مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الاقتصادية والقانونية المجلد (١٠) العدد (٢) ٢٠٢٦
Tartous University Journal for Research and Scientific Studies -Economic and Legal Sciences Series Vol. (10) No. (2) 2026

تداعيات القرصنة الالكترونية على العلاقات الدولية: "القرصنة الروسية في الانتخابات الأميركية أنموذجاً"

رشا مالك سليمانو*

(تاريخ الإيداع ١٦/١٠/ ٢٠٢٥ – تاريخ النشر ٩/٢/ ٢٠٢٦)

□ ملخّص □

يعد الفضاء الالكتروني بيئة ديناميكية تلعب دوراً جوهرياً في العلاقات الدولية، وتتصف هذه البيئة بسمات عدة أهمها الافتراضية، العالمية، الاتصال المباشر، اللامركزية والتفاعلية، وعدم القدرة من التحقق من الهوية بشكل مباشر والتنوع الكبير وغيرها من السمات الأخرى، هذا بدوره يجعل الفضاء الالكتروني عالماً معقداً وغنياً بالإمكانيات والفرص، ولكنه في ذات الوقت يحاط بكثير من التحديات، فضلاً عن أن تعدد الفواعل الموجودة به من شأنها التأثير في العلاقات الدولية سواء من حكومات ودول ومنظمات دولية حكومية وغير حكومية وشركات ومؤسسات عالمية وجماعات غير حكومية، وأبرز مثال على ذلك تأثر العلاقات الأميركية الروسية السياسية والعسكرية والأمنية بعملية القرصنة الالكترونية التي نفذتها روسيا عندما اخترقت حواسيب اللجنة الوطنية التابعة للحزب الديمقراطي الأميركي بقصد التلاعب بنتائج الانتخاب الرئاسية عام ٢٠١٦، وقد هدف البحث إلى عدة أهداف أهمها تحديد تداعيات القرصنة الروسية على سير عملية الانتخابات الأميركية، وقد تم الاستناد إلى المنهج الوصفي التحليلي والمنهج التاريخي، وتم التوصل إلى نتائج عدة كان أبرزها أن الهجوم على البنية المعلوماتية للدول الأخرى يشكل جزءاً هاماً من استراتيجية حرب المعلومات الروسية، باعتباره وسيلة للحد من فعالية الخصم، ناهيك عن فعالية عمليات القرصنة في تجزئة نظام القيادة لدى القوى المناوئة لموسكو، والسيطرة عليها حتى ولو بعد فترة زمنية محددة، ومن أبرز ما أوصى به البحث وجوب التعاون بين الدول فيما بينها بشأن ملاحقة مقترفي الجرائم الالكترونية وتسليمهم للعدالة نظراً لاتساع نطاق أثر تلك الجرائم كونها عابرة للحدود، فضلاً عن توقيع أشد العقوبات الجزائية بحق مرتكبيها.

الكلمات المفتاحية: الجرائم الكترونية، القرصنة الكترونية، العلاقات الدولية.

* باحثة، حاصلة على ماجستير في العلاقات الدولية، كلية الاقتصاد، جامعة اللاذقية، اللاذقية، سورية، مكان إجراء البحث: اللاذقية.
rasha.sulemano@latakia-univ.edu.sy

مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الاقتصادية والقانونية المجلد (١٠) العدد (٢) ٢٠٢٦
Tartous University Journal for Research and Scientific Studies -Economic and Legal Sciences Series Vol. (10) No. (2) 2026

The repercussions of electronic piracy on international relations: "Russian hacking in the American elections as an example"

Rasha Malek Sulemano*

(Received 16/10/2025.Accepted 9/2/2026)

□ABSTRACT □

Cyberspace is a dynamic environment that plays a fundamental role in international relations، This environment is characterized by several features, the most important of which are virtuality, globality, direct communication, decentralization and interactivity, the inability to verify identity directly, great diversity, and other features. This in turn makes cyberspace a complex world rich in possibilities and opportunities, but at the same time it is surrounded by many challenges, In addition, the multiplicity of actors present in it can influence international relations, whether from governments, states, international governmental and non-governmental organizations, companies, international institutions, and non-governmental groups. The most prominent example of this is the impact of US-Russian political, military and security relations by the electronic hacking operation carried out by Russia when it penetrated the computers of the National Committee of the US Democratic Party with the intention of tampering with the results of the 2016 presidential election.

The research aimed to achieve several goals, the most important of which was to determine the repercussions of Russian hacking on the conduct of the American election process. The descriptive analytical method and the historical method were relied upon, and several results were reached, the most prominent of which was that the attack on the information infrastructure of other countries constitutes an important part of the Russian information war strategy. Among the most prominent recommendations of the research is the necessity of cooperation between countries with regard to prosecuting the perpetrators of electronic crimes and bringing them to justice, given the wide scope of the impact of these crimes as they cross borders, in addition to imposing the most severe criminal penalties against their perpetrators.

Keywords: cybercrime, electronic piracy, international relations.

---

* Researcher, holds a Master's degree in International Relations, Faculty of Economics, University of Lattakia, Lattakia, Syria. rasha.sulemano@latakia-univ.edu.sy

مقدمة:

بات للفضاء السيبراني الافتراضي دوراً كبيراً في حركة التفاعلات والتحولات البنيوية، حيث أصبح مجالاً مستقلاً في العلاقات الدولية ينتقل أثره من تغييرات هيكلية وتحتية إلى تغييرات كلية في النظام الدولي، ونتيجة لذلك يشهد العالم اليوم تطورات كبيرة في المخاطر الأمنية، ونظراً لتعدد الخدمات العامة المتاحة عبر هذا الفضاء وتنوع العمليات الالكترونية التي تتم بواسطته كأثر يترتب على الثورة التقنية هذا بدوره شكل ظواهر جديدة ليست بالمرغوبة تدور في فلك شبكات الانترنت، مما يعني رواج تلك العمليات التي ترتب عليها تداعيات سلبية كثيرة تجسدت في مسمى "الجرائم المستحدثة التي تقترف عن طريق النظم والأدوات التكنولوجية"، ويتجسد الخوف من هذه الجرائم بأنها سريعة الانتشار كونها عابرة للحدود الدولية ولا تتمركز في حدود دولة أو مجتمع محدد فقط، ويزداد الوضع خطورة عندما ترتبط بأهداف أطراف خارجية تسعى بشكل غير مباشر إلى خلق أزمات وصعوبات جديدة ليست بالحسبان للدولة المستهدفة، لاسيما فيما يتعلق بالقدرة على اكتشاف تلك الجرائم وبيان مسألة إثباتها، وعليه لابد من تحليل هذه الظاهرة ودراستها وبيان أشكالها والصعوبات التي ترتبها حيال الدولة المستهدفة، كما أننا نسعى إلى تحديد تداعيات جرم القرصنة الالكترونية على العلاقات الدولية سواء من الناحية القانونية أو الاقتصادية أو السياسية أو الأمنية، مع بيان موقف القانون الدولي من تلك الجرائم وكيفية الحد منها، وعلى وجه الخصوص بيان موقفه من القرصنة الروسية لنتائج الانتخابات الأميركية بقصد التلاعب بها.

الدراسات السابقة:

أولاً: الدراسات العربية:

تمت مراجعة الدراسات الأقرب إلى الدراسة الحالية، ونبين فيما يأتي أهمها:

١. هدفت دراسة (شيماء، علوان، ٢٠٢٤، الصعوبات القانونية في مكافحة الجريمة) إلى تحديد الإطار النظري للجرائم المعلوماتية مع توضيح دور التشريعات في كيفية الحد منها وتحديد الصعوبات التشريعية والإجرائية التي تواجه المشرعين وكيفية تفاديها، استخدمت الدراسة المنهج التحليلي لاستعراض القواعد القانونية ذات الصلة بالموضوع، والمنهج المقارن لإجراء مقارنة بتلك القواعد في التشريع المقارن، ومن أبرز النتائج التي توصلت إليها الدراسة هي أن المصالح الواجب حمايتها في إطار التجريم الالكتروني هي حماية حق السرية وحرمة الحياة الخاصة وحماية حق الملكية الالكترونية والفكرية.

٢. كما هدفت دراسة (خنوسي، كريمة، ٢٠٢١، الحماية الدولية من جرائم التقليد والقرصنة الالكترونية وموقف المشرع الجزائري منها) إلى تعريف الجريمة الالكترونية وبيان الجهود الدولية المبذولة في سبيل مكافحتها وبيان التشريع الجزائري من ذلك، واتبعت الدراسة المنهج الوصفي لوصف الجانب النظري للجرائم الالكترونية والمنهج المقارن لإجراء مقارنة بين موقف التشريع الدولي والتشريع الوطني منها وكيفية الحد من انتشارها، ومن أبرز نتائجها وجوب تعديل التشريعات الوطنية تماشياً مع الاتفاقيات الدولية.

٣. هدفت دراسة (د شلوش، نورة، ٢٠١٨، القرصنة الالكترونية في الفضاء السيبراني "التهديد المتصاعد لأمن الدول") إلى التعرف على الآليات التي يمكن تفعيلها من قبل الأنظمة الدولية لتجسيد الأمن السيبراني الدولي، ومعرفة علاقة القرصنة الالكترونية بإحداث تغييرات في البيئة الأمنية السيبرانية بصفة عامة، واستخدمت الدراسة المنهج الوصفي التحليلي لوصف تلك الآليات والتغييرات التي تحدثها القرصنة الالكترونية في الساحة الدولية،

وقد توصلت الدراسة إلى جملة من النتائج كان أبرزها أن الهجمات الالكترونية أصبحت تهديداً حقيقياً لاقتصاديات الدول، ولم تعد هذه الجرائم تقتصر على سرقة أموال البنوك أو الأفراد، بل اجتاحت قطاعات جديدة.

٤. كما هدفت دراسة (مهني، شرف الدين، ٢٠١٨، استخدام القرصنة الالكترونية في السياسة الروسية "بين التجريم الدولي وحتمية التخابر")، إلى دراسة موقف القانون الدولي من القرصنة الالكترونية الروسية، واستخدمت الدراسة المنهج التاريخي لدراسة الأطوار السابقة للظاهرة المعنية والمنهج الوصفي التحليلي لوصف هذه الظاهرة وتحليلها، والمنهج القانوني ومنهج تحليل المضمون للاطلاع على الوثائق القانونية والتشريعية، ومن النتائج التي توصلت إليها هي إطلاق الفضاء الالكتروني سباقاً للتسلح السيبراني بين الدول وخاصة الدول الكبرى يتم فيها استخدام وحدات هجوم سيبرانية نظامية أو غير نظامية وتطوير استراتيجيات للدفاع والردع والرد السيبراني.

ثانياً: الدراسات الأجنبية:

1.(V.A. Oganyan, M.V. Vinogradova, D.V. Volkov, Internet Piracy and Vulnerability of Digital Content, Article published in Journal of European Research Studies Volume Twenty-One, Issue 4, 2018).

هدفت الدراسة إلى تحديد طرق دراسة سلوك شبكة المستخدمين فيما يتعلق بالمنتجات الرقمية، وكذلك استخدام التقنيات الحديثة لضمان حماية حقوق النشر على الإنترنت، أضف إلى الكشف عن مشكلة ثغرة المحتوى الرقمي المرتبطة بمزايا مستخدمي الانترنت، وقد استخدم البحث مجموعة من الأساليب العلمية العامة والأساليب العلمية الخاصة للمعرفة العلمية، وأما بالنسبة للبحث في الصكوك التنظيمية، تم استخدام الطريقة القانونية الرسمية وطريقة تفسير القانون، التي تعتبر ضرورية لصياغة التعريفات واستنباطها من وجهة نظر القانون، كما أتاحت هذه الأساليب الوصول إلى الوضع القانوني للمحتوى الرقمي ونظام حماية حقوق النشر على الإنترنت في الاتحاد الروسي، ومن أبرز النتائج إن استخدام التقنيات المبتكرة التي تجعل من الممكن الوصول إلى طريقة تخزين البيانات إلى مستوى جديد ولا سيما نظام blockchain، والذي يمكن تطبيق مبادئه بنجاح على حماية حقوق الطبع والنشر على الانترنت.

٢.(Michael N. Schmitt, Foreign Cyber Interference in Elections, Article published in Journal of International law studies, Volume 97,2021).

هدفت الدراسة إلى بيان مشروعية التدخل الدولي في شؤون الدول الأخرى بواسطة الوسائل السيبرانية وفقاً لأحكام القانون الدولي، واستخدم البحث المنهج الوصفي التحليلي، ومن أبرز النتائج التي توصل إليها الباحث هو عدم قانونية الأنشطة المقترفة عبر الفضاء السيبراني بسبب مخالفتها لمبدأ عدم التدخل في الشؤون الداخلية للدول الأخرى.

تعقيب على الدراسات السابقة:

تتفق الدراسة الحالية مع الدراسات السابقة في أنها تتناول الإطار النظري للقرصنة الالكترونية وتحديد الصعوبات التي تواجهها الدول في ظل التحول الرقمي، بينما تركز دراستنا هذه على القرصنة الروسية للانتخابات الرئاسية الأميركية عام٢٠١٦، وبيان مدى تأثيرها على العلاقات الروسية الأميركية السياسية والاقتصادية وغيرها.

فرضيات البحث:

تتمثل فرضيات البحث في فرضيتين اثنتين هما:

الفرضية الأولى– إن سرعة انتشار جرائم القرصنة الالكترونية وعدم القدرة على ملاحقة فاعليها نظراً لكونه من الجرائم العابرة للحدود من جهة، وضعف أحكام القانون الدولي في هذا الصدد من جهة أخرى يجعل مبدأ الحفاظ على السلم والأمن الدوليين عرضة للانتهاك بشكل أكبر.

الفرضية الثانية– للقرصنة الالكترونية تداعيات سلبية جسيمة على العلاقات الدولية الاقتصادية والسياسية والثقافية والعسكرية وغيرها.

أهمية البحث وأهدافه:

تتمثل أهمية البحث في بيان مدى أهمية الفضاء الالكتروني وإيضاح مدى خطورة العمليات المحدثة من خلاله، خاصة مع كثرة التفاعلات الدولية في هذا المجال، هذا بدوره جعل منه بيئة غير آمنة حاضنة لأفعال وأنشطة غير سلمية مقترفة من قبل الدول وغيرها من الأشخاص الدولية، كان أبرزها عملية القرصنة الالكترونية.

أما الأهداف التي يسعى إليها البحث تتمثل في:

- تحديد الإطار المفاهيمي للهجمات الالكترونية بصفة عامة وجرم القرصنة الالكترونية على وجه الخصوص.
- تحديد تداعيات القرصنة الالكترونية على البيئة الأمنية السيبرانية الدولية من جهة، وبيان مدى تأثير القرصنة الروسية على سير عملية الانتخابات الأميركية.
- بيان مدى تأثير القرصنة الروسية لحواسيب اللجنة الوطنية التابعة للحزب الديمقراطي الأميركي على استقرار العلاقات الدولية.
- تحديد الإجراءات التي اتخذها القانون الدولي في سبيل مكافحة جرم القرصنة الالكترونية والحد من انتشارها السريع.

مشكلة البحث:

باتت العلاقة بين التطور التكنولوجي والأمن الدولي والعلاقات الدولية علاقة طردية، فكلما تطورت التقنيات التكنولوجية كلما ازدادت إمكانية تعرض المصالح الاستراتيجية ذات الطبيعة الالكترونية والعلاقات الدولية إلى أخطار الكترونية ومنها خطر القرصنة الالكترونية الذي يمثل الخطر الأكبر لأمن الدولة، وخاصة أن الفضاء الالكتروني أصبح مصدراً لأدوات جديدة من الصراعات والتوترات الدولية متعددة الأطراف، وبناء على ما تقدم نطرح التساؤل الرئيسي:

ما تداعيات القرصنة الالكترونية الروسية على أمن الولايات المتحدة الأميركية؟ وما مدى تأثير ذلك على استقرار علاقاتها الدولية؟

ويتفرع عن التساؤل الرئيسي عدة تساؤلات فرعية كان أهمها:

- ما أبرز أنواع الهجمات الالكترونية؟ وما أثرها في ظهور أنواع جديدة للصراعات الدولية؟
- هل يمكن أن يؤدي التنافس بين الدول للحصول على النفوذ وفرض الهيمنة على الشكل الجديد للقوة "القوة الالكترونية" إلى اللجوء لطرق غير قانونية ومنها قرصنة المعلومات للدول الأخرى في سبيل الحصول على مكانة دولية رفيعة بين الدول؟

- ما تأثير القرصنة الروسية لحواسيب اللجنة الوطنية التابعة للحزب الديمقراطي الأميركي على الانتخابات الرئاسية الأميركية عام ٢٠١٦؟
- ما تداعيات التهديدات الالكترونية على العلاقات الروسية الأميركية؟
- ما موقف القانون الدولي من جرم القرصنة الالكترونية؟ وهل كانت الأحكام المنصوص عليها كفيلة للحد من هذا الجرم؟

حدود البحث:

· الحدود **الزمنية** للدراسة: بدأت عام ٢٠١٦ منذ وقوع جرم القرصنة الالكترونية من قبل روسيا لحواسيب اللجنة الوطنية التابعة للحزب الديمقراطي الأميركي للتلاعب بالنتائج الانتخابية، وتنتهي عام ٢٠١٩ وذلك لدراسة تأثيرات هذا الجرم على العلاقات الروسية الأميركية خلال هذه الفترة وقبل البدء بمرحلة الانتخابات الأخرى.

· الحدود **المكانية** يشمل النطاق المكاني لكل من روسيا والولايات المتحدة الأميركية.

منهج البحث:

تم الاستناد في هذا البحث إلى المنهج الوصفي التحليلي، حيث تم وصف الإطار المفاهيمي للقرصنة الالكترونية بغرض الوصول إلى تحليل أثر هذا الجرم على العلاقات الدولية عموماً، والعلاقات الروسية الأميركية على وجه الخصوص، كما تم الاستناد إلى المنهج التاريخي لدراسة الأطوار والحالات السابقة لظاهرة التهديدات الالكترونية، أضف إلى عرض النصوص القانونية والقرارات والمعاهدات الدولية المتعلقة بالهجمات الالكترونية وتحليلها للتوصل إلى موقف القانون الدولي من هذه الجرائم وكيفية ضبطه لها.

مصطلحات البحث:

· **الجرائم الالكترونية:** كل استخدام في صورة فعل أو امتناع غير مشروع للتقنية المعلوماتية، يهدف إلى التعدي على مصلحة مشروعة سواء أكانت تلك المصلحة مادية أم معنوية (كريز، ٢٠١٨، ص ١٢١).

· **القرصنة الالكترونية:** اختراق غير مصرح به لأنظمة الحاسوب أو الشبكات أو البيانات، بهدف سرقة المعلومات، أو تعطيل الخدمات، أو النسخ غير المشروع للمحتوى الرقمي، أو الوصول غير المصرح به لأغراض مالية أو سياسية أو انتقامية، مما يتجاوز الحدود الجغرافية للدولة (الصغير،٢٠٠١، ص٧٢و٧٣).

· **العلاقات الدولية:** مجموعة من العلاقات السياسية الاقتصادية الإيديولوجية، الدبلوماسية والاجتماعية، القانونية والعسكرية فيما بين الدول أو القوى السياسية، أو المنظمات، كما تشمل الحركات التي تتفاعل في المجتمع الدولي (فرج،٢٠٠٧، ص٤).

النتائج والتوصيات

المراجع

أولاً: الإطار النظري للقرصنة الالكترونية:

يشهد المجتمع الدولي في الفترة الراهنة نوعاً جديداً من سباق التسلح، يختلف عن أنواع الأسلحة التقليدية وغير التقليدية، ويقوم هذا السباق على استحداث أو تطوير برامج الكترونية معدة لأغراض عسكرية أو سياسية أو أمنية(شهاب، ٢٠٠٧، ص٣)، وتعد جرائم القرصنة الالكترونية نموذجاً جديداً للقوة يختلف عن مفهوم القوة التقليدية وعليه نعرف هذا الجرم ونحدد خصائصه:

١:١ تعريف القرصنة عبر الانترنت:

عندما نسمع كلمة "قرصنة" فإننا نتخيل عصابات سرقة السفن البحرية والسطو عليها، ونهب ما فيها وحجز طاقهما، وهذا المعنى ذاته ينطبق على القرصنة الالكترونية ولكن بطرق أكثر حداثة دون أي يعرض قرصان النظم الالكترونية نفسه لأي خطر (علوان، ٢٠٢٤، ص٣٦٥).

وعليه تعرف "القرصنة الالكترونية" بأنها عملية اختراق للأجهزة الحاسوبية عبر شبكة الانترنت، لأن أغلب الحواسيب في العالم ترتبط عبر هذه الشبكة، أو حتى عبر شبكات داخلية يرتبط فيها أكثر من جهاز حاسوب (د خنوسي، ٢٠٢١، ص٦٩و٧٠)، ويقوم بهذه العملية شخص محترف أو أكثر في مجال برامج الحاسوب وطرق إدارتها، حيث يقوم هؤلاء المبرمجون بواسطة برامج مساعدة واستناداً إلى خبرتهم باختراق حواسب معينة والتعرف على محتوياتها، ومن خلال ذلك يتم اختراق بقية الأجهزة المرتبطة معها في نفس الشبكة (بن يونس، ٢٠٠٤، ص ٤٥).

١:٢ خصائص القرصنة:

يعتمد الفضاء الالكتروني كمجال افتراضي على نظم الكمبيوتر وشبكات الانترنت ومخزون هائل من البيانات والمعلومات، وبالتالي ما يميز الجرم الذي يقترف في هذا الوسط بجملة من الخصائص تتمثل في:

· إن تنفيذ الجريمة الالكترونية لا يتطلب الكثير من الوقت، لكن هذا لا ينفي الحاجة إلى الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة، كما أن ربط العالم كله بشبكة من الاتصالات وذلك من خلال الانترنت والفضائيات والأقمار الصناعية جعل انتشار الجرائم في هذا المجال أمراً شائعاً جداً، لا يعترف بالحدود الجغرافية والإقليمية للدول ولا بالحدود الزمانية، ففي مجتمع المعلومات تلغى كافة أنواع الحدود بين الدول (عبد الصادق،٢٠٢٠، ص٣٦و٣٧).

· يمكن لمقترف الجريمة الالكترونية تنفيذ جريمته وهو بعيد كل البعد عن المستهدف بالجرم وذلك من خلال الدخول للشبكة المعنية أو اعتراض عملية تحويل مالية أو سرقة معلومات سرية أو تخريب أحد الأجهزة الحاسوبية التابعة للدولة المستهدفة (عياد، ٢٠٠٧، ص ٧٨) ، ويترتب على هذه الخاصية صعوبة متابعتها وإثباتها نظراً لافتقادها لوجود الآثار التقليدية للجريمة وغياب الأدلة الفيزيقية (بصمات، تخريب، أدلة مادية وما إلى هنالك) من جهة، وسهولة محو الأدلة وتدميرها في زمن قصير من جهة أخرى (شهاب، مرجع سابق، ص٢).

· تصنف الجرائم الالكترونية ضمن بند الجرائم الناعمة نظراً لعدم تطلبها أي عنف عند تنفيذها (علوان، ٢٠٢٤، ص٣٣٦)، ولكن بالمقابل تتطلب الجرائم التقليدية استخدام العنف والقوة لتنفيذها على أرض الواقع ودخولها الحيز المادي مثل جرائم الإرهاب والمخدرات وغيرها، فعلى سبيل المثال جرم نقل بيانات من حاسوب إلى آخر أو عملية السطو الالكتروني أو القرصنة الالكترونية لا يتطلب تنفيذ استخدام أي عنف أو تبادل إطلاق نار مع رجال الشرطة على خلاف الجرائم التقليدية (الصغير، مرجع سابق، ص ٧٢).

· تتصف جرائم الانترنت بالغموض، نظراً لصعوبة تحديد هوية الكيان الذي نفذ الهجمات السيبرانية في حالات كثيرة بسبب عولمة هذه الجرائم التي تؤدي إلى تشتيت الجهود الدولية في التحري لتعقبها، وتعد هذه الجرائم هي صورة

حقيقية من صور العولمة(جوزيف، ١٩٩٧،ص ٨٢)، كما أنه من حيث المكان يمكن ارتكاب الجرائم عن بعد وقد يتعدد هذا المكان بين عدة دول، ومن الناحية الزمنية تختلف المواقيت بين الدول الأمر الذي يطرح إشكالية جديدة وهي تحديد القانون الواجب التطبيق على الجريمة المقترفة، وبيان دور القانون الدولي في ملاحقة الفاعل وخاصة في ظل غياب التشريعات الدولية التي تضع الدول أو المؤسسات التي تقوم بمثل هذه الهجمات تحت طائلة المسؤولية الدولية، مما يعني عدم القدرة على ملاحقتها قانونياً على خلاف مجالات الجرائم التقليدية(جوزيف، ١٩٩٧،ص ٨٢).

ثانياً: نشأة القرصنة الالكترونية

بدأت ظاهرة القرصنة عبر الانترنت مع بداية ظهور الحاسبة الالكترونية، ولقد ازدادت بشكل كبير مع استخدام تقنية الشبكات، حيث شملت هذه الظاهرة كثير من الهجمات الالكترونية من قبل مبرمجين ذوي مستوى عال على النظم الحاسوبية لاختراقها وسرقة بياناتها، وعليه وبسبب عمليات القرصنة التي تتطور بسرعة فائقة باستخدام تقنيات حديثة ومعقدة-(V.A Oganyan, M.V. Vinogradova, D.V. Volkov,2018,p 739 74، اختلفت النظرة إلى هذه الجريمة مقارنة بالمراحل السابقة، (شرف الدين، ٢٠١٨/٢٠١٧، ص١و٢) وفي سياق الحديث لا بد من مراعاة التفرقة بين الجرائم الالكترونية التي يقترفها الأفراد بهدف السرقة وبين تلك التي تقترفها الدول بهدف التجسس على الدول الأخرى والحصول على معلومات واستثمارها في آليات الصراع المعلنة وغير المعلنة بهدف فرض سيطرتها والحصول على نفوذ دولي قوي:

- جريمة القرصنة الالكترونية المقترفة من قبل الأفراد:

تعد جريمة قرصنة الأفراد جريمة معلوماتية تقليدية ذات طابع شخصي أو جنائي مالي، وغالباً ما تقترف بهدف تحقيق مكاسب شخصية كالسرقة بهدف الحصول على مال أو التحايل على هيئات ومؤسسات مصرفية مما يجعلها خارجة عن نطاق تطبيق أحكام القانون الدولي، أو بهدف ابتزاز شخص ما أو إلحاق الأذى به باستخدام أدوات محدودة ومتاحة غالباً كالتصيد الاحتيالي أو برامج الفدية (Ransomware) أو القيام باختراق الحسابات الشخصية أو البنكية الخاصة بهم، كما أن حجم الضرر يكون أضيق نطاقاً فلا يشمل إلا الأشخاص المستهدفين، وتعد ملاحقة هذه الجريمة أكثر سهولة تبعاً لقوانين الجرائم الالكترونية المحلية والدولية أيضاً ومن أبرز الأمثلة على ذلك في عام ١٩٨٦ قام شخص يدعى "روبيرتو سوتو" كولومبي الجنسية بسرقة خط تيليكس حكومي، ليرسل مجموعة من الرسائل عبره إلى مصارف في المملكة المتحدة، ومنها إلى دولة أخرى، وترتب على إثر القيام بالتراسل مع تلك المصارف نقل ١٣.٥ مليون دولار من أرصدة الحكومة الكولومبية (شرف الدين، مرجع سابق، ص١و٢)، كما قام أحد طلاب جامعة كورل عام ١٩٨٨ بزراعة برنامج Wormفي شبكة حواسيب حكومية انتشر خلالها في ٦٠٠٠ حاسوب، وبعد أن تم كشفه طرد الطالب من الجامعة، وحكم عليه بإيقافه من عمله لمدة ثلاث سنوات، وغرم بمبلغ ١٠ آلاف دولار (شرف الدين، مرجع سابق، ص ١و٢).

وفي عام ١٩٩٤ قام مجموعة من القراصنة الروس بنقل مبلغ ١٠ ملايين دولار من City Bank إلى حسابات مصرفية

وفي العام التالي تعرضت حواسيب وزارة الدفاع الأميركية إلى ٢٥٠ ألف هجمة، كما تعرضت المواقع الفيدرالية للتشويه، واخترقت أيضاً مجموعة من القراصنة في عام ٢٠٠١ الموقع الالكتروني لشركة مايكروسوفت للبرمجيات، وعلى الرغم من أن المشكلة تم حلها في ساعات قليلة، إلا أن الملايين لم يتمكنوا من تصفح الموقع

لمدين يومين، وفي عام ٢٠٠٧ قام قرصان تركي يدعى كريم بالهجوم على موقع منظمة الأمم المتحدة عبر شبكة الانترنت، وفي عام ٢٠١٦ حاول الجيش الالكتروني الكوري سرقة مليار دولار من الاحتياطي الفيدرالي بولاية نيويورك في الولايات المتحدة الأميركية، وفي شهر ماي من عام ٢٠١٧ نفذت الجواسيس السيبرانية الكورية الخاصة بالرئيس "كيم جونغ أون" عمليات ضد آلاف الأجهزة الحاسوبية في عدة دول وجمدوا شبكة الصحة البريطانية لمدة ساعات باستخدام فيروس الفدية "Ransom Ware" واناكراي"WannaCry" (شرف الدين، مرجع سابق، ص ١و٢).

- وأما جريمة القرصنة الالكترونية المقترفة من قبل الدول:

تعد جريمة قرصنة الدول أداة صراع حديثة بيد الدول الكبرى حيث تسخر أجهزتها الاستخباراتية لارتكاب تلك الجرائم لتهدد الاستقرار الدولي، ومن أبرز أهدافها التجسس على الدول الأخرى والحصول على معلومات واستثمارها في آليات الصراع المعلنة وغير المعلنة بهدف فرض هيمنتها ونفوذها على العالم والتأثير على أمنها القومي وعلى علاقاتها الدولية أو تدمير البنى التحتية لها لأهداف سياسية أو عسكرية كالطرقات وموارد الطاقة والكهرباء وغير ذلك، أو التأثير على مجريات الأحداث الدولية كالتأثير على العمليات الانتخابية الجارية لدولة ما لتحقيق مآربها المرادة من وراء ذلك، ويجب الإشارة إلى أن الإمكانيات المتوفرة للدول في اقتراف جرمها تفوق إمكانيات الأفراد في اقترافهم للجرم المعني، حيث تقوم الدول بحشد وتمويل جيوش الكترونية تمتلك أسلحة سيبرانية متخصصة ومتطورة جداً، إلا أن التحدي الأكبر الذي يواجه الدول في صدد هذه الجرائم صعوبة إثبات الجرم على الدولة المقترفة ومعرفة من الفاعل بالضبط ناهيك عن صعوبة ملاحقته وبالتالي يعني صعوبة تطبيق أحكام القانون الدولي.

ومن أبرز الأمثلة على جرم قرصنة الدول اختراق روسيا لمواقع وأنظمة حكومية تابعة للولايات المتحدة الأميركية وذلك لقرصنة انتخاباتها الرئاسية لعام ٢٠١٦ والتلاعب بها وذلك لتحقيق أهداف سياسية كان أبرزها تسهيل وصول مرشحها "دونالد ترامب" إلى البيت الأبيض، وزعزعة أركان الديمقراطية الأميركية وإحداث حالة من الفوضى السياسية تثير الشكوك في مدى تماسك النظام السياسي في الولايات المتحدة الأميركية (Michael N. Schmitt,2018,p .742)

ثالثاً: تداعيات القرصنة الالكترونية الروسية في الانتخابات الرئاسية الأميركية:

في ضوء مفهوم الدولة الحديثة ودون إطلاق أية رصاصة أصبح أمر السيطرة على المعلومات وقرصنتها قادراً على إعاقة الدول الكبرى، وعلى الرغم من تعدد الأغراض التي تسعى إليها تلك الهجمات الالكترونية، ثمة هناك هجمات تسعى إلى زعزعة الوضع الاقتصادي للدولة المستهدفة، أو حتى سرقة بنوكها وحساباتها المصرفية لإضعاف موقفها في الساحة الدولية، بينما ثمة هجمات الكترونية أخرى تسعى إلى تدمير البنى التحتية لتلك الدولة، كل هذه المخاطر دفعت بالدول في سبيل تلافيها والتخلص منها إلى تطوير قدراتها المادية والتقنية لمواكبة التطورات العالمية استعداداً لمواجهة التهديدات الخطيرة، كما انصبت الجهود الدولية والإقليمية من أجل خلق آليات قانونية للحماية من تلك المخاطر وبرزت في هذا الصدد العديد من المنظمات الدولية والإقليمية سعياً منها في حماية الدول، فعلى سبيل المثال عقد مؤتمر القمة العالمي المعني بمجتمع المعلومات في جنيف عام ٢٠٠٣، ومن ثم في تونس عام ٢٠٠٥، كان من أبرز نتائج هذا المؤتمر وجوب تطوير مجتمع المعلومات في كافة البلدان ووضع الأطر اللازمة لتحقيق تلك الأهداف، بالإضافة إلى اتفاقية مجلس أوروبا بشأن الجريمة الالكترونية "اتفاقية بودابست" التي عقدت في عام ٢٠٠١ ودخلت حيز النفاذ في عام ٢٠٠٤ كان الهدف من وضعها تحديد الجرائم الالكترونية وتعيين التشريعات الخاصة بها وإنشاء القدرات والجهات المختصة للتحقيق في أشكالها وتعزيز التعاون في هذا المجال، كما قام مجموعة من الخبراء

بإعداد قانون نموذجي في عام ٢٠٠٢ مستوحى من اتفاقية بودابست وغير ذلك من الاتفاقيات التي تعد من آليات الحماية القانونية، فضلاً عن امتلاك تلك الدول لبرمجيات آمنة وخالية من الثغرات(كريمة، وجمال، ٢٠١٨، ص٣٥).

ومن خلال ما تقدم نستكشف الاختلاف بين مفهوم الحرب الالكترونية عن الحرب التقليدية، حيث تنطوي هذه الأخيرة على استخدام جيوش نظامية مع إعلان مسبق لبدء الحرب ووجود ساحة معركة محددة، بينما تفتقد الأولى لوجود جيش أو ساحة محددة لها أو حتى مجرد إعلان لها، فهي حرب غامضة من كافة النواحي وأهدافها غير واضحة أثناء تحركها عبر الشبكة المعلوماتية، وعليه نعرض مثال عملي من أرض الواقع عن هذا الجرم، مع بيان أثره على أمن الدولة المستهدفة واستقرارها (كريمة، مرجع سابق، ص٣٥و٣٦).

٣:١ آلية تنفيذ جرم القرصنة الالكترونية الروسية:

قامت روسيا باختراق مواقع وأنظمة حكومية تابعة للولايات المتحدة الأميركية وذلك لقرصنة انتخاباتها الرئاسية لعام ٢٠١٦، وقد أكدت هذه الأخيرة ذلك من خلال تقاريرها المقدمة، والتي تقضي بتنفيذ روسيا جريمتها وذلك من خلال اختراق خوادم Server حواسيب اللجنة الوطنية للحزب الديمقراطي الأميركي، وذلك بهدف تسهيل وصول مرشحها "دونالد ترامب" إلى البيت الأبيض، وزعزعة أركان الديمقراطية الأميركية وإحداث حالة من الفوضى السياسية تثير الشكوك في مدى تماسك النظام السياسي في الولايات المتحدة الأميركية، وكانت ردة فعل الرئيس الأميركي باراك أوباما آنذاك حيث قام بطرد ٣٥ دبلوماسياً من الجنسية الروسية قبل مغادرته للبيت الأبيض(Michael N. Schmitt,2018,p 742) .

وحسب بعض التقارير التي نشرتها صحيفة "نيويورك تايمز" أكد بعض المسؤولين في الاستخبارات الأميركية أن تحرك القراصنة الروس في نظم حواسيب الحزب الديمقراطي استمر لعدة أشهر وقد استهدف عدة مسؤولين في الحزب ومنها هيلاري كلينتون، واعتبرت هذه الأفعال أفعال غير قانونية وقد أدرجتها لجنة الأمم المتحدة في فئة الجرائم التي من شأنها تهديد الأمن والسلم الدوليين (شرف الدين، مرجع سابق، ص ١)، وحسب التحقيق الجاري بصدد الجرم المقترف اتضح أن روسيا استخدمت طريقتين اثنتين لتنفيذ الجرم فأما الطريقة الأولى اختراق البريد الالكتروني للحزب الديمقراطي وعلى وجه الخصوص المرشحة السابقة هيلاري كلينتون وأعضاء حملتها وكان أشهر تسريب رسائل مدير حملتها جون بوديستا، وأما الطريقة الثانية كانت عن طريق اختراق شبكات الحواسيب وتثبيت البرامج الضارة التي سمحت لهم بالتجسس على المستخدمين، والتقاط نقرات المفاتيح والصور وسرقة الملفات(ينظر الموقع التالي: https://www.aljazeera.net/، تاريخ الزيارة ٢٢-١١-٢٠٢٥، الساعة ٧:٣٣ مساء)

ويتضح من خلال ذلك أن دوافع روسيا من وراء التسريبات هو شن حرب الكترونية ضد الولايات المتحدة الأميركية، بهدف إحداث تغييرات سياسية في الأسباب الحاكمة بها، خاصة في ظل التحولات العميقة الجارية في مفهوم القوة وتوظيفاتها، خاصة لم تعد القوة تنحصر بامتلاك القدرات العسكرية والاقتصادية، بل في توظيف الإمكانيات المتاحة وفق استراتيجية فعالة لتحقيق الأهداف المرجوة، كما وضحت صحيفة أخرى "وول ستريت" أن وزارة العدل الأميركية جمعت أدلة كافية لمقاضاة ستة من أعضاء الحكومة الروسية الذين تورطوا في اختراق اللجنة الوطنية للحزب الديمقراطي "DNC" قبل الانتخابات الرئاسية لعام ٢٠١٦، لكنها استبعدت بدورها أحكام الاعتقال والسجن، وذكرت صحيفة Le Quotidien تعاون كل من الوكلاء الفيدراليين والمدعين

العامين من واشنطن وفيلادلفيا وبيترسبرغ وسان فرانسيسكو في التحقيق بالقضية لرفعها إلى المحكمة في العام التالي للانتخابات، ولكن تحديد المسؤولين عن القرصنة، يجعل سفرهم إلى الخارج أكثر تعقيداً، وهذا يتنافى مع ما أكدت عليه الصحيفة سابقاً وهو استبعاد الاعتقال أو حكم السجن حيال المتورطين بجرم القرصنة(البابلي، ٢٠١٨، ص ٤٤و٤٥).

٣:٢ الموقف الأميركي حيال الجرم المقترف

لقد أثار تسريب الوثائق التي تدين مرشحة الحزب الديمقراطي "هيلاري كلينتون" من أجل إحراج حملتها الانتخابية وتعزيز فرص نجاح "دونالد ترامب" غضب الكثير من الديمقراطيين، كما دفع رئيس الحزب الديمقراطي الأميركي "ديبي ويسرمان شولتز" إلى تقديم استقالتها، وهو الأمر الذي أجج الصراع بين داعمي السيناتور "بيرني ساندرز" "وهيلاري كلينتون"، وقد تسبب اختراق البريد الالكتروني لمرشحة الرئاسة عن الحزب الديمقراطي "هيلاري كلينتون" في كشف الديناميات الداخلية لحملتها خلال فترة السباق الرئاسي أمام الجمهوري "دونالد ترامب"، وعليه اعتبر "أوباما" أن الاختراق الروسي للجنة الديمقراطية يمثل تدخلاً دولياً واضحاً في العملية الانتخابية وفق ما أوردته صحيفة "ذا هيل" الأميركية"(مهني، ٢٠١٨، ص٣٩)، وفي سبتمبر وجه الرئيس "باراك أوباما" لنظيره الروسي "فلاديمير بوتن" تحذيراً من محاولة التلاعب في الانتخابات الأميركية، عقبه فرض عقوبات من جانب إدارته على وكالتي استخبارات، وأربعة مسؤولين، وثلاث شركات في روسيا(د شلاش،٢٠١٨، ص ١٨٨و١٨٩)، أضف إلى طرد ٣٥ دبلوماسياً روسياً وعائلاتهم من البلاد، في الوقت الذي يزعم فيه بعض المسؤولين صلتهم بهجمات القرصنة الأخيرة، وبحسب "نيويورك تايم" أغلقت وزارة الخارجية الأميركية اثنين من المرافق المستخدمة من جانب الاستخبارات الروسية في مدينة نيويورك بولاية ماريلاند (مهني، مرجع سابق، ص٤٠).

كما وجه "أوباما" نداء لتشكيل نوع من الوحدة الدولية لإعادة موسكو إلى الطريق الصحيح وإلا تتخذ إجراءات ضدها من شأنها زعزعة استقرارها، ومن جهة أخرى فرضت الولايات المتحدة الأميركية عقوبات اقتصادية على جهازي الأمن الفيدرالي "إف اس بي" واستخبارات الجيش "جي آر يو" الروسيين وعلى أربعة مسؤولين به من بينهم رئيس الاستخبارات الرئيسية "إيغور كوروبوف"، وأكد "أوباما" أن هذه التدابير جاءت كردة فعل على المضايقات غير المقبولة التي يتعرض لها الدبلوماسيون الأميركيون في موسكو من قبل الشرطة أو أجهزة الاستخبارات الروسية(مهني، ، مرجع سابق، ص٤١).

وقد أصدرت وزارة الأمن الداخلي الأميركية بياناً هاماً تمثل في أول اتهام مباشر توجهه إدارة أوباما ضد روسيا بأنها تسعى للتدخل في الانتخابات الأميركية، ومن أبرز ما جاء في البيان:(إن الأجهزة الاستخباراتية في الولايات المتحدة الأميركية واثقة كل الثقة أن الحكومة الروسية قد أمرت مؤخراً بكشف رسائل الكترونية لمواطنين ومؤسسات أميركية من ضمنها تلك القادمة من منظمات سياسية أميركية، وذلك بغاية التأثير على النتائج الانتخابية (يراجع التقرير الأميركي بشأن التدخل الروسي بالانتخابات المنشور على الموقع التاليhttps://www.aljazeera.net/encyclopedia، تاريخ الزيارة ٢٢-١١-٢٠٢٥، الساعة ٧:٤١مساء).

٣:٣: أثر القرصنة على العلاقات الروسية الأميركية

إن تحول الاقتصاد العالمي من مرحلة الاقتصاد التقليدي إلى مرحلة الاقتصاد الرقمي زاد احتمالية اقتراف جرائم الكترونية، حيث أن التصاعد المستمر لخطورة الجرائم الالكترونية زاد من حجم الخسائر التي يتكبدها العالم، ولكن الخطر الحقيقي يتجلى في أن السبب الرئيس لزيادة عدد الجرائم الالكترونية المقترفة من قبل الدول الكبرى هو سبب سياسي إما بقصد إضعاف قوة الدول المستهدفة وبسط نفوذها على العالم، وحسب التقديرات تشير إلى أن الاقتصاد

العالمي المستند إلى الانترنت يولد سنوياً نحو ثلاثة تريليونات دولار قابلة للزيادة، وتطال الجريمة الالكترونية نسبة عالية بين ١٥ و٢٠ في المئة من حجم الاقتصاد العالمي(http://www.alhadath.ps/article/34 870)، وحسب المنتدى العالمي الاقتصادي فإن ممارسات التزوير والقرصنة قد كلفت حوالي ١.٧٧ تريليونات دولار في عام ٢٠١٥ ما يمثل قرابة ١٠% من التجارة العالمية(فهيم، ٢٠١٥، بحث منشور على الموقع التالي: http://site.alroeya.ae/2015/11/16/292547).

وعليه باتت التهديدات الالكترونية تشكل مصدر قلق كبير في مجال العلاقات الدولية، فمثلاً العلاقة بين الولايات المتحدة الأميركية وروسيا تأثرت سلباً بسبب قرصنة روسيا لانتخاباتها عام ٢٠١٦، حيث انخرط كل منهما في شبكة معقدة من الهجمات الالكترونية والتجسس وحملات التضليل المعلوماتية التي أدت بدورها إلى توتر علاقاتهما الدبلوماسية (كامل،٢٠٢٤، ص٢و٣)، كما أصدر البيت الأبيض بتاريخ ٢٩ ديسمبر عام ٢٠١٦ قراراً يقضي بطرد ٣٥ دبلوماسياً روسياً من العاملين في السفارة في واشنطن والقنصلية في سان فرنسيسكو، وتم تبرير هذا القرار بأنه جاء رداً على ملاحقة أجهزة الأمن والشرطة للدبلوماسيين الأميركيين في روسيا، وقد فرض الرئيس الأسبق أوباما عقوبات ضد روسيا بسبب تدخلها في انتخاباتها الرئاسية، حيث شملت العقوبات جهازين تابعين للاستخبارات الروسية، وأربعة ضباط من المخابرات العسكرية الروسية، وثلاث شركات قدمت الدعم المادي للعمليات السيبرانية التابعة للمخابرات العسكرية الروسية.

والأمر الذي زاد حدة الصراع بين الدولتين، حين قامت موسكو بتخفيض عدد الدبلوماسيين الأميركيين كرد أولي على عقوبات واشنطن ضد روسيا، وطالبت وزارة الخارجية الروسية، الجانب الأميركي بتقليص عدد الدبلوماسيين على الأراضي الروسية إلى ٤٥٥ شخصاً، بحيث يغدو مماثلاً لعدد الدبلوماسيين الروس العاملين على الأراضي الأميركية، ولم يقف الأمر إلى حد التوتر العميق في علاقاتهما الدبلوماسية، مما عقد الجهود الرامية إلى تعزيز التعاون والحوار بينهما، أضف إلى أن هذه القضية استحوذت على اهتمامهما مما شكل لديهما حافزاً للتنافس على السيادة في الفضاء السيبراني(باسم، ٢٠٢١،.ص٣٦)، كما أنه في عام ٢٠١٨ وبعد اتهام بريطانيا لروسيا بشن هجمات سيبرانية ضدها من جهة، أضف إلى أن التوتر التجاري بين كل من الصين والولايات المتحدة الأميركية من جهة أخرى أدى إلى تصاعد الاتهامات حيث قامت الصين بالتجسس على الرئيس الأميركي "ترامب"، ومن ناحية أخرى عززت العقوبات الأميركية المفروضة على روسيا والصين من التقارب في الرؤى في مجال الفضاء السيبراني، وإثر ذلك تزايدت حدة الهجمات السيبرانية بين الدول الثلاث ضد بعضهم البعض، فخلال الفترة الممتدة بين ٢٠٠٩– ٢٠١٩ تم تنفيذ ٧٩ هجوماً سيبرانياً من قبل مهاجمين ترعاهم الصين استهدفت ٢٠ دولة، وكانت نسبة ٣٢% من تلك الهجمات موجهة ضد الولايات المتحدة الأميركية، وفي ذات الوقت استهدفت روسيا ١٩ دولة كان الهدف الأول لها الولايات المتحدة الأميركية أيضاً.

وعليه نستنتج وفي ضوء الاستجابة لتلك التهديدات وفي ظل التضارب بالمصالح أصبح الغرب بقيادة الولايات المتحدة الأميركية، والشرق بقيادة الصين وروسيا اللذان يتصارعان حول كيفية تشكيل قواعد ومبادئ دولية تنظم التعامل مع التهديدات المحتملة في الفضاء الالكتروني(فتح الله، ٢٠١٩، ص٤٥)، والأمر الذي زاد من حدة التوتر في الساحة الدولية هو تحول روسيا والصين من سياسة العزلة إلى سياسة الانخراط، ومحاولة خلق تكتل قوي يقابل التكتل الذي تقوده الولايات المتحدة الأميركية كل هذا بدوره يؤثر سلباً على الأمن السيبراني نتيجة اختلاف الاستراتيجيات والمبادئ المتبعة في هذا الصدد(كامل، مرجع سابق، ص ٢و٣).

رابعاً: موقف القانون الدولي من جرم القرصنة عبر الانترنت

إن المعاهدة الوحيدة المتعلقة بقضايا الأمن السيبراني الموجودة بالفعل هي "اتفاقية مجلس أوروبا بشأن الجرائم الالكترونية" والمعروفة أيضاً باسم "اتفاقية بودابست للضمانات الأمنية"، وقد وقعت في ٥ ديسمبر عام ١٩٩٤ في بودابست، وتندرج هذه الاتفاقية ضمن قائمة الاتفاقيات الإقليمية الرئيسة التي تتمتع بإمكانية قبول عالمي(خنوسي، مرجع سابق، ص ٦٠و٦١)، وقد تم اعتمادها من قبل ٣٩ دولة بما فيها الولايات المتحدة الأميركية، بينما امتنعت روسيا عن التصديق على المعاهدة باعتباره انتهاكاً لسيادتها، وهذا ما فتح المجال أمامها للتهرب من المسؤولية الدولية المترتبة عليها حيال اقترافها عدة هجمات الكترونية ضد الولايات المتحدة الأميركية وغيرها من الدول ولاسيما قيامها بقرصنة النتائج الانتخابية الأميركية والتلاعب بها عام ٢٠١٦، وأما بالنسبة للآليات المتبعة في مجموعة الدول الثمانيةG8 في سبيل مكافحة الجرائم الالكترونية فقد اعتمد وزراء العدل والداخلية التابعين للدول المعنية في اجتماعاتهم المختلفة مجموعة من السياسات التي تضم جملة من المبادئ في سبيل الحد من الهجمات السيبرانية والتي تتمثل في:

عدم السماح لمقترفي الجرائم الالكترونية بالفرار من البلاد، والعمل على التنسيق بين كافة الدول حول مسألة ملاحقتهم ومحاكمتهم بصرف النظر عن مكان وقوع الضرر، وإخضاع الموظفين المكلفين بتنفيذ القوانين لدورات تدريبية، والقيام بتجهيزهم بمعدات ضرورية للتعامل مع الجرائم ذات التقنية العالية (ناصر، ٢٠١٨، ص ١٠٨)، كما دأبت الدول الثمانية في سبيل وضع اتفاقيات دولية في هذا الصدد والعمل على وضع خطط عمل بشأن الجرائم الالكترونية عام ١٩٩٧، ومبادئ تتعلق بكيفية الحصول على المعلومات المخزنة على الحاسوب خارج حدود الدول لعام ١٩٩٩، كما أعلنت بياناً يتضمن نظام حماية المعلومات (د خنوسي، مرجع سابق، ص ٦٢).

أما موقف الأمم المتحدة من الجرائم الالكترونية فقد عملت منذ وقت طويل في مجال تأمين سلامة استخدام التكنولوجيا والشبكات المعلوماتية عبر مشاركة وكالاتها في مختلف المفاوضات لإيجاد معايير توفر الحماية لشبكة الانترنت، ومن أهم القرارات التي أصدرتها الجمعية العامة للأمم المتحدة في هذا المجال (د خنوسي، مرجع سابق، ص٦٤-٦٥):

- القرار ١٢١/٤٥ عام ١٩٩٠ والذي تضمن دليل منع الجرائم المتصلة بأجهزة الكمبيوتر ومكافحتها عام ١٩٩٤.
- القرارات ٧٠/٥٣ عام ١٩٩٨، ٤٩/٥٤ عام ١٩٩٩، ٢٨/٥٥ عام ٢٠٠٠، ١٩/٥٦ عام ٢٠٠١، ٥٣/٥٧ عام ٢٠٠٢، ٣٢/٥٨ عام ٢٠٠٣ تضمنت موضوع التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي.
- القرارات ٦٣/٥٥ عام ٢٠٠٠، ١٢١/٥٦ عام ٢٠٠١ بشأن مكافحة استخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات.
- القرارات ٢٣٩/٥٧ عام ٢٠٠٢، ٢٣٩/٥٧ عام ٢٠٠٣، و١٩٩/٥٨ عام ٢٠٠٤ الذي يتضمن إنشاء ثقافة عالمية للأمن السيبراني.

أما بالنسبة للقرارات الصادرة عن الأجهزة الأخرى التابعة للأمم المتحدة (د خنوسي، مرجع سابق، ص٦٤-٦٥)، (ناصر، مرجع سابق، ص ١٠٨):

- قرار لجنة مكافحة المخدرات ٨/٤٣ عام ٢٠٠٠ عبر الانترنت، وقرارها رقم ٥/٤٨ الذي ينص على منع استخدام شبكة الانترنت لارتكاب الجرائم المتصلة بالمخدرات.

· قرارات المجلس الاقتصادي والاجتماعي ٤٢/ ٢٠٠٤ بشأن بيع المخدرات المشروعة الخاضعة للمراقبة الدولية إلى الأفراد عن طريق الانترنت.

القرار E/٢٠٠/٢٠ عام ٢٠٠٧ ينص على تعزيز التعاون الدولي في سبيل تحري جرائم الاحتيال الاقتصادية والجرائم المتصلة بالهوية.

وبناء على ما تقدم نجد أن القانون الدولي يفتقر لمعاهدات وقوانين دولية تجرم القرصنة الالكترونية وتحرم استخدام الفضاء السيبراني كبيئة للجرائم نظراً لتأثيرها الكبير على العلاقات الدولية والأمن والسلم الدوليين، لذلك لا بد من صدور قوانين دولية ملزمة لكافة الدول والعمل على تكاتف الجهود الدولية لاتخاذ تدابير فعالة للحد من تلك الجرائم والقضاء عليها ومعاقبة مرتكبيها.

خاتمة:

أصبح الفضاء الالكتروني والحروب التي تتم من خلاله حقيقة واقعية لا مفر منها، وتعتبر هذه الحروب من الجيل الخامس، ويرى الكثير من الاختصاصيين أن هذا النوع هو نهاية الحروب في المستقبل، حيث أصبحت الرقمية هي الصيغة السائدة في عصرنا الحالي وكل شيء يتعامل به عبر الفضاء السيبراني من حكومات ونقود وأمن سيبراني وسيادة سيبرانية ودبلوماسية سيبرانية، وعليه يتوجب على الدول والأفراد أخذ الحيطة والحذر عند استخدام البيانات والمعلومات في المجال الافتراضي، لتجنب الوقوع في مخاطر القرصنة الالكترونية والتصيد عبر الشبكة، ناهيك عن ضرورة التعاون الدولي في مجال النظم القضائية وتبادل الخبرات والمعارف في مجال مكافحة هذه الهجمات.

النتائج والتوصيات:

النتائج:

١. بات الأمن الالكتروني عنصراً رئيساً في السياسة الأمنية الوطنية للدول، وخاصة لدى الدول صناع القرار كالولايات المتحدة الأميركية وروسيا والصين وغيرها.

٢. إن الاستخدام غير السلمي للفضاء الالكتروني من خلال هجمات القرصنة التي تحدث فيه تجعل منه بيئة غير آمنة خاصة مع توجه الدول إلى تبني الإدارة الالكترونية في إدارة شؤونها العامة.

٣. باتت التهديدات الالكترونية تشكل مصدر قلق كبير في مجال العلاقات الدولية السياسية والاقتصادية وغيرها، وخاصة بين الولايات المتحدة الأميركية وروسيا، حيث انخرط كل منهما في شبكة معقدة من الهجمات الالكترونية والتجسس وحملات التضليل المعلوماتية التي أدت بدورها إلى توتر علاقاتهما الدبلوماسية.

٤. يشكل الهجوم على البنية المعلوماتية للدول الأخرى جزءاً هاماً من استراتيجية حرب المعلومات الروسية، باعتباره وسيلة للحد من فعالية الخصم، ناهيك عن فعالية عمليات القرصنة في تجزئة نظام القيادة لدى القوى المناوئة لموسكو، والسيطرة عليها حتى ولو بعد فترة زمنية محددة.

التوصيات:

١. يجب على المشرع الدولي العمل على تطوير أحكام القانون الدولي ولاسيما في صدد المجال التكنولوجي الذي بات فضاء واسعاً لاقتراف الجرائم بصورها الحديثة، على أن يكون التطوير شاملاً للقواعد الموضوعية والشكلية في القانون حتى لا يكون هناك أية ثغرة تقف في وجه ملاحقة مقترف الجريمة الالكترونية أينما كان وبصرف النظر عن صفته.

٢. يجب على الدول التعاون فيما بينها بشأن ملاحقة مقترفي الجرائم الالكترونية وتسليمهم للعدالة نظراً لاتساع نطاق أثر تلك الجرائم كونها عابرة للحدود، فضلاً عن توقيع أشد العقوبات الجزائية بحق مرتكبيها، ناهيك عن نشر التوعية القانونية والتدريب الفعال لمنع اقترافها كإجراء وقائي.

٣. العمل على تحديث الأساليب المتبعة في قسم الأمن السيبراني الدولي لملاحقة مقترفي الجرائم الالكترونية وحماية البنى التحتية للدول كافة من أي تهديد محتمل، أضف إلى وجوب تفعيل التعاون الدولي بين المنظمات الدولية سواء أكانت حكومية أو غيرها، ناهيك عن تحديث المعاهدات الدولية حتى تواكب الأفعال غير المشروعة المقترفة عبر الانترنت وتعمل على تجريمها.

المراجع:

أولاً: المراجع العربية:

أ. صراع، كريمة، ودقيش جمال، *الأبعاد الاقتصادية للجريمة الالكترونية*، مقالة منشورة في مجلة الدراسات التسويقية وإدارة الأعمال، المجلد٢، العدد١، جانفي، ٢٠١٨.

أنور، فرج،٢٠٠٧، *نظرية الواقعية في العلاقات الدولية "دراسة نقدية مقارنة في ضوء النظريات المعاصرة"*، مركز كردستان للدراسات الاستراتيجية، ط١.

التقرير الأميركي بشأن التدخل الروسي بالانتخابات المنشور على الموقع التاليhttps://www.aljazeera.net/encyclopedia، تاريخ الزيارة ٢٢-١١-٢٠٢٥، الساعة ٧:٤١مساء).

تقي عثمان مصطفى كامل،٢٠٢٤، *التهديدات السيبرانية والعلاقات الأميركية الروسية*، بحث منشور في المركز العربي الديمقراطي. يوجد على الموقع: https://democraticac.de/?p=99583

جبران خليل، ناصر، ٢٠١٨، *حماية الملكية الفكرية: حقوق المؤلف في ظل التشريعات الوطنية والاتفاقيات الدولية*، أطروحة دكتوراه في علم المكتبات والعلوم الثقافية، كلية العلوم الإنسانية والعلوم الإسلامية، الجزائر، جامعة وهران١، أحمد بن بلة.

جميل عبد الباقي، الصغير،٢٠٠١، *الجوانب الإجرائية للجرائم المتعلقة بالانترنت*، دار النهضة العربية.

جورج، فهيم، *الجريمة الالكترونية تكبد الاقتصاد العالمي تريليون دولار سنوياً*، دبي ١٦، نوفمبر، ٢٠١٥، http://site.alroeya.ae/2015/11/16/292547 consulte le 25/05/2017

حسين، باسم، *تطور الحروب الحديثة وحرب ما بعد الحداثة، مجلة العلوم السياسية*، ع٦١، ٢٠٢١، https://jcopolicy.uobaghdad.edu.iq/index.php/jcopolicy/article/view/559/437، تاريخ الوصول: ٢٠٢٥/٩/٢٧، الساعة ١:١٤ مساء.

د كريمة، خنوسي،٢٠٢١، الحماية *الدولية من جرائم التقليد والقرصنة الالكترونية وموقف المشرع الجزائري منها* ، مقالة منشورة في مجلة مصداقية، المجلد٣، العدد٣.

د نور، شلاش، ٢٠١٨، *القرصنة الالكترونية في الفضاء السيبراني "التهديد المتصاعد لأمن الدول"*، مقالة منشورة في مجلة مركز بابل للدراسات الإنسانية، المجلد ٨، العدد٢

سامي، عياد، ٢٠٠٧، *الجريمة المعلوماتية وجرائم الانترنت*، الإسكندرية، دار الفكر الجامعي.

شيماء، علوان،٢٠٢٤، *الصعوبات القانونية في مكافحة الجريمة الالكترونية*، مقالة منشورة في مجلة العلوم الإنسانية والطبيعية، المجلد٥.

صباح، كريز،٢٠١٨، أثر الجرائم الالكترونية على أمن واستقرار الدول، قرصنة الموقع الالكتروني لوكالة الأنباء القطرية أنموذجاً، مقالة منشورة في مجلة الناقد للدراسات السياسية.

عادل، عبد الصادق، ٢٠١٧، الفضاء الالكتروني والعلاقات الدولية: دراسة بين النظرية والتطبيق، الهيئة المصرية العامة للكتاب، القاهرة.

عادل، عبد الصادق،٢٠٢٠، *الاقتصاد الرقمي وتحديات السيادة السيبرانية*، المركز العربي لأبحاث الفضاء الالكتروني، القاهرة.

عمار، البابلي،٢٠١٨، *الآليات الحديثة لحماية وتأمين نظم المعلومات وآثارها على المنظومة الأمنية*، رسالة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، القاهرة.

عمر، بن يونس، *الجرائم الناشئة عن استخدام الانترنت الجوانب الموضوعية والإجرائية*، القاهرة، دار النهضة العربية،٢٠٠٤.

محمود إبراهيم عبد الرحمن شهاب،٢٠٠٧، *الأسلحة غير التقليدية في الفقه الإسلامي*، رسالة ماجستير، الجامعة الإسلامية، كلية الشريعة والقانون، غزة، فلسطين.

محمود، فتح الله، ٢٠١٩، *الوسيط في الجرائم المعلوماتية*، الطبعة الأولى، دار الجامعة الجديدة، الإسكندرية، مصر.

مليار دولار خسائر الاقتصاد العالمي ينظر الموقع: http://www.alhadath.ps/article/34 870.

مهني، شرف الدين،٢٠١٧/٢٠١٨، *استخدام القرصنة الالكترونية في السياسة الروسية بين التجريم الدولي وحتمية التخابر*، رسالة ماجستير، جامعة قاصدي مرباح–ورقلة.

ناي، جوزيف، ١٩٩٧، المنازعات الدولية ترجمة أحمد أمين ومجدي كامل، القاهرة.

ثانياً: المراجع الأجنبية:

1-V.A. Oganyan, M.V. Vinogradova, D.V. Volkov*, Internet Piracy and Vulnerability of Digital Content*, Article published in Journal of European Research Studies Volume Twenty-One, Issue 4, 2018.

2-.Michael N. Schmitt, Foreign Cyber Interference in Elections, Article published in Journal of International law studies, Volume 97,2021.