المسؤولية الدولية الناتجة عن الجرائم السبرانية

International responsibility for cybercrimes

م.م. يوسف زبن خضير
كلية الطب –جامعة الفلوجة
Youssef.zabin@uofallujah.edu.iq

م.م. صباح عواد سلمان
كلية القانون –جامعة المعارف
sabah.awad@uoa.edu.iq

تاريخ استلام البحث ٢٠٢٤/٦/٢٠ تاريخ قبول النشر ٢٠٢٤/١٠/١٥

المستخلص

إن الجريمة الدولية هي جريمة قائمة بذاتها، تختلف عن الجرائم التقليدية، وتتميز تلك الجريمة بأنها قد أخذت عدة أنواع منها، الجرائم السيبرانية وهي التي تتم في الفضاء الخارجي بواسطة تقنيات تكنولوجية حديثة، فهي تختلف عن الحروب التقليدية، ولقد سعى الفقه الدولي إلى إقرار المسؤولية الدولية عن الجرائم السيبرانية، كما وضع المجتمع الدولي عدة مواثيق دولية لمواجهة تلك الجرائم.

الكلمات المفتاحية: مسؤولية دولية، الجرائم السيبرانية، الفضاء الخارجي، دليل تالين، أتفاقية بودابست.

Abstract

International crime is a crime in itself, different from traditional crimes, and this crime is distinguished by the fact that it has taken several types, including cybercrime, which were carried out in foreign courts using modern technological techniques, and they differ from traditional wars and international jurisprudence has sought to establish international responsibility for cybercrimes as well as international community has establish several international covenants to confront these crimes

Keyword: International responsibility, cybercrimes, extraterritorial jurisdiction, Tallinn manual, Budapest convention

المقدمة

إن الجريمة السيبرانية تعد من نتاج التقدم السريع الذي حدث مؤخرًا في تكنولوجيا المعلومات، إذ أنها تعد من أهم وأخطر الصعوبات والتحديات الأمنية التي تواجه كافة المجتمعات العالمية في الوقت الحالي، وخاصة في مجالات تقنية الإتصالات والمعلومات.

وفى ضوء هذا التقدم السريع في مجال العلوم والتقنية واستخداماتها في خدمة البشرية، فقد حدث تطور في مجال الجريمة السيبرانية، حيث أنه لم تعد الجريمة مقتصرة على طبقة معينة من طبقات المجتمع بل اتسعت لتشمل جميع الطبقات، وأخذت عدة صور منها تلك الجرائم التي يكون محلها الحاسب الآلي وكذلك الجرائم التي تستهدف نظم تقنية الإتصالات والمعلومات، والجرائم التي يعتبر جهاز الحاسب الآلي وسيلة تنفذ به جرائم الاحتيال المعلوماتي وكذلك سرقة الهويات والتعدي على بطاقات

الائتمان والأرصدة البنكية و جرائم التزوير وجرائم الاختلاس، وكذلك سرقة حقوق الملكية الفكرية والتعدي والإستغلال الجسدي للأطفال، وكذلك نشر الأفكار الإرهابية المتطرفة.

مما تطلب من المجتمع الدولي التصدى لتلك الظاهرة الإجرامية حديثة النشأة، فقام المجتمع الدولي بوضع العديد من الأراق التي تتضمن توصيات للدول بمواجهة تلك الجرائم، فالجرائم السيبرانية قد مست بأمن وسلامة الأفراد المنشأت الهامة داخل الدولة، وحتى أن البعض وصفها بانها حرب من نوع جديد، فالهجمات السيبرانية كان لها أضرار تتمثل مع أضرار الحروب التقليدية.

إشكالية البحث: تدور إشكالية البحث حول مدى إمكانية قيام المسؤولية الدولية عن الجرائم السيبرانية، فهناك العديد من الدول قد تعرضت في الأونه الأخير لهجمات سيبرانية، قامت بها دول أخرى بهدف التعدي وتعطيل الأنظمة العسكرية والإقتصادية للدولة المعتدى عليها، واللجوء لقواعد القوانين الداخلية قد لا يجدي في هذه الحالة لوجود فراغ تشريعي في العديد من الدول، مما يستوجب البحث عن المسؤولية الدولية للدولة المعتدية من حيث ماهية تلك الجرائم، وتكييفها، أركانها ومكافحتها.

تساؤلات الدراسة: سيقوم الباحث من خلال الدراسة بالأجابة على التساؤلات الأتية:

- ما المقصود بالجرائم السيبرانية؟
- ما هو التكييف القانوني للجرائم السيبرانية؟
- ما هي أركان وأساس قيام المسؤولية الدولية عن الجرائم السيبرانية؟
- ما هو دور القانون الدولي في مكافحة الجرائم السيبرانية؟

أهداف الدراسة: تهدف الدراسة إلى الوقوف على عدة نقاط:

- الوقف على ما هية الجرائم السيبرانية.
- التعرف على التكييف القانوني للجرائم السيبرانية.
- الوقوف على أركان وأساس المسؤولية الدولية عن الجرائم السيبرانية.
- التعرف على الإتجاهات الدولية في مكافحة الجرائم السيبرانية.

خطة البحث

- المبحث الأول: التعريف بالجرائم السيبرانية
- المبحث الثاني: خصوصية المسؤولية الدولية الناتجة عن الجرائم السيبرانية

المبحث الأول: التعريف بالجرائم السيبرانية

تعد الجريمة السيبرانية ظاهرة إجرامية حديثة النشأة، حيث أن ظهورها قد أرتبط بالتكنولوجيا الحديثة، ونتج عن حداثتها أن أحيط بها الكثير من الغموض، ومن ثم فقد أصبحت تقنية المعلومات من أساسيات الحياة في العصر الحالي، إلا أنها على الرغم من ذلك فهي تستغل في أغراض غير مشروعة، ولذلك فقد أصبح الحاسب الآلي بشكل عام وشبكة الإنترنت بشكل خاص محلا لارتكاب الجريمة بمفهومها الحديث، ونتيجة لذلك فقد احترف بعض الجناة ارتكاب العديد من الجرائم بواسطة الحاسب الآلي وشبكة الإنترنت.

وفى ضوء ذلك تتميز هذه الجريمة بأن ليس لها حدود جغرافية، مما يكسبها طابعًا دوليًا، ونتيجة للتقدم المذهل في وسائل الاتصالات والمواصلات فقد أصبحت تلك الظاهرة من الإجرام تؤرق العديد من الدول، وذلك لآثارها الخطيرة على مكانة تلك الدول، وتعد من المواضيع الحديثة والخطيرة التي تشغل اهتمامات رجال القانون والفقهاء.

وتتم الجريمة السيبرانية في الفضاء الخارجي بواسطة الوسائل الإلكترونية، وقد أثيرت العديد من التساؤلات حول تحديد الطبيعة القانونية للجريمة الإلكترونية، ويرجع سبب ذلك إلى أختلاف الرؤية لهذه الطائفة من الجرائم، حيث ظهرت عدة آراء فقهية لفهم المقصود بالجريمة الإلكترونية، وتحديد تعريف لها مع بيان طبيعتها القانونية. هذا ما سأنتناوله في هذا المبحث في مطلبين على النحو التالي: المطلب الأول وأتناول فيه ماهية الجرائم السيبرانية، والمطلب الثاني أتناول التكييف القانوني للجرائم السيبرانية.

المطلب الأول: ماهية الجرائم السيبرانية

أن تعريف الجريمة السيبرانية يستوجب الإلمام بالجانب الموضوعي والإجرائي لها، مع دراسة العوامل المختلفة التي تتداخل في تكوين الجريمة، والإحاطة بالأمور الفنية لها عن طريق بيان خصائصها.

الفرع الأول: مفهوم الجرائم السيبرانية

أختلف لفقهاء في وضع مفهوم شامل للجريمة السيبرانية، ويرجع ذلك لعدم تنظيمها تشريعيًا في مختلف دول العالم وحداثة نشأتها مقارنة بغيرها من الجرائم؛ ونتيجة لغياب التعريف القانوني لمثل هذا النوع من الإجرام المستحدث في غالبية النظم القانونية، بالإضافة إلى عدم وجود مصطلح قانوني موحد للتعريف بماهية الجرائم السيبرانية.

أن الفقه قد انقسم بدوره إلى اتجاهين رئيسيين، ومن ناحية المنطلقات التي ينظر بها لذلك النوع من الجرائم، حيث أن الاتجاه الأول يضيق مفهوم الجريمة السيبرانية، أما الاتجاه الثاني فقد حاول التوسع في تعريف الجريمة السيبرانية.

أولاً: التعريف الضيق للجريمة السيبرانية: ذهب هذا الإتجاه إلى حصر الجرائم السيبرانية في الأحوال التي تحتاج قدرًا كبيرًا من المعرفة بشؤون تقنية تكنولوجية المعلومات الحديثة، فالجرائم التي لا تصل لهذه الدرجة من المعرفة تعتبر جرائم تقليدية عادية تعكف على دراستها نصوص القوانين العقابية التقليدية.

فقد عرفها جانب من الفقه بأنها "الجرائم التي تلعب فيها بيانات الكمبيوتر والبرامج المعلوماتية دورًا هامًا، أو هي كل فعل إجرامي يستخدم الحاسب الآلي في ارتكابه كأداة رئيسية"[١].

كما عرفها جانب أخر بأنها " كل سلوك غير مشروع، أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات، أو نقل هذه البيانات" [٢].

كما قال عنها أخر بأنها " تلك الجرائم التي يكون قد حدث في مراحل ارتكابها بعض العمليات الفعلية داخل الحاسوب" [٣].

ومن الفقه الأجنبي ذهب أحد الفقهاء إلى أن الجريمة السيبرانية تتمثل في الفعل غير المشروع الذي يتدخل في إرتكابه الحاسب الآلي [٤].

ما يؤخذ على التعريفات السابقة أنها قاصرة عن الإلمام بأوجه الجرايمة السيبرانية، فأنصار هذا الاتجاه قد صبوا تركيزهم على موضوع الجريمة فقط، كما أن منهم من ركز على طريقة أرتكابها، ولكن لم يوجد تعريف تناول الظاهرة من مختلف الجوانب.

ثانيًا: التعريف الواسع للجريمة السيبرانية: ذهب جانب إلى تعريف الجريمة السيبرانية بأنها " كل عمل أو إمتناع عن عمل يأتيه الإنسان إضرارًا بمكونات جهاز الحاسب الآلي سواء كانت مادية أو معنوية أو شبكة الإتصال الخاصة بهذا الجهاز، وذلك بإعتبارها من القيم والمصالح التي يحميها القانون " [٥].

تناول رأي آخر من الفقه تعريف الجريمة السيبرانية بأنها: "عمل أو امتناع يأتيه الإنسان إضرار بمكونات الحاسوب وشبكات الاتصال الخاصة به، التي يحميها قانون العقوبات ويفرض لها عقابًا"(٦).

كما عرفت الجريمة السيبرانية في إطار المنظمة الأوربية للتعاون والتنمية الاقتصادية بأنها: "كل فعل أو امتناع من شأنه أن يؤدي إلى الاعتداء على الأموال المادية أو المعنوية، يكون ناتجًا بطريقة مباشرة عن تدخل التقنية المعلوماتية الإلكترونية"[٧].

وجاء تعريف الجريمة السيبرانية في توصيات منظمة مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقدة في فيينا سنة ٢٠٠٠م بأنها: "يقصد بالجريمة الإلكترونية أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي، أو شبكة حاسوبية، أو داخل نظام حاسوبي، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية"[٨].

كما عرفها أخر بأنه كل فعل إجرامي يتم في محيط جهاز الحاسب الآلي [٩].

وفي النهاية نقول: أن هذا الاتجاه قد توسع كثيرًا في مفهوم الجريمة السيبرانية، كما يؤخذ على هذا التوسع أن من شأنه أن يطلق وصف الجريمة السيبرانية على أفعال قد لا تدخل في طائفة الجرائم السيبرانية وذلك لمجرد أستخدام الحاسوب الآلي في النشاط الإجرامي، فبعض الجرائم كسرقة الحاسوب الآلي، أو الأقراص مثلًا، فلا يمكن إعطاؤها وصف الجريمة السيبرانية على سلوك الفاعل لمجرد أن الحاسوب، أو أحد مكوناته المادية كانت محلًا لفعل الاختلاس.

الفرع الثاني: خصائص الجرائم السيبرانية

نتج عن أرتباط الجريمة السيبرانية بجهاز الحاسب الآلي وشبكة الإنترنت إلى إضفاء عدة خصائص لهذه الجريمة تفرقها عن الجريمة التقليدية.

أولاً: الجريمة السيبرانية جريمة عابرة للحدود: إن أول خاصية تتميز بها الجريمة السيبرانية، أنها جريمة تتعدى حدود الدولة الواحدة؛ وذلك لإتصالها بعالم الإنترنت وهو عالم لا يعرف الحدود الجغرافية للدول، وينتج عن ذلك أن هناك دول تتأثر بهذه الجريمة، بسبب سرعة التنفيذ، فيمكن أن تقع تلك الجريمة من طرف الجاني في مكان، والمجني عليه في مكان أخر.

في زمن الحاسب الآلي وخصوصًا مع كثرة أستخدام تكنولوجيا الإنترنت تم ربط أعداد كبيرة من الحواسيب في أماكن جغرافية مختلفة بهذه الشبكة، فقد أصبح الاتصال بين تلك الأجهزة سهلًا، فيمكن الوصل للمرسل إليه بمجرد معرفة عنوانه، وسواء تم ذلك الأتصال بطرق مباحة أو غير مباحة، ويمكن أن نطلق على جرائم المعلومات التقنية بأنها جرائم عابرة لحدود الدول؛ فغالبًا ما نجد المعتدي في بلد والمعتدى عليه في بلد آخر، كما قد يقع الضرر عن الجريمة في بلد ثالث، وعليه تعد الجرايمة السيبرانية من الجرائم العابرة للحدود الجغرافية للدولة الواحدة(١٠).

ثانيًا: الجريمة السيبرانية تتم في الفضاء الخارجي: أن محل الجريمة السيبرانية هو الفضاء السيبراني فهي تصرف واقعي يتم في عالم أفتراضي (١١)، هذا العالم قائم على إستخدام بيانات رقمية ووسائل أتصال إلكترونية، وذلك نتيجة القيام بإختراق موقع إلكتروني ذو حساسية عالية، عادة ما تقوم تلك المواقع بوظائف ذات أولوية مثل محطات الطاقة النووية أو المحطات الكهربائية أو المطارات أو وسائل النقل (١٢).

ثالثًا: صعوبة الاكتشاف والإثبات: نظرًا للطبيعة الخاصة التي تتميز بها الجريمة السيبرانية، فإن إثباتها يكتنفه الكثير من الصعوبات، تتمثل في صعوبة الكشف عنها، فهي لا تترك أثرًا في العالم الخارجي، فالجريمة السيبرانية لا تقوم على العنف، فلا أثر لإقتحام في السرقة المعلوماتية مثلًا، ولكنها أرقام وبيانات تمحى أو يتم تغيرها أو تزويرها من السجلات المخزنة، فلا أثر خارجي لها، فالجريمة السيبرانية تعد جريمة فنية، هادئة لا تقوم على العنف.

وبالرغم من تلك الخاصية إلا إن هناك بعض الفقهاء يعتبر الجريمة السيبرانية من جرائم العنف، مثل ما ذهب إليه مكتب التحقيقات الفدرالي بالولايات المتحدة الأمريكية؛ بدافع تشابه دوافع المتعدين على أنظمة الحاسوب الآلي مع دوافع مرتكب جرائم العنف (١٣).

المطلب الثاني: التكييف القانوني للجرائم السيبرانية

هناك أكثر من بليون شخص على مستوى العالم يستخدمون الإنترنت، بفعل الثورة التكنولوجية أصبحت الدول والمجتمعات غير الحكومية، والأعمال التجارية والأوساط الأكاديمية والأفراد مترابطة إلى حد لا يمكن تخيله من قبل وفي الوقت نفسه ازداد الاعتماد العسكري على أنظمة الحواسيب وشبكاتها زيادة هائلة. مما ألقي بظلاله على بيان طبيعة الجرائم السيبرانية، فهناك من نظر إليها على أنها جريمة من نوع جديد، وهناك من نظر إليها على أنها نوع جديد من الحروب، يمثل أمتداد للحروب التي تتم بإستخدام الأسلحة.

الفرع الأول: تكييف الجرائم السيبرانية كحرب دولية

أن الجريمة السيبرانية هي نوع جديد من أنواع الحروب، فلم تعد الجرائم السيبرانية قاصرة على نطاف العلاقات التجارية، فقد تم توجيه الهجمات السيبرانية في الأونة الأخيرة على الدول بحد ذاتها.

فلقد لعب الفضاء الالكتروني دورًا هامًا في الاستحواذ على عناصر الجريمة السيبرانية في العلاقات

بين الدول، فقد أضحى التقدم في مجال الإلكترونيات عاملاً حيويًا في القيام بعمليات ذات فعالية، وذلك من خلال القدرة على القتال في الفضاء الخارجي، وهذا الأمر يستدعي بالضرورة تغير في مفهوم القوة، فقد بات بالإمكان تعريفها بأنها مجموعة الطاقات والإمكانيات المادية وكذلك غير المادية التي تحوزها أحد الدولة وتستخدمها في عملية صنع القرار، والقيام بفعل مؤثر، بما ينتج عنه تحقيق مصالح الدولة، والتأثير في سلوك الوحدات السياسية في الوقت نفسه (١٤).

فقد انتقلت عناصر القوة من نظام الحروب الكلاسيكية التي كانت تعمتد على إحتلال أرض الخصم والإستيلاء ثرواته بعد القيام بتدمير، إلى نوع جديد من الحروب، قوامها الإستحواذ على التكنولوجيا وسرقة الأسرار والإبتكارات العلمية والتحكم بالمعلومات، وكذلك العمل على إختراق الأمن القومي للدولة بدون أسلحة، أو حتى القيام بالتعدى على الحدود، وبدون عمليات التجسس، فذلك النوع الجديد من القوة له آثار تفوق الحرب التقليدية.

ففي الحرب السيبرانية يكون مجال الحرب هو الفضاء الالكتروني فهو الساحة التي يتم فيها الصراع، ففي تلك الساحة يتم التأثير على النواحي الثقافية والإقتصادية والإجتماعية للدولة المعتدى عليها، وإن كان مجال ذلك النوع الجديد من الحروب ضيق فلا تتطور إلى القوة المسلحة، ومن الصور التي قد تأخذها تلك الحروب الاختراقات المتعمدة للأنظمة وكذلك عمليات التجسس وكذا سرقة المعلومات، كما يمتد نطاق الحروب السيبرانية إلى شن الحرب الفكرية (١٥).

وبناء على ما سبق فإن الحروب السيبرانية تثير مشكلة تخص القواعد المتعلقة بحق الالتجاء إلى ذلك النواع من الحروب، وبالتالي البحث في مشروعية هذه الحروب الجديدة أو عدم مشروعيتها، وفي ضوء ميثاق الأمم المتحدة، والمتعلق بواجب عدم استخدام القوة أو عدم التهديد بإستخدامها في العلاقات بين الدول.

الفرع الثاني: تكييف الجرائم السيبرانية كإجرام دولي

ذهب جانب من الفقة إلى أن الجريمة السيبرانية تدخل في نطاق الجرائم الدولية.

ذهب جانب من الفقة إلى أن الجريمة الدولية هي تتمثل في كل مخالفة للقواعد القانون الدولي تقع من أجل الإضرار بالأفراد أو حتى بالمجتمع الدولي كله، سواء كان يمنعها القانون الوطني أو يبيحها وقد ترتكب تلك الجريمى بفعل أو بامتناع من شخص يتمتع بحريته في الاختيار وذلك إضرار بالأفراد والمجتمع (١٦).

الجريمة الدولية "هي فعل غير مشروع في القانون الدولي، صادر من شخص ذي إرادة معتبرة قانونا ومتصل على نحو معين بالعلاقة بين دولتين أو أكثر وله عقوبة توقع من أجله"، من خلال هذا التعريف يتضح أن الجريمة الدولية لها أربعة أركان تقوم عليها تتمثل في الركن المادي والركن المعنوي والركن الشرعي والركن الدولي (١٧).

وقد عرفها الدكتور فتوح عبد الله الشاذلي بقوله هي سلوك إنساني غير مشروع، هذا السلوك صادر عن إرادة إجرامية يقوم به الفرد بإسم أحد الدول أو برضائها، ينطوي هذا السلوك على إنتهاك لمصلحة أحد الدول والتي يقرر لها القانون الدولي حماية جنائية (١٨).

في حين عرفها أحد الفقهاء بأنها سلوك إرادي يصدر عن فرد بأسم الدولة أو بتشجيعها أو برضاها غير مشروع ينطوي على المساس بمصلحة أحد الدول تكون محمية قانونًا [١٩].

فذهب هذا الجانب من الفقة إلى أن أهم ما تتميز به الجريمة الدولية هو الركن الرابع المتمثل في الركن الدولي، وهذا الركن هو خاصية تتميز به الجرائم السيبرانية، فهي بطبيعتها جريمة عابرة للحدود، فهي بذلك جريمة دولية.

ومن جانبنا فإننا نرى أن تكييف الجريمة السيبرانية بوصفها جريمة وليست حرب هو الأقرب للصواب، حيث ان الجريمة السيبرانية تدخل في نطاق الجرائم بالرغم من خطورتها، كما تنطبق عليها أوصاف الجريمة الدولية والتي تتميز بركنها الدولي، كون السلوك الإجرامي في دولة والنتيجة الإجرامية في دولة أخرى.

المبحث الثاني: خصوصية المسؤولية الدولية الناتجة عن الجرائم السيبرانية

إن المسؤولية الدولية الناتجة عن الجرائم السيبرانية تعد من أهم الموضوعات التي يتناولها القانون الدولي في الأونة الأخيرة، فبالنظر إلى التطورات الحديثة في مجال التكنولوجيا نجد أنها قد أثرت بشكل كبير على العلاقة بين الدول، فقد ظهرت عدة إشكاليات لم يتناولها القانون الدولي بالتنظيم؛ مما أستدعى معالجة وحل تلك الإشكاليات بطريقة تفق مع طبيعتها الخاصة، وعليه سيتم التطرق إلى موضوع خصوصية المسؤولية الدولية الناتجة عن الجرائم السيبرانية في مطلبين الأول لأركان وأساس المسؤولية الدولية عن الجرائم السيبرانية والثاني لبيان الإتجاهات الدولية في مكافحة الجرائم السيبرانية.

المطلب الأول: أركان وأساس المسؤولية الدولية عن الجرائم السيبرانية

في الأونة الأخيرة دخل العالم في مرحلة جديدة حيث أصبح العالم قرية صغيرة وظهر مصطلح القرية الكونية، ويرجع السبب في ذلك للتطور الكبير الذي حدث في عالم تكنولوجيا الاتصال، فقد استحدثت طرق جديدة للتعامل بين الدول، ولكن مع هذا التطور الهائل في التكنولوجيا ظهرت العديد من التهديدات الجديد داخل هذا الفضاء متمثلة في الجرائم السيبرانية بمختلف أنواعها من القرصنة، التجسس، السرقة، والإرهاب الإلكترونية، لكن المجتمع الدولي وضع العديد من الاستراتيجيات لمواجهتها، والتقليل من أضرار هذه الجرائم، والتي أستلزم الامر تحديد أركان وأساس المسؤولية الدولية عن تلك الجرائم.

الفرع الأول: أركان المسؤولية الدولية عن الجرائم السيبرانية

هناك تشابه بين النظام القانوني الدولي والنظام القانوني الداخلي، فالفرد هو محور شخص النظام القانوني الداخلي، وكذلك الحال النظام القانوني الدولي له أشخاصه والمتمثلون في الدول، حيث يفرض نظام القانوني الدولي على الدول عدة التزامات، كما يرتب للدول عدة حقوق، فإذا قامت الدولة بأي عمل مخالف لقواعد القانون الدولي ونتج عن هذا العمل إحداث ثمة ضرر أصاب دولة أخرى فإن قواعد القانون الدولي تحملها نتيجة ذلك الضرر، فالإجرام السيبراني يقوم به أشخاص يخضعون لقواعد القانون الدولي، وينتج عنه أضرار فتقوم مسؤولية الدولة[٢٠].

أولاً: نسبة الجريمة السيبرانية إلى أحد أشخاص القانون الدولي: لا يكفي لقيام المسؤولية الدولية عن الجرائم السيبرانية أن يكون العمل غير مشروع، بل يلزم أن إسناد هذا العمل إلى دولة من أشخاص القانون الدول، فلا يكفي أن يكون العمل منسوبًا إلى دولة محددة، بل يلزم كذلك أن تكون تلك الدولة ذات سيادة، وينتج عن ذلك إن الدولة ناقصة السيادة لا تسأل عن أعمالها، فهي لا تمارس حقوق الدولة كاملة السيادة [٢١].

وبالتطبيق على الجرائم السيبرانية نجد أن ركن الضرر يقوم بمجرد وقوع هجمات سيبرانية، حيث أن الهجمات السيبرانية تهدف السيطرة على بنية الدولة التحتية، وهذا ما ينتج عنه أضرارًا تصيب الدولة المعتدى عليها، والدولة المعتدية هي بالقطع دول متقدمة تمتلك القوة إلكترونية الهائلة التي تمكنها من إتيان تلك الهجمات، كما قد تقوم بتلك الهجمات عناصر أخرى، فعلى سبيل المثال قد ترتكب الجرائم السيبرانية من الجماعات الإرهابية والجماعات المتمردة، وكذلك حركات التحرر الوطني، فهؤلاء ينطبق عليهم الركن الأول المتمثل في نسبة الفعل إلى الدولة [٢٢].

ثانيًا: أن تكون الجريمة السيبرانية غير مشروعة: إن الفعل غير المشروع دوليًا هو الفعل الذي يشكل إنتهاكًا لقواعد القانون الدولي، فالفعل غير المشروع طبقًا لقواعد القانون الدولي يتمثل في الإتيان بفعل أو إمتناع عن الإتيلن به مما يشكل مخالفة لأحد الإلتزامات الملقاه على الدولة، فمعيار عدم المشروعية بصفة عامة هو معيار موضوعي مجرد، ولا عبرة في وصف الفعل بعدم المشروعية بمنشأ الالتزام فقد تكون عدم المشروعية من فعل الدولة كما تكون من فعل أتاه الفرد، ولا عبره في وصف الفعل بعدم المشروعية بوصفه في القانون الداخلي، كما لا يعتد بالوسيلة التي يتحقق بها إنتهاك قواعد القانون الدولي، سواء أكان ذلك بفعل أيجابي أم امتناع عن فعل بسلوك سلبي[٢٣].

وفي الجرائم السيبرانية نجد أنها قد تسبب أضرارًا بشرية ومادية، وهذا ما يشكل مخالفة لميثاق الأمم المتحدة، ومخالفة لقواعد القانون الدولي الإنساني.

ثالثًا: إن ينتج عن الجريمة السيبرانية ضرر: يعتبر ركن الضرر أهم ركن من أركان المسؤولية الدولية عن الجرائم السيبرانية؛ لأنه متى إنعدم الضرر انعدمت معه مسؤولية الدولة، ويأخذ الضرر عدة أوصاف فهناك ضرر مباشر وضرر غير مباشر، وهناك الضرر المادي وهو كل اعتداء على حق من حقوق الدولة أو المساس بحقوق رعاياها، وهناك الضرر المعنوي ويتمثل في كل اعتداء أو حتى المساس بشرف الشخص الدولي أو بأحد رعاياه [٢٤].

وبالتطبيق على الجرائم السيبرانية نجد أن ركن الضرر متحقق بكافة أشكاله سواء أكان القائم بالفعل دولة كما حدث في الهجوم الفيروسي على البرنامج النووي الإيراني، كما يتحقق الضرر من فعل المنظمات الإجرامية، كما في فعل الهجمات التي تقوم بها بهدف سرقة المعلومات أو إختراق حسابات مصرفية، وكذلك سرقة أرقام بطاقات الوفاء والضمان ([٢٥]).

الفرع الثاني: أساس المسؤولية الدولية عن الجرائم السيبرانية

تشكل الجهود التي سعت إليها الدول ومختلف المنظمات العالمية وسيلة لمواجهة الجرائم السيبرانية، وذلك من خلال التنسيق بين مختلف الوسائط التقنية والأكاديمية، وتكثيف آليات الاتصال والتعاون، من خلال وضح استراتيجيات دولية متنوعة لمواجهة التهديدات السيبرانية في نطاق ومسؤولية كل طرف وضرورة مراقبة استخدام تكنولوجيا المعلومات والاتصالات، في ظل انكشاف العالم على بعضه.

أولاً: المسؤولية الدولية عن الجرائم السيبرانية أستنادًا لنظرية العمل غير المشروع: تقوم نظرية الفعل غير المشروع عن الإخلال بالتزام دولي يستوجب مسائلة الدولة المعتدية، ولا عبرة لمصدر هذا الإخلال فقد يكون صادرًا من السلطة التشريعية أو السلطة التنفيذية أو السلطة القضائية، متى نتج عنه ضررًا بأحد الأجانب في شخصه أو أمواله وكان متواجدا بأراضيها.

تعتبر الهجمات السيبرانية الدولية عمل غير مشروع، وتخضع للمسؤولية الدولية على هذا الأساس إذا توفر معيار الصفة الدولية والمتمثل في صدور هذه الهجمات من قبل الدولة، أما المعيار الثاني أن تكون الهجمات السيبرانية خارقة لمعاهدة أو عرف دولي، فيجب أن يترتب على الهجمات السيبرانية ثمة ضرر بمصالح أحد أشخاص القانون الدولي، أي أن يكون قد تم التعدي عليها من الناحية الاقتصادية أو من الناحية السياسية، أو تمس الهجمات السيبرانية بأحد المبادئ التي كرستها الأمم المتحدة من أجل حفظ السلم والأمن الدولي [٢٦].

وقد تعرضت نظرية العمل غير المشروع للنقد:

– إن عملية إسناد المسؤولية للدولة عن الأضرار الناتجة عن الجرائم السيبرانية التي تقوم عليها نظرية العمل غير المشروع، تثير مشكلة تتعلق بصعوبة تحديد ما إذا كان هذا العمل منسوبًا للدولة فعلا، وهذا الأمر مرتبط بالقدرة التكنولوجية للدولة المعتدى عليها، فيمكن للدولة منشأ التصرف (المعتدية) طمس هوية الفاعل [٢٧].

– إن عملية نسبة العمل الدولية تزداد تعقيدا في الحالة التي لا تكون الشبكات السيبرانية هي الوسط الذي تمت من خلاله هذه الهجمات، مثل عملية إرسال فيروسات توضع مباشرة في أجهزة الحاسوب الخاصة بالدولة المعتدى عليها، أو في الحالة أستخدام الدولة المعتدية إقليم دولة أخرى لتنفيذ الجرائم [٢٨].

ثانيًا: المسؤولية الدولية عن الجرائم السيبرانية أستنادًا لنظرية المخاطر (المسؤولية الموضوعية): ظهرت نظرية المخاطر بعد الإنتقادات التي وجهها الفقه لنظرية الفعل غير المشروع، بعد أن أصبحت عاجزة عن مواكبة التطور التكنولوجي و العلمي، فقد كان من نتاج هذا تطوير هذه النظرية ظهور ما يطلق علية العالم الافتراضي والذي أصبح مسرحًا تدار من خلاله شؤون الكثير من الدول في مختلف المجالات، سواء أكانت سياسية أو إجتماعية أو اقتصادية، وتقوم نظرية المخاطر على أساس مسائلة الدولة بوصفها شخص من أشخاص القانون الدولي متى قامت بارتكاب سلوك مخالف للقانون الدولي، وكان هذا السلوك على درجة عالية من الخطورة [٢٩].

وهنا العديد من الإتفاقيات الدولية التي أخذت بنظرية المخاطر كأساس لتحديد المسؤولية الدولية، فنجد على سبيل المثال الاتفاقيات الخاصة بالطاقة الذرية، فهذه الاتفاقيات تلزم الدولة متى قامت بأي نشاط ذري في وقت السلم أن تقوم بدفع التعويض عن كافة الأضرار الناجمة عن هذه الأنشطة، وذلك بناء على قواعد المسؤولية الموضوعية، دون أن تشترط أن يكون هناك أي خطأ للدولة [٣٠].

إن أغلب الأضرار التي تصيب دولا أخرى تكون نتيجة أعمال غير مشروعة للدول المتسببة في تلك الأفعال أو عن طريق القيام بأنشطة مشروعة بناء على قواعد القانون الدولي، إلا أنه يتعذر إثبات عدم المشروعية، من هنا أقيمت المسؤولية الدولية على أساس توفر ركن الضرر والعلاقة السببية، وعلى هذا الأساس يجب أن نبين ما إذا كانت شروط المسؤولية الموضوعية تنطبق على الفضاء السيبراني:

أ – الخطأ: فإن أول شرط يجب أن يتوفر لقيام نظرية المخاطر هو وجود نشاط خطر باعتبار أن الجرائم السيبرانية وكافة الأنشطة الضارة في الفضاء السيبراني، ينتج عنها ضررًا عابر للحدود يمس البنية التحتية للدول أو يمس الأمن والسلم الدولي، فإن الهجمات السيبرانية والأنشطة الضارة التي تقوم بها الدول في العالم الافتراضي تكييف على أنها نشاطات خطرة نظرا لما يترب عليها من آثار وخيمة على الأمن القومي والدولي، وبالتالي يكون عنصر الخطأ قد توافر [٣١].

ب – الضرر: يتميز ركن الضرر في الجرائم السيبرانية بانه عابر للحدود، ولا يستطيع أحد إنكار حقيقة أن الهجمات السيبرانية والأنشطة الضارة التي تمارسها الدولة المعتدية في الفضاء الإلكتروني تلحق أضرارا بالدولة المعتدى عليها، إذ أن تبني الدول الحكومة الإلكترونية في تسيير شؤونها وإتساع دائرة التعامل بوسائل التكنولوجيا والإتصال نتج عنه أن أصبحت قواعد البيانات القومية غير سرية مما عرضها إلى مخاطر هجمات الفضاء الإلكتروني [٣٢].

ج –علاقة السببية: إن قيام المسؤولية الموضوعية تشترط وجود علاقة سببية بين النشاط الخطر والأضرار الناتجة عنها، لذا يجب إثبات أن الأضرار التي لحقت الدول ومست أمنها القومي ناتج عن الهجمات السيبرانية التي قامت بها دولة أخرى [٣٣].

ومن جانبنا فإننا نرى أن نظرية المخاطر لا يمكن اعتماد عليها كأساس للمسؤولية الدولة عن الهجمات السيبرانية باعتبار أن نشاط الدولة في عالم الإفتراضي ليس مشروع فهو في زمن الحرب نزاعًا مسلحًا، وفي وقت السلم يكيف على أنه نشاط إجرامي تقوم به دولة ضد دولة أخرى من أجل تحطيم البنية التحية للدول مما يشكل تدخل في الشؤون الداخلية للدول.

ومنا جانبنا فإننا نرى أن الأساس الذي تبنى علية المسؤولية الدولية عن الجريمة السيبرانية هو نظرية المخاطر والتي قوامها المسؤولية الموضوعية، وذلك لصعوبة تحديد عناصر المسؤولية عن العمل غير المشروع مما قد ينتج عنه إفلات الجاني من المسؤولية الجنائية الدولية، ولكن في حالة المسؤولية الموضوعية فإن عناصر المسؤولية تكون مفترضة متى تحقق الفعل الخطأ والضرر.

المطلب الثاني: الإتجاهات الدولية في مكافحة الجرائم السيبرانية

لم يقف المجتمع الدولي مكفوف الأيدي حيال الجرائم السيبرانية، بل سارع الفقة والتشريع الدولي إلى إقرار العديد من الأوراق الدولية للتصدي لتلك الظاهرة الإجرامية الحديثة، فنجد دليل تالين بوصفه مجموعة من التوصيات التي قدمها الفقة الدولي للتصدي للجريمة السيبرانية، وكذلك شرع المجتمع الدولي أتفاقية بودابست بوصفها أتفاقية دولية لمكافحة الجريمة الدولية.

الفرع الأول: دور قانون تالين في مكافحة الجرائم السيبرانية ([٣٤])

إذا تم تكييف الجرائم السيبرانية على أنها حروب فإن دليل تالين قد تكفل بها، فطبقًا للدليل نجد أن الجرائم السيبرانية تقوم بإرتكابها دولة ضد دولة أخرى، وقد تم إعداد الدليل نتيجة لقصور قواعد القانون الدولي عن مواجهة هذا النوع المستحدث من الجرائم وكذلك التشريعات الداخلية، ومن جهة أخرى عدم وجود أي أساس قانوني ينظم اللجوء إلى الحروب السيبرانية، وتم إبرام هذا الدليل من أجل دراسة مدى إمكانية مدى تطبيق قواعد القانون الدولي الإنساني على الحروب السيبرانية بصفة عامة، وكذلك وذلك اثر الهجوم السيبراني الشامل الذي شنته روسيا ضد استونيا عام ٢٠١٧ ([٣٥]).

ويظهر دور دليل تالين في مواجهة الحرب السيبراني من خلال قيامه بتحديد أهم النقاط الحساسة ذات الصلة بالحروب والهجمات السيبرانية كمفهوم النظام التراع المسلح في إطار الحرب السيبرانية ومفهوم الجيوش السيبرانية، وكيفية إدارة الحرب السيبرانية من خلال قواعد الاشتباك السيبراني، وصفة المقاتلي السيبراني، إضافة إلى إمكانية مراعاة القانون الدولي الإنساني المعروفة كمبدأ التميز، ومدى شرعية استهداف المقاتل السيبراني بالوسائل العسكرية كالطائرات العسكرية بدون طيار ([٣٦]).

الفرع الثاني: دور أتفاقية بودابست في مكافحة الجرائم السيبرانية

إذا تم تكييف الجرائم السيبرانية على أنها أفعال إجرامية تنفذها الدول ضد بعضها البعض، وقد تكفلت أتفاقية بودابست (٢٠١١) بتحديد القانون الواجب التطبيق على تلك الجرائم، ولكن يلاحظ ان أتفاقية بودابست لم تتطرق للجرائم السيبرانية التي تشنها الدول ضد بعضها البعض، فقد تحدد نطاق الإتفاقية بالجرائم السيبرانية التي تنفذ من قبل الأفراد ضد الأفراد الأخرين، ويرجع السبب في ذلك إلى أن الأتفاقية قد كييف الجرائم السيبرنية بأنها جرائم وليست حروب.

أولاً: القواعد الموضوعية: عملت أتفاقية بودابست على توزيع الجرائم التي ترتكب بواسطة الانترنت، على أربع مجموعات تضم الأولى الجرائم التي تتعرض لخصوصية وسلامة وتوفر الأنظمة والبيانات، مثل النفاذ غير الشرعي، والاعتراض غير الشرعي، وتشويه البيانات، وسلامة النظام، وتضم المجموعة الثانية جرائم الإحتيال والتزوير، كما تضم المجموعة الثالثة، الجرائم المتصلة بالمحتوى، مثل إنتاج، توزيع، وحيازة مواد اباحية يستخدم فيها الأطفال، وتضم المجموعة الرابعة، جرائم الاعتداء على الملكية الفكرية، والحقوق المجاورة ([٣٧]).

وأتفاقية بودابست تلزم الدول الأعضاء فيها بإتخاذ التدابير التشريعية وكافة الإجراءات التي تتناسب لتجريم عدد (٩) جرائم في تعد هي عماد الجرائم السيبرانية وهي:

– الدخول غير القانوني المتعمد إلى أي نظام كمبيوتر أو جزء منه دون حق أو إذن سواء أكان هذا الدخول بنية إنتهاك وسائل الأمن أو حتى بنية الحصول على معطيات الكمبيوتر أو لأية نية أخرى غير مباحة.

– الاعتراض غير القانوني المتعمد ودون حق بواسطة وسائل تكنولوجية للبيانات المرسلة غير العامة إلى أو من نظام كمبيوتر وكذلك اعتراض الإشعاعات الكهرومغناطيسية المنبعثة من أي نظام كمبيوتر تحمل مثل هذه المعطيات.

– التدخل عن عمد أو الإرادي في المعطيات بالتدمير أو التشويه أو الحذف والإفساد أو تبديلها أو تغيرها أو تعديلها أو تعطيلها أو كبتها أو إخمادها.

– التدخل عن عمد في أنظمة التكنولوجيا.

– إساءة استعمال الأجهزة.

– التزوير المتعمد باستخدام جهاز الكمبيوتر: كذلك بإدخال أى حذف أو تعديل أو إخفاء بيانات الكمبيوتر على نحو يظهر بيانات غير البيانات الأصلية لتكون مقبولة قانونا وكأنها بيانات أصلية، وذلك بغض النظر عما إذا كانت هذه البيانات مقروءة أو غير مقروءة ويحق للدولة أن تشترك نية أو قصد الغش لقيام المسؤولية الجنائية.

– الإحتيال المتعمد بإستخدام أجهزة الكمبيوتر.

– الجرائم المرتبطة بإستخدام دعارة الأطفال.

– الجرائم المرتبطة بحق الملكية الفكرية والمؤلف.

ثانيًا العقوبات: ربطت أتفاقية بودابست بين الجرائم والعقوبات فتحدد مختلف الجرائم السيبرانية أو الجرائم المتصلة بالكمبيوتر التي ينبغي أن يعاقب عليها القانون الجنائي، وفقًا للالتزامات التي تفرضها تلك المواد، يلزم هذا الحكم الأطراف المتعاقدة بإستخلاص العواقب من الطبيعة الخطيرة لهذه الجرائم من خلال النص على عقوبات جنائية "فعالة ومتناسبة ورادعة"، تشمل، فيما يتعلق بالأشخاص الطبيعيين، وإمكانية فرض عقوبات بالسجن في القانون الداخلي ([٣٨]).

وقد أقرت الأتفاقية مبدأ مسؤولية الشخص المعنوي عن الجريمة السيبرانية، حيث نصت المادة (١٢) على ما يلى : سوف تتبنى كل دولة طرف إجراءات تشريعية، وأى تدابير أخرى وذلك لضمان قيام مسئولية الأشخاص المعنوية عن أي جريمة موصوفة في هذه المعاهدة، إذا ما ارتكبت لصالح الشخص المعنوى بواسطة شخص طبيعى ارتكبها بشكل منفرد أو بوصفه جزء من جهاز تابع للشخص المعنوى ويتبوأ منصباً قيادياً داخله، وذلك على أساس: أ– سلطة اتخاذ قرارات لصالح الشخص المعنوى "سلطة تمثيلية".، ب– تفويض قانونى من الشخص المعنوى.، ج– سلطة لممارسة رقابة أو سيطرة داخل الشخص المعنوى ([٣٩]).

الخاتمة

بعد انتهينا من موضوع دراستنا توصلنا إلى عدة نتائج وارتأينا أن نقدم بعض التوصيات لكي تكون دراسة متكاملة.

أولا: استنتاجات

١. إن الجرائم السيبرانية تعد عمل غير مشروع فهي بحد ذاتها تمثل إنتهاك لأحكام وقواعد القانون الدولي، فيترتب عليها أخترق أسرار ووثائق الدول، وهي تستهدف مصالح الدولة، وتعمل على أختلق قضايا دولية جديدة لم تعرفها الدول في زمن الحروب التقليدية.

٢. أن بناء المسؤولية الدولية عن الهجمات السيبرانية في سياق نظرية العمل غير المشروع قد لا تحقق أهدافها والسبب هو صعوبة تحديد هوية المهاجم السيبراني، وهذا بحد ذاته يعد عائقا أمام تحقيق أهداف القانون الدولي بإعتباره ينظم قواعد المسؤولية المتعلقة بإنتهاكات القانون الدولي العام والقانون الدولي الإنساني.

٣. إن نظرية المخاطر تعد الأنسب لبناء المسؤولية الدولية عن الجرائم السيبرانية حيث أنها تقوم على المسؤولية الموضوعية والتي تكون أركان الجريمة مفترضة مما يسهل مهمة المضرور المعتدى علية، وبما يراعي صفات تلك الجريمة، كجريمة صعبة الإثبات.

٤. أن دليل تالين محاولة فقهية لمكافحة الجرائم السيبرانية، وهو دليل متكامل بوصفه ورقة دولية تستطيع الدول أن تأخذ به عند وضع التشريعات التي تواجهه الجرائم السيبرانية.

٥. تعد أتفاقية بودابست من أهم الوثائق الدولية لمكافحة الجرائم السيبرانية، وتبدو أهميتها في إقرارها إجراءات وقواعد تلتزم الدول المنظمة بإدراجها في تشريعاتها الداخلية والتي تهدف إلى حفظ بيانات الأتصال وتحديد مصدرها.

٦. وضعت أتفاقية بودابست مجموعة من الأفعال الإجرامية حريًا بالدول تجريمها عند وضوع قانون لمواجهة الجرائم السيبرانية، كما ترك تحديد العقوبات للتشريعات الجنائية، على أن تكون العقوبات متناسبة مع الأفعال الإجرامية.

ثانيًا: التوصيات

١. نوصي بتفعيل التعاون بين الدول بما ينتج عنه تعظيم دور المعاهدات الدولية، وبما يرمي إلى إقرار مبدأ المساعدة القضائية والقانونية والأمنية بين كافة الجهات في حقل مكافحة الجرائم السيبرانية.

٢. نوصي بإعتماد نظرية المخاطر لبناء المسؤولية الدولية عن الجرائم السيبرانية والقائمة على أساس المسؤولية الموضوعية والتى تكون أركان الجريمة مفترضة مما يسهل مهمة المضرور المعتدى علية.

٣. نوصي بأن تقوم كافة الدول بإدخال اتفاقية بودابست ضمن تشريعاتها، سواء التشريعات العقابية أو حتى سن تشريعات مستقلة لمكافحة الجريمة السيبرانية، تكون مأخوذة من نصوص الإتفاقية.

الهوامش

(١) من أنصار هذا الجانب راجع د. حنان ريحان مبارك المضحاكي، الجرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، ٢٠١٤، ص: ٢٥.

(٢) د. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، بدون سنة نشر، ص: ٢٥.

(٣) د. باطلي غنية، الجريمة الإلكترونية "دراسة مقارنة"، الدار الجزائرية للنشر والتوزيع، الجزائر، ٢٠١٥، ص: ١٥

(4) MERWA (VANDER), COMPUTER CRIMES AND OTHER CRIMES AGAINST INFORMATION TECHNOLOGY IN SOUTH AFRICA , R.I.D.P , 1993 ,P 554.

(٥) د. محمد أمين الشوابكة، جرائم الحاسب والإنترنت، دار الثقافة، الأردن، ٢٠١١، ص ٩

(٦) د. طارق إبراهيم الدسوقي، عطية، الأمن المعلوماتي النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٩، ص ١٥٨.

(٧) د. حنان ريحان مبارك المضحاكي، المرجع السابق، ص ٢٦.

(٨) د. خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، ٢٠١١، ص ٢٨.

(9) roden (Adrian), computer crime and the law, c,l,j.,1991,vol.15,p.399

(١٠) أسامة أحمد المناعسة، جلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، الطبعة الثالثة، دار الثقافة للنشر والتوزيع، عمان، ٢٠١٤، ص ٩٣.

(١١) يعرف الفضاء السيبراني هو عالم إفتراضي مع عالمنا المادي يتأثر به ويؤثر فيه بشكل معقد، وتعتمد الهجمات السيبرانية على نظم الكمبيوتر وشبكات الإنترنت والمخزون الهائل من المعلومات والبيانات حيث يتم الاتصال بشبكات الإنترنت عبر الحواسيب أو الهواتف أو غيرها من

الأجهزة دون تقيد بالحدود الجغرافية.

(١٢) محمود محارب، قراءات في كتاب حرب الفضاء الإلكتروني، إتجاهات تأثيرات على إسرائيل، المركز القومي للأبحاث ودراسة السياسات، الدوحة، ٢٠١١، ص ١٣٢

(١٣) محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، ٢٠٠٤، ص ٥٣.

(١٤) د. جوزيف ناي، المنازعات الدولية مقدمة للنظرية والتاريخ، ترجمة احمد أمين الجمل ومجدي كامل، الجمعية المصرية لنشر المعرفة والثقافة العالمية، القاهرة، ٢٠١١، ص٨٢

(15) Heather Harrison Dinniss, The status and use of computer network attacks in international law, Phd thesis, London school of a economics and Political science, 2008, P 33

(١٦) د. أحمد بشارة موسى، المسؤولية الجنائية الدولية للفرد، دار هومة للنشر والتوزيع، الجزائر، ٢٠٠٩، ص ١٣٥

(١٧) د. عبد الفتاح بيومي حجازي، المحكمة الجنائية الدولية دراسة متخصصة في القانون الجنائي الدولي، دار الفكر الجامعى، الإسكندرية، ٢٠٠٤، ص ٩٧

(١٨) د. فتوح عبد الله الشاذلي، القانون الدولي الجنائي، أولويات القانون الدولي الجنائي، النظرية العامة للجريمة الدولية، الطبعة الثانية، دار النهضة العربية للنشر والتوزيع، ٢٠١٦، ص ٢٠٧

(١٩) د. حسنين إبراهيم صالح عبيد، الجريمة الدولية، دراسة تحليلية تطبيقية، الطبعة الأولى، دار النهضة العربية، القاهرة، ١٩٧٩، ص ٦

(٢٠) د. زياد البداينة، الأمن وحرب المعلومات، دار الشروق للنشر والتوزيع، الأردن، ٢٠٠٣، ص ١١٦

(٢١) د. محمد عبدالله أبو بكر، جرائم الكمبيوتر والإنترنت، منشاة المعارف، الإسكندرية، ٢٠٠٦، ص ٨٨

(٢٢) عبد الفتاح بيومي حجازي، الإثبات الجنائي " جرائم الكمبيوتر والإنترنت "، بدون ناشر، ٢٠٠٧، ص ٣٢٤

(٢٣) صلاح الطائي، حق الإسترداد في القانون الدولي، مكتبة الجامعة الحديثة، القاهرة، ٢٠٠٩، ص ١١٦

(٢٤) د. جميل عبد الباقي الصغير، الجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ١٩٩٨، ص ٢٥٦

(٢٥) جانكارلو أ. بارليتا، النزاع السيبراني والاستقرار الجيوسيبراني، الاتحاد الدولي للاتصالات، القاهرة، ٢٠١١، ص ١٨

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

(٢٧) 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، ص ٣٣٨

(٢٨) عباس بدران، الحروب الإلكترونية (الاشتباك في العالم المتغير)، مركز دراسات الحكومات الإلكترونية، بيروت، ٢٠١٠، ص١١١

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

(٣٠) د. صباح العيشاوي، المسؤولية الدولية عن حماية البيئة، ط ١، دار الخلدونية للنشر والتوزيع، الجزائر، ٢٠١٠، ص١٧٤

(٣١) عبد الفتاح مراد، شرح التحقيق الجنائي الفني و البحث الجنائي، دار الكتب و الوثائق المصرية، مصر، ٢٠٠٦، ص٢١٤

(٣٢) د. وسيم طعمة، السرقة لمعلوماتية "دراسة مقارنة"، مجلة جامعة البحث، جامعة دمشق، العدد ٦٨، سوريا، ٢٠١٧، ص١٧٦.

(٣٣) د. عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مكتبة الإسكندرية، وحدة الدراسات المستقبلية، مصر، ٢٠١٦ ص ١٤٥

(٣٤) صدر دليل تالين (le Manuel de Tallinn) عام ٢٠١٣ المتعلق بقواعد القانون الدولي المطبقة على الحرب السيبرانية، قام بإعداد هذا الدليل مجموعة من خبراء القانون الدولي بدعوة من منظمة حلف شمال الأطلس (NATO) بحضور اللجنة الدولية للصليب الأحمر، ويتكون هذا الدليل من (٩٥) مادة جاءت معظمها من ميثاق الأمم المتحدة وقواعد القانون الدولي الإنساني.

(٣٥) د. سعيد درويس، ماهية الحروب الالكترونية في ضوء قواعد القانون الدولي، حوليات جامعة الجزائر ١، العدد ٢٩، ص ١١٩

(٣٦) اللجنة الدولية للصليب الأحمر، "ماهية القيود التي يفرضها قانون الحرب على الهجمات السيبرانية؟"، على الرابط:
http://accronline.com/article_detail.aspx?id=28958

(٣٧) د. منى الأشقر جبور، السيبرانية هاجس العصر، دراسات وأبحاث، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، بيروت، ٢٠١٧، ص ١٠٥

(٣٨) د. وليد طه، التنظيم التشريعي للجرائم الإلكترونية في أتفاقية بودابست، قطاع التشريع بوزارة العدل، مصر، بدون سنة نشر، ص ٢٣ وما بعدها

(٣٩) د. إيهاب السنباطى، الترجمة الجديدة والكاملة للاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست ٢٠٠١)، والبروتوكول الملحق بها، لأول مرة باللغة العربية، دار النهضة العربية، القاهرة، ٢٠٠٩، ص ٢٢.

المراجع

الكتب

١) د. أحمد بشارة موسى، المسؤولية الجنائية الدولية للفرد، دار هومة للنشر والتوزيع، الجزائر، ٢٠٠٩

٢) أسامة أحمد المناعسة، جلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، الطبعة الثالثة، دار الثقافة للنشر والتوزيع، عمان، ٢٠١٤

٣) د. إيهاب السنباطى، الترجمة الجديدة والكاملة للاتفاقية المتعلقة بالجريمة الإلكترونية) بودابست ٢٠٠١)، والبروتوكول الملحق بها، لأول مرة باللغة العربية، دار النهضة العربية، القاهرة، ٢٠٠٩

٤) إيهاب خليفة، مجمع ما بعد المعلومات، تأثير الثورة الصناعية الرابعة على الأمن القومي، العربي للنشر والتوزيع، القاهرة

٥) د. باطلي غنية، الجريمة الإلكترونية "دراسة مقارنة"، الدار الجزائرية للنشر والتوزيع، الجزائر، ٢٠١٥،

٦) جانكارلو أ. بارليتا، النزاع السيبراني والاستقرار الجيوسيبراني، الاتحاد الدولي للاتصالات، القاهرة، ٢٠١١

٧) د. جميل عبد الباقي الصغير، الجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ١٩٩٨

٨) د. جوزيف ناي، المنازعات الدولية مقدمة للنظرية والتاريخ، ترجمة احمد أمين الجمل ومجدي كامل، الجمعية المصرية لنشر المعرفة والثقافة العالمية، القاهرة، ٢٠١١

٩) د. حسنين إبراهيم صالح عبيد، الجريمة الدولية، دراسة تحليلية تطبيقية، الطبعة الأولى، دار النهضة العربية، القاهرة، ١٩٧٩

١٠) د. حنان ريحان مبارك المضحاكي، الجرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، ٢٠١٤

١١) د. خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، ٢٠١١

١٢) د. زياد البداينة، الأمن وحرب المعلومات، دار الشروق للنشر والتوزيع، الأردن، ٢٠٠٣،

١٣) د. صباح العيشاوي، المسؤولية الدولية عن حماية البيئة، ط ١، دار الخلدونية للنشر والتوزيع، الجزائر، ٢٠١٠

١٤) صلاح الطائي، حق الإسترداد في القانون الدولي، مكتبة الجامعة الحديثة، القاهرة، ٢٠٠٩
١٥) د. طارق إبراهيم الدسوقي، عطية، الأمن المعلوماتي النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، مصر، ٢٠٠٩
١٦) د. عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مكتبة الإسكندرية، وحدة الدراسات المستقبلية، مصر، ٢٠١٦
١٧) عباس بدران، الحروب الإلكترونية (الاشتباك في العالم المتغير)، مركز دراسات الحكومات الإلكترونية، بيروت، ٢٠١٠،
١٨) د. عبد الفتاح بيومي حجازي، المحكمة الجنائية الدولية دراسة متخصصة في القانون الجنائي الدولي، دار الفكر الجامعى، الإسكندرية، ٢٠٠٤
١٩) عبد الفتاح بيومي حجازي، الإثبات الجنائي " جرائم الكمبيوتر والإنترنت "، بدون ناشر، ٢٠٠٧،
٢٠) عبد الفتاح مراد، شرح التحقيق الجنائي الفني والبحث الجنائي، دار الكتب والوثائق المصرية، مصر، ٢٠٠٦.
٢١) د. فتوح عبد الله الشاذلي، القانون الدولي الجنائي، أولويات القانون الدولي الجنائي، النظرية العامة للجريمة الدولية، الطبعة الثانية، دار النهضة العربية للنشر والتوزيع/٢٠١٦
٢٢) د. محمد أمين الشوابكة، جرائم الحاسب والإنترنت، دار الثقافة، الأردن، ٢٠١١
٢٣) د. محمد عبد الله أبو بكر، جرائم الكمبيوتر والإنترنت، منشاة المعارف، الإسكندرية، ٢٠٠٦
٢٤) محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، ٢٠٠٤
٢٥) محمود محارب، قراءات في كتاب حرب الفضاء الإلكتروني، إتجاهات تأثيرات على إسرائيل، المركز القومي للأبحاث ودراسة السياسات، الدوحة، ٢٠١١
٢٦) د. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، بدون سنة نشر
٢٧) د. وليد طه، التنظيم التشريعي للجرائم الإلكترونية في أتفاقية بودابست، قطاع التشريع بوزارة العدل، مصر، بدون سنة نشر

الدوريات

١) رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة للعلوم القانونية، المجلد ١٥، العدد ٢، ديسمبر، ٢٠١٨
٢) د. سعيد درويس، ماهية الحروب الالكترونية في ضوء قواعد القانون الدولي، حوليات جامعة الجزائر ١، العدد ٢٩

٣) لورنس سعيد الحوامدة، "الجرائم المعلوماتية أركانها وآلية مكافحتها، دراسة تحليلية مقارنة "، مجلة الميزان للدراسات الإسلامية والقانونية، كلية الحقوق، المملكة العربية السعودية، ٢٠١٦

٤) د. منى الأشقر جبور، السيبرانية هاجس العصر، دراسات وأبحاث، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، بيروت، ٢٠١٧

٥) د. وسيم طعمة، السرقة لمعلوماتية "دراسة مقارنة"، مجلة جامعة البحث، جامعة دمشق، العدد ٦٨، سوريا، ٢٠١٧

الكتب باللغة الأجنبية

1) MERWA (VANDER), COMPUTER CRIMES AND OTHER CRIMES AGAINST INFORMATION TECHNOLOGY IN SOUTH AFRICA, R.I.D.P, 1993
2) roden (Adrian), computer crime and the law, c,l,j.,1991,vol.15
3) Heather Harrison Dinniss, The status and use of computer network attacks in international law, Phd thesis, London school of a economics and Political science, 2008