مسألة إسناد المسؤولية الدولية عن أعمال العدوان التي تتم من خلال الهجمات السيبرانية في إطار القانون الدولي

The issue of assigning international responsibility for acts of aggression carried out through cyber attacks within the framework of international law

م.م. ريكان جوهر صادق

نقابة محامي كوردستان

Rekan.jawhar0750@gmail.com

تاريخ استلام البحث: ٢٠٢٤/٥/١٠ تاريخ قبول النشر: ٢٠٢٥/٨/١٨

الملخص:

إن المسؤولية القانونية الدولية معترف بها بالنسبة لجريمة العدوان حيث أنها تصنف كجريمة دولية تدخل في اختصاص المحكمة الجنائية الدولية. وقد تم دمج تعريف العدوان، كما هو مبين في المادة الأولى من قرار تعريف العدوان رقم ٣٣١٤ لعام ١٩٧٤، في النظام الأساسي للمحكمة الجنائية الدولية، وهو يشمل الأشكال التقليدية للعدوان والأفعال المحددة على أنها مجرمة في المادة الثالثة من القرار.

تتناول هذه الدراسة مسألة المساءلة الدولية عن أعمال العدوان التي تتم من خلال الهجمات السيبرانية، والتي لم يتم تناولها بشكل صريح في المادة الثالثة من القرار المذكور. على عكس أعمال العدوان التقليدية التي تستخدم القوة المادية، تنطوي الهجمات السيبرانية على استخدام الأسلحة الافتراضية في الفضاء السيبراني لاستهداف السلامة الإقليمية والاستقلال السياسي للدول. يقيم البحث مدى انطباق القواعد الحالية للمسؤولية الدولية عن أعمال العدوان التقليدية على الشكل الحديث للعدوان المتمثل في الهجمات السيبرانية.

الكلمات الافتتاحية: المسؤولية الدولية، العدوان، الهجمات السيبرانية، الجريمة الدولية، المحكمة الجنائية الدولية.

Abstract:

International legal responsibility is recognized for the crime of aggression, as it is classified as an international crime that falls within the jurisdiction of the International Criminal Court. The definition of aggression, as set out in Article 1 of the Definition of Aggression Resolution No. 3314 of 1974, has been incorporated into the Statute of the International Criminal Court and includes traditional forms of aggression and acts defined as criminal in Article 3 of the resolution.

This study addresses the issue of international accountability for acts of aggression carried out through cyber attacks, which is not explicitly addressed in Article Three of the aforementioned resolution. Unlike traditional acts of aggression that use physical force, cyberattacks involve the use of virtual weapons in cyberspace to target the territorial integrity and political independence of states. The research

evaluates the applicability of current rules of international liability for traditional acts of aggression to the modern form of aggression represented by cyberattacks.

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

المقدمة

لقد نفذ المجتمع الدولي تدابير قانونية مختلفة لمعالجة حدوث الحرب وتقليل تأثيرها على المجتمع الدولي، مع الاعتراف بالدمار الكبير الذي تسببه. وقد بذلت جهود للتخفيف من آثار الحرب واعتبارها عملاً إجرامياً، لأنها ترتبط في كثير من الأحيان بالعدوان الذي يحمل تداعيات دولية على الدول المعنية. كان الهدف من إنشاء الأمم المتحدة هو الحفاظ على السلم والأمن الدوليين، وأنيطت بمجلس الأمن مهمة التدخل لوقف أعمال العدوان وفرض التدابير المنصوص عليها في ميثاقه لدعم السلام العالمي. وأدى هذا إلى الدعوة إلى المسؤولية الجنائية الدولية عن العدوان، مع إنشاء محاكم جنائية دولية مؤقتة في نورمبرج وطوكيو، مما يشكل سابقة لمحاسبة الأفراد عن جرائم ضد السلام أثناء الحرب في أوروبا وشرق آسيا.

أسفرت الجهود الدولية التي امتدت على مدار عقدين من الزمن عن وضع تعريف قانوني محدد للعدوان، كما جاء في قرار الجمعية العامة رقم ٣٣١٤ لعام ١٩٧٤. وقد تناول هذا القرار مختلف أشكال العدوان والمسؤوليات القانونية الدولية المرتبطة بهذه الأعمال. وبعد ذلك، تم إنشاء المحكمة الجنائية الدولية، وأدرج نظامها الأساسي جريمة العدوان. وعلى الرغم من الانقسامات الأولية بين المؤيدين والمعارضين، توجت الجهود الجارية باعتماد قرار يحدد العدوان في مؤتمر كمبالا الاستعراضي عام ٢٠١٠. يتميز العصر الحالي بالتقدم التكنولوجي السريع، الذي يجلب فوائد ومخاطر، خاصة في مجال الحرب. ويطرح ظهور الحروب الحديثة، بما فيها الحرب السيبرانية، تحديات جديدة أمام المنظمات الإقليمية والدولية، حيث لا تلتزم هذه الصراعات بالتكتيكات والأسلحة العسكرية التقليدية.

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

١. هل تشكل الهجمات السيبرانية عدوانًا وفقًا للمادة ١ من قرار الجمعية العامة للأمم المتحدة رقم ٣٣١٤ لعام ١٩٧٤ الذي يعرف العدوان، والذي ينص على أن "العدوان هو استخدام القوة المسلحة أو أي شكل آخر من أشكال القوة ضد سيادة الدولة أو سلامة أراضيها أو استقلالها السياسي". دولة أخرى أو ضد ميثاق الأمم المتحدة."

٢. هل تقع الهجمات السيبرانية ضمن نطاق الأفعال المذكورة في المادة (٣) من قرار تعريف العدوان؟

٣. هل تقع الهجمات السيبرانية ضمن نطاق المادة ٤ من تعريف العدوان، والتي تمنح مجلس الأمن صلاحية النظر فيما إذا كانت هذه الأعمال تشكل انتهاكا للسلم والأمن الدوليين؟

٤. إذا كان الجواب الذي وصلنا إليه يؤكد أن الهجمات السيبرانية هي أعمال عدوانية، فهل تخضع جرائم العدوان المرتكبة من خلال الهجمات السيبرانية لنفس الأحكام الإجرائية وأحكام المسؤولية والجزاء مثل الجرائم الأخرى التي تدخل في اختصاص المحكمة؟

أهمية البحث: لقد برز تزايد الهجمات السيبرانية، ولا سيما تلك التي تعتبر عدوانية بطبيعتها، كعائق كبير أمام الخبراء في مجال القانون الدولي العام. إن التعقيدات في تحديد خصائص هذه الهجمات، خاصة عندما يتم تصنيفها على أنها أعمال عدوانية وجرائم دولية، تشكل تحديات في إسناد المسؤولية الجنائية والمدنية الدولية. لقد أصبحت ضرورة تعديل الأطر القانونية الدولية القائمة لمواجهة هذا الشكل الجديد من العدوان واضحة، حيث يمكن أن تؤدي هذه الهجمات إلى عواقب وخيمة تفوق عواقب النزاعات المسلحة التقليدية من حيث الدمار والخراب.

منهجية البحث: يركز البحث على تحليل مبادئ القانون الدولي العام فيما يتعلق بالهجمات السيبرانية، وعلى وجه التحديد دراسة التصنيف المحتمل لهذه الهجمات على أنها أعمال عدوانية وجرائم دولية. وهذا يتطلب اتباع نهج تحليلي في الغالب لتحديد المسؤولية القانونية لمرتكبي الجرائم المتورطين.

تقسيمات البحث:

المبحث الأول– ظاهرة العدوان عبر الهجمات السيبرانية في إطار الأعراف القانونية الدولية.

المطلب الأول– مفهوم وأساليب وخصائص الهجمات السيبرانية.

المطلب الثاني– الإطار القانوني الذي يحكم أعمال العدوان والهجمات السيبرانية في القانون الدولي.

المبحث الثاني– العدوان بالهجمات السيبرانية كجريمة دولية.

المطلب الأول– الأساس التشريعي لجريمة العدوان عن طريق الاختراقات السيبرانية.

المطلب الثاني– المسؤولية العالمية الناجمة عن أعمال العدوان عبر الحرب السيبرانية.

المبحث الأول: ظاهرة العدوان عبر الهجمات السيبرانية في إطار الأعراف القانونية الدولية

لقد لعب تطور القواعد القانونية الدولية دورًا مهمًا في تعريف مفهوم العدوان، مما أدى في النهاية إلى الاعتراف به كجريمة دولية متميزة من قبل المحكمة الجنائية الدولية. يُفهم العدوان على أنه استخدام القوة المسلحة من قبل دولة ما ضد سيادة دولة أخرى أو سلامة أراضيها أو استقلالها السياسي، في انتهاك لميثاق الأمم المتحدة. ومع ذلك، في العصر الحديث، تقوم بعض الدول بأعمال عدوانية باستخدام وسائل غير تقليدية وغير مادية مثل الهجمات السيبرانية. تهدف هذه الدراسة إلى استكشاف كيف يمكن أن تشكل مثل هذه الهجمات السيبرانية عدوانًا وتكون بمثابة أساس لاعتبارها جريمة عدوان كاملة الأركان في إطار القانون الدولي. وستناقش الدراسة خصائص وأساليب الهجمات السيبرانية، وكذلك أحكام العدوان من خلال الهجمات السيبرانية في القانون الدولي.

المطلب الأول: مفهوم وأساليب وخصائص الهجمات السيبرانية

لقد ظهر مفهوم الهجمات السيبرانية في الآونة الأخيرة نسبيا، تزامنا مع التقدم في تكنولوجيا المعلومات. وهذا المصطلح مشتق من أصول يونانية، وتحديداً من كلمة (kybemetes)، ويشير إلى القيادة والتحكم عن بعد.[1] علاوة على ذلك، يقدم قاموس المورد تعريفاً لعلم التحكم الآلي بأنه علم التحكم، وهو مستمد من مصطلح "علم التحكم الآلي"، والذي يتوافق مع مفهوم الهجمات السيبرانية التي تنطوي على

التحكم والتلاعب عن بعد.[٢] وفقًا للتعريف الوارد في قاموس أمن المعلومات، يشير مصطلح السيبرانية إلى اختراق إلكتروني يستهدف الأنظمة المحمية إلكترونيًا بقصد إعاقتها أو تفكيكها أو إضعافها.[٣]

يستخدم مصطلح الهجمات السيبرانية من قبل مجموعات مختلفة للإشارة إلى ظواهر متنوعة، تشمل أساليب الحرب التي تتم في الفضاء السيبراني والتي قد تتصاعد إلى أعمال عدوانية في إطار القانون الدولي. تطمس الهجمات السيبرانية الخط الفاصل بين العالمين الافتراضي والمادي، مما يؤثر على عالمنا بطرق معقدة. وتستغل هذه الهجمات أنظمة الكمبيوتر وشبكات الإنترنت، وتتجاوز الحدود الجغرافية. وهي تنطوي على التلاعب بالبيانات الرقمية والعمليات الإلكترونية في العالم الافتراضي لتحقيق أهداف عسكرية أو أمنية، وغالبًا ما تستهدف البنية التحتية الحيوية مثل المنشآت النووية ومحطات الطاقة والمطارات وأنظمة النقل.[٤] غالبًا ما يشار إلى الحرب السيبرانية على أنها الفرع الرابع للقوات العسكرية الحديثة، بالإضافة إلى القوات الجوية والبرية والبحرية. أصبح هذا الاعتراف أكثر بروزًا في عصر الإنترنت بسبب المناقشات حول إمكانية حدوث معارك فعلية في العالم الافتراضي. يرى بعض الخبراء أن الهجمات السيبرانية تشكل البعد الخامس للحرب، والتي تتميز بالإجراءات المتعمدة التي تتخذها الدولة لتعطيل أنظمة المعلومات والتلاعب بها، بينما تدافع في الوقت نفسه عن أنظمتها الخاصة من هجمات مماثلة.[٥] ويشير إلى شكل من أشكال الهجوم السيبراني حيث يتم اختراق مواقع الويب غير المصرح بها، وعادة ما يتم تنفيذه من قبل دولة ضد أخرى من خلال سلسلة من الهجمات الإلكترونية.[٦] التعريف المعترف به على نطاق واسع للهجمات السيبرانية بين الباحثين يوصف بأنه أي إجراء، سواء كان دفاعيًا أو هجوميًا، يُعتقد أنه من المحتمل أن يؤدي إلى ضرر أو وفاة فرد، أو يؤدي إلى ضرر جسدي أو تدمير الهدف الذي يتم الهجوم عليه.[٧]

- **وسائل الهجمات السيبرانية:** تشمل الأسلحة الإلكترونية، والمعروفة أيضًا بالهجمات السيبرانية، مجموعة من الأدوات المصممة لتشكل تهديدًا للأجهزة والأنظمة والبنية التحتية الإلكترونية. وتختلف هذه الأسلحة من حيث مستوى خطورتها وتعقيدها، فبعضها قادر على إحداث ضرر خارجي للأنظمة دون اختراقها، والبعض الآخر قادر على اختراق الأنظمة وإحداث ضرر جسيم قد يؤدي إلى تدميرها بالكامل أو توقفها عن العمل. وتشكل هذه الأسلحة خطراً كبيراً على أمن وسلامة الأنظمة الإلكترونية. ومن أهمها:[٨]

١. **استخدام برامج القنابل المنطقية:** تم تصميم هذا البرنامج بعناية وتم وضعه بشكل استراتيجي داخل شبكة لمراقبة وتقييم محتوى النظام. والغرض منه هو اكتشاف حالات أو حالات معينة داخل النظام. في بعض الحالات، قد يتم استخدام هذا البرنامج لأغراض ضارة، مثل إدخال تعليمات ضارة في نظام التشغيل لتنفيذ هجوم. على سبيل المثال، يمكن برمجة القنبلة المنطقية للبحث عن معلومات محددة وإزالتها، مثل الحرف "K" من أي سجل يحتوي على أوامر الدفع. [٩]

٢. **استخدام فيروسات الحاسب الآلي:** هذه الطريقة، المعروفة باسم فيروس الكمبيوتر، هي أداة واسعة الانتشار تتكون من تعليمات مشفرة مصممة لإنشاء نسخ متطابقة يمكن أن تصيب البرامج التطبيقية ومكونات النظام تلقائيًا. وهو يعمل خلال مرحلة محمية للتحكم في أداء النظام بمجرد اختراقه. وقد وصفه مركز الكمبيوتر الوطني

في الولايات المتحدة بأنه برنامج يهاجم أنظمة الكمبيوتر بطريقة تشبه الفيروسات البيولوجية التي تصيب الإنسان. يبحث الفيروس عن البرامج غير المصابة على الكمبيوتر ويكرر نفسه للتدخل فيها. عندما ينفذ البرنامج المصاب أوامر الفيروس، فإنه يُظهر قدرته على الانتشار والاختراق وتدمير النظام بأكمله في النهاية. [١٠]

٣. **هجمات إنكار الخدمة:** تتضمن هذه الهجمات السيبرانية إغراق مواقع الويب بكميات زائدة من البيانات من خلال برامج متخصصة، مما يتسبب في بطء الأداء وازدحام حركة المرور. يعيق هذا العائق وصول المستخدم إلى المواقع المتأثرة. [١١]

٤. **الهجوم الإلكتروني:** تُستخدم إجراءات مثل التشويش والخداع الإلكتروني والصواريخ المضادة للإشعاع الكهرومغناطيسي والتجسس على هدف لسرقة معلومات سرية لأغراض مختلفة سواء كانت اقتصادية أو استراتيجية أو عسكرية. قد تنطوي هذه العمليات على انتهاك للملكية الفكرية وقرصنة المعلومات والتوزيع غير المصرح به للمواد. وقد سهلت شبكة الإنترنت انتشار مثل هذه العمليات. في عام ٢٠١٤، شنت كوريا الشمالية هجومًا إلكترونيًا على شركة Sony Pictures Entertainment، مما تسبب في أضرار جسيمة وتعريض معلومات تجارية سرية للخطر. وأدى الهجوم أيضًا إلى سرقة أفلام غير منشورة وبيانات حساسة تتعلق بشخصيات وموظفين مشهورين. وكانت الهجمات الإلكترونية التي شنتها كوريا الشمالية مصحوبة بالإكراه والتهديد، مما يجعلها واحدة من أكثر الهجمات الإلكترونية تدميرا على كيان أمريكي. أثار هذا الحادث مناقشات حول التهديدات السيبرانية وأهمية تحسين تدابير الأمن السيبراني.[١٢]

لقد أدى تطور التكنولوجيا إلى تغيير جذري في الفهم التقليدي للقوة، مما أدى إلى عصر جديد حيث تشكل الهجمات السيبرانية مكونات أساسية للعمليات العسكرية عبر مختلف المجالات. يتصور جوزيف ناي القوة الإلكترونية على أنها تشمل الموارد والخبرات المتعلقة بالتحكم في الكمبيوتر وشبكات المعلومات والبنية التحتية.[١٣] يعتمد النهج المتبع في العمليات العسكرية في الفضاء السيبراني على قوة الدولة وأوامرها، بينما في الفضاء، يمكن تصنيفها إلى أربع مجموعات متميزة، لكل منها أهدافها المحددة[١٤]:

- **عمليات جمع المعلومات الاستخباراتية:** الهدف هو جمع البيانات من الأنظمة الإلكترونية للخصم. في عام ٢٠١٠، كشفت ألمانيا عن مواجهة أنشطة تجسس متطورة قامت بها الصين وروسيا، واستهدفت الصناعات الحيوية والبنية التحتية داخل البلاد، مثل شبكة الكهرباء الأساسية لعمليات الدولة وجمع البيانات.
- **عمليات تستهدف المعنويات:** الهدف هو تقويض معنويات سكان العدو وتصميمهم على الانخراط في عمليات قتالية باستخدام الدعاية والمعلومات المضللة والتكتيكات المختلفة لحرب المعلومات.
- **عمليات هجومية:** الهدف هو تعطيل أو تعطيل بيانات الخصم وأنظمته الإلكترونية، واحتمال إلحاق ضرر إضافي بأفراده أو معداته، مثل تقويض قدراته الدفاعية الإلكترونية، مثل شبكات الدفاع الجوي. ويتفق الباحثون على أن الهجوم السيبراني على إستونيا في عام ٢٠٠٧ كان من بين الهجمات الأولى من نوعها، حيث استهدف المواقع الحكومية والتجارية والمصرفية والدولية وأدى إلى خسائر مالية كبيرة وتعطيل واسع النطاق. وعلى الرغم من الشكوك التي تشير إلى موسكو، إلا أن مرتكب الهجوم لا يزال

مجهول الهوية، مما يسلط الضوء على تحديات الإسناد في الحرب السيبرانية. وقع الحادث في أعقاب الصراع الإستوني الروسي المثير للجدل، مما زاد من تعقيد الجهود المبذولة لتحديد أصول الهجوم.

- **عمليات دفاعية:** الهدف الأساسي هو حماية المعلومات الإلكترونية وشبكات الدولة، وكذلك التخفيف من المخاطر المحتملة على الأفراد والأصول.

تشتمل الوسائل والأسلحة السيبرانية على مجموعة من الخصائص المميزة، والتي يمكن تحديدها على النحو التالي:[١٥]

١. وتخضع الوسائل والأسلحة السيبرانية لعمليات تحديث وتطوير مستمرة، مما يعزز قدراتها التدميرية وفعاليتها في شن الهجمات الإلكترونية.

٢. البرنامج سهل الوصول إليه وسهل الاستخدام، مما يسمح للأفراد إما بتنزيله عبر الإنترنت أو شرائه. تمكن هذه الأداة المستخدمين من تنفيذ هجمات متطورة تتجاوز مستويات مهاراتهم الفعلية.

٣. وتتميز البرمجيات الخبيثة بالدقة والكفاءة والقدرة على اختراق مجموعة متنوعة من الأجهزة الإلكترونية، بما في ذلك أجهزة الكمبيوتر والخوادم وأي جهاز مرتبط بشبكة رقمية.

من المهم أن ندرك أن التأثيرات المباشرة للعمليات السيبرانية العسكرية على شبكات الدولة المعتدية قصيرة الأجل، وأن الاستراتيجية العسكرية التقليدية تملي هجومًا شاملاً باستخدام الأسلحة المادية للاستفادة من فوضى العدو وعجزه. إن مجرد إحداث الفوضى دون متابعة الهجوم الجسدي للقضاء على العناصر المعطلة أو السيطرة عليها يسمح للعدو بإعادة تجميع صفوفه والهجوم المضاد. ولذلك، فإن الحرب الإلكترونية تزيد من الميل نحو العمل الهجومي وتعزز عنصر المفاجأة.

المطلب الثاني: الإطار القانوني الذي يحكم أعمال العدوان والهجمات السيبرانية في القانون الدولي:

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

بدءاً بقرار الجمعية العامة بشأن وضع تعريف للعدوان، يطرح السؤال حول ما إذا كان يمكن تصنيف الهجمات السيبرانية على أنها أعمال عدوانية وفقاً للمعايير المبينة في القرار. وعلى وجه التحديد، يجب تحديد ما إذا كانت مثل هذه الهجمات تقع ضمن نطاق العدوان كما هو موضح في المادة الثالثة من القرار.

ويحدد القرار العدوان في مادته الأولى على أنه استخدام القوة المسلحة من قبل دولة ما ضد سيادة دولة أخرى أو سلامة أراضيها أو استقلالها السياسي، أو بأي شكل يتعارض مع ميثاق الأمم المتحدة. يتناول هذا التعريف على وجه التحديد الأعمال العسكرية المباشرة، باستثناء الأشكال غير المباشرة مثل التهديدات أو انتهاكات السلام. يتم تصنيف الهجمات السيبرانية على أنها عمليات عسكرية لأنها تنطوي على استخدام القوة عن بعد لإلحاق الضرر بالأصول العسكرية. كما يحدد القرار مبادئ الاستخدام الأول للقوة المسلحة والنوايا العدائية لتحديد الدول المعتدية. ومع ذلك، مع تطور التكنولوجيا وعنصر المفاجأة في الحرب الحديثة، قد يكون تطبيق هذه المبادئ أمرًا صعبًا. وفي حين أن القرار لا يذكر صراحة النية العدائية، فإنه يؤكد على أهمية البدء كعامل رئيسي في تحديد العدوان.

ولا تزال المسؤولية الصعبة تقع على عاتق مجلس الأمن في التحقق من الطرف الذي بدأ استخدام القوة في البداية. [١٦] إن تطبيق مبدأ النية العدائية على الهجمات السيبرانية يمكن أن يكشف عن النوايا العدوانية للدولة المهاجمة. وتحدد المادة الثالثة من القرار الخاص بتعريف العدوان مختلف الأفعال التي تشكل عدواناً، بغض النظر عما إذا تم إعلان الحرب رسمياً أم لا. وفي حين أن إعلان الحرب يمكن أن يشير إلى نوايا المعتدي، فإنه ليس ضروريا لإثبات العدوان. لم يتم ذكر الهجمات الإلكترونية على وجه التحديد في قائمة الأعمال العدوانية النموذجية، مما يترك مجالًا للتفسير. وتسمح المادة الرابعة لمجلس الأمن بتحديد الأفعال الأخرى التي قد تشكل عدوانا. وهذا الغموض يمكن استغلاله من قبل الدول المعتدية، خاصة في حالات العدوان غير المباشر مثل الهجمات الإلكترونية. غالباً ما يتم تنفيذ العدوان السيبراني من قبل دول قوية، بما في ذلك أعضاء مجلس الأمن الذين يتمتعون بحق النقض. وقد يكون من الصعب إثبات اتهامات العدوان السيبراني ضد مثل هذه الدول ذات النفوذ، لأنها تتمتع بنفوذ كبير في عملية صنع القرار الدولي.

علاوة على ذلك، فهي تتمتع بسلطة على التحالف العسكري العالمي الأكثر روعة، وتمتلك أكبر قوة ردع وتحافظ على وجود كبير في مناطق متعددة من العالم، بما في ذلك السيطرة على المنشآت العسكرية الأكثر أهمية من الناحية الاستراتيجية (حلف شمال الأطلسي). وعلى هذا النحو، فإن مجلس الأمن مكلف بتحديد أعمال العدوان.

ويحدد ميثاق الأمم المتحدة الحظر العام لاستخدام القوة المسلحة في العلاقات الدولية في المادة ٢ (٤)، دون تقديم تعريف واضح للقوة أو استخدامها. كما يذكر مصطلح "العدوان" في الفصل السابع، المادة ٣٩، دون تعريف له، ويشجع على الحل السلمي للنزاعات الدولية. ويؤكد الميثاق على أهمية حسن النية في العلاقات الدولية في المادة ٢ (٢)، وخاصة في سياق الدفاع عن النفس على النحو المبين في المادة ٥١ والدفاع الجماعي ردا على التهديدات أو انتهاكات السلام. إن مدى انطباق هذه الأحكام على الهجمات السيبرانية، وما إذا كان من الممكن اعتبارها أعمالاً عدوانية تستوجب الرد بموجب الميثاق، هو موضوع للنقاش. إن مسألة ما إذا كان الهجوم السيبراني يشكل "هجوماً مسلحاً" يستحق اتخاذ تدابير للدفاع عن النفس، أشبه بالهجوم العسكري التقليدي، ربما يسترشد بالحكم الذي أصدرته محكمة العدل الدولية في قضية نيكاراجوا عام ١٩٨٦.

لقد تناولت قضية نيكاراغوا المادة ٢ (٤) من ميثاق الأمم المتحدة من منظورين. أولا، أكدت محكمة العدل الدولية في الفقرة ١٨٧ من حكمها أن حظر استخدام القوة أو التهديد باستخدامها قد تطور من مبدأ إلى قاعدة دولية ملزمة لجميع الدول. وهذا يؤكد أهمية التمسك بالمبادئ الأساسية المنصوص عليها في ميثاق الأمم المتحدة. ثانيًا، أقرت المحكمة بالطبيعة الموسعة للمادة ٢ (٤) من خلال الاعتراف بأنها لا تقتصر على الاستخدامات التقليدية للقوة، مثل العمل العسكري خارج حدود الدولة. إن تفسير المحكمة بأن إرسال القوات، سواء كانت نظامية أو غير نظامية، يشكل انتهاكاً للميثاق، يبين خروجاً عن المفاهيم التقليدية لاستخدام القوة. ويعكس هذا الابتعاد نوايا الدول القوية المشاركة في صياغة المادة ٢ (٤)، كما

يتضح من الأعمال التحضيرية للميثاق. ومن المهم الإشارة إلى موقف المحكمة من هذه المادة، والذي يؤكد على أن أي تهديد باستخدام القوة أو استخدامها بين الدول الأعضاء من شأنه أن يشكل انتهاكا ويتعارض مع مبادئ الميثاق.

ومن المهم أن نلاحظ أن هذا الموقف الذي اتخذته المحكمة يأتي بعد الاعتراف بمسؤولية الدولة عن الأفعال غير المشروعة المباشرة وغير المباشرة، والتي قد تنجم عن فشلها في الوفاء بواجبها في منع إلحاق الضرر بالأفراد خارج حدودها.(١٧)

وتشير الاستنتاجات المستخلصة من أحكام المحكمة في قضية نيكاراغوا وقضية منصات النفط عام ٢٠٠٣ بين إيران والولايات المتحدة إلى أن المحكمة وسعت نطاق الإجراءات التي يمكن أن تؤدي إلى الحق في الدفاع عن النفس بموجب المادة ٥١ بما يتجاوز الهجمات العسكرية التقليدية لتشمل فئات مثل (التأثير والمقياس). ولوحظ أن الأعمال الأخرى غير الهجمات الحركية يمكن أن تشكل انتهاكًا للمادة ٤/٢ من الميثاق، كما هو موضح في القضية المتعلقة بالدعم العسكري غير المباشر الذي قدمته الولايات المتحدة إلى الجماعات المناهضة للحكومة في نيكاراغوا. وجدت المحكمة أن الولايات المتحدة تنتهك المادة ٤/٢ بسبب تورطها في دعم هذه الجماعات، وحكمت في النهاية لصالح نيكاراغوا.(١٨)

وانطلاقا من المعايير آنفة الذكر والتي استندت إليها المحكمة، فيمكن لنا أن نتخيل تصورا مشابها في حالة ادعاء دولة معينة على أخرى بشأن هجمة إلكترونية عندما تحقق هذه الهجمة معيار الحجم والتأثير على الدولة التي تتعرض للهجوم، بشرط اتصالها بالدولة المدعى عليها، إلى جانب ذلك، جاءت النسخة الأولى من دليل تالين للعام ٢٠١١ لكي تدعم هذه النتيجة حين جاءت القاعدة ١١ منه لتؤكد على أن العمليات الإلكترونية تعتبر استخداما للقوة عندما يكون مستواها وتأثيرها متقاربا مع العمليات غير الإلكترونية، ففي سياق هذا النص أقرت مجموعة من الخبراء أعدت هذا الدليل أنها قد استندت إلى معيار الحجم والتأثير في سياق تحديد فيما إذا كانت الهجمة الإلكترونية ترقى إلى استخدام غير مشروع للقوة خلافا للمادة (٤/٢)من ميثاق الأمم المتحدة، وأيضا فيما إذا كان هجوما عسكريا يبرر الدفاع عن النفس وفقا للمادة ٥١ ،وهما المعياران –ذاتهما– اللذان استندت إليهما محكمة العدل الدولية في قضية نيكاراغوا آنفة الذكر.(١٩)

المبحث الثاني: العدوان بالهجمات السيبرانية كجريمة دولية

وتتميز الجريمة الدولية بوجود عنصر متميز يعرف بالعنصر الدولي، وهو ما يميزها عن الجريمة العادية. ويشكل هذا الركن مع الركنين المادي والمعنوي المكونات العامة للجريمة الدولية. وتختلف هذه العناصر عبر أنواع مختلفة من الجرائم الدولية، مثل العدوان والإبادة الجماعية والجرائم ضد الإنسانية. وفي هذا السياق، سيتم استكشاف الأساس القانوني للعدوان السيبراني كشكل من أشكال الجريمة الدولية، بما في ذلك المعايير التي حددتها المحكمة الجنائية الدولية. بالإضافة إلى ذلك، سيتم دراسة مفهوم المسؤولية الدولية الناشئة عن الهجمات السيبرانية كشكل من أشكال العدوان.

المطلب الأول: الأساس التشريعي لجريمة العدوان عن طريق الاختراقات السيبرانية:

أولا– أحكام المحكمة الجنائية الدولية للنظر في جريمة العدوان: وقد نجحت الدول التي أيدت إدراج جريمة العدوان في نظام روما الأساسي في توسيع اختصاصات المحكمة لتشمل هذه الجريمة من خلال إدراجها في المادة ٢/٥ من نظام روما الأساسي. وكانت هذه أول حالة لنص جزائي دولي يدرج جريمة العدوان ضمن اختصاص محكمة جنائية دولية دائمة ويجرمها. وفي حين أن عدم وجود تعريف محدد يمثل تحديًا للولاية القضائية، فإنه يدل على اعتراف الدول بأن العدوان جريمة يمكن أن يرتكبها أفراد ويحاكم أمام هيئة قضائية دولية. يمكن للمحكمة أن تمارس اختصاصها على جريمة العدوان بمجرد صدور حكم يحدد الجريمة وفقا للمادتين ١٢١ و١٢٣ من النظام الأساسي للمحكمة الجنائية الدولية، ويحدد الشروط التي يمكن بموجبها للمحكمة أن تمارس اختصاصها في مثل هذه القضايا. ويجب أن يتوافق هذا الحكم مع الأحكام ذات الصلة والمبادئ المنصوص عليها في ميثاق الأمم المتحدة. يؤكد تعريف جريمة العدوان المنصوص عليه في مؤتمر كمبالا ٢٠١٠ على أن المسؤولية الجنائية الفردية عن هذه الجريمة تقتصر على القادة الذين يشاركون بشكل مباشر في التخطيط أو الإعداد أو إطلاق أو تنفيذ أعمال عدوانية تنتهك ميثاق الأمم المتحدة. وهذا يؤكد أن أولئك الذين يشغلون مناصب سلطة للسيطرة على الأعمال السياسية أو العسكرية لدولة ما هم وحدهم الذين يمكن تحميلهم المسؤولية الجنائية عن أعمال العدوان.[٢٠]

كانت هناك آراء مختلفة حول تفسير الفقرة الأولى من المادة ٨ مكرر في مؤتمر كمبالا الاستعراضي عام ٢٠١٠. ويرى البعض أن الفقرة تسلط الضوء على نقاط رئيسية، بما في ذلك شرط أن يكون العمل العدواني انتهاكا "واضحا" لميثاق الأمم المتحدة حتى يعتبر جريمة عدوان. بالإضافة إلى ذلك، يقترح التقرير أن الأفراد الذين يتمتعون بسيطرة أو توجيه كبيرين على الأعمال السياسية أو العسكرية للدولة هم وحدهم الذين يجب أن يتحملوا المسؤولية عن مثل هذه الأعمال.[٢١] ونظراً لعدم المشاركة في وضع السياسات والخطط العسكرية الكبرى، لا يمكن محاسبة الأفراد مثل الضباط والجنود والفنيين على جريمة العدوان أمام المحكمة الجنائية الدولية، حتى لو كانوا متورطين فعلياً في الفعل. تتعلق القضية المطروحة باتهام أفراد بتنفيذ هجمات فضائية (سيبرانية) من المحتمل أن تنتهك ميثاق الأمم المتحدة. في غياب تعريف مقبول عالميًا للعدوان منذ محكمة نورمبرغ، أصبح استخدام التعريف المبين في قرار الجمعية العامة للأمم المتحدة رقم ٣٣١٤ لعام ١٩٧٤ نهجًا أكثر أمانًا لمعالجة المخاوف وإرضاء جميع ممثلي الدول.[٢٢] وتعرف جريمة العدوان في الفقرة الثانية من المادة الثامنة مكرر بأنها استخدام القوة المسلحة من قبل دولة ضد سيادة دولة أخرى أو سلامة أراضيها أو استقلالها السياسي، أو انتهاكا لميثاق الأمم المتحدة. ويتوافق هذا التعريف مع قرار الجمعية العامة رقم ٣٣١٤ لعام ١٩٧٤، على الرغم من أن البعض يرى أن الإشارة إلى هذا القرار في المادة الثامنة قد تشكل تحديات من حيث الشرعية القانونية. ومن المهم أن يكون السلوك الإجرامي محدداً بوضوح في قاعدة قانونية قبل ارتكابه، انطلاقاً من مبدأ أنه لا جريمة ولا عقوبة إلا بنص قانوني. بالإضافة إلى ذلك، فإن قائمة الأعمال التي تشكل عدوانًا في المادة

الثالثة ليست شاملة، ويتمتع مجلس الأمن بسلطة تحديد ما إذا كانت الأعمال الأخرى يمكن اعتبارها عدوانًا وفقًا لميثاق الأمم المتحدة. وفي نهاية المطاف، وبموجب المادة ٣٩ من الفصل السابع، تقع على عاتق مجلس الأمن مسؤولية تقرير ما إذا كان فعل معين يشكل جريمة عدوان.

ثانيا– إن مكونات جريمة العدوان، على النحو المبين في المرفق الثاني من قرار مؤتمر كمبالا لعام ٢٠١٠ بشأن تعريف جريمة العدوان، تحدد العناصر المحددة للجريمة:

١. لقد ابتكر الفرد عملاً عدائيًا ونظمه وحرض عليه ونفذه بشكل استراتيجي.

٢. الشخص المسؤول عن الجريمة الجنائية هو الشخص الذي يشغل منصبًا ذا سلطة داخل التسلسل الهرمي السياسي أو العسكري للدولة، مما يسمح له بالإشراف على العمل العدواني وتنظيمه.

٣. لقد انخرطت دولة ما في عمل عدواني من خلال استخدام القوة المسلحة ضد دولة أخرى، منتهكة بذلك المبادئ المنصوص عليها في ميثاق الأمم المتحدة المتعلقة بالسيادة والسلامة الإقليمية والاستقلال السياسي.

٤. وكان لدى الجاني معرفة بالظروف التي يمكن التحقق منها والتي تثبت أن استخدام القوة المسلحة بهذه الطريقة ينتهك المبادئ المنصوص عليها في ميثاق الأمم المتحدة.

٥. إن العمل العدواني، بسبب طبيعته المتأصلة وشدته ومداه، ينتهك بشكل لا لبس فيه المبادئ المنصوص عليها في ميثاق الأمم المتحدة.

ثالثا/ الأركان الخاصة بجريمة العدوان بالهجمات السيبرانية: باختصار، يتم تحديد السمات المميزة لجريمة العدوان من خلال التوغلات السيبرانية بناءً على سلسلة من السمات المميزة التي يجب أن تظهرها الهجمات الإلكترونية حتى تعتبر بمثابة اعتداء مسلح. وسيتم الآن شرح هذه المعايير، كما وردت في دليل "تالين".

١. يتضمن العنصر الإجرامي للعدوان في المكونات الثلاثة الأولية أعمالًا نشطة غير قانونية ومعادية تجاه أراضي أو قوات دولة أخرى. إن ممارسة القوة دفاعاً عن النفس، وفقاً لحق الدفاع المشروع المنصوص عليه في المادة ٥١ من ميثاق الأمم المتحدة، لا تعتبر غير قانونية ولا تعتبر عدواناً. وكذلك فإن مجرد التهديد باستخدام القوة أو فرض عقوبات اقتصادية أو قطع العلاقات الدبلوماسية لا يستوفي معايير العدوان، وبالتالي يبطل الجانب المادي لجريمة العدوان. كما ورد في دليل تالين، وضعت اللجنة معيارا أساسيا لتعريف الهجوم العسكري على أساس الأذى الجسدي، سواء للأفراد أو الممتلكات. ويعتبر الدليل أن العمليات الإلكترونية لا تشكل هجومًا عسكريًا إلا إذا أدت إلى مثل هذا الضرر، باستثناء الإجراءات التي لا تسبب ضررًا جسديًا. ومع ذلك، فإن العمليات الإلكترونية التي تعرض المصالح الوطنية الحساسة للدولة المستهدفة للخطر، حتى في حالة عدم وجود أضرار مادية ملموسة، قد تظل مصنفة على أنها هجوم عسكري.

٢. يتطلب الجانب الأخلاقي لجريمة العدوان، المبين في البندين الرابع والسادس، أن يكون لدى مرتكب الجريمة معرفة بالظروف الواقعية التي تثبت أن استخدام القوة المسلحة ينتهك سيادة دولة أخرى أو سلامة

أراضيها أو استقلالها السياسي، ويؤدي إلى انتهاك سيادة دولة أخرى أو سلامة أراضيها أو استقلالها السياسي. فقدان أرواح مواطنيها، أو تتعارض بأي شكل من الأشكال مع مبادئ وأهداف وأحكام ميثاق الأمم المتحدة. ومن الضروري التحقيق في نية الجناة لتحديد مدى أفعالهم، وجمع الأدلة والقرائن القاطعة لإثبات وقوع العدوان، وتحديد الجهة المسؤولة، وإثبات القصد الجنائي.

واستنادا إلى المبادئ المبينة في دليل تالين، فإن وجود العداء هو عامل رئيسي في تحديد طبيعة العمليات الإلكترونية. عندما تكون الدولة المهاجمة قادرة على إثبات أن العملية الإلكترونية تتم بنوايا عدائية، مثل تقويض القدرات العسكرية للدولة المستهدفة من خلال التلاعب بأنظمتها الإلكترونية، يمكن اعتبار ذلك بمثابة عبور عتبة الهجوم المسلح. ويتجلى ذلك من خلال استهداف الشبكات الإلكترونية الآمنة والمحمية، خاصة تلك المتعلقة بالعمليات العسكرية، مما يدل على وجود نية استراتيجية وراء العملية. ويرتبط مستوى حماية الشبكة الإلكترونية المستهدفة بشكل مباشر بتحديد العداء، على النحو المبين في دليل تالين.

ويتجلى الجانب الدولي لهذه الجريمة في التركيز على البنود الثالثة والرابعة والخامسة التي تنص على أن استخدام القوة المسلحة من قبل دولة ضد أخرى يشكل انتهاكا للمصالح والمبادئ الدولية المنصوص عليها في ميثاق الأمم المتحدة. ويشمل هذا الانتهاك حظر استخدام القوة في حل النزاعات وتعزيز الحل السلمي للصراعات، فضلاً عن احترام سيادة كل دولة واستقلالها السياسي. وبالإضافة إلى ذلك، فهي تنطوي على دعم أهداف الأمم المتحدة، وخاصة صون السلام والأمن الدوليين.

وفي إطار تطبيق المحكمة الجنائية الدولية لهذا المعيار، فإنه يتعين اعتبار أن عمل العدوان يجب أن يتم باسم الدولة، كجزء من خطتها، أو برضاها ضد دولة أخرى، بأوامر. لهجمات عسكرية قادمة من أعلى سلطاتها. إن عضوية الدولة المعتدية أو اعترافها بها في الأمم المتحدة لا يؤثر على المعايير القانونية لمحاسبة الأفراد على ارتكاب جريمة العدوان. يقتصر اختصاص المحكمة الجنائية الدولية في محاكمة هذه الجريمة على الدول، ويستبعد صراحة الجهات الفاعلة غير الحكومية مثل الجماعات الإرهابية المسلحة. [٢٣]

وفي سياق تنفيذ دليل تالين، اعترفت اللجنة ضمنيًا في الفقرة الثانية من القاعدة ١٣ بأن السيطرة الفعالة ضرورية لتحمل المسؤولية في التصدي للدولة المسؤولة عن الهجوم. كما حددت اللجنة معايير إضافية، بما في ذلك الحاجة إلى الوضوح في تحديد تأثير الهجمات والقدرة على قياسه. ويشمل ذلك اشتراط قيام الدولة المهاجمة بتقييم الضرر الناجم عن الهجوم الإلكتروني، وكذلك اشتراط أن تكون العملية ذات طبيعة عسكرية، بما يتماشى مع مبادئ ميثاق الأمم المتحدة فيما يتعلق باستخدام القوة وارتباطها. للأنشطة العسكرية.

العنصر القانوني هو عنصر أساسي ينطبق على جميع حالات الجرائم الدولية، بغض النظر عن الجريمة المعنية على وجه التحديد. ولا يجوز محاكمة الأفراد ومعاقبتهم إلا على الجرائم المنصوص عليها صراحة في المادة ٥ من النظام الأساسي للمحكمة الجنائية الدولية. وبالتالي، فإن الالتزام بمبدأ "لا جريمة ولا عقوبة إلا بقانون" – لا جريمة ولا عقوبة بدون قانون – أمر بالغ الأهمية، سواء في سياق القانون الجنائي المحلي أو الدولي.

يقودنا تحليلنا إلى استنتاج مفاده أن المحكمة الجنائية الدولية تطبق عناصر الجرائم المنصوص عليها في نظامها الأساسي عند التعامل مع أعمال العدوان. بالإضافة إلى ذلك، فإنها تلتزم بالقواعد الإجرائية، وقواعد الإثبات، والمعاهدات ذات الصلة، ومبادئ القانون الدولي العام والقانون الإنساني المطبق في النزاعات المسلحة. كما تتناول المبادئ القانونية العامة المستمدة من القوانين الوطنية، طالما أنها لا تتعارض مع القواعد الدولية الراسخة. نظرًا لغياب قوانين دولية محددة تحكم الحرب السيبرانية أو الهجمات السيبرانية، خصص فريق من الخبراء القانونيين وقتًا كبيرًا لتوضيح تطبيق القانون الدولي في سياق الحرب الرقمية. وقد توجت هذه الجهود بإنشاء دليل غير ملزم للحرب السيبرانية يُعرف باسم دليل تالين، والذي تم تطويره بالتعاون مع مركز التميز للدفاع السيبراني التعاوني التابع لمنظمة حلف شمال الأطلسي (CCDCOE) في تالين، إستونيا.

المطلب الثاني: المسؤولية العالمية الناجمة عن أعمال العدوان عبر الحرب السيبرانية.

ويعتبر العمل العدواني جريمة دولية لما يترتب عليه من آثار قانونية بموجب القانون الدولي والحقوق والواجبات المنصوص عليها في ميثاق الأمم المتحدة. إن قرار الجمعية العامة بشأن العدوان يعرفه بأنه جريمة ضد السلام الدولي، يعترف بها القانون. تتمتع المحكمة الجنائية الدولية بالولاية القضائية على العدوان عندما يتم تعريفه على أنه جريمة وفقا لنظامها الأساسي. وتحمل جريمة العدوان مسؤولية قانونية دولية مدنية وجنائية. وتنطوي المسؤولية المدنية على قيام الدولة بتعويض الضرر الناجم عن أفعالها غير القانونية، في حين تنشأ المسؤولية الجنائية عن خرق الالتزامات القانونية في القانون الدولي. (٢٤)

إن القيام بأي عمل عدواني يشكل انتهاكا لالتزام قانوني دولي. من خلال التصديق على معاهدات مثل ميثاق الأمم المتحدة التي تحظر صراحة استخدام القوة في الشؤون الدولية والعدوان، فإن أي دولة تشارك في مثل هذه الاتفاقيات تتحمل المسؤولية عن ارتكاب عمل من أعمال العدوان. ويؤدي هذا الانتهاك للالتزام إلى المسؤولية القانونية للدولة المخالف.(٢٥)

أما المسؤولية الجنائية فهي تعني عموماً أن الشخص يجب أن يتحمل نتائج فعله الإجرامي بأن يخضع للعقوبة التي ينص عليها القانون على هذا الفعل. المسؤولية الجنائية الدولية تعني مساءلة الدولة عن ارتكاب فعل يعتبر جريمة دولية بموجب القانون الدولي ومعاقبتها من قبل المجتمع الدولي بالعقوبات المقررة للجريمة الدولية المرتكبة وإخضاعها لعقوبات تكفل ردعها عن تكرارها. جريمتها الدولية. شروط المسؤولية الدولية هي كما يلي:

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

وفي تحليل العلاقة بين معايير إسناد المسؤولية الدولية والهجمات الإلكترونية، من الواضح أن ارتكاب مثل هذه الهجمات من قبل كيان حكومي لا يستوفي الشرط الأول، لأنه يشمل جهة فاعلة من غير الدول، وبالتالي يحول دون إنشاء محكمة دولية. مسؤولية. والشرط الثاني، وهو ما يتعلق بوقوع الضرر، له أهمية قصوى. تشكل الهجمات الإلكترونية تهديدًا كبيرًا للأمن الدولي والمصالح الاستراتيجية، مما يؤدي إلى أضرار لا مفر منها عند تنفيذها على نطاق واسع. ويشكل هذا الضرر مبررًا أساسيًا لتحديد المسؤولية، لا سيما في سياق الهجمات التي تستهدف مصالح دولية قيمة وحاسمة. علاوة على ذلك، فإن عدم قانونية الهجمات الإلكترونية، التي تتعارض مع المبادئ الراسخة للقانون الدولي العام من خلال انتهاك أسرار الدولة ومصالحها، يؤكد انتهاكها للمعايير القانونية الدولية. ويطرح هذا الشكل الناشئ من الحرب تحديات وتعقيدات جديدة على الساحة الدولية، مما يسلط الضوء على الحاجة الملحة لمعالجة انتشار الأسلحة التقنية المتقدمة.[٢٦]

بعد العرض السابق، نوجه اهتمامنا إلى النتائج المتعلقة بمكونات ومعايير المسؤولية الدولية. ومما له أهمية قصوى المبدأ القائل بأن انتهاك التزام دولي يؤدي إلى مسؤولية دولية، مما يتعارض مع قواعد القانون الدولي التي تفرض تعويضات عن الضرر الناجم عن أفعال تنتهك أحكام القانون الدولي. ومن الأهمية بمكان أن نلاحظ أن المسؤولية الدولية لا تتحقق إلا في ظل وجود ضرر فعلي. ومن ثم، فإن وقوع الضرر يعتبر بمثابة المعيار الأساسي لنسب المسؤولية وضرورة الرد.

وتنشأ المسؤولية عن الجرائم الدولية من انتهاك الالتزامات الدولية الهامة التي تعتبر ضرورية لحماية المصالح الأساسية للمجتمع العالمي. يتم الاعتراف عالميًا بهذه الانتهاكات على أنها أعمال إجرامية ويتم تصنيفها على أنها جرائم دولية. إن انتهاكات الالتزامات الحاسمة، مثل تلك المتعلقة بسيادة الدول واستقلالها، والحق في تقرير المصير، وحظر العبودية والإبادة الجماعية، وحماية البيئة، تلعب دورا حيويا في دعم السلام والأمن الدوليين. إن هذه الجرائم الدولية، بما فيها الهجمات الإلكترونية التي تعرض السلام والأمن للخطر، وتهدد حقوق الإنسان ورفاهية الأفراد، وتتحدى سيادة الدولة، وتضر بالبيئة التي يقيم فيها البشر. إن حدوث مثل هذه الهجمات يمكن أن يؤدي إلى أضرار جسيمة مماثلة لتلك التي تسببها مختلف الجرائم الدولية الأخرى.

لقد اعتمد الأساس القانوني للمسؤولية الدولية تاريخياً على مفاهيم الخطأ والمخاطر في القانون الدولي التقليدي. ومع ذلك، في القانون الدولي المعاصر، ينصب التركيز الأساسي للمسؤولية الدولية على الأفعال الدولية غير المشروعة. عندما تشارك دولة ما في أنشطة ذات طبيعة خطرة وغير مألوفة، فقد تكون مسؤولة عن أي ضرر يلحق بالدول الأخرى. ومما يثير الاهتمام بشكل خاص دراسة الآثار المترتبة على التقدم العلمي والتكنولوجي، بما في ذلك أنشطة مثل عمليات الإنترنت، والتي يمكن تصنيفها على أنها مخاطر دولية. في الحالات التي تُتهم فيها دولة ما بارتكاب هجوم إلكتروني دولي، فقد تخضع للمسؤولية الدولية.

الخاتمة

العدوان السيبراني هو شكل من أشكال الجريمة الدولية التي تنطوي على استخدام دولة للقوة غير التقليدية ضد دولة أخرى، مما يؤثر على سيادتها واستقلالها السياسي. ويعتمد هذا النوع من العدوان على التكنولوجيا المتصلة بالإنترنت، مما يشكل تحديات مثل صعوبة الكشف وقدرة الجناة على استغلال تكنولوجيات المعلومات لاختراق أنظمة أمن الشبكات. على الرغم من عدم وجود مبادئ توجيهية قانونية دولية محددة تتناول الهجمات السيبرانية، فمن المهم الاعتراف بأهميتها في مجال القانون الدولي.

النتائج:

١. يمثل استخدام الهجمات السيبرانية قدرة تدميرية كبيرة لديها القدرة على تجاوز تأثير العمليات العسكرية التقليدية. وتظهر هذه الهجمات مستوى عالٍ من الدقة في استهداف الكيانات المدنية والعسكرية على حد سواء.

٢. تعتبر الهجمات السيبرانية شكلاً من أشكال العدوان غير المباشر وهي مدرجة ضمن معايير تعريف الجمعية العامة للعدوان على النحو المبين في القرار ٣٣١٤ لعام ١٩٧٤. ويرجع ذلك إلى أن مثل هذه الأعمال تمثل انتهاكًا كبيرًا للمبادئ الراسخة في الأمم المتحدة. ميثاق الأمم.

٣. إن العدوان السيبراني هو جريمة عابرة للحدود الوطنية تشمل عناصر مختلفة، ترتكز على فقه المحكمة الجنائية الدولية وتستند إلى المبادئ المبينة في دليل تالين. على الرغم من أن هذه الوثيقة ليست ملزمة قانونًا، إلا أنها بمثابة مرجع أساسي لمعالجة الحرب السيبرانية.

٤. ويعتبر ارتكاب الهجمات السيبرانية عملاً من أعمال العدوان بموجب القانون الدولي العام، مما يؤدي إلى مسؤولية قانونية دولية محتملة، بما في ذلك المسؤولية المدنية للدول والمسؤولية الجنائية للأفراد.

التوصيات:

١. توسيع نطاق تعريف العدوان في الجمعية العامة ليشمل العوامل المتطورة المتعلقة بالهجمات الإلكترونية.

٢. وفي حال ثبت أن برمجة الاتفاقيات الدولية للحد من استخدام تكنولوجيا المعلومات للهجمات السيبرانية يمثل تحديًا في إطار الالتزام بمبادئ القانون الدولي، فإن إبرام مثل هذه الاتفاقيات قد يكون معقدًا.

٣. يجب على لجنة أركان الحرب التابعة لمجلس الأمن إعطاء الأولوية لدمج الهجمات السيبرانية في القدرات العسكرية للدول، مع التركيز على التهديدات الكبيرة التي تشكلها على المجتمع العالمي والإنسانية ككل.

٤. إنشاء منظمة دولية تتألف من محترفين ومتخصصين في مجال الأمن السيبراني لتحديد وتخفيف الهجمات السيبرانية، فضلا عن تقديم الدعم الفني للدول المعرضة لمثل هذه الهجمات، على الرغم من الأضرار الناجمة عن الحوادث السيبرانية السابقة.

٥. الاعتراف بمساءلة الدولة عن تصرفات الأفراد أو الجماعات التي تعمل نيابة عنها أو تحت سلطتها، بما في ذلك جميع المكونات المشاركة في البرامج الإلكترونية التي تنتهك الالتزامات الدولية، بالإضافة إلى المسؤولية الفردية، وتسهيل ملاحقة المسؤولين عن توجيه الجرائم. مرتكبي جريمة العدوان المباشرين.

٦. وينبغي للمجتمع الدولي أن يكثف جهوده للحد من انتشار مثل هذه الأشكال من العدوان، وتحديدا الهجمات السيبرانية.

الهوامش:

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

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

(٣) المرجع السابق، ص١٠٨.

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

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

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

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

(٨) احمد عبيس نعمة الفتيلاوي، الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مرجع سبق ذكره، ص٦١٥.

(٩) محمد عبدالله ابوبكر، جرائم الكمبيوتر والانترنيت، منشأة المعارف، الاسكندرية، ٢٠٠٦، ص٤٠.

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

(١١) المرجع السابق، ص٦٨.

(١٢) محمد عبدالله ابوبكر، جرائم الكمبيوتر والانترنيت، مرجع سبق ذكره، ص٥٥.

(١٣) جون باسيت، حرب الفضاء الإلكترونية: التسلح وأساليب الدفاع الجديدة، الحروب المستقبلية في القرن الواحد والعشرين، ط١، مركز الإمارات للدراسات والبحوث الإستراتيجية،٢٠١٤، ص٥٧.

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

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

(١٦) أ. د. صلاح الدين احمد حمدي، دراسات في القانون الدولي العام، دراسات في القانون الدولي العام، ط١، منشورات ELGA، مالطا،٢٠٠٢، ص ٢٧٧:٢٧٣.

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

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

(١٩) نفس المرجع، ص٣٤٩.

(٢٠) علي جميل حرب، منظومة الفضاء الجزائي الدولي للمحاكم الجزائية الدولية والجرائم الدولية المعتبرة، مرجع سبق ذكره، ص٢٢٨.

(٢١) كمال حماد، النزاع المسلح والقانون الدولي العام، ط١، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت،١٩٩٧، ص٣١.

(٢٢) كمال حماد، النزاع المسلح والقانون الدولي العام، مرجع سبق ذكره، ص٣٢.

(٢٣) إبراهيم الدراجي، جريمة العدوان ومدى المسؤولية القانونية الدولية عنها، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٥، ص٥٢٤.

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

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

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

قائمة المصادر

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

٢) احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل، كلية القانون، العدد الرابع–السنة الثانية،٢٠١٦.

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

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

٥) جون باسيت، حرب الفضاء الإلكترونية: التسلح وأساليب الدفاع الجديدة، الحروب المستقبلية في القرن الواحد والعشرين، ط١، مركز الإمارات للدراسات والبحوث الإسترتيجية،٢٠١٤.

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

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

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

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

١٠) علي جميل حرب، منظومة الفضاء الجزائي الدولي للمحاكم الجزائية الدولية والجرائم الدولية المعتبرة،

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

١٢) محمد عبدالله ابوبكر، جرائم الكمبيوتر والانترنيت، منشأة المعارف، الاسكندرية، ٢٠٠٦.

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

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