مجلة جامعة تشرين – سلسلة العلوم الاقتصادية والقانونية

Violating The Sovereignty Of States Over Their Cyberspace The Crime Of Electronic Attacks As A Model

Dr Nidal Alou*

(Received 19 / 4 / 2023. Accepted 2 / 5 / 2023)

□ ABSTRACT □

Modern technologies of communication systems and digital systems are considered an essential part in the life of nations and individuals in the modern world, but at the same time these systems constitute a serious threat on the security of the states.

This study aimed at discussing the topic of cyberspace as a new type of conflicts and disputes between states and it shows the importance and seriousness of cyber- attacks.

The study focuses on the inclusion of Cyber- attacks and Aggression against states, international actors must adopt these attacks effectively and they must find legal justification in the Public International Law Allows to use the right of self- defense in the event of an international electronic attack.

However, there is no legal justification until now that allows self- defense in this type of attacks or legal item that puts these attacks under unarmed and indirect aggression.

* **Assistant Professor, Administrative Sciences, Al-Ittihad Private University, Syria.**
nedallb@tishreen.edu

انتهاك سيادة الدول على فضائها الإلكتروني
جريمة الهجمات الإلكترونية نموذجاً

الدكتور نضال علو*

(تاريخ الإيداع 19 / 4 / 2023. قُبِل للنشر في 2 / 5 / 2023)

□ ملخّص □

هذا البحث مخصص لمناقشة موضوع العدوان في الهجمات الالكترونية بوصفه نوعا جديدا من أنواع الصراع والخلاف بين الدول، وأنها ستصبح واقعة مستقبلاً.

يركز هذا البحث على ضرورة شمول الهجمات الإلكترونية بما يسري على الهجمات المسلحة وضرورة استعمال حق الدفاع الشرعي للدول التي تتعرض لهذه الهجمات بناء على نصوص ميثاق الأمم المتحدة والقانون الدولي العام، فعلياً لا يوجد أي سند قانوني يبرر استخدام حق الدفاع الشرعي ضد هذا النوع من الهجمات، ولكن في هذا الصدد نستطيع أن نوردها تحت بند العدوان غير المسلح وغير المباشر.

* أستاذ مساعد، العلوم الادارية، جامعة الاتحاد الخاصة، سورية. nedallb@tishreen.edu

مقدمة:

أصبح من الضروري البحث في مجال الفضاء الإلكتروني بوصفه بعداً جديداً للصراع الذي لم يكن يتوافر في القانون الدولي العام سابقاً، فقد كان من المعروف بأن المبرر الوحيد لحالة الدفاع الشرعي هو حصول هجوم مسلح من إحدى الدول على دولة أخرى عضو في الأمم المتحدة، وبما أن الرأي قد اختلف حول العدوان غير المسلح غير المباشر مثل العدوان الاقتصادي والأيديولوجي، حيث ذهب البعض إلى أن حق الدفاع الشرعي يسري في مواجهة هذا النوع من العدوان.

ومن هنا برزت الحاجة إلى إدراج هذا النوع من العدوان بوصفه إحدى صور العدوان غير المسلح غير المباشر. قياساً على ما سبق، وبما أن العمليات الالكترونية تتجاوز الهجوم المسلح في بعض الأحيان، الأمر الذي يسمح للدول بالدفاع عن نفسها بالقوة بما فيها القوة الالكترونية حسب المادة 51 من ميثاق الأمم المتحدة والقانون الدولي، لأن مفهوم الهجمات المسلحة على الأقل يشمل عمليات الكترونية ممكن أن تدمر منشآت استراتيجية وخدماتية ودمارها قد يؤدي إلى الأضرار الجسيمة أو الموت أحياناً.

وبالعودة إلى ميثاق الأمم المتحدة فقد كان ذلك محصورا في المادة 2 فقرة 4 من ميثاق الأمم المتحدة التي تمنع الدول عن التهديد باستعمال القوة او استخدامها ضد سلامة الأراضي او الاستقلال السياسي لأية دولة أو على وجه آخر لا يتفق ومقاصد الأمم المتحدة.

إشكالية البحث:

تكمن إشكالية البحث في الإجابة عن السؤال الآتي:

هل يمتد حق الدفاع الشرعي في القانون الدولي العام ليشمل مواجهة الهجمات الإلكترونية والرد عليها؟

منهجية البحث:

سوف يتم اعتماد المنهج الوصفي التحليلي لدراسة قضايا هذا البحث.

خطة البحث:

تم تقسيم هذا البحث إلى مطلبين وكل مطلب إلى فرعين وفق الآتي:

المطلب الأول: الهجمات الإلكترونية كظاهرة إرهابية دولية ومخاطرها

الفرع الأول: الهجمات الإلكترونية كظاهرة إرهابية دولية

الفرع الثاني: مخاطر الهجمات الالكترونية في القانون الدولي العام

المطلب الثاني: علاقة الهجمات الإلكترونية بجريمة العدوان والمسؤولية الدولية في فعل الهجمات الالكترونية

الفرع الأول: الهجمات الالكترونية وعلاقتها بجريمة العدوان.

الفرع الثاني: المسؤولية الدولية في فعل الهجمات الإلكترونية.

المطلب الأول

الهجمات الإلكترونية كظاهرة إرهابية دولية ومخاطرها

سيتم في هذا المطلب البحث في الهجمات الإلكترونية باعتبارها ظاهرة إرهابية دولية، بالإضافة إلى مخاطرها وفق القانون الدولي العام وذلك في الفرعين الآتيين.

الفرع الأول

الهجمات الإلكترونية كظاهرة إرهابية دولية

في مطلع الحديث عن الإرهاب الدولي تجدر الإشارة إلى الحديث عن ظهور مصطلح الإرهاب بصورته العصرية الحديثة، فكانت أحداث الحادي عشر من أيلول نقطة التحول العالمية الجديدة في مفهوم الإرهاب الدولي، ويستخدم مصطلح الإرهاب للدلالة على أعمال العنف التي تهدف إلى إثارة الرعب في المجتمع الدولي أو الداخلي.

وفي التعمق أكثر في موضوع الإرهاب الدولي نجد أن ثمة صلة وثيقة بين الإرهاب الدولي والهجمات الإلكترونية في الركن المعنوي. (القصد الجرمي) فمثيري الهجمات الإلكترونية لا يختلفون عن منفذي العمليات الإرهابية التقليدية من حيث المضمون، لأن هدفهم ونيتهم واحدة فهؤلاء يستخدمون المتفجرات ويخطفون الطائرات ويزرعون الرعب في المجتمعات، وهؤلاء يثيرون الرعب والخوف إلا أن طريقة تنفيذ هذا الإرهاب تختلف نوعاً ما لأن منفذي الهجمات الإلكترونية يستعملون التقنيات الحديثة الموجودة في أجهزة حواسيبهم للاختراق والتدمير والعبث غير المسؤول.

وبدقة أكثر، فإننا عندما نتحدث عن هجمات إلكترونية بمفهومها الدولي الصادر من جهة دولية أو منظمة دولية ضد جهة دولية أخرى فإن خطر الارهاب الدولي سوف يتسع تأثيره ومداه إلى المصالح الفردية، لأن الدولة في الأساس من أهم واجباتها حماية مقدرات الأفراد من التعدي والعبث والدمار، فخطر الهجمات الإلكترونية أثره كبير وفعال كخطر الإرهاب الدولي، وكما أنه للإرهاب الدولي دوافع سياسية واقتصادية وتاريخية ثم إعلامية وشخصية فإن للهجمات الإلكترونية نفس الدوافع لا بل أكثر أحياناً[1] .

في البداية نتحدث عن الدوافع السياسية نجدها واحدة، فعندما اندلعت الانتفاضة الفلسطينية في 27 أيلول من عام 2000 لسبب الانتهاكات "الإسرائيلية" للاتفاقيات المبرمة مع الفلسطينيين حول الحكم الذاتي ومفاوضات الوضع النهائي وحل قضية القدس– مع أنه كما يرى الباحث– الكفاح الفلسطيني لا يعد بتاتاً إرهاباً بل الأعمال المرتكبة ضد الشعب الفلسطيني تعتبر إرهاباً من طرف إسرائيل لأن كفاح الشعب الفلسطيني معترف به من قبل القانون الدولي والمنظمات الدولية جميعها على حد سواء، لأنه كفاح مسلح من أجل الحصول على تقرير حق المصير.

يرى الباحث أن جماعة (الأنونيمس) عندما اخترقوا المجال الافتراضي لإسرائيل ودمروا البنية التحتية الفضائية بالإغراق والهاكرز كان لدوافع سياسية بحتة ووجه الشبه واضح في الدوافع السياسية بين الإرهاب الدولي والهجمات الإلكترونية.

وعند إدراج الدوافع الاقتصادية لأنها كما هو معلوم القوة الجديدة في نظريات العالم المعاصر لأن تسمية غني ارتبطت بقوي وضعيف ارتبطت بفقير، فأصبح التدمير المتعمد لاقتصاديات بعض الدول من أهم دوافع الإرهاب في الوقت الحاضر، كما هو من أهم دوافع الهجمات الإلكترونية، فعندما قامت بعض الجهات المجهولة بزرع الغام بحرية بجزء من البحر الأحمر من أجل حرمان مصر من عائدات قناة السويس والإضرار باقتصاد دول الخليج لأن البترول وكما هو معروف أهم ركيزة للاقتصاد الخليجي[2]، مثلما فعل تماماً منفذي الهجمة الإلكترونية على مفاعل بوشهر الإيراني

[1] **حمودة، منتصر سعيد، الإرهاب الدولي، بدون طبعة، دار الجامعة الجديدة، الإسكندرية. (2006)، ص146.**

[2] **حمودة، منتصر سعيد، الإرهاب الدولي، مرجع سابق ، ص 147.**

والمنشآت النووية الإيرانية وأجهزة الطرد المركزي هناك التي تعتبر الساعد المهم في الاقتصاد الإيراني في حال نجاح هذا المفاعل وتحقيق أهدافه، وبذلك نجد أن الدافع الاقتصادي يوازي إلى حد كبير بين الإرهاب الدولي والهجمات الإلكترونية.

وعند الحديث عن الأسباب الدينية نجد أن الولايات المتحدة الأمريكية وفي مرحلة ما بعد حرب الخليج الثالثة 2003، واحتلال بغداد حاولت إثارة الفتنة الطائفية بين المسلمين السنة والشيعة، ونجد أن أمريكا وضعت أسلوب جديد للتدخل وهو التدخل لأسباب دينية بجانب يضفي عليه الصفة التشريعية فأصدر الكونجرس عام 1998 تشريعاً يسمح للولايات المتحدة الأمريكية فرض عقوبات اقتصادية، وعسكرية وسياسية على لدول التي تمارس الاضطهاد ضد الأقليات الدينية والطوائف المضطهدة[3] .

ولعل الدافع الأبرز والأهم المرتبط ارتباطاً وثيقاً بين الإرهاب الدولي من جهة والإرهاب الإلكتروني والهجمات الإلكترونية من جهة أخرى هو الدافع الإعلامي.

ونجد أن التطور العلمي الهائل الذي امتد ليشمل كل نواحي الحياة والذي أصبح يتيح للقنوات الإعلامية نشر أخبار وآراء الإرهابيين ويكون ذلك من خلال تغطية إعلامية ونقل الحدث لحظة بلحظة وعلى الهواء مباشرة ونتيجة لهذا التسابق المحموم بين وسائل الإعلام في السرعة لنقل الخبر وتهويله وجدت الجماعات الإرهابية تتخذ من الإعلام وسيلة لتسويق جرائمها وأعمالها الإرهابية إن لم تتخذ في بعض الأحيان قناة خاصة لها[4] .

ومثل جريمة الإرهاب الدولي المرئية على الإعلام نجد أن الهجمات الإلكترونية تستخدم الشبكات الإلكترونية نفسها التي يستخدمها الإرهابيون الدوليين.

بحيث إن عملية قرصنة المواقع الإلكترونية والدخول على عناوين البريدية تعود لأشخاص آخرين أصبح من السهل التشهير بهم من خلال بث المعلومات غير الصحيحة والمشوهة عنهم، من خلال مواقع التواصل الاجتماعي والشبكات الغير محمية، بحيث يتطلع كل شخص على هذه المعلومات التي تكون في غاية السرية والدقة أحياناً.

ولعل ثمة صوراً متعددة للإرهاب الدولي، وفي الماضي كان الإرهاب عبارة عن اغتيالات سياسية وتخريب المنشآت المدنية والاقتصادية ومن أهم صور الإرهاب الدولي، اختطاف الطائرات وتغيير مسارها بالقوة واحتجاز الرهائن، والاغتيالات[5].

وأهم وسيلة ربط بين الهجمات الإلكترونية وصورة التخريب للمنشآت الاقتصادية والمدنية في الإرهاب الدولي عنصر التخريب الذي يتفق بين الهجمات الإلكترونية والإرهاب الدولي.

ولعل من الأمثلة على هجمة الكترونية ارهابية دولية ما فعله جماعة (ماركس هيس) عندما هجموا على البنتاغون بحيث أن هذه المجموعة توصلت إلى خمسين جهاز حاسوب عسكري في البنتاغون ومجموعة شركات متعاقدة معها ومعمل الطاقة النووية في لوس الاموس ومعمل ارجون القومي وقسم النظم الفضائية للقوات الجوية وعدد من القواعد العسكرية المنتشرة في العالم، وطبقاً للتقارير أن نظم البنتاغون

قد هوجمت 250 ألف مرة بمستوى نجاح وصل إلى 160 ألف مرة وكان صاحب النجاح فتى بريطانيا عمره 16عاماً، أطلق على نفسه (راعي بقر تيار) ويعمل تحت إشراف رجل يستعمل البريد الإلكتروني يسمى (كوجي)، وبنظر الخبراء أن هذه المعلومات ليس لها أهمية استخباراتية لأن المعلومات الموجودة داخل وزارة الدفاع الأمريكية والمعرضة للاختراق

---

[3] الشكري، علي يوسف، الإرهاب الدولي في ظل النظام العالمي الجديد، بدون طبعة، ابتراك للنشر، القاهرة،(2008)، ص77.

[4] الشكري، علي يوسف، الإرهاب الدولي ... ، مرجع سابق، ص 79.

[5] حشمت درويش، الإرهاب الدولي وعمليات انقاذ الرهائن، بدون طبعة، بدون مكان نشر، مدبولي الصغير، ص26.

كانت تخص أموراً لوجستية وهذا في حد ذاته يعتبر كافياً للكشف عن قدرات الأمة الدفاعية ونواياها مثل نشاطها داخل مستودع معدات أو ذخيرة[6] .

ولعل الرابط الأقوى أن الحروب القادمة ستكون ضحاياها أقل أي أنها ليست حرب فيها إزهاق أرواح، أو قتل أو أخذ رهائن أو أسرى، بمعنى آخر أن الخسائر الإستراتيجية ستكون في الحرب الافتراضية القادمة أكثر فداحة من الإرهاب التقليدي والحروب التقليدية.

ولذلك نجد أن هذه الحروب والهجمات الإلكترونية ستكون أكثر تدميراً في المستقبل ومما لا يقبل الشك فيه أنها سوف تتسبب في شلل بلاد كاملة وعزلها عن العالم وإبعادها كل البعد وإعادتها إلى عصور الظلام البدائية لأنه حتى أقل الدول حضارة وتقدماً تكنولوجياً أصبحت شبكة الانترنت عبارة عن القلب النابض بكل ما فيها من خدمات واقتصاديات حتى أنها دخلت في كل مجالات الدولة الحديثة ومقدراتها.

الفرع الثاني

مخاطر الهجمات الالكترونية في القانون الدولي العام

لا بد من التطرق في هذا المجال إلى القانون الدولي العام كون خطر هذه الهجمات إذا امتد إلى دول أخرى يورث مصائب وكوارث قد لا يحمد عقباها[7]

حظرت المادة (2) فقرة (4) من ميثاق الأمم المتحدة استخدام القوة في العلاقات الدولية إلا في حالات معينة ومنها الإجراءات المتخذة في جزء منها عمليات الأمن الجماعي والفردي، وإن هذه الإجراءات هي وسيلة الدفاع عن النفس في حال حصول أي اعتداء على الدول[8] .

وتوضح الفقرة (4) من المادة (2) من الميثاق استخدام القوة والهجوم العسكري وتبحث وتناقش في القوة المسلحة، إلا أنه لم يتم التطرق فيها إلى موضوع الهجمات الإلكترونية وتحدياتها وعليه فإن هذا الجزء من المادة لم يقدم خطوط قانونية ضابطة وواضحة[9].

وبذلك نجد أن الإجراءات والمبادئ القانونية في الهجوم الإلكتروني يجب أن تمنع أطراف الدولة في علاقاتهم الدولية من استخدام القوة ضد السلامة الإقليمية والاستقلال السياسي أو في أي حالة أخرى تتنافى وتختلف عن أهداف ومبادئ الأمم المتحدة[10].

أي أن ما يهدد استقرار الدولة في أي مجال يجب اعتباره هجوم مسلح وبذلك نخلص إلى أن الهجمات الإلكترونية تهدد حماية واستقرار دول العالم كافة [11].

يرى الباحث أنه عند حدوث الهجمة الإلكترونية على أحد الدول الأعضاء في الأمم المتحدة وتتبناها جهة دولية معترف بها فيجب هنا على مجلس الأمن أن يتخذ التدابير المناسبة والإجراءات الفعالة لردع هذه الهجمة، والجدير بالذكر أن نص المادة (39) لم يضع تعريفاً محدداً للعدوان، بل تركها دائرة موسعة حتى يستطيع مجلس الأمن تكييف أي تصرف من شأنه تعريض سلامة الدول للخطر وبذلك نستطيع أن ندرج الهجمات الإلكترونية تحت هذا البند.

---

[6] ورقة عمل لمحمد محمد الألفي، العوامل الفاعلة في انتشار جرائم الإرهاب عبر الانترنت، في المؤتمر الدولي لحماية أمن المعلومات والخصوصية في قانون الانترنت 2008.

[7] Michael. N. Schmitt, The thin justice of international law, p. 177.

[8] The Law of Cyber Attack the California Law Review 2012 p.29.

[9] Article Cyber- attacks and the use of force: Back to the future of the Article 2 (4) .p. 426.

[10] The Law of Cyber Attack the California Law Review 2012 p.27

[11] International Law Studies p.116.

ويرتكز الهجوم الإلكتروني على ثلاثة أركان رئيسية أهمها وجود الدافع من وراء أحداث هذه الهجمة والركن الثاني هو الوسيلة أو الطريقة لإحداث الهجمة، أما الركن الثالث فهو وجود ثغرة في النظام المراد اختراقه، ويرى المتابع بأن أغلب الهجمات الإلكترونية يكون منفذيها هواة لا يوجد لهم أي أهداف. بينما تتكون نسبة ضئيلة منهم مما يسمون مرتزقة الكترونيين.

والناظر في شرح المادة (39) من الميثاق يلاحظ أنها تعطي وتمنح سلطات واسعة لمجلس الأمن لتحديد وجود أي تهديد أو خرق لشروط السلام أو أي تصرف عدواني وتقديمها على شكل توصيات للأمم المتحدة توضح الإجراءات التي يجب اتباعها في حالة حصول هذا الخطر وبذلك فإن القانون يدعم وجوب أخذ إجراءات في حالة حصول الهجمات الإلكترونية التي تهدد وتخرق الشروط الأمنية [12].

يرى الباحث على ضوء ما سبق اعتبار الهجمات الإلكترونية من قبيل أفعال العدوان التي يعاقب عليها القانون الدولي العام وذلك من خلال تفعيل دور مجلس الأمن الذي يكيف فعل العدوان على أي تصرف غير شرعي يرتكب في حق دولة عضو في هيئة الأمم المتحدة في حال أنه ارتكب من خلال دولة تبنت هذا الهجوم أو جماعة معينة تتبع لدولة.

المطلب الثاني

علاقة الهجمات الإلكترونية بجريمة العدوان والمسؤولية الدولية في فعل الهجمات الالكترونية

في هذا المطلب سيتم بيان علاقة الهجمات الإلكترونية بجريمة العدوان، ومن ثم البحث في المسؤولية الدولية في فعل الهجمات الالكترونية وذلك في الفرعين الآتيين.

الفرع الأول

الهجمات الالكترونية وعلاقتها بجريمة العدوان

بقي موضوع العدوان واضح ومحدد المعالم أثناء حصول نزاعات مسلحة حتى ظهرت لدينا القضايا المعاصرة التي أصبحت واقعة لا محالة وتعترضها في التطبيق العملي ويلتف حولها الغموض، منهم من اعتبرها أفعال عدوان ومنهم من لم يعتبرها وحتى نراعي الدقة في البحث عن أعمال العدوان في الهجمات الإلكترونية كان لا بد لنا من أن نسلط الضوء على موضوع العدوان بشكل عام.

ولعلنا نجد أن ميثاق الأمم المتحدة قد أورد في المادة (39) من الميثاق حيث جاء فيها: "يقرر مجلس الأمن ما إذا كان قد وقع تهديد للسلم والأمن أو إخلال به أو كان ما وقع عملاً من أعمال العدوان ويقدم في ذلك توصياته أو يقرر ما يجب اتخاذه من التدابير طبقاً لأحكام المادتين (41) و(42) لحفظ السلم والأمن الدوليين وإعادتهما إلى نصابهما (مادة (39) من ميثاق الأمم المتحدة).

وعند التمعن في تعريف العدوان لا نجد أن ثمة من عرفه بشكل نهائي ومع أن كل المفاهيم الموجودة تندرج تحت العدوان، إلا أن نتوصل إلى تعريف له على النحو الآتي: أنه مجموعة أفعال تتمثل في استخدام القوة المسلحة ضد سيادة الدول أو السلامة الإقليمية أو الاستقلال السياسي، أو أي شكل آخر يتعارض مع ميثاق الأمم المتحدة، ومن

[12] **The Law of Cyber Attack the California Law Review 2012 p.80,**

صوره الهجوم بالقوة المسلحة ضد إقليم دولة أخرى أو بدء هجوم بري أو بحري أو جوي من دولة ضد دولة أخرى أو إرسال عصابات بواسطة إحدى الدول أو أي عمل ضمن السياق ذاته[13].

إن تنوع وتفاوت تعريف الهجمات الإلكترونية ومجموعة الأنشطة العدائية التي يمكن أن تنفذ من الشبكات الإلكترونية ما زالت هائلة جداً، وهذا بحد ذاته يوضح خطورة الهجمات الإلكترونية التي قد تدمر أي أنظمة ومعلومات وشبكات وبرامج عن طريق إرسال فيروسات مدمرة بشكل مباشر أو غير مباشر، مما يعد وهذه الحال تهديد لأمن واستقرار الدول[14].

كذلك فقد أكد ميثاق الأمم المتحدة على السلطة التقديرية لمجلس الأمن الدولي وبقي موضوع العدوان مصطلح فضفاض وترك الباب مفتوحاً للمجلس بحيث أنه يتمتع بسلطة واسعة في هذا الصدد، ولعل ما يؤكد لنا أن مصطلح العدوان لا يوجد له تعريف محدد هو ما وجدناه في الاختصاص الموضوعي من اختصاصات المحكمة الجنائية الدولية، بحيث تحدثت عن جريمة العدوان التي يجب تعريفها ووضع الشروط اللازمة حتى تتمكن المحكمة الجنائية الدولية من ممارسة اختصاصها تجاه هذه الجريمة، حينما يتم إقرار تعريف لها[15]. بحيث إنه لم يتم تحديدها في النظام الأساسي كالجرائم الأخرى الداخلة ضمن اختصاص المحكمة وهي جرائم الحرب وجريمة إبادة الجنس البشري والجرائم ضد الإنسانية، وتحدثت المحكمة أيضاً أن هذه الجريمة ستصبح محل اختصاص بعد تعريفها والموافقة عليها من قبل جمعية الدول الأطراف، على ضوء ما سبق نجد أن العدوان كجريمة دولية لم يوضع لها لغاية الآن تعريف محدد نستطيع أن نطلق عليه اسم تعريف العدوان.

ونجد أن الميثاق يزخر بالعبارات التي تحافظ على الجنس البشري من القتل والهلاك والدمار فتجده تارة يلزم بالحفاظ على السلم والأمن الدوليين وتارة أخرى يحرم العدوان ويطلب من المجتمع الدولي الاستجابة السريعة وإيقاف أي فعل عدوان، ونجد كذلك أن الميثاق أعطى في الفصل السابع منه صلاحيات واسعة لمجلس الأمن الدولي وذلك لضمان السلم والأمن الدوليين وجميع أعمال العدوان وكما ذكرنا سابقاً أن المادة (39) من الميثاق أوجبت على المجلس أن يقرر فيما إذا كان قد وقع تهديد للسلم والأمن الدوليين وإخلال بهما أو كان ما وقع عملاً من أعمال العدوان، وأن يتخذ تدابير مناسبة لا تتطلب استخدام القوة تتمثل في العقوبات الاقتصادية وقطع الصلات مع الدولة المعتدية وغيرها من التدابير السلمية، وإن رآها لا تكفي ولن تفي بالغرض المطلوب وأن فعل العدوان ما زال قائماً فهنا أجاز له أن يتخذ من الإجراءات العسكرية ما يراه مناسباً لوضع حلاً جذرياً لهذا النزاع (المواد 39، 40 من ميثاق الأمم المتحدة).

والملاحظ من نص ديباجة ميثاق الأمم المتحدة والمادة الأولى من الميثاق على أن من مقاصد الهيئة هي حفظ السلم والأمن الدوليين وأعطى الميثاق مجلس الأمن الصلاحية في أي نزاع يخشى أن يؤدي إلى حرب، غير أنه لا يقتصر الأمر على فرض جزاء على الدولة التي تشن عدواناً أو حرباً غير مشروعة بل من الضروري كبح جماح من يثيرها أيضاً لمعاقبة ساسة الدول كمجرمي حرب، الذين يقودون بلادهم إليها، ويجرون شعوبها إلى الويلات والمحن والمصائب[16].

---

[13]– خلف، محمد محمود، حق الدفاع الشرعي في القانون الدولي الجنائي، بدون طبعة، مكتبة النهضة المصرية، القاهرة، 1973،ص294.

[14] Article cyber- attacks and the use of force: Back to the future of article 2 (4), p.422.)

[15]– طلال ياسين العيسى، علي جبار الحسيناوي، المحكمة الجنائية الدولية، بدون طبعة، دار اليازوري، عمان، 2005، ص66.

[16]– بشير مراد، الحرب في القانون الدولي العام، الطبعة الأولى، بدون دار نشر، دمشق، 1973، ص56.

وفي التعمق أكثر في الشروط التي تعتبر الفعل غير المشروع وتجعله عدواناً نجد أن أوجه التلاقي ضعيفة بين فعل العدوان والهجمات الإلكترونية، بحيث كانت الشروط أن يكون العدوان مسلحاً، حال وقائم بالفعل ومباشر وعلى قدر من الجسامة والخطورة[17].

أضحى موضوع الهجمات الإلكترونية العدوان الذي لا يقل خطورة عن العدوان المسلح، وبذلك نجد أن حلف شمال الأطلسي (الناتو) رفع خطر الهجمات الإلكترونية إلى مستوى (الاعتداء العسكري) وأن الحلف بصدد وضع آلية للتعامل مع من يتم ضبطه بهذا الجرم مستهدفاً أي دولة عضو في الحلف وفق قانون دولي ينظم الجرائم الإلكترونية سيصدر حديثاً. ويتبين لنا كذلك في آخر دراسات حلف الناتو أن العدوان العسكري التقليدي حقيقة لا يمكن إنكارها، ولا نستطيع أن نلغي وجودها من الأجندات والأولويات الدفاعية، ولكن هنالك مخاطر وشيكة لتهديدات غير تقليدية، وهذا التهديدات الغير تقليدية تمثل خطراً محدقاً وعدواناً وشيكاً، وندرج من أهمها صواريخ بالستية نووية موجهة بالإضافة إلى هجمات الكترونية تصيب أماكن استراتيجية وحساسة، وهذه الأخيرة تعتبر الأهم والأخطر [18]

وعند الحديث عن إلحاق الهجمات الإلكترونية بفعل العدوان فعلياً لا يوجد أي سوابق عملية دولية نستند إليها في قيام مجلس الأمن باتخاذ تدابير على هجمة الكترونية دولية، ومجلس الأمن لا يضع ضابطاً عملياً ومعياراً محدداً يتبعه في تكييف ما يعرض عليه من وقائع إلا أن مجلس الأمن ينفر من وضع القيود على سلطاته التقديرية[19] .

ونجد أن الميثاق وبالرجوع تحديداً إلى المادة (39) ألحق فعل العدوان وربطه بتهديد السلم والإخلال به وعند الحديث عن مصطلح (تهديد السلم) ممكن أن يكون ذلك بعيداً نوعاً ما عن الهجمات الإلكترونية الدولية لأن موضع تهديد السلم في غاية الخطورة والدقة.

ومن خلال القرارات السابقة لمجلس الأمن نجد أن الموضوع الأخطر هو تهديد حتمي للسلم والأمن الدوليين وهذا في الوقت الراهن قد لا يتطابق مع الهجمات الإلكترونية أما إذا أردنا الحديث عن الإخلال بالسلم والأمن الدولي فإننا نجد أن ثمة روابط معينة قد توصلنا إلى أن الهجمات الإلكترونية تحدث إخلالاً بالسلم والأمن الدولي من خلال حدوث هجمة الكترونية دولية معلنة ضد جهة دولية أخرى. والخطورة في مثل هذا النوع من الهجمات أنها قد تهاجم المصالح الاستراتيجية للدول وخصوصاً أنها قادرة على أن تؤثر وتشل أي حركة دولية أو منشأة في ثواني قليلة.

وإلحاق هذه التصرفات بفعل العدوان أمر قابل للتصور خصوصاً بأن العدوان كما أوردنا في السابق لم يتم تعريفه بالشكل المحدد في الميثاق لأن تحديد فعل العدوان بجوانب محددة سوف يضع قيوداً على بعض سلطات مجلس الأمن وعلى ضوءه فإن ما يستجد من أحداث سوف تجعل مجلس الأمن يقف مكتوف اليدين أمامها ومن بينها الهجمات الإلكترونية.

وإذا تأملنا ما يجري على صعيد الدول المتقدمة من إجراءات وتدابير نصل إلى أن هذا الفعل لا يقل خطورة عن العدوان، ولعل ما فعلته بريطانيا مؤخراً من إجراءات أمنية لتعزيز قدراتها الإلكترونية حيث تم إختيار مجموعة بنوك وبورصات الاستثمار في مواجهة هجوم منسق وتدريبي وهمي على الانترنت من جانب دولة معادية تتسبب بعطل كبير وخلل واضح وشارك في التمرين (220) خبيراً معرفياً ومسؤولاً حكوميا ومقدم لخدمات البنية التحتية [20]

---

[17]– **مجلة الرافدين للحقوق، مجلد رقم (9)، عدد (34)، كانون أول 2007، ص 184.**

[18]**https://www.nato.int/nato_static_fl2014/assets/pdf/2020/6/pdf/What_is_NATO_ara_iraq_20200507.pdf آخر زيارة 20 آذار 2023**

[19]– **أبو ربيع، مصطفى عبد العزيز، (2007)، استخدام القوة بتفويض مجلس الأمن، بدون طبعة، رسالة ماجستير، آل البيت.2007، ص78.**

[20]**تقرير إخباري، سكاي نيوز عربية، 2014.**

إجراء مثل هذه التجارب الوهمية يدل على أن دولاً كبرى قد تدق ناقوس الخطر، حيث بدا الوقوع أمام هجمات إلكترونية خطر وشيك الوقوع ويهدد بعدوان حتمي يهدد هذه الكيانات ومقدراتها الحساسة والاستراتيجية.

وحتى يتبلور لدينا منحى جديد واضح للعدوان في الهجمات الإلكترونية لا بد أن نسلط الضوء أكثر على حدوث عنصر العدوان في الهجمات الإلكترونية، من خلال بعض الأمثلة التي تظهر أن فعل العدوان حصل في هجمة الكترونية ولعل برنامج "ستكسنت" الذي كانت إيران في طليعة الدول المستهدفة من خلاله. حيث تعرضت 60% من أجهزة الكمبيوتر التي كانت في إيران لهجوم من هذا التطبيق. "وستكسنت" هو برنامج خبيث يهاجم أنظمة التحكم الصناعية على نطاق واسع في مراقبة الوحدات التي تعمل آلياً. وهذا البرنامج هو النموذج الحي للجهات التي تنوي إطلاق هجمات الكترونية تؤدي إلى اضطرابات حقيقية ودمار كارثي وإضعاف البلد.

فهذا البرنامج الخبيث على خلاف أنظمة الاختراقات والفيروسات المعتادة فإنه لا يعمل بشكل عشوائي وإنما يبحث عن علامة فارقة وبعد عثوره عليها يبدأ بتفعيل نفسه وإحداث الدمار وفي حال عدم عثوره على هذه العلامة فإنه يترك الجهاز ولا يعبث به.

ولذلك نجد أن هذا البرنامج كبير جداً ومعقد ويوظف تقنيات فائقة الذكاء ويعمل بدون تدخل البشر ويكلفه بطاقة ذاكرة يخزن بها متى بدأ عمله[21].

وبناء عليه أن عمل هذا البرنامج محدد ودقيق ويعمل بطريقة منظمة جداً وعدم عشوائية العمل والتخريب فهذا يقودنا إلى نقطة جوهرية مفادها أنه تم إنتاجه في دولة محددة ويستهدف دولة محددة ومنشأة محددة استناداً إلى عنوان بحثه عن علامة فارقة.

وبذلك نجد أن إيران كانت هي المستهدفة لأنه تم العثور عليه بكثافة في أجهزة موظفي محطة بوشهر ومع نفي القائمين على هذه المحطة أنها تعطلت إلا أنه وفي وقت تزامن مع ظهور هذا الفيروس تعطلت إحدى أكبر محطات تخصيب اليورانيوم في إيران وتم عزاء ذلك إلى أسباب مجهولة.

وبهذا الشق من المثال نجد أن دولة وهي إيران قد تعرضت لشن هجمة الكترونية مفتعلة وقد استهدفت موقع استراتيجي وحساس وذو أهمية اقتصادية وفي غاية الحساسية والخطورة فلو أخذنا النصف الأول من هذا المثال وأردنا أن نطبقه وأن نربط بينه وبين فعل العدوان نجد أنه يشكل إخلال بالسلم والأمن الدوليين كيف لا وفيه إلحاق ضرر كبير وبالغ في منشأة حساسة مثل مفاعل بوشهر الإيراني فلو افترضنا تسرب اشعاعات نووية مثلاً أو حصول عطل في أنظمة الطرد المركزية أدى إلى انفجار وعصف نووي شديد لم يعد إخلالاً بالسلم الدولي فقط بل يتعدى ذلك إلى جريمة إبادة جماعية وكارثة إنسانية لم يطلق فيه رصاصة واحدة وهذا بدوره لا بد وأن يقوم بناء عليه مجلس الأمن بالاستجابة الفورية وردة الفعل المناسبة لهذا الحدث الخطير.

وإذا انتقلنا لنفس المثال السابق، وأوردنا الجزء الثاني منه، وتم طرح تساؤلات عديدة أهمها إلى من تتجه أصابع الاتهام في استهداف هذه المنشأة النووية الإيرانية قبل ذلك يجب أن ننفي أي جهات خاصة وذات مصلحة شخصية لأن مثل هذه المنشأة العملاقة تخرج من دائرة المنافسة لمشاريع صغيرة أو شركات استثمارية بهدف الجذب للمستثمرين أو التنافس التجاري وبهذا التحليل المبدئي تخرج منه أي جهة خاصة أو مؤسسة خاصة.

وأول أصابع الاتهام في هذا الصدد أن تكون الولايات المتحدة وراء هذه الهجمات لأنها وفي أكثر من تصريح أعلنت نيتها لتعطيل البرنامج النووي الإيراني إضافة إلى أن الفايروس متطور جداً ووراء هذا التطور الإمكانيات الكبيرة لصفة قد تكون أمريكيا من أنتجه.

[21] https://www.tabnak.ir/ar/news/16805/ آخر زيارة 20 آذار 2023

إلا أن "إسرائيل" تحتل الصدارة في لائحة المتهمين في هذا الفايروس لأسباب عديدة أهمها أن إسرائيل بدأت تستخدم تقنيات حرب الفضاء لعدم رغبتها في الدخول في عمل عسكري تقليدي وتعقيداته وهذه التقنيات وبهدوء تتسلل إلى معلومات

أو تخريب أنظمة السيطرة والتحكم بالمنشآت مثلما حصل في إيران.

وقبل التفرع أكثر من ذلك في الربط بين ما حصل وفعل العدوان نشير إلى أن الولايات المتحدة الأمريكية هي من ضمن الدول الخمس الدائمة العضوية في مجلس الأمن الدولي، والتي تتمتع بحق النقض (الفيتو) وهذا الاستنتاج الأول الذي 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).

فهذا يقودنا إلى جوهر الخلاف أيضاً وهو في حال اتهام "إسرائيل" بهذه الهجمة ستقف أمريكا فوراً وتلوح في الأفق بحق النقض (الفيتو) باعتبارها الداعم والحليف الأكبر ل "إسرائيل" في العالم.

وبهذا المثال نصل إلى أداة ربط استنتاجية أن ثمة اعتداء فعلي وفعل عدوان حقيقي يقع على الدولة الضحية من خلال حصول هجمات الكترونية عليها، وهذا بدوره يعطل المصالح الاستراتيجية للدول ويضعف من كياناتها على الرغم من أن هذا النوع من العدوان لا يمس الاستقلال السياسي ولا يتم فيه احتلال الأراضي والغزو إلا أن أبعاده التدميرية وأضراره تجعله أشد من العدوان المسلح في بعض الأحيان والتي تؤدي إلى حدوث ضحايا وكوارث إنسانية.

الفرع الثاني

المسؤولية الدولية في فعل الهجمات الإلكترونية

عند النظر إلى نص المادة (51) من ميثاق الأمم المتحدة نجدها تنص على أنه ليس في الميثاق ما يضعف أو ينتقص الحق الطبيعي للدول فرادى أو جماعات في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء (الأمم المتحدة) وذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدولي.

والتدابير التي اتخذها الأعضاء استعمالاً لحق الدفاع عن النفس تبلغ المجلس فوراً ولا تؤثر تلك التدابير بأي حال فيها للمجلس – بمقتضى سلطته ومسؤولياته المستمرة من أحكام هذا الميثاق – من الحق في أن يتخذ في أي وقت ما يرى ضرورة لاتخاذه من الأعمال لحفظ السلم والأمن الدولي أو إعادته إلى نصابه (مادة 51 من ميثاق الأمم المتحدة).

للدول سيادة تامة تمارس هذه السيادة في داخلها ابتداء وكذلك في المحيط الدولي وهي بذلك لن تكون تابعة لأي دولة أخرى واستناداً إلى مبدأ السيادة يترتب للدولة حقوق أهمها حق البقاء وبه تستطيع الدولة الدفاع المشروع عن نفسها، وكذلك لها حق الحرية والاستقلال ولها الحق أيضاً بالمساواة بغض النظر عن وزن هذه الدولة السياسي[22].

ومما لا شك فيه أن الدولة ذات سيادة وتتمتع بالشخصية القانونية الدولية التي تؤهلها لتكون عضواً كامل الحقوق في المجتمع الدولي والانضمام إلى المنظمات الدولية، والقدرة على الاستعداد لتحمل تبعات هذه المسؤولية الدولية[23].

[22] **بشير مراد، الحرب في القانون الدولي العام، مرجع سابق، ص35.**

ويتمتع الدولة بهذه الشخصية القانونية الدولية يتقرر لها الدفاع عن مقدراتها وثرواتها البشرية والتقنية ومن هذا الباب ندرج لها مبرراً يجعلها تحافظ على نفسها من خلاله من خطر الهجمات الإلكترونية، وبهذه الشخصية القانونية نلاحظ أن للدول الشخصية الاعتبارية الدولية الكاملة ولا يحق لأي جهة الانتقاص من هذه البنية القانونية بأي شكل كان.

ومن هنا نجد أن الدول الصغيرة أو النامية تتعرض سيادتها للتهديد المستمر، كما تهدر هيبتها أول بأول في مواجهة احتكار الدول الكبرى لكل عناصر القوة خاصة بعد طوفان العولمة الذي جرفها في حين امتطت القوى الكبرى أعلى أمواجه دون أي خوف من غرق أو حتى بلل نظراً لقدراتها التكنولوجية الفائقة وإمكاناتها الاقتصادية التي ساعدتها توجيه أهدافها حيث تريد[24] .

ومع انتشار وتسارع ظاهرة العولمة عملت تياراتها على تذويب النزاعات الاقتصادية والعسكرية في عالم أصبح قرية كونية صغيرة تفاقمت الإشكاليات والمعضلات التي تطرح تساؤلات أهمها كيف تحمي الدول الصغرى نفسها من بطش الدول الكبرى، وكيف يمكن قيادة عالم على خريطة مثل الفسيفساء ذات الألوان والأحجام المتناقضة والمتداخلة والمتناثرة شرقاً وغرباً شمالاً وجنوباً خاصة أن جدول أعمال النظام العالمي الجديد لا يقتصر على المسائل العسكرية والأمنية والاقتصادية، بل إلى قضايا أكثر تعقيداً[25] .

ويرى الباحث أن الهجمات الإلكترونية اليوم في عالم متغير ومتسارع، وسنجد في السباق التقني الدولي أن الخلافات الاقتصادية والعسكرية قد تتنحى جانباً مقابل خطورة ودقة الفضاء الإلكتروني وما يحصل فيه من مناورات وصراعات قوية وسوف تكون مثاراً لجدل الشارع في وقت قريب مما لا يسمح ولا يدع مجالاً للشك في حدوث مثل هذه الهجمات وواقعية حصولها وحتى أحياناً دراسة خطورة نتائجها لأنها سوف تقع فجأة ودون سابق إنذار لأن الحرب الفضائية خدعة أيضاً كالحرب التقليدية.

وتظهر لدينا في معرض الحديث عن الهجمات الإلكترونية وتأثيرها على الدول المسؤولية الدولية التي تكون بالالتزام الذي تتحمله الدول أو المنظمة الدولية بحكم القانون الدولي المنسوب إليها بارتكاب أفعال أو امتناع مخالف لالتزاماتها الدولية بتعويض للمجني عليها في شخصها أو في رعاياها، وقيام المسؤولية الدولية يقوم على عنصرين أهمهما أن يكون منسوباً إلى دولة أو منظمة (شخص من أشخاص القانون الدولي العام)، أو يكون مخالفاً لمقتضيات قاعدة قانونية دولية، وبذلك تنحصر لدينا شروط المسؤولية الدولية بداية في حصول فعل أو امتناع عن فعل من شخص قانوني دولي ويكون أيضاً بإلحاق ضرر بشخص قانوني دولي بأي شكل وأن يكون هذا الفعل أو التصرف غير المشروع بالاستناد إلى الشرعية الدولية[26].

وبهذا الالتزام المفروض على الدولة أو المنظمة الدولية نجد أن حصول هجمة إلكترونية تأخذ طابعاً دولياً بمعنى أن القائم عليها دولة أو منظمة دولية واستهدفت دولة أو منظمة دولية فإن ذلك واستناداً إلى مبدأ المسؤولية الدولية يحمل هذه الجهة القائمة على الهجمة الإلكترونية أن تقوم بتعويض الجهة المجني عليها استناداً إلى مبدأ هذه المسؤولية الدولية التي ترتب عنها هذا الإخلال، وعند قياس فعل الهجمات الإلكترونية على عناصر المسؤولية الدولية فإننا نجد أن المقياس الأول أن تخضع هذه الهجمة إلى الصفة الدولية، أي أنه يجب أن تتبناها جهة

---

[23] عمر صدوق، محاضرات في القانون الدولي العام، بدون طبعة، ديوان المطبوعات، الجزائر، 1995، ص12.

[24] نبيل راغب، هيبة الدولة التحدي والتعدي، بدون طبعة، دار غريب، القاهرة، 2004، ص189.

[25] نبيل راغب، نفس المرجع، ص 41.

[26] عمر صدوق، مرجع سابق، ص21.

دولية أو منظمة دولية حتى يتم الحاقها بالمسؤولية الدولية أما المقياس الثاني فأن تكون هذه الهجمة الإلكترونية الدولية تخرق معاهدة أو عرف أو ميثاق دولي وبتوضيح أكثر لهذا العنصر يجب أن يترتب على هذه الهجمة الإضرار بمصالح الدولة المعتدى عليها الاقتصادية والسياسية والإستراتيجية، أو أنها تخل بمبدأ من مبادئ الأمم المتحدة والتي كان من أهم مقاصدها هو صون السلم والأمن الدوليين والمحافظة عليهما من أي اختراق أو تدخل يضر بمصالح الدول الأساسية التي لا يجوز انتهاكها، ونستنتج من المسؤولية الدولية مبرر آخر يورد لدينا أحقية فعل الدفاع الشرعي في حال حصول هجمة الكترونية دولية، وتنحصر شروط المسؤولية الدولية بما يلي:

1. وجود فعل أو امتناع عن فعل من شخص من أشخاص القانون الدولي العام.
2. إلحاق ضرر بشخص من أشخاص القانون الدولي العام بأي شكل.
3. 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 وذلك بالرجوع للشرط الأول فهذا يعني حصولها من جهة غير دولية لا يبرر قيام المسؤولية الدولية وعند البحث بالشرط الثاني وهو إلحاق الضرر فهذا أمر جوهري وفي غاية الأهمية فعند الحديث في السابق في دراستنا أوردنا 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 ديدن هذه الحرب.

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 فإن 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.

ومن خلال ما سبق نصل إلى نتائج بعد دراسة عناصر وشروط المسؤولية الدولية أهمها أن الإخلال بالالتزام الدولي ينتج المسؤولية الدولية التي بحد ذاتها تخترق وتخل بقواعد القانون الدولي الذي يوجب التعويض بحال حصول ضرر.

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[27] .

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

[27] **عدس، عمر حسن، مبادئ القانون الدولي العام المعاصر، بدون طبعة، مطابع القواسمي، بدون مكان نشر، 1995،ص 540.**

البيئة التي يعيش فيها الإنسان لأن حدوث فعل الهجمات قد يلحق أضراراً قد تحدث الكثير من الجرائم الدولية السابق ذكرها. ومثالها الصريح ما حصل في الهجوم الالكتروني على مفاعل بوشهر النووي في إيران.

وفي المحصلة النهائية للحديث عن قيام المسؤولية الدولية عن إحداث الهجمات الإلكترونية واشتراكها في الجرائم الدولية نستخلص مبرر جديد ألا وهو قيام وظهور استراتيجيات الدفاع، وهذه الاستراتيجيات التي تؤمن بها الدول وحق لا يمكن إنكاره ويقوم عندما تنتهك سيادة وحقوق الدول من خلال حصول جرائم دولية تؤدي إلى إلحاق الأضرار الجسيمة بمصالحها وإدراج فعل الهجمات الإلكترونية يؤكد ويساعد في نهوض المجتمعات الدولية على وضع خطط وبرامج واستراتيجيات تحمي فضائها وبنيتها الإلكترونية والفضائية والتقنية.

بالحديث عن الأساس القانوني للمسؤولية الدولية كان أساسه الخطأ ونظرية المخاطر، هذا في القانون الدولي التقليدي، أما في القانون الدولي المعاصر، فإن الأساس 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.

الخاتمة:

تناولت هذه الدراسة الهجمات الإلكترونية كصراع جديد بين الدول وكيفية معالجتها في نطاق القانون الدولي إذا حصلت على نطاق دولي وتبنتها جهة دولية، وحاولنا من خلال تسليط الأضواء على المادة (39) من ميثاق الأمم المتحدة والمادة (51) من ميثاق الأمم المتحدة اللتان أجازتا حق الدفاع الشرعي في حالة الاعتداء والهجوم المسلح ولكن حاولنا إيجاد رابط من خلال هذه الدراسة لعله يوصلنا إلى مبرر للدفاع الشرعي يحق للدول استخدامه في حالة حصول هذه الهجمات. وتم التوصل لمجموعة من النتائج والمقترحات نعرضها تباعاً:

النتائج و المناقشة:

1- تعتبر الهجمات الإلكترونية من أخطر الأسلحة الفتاكة في العصر الحديث سياسياً واقتصاديا.

2- إن سلاح الهجمات الإلكترونية له دور مهم ومؤثر في النزاعات الاقتصادية والسياسية بين مختلف دول العالم، والهجمات الإلكترونية جزء من تطور مصطلح الحرب والصراع.

الاستنتاجات و التوصيات:

1- تطوير تعريف جريمة العدوان على الدول ليشمل جرائم الهجمات الإلكترونية.

2- توسيع دائرة اختصاص المحكمة الجنائية الدولية لتشمل الفصل في الجرائم الالكترونية الدولية.

3- العمل على صياغة اتفاقية دولية تنظم حدود الفضاء الالكتروني للدول، وتبين بشكل دقيق حقوق وواجبات الدول فيما يتعلق باستخدام التقنيات الالكترونية الحديثة. وتضمن حق الدول بالدفاع المشروع عن سيادتها على فضائها الالكتروني بمواجهة أي اعتداء عليه.

References:

Arabic References:

Khalaf, Mohamed Mahmoud, (1973), The Right to Legal Defense in International Criminal Law, without edition, Al-Nahda Egyptian Bookshop, Cairo. -

-Talal Yassin Al-Issa, Ali Jabbar Al-Husseinawi, (2005), International Criminal Court, without edition, Dar Al-Yazuri, Amman.

Al-Anani, Ali Ibrahim, (2000), International Organizations, General View, without edition, Dar Al-Nahda.

- Bashir Murad, (1973), War in Public International Law, first edition, without publishing house, Damascus.
- Abu Rabie, Mustafa Abdel Aziz, (2007), the use of force authorized by the Security Council, without edition, master's thesis, Al al-Bayt.
- Omar Sadouq, (1995), Lectures on Public International Law, without edition, Publications Office, Algeria.

Nabil Ragheb, (2004), The Prestige of the State, Challenge and Transgression, without edition, Dar Gharib, Cairo.

-Adass, Omar Hassan, (1995), Principles of Contemporary Public International Law, without edition, Al-Qawasmi Press, without a place of publication.

-Hamisi Reda, (1999), International Responsibility, without edition, Caravan House, Algeria.

Hammouda, Montaser Saeed, (2006), International Terrorism, without edition, New University House, Alexandria.

-Al-Shukri, Ali Youssef, (2008), International Terrorism in the Shadow of the New World Order, without edition, Partnership for Publishing, Cairo.

-Heshmat Darwish, International Terrorism and Hostage Rescue Operations, without edition, without place of publication, Madbouly Al-Saghir.

-A working paper by Muhammad Muhammad Al-Alfi, the effective factors in the spread of terrorist crimes via the Internet, at the International Conference on the Protection of Information Security and Privacy in Internet Law 2008.

Websites, News Reports And Magazines:

- https://www.nato.int/nato_static_fl2014/assets/pdf/2020/6/pdf/What_is_NATO_ara_iraq_20200507.pdf آخر زيارة 20 آذار 2023

-News reports on Sky News Arabia TV station.

English References:

- Article cyber- attacks and the use of force: Back to the future of article 2 (4),
- The Law of Cyber Attack the California Law Review 2012
- Michael. N. Schmitt, The thin justice of international law