International Criminal Responsibility For Hostile Cyber Operations During Contemporary Armed Conflicts

Zena Ojel*

(Received 6 / 7 / 2025. Accepted 8 / 9 / 2025)

□ ABSTRACT □

Modern technological techniques prevail in today`s world and armed conflicts are no longer limited to the battlefields and traditional tools, but also created the fifth fields or what is know as "Cyber Space". And hostile cyber operations became an influential part of the methods of modern war (fifth generations war), in addition to traditional military operations in the fields of fighting. In light of this very rapid development of technology and modern technologies and employing them incorrectly during international and non-international contemporary armed conflicts, which is one of the most important challenges faced by international law in general and international humanitarian law in particular because it is explicitly contradicts its rules and principles that stipulate the protection of civilians notables and prohibits their targeting with random attacks that cause excessive suffering and unjustified pain. The legal and jurisprudential debate revolves around the extent of international criminal responsibility for these operations, the possibility of applying the traditional rules ruling international responsibility, and the implications of this on the possibility of classifying them as an international crime, the possibility of prosecution, trial, and the impact of the penalties due before the criminal international judiciary.

Key Words: Hostile cyber operations, criminal international responsibility, International criminal judiciary, International humanitarian law, The international criminal court.

Copyright **:**Latakia University journal (formerly tishreen) -Syria, The authors retain the copyright under a CC BY-NC-SA 04

***Master's degree – Department of International Law- Faculty of Law - University of Lattakia - Syria .zena.ojel@tishreen.edu.sy**

المسؤولية الدولية الجنائية عن العمليات السيبرانية العدائية أثناء النزاعات المسلحة المعاصرة

زينة عجيل *

(تاريخ الإيداع 6 / 7 / 2025. قبل للنشر في 8 / 9 / 2025)

□ ملخّص □

تسود التقنيات التكنولوجية الحديثة في عالم اليوم ولم تعد النزاعات المسلحة تقتصر على ساحات المعارك وأدواتها التقليدية فحسب، بل استحدث "المجال الخامس" أو ما بات يعرف "بالفضاء السيبراني". وأصبحت "العمليات السيبرانية العدائية" جزءاً مؤثراً من وسائل وأساليب الحرب الحديثة (حروب الجيل الخامس) إلى جانب العمليات العسكرية الحركية في ميادين القتال التقليدية. في ضوء هذا التطور السريع للغاية للتكنولوجيا والتقنيات الحديثة وتوظيفها المتزايد بشكل خاطئ أثناء النزاعات المسلحة المعاصرة الدولية وغير الدولية، والذي يعد من أهم التحديات التي يواجهها القانون الدولي عامةً، والقانون الدولي الإنساني على وجه الخصوص لكونه يتعارض صراحةً مع قواعده ومبادئه التي تنص على حماية المدنيين والأعيان المدنية وتحظر استهدافهم بهجمات عشوائية الأثر تسبب معاناةً مفرطة وآلاماً لا مبرر لها. يثور الجدل القانوني والفقهي حول مدى ترتب المسؤولية الدولية الجنائية عن هذه العمليات، ومدى إمكانية تطبيق القواعد التقليدية الناظمة للمسؤولية الدولية عليها، وتداعيات ذلك على إمكانية تصنيفها كجريمة دولية، وإمكانية الملاحقة والمحاكمة وتوقيع الجزاءات المستحقة أمام القضاء الدولي الجنائي.

الكلمات المفتاحية: العمليات السيبرانية العدائية، المسؤولية الدولية الجنائية، القضاء الدولي الجنائي، القانون الدولي الإنساني، المحكمة الجنائية الدولية.

حقوق النشر : مجلة جامعة اللاذقية (تشرين سابقاً)- سورية، يحتفظ المؤلفون بحقوق النشر بموجب الترخيص CC BY-NC-SA 04

* ماجستير- قسم القانون الدولي - كلية الحقوق- جامعة اللاذقية- سوريا zena.ojel@tishreen.edu.sy

مقدمة:

لعبت عوامل عديدة ومختلفة كالتقدم التقني والتكنولوجي، ثورة المعلومات والاتصالات، تنامي الاتجاه العالمي نحو الرقمنة (التحول الرقمي) والحوكمة الإلكترونية دوراً حاسماً في فرض واقع جديد على النظام الدولي في العصر الراهن. وساهمت في تشكيل مجال افتراضي جديد موازٍ للمجالات الدولية الأخرى (الأرض، البحر، الجو، الفضاء الخارجي) وهو "الفضاء السيبراني". الذي أحدث تغييراً واضطراباً في مفهوم تصنيف النزاعات المسلحة وأثر على طبيعة القواعد واجبة التطبيق عليها، بعد أن أدخل مفهوماً مختلفاً في مقاييس القوة (القوة السيبرانية) وطبيعة الصراع ومقتضيات الأمن القومي للدول، وأسلوباً حديثاً ومؤثراً في أساليب القتال أثناء النزاعات المسلحة المعاصرة الدولية وغير الدولية.

إن استخدام العمليات السيبرانية العدائية أصبح أمراً واقعاً وسمةً حقيقيةً من سمات النزاعات المسلحة اليوم للرد على استفزازات تقليدية أو لتمهيد الطريق أمام هجوم حركي بهدف تحقيق التفوق العسكري. وعلى الرغم من عدم الإقرار بها صراحةً يعمل عدد متزايد من الدول على تطوير القدرات العسكرية السيبرانية لأغراض هجومية ودفاعية، ومن المرجح أن يزداد استخدام هذه القدرات في المستقبل وتوظيفها في النزاعات المسلحة الدولية وغير الدولية بشكل سيبدو أكثر تواتراً وتنظيماً وحدةً مما يتوقع المختصون والخبراء، لما توفره من بدائل قد لا تتيحها سائر وسائل وأساليب القتال الأخرى. أثار هذا التطور عدد من الشواغل في دول ومجتمعات اليوم والتي تعتمد اعتماداً متزايداً على الفضاء السيبراني في معظم جوانب الحياة اليومية. وينتاب القلق إزاء التكلفة البشرية المحتملة للعمليات السيبرانية العدائية ضد السكان المدنيين والبنية التحتية الحيوية والمهمة للدولة، وحول الأثر الإنساني المحتمل لها على النزاعات المسلحة الحالية والمستقبلية. حيث أصبح بإمكان الدول التأثير على بعضها عن طريق شل الأنظمة المصرفية أو الأمنية أو العسكرية بكبسة زر واحدة عن بعد دون تكبد العناء ودون وقوع خسائر بشرية ومادية في صفوفها، إلا أنها تحدث آثاراً قد تكون مماثلة لتلك التي تخلفها الأسلحة الحركية (التقليدية) في النزاعات التقليدية. وما يترتب على ذلك من تداعيات خطيرة ومؤثرة كالقدرة على تعطيل توفير الخدمات الأساسية للمدنيين عن طريق استهداف الأعيان المدنية والبنى التحتية المدنية بشكل مباشر أو إلحاق الأضرار بها بشكل عرضي، كالمستشفيات، مرافق الرعاية الصحية، المحطات الكهربائية والمائية، أنظمة الاتصالات والمواصلات، والمنشآت الخطرة كالسدود والمحطات النووية والبتروكيماوية. وعليه شكلت العمليات السيبرانية العدائية تحدياً كبيراً في وجه التنظيم الدولي المعاصر، وأثارت العديد من المشكلات القانونية وباتت محل اهتمام العديد من باحثي وفقهاء القانون الدولي في السنوات الأخيرة. نظراً لصعوبة تكييفها وتحديد طبيعتها وعناصرها من جهة وخصائصها التقنية الخاصة والمتمايزة عن الأشكال التقليدية الأخرى لاستخدام القوة، ووسائل وأساليب الحرب المستخدمة في العمليات القتالية والمحظورة بموجب المواثيق والاتفاقيات الدولية الحالية، أو أحكام القانون الدولي العرفي من جهة أخرى.

ولإرساء مبدأ العدالة الجنائية الدولية، ولكي لا تكون الدول والكيانات التابعة لها حرة طليقة في سياق شنها للعمليات السيبرانية العدائية بما يشكل خطراً على الصعيد الوطني والإقليمي وعلى السلم والأمن الدوليين، وبما يحمي حقوق ومصالح كافة الفئات المشمولة بالحماية القانونية الدولية، وبما يحد من الأضرار والخسائر والآثار الناجمة عن استخدامها أثناء النزاعات المسلحة المعاصرة على نحو يتعارض مع القانون الدولي الإنساني والقانون الدولي الجنائي، كان من الضروري البحث فيما إذا كانت قواعد القانون الدولي التقليدية والمتعلقة بالمسؤولية الدولية الجنائية تنطبق عليها وتغطيها.

مشكلة البحث:

تتمحور النقطة الأساسية في البحث حول التساؤل الآتي:

مدى انطباق القواعد العامة التقليدية المتعلقة بالمسؤولية الدولية على العمليات السيبرانية العدائية رغم إشكاليتي القصور التشريعي والطبيعة التقنية التكنولوجية الخاصة التي تمتاز بها؟

يتفرع عن هذا التساؤل الرئيسي التساؤلات الفرعية الآتية:

1- هل تنشأ مسؤولية دولية على الدولة أو مسؤولية فردية جنائية على الأفراد عن العمليات السيبرانية العدائية؟
2-ما هي أركان المسؤولية الدولية ومعايير الإسناد القابلة للتطبيق في سياق العمليات السيبرانية العدائية لضمان محاسبة الدولة التي انتهكت القانون الدولي الإنساني خلال نزاع مسلح قائم؟
3-ما مدى إمكانية أن تصنف العمليات السيبرانية العدائية كجرائم حرب تستوجب قيام المسؤولية الدولية الجنائية والملاحقة والمحاكمة وفقاً للقانون الدولي الجنائي؟
4- هل يمكن أن تستغل الدول الفراغ القانوني المتمثل بعدم وجود معاهدة دولية واضحة تتعلق بالعمليات السيبرانية العدائية للإفلات من العقاب والمساءلة؟
5-ما هو أثر غياب الإطار القانوني الدولي الناظم للعمليات السيبرانية العدائية على وضع المسؤولية الدولية موضع تطبيق ضد من ينتهك القانون الدولي الإنساني أثناء النزاعات المسلحة المعاصرة؟
6-كيف يمكن أن تؤثر الطبيعة التقنية والتكنولوجية الخاصة والمتمايزة للعمليات السيبرانية العدائية على موضوع المساءلة والشفافية وأركان المسؤولية الدولية؟

أهمية البحث و أهدافه:

أهمية البحث:

تظهر أهمية البحث انطلاقاً من اعتباره محاولة بحثية قانونية تخوض في موضوع معاصر على مستوى الدراسات القانونية في مجال القانون الدولي ولها ارتباطات بعدد من فروعه، في ضوء الانتشار الهائل للعمليات السيبرانية العدائية في الوقت الراهن وخاصة أثناء النزاعات المسلحة المعاصرة الدولية وغير الدولية نتيجة تزايد ارتباط العالم بالفضاء السيبراني وما يترتب على ذلك من أضرار وخسائر، ولضمان عدم إفلات الجهات الدولية من المساءلة والملاحقة والعقاب في حال شنها لتلك العمليات بما يتعارض مع القانون الدولي الإنساني والقانون الدولي الجنائي متذرعةً بعدم وضوح المفاهيم والمبادئ التقليدية المتعلقة بالمسؤولية الدولية لجهة مدى شموليتها وانطباقها عليها نظراً لما تتمتع به من خصوصية وطبيعة تقنية متمايزة عن غيرها من وسائل وأساليب القتال الموجبة للمسؤولية الدولية.

أهداف البحث:

تتلخص أهداف البحث بالآتي:

1-يسعى إلى تحديد مدى المسؤولية الدولية الجنائية الناشئة عن العمليات السيبرانية العدائية والواقعة من دول ضد أخرى خلال نزاع مسلح قائم.

2-بيان مدى إمكانية تطبيق المبادئ التقليدية للمسؤولية الدولية المعروفة في الإطار القانوني الدولي القائم على العمليات السيبرانية العدائية المتبادلة بين الدول أثناء النزاعات المسلحة المعاصرة.

3-بيان التحديات والصعوبات المتعددة والتي تكتنف إقرار مبدأ المسؤولية الدولية الجنائية عن العمليات السيبرانية العدائية ضمن الإطار القانوني الدولي القائم.

4-مناقشة أركان المسؤولية الدولية وعناصرها ومعايير إسنادها ومدى انطباقها على العمليات السيبرانية العدائية رغم اختلافها وتمايزها عن سواها من وسائل وأساليب القتال الأخرى الموجبة للمسؤولية.

5-دراسة إمكانية أن تمارس المحكمة الجنائية الدولية اختصاصها القضائي وتتصدى للانتهاكات الجسيمة للقانون الدولي الإنساني الناجمة عن العمليات السيبرانية العدائية ومحاكمة المسؤولين عنها.

منهجية البحث:

تم اتباع المنهج الوصفي والمنهج التحليلي كمنهجين أساسيين في البحث من خلال توصيف مدى إمكانية الإقرار بقيام المسؤولية الدولية الجنائية عن العمليات السيبرانية العدائية التي تستخدم أثناء النزاعات المسلحة المعاصرة على الرغم من اختلافها وتمايزها عن العمليات العسكرية التقليدية الموجبة للمسؤولية في حال ثبوت انتهاكها للقانون الدولي الإنساني، وذلك بتحليل نصوص مواد المواثيق والاتفاقيات الدولية ذات الصلة بالموضوع، كاتفاقيات جنيف الأربع 1949، وبروتوكولاتها اللاحقة 1977، نظام روما الأساسي للمحكمة الجنائية الدولية 1998، مشروع لجنة القانون الدولي حول المسؤولية الدولية عن الأفعال غير المشروعة دولياً 2001، ودليل تالين للقانون الدولي المطبق على الحرب السيبرانية 2013 -2017.

النتائج والمناقشة:

المطلب الأول: أثر شن العمليات السيبرانية العدائية على إثارة المسؤولية الدولية.

عرفت المادة الأولى من مشروع تقنين مسؤولية الدول عن الأفعال غير المشروعة دولياً لعام 2001 المسؤولية الدولية: كل فعل غير مشروع دولياً تقوم به الدولية يستتبع مسؤوليتها الدولية[1].

تعد المسؤولية الدولية عنصراً من عناصر الشخصية القانونية الدولية، وهي من أهم الأسس التي يقوم عليها القانون الدولي كونها الأداة القانونية اللازمة لضمان المحافظة على تطبيق قواعده وتعزيز السلم والأمن الدوليين وتدعيم التعاون الدولي[2]. وفي عالم اليوم المترابط، أصبح من الصعب تخيل نزاع بين دولتين لا ينطوي على استخدام "القوة السيبرانية" فبرزت العمليات السيبرانية العدائية بشكل متزايد وشكلت مصدر قلق أمني عالمي ملح. هذه العمليات التي تستهدف البنية التحتية الحيوية وتعطل الخدمات الأساسية في الدولة وتلحق أضراراً واسعة النطاق بالمدنيين والأعيان المدنية مثلت تحديات عديدة للأطر القانونية القائمة بموجب القانون الدولي الإنساني والقانون الدولي الجنائي حيث تم التركيز

[1]- مشروع المواد المتعلق بمسؤولية الدول عن الأفعال غير المشروعة دولياً لعام 2001، تقرير لجنة القانون الدولي للجمعية العامة للأمم المتحدة عن أعمال دورتها الثالثة والخمسين، حولية لجنة القانون الدولي، المجلد الثاني، الجزء الثاني،ص41،المادة الأولى.

[2]- محمد سعادي، المسؤولية الدولية للدولة في ضوء التشريع والقضاء الدوليين. المصرية للنشر والتوزيع، الطبعة الأولى، 2019، ص20.

على أعمال العنف والعدوان التقليدية والملموسة(المادية)[3]. فكان من الضروري تناول عنصر المساءلة بوصفه عنصراً أساسياً من عناصر القانون الدولي الإنساني، حيث أثيرت الشكوك حول إمكانية المحافظة على معايير المسؤولية الدولية والسلوك المسؤول في سياق استخدام العمليات السيبرانية العدائية وتداعيات ذلك أثناء النزاعات المسلحة المعاصرة[4].

الفرع الأول: أركان المسؤولية الدولية ومدى انطباقها في سياق العمليات السيبرانية العدائية.

يجمع الفقهاء والمختصون في القانون الدولي على أن المسؤولية الدولية لا يمكن أن تثور في مواجهة دولة ما وفقاً لما هو ثابت في إطار قواعد ومبادئ ذلك القانون ما لم تتوافر ثلاثة أركان[5]:

أولاً: القيام بفعل غير مشروع من أحد أشخاص القانون الدولي ينطوي على انتهاك أو خرق لقواعده.

ثانياً: إلحاق ضرر بشخص آخر من أشخاص القانون الدولي.

ثالثاً: إسناد الفعل غير المشروع إلى أحد أشخاص القانون الدولي.

أولاً: الفعل غير المشروع.

هو الواقعة المنشأة للمسؤولية الدولية، ويقصد به أن تخالف الدولة التزاماً دولياً مفروضاً عليها والذي يتمثل طبقاً للمادة (38) من النظام الأساسي لمحكمة العدل الدولية في التزام تعاهدي (اتفاقية دولية) أو قاعدة عرفية دولية أو أحد المبادئ العامة للقانون[6]. أي أن المسؤولية الدولية لا يمكن أن تثور إلا إذا ثبت أن الفعل كان مخالفاً لأحكام القانون الدولي التعاهدية أو العرفية. ويكون كذلك في الحالات التالية[7]:

أ- خرق مبادئ الأمم المتحدة: كأن يرقى هجوم ما إلى مستوى استخدام القوة المحظورة بموجب المادة (2ف4) من الميثاق.

ب- خرق الالتزامات الدولية التي يفرضها القانون الدولي الإنساني كحظر استهداف المدنيين والأعيان المدنية والفئات المحمية أثناء النزاعات المسلحة.

ت- خرق القواعد الدولية في وقت السلم خارج سياق النزاعات المسلحة كخرق مبدأ عدم جواز التدخل في الشؤون الداخلية للدول بموجب المادة(2ف7) من الميثاق.

[3]- كارولين بويزمان، مقدمة بعنوان: الهجمات السيبرانية بموجب القانون الجنائي الدولي-تحديات التحقيق والملاحقة القضائية- في الكتاب الموسوم: الدليل إلى فهم جريمة العدوان السيبرانية: دراسة في إطار مواجهة قانونية سياسية فاعلة. أحمد عبيس نعمة الفتلاوي، قاسم محمد مهدي الغزي، منشورات زين الحقوقية، بيروت، الطبعة الأولى، 2025، ص1.

[4]- ابراهيم السيد أحمد رمضان، مواجهة الهجمات السيبرانية في ضوء أحكام القانون الدولي. مجلة العلوم القانونية والاقتصادية، العدد الأول، السنة السابعة والستون، 2025، ص1831.

[5]- محمد سعادي، المسؤولية الدولية للدولة في ضوء التشريع والقضاء الدوليين، مرجع سابق، ص21.

[6]- النظام الأساسي لمحكمة العدل الدولية لعام 1945، المادة38.

[7]- عدنان النقيب، الحرب الإلكترونية في ضوء بروتوكولي سبع وسبعين الملحقين باتفاقيات جنيف الأربع لسنة تسع وأربعين(الهجمات السيبرانية) المركز العربي للنشر والتوزيع، الطبعة الأولى، 2022، ص344.

على الصعيد السيبراني، وبالعودة إلى مشروع تقنين مسؤولية الدول عن الأفعال غير المشروعة دولياً لعام 2001، فقد أكدت المادة (19) على أن: فعل الدولة الذي يشكل مخالفة لالتزام دولي يعد فعلاً جائراً دولياً بغض النظر عن موضوع الالتزام الدولي الذي تمت مخالفته[8]. وجاءت القاعدة (6) من دليل تالين للقانون الدولي المطبق على الحرب السيبرانية لعام 2013 وتقابلها القاعدة(14) من ذات الدليل بإصداره الثاني لعام 2017 وأكدت على أن:

تتحمل الدولة المسؤولية القانونية الدولية للعمليات السيبرانية التي تنسب إليها والتي تعد خرقاً لالتزام دولي[9]. وبتحليل نصوص المواد سالفة الذكر يتبين أنها أكدت على تقرير أحكام المسؤولية الدولية عن العمليات السيبرانية باعتبار أنه وإن كانت بعض هذه العمليات لا تنتهك القانون الدولي بحد ذاتها إلا أن الطريقة التي تنفذ بها قد تعتبر فعلاً غير مشروع دولياً وخرقاً لالتزامات الدولة[10]، نظراً لأنها تنطوي في حقيقتها وآثارها على مخالفة واضحة وصريحة لمقاصد ومبادئ جوهرية ذات أهمية أساسية في الحفاظ على السلم والأمن الدوليين، أشارت إليها الاتفاقيات والأعراف والمواثيق الدولية وألزمت الدول باحترامها. كمبدأ عدم جواز انتهاك سيادة الدول، مبدأ عدم جواز استخدام القوة أو التهديد بها وفقاً للمادة(2فـ4)، مبدأ عدم جواز التدخل في الشؤون الداخلية للدول وفقاً للمادة(2فـ7)، ومبدأ حل النزاعات الدولية بالطرق السلمية وفقاً للمادة (33) من ميثاق الأمم المتحدة. بالإضافة لكونها تتعارض مع قواعد ومبادئ القانون الدولي الإنساني وتمثل انتهاكات جسيمة للالتزامات الدولية المفروضة بموجبه كتلك التي تحظر العدوان، استهداف المدنيين والأعيان المدنية بهجمات عشوائية أثناء النزاعات المسلحة وتؤدي لارتكاب جرائم حرب[11].

ثانياً: الضرر.

يعد عنصر الضرر أحد أهم وأبرز أركان المسؤولية الدولية، نظراً لأن انعدامه في بعض الحالات يعني انعدام المسؤولية الدولية[12]. وفي سياق العمليات السيبرانية العدائية فمن الملاحظ أنها تهدف في الغالب إلى المساس بالمصالح الاستراتيجية الحساسة، والأمن القومي والسياسي للدول المعتدى عليها لزعزعة الاستقرار فيها وتحقيق غايات أمنية أو عسكرية أو سياسية[13]. فعلى سبيل المثال تستهدف شبكة المعلومات التي تتحكم بالبنية التحتية الحرجة للدولة من خلال التسلل إلى الأنظمة الإلكترونية الخاصة بحماية وتنظيم عمل المنشآت الحيوية كشبكات الاتصال، محطات المياه والكهرباء، قطاع النقل والصحة، السدود، محطات الطاقة النووية والكيميائية والسيطرة عليها والتحكم بها ثم تعطيلها أو تدميرها كلياً أو جزئياً، مما يؤدي إلى وقوع خسائر في الأرواح والممتلكات، تدمير الأعيان المدنية والإضرار

[8]- مشروع المواد المتعلق بمسؤولية الدول عن الأفعال غير المشروعة دولياً، مرجع سابق، المادة19.

[9] دليل تالين للقانون الدولي المطبق على الحرب السيبرانية بإصداريه 2013، 2017، إعداد اللجنة الدولية للخبراء بدعوة من مركز التميز للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي(الناتو). ترجمة: علي محمد كاظم موسوي، انجلترا: جامعة كامبردج، الجزء الأول: القانون الدولي للأمن السيبراني، القسم الثاني: مسؤولية الدولة، القاعدة 6، 14، ص3.

[10]- طلال ياسين العيسى، عدي محمد عناب، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد19، العدد الأول، 2019، ص89.

[11]- محمود حسين الشرقاوي، الهجمات الإلكترونية في ضوء أحكام القانون الدولي الإنساني. رسالة مقدمة لنيل درجة الدكتوراه في القانون الدولي، قسم القانون الدولي، كلية الحقوق، جامعة بني سويف، مصر، 2022، ص118.

[12]- محمد سعادي، المسؤولية الدولية للدولة في ضوء التشريع والقضاء الدوليين. مرجع سابق، ص45.

[13]- ناجي محمد أسامة الشاذلي، الجوانب القانونية للحرب السيبرانية(دراسة في إطار القانون الدولي الإنساني)مجلة روح القوانين، العدد103، الجزء الثاني، 2023، ص1256.

بالبيئة الطبيعية[14]. وهذا يعني أن آثارها لن تقتصر على العالم الافتراضي بل ستصل للعالم المادي وتتسبب بأضرار تكاد تكون مماثلة لتلك التي يخلفها الاستخدام المادي للقوة العسكرية التقليدية المحظورة[15]. وعليه يتبين أن عنصر الضرر المتأتي من العمليات السيبرانية العدائية واقع لا محالة ويتحقق بكافة أشكاله (مباشر، غير مباشر، مادي، معنوي) وهو المبرر الأساسي لقيام المسؤولية الدولية[16].

ثالثاً: إسناد الفعل غير المشروع للدولة.

يعني ضرورة إسناد أو نسبة الواقعة المنشأة للمسؤولية الدولية إلى أحد أشخاص القانون الدولي (لدولة معينة) لإثارة مسؤوليتها الدولية[17]. وهو الركن الذي أكدته المواد (14-19) من مشروع تقنين مسؤولية الدول عن الأفعال غير المشروعة دولياً لعام 2001. على الصعيد السيبراني وعلى الرغم من أن مسألة إسناد العمليات السيبرانية العدائية لجهة محددة قد تكون ممكنة في حالات قليلة كقيام الفاعل بالكشف عن نفسه(الإقرار من الدولة) أو عندما تمثل تلك العمليات مرحلة أولية تسبق القيام بالهجمات التقليدية أو تستخدم لتغطية مصادر الهجوم الأصلية[18]. إلا أنها تبقى عملية عقدة لمالها من جوانب فنية، قانونية وسياسية. ويكتنفها تحديات وصعوبات كبيرة[19] والتي يمكن تلخيصها على النحو الآتي:

1-تخفي بعض الدول وراء كيانات فاعلة من غير الدول كالجماعات المسلحة أو الشركات العسكرية والأمنية الخاصة[20] بالتنسيق مع حكومة الدولة وتتلقى منها دعماً لوجستياً واستخباراتيا يمكنها من اختراق المواقع الإلكترونية للمصالح الحيوية والأنظمة الدفاعية والأمنية الموجودة في دولة أخرى[21].

2-إن الإقرار بالعمليات السيبرانية العدائية وتبنيها بشكل علني من غير المرجح أن يحدث، وذلك لأن العمليات السيبرانية أصبح الأداة المثالية للعمليات السرية، والإقرار بها والكشف عنها يعد اعترافاً صريحاً بالقدرات السيبرانية للدولة وأجهزتها[22].

3-جمع الأدلة الجنائية في السياق السيبراني يعد من المسائل المعقدة للغاية لإمكانية القيام بالعمليات السيبرانية في غضون ثوانٍ معدودة مع قابلية محو الأدلة وإخفاء الجناة في كثير من الأحيان وراء جهات فاعلة بالوكالة لمنع تعقب الفاعل الحقيقي[23].

[14]- حليمة صالح الدرمكي، وائل أحمد علام، المسؤولية الدولية الواقعة من كيانات من غير الدول. مجلة جامعة الشارقة للعلوم القانونية، المجلد21، العدد4، 2024، ص469.

[15]- محمود حسين الشرقاوي، الهجمات الإلكترونية في ضوء أحكام القانون الدولي الإنساني، مرجع سابق، ص15.

[16]- عدي محمد عناب، طلال ياسين العيسى، المسؤولية الدولية الناشئة عن الهجمات السيبرانية، مرجع سابق، ص89.

[17]- محمد سعادي، المسؤولية الدولية للدولة في ضوء التشريع والقضاء الدوليين، مرجع سابق، ص55.

[18]- عدنان النقيب، الحرب الإلكترونية، مرجع سابق، ص343.

[19]- حليمة صالح الدرمكي، وائل أحمد علام، المسؤولية الدولية عن الهجمات السيبرانية، مرجع سابق، ص482.

[20] Lauran Jesel, Telman Rodnhouser, Knoth Dorman. International humanitarian law and the protection civilians in the effects of cyber operations during armed conflicts, International Journal of the Red Cross, Geneva, Vol:102, No:913, 2020, P:308.

[21]- حليمة صالح الدرمكي، وائل أحمد علام، المسؤولية الدولية عن الهجمات السيبرانية، مرجع سابق، ص476-477.

[22]- محمود حسين الشرقاوي، الهجمات الإلكترونية في ضوء القانون الدولي الإنساني، مرجع سابق، ص117.

[23]- المرجع السابق، ص108.

4-صعوبة تحديد المصدر (الدولة أو الإقليم) الذي انطلقت منه العمليات نظراً لافتقار الفضاء السيبراني للحدود التقليدية الجغرافية والإقليمية[24]، وما يتمتع به من خصائص تمكن من شن العمليات السيبرانية من مصادر مجهولة باستخدام الحواسيب المأمورة أو حواسيب مسيرة أو استخدام خداع بروتوكول الإنترنت، إضافةً لقابلية إخفاء الهوية وتزويرها[25].

5-الخصائص التقنية والتكنولوجية المتطورة والمميزة للعمليات السيبرانية، إضافة إلى طبيعتها غير الملموسة وغير المادية، إلى جانب المسافة الجغرافية الفاصلة بين مكان ارتكابها ونطاق آثارها[26].

6-صعوبة توافر إسناد قاطع لصعوبة الحصول على أدلة إثبات كافية وراسخة وقانونية على تورط دولة ما بالهجوم السيبراني، نظراً لافتقاد أغلب الدول إلى وجود تشريعات متخصصة بالفضاء السيبراني وغياب القواعد القانونية ذات الصلة بالمسؤولية الدولية عن العمليات السيبرانية[27].

7-تتجاوز العمليات السيبرانية العدائية الحدود الوطنية نظراً لطبيعتها العابرة للحدود مما يعد عقبة كبيرة أمام مبدأ الولاية القضائية بسبب تأثيرها على العديد من الدول والولايات القضائية في آنٍ معاً[28].

في ضوء عدم وضوح المفاهيم التقليدية للمسؤولية الدولية في سياق التكنولوجيا والتقنيات الحديثة[29] يتبين أن المسؤولية الدولية عن العمليات السيبرانية العدائية في إطار القواعد التقليدية للقانون الدولي العام قد لا تحقق أهدافها وأغراضها نظراً للتحديات التي قد تحول دون وضعها موضع تطبيق فعلي وما يترتب على ذلك من تبعات الملاحقة القضائية وإكمال اجراءات المتابعة ضمن أطر التحقيق والمساءلة الدولية. لكن وعلى الرغم من ذلك لا يجب أن تكون هذه التحديات ذريعة لعدم القيام بمعالجة الجوانب القانونية للعمليات السيبرانية العدائية وخاصةً فيما يتعلق "بالمسؤولية الدولية الجنائية" سيما وأن مشكلة الإسناد موجودة بالفعل في العديد من المسائل الأخرى إلا أن ذلك لم يمنع من وضع إطار قانوني لها "كالإرهاب الدولي"[30]، بما يضمن تحقيق أهداف القانون الدولي الجنائي وإرساء العدالة الجنائية الدولية.

ويرأينا أن إرساء المسؤولية الدولية الجنائية بموجب القانون الدولي الجنائي يتطلب إعادة تقييم القواعد القانونية القائمة مع وضع معايير جديدة تتلاءم مع خصوصية العمليات السيبرانية العدائية لضمان التطبيق الفعال لقوانين وأطر التحقيق والمساءلة الدولية، ولمنع الدول التي تستغل الفضاء السيبراني لارتكاب عمليات سيبرانية خبيثة وضارة ترقى إلى مستوى الجرائم الدولية أو المساعدة في ارتكابها.

[24]- حليمة صالح الدرمكي، وائل أحمد علام، المسؤولية الدولية عن الهجمات السيبرانية، مرجع سابق، ص482.

[25]- عدنان النقيب، الحرب الإلكترونية، مرجع سابق، ص343.

[26]- كارولينا بويزمان، الهجمات السيبرانية بموجب القانون الدولي الجنائي، مرجع سابق، ص3.

[27]- ابراهيم السيد أحمد رمضان، مواجهة الهجمات السيبرانية، مرجع سابق، ص1846.

[28]- كارولينا بويزمان، الهجمات السيبرانية بموجب القانون الدولي الجنائي، مرجع سابق، ص4.

[29]- ابراهيم السيد أحمد رمضان، مواجهةالهجمات السيبرانية، مرجع سابق، ص1832.

[30]- محمود حسين الشرقاوي، الهجمات الإلكترونية في ضوء أحكام القانون الدولي الإنساني، مرجع سابق، ص108-109.

الفرع الثاني: المسؤولية الدولية الجنائية عن انتهاكات العمليات السيبرانية للقانون الدولي الإنساني.

تعرف المسؤولية الدولية الجنائية بأنها: مساءلة دولة ما عن ارتكابها لفعل 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، ويعد نظام روما الأساسي للمحكمة الجنائية الدولية لعام 1998 من الوثائق الدولية العديدة التي رسخت المبادئ العامة لقواعد المسؤولية الدولية الجنائية في إطار معاهدة متعددة الأطراف، وتثور عند ارتكاب الأفعال الموصوفة كجرائم دولية وفقاً للمادة (5) من النظام، فاحتلت أهمية كبرى في العلاقات الدولية سيما وأن إقرارها وقبولها يمكن أن يسهم في الحفاظ على السلم والأمن الدوليين واحترام حقوق الإنسان[31]. خاصة في ضوء تطور وسائل وأساليب القتال وظهور أدوات مستحدثة، حيث بات أطراف النزاعات المسلحة المعاصرة يوظفون كل ما يملكون من الأسلحة التقليدية والتكنولوجية بهدف تحقيق التفوق العسكري والقضاء على الطرف الآخر بما فيها العمليات السيبرانية العدائية دون الوضع في الاعتبار ما يسفر عنها من تداعيات وأضرار على المجتمع الدولي وما تنطوي عليه من انتهاكات جسيمة للقانون الدولي الإنساني[32].

في السياق السيبراني يفترض لقيام مسؤولية الدولة الجنائية تنفيذها لعمليات سيبرانية عدائية ترقى لمستوى "الهجوم المسلح" على النحو الوارد في القانون الدولي الإنساني خاصة إذا ما شكلت جريمة دولية (كجريمة العدوان على سيادة الدول أو جرائم حرب في سياق النزاعات المسلحة) ونجم عنها وفيات وإصابات بين السكان المدنيين أو تدمير للأعيان المدنية أو الإضرار بالبيئة الطبيعية[33]. وعليه ستكون الدولة منتهكة لقاعدة دولية تعاهدية أو عرفية أثناء النزاع المسلح، وأن المسؤولية الدولية الجنائية على ذلك الأمر ستكون في نطاق المبادئ الدولية الناظمة لسير الأعمال القتالية وتصرفات المقاتلين وطرائق العمليات العسكرية والتي تهدف إلى توفير حماية أكثر فاعلية للفئات المشمولة بالحماية بموجب القانون الدولي الإنساني. وهي[34]:

1-مبدأ حق أطراف النزاع في اختيار وسائل وأساليب القتال ليس حقاً مطلقاً. ويتفرع إلى مبدأين هما:

أ- مبدأ وجوب التمييز بين المدنيين والمقاتلين.

ب- مبدأ حظر الإصابات المفرطة الضرر والعشوائية الأثر والآلام التي لا مبرر لها.

2-مبدأ الضرورة العسكرية.

3-مبدأ التناسب في استخدام القوة.

4-شرط مارتنز.

وتأسيساً على أن الدولة ليست محلاً "للجزاءات الجنائية" وأن الشخص الطبيعي وحده القادر على خرق القانون وارتكاب الجرائم التي تكون سبباً للمسؤولية الجنائية، أقرت المادة (25) من نظام روما الأساسي مبدأ المسؤولية الجنائية الفردية

[31]- محمود شريف بسيوني، المحكمة الجنائية الدولية نشأتها ونظامها الأساسي مع دراسة لتاريخ لجان التحقيق الدولية والمحاكم الجنائية الدولية السابقة. مطابع روز اليوسف الجديدة، القاهرة، الطبعة الأولى،2001، ص42-43.

[32] -ICRC, ICRC Position paper: International humanitarian law and cyber operations during armed conflicts. International Review of the Red Cross, Geneva, Vol:102, No:913, 2020, p:482-483.

[33]- حليمة صالح الدرمكي، وائل أحمد علام، المسؤولية الدولية عن الهجمات السيبرانية، مرجع سابق، ص480.

[34]- أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر. مجلة المحقق المحلي للعلوم القانونية والسياسية، العدد الرابع، السنة الثامنة، 2016، ص642.

إلى جانب المسؤولية الدولية الجنائية، والذي يعد من أهم الضمانات القانونية والآليات العملية لمنع انتهاكات القانون الدولي الإنساني خلال النزاعات المسلحة، ويقضي بمسؤولية الأفراد عن الجرائم التي تدخل في اختصاص المحكمة، فنصت على أن: المسؤولية الجنائية مسؤولية فردية لا يمكن أن تتعدى الشخص ولا ممتلكاته. وبذلك تكون قد وجهت العقاب إلى جسد الإنسان أو حريته الشخصية أو أمواله[35].

وبناءً عليه، فإن مرتكبي العمليات السيبرانية العدائية من قادة عسكريين أو رؤساء مدنيين سيكونون محلاً للمسؤولية الجنائية الفردية (الشخصية) وفقاً للقانون الدولي الجنائي رداً على انتهاكاتهم الجسيمة للقانون الدولي الإنساني[36].

كما أقرت المادة (86) من البروتوكول الإضافي الأول لعام 1977 والملحق باتفاقيات جنيف الأربع 1949 مبدأ المسؤولية الجنائية الفردية للقادة والرؤساء ونصت:

أ- تعمل الأطراف السامية المتعاقدة وأطراف النزاع على قمع الانتهاكات الجسيمة واتخاذ الاجراءات اللازمة لمنع كافة الانتهاكات الأخرى للاتفاقيات ولهذا الملحق (البروتوكول) التي تنجم عن التقصير في أداء عمل واجب الأداء.
ب- لا يعفي قيام أي مرؤوس بانتهاك الاتفاقيات أو هذا الملحق (البروتوكول) رؤساءه من المسؤولية الجنائية أو التأديبية حسب الأحوال إذا علموا أو كانت لديهم معلومات تتيح لهم في تلك الظروف أن يخلصوا إلى أنه كان يرتكب أو أنه في سبيله لارتكاب مثل هذه الانتهاكات ولم ينجزوا كل ما في وسعهم من اجراءات مستطاعة لمنع أو قمع هذه الانتهاكات[37].
ووسعت أحكام المادة (87/أ) من مسؤولية القادة والرؤساء لتشمل الأشخاص الآخرين الخاضعين لسيطرتهم[38].

وعالجت المادتين (27-28) من النظام روما الأساسي قواعد هذه المسؤولية، فجاءت المادة (27) بعنوان: عدم الاعتداد بالصفة الرسمية لدفع المسؤولية، بينما كانت المادة (28) بعنوان: مسؤولية القادة والرؤساء الآخرين. فنصت (فـ1 من المادة 27 من نظام روما): يطبق هذا النظام الأساسي على الأشخاص بصورة متساوية دون تمييز بسبب الصفة الرسمية. وبوجه خاص فإن الصفة الرسمية للشخص سواء كان رئيساً لدولة أو لحكومة أو عضواً في الحكومة أو برلمان أو ممثلاً منتخباً او موظفاً حكومياً لا تعفيه بأي حال من الأحوال من المسؤولية الجنائية بموجب هذا النظام. كما أنها لا تشكل في حد ذاتها سبباً لتخفيف العقوبة[39]. أما (فـ2 من ذات المادة) نصت على: لا تحول الحصانات أو القواعد الاجرائية الخاصة التي قد ترتبط بالصفة الرسمية للشخص سواء كانت في إطار القوانين الوطنية أو الدولية دون ممارسة المحكمة اختصاصها على هذا الشخص[40].

في حين نصت المادة(28) من نظام روما على مسؤولية القادة العسكريين والرؤساء المدنيين بأنه: يكون القائد العسكري أو الشخص القائم فعلاً بأعماله مسؤولاً مسؤولية جنائية عن الجرائم التي تدخل في اختصاص المحكمة والمرتكبة من

[35]- نظام روما الأساسي للمحكمة الجنائية الدولية لعام 1998، المادة 25.

[36] -Ewan Lawson, Kubo Macak, Avoiding civilians harm from military cyber operations during armed conflicts. ICRC/ Expert Meeting 21-22 January 2020, Geneva, p:14.

[37]- البروتوكول الأول الملحق باتفاقيات جنيف الأربع لعام 1949 والخاص بحماية ضحايا النزاعات المسلحة الدولية لعام 1977، المادة86.

[38] - المادة 87 من البروتوكول ذاته.

[39] - نظام روما الأساسي للمحكمة الجنائية الدولية لعام 1998، المادة 27 الفقرة 1.

[40]- نظام روما الأساسي، المادة 27 الفقرة 2.

جانب قوات تخضع لسلطته وسيطرته الفعليتين نتيجة لعدم ممارسة القائد العسكري أو الشخص سيطرته على هذه القوات ممارسة صحيحة.

أ- إذا كان القائد العسكري قد علم أو يفترض أن يكون قد علم بسبب الظروف السائدة بأن القوات ترتكب أو على وشك أن ترتكب هذه الجرائم.

ب- إذا لم يتخذ القائد العسكري أو الشخص جميع التدابير اللازمة في حدود سلطته لمنع أو قمع ارتكاب هذه الجرائم أو لعرض المسألة على السلطات المختصة للتحقيق والمقاضاة[41].

أما بالنسبة للرؤساء المدنيين فيسأل الرئيس عن جرائم مرؤوسيه الخاضعين لسلطته وسيطرته الفعليتين في الحالات:

أ- إذا كان قد علم أو تجاهل عن وعي أية معلومات تظهر بوضوح أن مرؤوسيه يرتكبون أو على وشك أن يرتكبوا هذه الجرائم.

ب- إذا تعلقت الجرائم بأنشطة تندرج في إطار المسؤولية والسيطرة الفعلية للرئيس.

ت- إذا لم يقم بجميع التدابير اللازمة المعقولة في حدود سلطته لمنع أو قمع ارتكاب هذه الجرائم أو لعرض المسألة على السلطات المختصة للتحقيق والمحاكمة[42].

وتناولت كذلك قواعد دليل تالين للقانون الدولي المطبق على الحرب السيبرانية بإصداريه الأول 2013 والثاني 2017 المسؤولية الجنائية للقادة والرؤساء عن العمليات السيبرانية. فنصت القاعدة (24) من دليل تالين الأول والقاعدة (85) من دليل تالين الثاني على أنه:

أ- يتحمل القادة العسكريين والرؤساء المسؤولية الجنائية لإصدار الأوامر بشأن العمليات السيبرانية التي تشكل جرائم حرب.

ب- كذلك يكون القادة مسؤولين في حال علمهم أو وجوب علمهم بسبب الظروف السائدة في ذلك الوقت بأن مرؤوسيهم قد يرتكبون أو على وشك ارتكاب أو ارتكبوا جرائم حرب وفشل القائد في اتخاذ جميع التدابير المعقولة والمناسبة لمنع ارتكاب هذه الجرائم أو معاقبة المسؤولين عنها[43].

وبتحليل ومراجعة ما ذكر من مواد يتبين أن الشخص ملزماً بوصفه قائداً أو رئيساً بالتدخل الفوري عندما تشكل أفعال مرؤوسيه أو كان من شأنها أن تشكل انتهاكات جسيمة للقانون الدولي الإنساني وعليه منع هذه الانتهاكات أو قمعها، وعدم قيامه بذلك يعني أنه سيتحمل المسؤولية الجنائية عنها[44]. وتشمل هذه المسؤولية جميع من هم في التسلسل القيادي بدءاً من أعلى المستويات مصدري القرارات السياسية ومروراً بالضباط والجنود، وصولاً لأفراد الميليشيات والمدنيين الذين ارتكبوا تلك الجرائم والانتهاكات، إذا ما كانوا خاضعين لقيادتهم وسلطتهم الفعلية، وإذا ما علموا أو يفترض علمهم بأن هناك جريمة قد ترتكب وأهملوا في اتخاذ ما يلزم من اجراءات ضرورية لمنعها[45].

[41]- نظام روما الأساسي، المادة 28، الفقرة 1.

[42]- نظام روما الأساسي، المادة 28، الفقرة 2.

[43]- دليل تالين للقانون الدولي المطبق على الحرب السيبرانية، القاعدة 24 من الاصدار الأول 2013، والقاعدة 85 من الاصدار الثاني 2017.

[44]- عدنان النقيب، الهجمات الإلكترونية، مرجع سابق، ص358- 359.

[45]- متولي رشاد متولي الصعيدي، محمد سيد محمد عبد اللطيف، أحمد ربيع محمد، آثار الذكاء الاصطناعي والحرب السيبرانية على البيئة الإنسانية أثناء النزاعات المسلحة. مجلة البحوث الفقهية والقانونية، العدد47، 2024، ص3908.

ويرأينا أن الغرض الأساسي من إعمال مسؤولية القادة والرؤساء يكمن في إرساء العدالة الجنائية الدولية من جهة وضمان توخي ذوي السلطة في جميع المستويات القيادية العناية الكاملة لمنع انتهاكات القانون الدولي الإنساني. حتى ولو وقعت عبر وسائل إلكترونية أو سيبرانية لأن القانون الدولي الإنساني ينطبق على أساليب ووسائل الحرب الجديدة والمستحدثة حتى التي لم تكن قد ظهرت حينما تم صياغة هذا القانون.

المطلب الثاني: اختصاص القضاء الدولي الجنائي في التصدي للعمليات السيبرانية العدائية.

نص نظام روما الأساسي للمحكمة الجنائية الدولية لعام 1998 على الاختصاص الموضوعي للمحكمة وقصره على أربع جرائم دولية فقط تدخل في ولاية المحكمة القضائية وهي جريمة الإبادة الجماعية، الجرائم ضد الإنسانية، جرائم الحرب، وجرائم العدوان، باعتبار أنها من الجرائم التي تنطوي على انتهاك أو خرق القيم الأساسية للمجتمع الدولي[46]. يثور التساؤل في الوقت الراهن حول مدى استيفاء العمليات السيبرانية العدائية لعناصر الجريمة الأساسية المتعددة على النحو المنصوص عليه في نظام روما كونها تمثل نوعاً جديداً من أنواع الجرائم الدولية المستحدثة، نظراً للانتهاكات الجسيمة الناجمة عنها أثناء النزاعات المسلحة المعاصرة والتي قد تشكل جرائم حرب وفقاً للقانون الدولي الجنائي، ليصار إلى إقرار قانونية تصدي المحكمة الجنائية الدولية لها ومنع إفلات منفذيها من العقاب.

الفرع الأول: مدى إمكانية تصنيف العمليات السيبرانية كجرائم حرب.

يقصد بجرائم الحرب تلك الانتهاكات التي تقع ضد القوانين والأعراف الناظمة لسلوك الدول والقوات المتحاربة والأفراد في حالة وجود نزاع مسلح دولي أو غير دولي والتي من شأنها أن تمس بالأشخاص أو الممتلكات[47].

أشارت المادة (8) من نظام روما الأساسي للمحكمة الجنائية الدولية إلى صور جرائم الحرب التي تستوجب المسؤولية الدولية الجنائية وتدخل في الاخصاص الموضوعي للمحكمة على النحو التالي[48]:

الانتهاكات الجسيمة لاتفاقيات جنيف الأربع لعام 1949 لحماية المدنيين والمتمثلة في أي فعل موجه ضد الأشخاص أو المنشآت والممتلكات المحمية بموجبها (المادة 8/فقرة 2/أ) من نظام روما والتي اشتملت على ثمان صور من جرائم الحرب في النزاعات المسلحة الدولية.

الانتهاكات الخطيرة للقوانين والأعراف السارية أثناء النزاعات المسلحة الدولية (المادة8/ف 2/ب) من نظام روما واشتملت على (26) جريمة مختلفة من جرائم الحرب والتي يمكن أن ترتكب أثناء النزاعات المسلحة الدولية.

الانتهاكات الجسيمة للمادة الثالثة المشتركة من اتفاقيات جنيف الأربع أثناء النزاعات المسلحة غير الدولية (المادة8/ف2/ج) من نظام روما والتي اشتملت على أربع صور من جرائم الحرب في النزاعات المسلحة غير الدولية.

[46]- نظام روما الأساسي للمحكمة الجنائية الدولية لعام 1998، المادة 6،7،8.

[47]– محمود شريف بسيوني، المحكمة الجنائية الدولية، نشأتها ونظامها الأساسي، مرجع سابق، ص177.

[48]- نظام روما الأساسي للمحكمة الجنائية الدولية لعام 1998، المادة 8.

الانتهاكات الخطيرة الأخرى للقوانين والأعراف السارية أثناء النزاعات المسلحة غير الدولية(المادة8/ف2/هـ) من نظام روما والتي اشتملت على (15) جريمة من جرائم الحرب التي يمكن أن ترتكب أثناء النزاعات المسلحة غير الدولية.

وبتحليل فقرات المادة 8 من نظام روما الأساسي يتبين أن القانون الدولي الإنساني يحظر استهداف المدنيين أو الأعيان أو الممتلكات المدنية أو المنشآت الخطرة أثناء النزاعات المسلحة الدولية وغير الدولية. ويقع على عاتق أطراف النزاعات المسلحة واجب التمييز فيما بين الأشخاص الذين يشاركون في الأعمال العدائية والسكان المدنيين، وكذلك التمييز بين الأهداف العسكرية والأعيان المدنية وعليه يجب أن توجه الهجمات ضد الأهداف العسكرية دون المدنية وإلا عدّ ذلك جريمة من جرائم الحرب الواقعة ضد الأشخاص أو ضد الأعيان المدنية[49].

أولاً: جرائم الحرب ضد الأشخاص.

وهي الانتهاكات الجسيمة لاتفاقيات جنيف الأربع لعام 1949 وبروتوكولاتها اللاحقة لعام 1977 وللقوانين والأعراف السارية أثناء النزاعات المسلحة الدولية وغير الدولية[50]. تضمن المادة(50) من اتفاقية جنيف الأولى، المادة(51) من اتفاقية جنيف الثانية، المادة(130) من اتفاقية جنيف الثالثة، والمادة(147) من اتفاقية جنيف الرابعة تسع صور من صور جرائم الحرب ومن بينها القتل العمد للأشخاص المحميين بموجب تلك الاتفاقيات أثناء النزاعات المسلحة الدولية وهم[51]:

المرضى، الجرحى، الغرقى من أفراد القوات المسلحة البرية والبحرية وفقاً لجنيف الأولى والثانية.

أسرى الحرب وفقاً لجنيف الثالثة.

السكان المدنيين وفقاً لجنيف الرابعة.

وعليه، فإن تعمد توجيه هجمات عشوائية ضد البنى التحتية التي يتواجد فيها الفئات المذكورة بما يؤدي إلى وفاتهم يعد جريمة حرب وفقاً للمادة(8/ف2/أ) من نظام روما الأساسي[52].

كما حظرت المادة(3) المشتركة لاتفاقيات جنيف في النزاعات المسلحة الدولية على الأطراف المشاركة استهداف الأشخاص غير المنخرطين في الأعمال الحربية بمن فيهم أفراد القوات المسلحة الذين ألقوا سلاحهم أو الذين أضحوا غير قادرين على القتال بسبب مرضهم أو عجزهم أو إصابتهم او احتجازهم[53].

وعليه إن استهداف الفئات المذكورة والمحمية بموجب المادة (3) بهجمات عسكرية سيعد جريمة حرب وفقاً للمادة (8/ف2/ج) من نظام روما[54].

[49]– عبد علي محمد سوادي، المسؤولية الدولية عن انتهاك قواعد القانون الدولي الإنساني. المركز العربي للنشر والتوزيع، مصر: القاهرة، الطبعة الأولى، 2017، ص74.

[50]- المرجع السابق، ص142.

[51]- اتفاقيات جنيف الأربع لعام 1949: اتفاقية جنيف الأولى لتحسين حال الجرحى والمرضى بالقوات المسلحة في الميدان المادة 50، اتفاقية جنيف الثانية لتحسين حال جرحى ومرضى وغرقى القوات المسلحة في البحار المادة51، اتفاقية جنيف الثالثة بشأن معاملة أسرى الحرب المادة130، اتفاقية جنيف الرابعة بشأن حماية الأشخاص المدنيين وقت الحرب المادة 147.

[52]- نظام روما الأساسي للمحكمة الجنائية الدولية لعام 1998، المادة 8/الفقرة 2/أ

[53]- اتفاقيات جنيف الأربع لحماية المدنيين لعام1949، المادة الثالثة المشتركة.

أما بالنسبة للبروتوكول الأول والملحق باتفاقيات جنيف والمعني بحماية ضحايا النزاعات المسلحة الدولية، فقد نصت المادة(51) منه على أن: يتمتع السكان المدنيين والأشخاص المدنيين بحماية عامة ضد الأخطار الناجمة عن العمليات العسكرية ولا يجوز أن يكون السكان المدنيين بصفتهم هذه محلاً للهجوم طالما أنهم لم يقوموا بدور مباشر في الأعمال العدائية[55]. وبناءً عليه، فإن القيام بشن هجوم عسكري مع العلم أن من شأنه أن يسفر عن خسائر في الأرواح وإلحاق إصابات بين المدنيين إخلالً بمبدأ التناسب بين الضرورة العسكرية لهذا الهجوم والأضرار والخسائر التي قد تنجم عنه سيشكل جريمة حرب وفقاً للمادة (8/ف2/ب 1-24) من نظام روما[56]. كما نجد المادة(70) من البروتوكول ذاته نصت على أن: يتمتع بالحماية أفراد إرساليات الغوث ذات الصبغة المدنية المحايدة والتي تعمل وفقاً لميثاق الأمم المتحدة على تقديم المساعدات الإنسانية لسكان أخد أطراف النزاع[57]. وعليه، سيكون استهداف الموظفين المستخدمين في مهمة المساعدة الإنسانية أو حفظ السلام والمشمولين بالحماية التي توفر للمدنيين بموجب القانون الدولي الإنساني يشكل جريمة حرب وفقاً للمادة(8/ف2/ب 3/هـ3) من نظام روما[58]. إضافةً إلى استهداف أفراد طاقم الخدمات الطبية والأفراد المستعملين للشارات المميزة والمثبتة في اتفاقيات جنيف يعد جريمة حرب وفقاً للمادة (8/ف2/ب/4،2/هـ/2) من نظام روما[59].

وبتحليل نصوص المواد السابقة ومراجعة تلك الصور في سياق العمليات السيبرانية العدائية يتبين أن تعمد شن وتوجيه هجمات سيبرانية عدائية على نحو مخالف لما هو منصوص عليه في المواد السابقة والواردة في الاتفاقيات والمواثيق الدولية القائمة سيعد جريمة حرب تستوجب المسؤولية الدولية الجنائية وتدخل في الاختصاص الموضوعي للمحكمة الجنائية الدولية. كما هو الحال فيما لو تم شن عمليات سيبرانية عدائية لتستهدف النظام الملاحي الإلكتروني لطائرات الإنقاذ التي تنقل غرقى أو جرحى الحرب بما يتسبب بحادث يترتب عليه وفيات وإصابات[60].

ثانياً: جرائم الحرب ضد الأعيان المدنية.

من أهم الأعيان المدنية المتمتعة بالحماية وفقاً لاتفاقيات جنيف وبروتوكولاتها اللاحقة المستشفيات (المدنية والعسكرية) وما تحتويه من أدوات وأجهزة، المنشآت ذات الخطورة العالية كالسدود والجسور ومحطات توليد الطاقة الكهربائية، والأعيان الثقافية كالمدارس والمساجد والكنائس وفقاً لما جاء في اتفاقية لاهاي الخاصة بحماية الممتلكات الثقافية في النزاعات المسلحة[61]. وإن استهدافها وتدميرها يعد خرقاً للمواد (46) من اتفاقية جنيف الأولى، والمواد (18-21-22)

[54]- نظام روما الأساسي للمحكمة الجنائية الدولية لعام 1998، المادة 8/الفقرة2/ج.

[55]- البروتوكول الإضافي الملحق باتفاقيات جنيف والمعني بحماية ضحايا النزاعات المسلحة الدولية لعام 1977، المادة51.

[56]- نظام روما الأساسي، المادة8/ الفقرة2/ ب 1-24.

[57]- البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لعام1977، المادة 70.

[58]- نظام روما الأساسي، المادة8/ الفقرة2/ ب3/هـ3.

[59]- نظام روما الأساس، المادة 8، الفقرة2/ ب4،2/ هـ2.

[60]- سارة بنت علي بن ناصر العنبورية، المسؤولية الدولية الجنائية عن الهجمات السيبرانية أثناء النزاعات المسلحة. رسالة ماجستير مقدمة استكمالا لنيل درجة الماجستير في القانون، قسم القانون العام، كلية الحقوق، جامعة السلطان قابوس، سلطنة عمان، 2023، ص130-131-132.

[61]- اتفاقية لاهاي الخاصة بحماية الممتلكات الثقافية في النزاعات المسلحة لعام 1954، المادة2.

من جنيف الرابعة[62]. وكذلك للمادة (23/ز) من اتفاقية لاهاي الخاصة باحترام قوانين وأعراف الحرب البرية لعام 1907 والتي نصت على: حظر تدمير أموال العدو والاستيلاء عليها ما لم يبرر ذلك مقتضيات ضرورة الحرب[63]. أما المادة(52) من البروتوكول الأول 1977 فنصت على: ضرورة حماية الأعيان المدنية وقصر توجيه الهجمات ضد الأهداف العسكرية والتي تستخدم بشكل فعال في العمليات العدائية والتي يحقق تدميرها كلياً أو جزئياً او الاستيلاء عليها أو تعطيلها ميزة عسكرية أكيدة[64]. بينما نصت المادة(53) من البروتوكول: يتمتع بالحماية الأعيان الثقافية وأماكن العبادة والتي تشكل التراث الثقافي أو الروحي للشعوب ويحظر شن هجمات عشوائية ضد هذه الأعيان او استخدامها في دعم العمليات العدائية او اتخاذها محلاً لهجمات الردع[65]. وإلا كان ذلك جريمة من جرائم الحرب التي تدخل في اختصاص المحكمة الجنائية الدولية وفقاً للمادة (8/ف2/ب9) من نظام روما[66]. أما المادة (54) من البروتوكول فقد نصت على حماية الأعيان والمواد التي لا غنى عنها لبقاء السكان المدنيين على قيد الحياة كالمواد الغذائية والطبية والزراعية[67]. وعليه استهداف هذه المواد يعد جريمة من جرائم الحرب الداخلة في اختصاص المحكمة الجنائية الدولية وفقاً للمادة(8/ف2/ب/25) من نظام روما[68]. في حين حظرت المادة(55)من البروتوكول توجيه هجمات عشوائية قد يسفر عنها أضراراً مادية أو ضرراً شديد الأثر واسع النطاق وطويل الأجل بالبيئة الطبيعية بحيث يكون إفراطه ملاحظاً بالمقارنة مع إجمالي المبررات العسكرية المتوقعة والملموسة والمباشرة[69]. والمخالفة ستعد صورة من صور جرائم الحرب وفقاً لنص المادة(8/ف2/ب/4/1) من نظام روما[70]. وأخيراً المادة(56) من البروتوكول نصت على أن: تتمتع بالحماية الأشغال الهندسية والمنشآت المحتوية على قوى خطرة كالسدود والجسور والمحطات النووية ومحطات توليد الطاقة الكهربائية ويحظر توجيه هجمات عشوائية ضدها حتى ولو كانت أهدافاً عسكرية لشدة خطورتها[71] وإلا سيعد ذلك جريمة حرب وفقاً للمادة (8/ف2/أ) من نظام روما[72].

وبتحليل نصوص المواد السابقة يتبين أن توجيه عمليات سيبرانية عدائية ضد الأعيان والمنشآت والممتلكات المدنية على نحو مخالف لما ورد في المواثيق والاتفاقيات الدولية المرعية سيصنف كجرائم حرب تدخل في الولاية القضائية للمحكمة الجنائية الدولية[73]. **ويرأينا**، أنه ليس هناك ما يمنع من تصنيف العمليات السيبرانية العدائية كجرائم حرب شأنها شأن غيرها من الجرائم الناجمة عن الهجمات التقليدية المحظورة وذلك لخصوصيتها وصعوبة حصر نطاقها وآثارها على الأهداف العسكرية دون الأعيان المدنية، ولا سيما عندما ترتكب في إطار خطة ممنهجة او سياسة عامة

[62]- اتفاقيات جنيف الأربع، جنيف الأولى المادة 46، وجنيف الرابعة المواد 18-21-22.

[63]- اتفاقية لاهاي الخاصة باحترام قوانين وأعراف الحرب البرية لعام 1907، المادة 23/ز.

[64]- البروتوكول الإضافي الأول لعام 1977، المادة 52.

[65]- البروتوكول الإضافي الأول لعام 1977، المادة 53.

[66]- نظام روما الأساسي، المادة 8/ الفقرة 2/ ب9.

[67]- البروتوكول الإضافي الأول لعام 1977، المادة 54.

[68] - نظام روما الأساسي،المادة8/ الفقرة2/ب5.

[69]- البروتوكول الإضافي الأول لعام 1977، المادة 55.

[70]- نظام روما الأساسي، المادة8/ الفقرة2/ب4،1.

[71]- البروتوكول الإضافي الأول لعام 1977، المادة56.

[72]- نظام روما الأساسي، المادة8/ الفقرة2/ أ.

[73]- سارة بنت علي بن ناصر العنبورية، المسؤولية الدولية الجنائية عن الهجمات السيبرانية، مرجع سابق، ص134-135-136.

او عملية واسعة النطاق وفقاً لما نصت عليه المادة(8) من نظام روما الأساسي. أضف إلى ذلك أن جرائم الحرب الناشئة عن العمليات السيبرانية والتي يمكن حدوثها أثناء النزاعات المسلحة المعاصرة الدولية وغير الدولية هي تلك المرتبطة بانتهاك مبدأي التمييز والتناسب في شن وتوجيه تلك العمليات، حيث يثبت الواقع الدولي الراهن أن تنفيذ هجمات سيبرانية دقيقة التمييز والتناسب لتفادي إصابة المدنيين أو تدمير الممتلكات المدنية قد ينطوي على الكثير من التحديات التقنية بسبب الترابط الذي يميز الفضاء السيبراني.

الفرع الثاني: تصدي المحكمة الجنائية الدولية لجرائم الحرب السيبرانية.

لا تمارس المحكمة الجنائية الدولية ولايتها القضائية في نظر الدعاوى الناشئة عن بعض الجرائم الدولية من تلقاء نفسها بل يثور اختصاصها بناءً على توافر ما حدده نظام روما الأساسي من شروط مسبقة وحالات واجراءات معينة.

أولاً: شروط ممارسة المحكمة الجنائية الدولية اختصاصها بشأن جرائم الحرب السيبرانية.

يعد اختصاص المحكمة الجنائية الدولية بشأن الجرائم الدولية اختصاصاً احتياطياً (تكميلياً) لاختصاص المحاكم القضائية الجنائية الوطنية، بمعنى أن الاختصاص الأصيل بمحاسبة القائمين على جرائم الحرب مثلاً ينعقد للمحاكم الوطنية المختصة وفي حال فشلها، عدم رغبتها أو عدم قدرتها يثور اختصاص المحكمة الجنائية الدولية[74]. ومع ذلك لا بد من وجود شروط مسبقة لتمارس المحكمة الجنائية الدولية اختصاصها بشأن الجرائم المنصوص عليها في المادة (5) من نظام روما الأساسي والتي من بينها جرائم الحرب الناشئة عن العمليات السيبرانية العدائية أثناء النزاعات المسلحة المعاصرة. فنصت المادة(12) من نظام روما على شروط انعقاد اختصاص المحكمة على النحو التالي:

1- ارتكاب جريمة الحرب السيبرانية من قبل مواطني دولة طرف: إن انضمام دولة ما إلى النظام الأساسي للمحكمة يعد قبولاً منها لممارسة المحكمة ولايتها القضائية بشأن الجرائم الدولية الداخلة في اختصاصها وفقاً للمادة(12/ف1) من نظام روما[75]. وفي السياق السيبراني فإن جرائم الحرب التي ترتكبها الدولة باستخدام العمليات السيبرانية كتعمد استهداف المدنيين أو الأعيان أو المنشآت المدنية المحمية بعد أن أصبحت طرفاً في نظام روما تدخل في اختصاص المحكمة، بينما يخرج من اختصاصها جرائم الحرب السيبرانية التي تم ارتكابها قبل انضمام الدولة لنظام روما[76].

2- ارتكاب جريمة الحرب السيبرانية على إقليم دولة طرف: لتمارس المحكمة اختصاصها بشأن جرائم الحرب التي ترتكب على إقليم دولة طرف في نظام روما، أو على ظهر السفينة أو متن الطائرة التي تحمل جنسية دولة طرف وفقاً للمادة(12/ف2) من نظام روما[77]. فإذا تعرضت دولة طرف لهجوم سيبراني ضد أحد طائراتها المدنية التي تنقل سكان مدنيين خلال نزاع مسلح دولي لتعطيل نظام الملاحة الجوية بما يؤدي إلى حدوث اصطدام نجم عنه وفيات أو إصابات فإنه يجوز للمحكمة الجنائية الدولية أن تمارس اختصاصها بشأن هذه الواقعة بوصفها جريمة حرب حتى ولو لم تكن الدولة المهاجمة طرفاً في النظام الأساسي للمحكمة[78].

[74]- محمود شريف بسيوني، المحكمة الجنائية الدولية، نشأتها ونظامها الأساسي، مرجع سابق، ص20-21.

[75]- نظام روما الأساسي، المادة 12، الفقرة 1.

[76]- سارة بنت علي بن ناصر العنبورية، المسؤولية الدولية الجناءية عن الهجمات السيبرانية، مرجع سابق، ص107.

[77]- نظام روما الأساسي، المادة 12، الفقرة 2.

[78]- سارة بنت علي بن ناصر العنبورية، المسؤولية الدولية عن الهجمات السيبرانية، مرجع سابق، ص107.

3-قبول دولة غير طرف باختصاص المحكمة الجنائية الدولية: يمكن لدولة غير طرف في النظام الأساسي للمحكمة أن تقبل باختصاص المحكمة بموجب إعلان يودع لدى مسجل المحكمة ويكون قبولاً اختيارياً وفقاً للمادة(12/ف3) من نظام روما[79]. وإن قامت دولة غير طرف بشن هجوم سيبراني يشكل جريمة حرب ضد دولة غير طرف في نظام روما وقبلت الدولة الضحية غير الطرف باختصاص المحكمة بموجب المادة(3/12) من نظام روما ففي هذه الحالة ينعقد اختصاص المحكمة في جريمة الحرب السيبرانية[80].

ثانياً: أحوال ممارسة المحكمة الجنائية الدولية اختصاصها بشأن جرائم الحرب السيبرانية.

تمارس المحكمة الجنائية الدولية اختصاصها في النظر بجرائم الحرب الناشئة عن العمليات السيبرانية العدائية أثناء النزاعات المسلحة المعاصرة وفقاً للمادة(13) من نظام روما الأساسي في الحالات التالية:

1-الإحالة من أحد الدول الأطراف إلى المدعي العام للمحكمة: يحق لأي دولة طرف في النظام أن تحيل للمدعي العام أي حالة يبدو أنها تشكل جريمة أو أكثر من الجرائم الواقعة ضمن ولايتها وأن تطلب منه مباشرة اجراءات التحقيق فيها وفقاً للمادة(13/أ) من نظام روما[81]. وعليه إذا تبين وجود شبهة جريمة من جرائم الحرب بعمليات سيبرانية عدائية تم شنها من قبل دولة معادية فإنه يحق للدولة المتضررة إذا كانت طرفاً في نظام روما أن تحيل للمدعي العام هذه الشبهة مع كل ما يدعمها من مستندات ليباشر التحقيق فيها تمهيداً لعرضها أمام المحكمة[82].

2-الإحالة من مجلس الأمن الدولي إلى المدعي العام: يمكن لمجلس الأمن الدولي باعتباره المنوط بالحفاظ على السلم والأمن الدوليين أن يتخذ اجراء الإحالة للمدعي العام في حال اضطلاعه بوقوع جريمة من الجرائم التي تدخل في اختصاص المحكمة وفقاً للمادة(12/ب) من نظام روما. ويتطلب قرار الإحالة من مجلس الأمن موافقة (9) أعضاء على الأقل من أصل (15) عضواً من بينهم أصوات الدول الخمس دائمي العضوية في المجلس[83].

3-مباشرة المدعي العام التحقيق بنفسه: للمدعي العام أن يباشر التحقيق من تلقاء نفسه في أي جريمة من جرائم الحرب السيبرانية التي تدخل في اختصاص المحكمة[84] وذلك بناء على المعلومات والمستندات والوثائق التي يمكن أن تصل إليه من أي مصدر، بعد أن يقوم بدراستها وتحليل مدى جديتها وفقاً للمادة(13/ج) من نظام روما[85].

حاول مؤسسو المحكمة الجنائية الدولية أن يكون إطار العدالة الجنائية الدولية مرناً وقابلاً للتكيف مع ما قد يطرأ من تطورات مستقبلية وما يستحدث من تقنيات تكنولوجية عسكرية لأنها يمكن أن تؤدي إلى أضرار ومعاناة مماثلة لما سعى مؤسسو المحكمة إلى منعه[86]. ومع ذلك **ويرأينا** يبقى إدخال العمليات السيبرانية العدائية في إطار العدالة الجنائية الدولية ومحاسبة منفذيها لا يخلو من التحديات وبحاجة ملحة إلى معالجة فعالة ضمن أطر القانون الدولي المختلفة.

[79]- نظام روما الأساسي، المادة 12، الفقرة 3.

[80]- سارة بنت علي بن ناصر العنبورية، المسؤولية الدولية الجنائية عن الهجمات السيبرانية، مرجع سابق، ص108.

[81]- نظام روما الأساسي، المادة 13، الفقرة أ.

[82]- سارة بنت علي بن ناصر العنبورية، المسؤولية الدولية الجنائية عن الهجمات السيبرانية، مرجع سابق، ص109-110.

[83] -نظام روما الأساسي، المادة 13، ب.

[84]- سارة بنت علي بن ناصر العنبورية، المسؤولية الدولية الجنائية عن الهجمات السيبرانية، مرجع سابق، ص111.

[85] - نظام روما الأساسي، المادة 13، ج.

[86]- كارولينا بويزمان، الهجمات السيبرانية بموجب القانون الدولي الجنائي، مرجع سابق، ص2.

في ختام البحث تم التوصل إلى مجموعة من الاستنتاجات والتوصيات الآتية:

الاستنتاجات و التوصيات:

أولاً- الاستنتاجات:

1-تثير الخصائص التقنية المميزة للعمليات السيبرانية الكثير من الصعوبات القانونية فيما يتعلق بتطبيق قواعد القانون الدولي التقليدية ذات الصلة بالمسؤولية الدولية عليها وذلك لاختلاف هذه العمليات عن الأشكال التقليدية الأخرى لاستخدام القوة أو وسائل وأساليب الحرب المستخدمة في العمليات العدائية على النحو المنصوص عليه في المواثيق والاتفاقيات الدولية الحالية وأحكام القانون الدولي العرفي.

2-إن المسؤولية الدولية عن العمليات السيبرانية العدائية في إطار القواعد التقليدية للقانون الدولي العام قد لا تحقق أهدافها نظراً للتحديات التي قد تحول دون وضعها موضع تطبيق فعلي وما يترتب على ذلك من تبعات الملاحقة القضائية وإكمال اجراءات المتابعة وفقاً لأطر التحقيق والمساءلة الدولية.

3-إن إرساء المسؤولية الدولية الجنائية بموجب القانون الدولي الجنائي يتطلب إعادة تقييم القواعد القانونية القائمة ووضع معايير جديدة تتلاءم مع خصوصية العمليات السيبرانية لضمان التطبيق الفعال لقوانين وأطر التحقيق والمساءلة الدولية ولمنع الدول من استغلال الفضاء السيبراني لارتكاب عمليات سيبرانية ضارة ترقى لمستوى الجرائم الدولية.

4-ليس هناك ما يمنع من تصنيف العمليات السيبرانية العدائية كجرائم حرب أو جرائم ضد الإنسانية أو جرائم العدوان شأنها شأن غيرها من الجرائم الناجمة عن الهجمات التقليدية المحظورة والمرتكبة بوسائل أخرى غير سيبرانية، وذلك لصعوبة حصر نطاقها وآثارها على الأهداف العسكرية فقط دون الأعيان المدنية لا سيما عندما ترتكب في إطار خطة ممنهجة أو سياسة عامة أو عملية واسعة النطاق.

5-إن جرائم الحرب الناشئة عن العمليات السيبرانية والتي يمكن حدوثها أثناء النزاعات المسلحة المعاصرة هي تلك المرتبطة بانتهاك مبدأي التمييز والتناسب في توجيهها حيث يثبت الواقع الدولي الراهن أن تنفيذ هجمات سيبرانية دقيقة التمييز والتناسب لتفادي إصابة المدنيين أو تدمير الممتلكات المدنية ينطوي على الكثير من التحديات التقنية بسبب الترابط الذي يميز الفضاء السيبراني.

6-في ضوء عدم وجود وثيقة قانونية دولية تنص على التزامات محددة للدول في المجال السيبراني فلا يمكن إلا الاعتماد على المبادئ العامة للقانون الدولي العام وممارسات الدول والسوابق القضائية الدولية لمنع التذرع بإشكالية الفراغ القانوني وضمان محاسبة الأفراد المسؤولين عن انتهاكات القانون الدولي الإنساني.

7-إن عدم وجود محاكم دولية أو جنائية متخصصة بملاحقة المسؤولين عن ارتكاب العمليات السيبرانية الخطرة على المستوى العالمي يعني أن عدداً غير قليل من منفذيها سيكون بمنأى عن المسؤولية والعقاب.

ثانيا- التوصيات:

1-ضرورة إبرام اتفاقية دولية جماعية تصادق عليها الدول تحت مظلة الأمم المتحدة لسد القصور التشريعي الحاصل حول تحديد المسؤولية الدولية الناشئة عن العمليات السيبرانية ولتأكيد أهمية الملاحقة الجنائية ضد مرتكبيها خصوصاً فيما يتعلق بحفظ السلم والأمن الدوليين.

2-معالجة التحديات التي ينطوي عليها التصدي للعمليات السيبرانية العدائية في الإطار القانوني الدولي والمتعلقة بمسؤولية الدول المدنية والجنائية وإسنادها عن سلوك غير مسموح فيه أثناء النزاعات المسلحة المعاصرة.

3-اتخاذ اجراءات عاجلة وفعالة من قبل الدول لضمان حمايتها من العمليات السيبرانية من خلال توفير الاستثمار في الأمن السيبراني وحماية البيئة التحتية الرقمية التابعة لها وتدريب الكوادر الوطنية في مختلف المؤسسات على كيفية التعامل مع التهديدات السيبرانية ونشر الوعي في المجتمع من أجل الوصول إلى فضاء سيبراني آمن.

4-العمل على تزويد الجيوش الوطنية بتقنيات ومهارات التعامل مع التهديدات السيبرانية من خلال تدريب المهندسين المعلوماتيين للعاملين في القوات المسلحة بهدف اكتساب خبرات تؤهلهم إلى تولي مسؤوليات حماية البنية التحتية الوطنية الرقمية والأمن السيبراني للدولة.

5-ضرورة إعادة النظر في القواعد القانونية الدولية المنطبقة على المسؤولية الدولية وما يجب أن تكون عليه مستقبلاً لمواجهة العمليات السيبرانية العدائية والحفاظ على الأمن السيبراني العالمي الذي أصبح مصدر قلق على أمن الدول في الوقت الراهن.

6-إنشاء وكالة دولية متخصصة ومتعددة الأطراف تضم خبراء وفنيين وتقنيين في المجال السيبراني تعنى بالكشف عن العمليات السيبرانية وتقديم المساعدة التقنية للدول التي تتعرض لهذا النوع من العمليات وتقيم أن ما حدث من أضرار ودمار كان نتيجة لتعرضها لهجوم سيبراني، وتعالج قضايا الإسناد والمساءلة وتتولى اجراء التحقيقات عن العمليات السيبرانية المزعومة خاصة التي ترعاها الدول وتكون قادرة على إحالة القضايا إلى مجلس الأمن الدولي ثم للقضاء الدولي الجنائي.

References:

[1] A. A. M. Swady, International Responsibility for violating the rules of international humanitarian law, Egypt, Cairo, the Arab Center for Publishing and Distribution, (in Arabic), first edition, P:306, 2017.

[2] A. Al-Nnakeeb, Electronic warfare in the light of the seventy-seven protocols attached to the four-year-old Geneva Conventions(Cyber Attacks), Arab Center for Publishing and Distribution(in Arabic), first edition, p:394, 2022.

[3] C. Bouzman, Introduction entitled: Cyber attacks under International Criminal Law- challenges of Investigation and Judicial pursuit- In the Book Togs: The evidence for understanding the crime of cyber aggression: a study in the framework of an effective political legal confrontation, For the author: A. Al-Fatlawy, Q, Al-Gezzy, Zain Humanitarian Publications(in Arabic), first edition, Lebanon, Beirut, p: 15-23 from this book, 2025.

[4] M. Sh. Basyooni, The International Criminal Court has originated and its basic system with a study of the history of the investigation committees and former international criminal courts, The new Rose Al-Youssef press (in Arabic), The First edition, Egypt, Cairo, P: 296, 2001.

[5] M. Saady, The International responsibility of the state in the light of the international legislation and the Judiciary, Egyptian Publishing and Distribution (in Arabic), first edition, p: 208, 2019.

[6] M. H. Al-Sharkawy, Electronic attacks in light of the provisions of international humanitarian law, PhD thesis, Department of International law, Faculty of law, Beni Suef University, Egypt (in Arabic) 2022, P:420.

[7] S.A.N. Al-Anbouriah, International criminal responsibility for cyber operations during armed conflicts, Master thesis, Department of Public law, Faculty of law, Sultan Qaboos University, Sultanate of Oman (in Arabic) p: 153, 2023.
[8] A.O. Al-Fatlawy, Cyber attacks: its concept and arising international responsibility in the light of contemporary international organizations, Journal of the local investigator for legal and political sciences(in Arabic) No: 4, p: 611-687, 2016.
[9] E. Lawson, K. Macak, Avoiding civilians harm for military cyber operations during armed conflicts, ICRC, Expert Meeting, Geneva, 21-22 January, p:58, 2020.
[10] H.S. Al-Darmaki, W.A. Allam, International Responsibility for cyber attacks committed by Non-sate Entities, Sharjah University Journal of legal sciences, (in Arabic) Vol:21, No:4, p:468-492, 2024.
[11] ICRC, ICRC Position Paper: International Humanitarian law and cyber operations during armed conflicts, International Review of the Red Cross, Vol:102, No: 913, p:1-9, 2020.
[12] I.S.A. Ramadan, confronting cyber attacks in light of the provisions of international law, Journal of legal and economic sciences, (in Arabic) No: 1, p: 1744-1867, 2025.
[13] L. Jesel, T. Rodnhouser, K. Dorman, International humanitarian law and the protection civilians on the effects of cyber operations during armed conflicts, International Journal of the Red Cross, Geneva, Vol:102, No: 913, p: 287-324, 2020.
[14] M.R.M. Al-S,aidi, M.S.M. Abd Allateef, A.R. Mohammad, The Impact of Artificial Intelligence and Cyber Warfare on the Human Environment during armed conflicts, Journal of Jurisprudence and legal research (in Arabic) No: 47, p: 3837-3926, 2024.
[15] N.M.O. Al-Shazely, The legal aspects of the cyber war, A study within the framework of international humanitarian law, Spirit of laws Journal (in Arabic) No:103, Part: 2, P: 1229-1286, 2023.
[16] T.Y. Al-Eissa, O.M. Innab, International responsibility for cyber attacks in light of the contemporary international law, Zarqaa Journal for research and studies in humanities, (in Arabic), Vol:19, No:1, p:81-95,2019.
[17] The international group of experts at the invitation of the NATO Cooperative Cyber Defense Center of Excellence Tallinn Manual on the international law applicable to the cyber warfare, Cambridge University Press, Cambridge, 215, 2013-2017.
[18] The Hague Convention on respecting the laws and customs of the war war 1899-1907.
[19] The Statute of the International Courts of Justice 1945.
[20] The Four Geneva Conventions of 1949.
[21]The Hague Conventions of the protection of cultural property in armed conflicts 1954.
[22]The First additional protocol attached to the four Geneva Conventions to protect the victims of international armed conflicts 1977.
[23] Rome basic system for the international criminal courts 1998.
[24] Project of articles related to the responsibility of countries for unlawful acts internationally 2001.