الصراع السيبرانيّ في القانون الدوليّ

بين العقوبات السيبرانيَّة وإشكاليَّات التَّطبيق

أ.أسامة سالم محمد الفرجاني– كلية القانون – جامعة عمر المختار

ملخّص البحث

لوحظ في الفترات السابقة مدى سوء استعمال التطور العلمي بشأنِ اختراقات وهجماتٍ إلكترونيَّةٍ سيبرانيَّة؛ للوصول لأهدافٍ مختلفة غير مشروعة يقوم بها تارة أفراد للحصول على فائدة غير مشروعة، قد تتمثل بالحصول على فائدة ماليَّة أو معلوماتيَّة، وأيضاً قد تقوم بها بعض الدول لتحقيق غايات وأهدافٍ سياسيَّة أو عسكريَّة أو اقتصاديَّة، والهدف من كلِّ ذلك إلحاق الأذى والضَّرر بالدول والمنشآت المستهدفة، والحصول على معلومات وأسرار، ممَّا يؤثر سلباً على تلك الجهات المستهدفة.

ولقد أثارت العقوبات السيبرانيَّة المخاوف لدى العديد من أصحاب المصلحة في مجتمع المعلومات العالميّ، من أن يُشكّل ذلك سابقة يمكن أن تتكرَّر في الصراعات والنّزاعات المستقبليَّة، خاصة في ظل زيادة الأهميَّة الاستراتيجيَّة للمجال السيبرانيّ.

الكلمات المفاتيحية :

الصراع السيبراني – مشروعية العقوبات السيبرانية – الردع الالكتروني – قواعد القانون الدولي – الفضاء السيبراني .

Research Summary:

It has been observed in previous periods the extent of the misuse of scientific development regarding cyber penetrations and attacks to reach various illegal goals, sometimes carried out by individuals to obtain an illegal benefit, which may be represented by obtaining a financial or informational benefit, and also may be carried out by some countries to achieve political, military, or political goals and objectives. Economic, and the aim of all of this is to cause harm and damage to the targeted countries and facilities and to obtain information and secrets, which negatively affects those targeted parties.

Cyber sanctions have raised concerns among many stakeholders in the global information community that this will set a precedent that could be repeated in future conflicts and conflicts, especially in light of the increasing strategic importance of the cyber domain.

Keywords : Cyber conflict - legitimacy of cyber sanctions - electronic deterrence - rules of international law - cyberspace.

مقدّمة

ينطلق موضوع البحث من أهميَّة تداخل المجال السيبرانيّ مع بقيَّة المجالات الدوليَّة؛ كالبرّ والبحر والفضاء الخارجيّ، وهو الأمر الذي يجعل من العقوبات السيبرانيَّة فريدة في خصائصها وتأثيرها واتساع مجالها ومدى انتشارها، ممَّا يجعل تعرُّضها للأعمال العدائيَّة أو الانتقاميَّة يُمثل أضرارًا جسيمة بالمجتمع الدولي، خاصة في ظل تعاظم دور المتغيّرِ التّقنيّ في البيئة الدوليَّة، نتيجة حدّة الصراع السيبرانيّ، وتأثير ذلك في فاعليَّة وفرض العقوبات الدوليَّة.

وما يزيد من خطورة تطبيق نظام العقوبات السيبرانيَّة أنَّه تم تطويره بعيدًا عن حالة من التوافق الدولي أو المشروعيَّة الدوليَّة، ويُمثّل تهديدًا للجهود الدوليَّة في مجال حوكمة الإنترنت، وتعزيز التَّعاون الرَّقمي، وتجريم السلوك العدائيّ للدول في الفضاء السيبرانيّ. ويمكن تناول هذا الموضوع في الإطار الآتي:

أولاً: مشكلة البحث

تتمحور مشكلة البحث في تزايد الصراع السيبراني، وإشكاليَّة تطبيق العقوبات السيبرانيَّة، مع عدم وجود اتفاقيَّة دوليَّة بالخصوص تُلزم الأطراف الدوليَّة، ويثير ذلك التساؤلات الآتية:

1- ما أثر المتغيّر التكنولوجي في طبيعة العقوبات الدوليَّة؟

2 –ما إشكاليَّة تطبيق العقوبات السيبرانيَّة وفق القانون الدوليّ؟

3- ما التَّحديَّات أو الإشكالات التي تعترض بناء نظام دوليٍّ للعقوبات السيبرانيَّة؟

ثانياً: أهداف البحث

يهدف البحث إلى ما يلي:

1- دور الفضاء السيبراني في إدارة شئون الأفراد والمجتمع والدولة.

2- رصد طبيعة التحديَّات لبناء نظامٍ دوليٍّ للعقوبات السيبرانيَّة.

3- فهم طبيعة الصراع السيبرانيّ، ومدى مشروعيّته في ظل قواعد القانون الدولي.

ثالثاً: منهج البحث

تمَّ الاعتماد على المنهج التَّحليلي الذي اختصّ بتحليل أسباب التحوُّل في مفاهيم القوَّة والصراع، ومن ثمَّ أسباب التحوّل في شكل القوَّة، وأنماط التفاعلات الجديدة في الفضاء السيبراني، والمنهج المقارن الذي تمَّ اعتماده للمقارنة والتوصل إلى أوجه الاختلاف بين مظاهر القوة والصراع التقليدي، ومقارنتها بالفضاء السيبرانيّ.

رابعاً: مصطلحات البحث وتتمثل في الآتــي:

1-الفضاء السيبراني (Cyber Space):

عرَّفَ الاتحاد الدولي للاتصالات الفضاء السيبرانيّ بأنه: "المجال المادي وغيرالمادي الذي يتكوَّن وينتج عن عناصرهي: أجهزة الكمبيوتر، الشبكات، البرمجيَّات، حوسبة المعلومات، المحتوى، معطيات النقل والتحكُّم، ومستخدمي كل هذه العناصر"[1]. والفضاء السيبراني هو بيئةٌ تفاعليَّةٌ حديثة، تشمل عناصرماديَّة وغير ماديَّة، مكوَّن من مجموعة من الأجهزة الرَّقميَّة، وأنظمة الشبكات والبرمجيَّات، والمستخدمين سواء مشغلين أو مستعملين"[2].

2-العقوبات السيبرانية (Cyber Sanctions)[*]:

يمكن تعريفها بأنَّها استخدام -أو التهديد بفرض القيود على التعاملات الرَّقميّة- التأثير في إحداث تغيير سلوكي من قِبَلِ "فاعل" ما ينتج عنه التعرض للضغوط الاقتصاديَّة أو النفسيَّة، سواء كانت ضدَّ فرد أو مجموعة من الأفراد، أو نخبة سياسيَّة أو المجتمع داخل دولة ما، أو الحكومة أو أحد هيئاتها، أو تلك الإجراءات والتدابير المضادَّة التي يتمُّ فرضها من قِبَلِ طرفٍ دولي أو أكثر بُغية فرضِ حصار رقميٍّ

(1) The International Télécommunication Union ,**ITU Toolkit for CybercrimeLégislation,** Geneva, 2010, P. 12.

(2) سليم دحماني، أثر التهديدات السيبرانية على الأمن القومي الولايات المتحدة الأمريكية- أنموذجًا (2017-2021)، (رسالة ماجستير)، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، 2018م، ص23.

(*) من الشائع في الاستخدام قبل تبلور ظاهرة الفضاء السيبراني استخدام مصطلح العقوبات التكنولوجيَّة Technology Sanaction ، وأصبح يشير المجال السيبراني إلى كافة المكونات التي تتعلقب، وأصبح المجال السيبراني شاملًا لكل الأبعاد التقنية، وإن مصطلح Digital يشير إلى مكون من مكونات المجال السيبراني، وقد اعتمد الباحث على مصطلح Cyber Sanctions في هذا البحث.

شامل أو جزئيٍّ يكون له تبعات اقتصاديَّة وسياسيَّة على الجبهة الداخليَّة لدولة ما أو تحالفاتها الخارجيَّة[1].

خامساً: خطة البحث

تمَّ تقسيم الورقة البحثيَّة إلى المباحث الآتية:

المبحث الأول: الصراع السيبراني؛ ماهية ومستوياته وأسلحته.

المبحث الثاني: العقوبات السيبرانيَّة.

المبحث الثالث: مشروعية العقوبات السيبرانيَّة وإشكاليات التَّطبيق.

المبحث الأول

الصراع السيبراني: ماهية ومستوياته وأسلحته

قلَّص المجال الإلكتروني السيبراني حدود المكان والزمان، وأنشأ فضاءات دوليَّة وداخليَّة بالواقع الافتراضي، ممَّا أدَّى إلى نشوء مجالات جديدة للنّزاع تختلف عن النّزاعات القديمة التقليديَّة، وعلَّةُ التزايد الملحوظ لتلك الاختراقات سواءً كان مصدرها دول أو غيرها هو الوصول للسيطرة، وكأداة لتحقيق تلك الأهداف؛ الأمر الذي يتطلب تناول هذا الموضوع في إطار المطالب الآتية:

المطلب الأول : ماهية الصراع السيبراني

نتناول ماهية الصراع السيبرانيّ من حيث مفهومه والعديد من المصطلحات المرتبطة به، والعوامل المساهمة في نشوءه، كذلك تحديد طبيعته من خلال الفروع الآتية:

الفرع الأول : مفهوم الصراع السيبرانيّ

يُعرَّفُ الصراع (Cyber Conflict) في الساحة الافتراضيَّة، كونُهُ استخدام تكنولوجيا الحاسوب في الفضاء السيبراني (الإلكتروني)؛ لأغراض التدمير من أجل التَّأثير أو التغيير، أوِ التعديل في التفاعلات

(1) Maria Vsquez Callo-Müller, Iryna Bogdanova, "What is the Role of Unilateral Cyber Sanctions in the Context of The Global Cybersecurity Law-Making?", Voelkerrechtsblog, 10.05.2022. https://bit.ly/3wxuJJX

الدبلوماسيَّة والعسكريَّة بين الكيانات المختلفة، وذلك بعيدًا عن ساحة المعارك، وقد يأخذ ذلك الصراع نمطين:

الأول: الحوادث الفرديَّة (Cyber Incidents) ويُقصدُ بها العمليَّات والحوادث الافتراضيَّة التي تتمُّ على فترات مختلفة، وليست مستمرَّة لمدَّة معينة، أما الثاني: فهو النزاعات السيبرانيَّة (Cyber Disputs)، والتى تُدارُ بأدوات افتراضيَّة بين دولتين في مدَّة زمنيَّة معينة، ويحتوى على واحد أو أكثر من الحوادث الفرديَّة[1].

هنا من المهم الإشارة إلى أنَّ الصراعات السيبرانيَّة تختلف عن نظيراتها التقليديَّة، وبالأخص العسكريَّة، والتي تُعدُّ حكرًا على الدولة والجماعات المسلحة، وهى صراعات تدور في مساحة جغرافيَّة معيَّنة، وتستمرُّ لمدَّة زمنيَّة معيَّنة، وتكون محدَّدة الأطراف والأهداف، وإن كانت الصراعات المسلَّحة على أرض الواقع قد دخلت فيها أدوات تكنولوجيَّة لإدارة الصراعات بين الدول، فعندما تنشبُ حروب تقليدية بين الدول، تصبح قطاعات الاتصالات والمعلومات والبُنى التحتيَّة والمعلوماتيَّة ضمن الأهداف العسكريَّة، خاصة مع ارتباط تلك القطاعات بالأمن القومى للدول، ومن ثمَّ باتت هنالك أسلحة ذات طبيعة إلكترونيَّة ضمن الحروب، مثل وسائل التواصل الاجتماعي، والأقمار الصناعيَّة، وأسلحة النانو تكنولوجيَّة، والطائرات دون طيَّار، والأسلحة الروبوتيَّة.

وأيضًا ثمَّة فارق بين الصراعات السيبرانيَّة وما أسماه البعض "الهجمات الحركيَّة" أو ما يسميه البعض 'الهجمات غير المبرمجة Non Software-based Attacks، وهى تشمل الهجمات الماديَّة والمغناطيسيَّة ضدَّ الشبكات الإلكترونيَّة عبر أسلحة تقليديّة قد تشمل القنابل، والصواريخ، والعُبُوَّات النَّاسفة، وهى بذلك لا تُعدُّ هجمات إلكترونيَّة، أو نوعًا من الصراع في الفضاء السيبرانى، كونُها تستخدم آليات عسكريَّة تقليديَّة لإدارة الصراع[2].

بالإضافة لما سبق قد تختلف الصراعات في الفضاء السيبرانى عن نظيراتها التقليديَّة، حيث إنَّ الأخيرة تُفرّق بين مستويي الجرائم والحروب؛ فالجريمة هي مشكلة قانونيَّة تتمُّ مواجهتها بإنفاذ القانون ونظم العدالة، بينما تتعلَّق الحرب بالعسكريّين والأسلحة، أمَّا في سياق الصراعات السيبرانيَّة؛ فإنَّ جرائم

(1) Brandon Valeriano & Ryan C. Maness, The Dynamics of Cyber Conflict Between Rival Antaonists, Journal of Peace Research, 2014, Vol. 51, No. 3, pp. 48-349.

(2) وليد غسان سعيد، دور الحرب الإلكترونية في الصراع العربي- الإسرائيلي، (رسالة ماجستير)، جامعة النجاح الوطنية، كلية الدراسات العليا، 2013، ص97.

الإنترنت والحرب الإلكترونيَّة تنفذ باستخدام النوع ذاته من الأدوات والبنى التحتيَّة التقنيَّة، كما أنَّ تطور الهجمات الإلكترونيَّة هو دليلٌ على إلغاء الحدود بين جرائم الإنترنت والحرب الإلكترونيَّة، ذلك أنَّ كليهما يأتي من الصراع الإلكترونيّ.

وتعرَّضت ظاهرة الصراع إلى العديد من المتغيّرات، وذلك للتقدُّم التكنولوجي والإلكترونيّ كساحة للصراع بين الأشخاص المستخدمين سواءً دول أو غيرها، وهنا ظهر الصراع السيبراني كنوع من التضاد بأهداف ومصالح وقِيَم الفاعلين سواءً كان ذلك الخرقُ أو الإعتداء صادر عن الدول أو غيرها في المجال الإلكترونيّ.

وبالرَّغم من النَّتائج الكارثيَّة لتلك الصراعات والخروقات الغير منظورة للعيان، وبالشَّكل التقليديّ إلا أنَّه يؤدي خرق حسابات ومجالات إلكترونيَّة عديدة دون ترك أيّ أثر على ذلك، الأمر الذي يؤدّي في كثيرٍ من الحالات إلى الإضرار بالدول، وذلك بالعبث أو استخدام أسلحة الفضاءات الإلكترونيَّة المتعدّدة[1].

ونظراً لِلِاتساع والتطور التكنولوجي والإلكتروني زاد مجال تلك النّزاعات والإختراقات، وزاد عدد المحترفين بهذا المجال؛ الأمر الذي سبَّبَ الإرباك والخوف من الاستعمال غير المشروع والإجرامي لذلك المجال، ومن ثمَّ زاد الاهتمام بحيازة كافة وسائل الأمان، والحصول على كافة الوسائل الإلكترونيَّة الحديثة؛ لفرض السيطرة على المجال الإلكترونيّ، وضمان تطورهِ سواءً أكان ذلك بالمجال الداخلي أو الخارجي وتعزيز التَّنافس [2].

الفرع الثاني : مفاهيم أساسيَّة ذات علاقة بالصراع السيبرانيّ

من هذه المفاهيم، نذكر:

أولاً: ساحة صراع افتراضيَّة، بما أنه ليس صراعاً تقليدياً، إذًا هو صراعٌ مرتبطٌ بعالمٍ افتراضي يؤدي أحياناً إلى نتائج كارثيَّة لا يمكن تداركها بالمجالين الداخلي والخارجي، وبالرَّغم من أنَّها قليلة التَّكلفة من

(1) نوران شفيق، الفضاء الإلكتروني وأنماط التفاعلات الدولية: دراسة في أبعاد الأمن الإلكتروني، مرجع سابق، ص59.

(2) Paul Rosenzweig, Cyber Warfare How Conflicts In Cyberspace Are Challenging America And Changing The World Praeger Security International, 2013, pp. 15-16.

الصراعات الماديَّة إلا أنَّها أكثر منافسة وتحدٍّ بين مستخدميها وتعتمد على التطور، وهي بذلك أكثر تحدٍّ من النزاعات القديمة التقليديَّة [1].

ثانياً: زيادة الاعتماد الإلكترونى، إذ باتت الدول الحديثة تربط بِنْيَتَهَا التحتيَّة بالفضاء السيبراني، خاصة شبكات الكهرباء والمياه والبنوك والبورصة والاتصالات وغيرها، بالإضافة إلى أنظمة السيطرة والتحكم العسكريَّة، وجمع المعلومات، مثل الأقمار الصناعيَّة والطائرات دون طيار في الحروب، لذا أضحى استهداف تلك البُنى التحتيَّة للدولة ذات الطابع الإلكترونيّ أحد عوامل الصراع السيبراني[2].

ثالثاً: تمادي حدود الداخل والخارج؛ أي- وجود حالة من التأثير الشبكيّ المتزايد داخل الدول وخارجها، حيث اتَّسع استخدام الأفراد والجماعات والدول للتكنولوجيا الحديثة المرتبطة بالفضاء السيبراني؛ سواء أكانت مواقع تواصل اجتماعى على الإنترنت، أم هواتف ذكيَّة، أم مواقع عامَّة للتعاملات الماليَّة والتجاريَّة والخدميَّة، ويتصل كلُّ ذلك بشبكةٍ مترابطةٍ من خلال أنظمة تحكُّمٍ تكنولوجيَّة ترتبط بالإنترنت؛ بما يجعل الخدمات والمعلومات مُتاحة للجميع، الأمرُ الذى قد يُعرّضها للاستهداف.

رابعاً: صعوبة الرَّدع الإلكترونيّ، على أساس أنَّ الفضاء السيبرانيّ ساحة افتراضيَّة، لذا يصعب على الدول وضع حدود لسيادتها عليه، ومع ضعف القوانين الدوليَّة للسيطرة على هذا الفضاء، يغيب الرَّدع في ظل إمكانيَّة التنكر على شبكة الإنترنت، ومجهوليَّة مصدر الهجمات الإلكترونيَّة، وسهولة أن يقوم بها الأفراد، وليس الدول فقط، حيث زادت خبرات القراصنة بشكل متطور دون الحاجة لنُظُمٍ معقَّدة كانت تملكها الدول وحدها في الصراعات التقليديَّة[3].

خامساً: غياب الشفافية الإلكترونيَّة، مع عدم القدرة على معرفة هُويَّات القائمين على هجمات القرصنة نَشَبَتْ معضلة غياب الشفافية والقوانين المقيّدة للصراعات في المجال الإلكترونيّ، فضلًا عن ذلك فإنَّ مصدر الهجمات الإلكترونيَّة قد يُسبّب خسائر واسعة دون أن يعني ذلك وجود عنف ملموس، ممَّا لا يعنى بالضرورة وجود هجوم مضادّ أو استمرارِ الصراع[4].

---

(1) ايهاب خليفة، الكتائب الإلكترنية، الملامح العامة لحروب مواقع التواصل الاجتماعي في الشرق الأوسط : اتجاهات الأحداث، مركز المستقبل للدراسات والأبحاث المتقدمة، مج1، ع4، نوفمبر 2014م، ص9.

(2) محمود محارب، إسرائيل والحرب الإلكترونية: قراءة في كتاب حرب الفضاء الإلكتروني: اتجاهات وتأثيرات على إسرائل، المركز العربي للأبحاث ودراسة السياسات، الدوحة، أغسطس 2011م، ص3.

(3) إيهاب خليفة، إمكانيات تحقيق الردع في صراعات الفضاء الإلكتروني،اتجاهات الأحداث، ع13، 2015م، ص13.

(4) نوران شفيق، الفضاء الإلكتروني وأنماط التفاعلات الدولية: دراسة في أبعاد الأمن الإلكتروني، (رسالة ماجستير)، جامعة القاهرة: كلية الاقتصاد والعلوم السياسية، 2014، ص45.

الفرع الثالث :العوامل المساهمة في نشوء الصراع السيبرانيّ

أدَّتِ العديد من العوامل إلى اتّساع وانتشار الصراعات السيبرانيَّة؛ منها:

أولاً: اختلاف مفاهيم وطرق الحروب التقليديَّة وبشكلٍ شبه كامل، حيث كانت المفاهيم في السَّابق هي قمع العدو وهزيمته باحتلال أرضه والاستيلاء عليها وعلى كافة مواردها.

أمَّا حديثاً فقد تطورت أنماط الحروب، وذلك بالسيطرة على إرادة تلك الشعوب والمجتمعات، سواءً أكان ذلك الهدفُ متعلق بشعوب تلك الدول المستهدفة، أو بالتَّأثير والسيطرة على الرأي العام الداخلي والخارجي.

حيث لم تَعُدِ الحرب حرباً ماديَّة "تقليديَّة" –كما في السابق– بل تجاوزت ذلك إلى حربٍ معنويَّة هدفها نفسيّ، وهو التَّأثير على الرَّأي العام، ممَّا ساهم في تطور تلك الحروب الإلكترنيَّة السيبرانيَّة التطوُّرَ المهول في ذلك المجال، والذي أدَّى إلى ضعف الدول والحكومات بالتحكم في مفاهيم وتوجيهات مواطني تلك الدول، الأمرُ الذي أدَّى إلى تزايُدُ الإهتمام بذلك النوع من الحروب.

ثانياً: ظهور نزاعات محليَّة – دولية، ما بعد الحرب الباردة وكذلك الطبيعة القانونيَّة للنَّهج الدوليّ للتطور الإلكترونيّ في ظهور وتوفر مناخٍ ملائمٍ لِانخراط فئاتٍ كانت بالسابق غير بارزة، وإنشاء تكتُّلاتٍ بالمجتمع الدوليّ مستندة إلى مفاهيم واعتمادات ذات طبيعة عرفيَّة أو دينيَّة [1].

الأمرُ الذي أدَّى إلى تطور وبروز تلك الفئات من غير الدول، وشكلت قوة ماديَّة ومعنويَّة ذاتِ تأثير مباشر على الحروب.

الفرع الرابع :طبيعة الصراع السيبراني

وهي تختلف وفقاً لغاية وطبيعة الصراع السيبراني وذلك على النحو الآتي:

أولاً: صراع سيبرانيٌّ ذو طبيعة سياسيَّة، وهو صراع مدفوع بأسباب سياسيَّة بحتة، وقد يكون عسكريًّا هدفة وغايته نسف أنظمة المعلومات والبنى التحتيَّة، ويكون ذلك من قِبَلِ مستخدمين داخل الدولة والمجتمع نفسه، وقد يكون بالتعاون ودعمٍ مقدَّمٍ من جهات أخرى؛ للوصول لتلك الأهداف السياسيَّة.

(1) Johan Eriksson And Giampiero Giacomello, The Information Revolution, Security, And International relations: Ir Relevant Theory? International Political Science Review, Vol. 27, No. 3, Jul. 2006, pp. 229-235.

ثانياً: صراع سيبرانيٌّ أقل حدّة وسلاسة، هدفُهُ المباشر التأثير وكسب الرأي العام من خلال التحكُّم والتَّأثير الكبير المباشر على المشاعر والأحاسيس، وذلك عن طريق وسائل التواصل الاجتماعيّ المختلفة؛ كتسريب البيانات والمعلومات ذات الطبيعة الدوليَّة، مثال ذلك ما قام به موقع ويكليكس وما أحدثه من آثارٍ دبلوماسيَّة بين الدول.

ثالثاً: صراع سيبرانيٌّ على التقدم التكنولوجي, حيث يأخذ هذا النمط من الصراعات السيبرانيَّة طابعًا تنافسيًّا حول الاستحواذ على سباق التقدم التكنولوجي، وسرقة الأسرار الاقتصادية والعلميَّة، وقد يمتدُّ إلى محاولةٍ للسيطرة على الإنترنت، وعناوين المواقع، والتحكُّم بالمعلومات، والعمل على اختراق الأمن القوميّ للدول؛ كهجمات قراصنة الكمبيوتر، وتدمير المواقع والتجسُّس، بما قد يكون له من تأثيرات مدمرة على الاقتصاد والبنية التحتيَّة.

رابعاً: صراع سبرانيٌّ إستخباراتي، نظراً للتداخل بين الأنشطة الإستخبارتيَّة، وجمع المعلومات المنتجة من جهة، وكذلك الحروب الإلكترونيَّة من جهة أخرى ، بذلك يكون الفضاء الإلكترونيّ جواً ملائماً لتلك الصراعات السيبرانيَّة، حيث إنَّ ذلك ساهم بشكلٍ كبير في التطور الأمنيّ للدول، وحتى التشكيلات المختلفة في هذا المجال، مع صعوبة إثبات تورُّط تلك التشكيلات بشكلٍ مباشر، كذلك قلة التكاليف الماديَّة، وصعوبة الضبط والرقابة عليها بالشكل التقليديّ، فقد ساهم ذلك بنمو وتطور الأسلحة والمعدّات الإلكترونيَّة للوصول لأهداف قد تكون عسكريَّة أو سياسيَّة[1].

المطلب الثاني : مستويات الصراع السيبرانيّ وأسلحته

يُنظر لمستويات الصراع السيبرانيّ على أنَّها هرميَّة الشكل من حيث تأثيراته؛ فيأتي في قاعدته الحالات الأكثر حدوثًا، وهى الجرائم الإلكترونيَّة التي تنطوي على الاحتيال وسرقة الأموال والهُويَّات، وهى أحيانًا تكون كارثيَّة، ولكن تهديدها ليس ساحقًا، ولا تُمثل تهديدًا وجوديًّا، وفي أواسط الهرم يبرز "التجسُّس السيبراني"، وهو أكثر تطورًا، حيث يشمل هجمات إلكترونيَّة من فاعلين من الدول، وغير الدول لسرقة الأسرار القوميَّة، أو حقوق الملكيَّة الفكريَّة، وذلك النَّمطُ هو الأكثر انتشارًا على الساحة الدوليَّة، وله آثاراً سلبيَّة على الأمن القوميّ للدول، وفى قمَّة الهرم يظهر ما يسمَّى بـ "الحروب السيبرانيَّة" بين الدول ذات القدرات الحاسوبيَّة المتطورة التي تتصارع فيما بينها، ورغم أنَّ ذلك النوع من الحروب لم يظهر بشكلٍ

(1) Timothy J. Junio, The Politics And Strategy Of Conflict, Phd Thesis, University of Pennsylvania, 2013, pp. 28-30.

مستقلٍ عنِ الحروب التقليديَّة، فإنَّه حال كان منفصلًا؛ فقد تكون الآثار التدميريَّة له أعلى بكثيرٍ من الحرب التقليديَّة[1].

في هذا الإطار؛ هناك أربعة أسلحة رئيسة في الصراعات السيبرانيَّة هي:

أولاً: تخريب ومهاجمة مواقع الإنترنت Website Defacements or Vandalism وهو أبسط أشكال الأسلحة السيبرانيَّة، ويستهدف مهاجمة مواقع الخصم بغرض التدمير، أو التَّشويه عبر نشر النُّصوص والصور المسيئة، وذلك لتوصيل رسالة إلى الهدف بأنَّه يفتقر القدرة للسيطرة على عمليَّات الفضاء الإلكترونيّ الخاصة به، وبرغم أنَّ ذلك النَّوع من الأسلحة الإلكترونيَّة قد لا يؤثر في الحكومات؛ فإن تأثيراته قد تكون مضاعفة في المجتمعات.

ثانياً: الحرمان من الخدمة Denial of Service Method وهو سلاح أكثر تطورًا؛ حيث يستهدف أجهزة التَّوجيه التي تغلق المواقع الإلكترونيَّة وتوقف الخدمات، مثل توقُّف الخدمات الحكوميَّة المقدّمة عبر المواقع الرَّسميَّة للدولة.

ثالثاً: الاقتحام الفيروسي Intrusions وهو سلاح أكثر حدَّة على المدى الطويل في الهجمات الإلكترونيَّة، خاصة أنَّه يظل كامنًا لفترة طويلة، ويظهر دون سابق إنذار، ويتكون هذا السلاح من برامج خبيثة يصعب الكشف عنها، وتقوم بسرقة المعلومات، وتكون لها آثار كبيرة على المصالح الحيويَّة للدولة، وقد لا يحتاج هذا السلاح إلى قراصنة، وإنَّما برامج تقوم عليها الدول.

رابعاً: عمليَّات التسلل Infiltrations وفيها يقوم المهاجم بمحْوِ جميع البيانات داخل نظام أو شبكة إلكترونيَّة لدولةٍ أخرى، كما قد يتكرَّرُ الهجوم بقصد إفساد، أو تعديل الملفات؛ أي- التقاط المعلومات المتدفّقة عبر الويب، وهذه النَّوعيَّة من الأسلحة الإلكترونيَّة متطورة للغاية، وأكثر استهدافًا للعدو، نظرًا لفداحة تأثيراتها، خاصَّة إذا كانت تستهدف البنى التحتيَّة للدول[2].

(1) Jason Healey, The Five Futures of Cyber Conflict And Cooperation, Georgetown Journal of International Affairs, pp. 110-116.
(2) Brandon Valeriano & Ryan C. Maness, op. cit., pp. 353-355.

المبحث الثاني : العقوبات السيبرانيَّة

العقوبات السيبرانيَّة كنمطٍ جديدٍ للعقوبات الدوليَّة، تشير إلى تبنّي قيود اقتصاديَّة أحادية الجانب يتمُّ فرضها وفقًا للقوانين المحليَّة للدَّولة، وتهدف إلى ردع ومعاقبة الجهات الفاعلة المسئولةِ عنِ السلوك الخبيث القائم على الإنترنت.

والعقوبات الدوليَّة قد تُفرض بشكلٍ مؤقت أو دائم، وتأخذ أنماطًا عدة؛ منها: تجميد الأصول، وفرض قيود على العلاقات الاقتصاديَّة مع الأشخاص، أوِ الكيانات الخاضعة للعقوبات، إلى جانب حظر السفر على الأفراد، وغيرها من التَّدابير المضادة، مثل فرض الغرامات الماليَّة، أو منع تصدير، أو استيراد سلعة، أو تقنيات مرتبطة، بينما تُشيرُ العقوبات السيبرانيَّة إلى فرض (العُزلة الرقميَّة القسريَّة) ليس على الدولة المستهدفة فقط، بل كذلك على الأفراد والشُّركاء التجاريّين من الخارج، سواء كانت شركات أو دول أخرى[1].

ويختلف تأثير فرض العقوبات السيبرانيَّة عن تأثيرات (الفجوة الرَّقميَّة) Digital Divide التي تتعلقُ بالفجوة بين الذين بمقدورهم استخدام الإنترنت بسبب امتلاكهمُ المهارة اللازمة والقدرة الماديَّة، والذين لا يستطيعون، ويكون ذلك غير مقصود لكنَّه قد يحمل دلالات سياسيَّة وتنمويَّة؛ كحالة منع الدول الكبرى تصدير التكنولوجيا المتقدّمة إلى الدول النَّامية ممَّا تسبب في وجود فجوة رقميَّة وتكنولوجيَّة.

وتختلف العقوبات السيبرانية عن حالة الحروب السيبرانية (Cyber War)؛ لأنَّها تقع في المنطقة الرَّمادية بين الحرب والسلام؛ كحالة التَّنافس الدوليّ على الأسواق الرقميَّة بين القوى الدوليَّة التي من أهم إرهاصاتها الحرب التجارية بين الشرق "روسيا والصين"، والغرب "الولايات المتحدة وحلفاؤها"، وقد يتمُّ استخدام العقوبات السيبرانيَّة كنمطٍ من أنماط الدبلوماسيَّة السيبرانيَّة (Cyber) Diplomacy إلى جانب نمط التعاون الرقميّ، وتُعنى الدبلوماسيَّة السيبرانيَّة باستخدام الأدوات الدبلوماسيَّة لمعالجة القضايا النَّاشئة في الفضاء السيبرانيّ، وتشمل هذه القضايا مجموعة من الموضوعات الأمنيَّة والاقتصاديَّة وحقوق الإنسان، بما في ذلك معايير الأمن السيبرانيّ الدوليَّة، والوصول إلى الإنترنت، والخصوصيَّة، وحريَّة الإنترنت، والملكيَّة الفكريَّة، والجرائم الإلكترونيَّة[2].

(1) Maria Vásquez Callo-Müller, Iryna Bogdanova, "What is the Role of Unilateral Cyber Sanctions in the Context of The Global Cybersecurity Law-Making?", Voelkerrechtsblog, 10.05.2022. https://bit.ly/3wxuJJX

(2) Emily O. Goldman, "Fresh Thinking and new approaches are needed on diplomacy's newest frontier", The Froeign Service Journal, Kune2021.

ويمكن تناول العقوبات السيبرانيَّة من خلال المطالب الآتيـة:

المطلب الأول :العقوبات السيبرانيَّة ومفهوم السيادة الرَّقميَّة

يُعبّر مفهوم السيادة الرقميَّة Digital أوِ السيبرانيَّة Cyber Sovereignty عن جهود الدولة لإنشاء حدودٍ على الشَّبكة، ومن ثمَّ ممارسة شكلٍ من أشكال التحكم والسيطرة، ويمكن أن يأتي في شكل إنفاذ القانون على هذه الحدود، وترتبط بقدرة الدولة ذات السيادة على فرض قوانينها أو تشريعاتها على تدفُّقِ البيانات والمعلومات إليها من الخارج إلى الداخل، أو من الداخل إلى الخارج، ومن ثمَّ فإنها تُعدُّ بمنزلة اختيارٍ ذاتيٍّ "للعزلة الرقميَّة" Digital Isolation من قِبَلِ الدولة[1].

وتبنَّتِ العديد من الحكومات قوانين جديدة لتشكيل هُويّتها الوطنيَّة والإقليميَّة، والسيطرة على امتلاك البيانات، وبدأت فكرة سيادة الإنترنت وتشريعاته حول العالم تلعب دورًا في عمليَّة تفتيت وأقلمة الإنترنت، والكشف عن التّجسُّسِ الأمريكيّ على الملايين عبر العالم، وأخذت الهيمنة على الإنترنت ترتبط بأبعادٍ أمنيَّة واقتصاديَّة وتنظيميَّة وسياسيَّة واجتماعيَّة، والعمل على ممارسة المزيد من الرَّقابة والتحكُّمِ في تدفُّق المعلومات الحرجة والحسَّاسة؛ مثل تبنّي الصين، وفرض "جدار الصين العظيم للحماية" Great Firewall Of China الذي يحدُّ من الوصول إلى البيانات من جانب العديد من الشركات الأمريكيَّة» مثل شركة جوجل وميتا.

فقد أدى قيام الولايات المتحدة وبعض الدول الأوروبيَّة بفرض عقوبات على بعض الدول كإيران، وكوريا الشماليَّة مثالًا إلى بناء وتطوُّر كفاءاتٍ بهذا المجال للوصول إلى السيادة السيبرانيَّة [2].

كما إنَّ لغلق الإنترنت خسائر اقتصاديَّة تتكبّدها الحكومات التي قد تتمُّ لأسباب سياسيَّة أو أمنيَّة، وهو ما يكشف من جهة أخرى عن ما يُمكن أن تتكبّده الدول حال فُرِضَ عليها حصار رقميّ من الخارج؛ ففي عام 2022م بلغت الخسائر ما قيمته 1.5 مليار دولار في روسيا، وتأثر ما يزيد على 113 مليون مستخدم، وتأثر 16.1 مليون مستخدم، و429.5 مليون دولار في كازاخستان، و207.7 مليون دولار،

---

https://afsa.org/cyber-diplomacy-strategic-competition

(1) إبان ما عُرف بثورات الربيع العربي قامت العديد من الحكومات العربية بقطع الإنترنت؛ سعيًا منها للسيطرة على موجة الاحتجاجات عام 2011م لاعتبارات تتعلق بالأمن القومي.

(2) Philip N. Howard, Sheetal D. Agarwal, and Muzammil M. Hussain, "The Dictators' Digital Dilemma: When Do States Disconnect Their Digital Networks?", The Center for Technology Innovation, The Brookings Institution, Issues on innovation Technology , Number 13, October 2011.

https://www.brookings.edu

وتأثَّر 1.6 مليون مستخدم في ميانمار، وتأثَّر 104.4 مليون مستخدم و82.7 مليون دولار في نيجيريا، وتأثر نحو مليون مستخدم و33.2 مليون دولار في إثيوبيا، وفي العام ذاته شهدت 16 دولة 54 انقطاعًا للإنترنت بشكل متعمّد، وأدَّى ذلك لتكلفةٍ بلغت قيمتها 10.16 مليار دولار، بينما شهد عام 2021م 50 انقطاعًا بتكلفة 5.45 مليار دولار فقط [1].

المطلب الثَّاني : خصائص ومراحل وأنماط العقوبات السيبرانيَّة

تتميَّزُ العقوبات السيبرانيَّة بطبيعةٍ متداخلة من التأثير الاقتصادي أو العسكري أو الدبلوماسيّ، وغيره من الأبعاد المرتبطة بالنَّشاط السيبرانيّ، وعلاقته بتلبية الاحتياجات الإنسانيَّة، وهو الأمر الذي أحدث تأثيراتٍ عميقة تتجاوز التأثير التقليدي لباقي أنماط العقوبات الدوليَّة الأخرى، وذلك بالنَّظر إلى مداها وانتشارها والخسائر المتوقّعة منها، وتأثيرها العابر للحدود، وإمكانيَّة إصابة أطراف ثالثة ليست معنيَّة، أو طرفًا في الصراع المباشر مع الدولة التي فرضت تلك العقوبات السيبرانيَّة.

وأصبح لعزل الدولة كليًّا أو جزئيًّا عنِ المجال السيبرانيّ بشكلٍ قسريٍّ تأثيرات متعدّدة على السكان المدنيّين الأبرياء، ويتمُّ فرضها من قِبَلِ دولة أو أكثر، ويكون للشركات التقنيَّة العابرة دورٌ فيها، ويكون لها تأثير عميق بشكلٍ مباشر وغير مباشر في كافة القطاعات داخل الدولة، بما في ذلك المنشآت المدنيَّة، والخدمات المقدَّمة إلى المدنيّين، إلى جانب التَّأثير في الجهات الرَّسميَّة داخل الدولة.

وتتمُّ مراحل ومستويات الإسناد لفرض العقوبات السيبرانيَّة بعد حدوث الاعتداء السيبرانيّ أوِ النَّشاط المُعادي، وتحميل المسئوليَّة استنادًا إلى ما تراه (الدولة) من أدلة رقميَّة تُثبت التورُّطَ أو العلاقة بشكلٍ مباشر أو غير مباشر، أو كونُهَا تدخل في حالة التوتر الدوليّ بين القوى الدولية.

وتأتي المرحلة الأولى وهي ترتبط بالإسناد التقني من خلال التحرّي الإلكترونيّ، والبحث عن الأدلَّة لمعرفة هُويَّة المهاجم، ثمَّ تأتي المرحلة الثَّانية بالإسناد السياسي، وهي تتعلق بجمع المعلومات وتبادلها حول تحديد الإجراءات وتسمية الجُناة إن أمكن، ثمَّ تأتي المرحلة الثالثة بتوجيه اللَّوم الجنائيّ ولائحة الاتّهام، ثمَّ ينبثق من ذلك المرحلة الرَّابعة، وهي ردُّ الفعل السياسيّ والتَّشاورِ بين السلطة التنفيذيَّة والتشريعيَّة حول فرض العقوبات السيبرانيَّة.

(1) تقرير: قطع الإنترنت المتعمد تسبب في خسائر ب 10 مليارات دولارفي عام 2022م،صحيفة الشرق، 7 يوليو 2022م على الرابط:

https://bit.ly/3AsI4YV

ومن ضمن أنماط العقوبات السيبرانيَّة التي تأخذ نمطًا تقنيًّا أو ماليًّا أو تشريعيًّا يتمُّ تطبيقه بشكلٍ منفردٍ أو مجتمع من قِبَلِ الدولة الخصم ضدَّ دولٍ أخرى أوِ العكس، أو ضدَّ طرف من غير الدول[1]؛ منها:

أولاً: حجب مواقع إلكترونيَّة إعلاميَّة أو حكوميَّة رسميَّة من الولوج إلى الدَّاخل.

ثانياً: منع تصدير تقنيات التجسُّس ومراقبة الاتصالات أو التقنية المتقدّمة.

ثالثاً: منع عمل شركات تقنيَّة وطنيَّة في البلد المعنيّ بحُجَّة الحفاظ على الأمن.

رابعاً: ممارسة ضغوطٍ على الشركات التقنيَّة الكبرى لسحب خدماتها من الدَّاخل.

خامساً: تجميد التعاون في مجال البحث العلمي والإبتكار والإستثمار الأجنبيّ.

سادساً: شنُّ هجمات سيبرانيَّة ضدَّ البنية التحتيَّة الحيويَّة، خاصة المواقع الرَّسميَّة.

سابعاً: شنُّ تطبيقات الحروب النفسيَّة والمعلومات المضلّلة والأخبار الزَّائفة.

ثامناً: قطع الكابلات البحريَّة المرتبطة بخدمة الإنترنت الواصلة للدولة المستهدفة.

تاسعاً: فرض غرامات ماليَّة على الشركات الأجنبيَّة تحت دعاوَى انتهاك القوانين المحليَّة.

عاشراً: فرض رسوم جمركيَّة على استيراد مكونات تقنيَّة من الخارج من دولٍ محدَّدة.

وتدخل إجراءات فرض العقوبات السيبرانيَّة ضمن الرَّدع السيبرانيّ[2]، وضمان تعزيز القدرة على منع الخصم من الفعل أو رد الفعل داخل المجال السيبرانيّ، ولفرض الامتناع عن الإتيان بأنشطة سيبرانيَّة، سواء على مستوى الدفاع أو الهجوم، أوِ العمل على منعه من تطوير قدراته، سواء على مستوى الهجمات السيبرانيَّة، أو في مجال الدفاع السيبرانيّ، أو في مجال التنمية التقنيَّة.

ويتمُّ فرض العقوبات السيبرانيَّة إمَّا للرَّد على القيام بأنشطة سيبرانيَّة مُعاديةٍ في شكل قرصنةٍ أو اختراقات، أو أن تأتي للرَّد على تدخُّلات ناعمة عبر توظيف المجال السيبرانيّ في الأنشطة التجسُّسيَّة،

---

[1]) أندريه بوفر،الردع والإستراتيجية، ترجمة: أكرم ديري، دار الطليعة للطباعة والنشر ،بيروت،لبنان، 1970م،ص 31

[2]) رغدة البهي، الردع السيبراني، المفهوم والإشكاليات والمتطلبات،**مجلة العلوم السياسية والقانون**،العدد 1، 2017م،على الرابط :

https://democraticac.de

أو شنّ الحروب النفسيَّة، أو نشر المعلومات والأخبار المضلّلة، أوِ التدخُّلِ في الشئون الداخليَّة، أو تأتي العقوبات السيبرانيَّة –التي قد تفرضها الدولة محليًّا– للرَّد على انتهاك القوانين المحليَّة المُنظّمة للتجارة والاستثمار الأجنبيّ، وتبنّي الدَّولة سياسة حمائيَّة ضدَّ المنتجات المستوردة من الخارج.

وقد تأتي العقوبات السيبرانيَّة في محاولةٍ لتضييق الخناق على الدولة المتورّطة في صراعٍ عسكريٍّ مع دولةٍ أخرى، وممارسة الأطراف الدوليَّة المساندة لأحدِ طرفي الصّراع؛ للضغوط الاقتصاديَّة والماليَّة والتجاريَّة. ويتمُّ فرض العقوبات السيبرانيَّة لتعزيز قدرة الدولة على حماية أمنها القوميّ، وردع الجهات الفاعلة في الأنشطة والتهديدات السيبرانيَّة، وتضمين الاستجابة الوطنيَّة في إطار الجهود العالميَّة لمواجهة التَّهديدات السيبرانيَّة.

وبالرَّغم من غلبة الأهداف الأمنيَّة على فرض العقوبات السيبرانيَّة، إلا أنَّها تكشف عن أهداف اقتصاديَّة أو سياسيَّة أو قانونيَّة أو ثقافيَّة بشكلٍ فرديٍّ أو مجتمعة.

وتُفرض «العقوبات السيرانيَّة» من قِبَلِ الحكومة أو الدولة لحماية الصناعة أوِ الابتكار، أو حماية الملكيَّة الفكريَّة، أو حقوق النَّشر أو حماية الأسرار التجاريَّة.

المطلب الثالث : تأثير التطور التكنولوجيّ والمجال السيبرانيّ في البيئة المصاحبة للعقوبات الدوليَّة

تعتمد العقوبات الدوليَّة على تبنّي تدابير قمعيَّة أو إكراهيَّة للضغط على بلدٍ ما لتغيير سياساته المحدّدة، سواء تمّ ذلك تحت مظلَّة أمميَّة، أو بإجراءات أحاديَّة من جانب الدول، ولا تشتمل على استخدام القوة العسكريَّة المباشرة مثل العقوبات الدبلوماسيَّة والعسكريَّة والرياضيَّة والبيئيَّة والاقتصاديَّة [1]. وقد أثرت التطورات التكنولوجيَّة في البيئة الدوليَّة للعقوبات من خلال:

أولاً: توفير بيئة دوليَّة جديدة يغلب عليها زيادة حدّة التنافس الدولي ذي الطَّبيعة التجاريَّة أوِ الاستخباراتيَّة، سواء بين الدول القوميَّة أو بينها وبين الفاعلين من غير الدول.

(1) نيكو السمولدر، سلاح العقوبات، مجلة التمويل والتنمية، صندوق النقد الدولي، ع59، ق2، يونيو 2022م ص20. على الرابط:
File://c:/users/GR/Downloads/fd0622a.pdf

ثانياً: تصاعد اتجاه الدول لتوظيف الفضاء السيبراني في ممارسة الضغوط والإكراه[1] في صراعها مع الآخرين، وارتفاع تكلفة اللُّجوء إلى القوة العسكريَّة المباشرة مقارنة بالأنشطة السيبرانيَّة العدوانية، وضغوط الرَّأي العام العالمي المناهض للحرب، إلى جانب منظَّمات المجتمع المدنيّ العالميّ في منع الانزلاق في حرب مباشرة .

ثالثاً: إحداث العقوبات الدوليَّة خسائر تجاريَّة واقتصاديَّة أكثر من السابق في الوقت نفسه زادت القدرة على التَّخفيف من وطأتها، والالتفاف حول مساراتها عبر وسائط تِقنيَّة حديثة، وأصبحت لا تُشكّل العقوبات تهديدًا مباشرًا كما كانت عليه إبَّان فترة الثلاثينيَّات من القرن الماضي، وهو ما يحدُّ من تحقيق أهدافها التي منها التَّصعيد العسكري.

رابعاً: تغيُّر طبيعة العقوبات من حيث المخاطر والتكلفة النَّاجمة عنها، بينما ظلَّت قنوات انتشارها فضلًا عن تأثيرها على ارتفاع السلع الأوليَّة، وتعطيل سلاسل الإمداد العالميّ، والخسائر الاقتصاديَّة، ومستوى التأثير في حياة المواطنين بعيدًا عن النُّظم السياسيَّة.

خامساً: أصبح للتغييرات التقنيَّة دورٌ في وجود بنية تحتيَّة كونيَّة للمعلومات تُمثّلُ إدارتها أهمّ تحديات الأمن الجماعي الدوليّ، وغياب ذلك قد مثَّل مناطًا للتَّوظيف السياسي من جانب الدول المهيمنة تقنيًا مثل الدور الأمريكي في إدارة الموارد الحرجة للإنترنت.

سابعاً: إحداث تغييرات في التجارة الدوليَّة والتعاملات الماليَّة عبر الحدود، وتعاظم دور الشركات التقنية الكبرى، ما يطرح إشكالات أمام مستقبل النّظام الاقتصادي العالمى، خاصَّة طبيعة النظام المالي العالمي، مع ظهور العملات المشفّرة والأصول الرقميَّة.

المبحث الثالث : مشروعيَّة العقوبات السيبرانيَّة وإشكاليَّات التَّطبيق

لتبيان مشروعيَّة العقوبات السيبرانيَّة في ضوء القانون الدولي، يُثار التساؤل الآتي: إلى أيِّ مدىً حقَّقت العقوبات السيبرانيَّة ردعاً في مواجهة الصراعات السيبرانيَّة، وما الإشكاليَّات التي تواجه تطبيقها؟ هذا ما يمكن تناوله في المطالب الآتية:

1) أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية ومخاطر مواجهتها في القانون الدولي العام، **مجلة الشريعة والقانون**،عدد 35،ج3 ،2020م، ص 383 – 384

المطلب الأول :مشروعيَّة العقوبات السيبرانيَّة

تبدو العلاقة بين التَّقنية والقانون متسارعة، وكان للتّقنية دورٌ تاريخيّ في تبنّي قوانين دوليَّة جديدة تنظم الواجبات والحقوق وتنظم استخدام المجالات الدوليَّة، مثل المجال الجوي أو البحري أو الفضاء الخارجي، ودفعت حالة الفراغ القانونيّ نتيجة عدم وضع معايير دوليَّة ملزمة لتنظيم السلوك الدولي، ومسئوليَّة الدولة عبر المجال السيبرانيّ إلى اتّخاذ بعض الدول إجراءات أُحاديَّة، ومنفردة للدفاع عمَّا تراه مصالحها أو قيمها أو أمنها القوميّ.

وفي محاولةٍ للدفاع والحماية ضدَّ مخاطر الأمن القوميّ، ظهرت العقوبات السيبرانيَّة كأحد الإجراءات الأحاديَّة التي يتمُّ فرضها دون شرعيَّة دوليَّة، أو أي قرار يمكن أن يصدر من الجهة المخوَّلة دوليًّا بإصدار العقوبات الدوليَّة، وهي مجلس الأمن الدولى.

وأصبح للعقوبات السيبرانيَّة تأثيرات تتجاوز المجالات الدوليَّة والأبعاد المتعدّدة التي تتراوح بين التأثيرات الاقتصاديَّة والإنسانيَّة والثقافيَّة وغيرها، وينبع ذلك من حقيقة دور المجال السيبرانيّ في مختلف الخدمات المدنيَّة، وما يزيد الأمر صعوبة إمكانيَّة الاستخدام المزدوج بين العسكريّ والمدنيّ، وبين التعاون والصراع وبين الحقيقة والتَّضليل[1].

ومن جهةٍ أخرى فإنَّ العمل على توسيع دائرة العقوبات السيبرانيَّة إلى جهات حكوميَّة ورؤساء أو مسئولين سياسيّين يُعارضُ مقرَّرات القانون الدبلوماسي الذي يُعطي لهم حصانة دبلوماسيَّة من التعرُّض للمحاكمات أو العقوبات، وأنَّ ذلك يمكن أن يتمّ من خلال توجيه أدلَّة الِاتّهام إلى المحاكم المحليَّة أوِ اللُّجوء إلى محاكم دوليَّة، مثل المحكمة الجنائيَّة الدوليَّة أو محكمة العدل الدوليَّة [2].

وتُتيحُ قضيَّة عدم وجود معاهدة دوليَّة للفضاء السيبرانيّ الفرصة أمام الدول للمناورة والتهرُّب من تحمُّل المسئوليَّة عن سلوكها عبر الفضاء السيبراني، ولكن هذا لم يمنع من قيام الدول باتخاذ إجراءاتٍ تشريعيَّة

(1) Maria Vásquez Callo-Müller and Iryna Bogdanova, "Unilateral Cyber Sanctions: Between Questioned Legality and Normative Value, Vanderbilt", Journal of Transnational Law, Vol. 54, No. 4, 2021, pp. 20-35.

(2) IA Iftimie, Cyber Sanctions: Weaponising the Embargo of Flagged Data in a Fragmented Internet, Journal of Information Warfare, Vol. 19, No. 1 ,2020, pp. 48-61

https://www.jstor.org/stable/27033608

وتقنيَّة لتوقيع العقوبات على الجرائم السيبرانيَّة، إلى جانب تبنِّي الاتفاقيَّات الإقليميَّة، وتطوير وتحديث التَّشريعات الوطنيَّة.

وقد جاءت عمليَّة وضع نظام للعقوبات السيبرانيَّة The Cyber Sanctions Regime في شكل اتّخاذ إجراءات أُخرى مضادَّة من قِبَلِ طرف دوليٍّ أو أكثر لتعزيز قدرته على إحداث تغيير في السلوك الدوليّ لدى طرف آخر تحت ضغوط الإكراه، والعزل، وتضمن الفاعلين من الدول القوميَّة والفاعلين من غير الدول، مثل الأفراد أوِ الجماعات الإرهابيَّة، أو الشركات التقنيَّة أو مجموعات القرصنة الدوليَّة.

وإذا كان نظام العقوبات السيبرانيَّة، والذي يتمُّ التَّوافق عليه من المجتمع الدولي لم يتشكَّل بعد، إلا أنَّ هناك محاولات لتطويره في ظل الاتفاقيَّات الدوليَّة، خاصَّة تلك المعنيَّة بالجرائم السيبرانيَّة، وواجه ما تبنَّتْهُ دول الاتحاد الأوروبي والولايات المتحدة من وضع نظامٍ للعقوبات السيبرانيَّة مشكلات تقنيَّة وعمليَّة وتشريعيَّة بالرَّغم من التَّبايُن فيما بينهم، وانعكس ذلك على قياس مدى فاعلية نظام العقوبات السيبرانيَّة، الذي يجب أن يرتكز على تبنِّي مجموعة من التَّدابير المضادة التي يتمُّ فرضها لتغيُّر السلوك لدى طرف آخر بما يتوافق مع مصلحة الدولة أو المجتمع الذي يفرضها، ومن جهة أخرى، القدرة على تقاسم الأعباء والمكاسب جرَّاء تطبيق هذا النظام بين مختلف الفاعلين، وأن تكون مخرجات هذا النظام من العقوبات القابلة للتَّنفيذ، وأن يحظى هذا النّظام الاعترافَ والشرعيَّة من قِبَلِ المجتمع الدولي.

ويبقى للتطور في مجال فرض العقوبات الدوليَّة، تزايد درجات التَّعقيد في التَّطبيق مع التطور التكنولوجي وتبنّي استراتيجيَّات خرق العقوبات.

المطلب الثاني : إشكاليَّات تطبيق العقوبات السيبرانيَّة

يُثيرُ تطبيق العقوبات السيبرانيَّة، عدة إشكالاتٍ منها:

أولاً: صعوبة الاتهام المباشر للدولة عن الوقوف وراء الهجمات السيبرانيَّة، والتي غالبًا لا تلجأ للعمل من خلال أجهزة أو هيئات حكوميَّة رسميَّة، ويتم بدلًا من ذلك التعاون مع فاعلين آخرين من غير الدول.

ثانياً: صعوبة تحديد مكان انطلاق الهجمات مع إمكانيَّة التَّخفِّي التّقنيّ؛ فقد تنطلق الهجمات من مكان ثالث، أو عبر متعاطفين، أو عملاء لها منتشرين في أرجاء العالم، وهو أمرٌ يجعل هناك صعوبة في التحرّي الإلكتروني للأدلَّة التي تثبت العلاقة مع الفاعل.

ثالثاً: لا يُلقي القانون الدولي المسئوليَّة القانونيَّة على الدولة إلا إذا توافر الاعتراف الرَّسمي حول شن الأعمال العدائيَّة، وهو أمرٌ مستبعد بسبب محاولة الدولة التهرُّب من أيِّ مسئوليَّة أو دور في الهجمات السيبرانيَّة، وصعوبة إثبات العلاقة بين الدولة والفاعل من حيث التَّوجيه والسيطرة، أوِ التَّبنّى، أو الموقف المساند لها.

رابعاً: وفقاً للقاعدة القانونية (لا عقوبة إلا بنص)، لذا فإنَّ العقوبات السيبرانيَّة تفتقد المشروعيَّة حال تطبيقها، وهو ما يُقلّل فُرَصَ مثول دولة أو طرف للمساءلة.

خامساً: صعوبة تحديد الهدف والسيطرة على نتائج الأعمال العدائيَّة بما يجعله يتعارض مع قواعد القانون الدولي الإنساني وتصيب العقوبات السيبرانيَّة السكان المدنيّين بما يجعلها تفتقد التَّمييز.

سادساً: صعوبة تعريف (الهجوم السيبراني) بأنَّه (هجومٌ مسلَّحٌ) بموقف القانون الدولي، ومن ثمّ تُغَلُّ يد الدولة على ممارسة حقّها في الدفاع الشرعيّ عنِ النَّفس الذي يقره ميثاق الأمم المتحدة.

سابعاً: غلبة الطابع السري على تطوير القدرات السيبرانيَّة بشأن تطوير أسلحة سيبرانيَّة، أوِ امتلاكها أو نقلها أوبيعها، وهو ما يحدُّ من القدرة على فرض عقوبات سيبرانيَّة، ويضع إشكاليَّة أمام التحقق الدولي.

ثامناً: يصعب تطبيق العقوبات السيبرانيَّة في مجال الفضاء السيبراني، خاصَّة أنَّها تتمُّ في غياب توافق دوليٍّ حول بناء نظامٍ دوليٍّ لها تحت إشراف الأمم المتحدة، إلى جانب صعوبة تطبيق الإجراءات المضادَّة التي أتاحها الفصل السابع من الميثاق في حالة الاعتداء السيبرانيّ، أوِ التعامل مع الهجمات السيبرانيَّة.

تاسعاً: صعوبة تحقيق التَّوافق الدولي حول وصف الأعمال العدائيَّة في المجال السيبراني؛ فقد يتمُّ النظر إليها على أنَّها تُعبّرُ عن أنشطة تجاريَّة، أو أنشطة تهدف لحماية الأمن القومي، أو الأنشطة الاستخباراتيَّة، أو جمع المعلومات والبيانات، إلى جانب اعتبار الهجوم السيبرانيّ هجومًا مسلَّحًا وفق قواعد القانون الدولي.

عاشراً: إنَّ تشجيع عمليَّة فرض العقوبات السيبرانيَّة سيؤدي إلى تصاعد المزيد من الإجراءات الأُحاديَّة الانتقاميَّة التي يكون من شأنها تعكير صفو العلاقات الدوليَّة، ويزيد من حالة الفوضى، ويضرُّ بأمن الفضاء السيبراني، الذي أصبح مرفقًا دوليًا وتراثًا مشتركًا للإنسانيَّة.

الحادي عشر: تواجه عمليَّة فرض العقوبات السيبرانية إشكالات الاعتراف بالأدلَّة الجنائيَّة الرَّقميَّة، التي تستندُ إليها أجهزة إنفاذ القانون وسير التحقيقات القضائية.

الثاني عشر: هناك تحديَّات تتعلق بجمع الأدلة الرَّقميَّة، خاصة مع إمكانيَّة تغيير عناوينَ، أو إخفائها، ومن ثمَّ يصبح موقع عنوان الجاني لا يُشكّلُ دليلًا كافيًا، ومدى اعتراف الهيئات القضائيَّة بتلك الأدلة، خاصة أنَّ الجاني قد يعمد إلى تغيير عنوانه، أو شنّ الهجمات من موقع طرفٍ ثالث، وإمكانيَّة تعرض المعلومات الحساسة المرتبطة بالدَّليل الرَّقمي[1].

الخاتمـة

في ضوء دراستنا "للصراع السيبراني في القانون الدوليّ بين العقوبات السيبرانيَّة وإشكاليَّات التَّطبيق" توصَّلتِ الدراسة إلى مجموعة من النَّتائج والتّوصيات، أُوجزها على النَّحو الآتي:

أولاً: النَّتائج

1-أصبحت المعلومات في الوقت الحالي هي عملة هذا العالم الرئيسة، لذلك تعتمد كل الكيانات من الدول القومية إلى الأفراد على نحو متزايد على المعلومات وتكنولوجيا المعلومات، ومن ذلك تقنيات الحاسوب والاتصالات.

2-أصبح الفضاء السيبراني مجالًا للصراعات المختلفة، سواء للفاعلين من الدول أم من غيرها لحيازة أكبر قدر من النفوذ والتأثير السيبراني.

3-تحول الفضاء السيبراني إلى شبكة عالميَّة يمكن الوصول إليها من أي مكان، ومن أي شخص دون تمييز، وعلى أساس مبدأ حياديَّة الشبكة، وخاصة أنَّ المجال السيبراني وتطبيقاته المختلفة يلعب دورًا حيويًا واستراتيجيًا وإنسانيًا.

---

(1) يعرف الدليل الرقمي بأنه أية معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية، وما في حكمها والممكن تجميعه وتحليله باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة.انظـر :

- عائشة بن قارة ، حُجيَّة الدليل الإلكترونيّ في مجال الإثبات الجنائي، دار الجامعة الجديدة،الإسكندرية،2010م، ص 23 .

- نور الهدى محمودي، حُجيَّة الدليل الرَّقميّ في إثبات الجريمة المعلوماتيَّة، **مجلة الباحث للدراسات الأكاديمية**، جامعة باتنة، عدد 11،2017م، ص 911 .

4- يُمثّل فرض العقوبات السيبرانية تهديدًا للسكان الأبرياء والمنشآت المدنيَّة، ويُعدُّ انتهاكًا للقواعد التي أرساها القانون الدولي الإنساني بشأن الأعمال الحربيَّة، وأهميَّة التمييز بين المدنيين والمنشآت المدنيَّة في أثناء القتال، ويمثل انتهاكًا للقانون الدولي لحقوق الإنسان.

ثانياً: التوصيات

1-ينبغي حماية حريَّة الرأي والتعبير وحرية الاتصال وباقي حقوق الإنسان الرَّقميَّة والتي اعتبرت من قبل المجلس الدولي لحقوق الإنسان، رديفًا للحقوق في العالم المادي.

2- يجب تدخل المجتمع الدولي بشأن مواجهة سياسة الهجوم السيبرانيّ، والعمل على إيجاد أرضيّة مشتركة مع كافة الدول بشأن الصراع السيبراني.

3- اعتماد نهجٍ واضحٍ لتفاهمٍ متبادلٍ فيما يتعلق بمختلف وجهات نظر الدول في التقليل من حدَّة الصراع السيبرانيّ، وكيف تنطبق أو لا تنطبق قوانين الحرب وميثاق الأمم المتحدة على الهجوم السيبراني؟ وأهميَّة الأطراف من غير الدول التي قد تشنُّ هجمات سيبرانيَّة، وكيف ينبغي للدول أن ترد على مثل هذه الهجمات؟

4- يجب أن تدفع طبيعة التهديد السيبراني العابر للحدود الدوليَّة إلى ضرورة التعاون الدولي في مواجهة الفجوة القانونيَّة الدولية التي تتيح الفرصة للالتفاف حول أيَّة عقوبات جرَّاء التورط في الهجمات السيبرانيَّة.

قائمة المراجع:

أولًا- المراجع باللغة العربية

1. الإعلان العالمي لحقوق الإنسان، يمكن الوصول له عبر الرابط: https://bit.ly/3yGfeCh
2. أناسيغال، العقوبات الاقتصادية القيود القانونية والسياسية، (المجلة الدولية للصليب الأحمر، ع836, 31 ديسمبر 1999م) على الرابط: https://bit.ly/38yxsLd
3. عائشة بن قارة ،حجية الدليل الالكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة،الإسكندرية،2010م، ص 23 .

4. – نور الهدى محمودي، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية،جامعة باتنة،عدد 11،2017م،ص 911 .

5. إيهاب خليفة، الكتائب الإلكترنية، الملامح العامة لحروب مواقع التواصل الاجتماعي في الشرق الأوسط، (اتجاهات الأحداث، مركز المستقبل للدراسات والأبحاث المتقدمة، مج1، ع4، نوفمبر 2014م).

6. إيهاب خليفة، إمكانيات تحقيق الردع في صراعات الفضاء الإلكتروني، (اتجاهات الأحداث، ع13، 2015م).

7. أندريه بوفر، الردع والاستراتيجيّة، ترجمة: أكرم ديري، دار الطليعة للطباعة والنشر، بيروت،لبنان، 1970م،ص 31 .

8. إيهاب خليفة، تأثيرات قوة الفضاء الإلكتروني على التفاعلات الأمنية في العالم، (اتجاهات الأحداث، ع1، مج1، أغسطس 2014م).

9. تيم كول بان، الرئيس الصيني يدرك حاجته إلى التكنولوجيا المالية، (صحيفة الشرق الأوسط, 8 يونيو 2022م), على الرابط: https://bit.ly/3nz0A9g

10. سليم دحماني، أثر التهديدات السيبرانيَّة على الأمن القومي للولايات المتحدة الأمريكية– أنموذجًا (2017–2021)، (رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، 2018م).

11. سماح عبد الصبور، الإرهاب الرقمي: استخدامات الجماعات المسلحة لوسائل التواصل الاجتماعي، (اتجاهات الأحداث، مج1، ع2، سبتمبر 2014م).

12. محمود محارب، إسرائيل والحرب الإلكترونية: قراءة في كتاب حرب الفضاء الإلكتروني– اتجاهات وتأثيرات على إسرائيل، (المركز العربي للأبحاث ودراسة السياسات، الدوحة، أغسطس 2011م).

13. نوران شفيق، الفضاء الإلكتروني وأنماط التفاعلات الدولية: دراسة في أبعاد الأمن الإلكتروني، (رسالة ماجستير، جامعة القاهرة: كلية الاقتصاد والعلوم السياسية، 2014).

14. نوران شفيق، حوكمة الإنترنت: أبعاد الصراع على إدارة الفضاء الإلكتروني، (مركز المستقبل للأبحاث والدراسات المتقدمة، يوليو 2014م).

15. نيكوالسمولدر، سلاح العقوبات، (مجلة التمويل والتنمية، صندوق النقد الدولي، ع59، ق2، يونيو 2022م) ص20. على الرابط:
File://c:/users/GR/Downloads/fd0622a.pdf

16. هاورد ديفيز، هل تغير العقوبات الغربية النظام المالي العالمي، (صحيفة الاقتصادية، 4 مايو 2022م)، على الرابط:https://bitly/39rTVKi

17. وليد غسان سعيد، دور الحرب الإلكترونية في الصراع العربي– الإسرائيلي، (رسالة ماجستير، جامعة النجاح الوطنية، كلية الدراسات العليا، 2013)، ص97.

ثانيًا– المراجع الأجنبية:

1. Brandon Valeriano & Ryan C. Maness, The Dynamics of Cyber Conflict Between Rival Antaonists, Journal of Peace Research, 2014, Vol. 51, No. 3, pp. 48-349.

2. Cory Bennett, "Obama extends cyber sanctions power", The Hill.com,29/3/2016,https://bit.ly/3yh9yi4

3. Cyber Attack Statistics 2022, Data, and Trends, Parachute, January 2022.https://bit.ly/3yK8T8S

4. Emily O. Goldman, "Fresh Thinking and new approaches are needed on diplomacy's newest frontier", The Froeign Service Journal, Kune2021.
https://afsa.org/cyber-diplomacy-strategic-competition

5. IMF Executive Board Discusses the Rise of Public and Private Digital Money-A Strategy to Continue Delivering on the IMF's Mandate, International Monetary Fund, July 29, 2021.http://bit.ly/3FVevXo

6. Johnson, worldwide digital population as of April 2022, statista.com, May 9, 2022.https://bit.ly/3a5JAnB

7. Maria Vásquez Callo-Müller and Iryna Bogdanova, "Unilateral Cyber Sanctions: Between Questioned Legality and Normative Value,

Vanderbilt", Journal of Transnational Law, Vol. 54, No. 4, 2021, pp. 20-35.

.8 Maria Vásquez Callo-Müller and Iryna Bogdanova, Unilateral Cyber Sanctions and Global Cybersecurity Law Making, Opiniojuris, 24/10/2022. https://bit.ly/3Mo9gKr

.9 Maria Vásquez Callo-Müller, Iryna Bogdanova, "What is the Role of Unilateral Cyber

.10 Maria Vásquez Callo-Müller, Iryna Bogdanova, "What is the Role of Unilateral Cyber Sanctions in the Context of The Global Cybersecurity Law-Making?", Voelkerrechtsblog, 10.05.2022. https://bit.ly/3wxuJJX

.11 Paul Rosenzweig, Cyber Warfare How Conflicts In Cyberspace Are Challenging America And Changing The World Praeger Security International, 2013, pp. 15-16.

.12 Steven Morgan, "Cybercrime to Cost The World $10.5 Trillion Annually By 2025", Cybercrime Magazine. Nov. 13, 2020.

https://cybersecurityyventures.com/cybercrime-da-costs-10-trillion-by-2025/

.13 ITU Toolkit for ,The International Télécommunication Union CybercrimeLégislation, Geneva, 2010, P. 12.

.14 Timothy J. Junio, The Politics And Strategy Of Conflict, Phd Thesis, University of Pennsylvania, 2013, pp. 28-30.

.15 Tomaso Falchetta, Deborah Brown and Katitza Rodriguez, Opening Stages in UN Cybercrime Treaty Talks Reflect Human Rights Risks, justsecurity, April 18, 2022.

.16 Wendy H. Wong & Peter A. Brown, E-Bandits In Global Activism: Wikileaks, Anonymous And The Politics of No One, Perspectives On Politics, Vol. 11, No. 4, December 2013.