الأبعاد الاستراتيجية والقانونية للحرب السيبرانية

بقلم
د/ يحي مفرح الزهراني(*)

ملخص

يحاول الباحث في هذا البحث تسليط الضوء على مفهوم الحرب السيبرانية، والمصلحات والمفاهيم الخاصة بها، في دراسة للأبعاد الاستراتيجية والقانونية وكذلك التفرقة بين مجالاتها من ناحية الحرب السيبرانية وكذلك الأمن السيبراني (الالكتروني)، علاوة على تطور تلك الظاهرة في محاولة للوصول للقواعد القانونية التي يمكن أن تنطبق عليها، سواء في حال السلم أو الحرب.

حيث تتعرض الكثير من الدول لما يسمى بالاختراقات الإلكترونية وكذلك قد تتطور إلى ما يسمى الحرب السيبرانية بالمفهوم الشامل للظاهرة، والذي قد يشمل مصادر تهديد خارجية، وبالتالي يطرح التساؤل الاستراتيجي والقانوني، ما هو دور و مسؤولية الدول في ضوء القانوني الدولي في التعامل مع هذه الظاهرة، وما هي الاستراتيجيات (استباقية – دفاعية – احترازية) يمكن تطبيقها للحماية من الأخطار والتهديدات الالكترونية، مع التباين الذي يتشكل ما بين الحرب السيبرانية والحرب التقليدية.

الكلمات المفتاحية: القانون، السياسة، الحرب، الاستراتيجية، السيبرانية.

مقدمة

يشكل الفضاء الالكتروني وما يتعلق به من أدوات تقنية و معلوماتية بعدا مستقبليا هاماً للنزاع والصراع بشتى درجاته وأنواعه، ومع تزايد الاعتماد على الشبكات والاتصالات والمعلومات، تزداد يوما بعد يوم، الاعتمادات والطرائق التي تشكل فيها التقنية وسيلة هامة للأمن والدفاع.

ولذا، تسعى الدول للحفاظ على بنيتها وأجهزتها الحيوية التقنية الالكترونية والدفاع عنها،

(*) كلية العلوم الاستراتيجية ـ جامعة نايف للعلوم الأمنية ـ المملكة العربية السعودية.

ومن هنا تشكل هذه الدراسة أهمية في بحث الظاهرة والمفهوم، والتفصيل في مفهوم الحرب الالكترونية، وكذلك الجوانب القانونية الخاصة بالردع أو الدفاع الالكتروني من وجهة نظر القانوني الدولي.

حرب الانترنت هي حرب يتم شنها من خلال أجهزة الحاسب الآلي وشبكة الانترنت. وهي تشمل على حد سواء إجراءات هجومية لإلحاق الضرر والأذى بنظم معلومات الخصوم، وأخرى دفاعية لحماية النظم الخاصة بالمهاجمين، حماية لنظمهم من أن تهاجم. وما يسبب الإرباك استخدام المصطلح لوصف عمليات عسكرية تستخدم تقنيات تعتمد على المعلومات، و هذا جمع بينه وبين مصطلحي حرب المعلومات والحرب القائمة على الشبكات.إن الدول الحديثة وقواتها المسلحة تعتمد بشكل متزايد على أجهزة الحاسب، وقد تسبب الهجمات على هذه الأجهزة ضررا مساويا لما يسببه هجوم عسكري تقليدي[1]

لقد زادت التقنيات الرقمية من فاعلية الحروب الالكترونية، فكان أول إعلان عن دخول التقنيات الرقمية ميادين الحروب في حرب البلقان في نهايات القرن الماضي على يد حلف الناتو ضد الصرب فيما سمي "بالقنابل المعتمة"، وقد أدى هذا الهجوم الإلكتروني إلى توقف شبكة الحاسب الرئيسية مما أصاب نظم الكمبيوتر الخاصة بوزارة الدفاع اليوغسلافية بالشلل التام.

ولحرب الانترنت عدة أهداف، هي: استغلال معلومات الآخرين للمصلحة الشخصية أي التجسس على الآخرين، وخداع العدو، و تعطيل نظم معلومات العدو أو حرماته مؤقتا، أو تغييرها أو تدمير هذا النظام، وتشمل الطرق: مهاجمة البيانات، مثل إغراق البريد الالكتروني برسائل إعلانية يمكن أن تزيد الحمل على نظام الحاسوب وتسبب له التعطل، واختراق أجهزة الحاسوب من اجل انتزاع معلومات أو بث معلومات مغايرة، وعمليات مهاجمة البرامج مثل الفيروسات و الديدان الالكترونية و القنابل المنطقية، والهجمات المادية على أجهزة الحاسوب او نظم الاتصالات التي تربطها.[2]

وقد حاولت مختلف الأطراف الدولية التوصل إلى الأطر القانونية الدولية لتوضيح ما هو مقبول وما هو غير مقبول فيما يتعلق بالحروب السيبرانية وقد تم اصدرا دليل تالين، الذي نشر في عام 2013، وهو دراسة أكاديمية في القانون الدولي، ولاسيما في شن الحرب والقانون الإنساني الدولي، تنطبق على النزاعات السيبرانية والحرب الإلكترونية. وقد أصدر كذلك مركز حلف شمال الأطلسي مستنداً حول الدفاع السيبراني 2009 و 2012.

قامت كذلك منظمة شنغهاي للتعاون (تشمل أعضاء منها الصين وروسيا) بوضع تعريفات للحرب الإلكترونية لتشمل نشر المعلومات "الضارة إلى الأجواء الروحية والأخلاقية والثقافية

للدول الأخرى". في سبتمبر 2011، اقترحت هذه الدول إلى الأمين العام للأمم المتحدة وثيقة تسمى "مدونة السلوك الدولية لأمن المعلومات". [3] في المقابل، يركز نهج الولايات المتحدة على الضرر المادي والاقتصادي والإصابات، ووضع المخاوف السياسية في ظل حرية التعبير. وقد أدى هذا الاختلاف في الرأي إلى تردد في الغرب لمتابعة اتفاقيات الحد من الأسلحة السيبرانية العالمية.[4]

وقد وضع أستاذ للقانون الدولي، الكسندر مرسنكهو، مشروعا يسمى الاتفاقية الدولية لحظر حرب الإنترنت في الإنترنت. ووفقا لهذا المشروع، يرى الدكتور الكسندر بأن الإنترنت يجب أن تظل خالية من تكتيكات الحرب وأن تعامل على أنها معلما دوليا. ويذكر أن شبكة الإنترنت (الفضاء الإلكتروني) هو "التراث المشترك للبشرية".[5]

مشكلة الدراسة:

تسعى الدراسة لمعرفة كيفية التفاعل المستقبلي للحرب الالكترونية بين المكونات الاستراتيجية التقنية و المكونات القانونية التي تعطي حق الدفاع وعن أشكالها المتوقعة،وكيف يمكن للقانون الدولي تغطية تلك الأنماط المعقدة بحسب طبيعة الحرب ومصدرها.

وبصيغة أخرى يمكن القول: كيف عالج القانون الدولي والقانون الدولي الإنساني، مسألة الحرب السيبرانية وفي أي سياق مع اختلاف نمط وموقع الهجوم.

أهداف الدراسة:

- التعرف على مفهوم الحرب السيبرانية
- التعمق في معرفة أنماط الحرب السيبرانية
- التحليل القانوني والاستراتيجي لأنماط الهجمات وسبل الدفاع الالكتروني قانونياً

أهمية الدراسة:

تشكل الدراسة أهمية علمية في الإضافة للمكتبة العربية للأبحاث المتخصصة حول الحرب الالكترونية، حيث تعاني المكتبة العربية من شبه انعدام للمراجع المتخصصة حول هذا الموضوع الهام، والذي أصبح من الشواغل المستقبلية لجهات الأمن والدفاع الوطني.

تشكل كذلك الدراسة أهمية عملية في معرفة التحليلات والنصوص القانونية التي تعنى بالحرب الالكترونية، والتي ستكون أداة هامة في شرعية الدفاع والأمن الالكتروني، ومن ناحية أخرى أداة للدفاع الدولي في حال التقاضي القانوني أو السياسي كون ذلك الدفاع يرتكز على مبادئ الدفاع في القانون الدولي.

مصطلحات الدراسة:

الفضاء الالكتروني: مصطلح حديث، ظهر في العقود الأخيرة نتيجة لثورة تكنولوجيا

المعلومات. ويشمل الفضاء الالكتروني، في ما يشمل، جميع الحواسيب والمعلومات التي بداخلها والأنظمة والبرامج والشبكات المفتوحة لاستعمال الجمهور العام أو تلك الشبكات التي صممت لاستعمال فئة محددة من المستعملين ومنفصلة عن شبكة الإنترنت العامة.[6]

حرب الانترنت: هي حرب يتم شنها من خلال أجهزة الحاسب الآلي وشبكة الانترنت. وهي تشمل على حد سواء إجراءات هجومية لإلحاق الضرر والأذى بنظم معلومات الخصوم، وأخرى دفاعية لحماية النظم الخاصة بالمهاجمين، حماية لنظمهم من أن تهاجم. وما يسبب الإرباك استخدام المصطلح لوصف عمليات عسكرية تستخدم تقنيات تعتمد على المعلومات، و هذا جمع بينه و بين مصطلحي حرب المعلومات والحرب القائمة على الشبكات. يمكن كذلك تعريفها بمصطلح الحرب السيبرانية والتي تعرف بأنها إجراءات من قبل الدولة القومية لاختراق أجهزة الكمبيوتر أو شبكات دولة أخرى لأغراض التسبب في ضرر أو تعطيل ولكن تشمل التعاريف الأخرى أيضا الجهات الفاعلة غير الحكومية، مثل الجماعات الإرهابية، الشركات والجماعات السياسية أو الأيديولوجية المتطرفة، المخترقون الأفراد، والمنظمات الإجرامية العابرة للحدود.

الشبكة المعلوماتية: ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها، مثل الشبكات الخاصة والعامة والشبكة العالمية (الانترنت) (نظام مكافحة الجرائم المعلوماتية 2007).

الجريمة المعلوماتية: أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لإحكام هذا النظام (نظام مكافحة الجرائم المعلوماتية 2007).

نظام المعلومات: مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات أو المعلومات أو الرسائل الالكترونية أو غير ذلك (مدني، 2007).

حق الخصوصية: تعني حقوق الخصوصية هو التحرر من التدخل والحق في حفظ المعلومات الشخصية بدون اطلاع أحد عليها ولا يجوز لأحد الحق بالتدخل بهذه المعلومات الشخصية أو الإفصاح عنها أو تقديمها إلى العامة (معجم أكسفورد، 2009)

منهجية الدراسة:

المنهج الوصفي التحليلي ويمكن تعريف المنهج الوصفي بأنه أسلوب من أساليب التحليل المرتكز على معلومات كافية ودقيقة عن ظاهرة أو موضوع محدد، عبر فترة أو فترات زمنية معلومة وذلك من أجل الحصول على نتائج عملية تم تفسيرها بطريقة موضوعية تنسجم مع المعطيات الفعلية للظاهرة.

ولذا يعتبر المنهج الوصفي خطوة أولى وهامة في كل مجال معرفي، لأن طبيعة الدراسات

الوصفية أنها تكشف في معظمها عن ماهية الظاهرة و الظواهر المختلفة.

وسوف تقوم الدراسة، باستعراض مفهوم الحرب الالكترونية و الفضاء الالكتروني، وكذلك استعراض القوانين الخاصة بالحالات، عندما يكون الهجوم من خارج الإقليم الخاص بالدولة، و كذلك عندما يكون الهجوم من داخل إقليم الدولة، علاوة على استعراض مفهوم الدفاع الوقائي الالكتروني في القانون الدولي الإنساني.

المنهج الاستنباطي وهو المنهج الذي يبدأ من الحقائق الكلية لينتهي إلى الحقائق الجزئية، ومن هنا سعى البحث إلى استخلاص التحليلات من القانون الدولي والدولي الإنساني، إلى موضوع الحرب الإلكترونية تحديدا والتي هي من ضمن المواضيع المتعددة التي يغطيها هذا القانون، ليقوم بتطبيقها على الحالات الخاصة.

الدراسات السابقة:

"حرب الفضاء الالكتروني: اتجاهات وتأثيرات على إسرائيل"، للباحثين شموئيل ايفن ودافيد بن سيمان- طوف، العاملين في معهد أبحاث الأمن القومي.

ويضم الكتاب مقدمة وأربعة فصول وخاتمة وملحقين، بما مجموعه تسعين من الصفحات. وأشار المؤلفان إلى أن الفضاء الالكتروني بات مجال قتال جديد، وانظم بذلك إلى مجالات القتال الأخرى، في اليابسة والبحر والجو والفضاء. فالدول المتطورة وجيوشها تزيد من نشاطاتها وأبحاثها في الفضاء الإلكتروني الذي أصبح يشكل بالنسبة لها مصدر قوة عظيمة، ولكنه في الوقت نفسه يكشف خاصرتها الضعيفة، لأن البنى التحتية التي تقوم عليها الدول الحديثة مثل الكهرباء والمياه والمواصلات والاتصالات والبورصة والبنوك تعتمد في عملها على الفضاء الالكتروني. وكذلك شبكات القيادة والسيطرة والتحكم العسكرية ومختلف أنواع التكنولوجيا المتطورة في ساحات القتال؛ مثل: أنظمة جمع المعلومات، واستعمال الأقمار الصناعية والطائرات من دون طيار في الحرب؛ كلها تعتمد على الفضاء الإلكتروني.

ويقول صاحبا الكتاب إن الدفاع في حرب الفضاء الالكتروني يشكل تحدياً من نوع جديد لإسرائيل، وذلك لأنه بمقدور العدو شن هجمات بسرعة البرق ومن الصعوبة بمكان تحديد من هو المهاجم. ويوصي المؤلفان أن تتعلم إسرائيل وتستفيد من مفهوم "الدفاع الفعال" في الفضاء الإلكتروني الذي تتبعه الولايات المتحدة الأميركية. إذ يستند هذا "الدفاع الفعال" على قدرة مخابراتية متطورة لتحديد النشاطات في الإنترنت وعلى أنظمة دفاع دينامية ذات رد تلقائي من دون تدخل الإنسان. ويستطرد المؤلفان، إن "الدفاع الفعال" لا يعتمد فقط على التكنولوجيا المتطورة، وإنما أيضا على شبكة محكمة ذات قواعد وإجراءات صارمة وعلى ثقافة

تفهم المخاطر وعلى انضباط شديد وعلى حماية المواقع وعلى رقابة بشرية قوية.[7]

ويوصي المؤلفان، في ضوء اعتراف الجيش الإسرائيلي بالفضاء الالكتروني كساحة قتال إلى جانب الساحات الأخرى، بإجراء تغييرات في قوات الجيش الإسرائيلي والعمل على إقامة جيش خاص بالفضاء الالكتروني، أسوة بالقوات البرية والبحرية والجوية.

وكتب هيثر كينقزبري رسالة لنيل درجة الماجستير في الأمن السيبراني من جامعة أوتيكا في الولايات المتحدة الأمريكة، ديسمبر 2014، بعنوان "مدى انطباق القوانين الدولية على الحروب السيبرانية ."

تعد تلك الدراسة من الدراسات الحديثة و التي تهدف إلى البحث في سبب تضافر جهود الدول لإيجاد قوانين دولية تحكم الحرب الالكترونية، كمان أنها قامت بدراسة محاولات وضع تنظيم يحكم الفضاء السيبراني أثناء الهجمات السيبرانية المتوقعة مستقبلا. بالإضافة إلى تقديمها العديد من التوصيات والتي المتعلقة بالخطوات المطولة لإعداد قواعد قانونية دولية خاصة بالحروب السيبرانية.

وقد اشتملت فصول تلك الدراسة على تعريف بظاهرة الحروب السيبرانية، و مدى انطباق مبدأ حظر استخدام القوة المنصوص عليها في ميثاق الأمم المتحدة (المادة 4/2) على الهجمات السيبرانية، كمان أنه خصص أحد الفصول لدراسة دليل تالين الخاص بالحرب السيبرانية، ومن ثم خصص فصلا آخر لاتسعراض مدى انطباق القانون الدولي السيبراني على هذا النوع من الحروب، بالإضافة إلى الاستشهاد بالهجمات السيبرانية التي تعرضت لها استونيا كنموذج قضية لدعم هذه الدراسة.

أما البحث الحالي فهو سيثري المحتوى العربي فيما يتعلق بموضوع الحرب الالكترونية والأمن السيبراني، كما أن تلك الدراسات صادرة من كلية العلوم فتتناول الجانب البرمجي والحاسوبي أكثر من تناولها للجانب القانوني والسياسي.

الدراسة التي أعدها البروفيسور ماثيو واكسمان، بعنوان "الهجمات السيبرانية واستخدام القوة بالرجوع إلى المادة البند 4 من المادة الثانية في ميثاق الأمم المتحدة، بحث منشور في مجلة يال للقانون الدولي، الإصدار رقم 36، 2011م.

تهدف الدراسة إلى توضيح تفاسير حديثة متعلقة بالفقرة 4 من المادة 2 في ميثاق الأمم المتحدة، لمحاولة تطبيقها على الهجمات السيبرانية، ولتوضيح الآثار المترتبة على التطورات في قواعد القانون الدولي. كما تهدف هذه الدراسة إلى تقديم فهم أفضل للعلاقة بين قواعد استخدام القوة في القانون الدولي والتكنولوجيا. وستربط هذه الدراسة تفسيرات وكتابات

الفقهاء أثناء الحرب الباردة بخصوص المادة السالفة الذكر. فضلاً عن ذلك فقد استدل الباحث بجهود الولايات المتحدة الأمريكية في محاولات تفسير المادة (4/2) من الميثاق.

وقد تضمنت فصول ذلك البحث على استعراض لتفسيرات مصطلح "القوة" الوارد في المادة (4/2) من الميثاق، بالإضافة إلى تخصيص أحد البنود لاتسعراض تفسيرات الولايات المتحدة بهذا الشأن، كمان تناول الباحث في بقية الفصول الصراع التكنولوجي والكتابات الخاصة بالميثاق خلال الحرب الباردة، بالإضافة إلى توضيح التحديات التي تواجه مهمة تفسير المادة (2/4) في ظل الهجمات السيبرانية.

أما الدراسة الحالية، فهي لا تنحصر في تجربة الولايات المتحدة الأمريكية، ولم تنحصر في تفسير المادة (4/2) من الميثاق، بل تم تناول العديد من المبادئ الدولية والمواد الأخرى في الميثاق تم الارتكاز عليها أثناء هذه الدراسة.

مقدمة من ماثيو هوسينقتتون، بعنوان " استخدام القوة في الحرب الالكترونية و مبدأ الدفاع عن النفس "، بحث منشور في دورية جامعة بوسطن للقانون الدولي و القانون المقارن، المجلد رقم 32 الإصدار 2، 2006 م.

لقد سعت تلك الدراسة إلى رسم الخطوط العريضة لمعرفة حقوق كل أطراف النزاع السيبراني، وتحديدا الحق في الدفاع الشرعي، وذلك عن طريق محاولة الوصول إلى تعريف واضح و مجمع عليه للحرب الإلكترونية من خلال البحث في قانون اللجوء للحرب. بالإضافة إلى البحث في تصنيف واضح للهجمات الالكترونية قياسا على المعايير الخاصة بالحرب المادية (الحركية)، وقد تناولت الدراسة مدى أحقية التناول في الدفاع عن نفيها والرد بحسن نية على الهجمات السيبرانية وفقا للقانون الدولي وذلك لحماية البنية التحتية لتلك الدولة.

لقد اقتصرت هذه الدراسة على تناول حق الدفاع الشرعي ومحاولة تكييفه داخل مفهوم الحرب السيبرانية، ولكن الدراسة الحالية ستتناول حق الدفاع الشرعي ولكن بجانب موضوعات أخرى تثيرها الحرب الإلكترونية، مثل موقف القانون الدولي الإنساني ومدى انطباقه عليها، و.....

مقدمة من يورام دينستين، بعنوان "الهجمات على شبكات الكمبيوتر و الدفاع عن النفس"، مجلة دراسات القانون الدولي، المجلد 76، 2002 م.

تتناول هذه الدراسة مبدأ الدفاع الشرعي ضد الهجمات الالكترونية، و مدى أحقية الدول في اتخاذ التدابير الإلزامية ضد هذه الهجمات، كما تبين الدراسة حالة الدفاع الفردي أو الجماعي ضد هذا النوع من الهجمات، حيث تقوم هذه الدراسة على الاجتهاد من الباحث لإيجاد تنظيم فيما

يخص استعمال حق الدفاع عن النفس، في ظل عدم وجود قرارات ملزمة صادر من مجلس الأمن.

ويستهل الباحث الدراسة باستعراض مفهوم الهجمات الالكترونية، ومن ثم دراسة هذه الهجمات الموجهة إما للأفراد أو للشركات،وبعد ذلك توضيح مفهوم الدفاع الشرعي ومدى شرعيته في الحرب الإلكترونية، ويليه دراسة تحليلية للشروط الثلاثة الواجب توافرها– في نظر الكاتب – ليثبت الحق في الدفاع (الضرورة، التناسب، الفورية)، وفي فصل آخر يوضح الباحث مشكلة إثبات نسبة الهجمات لجهة معينة.

تلك الدراسة ركزت على الدفاع الشرعي بالتفصيل، وما يميز هذا البحث أنه تناول الدفاع الشرعي من عدة نظريات بشكل موجز لأنه لم يقتصر عليه، بالإضافة إلى أن هذه الدراسة تتسم بالحداثة ومواكبة التطورات، فمن عام 2002 حتى العام الحالي، الكثير من التغيرات والأحداث والهجمات السيبرانية استجدت.

boyd, d. m., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1), article 11

وتطرح هذه الدراسة تاريخ ونشأة تلك الشبكات الاجتماعية وتطورها والظواهر التي طرأت عليها وأبرز ما يميزها من سمات وقد تناولت كذلك هذه الدراسة تأثير الشبكات الاجتماعية على المجتمع وطرق التواصل البيني.

ويمكن كذلك أن يستفيد الباحث من هذه الدراسة عن طريق دراسة أهمية هذه الشبكات ومدى تأثيرها على المجتمع وأهمية التفاعل القانوني مع ما تمثله من دخول إلى حياة المواطن في المملكة العربية السعودية.

عولمة تكنولوجيا المعلومات وواقع التوظيف المجتمعي للإنترنت: دراسة تحليلية من منظور سوسيولوجي د.إبراهيم إسماعيل عبده محمد 2009.

وتتحدث هذه الدراسة عن "رصد واستيعاب بعض التحولات التي تجري في سياق العولمة، لاسيما ما يتعلق بالتوظيف المجتمعي لتتاجاتها في المجال التكنولوجي والمعلوماتي المتمثل في شبكة الإنترنت أيضا فإن شبكة الإنترنت تظل واحدة من الوسائل الاتصالية الحديثة التي تتطلب إجراء المزيد من الدراسات و البحوث حول الأبعاد المختلفة التي تكتنف استخداماتها المتنامية وغير المحدودة، وخاصة بالنظر إلي ما تثيره الجوانب الاجتماعية لهذه الاستخدامات من نقاشات واسعة ومحتدمة وذات أبعاد عدة على المستوى العالمي؛ فمن ناحية فإن شبكة الإنترنت تعد من أحدث وسائل الاتصال الإنساني و أكثرها فاعلية في العصر الحديث.

وقد تضمنت أهداف الدراسة إلقاء الضوء علي نماذج من المعالجات البحثية التي تناولت

بالأساس قضية التوظيف المجتمعي للإنترنت والجوانب محور الاهتمام في هذا الصدد. وقد انتهت الدراسة إلي صياغة رؤية استشرافية تتناول المحددات النظرية والآليات التطبيقية الملائمة نحو الإفادة الفاعلة من الإمكانات العولمية لتكنولوجيا المعلومات والإنترنت في المجتمعات العربية"(محمد، إبراهيم، 2009)

المبحث الأول: قوانين الانترنت والتداخل القانوني لتنظيماته

قوانين الانترنت هي مجموعة القواعد والتنظيمات التي تضع المعايير للمستخدمين ومقدمي الانترنت والعمليات التي تقوم بين المستخدمين بعضهم البعض أو المستخدمين ومقدمي الخدمات أو السلع ويطلق على هذا المصطلح باللغة الانجليزية مسمى "cyber law".

وقبل بدء الحديث عن قوانين الانترنت يجب أن نورد مقدمة بسيطة لقرائنا الأعزاء عن الانترنت كوسيلة اتصال لا محدودة.

مع ظهور عصر الانترنت والانفتاحية في مجال الاتصال تطورت أداة جديدة وهامة قادرة على تخطي الحدود الجغرافية وتخطي كل حاجز أمني بكل سهولة و إيصال أي معلومة إلى أي مكان بسرعة لم يكن لأحد أن يتخيلها.

والانترنت شبكة اتصال واسعة وعالمية تسيطر على تلك الخدمة الولايات المتحدة الأمريكية ممثلة بمنظمة "الايكان" "ICANN" وقد دارت عدة معارك سياسية ودبلوماسية بخصوص توزيع هذه السلطة الأمريكية لجعلها سلطة متعددة الإدارات لكن هذا يتطلب جهدا وإمكانيات جبارة وإعادة تعريف لبعض النطاقات الأساسية في أبجديات الانترنت.

أما بالنسبة لقوانين الانترنت فسوف نأتي فقط بمقدمة عما قد تتناوله تلك القوانين آملين أن تتاح لنا الفرصة للكتابة عن باقي تلك القوانين و حيثياتها والمواضيع المتعلقة بها مثل حوكمة الانترنت والعقود الالكترونية والجدل حول أسماء النطاقات و غيرها.

الجدير بالذكر أنه لا توجد معايير موحدة لقوانين الانترنت وإنما هي تخضع بشكل أو بآخر لما تسنه القوانين المحلية لذلك الإشكالية هنا عندما تكون المسألة القضائية "عابرة للدول" أي متعلقة بشخص أو شركة أو مقدم خدمة من دول مختلفة.

لهذا قد تتعرض قوانين الانترنت لثلاثة عناصر قضائية أو ثلاثة عوامل ألا وهي: أولا القوانين المحلية للمستخدم نفسه أو العميل، ثانيا القوانين المحلية لمكان وجود السيرفر أو مقدم الخدمة، ثالثا قوانين صاحب العمل ومقدم السلعة. وهنا نجد هذه العوامل تمضي بنا إلى مبدأ رئيسي من مبادئ القانون الدولي ألا و هو "استقلالية و سيادة الدول".

أما فيما يتعلق بالقضايا التي قد تعالج في قوانين الانترنت وهي على سبيل الذكر لا الحصر:

- الأمن والدفاع الإلكتروني.
- أسماء النطاقات التجارية.
- الجرائم الإلكترونية سواء عبر الإنترنت أو في الإنترنت.
- حقوق الملكية.
- قوانين الخصوصية الشخصية.
- حرية التعبير.

وفي المملكة تشرف هيئة الاتصالات وتقنية المعلومات على تنظيم الإنترنت وما يتعلق بقوانينه وحسب نظام مكافحة جرائم المعلوماتية الصادر عام 1428[8] والذي يؤكد على الأهداف التالية:

- المساعدة على تحقيق الأمن المعلوماتي.
- حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية.
- حماية المصلحة العامة والأخلاق والآداب العامة.
- حماية الاقتصاد الوطني.

ومع انتشار الجرائم المعلوماتية مؤخراً توجد الحاجة إلى التوعية بهذه القوانين وكذلك خلق ثقافة الاستخدام السليم للإنترنت والاستفادة من تلك الأداة بشكل أكبر و فاعلية أكثر.

المطلب الأول: المؤسسات الدولية والإقليمية والمحلية المسؤولة عن قطاع الاتصالات والانترنت

إن الجهة المؤسساتية التي تشرف على قطاع الاتصالات والإنترنيت هي مجلس الوزراء العرب للاتصالات والمعلومات والذي ينشأ في نطاق جامعة الدول العربية ويتألف من المسئولين عن قطاع الاتصالات وتقنية المعلومات في الدول العربية.

وذلك المجلس هو الجهة المخولة بتنظيم الإنترنت في العالم العربي وسيكون على عاتقها الأخذ بكل مزايا وتطوير هذه الخطوة الجبارة بإدخال الأسماء والحروف العربية في أسماء الحقول، وبعد ذلك ربما سيرى النور قانون عربي موحد بشأن قوانين الإنترنت والملكية الفكرية على الانترنت وكذلك التجارة الإلكترونية مما ستساعد على تخطي أي حاجز جغرافي.

ونطرح تساؤلا هنا حول كيفية تشجيع الجهات المعنية داخلياً لهذه المبادرة لتطوير المحتوى العربي للانترنت من جهة أو كذلك دعم التجارة الالكترونية وتحفيزها حيث إن التجارة الالكترونية بدأت بتبوء مكانة كبيرة على ساحة شبكة الانترنت.

وذلك الانفتاح المعلوماتي سيكون له نتائج ايجابية كثيرة و قد يكون أيضا له نتائج سلبية فالتحدي هنا ليس بفرض العقوبات أو حصار المستخدمين أو الحجب – لا شك أنه يجب

فرض نوع من الرقابة والقوانين الرادعة لكن الأهم من ذلك هو خلق ثقافة الاستخدام السليم من قبل المستخدم نفسه، إذ من الضروري البدء من الآن في العمل على تثقيف وتوعية المجتمع بالطرق السليمة لاستخدام الانترنت ليكون هناك ثقافة واعية ومسئولة عن استخدام الانترنت بما يعود لفائدة ومصلحة المستخدم والبلاد.

يعيش العالم اليوم متغيرات لا حصر لها و تطورا تقنياً فائقاً في مجال الانترنت والعالم الرقمي، حيث يوظف الانترنت اليوم، في غالب شؤون الحياة والتعاملات المالية والإدارية والمعلوماتية، وما يترتب عليه من تعليق للديناميكية الالكترونية التي أصبحت يعتمد عليها أكثر من أي وقت مضى، مما جعل تلك البيئة الافتراضية مسرحا للهجمات التي تتعرض لها دول العالم أجمع.

ولا شك أن الهجوم مؤخرا على وزارة الداخلية حين صرح مصدر مسؤول بالمركز الوطني للأمن الإلكتروني بوزارة الداخلية بأن العديد من المواقع الحكومية الإلكترونية في المملكة ومن بينها موقع بوابة وزارة الداخلية الإلكترونية تعرضت خلال الأيام الماضية لهجمات إلكترونية منسقه ومتزامنة.

ولا شك أن تلك الهجمات لم تكن الأولى، كما سبقها قبل ذلك عدد من الأمثلة على رأسها الهجوم على حواسيب شركة أرامكو.

ولعلنا نطرح سؤالاً بداية: إلى أي مدى لدينا الجاهزية لمثل تلك الهجمات التي حصلت مؤخرا والتي قد لا تكون الأخيرة؟ وهل يوجد استراتيجية وطنية تشرك أصحاب المصلحة لاسيما هيئة الاتصالات والمعلومات ووزارة الداخلية ووزارة الدفاع فيما يتعلق بأمن الانترنت أو الأمن المعلوماتي أو الأمن الإلكتروني، على اختلاف المسميات والدلالات وتداخلهم في وصف الظواهر التي قد يكون مسرح عملياتها حاسوبي بحت أو قد تنتقل إلى التحكم بآليات عسكرية أو مدنية لشن هجوم إرهابي،أو التحكم في عمليات حاسوبية و شبكات لتكبيد خسائر اقتصادية.

وقد عرّف كل من "ريتشارك كلارك" و"روبرتكناكي" الحرب الإلكترونية على أنها "أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها".

يرى المنظر العسكري كارل كلاوزفيتز أن "الحرب هي استخدام القوة لإجبار العدو على فعل ما نريد، ويضيف أن الحرب "إجراء سياسي.. استمرار للسياسة بوسائل أخرى" وتشكل النظرية الواقعية للعلاقات الدولية مجالا لتبرير الحرب إذا ما كانت في صالح تعظيم المصلحة،أو القضاء على تهديد.

وعلى الرغم من أن حرب الانترنت هو وصف لصراع غير عنيف بشكل مباشر، إلا أن

الكلفة الاقتصادية لعواقب تلك الحرب قد تكون كبيرة جدا، حيث ألحق الهجوم على أرامكو السعودية الضرر بحوالي 30 ألف جهاز كمبيوتر، وفي مثل ذلك الهجوم لا تحسب التكلفة المباشرة لمثل تلك الهجمات بل كذلك تحسب التكلفة من الوقت الذي أخر أو أوقف عمليات تلك الأجهزة وتبعات ذلك.

وكما يشير القاموس الدولي حول حرب الانترنت "هي حرب يتم شنها من خلال أجهزة الحاسوب وشبكة الانترنت، وهي تشمل – على حد سواء- إجراءات هجومية لإلحاق الضرر بنظم المعلومات عند الخصوم، وأخرى دفاعية لحماية النظم الخاصة بالمهاجمين،حماية لنظمهم من أن تهاجم. وما يسبب الإرباك استخدام المصطلح لوصف عمليات عسكرية تستخدم تقنيات تعتمد على المعلومات، وهذا جمع بينه و بين مصطلحي حرب المعلومات والحرب القائمة على الشبكات. فالدول الحديثة و قواتها المسلحة تعتمد بشكل متزايد على أجهزة الحاسوب وقد تسبب الهجمات على هذه الأجهزة ضررا مساويا لما يسببه هجوم عسكري تقليدي".

إن التكلفة الرخيصة نسبيا للأجهزة الإلكترونية والحاسوبية لشن هجوم إلكتروني يظهر أن مستوى الاستراتيجية في الحروب قد تغير وان صرف الأموال فقط على شراء المعدات العسكرية التقليدية قد لا يصبح هو فقط المطلوب بل إن التدريب الالكتروني قد يصبح ذو أولوية في تجهيز ما نسميه "الأمن الالكتروني" لواء الحرب الإلكتروني".

ولحرب الإنترنت كما يشير القاموس عدد من الأهداف منها التجسس والخداع والتعطيل، والتدمير وإغراق البريد الالكتروني بالرسائل. وكذلك واختراق الأجهزة من اجل انتزاع المعلومات منها، ومنها عمليات مهاجمة البرامج مثل الفيروسات، والديدان الالكترونية، والقنابل المنطقية، والهجمات المادية على الحاسوب أو معظم الاتصالات التي تربطها.

الجدير بالذكر أن تلك الحرب يمكن أن تشن من قبل فرد أو أفراد أو مجموعة تابعة لدول. ومن أشهر الدول التي صدر منها هجمات الكترونية روسيا والصين والتي حاولت الأخيرة اختراق موقع البنتاجون عام 2007.

ولعل الحاجة إلى حماية من هجوم كهذا يجعل أمن المعلومات أولوية حيوية للدول المعاصرة جمعاء وللمملكة خصوصا لاسيما بعد الهجوم على المواقع الإلكترونية الحكومية وموقع وزارة الداخلية خصوصا، في تحديث نظام مكافحة الجرائم المعلوماتية من جهة،ومن جهة أخرى اعتماد استراتيجية وطنية للدفاع الالكتروني.

عادة ما تشكل الجيوش الحربية الحديثة من ثلاثة أذرع عسكرية وهي القوة الجوية والقوة البرية والقوة البحرية تستخدمها للهجوم على أعدائها والدفاع عن أرضها. ولكن في عصر

الإنترنت والاتصالات بدأنا نسمع عن معارك يدور رحاها في الفضاء الإلكتروني وبين خصوم معظمهم مجهولي الهوية يهاجمون البنية التحتية الرقمية للدول التي يضعونها في خانة العدو حيث تهدف الهجمات الرقمية إلى الحصول على معلومات مخابراتية حساسة أو تدمير بنية الاقتصاد الذي بدأ يعتمد على المعلومات بشكل كبير أو لمجرد إشعار العدو أنهم موجودون على الجبهة الرقمية وبإمكانهم إزعاجه.[9]

إن استعمال الفضاء الإلكتروني في القتال وعمليات التطوير والاستعدادات التي قامت بها دول عديدة، يؤكد أن سباق التسلح في مجال الفضاء الإلكتروني قد بدأ. ويشار إلى أن العديد من الدول أقامت في السنوات الأخيرة مؤسسات وهيئات مختلفة ومختصة باستعمال الفضاء الإلكتروني كمجال قتال، وطورت استراتيجيات أمنية في الفضاء الإلكتروني.[10]

المطلب الثاني: تطور الحرب الالكترونية

تطورت الحرب الإلكترونية والتي أصبحت، في بعض السياقات يطلق عليها، الحرب القائمة على الشبكات، أو العلميات المفعلة بالشبكة، وهي عنصر مهم من عناصر الثورة في الشؤون العسكرية والتحول الدفاعي. وهي تعتمد بشدة على استخدم تقنيات المعلومات وأنظمة الاتصالات الحديثة. ويتمثل هدف الحرب القائمة على الشبكات في تمكين القوات المسلحة من العمل بمزيد من السرعة والكفاءة، ومن خلال الربط والتشبيك لجميع أنظمة القيادة و السيطرة والمعلومات بالأسلحة وصناعة القرار، ومن هنا تشكل هذه المنظومة جزءا حيويا جدا ومهما للدولة والتي يتوجب عليها حمايته والدفاع عنه وتأمينه.

ينبغي على الذين يتولون قيادة الأسلحة أن تتوافر لهم إمكانية الوصول الفوري من خلال شبكة الحاسوب الآلي لجميع المعلومات، و السماح لهم بضرب الأهداف بسرعة ودقة. وهكذا فإن الحرب القائمة على الشبكات تعزز القوة القتالية و تزود القوات المسلحة بتفوق حاسم في المعلومات على من لا يملكها. كذلك في علاقة الحرب القائمة على الشكبات، والثورة في الشؤون العسكرية.[11]

المبحث الثاني: الدفاع الشرعي ضد الهجمات السيبرانية

ليس من المتوقع أن لا يكون للدولة التي تمت مهاجمتها إلكترونيا أي رد أو دفاع، وكأحد الحقوق الطبيعية للدول و المنصوص عليها في ميثاق الأمم المتحدة، فقد أجازت المادة 51 من الميثاق للدول الدفاع عن أي اعتداء عليها وعلى إقليمها أو سيادتها أو أمنها، وليس في هذا الميثاق ما يضعف أو ينتقص الحق الطبيعي للدول، فرادى أو جماعات في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء "الأمم المتحدة"[12].

ولتتمكن من وضع إطار للدفاع الشرعي من الهجمات الإلكترونية فلابد من النظر بداية في

الشروط و الضوابط اللازمة لثبوت الحق لأي دولة في الدفاع عن نفسها، والتي تكونت من العرف الدولي وأثبتها الميثاق، أولا يجب أن يكون الهجوم مسلحا وثانيا أن يكون الهجوم واقعا وليس احتمالي الوقوع وثالثا أن يكون هذا الهجوم غير مشروع أي لا يكون دفاعا شرعيا أو تنفيذا لأحد قرارات الأمم المتحدة. أما ضوابط ممارسة هذا الحق وهي، تناسب رد الفعل مع الاعتداء، تقدير الضرورة وثبوت نسبة الاعتداء للدولة المتهمة بالهجوم[13] وأخيرا إبلاغ مجلس الأمن فوراً بالاعتداء ليتمكن من اتخاذ التدابير المناسبة للمحافظة على الأمن والسلم الدوليين.[14]

وبتطبيق هذه الشروط و الضوابط على الدفاع في حالة الهجوم الإلكتروني يجب تقدير كون الهجوم السيبراني يصنف اعتداءً مسلحا أم لا؟ بالرجوع إلى قرار الجمعية العامة الخاص بتعريف العدوان فقد نصت على أنه: "اعتماد القوة المسلحة من قبل دولة ما ضد سيادة دولة أخرى أو سلامتها الإقليمية أو استقلالها السياسي، أو بأية صورة أخرى تتناف مع ميثاق الأمم المتحدة..."[15]، فقد ذكر هذا التعريف أن العدوان يعني استخدام القوة المسلحة، فهل الهجوم الإلكتروني ينطوي على استخدام قوة مسلحة؟ يوجد ثلاث تحليلات كل منها سلك مذهبا مختلفا.

المطلب الأول: الاستنباط القانوني للدفاع الإلكتروني بحسب الأداة والأثر والمسؤولية

فالمذهب الأول، (بالنظر للأداة)، يقضي بأنه يجب تحديد ما إذا كان الهدف الموجه إليه الهجوم السيبراني كان قبل الاعتماد على الإلكترونيات لا يمكن الهجوم أو الاعتداء عليه إلا عن طريق القوة الحركية، فلنفترض أن هجوما إلكترونيا على مولدات الطاقة لدولة ما أدى إلى تدميرها، فبحسب هذا المذهب يتم النظر إلى مدى إمكانية تدمير هذه المولدات في السباق عن طريق أسلحة يدوية كتفجيرها مثلا.[16]

المذهب الثاني (بالنظر للأثر)، يتم تصنيف الهجوم كمسلح عن طريق قياس الأثر المترتب من جراء الهجوم السيبراني، أي النظر إذا ما كانت الآثار المترتبة على هذا الهجوم كان لا يمكن ترتيبها إلا عن طريق استخدام القوة المادية (الحركية)، كالتلاعب بالأنظمة المالية والبنكية لدولة ما.[17]

المذهب الثالث (المسئولية المطلقة)، من خلال هذا المذهب يجعل أي هجوم على البنية التحتية لدولة ما (المرتبطة بالصحة العامة أو الأمن مثلا) من قبيل الهجوم المسلح.[18]

بالرغم من اختلاف معايير قياس الهجوم السيبراني إلا أن كل المذاهب الثلاثة متفقة أن بإمكان الهجوم السيبراني أن يشكل هجوما مسلحاً، كما يرى الكاتب أن المذهب الثالث هو الأكثر منطقية والأسهل في القياس لوضوحه، كما أن استهداف البنية التحتية من أكثر المخاطر التي تهدد أمن أي دولة واستقرارها وتعد انتهاكا صريح لسيادتها مما يجعل انطباق الحق في

الدفاع واجباً.

ومن وجهة نظر أخرى، يمكننا القياس على الأجهزة النووية والمفاعلات النووية، حيث أنها تعتبر من قبيل الأسلحة بالرغم من أنها ليست مدافع ولا جنودا، ولهذا يمكن اعتبار الفيروسات التي تقوم بالاختراق و الهجوم سلاحا يستخدم لتنفيذ ذلك الهجوم السيبراني.

أما الشرط الثاني لمشروعية الدفاع وهو أن يكون الهجوم واقعا فعلا وليس احتمالي الوقوع فلا يكفي التهديد باستخدامه ولا يكفي أن تكون إحدى الدول المعادية تمتلك ذلك النوع من الفيروسات، وإنما يشترط أن يكون ذلك الهجوم قد تم بالفعل، وقد يضاف إلى ذلك الخطر الوشيك الوقوع لكن هذه الزاوية سنتناولها بالتفصيل عند الحديث عن الدفاع الوقائي والتوقعي[19].

وكما أنه لابد أن يكون هذا الهجوم غير مشروع، أي لا يكون هذا الهجوم السيبراني نتيجة لتنفيذ أحد قرارات الأمم المتحدة أو يكون دفاعا شرعيا بسبب هجوم من تلك الدولة بداية، وهذا الشرط من السهل التحقق منه و إثبات انطباقه.

ومن أهم الضوابط، أولا، التناسب بين عملية الدفاع الشرعي والهجوم، على سبيل المثال لا يجوز لدولة الدفاع القيام بعملية غزو لإقليم الدولة المتهمة كرد دفاعي لهجمة إلكترونية، ولكن هذا يشكل صعوبة في الفضاء السيبراني، حيث من الممكن أن يتعدى فعل الدفاع تلك الدولة ويضر بكيانات أخرى، وهذا ما حدث فعلاً في الهجوم بفعل فيروس ستكسنت (Stuxnet) والذي استهدف الأجهزة الإلكترونية الإيرانية، فقد تم رصد ما يزيد عن 40 ٪ من أجهزة الكمبيوتر تضررت خارج الحدود الإيرانية [20]. فلابد من التأكد والتثبت من أن عملية الدفاع ستنحصر في هدف معين ولا تنال دول أخرى ليس لا علاقة بالهجوم.

الإلزام الآخر وهو تقدير الضرورة [21]، أي استنفاذ أو استحالة أي إجراء سلمي آخر، و هذا ما تؤكده الأمم المتحدة كأحد مبادئها، وهو وجوب حل المنازعات الدولية بالطرق السلمية[22]، أي عن تعرض أي دولة لهجمات إلكترونية فيفترض قبل اللجوء لأي استخدام للقوة أن يكون هناك محاولات لحل هذا النزاع بأحد الطرق السلمية المقترحة من قبل القانون الدولي والاتفاقيات الدولية [23]، كالقيام بالمفاوضات أو التحكيم.

وفي هذا السياق يمكننا الحديث عن مدى مشروعية التدخل العسكري كرد دفاع على الهجوم الإلكتروني، فبتطبيق مبدأ التناسب، سيكون من الصعب اللجوء للقوة العسكرية وتحريك جيوش الدولة بسبب الهجوم الإلكتروني، ولكن يثار هنا التساؤل لو كان هذا الهجوم السيبراني قد مس المنشآت العسكرية والتحكم بالأسلحة الحربية هل من الممكن أن يباح في هذه الحالة حق اللجوء للدفاع العسكري ؟

ومن بين أهم الضوابط وهو ثبوت نسبة الاعتداء للدولة المتهمة بالهجوم، حيث إنه من الصعب تقديم دليل مقنع يحدد لي مصدر الهجمة الإلكترونية فالمستخدمين المجهولين الهوية والمتخفين وراء الشاشات والأجهزة هو ما يجعل إثبات مطلق الهجمات صعباً، وفي حالة المقدرة على ذلك فهذا الأمر يستغرق وقتا طويلا وقد يقود لمصدر خاطئ، فمثلاً من الممكن أن يقوم المهاجم باختراق جهاز شخص بريء وجعل تلك الهجمات تظهر وكأنها صدرت من ذلك الشخص[24]. فلابد من التحقق وإسناد قاطع لجهة معينة مرتكبة للهجوم.ويمكنني القول، إذا كان العالم الواقعي أغلقت فيه قضايا ضد مجهول فما الحل بالعالم الافتراضي؟

في هذا الصدد يجب تناول افتراضين: الأول، أن يكون مطلق الهجمات السيبرانية داخل إقليم الدولة والافتراض الثاني أن يكون موجهها خارج إقليم الدولة أي من دولة أخرى.[25]

المطلب الثاني: مصدر الهجمات السيبرانية من داخل إقليم الدولة

في الافتراض الأول، إما ستخضع الجهة المتهمة للقانون الوطني إذا كان مطلقي تلك الهجمات هم أفراد أو جماعات إرهابية غير تابعة لأي دولة، ولكن في حالة أن مصدر تلك الهجمات هو جهة رسمية تابعة لدولة أخرى وتقع في نفس إقليم تلك الدولة، مثل السفارات والقنصليات، فيأخذ حكم أن مصدر الهجوم هو إقليم تلك الدولة لأن كما هو مثبت في القانون الدولي السفارات والبعثات الدبلوماسية تتمتع بحصانات خاصة وتعامل كما لو كانت على إقليم دولتها المبعوثة منها.

المبحث الثالث: مصدر الهجمات السيبرانية من خارج إقليم الدولة

إذا تم تحديد أن الهجوم السيبراني انطلق من جهة رسمية لدولة معينة أو من أشخاص يمثلون الدولة بصفة رسمية أو يعملون لصالحها، أو أي جماعات قامت بهذا الهجوم اتباعا لتوجيهات من حكومة الدولة، فطبقا لمبادئ المسؤولية الدولية، تكون الدولة مسؤولة عن تلك الأفعال ويمكن استخدام الدفاع الشرعي ضده[26]. أما في حالة كان مطلقو الهجمات عبارة عن أفراد وجماعات إرهابية بدون أي أوامر من الدولة، فطبقاً لمبدأ احترام سيادة الدول وواجب عدم التدخل، لا يمكن للدولة المستهدفة القيام بأي عمليات ضد هؤلاء الجماعات ولكن هذا لا يمنع تنبيه الجهات الرسمية لتلك الدولة بضرورة اتخاذ الإجراءات اللازمة والعقوبات المفترضة ضد هذه الجماعات أو الأفراد، وهذا ما أقره ميثاق الأمم المتحدة في مادته (7/2) وأوجبت عدم التدخل[27].

ولكن هذا الأمر ليس مطلقاً، ابتداء من قضية كارولين 1837[28]، وقضية الكونغو[29]، والتي كان الحكم فيها يجيز للدولة الضحية اتخاذ عمليات دفاعية ضد هجمات من أشخاص أو جماعات غير تابعة أو مدعومة من الدولة بشرط أن تكون تلك الدولة عاجزة عن إيقاف تلك الجماعات واتخاذ

التدابير اللازمة ضدهم[30]، وفيما يخص الهجمات السيبرانية فقد أيد الخبراء المشاركون في إعداد دليل تالين في الحرب الالكترونية، أنه يجوز استخدام الدفاع الشرعي ضد هجمات قادمة من خارج إقليم الدولة إذا كانت تلك الدولة غير قادرة على قمع مطلقي ومنشئي تلك الهجمات، و معيار عدم القدرة على القمع يشمل عدم توفر الخبراء أو التكنولوجيا اللازمة لدى تلك الدولة أو تجاهلها لهذه الأفعال وعدم اتخاذ أي تدابير ضدها. بالرغم من ذلك يوجد قلة من خبراء دليل تالين، ضد استعمال حق الدفاع لقمع جهات على إقليم دولة أخرى إلا بموافقة تلك الدولة أو إذن من مجلس الأمن، وقد قيدت هذه القلة استعمال ذلك الحق بوجود ضرورة مبيحة (تطبيق مبدأ الضرورة) [31]. ومن الممكن أن يكون الأساس للدفاع الشرعي هو انتهاك الدولة المهاجمة لواجب عدم التدخل و الذي تقره الأمم المتحدة، و ذلك في المادة (4/2) من الميثاق: "يمتنع أعضاء الهيئة جميعا 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"[32].

المطلب الأول: الدفاع الاستباقي مابين الحروب التقليدية والسايبرية

الدفاع الاستباقي يمكن تعريف الدفاع الاستباقي بأنه الحق في اتخاذ كافة التدابير الفعالة ضد أي عمليات أولية أو تطويرية لم يتم اكتمالها بعد ولا تشكل خطراً في وضعها الحالي، ولكنها ستشكل خطرا وتهديدا إذا تم الانتهاء منها وتجهيزها [33].

بالنسبة لمدى مشروعية هذا النوع من الدفاع، فبعد أحداث 11 سبتمبر، تبنت الولايات المتحدة هذا المبدأ و أجازت القيام بأعمال دفاعية استباقية ضد أي خطر يهدد أمنها حتى لو لم يتم تفعيله بعد.[34] كما قامت إيران و كوريا الشمالية أيضا بالاعتراف بهذا النوع من الدفاعات.

ولكن على الصعيد الدولي فقد امتنعت محكمة العدل الدولية عن إبداء أي رأي في هذا النوع من الدفاع، بالرغم من أنها في قضائها سابقا كانت تجعل تحقق الهجوم ووقوعه شرطا أساسيا لثبات الحق في الدفاع[35].

بتطبيق ذلك على الدفاع الاستباقي ضد الهجمات السيبرانية، فلا يوجد سند قانوني دولي يسمح بالهجمات الدفاعية ضد أي أعمال بدائية لم تكتمل بعد.

المطلب الثاني: الدفاع التوقعي كوسيلة احترازية

الحق في اتخاذ كافة التدابير الفعالة ضد أي تهديد أو خطر لم يقع بعد، ولكن يشترط أن يكون هذا الخطر وشيك الوقوع، وقد أقر ذلك تقرير الأمم المتحدة عام 2004[36]، وجعل للدول الحق في الدفاع الشرعي ضد أي خطر يهددها مادام وشيكاً، وأيضا أكد الخبراء المشاركين في إعداد دليل "تالين" للقانون الدولي في الحرب الإلكترونية على أن إذا كانت الهجمات السيبرانية وشيكة فيحق للدولة الدفاع التوقعي[37]. وكما قال فرانسو دي فيتوريا "لا يمكنك معاقبة أحد بتهمة لم يتركبها

حتى الآن "، ولكن مايكل ويزلر من جهة أخرى يرى بأن أفضل وسيلة للدفاع هي الهجوم [38].

المطلب الثالث: مدى انطباق القانون الدولي الإنساني في حالة الحرب السيبرانية

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

لقد نصت المادة 36 من البروتوكول الإضافي الأول لاتفاقيات جنيف[39] بأنه "يلتزم أي طرف سام متعاقد، عند دراسة أو تطوير أو اقتناء سلاح جديد أو أداة للحرب أو اتباع أسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظوراً في جميع الأحوال أو في بعضها بمقتضى هذا الملحق "البروتوكول" أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد". فبهذا يجب على الدول عند تطوير التكنولوجيات الجديدة والتي قد تستخدم لشن هجمات على دولة أخرى أن تراعي قواعد القانون الدولي الإنساني بما فيها المبادئ الرئيسية والمتمثلة في (الإنسانية، الضرورة، التناسب، التمييز).

إذا كان استخدام هذه التكنولجيا الحديثة في سياق نزاع مسلح (حركي) قائم، فمن المؤكد ستنطبق قواعد القانون الدولي الإنساني مع استثناء الأجهزة و البنية التحتية التي تشكل أهدافا عسكرية حيث إن القانون الدولي الإنساني لا يضفي الحماية على الأهداف العسكرية أثناء الحروب ولكنه يضع قواعد وحدودا لاستهدافها حتى لا يتم الضرر بالمدنيين أو أعيان مدنية أخرى، أما إذا كان لا يوجد نزاع قائم ولكن تلك الهجمات السيبرانية ترقى لتكون نزاعا مسلحا فينظر إلى أثر تلك الهجمات على حياة المدنيين (كقطع إمدادات الطاقة و المياه) أو إصابة النظام المصرفي بخلل، أو أي تلاعب بالبنية التحتية للدولة [40].

ولا يمكن التنصل من أحكام القانون الدولي الإنساني بحجة أن ميدان الحرب هو الفضاء السيبراني، فحيث إن الحروب البرية و البحرية و الجوية ميادينها تكونت طبيعيا، إلا أن الحرب السيبرانية ميدانها من صنع الإنسان، ولكن هذا الاختلاف لا يخرج الحرب السيبرانية من إطار القانون الإنساني، وهذا ما أكدته محكمة العدل الدولية بقولها: إنّ مبادئ وقواعد القانون الإنساني المنطبق في النزاع المسلح المستقرة تنطبق على جميع أشكال الحروب وعلى جميع أنواع الأسلحة"، بما في ذلك" تلك المستقبلية"[41].

وقد استثنت اللجنة الدولية للصليب الأحمر في تقريرها عام 2015 [42]، عمليات التجسس من انطباق القانون الدولي الإنساني عليها، ولكنها استدركت على هامش التقرير أنه من الممكن أن يشملها القانون الدولي الإنساني إذا أدت إلى اختراقات تقود لأضرار مادية كبيرة، حيث إن اغلب العمليات السيبرانية تتم في بدايتها عن طريق التجسس والحصول على الإذن بالدخول للبيانات

المستهدفة عن طريق اختراق ذلك الجهاز.أما الاستثناء الثاني فيتعلق بتشويش الاتصالات اللاسلكية والبث التلفزيوني، فلم يتم اعتباره من قبيل الهجوم الوارد في القانون الدولي الإنساني.

ومما يشكل صعوبة على الالتزام بتطبيق أحكام القانون الدولي الإنساني في الحرب السيبرانية، هو صعوبة التفرقة بين الأهداف المدنية والعسكرية لارتباطها ببعضها في الفضاء السيبراني، ففي العصر الحالي يتم استخدام أجهزة الإنترنت والاتصالات لتوصيل الإمدادات اللوجستية إلى المدنيين وفي نفس الوقت يستخدم العسكريين هذه الاتصالات، بالإضافة إلى استخدام نظام تحديد المواقع العالمي(GPS) والمرتبط بالأقمار الصناعية من قبل المدنيين والعسكريين، وفي هذا السياق يجب التنبه إلى الضرر العرضي الناتج من استهداف نقاط عسكرية والتي قد تؤدي بصورة غير مباشرة لأضرار مدنية [43].

ومن الممكن أيضا أن تصبح الأهداف المدنية في الفضاء السيبراني أهدافا عسكرية، و في هذه الحال يجب مراعاة قواعد القانون الدولي الإنساني فيما يتعلق بحظر الهجمات العشوائية وقواعد التناسب والاحتياطات أثناء الهجوم[44].

والخبراء العاملون على دليل تالين، قد أكدوا ضرورة تدخل القانون الدولي الإنساني في الحروب السيبرانية، وقد فرقوا بين الحروب الدولية وغير الدولية في الفضاء السيبراني، كما جعلوا معيار انطباق قواعد القانون الدولي الإنساني هو الضرر المترتب، إذا ما كان الضرر سيودي بحياة المدنيين و يؤثر عليهم تأثيرا كبيرا أم لا؟

بالرغم من أن القانون الدولي الإنساني ينطبق في حالة الحرب إلا أنه لم يغفل واجبا على عاتق الدول في زمن السلم، وهو وجوب اتخاذ كافة التدابير الوقائية اللازمة لحماية البنية التحتية الأساسية والمرتبطة بالأجهزة الحيوية للدولة وتطوير نظام الحماية السيبراني وجعله ذا جاهزية عالية لصد أي هجمات قد تخل بالنظام الإلكتروني لدولة ما، وقد أوصت اللجنة الدولية للهلال الأحمر والصليب الأحمر في تقريرها السالف الذكر، بالعديد من التدابير والتي من بينها، النسخ الاحتياطي للبيانات المهمة، استخدام تدابير للحماية من الفيروسات، فصل البنية التحتية والشبكات السيبرانية العسكرية عن المدنية[45].

وبالنظر للتطور المتسارع للمنظومات السيبرانية والأجهزة المصممة لتنفيذ الاختراقات والهجمات فلابد من أن يكون التطور القانوني في هذا المجال متزامنا مع هذه البرمجيات الحديثة.

الخاتمة

في موجة الاجتياح السيبراني لكل أجهزة الدولة، وفي ظل الخطر الذي يهدد المرافق العامة والبنية التحتية لأي دولة، نكون أمام التزامين اثنين وهما: تعزيز الدفاع، وتكتيك الهجوم؛ مما يتطلب اقتناء برامج والعمل بآليات لحماية أجهزة الدولة من الهجمات السيبرانية والاختراقات

وعمليات التجسس الالكتروني.

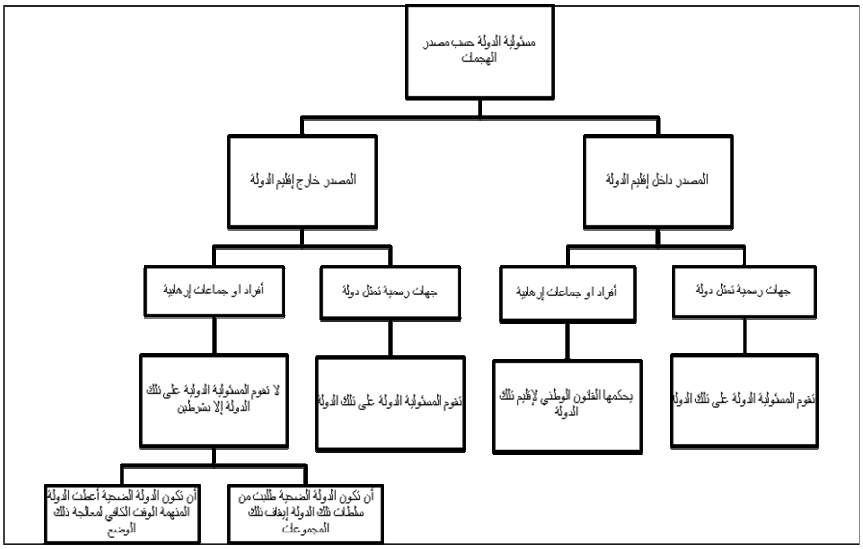
لقد عرضت هذه الدراسة، حق استخدام أي دولة الدفاع الشرعي ضد الهجمات السيبرانية، وهذا الحق تم إقراره في ميثاق الأمم المتحدة في مادته 51 حق الدول في الدفاع الشرعي عن إقليمها وسيادتها وأمنها في حالة وقوع أي هجمات عليها من دول أخرى، مع مراعاة شروط وضوابط ممارسة هذا الحق، ولو حاولنا تطبيق هذه الشروط على الدفاع في حالة الهجوم الإلكتروني يجب علينا في البداية تقدير كون الهجوم السيبراني يصنف هجوما مسلحا أم لا؟ ويمكننا القياس على الأجهزة النووية و المفاعلات النووية، حيث إنها تعتبر من قبيل الأسلحة بالرغم من أنها ليست مدافع ولا جنود، ولهذا يمكن اعتبار الفيروسات التي تقوم بالاختراق والهجوم سلاحا يستخدم لتنفيذ ذلك الهجوم السيبراني، و يشترط أيضا أن يكون الهجوم واقعا فعلا وليس احتمالي الوقوع فلا يكفي التهديد باستخدامه ولا يكفي أن تكون إحدى الدول المعادية تمتلك ذلك النوع من الفيروسات، وكما أنه لابد أن يكون هذا الهجوم غير مشروع أي لا يكون دفاعا شرعيا أو تنفيذا لأحد قرارات الأمم المتحدة، و من أهم الضوابط التناسب بين عملية الدفاع الشرعي والهجوم، و هذا ما يشكل صعوبة في الفضاء السيبراني، حيث من الممكن أن يتعدى فعل الدفاع تلك الدولة و يضر بكيانات أخرى.

أما اشتراط نسبة الفعل لجهة معينة، فهو مازال معضلة بالنسبة للدول، فمن الصعب اكتشاف من قام بتلك الهجمات، وهذا الأمر من شأنه تهديد الثقة والعلاقات بين الدول، ومن الممكن في حالة التشكك من الجهة مطلقة الهجمات وإصدار اتهامات علنية لها في وسائل الإعلام قد يثير لغطاً في الوسط الدولي ويؤثر على علاقات الدولتين الدبلوماسية، وقد يزداد الأمر سوءاً إذا كان بين الدولتين ماض مشحون بالأزمات والمناوشات والصراعات.

ومن المستقر عليه في القانون الدولّي أحكامه تختلف في حالة إطلاق الهجمات من عناصر إرهابية غير تابعة لأي دولة أو من عناصر تعمل لمصلحة تلك الدولة وبأمرها، وهذا ما وضحته هذه الدراسة، فبناء على المسؤولية غير المباشرة والتي توجب المسئولية الدولية على أفعال رعايا دولية ما، فإن الاعتداءات حتى لو لم تصدر من جهة رسمية في الدولة قد تعد الدولة مسئولة دوليا عندها، ولكن يشترط لذلك أحد الأمرين إما أن يكون هؤلاء العناصر عملوا بأمر من الدولة أو بعلم من الدولة ولكن الدولة لم تتخذ أي إجراء ضدهم لإيقافهم، أو أن هذه العناصر أو الأشخاص أو المجموعات مطلقة الهجمات السيبرانية قد كانت لها سوابق في هذا المجال وهذه الاعتداءات ولكن الدولة لم تصدر أي عقوبات بحقهم، الشرط الآخر أن تكون الدولة مقصرة في مراقبة فضائها السيبراني ولم تضع الإجراءات اللازمة لردع هذه المجموعات وقمعها منذ البداية، وما زل هناك جدل حول تحديد معيار "العناية" الواجبة على الدولة حتى تتحلل من مسؤوليتها

الدولية في مواجهة الدول الأخرى المعتدى عليها.

وقد طرحت هذه الدراسة موضوع مدى انطباق القانون الدولي الإنساني على الحرب السيبرانية، وتم الاستناد بشكل كبير على تقارير اللجنة الدولية للهلال الأحمر والصليب الأحمر، دليل تالين للقانون الدولي في الحرب الإلكترونية والصادر عن حلف شمال الأطلسي لعام 2013م، وقد كان هناك بعض الآراء المختلفة بهذا الخصوص والكثير من الجدل حوله، حيث إنه يستوجب في بداية الأمر وضع تكييف للحرب السيبرانية ومعرفة مدى انطباق مصطلح النزاع المسلح عليها، ومن ثم يأتي دور تطبيق المبادئ الخاصة بتنظيم استخدام الأسلحة والمحظور والمسموح منها وحدود استخدامها، ومحاولة حصر أمثلة على الأسلحة المستخدمة في الحرب السيبرانية وتحديد مدى إمكانية انطباق أحكام القانون الدولي الإنساني عليها، وأيضا تحديد الأهداف المدنية والعسكرية منها وهذا مما يصعب حسمه، وفي ذلك ذكرت اللجنة الدولية للصليب الأحمر في تقريرها عام 2015:"من أجل حماية البنية التحتية المدنية الأساسية التي تعتمد على الفضاء الإلكتروني، من الأهمية بمكان أيضا حماية البنية الأساسية للفضاء الإلكتروني بحد ذاته. بيد أنّ التحديات تقع في الترابط بين الشبكات المدنية والعسكرية. ومعظم الشبكات العسكرية تعتمد على البنية الأساسية السيبرانية المدنية، مثل كابلات الألياف البصرية البحرية أو الأقمار الاصطناعية أو أجهزة التوجيه أو العقد".



الشكل (1) من إعداد الباحث

ـ الإحالات:

[1] **بول روبنسون، قاموس الأمن الدولي(أبو ظبي: مركز الإمارات للدراسات والبحوث الاستراتيجية،2009)، 85**

[2] **عانت المملكة العربية السعودية بعدد من الاختراقات الإلكترونية الأمنية مثل الاختراق لشبكة المعلومات لشركة أرامكو، وكذلك الاختراقات لكثير من الوزارات والمواقع الشخصية، وهنا تدخل حرب الإنترنت في اتجاهين، الاتجاه الأول هو الدفاع الالكتروني والاتجاه الثاني هو الأمن الالكتروني.**

[3] International code of conduct for information security, "diplomacy online" ,*Embassy of Russian federation in UK*, 2016, http://www.rusemb.org.uk/policycontact/49.

[4] Tom Gjelten "*Seeing The Internet As An 'Information Weapon*, (23 September 2010), http://www.npr.org/templates/story/story.php?storyId=130052701.

[5] Alexander Mersihnko,"*International agreement on cyber war*" 2016, http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57

[6] Cyberspace*: The physical and non-physical terrain created by and/or composed of some or all of the following: computers, computer systems, networks and their computer programs, computer data, content data, traffic data, and users*, 2016, http://www.itu.int/ITU-D.

[7] **شموئيل إيفن ودافيد بن سيمان، حرب الفضاء الإلكتروني – تحديات على الصعيد العالمي والسياسي والتكنولوجي، (تل أبيب: معهد دراسات الأمن القومي 2011)**

http://www.dohainstitute.org/release/14e23aac-b76f-48f8-ba00-c94efe48fa36#1

[8] **هيئة الاتصالات وتقنية المعلومات، نظام مكافحة الجرام المعلوماتية، (المملكة العربية السعودية: هيئة الاتصالات،1428).**

[9] **عباس بدران، كتاب الحرب الالكترونية الاشتباكات في علم المعلومات (بيروت: مركز دراسات الحكومة الالكترونية، 2010).**

[10] **محمد محارب، حرب في الفضاء الإلكتروني اتجاهات وتأثيرات على إسرائيل (نابلس: كلية النجاح،2013)77–80.**

[11] **بول روبنسون، قاموس الأمن الدولي،(أبو ظبي: مركز الإمارات للدراسات والبحوث الاستراتيجية، 2009) 199**

[12] United Nations, *Charter of the United Nations*, 24 October 1945, 1 UNTS XVI, available at: http://www.refworld.org/docid/3ae6b3930.html [accessed 15 April 2016]

[13] **د.الدين جيلاني أبو زيد، د. ماجد الحموي، الوسيط في القانون الدولي العام،(الرياض: دار الشواف، 2003)144–148**

[14] **بالاستناد أيضا إلى حكم محكمة العدل الدولية عام 2005 في القضية بين الكونغو و أوغندا فقد قضت أن عدم إبلاغ أوغندا لمجلس الأمن بالهجمات وبعملية الدفاع التي قامت بها يعد دفاعا غير قانوني ويعد انتهاكا لمبدأ حظر استعمال القهوة.**

[15] **قرار من الجمعية العامة" تعريف العدوان"(رقم 3314 الصادر في 14 ديسمبر 1974).**

[16] Yoram Dinstein, *Computer Network Attacks and Self-Defense, in COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW* **(** Michael N. Schmitt & Brian T.O'Donnell eds., 2002**)** 99

[17] David E. Graham, **"**Cyber Threats and the Law of War", *JOURNAL OF NATIONAL SECURITY LAW & POLICY* ,Vol. 4:87, 13 Aug (2010**)**:91.

[18] **المرجع السابق.**

[19] نفس المرجع ص35

[20] Mary Ellen O'Connell, Louise Arimatsu, *Cyber Security and International Law, Meeting summary* ,(London: Chatham House,, 29 May 2012)7

[21] يمكن الاستشهاد على ذلك بفتوى محكمة العدل الدولية بشأن الآثار القانونية الناشئة عن تشييد جدار في الأرض الفلسطينية المحتلة A/ES-10/273، 2004، حيث قامت المحكمة بقياس مدى ضرورة بناء ذلك الجدار كأحد وسائل الدفاع من قبل إسرائيل وقد انتهت إلى أنه لا يوجد ضرورة محققة من تشييد الجدار لحماية أمن إسرائيل.

[22] United Nations, *the United Nations convention*, 1949, Article 2/3 available at: http://www.refworld.org/docid/3ae6b3930.html [accessed 15 April 2016]

[23] كاتفاقية لاهاي 1907م.

[24] المرجع السابق، David E. Graham، ص 92.

[25] انظر الشكل 1.

[26] المرجع السابق، SOPHIE CHARLOTTE PANK ، ص 39.

[27] المادة 2"7- ليس في هذا الميثاق ما يسوغ "للأمم المتحدة" أن تتدخل في الشؤون التي تكون من صميم السلطان الداخلي لدولة ما..."، ميثاق الأمم المتحدة، 1949 م.

[28] "قضية كارولين " *http://avalon.law.yale.edu/19th_century/br-1842d.asp*,1837 م

[29] حكم محكمة العدل الدولية في قضية الأنشطة المسلحة في أقليم الكونغو الديموقراطية، 19 ديسمبر 2005.

[30] المرجع السابق SOPHIE CHARLOTTE PANK ص 40.

[31] المرجع السابق.

[32] ميثاق الأمم المتحدة، 1949 م.

[33] Reisman, W. M. ,"The Past and Future of the Claim of Préemptive Self-défense". *THE AMERICAN JOURNAL OF INTERNATIONAL LAW*, Vol. 100:525 ,1. (Jan 2006).525..

[34] The Bush Doctrine Preemptive Strikes Against Threats To America's Security

[35] SOPHIE CHARLOTTE PANK ,"What is the scope of legal self□defense in International Law?", visited 2015, http://law.au.dk/fileadmin/Jura/dokumenter/forskning/rettid/Afh_2014/afh19-2014.pdf

[36] United Nations Secretary General, 2004, United Nations High□Level Panel on Threats, Challenges and Change

[37] حلف شمال الأطلسي، دليل تالين للقانون الدولي في الحرب الإلكترونية،(روما: الناتو 2013)

[38] المرجع السابق، SOPHIE CHARLOTTE PANK ، ص 33.

[39] "الملحق البروتوكول الأول الإضافي إلى اتفاقيات جنيف" المعقودة في(12 آب/أغسطس 1949) والمتعلق بحماية ضحايا المنازعات الدولية المسلحة.

[40] الصليب الأحمر، التقرير الرابع المعدّ من قبل اللجنة الدولية للصليب الأحمر اللجنة الدولية بشأن "القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة"، رقم 32IC/15/11، ديسمبر (2015)، ص54.

[41] محكمة العدل الدولية، مشروعية التهديد بالأسلحة النووية أو استخدامها، الرأي الاستشاري، 8 تموز/يوليو (1996)، تقارير محكمة العدل الدولية 226، 1996، الفقرة 86.

[42] الصليب الأحمر، التقرير الرابع المعدّ من قبل اللجنة الدولية للصليب الأحمر اللجنة الدولية بشأن "القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة"، رقم 32IC/15/11، ديسمبر (2015)، ص58.

[43] المرجع السباق، ص59.

[44] المرجع السابق.

[45] المرجع السابق، ص60.

Strategic and legal dimensions of cyber war

Dr. Yahia mefrah EL-ZAHRANI *

Abstract:

This researcher aims to focus on the concept of cyber war, distinction between the cyber war, and Cyber Security, as well as the evolution of this phenomenon in an attempt to reach the legal rules which may apply in different situation.

We tries to analyze the different legal and strategic aspect of cyber war under the International Law, its application with taking in consideration the different scenarios that may occur during cyber war.

This research also study the various threat source whether its external sources of threat, or internal, and thus raises the strategic and legal question, what is the role and responsibility of States in the international law in dealing with this phenomenon, and what are the strategies (proactive - defensive - precautionary) can be applied for protection from the dangers and electronic threats, with the variation that is forming between cyber war and conventional war.

Keywords: Law, politics, war, strategy, Cybernetics.

* The College of Strategic Sciences –Naïf Arab University for Security Sciences – Saudi Arabia.