جمهورية العراق

وزارة التعليم العالي والبحث العلمي

جامعة المستقبل

كلية القانون

المسؤولية القانونية عن الهجمات الالكترونية

بحث تقدمت به الطالبة (نور جاسم محمود)

الى مجلس كلية القانون جامعة المستقبل وهو جزء من نيل شهادة البكالوريوس في القانون

اشراف

م.م. رؤى خالد

1446هـ

2025م

بسم الله الرحمن الرحيم

﴿قَالَ إِنَّمَا ٱلۡعِلۡمُ عِندَ ٱللَّهِ وَأُبَلِّغُكُم مَّآ أُرۡسِلۡتُ بِهِۦ وَلَٰكِنِّيٓ أَرَىٰكُمۡ قَوۡمٗا تَجۡهَلُونَ ٢٣﴾

﴿الأَحْقَاف : ﴿﴿﴿

الاهداء

إلى صاحب السيرة العطرة، والفكر المُستنير؛

فلقد كان له الفضل الأوَّل في بلوغي التعليم العالي

(والدي الحبيب)، أطال الله في عُمره.

إلى من وضعتني على طريق الحياة، وجعلتني رابط الجأش،

وراعتني حتى صرت كبيرًا

(أمي الغالية)، حفظها الله

إلى إخوتي؛ من كان لهم بالغ الأثر في كثير من العقبات والصعاب.

إلى جميع أساتذتي الكرام؛ ممن لم يتوانوا في مد يد العون لي

أُهدي إليكم بحثي وثمرة تخرجي في القانون....

شكر وتقدير

الحمد لله رب العالمين الذي وفقنا وأعاننا على إنهاء هذا البحث والخروج به بهذه الصورة المتكاملة، فبالأمس القريب بدأنا مسيرتنا التعليمية ونحن نتحسس الطريق برهبة وارتباك، فرأينا أهدفًا ساميًة وحبًا وغاية تستحق السير لأجلها، وإن بحثنا يحمل في طياته طموح شباب يحلمون معهم احلاما كبيرا , وانطلاقًا من مبدأ أنه من لم يشكر المخلوق لم يشكر الخالق ، فإننا نتوجه بالشكر الجزيل للأستاذة (م.م. رؤى خالد) المشرفة على هذا البحث ونشكر جميع الأصدقاء والأحباب وكل من قدم لنا الدعم المادي أو المعنوي.

المقدمة

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 أن الدول تواجه مخاطر كبيرة في هذا الفضاء بسبب ما تتعرض 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.

إن الاستخدامات الواسعة للوسائل التكنولوجية الحديثة أدت إلى استحداث أمور جديدة كانت سبباً وبشكل مباشر في ظهور واستفحال نوع معين من الجرائم. هاته الجرائم التي انتشرت وتعددت صورها وازداد حجمها وتسارعت وتيرتها وسهل ارتكابها رغم اختلاف تسمياتها، فأصبحت تقاس مدة ارتكابها بالثواني، والأدهى أنها قد ترتكب في حضور المجني عليه دون علمه بحدوثها، فلم تعد الحدود الجغرافية ولا الحواجز الإدارية، ولا بعد المسافات واختلاف اللغات عائقاً أمام مرتكبيها، وباتت مخاطرها تهدد أمن المجتمعات وقيمها وشكل وجود جرائم إلكترونية بشكل مستمر ومتسارع تحديات كثيرة أمام النظم القانونية، الأمر الذي دفع الفقه والقضاء والباحثين القانونيين إلى البحث عن آليات مكافحة تكون قادرة على مجابهة هذه الظاهرة الإجرامية واحتوائها ومراعاة طبيعتها وخصوصيتها؛ لأنه ما لم نستطع تأمين بنيتنا التحتية ،الإلكترونية، وأمننا السيبراني، فإن كل ما يحتاجه المجرم الإلكتروني لتهديد

حياتنا الاجتماعية والاقتصادية والثقافية وحتى السياسية هي مجرد نقرات بسيطة على جهاز الحاسوب أو أي جهاز إلكتروني آخر، والاتصال عن طريق الإنترنت لتنفيذ جريمته لأنه من المرجح أن تصبح السيطرة على مصادر المعلومات ووسائل معالجتها أكثر أهمية من الموارد الأخرى الطبيعية منها أو حتى العسكرية، ويعد هذا الأمر أحد الأسباب التي تدفع الباحثين إلى إيجاد آليات ناجعة في مكافحة الجريمة الإلكترونية.

أهمية البحث :

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

هدف البحث:

إن البحث يهدف الى معرفة مدى انتشار الهجمات الالكترونية في العالم، والتي وأصبحت تمثل تهديداً للسلم الدولي، وأثارت نزعات دولية تمس سيادة وامن والدول ، وإن فقهاء القانون الدولي لم يتفقوا على آلية واضحة وصورة واحدة من هذه الهجمات ، كما ان آثار الهجمات الالكترونية لا تقل درجة قوته عن الهجوم المسلح لذا من الضروري مقارنته مع الهجوم المسلح المنصوص عليه في القانون الدولي بفرعيه المكتوب والعرفي للوصول إلى نتيجة واحدة بأن الهجمات الالكترونية محرمة دولياً.

مشكلة البحث:

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

منهجية البحث:

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

خطة البحث:

المطلب الأول: مفهوم الهجمات الإلكترونية

الفرع الأول: تعريف الهجمات الإلكترونية

الفرع الثاني: أسلحة الهجمات الإلكترونية

المطلب الثاني: المسؤولية الدولية عن اضرار الهجمات الإلكترونية في الفضاء الافتراضي

الفرع الأول: مدى انطباق شروط المسؤولية التقليدية على الهجمات الإلكترونية

الفرع الثاني: مدى انطباق شروط المسؤولية الحديثة على الهجمات الإلكترونية

ومن ثم الخاتمة والاستنتاجات والتوصيات.

المطلب الأول

مفهوم الهجمات الإلكترونية

لم تكن الهجمات الإلكترونية معروفة إلا في وقت قريب، ما يشكل إحدى أهم التحديات الراهنة التي يواجهها المختصون في القانون الدولي العام وبالخصوص في تحديد طبيعتها أو عناصرها، فضلًا عن نطاق هذه الهجمات في ضوء القانون الدولي الإنساني، وما يترتب عليها من تبعات المسؤولية الدولية الجنائية وما يزيد في اتساع التحدي الذي يواجهه المختصون في القانون الدولي العام والدولي الإنساني على وجه الخصوص، إنما يتجسد في الغموض الذي اكتنف مفهوم الهجمات الإلكترونية وعدم الاتفاق على تعريف محدد لها، يمكن الاستدلال في ضوئه لتنظيم استخدامها بالحظر أو التقييد لمواجهة عواقبها الخطرة على الصعيد الإنساني. [1]

الفرع الأول

تعريف الهجمات الإلكترونية

استخدمنا في هذه الدراسة مصطلح «الهجمات الإلكترونية» على عكس ما درج عليه البعض من المختصين، فمنهم من تبنى مصطلح الفضاء الإلكتروني بالاستناد إلى

---

[1])(ona` A Hathway, Rebecca Crootof, Philip Levtiz, aley Nix, Aileen Nowlan William Perdue and Julia Spiegel, «The Law of Cyber -Attack», California Law Review, 2012, p.7

المحيط الذي تجري فيه العمليات الإلكترونية الناشئة عن أداء أنظمة إلكترونية مهمتها متابعة وجمع المعلومات التي تعمل إلكترونيًا وتحليلها، ومن ثم اتخاذ إجراءات محددة لمهاجمتها عن طريق أنظمة الكترونية أخرى مخصصة لهذا الغرض [2] . وتبنى آخرون مصطلح الحرب الإلكترونية بالاستناد إلى إيديولوجية أمنية أو عسكرية، تضع منهجًا لتحقيق أهداف على الصعيد الأمني أو العسكري تجاه العدو المفترض. [3]

أما البعض الآخر فاختار مصطلح الهجمات الإلكترونية، كوصف واقعي يجمع بين كل ما ذكر آنفا [4]، فهو تصرُّف يدور في عالم افتراضي قائم على استخدام بيانات رقمية ووسائل اتصال تعمل إلكترونيًا، ومن ثم تطور ليتضمن مفهومًا أوسع يقوم على تحقيق أهداف عسكرية أو أمنية ملموسة ومباشرة، جراء اختراق مواقع إلكترونية حساسة، عادةً ما تقوم بوظائف تصنف بأنها ذات أولوية، كأنظمة حماية محطات الطاقة النووية أو الكهربائية أو المطارات ووسائل النقل الأخرى[5] لقد تعرض مصطلح الهجمات الإلكترونية إلى تعاريف متعددة ومن زوايا مختلفة، ومن تلك التعاريف ما ذهب إليه خبراء ومختصون في القانون الدولي الإنساني، من أهمهم:

فيورتس (Fuentes) حيث عرفها بالقول: هجوم عبر الإنترنت يقوم على التسلل إلى مواقع إلكترونية غير مرخص بالدخول إليها، بهدف تعطيل أو إتلاف البيانات

---

[2])(James A. Lewis, «Sovereignty and the role of Government in Cyberspace>>, Center for Strategic and International Studies Journal, Spring Summer, Vol : XVI, Issue II, 2010, P.56.

[3])(Shin, Beomchul,» The Cyber Warfare and the Right of Self-Defense: Legal Perspectives and the Case of the United States, IFANS, Vol. 19, No1, June 2011, p.104.

[4])(Scoot. j .Shckelford, "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem", University of Cambridge, Dept of politicos and International STUDIES, Cambridge, UK,2009.p.201

[5])(K .Saalbach, "Cyber War, Methods and Practice", Version 9.0, University of Osnabruck-17 Jun 2014, p.6

المتوفرة فيها أو الاستحواذ عليها، وهي عبارة عن سلسلة هجمات إلكترونية تقوم بها دولة ضد أخرى. [6]

– شميت (Schmitt) فقد عرفها بأنها مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نظم المعلومات المعادية بهدف التأثير والإضرار بها ، وفي الوقت نفسه للدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة . [7]

– ماركو روسيني (marco roscini عرفها بأنها: تطويع الإمكانيات الإلكترونية العسكرية لأجل التأثير في مواقع إلكترونية أخرى وتعطيلها أو تدميرها سواء أكانت تقدم خدمات مدنية أم عسكرية . [8]

– أما حلف الناتو فقد عرفها في المادة (٣٠) من دليل تالين بأنها عملية إلكترونية هجومية أو دفاعية يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الإضرار بأعيان أو تدميرها [9]

– ومن وجهة نظرنا، يمكن تعريف الهجمات الإلكترونية بأنها عمليات لإيقاع الفوضى في المعلومات الموجودة في أجهزة الحاسوب أو شبكات الحاسوب أو نفيها أو الانتقاص من شأنها أو تدميرها.

وفي هذا الشأن نطرح تساؤلاً له صلة باستخدام التقنيات الإلكترونية في الإطار العسكري: هل يمكن عد النشاط الإلكتروني إذا استخدم لأغراض عسكرية هجومًا

---

[6])(Michael S .Fuertes, «Cyber warfare, Unjust Actins in a just War», Florida International University, Full 2013, p.1.

[7])(Michael N .Schmitt «Computer Network Attack and the Use of Force in International Law through on a Normative», The Colombia Journal of Transitional Law, 1999, Vol.27, No.885-937, p.7.

[8])(Marco Roscini, «World Wide Warfare - Jus ad bellum and the use of Cyber Force» ,Max Planck Yearbook of United Nations Law, Volume 14,2010,p.91

[9])(Michael N.Schmitt, Tallinn Manual, op.cit.p.92.

بالمعنى الاصطلاحي ؟ وهل هو وسيلة أم طريقة قتالية؟ وبعبارة أخرى هل يمكن عده سلاحًا؟ وإذا كان كذلك، هل هو سلاح تقليدي؟

بداية لا بد من تعريف الهجوم المسلح ، إذ ورد في الفقرة (١) من المادة ٤٩من البروتوكول الإضافي الأول لعام ١٩٧٧ ، الملحق باتفاقيات جنيف الأربع لعام ١٩٤٩ بالنص: «تعني الهجمات أعمال العنف الهجومية والدفاعية ضد الخصم» [10] ، ومن قراءة النص المتقدم وتطبيقه على الهجوم الإلكتروني، فالظاهر أنه بعيد عن مصطلح الهجوم الوارد في الفقرة (١) سالفة الذكر لكون الهجوم الإلكتروني لا يصاحب أعمال عنف مسلح ملموسة ومباشرة أثناء الاستخدام. ولا يمكن القبول بفرضية أن كل تصرف إلكتروني ينشأ عنه قرصنة أو اختراق لبيانات إلكترونية هو بمثابة أعمال عنف مسلح، وعلينا أن نسأل هل الفرضية المتقدمة مقنعة في ضوء الآثار التي تتسبب بها الهجمات الإلكترونية على حياة الإنسان بالذات؟

إن قراءة نص الفقرة (١) من المادة (٤٩) – سالفة الذكر، بمعزل عن باقي أحكام البروتوكول الإضافي الأول، هو أمر غير صائب، بدليل تكشف عنه أحكام البروتوكول نفسه، إذ إن أعمال العنف المسلح، يحكمها أمران: إما أن تكون مباشرة وتؤدي بطبيعتها إلى إلحاق أذى مادي في الأعيان العسكرية أو المدنية، أو غير مباشرة بعد وقوع الهجوم أيا كانت الوسيلة أو الطريقة. [11]

وفي ضوء ما تقدم، فإننا نرى أن الأصح هو التركيز على نوع الآثار ،وجسامتها، فكلما ثبت أن المدنيين على سبيل المثال سيتأثرون جراء أ نشاط إلكتروني عسكري كاستهداف منظومة السيطرة والتحكم الإلكترونية لمفاعل نووي لتوليد الطاقة

---

[10]) (ICRC, «Exploring humanitarian law: IHL Guide, A legal manual for EHL teacher», ICRC, Geneva, January 2009.p.40.

[11]()د. حسام عبد الأمير خلف البعد الجديد الخامس في النزاعات المسلحة - الفضاء الإلكتروني»، مجلة كلية الحقوق جامعة النهرين بغداد المجلد ١٨ ، ٢٠١٦، ص ١٣٣ - ١٣٤ .

الكهربائية، سيعني أن وصف (هجوم) متحقق فيه. ولا أدل على ذلك ممَّا أشارت إليه الفقرة (٢) من المادة (٥١) من البروتوكول الإضافي الأول لعام ١٩٧٧ ، بالنص: «لا يجوز أن يكون السكان المدنيون بوصفهم هذا وكذا الأشخاص المدنيون محلا للهجوم. وتحظر أعمال العنف أو التهديد به الرامية أساسًا إلى بث الذعر بين السكان المدنيين. [12]

أما بخصوص تعريف وسائل القتال وطرائقها فقد عرفها موريس « MURICE AUBERT» بالقول: «وسائل القتال هي الأسلحة ذاتها، بينما طرائقها فتعني كيفية استخدامها»[13] . فيما تعرف الأسلحة التقليدية بأنها : أسلحة ليست أسلحة تدمير شامل جرى فهمها على أنها تتضمن أجهزة مصممة للقتل أو الجرح أو إلحاق الضرر، عادة لا حصرا، بواسطة تأثيرات المواد شديدة الانفجار أو الطاقة الحركية أو العوامل المحرقة ونظم إيصالها» [14]. وقد أطلق البعض من المختصين ومنهم هاري رادويج (4) «HARRY D. RADUEGE مصطلح التعطيل الشامل «MASS DISRUPTION ، لوصف الهجوم الإلكتروني وهو يُقابل مصطلح الدمار الشامل (MASS DESTRUCTION المعروفة به الأسلحة النووية والكيميائية والبيولوجية وبرأينا، أن للوصف مغزى قانونيًا وفنيًا في آن واحد، إذ يعكس هدف الهجوم الإلكتروني وهو التعطيل التام أو الجزئي للمنظومات الإلكترونية العسكرية أو المدنية للعدو المفترض، فضلًا عن التأثير على مجمل العمليات العسكرية التقليدية الأخرى.

---

[12])(ICRC," Exploring humanitarian law: IHL Guide, op.cit, p. 41

[13])(Murice Abuert, «The ICRC and the problem of excessively injuries or indiscriminate weapons», Extract print from ICRC, No.279, Nov-Dec, 1990, p.483, footnote.18

[14])ستيف توليو وتوماس شمالبرغر ، قاموس مصطلحات تحديد الأسلحة ونزع السلاح وبناء الثقة، معهد الأمم المتحدة لبحوث نزع السلاح، منشورات الأمم المتحدة، ٢٠٠٣، ص ٣٧

ومن خلال قراءة التعاريف المتقدمة ومضامينها، ومقارنتها مع خصائص الهجمات الإلكترونية يتضح لنا أنها وسيلة وطريقة في الوقت نفسه، وبعبارة أخرى يعتمد ذلك على الهدف من استخدامها فقد تسهم في توجيه العمليات العسكرية الأخرى كالصواريخ بعيدة المدى أو الطائرات بدون طيار «DRAWN»، لتحديد أهداف عسكرية منتخبة وتدميرها أو لتعطيل أجهزة الكشف المبكر للهجمات التي يقوم بها سلاح جو معاد أو وقف عمليات الاتصال في المطارات العسكرية أو المدنية، وهو ما تتصف به الهجمات الإلكترونية.

الفرع الثاني

أسلحة الهجمات الإلكترونية

إن الأسلحة الإلكترونية أصبحت تستخدم بشكل متزايد ضد أهداف عسكرية ومدنية، ومن المهم معرفة أن الأسلحة الإلكترونية تأتي في الواقع في شكلين مختلفين: الأول هو طريقة التسليم الفعلي للأسلحة، وهو جهاز قياسي مستخدم فعليًا بمثابة البوابة

الإلكترونية التي يتم من خلالها تنسيق الهجمات الإلكترونية والأسلحة الإلكترونية التي تم تأسيسها .[15]

أما النوع الثاني من الأسلحة الإلكترونية هو عنصر الفضاء الإلكتروني. هذه الأسلحة غير الملموسة يحتمل أن تكون مؤلفة من برامج الحاسوب، شبكة الفيروسات، وقيادة عمليات رقمية على الرغم من التطور المستمر، فإن الأنواع الأكثر شيوعًا من الأسلحة الإلكترونية، بما في ذلك وظائفها الأساسية، والقدرات، والاستخدامات، ترد أدناه [16]

اولاً: الحرمان من الخدمة

هجوم الحرمان من الخدمة DDOS_ DISTRIBUTED DENIAL OF SERVICE، يعرف بأنه: «اعتداء على الشبكة من خلال إغراقها بسيل من البيانات غير اللازمة أو طلبات إضافية ما يسبب بطء الخدمات أو توقفها تماما». عموما، هجمات DDOS، تعمل من خلال شلّ موارد الموقع الإلكتروني على شبكة الإنترنت أو شبكة الحاسوب، وجعلها غير صالحة للاستعمال من قبل الأكثرية المستعملة لهذا المورد مع كمية هائلة من طلبات الحصول على المعلومات؛ مما يؤدي إلى عدم القدرة على الاستجابة للمعلومات المشروعة وطلبات الحصول على البيانات. [17]بالإضافة إلى ذلك، هناك هجوم حرمان دائم من الخدمة PERMANENT

---

[15]()يقصد بذلك أنه يأخذ الأجهزة الموجودة داخل العالم المادي من واقع الحياة اليومية، مثل: أجهزة الحاسوب، وأجهزة المودم ، وكابلات التوصيل لبناء ونشر هجوم عبر الإنترنت. وثمة طريقة لمنع مثل هذه الهجمات سيكون تدمير هذه الأجهزة المادية التي هي في مجال الفضاء الإلكتروني للمزيد من المعلومات، انظر: د. منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، القاهرة ٢٠١٦، ص ٧٠٦٨.

[16])(Bradley Raboin, Corresponding Evolution: International Law and the Emergence of Cyber Warfare, Journal of the National Association of Administrative Law Judiciary -31-2,Fall 2011, p 610_611.

[17]()خالد وليد محمود الهجمات عبر الإنترنت: ساحة الصراع الإلكترونية الجديدة، المركز العربي للأبحاث ودراسة السياسات الدوحة، قطر، ٢٠١٣، ص ٩.

PDDOS (DISTRIBUTED DENIAL OF SERVICE)، هذا الهجوم يسبب أضرارا جسيمة في النظام، الأمر الذي يتطلب استبدال أو إعادة تثبيت الأجهزة، خلافًا لهجوم DDOS، الذي يُستخدم لتخريب خدمة أو موقع، أو كغطاء للبرامج الضارة، فإن هجوم PDDOS يهدف بشكل محض إلى تخريب الأجهزة . [18]

ثانياً: البرامج الخبيثة

البرامج الخبيثة، أو البرمجيات الخبيثة [19] ، تعمل عادة عن طريق (تعطيل وظائف الحاسوب العادية، أو عن طريق فتح باب خلفي لمهاجم بعيد من أجل السيطرة على جهاز الحاسوب . [20]

الفيروسات، هي الشكل الأكثر شيوعًا من البرامج الخبيثة، قد تعمل لحذف ملفات معينة في الحاسوب أو جعل مثل هذه الملفات غير صالحة للاستعمال. على وجه التحديد، الفيروس يعلق نفسه على برنامج حاسوب أو ملف وينتشر من جهاز حاسوب إلى آخر ، والانتقال عبر شبكات الحاسوب عن طريق التكرار الذاتي. بالإضافة إلى ذلك، أن الفيروس عادة يحمل (حمولة) التي تمثل أحد الآثار الجانبية للفيروس، وعادة يعمل على إفساد أو تدمير بيانات الحاسوب على جهاز الحاسوب المصاب. الفيروسات عادة لديها القدرة على البقاء بسرية موجودة في جهاز

---

[18](SCHAAP, ARIE J, CYBER WARFARE OPERATIONS: DEVELOPMENT

[19]()تعود فكرة إنشاء البرامج الخبيثة إلى عالم الرياضيات والمهندس المبتكر لأنظمة الحوسبة «جون فون نيومان»؛ حيث قام عام ١٩٤٩ بتقديم سلسلة من المحاضرات النظرية في جامعة الينوي دعا فيها إلى إنشاء منظمة معقدة للتشغيل الذاتي؛ حيث تستكشف إمكانية تطوير الآلات ذاتية التكرار. فون نيومان تصور الآلات التي يمكن أن تبني نسخ ذاتية، وهي تعتبر مقدمة لنظرية فيروس الحاسوب إن تكرار الذات هو السمة المميزة لفيروسات الحاسوب والديدان، فمن خلال تكرار الذات، يتم الانتشار في أجهزة الحاسوب أضعافا مضاعفة
انظر المصدر : Michael Gervais, Cyber Attacks and the Laws of War, berkeley journal of international law, Vol. 30:2, 2012.p.525.
وانظر أيضًا: جون باسيت، الحروب المستقبلية في القرن الحادي والعشرين ترجمة أحمد ياسين، الطبعة الأولى، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، ٢٠١٤، ص

[20](SCHAAP, ARIE J... op.cit.,p

الحاسوب المصاب، ليصبح مدمرًا فقط عند تشغيل المستخدم أو يفتح البرنامج الذي قد تم إدراج البرنامج الخبيث فيه . [21]

النموذج المشترك الآخر من البرامج الخبيثة هي الدودة COMPUTER WORM ، التي تؤدي وظائف مماثلة عن طريق الانتشار من حاسوب إلى آخر، وإصابة – في نهاية المطاف – شبكة الحاسوب بأكملها. مع ذلك، الدودة تختلف عن الفيروس بكونها أسرع منه، كما أنها قادرة على حد سواء الانتقال عبر نظام الحاسوب دون مساعدة من مستخدمي الحاسوب، وأنها قادرة على تكرار نفسها مباشرة آلاف المرات داخل جهاز حاسوب واحد الديدان تميل إلى أن تستهلك كميات هائلة من الذاكرة، ونتيجة لذلك، أجهزة الحاسوب المصابة ، والشبكات غالبًا ما تصبح لا تستجيب. ومع التطورات الأخيرة في مجال الإنترنت الديدان قد تمنح الآن الأفراد نفقاً في أنظمة الحاسوب والسيطرة من بعيد على الحاسوب المصاب. [22]

ثالثا: القنابل المنطقية

القنابل المنطقية، هي نوع أكثر تقدما من البرامج الخبيثة، وهي عبارة عن تعليمات برمجية ضارة مصممة بحيث تعمل عند حدوث أحداث معينة أو تحت ظروف معينة أو لدى تنفيذ أمر معين، وتؤدي إلى تخريب أو مسح بيانات أو تعطيل النظام) . القنبلة المنطقية يمكن أن تبقى نائمة لفترات طويلة من الزمن لم تكن متصورة ومن ثم يتم تفعيلها، مما يجعل آثارها أكثر بكثير من أن تكون واسعة الانتشار. بمجرد تفعيلها، والقنبلة المنطقية قد تسبب أضرارا بالغة لجهاز الحاسوب المصاب؛ مما

---

[21])(Bradley Raboin...op.cit.p.613. And, SCHAAP, ARIE J... op.cit,p.135-136.

[22]()د. عادل عبد الصادق الإرهاب الإلكتروني والقوة في العلاقات الدولية: نمط جديد وتحديات مختلفة، مركز الأهرام للدراسات السياسية والاستراتيجية، الطبعة الأولى، القاهرة، ٢٠٠٩ ، ص ١٢٦____١٢٨ .

يجعله غير صالح للاستعمال تمامًا، وحذف بيانات محددة، أو حتى تعمل لتنشيط أكثر تعقيدا لهجوم . [23] DDOS

رابعاً: برامج الخداع

تعرف أيضًا باسم انتحال العنوان آي بي SPOOFING IP ADRESS، وهو نوع من الاختطاف التقني الذي يسمح للمخترق المستخدم تشغيل الحاسوب في حين يظهر كمضيف موثوق به. أي إنه يؤدي إلى تضليل مستقبل المعلومات حيث يبدو أنها مرسلة من جهة معينة في حين أنها في الواقع مرسلة من جهة أخرى، الأمر الذي يسمح بدخول المعلومة إلى الشبكة ويجعل مستقبلها يتعامل معها دون معرفة هوية مرسلها الحقيقي[24]، فمن خلال إخفاء الهوية الحقيقية، يمكن للقراصنة الوصول إلى شبكات الحاسوب وموارد الشبكة. ففي اللحظة التي يتفاعل بها المستخدم مع أي من محتويات صفحة الويب الاحتيالية، يكسب المخترق اختطاف القدرة على الوصول إلشبكة المعلومات الحساسة أو ميزات البرامج الأساسية للحاسوب. [25]

---

[23])(Bradley Raboin...op.cit.p.614.

[24]()د. فاتن سعيد بامفلح حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى، ص ١٦ . انظر الموقع التالي: ttp://www.kau.edu.sa/Files/0012433/Researches/56927_27244.pdf.

[25])(SCHAAP, ARIE J...op.cit., p.132. And. Bradley Raboin...op.cit.p.615

المطلب الثاني

المسؤولية الدولية عن اضرار الهجمات الإلكترونية في الفضاء الافتراضي

بعد ان بينا الهجمات الالكترونية ومدى انطباق المبادئ الرئيسة في القانون الدولي العام والإنساني عليها بقى لدينا م اهو أهم وهو المسؤولية الدولية المترتبة في إطار الفضاء الافتراضي وذلك من خلال بيان مدى انطباق شروط المسؤولية التقليدية والحديثة على الهجمات الإلكترونية؟ هذا ما سنتناوله في هذا المبحث، في مطلبين، سيكون الأول لمدى انطباق شروط المسؤولية التقليدية على الهجمات الإلكترونية ، وسنخصص الثاني لمدى انطباق شروط المسؤولية الحديثة على الهجمات الإلكترونية .

الفرع الأول

مدى انطباق شروط المسؤولية التقليدية على الهجمات الإلكترونية

ان لتكنولوجيا المعلومات والاتصالات و تشكيلها لبيئة الأمن الدولي فائدة في الجوانب الاقتصادية والإجتماعية وتيسير أمور الدولة، فقد تستخدم لإغراض لا تتوافق مع السلم والامن الدوليين، فزادت مخاطر استخدامها في السنوات الاخيرة مما ادى إلى زيادة الحاجة إلى التعاون لمواجهة اضرارها ومعرفة ماهي مسؤولية الدولة

في هذا الفضاء [26] ، فإذا كان امر اثبات مسؤولية الدول يسير في حالة الحرب لأن الهجوم إذا كان منصباً على تعطيل وسائل اتصال عسكرية أو مدنية في وقت النزاع المسلح فالامر هنا يخضع للاحكام العامة للقانون الدولي الإنساني التي تتعلق بالعمليات القتالية وتصرفات المقاتلين [27] ، 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 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 وفقاً للأتي:-

أولاً:- خرق التزام دولي (الفعل غير المشروع دوليا تسأل الدولة على اساس خرق التزام دولي مفروض عليها، ومن أهم هذه الإلتزامات ذات الصلة بموضوع البحث هي:

1- الإلتزام بعدم التدخل في الشؤون الداخلية للدول: ان مبدأ عدم التدخل من ١- المبادئ الأساسية للأمم المتحدة وهو ضمانة من ضمانات سيادة الدولة وورد ذكره في المادة (٢) فقرة (٧) من ميثاق الأمم المتحدة، إذ نصت على انه ليس في هذا الميثاق ما يسمح للأمم المتحدة ان تتدخل في الشؤون التي تكون من صميم السلطان الداخلي لدولة ما .. وان مسؤولية الدولة حيال دورها في التدخل يضبطه امرين الأول

---

[26]()أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مصدر سابق، ص ٦٤٢.

[27]()علي محمد كاظم الموسوي، المشاركة المباشرة في الهجمات السيبرانية، المؤسسة الحديثة للكتاب، لبنان، ٢٠١٩، ص٢

ما ورد في المادة (٤) [28]من مسودة لجنة القانون الدولي عن مسؤولية الدول عن الأفعال غير المشروعة والتي تناولت مسؤولية الدولة عن التصرفات الدولية الخاطئة الصادرة من سلطاتها التشريعية والتنفيذية والقضائية، والمادة (٨)[29] 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 الأمريكية 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)[30]

---

[28]()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 أم جهاز من أجهزة وحدة إقليمية من وحدات الدولة، ٢- يشمل الجهاز أي شخص أو كيان له ذلك المركز وفقاً للقانون الداخلي للدولة

[29]()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 تصرف شخص أو مجموعة أشخاص إذا كان الشخص أو مجمو عة الأشخاص يتصرفون في الواقع بناء على تعليمات تلك الدولة أو بتوجيهات منها أو تحت رقابتها لدى القيام بذلك التصرف

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

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 (أو الشاملة 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) [31]

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 بالتزام المنع الإلتزام ببذل العناية الواجبة) :-

يقصد بهذا الإلتزام هو (على الدولة ان تمنع استخدام اراضيها بما يتعارض مع حقوق الدول الاخرى وهذا التزام عرفي وارد في المبدأ (٢١) من إعلان استوكهولم وتم تدوينه في تقرير لجنة القانون الدولي في المسؤولية عن أعمال لا يحظرها 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

[31]()طلال ياسين العسى وعدي أحمد عناب، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الانسانية، المجلد ١٩ ، العدد الاول، جامعة الزرقاء، الاردن، ٢٠١٩، ص٨٨.

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 [32]. 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 يقاوم 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 التزام العناية الواجبة فيما يتعلق بالبنى التحتية السيبرانية والأنشطة المنبعثة من اراضيها أو التي قد تمر بها، ويكون القائم بها جهات فاعلة غير حكومية [33]) ، و تم التاكيد على هذا الإلتزام في حكومية[34]، 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 تتعاون في وضع وتطبيق تدابير لزيادة الأمن والاستقرار.. وعليها منع استخدام

---

[32]()تقرير لجنة القانون الدولي لعام (٢٠٠١، مصدر سابق، ص١٩٣.

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

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

تلكنولوجيا الاتصالات إذا كانت ضارة أو قد تشكل تهديد للسلم والأمن الدوليين) [35] و هذا 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) [36] ، 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 لا يعني 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 ما يمكن لمنع هذه الهجمات.[37]

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 لكى يكون خرق للالتزام ام لا (٥) أما فيما يتعلق بالضرر كأحد سمات التزام العناية الواجبة، فحتى تكون الدولة مسؤولة عن مخالفة

---

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

[36]()رائد ،حميد مصدر سابق، ص١٩٢.

[37]()سلافة طارق الشعلان تكييف استخدام الحرب الالكترونية في الزاعات المسلحة وفقاً للقانون الدولي الإنساني، مجلة الكوفة للعلوم القانونية والسياسية، المجلد ١ ، العدد ٢٦ ، كلية القانون جامعة الكوفة، الكوفة، ٢٠١٦، ص ٢٥.

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 الكمبيوتر والذي يسبب عواقب وخيمة إذا تعطلت تلك النشاطات. [38]

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 التزام 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

لا يكفي 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 أن نصنف هل هذه الهجمة هي نزاع مسلح دولي ام لا، وعلى الرغم من ذلك فان هذا التحدي يتعلق بالوقائع لا بالناحية 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

---

[38]()رائد ،حميد مصدر سابق، ص١٩٨

معينة، فتسند العملية للدولة من خلال هذا الافتراض، خاصة وان قواعد القانون الدولي تتضمن التزام بان الدولة يجب عليها ان لا تسمح ، عن علم، باستخدام اراضيها للقيام بافعال تتعارض مع حقوق دولة اخرى، لكن هذا النهج يرد عليه اعتراضين وهما:- [39]

الأول: ان قواعد القانون الدولي القائمة لاتؤيد هذا الافتراض، ومثال ذلك ان المواد المتعلقة بمسؤولية الدول عن الافعال غير المشروعة دولياً لا تتضمن 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 التخفى تحت هوية مختلفة في الفضاء الافتراضي، فأن هذا سيلقي عبء كبير للغاية على الحكومات من ناحية تحملها مسؤولية جميع العمليات التي تطلق من اجهزة الكمبيوتر الخاصة بها دون اي دليل اخر. ومن ناحية اخرى، تجدر

---

[39]()كوردولا دوريجي، لا تقترب من حدود فضائي الالكتروني: الحرب الالكترونية والقانون الدولي الانساني وحماية المدنيين مختارات من المجلة الدولية للصليب الأحمر، المجلد ٩٤ ، اللجنة الدولية للصليب الأحمر، جنيف، ٢٠١٢ ، ص ٥٤٢ .

الاشارة إلى أن 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. [40]

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 . [41]

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،

---

[40]()طلال ياسين العسي وعدي أحمد ،عناب، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الانسانية، المجلد ١٩، العدد الاول، جامعة الزرقاء، الاردن، ٢٠١٩

[41]() المصدر السابق ، ص38

لكن وان كان صعبا انما هو ليس مستحيلا فيمكن تتبع عناوين (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 بالأمر السهل لانها قد تصل إلى جهاز خادم لا يتعاون 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. [42]

الفرع الثاني

مدى انطباق شروط المسؤولية الحديثة على الهجمات الإلكترونية

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؟

بداية اخذ مشروع لجنة القانون الدولي في تدوينه للمسؤولية عن أعمال لا يحظرها 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

---

[42]()انمار موسى جواد، حرب الفضاء الألكتروني المفهوم الأدوات والتطبيقات)، مجلة العلوم القانونية والسياسية، المجلده ، العدد ٢ ، كلية القانون والعلوم السياسية - جامعة ديالي ديالي ٢٠١٦، ص ١٣٢.

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. [43]

أما فيما يخص العلاقة بين الفضاء الخارجي والافتراضي، فأن كل من الفضائين يختلفان بشكل واضح، خاصة 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.[44]

---

[43])(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 tps://www.diplomacy.edu

[44])مصطفى بن عصام نعوس، التنظيم الدولي للأنترنيت، اطروحة دكتوراه مقدمة الى مجلس كلية الحقوق - جامعة حلب سوريا، ٢٠١١، ص ص ١٨٢.

من خلال ماتم ذكره والتشابه بين الأنشطة التي ذكرتها لجنة القانون الدولي في تقرير المسؤولية عن افعال لا يحظرها 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 أن 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. [45]

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 فى الاضرار العابرة للحدود واضرار البنى التحتية للدولة التي تعرضت للهجوم ومن ثم فإذا تحققت هذه الشروط في الأنشطة البيئية أو الفضاء الخارجي،

---

[45]()جمال العظامات جريمة العدوان في الهجمات الالكترونية في القانون الدولي العام، مجلة المنارة للدراسات القانونية والإدارية، المجلد ٢١ ، العدد ٤ ، مركز المنارة للدراسات والابحاث المغرب، ٢٠١٥، ص ٢٤.

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 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 [46]، هذا وللعلم فأن الهجمات المذكورة ليست الوحيدة في العالم الافتراضي لكنها الأهم والاشهر.

الخاتمة

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 وعلامات الاستفهام على المستوى الدولي سواء أكان القائم بها دولة أم جهات فاعلة من غير الدول، لذلك حاولنا تسليط الضوء على أهم المسائل التي تدور حولها علامات الاستفهام في هذا الخصوص فبينا ماهي الهجمات الإلكترونية وتكييفها القانوني وماهي المسؤولية المترتبة عليها، وتوصلنا إلى جملة من الاستنتاجات والمقترحات وهي:

أولاً: الاستنتاجات

---

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

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، مما يسبب 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 الأمور 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: التوصيات

1- الدعوة الى عقد اتفاقية دولية متعددة الاطراف لتنظيم الهجمات الإلكترونية وتقييدها لتحقيق الأمن 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.

3- 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 لا تعرف الحدود.

المصادر

1. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مصدر سابق، ص ٦٤٢.
2. انمار موسى جواد، حرب الفضاء الألكتروني المفهوم الأدوات والتطبيقات)، مجلة العلوم القانونية والسياسية، المجلده ، العدد ٢ ، كلية القانون والعلوم السياسية – جامعة ديالي ديالي ٢٠١٦، ص ١٣٢.

3. جمال العظامات جريمة العدوان في الهجمات الالكترونية في القانون الدولي العام، مجلة المنارة للدراسات القانونية والإدارية، المجلد ٢١ ، العدد ٤ ، مركز المنارة للدراسات والابحاث المغرب، ٢٠١٥، ص ٢٤.
4. جون باسيت، الحروب المستقبلية في القرن الحادي والعشرين ترجمة أحمد ياسين، الطبعة الأولى، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، ٢٠١٤،
5. خالد وليد محمود الهجمات عبر الإنترنت: ساحة الصراع الإلكترونية الجديدة، المركز العربي للأبحاث ودراسة السياسات الدوحة، قطر، ٢٠١٣، ص ٩.
6. د. حسام عبد الأمير خلف البعد الجديد الخامس في النزاعات المسلحة – الفضاء الإلكتروني»، مجلة كلية الحقوق جامعة النهرين بغداد المجلد ١٨ ، ٢٠١٦، ص ١٣٣ – ١٣٤ .
7. د. عادل عبد الصادق الإرهاب الإلكتروني والقوة في العلاقات الدولية: نمط جديد وتحديات مختلفة، مركز الأهرام للدراسات السياسية والاستراتيجية، الطبعة الأولى، القاهرة، ٢٠٠٩ ، ص ١٢٦_____١٢٨ .
8. د. فاتن سعيد بامفلح حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى، ص ١٦ . انظر الموقع التالي: ttp://www.kau.edu.sa/Files/0012433/Researches/56927_ .27244.pdf
9. د. منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، القاهرة ٢٠١٦، ص ٧٠٦٨.
10. رائد حميد صالح اثر التطبيقات الرقمية على سيادة الدول، رسالة ماجستير مقدمة الى مجلس كلية الحقوق جامعة النهرين ، بغداد، ٢٠١٩، ص١٥٣

11. ستيف توليو وتوماس شمالبرغر ، قاموس مصطلحات تحديد الأسلحة ونزع السلاح وبناء الثقة، معهد الأمم المتحدة لبحوث نزع السلاح، منشورات الأمم المتحدة، ٢٠٠٣، ص ٣٧

12. سلافة طارق الشعلان تكييف استخدام الحرب الالكترونية في الزاعات المسلحة وفقاً للقانون الدولي الإنساني، مجلة الكوفة للعلوم القانونية والسياسية، المجلد ١ ، العدد ٢٦ ، كلية القانون جامعة الكوفة، الكوفة، ٢٠١٦، ص ٢٥.

13. طلال ياسين العسى وعدي أحمد عناب، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الانسانية، المجلد ١٩ ، العدد الاول، جامعة الزرقاء، الاردن، ٢٠١٩، ص٨٨.

14. طلال ياسين العسي وعدي أحمد ،عناب، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الانسانية، المجلد ١٩، العدد الاول، جامعة الزرقاء، الاردن، ٢٠١٩

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

16. كوردولا دوريجي، لا تقترب من حدود فضائي الالكتروني: الحرب الالكترونية والقانون الدولي الانساني وحماية المدنيين مختارات من المجلة الدولية للصليب الأحمر، المجلد ٩٤ ، اللجنة الدولية للصليب الأحمر، جنيف، ٢٠١٢ ، ص ٥٤٢ .

17. مصطفى بن عصام نعوس، التنظيم الدولي للأنترنيت، اطروحة دكتوراه مقدمة الى مجلس كلية الحقوق – جامعة حلب سوريا، ٢٠١١، ص ص ١٨٢.

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

19. Bradley Raboin, Corresponding Evolution: International Law and the Emergence of Cyber Warfare, Journal of the National Association of Administrative Law Judiciary -31-2,Fall 2011, p 610_611.
20. Bradley Raboin...op.cit.p.613. And, SCHAAP, ARIE J... op.cit,p.135-136
21. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, General Assembly Nations, United decument .A/70/174,2015
22. ICRC, «Exploring humanitarian law: IHL Guide, A legal manual for EHL teacher», ICRC, Geneva, January 2009.p.40.
23. ICRC," Exploring humanitarian law: IHL Guide, op.cit, p. 41
24. James A. Lewis, «Sovereignty and the role of Government in Cyberspace>>, Center for Strategic and International Studies Journal, Spring Summer, Vol : XVI, Issue II, 2010, P.56.
25. 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 tps://www.diplomacy.edu

26. K .Saalbach, "Cyber War, Methods and Practice", Version 9.0, University of Osnabruck-17 Jun 2014, p.6
27. Marco Roscini, «World Wide Warfare - Jus ad bellum and the use of Cyber Force» ,Max Planck Yearbook of United Nations Law, Volume 14,2010,p.91
28. Michael Gervais, Cyber Attacks and the Laws of War, berkeley journal of international law, Vol. 30:2, 2012.p.525.
29. Michael N .Schmitt «Computer Network Attack and the Use of Force in International Law through on a Normative», The Colombia Journal of Transitional Law, 1999, Vol.27, No.885-937, p.7.
30. Michael N. Schmitt, In Defense of Due Diligence in Cyberspace, the yale law journal forum, N22, 2015,
31. Michael S .Fuertes, «Cyber warfare, Unjust Actins in a just War», Florida International University, Full 2013, p.1.
32. Murice Abuert, «The ICRC and the problem of excessively injuries or indiscriminate weapons», Extract print from ICRC, No.279, Nov-Dec, 1990, p.483, footnote.18
33. ona` A Hathway, Rebecca Crootof, Philip Levtiz, aley Nix, Aileen Nowlan William Perdue and Julia Spiegel, «The Law of Cyber -Attack», California Law Review, 2012, p.7
34. SCHAAP, ARIE J, CYBER WARFARE OPERATIONS: DEVELOPMENTSCHAAP, ARIE J... op.cit.,p
35. Scoot. j .Shckelford, "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem",

University of Cambridge, Dept of politicos and International STUDIES, Cambridge, UK,2009.p.201

36. Shin, Beomchul,» The Cyber Warfare and the Right of Self-Defense: Legal Perspectives and the Case of the United States, IFANS, Vol. 19, No1, June 2011, p.104.