العقوبات السيبرانية ومشروعيتها في ضوء قواعد القانون الدولى

إعداد

الدكتور / أسامة سالم محمد الفرجانى

مجلة حقوق دمياط للدراسات القانونية والاقتصادية – كلية الحقوق – جامعة دمياط

العدد العاشر يوليو–2024

مقدمة:

لقد شهد العالم في السنوات الماضية زيادة في حوادث إساءة استخدام التقدم العلمي من خلال هجمات سيبرانية لتحقيق أغراض مختلفة، هذه الأغراض قد تكون إجرامية يقوم بها أفراد للحصول على أموال أو معلومات، وقد تكون عسكرية أو سياسية أو اقتصادية، مصدرها جهات مرتبطة بدولة ما، بقصد ممارسة نوع من الإكراه على الدولة المستهدفة أو تدمير منشأة حيوية فيها، أو الاستيلاء على أسرار عسكرية أو صناعية فيها، وبالتالي التأثير على قدرتها.

فإذا ترتب على الهجمة السيبرانية وقوع أضرار مادية أو بشرية جسيمة في المنشأة المستهدفة بصفة فورية؛ فإن هذه الهجمة يمكن أن تؤسس لادعاء الدولة المستهدفة بأنها تعرضت إلى اعتداء، وأنها تمتلك حق الدفاع عن النفس باستخدام مختلف الوسائل بما فيها القوة العسكرية وفقًا لنص المادة (٥١) من ميثاق الأمم المتحدة، كحدوث هجمة سيبرانية نتج عنها حدوث دمار وخسائر بشرية

يبرر للدولة المستهدفة الادعاء بتعرضها لاعتداء متعمد من تلك الدولة ويرقى إلى تصنيف الهجمة على أنها نوع من استخدام القوة.

ولقد أثارت العقوبات السيبرانية المخاوف لدى العديد من أصحاب المصلحة في مجتمع المعلومات العالمي من أن يشكل ذلك سابقة يمكن أن تتكرر في الصراعات والنزاعات المستقبلية، خاصة في ظل زيادة الأهمية الاستراتيجية للمجال السيبراني كمقدم ومسهل ووسيط لعمل الخدمات المدنية وعمل المنشآت الحيوية من جهة، ودور في إدارة شئون الفرد والمجتمع والدولة من جهة أخرى والتي تنطلق من تداخل المجال السيبراني مع بقية المجالات الدولية كالبر والبحر والجو والفضاء الخارجي أو هو الأمر الذي يجعل من العقوبات السيبرانية فريدة في خصائصها وتأثيرها واتساع مجال ومدى انتشارها، ما يجعل تعرضها للأعمال العدائية أو الانتقامية يمثل أضرارًا جسيمة بالمجتمع الدولي، بما تحمله من تأثيرات إنسانية وسياسية وعسكرية واستراتيجية، خاصة في ظل تعاظم دور المتغير التقني في البيئة الدولية وتأثير ذلك في فاعلية وفرض العقوبات الدولية.

ويأتي ذلك في ضوء قواعد ومبادئ القانون والعرف الدولي، والاتفاقيات المعنية بحقوق الإنسان والمنظمة لحرية التجارة العالمية والاستثمار، وما يزيد من خطورة تطبيق نظام للعقوبات السيبرانية أنه تم تطويره بعيدًا عن حالة من التوافق الدولي أو المشروعية الدولية، ويمثل تهديدًا للجهود الدولية في مجال حوكمة الإنترنت، وتعزيز التعاون الرقمي، وتجريم السلوك العدائي للدول في الفضاء السيبراني.

مشكلة الدراسة:

تتمحور مشكلة الدراسة في التساؤل الرئيسي:

ما مشروعية فرض العقوبات السيبرانية كإجراءات مضادة في ضوء القانون الدولي وقوانين التجارة العالمية؟

ويندرج تحت هذا التساؤل الرئيس مجموعة من التساؤلات الفرعية يتمثل أهمها في:

- ما أثر المتغير التكنولوجي في طبيعة العقوبات الدولية؟
- ما إشكالية تطبيق العقوبات السيبرانية وفق القانون الدولي؟

- ما تأثير العقوبات السيبرانية على مستقبل النظام المالي العالمي؟
- ما تحديات وفرص بناء نظام دولي للعقوبات السيبرانية؟
- ما تأثير العامل التكنولوجي والمعلومات في بنية موازين لقوى العالمية؟

أهداف الدراسة:

- الحرمان القسري من الخدمات للحد من نفوذ الفاعلين من الدول وغير الدول.
- التعرف على ملامح ظاهرة الفضاء السيبراني ومدى اختلاف توظيفاتها في الصراعات السياسية بين الأنظمة الحاكمة.
- التعرف على استراتيجية الفضاء السيبراني ودوره في إدارة شئون افرد والمجتمع والدولة.
- الوقوف على الجوانب القانونية للتدابير المضادة في القانون الدولي.

أهمية الدراسة:

تتمثل أهمية الدراسة في النقاط التالية:

- رصد طبيعة التحديات لبناء نظام دولي للعقوبات السيبرانية.
- تفعيل دور المنظمات الدولية للحفاظ على الاستخدام السلمي للفضاء السيبراني.
- فهم طبيعة الصراع السيبراني ومدى مشروعيتها في ظل قواعد القانون الدولي.

منهج الدراسة:

تم الاعتماد على المنهج الوصفي التحليلي.

مصطلحات الدراسة:

الفضاء السيبراني (Cyber Space):

جاء تعريف الاتحاد الدولي للاتصالات للفضاء السيبراني بأنه: "المجال المادي وغير المادي الذي يتكون وينتج عن عناصر هي: أجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبة

المعلومات، المحتوى معطيا ت النقل والتحكم، ومستخدمي كل هذه العناصر"[١].

ويمكن القول بأن: "الفضاء السيبراني هو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكون من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين"[٢].

العقوبات السيبرانية (Cyber Sanctions) [*]:

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

([٢]) سليم دحماني، أثر التهديدات السيبرانية على الأمن القومي الولايات المتحدة الأمريكية- أنموذجًا (٢٠١٧-٢٠٢١)، (رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، ٢٠١٨م)، ص٢٣.

(*) من الشائع في الاستخدام قبل تبلور ظاهرة الفضاء السيبراني استخدام مصطلح العقوبات التكنولوجية Technology Sanaction ، ولكن أصبح يشير المجال السيبراني إلى كافة المكونات التي تتعلق بالبنية التحتية أو المحتوى أو بالسياسات الناظمة، ومن ثم أصبح المجال السيبراني شاملًا لكل الأبعاد التقنية إلى جانب الأبعاد الأخرى، ومن جهة أخرى؛ فإن مصطلح =

يمكن تعريفها بأنها استخدام أو التهديد بفرض القيود على التعاملات الرقمية التأثير في إحداث تغيير سلوكي من قبل "فاعل" بما ينتج عنه من التعرض للضغوط الاقتصادية أو النفسية، سواء كانت ضد فرد أو مجموعة من الأفراد، أو نخبة سياسية أو المجتمع داخل دولة ما، أو الحكومة أو أحد هيئاتها، أو تلك الإجراءات والتدابير المضادة التي يتم فرضها من قبل طرف دولي أو أكثر بغية فرض حصار رقمي شامل أو جزئي يكون له تبعات اقتصادية وسياسية على الجبهة الداخلية لدولة ما أو تحالفاتها الخارجية(١).

وبناء على ذلك تم تقسيم الورقة البحثية إلى :

=

Digital يشير إلى مكون من مكونات المجال السيبراني، ومن ثم اعتمد الباحث على مصطلح Cyber Sanctions في هذه الدراسة.

(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

المحور الأول: مفهوم الصراع السيبراني ومستوياته.

المحور الثاني: مشروعية العقوبات السيبرائية وإشكاليات التطبيق في ضوء القانون الدولي.

المحور الأول: مفهوم الصراع السيبراني ومستوياته:

اختصر الفضاء السيبراني حاجز الزمان والمكان، وخلق مساحات للتفاعلات الداخلية والدولية في الواقع الافتراضي، ومن ثم برزت فضاءات جديدة للصراع بأدوات مختلفة وأنماط جديدة تختلف عن الصراعات التقليدية، وتعود أسباب اهتمام الفاعلين سواء أكانوا من الدول، أم غيرها بهذا الفضاء، كمجال لتحقيق الهيمنة، وتنفيذ الأهداف وإدارة الصراعات، إلى امتلاكه عدة سمات أساسية من أبرزها ما يأتي:

١- **ساحة صراع افتراضية:** فبما أنه ليس مساحة جغرافية، لذلك يتخطى الفضاء السيبراني العديد من الثنائيات التى تظهر في الصراعات التقليدية، حيث يشارك في الصراعات ذات الطبيعة الإلكترونية المدنيون والعسكريون، كما ترتبط أيضًا بالتطورات المادية السياسية والعسكرية على الأرض، بخلاف أنها أقل تكلفة

من حيث الخسائر المادية، وأكثر تحديدًا للهدف مقارنة بنظيراتها التقليدية [١].

٢- **زيادة الاعتماد الإلكترونى:** إذ باتت الدول الحديثة تربط بنيتها التحتية بالفضاء السيبراني، خاصة شبكات الكهرباء والمياه والبنوك والبورصة والاتصالات وغيرها، بالإضافةإلى أنظمة السيطرة والتحكم العسكرية، وجمع المعلومات، مثل الأقمار الصناعية والطائرات دون طيار في الحروب، وبالتالي أضحى استهداف تلك البُنى التحتية للدولة ذات الطابع الإلكترونى أحد عوامل الصراع السيبراني[٢].

---

(١) ايهاب خليفة، الكتائب الإلكترنية، الملامح العامة لحروب مواقع التواصل الاجتماعي في الشرق الأوسط، (اتجاهات الأحداث، مركز المستقبل للدراسات والأبحاث المتقدمة، مج١، ع٤، نوفمبر ٢٠١٤م)، ص٩.

(٢) محمود محارب، إسرائيل والحرب الإلكترونية: قراءة في كتاب حرب الفضاء الإلكتروني- اتجاهات وتأثيرات على إسرائل، (المركز العربي للأبحاث ودراسة السياسات، الدوحة، أغسطس ٢٠١١م)، ص٣.

٣- تماهى حدود الداخل والخارج، أي وجود حالة من التأثير الشبكى المتزايد داخل الدول وخارجها، حيث اتسع استخدام الأفراد والجماعات والدول للتكنولوجيا الحديثة المرتبطة بالفضاء السيبراني سواء أكانت مواقع تواصل اجتماعى على الإنترنت، أم هواتف ذكية، أم مواقع عامة للتعاملات المالية والتجارية والخدمية، ويتصل كل ذلك بشبكة مترابطة من خلال أنظمة تحكم تكنولوجية ترتبط بالإنترنت؛ بما يجعل الخدمات والمعلومات متاحة للجميع الأمر الذى قد يعرضها للاستهداف.

٤- صعوبة الردع الإلكتروني: فعلى أساس أن الفضاء السيبرانى ساحة افتراضية، فيصعب بالتالي على الدول وضع حدود لسيادتها عليه، ومع ضعف القوانين الدولية للسيطرة على هذا الفضاء، يغيب الردع في ظل إمكانية التنكر على شبكة الإنترنت، ومجهولية مصدر الهجمات الإلكترونية، وسهولة أن يقوم بها الأفراد، وليس

الدول فقط، حيث زادت خبرات القراصنة بشكل متطور دون الحاجة لنظم معقدة كانت تملكها الدول وحدها في الصراعات التقليدية[١].

٥- **غياب الشفافية الإلكترونية،** فمع عدم القدرة على معرفة هويات القائمين على هجمات القرصنة نشبت معضلة غياب الشفافية والقوانين المقيدة للصراعات في المجال الإلكترونى، فضلًا عن ذلك فإن مصدر الهجمات الإلكترونية قد يسبب خسائر واسعة دون أن يعنى ذلك وجود عنف ملموس، مما لا يعنى بالضرورة وجود هجوم مضاد أو استمرار الصراع[٢].

ومع تحول الفضاء السيبراني إلى مجال متزايد لتنافس السياسات الخارجية للدول وغيرها من الفاعلين بات البعض يعرف الصراع في

---

(١) ايهاب خليفة، إمكانيات تحقيق الردع في صراعات الفضاء الإلكتروني، (اتجاهات الأحداث، ع١٣، ٢٠١٥م)، ص١٣.

(٢) نوران شفيق، الفضاء الإلكتروني وأنماط التفاعلات الدولية: دراسة في أبعاد الأمن الإلكتروني، (رسالة ماجستير، جامعة القاهرة: كلية الاقتصاد والعلوم السياسية، ٢٠١٤)، ص٤٥.

هذه الساحة الافتراضية (CyberConflict) كونه استخدام تكنولوجيا الحاسوب في الفضاء السيبراني (الإلكتروني) لأغراض التدمير من أجل التأثير أو التغيير، أو التعديل في التفاعلات الدبلوماسية والعسكرية بين الكيانات المختلقة، وذلك بعيدًا عن ساحة المعارك، وقد يأخذ ذلك الصراع نمطين:

الأول: الحوادث الفردية (Cyber Incidents) ويقصد بها العمليات والحوادث الافتراضية التي تتم على فترات مختلفة وليست مستمرة لفترة معينة، أما النمط الآخر فهو فهو النزاعات السيبرانية (Cyber Disputs) والتى تدار بأدوات افتراضية بين دولتين في فترة زمنية معينة، ويحتوى على واحد أو أكثر من الحوادث الفردية[1].

([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.

هنا من المهم الإشارة إلى أن الصراعات السيبرانية تختلف عن نظيراتها التقليدية، وبالأخص العسكرية، والتي تُعد حكرًا على الدولة والجماعات المسلحة، وهى صراعات تدور في مساحة جغرافية معينة، وتستمر لفترة زمنية معينة، وتكون محددة الأطراف والأهداف، وإن كانت الصراعات المسلحة على أرض الواقع قد دخلت فيها أدوات تكنولوجية لإدارة الصراعات بِين الدول، فعندما تنشب حروب تقليدبة بين الدول، تصبح قطاعات الاتصالات والمعلومات والبُنى التحتية والمعلوماتية ضمن الأهداف العسكرية، خاصة مع ارتباط تلك القطاعات بالأمن القومى للدول، ومن ثم باتت هنالك أسلحة ذات طبيعة إلكترونية ضمن الحروب، مثل وسائل التواصل الاجتماعي، والأقمار الصناعية، وأسلحة النانو تكنولوجية، والطائرات دون طيار، والأسلحة الروبوتية.

وأيضًا ثمة فارق بين الصراعات السيبرانية وما سماه البعض "الهجمات الحركية" أو ما يسميه البعض 'الهجمات غير المبرمجة Non Software-based Attacks، وهى تشمل الهجمات المادية والمغناطيسية ضد الشبكات الإلكترونية. عبر أسلحة تقليدية قد تشمل القنابل، والصواريخ، والعبوات الناسفة، وهى بذلك لا تعد

هجمات إلكترونية، أو نوعًا من الصراع في الفضاء السيبرانى، كونها تستخدم آليات عسكرية تقليدية لإدارة الصراع[١].

بالإضافة لما سبق فقد تختلف الصراعات في الفضاء السيبرانى عن نظيراتها التقليدية من حيث إن الأخيرة تفرق بين مستويي الجرائم والحروب؛ فالجريمة هى مشكلة قانونية تتم مواجهتها بإنفاذ القانون ونظم العدالة، بينما تتعلق الحرب بالعسكريين وبالأسلحة، أما في سياق الصراعات السيبرانية؛ فإن جرائم الإنترنت والحرب الإلكترونية تنفذ باستخدام النوع ذاته من الأدوات والبنى التحتية التقنية، ويمكن أن يُسهم فيها الفاعلون من غير الدول، كما أن تطور الهجمات الإلكترونية هو دليل على إلغاء الحدود بين جرائم الإنترنت والحرب الإلكترونية، ذلك أن كليهما يأتي من الصراع الإلكتروني.

---

(١) وليد غسان سعيد، دور الحرب الإلكترونية في الصراع العربي-الإسرائيلي، (رسالة ماجستير، جامعة النجاح الوطنية، كلية الدراسات العليا، ٢٠١٣)، ص٩٧.

وتعرضت ظاهرة الصراع إلى تغيرات مع بروز الفضاء الإلكتروني كمجال تنشا فيه نزاعات بين الفاعلين المختلفين، خاصة مع الاعتماد الكثيف على تكنولوجيا الاتصال والمعلومات، وهنا برز الصراع السيبراني كحالة من التعارض في المصالح والقيم بين الفاعلين، سواء أكانوا دولًا أم غير دول في الفضاء الإلكترونى.

وعلى الرغم من الآثار المدمرة لهذا النمط من الصراعات؛ فلا يرافقه دماء، وقد يتضمن التجسس والتسلل إلى مواقع الخصوم الإلكترونية، وقرصنتها دون أنقاض، أو غبار، كما أن اطرافه يتسمون بعدم الوضوح، وتنطوى كذلك تداعياته علي مخاطر عدة على أمن الدول، سواء عن طريق التخريب أو استخدام أسلحة الفضاء الإلكتروني المتعددة[١].

ومع انتشار الفضاء الإلكتروني، وسهولة الدخول إليه، اتسعت دائرة الصراعات السيبرانية، وزاد عدد الهاجمين، وباتت هناك حالة من

---

(١) نوران شفيق، الفضاء الإلكتروني وأنماط التفاعلات الدولية: دراسة في أبعاد الأمن الإلكتروني، مرجع سابق، ص٥٩.

الكر والفر في الهجمات الإلكترونية لتعبر عن الصراع الممتد؛ ولذا صار الصراع بين الفاعلين المختلفين حول امتلاك أدوات الحماية والدفاع، وتطوير القدرات الهجومية الإلكترونية يستهدف حيازة القوة والتفوق والهيمنة وتعزيز التنافس حول السيطرة، والابتكار، والتحكم في المعلومات، وتعظيم القدرات القادرة على زيادة النفوذ والتأثير في المستويين المحلي والدولى.

وبما أن المتنازعين يلجئون في الصراعات التقليدية إلى استخدام شتى أنواع أسلحة التدمير الممكنة؛ فقد انتقلت جبهات القتال بشكلٍ موازٍ إلى ساحة الفضاء الإلكتروني، وكان لهذا التغيير دور في إعادة التفكير في حركية وديناميكية الصراع، بل وبروز ما يعرف بـ "عصر القوة النسبية"، وعنت هذه الأخيرة أن "القوة العسكرية" قد لا

تكفِ وحدها لتأمين البنية التحتية للدول، الأمر الذي يخلف آثارًا استراتيجية هائلة على مستوى تركيبة وتوازنات النظام الدولى [1].

وأسهم عاملان رئيسيان في انتشار رقعة الصراع في الفضاء الإلكتروني، وبالتالي إفساح المجال لنشوء الحروب السيبرانية. وهما:

١- تغير منظور الحرب جذريًا، حيث انتقلت من نسق "الحروب بين الدول إلى وسط الشعوب"؛ فكان الغرض من الحرب قديمًا هو تدمير الخصم، إما باحتلال ارضه، أو الاستيلاء على موارده، أما الحروب الجديدة؛ فقد استهدفت بالأساس التحكم في إرادة وخيارات المجتمعات، ومن ثم بدا للشعوب أهمية محورية في هذا النمط الجديد من الحروب، سواء تعلق الأمر بالسكان المستهدفين في

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

أرضية المواجهة، أو بالرأي العام في الدولة التي تشن الحرب، أو بالرأي العام على الصعيدين الإقليمي والدولي.

مع هذا التغير أصبحت أهداف الحرب أقل مادية، وتركزت أكثر على العامل النفسي والدعائي، لاسيما مع تنامى التغطية الإخبارية والسمعية والبصرية المباشرة للأحداث لحظة وقوعها عبر مواقع الإنترنت والفضائيات، وضعف سيطرة أنظمة الحكم على توجهات مواطنيها.

٢- بروز الصراعات ذات الأبعاد المحلية- الدولية، حيث ساعد اشتعال الصراعات الداخلية في مرحلة ما بعد الحرب الباردة، وكذلك طبيعة السياق الدولى للفضاء الإلكتروني في توفير بيئة مناسبة لدمج الفئات والقوى المهمشة في السياسة الدولية، وخلق شبكة تحالفات مؤيدة أو معارضة ذات نطاق دولي عريض، إما على أساس قيم حقوقية أو انتماءات عرقية أو دينية[١].

---

(1) Johan Eriksson And Giampiero Giacomello, The Information Revolution, Security, And International =

إذ أسهم الفضاء الإلكتروني في دعم الهياكل التنظيمية والاتصالية للحركات والجماعات المحلية والمنظمات المدنية بما ساعد الفاعلين من غير الدول على ممارسة قوة التجنيد والحشد والتعبئة واستجلاب التمويل.

هنا تختلف أهداف الحروب الإلكترونية وفقًا لطبيعة أهداف الصراعات السيبرانية وذلك على النحو الآتي:

١- **صراع سيبراني ذو طبيعة سياسية،** حيث تحركه دوافع سياسية، وقد يأخذ شكلًا عسكريًا يتم فيه استخدام قدرات هجومية ودفاعية عبر الفضاء الإلكتروني بهدف إفساد النظم المعلوماتية والشبكات والبنية التحتية، ويتضمن هذا النوع من الصراعات توظيف أسلحة إلكترونية من قبل فاعلين داخل المجتمع

=

relations: Ir Relevant Theory? International Political Science Review, Vol. 27, No. 3, Jul. 2006, pp. 229-235.

المعلوماتي، أو من خلال التعاون مع قوى أخرى لتحقيق أهداف سياسية.

٢- **صراع سيبرانى ذو طبيعة ناعمة**، أي الصراع حول الحصول على المعلومات، والتأثير في المشاعر والأفكار، وشن حرب نفسية وإعلامية، ويتم ذلك من خلال تسريب المعلومات واستخدامها عبر منصات إعلامية بما يؤثر في طبيعة العلاقات الدولية، كالدور الذي لعبه موقع ويكيليكس في الدبلوماسية الدولية.

٣- **صراع سيبرانى على التقدم التكنولوجى**، حيث يأخذ هذا النمط من الصراعات السيبرانية طابعًا تنافسيًا حول الاستحواذ على سباق التقدم التكنولوجي، وسرقة الأسرار الاقتصادية والعلمية، وقد يمتد إلى محاولة للسيطرة على الإنترنت وأسماء النطاقات، وعناوين المواقع، والتحكم بالمعلوماتن والعمل على اختراق الأمن القومي للدول بدون استخدام طائرات أو متفجرات، أو حتى انتهاك حدود الدول، كهجمات قراصنة الكمبيوتر، وتدمير المواقع والتجسس، بما قد يكون له من تأثيرات مدمرة في الاقتصاد والبنية التحتية بذات قوة التفجير التقليدي.

٤- صراع سيبراني على المعلومات والاستخبارات؛ فمع صعوبة الفصل بين أنشطة الاستخبارات وجمع المعلومات وحروب الفضاء الإلكتروني، أو التمييز بين الاستخدام السياسي والإجرامي، يبدو الفضاء الإلكتروني بيئة أكثر مناسبة للصراعات المعلوماتية؛ إذ يُسهم في دعم قدرة الأجهزة الأمنية للدول، أو حتى الجماعات المختلفة على تشكيل شبكة عالمية من العملاء بدون تورط مباشر، بالإضافة إلى رخص التكلفة، وسهولة الاتصال وصعوبة الرقابة التقليدية على التفاعلات الإلكترونية، ومثل ذلك عنصرًا جاذبًا لاستخدام الأسلحة الإلكترونية وتوظيفها لتحقيق أهداف سياسية وعسكرية[١].

مستويات الصراع وأسلحته:

يمكن النظر لمستويات الصراع السيبراني على أنها هرمية الشكل من حيث تأثيراته؛ فيأتي في قاعدته الحالات الأكثر حدوثًا والأقل

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

ضررًا، وهى الجرائم الإلكترونية والتي تنطوي علي الاحتيال وسرقة الأموال والهويات، وهى أحيانًا تكون كارثية، ولكن تهديدها ليس ساحقًا، ولا تمثل تهديدًا وجوديًا، وفي أواسط الهرم يبرز "التجسس السيبراني)، وهو أكثر تطورًا حيث يشمل هجمات إلكترونية من فاعلين من الدول، وغير الدول لسرقة الأسرار القومية، أو حقوق الملكية الفكرية، وذلك النمط هو الأكثر انتشارًا على الساحة الدولية، وله آثار سلبية على الأمن القومي للدول.

فى قمة الهرم يظهر ما يسمى بـ 'الحروب السيبرانية" بين الدول ذات القدرات الحاسوبية المتطورة التى تتصارع فيما بينها، وعلى الرغم من أن ذلك النوع من الحروب لم يظهر بشكل مستقل عن الحروب التقليدية، فإنه حال كان منفصلًا؛ فقد تكون الآثار التدميرية له أعلى بكثير من الحرب التقليدية[١].

([1]) Jason Healey, The Five Futures of Cyber Conflict And Cooperation, Georgetown Journal of International Affairs, pp. 110-116.

في هذا الإطار؛ فإن هناك أربعة آسلحة رئيسية في الصراعات السيبرانية هي:

١- تخريب ومهاجمة مواقع الإنترنت Website Defacements or Vandalism وهو أبسط أشكال الأسلحة السيبرانية، ويستهدف مهاجمة مواقع الخصم بفرض التدمير، أو التشويه عبر نشر النصوص والصور المسيئة؛ وذلك لتوصيل رسالة إلى الهدف بأنه يفتقر القدرة على السيطرة على عمليات الفضاء الإلكترونى الخاصة به، وبرغم أن ذلك النوع من الأسلحة الإلكترونية قد لا يؤثر في الحكومات؛ فإن تأثيراته قد تكون مضاعفة في المجتمعات.

٢- الحرمان من الخدمة Denial of Service Method وهو سلاح أكثر تطورًا؛ حيث يستهدف أجهزة التوجيه التى تغلق المواقع الإلكترونية وتوقف الخدمات، مثل توقف الخدمات الحكومية المقدمة عبر الواقع الرسمية للدولة.

٣- الاقتحام الفيروسي Intrusions وهو سلاح أكثر حدة على المدى الطويل في الهجمات الإلكترونية، خاصة أنه 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 الحيوية للدولة، وقد لا يحتاج هذا السلاح إلى قراصنة، وإنما برامج تقوم عليها دول.

٤- **عمليات التسلل Infiltrations** وفيها يقوم المهاجم بمحو جميع البيانات داخل نظام أو شبكة إلكترونية لدولة أخرى، كما قد يتكرر الهجوم بقصد إفساد، أو تعديل الملفات، أي التقاط المعلومات المتدفقة عبر الويب وهذه النوعية من الأسلحة الإلكترونية متطورة للغاية، وأكثر استهدافًا للعدو، نظرًا لفداحة تأثيراتها خاصة إذا كانت تستهدف البنى التحتية للدول[١].

([1]) Brandon Valeriano & Ryan C. Maness, op. cit., pp. 353-355.

طبيعة الفاعلين المتصارعين في الفضاء السيبراني:

تتوزع القوة وأدوات إدارة الصراعات في الفضاء السيبراني على فاعلين، مثل الدول وغير الدول ولكل منهما أهدافه؛ إذ تسعى الدول من دخول هذه الصراعات إلى الحفاظ على مصالحها، وتأمين بنيتها التحتية وأمنها القومي من الهجمات الإلكترونية، بينما تتباين أهداف الفاعلين من غير الدول في الصراعات السيبرانية، لكنها في الأخير تخدم طبيعة الأنشطة التى يمارسونها على أرض الواقع، مثل الأفراد والتنظيمات السياسية وشبكات الجريمة المنظمة، والمنظمات الإرهابية، والشركات متعدية الجنسيات، ومن المهم الإشارة هنا إلى أن اختلاف القدرات بين الدول والفاعلين من غير الدول يصبح أقل حدة في الفضاء الإلكترونى، بعيدًا عن العتاد والأسلحة التقليدية التى تتميز فيها الدول(١).

(1) Steffen Westerburger, Cyber Conflict In The 21st Century The Future of War And Security Ib A Digitalizing World, Master Thesis International Relations, Radboud =

ويمكن تفصيل طبيعة الفاعلين في الصراعات السيبرانية على النحو الآتي:

١- **الدول والحكومات:** حيث يتم تنفيذ الهجمات الإلكترونية من قبل الجهات الفاعلة الحكومية سواء لأغراض متعددة (أمنية وسياسية وأيديولوجية وغيرها)، وقد تستغل الحكومات هنا فواعل دون الدول، سواء الأفراد أو الجماعات، للقيام بمثل هذه الهجمات على دولة معادية أو يقوم بعض أجهزتها بهذا الأمر، وحينئذ تصبح ذات خطورة عالية، نظرًا لامتلاك بعض الدول المتقدمة تكنولوجيات وإمكانات تقنية قد تفوق الأفراد في الصراعات السيبرانية، وفي هذا السياق يطرح "جوزيف ناي" أربعة تهديدات رئيسية على الأمن القومى للدول، عادة ما تكون محل اهتمام الحكومات في الصراعات

=

School of Mangement Radboud University, December 2014, pp. 10-12.

السيبرانية، وهى التجسس الاقتصادي، والجريمة الإلكترونية، والحرب السيبرانية، والإرهاب الإلكتروني[١].

ويمكن القول إن الفضاء الإلكترونى أصبح مجالًا للتفاعلات الصراعية الدولية، حتى في إدارة الأسلحة التقليدية، التى قد تستهدف البنية التحتية المدنية المرتبطة بالفضاء الإلكتروني، والذي يربط الشبكات الحيوية للدولة عبر نظم اتصال قد تستهدفها الهجمات الإلكترونية، بجانب تهديد البنى التحتية العسكرية وسرقة المعلومات العسكرية، أو التلاعب بها، واختراق أنظمة التحكم والسيطرة والحرب النفسية الإلكترونية على العدو[٢].

٢- القاعلون من غير الدول: حيث صارت لهم أنشطة تعاونية وأخرى صراعية في الفضاء السيبراني لما مثله الأخير من بديل

([1]) Joseph Nye, Cyber Power, Belfer Center For Science And International Affairs, May 2010, pp. 11-13.

([٢]) إيهاب خليفة، تأثيرات قوة الفضاء الإلكتروني على التفاعلات الأمنية في العالم، (اتجاهات الأحداث، ع١، مج١، أغسطس ٢٠١٤م)، ص٤١.

منخفض التكلفة المادية والمؤسسية والتنظيمية والبشرية لتنفيذ أهدافهم، ولعب هؤلاء الفاعلون دورًا مهمًا في وضع قواعد إدارة وحكومة الإنترنت والتى تقوم على الشراكة بين الدول والفاعلين من غير الدول على قدم المساواة في ظل عدم وجود وضع خاص للدول من قبل الكيانات الرئيسية المسئولة عن إدارة الإنترنت، ومن أبرز أمثلة الفاعلين من غير الدول ما يأتى:

- **الشركات المتعدية الجنسيات:** لديها موارد مالية ضخمة وأفرع في العديد من دول العالم مما يتيح لها السيطرة على التعليمات البرمجية الخاصة، والتى توفر لها مصادر أكبر من العديد من الحكومات؛ لذا يمكن أن تلعب تلك الشركات بسهولة دورًا في صراعات الفضاء السيبراني؛ بسبب انخفاض تكلفة الاستثمار

وصعوبة الكشف عن الهوية، وأحيانًا تتصرف بموافقة الحكومة وأحيانًا ضدها[١].

- **الجماعات المسلحة:** حيث يسعى هذا الفاعل لتوظيف الأدوات الإلكترونية في الفضاء السيبراني لتنسيق العمليات المسلحة على أرض الواقع، بالإضافة إلى أن الجماعات الإرهابية تستخدم مواقع التواصل الاجتماع، كوسيلة لتجنيد اتباع جدد ونشر الأفكار والمعتقدات، بخلاف الحصول على الدعمين المادي والمعنوي[٢].

- الأنونيموس وويكيليكس: (فالأنونيموس) أو المجهولون هم جماعات احتجاجية منتشرة حول العالم فى الفضاء الإلكتروني لهم

---

(١) نوران شفيق، حوكمة الإنترنت: أبعاد الصراع على إدارة الفضاء الإلكتروني، (مركز المستقبل للأبحاث والدراسات المتقدمة، يوليو ٢٠١٤م)، ص٦٦.

(٢) سماح عبد الصبور، الإرهاب الرقمي: استخدامات الجماعات المسلحة لوسائل التواصل الاجتماعي، (اتجاهات الأحداث، مج١، ع٢، سبتمبر ٢٠١٤م)، ص٥٣.

أهداف سياسية، ويقومون بتوزيع العلومات السرية وتشويه المواقع، وتوليد احتجاجات حول القضايا السياسية، وهم نمط جديد من الفاعلين السياسيين الذين يعتمدون على إخفاء الهوية، والقيادة بلا جسد وانخراط الأفراد بلا عضوية دائمة وعلى هجمات افتراضية ضد أهداف مادية من أجل تشجيع التغيير السياسي، أما "ويكيليكس"؛ فهو موقع تم تأسيسه في عام ٢٠٠٧م ويستهدف فضح الأنظمة السياسية، عبر تسريب الوثائق والأسرار حول الحكومات، والشخصيات العامة، وشكل كل من الأنونيموس وويكيليكس نماذج لما يمكن أن يسببه الفاعلون من غير الدول من تأثيرات صراعية في الحكومات في الفضاء الإلكتروني[١].

ثانيًا- العقوبات السيبرانية وخصائصها وأهدافها والمفاهيم ذات الصلة:

([1]) Wendy H. Wong & Peter A. Brown, E-Bandits In Global Activism: Wikileaks, Anonymous And The Politics of =

مفهوم العقوبات السيبرانية كنمط جديد للعقوبات الدولية:

هناك من يعرف (العقوبات السيبرانية) بأنها تشير إلى تبني قيود اقتصادية أحادية الجانب يتم فرضها وفقًا للقوانين لمحلية للدولة، وتهدف إلى ردع ومعاقبة الجهات الفاعلة المسئولية عن السلوك الخبيث القائم على الإنترنت.

وهذه العقوبات قد تفرض بشكل مؤقت أو دائم وتأخذ أنماطًا عدة، منها تجميد الأصول وفرض قيود على العلاقات الاقتصادية مع الأشخاص أو الكيانات الخاضعة للعقوبات إلى جانب حظر السفر على الأفراد وغيرها من التدابير المضادة، مثر فرض الغرامات المالية، أو منع تصدير أو استيراد سلعة أو تقنيات مرتبطة، بينما تشير العقوبات السيبرانية إلى فرض (العزلة الرقمية القسرية) ليس على الدولة المستهدفة ففقط، بل كذلك على الأفراد والشركاء

=

No One, Perspectives On Politics, Vol. 11, No. 4, December 2013.

التجاريين من الخارج، سواء كانت شركات أو دول أخرى، والتهديد برفض العقوبات في الة اختراق الحظر، أو عدم الالتزام بلائحة العقوبات المعلنة من قبل دولة أو أكثر(١).

واستقت "العقوبات السيبرانية" Cyber Sanctions بعضًا من خصائصها من التعريف التقليدي للعقوبات الدولية، ولكن أصبح مجال تطبيقها ومدى تأثيرها مختلفًا، إن العقوبات السيبرانية كغيرها من العقوبات الدولية لا تتطلب إعلان المسئولية عن الإجراء المستلزم للعقوبات، ومن ثم تبتعد عن الطبيعة القانونية لما إلى الطابع السياسي، خاصة إذا تمت من قبل أطراف دولية خارج نظام الأمم المتحدة.

([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

وتحد العقوبات السيبرانية من فرص التعاون الدولي في مجال المعرفة والتقنية، وهو ما يعني أن فرضها يحمل تأثيرات سلبية على تقدم الحضارة الإنسانية.

ويختلف تأثير فرض العقوبات السيبرانية عن تأثيرات (الفجوة الرقمية) Digital Divide التي تتعلق بالفجوة بين الذين بمقدورهم استخدام الإنترنت، بسبب امتلاكهم المهارة اللازمة والقدرة المادية، والذين لا يستطيعون، ويكون ذلك غير مقصود لكنه قد يحمل دلالات سياسية وتنموية كحالة منع الدول الكبرى تصدير التكنولوجيا المتقدمة إلى الدول النامية بما تسبب في وجود فجوة رقمية وتكنولوجية ترتبط (في جزء منها) بالورث الاستعماري الغربي.

وهناك فجوة رقمية غير متعمدة بين الريف والحضر داخل الدولة، لكنها قد ترجع لأسباب جغرافية أو اقتصادية، وذلك كأثر التعليم ومستوى الدخل على حجم التفاوت بين مواطني الدولة في الحصول على خدمات الإنترنت أو الهواتف الذكية.

وتختلف العقوبات السيبرانية عن حالة (الحروب السيبرانية) Cyber War؛ لأنها تقع في المنطقة الرمادية بين الحرب والسلام، كحالة التنافس الدولى على الأسواق الرقمية بين القوى الدولية التي من أهم إرهاصاتها الحرب التجارية بين الشرق "روسيا والصين"، والغرب "الولايات المتحدة وحلفائها"، والحروب السيبرانية تشير إلى استخدام الهجمات السيبرانية ضد دولة قومية، مما يتسبب في ضررها البالغ بها في ذلك توظيفها في الحرب المادية وتعطيل أنظمة الكمبيوتر الحيوية وفقدان الأرواح، وهناك نمط الحرب الساخنة ونمط الحرب الباردة (السيبرانية).

وقد يتم استخدام العقوبات السيبرانية كنمط من أنماط (الدبلوماسية السيبرانية) Cyber Diplomacy إلى جانب نمط التعاون الرقمي، وتعني الدبلوماسية السيبرانية باستخدام الأدوات الدبلوماسية لمعالجة القضايا الناشئة في الفضاء السيبراني من خلاله، وتشمل هذه القضايا مجموعة من الموضوعات الأمنية والاقتصادية وحقوق الإنسان بما في ذلك معايير الأمن السيبراني الدولية، والوصول إلى الإنترنت، والخصوصية، وحرية الإنترنت، والملكية الفكرية، والجرائم

الإلكترونية، وحالة الصراع والتنافس السيبراني الذي ترعاه الدولة، إلى جانب الاستخدام الأخلاقي للتكنولوجيات الرقمية والتجارة [1].

٢- العقوبات السيبرانية ومفهوم السيادة الرقمية:

يعبر مفهوم (السيادة السيبرانية) Cyber Sovereignty عن جهود الدولة لإنشاء حدود على الشبكة، ومن ثم ممارسة شكل من أشكال التحكم والسيطرة، ويمكن أن يأتي في شكل من إنفاذ القانون على هذه الحدود، وترتبط بقدرة الدولة ذات السيادة على فرض قوانينها أو تشريعاتها على تدفق البيانات والمعلومات إليها من الخارج إلى

---

(1) 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

الداخل، أو من الداخل إلى الخارج، ومن ثم فإنها تعد بمنزلة اختيار ذاتي "للعزلة الرقمية" Digital Isolation من قِبَل الدولة(١).

وتبنت العديد من الحكومات قوانين جديدة لتشكيل هويتها الوطنية والإقليمية والسيطرة على امتلاك البيانات، وبدأت فكرة (سيادة الإنترنت) وتشريعاته حول العام تلعب دور في عملية تفتيت وأقلمة الإنترنت، إلى جانب الأبعاد الثقافية والجغرافية، والكشف عن التجسس الأمريكي على الملايين عبر العالم، وقضية (إدوارد سنودن) الموظف السابق في هيئة الأمن القومى الأمريكي، وأخذت الهيمنة على الإنترنت ترتبط بأبعاد أمنية واقتصادية وتنظيمية وسياسية واجتماعية، والعمل على تطوير أطر تشريعية لممارسة المزيد من الرقابة والتحكم في تدفق المعلومات الحرجة والحساسة؛ مثل تبني الصين، وفرض "جدار الصين العظيم للحماية" Great

(١) إبان ما عرف بثورات الربيع العربي قامت العديد من الحكومات العربية بقطع الإنترنت؛ سعيًا للسيطرة على موجة الاحتجاجات عام ٢٠١١م لاعتبارات تتعلق بالأمن القومي.

Firewall Of China الذي يحد من الوصول إلى البيانات من جانب العديد من الشركات الأمريكية» مثل شركة جوجل وميتا.

ولعبت عملية فرض العقوبات الدولية من جانب الولايات المتحدة وبعض الدول الغربية ضد كوريا الشمالية وإيران والصين وروسيا والبرازيل في تطوير قدرات وطنية لدى هذه الدول في سبيل بناء مشروعات للسيادة السيبرانية.

وعلى الرغم من الاعتقاد الشائع بأن النظم (السلطوية) هي الأكثر إقبالًا على قطع الإنترنت، إلا أن هناك دراسة شملت ٩٩ دولة بين عامي (١٩٩٥ – ٢٠١٠م) كشفت عن وجود ٦٠٦ حالات قامت فيها حكومات ديمقراطية وأخرى ناشئة بقطع نقاط تبادل الإنترنت أو تقييد عبور البيانات، ومثلت ٣٩% منها في الدول الديمقراطية، و٥٢% وقعت في الأنظمة الاستبدادية، و٦% في الديمقراطيات الناشئة؟، و٣% وقعت في دول هشة[١].

([1]) Philip N. Howard, Sheetal D. Agarwal, and Muzammil M. Hussain, "The Dictators' Digital Dilemma: When Do =

وأصبح لغلق الإنترنت خسائر اقتصادية تتكبدها الحكومات، خاصة داخل النظم السلطوية، التي قد تتم لأسباب سياسية أو أمنية، وهو ما يكشف من جهة أخرى عما يمكن أن – تتكبده الدول حال فرض عليها حصار رقمي من الخارج؛ ففي عام ٢٠٢٢م بلغت الخسائر ما قيمته ١,٥ مليار دولار في روسيا، وتأثر ما يزيد على ١١٣ مليون مستخدم، وتأثر ١٦,١ مليون مستخدم، و٤٢٩,٥ مليون دولار في كازاخستان، و٢٠٧,٧ مليون دولار وتأثر ١,٦ مليون مستخدم في ميانمار، وتأثر ١٠٤,٤ مليون مستخدم و٨٢,٧ مليون دولار في نيجيريا، وتأثر نحو مليون مستخدم و٣٣,٢ مليون دولار في إثيوبيا، وفي عام ٢٠٢٢م شهدت ١٦ دولة حتى يوليو ٥٤

=

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/wp-content/uploads/2016/06/10_dictators_digital_network.pdf

انقطاعًا للإنترنت بشكل متعمد، وذلك أدى لتكلفة بلغت قيمتها ١٠,١٦ مليار دولار، بينما وشهد عام ٢٠٢١م ٥٠ انقطاعًا بتكلفة ٥,٤٥ مليار دولار فقط [١].

٣- خصائص وأنماط العقوبات السيبرانية ومراحل الإسناد لفرضها:

تتميز العقوبات السيبرانية بطبيعة متداخلة من التأثير الاقتصادي أو العسكري أو الدبلوماسي وغيره من الأبعاد المرتبطة بالنشاط السيبراني وعلاقته بتلبية الاحتياجات الإنسانية، وهو الأمر الذي أحدث تأثيرات عميقة تتجاوز التأثير التقليدي لباقي أنماط العقوبات الدولية الأخرى، وذلك بالنظر إلى مداها وانتشارها والخسائر المتوقعة منها، وتأثيرها العابر للحدود، وإمكانية إصابة أطراف ثالثة

(١) تقرير: قطع الإنترنت المتعمد تسبب في خسائر ب ١٠ مليارات دولار في عام ٢٠٢٢م (صحيفة الشرق، ٧ يوليو ٢٠٢٢م) على الرابط:

https://bit.ly/3AsI4YV

ليست معنية أو طرفًا في الصراع المباشر مع الدولة التي فرضت تلك العقوبات السيبرانية.

وأصبح لعزل الدولة كليًا أو جزئيًا عن المجال السيبرانى بشكل قسري تأثيرات متعددة على السكان المدنين الأبرياء، ويتم فرضها من قبل دولة أو أكثر، ويكون للشركات التقنية العابرة دور فيها، ويكون لها تأثير عميق بشكل مباشر وغير مباشر في كافة القطاعات داخل الدولة، بما في ذلك المنشآت المدنية والخدمات المقدمة إلى المدنيين، إلى جانب التأثير في الجهات الرسمية داخل الدولة.

ويتوقف نجاح العقوبات السيبرانية وتقييم أثرها على الجهات التي تفرضها، سواء تمت تحت مظلة أممية أو سلوك أحادي من جانب الدولة، وانعكاس ذلك على المشروعية والاعتراف الدولى بها، وعلى امتلاك تلك الدول نظام للعقوبات يتميز بالمراجعة والفاعلية.

وتتم مراحل ومستويات الإسناد لفرض العقوبات السيبرانية بعد حدوث الاعتداء السيبراني أو النشاط المعادي، وتحميل المسئولية استنادًا إلى ما تراه (الدولة) من أدلة رقمية تثبت التورط أو العلاقة

بشكل مباشر أو غير مباشر، أو كونها تدخل في حالة التوتر الدولي بين القوى الدولية.

وتأتي المرحلة الأولى وهي ترتبط بالإسناد التقني من خلال التحري الإلكتروني والبحث عن الأدلة لمعرفة هوية المهاجم، ثم تأتي المرحلة الثانية بالإسناد السياسي، وهي تتعلق بجمع المعلومات وتبادلها حول تحديد الإجراءات وتسمية الجناة إن أمكن، ثم تأتي المرحلة الثالثة بتوجيه اللوم الجنائي ولائحة الاتهام، ثم ينبثق من ذلك المرحلة الرابعة، وهي رد الفعل السياسي والتشاور بين السلطة التنفيذية والتشريعية حول فرض العقوبات السيبرانية.

ومن ضمن أنماط العقوبات السيبرانية التي تأخذ نمطًا تقنيًا أو ماليًا أو تشريعيًا يتم تطبيقه بشكل منفرد أو مجتمع من قبل الدولة الخصم ضد دول أخرى أو العكس، أو ضد طرف من غير الدول؛ منها:

- حجب مواقع إلكترونية إعلامية أو حكومية رسمية من الولوج الى الداخل [1].
- منع تصدير تقنيات التجسس ومراقبة الاتصالات أو التقنية المتقدمة.
- منع عمل شركات تقنية وطنية في البلد المعني بحجة الحفاظ على الأمن.
- ممارسة ضغوط على الشركات التقنية الكبرى لسحب خدماتها من الداخل.
- تجميد التعاون في مجال البحث العلمي والابتكار والاستثمار الأجنبي.
- شن هجمات سيبرانية ضد البنية التحتية الحيوية، خاصة المواقع الرسمية.

(١) والتي كان منها إبان الأزمة القطرية مع دول الرباعية العربية، حيث تم اتخاذ إجراءات عقابية متبادلة كحجب لموقع قناة الجزيرة أو المواقع الرسمية القطرية والتي رأت أن تلك العقوبات من شأنها الحد من التأثير القطري في =

- شن تطبيقات الحروب النفسية والمعلومات المضللة والأخبار الزائفة.
- قطع الكابلات البحرية المرتبطة بخدمة الإنترنت الواصلة للدولة المستهدفة.
- فرض غرامات مالية على الشركات الأجنبية تحت دعاوى انتهاك القوانين المحلية.
- فرض رسوم جمركية على استيراد مكونات تقنية من الخارج من دول محددة.

٤- أهداف الفاعلين في تطبيق العقوبات السيبرانية:

تهدف عملية فرض التدابير والإجراءات السيبرانية القسرية إلى تغيير سلوكيات الأطراف المعنية، والتي يثبُت بشكل مباشر أو غير مباشر بتورطها أو قيامها بأنشطة سيبرانية ضارة أو اختراقات ضد الأشخاص الطبيعيين أو الاعتباريين، أو الكيانات أو الهيئات

=

الداخل؛ وهناك كذلك اتجاه لحجب بعض المواقع من قبل الحكومات التي تراها تحمل محتوى إباحيًا أو سياسيًا معارضًا.

الحكومية أو الخاصة في دولة أخرى أو أكثر، وتهدف كذلك العقوبات إلى تقييد الوصول إلى المجال السيبراني أو مقدراته لإحداث تأثير اقتصادي ومالي وتجاري وسياسي بما يمثل ضغطًا لتغيير السلوك لدى الدولة التي يتم فرض تلك العقوبات عليها، أو ضد الفاعل من غير الدول.

وتدخل إجراءات فرض العقوبات السيبرانية ضمن الردع السيبراني، وضمان تعزيز القدرة على منع الخصم من الفعل أو رد الفعل داخل المجال السيبراني، ولفرض الامتناع عن الإتيان بأنشطة سيبرانية، سواء على مستوى الدفاع أو الهجوم، أو العمل على منعه من تطوير قدراته، سواء على مستوى الهجمات السيبرانية، أو في مجال الدفاع السيبراني، أو في مجال التنمية التقنية.

ويتم ذلك عبر تبني إجراءات مادية عبر القرصنة، أو الاختراق، أو التدمير للقدرات السيبرانية، أو البنية التحتية المعلوماتية، أو عبر القيام بإجراءات أخرى معنوية وشن حروب نفسية عبر المجال السيبراني للتأثير في تماسك الخصم، أو من خلال التأثير في البيئة الاستراتيجية المحيطة بالمجال السيبراني للدولة أو المستهدف عبر

تعزيز التعاون الدولي ضدها أو تبني اتفاقيات ثنائية وإقليمية لمواجهة التهديدات السيبرانية أو عبر تطوير منظومة دولية قانونية للتعامل مع الأنشطة السيبرانية الضارة.

ويتم فرض العقوبات السيبرانية إما للرد على القيام بأنشطة سيبرانية معادية ذات طبيعة صلبة في شكل قرصنة أو اختراقات، أو أن تأتي للرد على تدخلات ناعمة عبر توظيف المجال السيبراني في الأنشطة التجسسية، أو شن الحروب النفسية، أو نشر المعلومات والأخبار المضللة أو التدخل في الشئون الداخلية، أو تأتي العقوبات السيبرانية التى قد تفرضها الدولة محليًا للرد على انتهاك القوانين المحلية المنظمة للتجارة والاستثمار الأجنبي، وتبني الدولة سياسة حمائية ضد المنتجات المستوردة من الخارج.

وقد تأتي العقوبات السيبرانية في محاولة لتضييق الخناق على الدولة المتورطة في صراع عسكري مع دولة أخرى، وممارسة الأطراف الدولية المساندة لأحد طرفي الصراع للضغوط الاقتصادية والمالية والتجارية.

ويتم فرض العقوبات السيبرانية لتعزيز قدرة الدولة على حماية أمنها القومي وردع الجهات الفاعلة في الأنشطة والتهديدات السيبرانية، وتضمين الاستجابة الوطنية في إطار الجهود العالمية لمواجهة التهديدات السيبرانية.

وعلى الرغم من غلبة الأهداف الأمنية على فرض العقوبات السيبرانية، إلا أنها تكشف عن أهداف اقتصادية أو سياسية أو قانونية أو ثقافية بشكل فردي أو مجتمعة.

وتفرض «العقوبات السيرانية» من قبل الحكومة أو الدولة لحماية الصناعة أو الابتكار، أو حماية الملكية الفكرية، أو حقوق النشر أو حماية الأسرار التجارية.

ويمكن للدولة القومية والشركات الكبرى ممارسة حق تقييد الوصول إلى البيانات بشن هجوم سيبراني يكون من شأنه منع قدرة الخصم أو الهدف من رغبته في المشاركة أو المعرفة أو الثروة، ومنعه من تطوير قدراته في مجال الأسلحة السيبرانية، وهو ما ذكرته استراتيجية الأمن السيبراني لعام ٢٠١٥م الصادرة عن وزارة الدفاع الأمريكية.

وينقسم الفاعلون في فرض العقوبات السيبرانية إلى فاعلين من الدول أو من قبل منظمات دولية أو من فاعلين من غير الدول من الشركات التقنية الكبرى، والتي تخضع لسياسات الدولة التي تعمل من خلالها أو تدفع ضرائبها لها، وقد يكون المستهدف من تلك العقوبات:

أ- أن تكون (الدولة) كوحدة جغرافية متكاملة كحالة قطع كابلات الإنترنت وفرض حصار رقمي شامل.

ب- فرض عقوبات على هيئة أو هيئات حكومية يتم اتهامها بالضلوع في الأنشطة السيبرانية العدوانية.

ج- بتعرض فرد أو أفراد من مواطني الدولة للعقوبات من جراء اتهامهم بالقرصنة أو اختراق للبنية التحتية الحيوية في دولة أخرى.

د- تعرض الشركات التقنية الكبرى العابرة للحدود أو الشركات التقنية المحلية في توسعها الخارجي إلى عقوبات لمنعها من التطور أو تحقيق الأرباح، أو التوسع في الأسواق الخارجية، أو الحد من استفادتها من سياسات اقتصاد السوق.

٥- العلاقة بين العقوبات السيبرانية ونظيرتها الاقتصادية:

تشمل العقوبات الاقتصادية فرض مجموعة من العقوبات التجارية والمالية التي يفرضها بلد أو مجموعة من البلدان ضد بلد آخر، أو مجموعة من الأفراد أو المنظمات. وهناك عدة اتجاهات، يرى الأول أن العقوبات السيبرانية جزء من العقوبات الاقتصادية، خاصة فيا يتعلق بالتصدير أو الاستيراد للمنتجات التقنية، بينما يرى الاتجاه الثاني أن العقوبات السيبرانية عقوبات يسيطر عليها البُعد التقنى أكثر من الاقتصادي، بينما يرى الاتجاه الثالث والأخير أن العقوبات السيبرانية عقوبات خاصة في طبيعتها؛ فهى غير مسبوقة بالنظر إلى ارتباطها وتدخلها مع مختلف الأنشطة السياسية والاقتصادية والأمنية والثقافية وغيرها .

فقد أصدر الرئيس باراك أوباما أمرًا تنفيذيًا بتأسيس أول عقوبات اقتصادية ضد من يقوم أو يتورط في شن هجمات سيبرانية والتى تستهدف الأفراد والهيئات، وتؤثر في مقتضيات الأمن القومي، أو السياسة الخارجية، أو النمو الاقتصادى، أو الاستقرار المالي وخولت وزارة الخزانة بتجميد أصول الجهات المستهدفة واتسع مجال

توجيه العقوبات ليشمل أي نشاط يهدد ديمقراطية الانتخابات، وليس فقط أمن البنية التحتية الحرجة [1].

وتركز العقوبات الاقتصادية بمفهومها التقليدي على وضع قيود على "الحاجة إلى البيع" و"الحاجة إلى الشراء" بينما جاءت بيئة المجال السيبراني لتضيف أبعادًا جديدة ترتبط بالحاجة إلى المعرفة و"الحاجة إلى المشاركة"، ويتم ذلك بالاقتران مع العقوبات الاقتصادية، أو بصورة منفردة كوسيلة للإكراه.

وظهر نمط من العقوبات التي ترتبط بالمخاوف من تأثر نقل التكنولوجيا على الأمن القومي، أو الاستحواذ على الأسواق أو الهيمنة التجارية، ومن جهة أخرى مكنت التغييرات التكنولوجية (المستهدف) بالعقوبات من القدرة للالتفاف عليها، سواء كان من الفاعلين من الدول، أو من غير الفاعلين من الدول.

([1]) Cory Bennett, "Obama extends cyber sanctions power", The Hill.com,29/3/2016, https://bit.ly/3yh9yi4

العقوبات السيبرانية لا تتطلب بالضرورة أن يقوم من يستخدمها بالسيطرة المادية على الشبكات أو قطع لكابلات الإنترنت، والتي تكون مملوكة لدول أخرى، بل يتم التركيز على إحباط ومحاصرة رغبة الخصم في الحاجة الرقمية في المعرفة والمشاركة والتوسع في الأسواق، والتى تكون لسلامة البنية التحتية دور في تفعيلها أو القدرة على تطبيقها من جانب طرف آخر معاد.

ويوفر المجال السيبراني بيئة تسهل من فرض العقوبات السيبرانية مقارنة بالأخرى الاقتصادية، ويمكن أن يتم فرضها بناء على السلوك الأحادي من جانب الدولة أو غيرها دون الحاجة إلى التوصل إلى توافق دولي بشأنها.

وتهدف العقوبات الاقتصادية بشكل واضح لتقييد ممارسة الدولة لسيادتها، في حين يصعب تطبيقها في مجال فرض العقوبات السيبرانية؛ فاحترام سيادة الدولة لا تمنع الدولة من القيام بعملية سيبرانية ضد البنية التحتية المعلوماتية التي يستخدمها الإرهابيون في دول أخرى، حتى دون موافقة الدولة الأخيرة مادامت العملية لم

تشتمل على استخدام القوة الفعلية أو التدخل العسكري الذى يقترب من الأنشطة الاستخباراتية – السيبرانية.

وتتوقف فاعلية العقوبات السيبرانية على قدرة الدولة أو الطرف المستهدف على الاعتماد بشكل كبير على المعرفة أو المشاركة من الخارج، وتوافر درجة ما من الهيمنة السيبرانية بشكل يمكن الدولة من فرض العقوبات وشل قدرات الخصم، مثل مواجهة الولايات المتحدة تحديات أمام هيمنتها السيبرانية التقليدية لمصلحة قوى جديدة مثل الصين وروسيا.

تأثير التطور التكنولوجي والمجال السيبرانى في البيئة المصاحبة للعقوبات الدولية:

١- تأثير التطور التكنولوجي في طبيعة العقوبات الدولية:

استندت الأمم المتحدة منذ تأسيسها بعد نهاية الحرب العالمية الثانية إلى وجود إطار قانوني يُنظم عملية فرض العقوبات الدولية للحيلولة دون نشوب حروب جديدة، وعُدَّت ضمن التدابير المضادة في القانون الدولي العام للتأثير في سلوكيات الدول القومية لجعلها أكثر التزامًا بالقانون الدولي، وارتبطت شرعية تطبيق العقوبات

بوجود شروط لفرضها ومراجعتها، والاعتراف بطابعها الاستثنائي في العلاقات الدولية، ومن ثم تم النظر إلى "العقوبات الدولية" International Sanctions على أنها مجرد وسيلة (لتصحيح المسار) وليست هدفًا في حد ذاتها، وتحولت كـ "أداة تستخدمها الدول أو المنظات الدولية لإقناع حكومة معينة أو مجموعة من الحكومات بتغيير سياستها عن طريق تقييد التجارة أو الاستثمار أو أي نشاط تجاري آخر[١].

وتعتمد العقوبات الدولية على تبني تدابير قمعية أو إكراهية للضغط على بلد ما لتغيير سياساته المحددة، سواء تم ذلك تحت مظلة أممية أو بإجراءات أحادية من جانب الدول، ولا تشتمل على استخدام القوة العسكرية المباشرة مثل العقوبات الدبلوماسية والعسكرية والرياضية والبيئية والاقتصادية.

(١) نيكوالس مولدر، سلاح العقوبات، (مجلة التمويل والتنمية، صندوق النقد الدولي، ع٥٩، ق٢، يونيو ٢٠٢٢م) ص٢٠. على الرابط:
File://c:/users/GR/Downloads/fd0622a.pdf

وأثرت التطورات التكنولوجية في البيئة الدولية للعقوبات من خلال:

أ- توفير بيئة دولية جديدة يغلب عليها زيادة حدة التنافس الدولي ذى الطبيعة التجارية أو الاستخباراتية، سواء بين الدول القومية أو بينها وبين الفاعلين من غير الدول.

ب- تصاعد اتجاه الدول لتوظيف الفضاء السيبراني في ممارسة الضغوط والإكراه في صراعها مع الآخرين، وارتفاع تكلفة اللجوء إلى القوة العسكرية المباشرة مقارنة بالأنشطة السيبرانية العدوانية، وضغوط الرأي العام العالمي المناهض للحرب، إلى جانب منظمات المجتمع المدني العالمي في منع الانزلاق في حرب مباشرة[١].

(١) الجدير بالذكر أن التطور في الاتصالات كان له دور في تاريخ الصراعات والحروب الدولية؛ فقد كان من بين أسباب دخول الولايات المتحدة الحرب العالمية الثانية إقدام اليابان على قطع خطوط وكابلات التلغراف بين بريطانيا والولايات المتحدة.

ج- إحداث العقوبات الدولية خسائر تجارية واقتصادية أكثر من السابق في الوقت نفسه زادت القدرة على التخفيف من وطأتها والالتفاف حول مساراتها عبر وسائط تقنية حديثة، وأصبحت لا تشكل العقوبات تهديدًا مباشرًا كما كانت عليه إبان

فترة الثلاثينات من القرن الماضي، وهو ما يحد من تحقيق أهدافها التي منها التصعيد العسكري.

د- إفساح المجال لانتشار الصدمات الناجمة عن العقوبات عبر مختلف أجزاء الاقتصاد العالمي نتيجة زيادة التكامل والتشبيك بين الأسواق، ومن ثم أدت العولمة إلى زيادة التكلفة الاقتصادية لاستخدام العقوبات ضد الاقتصادات الكبرى التي تتمتع بقدر كبير من التكامل فيما بينها، وأتاحت هذه البلدان فرصة أكبر للثأر من خلال الروابط الاقتصادية والتكنولوجية بدلًا من التدخل العسكري.

هـ- تغير طبيعة العقوبات من حيث المخاطر والتكلفة الناجمة عنها، بينما ظلت قنوات انتشارها فضلًا عن تأثيرها على ارتفاع السلع الأولية، وتعطيل سلاسل الإمداد العالمى، والخسائر

الاقتصادية، ومستوى التأثير في حياة المواطنين بعيدًا عن النظم السياسية.

و- أصبح للتغييرات التقنية دور في وجود بنية تحتية كونية للمعلومات تمثل إدارتها أهم تحديات الأمن الجماعي الدولي، وغياب ذلك قد مثل مناطًا للتوظيف السياسي من جانب الدول المهيمنة تقنيًا مثل الدور الأمريكي في إدارة الموارد الحرجة للإنترنت.

ز- إحداث تغييرات في التجارة الدولية والتعاملات المالية عبر الحدود وتعاظم دور الشركات التقنية الكبرى، ما يطرح إشكاليات أمام مستقبل النظام الاقتصادي العالمى، خاصة طبيعة النظام المالي العالمى، مع ظهور العملات المشفرة والأصول الرقمية.

٢- تصاعد المصالح والمخاطر في المجال السيبراني:

دفعت تطبيقات الثورة الصناعية الرابعة إلى زيادة حدة الصراع والتنافس والتعاون بين القوى في النظام الدولي، وانعكس ذلك على تحول وانتقال القوة وممارستها وطرق الحصول عليها، سواء على مستوى الحكومات أو الأفراد أو الشركات، وأصبح للمجال السيبراني

دور في تقديم الخدمات المدنية والعسكرية على حد سواء، وتوفير بيئة رقمية وسيطة لانتقال الأفكار والأموال عبر الحدود، بالاعتماد على البنية التحتية المعلوماتية.

ودفع التقدم الحاصل خلال العقدين الأخيرين في انتشار ونفاذ تكنولوجيا الاتصال والمعلومات عالميًا؛ ففي الفترة بين عامي ٢٠١٩- ٢٠٢١م ارتفعت نسب استخدام الإنترنت في أفريقيا ومنطقة آسيا والمحيط الهادي بنسبة تتراوح بين ٢٣% و٢٤% على التوالي. وارتفع عدد المستخدمين عالميًا بمقدار ما يقرب من ٨٠٠ مليون ليصل إلى ٤,٩ مليار شخص عام ٢٠٢١م أو ٦٣% من سكان العالم، وبات نحو ثلث سكان العالم غير متصل أي ما يعادل نحو ٢,٩ مليار شخص يعيش ٩٦% منهم في البلدان النامية[١].

([1]) Johnson, worldwide digital population as of April 2022, statista.com, May 9, 2022. https://bit.ly/3a5JAnB

جاء ذلك مع زيادة مقابِلة أخرى في معدلات التعرض للجرائم السيبرانية كأحد أنماط التهديدات السيبرانية، التي ارتفعت بنسبة وصلت لـ ٦٠٠% عام ٢٠٢١% وتلقت الشركات وحدها ٤٠% منها مقارنة بعام ٢٠٢٠م وبمتوسط ٨٧٠ هجومًا سيبرانيًا، وشهدت أوروبا وأمريكا الشمالية أكبر ارتفاع في الهجمات السيبرانية مقارنة بالعام ٢٠٢١م حيث وصلت إلى ٥٦% و٥٧% على التوالي، وشهدت منطقة آسيا والمحيط الهادي أكبر عدد من محاولات هجوم الفدية، وزادت الهجمات السيبرانية بها بنسبة ٢٠% في حين بلغت ٣٧% في أمريكا اللاتينية، و١٥% في أفريقيا(١).

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

وبلغت الخسارة العالمية ٦,٥ تريليون دولار سنويًا عام ٢٠٢١م، ويتوقع أن تصل إلى ٥ تريليون دولار عام ٢٠٢٥م بعد أن كانت ٣ تريليونات عام ٢٠١٥م [١].

وأصبحت الهجرات السيبرانية تقع في مرتبة عالية من المخاطر التي تهدد الاقتصاد والتجارة الدوليين، خاصة مع نمو التجارة الإلكترونية في الاقتصاد العالمى، وفي ظل وجود درجة عالية من التعقيد والتشبياك والاعتاد الدولي المتبادل، سواء على المستوى الفوقي أو التحتي، وفي ظل بيئة دولية "سيبرانية" جديدة تحولت معها ممارسة أنماط القوتين الصلبة والناعمة، ويقف وراء تلك التهديدات السيبرانية فاعلون من الدول التي تشن التهديدات على دول أخرى في ظل حالة الصراع فيما بينها، وهناك هجمات يقف وراءها من يعملون في الجريمة المنظمة، والقراصنة الذين ينشطون

(1) 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/

بشكل مستقل أو بالتحالف مع أحد الأطراف الدولية، وهناك هجمات سيبرانية يمكن أن تأتي من الداخل عبر الموظفين أو الساخطين أو المعارضين للنظام السياسي، وهناك هجرات يمكن أن تشنها الجماعات الإرهابية ضد المنشآت الحيوية بهدف تحقيق هدف سياسي.

وفي الأزمات الدولية بدأ يظهر دور الإنترنت وتوظيفه في العمل العسكري، والحفاظ على مرونة الخدمات الحكومية والعمل على تماسك الجبهة الداخلية، وإبقاء المواطنين على اتصال ومعرفة بالمعلومات، ناهيك عن إمكانية تلقيهم المساعدات والإغاثة، وبرز دور شبكات التواصل الاجتماعي في التأثير في الرأي العام تجاه الموقف من الحرب، سواء على مستوى الجبهة الداخلية أو الرأي العام العالمي.

وبرزت عدة متغيرات داخل البيئة الدولية منها:

المتغير الأول: إن تسارع وتيرة التغييرات التقنية عمل على الحد من القدرة على التنبؤ بالمخاطر، ما يعزز من أهمية الاستجابة للتهديدات وإنشاء نظام للردع السيبراني.

المتغير الثاني: إن أمن الفضاء السيبراني يتطلب وجود نظام مرن وآمن للأفراد والشركات والحكومات، وهو ما يعزز من الثقة في البيئة الرقمية ودورها في تحقيق أهداف التنمية المستدامة.

المتغير الثالث: تزايد حجم الخسائر الاقتصادية وارتفاع تكلفة التهديدات السيبرانية والوعي لدى صانعي القرار من الحكومات ومختلف أصحاب المصلحة في مجتمع المعلومات العالمي.

المتغير الرابع: وجود حالة من التبني السريع للرقمنة من قبل الحكومات، سواء كانت في شكل تطبيقات أو منتجات أو لتقديم الخدمات، ومن ثم إمكانية زيادة التعرض للمخاطر.

المتغير الخامس: تصاعد دور المجال السيبراني في عمل وتكامل سلاسل التوريد العالمية، ووجود البرمجيات مفتوحة المصدر أو الطابع العابر للحدود للمكونات التقنية أو البرامج بما يطرح إشكاليات حول ملكية الأنظمة والاختصاص القانوني، ووجود أطراف ثالثة لتقديم وظائف مهمة.

المتغير السادس: تزايد اعتماد الدول على الخدمات الرقمية المتكاملة مع تبني إنترنت الأشياء (IOT) وتطبيقات الذكاء

الاصطناعي، التي يمكن أن تتم –في جزء كبير منها– عبر الحدود الدولية، ومن قبل شركات أجنبية كبرى.

المتغير السابع: تصاعد أهمية الاقتصاد الرقمي في توسيع الأسواق، وفي جني الأرباح، وفي الاستثمار في الإبداع والابتكار.

المتغير الثامن: حالة التداخل الوظيفي بين المجال السيبراني وغيره من المجالات الدولية الأخرى كالبر والبحر والجو والفضاء الخارجى.

المحور الثاني: مشروعية العقوبات السيبرائية وإشكاليات التطبيق في ضوء القانون الدولي:

١– مشروعية العقوبات السيبرانية في ضوء القانون الدولي:

على الرغم من تأكيد ميثاق الأمم المتحدة على أهمية حل الخلافات بالطرق والوسائل السلمية، إلا إن الفصل السابع من المثاق نصت المادة (٤١) منه على أن (لمجلس الأمن أن يقرر ما يجب اتخاذه من التدابير التي لا تتطلب استخدام القوات المسلحة لتنفيذ قراراته؛ وله أن يطلب إلى أعضاء الأمم المتحدة تطبيق هذه التدابير،

ويجوز أن يكون من بينها وقف الصلات الاقتصادية والمواصلات الحديدية والبحرية والجوية والبريدية والبرقية واللاسلكية وغيرها من وسائل المواصلات وقفًا جزئيًا أو كليًا وقطع العلاقات الدبلوماسية)[1].

وهذه الحالة تفترض ابتداء أن يكون هناك تهديد وخرق للسلام أو القيام بعمل من أعمال العدوان، وهو ما ورد في المادة ٣٩ وللحفاظ على الأمن الجماعى الدولي، وتقر المادة (٤٠) من الميثان بأنه إن لم تفلح هذه الإجراءات انتقل مجلس الأمن إلى إجراءات المادة ٤١ من الميثاق، وهي (إجراءات عقوبات) لا تنطوي على استخدام القوة المسلحة؛ فإن لم تفلح في ردع (الدولة) يتم الانتقال إلى إجراءات القمع العسكرية كما ورد في المادة ٤٢ من الميثاق.

وأباح ميثاق الأمم المتحدة العقوبات الدولية لظروف استثنائية وضرورة إصدار قراراتها من خلال مجلس الأمن بأغلبية الأصوات، ومراعاة مبادئ القانون الدولى لحقوق الإنسان والقانون الدولي

(1) انظر في ذلك لميثاق الأمم المتحدة ١٩٤٥م.

الإنساني، وأن يكون هناك مراجعة دورية لها من قبل المجلس، وإذا ما فرضت العقوبات في سياق نزاع مسلح دولي أو داخلى، يتم تطبيق القواعد العامة للقانون الدولي الإنساني المتعلقة بحماية المدنيين من آثار العمليات العسكرية والقواعد المتصلة بالإمدادات الطبية والغذائية إلى مختلف شرائح الأشخاص موضع الحماية [١].

وقد أقرت محكمة العدل الدولية بأن يأتي الإجراء المضاد في إطار الرد على إجراء آخر غير مشروع ومتعمد، وأن يتم استنفاد الطرق الدبلوماسية بالمطالة بالتوقف عن هذا الإجراء، وأن يتناسب الإجراء المضاد مع الضرر الناجم، وأن يكون الهدف هو الدفع للالتزام بمبادئ القانون الدولي [٢].

---

(١) أنا سيغال، العقوبات الاقتصادية القيود القانونية والسياسية، (المجلة الدولية للصليب الأحمر، ع٨٣٦، ٣١ ديسمبر ١٩٩٩م) على الرابط: https://bit.ly/38yxsLd

(٢) انظر في ذلك قرار محكمة العدل الدولية بين المجر وتشيكوسلوفاكيا على نهر الدانوب في قضية مشروع (Gabcikovo– Nagymaros) الصادر في ٢٥ سبتمبر ١٩٩٧م في قضية غابشيكوفو– ناغيماروس السدود، وقد ذكرت =

أن العلاقة بين التقنية والقانون متسارعة، وكان للتقنية دور تاريخي في تبني قوانين دولية جديدة تنظم الواجبات والحقوق وتنظم استخدام المجالات الدولية، مثل المجال الجوي أو البحري أو الفضاء الخارجي، وتم الاستناد في ذلك إلى ما أقره العرف والمبادئ العامة للقانون الدولي، وميثاق الأمم المتحدة [1].

وساعد ذلك في تحقيق عدة أهداف:

الأول: المرونة الكافية للخروج عن جمود القاعدة القانونية.

الثاني: سد الثغرات.

=

المحكمة أنه لكي يكون الإجراء المضاد مبررًا؛ فيجب أن يفي بعدد من الشروط.

(1) مثل مبدأ التراث المشترك للإنسانية وهو مبدأ مستحدث في القانون الدولي ينصب على مجال جغرافي يحفظ حقوقًا استثنائية ويحد من سيادة الدول بما يتيح لها الاستعمال والاستغلال كمال عام أو ملكية مشتركة لفائدة كيان يسمى الإنسانية.

الثالث: تفسير ماهو غامض من نصوص بها، ووضع أساس لتكوين قواعد جديدة بالقياس أو الاستنباط تدخل ضمن القانون الدولي.

ودفعت حالة الفراغ القانوني نتيجة عدم وضع معايير دولية ملزمة لتنظيم السلوك الدولي ومسئولية الدولة الدولة عبر المجال السيبراني إلى اتخاذ بعض الدول إجراءات أحادية، ومنفردة للدفاع عما تراه مصالحها أو قيمها أو أمنها القومي، ويأتي هذا في ظل وجود درجة عالية من الاستقطاب بين نظريتي الفوضى والتنظيم للمجال السيبراني.

جاء ذلك في ظل (هيمنة سيبرانية) أمريكية مقابل محاولة دولأخرى مثل روسيا والصين، كسر تلك الهيمنة التقليدية، وإحداث تغيير في هيكل النظام الدولي وجعله أكثر تعبيرًا عن حالة التغير الحقيقي في الأوزان النسبية للقوة، والدفع للانتقال من نظام الأحادية القطبية إلى التعددية في النظام الدولي.

وتشهد هذه المرحلة الانتقالية حالة من الصراع بين الأطراف الدولية عبر المجال السيبراني، وهو الأمر الذي يهدد بعسكرته في ظل

تصاعد أنشطة التجسس والقرصنة والاختراقات وسرقة الأفكار الصناعية وغيرها من التهديدات السيبرانية.

وفي محاولة للدفاع والحماية ضد مخاطر الأمن القومي، ظهرت العقوبات السيبرانية كأحد الإجراءات الأحادية التي يتم فرضها دون شرعية دولية، أو أي قرار يمكن أن يصدر من الجهة المخولة دوليًا بإصدار العقوبات الدولية، وهي مجلس الأمن الدولى.

وعلى عكس باقى أنماط العقوبات الدولية؛ فإن العقوبات السيبيرانية أصبح لها تأثيرات تتجاوز المجالات الدولية والأبعاد المتعددة التي تتراوح بين التأثيرات الاقتصادية والإنسانية والثقافية وغيرها، وينبع ذلك من حقيقة دور المجال السيبراني في مختلف الخدمات المدنية، وما يزيد الأمر صعوبة إمكانية الاستخدام المزدوج بين العسكري والمدني وبين التعاون والصراع وبين الحقيقة والتضليل.

ووفق مبادئ القانون الدولي العام، وكذلك القانون الاقتصادي الدولي، والقانون الدولي الإنساني، والقانون الدولي لحقوق الإنسان، وغيرها من المواثيق ذات الصلة، تضعف مشروعية استخدام العقوبات السيبرانية، سواء في عملية فرضها أو بحجم الضرر

الواقع على غير الأطراف المعنية بها، وهو ما ينفي صفة التناسب أو الإبلاغ لمجلس الأمن [1].

ومن ثم فإن اتخاذ إجراءات أو تدابير أحادية قد تمثل تبديدًا للأمن الجماعى الدولي؛ لأن أية عملية لشن هجمات أو إجراءات أحادية من شأنه انتقال التأثير بين الأطراف المعنية إلى باقي الأطراف والفاعلين في المجتمع الدولي، ومن شأنه قيام صراع أو أعمال انتقامية بين طرفين أو أكثر، مثل شن هجمات سيبرانية، أو قطع أو تقييد أو حجب الوصول إلى الشبكة، أو قطع كابلات الإنترنت، أو منع تصدير أو استيراد مواد تقنية، أو تعطيل خدمات الشركات الأجنبية العابرة للحدود، أو فرض غرامات مالية ضخمة على انتهاك قوانين محلية دون مرجعية قانونية دولية.

---

(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.

وعلى مستوى حماية البنية التحتية المعلوماتية خاصة الكابلات البحرية، ينص القانون الدولي للبحار على حماية وضع الكابلات في أعالي البحار في المادة (١١٢) وتم تأكيده في المادة (١١٣) [١]، وهو ما يدخل الأنشطة السبرانية العدوانية في إطار انتهاك للأمن الجماعي الدولي، خاصة مع سوء تطبيق تلك العقوبات، وغلبة التوظيف السياسى عليها، وتأثرها في تقويض النظم القضائية الوطنية، وإحداث حالة من الفوضى والريبة في العلاقات الدولية، وذلك مع إطلاق الاتهامات دون أدلة دامغة تصدر من جهات تحقيق دولية محايدة، وفرض العقوبات دون قدرة الطرف الواقع عليه أن يمارس حق الدفاع ضدها أو تفنيد أسانيدها، ومن ثم تتحول الدول (الفارضة) للعقوبات السيبرانية إلى خصم وحكم في الوقت نفسه، وتجاهل ردود أفعال الأطراف الأخرى، خاصة أن دول «مثل روسيا والصين تقول إنها ضحية كغيرها للتهديدات السيبرانية، وأنها تدعم الجهود الدولية للتوصل لاتفاقية دولية للفضاء السيبراني والجرائم السيبرانية، وأن الولايات المتحدة هي من تقف ضد التقدم

(١) انظر في ذلك القانون الدولى للبحار لعام ١٩٨٢م.

في هذا المشروع، وأن فرض العتوبات السيبرانية يمكن أن يتضرر منه السكان المدنيون الأبرياء بما يجعلها تتعارض مع القانون الدولي الحقوق الإنسان والقانون الدول الإنساني.

من جهة أخرى إن العمل على توسيع دائرة العقوبات السيبرانية إلى جهات حكومية ورؤساء أو مسئولين سياسيين يعارض مقررات القانون الدبلوماسي الذي يعطي لهم حصانة دبلوماسية من التعرض للمحاكمات أو العقوبات، وأن ذلك يمكن أن يتم من خلال توجيه أدلة الاتهام إلى المحاكم المحلية أو اللجوء إلى محاكم دولية، مثل المحكمة الجنائية الدولية أو محكمة العدل الدولية [١].

كما أن تقييد الوصول إلى الإنترنت يمثل انتهاكًا للقانون الدولى لحقوق الإنسان، حيث أضحت حقوق الإنسان الرقمية رديفًا لحقوق

([1]) 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

الإنسان في العالم المادي، ومتداخلة مع مختلف الحقوق الافتصادية و الاجتماعية والثقافية، والمدنية والسياسية، وأصبحت عملية الوصول إلى الإنترنت لا تعتبر في حد ذاتها حقًا من حقوق الإنسان، بل ترتبط كذلك بحقوق الإنسان في الخصوصية، وحرية التعبير والوصول إلى المعلومات، وحرية الاتصال والتجمع، وأصبح الإنترنت ليس فقط منصة لممارسة حقوق الإنسان، بل كذلك للحصول على الخدمات الرقمية بها يعني عدم الاتصال والحرمان من الحصول على الخدمة بها يعني الفقر والاضطهاد والبطالة وتعزيز الفجوة الرقمية، وضعف الاندماج في المجتمع المحلي والعالمي[1].

كذلك من شأن فرض العقوبات السيبرانية التأثير في أمن واستقرار المجال السيبراني الذي بات مرفقًا دوليًا وتراثًا مشتركًا للإنسانية.

([1]) انظر في ذلك إلى الإعلان العالمي لحقوق الإنسان، يمكن الوصول له عبر الرابط:

https://bit.ly/3yGfeCh

٢- العقوبات السيبرانية في ضوء اتفاقيات حرية التجارة العالمية والاستثمار:

إن كان الهدف من العقوبات الدولية حمل الدولة المعنية على احترام قواعد القانون الدولي؛ فإن الهدف من التدابير المضادة في منظمة التجارة هو حمل الدولة المخلة على احترام التزاماتها الناتجة عن الاتفاقيات المتعددة الأطراف، وأنه لا يجوز اللجوء إليها إلا بعد المرور بمراحل إجرائية منصوص عليها في النظام القانوني للمنظمة، ولا تخضع للإرادة المنفردة للدولة المتضررة، وبخاصة في ظل وجود آلية لتسوية المنازعات يمكن لسلطات الدولة أن تحيل قضيتها إلى منظمة التجارة العالمية[١].

وتعطي المادة ٢١ ب ٣ في الاتفاقية العامة للتعريفات الجمركية والتجارة (الجات) التى أصبحت جزءً من اتفاقيات وقواعد التجارة

(١) في نوفمبر ٢٠١٩م وافقت منظمة التجارة العالمية على فرض الصين عقوبات على الولايات المتحدة بقيمة ٣,٦ مليار دولار في نزاع تجاري بينهما يعود إلى ما قبل بدء الحرب التجارية بين البلدين، لكنها قد تؤدي إلى زياداة حدة الحرب التجارية بين البلدين.

العالمية، الحق للدول الأعضاء في فرض عقوبات لحماية أمنها القومي [١]، إلا أنه لا يمكن استخدام استثناء الأمن القومي لتبرير أنواع العقوبات السيبرانية أحادية الجانب، حتى لو تم تأسيسها على أساس معالجة مخاوف الأمن القومى، خاصة أن نص المادة لا يوضح الحدود المعنية لبند الأمن القومي، وهو الأمر الذي يقلل من شرعية العقوبات السيبرانية أحادية الجانب، ويؤثر في طبيعة العلاقة بين السيادة الوطنية والنظام التجاري المتعدد الأطراف القائم عليه القواعد الدولية المنظمة[٢].

---

(١) وتنص هذه المادة على أنه (أ) لا يجوز تفسير أي شيء في هذه الاتفاقية (ب) لمنع أي بلد عضو من اتخاذ أي إجراء يراه ضروريًا لحماية مصالحه الأمنية الأساسية.

(٢) هجيرة تومي، فاعلية التدابير المضادة في ظل منظمة التجارة العالمية، (مجلة العلوم القانونية والسياسية، جامعة الشهيد، ع٩، يونيو ٢٠١٤م) ص ص١١٤-١١٦.

https://www.asjp.Cerist.dz/en/downArticle/110/5/2/5838

وتضع اتفاقية التجارة العالمية الاستثناء الوارد لشرعية فرض العقوبات على ما إذا كان هناك عنصر موضوعي في وقت الحرب أو أي حالة طوارئ أخرى في العلاقات الدولية [1]، ومدى قيام أحد أعضاء منظمة التجارة العالمية بالإبلاغ عن تلك (المصالح الحيوية الأمنية) الحرجة، ومستوى التهديد الذي تتعرض له، ومدى تحقيق التوازن بين القيود التجارية المفروضة ومصالح الأمن القومي المعلنة، من جهة أخرى لا تلبي العقوبات السيبرانية كإجراءات مضادة الحد الأدنى الذي حدده فقه منظمة التجارة العالمية فيه يتعلق بوضع قيود استثنائية لحماية الأمن القومي، وتؤثر عملية

(1) تم تعريف عبارة (الطوارئ في العلاقات الدولية) على أنها حالة نزاع مسلح، أو نزاع مسلح كامن، أو توتر أو أزمة متصاعدة، أو عدم استقرار عام يهدد أو يحيط بالدولة.

فرض العقوبات السيبرانية في تعطيل العلاقات الاقتصادية والتجارية والتأثير في عمل سلاسة القيمة العالمية [1].

من جهة أخرى، تنتهك العقوبات السيبرانية معايير اتفاقيات الاستثمار الدولية (IIAS)، وذلك من قبيل أن القيود المفروضة على ممتلكات المستثمرين والتعاملات مع الأطراف الخاضعة للعقوبات ستؤدي إلى انتهاك المعاملة العادلة والمنصفة وغيرها من معايير المعاملة المنصوص عليها في اتفاقيات الاستثمار الدولية.

ويمكن للدول أن تبرر العقوبات السيبرانية بموجب استثناءات الأمن العام وبنود السلام والأمن الدوليين المنصوص عليها في اتفاقيات الاستثمار الدولية، خلافًا لقانون منظمة التجارة العالمية، على الرغم

([1]) Jason Bartlett and Megan Ophel, Sanctions by the Numbers: Spotlight on Cyber SSantions, Center for a New American Security, May4, 2021.
https://www.cnas.org/publications/reports/sanctions-by-the-numbers-cyber

من اعتراف اتفاقيات الاستثمار الدولية باتخاذ إجراءات وتدابير مضادة مشروعة[1].

٣ – إشكاليات تطبيق العقوبات السيبرانية وفق القانون الدولي:

- صعوبة الاتهام المباشر للدولة عن الوقوف وراء الهجمات السيبرانية، والتي غالبًا لا تلجأ للعمل من خلال أجهزة أو هيئات حكومية رسمية، ويتم بدلًا من ذلك التعاون مع فاعلين آخرين من غير الدول، وقد لا يرتبطون رسميًا معها في إلقاء المسئولية القانونية والتنفيذية.
- صعوبة تحديد مكان انطلاق الهجمات مع إمكانية التخفي التقني؛ فقد تنطلق الهجمات من مكان ثالث أو عبر متعاطفين أو عملاء لها منشرين في أرجاء العالم، وهو أمر يجعل هناك صعوبة في التحري الإلكتروني للأدلة التي

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

تثبت العلاقة مع الفاعل، ويحتاج تطبيق العقوبات السيبرانية إلى اتفاقيات خاصة بالتعاون القضائي المسبق، وهو أمر قد لا يوجد بين دول ليست على علاقة طبيعية مع بعضها بعضًا.

- لا يلقي القانون الدولي المسئولية القانونية على الدولة إلا إذا توافر الاعتراف الرسمي حول شن الأعمال العدائية، وهو أمر مستبعد بسبب محاولة الدولة التهرب من أي مسئولية أو دور في الهجمات السيبرانية، وصعوبة إثبات العلاقة بين الدولة والفاعل من حيث التوجيه والسيطرة ؛ أو التبنى أو الموقف المساند لها[١].
- تقول القاعدة القانونية (لا عقوبة إلا بنص)، ومن ثم فإن العقوبات السيبرانية تفتقد المشروعية جال تطبيقها، وهو ما يقلل فرص مثول دولة أو طرف للمساءلة العامة بموجب الإطار القانوني الحالي.

---

(١) رأت محكمة العدل الدولية أنه لا بد من إثبات أن دولة ما كان لديها "سيطرة فعالة" على كل عمل من الأعمال التى يُسعى إلى نسبتها إلى فاعلها.

- صعوبة تحديد الهدف والسيطرة على نتائج الأعمال العدائية بما يجعله يتعارض مع قواعد القانون الدولي الإنساني وتصيب العقوبات السيبرانية السكان المدنيين بما يجعلها تفتقد التمييز وتؤثر في المنشآت المدنية والحيوية التي يكفل حمايتها القانون الدولى الإنساني.
- صعوبة تعريف (الهجوم السيبراني) بأنه (هجوم مسلح) بموقف القانون الدولي، ومن ثم تغل يد الدولة على ممارسة حقها في الدفاع الشرعي عن النفس الذي يقره ميثاق الأمم المتحدة، والذي اقتضي كذلك لممارسته توافر شروط التناسب والضرورة والإبلاغ لمجلس الأمن الدولي.
- غلبة الطابع السري على تطوير القدرات السيبرانية بشأن تطوير أسلحة سيبرانية أو امتلاكها أو نقلها أو بيعها، وهو ما يحد من القدرة على فرض عقوبات سيبرانية على تطوير أسلحة سييرانية، ويضع إشكالية أمام التحقق الدولي أو فرض إخلاء أو نزع الفضاء السيبراني من الأسلحة السيبرانية.

- على الرغم من إجازة القانون الدولي لفرض العقوبات الدولية، لكنه وضع شروطًا لتنفيذها، يصعب تطبيقها في محال الفضاء السيبراني، خاصة أنها تتم في غياب توافق دولي حول بناء نظام دولي للعقوبات السيبرانية تحت إشراف الأمم المتحدة، إلى جانب صعوبة تطبيق الإجراءات المضادة التي أتاحها الفصل السابع من الميثاق في حالة الاعتداء السيبراني أو التعامل مع الهجمات السيبرانية.
- صعوبة تحقيق التوافق الدولي حول وصف الأعمال العدائية في المجال السيبراني؛ فقد يتم النظر إليها على أنها تعبر عن أنشطة تجارية، أو أنشطة تهدف لحماية الأمن القومي، أو الأنشطة الاستخباراتية، أو جمع المعلومات والبيانات، إلى جانب اعتبار الهجوم السيبراني هجومًا مسلحًا وفق قواعد القانون الدولي.
- إن تشجيع عملية فرض العقوبات السيبرانية سيؤدي إلى تصاعد المزيد من الإجراءات الأحادية الانتقامية التي يكون من شأنها تعكير صفو العلاقات الدولية، ويزيد من

حالة الفوضى ويضر بأمن الفضاء السيبراني، الذي أصبح مرفقًا دوليًا وتراثًا مشتركًا للإنسانية، ومن ثم فإن حماية البنية التحية المعلوماتية الكونية هي مسئولية جماعية مشتركة.

- تواجه عملية فرض العقوبات السيبرانية إشكاليات الاعتراف بالأدلة الجنائية الرقمية، التى تستند إليها أجهزة إنفاذ القانون وسير التحقيقات القضائية، وتم جمعها عبر مصادر متنوعة من الحواسيب والهواتف الذكية، وأجهزة التخزين عن بُعد، والطائرات بدون طيار والمعدات المحمولة على متن السفن، وغيرها، ويتم الاعتماد عليها في استخلاص البيانات زمعالجتها وتحويلها إلى معلومات استخبارتية يمكن بناء وتوجيه الاتهامات على أساسها.
- مدى تأثير ممارسة العقوبات السيبرانية في حقوق الإنسان والحريات الأساسية با فيها الحق في الخصوصية والتعرض لتجميد الأصول أو الممتلكات، وانتهاك للحق في الملكية وحرية ممارسة الأعمال التجارية، وانتهاك للحق في حماية

البيانات الشخصية والإضرار بالسمعة، وحقوق الدفاع والحق في المراجعة القضائية الفعالة.

- هناك تحديات تتعلق بجمع الأدلة الرقمية، خاصة مع إمكانية تغيير عناوين IP أو إخفائها، ومن ثم يصبح موقع عنوان الجاني لا يشكل دليلًا كافيًا ومدى اعتراف الهيئات القضائية بتلك الأدلة، خاصة أن الجاني قد يعمد إلى تغيير عنوانه أو شن الهجمات من موقع طرف ثالث، وإمكانية تعرض المعلومات الحساسة المرتبطة بالدليل الرقمي[١].

العقوبات السيبرانية ومستقبل النظام المالي العالمي:

١- تصاعد الاتجاه نحو بناء نظم مدفوعات وطنية رقمية:

---

(١) 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.

مع التطور في مجال فرض العقوبات الدولية، تزايدت درجات التعقيد في التطبيق مع التطور التكنولوجي وتبني استراتيجيات "خرق العقوبات"، وفرضت الدول الغربية العقوبات لتعطيل النظام المالي الروسي، ولكن ساهم وجود نظام إلكتروني للمدفوعات المحلية في العمل بسلاسة، وعقب انسحاب شركتي "فيزا" و"ماستر كارد" الأمريكيتين من السوق الروسية، ونجحت شركة "مير" Mir لبطاقات الدفع الإلكتروني والمصرفي في تطوير عملها عبر ٨ سنوات وتعزيز قدرة الاقتصاد الروسي في مواجهة الضغوط المالية الغربية وأصدرت أكثر من ١٠٠ مليون بطاقة منذ إطلاقها في عام ٢٠١٥م، وذلك بعد عقوبات عام ٢٠١٤م إبان الحرب الروسية – الأوكرانية وضم شبه جزيرة القرم، وأدركت روسيا مخاطر الاعتماد على حلول أمريكية للدفع المالي في الاقتصاد الوطني، ولم يقتصر نشاط "مير" في السوق المحلية، بل توسعت خارجيًا، كجزء من

تطوير شبكة المدفوعات الأوروبية– الآسيوية المستقلة عن الحلول الأمريكية[1].

ومن غير المتوقع أن يصبح "مير" عالمي الانتشار بشكل أسرع إلا أنه يعبر عن تصاعد القوة الناعمة الروسية على حساب القوة الأمريكية، خاصة مع الجهود الصينية لإطلاق منظومتها المستقلة "أليباي" Alipay للدفع الإلكتروني، وبات توجه بناء نظم دفع وطنية لتوفير طرق آمنة للمدفوعات والإيرادات الحكومية، وحماية الحكومات من مخاطر تأثير العقوبات المالية، وضمان استقلال الشبكات الحيوية هو ما يمثل تهديدًا للهيمنة المالية والاقتصادية

---

(1) Tomaso Falchetta, Deborah Brown and Katitza Rodriguez, Opening Stages in UN Cybercrime Treaty Talks Reflect Human Rights Risks, justsecurity, April 18, 2022. https://bit.ly/3Ps1SzF

للولايات المتحدة، ومن ثم قدرتها على التأثير في سلوك تلك البلدان من خلال العقوبات التي تستهدف أنظمتها المصرفية [١].

٢- زيادة التحدي المالي للعملات المشفرة مع ضعف التنظيم:

حذر صندوق النقد الدولي من مخاطر العملات المشفرة على النظام المالي للدول وأن تعدين العملات المشفرة يمكن أن يوفر مسلكًا لدول، مثل روسيا وإيران، لتجاوز العقوبات، وإعادة توجيه الموارد الطبيعية التي لا تستطيع تصديرها نحو عمليات التعدين كثيفة الاستهلاك للطاقة، وفي عام ٢٠٢١م حقق تعدين «بتكوين»

---

(١) هاورد ديفيز، هل تغير العقوبات الغربية النظام المالي العالمي، (صحيفة الاقتصادية، ٤ مايو ٢٠٢٢م)، على الرابط:

https://bitly/39rTVKi

عائدات تقدر بنحو ١,٤ مليار دولار شهريًا، وذهب نحو ١١% منها إلى المُعدّنِينَ الروس[١].

وقد بلغت أرباح تداول العملات المشفرة عالميًا ١٣٦ مليار دولار في عام ٢٠٢١ بزيادة ١٣٠ مليار عن عام ٢٠٢٠م، وكانت أمريكا الأكثر تحقيقًا للأرباح بواقع ٤٧ مليار دولار، تلتها بريطانيا بفارق كبير، حيث بلغت أرباح متداولي العملات المشفرة هناك ٨,٢ مليار دولار، ثم جاءت ألمانيا بأرباح بلغت ٥,٨ مليار دولار[٢].

وقد استخدمت أوكرانيا العملات المشفرة في تلقي التبرعات من دول ومؤسسات عالمية، وبلغ حجم نشاط التشفير العالمي غير المشروع ١٤ مليار دولار في عام ٢٠٢١م، أي نحو ٠,٠١٥% من الناتج

([1]) 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

([٢]) كم بلغت أرباح مستثمري العملات المشفرة في ٢٠٢١م (صحيفة الشرق؛ ١٣ مايو ٢٠٢٢م).

المحلي الإجمالي العالمي، ومن شأن تلك العقوبات دفع المرمجين إلى الهروب إلى الملاذات الآمنة، مثل أمريكا الشمالية، خاصة مع القيود التي فرضتها الصين عام ٢٠٢١م، وتمثل خطوة لتحقيق مصالح للشركات الأمريكية، وتحتل روسيا المركز الثالث عالميًا في مجال العملات المشفرة، والتي تؤدى إلى نظام نقدي هش[١].

٣- جاذبية العملات المشفرة كوسيط للتهرب من العقوبات الدولية:

قدمت العملات المشفرة طريقة جذابة محتملة للتهرب من العقوبات، ويساعد في ذلك عدم التنسيق الجيد لإنفاذ القانون عبر الحدود الدولية، ومحدودية قدرة القانون على وقف تدفق العملات المشفرة غير المشروعة في جميع أنحاء العالم.

---

(١) "النقد الدولي" الأصول المشفرة يمكن استخدامها لنقل عائدات الصفقات المشبوهة، (اندبندنت عربية، ١١ أبريل ٢٠٢٢م)، على الرابط:
https://bit.ly/3wrqXSu

وقدر تقرير فريق الخبراء التابع للأمم المتحدة، الصادر في أغسطس ٢٠١٩م أن كوريا الشالية من خلال أنشطتها الإلكترونية في محاولة للتهرب من العقوبات الدولية، وحصلت على ١٧٠ مليون دولار على الأقل [١]، تم استخدامها في غسل الأموال والتهرب من العقوبات، وتحويل الأصول إلى عملات مشفرة.

ففي حالة تحويل (الروبل) إلى عملة مشفرة، يتم التعتيم بشكل أكبر على مصدر الأموال، أو عبر سوق الرموز غير القابلة للاستبدال سريعة النموه خاصة وأن البورصات غير ملزمة بتحديد هوية المستخدمين أو الإبلاغ عن النشاطات المشبوهة.

---

(١) في يوليو ٢٠٢١م حكم القضاء الأمريكي على "فيرجيل جريفت" وهو خبير عملات مشفرة بالسجن ٦ سنوات ونصف السنة، بعد صفقة الإقرار بالذنب، بتهمة تقديم معلومات تقنية عن الـ"بلوكتشين" إلى نظام الديكتاتور كيم جونغ أون عن طريق حضوره مؤتمر تم عقده هناك في عام ٢٠١٩م، إذ قال المدعون، إنه يمكن استخدامها لمساعدة البلاد في غسل الأموال والتهرب من العقوبات.

ويتم بعد ذلك تحويل العملات المشفرة إلى أموال مشروعة ودولارات في أي بورصة للتشفيرن وإيداعها سرًا في حساب منشأة تسيطر عليها الجهة أو الفرد الخاضع للعقوبات، وبلغ حجم تحويلات (الروبل) إلى عملات مشفرة ثابتة لأعلى مستوياته منذ عام ٢٠٢١م وفي ظل عدم كفاية قواعد مكافحة غسل الأموال وتمويل الإرهاب في مختلف البلدان، وصعوبة التحقيق في المعاملات غير المشروعة عندما تتدفق الأموال إلى الخارج[١].

٤- العقوبات السيبرانية على النشاط الروسي في العملات المشفرة:

فرضت وزارة الخزانة الأمريكية عقوبات على شركات تعدين العملات المشفرة، مثل شركة Compass Mining بسبب عملياتها في روسيا، وشركة (بتريفر) (Bit River) أحد أكبر مزودي

(١) ٦٠٠ مليون دولار من العملات المشفرة، والتي تمت سرقتها من خلال لعبة الفيديو Axie Infinity

خدمات مراكز البيانات في صناعة التشفير، بالإضافة إلى ١٠ شركات تابعة لها في روسيا[١].

وفي ٢٠ أبريل ٢٠٢٢م فرضت عقوبات أخرى على عشرات الأشخاص والكيانات الروسية لمواجهة التهرب من العقوبات الدولية، وأصدر مكتب مراقبة الأصول الأجنبية التابع لوزارة الخزانة الأمريكية عقوباته الأولى ضد بورصة العملات المشفرة، مستهدفة SUEX OTC بدعوى تسهيل مدفوعات الفدية للقراصنة، والتعاون بين وكالات إنفاذ القانون، وبورصات العملات المشفرة لتحسين القدرات للتعرف على العناوين المتعلقة بالجريمة وربطها بالأفراد ومن ثم تمكين السلطات بمصادرة الأموال المسروقة واعتقال المتورطين، حتى بعد سنوات من وقوع جرائم غسل الأموال [٢].

---

(١) عقوبات أمريكية على بنك روسي وشركة لتعدين العملات الرقمية، (صحيفة الشرق، ٢٠ أبريل ٢٠٢٢م).

(2) Kayla Izenman Sam Cousins, The Cyber – Crypto – Sanctions Nexus, ukfinance.org 4/2/2020. https://bit.ly/3NhWEnz

ومع تهديد تلك الكيانات ضمنيًا بفرض غرامات على عدم الإبلاغ عن تلك المعاملات، وأعلنت (Binance Holdings) وهي أكبر بورصة عالمية للعملات المشفرة من حيث حجم التداول وضع قيود على تقديم الخدمات للمواطنين الروس، أو الكيانات التي تتجاوز أصولها المشفرة قيمة ١٠ آلاف يورو، وجاء ذلك بعد موافقة الاتحاد الأوروبي في أبريل ٢٠٢٢م على حظر المعاملات المشفرة عالية القيمة مع روسيا في إطار العقوبات الشاملة.

٥- تأثيرات العقوبات في مستقبل النظام المالي العالمي:

كان للعقوبات السيبرانية تأثير كبير في النظام المالي العالمى والثقة فيه خاصة من جانب الدول التي على خلاف مع الولايات المتحدة، لاسيما مع هبوط حصة الدولار في احتياطيات النقد الأجنبي العالمية من ٧١% عام ٢٠٠٠م إلى أقل من ٦٠% عام ٢٠٢٢م، ومن ثم فإن العقوبات المالية ستؤثر في مستقبل النظام المالي العالمى على المدى البعيد ويأتي ذلك في ظل عدد من الاعتبارات، نرصدها على النحو التالي:

أ- سابقة التوظيف السياسى لنظام التحويلات المالية الدولي المعترف به (سويفت) SWIFT، ومنع تعامل البنوك الروسية معه في إدارة المعاملات الدولية، ومن المتوقع أن يدفع الخوف من (الحرمان من سويفت) إلى تطوير نظام خاص للدفع، يستخدم صيغة رسائل نظام سويفت لتقديم التسويات بالعملة الرقمية عبر الحدود بين أعضائه.

ب- تصاعد العملات الرقمية لدى البنوك المركزية التي تعتمدها الدول وتأثيرها في الحد من قدرة الولايات المتحدة على توظيف العقوبات المالية، خاصة في حالة تطوير الصين لـ اليوان الرقمي، وأثره في تدفقات التجارة العالمية.

ج- نمو اتجاه نظم الدفع الرقمية الوطنية لدى روسيا والصين؛ ففي ٢٣ يونيو ٢٠٢٢م وجه الرئيس الصينى انتقادات شديدة لتسليح النظام المال العالمي، وأعلن تعهده بتحقيق تقدم في مجال التكنولوجيا المالية في الصين، ودعى للانفصال عن الغرب ووضعت الحكومة سلسلة من إجراءات الدعم، وضوابط للقطاع التكنولوجي، وتحسين القوانين، وتقوية الروابط

المؤسسية الضعيفة، وضمان أمن عمليات الدفع والبنى التحتية المالية، والحماية من المخاطر المالية المحتملة [1].

د- عدم وجود معايير مشتركة لتنظيم العملات المشفرة للحد من تهرب الجهات المسئولة عن الانتهاكات، وقد أدركت الولايات المتحدة خطورة ذلك؛ ففي ٧ يوليو ٢٠٢٢م أعلنت وزارة الخزانة الأمريكية إنه يجب على الولايات المتحدة وحلفائها في الخارج وضع معايير مشتركة لتنظيم العملات المشفرة.

تحديات وفرص بناء نظام دولي للعقوبات السيبرانية:

تتيح قضية عدم وجود معاهدة دولية للفضاء السيبراني الفرصة أمام الدول للمناورة والتهرب من تحمل المسئولية عن سلوكها عبر الفضاء السيبراني، ولكن هذا لم يمنع من قيام الدول باتخاذ إجراءات تشريعية وتقنية لتوقيع العقوبات على الجرائم السيبرانية،

(1) تيم كولبان، الرئيس الصيني يدرك حاجته إلى التكنولوجيا المالية، (صحيفة الشرق الأوسط، ٨ يونيو ٢٠٢٢م)، على الرابط:

https://bit.ly/3nz0A9g

إلى جانب تبني الاتفاقيات الإقليمية، مثل اتفاقية بودابست للجرائم السيبرانية، وتطوير وتحديث التشريعات الوطنية.

يأتي هذا مع تحول الفضاء السيبراني لساحة للتفاعلات العابرة للحدود، وتمكين الدول من الوصول إلى المعلومات والاتصال عبر أراضي دول أخرى، وذلك في تجاوز للمفاهيم التقليدية حول السيادة الوطنية للدولة، وباتت تتعرض عناصر تحققهاء كالثروة والشعب والإقليم وعمل الحكومة، لمحددات جديدة، ومن ثم تحاول الدول منفردة الدفاع عن مصالحها القومية وما تراه ضمن اعتبارات الأمن القومي لديها.

وجاءت عملية وضع نظام للعقوبات السيبرانية The Cyber Sanctions Regime في شكل اتخاذ إجراءات أخرى مضادة من قبل طرف دولي أو أكثر، لتعزيز قدرته على إحداث تغيير في السلوك الدولي لدى طرف آخر تحت ضغوط الإكراه، والعزل، وتضمن الفاعلين من الدول القومية والفاعلين من غير الدول، مثل الأفراد أو الجماعات الإرهابية، أو الشركات التقنية أو مجموعات القرصنة الدولية.

وإذا كان نظام العقوبات السيبرانية، والذي يتم التوافق عليه من المجتمع الدولي لم يتشكل بعد إلا أن هناك محاولات لتطويره في ظل الاتفاقيات الدولية، خاصة تلك المعنية بالجرائم السيبرانية، وواجه ما تبنته دول الاتحاد الأوروبي والولايات المتحدة من وضع نظام للعقوبات السيبرانية مشكلات تقنية وعملية وتشريعية على الرغم من التباين فيما بينهم، وانعكس ذلك على قياس مدى فاعلية نظام العقوبات السيبرانية، الذي يجب أن يرتكز على تبني مجموعة من التدابير المضادة التي يتم فرضها لتغير السلوك لدى طرف آخر بما يتوافق مع مصلحة الدولة أو المجتمع الذي يفرضها، ومن جهة أخرى، القدرة على تقاسم الأعباء والمكاسب من جراء تطبيق هذا النظام بين مختلف الفاعلين، وأن تكون مخرجات هذا النظام من العقوبات القابلة للتنفيذ، وأن يحظى هذا النظام الاعتراف والشرعية من قبل المجتمع الدولي.

ويكون لذلك دور في الحد من التهديدات التي يقف من ورائها فاعل من الدولة أو من غير الدولة، وكلما استطاع هذا النظام معالجة القضايا والخلافات وتحقيق القرار والشرعية كان قادرًا على الاستمرار والاستدامة مع تطويره لنظام للمراجعة، وفي إطار

المبادئ العامة للحوكمة، ومواجهة السلوك العدواني عبر المجال السيبراني.

وتدفع طبيعة (التهديد السيبراني) العابر للحدود الدولية لأهمية التعاون الدولي في مواجهة الفجوة القانونية الدولية التي تتيح الفرصة للالتفاف حول أية عقوبات جراء التورط في الهجمات السيبرانية، ومن جهة أخرى دفع الحكومات إلى الانفتاح على التعاون مع القطاع الخاص وغيره من أصحاب المصلحة في الداخل لتحسين وجودة نمط الاستجابة، والتوصل إلى توافق عالمي حول التهديدات السيبرانية والوصول إلى حلول وسط وتفاهم مشترك بين اعتبار الهجمات السيبرانية أنشطة تجسسية أو تخريبية أكثر من كونها أعمال حرب، واعتبار الأنشطة السيبرانية تأتي في إطار التنافس التجاري بمعزل عن اعتبارها تهديدًا للأمن القومي، ومواجهة عدم الوضوح بشأن تأثير العقوبات السيبرانية في فرض أي تكاليف على الأفراد أو الكيانات الخاضعة للعقوبات ودرجة الارتباط بين فرضها على (الفاعل المهدد) وقدرتها على إحداث تغيير حقيقي في سلوك الأفراد أو الكيانات الخاضعين لها، أو دورها في ردع سلوك الدولة التي ينتمون لها، خاصة أن الدول قد

تلجأ إلى الاستعانة بمجموعات قراصنة عبر الحدود للقيام بأعمال عدوانية ضد الغير لمصلحتها، إلى جانب القدرة على إخفاء التمويل لتلك الأنشطة إما عبر طرق غير مباشرة للتمويل، أو عبر استخدام العملات المشفرة أو عبر استخدام حسابات لأشخاص غير خاضعة للعقوبات في تلقي التمويل.

ومن ثم تصبح هناك حالة من تقويض أهداف فرض العقوبات السيبرانية مع افتقاد القدرة على تغيير السلوك بالإكراه، وأن نجاح تطبيق نظام دولي للعقوبات السيبرانية يحتاج إلى اتفاقيات خاصة كاتفاقيات التعاون القضائي المسبق، وهو أمر قد لا يوجد بين دول ليست على علاقة طبيعية مع بعضها بعضًا، وتأثير ذلك في معدلات الثقة والأمن في الفضاء السيبراني، ومدى امتلاك ذلك النظام لاستراتيجية واضحة حول طبيعة السلوك الذي يتعرض للعقوبات، وطبيعة الإجراءات التي يتم فرضها في حالة خرقها، ووجود فهم مشترك بطبيعة المخاطر والتهديدات السيبرانية التي تمثل تهديدًا للأمن القومي.

كذلك طبيعة الأطر القانونية والتشريعية التي تعطي للسلطة التنفيذية المشروعية لفرض تلك العقوبات، وقدرة السلطة التنفيذية كوزارة الخزانة أو التجارة في تلبية الموارد الكافية لتنفيذ برامج العقوبات السيبرانية، أيضًا طبيعة الإجراءات المصاحبة لعملية فرض العقوبات السيبرانية بما فيها الضغوط الأخرى التي يكون من شأنها التأثير في إرادة الخصم أو المستهدف من وراء تلك العقوبات، ومدى الأخذ بعين الاعتبار تأثير فرض العقوبات السيبرانية في ظهور مخاطر أخرى جديدة، وقدرة النظام على تحديد المكافآت أو المكاسب لهؤلاء الملتزمين بعدم الإتيان بالسلوك العدواني عبر المجال السيبراني، وقدرة نظام العقوبات السيبرانية على اعتهاد منهج التعددية والشفافية والمحاسبة، وقدرة نظام العقوبات السيبرانية لقهم طبيعة التحديات في التطبيق، والقدرة على مراقبة وتقييم فاعلية نظام العقوبات، وتتطلب تنمية القدرات في مجال الأدلة الجنائية الرقمية توافر الدعم التقني وبناء القدرات وإقامة المختبرات والتعاون الدولي في نقل الخبرات، وهو أمر قد لا يتوافر لعدد من الدول بما يحول دون المساعدة الفاعلة في

التحقيقات السيبرانية وتوفير تعددية واستقلالية في توجيه الاتهامات، ومنع تحويل الأدلة من طبيعتها التقنية إلى التوظيف السياسي.

وبناء عليه يواجَه نظام العقوبات السيبرانية بالعديد من الانتقادات خاصة في ظل تأثيره في المجال السيبراني وارتباطه بالعديد من الخدمات المائية وصعوبة الفصل مع الأخرى ذات الطبيعة العسكرية، وتتوقف درجة التأثير والتأثر بالعقوبات السيبرانية على عدة عوامل لعل أهمها درجة اعتماد (المعاقب) الدولة على الاقتصاد العالمي، ومستوى تقدمها التقنى خاصة في مجال تطبيقات الفضاء السيبراني، وقدرتها على الصمود والمرونة أمام التعرض للهجمات السيبرانية، وإلى جانب القدرة على تبني مشروع وطني ممتد للنهضة العلمية والتقنية.

وترتبط عملية التعرض للعقوبات السيبرانية أو الإجراءات الانتقامية من جانب بعض الدول بمدى تورط دول أخرى في شن هجمات سبيرانية أو القيام بأنشطة تجسسية أو تهديد أمنها القومي ومصالحها الحيوية للخطر، ناهيك عن التدخل في الشئون الداخلية، سواء عبر التأثير في الرأي العام، أو في الثقة بين

المجتمع والدولة، أو عبر دعم المعارضة، أو عبر التأثير في العملية الانتخابية وطبيعة النظام السياسي.

وجاءت العقوبات السيبرانية لتعبر عن انتقال مستويات التوتر الدولي على المصالح المادية بين القوى الكبرى إلى المجال السيبراني وهو ما يفسر تصاعد عملية توجيه الاتهامات المتبادلة بين الشرق والغرب دون أدلة واضحة، أو من خلال تحقيق رقمي مستقل وهو الأمر الذي يظهر الدولة التي تعرضت للهجوم على أنها الخصم والحكم في الوقت نفسه، خاصة وأن تحديد المسئولية من قبل القانون الدولي عن الأعمال غير المشروعة تتطلب أن يتم

توصيف الهجمات السيبرانية على أنها هجوم مسلح، ومن جهة أخرى، لا يتم إعلان المسئولية عن هذه الهجمات، بما يجعل هناك صعوبة في توجيه الاتهامات بشكل قانوني، والتي يمكن أن تتم عبر تحديد أجهزة الكمبيوتر والشبكات المستخدمة في التهديدات من جهة، وربط العملية بالأفراد أو الفاعلين الذين يقفون وراءها من جهة أخرى.

وفي ظل غياب قانون دولي واضح يتعامل مع الأنشطة السيبرانية العدائية التي تقودها الدولة أو ترعاها؛ فإن ثمة حاجة ملحة لوضع معايير تحاول أن تعيد توصيف تلك التهديدات وتفسرها.

وعلى الرغم من كون العقوبات السيبرانية وسيلة لوضع المعايير المتعلقة بسلوك الدولة عبر المجال السيبراني، إلا أنها في تطبيقها كشفت عن تبني نمط انتقائي ومزدوج المعايير، وهو ما يدفع لأهمية بناء نظام للقواعد السيبرانية شامل وواضح، وإنشاء نظام للعقوبات السيبرانية يحظي بتوافق المجتمع الدولي، ودعم الجهود الحثيثة من قبل الأمم المتحدة في تبني اتفاقية دولية للجرائم السيبرانية، والتي يمكن أن توفر نظامًا دوليًا لتطبيق العقوبات.

الخاتمة:

مع تحول الفضاء الإلكتروني إلى ساحة للتفاعلات الدولية، برز العديد من الأنماط التوظيفية له، سواء على صعيد الاستخدامات ذات الطبيعة المدنية أو العسكرية ، الأمر الذي جعل هذا الفضاء مجالًا للصراعات المختلفةسواء للفاعلين من الدول أو غير الدول لحيازة أكبر قدر من النفوذ والتأثير السيبراني.

تبلورت ظاهرة الحروب السيبرانية التي اتسمت بخصائص مختلفة عن نظيراتها التقليدية من حيث طبيعة الأنشطة العدائية، والفواعل والتأثيرات في بنية الأمن العالمي، وعبرت تلك الحرب عن نمطين من القوة (الناعمة والصلبة) في عملية توظيف التفاعلات في الفضاء الإلكتروني، مما يعطس تنامي القدرات والتهديدات المتصاعدة لأمن البنية التحتية للمعلومات.

ولقد تحول الفضاء السيبراني إلى شبكة عالمية يمكن الوصول إليها من أي مكان، ومن أي شخص دون تمييز، وعلى أساس مبدأ حيادية الشبكة، وخاصة أن المجال السيبراني وتطبيقاته المختلفة يلعب دورًا حيويًا واستراتيجيًا وإنسانيًا، وأصبح المدنيون الذين

يعانون من صراعات دولية يعتمدون عليها، إما في جمع المعلومات وتوفير الحماية أو بالتعريف بمعاناتهم على النحو الذي يدفع إلى تدخل المجتمع الدولي.

بات فرض العقوبات السيبرانية يمثل تهديدًا للسكان الأبرياء والمنشآت المدنية، نا يُعد انتهاكًا للقواعد التي أرساها القانون الدولي الإنساني بشأن الأعمال الحربية وأهمية التمييز بين المدنيين والمنشآت المدنية في أثناء القتالن ويمثل انتهاكًا للقانون الدولي لحقوق الإنسان، خاصة فيما يتعلق بحرية الرأي والتعبير وحرية الاتصال وباقي حقوق الإنسان الرقمية والتي اعتبرت من قبل المجلس الدولي لحقوق الإنسان، رديفًا للحقوق في العالم المادي.

وعلى الرغم من الافتراض النظري لتأثير عملية فرض العقوبات السيبرانية في الحد من التهديدات السيبرانية، إلا أن واقع الحال يشير إلى أنها بعد نحو عقد من بدء سياسات العقوبات السيبرانية، لم تؤدِ بالضرورة إلى انخفاض وتيرة تلك التهديدات السيبرانية، بل إنها زادت من وتيرتها وخسائرها للاقتصاد الدولي، بما يزيد على مليار دولار سنويًا.

وعلى الرغم من أن توظيف العقوبات السيبرانية ساهم في تعزيز سياسات القوة الأحادية، إلا أنها مع مرور الوقت باتت تفقد قوتها في الردع، خاصة أنها تساعد من جهة أخرى في نمو القدرات السيبرانية الوطنية، وزيادة ممارسة الدولة لـ "السيادة السيبرانية"، ما من شأنه أن يساعد في تحويل تلك العقبات السيبرانية من تحدٍ إلى فرصة للتنمية الرقمية المستقلة لتلك البلدان.

ومن شأن التدابير المضادة خارج نطاق الأمم المتحدة أن تقوض من أهداف ومقاصد ميثاق الأمم المتحدة والتي تحض على حل الأزمات عبر الطرق الدبلوماسية، ومن ثم فإن التركيز على سلاح العقوبات كسبيل للضغط يزيد من التوتر الدولي، ويتيح الفرصة إلى الالتفاف عليها والحد من فاعليتها، ويضفي على عملية فرض العقوبات غطاء يمنع البحث عن الحلول الجذرية ومعالجة أسباب الأزمة من وجهة النظر لدى طرفي أو أطراف الصراع، والحد من التوافق في المصالح الدولية والحفاظ على الأمن والسلم الدوليين.

وعلى الرغم من إباحة القانون الدولي لفرض العقوبات الدولية، إلا أنه وضع شروطًا ترتبط بها، من أهمها إصدار قرار من مجلس

الأمن، ومن ثم فإن عملية فرض العقوبات السيبرانية تواجه كتصرف أحادي بفقدان المشروعية الدولية، وهو ما قد يدفع الدول المتضررة إلى المطالبة بالتعويضات واعتبار ذلك انتهاكًا للقانون والعرف الدولي.

من ثم فإن فشل العقوبات السيبرانية في تحقيق الردع ومنع تكرار السلوك من قبل الدول التي وقعت عليها اعقوبات بفقدها فاعليتها، ومن ثم تصبح وسيلة لزعزعة الأمن الدولي بدلًا من حمايته، وذلك لارتباط الفاعلية بطبيعة العقد الاجتماعي والسياسي الدولي، والتوافق على تقييم انتهاكات معايير وأسس بناء النظام الدولي للعقوبات السيبرانية، وبما يراعي المصالح الدولية، ومن ثم فإنه لا عقوبة إلا بنص، وعدم وجوده يجعل من عملية فرض تلك العقوبات غير شرعية.

قائمة المراجع:

أولًا– المراجع باللغة العربية:

١. إبان ما عرف بثورات الربيع العربي قامت العديد من الحكومات العربية بقطع الإنترنت؛ سعيًا للسيطرة على موجة الاحتجاجات عام ٢٠١١م لاعتبارات تتعلق بالأمن القومي.

٢. الإعلان العالمي لحقوق الإنسان، يمكن الوصول له عبر الرابط: https://bit.ly/3yGfeCh

٣. أنا سيغال، العقوبات الاقتصادية القيود القانونية والسياسية، (المجلة الدولية للصليب الأحمر، ع٨٣٦، ٣١ ديسمبر ١٩٩٩م) على الرابط: https://bit.ly/38yxsLd

٤. ايهاب خليفة، الكتائب الإلكترنية، الملامح العامة لحروب مواقع التواصل الاجتماعي في الشرق الأوسط، (اتجاهات الأحداث، مركز المستقبل للدراسات والأبحاث المتقدمة، مج١، ع٤، نوفمبر ٢٠١٤م).

٥. ايهاب خليفة، إمكانيات تحقيق الردع في صراعات الفضاء الإلكتروني، (اتجاهات الأحداث، ع١٣، ٢٠١٥م).

٦. إيهاب خليفة، تأثيرات قوة الفضاء الإلكتروني على التفاعلات الأمنية في العالم، (اتجاهات الأحداث، ع١، مج١، أغسطس ٢٠١٤م).

٧. تقرير: قطع الإنترنت المتعمد تسبب في خسائر ب ١٠ مليارات دولار في عام ٢٠٢٢م (صحيفة الشرق، ٧ يوليو ٢٠٢٢م) على الرابط: https://bit.ly/3AsI4YV

٨. تيم كولبان، الرئيس الصيني يدرك حاجته إلى التكنولوجيا المالية، (صحيفة الشرق الأوسط، ٨ يونيو ٢٠٢٢م)، على الرابط: https://bit.ly/3nz0A9g

٩. سليم دحماني، أثر التهديدات السيبرانية على الأمن القومي الولايات المتحدة الأمريكية- أنموذجًا (٢٠١٧-٢٠٢١)، (رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، ٢٠١٨م).

١٠. سماح عبد الصبور، الإرهاب الرقمي: استخدامات الجماعات المسلحة لوسائل التواصل الاجتماعي، (اتجاهات الأحداث، مج١، ع٢، سبتمبر ٢٠١٤م).

١١. عقوبات أمريكية على بنك روسي وشركة لتعدين العملات الرقمية، (صحيفة الشرق، ٢٠ أبريل ٢٠٢٢م).

١٢. القانون الدولى للبحار لعام ١٩٨٢م.

١٣. كم بلغت أرباح مستثمري العملات المشفرة في ٢٠٢١م (صحيفة الشرق؛ ١٣ مايو ٢٠٢٢م).

١٤.محمود محارب، إسرائيل والحرب الإلكترونية: قراءة في كتاب حرب الفضاء الإلكتروني– اتجاهات وتأثيرات على إسرائل، (المركز العربي للأبحاث ودراسة السياسات، الدوحة، أغسطس ٢٠١١م).

١٥.ميثاق الأمم المتحدة ١٩٤٥م.

١٦.النقد الدولي الأصول المشفرة يمكن استخدامها لنقل عائدات الصفقات المشبوهة، (اندبندنت عربية، ١١ أبريل ٢٠٢٢م)، على الرابط:
https://bit.ly/3wrqXSu

١٧.نوران شفيق، الفضاء الإلكتروني وأنماط التفاعلات الدولية: دراسة في أبعاد الأمن الإلكتروني، (رسالة ماجستير، جامعة القاهرة: كلية الاقتصاد والعلوم السياسية، ٢٠١٤).

١٨.نوران شفيق، حوكمة الإنترنت: أبعاد الصراع على إدارة الفضاء الإلكتروني، (مركز المستقبل للأبحاث والدراسات المتقدمة، يوليو ٢٠١٤م).

١٩.نيكوالس مولدر، سلاح العقوبات، (مجلة التمويل والتنمية، صندوق النقد الدولي، ع٥٩، ق٢، يونيو ٢٠٢٢م) ص٢٠. على الرابط:
File://c:/users/GR/Downloads/fd0622a.pdf

٢٠. هاورد ديفيز، هل تغير العقوبات الغربية النظام المالي العالمي، (صحيفة الاقتصادية، ٤ مايو ٢٠٢٢م)، على الرابط: https://bitly/39rTVKi

٢١. هجيرة تومي، فاعلية التدابير المضادة في ظل منظمة التجارة العالمية، (مجلة العلوم القانونية والسياسية، جامعة الشهيد، ع٩، يونيو ٢٠١٤م). https://www.asjp.Cerist.dz/en/downArticle/110/5/2/5838

٢٢. وليد غسان سعيد، دور الحرب الإلكترونية في الصراع العربي-الإسرائيلي، (رسالة ماجستير، جامعة النجاح الوطنية، كلية الدراسات العليا، ٢٠١٣)، ص٩٧.

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. https://bit.ly/3Ps1SzF
6. 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

7. 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
8. Jason Bartlett and Megan Ophel, Sanctions by the Numbers: Spotlight on Cyber SSantions, Center for a New American Security, May4, 2021.

https://www.cnas.org/publications/reports/sanctions-by-the-numbers-cyber

9. Jason Healey, The Five Futures of Cyber Conflict And Cooperation, Georgetown Journal of International Affairs, pp. 110-116.
10. 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.

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

12. Joseph Nye, Cyber Power, Belfer Center For Science And International Affairs, May 2010, pp. 11-13.

13. Kayla Izenman Sam Cousins, The Cyber – Crypto – Sanctions Nexus, ukfinance.org 4/2/2020. https://bit.ly/3NhWEnz

14. 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.

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

16. 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

17. 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

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

19. 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/wp-content/uploads/2016/06/10_dictators_digital_network.pdf

20. Steffen Westerburger, Cyber Conflict In The 21st Century The Future of War And Security Ib A Digitalizing World, Master Thesis International Relations, Radboud School of Mangement Radboud University, December 2014, pp. 10-12.

21. 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/

22. The International Télécommunication Union ،**ITU Toolkit for CybercrimeLégislation,** Geneva, 2010, P. 12.

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

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

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.