Additional I, supra note 130, arts. 51(5)(b), 54, 57(2)(a)(iii). A

fter deciding that the target is a military objective, the elements of the balancing test include "target selection, the means and methods chosen for the military strike, the lack of negligence in the execution of the military strike, and the determination of what constitutes the military advantage of a particular military strike." Randy W. Stone, Protecting Civilians During Operation Allied Force: The Enduring Importance of

the Proportional Response and NATO's Use of Armed Force in Kosovo, 50 CATH. U. L. REV. 501,

2-Military objectives are targets that meet two criteria: they serve a military purpose and

their incapacitation conveys a definite advantage. Protocol Additional I, supra note 130, art. 52(2). For example, the first missile strikes of Operation Desert Storm in 1991 targeted Iraqi radar stations. Kanuck, supra note 121, at 282. On distinction, see Doswald-Beck, supra note 134, at 165-71; Brown, supra note 86, at 195 (comparing malicious code, which is indiscriminate, to biological weapons). Schmitt also argues that indiscriminate weapons are unlawful, including in that category not only cyber-attacks that cannot distinguish civilian and military objects, but also those which cannot be limited to a military objective. Schmitt, supra note 84,

وكذلك فإن مبدأ التناسب ينطبق على التأثير غير المباشر للهجوم فإن الدولة المهاجمة مسئولة عن إي نتائج غير مباشرة عن الهجوم الذي حصل، وهذا ما نصت عليه المادة ٥٧ من الملحق الإضافي لاتفاقية جنيف لذا فإن الدولة التي تنوي استخدام حق الدفاع الشرعي وفقا لهذا المبدأ تفضل استخدام الهجوم الالكتروني عن الهجوم التقليدي لأن المخاطر المادية والبشرية التي تمس المدنيون والناجمة عن الهجوم الالكتروني اقل بكثير عن الهجوم التقليدي(١).

وأخيراً يجب على الدولة التي قررت استخدام القوة رداً على الهجوم الالكتروني أن تميز بين الأهداف العسكرية والأهداف الحكومية الأخرى، فلا يجوز للدولة أن تستخدم الدفاع الشرعي كذريعة لتدمير البنى التحتية لدولة المعتدية ، فإن الدولة التي تنوي الرد عن طريق استخدام هجوم الكتروني مضاد فعليها أن تلتزم بهذه المبادئ وأن تكون أهداف الهجوم مقتصرة على المطارات العسكرية، ومنشآت الأسلحة، والمفاعل النووية، لذا يجب على الدولة أن لا تهاجم مصالح المدنيين من بنوك ومستشفيات ومواصلات تطبيقاً لهذه المبادئ الإنسانية (٢).

---

at 201 (citing Protocol Additional I, supra note 130, art. 51(4)) 138. Protocol

2-Geoffrey S. Corn, Unarmed but How Dangerous? Civilian Augmentees, the Law ofArmed Conflict, and the Search for a More Effective Test for Permissible Civilian BattlefieldFunctions, 2 J. NAT'L SEC. L. & POL'Y 257, 286-87 (2008). Although the principle that a civilian who directly participates in hostilities or who adopts a continuous combat function may be lawfull yattacked is not in dispute, the status of a civilian who provides indispensable, contemporaneous assistance in cyber-attacks remains unresolved.

الخاتمة

بعد الانتهاء من عرض المباحث الأساسية في بحثنا فقد توصلنا إلى مجموعة من النتائج والتوصيات وكما يأتي:

أولا-الاستنتاجات

١- غالباً ما يكون الفرق بين الجريمة الالكترونية والهجمات الالكترونية هو اختلاف الهدف في كل منهما، فالهدف في الهجوم الالكتروني سياسي إما الهدف في الجريمة الالكترونية هو مالي.

٢-لا يوجد نص صريح في القانون الدولي سواء كأن مكتوباً أو عرفياً يتعامل مع الهجوم الالكتروني فهو وليد التطور التكنولوجي الذي حصل في العالم، بالتالي فإن تطبيق نصوص ميثاق الأمم والمتحدة ومعاهدة جنيف الأربع على الفعل أصبح من القواعد الأساسية المتعارف عليها في القانون الدولي للتشابه الكبير بين الهجوم الالكتروني والهجوم التقليدي.

٣-أن الدولة المعتدى عليها لها الحق في استخدام حق الدفاع الشرعي ولكن يجب أن تلتزم بالحدود المقررة في القانون الدولي كالضرورة والتناسب والضربات الموجهة ضد الأهداف العسكرية.

٤-لا يمكن أن يطبق القانون الدولي الإنساني على المهاجمين ولا يمكن اعتبارهم أسرى حرب.

ثانيا-التوصيات

١-على الدول عقد معاهدات شارعه تؤكد فيه مخالفة هذا التصرف للقانون الدولي وتحدد العقوبات المناسبة لردع الدول التي تنوي استخدام مثل هذه الأسلحة.

٢-يجب تعديل ميثاق الأمم المتحدة ليشمل بعض التصرفات التي تهدد الأمن والسلم الدوليين ومنها الهجمات الالكترونية .

٣-على الدول عدم استخدام هذا النوع من الهجمات في حال حدوث توتر أو نزاع لأنه يؤدي إلى كوارث عالمية.

المصادر

أولا–المؤلفات العامة

١–د.حازم علتم ، قانون المنازعات المسلحة الدولية، ط١ ، القاهرة،١٩٩٤ .

٢–د. رياض الصمد، تطور الإحداث الدولية في القرن العشرين، المؤسسة الجامعية للدراسات والنشر، بيروت، ط١ ،١٩٩٩ .

٣–كمال حماد، النزاع المسلح والقانون الدولي العام، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، لبنان الطبعة الأولى ١٩٩٧ .

٤–محمد يونس الصائغ، حق استخدام الدفاع الشرعي وإباحة استخدام القوة في العلاقات الدولية، الرافدين للحقوق ، ٢٠٠٧ .

ثانيا–المعاهدات الدولية

١– معاهدة لاهاي الرابعة ١٨٩٩–١٩٠٧.

٢–ميثاق الأمم المتحدة ١٩٤٥ .

٣–معاهدة جنيف عام ١٩٥١ .

٤– قانون المحكمة الجنائية الدولية ٢٠٠٢.

ثالثاً–المصادر باللغة الانكليزية :

1–Scott J. Shackelford, From Nuclear War to Net War: Analogizing Cyber Attacks in International Law, Shackelford

2– Ian Traynor, Russia Accused of Unleashing Cyber war to Disable Estonia, GUARDIAN (LONDON), May 17, 2007

3–Pamela Hess, Pentagon Puts Hold on USAF Cyber Effort, ASSOCIATED PRESS, Aug. 13 2008.

4-France v. Turkey (the Lotus Case) PCIJ, 1927, PCIJ Reports series A, No. 104.

5-Oona A. Hathaway, The Law of Cyber Attack, Yala Law School, 2012.

6- Joshua Correll and Tracie Keesee, "Racial Bias in the Decision to Shoot?" The Police Chief, May 2009.

7- Matthew C. Waxman, Cyber-Attack and Use of Force: Back of the Future of Article 2(4), Yale Journal of International law Vol 36, 2013

8- Malcolm N. Shaw, International Public Law, Cambridge: Cambridge University Press, 2008.

9- Michael N. Schmitt et al., Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge: Cambridge University Press, 2013)

10-Oren Gross, Cyber Responsibility to Protect Legal Obligation of States Directly Affected by Cyber Incident, Cornell International Law Journal, Vol.48,

11- MichealGervais, Cyber Attack an Law of wars, Berkeley Journal of International law, Volume 30, 2012.

12-Geoffrey S. Corn, Unarmed but How Dangerous? Civilian Augmenters, the Law of Armed Conflict, and the Search for a

More Effective Test for Permissible Civilian Battlefield Functions, 2 J. NAT'L SEC. L. & POL'Y (2008).

رابعا-المقالات والكتب الالكترونية:

1-Amir Efrati& Siobhan Gorman, Google Mail Hack Is Blamed on China, WALL ST. J., June 2, 2011, at A1; Wyatt Andrews, China Google Hacker's Goal: Spying on U.S. Govt, CBs NEWS (June 2, 2011),

http://m.cbsnews.com/fullstory.rbml?catid=20068474&feed_i.

2-Bahrain Government, the Central management for combating the corruption

http://www.acees.gov.bh/cyber-crime/the-concept-of-e-crime

3-Brian Krebs, Report: Russian Hacker Forums Fueled Georgia Cyber Attacks WAS.POST SECURITY FIX BLOG (Oct. 16, 2008, 3:15 PM), http://voices.washingtonpost.com/securityfix

4-Ian Traynor, Russia Accused of Unleashing Cyber war to Disable Estonia∧GUARDIAN (May 16, 2007),

http://www.guardian.co.uk/world/2007/may/17/topstories3.russia

5-Ryan Gabrielson, RyannGrochowski Jones and Eric Sagara, "Deadly Force, in Black and White," ProPublica, October 10, 2014,

http://www.propublica.org/article/deadly-force-in-black-and-whit

المـلخـص:

تثير الهجمات الالكترونية أهمية بالغة لما تخلفه من آثار كارثية على الدولة ومرافقها العامة، فضلا عن تأثيرها المباشر الذي يمس المواطنون المدنيين في الدولة، فالهجمات الالكترونية هي نتيجة لتطور المجتمع والتعقيدات التقنية التي حصلت بعد الثورة التكنولوجية في العالم، فقد أصبحت كل المرافق الحكومية وغير الحكومية تدار الكترونياً، فإن تعطليها أو إيقافها أمراً له خطورة بالغة، لذا فإن النظم القانونية الدولية في بداية الأمر لم تتعامل معها باعتبارها أمراً يهدد امن الدولة وسيادتها ولكن العالم أدرك بعد تكرار هذه الهجمات وفعاليتها التي تتساوى مع الأسلحة التقليدية المدمرة أنهم بحاجة التي إعادة تكييف النظام القانوني الذي يتعامل مع الأسلحة التقليدية لجعله واسع النطاق ليشمل هذا النوع من الاعتداءات، فلا مناص الآن من تطبيق قواعد ميثاق الأمم المتحدة وبعض المعاهدات الخاصة بقانون الفضاء والنزاعات المسلحة على هذا النوع الجديد من الأسلحة، فالقوة الناتجة عنه فاقت في بعض الدول المتضررة مثل استونيا القوة الناتجة عن السلاح النووي، وأدت إلى تعطيل شبه كامل لكل مرافق الحياة في هذه الدول، لذا فقد ذهب معظم فقهاء القانون الدولي في اتجاه البحث عن مخرج يجعل من تطبيق قواعد ميثاق الأمم المتحدة ونظمها على الهجمات الإلكترونية لا يتعارض مع القانون الدولي بشقيه العرفي والمكتوب.

ABSTRACT :

The cyber attack is extremely important for its disastrous effects on the state and its public facilities, as well as its direct impact on the country's civilian population, Electronic attack is the result of the development of society and the technical complexities that occurred after the technological revolution in the world, All the governmental and non-governmental facilities have been electronically managed, International legal systems initially do not deal with it as a threat to the security and sovereignty of the state, Nowadays, There is no way to get rid of this threat just to apply the rules of the Charter of the United Nations and some treaties on the law of space and armed conflicts to this new type of weapons, the resulting force exceeded in some of the affected country, such as Estonia, the power resulting from nuclear weapons, has led to almost complete disruption of all life facilities in these Countries.