المسؤولية الدولية عن جريمة العدوان بالهجمات السيبرانية في ضوء أحكام القانون الدولي

Doi: 10.23918/ilic2021.18

م. ليلى عيسى ابوالقاسم – كلية القانون والعلاقات الدولية- قسم القانون – جامعة جيهان -اربيل
laylalayla630@gmail.com

المقدمــة

لقد بذل المجتمع الدولي الكثير من الجهود لسن قواعد قانونية تضع ظاهرة الحروب في إطارها وتحد من انتشارها في كل ارجاء المجتمع الدولي وما الحقت به من خراب ودمار يعجز عن الوصف. و جرت محاولات عدة للتقليل من حدة الحرب وتجريمه لارتباطه بالعدوان، ويترتب عنه المسؤولية الدولية للدول القائمة بفعله. وبنشأت هيئة الأمم المتحدة كان أولى مقاصدها حفظ السلم و الأمن الدوليين، وكلف مجلس الأمن أحدى أجهزتها بمهمة حفظه والتدخل للحد من العدوان بموجب اختصاصاته فيفرض تدابير وعقوبات الواردة في السابع من الميثاق على الدول التي تخل بالسلم و الأمن الدوليين . وساعد ذلك على مسألة معاقبة الأشخاص الطبيعيين الذين يعملون باسم الدولة إذا نادى فقهاء القانون الدولي بتجسيد المسؤولية الدولية الجنائية عن جريمة العدوان تحقيقا للعدالة الجنائية الدولية وتزامن ذلك مع تأسيس أول محكمتين جنائيتين دوليتين بصفة مؤقتة مثلت المحكمتين العسكريتين في نورنبورغ و طوكيو أول سابقة تاريخية في المعاقبة على جريمة العدوان إذ كرست و فقا لهما مسؤولية الأشخاص الطبيعيين عن الجرائم ضد السلام المرتكبة آنذاك في أوروبا و شرق آسيا.

واستمرت الجهود الدولية التي استغرق عقدين من الزمن لإيجاد تعريف محدد وقانوني للعدوان، وتكللت هذه الجهود بصدور قرار الجمعية العامة لتعريف العدوان رقم ٣٣١٤ لعام ١٩٧٤ متضمنا صوره والمسؤولية القانونية الدولية الناشئة عن العدوان ، ثم إنشاء المحكمة الجنائية الدولية، وتضمن نظامها الأساسي جريمة العدوان من ضمن الجرائم التي تنظر فيها. وإن انقسمت الآراء بين مؤيد ومعارض ولكن بالنهاية تواصلت الجهود في مؤتمر كمبالا الاستعراضي ٢٠١٠ وتبنت قرار الجمعية العامة لتعريف العدوان. ولكن يشهد عصرنا الحالي تطور تكنولوجي سريع ومنافع جمة، و يصنع ايضا العديد من الأخطار خاصة في مفهوم الحرب، وذلك بتوفير الوسائل المتطورة التي تجعلها أكثر فتكا و تدميرا، وتخلق نوع جديد من الحروب سميت بالحروب الحديثة (الحروب السيبرانية)، التي اصبحت محل اهتمام مختلف المنظمات الإقليمية و الدولية، مع ما تهدد به من أخطار، فهي تتخذ مفهوما مغايرا للحرب التقليدية لكونها لا تستعمل الجيوش و الاسلحة التقليدية.

مشكلة البحث: تتمحور مشكلة البحث في الإجابة عن الأسئلة الآتية:

١- هل تشكل الهجمات السيبرانية عدوان طبقا لما نصت عليه المادة الأولى من قرار الجمعية العامة لتعريف العدوان رقم ٣٣١٤ لعام ١٩٧٤، بأنه" العدوان هو استعمال القوة المسلحة من قبل دولة ما ضد سيادة دولة أخرى أو سلامتها الإقليمية أو استقلالها السياسي، أو بأية صورة أخرى تتنافى مع ميثاق الأمم المتحدة".

٢- هل الهجمات السيبرانية من افعال الواردة في المادة الثالثة من قرار تعريف العدوان؟

٣- هل الهجمات السيبرانية من الحالات التي نصت عليها المادة الرابعة تعريف العدوان اعطت الاختصاص لمجلس الأمن النظر إذا كانت هذه الحالة تشكل انتهاك للسلم الأمن الدوليين.

٤- وإذا وصلنا إلى اجابات تؤكد إن الهجمات السيبرانية فعل من افعال العدوان، هل تخضع جريمة العدوان بالهجمات السيبرانية لنفس الأحكام الإجرائية وأحكام المسؤولية والعقاب التي تخضع لها بقية الجرائم ضمن اختصاص المحكمة.

أهمية البحث:

باتت الهجمات السيبرانية وخاصا التي تشكل عدوان، من أهم التحديات التي يواجهها المتخصصين في القانون الدولي العام؛ وذلك لصعوبة تحديد طبيعتها وعناصرها خاصا عندما تشكل فعل من افعال العدوان، وتصنف جريمة دولية، ما يترتب على هذه الهجمات المسؤولية الدولية الجنائية و المدنية. فبرزت اهمية البحث لملائمة قواعد القانون الدولي التقليدية على هذا النوع من العدوان نظرا لما ينتج عنها من نتائج سلبية ودمار وخراب تفوق العدوان بالقوة المسلحة التقليدية.

منهجية البحث:

إن طبيعة البحث وموضوعه تستدعي الاعتماد بدرجة كبيرة على المنهج التحليلي، من اجل تحليل القواعد العامة للقانون الدولي العام لمعرفة مدى امكانية تطبيقها على الدول التي تقوم بالهجمات السيبرانية والتي قد تشكل فعل من افعال العدوان ويمثل جريمة دولية تقع على مرتكبيها المسؤولية القانونية الدولية.

تقسيمات البحث

المبحث الأول- مفهوم العدوان بالهجمات السيبرانية في ضوء أحكام القانون الدولي.

المطلب الأول- مفهوم ووسائل الهجمات السيبرانية وسماتها.

المطلب الثاني- أحكام العدوان بالهجمات السيبرانية في القانون الدولي.

المبحث الثاني- العدوان بالهجمات السيبرانية كجريمة دولية.

المطلب الأول- الأساس القانوني لجريمة العدوان بالهجمات السيبرانية.

المطلب الثاني-المسؤولية الدولية الناشئة عن جريمة العدوان بالهجمات السيبرانية.

المبحث الأول
مفهوم العدوان بالهجمات السيبرانية في ضوء أحكام القانون الدولي

ساهمت الجهود الدولية لتطوير القواعد القانون الدولي في تحديد مفهوم للعدوان وصولا إلى إدراجه من ضمن الجرائم الدولية التي تنظر فيها المحكمة الجنائية الدولية، باعتبارها جريمة دولية متكاملة الأركان. ويكون فعل العدوان المتمثل في استعمال القوة المسلحة من جانب دولة ما ضد سيادة دولة أخرى أو سلامتها الإقليمية أو استقلالها السياسي أو بأي صورة أخرى تتعارض مع ميثاق الأمم المتحدة. إلا انه في وقتنا الحاضر نرى بعض الدول تستعمل قوة غير مسلحة وغير متحركة وغير مرئية ضد دولة أخرى عبر وسائل غير تقليدية (الكترونية) وقد يشكل عدوان واساس قانوني لاعتبار هذا الفعل جريمة عدوان متكاملة الأركان، وهذا ما سوف نبينه في هذا المبحث، ففي المطلب الأول مفهوم ووسائل الهجمات السيبرانية وسماتها، والمطلب الثاني يتناول أحكام العدوان بالهجمات السيبرانية في القانون الدولي.

المطلب الأول- مفهوم ووسائل الهجمات السيبرانية وسماتها

يعتبر مصطلح الهجمات السيبرانية حديث النشأة ظهر في العقود الأخيرة؛ نتيجة لثورة تكنولوجيا المعلومات، ولم تكن الهجمات السيبرانية معروفة إلا في والعقود الأخيرة. فهي مصطلح يوناني الأصل، وترجع إلى مصطلح (kybemetes) ويعني القيادة والتحكم عن بعد [١]. واستدراكا على ذلك، فقد ورد في قاموس المورد تعريف للسيبرانية، حيث عرفها بأنها: علم الضبط، ومصدرها (Cybemtice) وهو مصدر يتطابق مع مفهوم الهجمات السيبرانية، أي ضبط الأشياء عن بعد، والسيطرة عليها [٢]، بينما قاموس مصطلح الأمن المعلوماتي، فقد عرف السيبرانية بقوله بأنها: هجوم عبر الفضاء الإلكتروني، أو البنى المحمية إلكترونيا؛ لتعطيلها أو تدميرها، أو الأضرار بها [٣].

ويستخدم مصطلح الهجمات السيبرانية من قبل فئات عديدة من الناس، للإشارة إلى أشياء مختلفة، كالإشارة إلى وسائل القتال وأساليبه، تلك التي تتألف من عمليات الفضاء الإلكتروني، وقد ترتقي إلى مستوى العدوان أو تجري في سياقه ضمن مفهوم العدوان في القانون الدولي. ويوصف الهجمات السيبرانية بأنه: عالم افتراضي مع عالمنا المادي، يتأثر به ويؤثر فيه بشكل معقد، وتعتمد الهجمات السيبرانية على نظم الكمبيوتر، وشبكات الإنترنيت، عبر الحواسيب، أو الهواتف أو غيرها من الأجهزة دون تقيد بالحدود الجغرافية، لذلك فإن الهجمات السيبرانية- في هذا الاتجاه – يمكن وصفها بأنها عبارة عن تصرف واقعي، يدور في عالم افتراضي قائم على استخدام بيانات رقمية، ووسائل تعمل إلكتروني، ومن ثم تطور هذا المفهوم، حيث أصبح واسعا يقوم على تحقيق أهداف عسكرية أو أمنية مباشرة جراء اختراق مواقع إلكترونية حساسة، عادة ما تقوم بوظائف تصنف بأنها ذات أولوية، كأنظمة حماية محطات الطاقة النووية، أو الكهربائية أو المطارات ووسائل النقل الأخرى[٤]. وكما عرفت بأنها: الذراع الرابعة للجيوش الحديثة، بجانب القوات الجوية والبرية والبحرية، خاصة أن عصر الانترنيت شهد بداية الحديث عن معارك حقيقية تدور في هذا العالم الافتراضي. وهناك من يرى أن الهجمات السيبرانية تمثل البعد الخامس للحرب، وفي هذا الاتجاه تم تعريفها بأنها: "مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نظم المعلومات العادية؛ بهدف التأثير و الإضرار بها، وفي الوقت نفسه الدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة[٥] . ويقصد بها ايضا " الهجوم عبر الانترنيت يقوم على التسلل إلى مواقع إلكترونية غير مرخص الدخول إليها، وهي عبارة عن سلسلة هجمات إلكترونية تقوم بها دولة ضد أخرى [٦]. اما التعريف الذي حصل على قبول اغلب الباحثين للهجمات السيبرانية بأنها: "أي تصرف سواء كان دفاعيا أم هجوميا، يتوقع منه، وعلى نحو معقول، في التسبب بإصابة شخص، أو قتله، أو إلحاق أضرار مادية، أو دمار بالهدف المهاجم"[٧].

- وسائل الهجمات السيبرانية:

تشير الأسلحة الإلكترونية، أو الهجمات السيبرانية إلى تلك الأدوات التي يتم استخدامها لتهديد لإحداث الضرر المادي أو الوظيفي للأجهزة أو النظم والهياكل الإلكترونية، وتختلف هذه الأسلحة والأدوات من حيث درجة خطورتها وتعقيدها، وتتراوح ما بين أسلحة بسيطة قادرة على إحداث ضرر خارجي بالنظام الإلكتروني دون اختراقه، وأخرى معقدة يمكن من خلالها اختراق النظام، واختراق النظم، وإحداث أضرارا بالغة به قد تصل إلى تدميره كليا أو توقفه عن العمل كليا [٨]. ومن اهمها:

١- **استخدام برامج القنابل المنطقية:** وتعد بمثابة برنامج ينفذ في لحظة محددة، أو في فترة زمنية منتظمة، ويتم وضعه في شبكة معلوماتية بهدف تحديد ظروف أو حالة مضمون النظام؛ بغية تسهيل تنفيذ العمل غير المشروع، كإدراج تعليمات في نظام التشغيل للبحث عن عمل معين يكون محلا للاعتداء، كأن تسعى قنبلة منطقية إلى البحث عن حرف (K)، في أي سجل يتضمن أمرا بالدفع، وعندما تكتشفه، تحرك متتالية منطقية تعمل إزالة هذا الحرف من السجل [٩].

٢- **استخدام فيروسات الحاسب الآلي**: وهذه تعد من أكثر الوسائل انتشارا وهي بمثابة مجموعة من التعليمات المرمزة التي تنتج لنفسها نسخا مطابقة تلحق من تلقاء ذاتها ببرامج التطبيقات، ومكونات النظام المنفذ، لتقوم في مرحلة محمية بالتحكم في أداء النظام الذي أصابته. وقد عرفه المركز القومي للحاسب الآلي في الولايات المتحدة الأمريكية بأنه: " برنامج مهاجم يصيب أنظمة

---

[١] احمد عبيس نعمة الفتيلاوي، الهجمات السيبرانية مفهومها و المسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية و السياسية، جامعة بابل، كلية القانون، العدد الرابع- السنة الثانية،٢٠١٦،ص٦١٤.

[٢] سراب أحمد تامر، الهجمات على شبكات الحاسوب في القانون الدولي الإنساني، أطروحة دكتوره، جامعة النهرين كلية الحقوق،بغداد،٢٠١٥،ص١٠٧.

[٣] المرجع السابق، ص١٠٨.

[٤] نوران شفيق، أثر التهديدات الالكترونية على العلاقات الدولية (دراسة في ابعاد الأمن الالكتروني)، المكتب العربي للمعارف، القاهرة،٢٠١٦ ،ص٢٩.

[٥] سراب أحمد تامر، الهجمات على شبكات الحاسوب في القانون الدولي الإنساني، مرجع سبق ذكره، ص١٠٨.

[٦] نوران شفيق، أثر التهديدات الالكترونية على العلاقات الدولية (دراسة في ابعاد الأمن الالكتروني)، مرجع سبق ذكره ،ص٣٠.

[٧] سراب أحمد تامر، الهجمات على شبكات الحاسوب في القانون الدولي الإنساني، مرجع سبق ذكره، ص١٠٩.

[٨] احمد عبيس نعمة الفتيلاوي، الهجمات السيبرانية مفهومها و المسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مرجع سبق ذكره،ص٦١٥.

[٩] محمد عبدالله ابوبكر، جرائم الكمبيوتر و الانترنيت، منشأة المعارف، الاسكندرية، ٢٠٠٦،ص٤٠.

الحاسبات، بأسلوب يماثل لحد كبير أسلوب الفيروسات الحيوية التي تصيب الإنسان، حيث يقوم هذا البرنامج بالتجول في الحاسب الألي باحثا عن برنامج غير مصاب، وعندما يجد أحدها ينتج نسخة من نفسه لتدخل فيه، حيث يقوم البرنامج المصاب فيما بعد بتنفيذ أوامر الفيروس، ومن أهم خصائصه قدرته الفائقة على الاختفاء، و الانتشار، و الاختراق وقدرته على تدمير الحاسب الآلي بأكمله (١).

٣- **هجمات إنكار الخدمة:** وهي عبارة عن هجمات إلكترونية تتم إغراق المواقع بسيل من البيانات غير اللازمة، التي يجري إرسالها ببرامج متخصصة تعمل على نشرها، فتؤدي إلى بطء في الخدمات أو ازدحام في المرور على هذه المواقع، فيصعب بالتالي وصول المستخدمين إليها (٢).

٤- **الهجوم الإلكتروني:** كالتشويش والخداع الإلكتروني والصواريخ المضادة للإشعاع الكهرومغناطيسي والقيام بالتجسس على الهدف؛ لسرقة معلومات سرية، بغض النظر عن الأهداف، والتي قد تكون اقتصادية كالتجارة بين الشركات، أو استراتيجية أو عسكرية بين دول معينة، ومن تلك العمليات ايضا التعدي على الملكية الفكرية، وقرصنة المعلومات، كسرقة البرامج الحاسوبية، وتوزيع مواد مكتوبة أو مصورة بدون إذن المالك الشرعي، وخاصة وأن وجود شبكة الإنترنيت قد أدى إلى توسيع انتشار مثل تلك العمليات؛ لسهولة النشر والتوزيع على هذه الشبكة. وفي عام ٢٠١٤ أجرت كوريا الشمالية هجوم إلكتروني ضد شركة Pictures Sony Entertainment ، مما جعل الآلف من أجهزة كمبيوتر سوني غير صالحة للعمل، وتم اختراق المعلومات التجارية السرية للشركة. بالإضافة إلى الطبيعة المدمرة للهجمات، سرقت كوريا الشمالية نسخ رقمية لعدد من الأفلام التي لم يتم إطلاقها، بالإضافة إلى آلاف المستندات التي تحتوي على بيانات حساسة تتعلق بالشخصيات الشهيرة وموظفي شركة Sony.رافقت كوريا الشمالية هجماتها الإلكترونية بالإكراه والتخويف والتهديد. كان هجوم كوريا الشمالية على سوني واحد من أكثر الهجمات الإلكترونية تدميرا على أي كيان أمريكي حتى الأن. أدى هذا الهجوم إلى مزيد من النقاش حول طبيعة التهديد السيبراني والحاجة إلى تحسين الأمن السيبراني(٣).

ولقد أحدث التطور تحولا كبيرا في مفهوم القوة ترتب عليه دخول المجتمع الدولي في مرحلة جديدة تلعب فيها هجمات الفضاء الإلكتروني عنصرا حيويا في تنفيذ عمليات ذات فاعلية في الأرض وفي البحر والجو والفضاء واعتماد القدرة القتالية في الفضاء الإلكتروني على نظم التحكم والسيطرة. ويعرف "جوزيف ناي" مفهوم القوة الإلكترونية بأنها تشير إلى مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الإلكترونية والبنية التحتية المعلوماتية والمهارات المدربة للتعامل مه هذه الوسائل"(٤). هذا وتختلف العمليات ذات الطابع العسكري في الفضاء السيبراني حسب قوة الدولة وتوجيهاتها، ويمكن تصنيفها في الفضاء إلى أربع فئات منفصلة لكل منها أهدافها (٥):

- **عمليات جمع المعلومات الاستخباراتية**: تهدف إلى جمع المعلومات من بيانات العدو الإلكترونية ففي عام ٢٠١٠أعلنت ألمانيا أنها واجهت عمليات تجسس شديدة التعقيد لكل من الصين وروسيا كانت تستهدف القطاعات والبنى التحتية الحساسة في البلاد ومن بينها شبكة الكهرباء التي تغذي الدولة .ويجمع.
- **عمليات تستهدف المعنويات**: يهدف إلحاق الضرر بالروح المعنوية وإرادة القتال لدى شعب العدو من خلال الدعاية والتضليل المعلوماتي، وغير ذلك من تقنيات حرب المعلومات.
- **عمليات هجومية:** تستهدف إلحاق الضرر ببيانات العدو وشبكاته الإلكترونية أو تعطيلها، و، أو إلحاق المزيد من الضرر المادي بأفراد العدو أو عتاده، على سبيل المثال إضعاف دفاعات العدو الإلكتروني مثل (شبكات الدفاع الجوي).

ويجمع الخبراء على أن الهجوم الإلكتروني الذي استهدف استونيا العام ٢٠٠٧ ،يكاد يكون الهجوم الإلكتروني الأول الذي يتم على هذا المستوى ويستخدم لتعطيل المواقع الإلكترونية الحكومية والتجارية والمصرفية والعالمية مسببا خسائر بعشرات الملايين من الدولارات إضافة إلى شلل البلاد، وعلى الرغم من أن الشكوك كانت تحوم حول موسكو على اعتبار أن الهجوم جاء بعد فترة قصيرة من خلاف استوني روسي كبير، إلا أن أحدا لم يستطع أن يحدد هوية الفاعل الحقيقي أو مصدر الهجوم الذي تم، وهي من المصاعب والمشاكل التي ترتبط بحروب الأنترنت

- **عمليات دفاعية**: هدفها حماية البيانات الإلكترونية والشبكات الخاصة بالدولة و الحيلولة دون إلحاق الضرر بالشعب و الممتلكات.

وتتسم وسائل و أسلحة السيبرانية بأنواعها المختلفة بمجموعة الخصائص ويمكننا تحديدها بالآتي(٦):

أ- تتسم وسائل السيبرانية و أسلحتها بخضوعها لعمليات تحديث وتطوير مستمرين؛ مما يزيد في قدرتها التدميرية وفاعليتها في شن الهجمات الإلكترونية.

ب- سهلة الاستخدام ومتوفرة على نطاق واسع، بحيث يمكن تحميلها من الإنترنيت أو شراؤها، وتكمن مستخدمها من القيام بهجمات معقدة تتخطى مستوى قدراتهم الحقيقية.

---

(١)إيهاب خليفة، القوة الإلكترونية وابعاد التحول في خصائص القوة، مكتبة الاسكندرية،٢٠١٤،ص ٦٧.

(٢)المرجع السابق،ص٦٨.

(٣)محمد عبدالله ابوبكر، جرائم الكمبيوتر و الانترنيت، مرجع سبق ذكره، ص٥٥.

(٤)جون باسيت، حرب الفضاء الإلكترونية: التسلح و أساليب الدفاع الجديدة، الحروب المستقبلية في القرن الواحد و العشرين،ط١، مركز الإمارات للدراسات و البحوث الإسترتيجية،٢٠١٤،ص٥٧.

(٥)موسى نعيم، نهاية عصر القوة من قاعات اجتماعات مجلس الإدارة إلى ساحات الحرب و الكنائس إلى الدول لماذا لم يعد تولي المسؤولية كما كان في السابق؟، ط١، مركز الإمارات للدراسات و البحوث الإستراتيجية،٢٠١٦ ، ص١٨٣- ١٨٤.

(٦) موسى نعيم، نهاية عصر القوة من قاعات اجتماعات مجلس الإدارة إلى ساحات الحرب و الكنائس إلى الدول لماذا لم يعد تولي المسؤولية كما كان في السابق؟،مرجع سبق ذكره، ص١٨٥.

ج- تتسم بدقتها وفاعليتها وقدرتها على إصابة أنواع مختلفة من الأجهزة الإلكترونية، سواء أكانت أجهزة الحاسب الآلي، أم مقدم الخدمة، أم أي جهاز متصل بشبكة إلكترونية.

وتجدر الإشارة إلى أن التأثير الأولي للعمليات العسكرية في الفضاء السيبراني على شبكات الدولة المعتدي عليها بشكل مؤقت، و المنطق العسكري يدعو إلى هجوم مكتمل بالمعدات العسكرية للاستفادة من ارتباك العدو وشله. فبدون هجوم لتدمير أو الاستيلاء على ما تم إيقاع الفوضى فيه. سيقوم العدو بكل بساطة بإصلاح موقفه و العودة إلى الهجوم، وبالتالي فإن المعركة الإلكترونية تعزز الاتجاه إلى الهجوم، وميزة عنصر المفاجأة.

المطلب الثاني- أحكام العدوان بالهجمات السبرانية في القانون الدولي

أولا- مكانة الهجمات السيبرانية في قرار الجمعية العامة لتعريف العدوان رقم ٣٣١٤ لعام ١٩٧٤:

البدء بقرار الجمعية العامة لقرار تعريف العدوان للإجابة على السؤال الذي مفادها ، هل الهجمات السيبرانية عدوان طبقا لقرار التعريف؟ وهل من ضمن حالات العدوان التي عددها قرار التعريف في مادته الثالثة؟

يعرف قرار التعريف العدوان في مادته الأولى بأنه " استعمال القوة المسلحة من قبل دولة ما ضد سيادة دولة أخرى أو سلامتها الإقليمية أو استقلالها السياسي، أو بأية صورة أخرى تتنافى مع ميثاق الأمم المتحدة". تخص هذه المادة استعمال القوة بشكل مباشر، وهذا يعني أن العدوان غير المباشر وفقا للمادة المذكورة، والذي ليس فيه استخدام القوة المسلحة سيبقى خارج التعريف، مثل التهديدات أو الإخلال بالسلم وستبقى الحالات التي تستعمل فيها الدولة المسلحة بشكل غير مباشر ضمن نصوص تعريف العدوان الأخرى وضمن اختصاصات مجلس الأمن. وتعتبر والهجمات السيبرانية من خلال تصنيفاتها السالفة الذكر بأنها تصنف كعمليات هجومية عسكرية من خلالها تستخدم القوة العسكرية التي يمكن الطرف المعتدي على تحريكها عن بعد، وإلحاق ضرر بقواتها العسكرية وعتادها. وبموجب المادة الثانية من قرار التعريف نفسه التي مضمونها يستند على مبدأين قانونيين مهمين هما مبدأ الاستعمال الأول للقوة المسلحة (المبادأة) و مبدأ القصد العدائي. فالدولة التي تستعمل القوة المسلحة أولا هي الدولة المعتدية. وعند البدء بارتكاب فعل من أفعال العدوان التي تشتمل عليها قائمة الأفعال الأنموذجية في المادة (الثالثة) أو أي عمل آخر قد يقرره مجلس الأمن ضمن اختصاصاته ووفقا للميثاق بأنه عمل من أعمال العدوان. ولكن في ظل التطور الهائل للتكنولوجيا و الاعتداء بالهجمات السيبرانية و النتائج التي تترتب على عنصر المباغتة في الحروب الحديثة يجعلان من الصعوبة تطبيق أو إمكان التحقق من حقيقة الموقف بالاستناد على مبدأ المبادأة. أما بالنسبة لمبدأ القصد العدائي لم يدرج ، واكتفى واضعي التعريف بعنصر (المبادأة) على اعتبار أن ليس هناك عدوان بدون قصد عدائي من جهة، ولعدم فسح المجال لوجود ثغرة ينفذ منها المعتدي لتبرير عدوانه.

وتبقى المهمة الصعبة لدى مجلس الأمن يحدد الجهة التي بدأت باستخدام القوة أولا [1] . وإذا طبقنا مبدأ القصد العدائي على الهجمات السيبرانية بكل تأكيد تظهر في نتائجه الهدف منها القصد العدائي بوضوح من قبل الدولة المعتدية. وأما المادة الثالثة من قرار تعريف العدوان تشتمل على الحالات الأنموذجية من أفعال العدوان التي تعد الدولة البادئة بارتكاب واحد منها قد ارتكب(العدوان) سواء كان ذلك بإعلان للحرب أم بدونه، وهذا يعني انها تكون كافية لإثبات العدوان، ولا يعد إعلان الحرب بديلا عنه حسب قرار التعريف وإن كان إعلان الحرب الذي يصاحب العدوان في الوقت نفسه يفصح عن نوايا المعتدي ويثبت وقوع العدوان. إن قائمة الأفعال الإنموذجية لا تتضمن الهجمات السيبرانية و لأي إشارة لها من بعيد أو قريب على هذا النوع من الحروب (السيبرانية) و الذي أبعد من أن يعلن عنها. ولعل المادة الرابعة نجد فيها ما يمكننا اعتبار الهجمات السيبرانية فعل من أفعال العدوان، حيث أنها تنص على " إن الأفعال التي ذكرنها في ما مر ليست شاملة ، وأن مجلس الأمن له أن يحدد أية أعمال أخرى، تشكل العدوان أيضا بمقتضى نصوص الميثاق". نلاحظ إن إغفال التعريف في النص نذكر أنواع أخرى يتيح منافذ للمعتدي، مع بقاء اختصاصات مجلس الأمن في اتخاذ القرار بتخصيص أفعال أخرى من العدوان محصورة ضمن تصويت الدول الكبرى، وهذه مهمة صعبة لمجلس الأمن أن يحدد أفعال لم تدرج تحت مفهوم العدوان. وهي لا شك أفعال أقل وضوحا وأكثر تعقيدا مثل العدوان غير مباشر كالهجمات السيبرانية. وقد يحدث العدوان بالهجمات السيبرانية من ضمن الدول الخمس الدائمة العضوية في مجلس الأمن الدولي، والتي تتمتع بحق النقض (الفيتو) وهذا يقودنا إلى العدوانية الحقيقية في فعل الهجمات الإلكترونية وأنه لا يصدر إلا من دول كبرى وذات نفوذ دولي وصاحبة سلطة عليا في القرارات الدولية فلو افترضنا جدلاً أن الاتهام الرسمي وقع فعلاً على الولايات المتحدة من الذي يجرأ على اتهامها ووضعها في قفص الاتهام في القانون الدولي وهي المسيطرة على تمرير القرارات التي ترغبها في مجلس الأمن والقوة العظمى الأولى في العالم عسكرياً واقتصاديا.

هذا بالإضافة إلى أنها المسيطرة على أقوى حلف عسكري في العالم وأكبر قوة ردع عسكرية والأوسع انتشارا في مختلف أصقاع الأرض وصاحب أكثر القواعد العسكرية الاستراتيجية بالعالم (حلف الناتو). وبالتالي ستكون مهمة مجلس الامن في تحديد فعل العدوان.

ونص ميثاق الأمم المتحدة على مبدأ التحريم العام لاستخدامات القوة المسلحة في العلاقات الدولية المادة (٢-ف٤) ولكن دون تحديد مفهوم القوة واستخدامها كما نص على مصطلح (العدوان) في الفصل السابع المادة (٣٩) دون تعريفه وحث الدول على فض النزاعات الدولية بالطرق السلمية وإبداء حسن النية في العلاقات الدولية المادة (٢ف٢) التي يجب أن تتحلى في حالة الدفاع عن النفس فقط المادة (٥١) والدفاع الفردي و الجماعي تحت وقع أي تهديد أو إخلال بالسلم أو ما قد وقع بما يشكل عملا من أعمال العدوان المادة (٣٩)من الميثاق. فالسؤال الذي يفرض نفسه هو مدى انطباق أحكام النصوص القانونية المذكورة على الهجمات السيبرانية لكي تعد فعل من أفعال العدوان عندما تقوم بها أحد الدول الأعضاء بانتهاكها. وفي حالة الهجوم السيبراني يمكن اعتباره بمستوى "الهجوم المسلح" هل يثبت لها حق الدفاع عن النفس كما هو الحال بالنسبة الدولة المعتدي عليها عسكريا.

---

[1] أ.د. صلاح الدين احمد حمدي، دراسات في القانون الدولي العام، دراسات في القانون الدولي العام،ط١، منشورات ELGA ، مالطا، ٢٠٠٢ ،ص ٢٧٣:٢٧٧.

وللإجابة عن هذا السؤال لابد أن نستحضر موقف محكمة العدل الدولية، و بالتحديد موقف المحكمة في قضية نيكارغوا لعام ١٩٨٦.

تصدت محكمة العدل الدولية في قضية نيكاراغوا إلى المادة (٤/٢) من ميثاق الأمم المتحدة من زاويتين، الأولى عندما تعرضت المحكمة إلى طبيعة هذه المادة، حيث أكدت في الفقرة (١٨٧) من حكمها على تحول مبدأ حظر استخدام القوة أو التهديد بها إلى قاعدة عرفية دولية يقع على جميع الدول واجب الالتزام بها أن ذلك يأتي منسجما مع حقيقة أن معظم بنود ميثاق الأمم المتحدة قد وصلت إلى كونها مبادئ أساسية ال يجوز ألي دولة مخالفتها أو القفز عنها، اما الزاوية الثانية فتتمثل في الحالات التي يمكن أن تعتبر استخداما للقوة خلافا لهذه المادة، في هذا الصدد أقرت المحكمة بشمولية المادة وعدم اقتصارها على استخدام القوة بالمعنى التقليدي، والمتمثل في استخدام قوات عسكرية نظامية خارج حدود الدولة؛ حين أسهبت وأقرت أن "إرسال القوات من لدن الدولة أو بالنيابة عنها سواء كانت على شكل مجموعات نظامية أو غير نظامية أو أية أدوات أخرى" يعتبر مخالفة للمادة (٤/٢)من الميثاق، ويمكن لمثل هذا التصرف أن يعتبر هجوما مسلحا وفقا أحكام المادة ٥١ من الميثاق بالاستناد إلى حجم وتأثير استخدام القوة بعيدا عن الفرق في التعبيرات المستخدمة من قبل المحكمة بين استخدام القوة والهجوم المسلح هنالك نقطة جوهرية يجب الوقوف عندها هنا تتمثل في الخروج الواضح للمحكمة عن النهج التقليدي لفهم استخدام القوة؛ ذلك الاستخدام لأدوات التقليدية في الاعتداء، والذي كان يشترط قرارا مباشرا من الدولة باتجاه استخدام ، وهذا الموقف للمحكمة جاء تأكيدا على النية الحقيقية للدول القوة في إقليم دولة أخرى المشاركة في صياغة المادة (٤/ ٢)من الميثاق، حيث إن الأعمال التحضيرية لهذه المادة تشير وبوضوح إلى أن أي تهديد أو استخدام للقوة بين الدول الأعضاء سوف يشكل خرقا . يشار إلى أن هذا الموقف للمحكمة لهذه المادة، شريطة أن يكون مخالفا لمبادئ الميثاق.

يشار إلى أن هذا الموقف للمحكمة بعد تأكيد لفكرة مسؤولية الدولة عن الممارسات الخاطئة المباشرة وغير المباشرة، بما فيها تلك الناشئة عن تقصيرها بواجب عدم التسبب بأذى للأخرين خارج نطاق إقليمها[١].

و نصل إلى نتيجة محددة مفادها أن المحكمة من خلال حكمها في قضية نيكاراغوا، و قضية منصات النفط بين إيران والولايات المتحدة ٢٠٠٣ إلى ضم فئات أخرى غير الهجوم الحركي لكي يعطي الحق للدولة التي تتعرض إلى هجوم الارتكاز إلى المادة ٥١ والدفاع عن نفسها ولكن ضمن شروط أبرزها الحجم والتأثير(Effect and Scale) .فقد كانت مهيأة لضم فئات أخرى غير الهجوم العسكري التقليدي في إطار التصرفات التي يمكن أن تشكل خرق للمادة (٤/٢) من الميثاق، ويجب أن نشير إلى أن موضوع النزاع أمام المحكمة في هذه القضية لم يكن في إطار الهجمات الإلكترونية، وإنما كان يتمحور حول الدعم العسكري غير المباشر الذي كانت تقدمه الولايات المتحدة لمجموعات مناهضة للحكومة في نيكاراغوا، وبسبب الاتصال بين هذه المجموعات وحكومة الولايات المتحدة أقرت المحكمة بالخرق من جانب الولايات المتحدة للمادة(٤/٢)حيث حكمت المحكمة لصالح نيكاراغوا[٢].

وانطلاقا من المعايير آنفة الذكر والتي استندت إليها المحكمة، فيمكن لنا أن نتخيل تصورا مشابها في حالة ادعاء دولة معينة على أخرى بشأن هجمة إلكترونية عندما تحقق هذه الهجمة معيار الحجم والتأثير على الدولة التي تتعرض للهجوم، بشرط اتصالها بالدولة المدعى عليها، إلى جانب ذلك، جاءت النسخة الأولى من دليل تالين للعام ٢٠١١ لكي تدعم هذه النتيجة حين جاءت القاعدة ١١ منه لتؤكد على أن العمليات الإلكترونية تعتبر استخداما للقوة عندما يكون مستواها وتأثيرها متقاربا مع العمليات غير الإلكترونية، ففي سياق هذا النص أقرت مجموعة من الخبراء أعدت هذا الدليل أنها قد استندت إلى معيار الحجم والتأثير في سياق تحديد فيما إذا كانت الهجمة الإلكترونية ترقى إلى استخدام غير مشروع للقوة خلافا للمادة (٤/٢)من ميثاق الأمم المتحدة، وأيضا فيما إذا كان هجوما عسكريا يبرر الدفاع عن النفس وفقا للمادة ٥١ ،وهما المعياران -ذاتهما- اللذان استندت إليهما محكمة العدل الدولية في قضية نيكاراغوا آنفة الذكر[٣].

المبحث الثاني

العدوان بالهجمات السيبرانية كجريمة دولية

تتميز الجريمة الدولية بركنها الثالث الذي يبرز خصوصيتها وخطورتها وهو الركن الدولي، عن الجريمة العادية حيث من المعروف يتم التمييز عادة بين ركنين الجريمة هما الركن المادي والمعنوي. وتعتبر الاركان الأربعة (المادي والمعنوي و الشرعي و الدولي) من الاركان العامة للجريمة الدولية، وهي تختلف عن الأركان الخاصة عن جريمة إلى أخرى، فتختلف أركان جريمة العدوان عن اركان الجرائم الدولية الأخرى كجريمة الإبادة الجماعية والجرائم ضد الإنسانية. ولذلك سوف نبين في المطلب الأول الأساس القانوني لجريمة العدوان السيبرانية ويتضمن أحكام المحكمة الجنائية الدولية للنظر في جريمة العدوان وبيان اركان جريمة العدوان، ويتناول المطلب الثاني المطلب الثاني- المسؤولية الدولية الناشئة عن جريمة العدوان بالهجمات السيبرانية.

---

[١] رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة للعلوم القانونية، المجلد ١٥، العدد ٢، ربيع الثاني١٤٤٠- ديسمبر- ٢٠١٨ ، ص٣٤٨.

[٢] رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة للعلوم القانونية، مرجع سبق ذكره، ص ٣٤٩.

[٣] نفس المرجع، ص٣٤٩.

المطلب الأول- الأساس القانوني لجريمة العدوان بالهجمات السيبرانية

أولا- أحكام المحكمة الجنائية الدولية للنظر في جريمة العدوان:

استطاعت الدول المؤيدة لإدراج جريمة العدوان في النظام روما الأساسي بسط سلطاتها على اختصاص المحكمة بنظر جريمة العدوان عن طريق إدراجها في المادة ٢/٥ من نظام روما الأساسي، الذي يمثل النص الجزائي الدولي الأول الذي وضع هذه الجريمة ضمن اختصاص قضاء دولي جنائي دائم و جرمها، و إن كان عدم تعريفها يشكل عقبة في تطبيق الاختصاص إلا أنه اعتراف من الدول أن العدوان جريمة يرتكبها الأفراد و يتابعون عليها أمام هيئة قضائية دولية. وتمارس المحكمة الاختصاص على الجريمة العدوان متى اعتمد حكم بتعريف هذه الجريمة وفقا للمادتين (١٢١،١٢٣) من النظام الأساسي للمحكمة الجنائية الدولية، يعرف جريمة العدوان ويضع الشروط التي بموجبها تمارس المحكمة اختصاصها فيما يتعلق بهذه الجريمة ، ويجب أن يكون هذا الحكم متسقا مع الأحكام ذات العلاقة من ميثاق الأمم المتحدة. فعرفت الفقرة الأولى من المادة (٨) في مؤتمر كمبالا ٢٠١٠ جريمة العدوان بأنها "قيام شخص ما وضع يتيح له التحكيم بالفعل السياسي أو العسكري للدولة أو توجيهه بتخطيط أو إعداد أو شن أو تنفيذ عمل عدواني من شأنه، بحكم طبيعته وخطورته ونطاقه، أن يعد انتهاكا واضحا لميثاق الأمم المتحدة". والذي يمكن ملاحظته على ما ورد في هذه الفقرة، أن المسؤولية الجنائية الفردية فيما يتعلق بجريمة العدوان مقتصرة على القادة المسؤولين عن أوضح وأخطر حالات الاستخدام غير المشروع للقوة من جانب دولة ضد دولة أخرى، فأي عمل من هذا القبيل من شأنه "بحكم طبيعته وخطورته ونطاقه، أن يشكل انتهاكا واضحا لميثاق الأمم المتحدة"، وهو ما أكدت عليه الفقرة (٣) مكرر من المادة (٢٥) من النظام الأساسي للمحكمة و المتعلقة بالمسؤولية الجنائية الفردية، من أنه لا تنطبق أحكام هذه المادة إلا على الأشخاص الذين يكونون في وضع يمكنهم من التحكم فعلا في العمل السياسي أو العسكري للدولة أو من توجيهه [١].

تباينت الآراء حول تفسير ما ورد في نص الفقرة الأولى المادة ٨ مكرر، في مؤتمر كمبالا الاستعراض ٢٠١٠. حيث أنه يرى البعض أنه يثير بعض النقاط المهمة هي: أولا، ليس كل عمل عدوان يعد جريمة عدوان، فمن أجل أن يشكل عمل عدوان جريمة عدوان، يجب أن يشكل انتهاكا "واضحا" لميثاق الأمم المتحدة من حيث طبيعته ونطاقه. ثانيا، أن فئة الأشخاص الذين يحتمل أن يكونوا مسئولين عن العدوان يجب أن يكونوا مسئولين عن العدوان يجب أن تكون محدودة جدا في معظم الحالات، وتقتصر فقط على أولئك الذين في وضع يتيح لهم أن يتحكموا أو يوجهوا العمل السياسي أو العسكري للدولة[٢]. ولهذا الاشخاص فإن الضباط و الجنود والفنيين الذين لا يشاركون في صنع السياسات و الخطط العسكرية الكبرى لا يمكن أن يتهموا بارتكاب جريمة عدوان أمام المحكمة الجنائية الدولية، حتى ولو انهم شاركوا بنشاط فيها. فالسؤال فكيف كيف يمكن اتهام أشخاص قاموا بهجمات فضائية (سيبرانية) وقد يشكل عدوانا يشكل انتهاكا واضحا لميثاق الأمم المتحدة؟ إن عدم وجود تعريف مقنن لفعل العدوان منذ محكمة نورنمبرغ فإن استخدام التعريف الذي حصل على تأييد في الأمم المتحدة بموجب قرار الجمعية العامة للأمم المتحدة رقم (٣٣١٤) لسنة ١٩٧٤، بدأ الأكثر أمانا من أجل إرضاء جميع مندوبي الدول [٣]. ولأغراض تعريف جريمة العدوان عرفت الفقرة الثانية من المادة الثامنة مكرر "عمل العدوان " بأنه استعمال القوة المسلحة من قبل دولة ما ضد سيادة دولة أخرى أو سلامتها الإقليمية أو استقلالها السياسي، أو بأي طريقة أخرى تتعارض مع ميثاق الأمم المتحدة. وتنطبق صفة فعل العدوان كما وردت في المادة الثالثة لقرار الجمعية العامة لتعريف العدوان رقم ٣٣١٤ عام ١٩٧٤, وإن رأى البعض إن الإحالة في الفقرة الثانية من المادة (٨) مكرر لقرار التعريف، قد تكون لها في الواقع نتائج عكسية، وربما تشكل معضلة في مواجهة مبدأ الشرعية طبقا لمبدأ (لا جريمة و لا عقوبة إلا بنص قانوني). يعني أن كل سلوك إجرامي يجب أن يوصف بوضوح في قاعدة قانونية تجرمه تسبق ارتكاب الجريمة المزعومة. علاوة على ذلك، وفقا للمادة (٤) من قرار التعريف، فإن قائمة الأعمال التي ذكرت في المادة الثالثة ليست شاملة، ويجوز لمجلس الأمن أن يقرر بأن أعمالا أخرى تشكل عدوانا وفقا لأحكام ميثاق الأمم المتحدة.

وبالنهاية الأمر متروك لمجلس الأمن بموجب الفصل السابع المادة (٣٩) إذ ما كان هذا الفعل يشكل جريمة عدوان أم لا.

ثانيا- اركان جريمة العدوان، بموجب ما نص عليه المرفق الثاني من قرار مؤتمر كمبالا لعام ٢٠١٠ الخاص بتعريف جريمة العدوان، وعليه فأن أركان الجريمة هي كالآتي:

١- قيام مرتكب الجريمة بتخطيط فعل عدواني أو بإعداده أو بدئه وتنفيذه.

٢- مرتكب الجريمة شخص كان في وضع يمكنه من التحكم فعلا في العمل السياسي أو العسكري للدولة التي ارتكبت فعل العدوان أو من توجيه هذا الفعل.

٣- فعل العدوان المتمثل في استعمال القوة المسلحة من جانب دولة ما ضد سيادة دولة أخرى أو سلامتها الإقليمية أو استقلالها السياسي أو بأي صورة أخرى تتعارض مع ميثاق الأمم المتحدة قد ارتكب.

٤- مرتكب الجريمة كان مدركا للظروف الواقعية التي تثبت أن استعمال القوة المسلحة على هذا النحو يتعارض مع ميثاق الأمم المتحدة.

٥- فعل العدوان يشكل بحكم طابعه وخطورته ونطاقه، انتهاكا واضحا لميثاق الأمم المتحدة.

ثالثا - الأركان الخاصة بجريمة العدوان بالهجمات السيبرانية:

لاستنتاج الاركان الخاصة لجريمة العدوان بالهجمات السيبرانية ونعتمد على مجموعة من الصفات التي يجب أن تتسم بها الهجمات الإلكترونية حتى ترقى إلى عتبة الهجوم المسلح، اتي تضمنتها دليل "تالين" ونبينها كما يلي:

١- الركن المادي لجريمة العدوان في البنود الثلاثة الأولى. حيث أن السلوك الإجرامي يظهر هنا بأنه سلوك إيجابي يتمثل ،و بشكل غير مشروع ضد إقليم دولة أخرى أو ضد قواتها. اما استخدام القوة دفاعا عن النفس استنادا إلى الحق في الدفاع الشرعي

---

[١]علي جميل حرب، منظومة الفضاء الجزائي الدولي للمحاكم الجزائية الدولية و الجرائم الدولية المعتبرة، مرجع سبق ذكره ،ص٢٢٨,

[٢]كمال حماد، النزاع المسلح والقانون الدولي العام، ط١، المؤسسة الجامعية للدراسات والنشر و التوزيع،بيروت،١٩٩٧،ص٣١,

[٣] كمال حماد، النزاع المسلح والقانون الدولي العام، مرجع سبق ذكره،،ص٣٢.

الذي نصت عليه المادة (٥١) من ميثاق الامم المتحدة، لا يعد استخداما غير مشروع للقوة و لا يشكل بأي حال من الاحوال جريمة عدوان. و كما أن التهديد باستعمال القوة أو فرض العقوبات الاقتصادية وقطع العلاقات الدبلوماسية لا يشكل بحد ذاته فعل عدوان، وبالتالي ينتفي الركن المادي لجريمة العدوان.

وطبقا لدليل "تالين" قامت اللجنة بوضع معيار أساس يستند إلى الضرر المادي سواء قد وقع على الأفراد أو على الممتلكات، ففي مثل هذه الحالة تعتبر العملية الإلكترونية هجوما عسكريا، أما تلك التصرفات التي ال تلحق مثل هذا النوع من الضرر فتخرج حسب اللجنة من دائرة الهجوم العسكري، إلا في الحالة التي تضر فيها هذه العمليات الإلكترونية بمصلحة وطنية حساسة للدولة المعتدى عليها دون أن تتصل بضرر مادي محسوس.

٢- الركن المعنوي لجريمة العدوان، فقد نص عليه البندان الرابع و السادس حيث إن مرتكب الجريمة يجب أن يكون مدركا للظروف الواقعية التي تثبت أن استعمال القوة المسلحة على هذا النحو ضد سيادة دولة اخرى أو سلامتها الإقليمية أو استقلالها السياسي أو إزهاق ارواح مواطنيها أو بأي صورة أخرى تشكل انتهاكا واضحا لميثاق الأمم المتحدة ويتعارض مع مبادئه و أهدافه و احكامه. بمعنى لابد من البحث عن نية وقصد مرتكبيه لتحديد مدى وقوعه، حتى يتأكد الدليل القاطع وقرينة لإثبات العدوان، وتحديد الطرف المعتدي وتوفر القصد الجنائي.

وعلى هذا الأساس جاء دليل تالين متضمنا شرط العدائية، والذي يتمثل في النية خلف العملية الإلكترونية، فبحسب هذا الشرط ترتقي العملية الإلكترونية إلى عتبة الهجوم المسلح كلما كانت الدولة المعتدى عليها قادرة على إثبات أن هذا التصرف يسعى إلى تحقيق أهداف عدائية في الدولة الأخرى، كإضعاف القدرة العسكرية من خال التأثير على برامجها الإلكترونية العسكرية، ويمكن أن يتبين من خلال استهداف الدولة مصدر الهجوم شبكات إلكترونية محمية ومؤمنة في مواجهة خروقات إلكترونية مستقبلية من جهات أخرى، بسبب كونها تعمل في ميدان استراتيجي للدولة المعتدى عليها .فالاعتداء-على سبيل المثال-على الشبكات الخاصة بوزارة الدفاع في دولة ما لا يمكن من حيث المبدأ أن يقرأ إلا في إطار العدائية حسب المادة ٥١ ،حيث إن هذه الشبكات في طبيعة الحال من أكثر الشبكات الإلكترونية حماية في أي دولة، ولذا يمكن لنا أن نخرج بنتيجة مفادها أنه وبحسب دليل تالين هنالك علاقة طردية بين درجة الحماية للشبكة الإلكترونية موضع الهجوم وشرط العدائية وبالتالي النية وراء هذا الهجوم.

٣- الركن الدولي لهذه الجريمة يتمثل فيما ورد التأكيد عليه في البنود الثالث و الرابع و الخامس. والذي يعني أن فعل العدوان لابد أن يقع من خلال استعمال دولة للقوة المسلحة ضد دولة اخرى ، ويشكل انتهاكا واضحا للمصلحة الدولية للمجتمع الدولي من خلال انتهاك مبادئ ميثاق منظمة الامم المتحدة، واهمها مبدأ حظر استخدام القوة في حل النزاعات الدولية وضرورة اللجوء للطرق السلمية بدلا منها، واحترام سيادة كل دولة و استقلالها السياسي وعدم التدخل في شؤونها الداخلية. وكذلك احترام الأهداف التي قامت المنظمة من أجلها وأهمها حفظ السلم والأمن الدوليين.

وفي إطار تطبيق المحكمة الجنائية الدولية لهذا الركن، فإنها تلتزم بمراعاة اشتراط قيام العدوان باسم الدولة أو بناء على خطتها أو برضاها على وقوع فعل العدوان ضد دولة أخرى، وأن تصدر الأوامر المتضمنة شن هجوم عسكري من السلطات العليا فيها. وإن كانت الدولة المعتدية غير عضو في الامم المتحدة او غير معترف بها. فلا يؤثر ذلك على اكتمال عناصرها القانونية للمساءلة عن ارتكاب جريمة العدوان. واما بالنسبة لاختصاص المحكمة الجنائية الدولية في هذه الجريمة يقتصر على الدول فقط مستبعدا صراحة اختصاصها على الفاعلين من غير الدول مثل (الجماعات الإرهابية المسلحة)[١].

وفي نفس السياق لتطبيق دليل "تالين" أقرت اللجنة بشكل ضمني في الفقرة الثانية من القاعدة ١٣ أن التحكم الفعال هو فقط ما ينهض بالمسؤولية في مواجهة الدولة مصدر الاعتداء، وكما قامت اللجنة بوضع شروط أخرى تتمثل في وضوح نتائج الهجمات أو القدرة على قياسها، بمعنى قدرة الدولة المعتدى عليها تحديد الضرر الذي تسببت به الهجمة الإلكترونية، إضافة إلى شرط الطابع العسكري للعملية الإلكترونية وهو شرط مستمد من مجمل مواد ميثاق الأمم المتحدة الخاصة باستخدام القوة والتي تربط بين استخدام القوة وبين الطبيعة العسكرية لهذه النشاطات.

٤- الركن الشرعي فهو ركن عام لجميع الجرائم الدولية ولا يخص جريمة بعينها، فلا يمكن محاكمة شخص و معاقبته على جريمة لم يرد النص عليها في المادة (٥) من النظام الأساسي للمحكمة الجنائية الدولية. و بالتالي لابد من احترام مبدأ " لا جريمة و لا عقوبة إلا بنص" الذي يعد أساسيا سواء في القانون الجنائي الداخلي أو الدولي.

ونصل إلى نتيجة مفادها تطبق المحكمة الجنائية الدولية في تجريم العدوان و المعاقبة عليها اركان الجرائم الواردة في نظامها الأساسي، كما تطبق القواعد الإجرائية و قواعد الإثبات الخاصة بذلك، وتعمل بالمعاهدات الواجبة التطبيق و قواعد ومبادئ القانون الدولي العام و الإنساني، المطبق في النزاعات المسلحة. وكذلك المبادئ العامة للقانون التي نستخلصها من القوانين الوطنية للنظم القانونية في العالم حسبما يكون مناسبا، شريطة إلا تتعارض هذه المبادئ مع النظام الأساسي و القواعد المعترف بها دوليا. ونظرا لعدم شمول قواعد القانون الدولي الحرب السيبرانية أو الهجمات السيبرانية بشكل خاص، إذ أمضت مجموعة من علماء القانون سنوات في العمل لتوضيح كيفية تطبيق القانون الدولي على الحرب الرقمية. وقد شكل هذا العمل أساس دليل خاص بالحرب السيبرانية سُمِّي (دليل تالين) ،وإن كان غير ملزم، وهو كتاب أعدته تلك المجموعة بدعم من مركز التميز للدفاع الإلكتروني التعاوني المرتبط بحلف الناتو (CCDCOE) ومقره العاصمة الإستونية تالين، التي سمي الدليل باسمها.

المطلب الثاني- المسؤولية الدولية الناشئة عن جريمة العدوان بالهجمات السيبرانية

يعتبر فعل العدوان جريمة دولية لأنه يشتمل على النتائج القانونية للجريمة الدولية. كذلك ما يؤكد عليه ميثاق الأمم المتحدة من حقوق والتزامات. و طبقا لنص المادة الخامسة الفقرة الثانية من قرار الجمعية العامة لتعريف العدوان " إن حرب العدوان هي

[١] إبراهيم الدراجي، جريمة العدوان ومدى المسؤولية القانونية الدولية عنها، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٥،ص٥٢٤.

جريمة ضد السلم الدولي. وإن العدوان هو ما يعترف به قانونا ". وتمارس المحكمة الاختصاص على الجريمة العدوان متى اعتمد حكم بتعريف هذه الجريمة وفقا للمادتين (١٢١،١٢٣) من النظام الأساسي للمحكمة الجنائية الدولية. وسبق أن ذكرناها في أحكام المحكمة الجنائية الدولية للنظر في جريمة العدوان. وتثير جريمة العدوان مسئولية قانونية دولية مزدوجة مدنية وجزائية. حيث يقصد بالمسئولية المدنية الدولية إلزام دولة ما بأداء تعويض مادي أو معنوي نتيجة لارتكابها بصفتها أو ارتكاب أحد اشخاصها باسمها فعلا غير مشروع في القانون الدولي ترتب عليه ضرر مادي أو معنوي لدولة أخرى أو لرعاياها، فقوام هذه المسؤولية هو التعويض وإصلاح الضرر وتنقسم إلى مسئولية عقدية نتيجة إخلال الدولة باتفاق تعاقدي بينها وبيد دولة أخرى، بينما تنهض المسئولية التقصيرية لإخلالها بالتزاماتها القانونية التي يفرضها عليها القانون الدولي العام(١).

إن ارتكاب جريمة العدوان هو إخلال بالتزام تعاقدي دولي، فنتيجة لإبرام اتفاق كميثاق الأمم المتحدة وما تضمنه من قواعد وأحكام لحظر استخدام القوة في العلاقات الدولية وتحريم حرب العدوان فقد ترتب على ذلك كله أن أصبح بحرب عدوانية من جانب أية دولة اشتركت في إحدى هذه الاتفاقيات أو انضمت إليها لاحقا يعتبر إخلالا بالتزام تعاقدي تترتب عليه مسئولية تعاقدية قبل الدولة المخالفة(٢).

وأما المسئولية الجزائية فهي تعني عموما وجوب تحمل الشخص تبعة عمله المجرم بخضوعه للجزاء المقرر لهذا العمل القانون. فالمسئولية الجزائية الدولية تعني مساءلة دولة ما عن ارتكابها فعلا يعتبره القانون الدولي جريمة دولية ومعاقبتها من قبل المجتمع الدولي، بالعقوبات المقررة للجريمة الدولية المرتكبة وخضوعها للجزاءات التي تكفل ردعها عن تكرار ارتكاب جريمتها الدولية. وتتمثل شروط المسؤولية الدولية بما يلي:-

١. وجود فعل أو امتناع عن فعل من شخص من أشخاص القانون الدولي العام.
٢. الحاق ضرر بشخص من اشخاص القانون الدولي العام بأي شكل.
٣. أن يكون هذا الفعل أو التصرف غير مشروع بالاستناد إلى الشرعية الدولية.

وفي محاولة للربط بين شروط قيام المسؤولية الدولية والهجمات الإلكترونية نجد أن حصول الهجمة من شخص قانوني دولي (الدولة)، وذلك بالرجوع للشرط الأول فهذا يعني حصولها من جهة غير دولية لا يبرر قيام المسؤولية الدولية وعند البحث بالشرط الثاني وهو الحاق الضرر فهذا أمر جوهري وفي غاية الأهمية ولقد بينا مدى الخطورة الكبيرة التي ممكن أن تلحقها الهجمات الإلكترونية عندما تستهدف مصالح استراتيجية دولية وحساسة، في نفس الوقت فعنصر الضرر شيء واقع لا محال عندما تقع بشكل كبير وعدواني، وكذلك أن هذا الموضوع –الضرر- ليس بحاجة إلى التبرير لأنه مبرر أساسي لحصول المسؤولية الدولية، لأنه على الأغلب تكون الهجمة الإلكترونية الدولية باستهداف مصالح ذات قيمة وأهمية، وليست بمصالح فردية بسيطة، وبذلك لا نستطيع إبعاد عنصر الضرر عن الهجمة الدولية لأن الضرر والتأثير هو هدفها الأساسي. وعند البحث في الشرط الأخير نجد أن الفعل غير المشروع الذي يعد انتهاكاً لأحكام القانون الدولي العام أو مخالفة لقواعد القانون الدولي أو المبادئ العامة للقانون، وبذلك أن فعل الهجمات الإلكترونية هو غير مشروع ابتداء، وهو بحد ذاته ينتهك أحكام وقواعد القانون الدولي لأنه يخترق أسرار ووثائق الدول ويستهدف مصالحها الكبرى ويختلق مشاكل وقضايا دولية معاصرة لم تكن موجودة في السابق في عهد الحروب التقليدية ولا حتى الحرب الباردة، فهذا التسابق في التسلح التقني الجديد نعتبره في غاية الخطورة والدقة والأهمية (٣).

وبعد العرض السابق نصل إلى نتائج عناصر وشروط المسؤولية الدولية أهمها أن الإخلال بالالتزام الدولي ينتج المسؤولية الدولية التي بحد ذاتها تخترق وتخل بقواعد القانون الدولي الذي يوجب التعويض، وبحصول الضرر من الفعل المخالف لأحكام القانون الدولي أما إذا لم يحصل ضرر فإن المسؤولية الدولية لا تقوم. إذاً الضرر هو الأساس في قيام المسؤولية ولزوم التعويض.

والمسؤولية عن الجرائم الدولية تكون على الإخلال بالتزام دولي على درجة كبيرة من الأهمية، وضروري لحماية المصالح الأساسية للمجتمع الدولي، ويعتبر الإخلال به جريمة في نظر المجتمع الدولي بأسره، ويندرج تحت الجريمة الدولية الإخلال الجسيم بالالتزام له أهمية في المحافظة على السلم والأمن الدوليين، مثل تحريم الاعتداء على سيادة الدول واستقلالها، وكذلك الإخلال بالتزام يهدف إلى حماية حق تقرير المصير مثل تحريم الاستعمار، وكذلك الإخلال الجسيم بالتزام يهدف إلى حماية الإنسان مثل تحريم العبودية وجرائم الإبادة الجماعية، وأخيراً الاخلال الجسيم في الالتزام يهدف إلى حماية بيئة الإنسان التي يعيش فيها مثل حماية الهواء من التلوث وحماية البيئة البحرية وبإدراج هذه الجرائم الدولية نجد تطابقها إلى حد ما مع الهجمات الإلكترونية، عند تعرض السلم والأمن الدوليين للخطر وحماية الإنسان وحقه في العيش الكريم، من تعرض مصالحه التي تحميها وتقررها الدول وكذلك حماية البيئة التي يعيش فيها الإنسان لأن حدوث فعل الهجمات قد يلحق أضراراً قد تحدث الكثير من الجرائم الدولية السابق ذكرها.

فالأســاس القانوني للمسؤولية الدولية كان أســاســه الخطـأ ونظرية المخاطر، هذا في القانون الدولي التقليدي، أما في القانون الدولي المعاصر، فإن الإحساس الجوهري للمسؤولية الدولية هو العمل الدولي غير المشروع، فالبحث في موضوع المخاطر عند ممارسة الدولة نشاطاً ذات طبيعة خطيرة وغير مألوفة تتحمل الدولة مسؤوليتها عن الأضرار التي تصيب الدول الأخرى، من هذه النشاطات وأكثر ما يهمنا في هذا الصدد الاعتبار الذي يتحدث عن التطور العلمي والتكنولوجي والأنشطة المتصلة به، فنشاط الانترنت يندرج تحت بند المخاطر الدولية التي تقع الدولة في خانة المسؤولية الدولية عند اتهامها في إحداث هجمة الكترونية دولية.

---

(١)د. إبراهيم الدراجي، جريمة العدوان ومدى المسؤولية القانونية الدولية عنها،ط١، منشورات الحلبي،٢٠٠٥،ص٥٧٧.

(٢)د. إبراهيم الدراجي، جريمة العدوان ومدى المسؤولية القانونية الدولية عنها، مرجع سبق ذكره ،ص٥٧٨،

(٣)عمر حسن عدس، محاضرات في القانون الدولي العام المعاصر ،ديوان المطبوعات، الجزائر،١٩٩٥،ص٥٤٠.

الخاتمة

يعد العدوان بالهجمات السيبرانية جريمة دولية، متكاملة الأركان وتترتب عنها المسؤولية الدولية، وذلك باستخدام القوة لدولة ما غير التقليدية ضد دولة أخرى وتمس بسيادتها و استقلالها السياسي. باستخدام التكنولوجية التي ظهرت مؤخر التكنولوجي وانتشرت بسرعة لإرتباطها بجهاز الحاسب الآلي (الكمبيوتر), وتتمثل أداة الهجمات السيبرانية في شبكة الإنترنت, إذ يثير هذا النوع من العدوان في مجمله الكثير من الإشكالات من مختلف الجوانب ؛ ثباته, واتسامه بطابع كصعوبة اكتشافا والحيلة والدهاء من طرف مرتكبيه ؛ من خلال استعمال تقنيات معلوماتية عالية الكفاءة , مما يؤدي إلى اختراق الشبكات, وأجهزة الحاسب الآلي المرتبطة بالإنترنت, حيث يتم اختراق نظام الأمن بالشبكة والدخول إلى الجهاز للكشف عن محتوياته, أو إتلافها ,والتلاعب بالمعلومات المخزنة فيه، وتنفيذ هجمات عسكرية على المواقع العسكرية. وإن وضع العدوان بالهجمات السيبرانية كجريمة دولية في إطار قواعد القانون الدولي صعبة جدا، بسبب الطبيعة الخاصة بها، ولعدم وجود قواعد قانونية دولية تحكمها. و لكن يمكننا إجمال البحث في النتائج الآتية:

النتائج:

١- الهجمات السيبرانية بوسائلها المختلفة تشكل قوة تدميرية هائلة قد تفوق القوة بالهجمات العسكرية التقليدية. وتصيب اهادفها بدقة سواء كانت اهداف مدنية او عسكرية.

٢- إن الهجمات السيبرانية تشكل حالة من حالات العدوان غير المباشر، و لها مكانة في تعريف الجمعية العامة لقرار تعريف العدوان ٣٣١٤ لعام ١٩٧٤ لأن هذا الفعل يعد انتهاك خطير لما نص عليه ميثاق الأمم المتحدة.

٣- العدوان بالهجمات السيبرانية جريمة دولية متكاملة الاركان بالاستناد إلى الاساس القانوني أحكام المحكمة الجنائية الدولية والاعتماد على (دليل تالين) ،وإن كان غير ملزم، فقد شكل هذا العمل أساس دليل خاص بالحرب السيبرانية .

٤- العدوان بالهجمات السيبرانية جريمة دولية طبقا لقواعد القانون الدولي العام تنشأ عنها المسؤولية الدولية يشقيها المدني (الدولة) و الجنائي (الاشخاص).

التوصيات:

١- اعطاء تفسير أوسع لقرار الجمعية العامة لتعريف العدوان، ليشمل جميع الظروف المتغيرة، المتعلقة بوسائل واساليب الهجمات الإلكترونية.

٢- ابرام اتفاقيات دولية تعمل على تقييد استخدام تكنلوجيا المعلومات بصورة هجمات سيبرانية، إذا كان من العسير برمجتها وفقاً للتطبيق الأمثل لقواعد القانون الدولي.

٣- أن تعمل لجنة اركان الحرب التابعة لمجلس الأمن على إدراج الهجمات السيبرانية من ضمن القوة المسلحة للدول مع بيان مخاطرها على المجتمع الدولي والبشرية جمعاء.

٤- إنشاء وكالة دولية تضم خبراء وفنيين في المجال الإلكتروني تعنى بالكشف عن الهجمات السيبرانية وتقدم المساعدة الفنية للدول التي تتعرض إلى هذا النوع من الهجمات وإن ما حدث من دمار كانت نتيجة تعرضها لهجوم إلكتروني.

٥- إقرار مسؤولية الدولة على جميع التصرفات التي يقوم بها افراد أو مجموعات يعملون في ضوء تعليماتها أو تحت ادارتها أو سيطرتها، لتشمل جميع العناصر المساهمة في البرامج الإلكترونية التي تشكل خرقاً لالتزام دولي، فضلاً عن المسؤولية الجنائية الفردية، والتمكين من الملاحقة القضائية لأشخاص يقفون وراء المرتكبين المباشرين لجريمة العدوان.

٦- على المجتمع الدولي أن يسخر أن يبذل المزيد من الجهود في وجه هذا النوع من العدوان (الهجمات السيبرانية) للحد من انتشاره.

قائمة المراجع

١. إبراهيم الدراجي، جريمة العدوان ومدى المسؤولية القانونية الدولية عنها، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٥.

٢. احمد عبيس نعمة الفيتلاوي، الهجمات السيبرانية مفهومها و المسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية و السياسية، جامعة بابل ،كلية القانون، العدد الرابع- السنة الثانية،٢٠١٦.

٣. ايهاب خليفة، القوة الإلكترونية وابعاد التحول في خصائص القوة، مكتبة الاسكندرية،٢٠١٤.

٤. بشرى حسيت الحمداني، القرصنة الإلكترونية: أسلحة الحرب الجديدة، نبلاء ناشرون وموزعون، عمان ،٢٠١٣.

٥. جون باسيت، حرب الفضاء الإلكترونية: التسلح و أساليب الدفاع الجديدة، الحروب المستقبلية في القرن الواحد و العشرين،ط١، مركز الإمارات للدراسات و البحوث الإستراتيجية،٢٠١٤.

٦. رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة للعلوم القانونية، المجلد ١٥، العدد ٢، ربيع الثاني١٤٤٠- ديسمبر- ٢٠١٨ .

٧. سراب أحمد تامر، الهجمات على شبكات الحاسوب في القانون الدولي الإنساني، أطروحة دكتوره، جامعة النهرين كلية الحقوق،بغداد،٢٠١٥.

٨. صلاح الدين احمد حمدي، دراسات في القانون الدولي العام، منشورات ELGA،مالطا،٢٠٠٢.

٩. عمر حسن عدس، محاضرات في القانون الدولي العام المعاصر ،ديوان المطبوعات، الجزائر،١٩٩٥.

١٠. علي جميل حرب، منظومة الفضاء الجزائي الدولي للمحاكم الجزائية الدولية و الجرائم الدولية المعتبرة،

١١. كمال حماد، النزاع المسلح والقانون الدولي العام، ط١، المؤسسة الجامعية للدراسات والنشر و التوزيع،بيروت،١٩٩٧.

١٢. محمد عبدالله ابوبكر، جرائم الكمبيوتر و الانترنيت، منشأة المعارف، الاسكندرية، ٢٠٠٦.

١٣. موسى نعيم، نهاية عصر القوة من قاعات اجتماعات مجلس الإدارة إلى ساحات الحرب و الكنائس إلى الدول لماذا لم يعد تولي المسؤولية كما كان في السابق؟، ط١، مركز الإمارات للدراسات و البحوث الإستراتيجية،٢٠١٦ .

١٤. نوران شفيق، أثر التهديدات الالكترونية على العلاقات الدولية (دراسة في ابعاد الأمن الالكتروني)، المكتب العربي للمعارف، القاهرة،٢٠١٦.

ملخص البحث

تقام المسؤولية القانونية الدولية عن جريمة العدوان كونها من الجرائم الدولية، التي تنظر فيها المحكمة الجنائية الدولية. كما أن نظامها الأساسي تبنى تعريف العدوان، الذي ورد في المادة الأولى من قرار تعريف العدوان رقم ٣٣١٤ لعام ١٩٧٤.إذ تضمن على العدوان بشكله التقليدي، وكذلك اعتمد على الأفعال التي جرمها القرار التي وردت في مادته الثالثة.

ويتناول هذا البحث المسؤولية الدولية عن جريمة العدوان بالهجمات السيبرانية كونها، تشكل فعل من افعال العدوان التي لم ترد في المادة الثالثة من القرار المذكور، ولا تتم باستخدام القوة المسلحة بمفهومها التقليدي وإنما تتم بواسطة الأسلحة الافتراضية التي ترتكب في الفضاء الإلكتروني، وتعتدي على السلامة الإقليمية و الاستقلال السياسي للدول ويركز البحث على مدى ملاءمة قواعد المسؤولية الدولية التي تترتب على جريمة العدوان بشكلها التقليدي، على جريمة العدوان بشكلها الحديث المتمثل في الهجمات السيبرانية.

الكلمات الافتتاحية: المسؤولية الدولية- العدوان- الهجمات السيبرانية- الجريمة الدولية- المحكمة الجنائية الدولية

Abstract

International legal responsibility is established for the crime of aggression as it is an international crime, which is considered by the International Criminal Court. Its statute also adopted the definition of aggression, which was contained in Article 1 of the Definition of Aggression Resolution No. 3314 of 1974. It included aggression in its traditional form, as well as relied on the acts criminalized by the resolution contained in its third article

This research deals with the international responsibility for the crime of aggression by cyber-attacks, as it constitutes an act of aggression that is not mentioned in Article 3 of the aforementioned resolution, and is not carried out by using armed force in its traditional sense, but rather by virtual weapons that are committed in cyberspace, and infringe on territorial integrity and political independence of states.

The research focuses on the appropriateness of the rules of international responsibility that result from the crime of aggression in its traditional form, to the crime of aggression in its modern form represented by cyber-attacks.

keywords: international responsibility, aggression, Cyber attacks, international crime, International Criminal Court.