المسؤولية الدولية عن الاضرار التي تحدثها الهجمات الإلكترونية

International responsibility for damage caused by cyber attacks

أ.م.د.لمى عبد الباقي محمود
كلية القانون-جامعة بغداد
lumam629@gmail.com

الطالبة: إسراء نادر كيطان
كلية القانون-جامعة بغداد
Esraamader743@gmail.com lumam629@gmail.com

الملخص

يسلط البحث الضوء على موضوع جديد من مواضيع القانون الدولي واهمها، والذي لاتزال تدور حوله علامات استفهام واختلاف في اغلب جوانبه، وخاصةً فيما يتعلق بالمسؤولية الدولية عن الاضرار التي تحدثها الهجمات الإلكترونية في الفضاء الافتراضي، فالاخير هو المجال الخامس الذي ظهر إلى جانب المجالات الاخرى(البرية، البحرية، الجوية والفضاء الخارجي) واصبح فضلاً عن كونه فضاء تعتمد عليه الدول في اداء وظائفها وعلاقاتها الدولية هو ساحة جديدة للحرب ومصدر خطر على امن الدول، إذ ازداد في ظله الانكشاف الامني لاسرار الدول بسبب التجسس والقرصنة وازدادت الهجمات على البنى التحتية للدول وان سكوت الدول في بعض الاحيان وصعوبة معرفة المهاجم أو نسبة الفعل لدولة أو جهة معينة ادى إلى تفاقم المشكلة التي قد تتحول من مجرد هجوم إلى حرب على ارض الواقع، لذلك يجب تخطي مشكلة اخفاء هوية المهاجم و تفعيل نظام المسؤولية الدولية في هذا الفضاء لانها الاساس للنظام القانوني الدولي كما يمكن من خلال تفعيلها مواجهة الاخطار والحفاظ على الامن السيبراني الذي اصبح مسالة مهمة في وقتنا الحاضر.

الكلمات المفتاحية: الفضاء الافتراضي، الهجمات الإلكترونية، المسؤولية الدولية، البنى التحتية، التكنولوجيا الرقمية.

Summary

The research sheds light on a new topic of international law, the most important of which is, around which there are still question marks and differences in most of its aspects, especially with regard to international liability for damage caused by cyber attacks in the virtual space, the last is the fifth area that appeared alongside other area (Land, sea, air and outer space) and in addition to being a space on which states depend in the performance of their functions and international relations, it is a new arena for war and a source of danger to the security of states, As the security exposure to the secrets of states increased due to espionage and piracy, and the attacks on the infrastructure of countries increased, and the silence of states at times and the difficulty in knowing the attacker or the attributing the act to a specific country or party led to an exacerbation of the problem that may turn from a mere attack to a war on the ground, Therefore, the problem of concealing the identity of the attacker must be overcome and the international liability system must be activated in this space because it is the basis of the international legal system. Through its activation, it is possible to confront the dangers and preserve cyber security, which has become an important issue in our time.

Key words: cyberspace, cyber attacks, international liability , infrastructure**,** digital technology**.**

المقدمة

(Introduction)

يشهد المجتمع البشري تطوراً مطرداً في مجال التكنولوجيا الرقمية وتطبيقاتها بشكل خاص، مما جعل حياة الانسان والدول ومصالحها اكثر ارتباطاً بالفضاء الافتراضي والاجهزة الإلكترونية، إذ اثرت تلك التكنولوجيا على الانظمة السياسية والعلاقات الدولية للدول وامنها القومي وسيادتها ومصالحها، فهو يسهل عمل الدول وقيامها بمهامها، إلا ان الدول تواجه مخاطر كبيرة في هذا الفضاء بسبب ماتتعرض له من هجمات تهدد سيادتها وتعرض مصالحها للخطر على مختلف المستويات، فكان لابد من مواجهة تلك التهديدات لان استمرارها سيؤدي إلى تهديد السلم والامن الدوليين، لذلك يجب التركيز على نظام المسؤولية الدولية لمواجهة الدول التي تشن تلك الهجمات، إذ تعد المسؤولية الدولية العمود الفقري لاي نظام قانوني وعلى وجه الخصوص في النظام القانوني الدولي.

لذلك فان مشكلة بحثنا تتجسد في بيان ماهي المسؤولية الدولية عن اضرار الهجمات الإلكترونية؟ والذي يتفرع عنها أمور عدة تدور حولها علأمات الاستفهام بخصوص تلك الهجمات ومنها، ماهو التكييف القانوني لتلك الهجمات؟ وهل هناك مسؤولية دولية في حالة الهجوم السيبراني؟ وماهو اساسها؟ للاجابة عن تلك التساؤلات سوف نقسم هذا البحث إلى مبحثين، نتناول في الأول، التكييف القانوني للهجمات الإلكترونية وفقاً لمبادئ القانون الدولي، أما الثاني فسيكون للمسؤولية الدولية عن اضرار الهجمات الإلكترونية في الفضاء الافتراضي.

وللاجابة عن ماطرح من التساؤلات فقد اتبعنا المنهج الوصفي التحليلي في هذا البحث من خلال بيان مفهوم تلك الهجمات وتحليل مدى انطباق المبادئ العامة في القانون الدولي عليها، فضلاً عن تحليل مدى توفر شروط المسؤولية عليها، لان الموضوع لايزال يثير العديد من التساؤلات لكونه في تطور مستمر إلى جانب العدد القليل من البحوث الاكاديمية والممارسات الدولية المتعلقة به.

واستناداً إلى ماتقدم سنتناول موضوع البحث وفقاً للخطة الآتية:-

المبحث الأول:- التكييف القانوني للهجمات الإلكترونية وفقاً لمبادئ القانون الدولي.

المطلب الأول:- تكييف الهجمات الإلكترونية وفقاً للمبادئ الرئيسة في القانون الدولي العام.

المطلب الثاني:- تكييف الهجمات الإلكترونية وفقاً لمبادئ القانون الدولي الإنساني.

المبحث الثاني:- المسؤولية الدولية عن اضرار الهجمات الإلكترونية في الفضاء الافتراضي.

المطلب الأول:- مدى انطباق شروط المسؤولية التقليدية على الهجمات الإلكترونية.

المطلب الثاني:- مدى انطباق شروط المسؤولية الحديثة على الهجمات الإلكترونية.

المبحث الأول

التكييف القانوني للهجمات الإلكترونية وفقاً لمبادئ القانون الدولي (Legal adaptation of cyber attacks in accordance with principles of international law)

ان الهجمات الإلكترونية تعد أحدى السبل والأساليب المؤثرة الناتجة عن التطور التكنولوجي والتي تتميز بسرعة وسهولة تنفيذها، فمن خلال هذه الهجمات يمكن ان تؤثر الدول ببعضها وذلك عن طريق شل الأنظمة الأقتصادية والأمنية أو العسكرية والبنى التحتية لدولة ما، لذلك سنتنأول في هذا المبحث التكييف القانوني لتلك الهجمات في مطلبين، الأول الهجمات الإلكترونية وفقاً للمبادئ الرئيسة في القانون الدولي العام ، والثاني سيكون للهجمات الإلكترونية وفقاً لمبادئ القانون الدولي الإنساني.

المطلب الأول

تكييف الهجمات الإلكترونية وفقاً للمبادئ الرئيسة في القانون الدولي العام (Adapting cyber attacks according to the basic principles of public international law)

قبل البدء في بيان التكييف القانوني للهجمات السيبرانية يجب ان نعرف ماهو الفضاء الافتراضي وماهي الهجمات الإلكترونية، إذ يقصد بالفضاء الافتراضي استناداً إلى تعريف الاتحاد الدولي للاتصالات بانه(الحيز المادي وغير المادي الذي ينشئ أو يتكون من جزء أو كل العناصر الاتية: وهي الحواسيب أو اجهزة ممكننة وشبكات ومعلومات محوسبة وبرامج ومضامين ومعطيات ومرور ورقابة والذين يستخدمون كل ذلك)[١]، أما الهجمات الإلكترونية فهي (اعمال تقوم بها دولة تحأول من خلالها اختراق اجهزة الكمبيوتر والشبكات التابعة لدولة اخرى، يكون الهدف منها الحاق اضراراً بالغة بتلك لدولة)[٢]، أما تكييفها وفقاً للمبادئ الرئيسة في القانون الدولي والتي نص عليها ميثاق الأمم المتحدة وهي مبدأ السيادة للدول ومبدأ حظر استخدام القوة أو التهديد باستخدامها، وبما ان التطور الحاصل اظهر مجالات جديدة كالسيادة السيبرانية ومايهدد تلك السيادة من هجمات، لذلك هل تعد الهجمات الإلكترونية استخدام للقوة ضد سيادة الدولة؟ ومامدى انطباق هذه المبادئ على الهجمات الإلكترونية؟ وعليه سنتنأول هذين المبدأين وفقاً للأتي:

أولاً:- مبدأ السيادة:- يرجع مفهوم السيادة بشكل عام إلى معاهدة وستفاليا لعام(١٦٤٨) والتي كانت أول من ارسى هذا المبدأ، ويقصد به(ان تقوم الدولة بادراة شؤونها دون تدخل من اي دولة أو دول اخرى)[٣].

هذا وتعد فكرة السيادة والاعتراف بها من المبادئ التي تم الاتفاق عليها في ميثاق الأمم المتحدة، إذ جاء فيه بأن(تقوم الهيئة على مبدأ المسأواة في السيادة بين جميع اعضائها)[٤].

إن المفهوم التقليدي للسيادة لم يعد كما هو، انما طرأ عليه تغييربسبب التطور التكنولوجي وظهور الفضاء الافتراضي، فبرز مايسمى بالسيادة السيبرانية[٥] مما دفع دول العالم لفرض الرقابة الامنية عليها، فهي مفهوم جديد مشتق من مصطلح الامن السيبراني الذي يتعلق بحماية البنى التحتية الرقمية والتقنيات والمحتويات الرقمية والاتصالات وكل مايمكن ان يرتبط بالفضاء السيبراني[٦].

هذا وواجهت السيادة تحدي جديد وهو الهجمات الإلكترونية فان من يقوم بهذه الهجمات عبر شبكات الانترنيت في الفضاء الخامس ينتهك في سبيل ذلك السيادة الوطنية لدولة ما عندما يكون مصدر الهجوم قد وقع ضمن سيادة دولة اخرى، وعلى هذا فأن مفهوم السيادة التقليدي بدء يتقلص بسبب وسائل الاتصال الإلكترونية التي جعلت الحدود الاقليمية تتضاءل شيئاً فشيئاً، ولاضمحلال تلك الحدود في الفضاء الافتراضي ومايتنتج عنها من مخاطر، فقد قامت الدول بتطوير تشريعاتها الوطنية لإستيعاب الجرائم التي تحدث في ذلك الفضاء[٧].

هذا وينطبق مبدأ السيادة الاقليمية على الفضاء السيبراني، ويشمل البنية التحتية الإلكترونية كشبكات الاتصال وتنظيم الحواسيب وقطاعات الطاقة والنقل...الخ، إذ يكون للدولة حق في ان تمارس الرقابة على انشطة تلك البنية التحتية، ولها حق سيادي عليها وممارسة تلك السيادة مقيدة بالمبادئ العرفية أو المقننة في القانون الدولي[٨]، وذهب خبراء حلف الناتو برأي لهم إلى ابعد من ذلك فاكدوا أن على الدول واجب منع استخدام البنى التحتية السيبرانية التي تقع على اقليمها وتخضع لسيطرتها في نشاطات تمس الحقوق السيادية لدول اخرى، وان سيادة الدولة تكون ليست على البنى المشيدة في اراضيها فقط انما حتى على البنى التحتية التي تحت سيطرتها وان كانت على اقليم دولة اخرى[٩].

ومن خلال ماتقدم فان الهجمات الإلكترونية التي تقوم بها دولة ضد دولة اخرى تكون خرقاً لسيادة تلك الدولة، ومن ثم ينطبق مبدأ السيادة في الفضاء السيبراني لكن ليس بالشكل الذي ينطبق فيه بالعالم الواقعي، لان الفضاء الافتراضي لايعرف الحدود، وعلى الرغم من ذلك اقرت السيادة للدولة في هذا الفضاء، لأن آثار الهجمات الإلكترونية قد تكون خطرة .

ثانياً:- مبدأ حظر استخدام القوة والتهديد بأستخدامها:- ورد هذا المبدأ في ميثاق الأمم المتحدة الذي نص على ان(يمتنع اعضاء الهيئة في علاقاتهم الدولية عن التهديد باستخدام القوة أو استخدامها ضد سلامة الاراضي أو الاستقلال السياسي لأي دولة...)[١٠]، ويستكمل الحظر المنصوص في الميثاق بقاعدة اخرى في القانون الدولي العرفي وهي قاعدة عدم التدخل في الشؤون الداخلية للدول، وهذا

ماقررته محكمة العدل الدولية في ان هذه القاعدة متوافقة مع ماجاء في الميثاق[١١]،وعلى الرغم من مالهذا المبدأ من اهمية في حفظ السلم والامن الدوليين، إلا انه يرد عليه استثنائين، الأول هو مأورد في المادة(٣٩) من الميثاق والتي نصت على ان(لمجلس الأمن ان يقرر ما إذا كان قد وقع تهديد للسلم أو إخلال به أو كان ما وقع عملاً من أعمال العدوان، ويقدم في ذلك توصياته أو يقرر ما يجب اتخاذه من التدابير طبقاً لأحكام المادتين ٤١ و٤٢ لحفظ السلم والأمن الدولي أو إعادته إلى نصابه)، والثاني مأورد في المادة(٥١)[١٢] منه التي تتعلق بحق الدفاع الشرعي للدولة في حال تعرضت لأي اعتداء، والتي نصت على انه(ليس 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" وذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدولي، والتدابير التي اتخذها الأعضاء استعمالاً لحق الدفاع عن النفس تبلغ إلى المجلس فوراً، ولا تؤثر تلك التدابير بأي حال فيما للمجلس - بمقتضى سلطته ومسؤولياته المستمرة من أحكام هذا الميثاق - من الحق في أن يتخذ في أي وقت ما يرى ضرورة لاتخاذه من الأعمال لحفظ السلم والأمن الدولي أو إعادته إلى نصابه).

ومن خلال قراءة نصوص المادتين يثور لدينا سؤالين وهما إذا كان نص هذين المادتين يطبق على الهجمات التقليدية واستخدام القوة في المجال الواقعي، هل يمكن ان تطبق ذاتها على الهجمات الإلكترونية في الفضاء الافتراضي؟ وهل يكون للدولة التي تتعرض للهجوم السيبراني حق الدفاع عن نفسها؟

للاجابة عن هذين السؤالين يجب ان نتطرق إلى ثلاث نظريات في خصوص الهجمات الإلكترونية وهي:-

١-**نظرية النهج القائم على الوسيلة:-** تستند هذه النظرية إلى الوسيلة التي تستخدم في الهجوم، إذ تؤكد على ان الهجوم السيبراني وحده لايكون هجوم مسلح ومن ثم لايكون للدولة حق في الدفاع عن نفسها وفقاً للمادة(٥١) من ميثاق الأمم المتحدة سالفة الذكر، لان هذا الهجوم ليس فيه الخصائص الفيزيائية التي ترتبط بالاكراه العسكري، وبتعبير آخر فهو لايحتوي على الطاقة الحركية[١٣] كما في الاسلحة التقليدية، وما يؤيد هذه النظرية هو مأورد في القرار الصادر عن الجمعية العامة للأمم المتحدة، والذي جاء فيه ان العدوان (هو قيام القوات المسلحة لدولة ما بمهاجمة القوات البرية والبحرية والجوية أو الاسطولين البحري والجوي لدولة ما)، كما وعدد في المادة الثالثة منه أعمال العدوان، والتي جاءت على سبيل المثال لا الحصر[١٤]، وعلى الرغم من سهولة تطبيق هذه النظرية إلا انها لاتأخذ بالاعتبار الهجمات الإلكترونية التي قد تسبب اضراراً بالغة.

٢- **نظرية النهج القائم على الأهداف:-** والتي جاء فيها، إذا استهدف الهجوم السيبراني نظأما مهماً لدولة ما يمكن ان يصنف بأنه هجوم مسلح ويكون لها حق الدفاع عن النفس، ومثال على ذلك استهداف البنى التحتية لدولة معينة فيكون الهجوم السيبراني على تلك البنى التحتية المهمة للدولة هجوماً مسلحاً وفقاً لهذه النظرية، لكن هذه النظرية انتقدت لأنها تجاهلت مفهوم البنى التحتية الحرجة وجسامة الهجوم السيبراني و آثاره[١٥].

٣-**نظرية النهج القائم على الآثار:-** تعد هذه النظرية وسط بين النظريتين السابقتين وهي تقوم على خطورة آثار الهجوم، فوفقاً لها يعد الهجوم الالكتروني مسلحاً إذا كانت آثاره خطيرة، مثال ذلك الهجوم ضد نظام مراقبة الملاحة الجوية والتسبب بحوادث للطائرات، فيعد هذا الهجوم مسلحاً لأنه من المتوقع ان يسبب خسائر في الأموال والارواح، ومن ناحية اخرى فالهجوم الالكتروني على شبكة الويب أو مجرد اختراق لنظام الكمبيوتر بشكل عام فهذا لايعد بمثابة هجوم مسلح مالم ينتج عنه اضراراً مادية وجسدية، ومن ثم يمكن القول ان هذا الاتجاه هو الاكثر قبولاً من الاتجاهات التي ذكرناها، وعلى الرغم من ذلك فأن هذه النظرية لاتنطبق إلا على مجموعة صغيرة من الهجمات الإلكترونية الضارة اي التي يكون لها آثاراً تشبه آثار الأسلحة التقليدية من ناحية الاضرار[١٦].

من ماتقدم يمكننا ان نبين، ان الهجوم السيبراني متى ماكانت آثاره ضارة يكون بمثابة هجوم مسلح واستخدام للقوة ضد دولة ما، فيكون للاخيرة حق الدفاع عن نفسها، فيطبق الاستثناء الوارد في الميثاق وهو حق الدفاع الشرعي التي نصت عليه المادة(٥١)، وهذا بدلالة القاعدة(١٣) من دليل تالين بقولها(يجوز للدولة التي تكون هدفاً للعمليات السيبرانية التي تصل لمستوى الهجوم المسلح ان تمارس حقها الطبيعي في الدفاع عن النفس..)[١٧].

أما بخصوص المادة (٢) الفقرة(٤) من الميثاق سالفة الذكر، التي حظرت استخدام القوة أو التهديد باستخدامها، فأن الهجمات الإلكترونية إذا لم تصل إلى حد النزاع المسلح ولم تكن آثارها ضارة هنا لايمكن ان تعد استخدأما للقوة وفقاً لمفهوم هذه الفقرة، انما يمكن ان تعد شكلاً اخر يشبه اعمال الضغط السياسي والاقتصادي، ومن ثم فأن الخرق في هذه الحالة يكون لقاعدة(عدم التدخل) الواردة في القانون العرفي[١٨]، وهذا يعني ان ميثاق الأمم المتحدة بشكل عام والمبدأين المذكورين بشكل خاص يطبقان على الهجمات الإلكترونية، وان الاخيرة تشكل تهديداً لهذه المبادئ الرئيسة في القانون الدولي، وهذا الرأي بدلالة ماجاء بتقرير فريق الخبراء الحكوميين بقولهم ان ميثاق الأمم المتحدة قابل للتطبيق وضروري للحفاظ على سلم واستقرار بيئة تكنولوجيا المعلومات والاتصالات وان مبدأ السيادة ينطبق على تصرفات الدول في المجال

السيبراني[١٩]،أما من ناحية تطبيقها على تلك الهجمات واقعيا فمن وجهة نظرنا يكون بشكل يختلف عن تلك المطبقة على الهجمات التقليدية.

المطلب الثاني

تكييف الهجمات الإلكترونية وفقاً لمبادئ القانون الدولي الإنساني (Adapting cyber attacks according to the principles of international humanitarian law)

يطبق القانون الدولي الإنساني في المنازعات الدولية من أجل حماية المدنيين والأعيان المدنية من آثار النزاعات المسلحة التقليدية، لكن بعد ان ظهر الفضاء الافتراضي ووجد مايسمى بالهجمات الإلكترونية التي تقوم بها دولة ضد دولة اخرى، يثور في هذا الإطار سؤالين، الأول هل تطبق مبادئ القانون الدولي الإنساني على الهجمات الإلكترونية كما تطبق على الهجمات التقليدية؟ والثاني، متى يطبق القانون الدولي الإنساني على الهجمات الإلكترونية؟ والإجابة عن هذه الاسئلة سنبينها وفقاً للأتي:-

أولاً:- مدى انطباق مبادئ القانون الدولي الإنساني على الهجمات الإلكترونية:- من أهم مبادئ هذا القانون هي:-

١-**مبدأ الضرورة العسكرية:-** يعد هذا المبدأ من المواضيع المهمة في القانون الدولي الإنساني، إذ يقوم أساساً على الموازنة بين متطلبات الضرورة العسكرية والإعتبارات الإنسانية، فتلك الضرورة تتطلب إستخدأما للقوة العسكرية المتاحة لتحقيق تفوق أو ميزة عسكرية، بينما الإعتبارات الإنسانية تقتضي تقييد إستخدام هذه القوة لتحقيق الميزة العسكرية المبتغاة بأقل الخسائر في الارواح والاعيان وبوسائل وأساليب قتالية إنسانية، ولإهمية هذا المبدأ يمكن تعريفه بأنه(تلك التدابير التي لاغنى عنها لتحقيق غايات الحرب، على ان تكون هذه التدابير مشروعة وفقاً لاعراف وقوانين الحرب، وبتعبير آخر ان الضرورة العسكرية هي الملإذ الأخير الذي يبرر كل التدابير التي لاغنى عنها لضمان التقدم على العدو، بشرط ان لايتعارض مع قانون النزاعات المسلحة)[٢٠].

هذا وقد تم النص على هذا المبدأ في صكوك دولية عدة، ومنها إعلان سان بترسبورغ في عام(١٨٦٨)، بالقول(ضرورات الحرب يجب ان تخضع للمتطلبات الإنسانية)،كذلك ورد في اتفاقية لاهاي بشأن الحرب البرية لعام(١٩٠٧) التي نصت على ان(يمنع...تدمير ممتلكات العدو أو حجزها،إلا إذا كانت ضرورات الحرب تقتضي هذا التدمير)[٢١]،والبرتوكول الاضافي الأول لعام(١٩٧٧) الذي نص على ان(تقتصر الهجمات على الأهداف العسكرية فحسب، وتنحصر الأهداف العسكرية فيما يتعلق بالأعيان على تلك التي تسهم مساهمة فاعلة في العمل العسكري، سواء كان ذلك بطبيعتها أم بموقعها أم

بغايتها أم باستخدامها، و التي يحقق تدميرها التام أو الجزئي أو الإستيلاء عليها أو تعطيلها ، في الظروف السائدة حينذاك، ميزة عسكرية أكيدة)[٢٢].

من خلال هذه النصوص يتبين مدى أهمية هذا المبدأ فهو يطبق في حال الهجمات التقليدية، أما بالنسبة للهجمات السيبرانية فقال(ركس هوجيس) (ان الهجمات الرقمية تنشئ تحدياً أمام تطبيق مبدأ الضرورة العسكرية لذلك لابد من تضافر جهود خبراء القانون الدولي ومهندسي الصناعات الإلكترونية لتحديد مايمكن ان يوصف بانه هدف عسكري...)[٢٣]، فان عدم تحديد أو وضع معايير منظمة لاستخدام تكنولوجيا المعلومات لإغراض عسكرية، هذا يعني امكانية اللجوء في استخدامها بداعي الضرورة العسكرية، وهذا مانجده في التصريحات المتبادلة بين روسيا والولايات المتحدة الامريكية، عندما اصدرت وزارة الدفاع الامريكية بيان بأن خبراء روسيين نشروا دراسة قانونية تقول(ان لروسيا الحق في استخدام الاسلحة النووية إذا تعرضت لهجوم سيبراني)، أما روسيا فقد اعلنت من جانبها(ان توجيه هجمة سيبرانية ضد منشآت الاتصال الإلكترونية الامريكية، هذا يعني وقوع نتائج كارثية توازي استخدام اسلحة الدمار الشامل)، وهذا يعني ان هجوم سيبراني يمكن ان يكون الرد عليه بهجوم مادي على الدولة القائمة به، ومن ذلك يتبين ان مبدأ الضرورة العسكرية هو مبدأ حاضر في الهجمات الإلكترونية [٢٤].

٢- مبدأ التناسب في استخدام القوة:- ان هذا المبدأ من المبادئ الجوهرية التطبيقية في إطار النازعات المسلحة بكافة انواعها الداخلية والدولية، فهو يرمي إلى الإقلال من الخسائر أو أوجه المعناة التي تترتب على العمليات العسكرية، سواء أكان بالنسبة للأشخاص أو الأشياء، ومن ثم فإذا كانت وسائل القتال المستخدمة لاتتناسب مع الميزة العسكرية المرجوة من العملية العسكرية فلا يجوز استخدامها، ومثال ذلك الهجوم العشوائي الذي يتوقع ان يسبب خسائر كبيرة للمدنيين أو المنشآت المدنية، تتجأوز بكثير الميزة العسكرية المترتبة عليها[٢٥].

هذا و يثير تطبيق المبدأ المذكور في الهجمات الإلكترونية صعوبات عدة، بسبب عدم وجود فاصل في الكثير من الاحيان بين الفضاء السيبراني الذي يستخدمه المدنيين وبين الفضاء الذي تستخدمه القوات المسلحة المشاركة في العمل العدائي، وعلى الرغم من هذه الصعوبة، إلا ان دليل تالين تضمن وجوب الإلتزام بهذا المبدأ، إذ حظر الهجمات الإلكترونية التي قد تسبب خسائر في ارواح المدنيين أو اضرار في الاعيان المدنية التي قد تكون مفرطة مقارنة مع الميزة العسكرية التي يحققها ذلك الهجوم[٢٦]، كما ويمكن ان يكون تحقيق هذا المبدأ مستحيلاً في احيان اخرى، لان تكنولوجيا المعلومات والاتصالات غير متسأوية بين الدول، فقد تكون الدولة غير متطورة تكنولوجياً لرد الهجوم

السيبراني الموجه ضدها[٢٧]، ومن ثم يمكن ان يطبق مبدأ الضرورة العسكرية والتناسب بدلالة القاعدة(١٤) من دليل تالين التي جاء فيها(ان استخدام القوة الذي ينطوي على عمليات سيبرانية تقوم بها دولة في ممارسة حقها في الدفاع الشرعي ينبغي ان تكون ضرورية ومتناسبة)[٢٨].

٣- **مبدأ التمييز:-** لتأمين الإحترام والحماية للسكان والأعيان المدنية، فقد تم إلزام اطراف النزاع وفي كل الأوقات بالتمييز بين السكان المدنيين والمقاتلين، وبين الاعيان المدنية والأهداف العسكرية، ومن ثم يكون توجيه العمليات العسكرية ضد الاهداف العسكرية دون غيرها[٢٩]، إذ تم النص على هذا المبدأ في البروتوكول الإضافي الأول لإتفاقيات جنيف عام (١٩٧٧) والذي نص على ان(تعمل اطراف النزاع على التمييز بين السكان المدنيين والمقاتلين وبين الأعيان المدنية والأهداف العسكرية، ومن ثم توجه عملياتها ضد الأهداف العسكرية دون غيرها من اجل تأمين إحترام السكان المدنيين والأعيان المدنية)[٣٠].

يعد هذا المبدأ من المبادئ الأساسية في القانون الدولي الإنساني واكدت ذلك محكمة العدل الدولية، بقولها لايجوز توجيه الهجمات إلا نحو المقاتلين والاهداف العسكرية فقط، وهذا يعني انه عند تخطيط وتنفيذ العمليات الإلكترونية فالاهداف التي يكون مسموح بها هي الأهداف العسكرية، كأجهزة الكمبيوترأو النظم الحاسوبية التي تسهم بشكل فاعل في العمليات العسكرية، فلا يجوز توجيه الهجمات عبر الفضاء الالكتروني نحو نظم حاسوبية مستخدمة في منشآت مدنية بحتة[٣١].

وعلى الرغم من ذلك، فأن تطبيق هذا المبدأ فعلياً على الهجمات الإلكترونية هو مسألة غاية في التعقيد على عكس الهجمات التقليدية، لأن المهاجم السيبراني يكون غالباً بعيد عن المكان المستهدف، وهذا يعني ان التمييز بين المدنيين والمقاتلين أمر في غاية الصعوبة ان لم يكن مستحيلاً، وهذا مادفع المحامين الدوليين إلى المطالبة بتطبيق هذا المبدأ على الهجمات التي تقوم بها الروبوتات (الطائرات بدون طيار)[٣٢].

٤- **مبدأ مارنتز:-** وضع هذا المبدأ من قبل الدبلوماسي الروسي (فيدور فيودفج مارتنز) في مؤتمر السلام عام(١٨٩٩) وجاء فيه(في الحالات غير المشمولة بالاحكام يبقى السكان المتحاربون تحت سلطان وحماية مبادئ قانون الأمم كما جاءت من تقاليد استقرت عليها الشعوب المتمدنة والقوانين الإنسانية ومقتضيات الضمير العام)[٣٣]، وتم ذكر هذا المبدأ في كل من(اتفاقية لاهاي لعام١٨٩٩-١٩٠٧ الخاصة بقواعد واعراف الحرب البرية، واتفاقيات جنيف لعام ١٩٤٩، والبروتوكول الاضافي الأول لعام ١٩٧٧)، وبما ان هذا المبدأ ذات أهمية كبيرة في القانون الدولي ويعد صمام الأمان لذلك القانون، يثور سؤال بهذا الخصوص،

وهو إذا كان هذا المبدأ يطبق في الحالات التي لايكون هناك نص ينظمها في النزاعات التقليدية، وبما ان الهجمات الإلكترونية غالباً لايوجد لها تنظيم دولي متفق عليه إلى الآن، فهل يطبق هذا المبدأ عليها؟

للإجابة على هذا السؤال، نستشهد برأي محكمة العدل الدولية المتعلق بشرعية التهديد واستعمال الاسلحة النووية، الذي فسرت فيه المحكمة وحللت واستنتجت ان استخدام السلاح النووي محرم بسبب طبيعته التدميرية ونظرت إلى ماينتجه استخدام هذا السلاح من اضرار للبشرية بصرف النظر عن الوسيلة، خاصةً وان للطاقة النووية استخدأمات سلمية ايضاً، لذلك فأن المحكمة وضعت تفسيرات جديدة لمبادئ القانون الدولي الإنساني وقواعده، حتى يتم تطبيقها على جميع الاسلحة التي لم يتمكن المجتمع الدولي من تحريمها أو وضع قيود على استخدامها بعد، ولكي تمتنع الدول من استخدام الاسلحة الفتاكة الجديدة بحجة عدم وجود نص قانوني يحرم استخدامها[٣٤]،إذ قالت المحكمة بخصوص هذا المبدأ(اثبت انه وسيلة فعالة لمواجهة التطور السريع في التكنولوجيا العسكرية)، كما واكدت ان المبادئ الاساسية للقانون الدولي الإنساني تبقى منطبقة على جميع الاسلحة الجديدة بما في ذلك الاسلحة النووية[٣٥].

ومن هذا الرأي وبسبب عدم وجود قواعد عرفية وتعاقدية بين الدول تتعلق بالهجمات الإلكترونية، يمكن من وجه نظرنا، ان ينطبق شرط مارتنز عليها لسد الفراغ القانوني ومواكبة التطور التكنولوجي الحاصل وظهور اساليب واسلحة جديدة للحرب.

ومن خلال ماتم ذكره من مبادئ القانون الدولي الإنساني واجابة على السؤال الذي تم طرحه في بداية هذا الفرع، ان مبادئ القانون الدولي الإنساني يمكن تطبيقها على الهجمات الإلكترونية بدلالة ما اشارت إليه محكمة العدل الدولية فيما يتعلق بمشروعية الاسحة النووية بقولها(ان مبادئ وقواعد القانون الدولي الإنساني المنطبق في النزاع المسلح، تنطبق على كل اشكال الحرب وكل انواع الاسلحة...بما في ذلك تلك المستقبلية)[٣٦]، ومن ثم فان تكييف الهجمات الإلكترونية يدور في فرضيتين هما[٣٧] :-

الأولى:- عدم القدرة على اثبات الدليل المادي الناجم عن استخدام الهجمات الإلكترونية، وهو مايمثل العائق الأكبر الذي يواجهه المختصون وهذا على عكس ماتتركه وسائل القتال العادية من اثر مادي كالدمار والتعطيل الكلي والجزئي للمواقع العسكرية والمدنية.

الثانية:- إذا ثبت ان الهجمات الإلكترونية، قد تؤدي إلى آثار مادية ملموسة على كل المستويات الاقتصادية والامنية والعسكرية هنا يكون المعيار في تكييف تلك الهجمات أما من قبيل التصرف العدائي أو من قبيل التصرف لرد العدوان، إذ يعتمد بدرجة اساسية على القواعد القانونية التي لها صلة وبالذات حكم

الفقرة(٤) من المادة(٢)، والمادة(٥١) من ميثاق الأمم المتحدة، والتي ترتب آثار قانونية في حال اللجوء اليها.

أما امر تطبيق تلك المبادئ عملياً من من وجهة نظرنا، مسألة في غاية الصعوبة ان لم تكن مستحيلة، لان الفضاء الافتراضي لايعرف الحدود، وقلل الفواصل بين امورعدة فاصبحنا لانميز بين السلم والحرب وبين المدنيين والمقاتلين وبين الاعيان العسكرية والمدنية، وهذا مايميز الفضاء الافتراضي عن العالم الواقعي.

أما فيما يتعلق بالسؤال الآخر وهو متى يطبق القانون الدولي الإنساني على الهجمات الإلكترونية ؟

في ظل الصعوبات المذكورة يجب معرفة الوقت الذي يطبق فيه هذا القانون على الهجمات الإلكترونية، فأستناداً إلى دليل تالين وهو الصك الدولي المنظم للحروب الإلكترونية في الفضاء السيبراني، يطبق هذا القانون إذا نفذت العمليات الإلكترونية في سياق النزاع المسلح وكانت مرتبطة به، ومثال على ذلك إذا قام احد اطراف النزاع بالتزامن مع قصف بالمدفعية أو القذائف بشن هجوم الكتروني على الخصم، هنا تكون الهجمات الإلكترونية في إطار نزاع مسلح فيطبق عليها القانون الدولي الإنساني ودليل تالين[٣٨].

المبحث الثاني

المسؤولية الدولية عن اضرار الهجمات الإلكترونية في الفضاء الافتراضي

(International responsibility for the damage of cyber attacks in the virtual space)

بعد ان بينا التكييف القانوني للهجمات الإلكترونية ومدى انطباق المبادئ الرئيسة في القانون الدولي العام والإنساني عليها، بقى لدينا ماهو أهم وهو المسؤولية الدولية المترتبة في إطار الفضاء الافتراضي وذلك من خلال بيان مدى انطباق شروط المسؤولية التقليدية والحديثة على الهجمات الإلكترونية؟ هذا ماسنتنأوله في هذا المطلب، في فرعين، سيكون الأول لمدى انطباق شروط المسؤولية التقليدية على الهجمات الإلكترونية ، وسنخصص الثاني لمدى انطباق شروط المسؤولية الحديثة على الهجمات الإلكترونية .

المطلب الأول

مدى انطباق شروط المسؤولية التقليدية على الهجمات الإلكترونية

(The extent to which traditional terms of liability Applicable to cyber attacks)

ان لتكنولوجيا المعلومات والاتصالات و تشكيلها لبيئة الأمن الدولي فائدة في الجوانب الاقتصادية والإجتماعية وتيسير أمور الدولة، فقد تستخدم لإغراض لاتتوافق مع السلم والامن الدوليين، فزادت مخاطر استخدامها في السنوات الاخيرة مما ادى إلى زيادة الحاجة إلى التعأون لمواجهة اضرارها ومعرفة ماهي مسؤولية الدولة في هذا الفضاء[٣٩]، فإذا كان امر اثبات مسؤولية الدول يسير في حالة الحرب لان الهجوم إذا كان منصباً على تعطيل وسائل اتصال عسكرية أومدنية في وقت النزاع المسلح فالامر هنا يخضع للاحكام العامة للقانون الدولي الإنساني التي تتعلق بالعمليات القتالية وتصرفات المقاتلين[٤٠]،كما ان دليل تالين هو المختص بشأن القانون الدولي المطبق على الحرب السيبرانية فهو نظم المسؤولية القانونية للدولة عن تلك الهجمات وهذا ماجاء في القاعدة(٦) منه بالقول(تتحمل الدولة المسؤولية القانونية الدولية للعمليات السيبرانية التي تنسب اليها والتي تشكل خرقاً لالتزام دولي)[٤١].

أما في وقت السلم فالأمر ليس بهذا اليسر، إذ قد تتعرض الدول لهجمات سيبرانية يكون القائم بها دول اخرى أو جهات فاعلة من غير الدول فالمسؤولية في هذه الحالة تكون عن خرق قواعد والمبادئ العامة عرفية كانت أو مكتوبة في القانون الدولي، ومن هنا سنتكلم عن شروط المسؤولية التقليدية وفقاُ للأتي:-

أولاً:- خرق إلتزام دولي (الفعل غير المشروع دولياً)

تسأل الدولة على اساس خرق التزام دولي مفروض عليها، ومن أهم هذه الإلتزامات ذات الصلة بموضوع البحث هي:-

١- **الإلتزام بعدم التدخل في الشؤون الداخلية للدول:-** ان مبدأ عدم التدخل من المبادئ الأساسية للأمم المتحدة وهو ضمانة من ضمانات سيادة الدولة وورد ذكره في المادة(٢/فقرة٧) من ميثاق الأمم المتحدة، إذ نصت على انه(ليس في هذا الميثاق ما يسمح للامم المتحدة ان تتدخل في الشؤون التي تكون من صميم السلطان الداخلي لدولة ما..)، وان مسؤولية الدولة حيال دورها في التدخل يضبطه امرين الأول مأورد في المادة(٤)[٤٢] من مسودة لجنة القانون الدولي عن مسؤولية الدول عن الأفعال غير المشروعة والتي تنأولت مسؤولية الدولة عن التصرفات الدولية الخاطئة الصادرة من سلطاتها التشريعية والتنفيذية والقضائية، والمادة (٨)[٤٣] من المسودة نفسها التي تكلمت عن مسؤولية الدولة عن تصرفاتها وتصرفات المجموعات التي تسيطر عليها، وهذا يقودنا إلى ضرورة الحديث عن السوابق القضائية في هذا الخصوص، ففي قضية (الأنشطة العسكرية وشبه العسكرية بين نيكاراغوا ضد الولايات المتحدة الامريكية) التي تجسد بها مفهوم السيطرة، ففي عام(١٩٨٤) قدم سفير نيكاراغوا طلباً لتسجيل دعوى أمام محكمة العدل الدولية ضد الولايات المتحدة الامريكية، فذكر في الادعاء ان ان الولايات المتحدة الامريكية قامت بتدريب وتجهيز وتسليح وتمويل ومساعدة قوات (الكونترا) وان ماقامت به هو انتهاك للمادة(٢/الفقرة٤) من ميثاق الأمم المتحدة، واستناداً إلى ذلك فان الولايات المتحدة لها سيطرة كاملة على قوات (الكونترا)، وقد عارضت الولايات المتحدة الامريكية هذا الادعاء واختصاص محكمة العدل الدولية للنظر في هذه القضية لكن المحكمة ردت هذا الاعتراض وقضت بمسؤولية الولايات المتحدة الامريكية استنادا إلى (معيار السيطرة الفعالة)[٤٤].

أما القضية الأخرى التي نسب بها الفعل للدولة من جراء ماقامت به مجموعة مسلحة كانت مدعومة من قبلها هي قضية(تاديش) في عام(١٩٩٧) والتي نظرتها دائرة الاستئناف التابعة للمحكمة الجنائية الدولية في يوغسلافيا، إذ ركزت على معيار(السيطرة الكاملة أوالشاملة) بقولها(ان درجة الرقابة التي يشترط القانون الدولي أن تمارسها السلطات اليوغسلافية على هذه القوات المسلحة لاعتبار النزاع المسلح نزاعاً دولياً هي(الرقابة الشاملة) التي تتعدى مجرد تمويل وتجهيز هذه القوات وتنطوي أيضاً على المشاركة في تخطيط العمليات العسكرية والإشراف عليها)[٤٥]، وهذا يعني ان الدولة تكون مسؤولة عما تقوم به اجهزتها والجهات الاخرى التي تمارس عليها الرقابة والتوجيه

والسيطرة ، أما في حالة الهجمات الإلكترونية فهذه المعايير قد تكون غير واقعية لصعوبة اثباتها لان الهجمات الإلكترونية ذات وضع خاص ومختلف.

٢- الاخلال بإلتزام المنع (الإلتزام ببذل العناية الواجبة):- يقصد بهذا الإلتزام هو(على الدولة ان تمنع استخدام اراضيها بما يتعارض مع حقوق الدول الاخرى) وهذا إلتزام عرفي وارد في المبدأ(٢١) من إعلان استوكهولم وتم تدوينه في تقرير لجنة القانون الدولي في المسؤولية عن أعمال لايحظرها القانون الدولي في واجب المنع في المادة(٣) منه بقوله(تتخذ دولة المصدر كل التدابير المناسبة لمنع وقوع ضرر جسيم عابر للحدود والتقليل من مخاطره إلى ادنى حد)، وهذا يعني، ان على الدولة واجب منع الاضرار العابرة للحدود، ويسمى بالتزام العناية الواجبة ايضاً، وهذا الإلتزام هو إلتزام بسلوك وليس بتحقيق نتيجة، ويخضع لتقدير الدولة ويتاثر بعوامل عدة منها(قدرة الدولة، خطورة الفعل، الضرر الحاصل)، ويشترط في الضرر المطلوب لبذل عناية لمنعه، هو الضرر الجسيم العابر للحدود، كالاضرار البيئية واضرار استخدام الفضاء الخارجي والأنشطة النووية، فعلى الدولة تحديد النشاط الخطر واتخاذ مايلزم من تدابير، وهو التزام يتسم بطابع الاستمرار.[٤٦].

هذا وإذا كان هذا الإلتزام يطبق على الاضرار البيئية العابرة للحدود، فأنه يتبادر للذهن سؤال، وهو، هل يمكن ان يفعل هذا الإلتزام في إطار الهجمات الإلكترونية كون الاضرار التي تحدثها هذه الهجمات وقت السلم قد تكون اضراراً جسيمة وعابرة للحدود؟

هناك من يقأوم تطبيق هذا الإلتزام على الأنشطة والهجمات الإلكترونية، لانهم يخشون العبء الذي يفرضه هذا الإلتزام، لكن في المقابل هناك من يرغب في تطبيقه لوضع حد للأنشطة الإلكترونية الضارة، وعلى الرغم من هذا الخلاف، فقد اتفق الخبراء بالاجماع على ان الدولة تتحمل إلتزام العناية الواجبة فيما يتعلق بالبنى التحتية السيبرانية والأنشطة المنبعثة من اراضيها أو التي قد تمر بها، ويكون القائم بها جهات فاعلة غير حكومية[٤٧]، و تم التاكيد على هذا الإلتزام في تقرير فريق الخبراء الحكوميين حول التطورات في مجال المعلومات بالقول (تماشياً مع مقاصد الأمم المتحدة بما في ذلك صون السلم والأمن الدوليين، ينبغي للدول ان تتعأون في وضع وتطبيق تدابيرلزيادة الأمن والاستقرار.. وعليها منع استخدام تلكنولوجيا الاتصالات إذا كانت ضارة أو قد تشكل تهديد للسلم والأمن الدوليين)[٤٨]وهذا ايضاً ما اكده دليل تالين في القاعدة رقم(٥) منه بقولها(لايجوز للدولة ان تسمح بمعرفتها باستخدام البنية التحتية السيبرانية الواقعة في اقليمها أو التي تحت سيطرتها الحكومية الحصرية ان تستخدم في الاعمال التي تؤثر سلباً وبشكل غير شرعي على الدول الاخرى)[٤٩]، وهذا يعني انطباقها على الفضاء الافتراضي، كما وان أهم السمات الأساسية لهذا الواجب هو المعرفة أو العلم

والضرر، فبالنسبة للعلم بالتهديد فيعد هذا العنصر حاسماً، فإذا كانت الدولة على علم بالتهديد الحاصل كان واجب عليها اتخاذ التدابير اللازمة لقمعه، لكن ظهور تهديد من داخل اراضي الدولة لايعني انها تكون تلقائياً قد علمت به، وفي نطاق الفضاء الافتراضي يجب ان تكون الدولة على علم بالتهديد، ويكون ذلك من خلال مراقبتها المكثفة لأنشطة بنيتها التحتية، ففي حالة معرفتها ان بنيتها التحتية الرقمية مصابة ببرامج خبيثة أو انها اصبحت ملجأ لمن يرغب في اطلاق مثل هذه البرامج الضارة، فعليها ان تقوم باتخاذ مايمكن لمنع هذه الهجمات(٥٠)، واكدت على عنصر العلم محكمة العدل الدولية في قضية الابادة الجماعية لعام(١٩٩٣) بقولها(تتحمل الدولة المسؤولية...إذا كانت على علم أو كان يجب ان تكون على علم..)، ففي النطاق الرقمي رأى جميع الخبراء ان الدولة الاقليمية يجب ان تكون لديها معرفة بالنشاط الضار المعني، إلا انهم فشلوا في التوصل إلى اتفاق حول إذا كانت المعرفة كافية لكي يكون خرق للالتزام ام لا(٥١) .

أما فيما يتعلق بالضرر كأحد سمات إلتزام العناية الواجبة، فحتى تكون الدولة مسؤولة عن مخالفة الإلتزام، يجب ان يكون الضرر جسيم عابر للحدود، وهذا ماتبناه دليل تالين موضحا ان التزام العناية الواجبة يطبق على الأنشطة التي تسبب اضراراً جسيمة وعابرة للحدود، والضرر المقصود هنا ليست الاضرار المادية فقط، انما ممكن ان يشمل الضرر الذي يلحق بنظام الكمبيوتروالذي يسبب عواقب وخيمة إذا تعطلت تلك النشاطات(٥٢).

هذا ومن خلال ماتقدم، يمكن القول، انه متى ماكانت الدولة على علم بالسلوك أو الهجوم السيبراني الضار بالدول الاخرى ولم تتخذ التدابير اللازمة والوقاية لمنعه، كانت مسؤولة دولياً على أساس خرق إلتزام دولي، اي على أساس الفعل غير المشروع، أما إذا اتخذت العناية اللازمة لكن مع ذلك حدث الضرر، تكون مسؤولة على أساس المخاطر، كما وتجدر الاشارة ان التزام العناية الواجبة هو مفهوم مرن ومتغير ويتطلب من الدولة ان تواكب التطورات التكنولوجية والعلمية الحاصلة.

ثانياً:- نسبة الفعل إلى لدولة

لايكفي القول بوجود المسؤولية بمجرد خرق الإلتزام الدولي، انما يجب ان ينسب الفعل إلى الدولة، وهذه اكبر صعوبة تواجه المسؤولية الدولية في الفضاء الافتراضي الذي يكون فيه عدم الكشف عن الهوية هو القاعدة وليس الاستثناء، ومادام ان الاطراف لايمكن تحديد هوياتهم كدولة أو جهة فاعلة من غير الدول، فلانستطيع ان نصنف هل هذه الهجمة هي نزاع مسلح دولي ام لا، وعلى الرغم من ذلك فان هذا التحدي يتعلق بالوقائع لابالناحية القانونية، ومن السبل التي من خلالها يمكن التغلب على عدم اليقين، هو استخدام الافتراضات القانونية، ومثال على ذلك ان الهجوم على شبكة الكمبيوتر إذا يشن من بنية أساسية حكومية لدولة

معينة، فتسند العملية للدولة من خلال هذا الافتراض، خاصة وان قواعد القانون الدولي تتضمن التزام بان الدولة يجب عليها ان لاتسمح،عن علم، باستخدام اراضيها للقيام بافعال تتعارض مع حقوق دولة اخرى، لكن هذا النهج يرد عليه اعتراضين وهما:-(٥٣)

الأول:- ان قواعد القانون الدولي القائمة لاتؤيد هذا الافتراض، ومثال ذلك ان المواد المتعلقة بمسؤولية الدول عن الافعال غير المشروعة دولياً لاتتضمن اي قواعد بشأن افتراض اسناد التصرف إلى دولة معينة، كما ووصفت محكمة العدل الدولية اسناد التصرف إلى دولة معينة في سياق حق الدفاع عن النفس، إذ قررت فعلياً في قضية منصات النفط لعام (١٩٨٧) ان عبء الاثبات يقع على عاتق الدولة التي تحتج بحق الدفاع عن النفس، فالمحكمة ببساطة عليها ان تقرر إذا كانت الولايات المتحدة ضحية الهجوم الذي شنته ايران وانها استخدمت القوة المسلحة دفاعاً عن النفس وهذا يقع على عاتق من مارس هذا الحق وهي الولايات المتحدة الامريكية، وعلى الرغم من إن هذه العبارة صدرت في سياق حق الدفاع عن النفس، فيمكن تعميمها على كل المسائل الواقعية المتعلقة بإسناد التصرف إلى دولة معينة، وبما انه افتراض حول الوقائع، فسيكون من غير المنطقي افتراض حقائق لغرض واحد معين ليس لغرض آخر.

الثاني:- ان هذا الافتراض بعيد المدى للغاية في إطار الحرب السيبرانية، فبسبب صعوبة تحصين البنية التحتية الاساسية الحاسوبية من التلاعب وسهولة التخفي تحت هوية مختلفة في الفضاء الافتراضي، فأن هذا سيلقي عبء كبير للغاية على الحكومات من ناحية تحملها مسؤولية جميع العمليات التي تطلق من اجهزة الكمبيوترالخاصة بها دون اي دليل اخر.

ومن ناحية اخرى، تجدر الاشارة إلى ان الهجمات الإلكترونية التي تستهدف البنى التحتية للدولة وتخلق اضرار كبيرة، تقوم بها الدول المتقدمة والتي تمتلك قوة الكترونية كبيرة، إلى جانبها قد يقوم بتلك الهجمات جهات اخرى غير الدول، كالمنظمات الحكومية عالمية كانت أو اقليمية أو بعض الافراد ممن تتهيأ لهم دون غيرهم امكانية التحرك على نطاق واسع نسبياً من الاتصالات الدولية أو الجماعات الارهابية وحركات التحرير الوطنية والمتمردين، وهؤلاء ينطبق عليهم مايسمى بنسبة الفعل للدولة، وذلك لان الدولة تسأل عن افعال رعاياها في حالة التقصير(٥٤).

ثالثاً:- الضرر

ان الضرر ليس شرط أساسي في المسؤولية التقليدية، فكما ذكرنا سابقاً، تكون الدولة مسؤولة بمجرد خرق الإلتزام ونسبة الفعل لها، أما في وضع الهجمات الإلكترونية، فالأمر مختلف لان تلك الهجمات تحقق الضرر بكافة اشكاله، سواء أكان الفاعل دولاً كما حصل في الهجوم الفايروسي على البرنامج النووي

الايراني في عام(٢٠١٠)، أو قد تقوم بها منظمات اجرامية تلحق اضراراً فادحة بالآخرين، كهجمات سرقة المعلومات واختراق الحسابات الذكية[٥٥] .

من هنا يجب ان نعرف مدى توفر شروط نظرية الفعل غير المشروع على الهجمات أو الأنشطة السيبرانية الضارة، فبالنسبة لشرط خرق إلتزام دولي وهو امكانية تحققه كما فصلنا فيما سبق ذكره، أما الضرر ايضاً امكانية تحققه لكنه ليس شرطا أساسياً في هذه النظرية ، لكن ماهو صعب هو نسبة الفعل للدولة أو لجهة فاعلة غير حكومية، لان في إطار الفضاء الافتراضي يمكن للفاعل اخفاء هويته بكل سهولة، لكن وان كان صعبا انما هو ليس مستحيلا فيمكن تتبع عنأوين(IP) الخاصة بكل دولة، لكن هذا يتطلب وقت طويل جداً، فضلاً عن برامج تسمى ببرامج اقتفاء الأثر العكسي لمعرفة هوية المهاجم، لكن هذه هي الاخرى ليست بالامر السهل، لانها قد تصل إلى جهاز خادم لايتعأون لمعرفة الهوية، كما قد يكون القائم بالهجمة اتخذ التدابير اللازمة لاخفاء الهوية، ومن ثم فأن هناك امكانية لتاسيس مسؤولية الدولة على نظرية الفعل غير مشروع[٥٦].

المطلب الثاني

مدى انطباق شروط المسؤولية الحديثة على الهجمات الإلكترونية (The extent to which modern liabilityTerm Applicability to cyber attacks)

ظهرت نظرية المخاطر لسد النقص الحاصل في نظرية الفعل غير المشروع ومواكبة التطور العلمي والتكنولوجي، وبما ان الفضاء الافتراضي هو نتاج هذا التطور، فهل تطبق هذه النظرية على الفضاء الافتراضي وتكون الدولة مسؤولة مسؤولية مطلقة؟

بدايةً اخذ مشروع لجنة القانون الدولي في تدوينه للمسؤولية عن أعمال لايحظرها القانون الدولي مجالات عدة ومنها البيئة والفضاء الخارجي، وكما نعلم ان الفضاء الافتراضي لم يتم تنظيمه لافي مواد اللجنة ولافي اتفاقية بين الدول، لذلك سنقارن بين كل من البيئة والفضاء الخارجي ومدى امكانية القياس مع الفارق بينهم وتطبيق احكامهما المتعلقة بالمسؤولية على الفضاء الافتراضي، فبالنسبة للبيئة فأنها تختلف عن الفضاء الافتراضي من نواحي عدة وتتشابه معه في نواحي اخرى، الاختلاف يظهر في ان البيئة طبيعية لم يتدخل الإنسان في وجودها في حين ان الفضاء الافتراضي هو من صنع الإنسان، أما من ناحية التنظيم فالبيئة تحكمها اتفاقيات دولية خاصة بها كالاتفافية الإطارية بشان تغيير المناخ لعام (١٩٩٢) واتفاقيات حماية البيئة من التلوث أما الفضاء الافتراضي فلايوجد اتفاقية دولية تنظمه، واختلاف آخر هو ان الاضرار البيئة لاتظهر مباشرة انما تحتاج إلى وقت أما اضرار الفضاء الافتراضي فهي فورية الأثر، أما التشابه بين النموذجين فهو ان كلاهما ذات اضرار عابرة للحدود[٥٧] .

أما فيما يخص العلاقة بين الفضاء الخارجي والافتراضي، فأن كل من الفضائين يختلفان بشكل واضح، خاصةً وانهما ينتميان إلى عالمين مختلفين وبالتحديد عالم الذرات وعالم الالكترونيات، كما وان الفضاء الخارجي منظم دولياً وتحكمه اتفاقيات عدة، منها معاهدة الفضاء الخارجي لعام(١٩٦٨) واتفاقية المسؤولية الدولية القانونية عن الضرر الذي تسببه الاجسام الفضائية لعام (١٩٧٢) وغيرهم، بينما الفضاء الافتراضي لا تحكمه سوى قوانين وطنية واتفاقية بودابست لعام(٢٠٠١) وعدد من المبادئ التي اقرتها مؤتمرات القمة العالمية لمجتمع المعلومات في جنيف عام(٢٠٠٣) وتونس عام(٢٠٠٥)، وعلى الرغم من هذا الاختلاف لكن الفضائين يشتركان في امور عدة و منها ان كلاهما لاتحده حدود دولية وان الفضاء الافتراضي عالماً مفتوحاً للإنسانية جمعاء كذلك الفضاء الخارجي يعد هو الآخر عالماً مفتوحاً ومشاعاً لكل من يكون قادراً على استكشافه واستعماله للاغراض السلمية حصراً، فضلاً عن ان كلاهما يمثلان خطراً على امن الدول، ففي ظل وجود الاجهزة والاقمار الصناعية والانترنيت لم تعد اغلب الدول تستطيع ستر اسرارها العسكرية والمدنية مما يؤدي إلى زعزعة الاستقرار وامن الدول، كما ان كلاهما ذات اضرار عابرة للحدود[٥٨].

من خلال ماتم ذكره والتشابه بين الأنشطة التي ذكرتها لجنة القانون الدولي في تقرير المسؤولية عن افعال لايحظرها القانون الدولي، فأن الدولة تكون مسؤولة مسؤولية مطلقة إذا مارست هذه النشاطات التي تسبب الضرر العابر للحدود، وبما ان الهجمات والأنشطة الضارة في الفضاء السيبراني تسبب الضرر نفسه، فهنا يجب ان نبين فيما إذا كانت شروط المسؤولية الموضوعية متحققة وتطبق على الفضاء السيبراني ام لا، ان شروط المسؤولية المطلقة هي:-

1 -النشاط الخطر:- ان الهجمات الإلكترونية والأنشطة الضارة التي تمارسها الدول في هذا الفضاء تكون خطرة على أمن الدول وتهدد أو تحدث اخلال بالسلم والأمن الدوليين، فنشاط الانترنيت يندرج تحت بند المخاطر الدولية التي تقع الدولة على أثرها في خانة المسؤولية الدولية عند اتهامها في إحداث هجمة سيبرانية دولية[٥٩].

٢- الضرر العابر للحدود:- هذا الشرط متحقق في الهجمات الإلكترونية والأنشطة الضارة التي تمارسها الدول في هذا الفضاء، لانها تستهدف بنى تحتية للدول، كالسدود ومحطات الطاقة الكهربائية والنووية والقطاع الصحي للدولة المستهدفة أو دولاً اخرى، مثلا عند اطلاق فايروس فقد يفقد من قام بإطلاقه السيطرة عليه، فهو بذلك سبب اضراراً عابرة للحدود.

٣-العلاقة السببية بين النشاط الخطر والضرر:- ان مسألة اثبات العلاقة السببية بالنسبة للانشطة البيئية والنووية مسألة صعبة، لان آثار هذه النشاطات لاتظهر مباشرة، بينما في الفضاء الافتراضي يمكن اثباتها، فأن الهجمة السيبرانية

الحاصلة هي السبب في الاضرار العابرة للحدود واضرار البنى التحتية للدولة التي تعرضت للهجوم .

ومن ثم فإذا تحققت هذه الشروط في الأنشطة البيئية أو الفضاء الخارجي، حينها تكون الدولة مسؤولة موضوعياً لان نشاط الدولة الخطر هو نشاط مشروع، لكن في الفضاء الافتراضي حتى لو تحققت الشروط ،لاتسأل الدولة على أساس النظرية المطلقة أو نظرية المخاطر، لان نشاط الدولة في هذا الفضاء ليس فعلا مشروعاً، فهو في وقت الحرب سيكون نزاعاً مسلحاً وفي وقت السلم سيكون نشاطاً اجرامياً إذا قامت به جهات فاعلة غير حكومية، وتدخل في الشؤون الداخلية للدول إذا قامت به دولة، ومن هنا فأن نظرية المسؤولية المطلقة في الفضاء السيبراني لاتطبق.

هذا ومن الجدير بالذكر ان اهم الهجمات الإلكترونية التي حدثت هي الهجوم الروسي على استونيا عام (٢٠٠٧) وعلى جورجيا عام (٢٠٠٨) الذي كان على اثر الحرب التي كانت بينهم، والهجوم الالكتروني على البرامج النووية الايرانية عن طريق فايروس(ستاكنست) في عام (٢٠١٠) الذي قيل ان من قام به هو الولايات المتحدة الامريكية والكيان الصهيوني، إذ هاجم هذا الفايروس انظمة التحكم المركزية والذي كان مصمماً للعمل فقط عند وصوله إلى المفاعل النووي الايراني، واتضح في عام(٢٠١٢) ان الولايات المتحدة واسرائيل عملا بشكل مشترك على تطوير فايروس(ستاكنست) لتخريب البرنامج النووي الايراني، فهناك اعتقاد ان هاتين الدولتين هما المسؤولتين عن الهجوم، على الرغم من عدم اعتراف اياً منهما بالمسؤولية، إلى جانب هذا الهجوم، تعرضت ايران لهجمات عدة كان آخرها في عام(٢٠٢٠)،عندما تعطلت شبكة الاتصالات لساعات، لكن ايران التزمت الصمت حول الجهة التي شنت هذا الهجوم، ويعد صمت الدول التي تتعرض للهجوم احدى العوائق أمام معرفة القائم به[٦٠]،هذا وللعلم فأن الهجمات المذكورة ليست الوحيدة في العالم الافتراضي لكنها الأهم والاشهر.

الخاتمة

(Conclusion)

ان الهجمات الإلكترونية كنوع جديد من أنواع الصراع بين الدول، والتي ظهرت مؤخراً مع التطور التكنولوجي الحاصل فهي تسبب اضراراً عابرة للحدود تصيب مصالح الدول وبنيتها التحتية، فأن هذه الهجمات اثارت العديد من المشاكل وعلأمات الاستفهام على المستوى الدولي سواء أكان القائم بها دولة أم جهات فاعلة من غير الدول، لذلك حأولنا تسليط الضوء على أهم المسائل التي تدور حولها علأمات الاستفهام في هذا الخصوص فبينا ماهي الهجمات الإلكترونية وتكييفها القانوني وماهي المسؤولية المترتبة عليها، وتوصلنا إلى جملة من الاستنتاجات والمقترحات وهي:-

أولاً:- الاستنتاجات

١-ان الفضاء الاقتراضي هو أهم ما انتجته الثورة التكنولوجية والذي ارتبطت به كل مفاصل الدولة وبناها التحتية وسهل اداء وظائفها، لكن من جانب آخر فهو خطر على أمن الدول بسبب ماتتعرض له من هجمات الكترونية من قبل دول اخرى أو جهات فاعلة من غير الدول، ممايسبب اضراراً قد تكون كارثية للدولة التي تعرضت للهجوم.

٢- ان القانون الدولي الإنساني يطبق على الهجمات الإلكترونية التي تشن وقت الحرب أو اثناء النزاع المسلح، وان دليل تالين هو المنظم لتلك الهجمات بشكل خاص على الرغم من انه وثيقة غير ملزمة لكنها الوحيدة التي نظمت موضوع الحرب والهجمات الإلكترونية في هذا الإطار، ومن ثم فان مبادئ القانون الدولي الإنساني تطبق على تلك الهجمات استناداً لدليل تالين على الرغم من الصعوبات الواقعية لتطبيقها في ذلك الفضاء.

٣- ان الهجوم السيبراني وقت السلم من الامور التي يوجد اختلاف حولها، من خلال تحيل المبادئ العامة للقانون الدولي العام نجد ان للدولة التي تعرضت للهجوم السيبراني إذا كانت آثاره تشبه آثار الهجوم المسلح يكون لها حق الدفاع عن النفس سواء أكان بهجمة سيبرانية أم بهجوم مسلح.

٤- تكون الدولة مسؤولة عن الهجمات الإلكترونية على أساس خرقها لإلتزام دولي ومنها الإلتزام بعدم التدخل في الشؤون الداخلية للدول والتزام بمنع الهجمات الحاصلة، اي ان نظرية الفعل غير المشروع لها تطبيقها على الهجمات في الفضاء السيبراني، أما نظرية المخاطر وبسبب عدم مشروعية فعل الدولة بكل الحالات فانها غير قابلة للتطبيق عليها.

ثانياً:- المقترحات

١- الدعوة الى عقد اتفاقية دولية متعددة الاطراف لتنظيم الهجمات الإلكترونية وتقييدها لتحقيق الامن السيبراني للدول وحماية البنى التحتية والحفاظ على السلم والامن الدوليين.

٢- العمل على تكثيف الدراسات ووضع مشاريع وابتكار تقنيات جديدة لمعرفة المهاجم السيبراني وبها يتم تجاوز عقبة اخفاء الهوية للقائم بالهجوم التي تعد الصعوبة الاكبر التي تواجه اثبات المسؤولية.

٣- دعوة الجهات المختصة الى فصل الشبكات السيبرانية العسكرية عن البنى التحتية المدنية من أجل حماية السكان المدنيين من اخطار تلك الهجمات التي تقع في وقت السلم أو الحرب والتي لاتعرف الحدود.

الهوامش (Margins)

(١) خالد وليد محمود، الهجمات عبر الانترنيت: ساحة الصراع الالكتروني الجديدة، المركز العربي ودراسة السياسات، قطر، ٢٠١٣، ص٤.

(٢) عادل عبد الصادق، اسلحة الفضاء الالكتروني في ضوء القانون الدولي الانساني، مكتبة الاسكندرية، وحدة الدراسات المستقبلية، مصر، ٢٠١٦، ص٥٥.

(٣) Marie Baezner, Patrice Robin, Trend Analysis: Cyber Sovereignty and Data Sovereignty, Center for Security Studies (CSS), 2018,p7.

(٤) المادة(٢)/ الفقرة(١) من ميثاق الأمم المتحدة.

السيادة السيبرانية (هي بسط الدولة سيطرتها وولايتها القضائية على الفضاء الرقمي المتمثل بشبكة الانترنيت))٥(

-حسام جاسم محمد أحمد الدليمي، التطور التكنولوجي واثره في سيادة الدول، رسالة ماجستير مقدمة الى مجلس كلية القانون والعلوم السياسية- جامعة الانبار، الانبار، ٢٠١٨، ص١١٤.

(٦) فاطم بيرم، السيادة الوطنية في ظل الفضاء السيبراني والتحولات الرقمية:الصين نموذجاً، المجلة الجزائرية للامن الانساني ، المجلد الخامس، العدد الاول ، مخبر الامن الانساني-جامعة باتنة، الجزائر، ٢٠٢٠، ص٧٩٨.

(٧) أحمد عبيس نعمة الفتلاوي وزهراء عماد محمد، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، المجلد٤٤، العدد١، كلية القانون والعلوم السياسية –جامعة الكوفة، النجف، ٢٠٢٠، ص٥٧.

(٨) Wolff Heintschel von Heinegg, Territorial Sovereignty and Neutrality in Cyberspace, International Law Studies ,U. S. Naval war college , Vol 89,2013, p128.

(٩) علي محمد كاظم الموسوي، المشاركة المباشرة في الهجمات السيبرانية، المؤسسة الحديثة للكتاب، لبنان، ٢٠١٩، ص٢ .

(١٠) المادة (٢)/ الفقرة(٤) من ميثاق الأمم المتحدة.

(١١) Oona A. Hathaway, The Law of Cyber-Attack, Yale Law School, United States of America, Vol. 100:817, 2012 ,p842

(١٢) المادة(٥١) من ميثاق الأمم المتحدة.

(١٣) أحمد عبيس نعمة الفتلاوي وزهراء عماد محمد، مصدر سابق،ص٥٩.
(١٤) United Nations Audiovisual Library of International Law, General Assembly Resolution 3314, Defining aggression,p5
(١٥) أحمد عبيس نعمة الفتلاوي وزهراء عماد محمد، مصدر سابق، ص٦٠.
(١٦) Oona A. Hathaway, op. cit, p848.)
(١٧) علي محمد كاظم الموسوي، مصدر سابق، ص٤.
(١٨) أحمد عبيس نعمة الفتلاوي وزهراء عماد محمد ، مصدر سابق، ص٦١.
(١٩) Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Sixty-eighth session, document (A/68/98),2013,p8.
(٢٠) مروة إبراهيم محمد، مبدأ الضرورة العسكرية في القانون الدولي الإنساني، رسالة ماجستير مقدمة الى مجلس كلية القانون- جامعة بغداد، بغداد،٢٠١٥، ص١٩.
(٢١) المادة(٣)/الفقرة(٢/ز) من اتفاقية لاهاي للحرب البرية لعام ١٩٠٧.
(٢٢) المادة (٥٢)/الفقرة(٢) من البروتوكول الاضافي الاول لعام ١٩٧٧.
(٢٣) أحمد عبيس نعمة الفتلاوي،الهجمات السيبرانية:مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية ،المجلد ٨، العدد ٤، جامعة بابل، بابل، ٢٠١٦، ص٦٣٥.
(٢٤) أحمد عبيس نعمة الفتلاوي،المصدر نفسه.
(٢٥) مروة إبراهيم محمد، مصدر سابق، ص٩٥.
(٢٦) يحيى ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الانساني، المجلة القانونية، المجلد(٤)،العدد(٤)، كلية الحقوق- جامعة القاهرة، مصر، ص٩٤.
(٢٧) أحمد عبيس نعمة الفتلاوي وزهراء عماد محمد، مصدر سابق، ٦٣.
(٢٨) علي محمد كاظم الموسوي، مصدر سابق، ص٤.
(٢٩) ليث الدين صلاح حبيب، الحماية الدولية لضحايا النزاعات المسلحة من غير الأسرى، رسالة ماجستيؤ مقدمة الى مجلس كلية القانون- جامعة بغداد، بغداد، ٢٠٠٦، ص١٦.
(٣٠) المادة(٤٨) من البروتوكول الإضافي الأول لإتفاقيات جنيف لعام ١٩٧٧.
(٣١) بن تغري موسى، الحرب السيبرانية والقانون الدولي الإنساني، مجلة الاجتهاد القضائي، المجلد(١٢)، العدد(٢٢)، مخبر الاجتهاد القضائي على حركة التشريع، جامعة محمد خيضر بسكرة، الجزائر، ٢٠٢٠، ص٢٠٩.
(٣٢) أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية:مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مصدر سابق، ص٦٣٦.
(٣٣) Antonio Cassese, The Martens Clause: Half a Loaf or Simply Pie in the Sky? , Vol. 11,2000, p187.
(٣٤) سلافة طارق الشعلان، تكييف استخدام الحرب الالكترونية في الزاعات المسلحة وفقاً للقانون الدولي الإنساني، مجلة الكوفة للعلوم القانونية والسياسية، المجلد١، العدد٢٦، كلية القانون جامعة الكوفة، الكوفة، ٢٠١٦، ص٢٥.
(٣٥) أحمد عبيس نعمة الفتلاوي وزهراء عماد محمد، مصدر سابق، ص٦٤.
(٣٦) المصدر نفسه، ص٦١.

([٣٧]) طلال ياسين العسى وعدي أحمد عناب، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الانسانية، المجلد١٩، العدد الاول، جامعة الزرقاء، الاردن، ٢٠١٩، ص٨٨.

([٣٨]) كوردولا دوريجي، لاتقترب من حدود فضائي الالكتروني: الحرب الالكترونية والقانون الدولي الانساني وحماية المدنيين، مختارات من المجلة الدولية للصليب الأحمر، المجلد٩٤، اللجنة الدولية للصليب الأحمر، جنيف،٢٠١٢، ص٥٤٢.

([٣٩]) Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,op,cit,p2.

([٤٠]) أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئةعنها في ضوءالتنظيم الدولي المعاصر، مصدر سابق، ص٦٤٢.

([٤١]) علي محمد كاظم الموسوي، مصدر سابق، ص٣.

(٣١) نصت المادة(٤) من مسودة لجنة القانون الدولي عن مسؤولية الدول عن الافعال غير المشروعة على ان(١-يعد تصرف أي جهاز من أجهزة الدولة فعلاً صادراً عن هذه الدولة بمقتضى القانون الدولي، سواء أكان الجهاز يمارس وظائف تشريعية أم تنفيذية أم قضائية أم أية وظائف أخرى، وأيّاً كان المركز الذي يشغله في تنظيم الدولة، وسواء أكانت صفته أنه جهاز من أجهزة الحكومة المركزية أ م جهاز من أجهزة وحدة إقليمية من وحدات الدولة،٢- يشمل الجهاز أي شخص أو كيان له ذلك المركز وفقاً للقانون الداخلي للدولة).

([٤٣]) نصت المادة(٨) من مسودة لجنة القانون الدولي عن مسؤولية الدول عن الافعال غير المشروعة على ان (يعتبر فعلاً صادراً عن الدولة بمقتضى القانون الدولي تصرفُ شخص أو مجموعة أشخاص إذا كان الشخص أو مجموعة الأشخاص يتصرفون في الواقع بناء على تعليمات تلك الدولة أو بتوجيهات منها أو تحت رقابتها لدى القيام بذلك التصرف.

-تقرير لجنة القانون الدولي ٢٠٠١، الدورة ٥٣ الوثيقة، A/CN.4/SER.A/2001/ADD.IC.PART2

([٤٤]) رائد حميد صالح، اثر التطبيقات الرقمية على سيادة الدول، رسالة ماجستير مقدمة الى مجلس كلية الحقوق- جامعةالنهرين ، بغداد، ٢٠١٩، ص١٥٣

([٤٥]) تقريرلجنة القانون الدولي، مصدر سابق، ص٦٠.

([٤٦]) تقريرلجنة القانون الدولي لعام ٢٠٠١، مصدر سابق، ص١٩٣.

([٤٧]) Michael N. Schmitt, In Defense of Due Diligence in Cyberspace, the yale law journal forum, N22, 2015, p70.

([٤٨]) Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, General Assembly United Nations, decument A/70/174,2015.

([٤٩]) علي محمد كاظم الموسوي، مصدر سابق، ص٣.

([٥٠]) رائد حميد، مصدر سابق، ص١٩٢.

([٥١]) Michael N. Schmitt, op, cit,p71.)

([٥٢]) رائد حميد، مصدر سابق، ص١٩٨

([٥٣]) كوردولا دوريجي، مصدر سابق،ص ٥٤٤.

([٥٤]) طلال ياسين العيسى وعدي أحمد عناب، مصدر سابق، ص٨٩.

([٥٥]) المصدر نفسه.

(٥٦) انمار موسى جواد، حرب الفضاء الألكتروني(المفهوم الأدوات والتطبيقات)، مجلة العلوم القانونية والسياسية، المجلد٥، العدد٢، كلية القانون والعلوم السياسية -جامعة ديالى، ديالى، ٢٠١٦، ص١٣٢.

(٥٧) Jovan Kurbalija, State responsibility in the digital space, Swiss Review of International & European Law, issue 2,2016,p6, on the , done at 2020/9/25. link https://www.diplomacy.edu

(٥٨) مصطفى بن عصام نعوس، التنظيم الدولي للأنترنيت، اطروحة دكتوراه مقدمة الى مجلس كلية الحقوق-جامعة حلب، سوريا،٢٠١١، ص ص١٨٢.

(٥٩) جمال العظامات، جريمة العدوان في الهجمات الالكترونية في القانون الدولي العام، مجلة المنارة للدراسات القانونية والإدارية، المجلد٢١، العدد٤، مركز المنارة للدراسات والابحاث، المغرب، ٢٠١٥، ص٢٤.

(٦٠) الهجمات السيبرانية على ايران: ابعاد وتداعيات، مركز الامارات للسياسات، ابوظبي، ٢٠٢٠، مقال منشور
في شبكة الانترنيت على الرابط الالكتروني، https://epc.ae/ar ، تم الاطلاع، ٢٠٢٠/١٠/١.

المصادر
(Sources)

-المصادر العربية

اولا:- الكتب القانونية

I. خالد وليد محمود، الهجمات عبر الانترنيت: ساحة الصراع الالكتروني الجديدة، المركز العربي ودراسة السياسات، قطر، ٢٠١٣.
II. علي محمد كاظم الموسوي، المشاركة المباشرة في الهجمات السيبرانية، المؤسسة الحديثة للكتاب، لبنان، ٢٠١٩.

ثانيا:- الرسائل والاطاريح

I. حسام جاسم محمد أحمد الدليمي، التطور التكنولوجي واثره في سيادة الدول، رسالة ماجستير مقدمة الى مجلس كلية القانون والعلوم السياسية- جامعة الانبار، الانبار، ٢٠١٨.
II. مصطفى بن عصام نعوس، التنظيم الدولي للأنترنيت، اطروحة دكتوراه مقدمة الى مجلس كلية الحقوق-جامعة حلب، سوريا،٢٠١١.
III. ليث الدين صلاح حبيب، الحماية الدولية لضحايا النزاعات المسلحة من غير الأسرى، رسالة ماجستير مقدمة الى مجلس كلية القانون- جامعة بغداد، بغداد، ٢٠٠٦.
IV. رائد حميد صالح، اثر التطبيقات الرقمية على سيادة الدول، رسالة ماجستير مقدمة الى مجلس كلية الحقوق- جامعةالنهرين ، بغداد، ٢٠١٩.
V. مروة إبراهيم محمد، مبدأ الضرورة العسكرية في القانون الدولي الإنساني، رسالة ماجستير مقدمة الى مجلس كلية القانون- جامعة بغداد، بغداد،٢٠١٥.

ثالثاً:- البحوث والمجلات

I. أحمد عبيس نعمة الفتلاوي وزهراء عماد محمد، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، المجلد٤٤، العدد١، كلية القانون والعلوم السياسية –جامعة الكوفة، الكوفة، ٢٠٢٠.

II. أحمد عبيس نعمة الفتلاوي، بحث الهجمات السيبرانية:مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية ،المجلد ٨، العدد ٤، جامعة بابل، بابل، ٢٠١٦.
III. انمار موسى جواد، حرب الفضاء الألكتروني(المفهوم الأدوات والتطبيقات)، مجلة العلوم القانونية والسياسية، المجلد٥، العدد٢، كلية القانون والعلوم السياسية -جامعة ديالى، ديالى، ٢٠١٦.
IV. بن تغري موسى، الحرب السيبرانية والقانون الدولي الانساني، مجلة الاجتهاد القضائي، المجلد(١٢)، العدد(٢٢)، مخبر الاجتهاد القضائي على حركة التشريع، جامعة محمد خضير بكسرة، الجزائر، ٢٠٢٠، ص٢٠٩.
V. جمال العظامات، جريمة العدوان في الهجمات الالكترونية في القانون الدولي العام، مجلة المنارة للدراسات القانونية والإدارية، المجلد٢١، العدد٤، مركز المنارة للدراسات والابحاث، المغرب، ٢٠١٥.
VI. سلافة طارق الشعلان، تكييف استخدام الحرب الالكترونية في الزاعات المسلحة وفقاً للقانون الدولي الإنساني، مجلة الكوفة للعلوم القانونية والسياسية، المجلد١، العدد٢٦، كلية القانون جامعة الكوفة، الكوفة، ٢٠١٦.
VII. طلال ياسين العسي وعدي أحمد عناب، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الانسانية، المجلد١٩، العدد الاول، جامعة الزرقاء، الاردن، ٢٠١٩.
VIII. عادل عبد الصادق، اسلحة الفضاء الالكتروني في ضوء القانون الدولي الانساني، مكتبة الاسكندرية، وحدة الدراسات المستقبلية، مصر، ٢٠١٦.
IX. فاطم بيرم، السيادة الوطنية في ظل الفضاء السيبراني والتحولات الرقمية:الصين نموذجاً، المجلة الجزائرية للامن الانساني ، المجلد الخامس، العدد الاول ، مخبر الامن الانساني-جامعة باتنة، الجزائر، ٢٠٢٠، ص٧٩٨.
X. كوردولا دوريجي، لاتقترب من حدود الفضائي الالكتروني: الحرب الالكترونية والقانون الد.لي الانساني وحماية المدنيين، مختارات من المجلة الدولية للصليب الأحمر، المجلد٩٤، اللجنة الدولية للصليب الاحمر، جنيف،٢٠١٢.
XI. يحيى ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الانساني، المجلة القانونية، المجلد(٤)،العدد(٤)، كلية الحقوق- جامعة القاهرة(فرع الخرطوم)، مصر.

ثالثاً:- التقارير والوثائق الدولية

I. اتفاقية لاهاي للحرب البرية لعام ١٩٠٧.
II. البروتوكول الاضافي لعام ١٩٧٧.
III. دليل تالين ٢٠١٣.
IV. ميثاق الأمم المتحدة
V. -تقرير لجنة القانون الدولي ٢٠٠١، الدورة ٥٣ الوثيقة،

A/CN.4/SER.A/2001/ADD.IC.PART2

VI. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Sixty-eighth session, document (A/68/98),2013
VII. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of

International Security, General Assembly United Nations, decument A/70/174,2015.

-المصادر الاجنبية

I. Marie Baezner, Patrice Robin, Trend Analysis: Cyber Sovereignty and Data Sovereignty, Center for Security Studies (CSS), 2018.
II. Wolff Heintschel von Heinegg, Territorial Sovereignty and Neutrality in Cyberspace, International Law Studies ,U. S. Naval war college , Vol 89,2013.
III. Oona A. Hathaway, The Law of Cyber-Attack, Yale Law School, United States of America, Vol. 100:817, 2012.
IV. United Nations Audiovisual Library of International Law, General Assembly Resolution 3314, Defining aggression.
V. Antonio Cassese, The Martens Clause: Half a Loaf or Simply Pie in the Sky? , Vol. 11,2000.
VI. Michael N. Schmitt, In Defense of Due Diligence in Cyberspace, the yale law journal forum, N22, 2015.

-المواقع الالكترونية

I. الهجمات السيبرانية على ايران: ابعاد وتداعيات، مركز الامارات للسياسات، ابوظبي، ٢٠٢٠، مقال منشور في شبكة الانترنيت على الرابط الالكتروني، https://epc.ae/ar ، تم الاطلاع، ٢٠٢٠/١٠/١.
II. Jovan Kurbalija, State responsibility in the digital space, Swiss Review of International & European Law, issue 2,2016,p6, on the link https://www.diplomacy.edu , done at 2020/9/25.