مشروعية استخدام الهجمات السيبرانية في النزاعات الدولية والمسؤولية الدولية عنها

The legality of the use of cyber-attacks in international conflicts and international responsibility for them

طالب – ماجستير
محمد دهام مسعف
جامعة بغداد - كلية القانون
mohammed.mosaef1204a@colaw.uobaghdad.edu.iq

الأستاذ المساعد الدكتور
محمود خليل جعفر
جامعة بغداد - كلية القانون
khlil_mahmoud@yahoo.com

الملخص

صاحب ظهور الحاسب الآلي والتوسع في استخدام شبكة الإنترنت في مجالات الحياة المختلفة ظهور بعض الآثار السلبية والمخاطر المترتبة على هذا التوسع، إذ كلما زاد الاعتماد على هذه التقنيات في التنمية، كلما زادت معه المخاطر الخاصة بحماية المعلومات، ومع تزايد الاعتماد العالمي على تكنولوجيا المعلومات والاتصالات، سيما فيما يتعلق الجانب الحكومي والمنشآت العامة، فقد تزايد أيضاً تعرض الدول للهجمات عن طريق الفضاء السيبراني، إذ أصبح هذا الفضاء عرضة للانتهاكات من قبل مخترقي الشبكات سواء كانوا دولا أو هيئات او افراد، ومن هنا بات من الضروري البحث في مدى مشروعية استخدام هذا النوع من الهجمات، سيما اثناء وقوع نزاع مسلح بين دولتين.

الكلمات المفتاحية :- الهجمات السيبرانية ، النزاعات الدولية ، المسؤولية الدولية.

Abstract

The emergence of the computer and the expansion of the use of the Internet in all areas of life The various negative effects and risks arising from this expansion will appear, as the greater the reliance On these technologies in development, the greater the risks associated with protecting information, and with increasing Global reliance on information and communication technology, especially with regard to the governmental aspect Countries are vulnerable to attacks through cyberspace, as it has become and public facilities, it has also increased This space is vulnerable to violations by network intruders, whether they are countries, organizations or individuals. Hence, it has become necessary to research the legality of using this type of attack, especially During an armed conflict between two countries.

Keywords:- Cyber attacks, international conflicts, international responsibility.

مقدمة (Introduction)

دأبت البشرية ومنذ أمد بعيد على تطوير طرائق ووسائل القتال الأضعاف عدوها إلى أكبر قدر ممكن، دون أن تأبه - وعلى نحو يفصله التاريخ - بنتائج الوسائل تلك ومدى الخطورة التي تشكلها على الحياة الإنسانية، ولأجل ذلك لم تتوقف عمليتا الاستحداث أو التطوير الذان شهدهما القطاع العسكري والأمني، ليشهد العالم سباقا جديدا للتسلح خاض غماره الأقوى على الصعيد التكنولوجي ونقصد بذلك موضوع الدراسة ألا وهي السيبرانية كمفهوم جديد للحرب الخفية الحالية، والظاهرة للعيان في المستقبل القريب كبديل للحرب التقليدية. بما إن سنة الحياة هي التغيير المستمر، فإنه يتسم حاليا بتزايد سرعته باستمرار. من خلال تطور المجتمعات البشرية التي غالبا ما تمر بمنعطفات تاريخية تحددها الثورات في العلوم والتكنولوجيا وتطور وسائل الإنتاج المتاحة و انعكاساتها على المجتمع ، وكامتداد لهذه المنعطفات الحادة في التاريخ البشري ، فإننا الأن نعيش ثورة جديدة شهدها قطاع وسائل الاتصال، والا سيما في نطاق تكنولوجيا المعلومات.

وعليه سنحاول في هذا البحث بيان مشروعية استخدام الهجمات السيبرانية في حالة الحرب كمبحث أول فيما قسم هذا المبحث إلى مطلبين : المطلب الأول مشروعية استخدام هجمات السيبرانية في حالة النزاع المسلح وتعارضها مع مبادئ الحرب التقليدية ، أما في المطلب الثاني مشروعية استخدام هجمات الفضاء السيبراني في حالة الدفاع الشرعي ، في حين يتناول المبحث الثاني تحديات التعاطي القانوني مع الهجمات السيبرانية والمسؤولية الدولية عنها نتناول فيه تحديات واشكاليات التعاطي مع الهجمات السيبرانية كمطلب أول أما في المطلب الثاني اركان المسؤولية الدولية عن الهجمات السيبرانية، وفي المطلب الثالث ولأخير سوف نتناول فيه مستويات ووسائل الهجمات السيبرانية.

المبحث الاول
مشروعية استخدام الهجمات السيبرانية في حالة الحرب

واجهت مسألة اضفاء المشروعية القانونية على العمليات السيبرانية العديد من التعقيدات والاشكاليات القانونية من حيث تطابقها وتباينها مع جملة من القواعد والمبادئ والاحكام الاساسية التي تحكم النزاعات المسلحة التقليدية في القانون الدولي، سيما وان هذا الاسلوب المتطور من اساليب الحرب له من الخصائص ما يميزه عن الاسلحة التقليدية من حيث الاثار، ومدى امكانية الالتزام بقواعد الحرب

ومبادئ القانون الدولي الانساني التي تحكم النزاع من حيث حماية الافراد المدنيين المحميات الطبيعية والبشرية.

سنقسم هذا المبحث الى مطلبين: **المطلب الاول:** مشروعية استخدام الهجمات السيبرانية في حالة النزاع المسلح وتعارضها مع مبادئ الحرب التقليدية ، اما **المطلب الثاني:** مشروعية استخدام هجمات الفضاء السيبراني في حالة الدفاع الشرعي.

المطلب الاول
مشروعية استخدام الهجمات السيبرانية في حالة النزاع المسلح موقفها من مبادئ الحرب التقليدية
The legality of the use of cyber-attacks in the event of armed conflict and its conflict with the principles of conventional warfare

ان تحليل مشروعية استخدام الفضاء الالكتروني من منظور القانون الدولي الانساني، وما يثيره من قضايا قانونية أساسية، حيث لا يتضمن قانون الحرب أي قواعد صريحة بشان الفضاء السيبراني، حيث لا تكون هذه الاعتداءات حركية، أي ليست اعتداءات مسلحة في حد ذاتها، وينطبق القانون الدولي الانساني بالفعل بالنظر إلى هدفه الاساسي، وهو حماية المدنيين من ويلات الحرب، ويكون استخدام الفضاء السيبراني هو تعرض الاشخاص المحميين او الممتلكات المحمية من الخطر، ويصبح القانون الدولي الانساني منطبقا، وتندرج تلك الاعتداءات تحت قانون الحرب[1].

وتحليل مدى مشروعية استخدام هجمات الفضاء السيبراني او في حالة الدفاع الشرعي عن النفس وفق الاطر القانونية الدولية الحالية، ويثير ذلك مدى امكانية ان يكون لتلك المبادئ علاقة في حال تطبيقها على هجمات الفضاء السيبراني، [2].

وفيما يلي توضيح لاهم مبادئ وقواعد القانون الدولي الانساني في الحرب التقليدية، ومدى توافقها مع قواعد الحرب باستخدام الهجمات السيبرانية.

اولا: مبدأ تقييد حقوق المتحاربين في استخدام أسلحة الحرب في النزاع.

انطلاقًا من تغيُّر طبيعة الحرب ومداها ومجالها فإن القيود التي يجب أن تطبق على المتحاربين أثناء النزاع المسلح يجب أن تتم زيادتها، تلافيًا للضرر الذي يمكن أن يصيب غير الهدف المقصود، سواء من الاشخاص او المنشآت المدنية أو ما يمكن أن ينتج من خسائر عرضية، خاصة مع تزايد الترابط بين دول العالم من

خلال شبكات الاتصال والمعلومات، وتدخُّل ذلك في عمل منشآت حيوية وبنية تحتية كونية يصبح من شأن الحاق الضرر بها إحداث خسائر مدمرة[3].

ان أي سلاح لم يتم ذكره في أي اتفاقية لا يعني بالضرورة إباحة استخدامه، ويُعَدُّ المثال الواضح للحظر الوقائي الوحيد هو ما ورد في البروتوكول الرابع لاتفاقية الاسلحة التقليدية لعام 1980م الخاص بحظر استخدام أسلحة الليزر المعية والذي الحق باتفاقية عام 1995م.

وهذا السلاح تمَّ تحريمُه بمجرد بدء التجارب عليه، وقبل وضعه موضع الاستخدام العسكري الفعلي. لكن هذا المثال لا يمكن تعميمه؛ لان معظم التجارب على الاسلحة الجديدة تعتبر أسرارًا عسكرية، وبالتالي من النادر التعرُّف على آثار تلك الاسلحة. ومن ثم، يأخذ تحريم استخدام سلاح معين حيزًا من الجهد والوقت والنيات الحسنة، وهذا ما قد لا يتوافر، أو يتم التحقق من صحته[4].

في المقابل تم التركيز في اتفاقية جنيف للعام 1949 على حماية الاشخاص في حالة الحرب، دون الاشارة إلى هجمات الفضاء الالكتروني، ودون الاشارة إلى استخدام أسلحة معينة. وتناولت البروتوكولات الاضافية عددًا من طرق الحرب ووسائلها بصفة عامة. لذلك تعد البروتوكولات الاضافية أكثر ملاءمة لتقديم خريطة عمل للموقف من استخدام هجمات الفضاء الالكتروني. وتمت الاشارة بشكل واضح في المادة (36) من البروتوكول الاضافي الاول الى تبني واضعي تلك المادة التطورات الحديثة في وسائل القتال وطرقه، والتي نصت على أن «يلتزم أي طرف سامٍ متعاقد - عند دراسة أو تطوير أو اقتناء سلاح جديد أو أداة للحرب أو اتباع أسلوب للحرب - بأن يتحقق مما إذا كان ذلك محظورًا في جميع الأحوال أو في بعضها بمقتضى هذا الملحق (البروتوكول) أو أي قاعدة أخرى من قواعد القانون الدولي[5].

اقرَّت بذلك تلك المادة حقيقة أن أي نشاط عسكري معين يرتبط بطرق الحرب لم يتم تنظيمه بشكل دقيق لا يعني ذلك أنه يمكن استخدامه بدون أي قواعد. ولذلك فإن الاشكال الحديثة لهجمات الفضاء السيبراني وحرب المعلومات - التي لم يتمّ تضمينها في استخدامات الاسلحة التقليدية في الاتفاقيات الدولية - ترتبط بالقانون الدولي الانساني وتخضع له كأي سلاح جديد عندما يتمُّ استخدامه في النزاع المسلح. فإحدى القواعد الاساسية للقانون الدولي الانساني تقرُّ بأن «حقَّ أطراف النزاع في اختيار وسائل القتال وطرقه ليس مطلقًا »، كما جاء في المادة (35 فقرة 1) من البروتوكول الاضافي الاول[6].

يتمُّ توجيه هجمات الفضاء الالكتروني للعدوّ أو الخصم، وذلك بهدف تحقيق أضرار، وهذا ما يجعلها طريقة للحرب ووسيلة، لاسيما و أنها تتميز بقدرتها الفائقة على تعدي الحدود الدولية، سرعه تنفيذها، عدم القدرة على تحجيم آثارها، كذلك صعوبة تحديد حجم المسؤولية القانونية للدولة، خاصة أنه قد يستخدمها أشخاص مدنيون خارج نطاق القوات المسلحة أو فاعلون من غير الدول.

ثانيا: مبدأ حظر الآلام التي لا مبرر لها.

تعتمد البنية الاساسية الحرجة في الكثير من الدول في عملها على شبكات تكنولوجيا الاتصال والمعلومات، التي تتراوح ما بين الاتصالات إلى خدمات الطوارئ، ومن الصفقات المالية إلى العمليات العسكرية والخدمات الحكومية والتجارة الالكترونية والاقتصاد الرقمي، ويعكس ذلك مدى الارتباط الشديد بين الطابع المدني للفضاء السيبراني وإمكانية تعرّضه للخطر، بما يسبب أضرارًا اقتصادية وسياسية واجتماعي [7].

من ثم فإن استخدام هجمات الفضاء الالكتروني قد ينتج عنه الام مفرطة، بما يتنافى مع الاتفاقيات الدولية التي حظرت استخدام الاسلحة التي تسبب آلاما لا مبرر لها، وبالرغم من عدم تحديد الفضاء الالكتروني باعتباره مجالاً لذلك التحريم، فإننا يمكننا قياس ما ورد في تلك الاتفاقيات على ما يمكن أن ينتج عن استخدام الفضاء الالكتروني لإصابة أي بنى تحتية حيوية، تشكل مصلحة للمجتمع الدولي قاطبة، ولا تختلف عن نتائج استخدام القوة والعمل العسكري التقليدي. حيث إن هناك اختلافًا في الاليات العدائية، ولكنها تتشابه في الاثار والنتائج، عبر استخدام أسلحة الفضاء السيبراني المتنوعة[8].

ثالثا: مبدأ حظر الهجمات العشوائية.

ان الهجمات العشوائية «هي التي من شأنها أن تصيب الاهداف العسكرية والاشخاص المدنيين أو الاعيان المدنية دون تمييز». وأقرَّت المواد (8- 51 – 57) من البروتوكول الاضافي الاول لاتفاقيات جنيف للعام 1977م حظر الهجمات العشوائية التي لا توجَّه إلى هدف عسكري محدد، أو التي تستخدم طريقة أو وسيلة للقتال لا يمكن أن توجَّه إلى هدف عسكري، أو التي تستخدم طريقة أو وسيلة للقتال لا يمكن حصر آثارها على النحو الذي يتطلبه البروتوكول. ومن ثم فإن من شأنها أن تصيب في كل حالة كهذه الاهداف العسكرية والاشخاص المدنيين أو الاعيان المدنية دون تمييز؛ حيث إن طبيعة تلك الهجمات لا تملك القدرة على التمييز بين ما هو مدني وما هو عسكري[9].

وجرى تأكيد حظر الهجمات العشوائية في المادة (4/51) من البروتوكول الاضافي الاول؛ حيث إن الهجمات العشوائية هي تلك الهجمات التي لا تستهدف هدفًا عسكريًّا محددًا، أو ذلك الهجوم الذي لا يمكن التحكم في آثاره أو التنبؤ بتداعياته. وان المادة (4/51 و5) من البروتوكول الاول تعدِّد خمسة أنواع من الهجمات العشوائية، هي تلك التي[10].

1. لا توجَّه إلى هدف عسكري محدد
2. تستخدم طريقة أو وسيلة للقتال لا يمكن أن توجَّه إلى هدف عسكري محدد.
3. لا يمكن حصر آثارها على النحو الذي يتطلبه البروتوكول.
4. تعالج عددًا من الاهداف العسكرية واضحة التباعد والتميُّز بعضها عن البعض الاخر والواقعة في منطقة حضرية، على أنها هدف عسكري واحد.
5. تنتهك مبدأ التناسب بين الميزة العسكرية وخسائر المدنيين وتبعد تلك القواعد في حال تطبيقها على هجمات الفضاء الالكتروني، والتي ربما تمثل عملية استخدامها خطورة أكثر، وتبقى مسألة توجيه هجمات الفضاء الإلكتروني إلى أهداف محددة شيئًا غير متوقع أو يمكن التحكم فيه وفي نتائجه على الأهداف المدنية وغير المدنية كذلك؛ حيث تتميز تلك الهجمات باتساع مجالها، كارثية نتائجها، وعشوائية الإصابة[11].

رابعا: مبدأ الحياد في القانون الدولي.

ان استخدام الفضاء السيبراني لشنِّ هجمات يمثل انتهاكًا لمبدأ الحياد في القانون الدولي، حيث إن الفضاء الالكتروني يمرُّ عبر حدود العديد من الدول، ومن ثم فان الطابع الدولي للفضاء السيبراني يجعل أيًّا من أطراف النظام الدولي معرضين للإصابة من جراء شنِّ تلك الهجمات. كما أنه إذا تمَّ شنُّ تلك الهجمات فإنها تمرُّ عبر دولة ثالثة أو أكثر غير متورطة في الصراع، وعلى الرغم من عدم مسؤوليتها القانونية فإنها قد تصبح متورطة في تلك الهجمات، وهذا ما يُعَدُّ انتهاكًا للقانون الدولي الانساني واتفاقية جنيف؛ حيث جاء فيها: « إن الدول والاطراف المشاركة في النزاع تمتنع عن تحريك القوات أو إرسال مستلزمات الحرب أو الامدادات عن طريق أراضي الطرف المحايد[12].

يتحرك الهجوم السيبراني عبر شبكات الاتصال والمعلومات العابرة للحدود، وبالتالي فإنها تمرُّ بدول محايدة. ويمكن أن تحمل أسلحة خاصة تختلف في التكتيك وطرق العمل، ولكنها تدخل ضمن تعريف الاسلحة باعتبارها أدوات للقتل أو إلحاق الضرر أو التسبب في وجود جرحى أو تدمير ممتلكات للخصم ». ومن ثم فإن الدول المحايدة تمتنع عن نقل أسلحة الفضاء السيبراني عبر شبكات الاتصال والمعلومات

التي تمرُّ عبر أراضيها. فأسلحة الفضاء السيبراني يمكن أن تُلحق الضرر بالمدنيين والمنشآت المدنية؛ ولذلك فإن هجوم الفضاء الالكتروني مثل غيره من أنواع الهجوم التقليدي، وقد يمرُّ ذلك الهجوم عبر دولة أخرى وقد لا تشعر به[13].

المطلب الثاني
مشروعية استخدام الفضاء السيبراني في حالة الدفاع الشرعي
The legality of using cyber in the case of legitimate defense

توجد في ميثاق الامم المتحدة قواعد قانونية تتعلق بحقِّ الدفاع الشرعي كونه حقًّا مشروعًا لكل معتدَى عليه عندما يقع عليه فعل الاعتداء، والذي يُعَدُّ جريمة على النفس أو المال. ونظمت كل القوانين الداخلية وبيّنت نشوء هذا الحقِّ واستعماله، والمادة (51) من ميثاق الامم المتحدة نصت على حق الدفاع الشرعي والتي جاء فيها: «ليس في هذا الميثاق ما يُضعف أو ينقص الحق الطبيعي للدول فرادى أو جماعات في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء هذه الهيئة، وذلك إلى أن يتخذ مجلس الامن التدابير اللازمة لحفظ السلم والامن الدوليين»، وحتى عصبة الامم اعترفت بهذا الحق. ونص بروتوكول جنيف للعام 1924 على هذا الحق في المادة (2) منه والتي جاء فيها « أن الدول الموقعة قد اتفقت على أنها سوف لا تلجأ للحرب وسيلةً لفض النزاعات بأي حال إلا في حالة مقاومة العدوان»[14].

ولاستعمال حقِّ الدفاع الشرعي شروط في القانون الدولي، حيث إن الردَّ يجب أن يتقيّد بشرطين: الاول، أن تكون القوة المبذولة للردِّ موجهة إلى مصدر الاعتداء، فلا يجوز أن يكون المعتدي دولة وأن يوجَّه الردُّ لدولة أخرى. وعندما تمارَس هذه الحالة فإنها عدوان.

والثاني، أن تكون القوة المبذولة للردِّ متناسبة مع العدوان، وفي حدود القدر الضروري لردِّ العدوان وإيقافه عند حدِّه. و أجاز القانون الدولي فعل الدفاع الذي يمكن أن يمارَس من قِبل الغير على مصدر الاعتداء، شريطة أن يكون قرار التدخل حصريًّا لمجلس الامن، وهذا ما نص عليه في مواد الميثاق (42،41،40،39)[15].

حددت المادة (51) الاطار المنظم لكيفية الدفاع الشرعي والذي يمكن أن يتمَّ في شكل هجمات واضحة يتمُّ تصنيفُها على أنها هجوم مسلح. وجاءت هجمات الفضاء السيبراني أو حرب المعلومات لكي يتمَّ شنُّها على نطاق واسع. و أصبح غير كافٍ تصنيفها هجومًا مسلحًا وفق القانون الدولي التقليدي. ومن ثم لا تخضع لسلطة قانون الاتفاقيات الدولية أو القانون الدولي العام أو القانون الجنائي العرفي[16].

كما أن ميثاق الامم المتحدة يركز على مسألة تنظيم استخدام القوة فيما بين الدول وفق المادة (4/2) التي وضعت شروط التزام استخدام هذه القوة ونطاقها، وعند النظر إلى الهجمات التي يتمّ شنُّها في الفضاء السيبراني وفق ما جاء في نص المادة (51) فإنه يبقى تساءل حول إذا ما كان يمكن تصنيف تلك الهجمات باعتبارها تخضع للتصنيف الخاص بالهجوم المسلح. ولكن عند التركيز على الوسائل المستخدمة في هجوم حرب المعلومات والارهاب الالكتروني فانه يمكن القول إنها تضاهي ما يتم استخدامه في الحروب التقليدية في آثارها وتداعياتها، كما ينتج عنها قدر من القنابل والاسلحة والقصف والعدوان وغيرها من مظاهر استخدام القوة داخل الفضاء السيبراني، والذي يكون له تأثير مماثل لتأثير الهجمات التقليدية[17].

واكد ميثاق الامم المتحدة تحريم استخدام القوة المسلحة أو التهديد باستخدامها ضد السلامة الاقليمية أو الاستقلال السياسي للدول الاعضاء في المتحدة، وذلك مع وجود حالات الضرورة التي حرص القانون الدولي من خلالها على تحجيم الحرب ووضع قيود عليها إذا ما وقعت. وأورد ميثاق الامم المتحدة استثناءات لحالة الاستخدام المشروع للقوة في القانون الدولي، وهي حالات: الدفاع الفردي والجماعي الذي تضمنته المادة (51) من ميثاق الامم المتحدة، وحق تقرير المصير، وحروب التحرير، والعمليات الحربية التي يقوم بها المجتمع الدولي التي يقرُّها مجلس الامن التابع للأمم المتحدة وفق أحكام الفصل السابع[18].

لقد اصبح المجتمع الدولي أمام نمط جديد من الحرب يحمل أساليب جديدة وهجومًا غير تقليدي في بيئة غير تقليدية ولها تداعيات غير محسوبة، و إذا ما نجحت فإنها تصيب المنشآت المدنية وتبثُّ الرعب والخوف وتؤثر على الاستقرار السياسي داخل الدول وعلى المجتمع الدولي قاطبة. ففي أحد السيناريوهات فإن هجمات الفضاء الالكتروني قد تتمُّ من خلال الدخول إلى شبكات المعلومات بشكل غير شرعي، وبما يؤثر على عمل البنية التحتية الكونية للمعلومات، وما يكون له من تأثير على الدول فرادى وعلى المجتمع الدولي ككل، والذي أصبح يعتمد بشكل متزايد على تلك الشبكات الدولية باعتبارها مسهلات لتقديم الخدمات التي تتعلق بنمط الحياة المعاصر[19].

هذه الشبكات إن أصابها الضرر فإنها تهدد بوقوع خسائر و أضرار يقف خلفها دولة أو فاعل من غير الدول في مواجهة دولة أطراف من غير الدول، ويكون من آثار ذلك بروز عمليات دفاع شرعي تأتي في مضمونها مع الحقِّ الذي أقرَّه القانون الدولي. إلا أن ظروف استخدام هذا الحقِّ وشروطه الموضوعة في ميثاق الامم

المتحدة أصبحت غير ملائمة لممارسته داخل بيئة جديدة وتحديات جديدة يفرضها استخدام القوة في الفضاء السيبراني للدفاع الشرعي.

كما يفرض تحديات تتعلق بإجراءات الوقاية والحماية ضد التعرّض لمثل تلك الهجمات. ومن ثم فإن أفعال الدفاع الشرعي قد لا تأتي في شكل القيام بهجوم مسلح تقليدي، بل قد تتخذ أشكالاً أخرى لها تأثيراتها وتداعياتها على الفضاء الالكتروني بوصفه مجالا واحدا تسبح به جميع المصالح والخدمات والتواصل العالمي، ويشكل أهمية استراتيجية للمجتمع الدولي، وينتج عن تعرُّضه لمسألة الدفاع والهجوم بلا شك تأثير على وظيفته وطبيعة دوره ومستقبله ويمسُّ أهميته للمجتمع الدولي[20].

هناك خطر تصاعد الهجمات عبر الفضاء الالكتروني بالتزامن مع النمو ذاته فيما يتعلق بأسلحة الدمار الشامل. كما أن هناك دولاً عدة تعمل على نمو قدراتها في مجال حرب المعلومات وأسلحة الفضاء، الالكتروني. وأخذت هجمات الكمبيوتر والارهاب الالكتروني Cyber Attacks المزيد من الاهتمام إلى الحدِّ الذي وضعته الدول في إطار استراتيجيتها العسكرية، وما يثيره ذلك من تساؤلات حول حدود استخدام القوة في الفضاء السيبراني للردِّ على الهجمات في إطار الدفاع الشرعي أو في استخدامها باعتبارها نمطًا من أنماط استخدام القوة في العلاقات الدولية أو فيما يتعلق بالهجمات الوقائية؛ حيث فرضت هواجس التعرُّض للخطر في أي وقت انتهاج شتى الطرق للحماية، والتي تأخذ شكلا وقائيًّا أو إستباقيا على مصدر التهديد المحتمل، أو العمل على تقوية نظم الحماية والمنعة ضد التعرُّض لمثل تلك الهجمات[21].

ان اندفاع دولة في الهجوم على دولة أخرى يمكن أن يدفع الدولة المعتدَى عليها للردّ بهجمات مضادة دفاعًا عن النفس. وتلك الهجمات لم يتمّ تحديدها قانونًا في حق الدفاع الشرعي عن النفس. كما يواجَه الهجوم في الفضاء الالكتروني بتحديات تتعلق بخصائص هذا الهجوم، الذي يتميز بان المهاجمين يتسببون في سلسلة من الاضرار عن طريق الدخول إلى نظم المعلومات. وطبيعة تلك الهجمات تجعل من الصعوبة بمكان - إن لم يكن مستحيلاً - تحديد مركز الهجوم المباشر، بما يؤثر على فاعلية الردِّ الدفاعي. ولا توجد دولة يمكنها أن تصل إلى درجة عالية من المنعة ضد تلك الهجمات[22].

اما التحدي الثاني فيتعلق بإمكانية التعامل مع أي قاعدة قانونية جديدة تعمل على تنظيم استخدام هجمات الفضاء السيبراني في حالة الدفاع الشرعي عن النفس. فإذا ما استندت الدول إلى مثل ذلك في مواجهة هجمات الفضاء الالكتروني بصورة فردية، فإنها تحمل تقديرًا لعدم مشروعية العمل المبرر للردِّ، وتتطلب أن يتمَّ تأكيد

أن تلك التدابير تلعب دورًا أكثر فاعلية في العلاقات الدولية من أعمال الانتقام غير المبرَّر. وقد تنطوي تدابير الردِّ بالمثل على تعسف في استعمال الحق، أو تمثل شكلاً من أشكال التدخل في الشؤون الداخلية للدولة الذي حرصت على حمايته مواثيق الامم المتحدة والحفاظ عليه[23].

هناك تحدٍّ آخر يتعلق بالحاجة إلى أن يتبنى المجتمع الدولي نظام قانون دولي يتعامل مع التنظيم الفعال لاستخدام هجمات الفضاء الالكتروني وحرب المعلومات وأي أنشطة قد ترتبط بها والتمييز بينها، وتستطيع أن تتعامل مع أسلحة إلكترونية حديثة وتكتيكاتها، والتي قد تكون أدوات في أيدي فاعلين عدوانيين، وكذلك إيجاد مفهوم واضح للهجوم المسلح.

كذلك هناك تحدٍّ يتعلق بصعوبة التمييز بين هجمات شبكات الكمبيوتر التي ترتبط بالنشاط الاجرامي عن الاخرى التي ترتبط بأنماط الارهاب وعن النشاط الذي تقف وراءه وتسانده الدولة[24].

كما أن هناك عددًا من المفاهيم والتعريفات التي ترتبط بالحرب في الفضاء الالكتروني، ويمكن تفسيرها بطرق عديدة تبعًا لمن يستخدمها والهدف من ورائها، والذي يصعب تحديده بسهولة.

اما القضية الاخطر التي يمكن أن تثار في إطار محاولة تنظيم هجمات شبكات الكمبيوتر، والتي لم يتم تناولها في القواعد القانونية الخاصة بالدفاع الشرعي، فهي تتبدى في أبهى حلها في أن الفضاء الالكتروني يحمل بعدًا عسكريًّا إلى جانب أنه يحمل في الوقت نفسه بعدًا مدنيًّا، وهذا ما يحتاج إلى تحديد مقتضيات وخصائص الهجوم الذي يُعَدُّ عدوانًا وحربًا و إرهابًا ومبدأ الدفاع الشرعي عن النفس بصفة خاصة، وما يمكن أن يتعلق بالجهد الدفاعي أمام تلك الهجمات[25].

وهناك ايضا تحدٍّ خطير يتعلق بإمكانية المواءمة ما بين الهجوم والردِّ عليه، وشرط التناسب مع فعل الاعتداء الذي هو شرط من شروط الدفاع الشرعي عن النفس وفق القانون الدولي؛ حيث إن شبكات الكمبيوتر تسمح بتعدي آثار الاعتداء لأكثر من دولة. كما أن الردَّ على مثل هذا الاعتداء يتعدى أيضا أكثر من دولة، دون القدرة على تحديد مصدر الهجمات. ومن ثم فإن الدفاع الشرعي يصبح عدوانًا؛ وذلك لعدم قدرته على التمييز. بالإضافة إلى إمكانية إحداثه لأضرار لا مبرر لها؛ حيث يمكن أن تطول مرافق حيوية، والتي فرض القانون الدولي حماية خاصة لها في أثناء النزاعات المسلحة[26].

المبحث الثاني
تحديات التعاطي القانوني مع الهجمات السيبرانية والمسؤولية الدولية
Challenges of Legal Dealing with Cyber Attacks and International Responsibility

لا زالت حتى يومنا مسألة التعاطي القانوني وتكييف الهجمات السيبرانية تثير الاشكال سواء بين الدول او الفقه القانوني والخبراء في مجال القانون الدولي الانساني والقانون الدولي العام، سيما في ظل استمرار الغموض وكثرة التأويلات بشان نصوص الميثاق الامم المتحدة بهذا الصدد وعدم الاتفاق على تفسير محدد يتم الاستشهاد به لتكييف مثل هذه العمليات، وعلى الرغم من تعدد المناسبات التي حاولت من خلالها الجهود الدولية الرامية الى تقنين العمليات السيبرانية الا ان اعتراض بعض الدول سيما الكبرى منها ساهمت بتعقيد المشهد في ظل تعدد الآراء والمقترحات، سيما وان هذه الدول المستفيد الاكبر من بقاء هذا النوع من العمليات دون غطاء قانوني صريح، بسبب ما تتمتع به من قدرات بهذا المجال لذا فإنها غالبا ما تحاول جاهدة توظيف نفوذها الدولي لعرقلة أي اتفاق يقضي بتقنين مثل هذه العمليات وقولبتها ضمن قواعد محددة، ومع تنامي هذه العمليات في العديد من المناسبات الدولية وزيادة حدتها واثارها المدمرة فقد باتت المسؤولية الدولية عن هذه العمليات محل نقاش وجدل بين الفقه القانوني الدولي، والذي يشترط توافر العديد من العناصر كأركان اساسية لقيام هذه المسؤولية.

وفيما يلي سنناقش ذلك من خلال تقسيم هذا المبحث الى ثلاثة مطالب، نتناول في **المطلب الاول:** منه تحديات واشكاليات التعاطي مع الهجمات السيبرانية، في حين خصصنا **المطلب الثاني:** منه لبيان اركان المسؤولية الدولية عن الهجمات السيبرانية، واخيرا في **المطلب الثالث:** منه نوضح مستويات ووسائل الهجمات السيبرانية.

المطلب الاول
تحديات واشكاليات التعاطي مع الهجمات السيبرانية
Challenges and problems of dealing with cyber attacks

ينصب قدر كبير من الاهتمام السياسي والقانوني الدولي اليوم على حماية المعلومات وتكنولوجيا المعلومات التي لها أهمية كبيرة للدولة، نظرا لمساسها بالسلم والامن المجتمعي، ومن ثم يصبح من الواجب على الدولة حمايتها بكافة السبل الممكنة من أي اعتداء، وثمَّة وسيلتان (لا تستبعد إحداهما الأخرى) لتوفير مثل هذه

الحماية، اما الدفاع عن أصول البلد من العمليات الهجومية، او ردع الطرف المعادي عن القيام بمثل هذه العمليات.

ويتضمَّن الدفاع اتخاذ إجراءات تقلل من احتمالية نجاح عملية هجومية، ويمكن لمثل هذه الاجراءات ان تمنع الجاني من الوصول إلى مراده وغاياته، أو تزيل على الاقل مواطن الضعف والقصور، أو تُمكِّن ضحية العملية من التعافي سريعًا من عملية هجومية ناجحة، وقد تم طرح عدداً من الإشكاليات القانونية سنقف عندها بالبحث والتحليل وأهمها، هل ينطبق القانون الدولي، سيما القانون الدولي الإنساني على الهجمات السيبرانية؟ وبعبارة أخرى، ما هو الموقف منها في ظل وجود فراغ قانوني يعتقد به البعض من المختصين[27].

ومن جهة أخرى يطرح بعض الفقه إشكاليات من زاوية مختلفة، منها: ما هو الموقف من مبدأي الشرعية والمشروعية فيما يتعلق بالهجمات السيبرانية، بالتركيز على مبدأ الضرورة العسكرية ومبدأ التناسب ومبدأ وجوب التمييز في استخدام القوة.

ويرى آخرون أن الهجمات السيبرانية يمكن أن تكيف لا في ظل أحكام القانون الدولي الإنساني المدونة فحسب، بل في أحكام القانون الدولي العام ككل، على أساس أن الصورة الأولية تظهر أن مثل هذه الهجمات يمكن أن ترتكب أثناء النزاعات المسلحة الدولية أو غير الدولية، وفي أوقات السلم أيضاً، ما يلوح في الأفق مواضيع أخرى، يطرحها هؤلاء وأهمها المسؤولية الدولية الناشئة عن الهجمات السيبرانية في وقت السلم، ومفهوم السيادة والولاية القضائية[28].

ومن ناحية اخرى نجد أن معظم الهجمات السيبرانية لا تتبناها الدول رسمياً، إنما قد يعلن فرد أو مجموعة من الأفراد المسؤولية عنها، فكيف يمكن للقانون الدولي أن يتصدى لهذا الموضوع، وبعبارة أخرى أيهما سيطبق معيار السيطرة الكاملة(Overall Control) ، أم السيطرة الفاعلة (Effective Control)[29] ، ام الاثنان معاً لتقرير المسؤولية الدولية؟.

كما تشكل الهجمات السيبرانية تهديدا لأحد المبادئ الرئيسة في القانون الدولي، وهو احترام سيادة الدول، بوصفه واجبا أساسيا، وهو واجب "عدم التدخل"، الذي نصت عليه المادة (4/2) من ميثاق الأمم المتحدة، لما فيها من تسريب لمعلومات أمنية وسرية عن حكومات الدول، وقد يتجاوز الأمر ذلك الى الحد الذي يصل به الى الإضرار بالمدنيين، عندما ينتج عن هذه الهجمات قطع للخدمات الحيوية كالماء والكهرباء ووسائل النقل العام.

يرى البعض بأن الفترة التي جرى فيها تقنين القواعد القانونية ذات الصلة باستخدام وسائل وطرائق القتال، لم يكن لاستخدام الأنظمة الالكترونية للأغراض

العسكرية فيها أي وجود يذكر، ما يعني أنها غير مقننة أصلاً، وأنها غير منظمة وفقاً للقواعد الدولية العرفية ما يفهم أنها خارج التنظيم القانوني الدولي[30].

وعليه فان تكييف استخدام الهجمات السيبرانية يدور في فرضيتين، الأولى عدم القدرة على إثبات الدليل المادي الناجم عن استخدام الهجمات السيبرانية، وهي العائق الأكبر الذي يواجهه المختصون بهذا الصدد، على عكس وسائل وطرق القتال الأخرى المعروفة، والتي تترك أثراً مادياً ملموساً مباشراً أم غير مباشر بعد الهجوم، كالدمار أو التعطيل الجزئي أو الكلي الذي تتعرض له الأعيان العسكرية أو المدنية أو القتل أو الجرح الذي يصيب المقاتلين أو المدنيين[31].

أما الفرضية الثانية فعلى العكس من ذلك، إذ ما ثبت أن الهجمات السيبرانية قد تؤدي إلى آثار مادية ملموسة على المستويات الاقتصادية والأمنية والعسكرية كافة[32].

ولدى قراءة ديباجة القرار الصادر عن الجمعية العامة للأمم المتحدة رقم (55/٣٦) لعام 2000م، بشأن "مكافحة إساءة استعمال تكنولوجيا المعلومات"، يتضح أن آثار الهجمات السيبرانية غير محدودة بنطاق معين، ويمكن أن تطال اثارها مختلف مجالات الحياة، ومع ذلك لا يزال البحث في خطورتها يناقش على المستوى الأدنى من التنظيم الدولي[33].

أن تأخر الدول في التوصل إلى اتفاقية دولية معنية بالهجمات السيبرانية، يعيد بالذاكرة إلى الوراء، وتحديدا بشأن حدث من تأخر التنظيم القانوني الصريح لاستخدام الأسلحة النووية، سواء بالحظر أو التقييد حتى وقتنا الحالي، حيث مانعت الدول الحائزة على هذه الاسلحة وعرقلت التنظيم القانوني لاستخدام هذه الاسلحة في العديد من المناسبات، لحين التوصل لاتفاقية حظر الانتشار النووي لعام ١٩٦٨، واتفاقية الحظر الشامل للتجارب النووية لعام ١٩٩٦م[34].

ومن خلال ما تقدم يبدو أن العائق في تكييف الهجمات السيبرانية كإحدى وسائل أو طرائق القتال، إنما يعود لمصالح بعض الدول الرائدة في مجال استخدامها، فضلاً عن قدرة الأنظمة الالكترونية في تحويل تلك الأوامر(برامج الكترونية عدائية) إلى آثار مادية ملموسة، وبعبارة أخرى لها حركة وقابلة لإحداث خسائر بحق أهداف منتخبة مسبقاً في الدولة الضحية للهجوم السيبراني وهو ما يطلق عليه عادة بالأثر الحركي[35].

المطلب الثاني
اركان المسؤولية الدولية عن الهجمات السيبرانية
Elements of international responsibility for cyber attacks

هناك تشابه الى حد ما بين كلا من قواعد القانون الوطني وتلك التي تحكم القانون الدولي، واذا ما كان المخاطر بالقانون تشابه الى حد كبير بين النظام القانوني المحلي، والنظام القانوني الدولي، واذا ما كان المخاطب بالقانون الداخلي هم الاشخاص، فان القانون الدولي له اشخاصه، وهؤلاء يتجسدون بهيئة دول، وكلا القانونين يفرض التزامات يقابلها حقوق على الاشخاص المعنيين به، اذ نجد ان الدولة في نطاق القانون الدولي تثور مسؤوليتها متى ما اقدمت على أي فعل من شأنه ان يتسبب باي ضرر يصيب دولة اخرى او مجموعة دول، ومن هذا القبيل.

فالدولة التي تقوم بأي فعل من شأنه إحداث ضرر يصيب دولة أخرى أو عدة دول، فتتحمل الدولة التي أحدثت ذلك الضرر، أو تسببت في إحداثه، تبعات المسؤولية الدولية عن ذلك الفعل، فالهجمات السيبرانية يقوم بها أشخاص يخضعون للقانون الدولي، وتؤدي إلى أضرار، وبذلك تكون الهجمات السيبرانية مستوفية شروط قيام المسؤولية الدولية، لكن لنقص القواعد القانونية، وصعوبة إثبات مصدر تلك الجهات، فإنه يتعذر ذلك[36].

ويجمع الخبراء وفقهاء القانون الدولي الحديث، على ان قيام مسؤولية الدولة عن الهجمات السيبرانية تتطلب لإثباتها توافر العناصر التالية والتي تشكل اركان هذه الجريمة في نطاق القواعد والمبادئ الثابتة في القانون الدولي العام.

1: نسبة الفعل إلى الدولة

اذ لا يكفي الاعتراف بوجود مسؤولية نتيجة وقوع فعل ضار، او غير مشروع بموجب القانون الدولي، بل يجب بالإضافة الى ذلك ان يتم اسناد هذا الفعل الى دولة معينة، فلا مسؤولية دون تحديد الفاعل الاصلي للفعل الذي يشكل جريمة، ويشترط بهذا الصدد ان تكون الدولة ذات سيادة تامة كشرط اساسي لقيام مسؤوليتها عن تصرفاتها الضارة، بمعنى ان تتمتع بكامل الاستقلالية وبالتالي يمكن مساءلتها عن سلطاتها التنفيذية والتشريعية والقضائية، وعليه فان الدول المنظمة في ظل دولة اتحادية لا يمكن مساءلتها عما ارتكبته من سلوك مجرم قانونا، لانتفاء صفة الدولة عنها وبالتالي لم تعد من اشخاص القانون الدولي العام[37].

وعند مقارنة ما سبق بحالة الهجمات السيبرانية، يلاحظ ان الضرر يتحقق في مثل هذا النوع من الهجمات بمجرد تنفيذها، سيما وانها تستهدف البنية التحتية للدول في الغالب، مخلفة وراءها اثارا ضارة قد تفوق احيانا ما ينتج عن الاسلحة التقليدية

من اضرار، نظرا لاتساع نطاق العمليات السيبرانية وسرعة انتشارها في عدد من الانظمة المخترقة في ظل ثوان معدودة، وبغض النظر عما اذا كانت الجهة صاحبة الاعتداء الدولة ذاتها ام منظمات حكومية او اشخاص عاديين او مجاميع ارهابية، ففي جميع الحالات السابقة يتوافر الركن الاول، وهو صفة الدولة وبالتالي قيام مسؤولية الدولة عن هذه الافعال، استنادا لمسؤولية الدولة عن افعال رعاياها في حالة التقصي[38].

2: أن يكون الفعل غير مشروع دوليا

يكاد لا يختلف اثنين على ان الفعل غير المشروع، هو كل تصرف يشكل انتهاكا لاحكام ومبادئ القانون الدولي، وبالتالي فان الفعل الغير مشروع على المستوى الدولي يتمثل في أي سلوك يصدر عن الدولة بما يخالف الالتزامات المفروضة عليها بموجب الاعراف والقوانين الدولية، وان معيار عدم المشروعية هنا هو معيار موضوعي دولي، لا دخل لمنشأ الالتزام فيه، نظرا لان مخالفة أي التزام دولي مهما كان مصدره يولد مباشرة قيام مسؤولية الدولة عن هذا التصرف، بغض النظر عن الوصف القانوني لهذا الفعل وتكييفه وفقا للقانون الداخلي للدولة، وسواء كان هذا الفعل بالسلب أي الامتناع عن تنفيذ التزام قانوني، ام بالإيجاب، أي من خلال الاتيان باي سلوك يشكل انتهاكا لقواعد واحكام القانون الدولي[39].

وفي التطبيق على الهجمات السيبرانية، نجد أنها مخالفة لقواعد القانون الدولي، نظرا لما ينتج عنها من اضرار ومخلفات مدمرة فيها مخالفة واضحة وصريحة لمقاصد ومبادئ جوهرية اشارت اليها الاتفاقيات والمواثيق الدولية والزمت الدول باحترامها، وعلى راسها ميثاق الامم المتحدة .

3: الضرر

يشكل عنصر الضرر احد ابرز عناصر واركان تحقق المسؤولية، ان لم يكن اهمها على الاطلاق، نظرا لان انعدام هذا الركن يهدم قيام المسؤولية ويلغي أي مبرر لوجودها، وللضرر عدة صور وانواع، منها ما يقسم نظرا لمصلحة المعتدى عليه، ومنها ما يقسم وفقا للجهة المتضررة ممن لحقها الضرر، (كالضرر المباشر، او الغير مباشر)[40].

فمن حيث المصلحة محل الاعتداء يقسم الضرر الى ضرر مادي، وهو كل ما يمس بحق مادي للدولة، او رعاياها، الامر الذي يترتب عليه اثرا مباشرة ظاهرا للعيان، في حين يتمثل الضرر المعنوي بكل مساس بالشخصية الاعتبارية للدولة، او احد رعاياها، فهو كل اعتداء ينصب على احد الحقوق المعنوية للأشخاص مما يرتب اثارا غير ملموسة، الا انها تشكل قيمة ادبية للمعتدى عليه[41].

ولدى مقارنة ما سبق على حالة الهجمات السيبرانية نجد ان الضرر في الاخيرة يتحقق بكافة اشكاله، سواء كان الفاعل دولة ام هيئات ام اشخاص عاديين، فان ركن الضرر يتحقق بمجرد وقوع الفعل الضار على الدولة والذي يمس سيادتها وامنها القومي، الا انه بالرغم من ذلك تبقى مسألة تتبع الفاعلين وتقديمهم الى العدالة مهمة مصحوبة بالمخاطر لما يتمتع به الفضاء السيبراني من خصوصية وسهولة اخفاء معلومات وبيانات الفاعلين، ومن ثم التخفي للحيلولة دون الكشف عن هويته، مما يعقد من عملية مساءلة القائمين على هذه الهجمات[42].

المطلب الثالث
مستويات ووسائل الهجمات السيبرانية
Levels and means of cyber attacks

يمكن القول إنّ الهجمات السيبرانية تنقسم إلى ثلاثة مستويات هي:

1) حرب المعلومات الشخصية (التجسس الإلكتروني):

(Cyber espionage): التجسس الإلكتروني هو عملية اختراق شبكة أو جهاز إلكتروني، بهدف سرقة المعلومات المخزّنة فيه، والتي عادة ما تكون على درجة كبيرة من الأهمية، سواء أكانت معلومات عسكرية، أم اقتصادية، أم صناعية، أم تجارية، أم غيرها، وهو ما يترتب عليه آثار إستراتيجية فادحة في الطرف المستهدف[43].

ويوصف هذا المستوى بأنه تجاوز لحدود الخصوصية الإلكترونية الفردية، مما يشكل اعتداء على الحقوق الشخصية للفرد، وانتهاكا لحرمة الحياة الخاصة، ومنها سرقة البيانات المالية ونشرها عبر الشبكة الإلكترونية للمعلومات (الإنترنت)، أو العبث بالسجلات الرقمية، وتغيير مدخلاتها المخزونة في قواعد البيانات[44].

ولأن هذه الهجمات تستطيع إحداث خسائر كبيرة في وقت محدود، أصبحت العديد من الدول تلجأ إليها، إما اثناء قيام النزاعات السياسية والتوتر السياسي بين الدول، او في وقت الحروب بالتزامن مع العمليات العسكرية التقليدية، ومن أبرز أمثلة التجسس الإلكتروني الذي تقوم به دول ضد أخرى، ما ورد في تقرير لجنة التحقيقات التي شكّلها البرلمان الأوروبي في عام 2001 ، والذي انتهت الى اتهام الولايات المتحدة باستخدام شبكة تجسس إلكترونية تحت اسم (Echelon network) والتي تأسست أثناء الحرب، الباردة للتجسس، وسرقة المعلومات الصناعية الخاصة بالصناعات الأوروبية[45].

وتجدر الإشارة إلى أن الدول ليست هي الهدف الوحيد لمثل هذه الهجمات، وانما أيضا الشركات سواء أكانت التجارية أم الخدمية، والمنظمات غير الحكومية، التي باتت عرضة هي الأخرى للعديد من عمليات التجسس الإلكتروني.

2)حرب المعلومات بين الشركات والمؤسسات:

ويدور هذا المستوى ضمن إطار المنافسة بين الشركات والمؤسسات، قوامها استباق كل شيء لتعطيل المنافس، وتهديد أسواقه، بحيث تقوم شركة معينة باختراق النظام المعلوماتي لمنافستها، وسرقة نتائج أبحاثها وتفاصيلها، وتدمير البيانات الخاصة بها، واستبدالها ببيانات أخرى غير صحيحة(46).

3)حرب المعلومات العالمية (الحرب السيبرانية):

تشير الحرب الإلكترونية، أو الحرب السيبرانية، إلى تلك الحرب التي تتم إدارتها في مجال الفضاء الإلكتروني، والتي يتم فيها استخدام الآليات والأسلحة الإلكترونية في الهجوم، ويكون هذا الهجوم موجه بالأساس إلى أجهزة الحاسب الآلي، أو الشبكات الإلكترونية الخاصة بالعدو، أو الأنظمة الإلكترونية التي تدير الدولة، وما تحتوي عليه من معلومات، بهدف عرقلة الخصم عن استخدام هذه الأنظمة، والأجهزة، والشبكات، أو تدميرها بالكامل(47).

وهذا المستوى يمثل الحروب التي تحصل بين بعض الدول، أو الذي قد تشنه القوى الاقتصادية العالمية على بلدان بعينها، بغية سرقة أسرار الخصوم أو الأعداء، وتوجيه تلك المعلومات توجيها مضادا لمصالحهم، حيث إن الدولة التي تمتلك هذه التكنولوجيا تحظى بالتفوق في ميدان المعركة، من خلال استخبارات نوعية وشاملة، وقدرة هجومية دقيقة وخاطفة، وقدرة على الدفاع عن بنيتها التحتية الحيوية، إلى جانب قدرات عالية على السيطرة والتحكم وما يتبع ذلك، إلا أن التطور في مجال تكنولوجيا المعلومات، وعلى وجه الخصوص الحواسيب، ووسائل الاتصال، والشبكات الإلكترونية، جعل من الممكن القيام باستهداف الخصم فردا أو دولة أو مؤسسة، بأساليب جديدة تلائم طبيعة ذلك التطور(48).

وبشكل عام يمكن تحديد ثلاثة مستويات رئيسة للحرب السيبرانية أو الهجمات السيبرانية على النحو الاتي:

-**المستوى الأول**:- ويتمثل في تلك العمليات المصاحبة للحروب التقليدية، لتحقيق التفوق المعرفي، كمهاجمة نظام الدفاع الجوي، والذي يؤدي إلى حدوث خسائر إستراتيجية واسعة النطاق نتيجة لأهمية الدفاع الجوي بالنسبة للدول.

-**المستوى الثاني**:- ويتمثل في الحرب الإلكترونية المحدودة، والتي تتعرض فيها البنية التحتية، والأهداف المدنية للهجمات السيبرانية.

-**المستوى الثالث**-: ويتمثل في الحرب الإلكترونية غير المحدودة، والتي يسعى من خلالها القائم بالهجوم إلى تعظيم الآثار المدمرة للبنية التحتية، حيث يؤثر سلبا في البناء الاجتماعي للدولة، كمهاجمة أسواق رأس المال، وخدمات الطوارئ، والأنظمة الإلكترونية الخاصة بمولدات الطاقة، وغيرها من الأهداف التي يترتب عليها آثار تدميرية واسعة النطاق، ويكون الهدف من هذا النوع من الحروب، هو توسيع نطاق الخسائر المادية قدر الإمكان(49).

وعليه، فإن الهجمات السيبرانية تستهدف معلومات أو نظم معلومات محددة عند الطرف المراد مهاجمته، وذلك لزيادة قيمة تلك المعلومات أو نظمها بالنسبة للمهاجم، أو تقليل قيمتها بالنسبة للمدافع، أو بالاثنين معا، نظرا لأن قيمة المعلومات ونظمها هو المقياس لمقدار استحواذ المهاجم أو المدافع للمعلومات ونظمها، على أن الهدف الذي يسعى المهاجم في حربه لتحقيقه قد يتشكّل ضمن أهداف مالية، كأن يقوم بسرقة وبيع سجلات لحسابات مصرفية، وقد تكون تلك الحرب لأهداف سياسية، أو عسكرية، أو حتى لمجرد الإثارة واظهار القدرات، كما في حالة قراصنة المعلومات(50).

اما من ناحية الوسائل الخاصة بالهجمات السيبرانية، او الأسلحة الإلكترونية، والتي تشير إلى تلك الأدوات التي يتم استخدامها للتهديد بإحداث ضرر مادي أو وظيفي للأجهزة أو النظم والهياكل الإلكترونية، وتختلف هذه الأسلحة والأدوات من حيث درجة خطورتها وتعقيدها، وتتراوح ما بين أسلحة بسيطة قادرة على إحداث ضرر خارجي بالنظام الإلكتروني دون اختراقه، وأخرى معقدة يمكن من خلالها اختراق النظام، واختراق النظم، واحداث أضرار بالغة به قد تصل إلى تدميره كليا، أو توقفه عن العمل كليا(51).

وفيما يلي سنتعرض لأبرز الوسائل التي تعد من قبيل الاسلحة فيما يعرف بالحرب السيبرانية، والتي تُعدّ الأكثر استخداما على الساحة الدولية في وقتنا الحاضر، ومنها:

1-(Logic Bombs) برامج القنابل المنطقية

وهي عبارة عن برنامج ينفذ في لحظة محددة، أو في فترة زمنية منتظمة، يتم وضعه في شبكة معلوماتية بهدف تحديد ظروف أو حالة مضمون النظام، بغية تسهيل تنفيذ العمل غير المشروع، كإدراج تعليمات في نظام التشغيل للبحث عن عمل معين يكون محلا للاعتداء، كأن تسعى قنبلة منطقية إلى البحث عن حرف (A)

في أي سجل يتضمن أمرا بالدفع، وعندما تكتشفه، تحرك متتالية منطقية تعمل على إزالة هذا الحرف من السجل[52].

2-(Worm Software) برامج الدودة

هي مجموعة برامج مصممة لاستغلال أية فجوات في نظم تشغيل الحاسب الآلي، بهدف الانتقال من حاسب إلى آخر، مغطية شبكة بأكملها، والغاية من وراء ذلك التسبب بآثار تخريبية للملفات، والبرامج، ونظم التشغيل، وبروتوكولات الاتصال[53].

3-(Programs Virus) فيروسات الحاسب الآلي

تعد هذه الوسيلة من أكثر وسائل الهجمات السيبرانية انتشارا، وهي بمثابة مجموعة من التعليمات المركزة، تنتج لنفسها نسخا مطابقة تلحق من تلقاء ذاتها ببرامج التطبيقات، ومكونات النظام المنفذ، لتقوم في مرحلة محمية بالتحكم في أداء النظام الذي أصابته. وقد عرّفه المركز القومي للحاسب الآلي في الولايات المتحدة الأمريكية بأنه: "برنامج مهاجم يصيب أنظمة الحاسبات، بأسلوب يماثل إلى حد كبير أسلوب الفيروسات الحيوية التي تصيب الإنسان، حيث يقوم هذا البرنامج بالتجول في الحاسب الآلي باحثا عن برنامج غير مصاب، وعندما يجد أحدها ينتج نسخة من نفسه لتدخل فيه، حيث يقوم البرنامج المصاب فيما بعد بتنفيذ أوامر الفيروس، ومن أهم خصائصه قدرته الفائقة على الاختفاء، والانتشار، والاختراق، وقدرته على تدمير نظام الحاسب الآلي بأكمله[54].

4-(Denial of Service Dos) هجمات قطع الخدمة

وهي عبارة عن هجمات إلكترونية تتم بإغراق المواقع بسيل من البيانات غير اللازمة، التي يجري إرسالها ببرامج متخصصة تعمل على نشرها، فتؤدي إلى بطء في الخدمات أو ازدحام في المرور على هذه المواقع، فيصعب بالتّالي وصول المستخدمين إليها.

5-الهجوم الإلكتروني

كالتشويش، والخداع الإلكتروني، والصواريخ المضادة للإشعاع الكهرومغناطيسي، والقيام بالتجسس على الهدف لسرقة معلومات سرية، بغض النظر عن الأهداف، او قد تكون اقتصاديّة كالتجارة بين الشركات، أو إستراتيجية أو عسكرية بين دول معينة، ومن تلك العمليات أيضا التعدي على الملكية الفكرية، وقرصنة المعلومات ،كسرقة البرامج الحاسوبية، وتوزيع مواد مكتوبة أو مصورة بدون إذن المالك الشرعي، خاصة وأن وجود شبكة الإنترنت قد أدى إلى توسيع انتشار مثل تلك العمليات، لسهولة النشر والتوزيع على هذه الشبكة[55].

الخاتمة Conclusion

أفرزت مسألة الهجمات السيبرانية مجموعة من الأسئلة القانونية المعقدة في العلاقات بين الدول والتي عجزت قواعد القانون الدولي في الاجابة عليها حتى هذه اللحظة، اذ رغم شيوع استخدامها على نطاق واسع في الاونة الاخيرة الا انها حتى الحظة لا تزال على درجة عالية من الغموض، لذا سعت هذه الدراسة لفهم معالم الإجابات أو على الأقل تحديد مواطن الغموض بهذا الصدد.

فقد توصل البحث الي اجابات عن بعض الأسئلة والتي منها فيما اذا كانت الهجمات السيبرانية تصل الى حد استخدام القوة، واذا كان الأمر كذلك ماذا يمكن للدولة المعتدى عليها استخدامه من أجل ممارسة حقها في الدفاع عن النفس. مع الوضع في الاعتبار أن آثار الهجمات السيبرانية على البنى التحتية الحيوية مثل محطات الكهرباء والماء هي ذات الآثار الناجمة عن أسلحة الدمار الشامل، فكلما كانت الدولة أكثر تقدماً من الناحية التكنولوجية تكون أكثر عرضة للتهديدات السيبرانية.

وعلى هذا الأساس، يمكن التوصل إلى بعض الاستنتاجات والتوصيات على النحو الأتي:

اولا/ الاستنتاجات:

1-ان الهجوم السيبراني يعد استخداماً للقوة وفقا للرأي الغالب في الفقه الدولي المعاصر، نتيجة ما يخلفه من اثار مقارنةً مع الهجوم المسلح، وكلاهما يحقق ذات النتيجة ويمكن ان تكون نتائج الهجوم السيبراني أكثر تدميراً وخطورة، لذا فهو يرتقي الى مستوى الهجوم التقليدي، كما ان المادة (4/2) من ميثاق الامم المتحدة جاءت مرنه بالشكل الكافي لاستيعاب الهجوم السيبراني باعتباره صورة مستحدثة من صور القوة نتيجة اثاره المتشابهة مع ما ينتج عن استخدام القوة العسكرية التقليدية.

2-يعد الدفاع الشرعي ضد الهجمات السيبرانية استثناءً من قاعدة عدم اللجوء إلى القوة لأنه يهدف إلى الوقاية وليس الانتقام من المعتدي، إذ يعد سبباً للإباحة في القانون الدولي بشرط أن يسبقه هجوم سيبراني غير مشروع حال على أحد الحقوق الجوهرية التي يحميها القانون.

3-ان الدولة المعتدى عليها يكون لها الحق في استخدام القوة في الدفاع عن النفس وفقاً للمادة (51) من ميثاق الامم المتحدة، بشرط ان يكون الرد على الهجوم السيبراني ضرورياً لكي يكون الرد قانونياً ينطبق عليه صفة الدفاع الشرعي، كما يجب ان يستوفي رد الفعل في الدفاع عن النفس ضد الهجمات السيبرانية التي ترتقي

الى مستوى الهجوم المسلح بمتطلبات الضرورة والتناسب التي نصت عليها اتفاقية جنيف في الملحق الإضافي.

4-أن تطبيق مبدأ التمييز بين المقاتلين وغير المقاتلين على الهجمات السيبرانية للأغراض العسكرية سيما في حالة الدفاع والردع، هي مسألة في غاية التعقيد بالقدر الذي يمكن تصوره أن يكون المهاجم في اغلب الاحيان بعيداً عن المكان المستهدف من الهجوم والتي قد تصل احياناً لمسافة تتجاوز الالاف الكيلومترات.

ثانيا// التوصيات:

1-ضرورة ابرام اتفاقيات دولية تعمل على تقييد استخدام تكنلوجيا المعلومات على شكل هجمات سيبرانية، إذا كان من العسير برمجتها وفقاً للتطبيق الامثل لقواعد القانون الدولي، وفي ضوء الموازنة بين المصالح القومية والدفاع عن النفس، وبين الآثار غير الإنسانية التي قد تتسبب بها تلك الهجمات.

2-ضرورة انشاء لجنة دولية لإدارة الازمات السيبرانية تضطلع بمهام دراسة الهجمات الالكترونية، والعمل على اجراء التحقيقات الدولية المستقلة، ويكون لها صلاحية توجيه المسؤولية الدولية عن هذه الهجمات.

3- التأكيد على ضرورة مراعاة شرط التناسب والالتزام به في ممارسة حق الدفاع الشرعي ضد الهجمات السيبرانية، اذ ان تخلف هذا الشرط يؤدي الى التجاوز في الدفاع الشرعي وبالتالي قيام المسؤولية الدولية عن ارتكاب جريمة عدوان.

4- يعد إخفاء هوية الفاعل في الفضاء السيبراني احد ابرز التحديات التي تصعب من عملية الكشف عن الجاني وتعقبه ومن ثم تقديمه للعدالة، نظرا لما تنطوي عليه الاساليب التقنية المستخدمة لشن الهجمات السيبرانية من خصائص تمكنها من اخفاء هوية الجاني، لذا نرى بضرورة وضع استراتيجية دولية لأنشاء نظام رقمي للحد من هذه الظاهرة، بجانب تحديث أنظمة الحماية لتتضمن متطلبات الأمن الشيباني.

الهوامش Endnotes

1)Michael Schmitt. "Wired Warfare: Computer Network Attack and Jus in Bello", IRRC 84, no. 846 June 11(2002): 365-400, online e-article, at https://www.icrc.org/eng/assets/files/other/365_400_schmitt.pdf.

2)مايكل شميث، الحرب بواسطة شبكات الاتصال:الهجوم على شبكات الكمبيوتر(الحاسوب) والقانون في الحرب، المجلة الدولية للصليب الاحمر،2002، ص124.

حمدون توريه، الاستجابة الدولية للحرب السيبرانية، البحث عن الامن السيبراني،الاتحاد الدولي للاتصالات، 2011 ص338)

4)جون ماري هنكرتس، لويز دوزوالد–بك، القانون الدولي الإنساني العرفي، ج1، مطبعة برنت رايت للإعلان والدعاية، القاهرة ، ٢٠٠٧، ص82.

5)ايهاب خليفة، الميدان الخامس، الفضاء السيبراني في العقيدة العسكرية لحلف الناتو،وحدة التطورات التكنلوجية مركز المستقل للأبحاث والدراسات المتقدمة، ابو ظبي،2020، ص103.

6)Kugler Richard, "From Cyber Space to Cyber Power: Defining the Problems", Chapter2 in Cyber Power and National Security, edited by Franklin D. Krammer, Stuart Starr and Larry K. Wentz. National Defense University Series. Washington,DC: Center for Technology and National Security Policy, 2009, p.329.

هشام بشير، المدخل للقانون الدولي الانساني، ط9، المركز القومي للإصدارات القومية، القاهرة، 2012،ص.789)

8)لمزيد من المعلومات راجع الملحق (البروتوكول الاول) الإضافي لاتفاقيات جنيف، 1977، اللجنة الدولية للصليب الأحمر، منشور على الموقع:

.https://www.icrc.org/ara/resources/documents/misc/5ntccf.htm.

9)Karatzogianni Athina, Karatzogianni, Athina, ed. "Cyber-Conflict and Global Politics Contemporary Security Studies". London: Routledge, 2008 p.294.

10)جانكارلو واخرون، النزاع السيبراني والاستقرار الجيوسيراني،الاتحاد الدولي للاتصالات وبرنامج الامن السيبراني العالمي،2011، ص73.

11)Libicki Martin, "Conquest in Cyberspace: National Security and Information Warfare" New York: Cambridge University Press, 2007, p.281.

12) مفيد شهاب، دراسات في القانون الدولي الإنساني، دار المستقبل العربي، القاهرة، 2000، ص.34 – 35.

13) هشام بشير، المدخل للقانون الدولي الانساني،ط9، المركز القومي للإصدارات القومية،القاهرة،2012، ص94.

14)ربيع محمد يحيى، اسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الاوسط، دراسة حول استعدادات ومحاور عمل الدولة العبرية في عصر الانترنت،2002م-2013م، ص87.

15)Nye Joseph S, The Future of Power. New York: PublicAffairs, 2011, p.238

16)احمد فتحي سرور، القانون الدولي الإنساني، دليل للتطبيق على الصعيد الوطني، دار المستقبل العربي، القاهرة، 2003، ص320 – 321.

سلوان جابر هاشم، حالة الضرورة العسكرية في القانون الدولي الانساني، ط9، المؤسسة الحديثة للكتاب، بيروت، 2013، ص17105)

18)Dimitrios Delibasis, "State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century", Peace Conflict and Development, no8, 2006, p.12.

19)Aleksandar KLAIC, "A Method for the Development of Cyber Security Strategies", Information & Security: An International Journal, I&S Volume 34, (2015), p.428.

20)نسرين الشحات، الابعاد العسكرية للقوة السيبرانية على الامن القومي للدول دراسة حالة"اسرائيل منذ عام 2010م"،المركز الديمقراطي العربي،29 ابريل2016م، ص.109

21) قام مايك ماكونيل المدير السابق للمخابرات الوطنية في الولايات المتحدة عام 2009 بتصنيف الأسلحة السيبرانية على أنها من أسلحة الدمار الشامل (أو أنها يمكن أن تكون كذلك)، ينظر:

22)Oona Hathway,"The Law of cyber-Attack", Yale Law school Legal Scholarship Repository,val64,2012. p.873.

23)Peter Margulies, "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility", Melbourne Journal of International Law, Vol.14.2013, p.1.

(24) تم ذكر مصطلح السيطرة الكاملة والسيطرة الفاعلة في قرار محكمة العدل الدولية في قضية الانشطة العسكرية وغير العسكرية (نيكاراغوا ضد الولايات المتحدة الأمريكية) وذلك في عام ١٩٨٦، فمبدأ السيطرة الكاملة يشير إلى سيطرة الدولة على مجموعات مسلحة إما تابعة لها رسميا وبعبارة أخرى ضمن تشكيلاتها العسكرية الرسمية أو أنها تتواجد على إقليمها بشكل معترف منها وبرضاها التام.

أما مصطلح السيطرة الفاعلة فيشير إلى سيطرة الدولة على مجموعات مسلحة لا تنتمي لها رسميا ولا تتواجد على إقليمها ومع ذلك تتلقى دعما ماديا أو لوجستيا كإمدادات الأسلحة أو التدريب، للمزيد مراجعة ما جاء في قضية (نيكاراغوا ضد الولايات المتحدة) لعام ١٩٨٦، نقلا عن نبيل احمد حلمي، مصدر سابق، ص141..

25)Rwx HUGES, "Atreaty for Cyberspace", International Affairs journal, Vol86, No2, 2010, p.533.

26)Emily Haslam, "Information Warfare: Technological Changes and International Law", Journal of Conflict and Security Law, Vol5, 2000, p.157.

27)Micheal Schmitt,"Bellum Americium: The law of armed conflict into the next millennium", Newport: Naval War College, 1998, P.408.

28)Matthew Evangelista, "Cooperation theory and Disarmament Negotiations in the 1950s", World political Journal, Vol.42, No.4, 1990, P.515.

29)Matthew Waxman, "Cyber–Attack and the Use of Force: Back to the Future of Article 2 (4)", The Yale Journal of International Law, Vol36, No.421, 2011, p.431.

30) فائزة يونل الباشا، الجريمة المنظمة في ظل الاتفاقيات الدولية والقوانين الوطنية، دار النهضة العربية، ط1،القاهرة،2001، ص98.

31) عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، 2007، ص32.

32)طالب حسن موسى، عمر محمود عمر،الانترنت قانونا، مجلة الشريعة والقانون، جامعة الامارات العربية المتحدة،العدد67، 2016، ص352.
33) عبد الكريم علوان، الوسيط في القانون الدولي العام،دار الثقافة، عمان، 2006، ص320.
34) نبيل أحمد حلمي،القانون الدولي وفقا لقواعد القانون الدولي العام، دار النهضة العربية، القاهرة، 1999، ص143.
35) طلال ياسين العيسى، عدي محمد عناب، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الانسانية، المجلد 19، العدد 1، 2019، ص89.
36) نوران شفيق، أثر التهديدات الإلكترونية على العلاقات الدولية: دراسة في أبعاد الأمن الإلكتروني، المكتب العربي للمعارف، القاهرة، 2016، ص128
37) Donnb Parker, "fighting computer crime" ,Charles Scribner Son, New York, 1983, p.273.
38) محمود عبابنة، محمد معمر الرازقي، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للتوزيع والشر، عمان، 2005، ص381.
39) Clay Wilson, "Cyber power and National Security", Potomac Book, 2009, p.131.
40) محمود الألوسي، جرائم الحاسب الآلي ورقة عمل مقدمة من الأمانة العامة لمجلس التعاون الخليجي لاجتماع اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجرائم الإلكترونية "الإنترنت" الأول والذي أنعقد بمقر الأمانة العامة بالرياض، 2006، ص.23
41) إيهاب خليفة، القوة الإلكترونية وأبعاد التحول في خصائص القوة، مكتبة الإسكندرية للطباعة والنشر، مصر، 2014، ص173.
42) Clay Wilson, Cyber Power and National Security", Potomac Book,2009, p.143.
43) محمود عبابنة، محمد معمر الرازقي، جرائم الحاسوب وابعادها الدولية، دار الثقافة للتوزيع والنشر، عمان، 2005، ص384.

المصادر Reference

اولا/ الكتب باللغة العربية:

i. احمد فتحي سرور، القانون الدولي الإنساني، دليل للتطبيق على الصعيد الوطني، دار المستقبل العربي، القاهرة.2003
ii. ايهاب خليفة، القوة الالكترونية، كيف يمكن ان تدير الدول شؤونها في عصر الانترنت، دار العربي للنشر، القاهرة. ط1، 2017.
iii. إيهاب خليفة، الميدان الخامس، الفضاء السيبراني في العقيدة العسكرية لحلف الناتو، وحدة التطورات التكنولوجية مركز المستقبل للأبحاث والدراسات المتقدمة، أبو ظبي، 2020.
iv. إيهاب خليفة، القوة الإلكترونية وأبعاد التحول في خصائص القوة، مكتبة الإسكندرية للطباعة والنشر، مصر، 2014.
v. جانكارلو واخرون، النزاع السيبراني والاستقرار الجيوسيبراني، الاتحاد الدولي للاتصالات وبرنامج الأمن السيبراني العالمي، 2011.
vi. جون ماري هنكرتس، لويز دوزوالد–بك، القانون الدولي الإنساني العرفي، ج1، مطبعة برنت رايت للإعلان والدعاية، القاهرة ، 2007.
vii. سلوان جابر هاشم، حالة الضرورة العسكرية في القانون الدولي الانساني، ط9، المؤسسة الحديثة للكتاب، بيروت 2013.
viii. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، 2007.
ix. عبد الفتاح بيومي، المحكمة الجنائية الدولية، دار الفكر الجامعي، الاسكندرية، 2005.
x. عبد الكريم علوان، الوسيط في القانون الدولي العام، دار الثقافة، عمان، 2006.
xi. فائزة يونل الباشا، الجريمة المنظمة في ظل الاتفاقيات الدولية والقوانين الوطنية، دار النهضة العربية، ط1،القاهرة، 2001.
xii. مايكل شميت، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكومبيوتر (الحاسوب) والقانون في الحرب، المجلة الدولية للصليب الأحمر، 2002.
xiii. مفيد شهاب، دراسات في القانون الدولي الإنساني، دار المستقبل العربي، القاهرة، 2000.
xiv. نبيل أحمد حلمي، القانون الدولي وفقًا لقواعد القانون الدولي العام، دار النهضة العربية، القاهرة، 1999.
xv. هشام بشير، المدخل للقانون الدولي الانساني، ط9، المركز القومي للإصدارات القومية، القاهرة، 2012.
xvi. نوران شفيق، أثر التهديدات الإلكترونية على العلاقات الدولية: دراسة في أبعاد الأمن الإلكتروني، المكتب العربي للمعارف القاهرة، 2016.

ثانيا/ الرسائل والاطاريح الجامعية

أ_ الرسائل:

i. محمود الألوسي، جرائم الحاسب الآلي ورقة عمل مقدمة من الأمانة العامة لمجلس التعاون الخليجي لاجتماع اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجرائم الإلكترونية "الإنترنت" الأول والذي أنعقد بمقر الأمانة العامة بالرياض، 2006.
ii. محمود عبابنة، محمد معمر الرازقي، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للتوزيع والشر، عمان، 2005.

ثالثا// البحوث القانونية:

i. طلال ياسين العيسى، عدي محمد عناب، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الانسانية، المجلد 19، العدد1، 2019.

ii. طالب حسن موس عمر محمود عمر، الإنترنت قانونا، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة، العدد67، 2016.

iii. دليل سان ريمو بشأن القانون الدولي المطبق في النزاعات المسلحة في البحار، المجلة الدولية للصليب الأحمر، العدد309.1995.

رابعا: والاتفاقيات الدولية والإعلانات والمواثيق:

1. البروتوكول الاضافي الأول الملحق باتفاقيات جنيف لسنة 1977.

المصادر الاجنبية:

I. Aleksandar KLAIC, "A Method for the Development of Cyber Security Strategies", Information & Security: An International Journal, I&S Volume 34, (2015).

II. Clay Wilson, "Cyber power and National Security", Potomac Book, 2009,

III. Dimitrios Delibasis, "State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century", Peace Conflict and Development, no8, 2006.

IV. Donnb Parker, "fighting computer crime" ,Charles Scribner Son, New York, 1983.

V. Emily Haslam, "Information Warfare: Technological Changes and International Law", Journal of Conflict and Security Law, Vol5, 2000, Franklin Kramer et al, "Cyber power and National Security", National Defense University Press, 2009.

VI. Joseph S.Nye JR, "Cyber Power", Harvard Kennedy School, 201, .

VII. Kugler Richard, "From Cyber Space to Cyber Power: Defining the Problems", Chapter2 in Cyber Power and National Security, edited by Franklin D. Krammer, Stuart Starr and Larry K. Wentz. National Defense University Series. Washington,DC: Center for Technology and National Security Policy, 2009.

VIII. Libicki Martin, "Conquest in Cyberspace: National Security and Information Warfare" New York: Cambridge University Press, 2007,

IX. Matthew Evangelista, "Cooperation theory and Disarmament Negotiations in the 1950s", World political Journal, Vol.42, No.4, 1990,

X. Matthew Waxman, "Cyber–Attack and the Use of Force: Back to the Future of Article 2 (4)", The Yale Journal of International Law, Vol36, No.421, 2011,.

XI. Michael Schmitt. "Wired Warfare: Computer Network Attack and Jus in Bello", IRRC 84, no. 846 June 11(2002): 365-400, online e-article, at:

XII. Peter Margulies, "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility", Melbourne Journal of International Law, Vol.14.2013.