المسؤولية الدولية الجنائية عن الهجمات السيبرانية

دِ. سعاد محمد عواد النجم
دائرة البعثات والعلاقات الثقافية
وزارة التعليم العالي والبحث العلمي

البريد الإلكتروني Email : suadalawad71@gmail.com

الكلمات المفتاحية: الهجوم السيبراني، الجريمة السيبرانية، المجرم السيبراني، محل الجريمة السيبرانية، الطبيعة القانونية.

كيفية اقتباس البحث

النجم، سعاد محمد عواد ، المسؤولية الدولية الجنائية عن الهجمات السيبرانية،مجلة مركز بابل للدراسات الانسانية، تشرين الثاني ٢٠٢٦، المجلد:١٦ ،العدد:١١ .

هذا البحث من نوع الوصول المفتوح مرخص بموجب رخصة المشاع الإبداعي لحقوق التأليف والنشر (Creative Commons Attribution) تتيح فقط للآخرين تحميل البحث ومشاركته مع الآخرين بشرط نَسب العمل الأصلي للمؤلف، ودون القيام بأي تعديل أو استخدامه لأغراض تجارية.

مفهرسة في Indexed
IASJ

مسجلة في Registered
ROAD

International Criminal Liability for Cyber Attacks

Dr. Suad Mohammed Awad Al-Najm
Department of Scholarships and Cultural Relations
Ministry of Higher Education and Scientific Research

Keywords : Cyber Attack, Cybercrime, Cybercriminal, Subject Matter of

How To Cite This Article
Al-Najm, Suad Mohammed Awad , International Criminal Liability for Cyber Attacks,Journal Of Babylon Center For Humanities Studies, November 2026,Volume:16,Issue 11.

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

Abstract:

The cyber attack is considered a criminal phenomenon that has emerged in the field of information technology. It is carried out through attacks, breaches, and infiltration into the information systems of public or private institutions, with the aim of either destroying them or obtaining classified stored information, whether military or economic in nature. These attacks possess a unique character as they do not target a tangible physical object; rather, they target data and information stored within computers. Consequently, the objective of such attacks is either to access and remove classified information stored on computers, leading to loss for the victim—whether through the exposure or deletion of the information. Thus, information has acquired monetary value and become susceptible to infringement, serving as the subject matter of a crime provided certain conditions are met. Moreover, cybercrime is characterized by a low rate of detection, as its commission involves no violence and leaves no physical traces behind, thereby making it difficult to prove. Additionally, the cybercriminal is distinguished from the

traditional criminal in terms of the motive for committing the crime and the locations from which it is perpetrated.

المستخلص:

يُعدُّ الهجوم السيبراني ظاهرة إجرامية نشأت في مجال تكنولوجيا المعلومات، وتتم عن طريق هجمات واختراقات وتسلل داخل النظم المعلوماتية للمؤسسات العامة أو الخاصة لغرض إما تدميرها أو لأجل الحصول على المعلومات السرية المخزونة سواءٌ أكانت عسكرية أم اقتصادية، فهي ذات طبيعة خاصة كونها لا تنصب على شيء مادي ملموس، وإنما تقع على البيانات والمعلومات المخزونة داخل الحاسب الآلي فيكون الهدف من هذه الهجمات هو إما معرفة المعلومات السرية المخزونة على الحاسب الآلي وإزالتها، مما يؤدي إلى خسارة المجني عليه سواءٌ بسبب معرفة المعلومات أو إزالتها، وبذلك أصبحت المعلومة تُقوّم بالمال ويمكن الاعتداء عليها، وأن تكون محلاً للجريمة إذا توافرت فيها شروط معينة، كما تتميز الجريمة السيبرانية بقلة حالات اكتشافها، إذ لا يشوب ارتكابها أي عنف ولا تترك ورائها أي آثار مما يؤدي إلى صعوبة إثباتها، كما يتميز المجرم المعلوماتي عن المجرم التقليدي من حيث الغرض من ارتكاب الجريمة ومواقع ارتكابها.

المقدمة:

شهد العالم في العقود الأخيرة ثورة معلوماتية غير مسبوقة حولت الفضاء السيبراني إلى ساحة جديدة للصراع، لا تقل خطورة عن البر والبحر والجو والفضاء الخارجي، فلم تعُد الحروب تُدار بالأسلحة التقليدية وحدها، بل أصبحت الهجمات السيبرانية أداة فعالة تستخدمها الدول والجماعات وحتى الأفراد لتحقيق أهداف سياسية وعسكرية واقتصادية، من خلال تعطيل البنى التحتية الحيوية، وسرقة البيانات، والتجسس، وتقويض الأمن القومي للدول .

وتكمن خطورة هذه الهجمات في خصائصها الفريدة التي تتميز بها عن الجرائم التقليدية، فهي عابرة للحدود، صعبة الاسناد، منخفضة التكلفة، عالية التأثير، ويمكن ارتكابها عن بعد دون الحاجة للتواجد المادي في إقليم الدولة الضحية، وقد أدى ذلك إلى ظهور فراغ قانوني كبير على المستوى الدولي، حيث أن القواعد التقليدية للقانون الدولي العام والقانون الدولي الجنائي وضعت لتنظيم حروب تقليدية، ولم تعُد كافية لمواجهة هذا النمط المستحدث من الجرائم .

وبالرغم من الجهود الدولية المبذولة، سواءً على مستوى الأمم المتحدة من خلال فريق الخبراء الحكوميين المعني بالتطورات في مجال المعلومات، أم على مستوى المنظمات الإقليمية كاتفاقية بودابست لمكافحة الجريمة السيبرانية لعام ٢٠٠١، إلا أن المجتمع الدولي لا يزال يفتقر إلى نظام قانوني متكامل يحدد بشكل واضح أركان المسؤولية الدولية الجنائية عن الهجمات السيبرانية،

وشروط إسنادها للدولة أو الفرد والآليات القضائية المختصة بمحاكمة مرتكبيها، سواءً أمام المحكمة الجنائية الدولية أو المحاكم الوطنية .

أهداف البحث:

لتكوين صورة واضحة المعالم حول الهجمات السيبرانية التي تحدث في العالم الافتراضي الذي يُعدُّ ساحة جديدة للقتال.

أهمية البحث:

لبيان إمكانية المسؤولية الدولية عن الأضرار التي يخلّفها الهجوم السيبراني في القانون الدولي، ومدى انطباق قواعد المسؤولية الدولية عليها، لاسيّما أن الفضاء السيبراني أصبح مسرحاً للهجوم العسكري الذي قلبَ قواعد القانون الدولي رأساً على عقب.

إشكالية البحث:

نظراً لاتساع خطر تعرّض البنية التحتية الكونية للمعلومات لهجوم إلكتروني، فضلاً عن استخدامه من قبل أطراف فاعلة من غير الدول، كالجماعات الإرهابية لتحقيق أهدافها للنيل من الأمن القومي للدول، لذا يكون السؤال المطروح هنا هو " ما مدى إمكانية المسؤولية الدولية عن الأضرار التي يخلّفها الهجوم السيبراني؟

منهجية البحث:

سوف نتّبع في بحثنا المنهج الوصفي في توصيف ظاهرة الهجوم السيبراني من خلال عرض ما تتميز به من خصائص ومحددات، كما تم استعمال المنهج التحليلي في تحليل قواعد ومبادئ القانون الدولي في زمن السلم والنزاعات المسلحة من أجل تقييم تطبيقها على الهجوم السيبراني وتحليل أُسس المسؤولية الدولية عن الهجوم التقليدي ومدى الاعتماد عليها في تقرير المسؤولية الدولية عن الأضرار الناجمة عن الهجوم السيبراني.

هيكلية البحث:

وانطلاقاً من ذلك سوف يتم تقسيم هذا البحث على مبحثين:

نخصص المبحث الأول للكلام عن الطبيعة القانونية للهجوم السيبراني وبواقع ثلاثة مطالب، يتضمن المطلب الأول تعريف الهجوم السيبراني، أما المطلب الثاني فيتضمن التكييف القانوني للهجوم السيبراني، والمطلب الثالث نبين فيه أنواع الحروب السيبرانية.

أما المبحث الثاني فسوف نخصصه للكلام عن المسؤولية الدولية الجنائية عن الهجمات السيبرانية وبواقع أربعة مطالب، نتحدث في المطلب الأول عن ماهية المسؤولية الدولية الجنائية، وفي المطلب الثاني نتطرق إلى مفهوم المسؤولية الجنائية الفردية الدولية، أما المطلب الثالث

فسنبحث فيه الاختصاص القضائي للمحكمة الجنائية الدولية على الهجمات السيبرانية وأخيراً نناقش في المطلب الرابع الاتفاقيات الدولية في مجال مكافحة الهجوم السيبراني.

المبحث الأول: الطبيعة القانونية للهجوم السيبراني

تُعدُّ الحرب السيبرانية سيناريو افتراضي لحرب المستقبل أو ما يُعرف بالحرب السيبرانية فتكون على شكل هجمات دقيقة، ومعقدة للغاية عبر نظم وشبكات الكومبيوتر والأجهزة الذكية، التي تمس الأمن القومي للدولة وتؤثر على الأمن والسلم الدوليين، باستهدافها البُنى التحتية المدنية والعسكرية للدول من محطات الطاقة والكهرباء، ونظم الاتصالات والمواصلات والأقمار الصناعية، وخدمات الموقع الجغرافي والسيارات ذات القيادة، فضلاً عن المفاعلات النووية والسدود والخزانات المائية، وعليه سوف نتطرق إلى تعريف الهجوم السيبراني في المطلب الأول: أما المطلب الثاني فقد خصصناه للتكييف القانوني للهجمات السيبرانية، أما المطلب الثالث فسنبحث فيه أنواع الحروب السيبرانية.

المطلب الأول: تعريف الهجوم السيبراني

إنَّ الاعتماد على التقنيات الذكية والحديثة وتبني نماذج الحكومات والمدن الذكية، فمن المعلوم أن يصبح أكثر انكشافاً وعُرضة للهجمات السيبرانية، كذلك كثرة الاعتماد على الأنترنت في أثناء جائحة كورونا لتيسير مهام العمل والتعليم عن بُعد أدّى إلى تزايد نشاط القراصنة مستغلين ضعف الثقافة الأمنية لكثير من مستخدمي الأنترنت حول العالم، وهو ما يتسبب في تهديد الأمن القومي وتعريض مصالح الأفراد والدول للخطر.

لقد وجد بعض الفقهاء تعريفاً مبسطاً للهجمات السيبرانية، إذ عدّوها الأعمال العدائية، التي تشنها دولة ما ضد معطيات الدولة الإلكترونية المخزونة أو المعالجة أو المرسل من حاسوب لآخر بقصد سرقتها أو إتلافها أو حتى تعديلها ونسخها[١].

كما تم تعريف الهجمات السيبرانية بأنها هجمة إلكترونية معلوماتية حديثة ومتطورة توجهها دولة عبر الشبكات العنكبوتية تجاه دولة أخرى معتدية عليها بغية أن تسيطر على شبكات ومحتوى الكومبيوتر التابع لمرفق عسكري أو حيوي للدولة المستهدفة، فقد يؤدي الهجوم إلى تحكّم وسيطرة الدولة المهاجمة على أجهزة الدولة الخصم أو الدولة المستهدفة والتشويش عليها، وأحياناً يسبق الهجوم السيبراني الهجوم العسكري التقليدي أو يرافقه وتجري في أحيان أخرى بشكل منفصل، إذ يُشن الهجوم بغتةً من دون علم الدولة المستهدفة أو الخصم[٢].

ولا يوجد تعريف للهجمات السيبرانية متفق عليه بين فقهاء القانون الدولي.

فقد ذهب فقهاء القانون الدولي الإنساني إلى أن الهجمات السيبرانية هي استخدام الطيف الإلكتروني أو الكهرومغناطيسي لتخريب وتعديل وتبادل البيانات وجهاً لوجه مع أنظمة تحكم في بنى تحتية مرتبطة بها[٣].

كما عُرّفت الهجمات السيبرانية بأنها مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نظم المعلومات المعادية بهدف التأثير والإضرار بها، وفي الوقت نفسه للدفاع عن نظم المعلومات الخاصة بالدول المهاجمة[٤].

أما الفعاليات الدولية فقد عرَّفت الهجمات السيبرانية تعريفات عدّة، ومن هذه التعريفات تعريف القيادة السيبرانية الأمريكية في عام ٢٠٠٧ بأنها تطويع عمليات نظام الكومبيوتر بهدف منع الخصوم من الاستخدام الفعّال لها، فضلاً عن التسلل إلى أنظمة المعلومات وشبكات الاتصال بهدف جمع وحيازة وتحليل البيانات التي تحتويها[٥]. ونرى بأن هذا التعريف يتوافق مع مفهوم استخدام الوسائل الإلكترونية للأغراض العسكرية.

أما تعريف دليل تالين للهجمات السيبرانية وفقاً لما ورد في القاعدة (٣٠) منه فهو: عمليات سيبرانية سواء كانت هجومية أم دفاعية، يهدف من خلالها بصورة معقولة التسبب بالإصابة أو الوفاة للأشخاص أو الإضرار أو تدمير الأعيان[٦]. ويُعدُّ من أفضل التعريفات وأقربها للواقع لكونه يجمع بين الوسيلة المستخدمة والغرض أو الهدف من الهجمات.

وبدورنا نقترح التعريف الآتي: أي تصرف سواءً كان دفاعياً أم هجومياً، يتوقع منه وعلى نحو غير معقول، في التسبب بإصابة شخص، أو قتله، أو إلحاق أضرار مادية، أو دمار بالهدف المُهاجَم، إذ نرى بأن هذا التعريف أقرب وأشمل للحرب السيبرانية.

ونرى من التعاريف أعلاه بأن هناك تشابه بين الهجوم السيبراني والهجوم العادي في أن القائم بكلا الهجومين له دافع للقيام بالهجوم، وضحية قد تكون شخص طبيعي أو معنوي، أما الاختلاف بينهما يظهر في أداة الهجوم، ففي الهجوم السيبراني الأداة تكون ذات تقنية عالية، كما لا يتطلب انتقال فاعله انتقالاً جسمانياً لأنهُ يتم عن بُعد بواسطة خطوط أو شبكات الاتصال بين المهاجم ومكان الهجوم.

المطلب الثاني: التكييف القانوني للهجوم السيبراني

تقدّم الجيوش السيبرانية في زمن السلم الدعم المعلوماتي واللوجستي فيقومون بالتجسس على العدو عبر اختراق شبكاته لكشف أسراره، وسرقة تصميمات الأسلحة المتقدمة التي يمتلكها والخطط الاستراتيجية والاقتصادية في حالة الحرب، ونوع التسليح الذي يمتلكه ومناطق توزيعه وانتشاره. أما في زمن النزاعات المسلحة، فيقومون بمهمتي الهجوم والدفاع على حدٍّ سواء، فضلا

عن تقديم الدعم للوحدات العسكرية المقاتلة في الميادين المختلفة. إذ يقومون بمهمة الهجوم عن طريق محاولة شن هجمات سيبرانية تستهدف نظم التحكم والسيطرة الخاصة بالعدو عن طريق تعطيل نظم الدفاع الجوي، ومنصات إطلاق الصواريخ، والسيطرة على الأسلحة ذاتية التشغيل كالروبوتات العسكرية، وقطع شبكات الاتصال بين الوحدات العسكرية، فضلاً عن القيام بعمليات الخداع والتشويش الرقمي على أجهزة العدو.

ونظراً لحساسية استخدام القوة في العلاقات الدولية، وكذلك تعقد الفضاء السيبراني الذي أصبح يشكّل قلقاً كبيراً للمجتمع الدولي لخطورة الهجمات التي تُشن من خلاله، إذ تُعدُّ ظاهرة الهجمات السيبرانية من الأساليب المستحدثة والمتطورة في الوقت نفسه والتي لا تزال تُثير جدلاً لعدم وجود موقف محدد تجاهها، إذ ينطبق القانون الدولي على الهجوم السيبراني إذا عُدَّ هذا الهجوم قوة وفقاً لميثاق الأمم المتحدة، فالقواعد المعاصرة للقانون الدولي تحظر استخدام القوة باستثناء حق الدول أو الجماعات في الدفاع عن نفسها[٧].

أما بالنسبة لميثاق الأمم المتحدة لسنة ١٩٤٥، فقد حظرت الفقرة (٤) من المادة (٢) منهُ على الدول اللجوء إلى الحرب، أو التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي، أو الاستقلال السياسي لأي دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة، إلّا أن الميثاق قد ترك تحديد المعنى الحقيقي لهذه القاعدة القانونية لمجلس الأمن الذي يقررها تبعاً للظروف المحيطة بكل حالة على حدة، وهذا واضح من نص المادة (٣٩) من الميثاق التي تمنح مجلس الأمن سلطة تقرير الإجراءات القهرية، وقد ورد هذا النص بصورة غير ملزمة وذلك بسبب تمتع مجلس الأمن بصلاحيات تقرير ما إذا وقع تهديد للأمن والسلم الدوليين، أو الإخلال به، أو كان قد وقع عملاً من أعمال العدوان.

ونجد أن مصطلح القوة الوارد في الفقرة (٤) من المادة (٢) من ميثاق الأمم المتحدة جاء واسعاً إذ لا ينحصر فقط بالقوة العسكرية، وإنما يشمل كل أنواع التهديدات طالما أن هناك النيّة العدائية، وهذه الفقرة جاءت مرنة بحيث تستوعب الهجوم السيبراني نتيجة الآثار المشابهة بالنسبة للقوة العسكرية التقليدية، لذلك فإن الكود الضار أو الفايروسات لها خصائص السلاح نفسها التي يمكن أن تكون أداة للتخريب والتدمير كالسلاح الحركي، وهنا لا يهم الوسيلة المستخدمة في الهجوم سواءً التقليدي أو السيبراني وإنما المهم هو الأضرار التي تترتب عن الهجوم والتي تشكّل خطراً على سيادة الدول والأمن الدولي[٨].

أما التكييف القانوني للهجمات السيبرانية على وفق قواعد القانون الدولي الإنساني، فنجد على سبيل المثال مما نصت عليه المادة (٤٨) من القواعد الأساسية التي تحكم الهجمات ما ينطبق

إلى حد كبير مع الهجمات السيبرانية، والتي تفرض على المتنازعين التمييز بين المدنيين والمقاتلين وبين الأعيان المدنية والعسكرية، أي تحظر شن أي نوع من الهجمات مهما كانت وسائلها وماهيتها[٩]، وهذا ما أكدته القاعدة السابعة الواردة في القانون الدولي الإنساني التي تنص على أن يميز أطراف النزاع في جميع الأوقات بين الأعيان المدنية والأهداف العسكرية[١٠]، وكذلك ما أوردته المادة (٥١) في الفقرة الثانية بخصوص حظر الهجمات ضد السكان المدنيين الرامية أساساً إلى نشر الرعب بينهم[١١].

فإذا ما تساءلنا هل توجد قواعد قانونية في القانون الدولي النافذ قادرة على مواءمة التحديات التي يفرضها استخدام هذه الأسلحة الجديدة في النزاع المسلح الحديث والتي لا تتقاتل خلالها الجيوش النظامية أو فئات مسلحة تكون منظمة أخرى، وجدنا بأن العديد من فقهاء القانون الدولي قد تطرقوا إلى موضوع الحرب السيبرانية فطرحوا عدداً من الإشكاليات القانونية المتمحورة حول القانون الواجب التطبيق عليها، إلّا أن غالبية الفقهاء يؤكدون إمكانية تطبيق قواعد القانون الدولي الإنساني على هذه الحروب، إلّا أنه في الوقت نفسه هناك جانب آخر من الفقه رفض هذا الطرح وأقروا بوجود فراغ قانوني في هذه المسألة.

المطلب الثالث: أنواع الحروب السيبرانية

شهدت الأحداث والنزاعات المسلحة الدولية خلال العقدين الأخيرين استخدام التكنولوجيا الإلكترونية بنحو كبير من خلال ما تمتلكهُ الدول من إمكانيات إلكترونية سيبرانية وتنفيذ هجمات سيبرانية بمختلف الأسلحة السيبرانية، وهناك أنواع متعددة من الحروب السيبرانية وكالآتي:

أولاً: الحرب السيبرانية الباردة " منخفضة الشدة "

يُعدُّ الفضاء السيبراني ساحة للصراع منخفض الشدة، وإن هذا الصراع مستمر بين الفاعلين، وقد يكون ذات طبيعة ممتدة، ودائمة النشاط العدائي أو غير السلمي، ويوصف بأن جذوره عميقة ومتداخلة، وله نواحس متعددة اقتصادية، اجتماعية، وثقافية، وفي الغالب يتم اللجوء إلى القوة الناعمة للحروب السيبرانية في مثل هذه الصراعات، على الرغم من أنها لا تتطور لتصل إلى الحروب التقليدية في الغالب، أو شن حرب سيبرانية شاملة[١٢].

ومن أمثلتها التوتر بين أستونيا وروسيا عام ٢٠٠٧م إذ تعرضت أستونيا إلى هجمات سيبرانية من قبل روسيا الاتحادية بحسب اتهامات أستونيا لها كرد فعل على رفع تمثال من العاصمة تالين، لكن روسيا لم تعترف بها رسمياً، وهذه إحدى أهم إشكاليات الهجمات السيبرانية في إطار الأسناد وتحديد المسؤولية الدولية، واستهدفت الهجمات السيبرانية البنى التحتية والمواقع

الإلكترونية الحكومية والجامعات والمستشفيات، ويُعدُّ هذا المثال الأبرز على مشاركة المتطوعين من غير العسكريين في تنفيذ هجمات بهذا النوع والحجم (ميليشيات أو أفراد متفرقون)[١٣].

ونلحظ بأن هجمات (أستونيا) تُعدُّ الحدث الأبرز الذي يمثل البداية التاريخية لاستخدام الهجمات السيبرانية بوصفها الحقيقي، كذلك كونها مثّلت اختباراً لردة فهل حلف شمال الأطلسي، والذي تُعدُّ أستونيا عضواً فيه، إذ طلبت عقد اجتماع عاجل للحلف لاتخاذ موقف من تلك الهجمات، وبالمقابل عدَّ الحلف تلك الهجمات بمثابة هجوم مسلح يهدد دول الحلف جميعاً، استناداً لنص المادة (٥) من اتفاقية حلف شمال الأطلسي لعام ١٩٤٩[١٤].

ثانياً: نمط الحرب السيبرانية متوسطة الشدة

في هذا النوع من النمط يتحول الصراع في الفضاء السيبراني إلى ساحة موازية لحرب تقليدية دائرة على الأرض، ويكون ذلك تعبيراً عن حدّة الصراع القائم بين الأطراف، كما أن هذا قد يمهّد لعمل عسكري، وتدور حرب الفضاء السيبراني عن طريق اختراق المواقع السيبرانية، وتخريبها وشن حرب نفسية ضد الخصوم، وتستمد هذه الحروب السيبرانية شدتها من قوة أطرافها، وارتباطها أيضاً بأعمال عسكرية تقليدية، وإن بعض التقديرات تشير إلى رخص التكلفة للحروب السيبرانية، فقد تموّل حرب سيبرانية كاملة بسعر دبابة، وقد استخدم هذا النوع من الحروب السيبرانية متوسطة الشدة عام (١٩٩٩) من قبل حلف الناتو على يوغسلافيا، واستهدفت الهجمات السيبرانية تعطيل الاتصالات للخصوم أيضاً، كما برزت خلال الحرب بين حزب الله وإسرائيل عام (٢٠٠٦)، كما حصل ذلك بين روسيا وجورجيا في عام (٢٠٠٨)، وكذلك في المواجهات بين حماس وإسرائيل في الأعوام (٢٠٠٨) و(٢٠١٢)[١٥].

ثالثاً: نمط الحرب السيبرانية الساخنة مرتفعة الشدة

يُعدُّ هذا النمط من الحروب عند نشوئها في الفضاء السيبراني منفردة، وهي متوازية مع الأعمال العسكرية التقليدية، وإلى الآن لم يشهد العالم هذا النوع من الحروب، وإنْ كانت احتمالات حصولها واردة في المستقبل، ولاسيّما في ظل تطورات القدرات الخارجية، وتوسع الاعتماد على الفضاء السيبراني من قبل الدول والفواعل من غير الدول، وينطوي هذا النمط من الحروب على سيطرة البُعد التكنولوجي على إدارة العمليات الحربية، ويستخدم فيه الأسلحة السيبرانية ضد منشآت العدو، وأيضاً اللجوء إلى الروبوتات الآلية في الحروب والطائرات من دون طيار، وإدارتها عن بُعد، بخلاف تطوير القدرات في مجال الدفاع والهجوم السيبراني، والاستحواذ على القوة السيبرانية، وفي هذا السياق يتم استخدام الفضاء السيبراني لاستعادة مستقبل الحروب وهذا يتم عبر قيام الدول بتدريبات ضربة أولية لحواسيب العدو، واختراق العمليات العسكرية عالية

التقنية، أو حتى باستهداف الحياة المدنية، والبنية التحتية المعلوماتية، والهدف من ورائها تحقيق " الهيمنة السيبرانية الواسعة " بشكل أسرع في حالة نشوب صراع[١٦].

لقد شهدت الأسلحة السيبرانية تطوراً كبيراً في قدرتها على التأثير في الخصوم، ومن النماذج على ذلك تعرض إيران لهجوم سيبراني من خلال سلاح برنامج (Stuxnet) لمدة تسعة أشهر من نهاية عام ٢٠٠٩ إلى بدايات عام ٢٠١٠، إذ تم هذا الهجوم من خلال التسلل في أنظمة السيطرة المستخدمة في أهم المنشآت النووية الإيرانية (نطنز وبوشهر) عن طريق فايروس يسمى(Stuxnet)، والذي يُعدُّ الأخطر على صعيد الهجمات السيبرانية ضد المنشآت العسكرية، إذ صمم لكي ينتشر بصورة سريعة، ومن دون التسبب بأضرار للمنشآت الأخرى والأشخاص الذي لم يتم برمجته على ذلك، ولفايروس (Stuxnet) ثلاثة أجزاء أو وحدات، الأولى الوحدة التي تنفذ الأعمال التخريبية الخبيثة كافة، والثانية هي الوحدة التي تنسخ الفايروس تلقائياً وتعمل على انتشاره، والثالثة هي الوحدة التي تكون مسؤولة عن إخفاء الملفات والعمليات الخبيثة، ويعمل هذا الفايروس على مرحلتين الأولى السيطرة على نظام التحكم الموجود في أجهزة القيادة والسيطرة في المنشأة واستخدام الحواسيب المربوطة بهذه الأنظمة للدخول في نظام (SCADA) والبحث عن شفرات موجودة فقط في أنظمة(SCADA) الموجودة في المحطات النووية الإيرانية، والمرحلة الثانية بعد التحقق من وصول الفايروس للهدف المقصود فيبدأ بعمليات التخريب والتلاعب في أجهزة الطرد المركزية عن طريق زيادة السرعة والضغط وتقليلها في الأجهزة إلى أن يتم تعطيلها وتخريبها[١٧].

المبحث الثاني: المسؤولية الدولية الجنائية عن الهجمات السيبرانية

بما أن الهجمات السيبرانية تتسبب في حدوث ضرراً عابراً للحدود يمس البنية التحتية للدول والأمن والسلم الدوليين، لذا فإن الهجمات السيبرانية والأنشطة الضارة التي تقوم بها الدول في العالم الافتراضي تتكيف على أنها نشاطات خطرة نظراً لما يترتب عليها من آثار وخيمة على الأمن القومي الدولي ولا يقتصر الأثر القانوني لتنفيذ الهجمات السيبرانية على قيام المسؤولية الدولية بشقها المدني فقط، فعندما يترتب على ارتكابها جرائم دولية ينتج عنها إصابات ووفيات بين الأفراد المدنيين أو أضرار بالأعيان المدنية، فإن مرتكبيها المباشرين من القادة العسكريين والرؤساء سيخضعون للمسؤولية الجنائية الدولية استناداً لأحكام القانون الدولي الجنائي على اعتبار أن الهجمات السيبرانية تُعدُّ طرقاً لأحكام القانون الدولي والقانون الإنساني.

وبناءً عليه سيتم تقسيم هذا المبحث على ثلاثة مطالب، نخصص المطلب الأول للحديث عن ماهية المسؤولية الدولية الجنائية، أما المطلب الثاني فسنخصصه للكلام عن مفهوم المسؤولية

الجنائية الفردية الدولية، والمطلب الثالث سنتكلم فيه عن الاختصاص القضائي للمحكمة الجنائية الدولية على الهجمات السيبرانية.

المطلب الأول: مفهوم المسؤولية الدولية الجنائية

لم يعترف الفقه الدولي التقليدي بوجود مسؤولية جنائية دولية في القانون الدولي بسبب عدم تعريف الجريمة الدولية[١٨]. وعلى الرغم من تسليم الفقه المعاصر بذلك، إلّا أنه اختلف حول من تنسب إليه هذه المسؤولية، فأنصار الرأي القائل بمسؤولية الدولة جنائياً تُعدُّ فكرة حديثة ظهرت لمساءلة الدول عن الجرائم التي يرتكبها رؤسائهم، ودعا أصحاب هذا الرأي إلى التمسك بمساءلة الدولة وحدها عن الجرائم الدولية، كون هذا النوع من الجرائم ى يتصور ارتكابها إلّا من قبل الدول، أما الفرد عند ارتكابه الجريمة يخضع للمساءلة من قبل قانونه الجنائي الوطني، ولا يمكن أن يخضع للقانونين معاً القانون الجنائي الدولي والقانون الجنائي الوطني[١٩].

ومع تطور القانون الدولي الجنائي، لاسيّما بعد محاكمات ما بعد الحربين في إطار محكمة (نورمبرغ) و(طوكيو) ومع تطور مبادئ حقوق الإنسان وإبرام اتفاقية منع ومحاكمة مرتكبي جريمة الإبادة الجماعية في عام ١٩٤٨م، والإعلان العالمي لحقوق الإنسان ١٩٤٨م، وما ترتب على ذلك من اعتبار الفرد مؤهلاً لتلقي الحقوق وتحمل الالتزامات القانونية الدولية وأهمية مكافحة انتهاكات القانون الدولي الإنساني والقانون الدولي لحقوق الإنسان، بزغت فكرة المسؤولية الجنائية الفردية الدولية، كما أن مسؤولية الأفراد فرضها الواقع الإجرامي وجرائم وفضائع الحروب والنزاعات المسلحة وانتهاكات القانون الدولي الإنساني، فقد أصبحت المسؤولية الجنائية الفردية الدولية قاعدة عامة وآمرة في القانون الدولي[٢٠].

إنَّ قيام المسؤولية الدولية الجنائية يفترض ارتكابه فعل غير مشروع قام به وكلاء أو ممثلو الدولة من قادة ومسؤولين وأفراد، ويشكّل هذا الفعل غير المشروع جريمة دولية وخرقاً لأحكام القانون الدولي، سواء تحقق الضرر أم لم يتحقق لأنَّ الجرائم الدولية من جرائم الخطر، وتكون المسؤولية الجنائية متحققة فيها بمجرد الاعتداء على المصلحة القانونية التي يحميها القانون الدولي[٢١].

كما أن اعتماد فرضية الذنب الشخصي أساساً للمسؤولية الجنائية الدولية في القانون الدولي الجنائي يعني أن لا يكون الشخص مسؤولاً عن أفعال لم يكن فيها فاعلاً أصلياً أو شريكاً بالتحريض أو المساعدة أو الإعداد في مدة ما قبل التنفيذ، انسجاماً مع قاعدة لا جريمة ولا عقوبة إلّا بنص، وإن الأثر المترتب على قيام المسؤولية الجنائية الفردية هو الجزاء الجنائي الذي يكون سجناً وحبساً، وهي عقوبات جسدية مقيدة للحرية تنطبق على الأفراد الطبيعيين، أما بالنسبة

للدولة فمن الممكن أن يكون جزاءها عقوبات اقتصادية أو سياسية كما هو الحال في القرارات التي يتخذها مجلس الأمن الدولي في فرض التدابير والإجراءات اللازمة لحفظ السلم والأمن الدوليين، وهذه النقطة اختلف عليها الفقه الدولي اختلافاً كبيراً، إذ يرى بعضهم صعوبة تصور إخضاع الدول أو الشخص الدولي إلى الجزاء الجنائي[٢٢].

المطلب الثاني: موقف نظام روما الأساسي من الاختصاص الإقليمي للمحكمة الجنائية الدولية على الهجمات السيبرانية

تضمن نظام روما الأساسي للمحكمة الجنائية الدولية الإشارة إلى الولاية الإقليمية للمحكمة على الجرائم الدولية المنصوص عليها في المادة (٥) منه، التي تقع في إقليم إحدى الدول الأطراف في النظام، أو يكون المتهم بارتكاب الجريمة أحد رعاياها[٢٣].

نلحظ أن النظام الأساسي للمحكمة الجنائية الدولية لم يتضمن في أي من مواده إيضاح المقصود بمصطلح الإقليم، فهل هو الإقليم الذي ترتكب فيه الجريمة الدولية؟ أم هو الإقليم الذي تترتب فيه آثارها ونتائجها ؟ فكيف هو الأمر بالنسبة للجرائم الدولية التي تنفذ عن بُعد كالهجمات السيبرانية، إذ يزداد الأمر غموضاً في هذه الحالة، فهل يكون للمحكمة الجنائية الدولية أو (المحاكم الجنائية الدولية الخاصة الأخرى) الولاية الإقليمية على تلك التصرفات التي ترتكب عن بُعد في دولة لم تكن طرفاً في نظام روما الأساسي ولكن تقع نتائجها في دولة طرف في هذا النظام؟ أو عكس ذلك.

ومما تجدر الإشارة إليه ما تضمنته مفاوضات صياغة تعريف جريمة العدوان، التي كان الهدف منها إضافة الجريمة لاختصاص المحكمة الجنائية الدولية، إذ انقسم المفاوضون على أربعة فئات:

رأت الأولى بأن اختصاص المحكمة يجب أن يحدد على وفق الإقليم الذي تقع فيه الجريمة أي الذي تظهر فيه تصرفات الجريمة، أما الفئة الثانية فقد رأت إلى أن تحديد الولاية الإقليمية ينبغي أن يتم على أساس النتائج الجرمية التي تحدث أو تظهر في دولة ما[٢٤]، بينما ذهبت الفئة الثالثة إلى أن الطبيعة الدولية لهذه الجرائم تستلزم أن يتم ترك تحديد الولاية الإقليمية إلى المحكمة، وأخيراً رأت الفئة الرابعة إلى أن مسألة تحديد الولاية الإقليمية تحتاج إلى المزيد من الوقت والمزيد من الممارسات القضائية من قبل المحكمة الجنائية الدولية[٢٥].

ونتيجة الاختلاف في وجهات نظر الدول المشتركة في المفاوضات لم يصل المتفاوضون من ممثلي الدول إلى اتفاق بشأن الولاية الإقليمية للمحكمة الجنائية الدولية.

إلّا أن مؤتمر كمبالا لعام ٢٠١٠ خرج بمخرجات ونتائج مهمة، لعلَّ أهمها الاتفاق على تعريف محدد لجريمة العدوان لأغراض النظام الأساسي للمحكمة الجنائية الدولية[٢٦]، والاتفاق على صيغة وطبيعة وحدود الولاية القضائية للمحكمة، التي بموجبها استبعدت الدول غير الأطراف في النظام الأساسي منها عندما يرتكب مواطنوها الجريمة الدولية أو ترتكب الجريمة على أراضيها[٢٧].

ومن خلال ذلك يتبين لنا أن المحكمة الجنائية الدولية يتركز اختصاصها الأساسي على الجرائم الأشد خطورة، والتي تثير قلق المجتمع الدولي كجرائم (الإبادة الجماعية، والجرائم ضد الإنسانية، جرائم الحرب، وجريمة العدوان). لذا نجد أنها تطبق اختصاصها على الهجمات السيبرانية في حال كانت هذه الهجمات ترقى إلى مستوى هذه الجرائم، وتتوافق مع شروط الاختصاص الإقليمي والشخصي، لاسيّما مع تعديل جريمة العدوان وتركيز الجهود على المساءلة الفردية عن الجرائم السيبرانية التي ترقى لجرائم حرب أو عدوان.

وعلى الرغم من ذلك نجد ان الهجمات السيبرانية تبقى تحدياً بسبب صعوبة تحديد الفاعل، وتعالج عادةً عبر التعاون الدولي وقوانين الدول الوطنية مع وجود محاولات دولية مثل اتفاقية الأمم المتحدة لمكافحة الجرائم السيبرانية لتعزيز مواجهتها.

أما موقف دليل تالين فقد تضمن السير باتجاه أن الدولة تمارس ولايتها القضائية على أساس الوجود المادي أو الوجود القانوني للشخص أو الأعيان المدنية على إقليمهم. وقد تبنى خبراء دليل تالين رأي بأن للدولة صورتين من الولاية الإقليمية الأولى ذاتية تمكّن الدولة من ممارسة اختصاصها الإقليمي على الهجمات السيبرانية التي تنفذ على إقليمها ومن الممكن أن ترتب نتائج خارج الإقليم، والثانية موضوعية تعطي للدولة حق ممارسة اختصاصها الإقليمي على العمليات والحوادث والهجمات السيبرانية التي ترتب آثارها في إقليمها على الرغم من ارتكابها أو أن بداية التنفيذ كانت خارج إقليمها[٢٨].

ونرى بأن تعديل نظام روما الأساسي للمحكمة الجنائية الدولية والنص صراحةً في نصوصه على تجريم استخدام الهجمات السيبرانية في التعاملات الدولية، ضرورة ملحة لضمان التطبيق الفعلي لمتطلبات تحقيق العدالة الجنائية الدولية وتحقيق السلم والأمن الدوليين.

المطلب الثالث: أساس المسؤولية الدولية عن الأضرار التي يسببها الهجوم السيبراني

تنبعث المسؤولية الدولية للهجوم السيبراني بالمعنى الدقيق من القانون الدولي العرفي، والمواثيق الدولية بوصفها تمس القيم الأساسية للمجتمع الدولي، فقد أصبحت شبكة الأنترنت تشكل قوة اجتماعية واقتصادية وسياسية، مؤثرة في العالم، لذا تضافرت الجهود من خلال سعي الدول

والمنظمات العالمية لمواجهة الجرائم السيبرانية، من خلال التوفيق بين مختلف الوسائط التقنية والأكاديمية، وتكثيف آليات الاتصال والتعاون، من وضع استراتيجيات دولية متنوعة، لمواجهة التهديدات السيبرانية في نطاق ومسؤولية كل طرف، وضرورة مراقبة استخدام تكنولوجيا المعلومات والاتصالات في ظل انكشاف العالم على بعضه.

من هذا المنطلق سوف نتناول في الفرع الأول: المسؤولية عن الهجمات السيبرانية على أساس عمل غير مشروع، وفي الفرع الثاني نتطرق إلى المسؤولية عن الهجمات السيبرانية استناداً إلى نظرية المخاطر.

الفرع الأول: المسؤولية عن الهجمات السيبرانية على أساس العمل غير المشروع

يترتب على نظرية العمل غير المشروع بأن كل إخلال بالتزام دولي من قبل دولة ما يستوجب مسؤولية هذه الدولة سواءً كان هذا الإخلال صادر عن سلطتها التشريعية أو التنفيذية أو القضائية وألحق ضرراً بأحد الأجانب في شخصه أو أمواله وكان متواجداً على أراضيها، ويُعدُّ الفقيه أنزلوتي أول مَنْ تبنى نظرية الفعل غير المشروع[٢٩].

تُعدُّ الهجمات السيبرالية الدولية عملاً غير مشروع، وتخضع للمسؤولية الدولية على هذا الأساس إذا توافر معيار الصفة الدولية، والمتمثل في صدور هذه الهجمات من قبل دولة ما، أما المعيار الثاني أن تكون الهجمات السيبرانية خارقة لمعاهدة أو عرف دولي، فيجب أن يترتب على الهجمات السيبرانية ثمت ضرر بمصالح أحد أشخاص القانون الدولي، إذ يكون قد تم التعدي عليها من الناحية الاقتصادية، أو من الناحية السياسية، أو أن تمس الهجمات السيبرانية بأحد المبادئ التي كرستها الأمم المتحدة من أجل حفظ السلم والأمن الدوليين[٣٠].

وقد تعرضت نظرية العمل غير المشروع للنقد من أوجه عدّة مثل إسناد المسؤولية الدولية للدولة عن الأضرار الناتجة عن الهجمات السيبرانية يمكن أن تثير مشكلة تتمثل في صعوبة تحديد ما إذا كان هذا العمل منسوباً للدولة فعلاً، وهذا مرتبط بالقدرة التكنولوجية المتنامية، والتي يمكن أن يُمكّن الدولة منشأ التصرف أن تطمس هوية الفاعل الحقيقي[٣١]، فضلاً عن ذلك فإن عملية نسبة العمل الدولية تزداد تعقيداً في الحالة التي لا تكون الشبكات السيبرانية هي الوسط الذي تمت من خلاله هذه الهجمات، كإرسال فايروسات توضع مباشرة في أجهزة الحاسوب الخاصة بالدولة المستهدفة، أو في الحالة التي يستخدم فيها إقليم دولة أخرى لتنفيذ هذه الهجمات، كما أن التحقيقات بشأن الهجمات السيبرانية قد تجمع بين المبادئ الأساسية لعمل أجهزة الاستخبارات بوصفها عملاً عادياً طبيعياً وبين الإلكتروني العابر للشبكات والحدود الدولية، لكن المحققين في

أجهزة الاستخبارات الدولية قد لا يستطيعون الولوج إلى الدول الأخرى لأنهُ يشكّل مساساً وانتهاكاً بسيادتها[٣٢].

إنَّ استخدام العمليات السيبرانية بوصفها وسائل أو أساليب للحرب في النزاعات المسلحة يشكّل خطراً حقيقياً بإلحاق الضرر بالمدنيين، ومن الضروري فهم الكيفية التي يكفل بها القانون الدولي الإنساني الحماية للمدنيين والبيئة التحتية المدنية والبيانات المدنية ضد التهديدات السيبرانية[٣٣].

عليه تُعدُّ العمليات الإلكترونية عمل غير مشروع ابتداءً، وهو بحد ذاته ينتهك أحكام وقواعد القانون الدولي كأنهُ يخترق أسرار ووثائق الدول، ويستهدف مصالحها الكبرى ويختلق مشاكل وقضايا دولية معاصرة لم تكن موجودة في السابق في عهد الحروب التقليدية ولا في الحرب الباردة، فهذا التسابق في التسلح التقني الجديد نعدّهُ في غاية الخطورة والدقة والأهمية.

الفرع الثاني: المسؤولية عن الهجمات السيبرانية استناداً إلى نظرية المخاطر

نتيجة الانتقادات التي وجهت إلى نظرية الفعل غير المشروع والتي أصبحت عاجزة عن مواكبة التطور التكنولوجي والعلمي، جاءت نظرية المخاطر كنظرية حديثة، وكان من نتائج ذلك تطوير هذه النظرية وظهور ما يطلق عليه العالم الافتراضي الذي أصبح مسرحاً تُدار من خلاله شؤون الكثير من الدول في مختلف الاتجاهات سواء أكانت سياسية أم اجتماعية أم اقتصادية، وتقوم نظرية المخاطر على أساس مساءلة الدولة بوصفها شخص من أشخاص القانون الدولي متى قامت بارتكاب سلوك مخالف للقانون الدولي، وكان هذا السلوك على درجة عالية من الخطورة[٣٤].

ونجد الاتفاقيات الخاصة بالطاقة الذرية هي من أهم الاتفاقيات الدولية التي أخذت بنظرية المخاطر، إذ تلزم هذه الاتفاقيات الدولة التي تقوم بأي نشاط ذري وقت السلم بتعويض الأضرار الناجمة عن هذا النشاط على أساس المسؤولية المطلقة المتجردة عن نسبة أي خطأ للدولة، كاتفاقية باريس المتعلقة بالمسؤولية الدولية قبل الغير في ميدان الطاقة النووية لسنة ١٩٦٠، التي وازنت بين المصالح بما يضمن تطوير الاستخدامات السلمية للطاقة النووية، وتكون المسؤولية بموجب هذه الاتفاقية مطلقة تقع على عاتق المشغل القائم بإدارة المنشأة النووية، فهو المسؤول عن أي خسارة أو ضرر للأشخاص أو الممتلكات، وعما يقع خارج المنشأة ولا تنتفي المسؤولية إلّا في حالة وقوع حادث إبان النزاعات المسلحة أو كارثة طبيعية أو غزو، وإلّا عليه أن يدفع التعويض اللازم.

إنَّ أغلب الأضرار التي تصيب دولاً أخرى تكون نتيجة أعمال غير مشروعة للدول المتسببة فيها أو عن أنشطة مشروعة وفقاً لمعايير القانون الدولي، وعلى الرغم من ذلك نجد أنه يتعذر إثبات

عدم مشروعيتها أو يتعذر إثباتها بصفة عامة، لذلك أُقيمت المسؤولية الدولية على أساس توافر ركن الضرر والعلاقة السببية بين الضرر والنشاط الذي تقوم به الدولة، وتُعدُّ أول مرة نُفذت فيها الهجمات السيبرانية، كانت في حرب كوسوفو سنة ١٩٩٩، من خلال استهداف سلاح الجو التابع لحلف شمال الأطلسي لشبكات الهاتف في يوغسلافيا السابقة وفي النزاع المسلح ذاته، وبعد استهداف طيران حلف شمال الأطلسي للسفارة الصينية في بلغراد، قام عدداً من القراصنة الصينيين وكردة فعل بمهاجمة مواقع إلكترونية رسمية منتخبة تابعة للولايات المتحدة الأمريكية، وبالذات الموقع الإلكتروني للبيت الأبيض نجم عن ذلك الاستحواذ على الآلاف من البيانات الرقمية المصنفة آنذاك بأنها عالية السرية[٣٥].

الخاتِمة:

من خلال بحثنا وجدنا بأن الهجمات السيبرانية لم تعالج بشكل صريح بموجب قواعد القانون الدولي ولا من خلال مبادئ قواعد القانون الدولي الإنساني، ويعود سبب ذلك وبالدرجة الأولى إلى حداثة هذه الهجمات بالقياس إلى تاريخ نشوء تلك القواعد والأحكام، إلّا أن ذلك لم يحل دون سعي المنظومة القانونية والقضائية والفقهية الدولية لبذل الجهود لإيجاد الحلول المناسبة من أجل سد الفراغ القانوني وللحد من آثار الهجمات السيبرانية وذلك من خلال إخضاعها لما هو متوافر ومعمول به من قواعد ومبادئ عامة قد تضمنها القانون الدولي، من خلال الاستعانة بالقرارات والسوابق القضائية الصادرة من القضاء الدولي، فضلاً عما يقدمه الفقه الدولي في هذا المجال، لحين التوصل إلى اتفاق دولي لإبرام اتفاقية عامة وشاملة وصريحة لتنظيم العمليات السيبرانية في إطار القانون الدولي.

وبناءً عليه توصلنا إلى جملة من النتائج والتوصيات وكالآتي:

النتائج:

١-لا تحتاج الدول إلى تخصيص ميزانيات ضخمة لإنتاج أسلحتها أسوة بالأسلحة المستخدمة في النزاعات التقليدية ذات الكلفة العالية، وإنما ذات كلفة متدنية نسبة للأدوات اللازمة لشنها، لذا يتزايد السباق غير التقليدي نحو الأسلحة السيبرانية في الوقت الحاضر بسبب المميزات التي تتمتع بها هذه الأسلحة. وهكذا حروب، من قلة التكاليف، سرعة الأداء فاعلية التدمير والنتائج ، صعوبة الكشف عن القائم بهذا الهجوم وغيرها من المميزات تُعدُّ سبباً رئيساً في دفع الدول إلى محاولة الحصول واحتكار هذه الأسلحة والتقنيات المرتبطة بالحروب السيبرانية.

٢-إنَّ تنفيذ الهجمات السيبرانية من قبل كيانات أو مجموعات مسلحة غير مرتبطة بالدولة، وهي ليست جزءً من قواتها المسلحة ولم تعمل على وفق توكيل أو تخويل قانوني، قد يثير مشكلة في

إطار تطبيق أحكام المسؤولية الدولية والمسؤولية الجنائية الفردية، من حيث آليات تحديد الارتباط والتبعة، وبما يسهل الإفلات من تطبيق أحكام المسؤولية الدولية.

٣-لا يوجد لغاية الآن اتفاق دولي بشأن تعريف الهجمات السيبرانية كونها من المفاهيم الحديثة، ما يؤدي إلى صعوبة تكييفها وتحديد مرتكب الجريمة، لذا ليس من المستغرب اليوم تربُّع موضوع الهجمات السيبرانية قمة الدراسات القانونية.

التوصيات:

١-يجب أن يتضمن أي تشريع أو اتفاقية دولية مستقبلية لتنظيم الهجمات السيبرانية تعريفاً دقيقاً ومحدداً للأسلحة والهجمات السيبرانية، وتحديد ما هو محظور منها في التعاملات الدولية وبشكل دقيقن وحدود استخدامها.

٢-نظراً لقصور القانون الدولي وعدم وجود أساس قانوني يحكم استخدام الحرب الإلكترونية، أصبح من الضروري على خبراء القانون تطوير القانون الدولي تزامناً مع التطور الكبير في تكنولوجيا المعلومات ولمعالجة هذا القصور.

٣-لتحديد تبعية الجهات المنفذة للهجمات السيبرانية يجب تطبيق معيار السيطرة الكاملة؛ لكونه معياراً أشمل وأعم ويُراعي الطبيعة الخاصة للهجمات السيبرانية، ومن ثمَّ تحديد وإثبات قيام المسؤولية الدولية على الدول والمسؤولية الجنائية الفردية على القادة والرؤساء والآمرين.

الهوامش

(١) درويش سعيد: الحرب السيبرانية وأثرها على حقوق الإنسان، دراسة في ضوء أحكام دليل تالين، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، المجلد(٥٤)، العدد (٥)، الجزائر،٢٠١٧، ص ١٨٢.

(٢) د. صابر محمد محمود المزمل ود. ياسين محمد حسن يونس: القانون الدولي والنزاعات المسلحة، المجلة الدولية لنشر البحوث والدراسات المجلد (٦)، العدد (٦٢)، ٢٠٢٤، عمّان – الأردن، ص ٣٨-٣٩.

(٣) د. أحمد عبيس الفتلاوي، الهجمات السيبرانية، دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، منشورات مكتبة زين الحقوقية، بيروت – لبنان، ط١، ٢٠١٨، ص ١٦.

(٤) د. محمود حسين الشرقاوي، الهجمات السيبرانية في ضوء أحكام القانون الدولي الإنساني، منشورات دار النهضة العربية، القاهرة – مصرت ط١، ٢٠٢١، ص ٧٣.

(٥) د. عدنان النقيب، الحرب الإلكترونية في ضوء بروتوكولي سبع وسبعين الملحقين باتفاقيات جنيف الأربع لسنة تسعة وتسعين (الهجمات السيبرانية)، المركز العربي للنشر والتوزيع، ط١، ٢٠٢٢، ص١٦٣.

(٦) دليل تاين: هو المشروع الدولي الأهم في مجال السيبرانية والمطبق على الحرب السيبرانية وتم إعداده من قبل مجموعة من خبراء وفقهاء القانون الدولي الإنساني عام ٢٠١٣ ثم أُجريت عليه تعديلات عام ٢٠١٧ وبالتعاون مع حلف شمال الأطلسي ويدعم فريق من المختصين من اللجنة الدولية للصليب الأحمر إضافة للقيادة السيبرانية الأمريكية. وإن اسم مرتبط باسم مدينة عاصمة دولة أستونيا ومركزها الإداري.

(7) Herbert Lin, Cyber conflict and international humanitarian Law, international review of the red Cross, 2012, Vol. 44, No.886.

(8) Priyanka r, dev, (Use of Force and armed Attach) Thresholds in Crber Conflict, Looming Definitional Gaps and phe Growing, Need for formal U.N, Response, Texas international law Journal, Vol.50, 2015, Issue 2.

(٩) المادة (٤٨) البروتوكول الإضافي الأول لاتفاقيات جنيف لعام ١٩٧٧.

(١٠) جون – ماري هنكرتس ولويزدوز والديكن القانون الدولي الإنساني العرف، اللجنة الدولي للصليب الأحمر، المجلد الأول، ص ٢٣.

(١١) اللجنة الدولية للصليب الأحمر" الملحقان " البروتوكولان الإضافيان إلى اتفاقية جنيف المعقودة في ١٢ آب/ أغسطس ١٩٤٩، ص ٤٠.

(١٢) حازم جري الشمري، توظيف القوة السيبرانية في استراتيجيات الدول الكبرى الولايات المتحدة الأمريكية وروسيا أنموذجاً ، دار إنكي للنشر والتوزيع، بغداد – العراق، ط١، ٢٠٢٢، ص ١٠٥.

(١٣) د. أحمد عبيس الفتلاوي، الهجمات السيبرانية مفهومها والمسؤولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، بحث منشور في مجلة الحلي للعلوم القانونية والسياسية، العدد (٤)، السنة الثامنة، ٢٠١٦، ص ٦٢٤.

(١٤) نصت المادة (٥) من معاهدة حلف شمال الأطلسي (الناتو) ١٩٤٩ على " تتفق الأطراف على أن الهجوم المسلح ضد واحد أو أكثر منهم في أوربا أو أمريكا الشمالية يعتبر هجوماً ضدهم جميعاً، وبالتالي يتفقون على أنه في حالة وقوع مثل هذا الهجوم المسلح، فإن كل منهم، ممارسة لحق الدفاع الفردي أو الجماعي عن النفس المعترف به بموجب المادة (٥١) من ميثاق الأمم المتحدة، سيساعد الطرف أو الأطراف التي تعرضت للهجوم من خلال اتخاذ الإجراءات التي يراها ضرورية، بما في ذلك استخدام القوى المسلحة، على الفور، منفردة وبالتنسيق مع الأطراف الأخرى، لاستعادة امن منطقة شمال المحيط الأطلسي والحفاظ عليها ".

ويبلّغ مجلس الأمن فوراً بأي هجوم مسلح من هذا القبيل وبجميع التدابير المتخذة نتيجة له، وتنتهي هذه التدابير عندما يتخذ مجلس الأمن التدابير اللازمة لاستعادة السلم والأمن الدوليين وصونهما ".

(١٥) د. حازم جري الشمري، مصدر سابق، ص ١٠٦.

(١٦) د. حازم جري الشمري، مصدر سابق، ص ١٠٧.

(١٧) علي محمد كاظم الموسوي، المشاركة المباشرة في الهجمات السيبرانية، شركة المؤسسة الحديثة للكتاب، بيروت – لبنان ، ط١،٢٠١٩، ص ٣٧–٣٨.

(١٨) د. محمد عبد المنعم عبد الغني، الجرائم الدولية، دراسة في القانون الدولي الجنائي، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٧م ص ٤٤٥

(١٩) د. سامي محمد عبد العال، الجزاءات الجنائية في القانون الدولي العام، دار الجامعة الجديدة، الإسكندرية، ٢٠١٥، ص ٢٨٣.

(٢٠) د. أمجد هيكل، المسؤولية الجنائية الفردية الدولية أمام القضاء الجنائي الدولي: دراسة في إطار القانون الدولي الإنساني، دار النهضة العربية، مصر، ط١، ص ٤٩٤.

(٢١) د. نزار العنبكي، القانون الدولي الإنساني، دار وائل للنشر والتوزيع، الأردن، ط١، ٢٠٠٧، ص ٤٨٢.

(٢٢) د. أمجد هيكل، مصدر سابق، ص ١١٠.

(٢٣) نصت الفقرة (٢) من المادة (١٢) من النظام الأساسي للمحكمة الجنائية الدولية على (٢- يجوز للمحكمة أن تمارس اختصاصها إذا كانت واحدة أو أكثر من الدول التالية طرفاً في هذا النظام:

أ- الدولة التي وقع في إقليمها السلوك قيد البحث أو دولة تسجيل السفينة أو الطائرة إذا كانت الجريمة قد ارتكبت على متن سفينة أو طائرة. ب- الدولة التي يكون المتهم بالجريمة أحد رعاياها.

(٢٤) المحكمة الجنائية الدولية، جمعية الدول الأطراف، الدورة السابعة، لاهاي، ٢٠٠٨، (١٤-٢٢ تشرين الثاني/ نوفمبر) (Icc-Asp/7/20) ، المرفق الثالث، الفقرة ٢٨، ص ٥٨.

(٢٥) المحكمة الجنائية الدولية، جمعية الدول الأطراف، الدورة السابعة (الاستئناف الثاني)، نيويورك، ٢٠٠٩، (٩-١٣ شباط/ فبراير) (Icc-Asp/7/20/Add.1) المرفق الثاني الفقرات ٣٨-٣٩، ص٣١.

(٢٦) عرَّف مؤتمر كمبالا ٢٠١٠ جريمة العدوان لأغراض المحكمة الجنائية الدولية بانها (قيام شخص ما – له وضع يمكنه فعلاً – بالتحكم في العمل السياسي أو العسكري للدولة أو توجيه هذا العمل بتخطيط أو إعداد أو بدء أو تنفيذ عمل عدواني، يشكل بحكم طابعه وخطورته ونطاقه انتهاك واضح لميثاق الأمم المتحدة.

(٢٧) نصت المادة (١٥/١٥) من تعديلات مؤتمر كمبالا على النظام الأساسي للمحكمة الجنائية الدولية التي أصبحت تحت رقم (١٥ مكرر) على: (٥- فيما يتعلق بدولة ليست طرفاً في هذا النظام الأساسي لا يجوز للمحكمة أن تمارس اختصاصاتها المتعلقة بجريمة العدوان عندما يرتكبها مواطنو تلك الدولة أو ترتكب على إقليمها).

(٢٨) نصت القاعدة (٢٩ من دليل تالين على: من دون الإخلال بالالتزامات الدولية الأخرى المعمول بها يجوز للدولة أن تمارس ولايتها القضائية على:

أ- الأشخاص المتورطين في الأنشطة السيبرانية على إقليمها.

ب- البنية التحتية السيبرانية الواقعة على أراضيها.

ج- خارج أراضيها على وفق القانون الدولي.

(٢٩) عبد العزيز العيشاوي، محاضرات في المسؤولية الدولية، دار هومة للنشر والتوزيع، الجزائر، ٢٠٠٧، ص ١٨.

(٣٠) لورنس سعيد الحوامدة، الجرائم المعلوماتية أركانها وآلية مكافحتها، دراسة تحليلية مقارنة، مجلة الميزان للدراسات الإسلامية والقانونية، كلية الحقوق – المملكة العربية السعودية، ٢٠١٦، ص ١٩،

(٣١) رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة للعلوم القانونية، المجلد ١٥، العدد ٢ن ديسمبر، ٢٠١٨، ص ٣٣٨.

(٣٢) عباس بدران، الحرب الإلكترونية (الاشتباك في العالم المتغير)، مركز دراسات الحكومات الإلكترونية، بيروت، ٢٠١٠، ص ١١١.

(٣٣) اللجنة الدولية للصليب الأحمر، العمليات السيبرانية أثناء النزاعات المسلحة، منشور على شبكة الأنترنت على الموقع: https://www.icrc.org ، تاريخ النشر: ٢٠٢٥/١٢/٢٦.

(٣٤) إيهاب خليفة، مجمع ما بعد المعلومات، تأثير الثورة الصناعية الرابعة على الأمن القومي، العربي للنشر والتوزيع، القاهرة، ص ١٨٨.

(٣٥) صباح العيشاوي، المسؤولية الدولية عن حماية البيئة، دار الخلدونية للنشر والتوزيع، الجزائر، ط١، ٢٠١٠، ص ١٧٤.

المصادر والمراجع

١-د. أحمد عبيس الفتلاوي، الهجمات السيبرانية، دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، منشورات مكتبة زين الحقوقية، بيروت – لبنان، ط١، ٢٠١٨.

٢-د. امجد هيكل، المسؤولية الجنائية الفردية الدولية أمام القضاء الجنائي الدولي، دراسة في إطار القانون الدولي الإنساني، دار النهضة العربية، مصر، ط١، ٢٠٠٨.

٣-د. إيهاب خليفة، مجتمع ما بعد المعلومات، تأثير الثورة الصناعية الرابعة على الأمن القومي، العربي للنشر والتوزيع، القاهرة، ٢٠١٩.

٤-جون ماري هنكرتس ولويزدوز والديك، القانون الدولي الإنساني العرفي، اللجنة الدولية للصليب الأحمر، المجلد الأول.

٥-د. حازم جري الشمري، توظيف القوة السيبرانية في استراتيجيات الدول الكبرى (الولايات المتحدة وروسيا) أنموذجاً، دار إنكي للنشر والتوزيع، بغداد – العراق، ط١، ٢٠٢٢.

٦-د. سامي محمد عبد العال، الجزاءات الجنائية في القانون الدولي العام، دار الجامعة الجديدة، الإسكندرية، ٢٠١٥.

٧-د. صباح العيشاوي، المسؤولية الدولية عن حماية البيئة، دار الخلدونية للنشر والتوزيع، الجزائر، ط١، ٢٠١٠.

٨-د. عباس بدران، الحرب الإلكترونية (الاشتباك في العالم المتغير)، مركز دراسات الحكومات الإلكترونية، بيروت، ٢٠١٠.

٩-د. عبد العزيز العشوي، محاضرات في المسؤولية الدولية، دار هومة للنشر والتوزيعن الجزائر، ٢٠٠٧.

١٠-د. عدنان النقيب، الحرب الإلكترونية في ضوء بروتوكولي سبع وسبعين الملحقين باتفاقيات جنيف الأربع لسنة تسعة وتسعون (الهجمات السيبرانية)، المركز العربي للنشر والتوزيع، ط١، ٢٠٢٢.

١١-علي محمد كاظم الموسوي، المشاركة المباشرة للهجمات السيبرانية، المؤسسة الحديثة للكتاب، بيروت – لبنان، ط١، ٢٠١٩.

١٢-محمد عبد المنعم عبد الغني، الجرائم الدولية، دراسة في القانون الدولي الجنائي، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٧.

١٣-د. محمود حسين الشرقاوي، الهجمات السيبرانية في ضوء أحكام القانون الدولي الإنساني، منشورات دار النهضة العربية، القاهرة – مصر، ط١، ٢٠٢١.

١٤-د. نزار العنبكي، القانون الدولي الإنساني، دار وائل للنشر والتوزيع، الأردن، ط١، ٢٠١٠.

مجلات عربيـة

١–د. أحمد عبيس الفتلاوي، الهجمات السيبرانية مفهومها والمسؤولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، بحث منشور في مجلة الحلي للعلوم القانونية والسياسية، العدد (٤)، السنة الثامنة، ٢٠١٦.

٢–د. درويش سعيد، الحرب السيبرانية وأثرها على حقوق الإنسان، دراسة في ضوء أحكام دليل تالين، المجلة الجزائرية للعلوم القانونية والاقتصادية، المجلد (٥٤)، عدد(٥)، الجزائر، ٢٠١٧.

٣–د. 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، ديسمبر، ٢٠١٨.

٤–د. صابر محمد محمود المزعل، وياسين محمد حسن يونس، القانون الدولي والنزاعات المسلحة، المجلة الدولية لنشر البحوث والدراسات، المجلد (٦)، العدد(٦٢)، عمّان – الأردن، ٢٠٢٤.

٥–د. لورنس سعيد الحوامدة، الجرائم المعلوماتية أركانها وآلية مكافحتها، دراسة تحليلية مقارنة، مجلة الميزان للدراسات الإسلامية والقانونية، كلية الحقوق، المملكة العربية السعودية، ٢٠١٦.

مجـلات أجنبيـة

1-Herbert Lin, Crber Conflict and international humanitarian Law, international review of the red Cross, 2012, Vol.94, No. 886.

2-Priyanka R. Dev, (Use of Force and Armed Attach) Thresholds in Cyber Conflict, The Looming Definitional Gaps. And the Griewing Need for Formal U.N. Response, Texas international Law, Journal Vol. 50, 2015, Issue 2.

المعاهـدات

١–اتفاقيات جنيف لعام ١٩٧٧ وبروتوكوليها الإضافيين.

٢–معاهدة حلف شمال الأطلسي(الناتو) ١٩٤٩.

٣–معاهدة روما للنظام الأساسي للمحكمة الجنائية الدولية.

المؤتمـرات

١–مؤتمر كمبالا ٢٠١٠.

Sources and References

-١Dr. Ahmed Obeis Al-Fatlawi, *Cyberattacks: An Analytical Legal Study on the Challenges of Their Contemporary Regulation*, Zain Legal Library Publications, Beirut, Lebanon, 1st ed., 2018.

-٢Dr. Amjad Haikal, *Individual International Criminal Responsibility Before International Criminal Tribunals: A Study Within the Framework of International Humanitarian Law*, Dar Al-Nahda Al-Arabiya, Egypt, 1st ed., 2008.

-٣Dr. Ehab Khalifa, *The Post-Information Society: The Impact of the Fourth Industrial Revolution on National Security*, Al-Arabi Publishing and Distribution, Cairo, 2019.

-٤Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law*, International Committee of the Red Cross (ICRC), Volume I.

-٥Dr. Hazem Jari Al-Shammari, *The Employment of Cyber Power in the Strategies of Major Powers (The United States and Russia as a Case Study)*, Dar Enki Publishing and Distribution, Baghdad, Iraq, 1st ed., 2022.

-٦Dr. Sami Mohamed Abdel Aal, *Criminal Sanctions in Public International Law*, Dar Al-Jami'a Al-Jadida, Alexandria, 2015.
-٧Dr. Sabah Al-Aishawi, *International Responsibility for Environmental Protection*, Dar Al-Khaldounia Publishing and Distribution, Algeria, 1st ed., 2010.
-٨Dr. Abbas Badran, *Cyber Warfare: Engagement in a Changing World*, Center for E-Government Studies, Beirut, 2010.
-٩Dr. Abdelaziz Al-Ashawi, *Lectures on International Responsibility*, Dar Houma Publishing and Distribution, Algeria, 2007.
-١٠Dr. Adnan Al-Naqib, *Cyber Warfare in Light of the 1977 Additional Protocols to the Four Geneva Conventions (Cyberattacks)*, Arab Center for Publishing and Distribution, 1st ed., 2022.
-١١Ali Muhammad Kazim Al-Musawi, *Direct Participation in Cyberattacks*, Modern Book Foundation, Beirut, Lebanon, 1st ed., 2019.
-١٢Muhammad Abd al-Mun'im Abd al-Ghani, *International Crimes: A Study in International Criminal Law*, Dar Al-Jami'a Al-Jadida, Alexandria, 2007.
-١٣Dr. Mahmoud Hussein Al-Sharqawi, *Cyberattacks in Light of the Provisions of International Humanitarian Law*, Dar Al-Nahda Al-Arabiya, Cairo, Egypt, 1st ed., 2021.
-١٤Dr. Nizar Al-Anbaki, *International Humanitarian Law*, Dar Wael for Publishing and Distribution, Jordan, 1st ed., 2010.

Arabic Journals

-١Dr. Ahmed Ubais Al-Fatlawi, "Cyberattacks: Concept and Resulting Liability in Light of Contemporary International Regulation," published in *Al-Hilli Journal for Legal and Political Sciences*, Issue (4), Year 8, 2016.
-٢Dr. Darwish Said, "Cyber Warfare and Its Impact on Human Rights: A Study in Light of the Provisions of the Tallinn Manual," *Algerian Journal of Legal and Economic Sciences*, Vol. 54, Issue 5, Algeria, 2017.
-٣Dr. Ahmed Samoudi, "The Right to Self-Defense in Response to Cyberattacks in Light of the Rules of Public International Law," *University of Sharjah Journal for Legal Sciences*, Vol. 15, No. 2, December 2018.
-٤Dr. Saber Mohammed Mahmoud Al-Muzal and Yassin Mohammed Hassan Younis, "International Law and Armed Conflicts," *International Journal for the Publication of Research and Studies*, Vol. 6, No. 62, Amman, Jordan, 2024.
-٥Dr. Lawrence Saeed Al-Hawamdeh, "Cybercrimes: Elements and Mechanisms for Combating Them – A Comparative Analytical Study," *Al-Mizan Journal for Islamic and Legal Studies*, Faculty of Law, Saudi Arabia, 2016.

Foreign Journals

-١Herbert Lin, "Cyber Conflict and International Humanitarian Law," *International Review of the Red Cross*, 2012, Vol. 94, No. 886.
-٢Priyanka R. Dev, "Use of Force and Armed Attack Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for a Formal U.N. Response," *Texas International Law Journal*, Vol. 50, 2015, Issue 2.

Treaties

-١The 1977 Geneva Conventions and their Additional Protocols.
-٢The North Atlantic Treaty (NATO), 1949.
-٣The Rome Statute of the International Criminal Court.

Conferences

-١The Kampala Conference, 2010.