مجلة جامعة الشارقة للعلوم القانونية

اسم المقال: المسؤولية الدولية عن الهجمات السيبرانية الواقعة من كيانات من غير الدول
اسم الكاتب: حليمة صالح الدرمكي، وائل أحمد علام
رابط ثابت: https://political-encyclopedia.org/index.php/library/8717
تاريخ الاسترداد: 2026/11/02 01:09 +03

الموسوعة السياسيّة هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترنت.
لمزيد من المعلومات حول الموسوعة السياسيّة – Encyclopedia Political، يرجى التواصل على info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسيّة – Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام المتاحة على الموقع https://political-encyclopedia.org/terms-of-use

تم الحصول على هذا المقال من موقع مجلة جامعة الشارقة للعلوم القانونية ورفده في مكتبة الموسوعة السياسيّة مستوفياً شروط حقوق الملكية الفكريّة ومتطلبات رخصة المشاع الإبداعي التي ينضوي المقال تحتها.

جامعة الشارقة
UNIVERSITY OF SHARJAH

مجلة جامعة الشارقة

مجلة علمية محكمة

للعلوم القانونية



المجلد 21، العدد 4
جمادي الثاني 1446هـ / ديسمبر 2024م

المجلد 21، العدد 4
جمادي الثاني 1446هـ / ديسمبر 2024م

الترقيم الدولي المعياري للدوريات 2616-6526

سبتمبر 2024م مجلة جامعة الشارقة للعلوم القانونية المجلد 21 العدد 4
https//:doi.org/10.36394/jls.v21.i4.18

المسؤولية الدولية عن الهجمات السيبرانية الواقعة من كيانات من غير الدول

حليمة صالح الدرمكي[1]
وائل أحمد علام[2]

تاريخ الاستلام: 09-09-2023 تاريخ القبول: 30-10-2023

ملخص البحث:

شهدت العقود الأخيرة وقوع هجمات سيبرانية من كيانات من غير الدول (الأفراد، والجماعات، والمنظمات)؛ كتلك التي وقعت في جورجيا واستونيا.

وتُعَدُّ هذه الهجمات أكثر تعقيدا من الهجمات السيبرانية التي ترتكبها الدول، وفي الوقت نفسه، توازيها في الخطورة.

وتؤدي هذه الهجمات إلى حدوث أضرار جسيمة بالمصالح الحيوية للدول؛ كشبكات الاتصال، ومحطات الكهرباء والماء، وقطاع النقل، والصحة، والتي تعمل إلكترونيًا، بهدف تعطيلها أو تدميرها كليا أو جزئيا. ولهذا، يهدُف البحث إلى بيان المسؤولية الدولية الناشئة عن هذه الهجمات؛ فيُبين البحث مسؤولية الدولة التي منها مارست الكيانات غير الحكومية الهجمات السيبرانية، وكذلك مسؤولية هذه الكيانات. ويوضح البحث هذه المسؤولية في إطار قواعد القانون الدولي العام.

ويخلُص البحث إلى أنه تُنسب الهجمات السيبرانية الواقعة من كيانات من غير الدول إلى هذه الكيانات إذا قامت بها على نحو مستقل عن أية دولة. ومن ثم، تتقرر المسؤولية الدولية الجنائية بشأن أفراد هذه الكيانات. وتُنسب إلى الدولة إذا كانت الكيانات تخضع لتوجيهات الدولة أو تعليماتها أو سيطرتها، أو كانت الدولة لا تبذل العناية الواجبة لوقف هذه الجهات. ومن ثم، تتقرر المسؤولية الدولية للدولة؛ فتلتزم بوقف هذه الهجمات، وبجبر الضرر الحادث بسببها.

ويوصي البحث بوضع وثيقة قانونية مُلزِمَة تتضمن أحكاما وقواعد تتعلق بتنظيم المسؤولية الدولية عن هذه الهجمات السيبرانية

الكلمات الدالة: الهجمات السيبرانية، المسؤولية الدولية الجنائية، الكيانات من غير الدول، الأمن السيبراني، الفضاء السيبراني.

---

(1) كلية القانون – جامعة الشارقة (الشارقة – الإمارات العربية المتحدة)
wallam@sharjah.ac.ae

(2) كلية القانون – جامعة الشارقة (الشارقة – الإمارات العربية المتحدة)

المقدمة

باتت الهجمات السيبرانية التي ترتكبها الكيانات من غير الدول حقيقة واقعية في العالم المعاصر. ومن أمثلة ذلك، الهجمات السيبرانية التي شارك فيها الأفراد بجانب القوات المسلحة ضد جورجيا واستوينا؛ ففي جورجيا عام 2008، بدأت الحرب بين جورجيا وروسيا عندما استقلت أوستيتا الجنوبية عن جورجيا، وسبق الحرب بين الدولتين بيوم واحد وقوع هجمات سيبرانية ضربت البنية التحتية في جورجيا، وقطعت اتصالها مع الدول الأخرى (خليفة، 2021، ص 99 – 105). وفي استوينا عام 2007 وقع هجوم سيبراني ضدها من روسيا الاتحادية (ثامر، 2015، ص 35؛ Clover, 2007, p: 8) ويعد هذا الهجوم أبرز مثال على مشاركة متطوعين غير عسكريين في هجمات سيبرانية (Schmidt, 2013, pp. 3 -1). وكذلك، الهجمات السيبرانية التي شنتها أوكرانيا أثناء الغزو الروسي لشبه جزيرة القرم في عام 2014.

والغالبية من الهجمات السيبرانية قد حدثت على الأرجح من الجهات الفاعلة من غير الدول. (McReynolds, 2015, p.428) فلقد استفادت هذه الكيانات من التطور التكنولوجي الكبير في مجال الاتصالات والكمبيوتر والإنترنت، فاستخدمته في تهديد المصالح العسكرية والسياسية والاقتصادية للدول، من خلال التَّسَلُّل إلى الأنظمة الإلكترونية الخاصة بحماية وتنظيم عمل المنشآت الحيوية (كمحطات الكهرباء والمياه، ومحطات الطاقة النووية، والسدود، ووسائل النقل)، والسيطرة عليها والتحكم فيها، ومن ثم، تعطيلها كليا أو جزئيا، مما يؤدي إلى وقوع أضرار وخسائر في الأرواح، أو الممتلكات، أو البيئة، أو غير ذلك

ويمثل التعامل مع الهجمات السيبرانية الواقعة من كيانات من غير الدول في الفضاء الإلكتروني تحديا للقانون الدولي، لا سيما وأن الحكومات قد تختبئ وراء هذه الكيانات التي تظهر في العلن على أنها تعمل بشكل مستقل، بينما هي في واقع الأمر تابعة للحكومة

وعليه، يسعى هذا البحث إلى تحديد المسؤولية الدولية عن الهجمات السيبرانية الواقعة من هذه الكيانات، ودور القانون الدولي في محاسبة هذه الكيانات، وتحديد مسؤولية الدول التي تقف وراءها

مشكلة البحث:

تكمن مشكلة الدراسة في زيادة الهجمات السيبرانية من قبل الكيانات من غير الدول سواء في أوقات السلم أو النزاعات المسلحة، بما يهدد السلم والأمن الدوليين، وينتهك قواعد القانون الدولي، وعلى وجه الخصوص القانون الدولي الإنساني والقانون الدولي الجنائي، بل والقانون الدولي لحقوق الانسان، ويؤدي إلى إصابات ووفيات بين المدنيين وتدمير للأعيان المدنية.

وعلى الرغم مما سبق، لا توجد معاهدة دولية واضحة تتعلق بالهجمات السيبرانية، ومن ثم، يمكن أن تستغل الكيانات من غير الدول هذا الفراغ التشريعي للإفلات من المسؤولية

وبناء عليه، تتمحور الإشكالية الرئيسة لدراستنا الحالية في التساؤل الآتي: ما المسؤولية الدولية عن الهجمات السيبرانية الواقعة من كيانات من غير الدول؟ بتعبير آخر، هل تنشأ عن هذه الهجمات مسؤولية دولية مدنية على الدولة؟ وكذلك، مسؤولية دولية جنائية على الأفراد؟

أهداف البحث:

يهدُف البحث إلى بيان المسؤولية الدولية الناشئة عن الهجمات السيبرانية التي تقوم بها كيانات من غير الدول. ويؤكد البحث على أهمية مبادئ السيادة والمسؤولية الدولية عند مواجهة الهجمات السيبرانية من غير الدول. ولهذا، يُبين البحث مدى إمكانية تطبيق قواعد المسؤولية الدولية المعروفة على الهجمات السيبرانية الواقعة من كيانات من غير الدول، وأثر التمسك بمبدأ السيادة على قيام المسؤولية الدولية في مثل هذه الحالات

منهج البحث:

اتبع البحث المنهجين الآتيين:

1. **المنهج الوصفي:** من خلال التعريف بقواعد المسؤولية الدولية للدولة، وللكيانات من غير الدول، عن الهجوم السيبراني وآثارها.
2. **المنهج التحليلي:** من خلال جمع الحقائق والمعلومات، ومناقشة النصوص القانونية التي تحدد المسؤولية الدولية عن الهجمات السيبرانية للكيانات من غير الدول، إضافة إلى تحليل الاتجاهات الفقهية والتطبيقات القضائية بغرض الوصول لأهداف البحث والعمل على استخلاص أهم القواعد والأحكام التي ترتبط بالموضوع.

خطة البحث:

للوصول إلى هدف البحث قسمنا البحث ثلاثة مباحث؛ تناول كل واحد منها مسألة معينة ضرورية لتحديد المسؤولية الدولية الناشئة عن الهجمات السيبرانية التي تقوم بها كيانات من غير الدول. فيُبين المبحث التمهيدي بإيجاز مفهوم الهجوم السيبراني، ومفهوم الكيانات من غير الدول. ويعرض المبحث الأول للمسؤولية الدولية للدولة عن الهجمات السيبرانية للكيانات من غير الدول؛ فهو يوضح متى تنشأ مسؤولية الدولة عن هذه الهجمات، ويتعمق في جوهر شروط مسؤولية الدولة، والآثار المترتبة عليها. ويتناول المبحث الثاني المسؤولية

الدولية للكيانات من غير الدول عن الهجمات السيبرانية، فيسلط الضوء على المشكلة، ويقترح ضرورة إصدار وثيقة دولية تتعلق بمسؤوليتها. ومن ثم، جاء تقسيم البحث على النحو التالي:

مبحث تمهيدي: ماهية الهجوم السيبراني الواقع من كيانات من غير الدول.

المطلب الأول: مفهوم الهجوم السيبراني،

المطلب الثاني: مفهوم الكيانات من غير الدول.

المبحث الأول: المسؤولية الدولية للدولة عن الهجمات السيبرانية للكيانات من غير الدول

المطلب الأول: إسناد الهجمات السيبرانية (الواقعة من كيانات من غير الدول) للدولة.

المطلب الثاني: الآثار المترتبة على مسؤولية الدولة عن الهجمات السيبرانية الواقعة من الكيانات غير الدول

المبحث الثاني: المسؤولية الدولية للكيانات من غير الدول عن الهجمات السيبرانية

المطلب الأول: إسناد الهجمات السيبرانية للكيانات من غير الدول،

المطلب الثاني: المسؤولية الدولية الجنائية للكيانات من غير الدول عن الهجمات السيبرانية

الخاتمة وتتضمن النتائج والتوصيات.

مبحث تمهيدي: ماهية الهجوم السيبراني الواقع من كيانات من غير الدول

مع التطور العلمي الكبير في مجال الحاسوب والإنترنت، نشأت فكرة الهجوم السيبراني (الشرقاوي، 2021، ص 69)، لا سيما مع تزايد الاعتماد على الأنظمة المعلوماتية والأجهزة المتصلة بالإنترنت (الردايدة، 2013، ص15 - 17). فقد شهد العالم نشأة عالم افتراضي؛ وهو الفضاء السيبراني، وفي إطاره نشأ سباق تسلح غير تقليدي يتمثل في استحداث برامج تقنية إلكترونية متطورة تقوم بهجمات سيبرانية (كاظم، 2019، ص 19). ومن ثم، أصبح الفضاء الإلكتروني المجال الخامس بعد المجالات التقليدية الأربعة (الجو والأرض والفضاء والبحار) كساحة جديدة للحروب والنزاعات الدولية (القريطي، 2022، ص 69)

وفي البَدء، كان الهجوم السيبراني تقوم به الدولة لما يتوفر لديها من إمكانيات تكنولوجية كبيرة، لكن مع تقدم التكنولوجيا وسهولة التوصل لها، أصبح من الممكن أن تقوم به كيانات من غير الدول

وقبل الخوض في بيان المسؤولية الدولية عن الهجوم السيبراني، نوضح في هذا المبحث التمهيدي المقصود بالهجوم السيبراني، وكذلك، المقصود بالكيانات من غير الدول. وعليه، نتناول هذا المبحث في المطلبين الآتيين:

المطلب الأول: مفهوم الهجوم السيبراني،

المطلب الثاني: مفهوم الكيانات من غير الدول.

المطلب الأول: مفهوم الهجوم السيبراني

حتى وقت قريب، لم يكن الهجوم السيبراني معروفا، وإنما ظهر وتطوَّر بدرجة ملحوظة في العقود الأخيرة (الفتلاوي، 2016، ص624). وتُعد الهجمات التي تعرضت لها جمهورية استونيا - إحدى جمهوريات الاتحاد السوفيتي السابق - في عام 2007 بداية ظهور الهجمات السيبرانية على الصعيد الدولي حيث تعرضت لهجمات سيبرانية من قبل روسيا - حسب اتهامات استونيا لها - كرد فعل على رفع تمثال من العاصمة تالين، لكن روسيا لم تعترف بذلك رسميا. وقد شارك في تنفيذ هذه الهجمات أفراد وميلشيات (الفتلاوي، 2016، ص624). فتم تنفيذ الهجمات من خلال إصدار أوامر لآلاف من مستخدمي أجهزة الكومبيوتر في مناطق مختلفة من العالم للمشاركة بتنفيذ هجوم سيبراني - من نوع رفض الخدمة (DOS) – موجه ضد أنظمة إستونيا، وتم تعطيل الخدمة في البنية التحتية السيبرانية، إضافة إلى هجمات تشويش وعرقلة الخدمة (Clarke, & Nick, 2012, p. 28)

ثم تلا ذلك، حدوث هجمات سيبرانية عديدة، لعل من آخرها الهجمات السيبرانية في النزاع الروسي الأوكراني (2022) الذي ما زال مستمرًا حتى الآن، والذي استخدمت فيه كافة أنواع الأسلحة التقليدية والسيبرانية (القريطي، 2022، ص 22)

والهجوم السيبراني فعل أو أفعال تتم في عالم افتراضي حيث يتم استخدام بيانات رقمية ووسائل اتصال تعمل إلكترونيًا. وقد تطوَّر الهجوم السيبراني ليتضمن مفهومًا أوسع يستهدف تحقيق أهداف عسكرية أو أمنية ملموسة ومباشرة (Clarke, R., & Nick, R. 2012, p. 28)، عن طريق اختراق مواقع إلكترونية حساسة، كأنظمة حماية محطات الطاقة النووية أو الكهربائية أو المطارات ووسائل النقل الأخرى (saalbach, 2014, P. 6).

والهجمات السيبرانية واسعة النطاق؛ أي أنها هجمات لها تأثير كبير على المصالح الحيوية في الدولة، كأن تستهدف البنى التحتية في الدولة (كالمستشفيات والسدود ومحطات توليد الطاقة وغيرها)، أو تكون الهجمات السيبرانية جزءا من تنفيذ عمليات عسكرية (كإيقاف أجهزة الرادارات والإنذار المبكر). ومن ثم، لا تشمل الأنشطة السيبرانية صغيرة النطاق مثل أنشطة الجرائم السيبرانية الشائعة بهدف ابتزاز الأفراد وسرقة الحسابات

وقد شَكَّلَ ظهور الهجوم السيبراني تحديًا كبيرًا للباحثين في القانون الدولي (حسن، 2021، ص25) إذ يجب تحديد هذا المفهوم حتى يتسنى وضع قواعد لتنظيمه أو تقييده، لمواجهة المخاطر المترتبة عليه (الشرقاوي، 2021، ص 69). ويتعين تحديد هذا المفهوم على وجه الخصوص في ضوء تزايد اللجوء إلى الهجمات والجرائم السيبرانية مما يُشَكِّل تحديًا حقيقيًا للسياسات الجنائية في الدولة ولأجهزتها التشريعية والتنفيذية والقضائية (سلطان، 2016، ص970)

وقد عَرَّفَ الفقهاء الهجوم السيبراني تعريفات عدة؛ من بينها ما يأتي: الهجمات السيبرانية هي "استخدام الطيف الإلكتروني أو الكهرومغناطيسي لتخريب وتعديل وتبادل البيانات وجها لوجه مع أنظمة تحكم في بنى تحتية مرتبطة بها" (الفتلاوي، 2016، ص 16). وعُرِّفَت الهجمات السيبرانية أيضا بأنها "مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نظم المعلومات المعادية بهدف التأثير والإضرار بها، وفي الوقت نفسه للدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة" (الشرقاوي، 2021، ص 73). وذهب مجموعة من الباحثين في جامعة بيل الأمريكية إلى أن الهجمات السيبرانية هي "أن تصل لتقويض وظيفة شبكة الكمبيوتر لأغراض سياسية أو ماسة بالأمن القومي" (Schmidt, 1998, p. 890). كذلك، عُرِّفَت بأنها "أي عملية تعطل أو تقلل أو تدمر المعلومات الموجودة في أجهزة الكمبيوتر أو شبكات الكمبيوتر." وقُسِمَت إلى خمسة أنواع عامة، تتراوح من الأخف إلى الأشد: (1) التخريب عبر الإنترنت، (2) حملات التضليل، (3) جمع البيانات السرية، (4) تعطيل المجال، و (5) الهجمات على البنية التحتية الوطنية الحيوية." (Blank, 2013, pp.435-436).

كما عُرِّفَت في دليل تالين للهجمات السيبرانية (Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations) في القاعدة 30 منه بأنها: "عمليات سيبرانية سواءً كانت هجومية أم دفاعية، يهدف من خلالها بصورة معقولة التسبب بالإصابة أو الوفاة للأشخاص أو الإضرار أو تدمير الأعيان." ودليل تالين هو عمل أكاديمي غير ملزم قانونا. والتعريف الوارد في الدليل يُعد مقبولا لتَضَمُّنه الوسيلة المستخدمة والهدف من الهجوم. فهو يشترط أن يتم الهجوم باستخدام الوسائل التقنية في الفضاء السيبراني، ويجب أن يؤدي الهجوم أو يُحتمل أن يؤدي إلى خسائر مادية أو إصابات أو وفاة أو الإضرار أو تدمير الأعيان

وعلى المستوى الدولي، مازال مفهوم "الهجوم السيبراني" غير متفق عليه، وهو ما يتطلب أن يتصدى المجتمع الدولي لتحديده وبيانه في أي اتفاقية دولية أو قرار دولي

ويعتمد هذا البحث التعريف الوارد في دليل تالين. ومن ثم، يُستَخدم مصطلح "الهجوم السيبراني" لوصف مجموعة متنوعة من الأنشطة الضارة التي تحدث في الفضاء السيبراني، وهذه الأنشطة تكون واسعة النطاق؛ أي هجمات سيبرانية تهدف إلى اختراق أجهزة الكمبيوتر والإضرار بالمعلومات الموجودة فيها أو تعطيلها أو رفضها أو تدميرها. ولا تقتصر آثار هذه الهجمات على الإضرار الداخلي بأجهزة الكمبيوتر أو الشبكات فحسب، بل تؤدي أيضا إلى الإضرار الخارجي بالأنظمة والمرافق والأشخاص. فعلى سبيل المثال، يؤدي الهجوم السيبراني إلى التأثير على نظام مراقبة الحركة الجوية، فيُغيِّر المعلومات المتعلقة بموقع الطائرات، مما قد يتسبب في حوادث جوية تؤدي إلى خسائر بشرية ومادية.

المطلب الثاني: مفهوم الكيانات من غير الدول

في إطار القانون الدولي، تعتبر "الدولة" هي الشخص الرئيس لهذا القانون، وهي المخاطبة أساسا بقواعده وأحكامه. ثم مع تطور العلاقات الدولية أضيفت إليها المنظمات الدولية كأشخاص للقانون الدولي العام، وظل الفرد غير معترف به كشخص من أشخاص القانون الدولي العام. إلا أنه مع التطور الكبير في الحياة الدولية، ظهر فاعلون جدد كجماعات التمرد والجماعات المسلحة والشركات متعددة الجنسيات. وبذلك لم تَعُد الدولة الفاعل الوحيد في السياسات الدولية (Call, 2015, pp. 6 - 8)، وأصبح هناك مركز أو وضع للفرد في القانون الدولي، وإن لم يُعترف له بعد بالشخصية القانونية الدولية

ويتمتع بعض الأفراد والجماعات (كيانات من غير الدول) بإمكانيات متطورة واحترافية في المجال الإلكتروني، وقد يكون الأفراد قراصنة هواة أو محترفين ولديهم قدرات عالية (خليفة، 2021، ص 100؛ ثامر، 2015، ص 42). ومن الأمثلة الواضحة موقع ويكلكس wikaleaks الذي قام بنشر العديد من الوثائق التي كانت تعتبر سرية لدى الدبلوماسية الأمريكية. ولهذا، لا يمكن تجاهل ما تقوم به الكيانات من غير الدول (الأفراد والجماعات) من أنشطة سيبرانية لها دور فاعل ومؤثر على الساحة الدولية

ويتضمن مفهوم "الكيانات من غير الدول" عناصر فاعلة ذات هياكل، وموارد، وطرق مختلفة في التأثير (Willetts, 2001, p. 356). وقد تعمل هذه الكيانات في أكثر من دولة وحينئذ توصف بعبر الوطنية Transnational (Williams, 2008, pp. 9 - 14)

ويُعد مفهوم "الكيانات من غير الدول" أو "الفاعلين من غير الدول" من المفاهيم التي تتسم بالغموض في مجال العلاقات الدولية، حيث لا يوجد تعريف له من قبل المنظمات الحكومية الدولية (شوقي، 2017، ص 187).

وعلى الرغم من أن مفهوم الكيانات من غير الدول لا يمكن تحديده بدقة، إلا أنه يُشير إلى أي كيان لا يعد دولة أو منظمة حكومية دولية، ومن ثم، فهو يشمل الأفراد والمجموعات التي تعمل بصفة مستقلة عن إرادة وسلطة الدول؛ فهي أي كيان منظم له إرادة سلطة مستقلة عن الحكومة، ويتمتع بنفوذ، وقادر على التحكم والتأثير، في الوضع الداخلي والدولي (النقيب، 2022، ص 163).

والخلاصة أن مفهوم الكيانات من غير الدول مفهوم واسع يشمل جميع الجهات الفاعلة في العلاقات الدولية التي ليست دولا أو منظمات حكومية دولية، فهو يضم الأفراد، والجماعات، والعصابات، والحركات المتمردة أو الفصائل الأخرى. وهذه الكيانات قد ترتكب الهجمات السيبرانية على الدول الأخرى

المبحث الأول: المسؤولية الدولية للدولة عن الهجمات السيبرانية للكيانات من غير الدول

إذا قام كيان من غير الدول (كأفراد أو جماعة أو منظمة) موجود في دولة ما بهجوم سيبراني في دولة ثانية، فإنه ينشأ التساؤل حول ما مسؤولية الدولة الأولى عن هذا الهجوم السيبراني الذي قام به الكيان (من غير الدول)؟ بتعبير آخر، هل يُسنَد الهجوم السيبراني للدولة التي منها قام الكيان بالهجوم؟ وما الآثار المترتبة على مسؤولية الدولة عن الهجمات السيبرانية الواقعة من كيانات من غير الدول؟ ونُجيب عن هذين التساؤلين من خلال المطلبين الآتيين:

المطلب الأول: إسناد الهجمات السيبرانية (الواقعة من كيانات من غير الدول) للدولة،

المطلب الثاني: الآثار المترتبة على مسؤولية الدولة عن الهجمات السيبرانية الواقعة من الكيانات غير الدول

المطلب الأول: إسناد الهجمات السيبرانية (الواقعة من كيانات من غير الدول) للدولة

وفقا لأحكام المسؤولية الدولية، يشترط أن تكون هناك واقعة منشئة للمسؤولية الدولية بالإضافة إلى إسناد الفعل إلى شخص من أشخاص القانون الدولي (دولة أو منظمة دولية) مع وقوع ضرر جراء هذا الفعل (الدقاق، 1983، ص 51). وعلى الرغم من أن قواعد الإسناد قديمة لا تتناسب مع الهجمات السيبرانية، إلا أنه في ضوء عدم وجود وثيقة قانونية تنص على التزامات مُلزِمَة محددة للدول في المجال السيبراني، فلا يمكن إلا الاعتماد على المبادئ العامة للقانون الدولي العام، وممارسات الدول، والسوابق القضائية

فوفقا لمشروع لجنة القانون الدولي حول مسؤولية الدول عن الأفعال غير المشروعة دوليا (حولية لجنة القانون الدولي، 2001، المجلد الثاني، الجزء الثاني، ص 41) فإنه يُتَطَلَّب لقيام المسؤولية الدولية القيام بفعل غير مشروع دوليا (الشرط الأول)، وأن يُسند هذا الفعل غير المشروع للدولة (الشرط الثاني)

وفي حالة الهجوم السيبراني، فإن هناك فعلا غير مشروع ترتب عليه ضرر؛ كحدوث وفيات أو أصابات أو تدمير، ومن ثم، فإن الشرط الأول لقيام المسؤولية الدولية يكون متحققا. أما بالنسبة للشرط الثاني وهو الإسناد، فإنه يجب أن يُتحقق منه حتى تكون الدولة مسؤولة عن الهجوم السيبراني الذي قام به كيان موجود في هذه الدولة

ويُقصَد بالإسناد نسبة الواقعة المنشئة للمسؤولية الدولية إلى دولة، والقاعدة أن ما يصدر عن أجهزة الدولة من أعمال ينسب إلى الدولة لأن هذه الأجهزة تتصرف باسم الدولة. (علام، 2001، ص 22)

ولكي يُنسَب الهجوم السيبراني إلى الدولة لا بد من تحديد صفة الكيان ومدى ارتباطه بالدولة.

والقاعدة العامة أن الدولة لا تُسأَل عن الهجوم السيبراني الذي يقوم به كيان من غير الدول، والاستثناء أنه تنعقد المسؤولية الدولية للدولة في الحالتين الآتيتين:

أولا- إذا كان الهجوم السيبراني قد تم بناء على تعليمات من الدولة، أو بتوجيه منها، أو بإيعاز منها، أو تحت رقابتها لدى القيام بالهجوم السيبراني

ثانيا- عدم بذل الدولة العناية الواجبة لمنع الهجوم السيبراني.

أولا- قيام الكيان بهجوم سيبراني بالنيابة عن الدولة

نصت المادة 8 من مشروع لجنة القانون الدولي على أنه: "يعتبر فعلا صادرا عن الدولة بمقتضى القانون الدولي تصرف شخص أو مجموعة أشخاص إذا كان الشخص أو مجموعة الأشخاص يتصرفون في الواقع بناء على تعليمات تلك الدولة أو بتوجيهات منها أو تحت رقابتها لدى القيام بذلك التصرف."

فيتحقق إسناد الهجوم السيبراني للدولة إذا كان ما قام به الكيان باسم الدولة، أو نيابة عنها، أي أن الكيان في حقيقة الأمر كان وكيلا عن الدولة. ففي الممارسة، تتخفى بعض الدول وراء كيانات (من غير الدول) يبدو في الظاهر أنها تتحرك بشكل مستقل، ولكن في الواقع هي تعمل بالتنسيق مع حكومة الدولة، وتتلقى منها دعما لوجستيا واستخباراتيا

يُمكِّنها من اختراق المواقع الإلكترونية للمصالح الحيوية، والأنظمة الدفاعية، الموجودة في دولة أخرى

وفي الممارسة، نجد بعض الحكومات تختبئ خلف كيانات فاعلة من غير الدول، وتقوم على نحو متزايد بتوظيف هذه الكيانات لشن هجمات سيبرانية على دول أخرى. (Van der Meer, 2020, p. 1)

وعلى ذلك، فإن الهجمات السيبرانية التي يقوم بها كيان في دولة ما، لا تُسأل عنها هذه الدولة إلا إذا كان الكيان تابعا للدولة، أي أنه حتى تُنسَب للدولة الهجمات السيبرانية الواقعة من جانب كيان، فإنه يجب أن تكون للدولة سيطرة عليه. ولكن، ما درجة السيطرة التي يجب أن تَتَمَتَّع بها الدولة على الكيان؟ أي ما معيار سيطرة الدولة على الكيان؟ ويطرح سؤال آخر حول الجهة الموكل إليها تحديد درجة السيطرة؟

لا يشكل الأمر صعوبة إذا كان الكيان تابعا للدولة أو لقواتها المسلحة بصفة رسمية أو بشكل مباشر، إذ تكون الدولة مسؤولة عن الهجمات السيبرانية التي قام بها الكيان. ولكن تظهر الصعوبة عندما لا يكون الكيان تابعا رسميا للدولة، أو فعليا؛ فتُسأل الدولة عن سلوك أجهزتها الرسمية حتى ولو تجاوزت حدود اختصاصها، وكذلك، تُسأل عن الكيان الذي يعتمد كليةً على سلطاتها، إذ يمكن اعتباره جهازا حكوميا بحكم الواقع؛ حتى لو لم يكن لديه هذا الوضع وفقا لقانون الدولة. ولتحديد ما إذا كان الكيان تابعا للدولة أم لا، يوجد المعياران الآتيان:

الأول: يشترط أن تُمَارِس الدولة سيطرة ورقابة قوية ومباشرة على الكيان من غير الدول حتى تُنسَب الهجمات السيبرانية للدولة. فالمقصود بـ"السيطرة": السيطرة الفِعلِيَّة" (effective control)؛ أي أن تُعطِيَ الدولة للكيان تعليمات محددة بخصوص الهجوم، ولعل السبب في هذا التشدد أن تحقق التبعية في هذه الحالة سيترتب عليه إسناد الفعل إلى الدولة (Milanović, 2009, p. 315). وهذه وجهة نظر محكمة العدل الدولية في القضية المتعلقة بالأنشطة العسكرية وشبه العسكرية في نيكاراجوا وضدها (1986)، فلم تَعتَبِر المحكمة الولايات المتحدة الأمريكية مسؤولة عن أعمال أفراد جماعة الكونترا في نيكاراجوا لمجرد قيامها بتنظيمهم وتمويلهم وتدريبهم وتجهيزهم، وذلك لأنه لم تكن للولايات المتحدة الأمريكية "السيطرة الفِعلِيَّة" على أفراد الكونترا (Case Concerning Military and Paramilitary Activities In and Against Nicaragua, Judgment of 27 June 1986. para 115).

الثاني: يشترط أن تُمَارِس الدولة سيطرة ورقابة عامة على الكيان من غير الدول حتى تُنسَب الهجمات السيبرانية للدولة. فالمقصود بـ"السيطرة": السيطرة العامة"(overall

control) والذي يعتبر معيارا أكثر اتساعا من معيار السيطرة الفعلية. وهذه وجهة نظر المحكمة الجنائية الدولية ليوغسلافيا السابقة في قضية تاديتش (1999)، فقد رفضت المحكمة أن تأخذ بمعيار "السيطرة الفِعلِيَّة" لأنه يَتَطَلَّب شرطا شديدا لجعل دولة مسؤولة، اكتفت المحكمة - لقيام مسؤولية الدولة – بشرط أقل تشددا؛ وهو أن تكون لها "السيطرة العامة"؛ أي يكون لها " السيطرة العامة على الجماعة، وليس السيطرة الفِعلِيَّة". (Prosecutor v. Dusko Tadic, Judgment of 15 July 1999, paras 115, 116 - 145) وأقرت المحكمة أن درجة السيطرة تختلف وفقا للظروف الواقعية لكل قضية على حدة (ICTY, 1999, para 117)، كما أشارت إلي أن معيار السيطرة الفعلية الذي تبنته محكمة العدل الدولية في القضية المتعلقة بالأنشطة العسكرية وشبه العسكرية في نيكاراجوا وضدها هو أقل اتساقا مع القواعد الخاصة بالمسؤولية الدولية (ICITY, 1999, para 116). ويُعد معيار السيطرة العامة أكثر اتساعا لإسناد السلوك للكيان؛ فطبقا له يكفي أن يكون للدولة دور في التنظيم أو التنسيق، أو التخطيط للهجوم، بالإضافة إلى التمويل والتدريب والتجهيز، أو تقديم الدعم، وذلك بغض النظر عن وجود تعليمات محددة من قبل الدولة المسيطرة فيما يتعلق بالهجوم (ICITY, 1999, para 137)، وبالتالي فإن معيار السيطرة العامة لا يتطلب السيطرة على الفعل، ولكن على الفاعل نفسه؛ أي الكيان بشكل عام (Milanović, 2009, p. 317)

والذي نميل إليه بشأن مسؤولية الدولة عن الهجمات السيبرانية الواقعة من الكيانات غير التابعة للدولة إلى ما تبنته المحكمة الجنائية الدولية ليوغوسلافيا السابقة؛ أي معيار "السيطرة العامة" للأسباب المذكورة سلفاً، وهو يمثل معيارا أكثر اتساعا من معيار السيطرة الفعلية الذي تبنته محكمة العدل الدولية في القضايا السابق ذكرها؛ إذ أقرت المحكمة أن درجة السيطرة تختلف وفقا للظروف الواقعية لكل قضية على حدة

ثانيا- عدم بذل الدولة العناية الواجبة لمنع الهجوم السيبراني:

يتحقق إسناد الهجوم السيبراني للدولة إذا قصرت في منعه؛ فالدولة عليها ما يُعرَف بواجب المنع والقمع؛ أي واجب المنع أو الحيطة قبل وقوع الهجمات السيبرانية، وواجب القمع بعد وقوعها. فالدولة ليست مسؤولة عن قيام الكيان بهجمات سيبرانية في الدول الأخرى إلا إذا كانت الدولة مُقَصِّرَة في اتخاذ التدابير الضرورية لمنع هذه الهجمات، وملاحقة ومحاكمة الأفراد المتهمين بارتكابها.

وعلى ذلك، فإن الهجمات السيبرانية التي يقوم بها كيان في دولة ما، لا تُسأَل عنها هذه الدولة إلا إذا قصرت في منعها؛ فلم تتخذ العناية الواجبة لمنع وقوع الهجمات السيبرانية

مفهوم العناية الواجبة:

يُقصد بالعناية الواجبة أن تتخذ الدولة الاحتياطات والتدابير اللازمة لمنع وقوع هجمات سيبرانية من أراضيها - التي تتمتع بالسيادة عليها - موجهة ضد الدول الأخرى. وقد أكدت محكمة العدل الدولية على المفهوم في قضية قناة كورفو، حيث انتهت المحكمة إلى مسؤولية ألبانيا على أساس أنها كانت تعلم، أو كان يجب أن تعلم، بوجود ألغام في مياهها الإقليمية، ولكن امتنعت عن القيام بتحذير الدول الثالثة من وجودها؛ فذَكَرَت: ""في الواقع، لم تحاول السلطات الألبانية القيام بأي شيء لمنع الكارثة. هذه الامتناعات الجسيمة تنطوي على المسؤولية الدولية لألبانيا." (Corfu Channel case, I.C.J. Reports 1949, p. 23) كذلك، في قضية الموظفين الدبلوماسيين والقنصليين التابعين للولايات المتحدة، انتهت المحكمة إلى أن مسؤولية الحكومة الإيرانية تَتَرَتَّب على امتناعها عن القيام بأي فعل؛ فذَكَرَت: "في 4 نوفمبر 1979، فشلت الحكومة الإيرانية تماما في اتخاذ أي "خطوات مناسبة" لحماية مباني وموظفي ومحفوظات بعثة الولايات المتحدة ضد هجوم المسلحين، واتخاذ أي خطوات إما لمنع هذا الهجوم أو لإيقافه قبل اكتماله. كما يظهر أنه في 5 نوفمبر 1979، فشلت الحكومة الإيرانية بالمثل في اتخاذ الخطوات المناسبة لحماية قنصليتي الولايات المتحدة في تبريز وشيراز." (United States Diplomatic and Consular Staff in Tehran, Judgment, I.C.J. Reports 1980, para. 63)

والعناية الواجبة قابلة للتطبيق وملزمة، فيُلزِم القانون الدولي العرفي الدول بأن تمتنع عن استخدام البنية التحتية السيبرانية الموجودة على أراضيها بطريقة تضر بالدول الأخرى. وهذا مفهوم راسخ بموجب قانون البيئة، كما له تطبيق في قانون البحار، وقانون الاستثمار، والأنظمة القانونية الأخرى. (Kavaliauskas, 2022, p.9)

ويتضمن هذا الالتزام أمرين:

أ. التزام بنتيجة؛ وهو وضع وتنفيذ التدابير والاحتياطات والإجراءات اللازمة لمنع استخدام أراضيها للقيام بهجمات سيبرانية تضر الدول الأخرى،

ب. التزام بسلوك، وهو عندما ينشأ هجوم سيبراني من دولة، فإن على هذه الأخيرة أن تتصرف بشكل معقول لمنعه.

وتتوقف التدابير والاحتياطات والإجراءات، والتصرف بشكل معقول، على قدرات الدول، وللدولة سلطة تقديرية واسعة. (Buchan, 2016, pp.33 - 34.)

وخلاصة الأمر، أنه التزام بتحقيق نتيجة؛ أي ضرورة وهو وضع التدابير والاحتياطات والإجراءات اللازمة لمنع الهجمات السيبرانية، فإذا لم تضع الدولة هذه التدابير تكون مخلة

بالتزامها. وهو كذلك، التزام ببذل عناية أو سلوك، فإذا نشأ هجوم سيراني على الدولة أن تبذل قصارى جهدها لوقفه، فإذا لم تنتهج الدولة أي سلوك لوقف الهجوم السيبراني، فإنها تتحمل المسؤولية

مسؤولية القادة والرؤساء

يمكن أن تقوم مسؤولية الدول عند تنفيذ هجمات سيبرانية يترتب عليها ارتكاب جرائم دولية (محيدلي، 2014، ص 160)، كجريمة العدوان على سيادة الدول عندما تُنسب الهجمات لها كدولة أو بالنسبة للجرائم التي يرتكبها الأفراد التابعون لها من قادة ورؤساء ومرؤوسين (العنبكي، 2010، ص 494؛ عبد الجبار، 2019، ص 26)

فعندما يترتب على ارتكاب الهجمات السيبرانية جرائم دولية ينتج عنها إصابات ووفيات بين الأفراد المدنيين أو أضرار بالأعيان المدنية (المهدي، 2011، ص 217)، فإن مرتكبيها من القادة العسكريين والرؤساء، ومن كيانات من غير الدول، يكونون محلا للمسؤولية الجنائية الدولية وفقا للقانون الدولي الجنائي؛ لأن هذه الهجمات تشكل انتهاكا لأحكام القانون الدولي والقانون الدولي الإنساني (الطراونة، 2016، ص 373). أما بالنسبة للدولة فمن الممكن أن يكون جزاؤها عقوبات اقتصادية أو سياسية كما هو الحال في القرارات التي يتخذها مجلس الأمن الدولي لاسيما وأنها ليست محلا للجزاءات الجنائية (هيكل، 2009، ص 110)

ويفترض لقيام المسؤولية الدولية الجنائية ارتكاب هجمات سيبرانية قام به وكلاء أو ممثلو الدولة من قادة أو مسؤولين. ويُمكن أن تُشكل هذه الهجمات جريمة دولية، سواءً تحقق الضرر أم لم يتحقق، لأن الجرائم الدولية من جرائم الخطر، فتتحقق المسؤولية الجنائية فيها بمجرد الاعتداء على المصلحة القانونية التي يحميها القانون الدولي (العنبكي، 2010، ص 482)

المطلب الثاني: الآثار المترتبة على مسؤولية الدولة

عن الهجمات السيبرانية الواقعة من الكيانات غير الدول

يترتب على مسؤولية الدولة عن الهجمات السيبرانية الواقعة من الكيانات غير الدول أن تلتزم بإيقاف هذه الهجمات، وبجبر الضرر الحادث نتيجة لها

أولا- التزام الدولة بوقف الهجمات السيبرانية الواقعة من كيانات من غير الدول:

تلتزم الدولة بوقف الهجمات السيبرانية الواقعة من كيانات من غير الدول إذا كانت هذه الهجمات ما زالت مستمرة؛ فعلى سبيل المثال، عليها إيقاف أنشطة الفيروسات الإلكترونية

الخبيثة أو إعادة الملفات والبيانات التي سبق الحصول عليها إلكترونيا. وعلى الدولة أيضا تقديم التأكيدات والضمانات الملائمة بعدم التكرار في المستقبل. (المادة 30 من مشروع قانون المسؤولية الدولية). وعلى الدولة إذا لم تكن قادرة على إيقاف هذه الهجمات أن تطلب المساعدة الفنية من الدول الأخرى؛ ولا سيما الدول المضرورة بهذه الهجمات

ثانيا- جبر الضرر الحادث بسبب الهجمات السيبرانية الواقعة من كيانات من غير الدول:

على الدولة المسؤولة الجبر الكامل للخسارة الناجمة عن الهجمات السيبرانية الناشئة من إقليمها، من قِبل كيانات من غير الدول (المادة 34 من مشروع قانون المسؤولية الدولية). ومسؤولية الدولة مسؤولية دولية مدنية.

ويُمكن للدول المضرورة أن ترفع الأمر إلى المنظمات الدولية، أو إلى محكمة العدل الدولية أو المحكمة الجنائية الدولية (إذا توافر لهما الاختصاص)

رد فعل الدولة المتضررة من الهجمات السيبرانية الواقعة من كيانات من غير الدول

يمكن أن تلجأ الدولة المتضررة إلى تدابير مضادة أبعد مدى من الإجراءات الدبلوماسية كالاحتجاج؛ فتعتبر نفسها في حالة دفاع عن النفس، ومن ثم، تقوم بهجوم مضاد؛ كهجوم سيبراني وذلك لإلحاق الضرر بأجهزة الكمبيوتر التابعة لكيان من غير الدول، أو شل بعض البنى التحتية الرقمية التابعة للدولة التي تنطلق منها الهجمات السيبرانية.

وقد يتطور الأمر إلى حد توجيه ضربة عسكرية ضد موقع محدد يخص الكيان الذي يقف وراء الهجوم السيبراني أو الدولة التي يعمل منها. (Van der Meer, 2020, p. 3) فيمكن للدولة المضرورة أن تستخدم القوة دفاعا عن النفس ضد دولة أخرى إذا كان الهجوم قد ارتكبته أجهزتها أو وكلاؤها أو ارتكبته كيانات من غير الدول (Tsagourias, 2012, pp.229 - 244).

وعند ممارسة الدفاع عن النفس، يجب على الدولة المضرورة أن تُراعي شروط الضرورة والفورية والتناسب، وأن تقوم أولا بتحديد مصدر الهجوم السيبراني، وإسناده على نحو غير مشكوك فيه لدولة؛ ولهذا فإن الإسناد مهم جدا لفعالية الرد ولشرعيته.

ونظرا لصعوبة الإسناد في الفضاء السيبراني، قد لا يكون من الممكن إسناد الهجمات التي ترعاها الدولة؛ فالهجمات السيبرانية التي ترتكبها كيانات من غير الدول تتم عن طريق الاختراق والتسلل داخل النظم المعلوماتية، بغرض تدميرها أو الحصول على معلومات سرية سواء عسكرية أو اقتصادية. ولهذا، فإنه من الأفضل للدول المضرورة من الهجمات السيبرانية الواقعة من كيانات من غير الدول أن تتقدم بشكوى لمجلس الأمن

(الأمم المتحدة) والذي له صلاحيات واسعة وفقا للفصل السابع في الميثاق. كذلك، من الأهمية أن تقوم الدول بتطوير آليات منع الهجمات السيبرانية أو التخفيف منها؛ على سبيل المثال، جعل شبكات البنية التحتية الحيوية أكثر أمانًا وأصعب اختراقا.

المبحث الثاني: المسؤولية الدولية للكيانات من غير الدول عن الهجمات السيبرانية

شهدت السنوات الأخيرة العديد من الهجمات السيبرانية التي تقوم بها كيانات من غير الدول. فقد حدثت هجمات سيبرانية عن طريق كيانات تتصرف باستقلال كامل عن الدول، وبمعزل عنها. ومن ثم، ينشأ التساؤل حول مسؤولية هذه الكيانات عن الأضرار التي تُحدثها الهجمات السيبرانية. ونوضح هذا الأمر من خلال المطلبين الآتيين:

المطلب الأول: إسناد الهجمات السيبرانية للكيانات من غير الدول.

المطلب الثاني: المسؤولية الدولية الجنائية للكيانات من غير الدول عن الهجمات السيبرانية

المطلب الأول: إسناد الهجمات السيبرانية للكيانات من غير الدول

في البَدء، كانت الهجمات السيبرانية تقع من الدول لما تملكه من موارد وقدرات عالية في مجال تكنولوجيا الكمبيوتر، ولهذا كان من المنطقي أن يهتم القانون الدولي بالهجمات السيبرانية الواقعة من الدول. غير أنه مع التقدم التكنولوجي الكبير في مجال استخدام الفضاء السيبراني، وفي ضوء حرية الإنسان في الوصول إلى الإنترنت (بل واعتباره في بعض الدول حقا أساسيا من حقوق الإنسان)، طوَّرت الكيانات من غير الدول من قدراتها التكنولوجية فأصبحت تُضاهي قدرات الدول في هذا المجال، وأصبح في مَقدور هذه الكيانات القيام بهجمات سيبرانية ضد المصالح الحيوية للدول. (Schmitt & Watts, 2016, p.595)

فيُمكن أن يقوم كيان (من غير الدول) موجود في دولة ما بهجوم سيبراني موجه للمصالح الحيوية في دولة أخرى. وعادة تكون الهجمات السيبرانية التي تنفذها الكيانات من غير الدول في الإطار الهجومي حيث تستهدف المواقع الإلكترونية والأنظمة الدفاعية

ويعد الإسناد أمرا بالغ الأهمية لقيام مسؤولية الكيانات من غير الدول؛ لكن الإسناد عملية معقدة لها جوانب فنية وسياسية وقانونية. فمن الناحية العملية، هناك صعوبة في إسناد الهجمات لكيان من غير الدول؛ فهناك صعوبة في تحديد الدولة أو المكان الذي يقوم منه الكيان بالهجوم، وكذلك صعوبة في تحديد هوية المنفذين، فالهجمات السيبرانية تتم عن بعد، وتجري في الفضاء الإلكتروني الذي لا يعرف الحدود الجغرافية والإقليمية.

فالهجوم السيبراني يتسم بخصائص صعبة، ولذلك، يجب أن تكون لدى المدعين العامين والمحققين في الدول المهارات الفنية والقانونية عند إجراء التحقيقات في الأدلة، وفي الانتهاكات الجسيمة للقانون الدولي المرتكبة في الفضاء الإلكتروني، لكي يستطيعوا التحقق من إسناد الهجوم السيبراني للكيانات. (Saxon, 2016, pp. 555 - 574)

والقاعدة أنه إذا كان هذا الكيان يقوم بالهجوم السيبراني وفقا لإرادته، وباستقلال ومعزل عن أية دولة، فإن هذا الهجوم يُسنَد لهذا الكيان وحده، ويكون مسؤولا عنه. ومن الأهمية أن يكون عزو الهجوم السيبراني لكيان ما مؤسسا على أدلة وبراهين مقنعة حتى يكون من الصعب على هذا الكيان الذي قام بالهجوم السيبراني الإنكار. مع ملاحظة أنه قد يُعلن الكيان مسؤوليته عن هجمات سيبرانية في دولة أخرى؛ في قطاعات حيوية كالاتصالات والاقتصاد والبيئة

ومما يُفاقم من مشكلة الهجمات السيبرانية من كيانات من غير الدول عدم وجود أحكام دولية صريحة تنظمها، وزيادة اللجوء إليها، وإمكانية قيام الكيانات بهجمات سيبرانية من خلال الذكاء الاصطناعي، وكذلك مشاكل عدم الكشف عن هوية الكيان وإسناده، والقضايا المتعلقة بالولاية القضائية، والافتقار الحالي إلى التعاون الدولي في مواجهة الهجمات السيبرانية.

والهجمات السيبرانية – بوصفها عابرة للحدود- لا يمكن مواجهتها إلا من خلال التعاون الدولي. فمن الضروري المزيد من التعاون بين الدول. ومن العقبات التي تحول دون التوصل إلى مبادئ مشتركة انعدام الثقة المتبادلة والشفافية بين الدول التي تمتلك تلك التكنولوجيا وبالأخص بين الولايات المتحدة الأمريكية وروسيا. كذلك، من الأهمية بمكان أن يتضمن القانون الدولي العام قواعد قانونية ملزمة تتعلق بالهجمات السيبرانية الواقعة من كيانات من غير الدول. (Schmitt & Watts, 2016, p.595)

المطلب الثاني: المسؤولية الدولية الجنائية للكيانات من غير الدول عن الهجمات السيبرانية

اهتم القانون الدولي التقليدي بالدول، غير أنه مع تطور الدور الذي يقوم به الفرد في بعض الأحداث، استجاب القانون الدولي لهذه التطورات، واعترف بمركز محدود للفرد على المستوى الدولي؛ كالجماعات المسلحة في النزاعات الداخلية، والشركات متعددة الجنسيات

ومن ذلك أيضا، الهجمات السيبرانية الواقعة من كيانات من غير الدول؛ فهذه الهجمات تنتهك سيادة الدول وتضر بأمنها واستقرارها، ومن ثم، كان لا بد من الرجوع للقواعد العامة للقانون الدولي لتقرير مسؤولية هذه الكيانات

فيترتب على الهجمات السيبرانية حدوث إضرار بالدول؛ كالتسبب في أضرار فادحة بالمنشآت الحيوية. وهذه الهجمات السيبرانية يقوم بها أشخاص طبيعيون سواء كانوا يعملون بالنيابة عن دولة أو كوكلاء لها، أو كانوا يعملون باستقلال عن أية دولة. وفي الحالتين هناك مسؤولية دولية جنائية على هؤلاء الأشخاص؛ أي يمكن تحميل الكيانات من غير الدول مسؤولية انتهاكات القانون الدولي، وعلى وجه الخصوص القانون الدولي الإنساني

فلا تقتصر آثار الهجمات السيبرانية على قيام المسؤولية الدولية بشقها المدني فقط في حق الدولة، وإنما هناك أيضا مسؤولية دولية جنائية في حق الأشخاص الطبيعيين

ويفترض لقيام المسؤولية الدولية الجنائية ارتكاب هجمات سيبرانية قام به كيان من غير الدول.

وتجدر ملاحظة أنه قد تكون البواعث على الهجمات السيبرانية التي تقوم بها كيانات من غير الدول غير إجرامية؛ فعلى سبيل المثال، ردا على فرض رقابة وإسكات أو تقييد ويكيليكس (الموقع الذي كان ينشر البرقيات الدبلوماسية الأمريكية وغيرها من الوثائق السرية التي تم تسريبها إلى تلك المنظمة)، تم تنفيذ هجمات من جماعات لإسقاط المواقع. مع ملاحظة أنه في هذه الحالة، لم يتم التحريض على الحرب من قبل دولة ضد دولة أخرى، ولكن من قبل كيانات من غير الدولة ضد شركات خاصة وأفراد لتصحيح ما اعتبرته هذه الكيانات خطأً أمرت به حكومة الولايات المتحدة. (McReynolds, 2015, p.427). ويمكن أن تُجادل الكيانات من غير الدول بأن هجماتها مشروعة وذلك لأن شرط الواقعة المنشئة للمسؤولية الدولية غير متحقق. فالفعل يعد غير مشروع دوليا إذا كان يشكل إخلالا بالتزام دولي سواء أكان هذا الإخلال بفعل إيجابي أم سلبي (علام، 2001، ص 21). أما إذا لم يكن هناك التزام على الدولة، فإن الشرط الأول للمسؤولية الدولية وهو الواقعة المنشئة للمسؤولية لم يتحقق، ومن ثم لا تنعقد المسؤولية الدولية عن هذا الهجوم السيبراني (الغنيمي، 1993، ص 457). وفي الحقيقة، يجب أن تكون الهجمات السيبرانية العشوائية التي تقوم بها جماعات من غير الدول محظورة في القانون، ومدانة من الناحية الأخلاقية، أيا كانت البواعث لها. فعلى سبيل المثال، إذا كان هناك استغلال اقتصادي من دولة ما، فإن هذا لا يُبرر قيام كيان من غير الدول بهجوم سيبراني ضد بنوك أو مؤسسات اقتصادية لهذه الدولة. ومن الأهمية، حتى لا يفلت أفراد الكيانات من غير الدول من المسؤولية الجنائية أن يتم تجريم الهجمات السيبرانية العشوائية الواقعة منها أيا كانت بواعثها. فعلى الرغم من أن الهجمات السيبرانية تُسبب دماراً هائلاً لا يقل عن الهجوم المسلح، إلا أنها مازالت خارج دائرة القواعد القانونية الملزمة؛ لذا يمكن لبعض الكيانات من غير الدول أن تستغل هذه الثغرة لتحقيق أهدافها عبر الفضاء السيبراني (كاظم، 2019، ص 19).

ويترتب على قيام المسؤولية الجنائية الدولية الفردية إمكانية توقيع عقوبات جنائية على الأفراد المدانين؛ كالعقوبات الجسدية المقيدة للحرية (محيدلي، 2014، ص160)، ولا شك أن معاقبة هؤلاء الأفراد ستردعهم (الردع الخاص)، كذلك، ستردع من يريد أن يحذو حذوهم (الردع العام).

ويمكن محاكمة أفراد الكيانات من غير الدول عن الهجمات السيبرانية أمام محكمة داخلية أو دولية. فيمكن لدولة أن تتهم أفراد كيانات من غير الدول موجودين في دولة أخرى بالقيام بهجمات سيبرانية ضدها أدت إلى أضرار بشرية أو مادية. وتطلب هذه الدولة تسليم هؤلاء المتهمين لمحاكمتهم أمام قضائها الداخلي. كما يمكن لها أن تُصدِر بحقهم مذكرة استيقاف، وتطلب من المنظمة الدولية للشرطة الجنائية (الإنتربول) تعميمها على الدول

الخاتمة

يواجه المجتمع الدولي تحديا خطيرا يتمثل في قيام كيانات من غير الدول بهجمات سيبرانية بغرض الإضرار بالدول الأخرى. وقد تكون هذه الكيانات تعمل بنحو مستقل عن أية دولة، كما قد تقوم الدول – للهروب من المسؤولية – بتوظيف كيانات لشن هجمات سيبرانية

ويواجه تنظيم الهجمات السيبرانية من كيانات من غير الدول معضلة كبيرة تتمثل في عدم وجود أحكام دولية صريحة تنظمها، على الرغم من تزايد استخدامها.

ونظرا لأن قواعد القانون الدولي – في الأساس – تتمحور حول "الدولة"، فإن الهجمات السيبرانية من كيانات من غير الدول لم تتعرض لها بشكل صريح قواعد القانون الدولي، لا سيما وأن موضوع الهجمات السيبرانية يُعَدَّ حديثا. وفي ضوء ذلك، فإنه يُعوَل على مبادئ القانون الدولي، وممارسات الدول، والسوابق القضائية وآراء الفقه بشأن المسؤولية الدولية عن هذه الهجمات السيبرانية الواقعة من كيانات من غير الدول

ويخلُص البحث إلى النتائج والتوصيات الآتية:

أولاً: النتائج:

1. تُنسب الهجمات السيبرانية الواقعة من كيانات من غير الدول إلى هذه الكيانات إذا قامت بها على نحو مستقل عن أية دولة. ومن ثم، تتقرر المسؤولية الدولية الجنائية بشأن أفراد هذه الكيانات.

2. تُنسب الهجمات السيبرانية الواقعة من كيانات من غير الدول إلى الدولة إذا كانت الكيانات تخضع لتوجيهات الدولة أو تعليماتها أو سيطرتها، أو كانت الدولة لا تبذل العناية الواجبة لوقف هذه الجهات. ومن ثم، تتقرر المسؤولية الدولية للدولة؛ فتلتزم بوقف هذه الهجمات، وبجبر الضرر الحادث بسببها.

3. تلتزم كل دولة باتخاذ التدابير والإجراءات والاحتياطات اللازمة لمنع استخدام إقليمها في هجمات سيبرانية تقوم بها كيانات من غير الدول (التزام بتحقيق نتيجة). وللدولة هامش واسع من التقدير بالنسبة لتحديد محتوى هذه التدابير والإجراءات والاحتياطات. ومع ذلك، إذا امتنعت أو قصرت دولة في اتخاذ هذه التدابير فإنها تكون مسؤولة. وكذلك، تلتزم الدولة أن تبذل قصارى جهدها لوقف الهجمات السيبرانية من إقليمها (التزام ببذل عناية أو سلوك)، فإذا لم تنتهج الدولة أي سلوك لوقف الهجوم السيبراني، فإنها تتحمل المسؤولية.

ثانيًا- التوصيات:

1. وضع وثيقة قانونية ملزمة تتضمن أحكاما وقواعد تتعلق بتنظيم الهجمات السيبرانية الواقعة من كيانات من غير الدول، بما في ذلك، أحكام المسؤولية الدولية عن هذه الهجمات السيبرانية.

2. التعاون بين الدول في مجال الأمن السيبراني. ويكون هذا التعاون بشكل مسبق لمنع الهجمات السيبرانية الواقعة من كيانات من غير الدول، كما يكون أثناء وبعد وقوعها للكشف عن منفذيها، ومحاسبة مرتكبيها.

3. اللجوء لمجلس الأمن هو الخيار الأفضل للرد على الهجمات السيبرانية الواقعة من كيانات من غير الدول، عندما تكون هذه الكيانات تعمل على نحو مستقل عن أية دولة، وتكون الدولة التي تنطلق منها هذه الهجمات غير قادرة على وقفها.

4. الهجمات السيبرانية التي تقوم بها جماعات من غير الدول، وتُلحق أضرارا عشوائية، يجب أن تكون محظورة في القانون (الوطني والدولي)، ومدانة من الناحية الأخلاقية، أيا كانت البواعث لها.

وفي الأخير، يظل موضوع المسؤولية الدولية عن الهجمات السيبرانية الواقعة من كيانات من غير الدول يحتاج إلى مزيد من البحث والدراسة لمواجهة تطوراته المتسارعة والمتزايدة

قائمة المصادر والمراجع:

أولاً: المراجع العربية:

بخيت، شريف نسيم قلته (2017). الهجمات الإلكترونية وحظر استخدام القوة. موقع المركز العربي الأبحاث الفضاء الإلكتروني.

جلال، محمد منذر (2021). تكنولوجيا الحروب السيبرانية واستراتيجيات المواجهة الدولية. منشورات دار ومكتبة عدنان للطباعة والنشر والتوزيع.

حسن، كاميران عزيز (2021). الجهود الدولية في مواجهة الجرائم السيبرانية. منشورات الحلبي الحقوقية.

خليفة، إيهاب (2021). الحرب السيبرانية. الاستعداد لقيادة المعارك العسكرية في الميدان الخامس. منشورات دار المستقبل للأبحاث والدراسات.

الدقاق، محمد السعيد (1983). شرط المصلحة في دعوى المسؤولية عن انتهاك الشرعية الدولية. الدار الجامعية للطباعة والنشر.

الردايدة، عبد الكريم (2013). الجرائم المستحدثة واستراتيجية مواجهتها. دار ومكتبة حامد للنشر والتوزيع.

الرشيدي، هالة أحمد (2021). الإرهاب السيبراني. منشورات دار النهضة العربية.

سلطان، كوثر حازم (2016). موقف القانون والقضاء من الجريمة الإلكترونية السيبرانية. دراسة مقارنة. مجلة كلية التربية الأساسية الجامعة المستنصرية، *22*(96)، 969-998. https://doi.org/10.35950/cbej.v22i96.8898

الشرقاوي، محمود حسين (2021). الهجمات السيبرانية في ضوء أحكام القانون الدولي الإنساني. منشورات دار النهضة العربية.

شوقي، أسماء (2017). الفواعل العنيفة من غير الدول وتأثيرها على العلاقات الشرق أوسطية. دراسة حالة داعش. مجلة شؤون عربية، (170)، 185-202.

الطراونة، مخلد أرخيص (2005). الجرائم الإسرائيلية في الأراضي الفلسطينية المحتلة ومدى إمكانية تقديم المسؤولين عنها للمحاكمة. مجلة الحقوق جامعة الكويت، *29*(2)، 285-353. https://doi.org/10.34120/jol.v29i2.1403

الطراونة، مخلد أرخيص (2016). الوسيط في القانون الدولي الإنساني. منشورات دار وائل للنشر والتوزيع.

عبد الجبار، سجا جواد (2019). المسؤولية الجنائية الفردية عن الجرائم ضد الإنسانية. دار وائل للنشر والتوزيع.

علام، وائل أحمد (2001). مركز الفرد في النظام القانوني للمسؤولية الدولية. دار النهضة العربية.

محمد، زهراء عماد (2021). المسؤولية الدولية الناشئة عن الهجمات السيبرانية. منشورات مكتبة القانون المقارن.

العنبكي، نزار (2010). القانون الدولي الإنساني. منشورات. دار وائل للنشر والتوزيع.

الغنيمي، محمد طلعت (1993). الوسيط في قانون السلام. منشأة المعارف.

الفتلاوي، أحمد عبيس (2016). الهجمات السيبرانية. مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر. مجلة الحلي للعلوم القانونية والسياسية، *8*(4)، 611-687. https://doi.

org/10.36528/1150-008-004-013

القريطي، دحان حزام (2022). الأمن السيبراني وحماية أمن المعلومات. دار الفكر الجامعي.

كاظم، علي محمد (2019). المشاركة المباشرة في الهجمات السيبرانية. منشورات المؤسسة الحديثة للكتاب.

محيدلي، حسين علي (2014). أثر نظام المحكمة الجنائية الدولية على سيادة الدول عن الجرائم الداخلة في اختصاصها. منشورات الحلبي الحقوقية.

المهدي، محمد أمين (2011). المدخل لدراسة القانون الدولي الجنائي. دار النهضة العربية للنشر والتوزيع.

النقيب، عدنان (2022). الحرب الإلكترونية في ضوء بروتوكولي سبع وسبعين الملحقين باتفاقيات جنيف الأربع لسنة تسع وأربعين (الهجمات السيبرانية). منشورات المركز العربي للنشر والتوزيع.

هيكل، أمجد (2009). المسؤولية الجنائية الفردية الدولية أمام القضاء الجنائي الدولي. دراسة في إطار القانون الدولي الإنساني. دار النهضة العربية.

ثانياً: المراجع الأجنبية:

Blank, Laurie R. (2013). International Law and Cyber Threats from Non-State Actors. *International Law Studies, 89* INT'L L. STUD. 406-437. https://doi.org/10.1163/9789004242081_006

Buchan, R. J. (2016). Cyberspace. Non-State Actors and the Obligation to Prevent Transboundary Harm. *Journal of Conflict & Security Law*, *21*(3), pp. 429-453. https://doi.org/10.1093/jcsl/krw011

Call, G. (2015). Armed Non-State Actors: Current Trends & Future Challengers. *DCAF*, (5).

Christopher, D. (2013). The need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors. *Pace International Law Review*, *3*(9), 278-315

Clarke, R., & Nick. R. (2012). *Cyber Warfare.* Publications of the Emirates Center for Strategic Studies and Research.

Clover, C. (2007). *Kremlin- Backed Group Behind Estonia Cyber blitz.* Financial Times.

Kavaliauskas, A. (2022). *Can the Concept of Due Diligence Contribute to Solving the Problem of Attribution with Respect to Cyber-Attacks Conducted by Non-State Actors Which Are Used as Proxies by States?.* 26 Teises Apzvalga L. Rev. 4. 4-30. https://doi.org/10.7220/2029-4239.26.1

McReynolds, P. (2015). *How to Think About Cyber Conflicts Involving Non-state Actors.* Philos. Technol. 28.https://doi.org/10.1007/s13347-015-0187-x

Meer, S. (2020). *How states could respond to non-state cyber-attackers.* Clingendael – the Netherlands Institute of International Relations. Clingendael Policy Brief. 1-4.

Michael, N., & Watts, S. (2016). Beyond State-Centrism: International Law and Non-State Actors in Cyberspace. *21 Journal of Conflict & Security Law*, *21*(3), 595-611. https://doi.org/10.1093/jcsl/krw019

Milanović, M. (2009). State Responsibility for Acts of Non- state Actors: A Comment on Griebel and

Plűcken. *Leiden Journal of International Law*, 307-324. https://doi.org/10.1017/S0922156509005834

Saalbach, K. (2014). *Cyber War. Methods and practice* (Version 9.0). University of Osnabruck - 17 Jun.

Saxon, D. (2016). *Violations of International Humanitarian Law by Non-State Actors during Cyberwarfare: Challenges for Investigations and Prosecutions.* 21 J. Conflict & Sec. L. 555-574. https://doi.org/10.1093/jcsl/krw018

Schmidt, A. (2013). *The Estonian Cyberattacks.* Atlantic Council.

Schmidt, M. (1998). *Computer Network Attack and the Use of Force in International law; Thoughts on Anormative Framework.* Columbia Journal of Transnation aw.

Shckelford, S. (2009). *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem.* University of Cambridge. Dept of politicos and International STUDIES. Cambridge.

Tsagourias, N. (2012). Cyber attacks. self-defence and the problem of Attribution. *Journal of Conflict & Security Law*, *17*(2), 229–244. https://doi.org/10.1093/jcsl/krs019

Willetts, P. (2001). *Transnational Actors and International Organizations in Global Politics* (2nd ed.). Oxford University Press.

Williams, Phil. (2008). *Violent Non-State Actors and National and International Security.* International Relations and Security Network (ISN).

ICJ. Corfu Channel case. Judgment of April 9th. 1949: I.C. J. Reports 1949. https://doi.org/10.2307/4609362

ICJ. Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America). Judgment of 27 June 1986.

ICITY. Prosecutor v. Dusko Tadic. Judgment of 15 July 1999. Case No. IT-94-1-A. A. Ch.

ICJ. United States Diplomatic and Consular Staff in Tehran. Judgment. I.C.J. Reports 1980.

الترجمة الصوتية لمصادر ومراجع اللغة العربية: Romanized Arabic References:

bkhyt sharīf nasīm qultahu (2017). alhajamātu al-'iliktirūniyyatu waḥaẓru astikhdāmi alqūwwati mawqi'u almarkazi al'arabiyyi al'abḥāthu alfaḍā'u al'iliktirūniyyi

jalālun muḥammad mundhirin (2021). tiknūlūjyā alḥurūbi al-saybrānyyati wisatrātījyāt almūājahati al-dawliyyati munshawarit dāri wamaktabati 'adnāna lil-ṭibā'ati wa-l-nashri wa-l-tawzī'i

ḥasanin kāmyrān 'azīzin (2021). aljuhūdu al-dawliyyatu fī mūājahati aljarā'imi al-saybrānyyati munshawarit alḥalabiyyi alḥuqūqiyyati

khalīfatu 'īhābi (2021). alḥarbu al-saybrānyya aliāsti'dādu liqīādati alma'āriki al'askariyyati fī almaydāni alkhāmis munshawarit dāri almustaqbali lil-'ābḥāthi wa-l-dirāsāti

al-daqqāqu muḥammadi al-sa'īdi (1983). sharṭu almaṣlaḥati fī da'wā almas'ūliyyati 'ani antihāki al-shar'iyyati al-dawliyyati al-dāru aljāmi'iyyatu lil-ṭibā'ati wa-l-nashri

al-radāyada 'abd alkarīmi (2013). aljarā'imu almustaḥadutha wāstirātiyyajya mūājahatihā dāru wamaktabatu ḥāmidin lil-nashri wa-l-tawzī'i

al-rashīdiyyu hālatu 'aḥmadu (2021). al-'irhābu al-saybrānyyu munshawarit dāri al-nahḍati al'arabiyyati

sulṭānun kawthara ḥāzimin (2016). mawqifu alqānūni wa-l-qaḍā'i mina aljarīmati al'ilktrūniyyati al-sībrānyyati dirāsatun muqārinatun mijallatu kulliyyati al-tarbiyati al'asāsiyyati aljāmi'ati almustanṣrya 22(96)969-998 ، https://doi.org/10.35950/cbej.v22i96.8898

al-sharqāwiyyu maḥmūd ḥusaynin (2021). alhajamātu al-saybrāniyyatu fī ḍaw'i 'aḥkāmi alqānūni al-dawliyyi al'insāniyyi munshawarit dāri al-nahḍati al'arabiyyati

shawqī 'asmā'a (2017). alfawā'ilu al'anīfatu min ghayri al-dū'ali wata'athīrihā 'alā al'alāqāti al-sharqi 'awasiṭṭaya dirāsatun ḥālati dā'sh mijallatu shu'ūnin 'arabiyyatin (170).185-202 ،

al-ṭrāwna mkhld 'arkhyṣ (2005). aljarā'imu al-'isrā'īlyya fī al-'ārāḍy alfilasṭīniyyati almuḥtallati wamadā 'imkāniyyati taqdīmi almas'ūlīna 'nhā lil-muḥākamati mijallatu alḥuqūqi jāmi'atu alkū'ayti 29(2)285-353 ، https://doi.org/10.34120/jol.v29i2.1403

al-ṭarāwanatu makhladun 'arkhīṣun (2016). alwasīṭu fī alqānūni al-dawliyyi al'insāniyyi manshūrātu dāri wā'ilin lil-nashri wa-l-tawzī'i

'abdu aljabbāri sajā jawādi (2019). al-mas'ūliyyatu al-jinā'iyyati alfardiyyatu 'ani aljarā'imi ḍidda al'insāniyyati dāru wā'ilin lil-nashri wa-l-tawzī'i

'alāmun wā'ilu 'aḥmadu (2001). markazu alfardi fī al-niẓāmi alqa'anwinyi lil-mas'ūliyyati al-dawliyyati dāru al-nahḍati al'arabiyyati

muḥammadun zahrā'u 'imād (2021). al-mas'ūliyyatu al-dawliyyatu al-nāshi'iatu 'ani alhajamāti

al-saybrānyyati manshūrātu maktabati alqānūni almuqārini

al'unubkiyyu nizārun (2010). alqānūnu al-dawliyyu al'insāniyyu manshūrātun dāru wā'ilin lil-nashri wa-l-tawzī'i

al-ghunaymiyyu muḥammadu ṭala'at (1993). al-wasīṭi fī qānūni al-salāmi mansha'atu al-ma'ārifi

al-ftlāwiyyu 'aḥmd 'ubays (2016). alhajamātu al-sybrānyyatu mafhūmuhā wa-l-mas'ūliyyatu al-dawliyyatu al-nāshi'iatu 'anhā fī ḍaw'i al-tanẓīmi al-dawliyyi almu'āṣiri mijallatu alḥuliyyi lil-'ulūmi alqānūniyyati wa-l-sīāsiyyati 8(4)611-687 ،. https://doi.org/10.36528/1150-008-004-013

al-qurayṭiyyu daḥḥān ḥizāmin (2022). al-'āmnu al-saybrāniyyu waḥimāyatu 'amni alma'lūmāti dāru alfikri al-jāmi'iyyi

kāẓimun 'alī muḥammadin (2019). almushārakatu almubāsharatu fī alhajamāti al-saybrānyyati manshūrātu almu'uassasati alḥadīthati lil-kitābi

muḥaydaliyyun ḥusaynu 'aliyyin (2014). 'atthara niẓāmi almaḥkamati aljinā'iyyati al-dawliyyati 'alā sīādati al-dū'ali 'an aljarā'imi al-dākhilati fī akhtiṣāṣihā manshūrātu alḥalabiyyi alḥuqūqiyyatu

almahdiyyu muḥammadu 'amīnin (2011). almadkhalu lidirāsati alqānūni al-dawliyyi aljuni'i'ī dāru al-nahḍati al'arabiyyati lil-nashri wa-l-tawzī'i

al-naqībi 'adnāna (2022). alḥarbu al-'iliktirūniyyatu fī ḍaw'i burwitwakwly sab'in wasab'īna almulḥaqayna biāttifāqiyyāti jinīfa al'arba'i lisanati tis'in wa'arba'īna) alhajamāti al-sībrānyyati manshūrātu almarkazi al'arabiyyi lil-nashri wa-l-tawzī'i

hīkal 'amjadu (2009). almas'ūliyyata aljinā'iyyati alfardiyyatu al-dawliyyatu 'amāma alqaḍā'i aljuni'i'ī al-dawliyyi dirāsatun fī 'iṭāri alqānūni al-dawliyyi al'insāniyyi dāru al-nahḍati al'arabiyyati

International Responsibility for Cyberattacks Committed by Non-State Entities

Halima Saleh Aldarmaki(1)
Wael Ahmed Allam(2)

Abstract:

In recent decades, cyberattacks have been carried out by non-state entities (individuals, groups, and organizations), such as those that occurred in Georgia and Estonia. These cyberattacks are more sophisticated than those carried out by states, but they are also just as dangerous. The vital interests of governments are severely jeopardized by these entities. Therefore, the study aims to clarify the international responsibility resulting from these attacks. It examines both the responsibility of the state from which non-state entities launched cyberattacks and the responsibility of these entities themselves. The study concludes that if cyberattacks are carried out by non-state entities without the involvement of any states, these entities are responsible. As a result, individuals associated with these businesses are now considered to have international criminal responsibility. These cyberattacks may be attributed to a state if the entities are under the direction, instruction, or control of the state, or if the state fails to exercise due diligence to prevent these attacks. In such cases, the state is internationally responsible and is obligated to stop the attacks and provide compensation for any damages caused. This research recommends adopting a binding legal document that would include provisions and rules regulating international responsibility for these attacks.

Keywords: Cyberattacks, International Criminal Responsibility, Non-State Entities, Cybersecurity, Cyberspace.

(1) College of Law – University of Sharjah (Sharjah – U.A.E.)
wallam@sharjah.ac.ae

(2) College of Law – University of Sharjah (Sharjah – U.A.E.)