

تداعيات الحروب السيبرانية على السيادة الرقمية

The Implications of Cyber Wars on the Digital Sovereignty

بن قشاط خديجة*

مخبر القانون الدولي للتنمية المستدامة

جامعة عبد الحميد بن باديس مستغانم الجزائر

khadidja.benguettat@univ-mosta.dz

- تاريخ الإرسال: 2024/09/30 - تاريخ القبول: 2024/12/08 - تاريخ النشر: 2024/12/28

الملخص: تعد الحروب السيبرانية أعمالا عدائية فهي تتضمن الهجمات الإلكترونية التي تستهدف أنظمة المعلومات والبنية التحتية الرقمية، وهو الوضع الذي يمس بقدرة الدول على إدارة وحماية بياناتها ومعلوماتها الرقمية من التهديدات الخارجية، مما يشكل مساسا بسيادتها الرقمية. إن الانتهاكات الواقعة على السيادة الرقمية خلال الحروب تأتي في صور متعددة مثل التجسس على البيانات، والهجمات على الشبكات الحكومية. إن هذا الوضع يستوجب البحث في آليات الحفاظ على السيادة الرقمية، والتي تشمل تعزيز الحماية القانونية الدولية من أجل تحقيق الأمن السيبراني، مع ضرورة تدخل هيئة الأمم المتحدة من أجل حفظ الأمن السيبراني، والتعاون الدولي لمشاركة المعلومات، وكذا التوعية لدى المواطنين حول المخاطر السيبرانية.

الكلمات المفتاحية: السيادة الرقمية؛ الحروب السيبرانية؛ الأمن السيبراني؛ الأنترنت، التعاون الدولي.

Abstract: Cyber wars are considered hostile actions as they involve electronic attacks targeting information systems and digital infrastructure, which affects the ability of states to manage and protect their data and digital information from external threats, thus undermining their digital sovereignty. The violations of digital sovereignty during wars occur in various forms, such as data espionage and attacks on government networks. This situation necessitates exploring mechanisms to preserve digital sovereignty, which include enhancing international legal protections to achieve cybersecurity, the need for intervention by the United Nations to maintain cybersecurity, international cooperation for information sharing, and raising awareness among citizens about cyber risks.

Keywords: Digital Sovereignty; Cyber Wars; Cybersecurity; Internet; International Cooperation.

* المؤلف المرسل: بن قشاط خديجة.

مقدمة:

يعد الفضاء السيبراني فضاء معياريا، حيث لا يزال شاغراً بشكل يسمح لنا بالتشكيك في دور ومكان وشكل القانون الدولي في إطار ممارسة سلطات الدولة في مجال المراقبة الرقمية، مما أدى إلى تزايد مخاوف الكثير من الدول بشأن مسألة التحكم في موارد الإنترنت، خاصة أن الهجمات السيبرانية اليوم أصبحت جزءاً لا يتجزأ من أسلوب جديد للحرب أو أداة تستخدمها الدول ضد مصالح الدول الأخرى، في سياق حرب عالمية هجينة جديدة، حيث لم تعد العمليات السيبرانية تتعلق فقط بأجهزة المخابرات، ولكن سرعان ما تم اكتشاف إمكانية استخدامها لتخريب البنية التحتية للعدو، بالإضافة إلى ذلك، يمكن أن تتسبب بعض الهجمات الإلكترونية في حدوث وفيات مباشرة أو غير مباشرة، مما يعد تعدياً وخيماً على سيادة الدول.

لقد أظهرت النصوص الدولية والوطنية أن السيادة مفهوم قانوني مستقل منفصل عن الحقائق السياسية، إلا أنه وبالرجوع إلى تطور هذا المفهوم نجد أن السيادة تمثل ببساطة التعبير القانوني والمهذب عن ممارسة القوة، حيث كان لهذه القوة علاقة بالأسلحة بمختلف أنواعها وصولاً عند الأسلحة البيولوجية والكيميائية، ليقترن مفهوم السيادة لاحقاً بالمجال الرقمي في إطار حرب التكنولوجيا، فظهر مفهوم السيادة الرقمية، فلا ينبغي أن يكون مفاجئاً أن السيادة تبدو اليوم في حالة تحور كامل، حيث لم يعد مبدأ السيادة يقتصر على الأبعاد السياسية فحسب، وإنما أدى ظهور التقنيات الحديثة إلى سهولة النفاذ إلى حدود الدولة واختراق سيادتها، خاصة بالنسبة للدول النامية.

تعد المراقبة الرقمية لغرض حماية الأمن القومي مجال ذو سيادة، حيث اعتبرته الدول منذ فترة طويلة مجالا محجوراً غير قابل تقريباً لأي شكل من أشكال التنظيم، حيث لا نجد تنظيم ملزم للمراقبة الرقمية على نطاق عالمي، على الرغم من أن الوعي العالمي غير المسبوق بدرجة تدخل الجهات الرقمية العامة والخاصة في الحقوق الأساسية قد عجل بإدراج هذا النشاط في مجال الرقابة الشرعية، حيث تم استخدام تعبير "السيادة الرقمية" منذ عام 2012 خلال المؤتمر العالمي للاتصالات الدولية، ولا سيما من قبل روسيا والصين، اللتين تطلبان باستعادة "حقوقهما السيادية" على إدارة الشبكة ووضع معاهدة دولية لتقاسم المسؤوليات بشكل أفضل.

بناء على ما تقدم فإن إشكالية البحث تتمحور فيما يلي: إلى أي مدى يمكن أن تؤثر الحروب السيبرانية على السيادة الرقمية الوطنية لكل دولة في ظل غياب نصوص قانونية دولية في مجال الرقابة الرقمية؟

إن طبيعة البحث وموضوعه تستدعي الاعتماد بدرجة كبيرة على المنهج الوصفي التحليلي، حيث وجب البحث في ماهية الحروب السيبرانية وكذا السيادة الرقمية مستخدمين المنهج الوصفي، أما المنهج

التحليلي فقد اعتمدنا عليه من أجل تحليل التأثيرات التي تخلفها الحروب الإلكترونية وما مدى تأثيرها على سيادة الدول.

وعليه تم تقسيم هذه الدراسة إلى مبحثين، تضمن المبحث الأول الإطار المفاهيمي للحروب السيبرانية وللسيادة الرقمية، أما المبحث الثاني فقد تناول تأثيرات الهجمات الرقمية على سيادة الدول وآليات المواجهة.

المبحث الأول: الإطار المفاهيمي للحرب السيبرانية والسيادة الرقمية

أصبحت الحروب السيبرانية من أبرز التحديات التي يواجهها المتخصصون في القانون الدولي العام، وذلك بسبب صعوبة تحديد طبيعتها وعناصرها، وما يترتب عليها من مسؤوليات جنائية أو مدنية دولية. خاصة وأن بعض الدول قد تلجأ إلى هذه الهجمات لتحقيق السيطرة على الدول والمساس بسيادتها الرقمية. ومن أجل دراسة تداعيات هذه الهجمات وجب البحث في مفهوم الحروب السيبرانية وكذا مفهوم السيادة الرقمية.

المطلب الأول: مفهوم الحرب السيبرانية

يواجه مفهوم الحرب الإلكترونية العديد من الإشكالات، مما يستدعي ضرورة تحديد مفهوم الحرب السيبرانية. سنركز على المفهوم الذي يتعلق بوجود نزاع مسلح، إذ يُستخدم مصطلح الحرب الإلكترونية في مجالات متعددة تتجاوز نطاق النزاع المسلح، وبالتالي خارج نطاق تطبيق قواعد القانون الدولي الإنساني. فهناك أيضًا مجالات تتعلق بتطبيق هذه الأنشطة تشمل الشركات التجارية والحكومات وجرائم الفضاء الإلكتروني، بالإضافة إلى الجرائم الجنائية الأخرى، بنفس القدر الذي تهتم به الهجمات السيبرانية التي يخضع تنظيمها للقانون الدولي الإنساني. لذا، من المهم التعريف بالحرب الإلكترونية، واستكشاف خصائصها، وعرض بعض النماذج لهجمات إلكترونية وقعت أثناء نزاعات مسلحة.

أولاً: تعريف الحرب السيبرانية

تتعدد المصطلحات والمفاهيم المرتبطة بالحرب السيبرانية، حيث يُشار إليها أحيانًا بالحرب الافتراضية أو الحرب الإلكترونية، مما يستدعي الحاجة إلى البحث في مفهوم الحرب السيبرانية بشكل أكثر تفصيلاً.

لا يُمكن استخدام مصطلح الحرب السيبرانية إلا إذا كان الاعتداء السيبراني مرتبطاً بنزاع مسلح، أو إذا كان يعبر عن عدوان بين دول. فالهجمات التي ينفذها كيان غير مشروع لا تُعتبر نوعاً من الحرب السيبرانية التي تُعالج وفقاً لقواعد القانون الدولي العام. مما يعني أن مفهوم الحرب السيبرانية أضيق من مفهوم الهجمات السيبرانية، حيث يشمل أي اعتداء سيبراني بغض النظر عن أطرافه، ويتوقع منه إلحاق

الأضرار بالأشخاص أو الممتلكات، سواء كان مصدره أشخاصاً من القانون الدولي أو غيرهم. قد تقع الهجمات السيبرانية ضمن نطاق الحرب السيبرانية أو خارجه، لذا يمكن القول إن مفهوم الهجمات السيبرانية يتضمن مفهوم الحرب السيبرانية.¹

لا يوجد حتى الآن توافق واسع على تعريف دقيق ومحدد لمفهوم الحرب السيبرانية، وتتمثل المشكلة الرئيسية في غياب هذا التعريف في الطبيعة القانونية المتغيرة للمصطلحات الحديثة التي ظهرت في سياق النزاعات المسلحة. فهناك تحديات تتعلق بالهجمات السيبرانية التي تُنفذ عبر الشبكة العنكبوتية من جهة، وحداثة الهجمات على شبكات الحواسيب التي تُعتبر ظاهرة جديدة من جهة أخرى.²

عند الرجوع إلى المعنى اللغوي للحرب السيبرانية، نجد أن معظم المعاجم الحديثة لا تشير إلى مصدر كلمة "السيبرانية". يتضح أن "السيبرانية" هي مصطلح ذو أصل يوناني، حيث يعود إلى كلمة (Kybernetes) التي ظهرت في مؤلفات الخيال العلمي، وتُعني القيادة والتحكم عن بُعد.³

أما في الاصطلاح نجد أن هناك بعض الهيئات التي عرفت الحرب السيبرانية، كتعريف اللجنة الدولية للصليب الأحمر الحرب السيبرانية بأنها: "الاستغلال المتعمد لعدد من الأنشطة بهدف إفساد أو إتلاف أو تدمير الأنظمة الخاصة بالحاسب الآلي أو الشبكات الرقمية الخاصة بالخصم، وتقع على المعلومات والبيانات والأنظمة والشبكات وأي كيان يرتبط مع هذه الأنظمة والشبكات، وتستخدم هذه الهجمات إما للإضرار بالممتلكات الإلكترونية للخصم، أو لحرمانه من استخدام هذه الممتلكات، عن طريق منعه منولوج للمواقع الرسمية الخاصة به واستخدامها على النحو الذي يراه، كما قد تستخدم هذه الهجمات على نحو عكسي في الدفاع عن المنشآت الإلكترونية للدولة، وذلك عن طريق منع أي دخول غير مرخص له للمواقع الإلكترونية الخاصة بالدولة". أما بالنسبة للخبراء القانونيين في دليل تالين⁴ فقد عرفوا الحروب

¹ إسلام رمضان هديب، الحرب السيبرانية في ضوء القانون الدولي، مجلة البحوث القانونية والاقتصادية، المجلد 36، العدد 1، كلية الحقوق، جامعة بني سويف، 2024، ص 232. تم الاطلاع بتاريخ: 22 جويلية 2024.

https://lsey.journals.ekb.eg/article_350838_f6bcb760b5b2ba7feb76b11ef12ff89c.pdf

² أسامة صبري محمد، "الحرب الإلكترونية ومبدأ التمييز في القانون الدولي الإنساني"، مجلة القانون للدراسات والبحوث القانونية، العدد 7، 2013، ص 5.

³ طلال ياسين العيسى، عدي محمد عناب، "المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر"، مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد 19، العدد 1، 2019، ص 83.

⁴ دليل "تالين" (Manual Tallinn) صدر في نسخته الأولى في مارس 2013، وكان هدفه الرئيسي التحقيق في القضايا وتطبيق القانون الدولي في مجال الحرب السيبرانية. يتكون الدليل من قسمين رئيسيين: قانون الأمن السيبراني الدولي، وقانون النزاعات المسلحة السيبرانية، ويحتوي على سبعة فصول. تم صياغته بواسطة لجنة من خبراء القانون الدولي البارزين في تالين، استونيا، بدعوة من حلف الناتو، لتحديد الخطوط الحمراء التي تستوجب التدخل العسكري وطرق مشاركة مختلف الأطراف. في عام 2016، صدرت النسخة المحدثة من دليل تالين تحت عنوان "القانون الدولي المطبق على عمليات الإنترنت"، والتي شملت القواعد التي تم تحقيقها في الإصدار الأول. تضم النسخة المحدثة أربعة أجزاء رئيسية، وبلغ عدد القواعد القابلة للتطبيق على العمليات السيبرانية 154 قاعدة.

السيبرانية بأنها: "عمليات سيبرانية، سواء كانت هجومية أو دفاعية، يهدف من خلالها التسبب بالإصابة أو الوفاة لأشخاص أو إضرار وتدمير الأهداف".⁵

بالرجوع إلى دليل العمليات السيبرانية والإرهاب السيبراني التابع للجيش الأمريكي، نجده قد عرف الحرب السيبرانية بأنها: "الاستخدام المتعمد للأنشطة التخريبية، أو التهديد بها، ضد الحواسيب و/أو الشبكات، بقصد إلحاق الضرر أو تعزيز أهداف اجتماعية أو أيديولوجية أو دينية أو سياسية أو مشابهة. أو لتخويف أي شخص في إطار تحقيق هذه الأهداف".⁶

ويعتبر آخرون أن الحرب السيبرانية هي: "امتداد للحروب التقليدية والمادية، إذ يتألف جندها من المدنيين والعسكريين في آن واحد، كما أنها حرب أدمغة بالدرجة الأولى، كونها تستهدف في المقام الأول تدمير البنية العلمية والمعلوماتية للهدف، وتأخذ أشكال عدة، كشكل الاتصالات بين الجيوش وقياداتها، وإضعاف شبكات النقل والإمدادات اللوجستية، وضرب المعلومات الاقتصادية، والعبث بالمحتوى التقني والرقمي وغيرها".⁷ في المعنى التقني، تعني الحرب السيبرانية الاستخدام العسكري للأدوات الرقمية التي تُستخدم في الهجمات من نظام إلى آخر من خلال تدفق البيانات.⁸

وفي تعريف مبسط للحرب السيبرانية يقال أنها: "أحدث أشكال الحرب المعلوماتية، ويمكن أن تشمل هجمات الشبكات الحاسوبية (CNA)، التي تتكون من "عمليات تهدف إلى تعطيل أو إنكار أو تقليل أو تدمير المعلومات المخزنة في الحواسيب أو الشبكات الحاسوبية، أو تدمير الحواسيب والشبكات نفسها".⁹

يتضح من ما سبق أن مصطلح "الحرب السيبرانية" لا يُستخدم إلا إذا كان الاعتداء السيبراني مرتبطاً بنزاع مسلح، أو يعبر عن عدوان بين الدول. فلا يمكن اعتبار الهجمات التي تنفذها كيانات غير مشروعة نوعاً من الحرب السيبرانية التي تُعالج بموجب قواعد القانون الدولي العام. وهذا يعني أن مفهوم الحرب السيبرانية أضيق من مفهوم الهجمات السيبرانية، حيث يشمل أي اعتداء سيبراني بغض النظر عن أطرافه، والذي من المحتمل أن يلحق الضرر بالأشخاص أو الممتلكات. سواء كان مصدره أحد أشخاص القانون الدولي أو غيرهم، قد تقع الهجمات السيبرانية ضمن نطاق الحرب السيبرانية أو خارجه. لذا، يمكن القول إن

⁵ هريبرت لين، النزاع السيبراني والقانون الدولي الإنساني، مجلة اللجنة الدولية للصليب الأحمر، مجلد 94، العدد 886، جنيف 2012، ص 522.

⁶ Lesley Swanson, The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 RussianGeorgian Cyber Conflict, 32 Loy. L.A. Int'l & Comp. L. Rev. 303 (2010), p 307. Available at: <https://digitalcommons.lmu.edu/ilr/vol32/iss2/5>

⁷ حكيم غريب، صبرينة شرقي، "تداعيات الحرب الإلكترونية على العلاقات الدولية: دراسة في الهجوم الإلكتروني على إيران فيروس سكتنست"، دفاثر السياسة والقانون، المجلد، 12 العدد، 2، 2020، ص 96.

⁸ SOHAIL HUMNA (2022) "Fault Lines In The Application Of International Humanitarian Law To Cyberwarfare," Journal of Digital Forensics, Security and Law: Vol. 17, Article 8, p 5.

DOI: <https://doi.org/10.15394/jdfsl.2022.1761>

⁹ Lesley Swanson, Op.cit. p 308 .

مفهوم الهجمات السيبرانية يتضمن ضمنه مفهوم الحرب السيبرانية.¹⁰ كما يعتقد الكثير من المختصين أنه إذا استوفت العملية السيبرانية معايير النزاع المسلح، فيمكن أن تُعتبر حرباً سيبرانية في حد ذاتها. أما إذا كانت العملية تهدف إلى تعزيز نزاع مسلح قائم، فيمكن وصفها أيضاً بأنها حرب سيبرانية.¹¹

يمكن القول إن الحرب السيبرانية تتضمن العمليات الإلكترونية التي تنفذها الدول أو مجموعات حكومية أو غير حكومية، سواء كانت هجمات هجومية أو ردود فعل دفاعية. يهدف هذا النوع من العمليات إلى استهداف أفراد أو تدمير أهداف معينة، حيث يتم توجيه الفعل ضد شخص محدد من خلال التدخل غير المشروع في أنظمة الحواسيب أو المواقع الإلكترونية أو المنظومات الإلكترونية. قد يتجلى هذا الفعل أيضاً في حذف البيانات أو تعديلها أو تشفيرها، أو تقييد قدرة مالك الموقع على التحكم في موقعه، أو استخدام برمجيات خبيثة من أي نوع، وذلك بهدف إلحاق الضرر بالأجهزة الإلكترونية أو الأنظمة المعلوماتية للخصم.

تساهم جميع هذه العناصر في خلق خصوصية فريدة لهذه الحرب، مما يميز كل الأفعال التي تتم داخلها. وبالتالي، فإن هذا يدفعنا إلى استكشاف خصائص هذا النوع من الحروب بشكل أعمق.

ثانياً: خصائص الحرب السيبرانية

تتسم الحرب السيبرانية بالخصائص التالية:

1. **حرب غير مكلفة:** تتميز هذه الحرب بتكلفة منخفضة، حيث إن الأدوات اللازمة لشنها تتطلب نفقات بسيطة مقارنة بتكاليف الحروب التقليدية. بالإضافة إلى ذلك، لا تحتاج إلى تعاون مع دولة أخرى لتصنيع أسلحة باهظة الثمن مثل حاملات الطائرات والمقاتلات المتطورة، مما يجعلها تهديداً حقيقياً وخطيراً لدولة أخرى.¹²
2. **حرب رقمية متطورة:** تُعتبر الحرب الرقمية حرباً تقنية متطورة، حيث تركز على شبكة الإنترنت وما تتميز به من تطور مستمر وتنوع وابتكار في الوسائل والتقنيات المستخدمة. كما ترتبط هذه الحرب بالمصالح الحيوية للدول.
3. **السرعة والمراوغة:** تتميز الحرب السيبرانية بسرعة تنفيذ العمليات وإمكانية المراوغة، مما يمنح المهاجم أفضلية واضحة على المدافع.

¹⁰ [Oona A. Hathaway](#), The law of cyber- Attack, CALIFORNIA LAW REVIEW, Vol. 100, Issue 4, Berkeley, 2012, PP 833-835.

¹¹ SOHAIL HUMNA, Op.cit, p6.

¹² حكيم غريب، صبرينة شرقي، المرجع السابق، ص 96.

4. **عدم تحديد الأهداف والتأثير:** تتسم الحرب السيبرانية بعدم وضوح الأهداف والتأثير، إذ قد تتجاوز أخطارها ميادين القتال التقليدية لتطال أكثر المواقع السيادية والحساسة، حتى لو كانت بعيدة عن دائرة القتال.¹³

5. **أفضلية استراتيجية للمهاجم:** تتيح الحرب السيبرانية للمهاجم ميزة استراتيجية، حيث يمكنه اختيار وقت ومكان الهجوم وفقاً لرؤيته، مما يجعل من الصعب على الخصم توقع هذه الهجمات. ويصعب على الخصم توفير الحماية الكافية لجميع الأهداف السيبرانية المتنوعة.¹⁴

6. **عدم أهمية المسافات:** في الحرب السيبرانية، لا تعتبر المسافات عاملاً مؤثراً، حيث تحدث اختراقات للحدود الوطنية سواء للهجوم أو للاستغلال بشكل روتيني ودون أن يلاحظها أحد.¹⁵

وعليه، فإن خصوصية هذه الحروب ترتبط بخصوصية الفضاء السيبراني، حيث تتميز بالسرعة والسهولة، فضلاً عن عدم محدودية الانتشار. كما أنها تتسم بالسرية وصعوبة تتبعها أو الحصول على أدلة تثبت الأفعال المدمرة التي تتركها. هذا الطابع غير المادي يجعل التهديد أكبر وأكثر رعباً، ويؤثر بشكل كبير على العلاقات الدولية، مما يجعل الطرف المتحكم في هذا الفضاء هو الأقوى، حتى وإن كان الآخر يمتلك جيوشاً قوية.¹⁶

المطلب الثاني: مفهوم السيادة الرقمية

سننطلق ضمن هذا المطلب إلى مفهوم السيادة الرقمية من خلال البحث في المقصود بالسيادة عموماً ثم السيادة الرقمية على وجه الخصوص، ثم سنحاول البحث في جدلية الاعتراف بسيادة الدول على فضاءها الرقمي.

أولاً: تعريف السيادة الرقمية

يرتبط مفهوم السيادة بمعاهدة وستفاليا لعام 1648، التي أرست مبدأ سيادة الدولة على أراضيها وإدارتها لشؤونها الداخلية دون تدخل خارجي. ويعتبر هذا المبدأ من الأسس الجوهرية التي قام عليها القانون الدولي الحديث، كما أنه حظي باهتمام كبير من قبل فقهاء القانون الدولي والباحثين في مجال السياسة.¹⁷

¹³ جيلالي شويرب، فائزة دمراد، مفهوم الحروب السيبرانية والأمن السيبراني، مجلة الحقوق والحريات، المجلد 11، العدد 1، الجزائر، 2023، ص 163.

¹⁴ أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، منشورات زين الحقوقية، بيروت، 2018، ص 60.

¹⁵ هيربرت لين، المرجع السابق، ص 521.

¹⁶ جيلالي شويرب، فائزة دمراد، المرجع السابق، ص 164.

¹⁷ علي صادق أبو هيف، القانون الدولي العام، منشأة المعارف، الإسكندرية، 1995، ص 35.

تعددت تعريفات السيادة باختلاف المنطلقات الفكرية والظروف المحيطة بنشأة مفهوم السيادة. فكلمة "Sovereignty" الإنجليزية مشتقة من الكلمة اللاتينية "Superanus"، التي تعني "السمو" أو "الأعلى". وكان أول من استخدم هذا المصطلح هو "جون بودان" (1530-1596) في كتابه "الكتب الستة للجمهورية"، حيث قدّم أول نظرية متكاملة حول السيادة.¹⁸ كما وضع "جون أوستين" (1790-1859)، أحد رواد النظرية الكلاسيكية، نظرية السيادة على أساس أن الدولة هي نظام قانوني تتجسد فيه سلطة عليا تعمل كمصدر نهائي للقوة.¹⁹ يُعد مبدأ السيادة من الركائز الأساسية التي تعتمد عليها نظرية الدولة، ولذلك يُعتبر مصطلح السيادة مرادفاً لمصطلح الدولة في السياسة الدولية. فلا وجود للسيادة دون دولة، ولا يمكن أن توجد دولة بدون سيادة.

ففي النظام الدولي، شهد مفهوم "السيادة" تحولاً كبيراً من كونه مطلقاً إلى نسبي، وذلك نظراً للتغيرات العالمية المستمرة. ومن أبرز التطورات التي ساهمت في هذا التحول هو الفضاء السيبراني، الذي شكل تحدياً لمفهوم السيادة التقليدية في القانون الدولي. ويعد هذا التحدي من أبرز الدلائل على إعادة النظر في مفاهيم السيطرة والتحكم، حيث أضاف الفضاء السيبراني بُعداً جديداً للتفاعلات الدولية، مما يتطلب إعادة تقييم آليات السيادة في هذا المجال.²⁰

ظهرت فكرة "السيادة الرقمية" في أوائل العقد 2000. في عام 2011، قدم بيير بيلانجر، رئيس شركة "سكايروك"، محاولة أولى لتعريف هذا المفهوم: "السيادة الرقمية هي التحكم في حاضرتنا ومصيرنا كما يظهران ويتجهان من خلال استخدام التكنولوجيا والشبكات المعلوماتية".²¹ لذلك، أصبحت السعي لتحقيق السيادة الرقمية هدفاً مشتركاً بين الشركات، والجهات العامة، ومؤخراً، مستخدمي الإنترنت، سواء كانوا مواطنين أو مستهلكين.²²

عرفت السيادة الرقمية بالقول: "هي بسط الدولة لسيطرتها وولايتها القضائية على الفضاء الرقمي المتمثل في الأنترنت".²³ كذلك تم تعريفها على أنها "مجال قانوني تقني يتميز بمطالبات الدول والشركات والأفراد بالتحكم فيه، كما تعني خضوع الفضاء السيبراني لمصالح وقيم الدولة، وبالتالي قدرة الأخيرة بالتحكم

¹⁸ الصديق الشيباني، أزمة الديمقراطية المعاصرة، مطابع الشروق، القاهرة، د س ن، ص.50.

¹⁹ عبد الوهاب الكيالي، الموسوعة السياسية، ج 2، ط2، المؤسسة العربية للنشر و التوزيع، بيروت، 1996، ص.163.

²⁰ أنديرا عراجي، القوة في الفضاء السيبراني؛ فصل عصري من التحدي والاستجابة، دار ميرزا، بيروت، 2019، ص ص 83-86.

²¹ Pierre Bellanger, « De la souveraineté en général et de la souveraineté numérique en particulier », Les Échos, 30 août 2011 (archives.lesechos.fr/archives/cercle/2011/08/30/cercle_37239.htm). Consulter le : 18-09-2024.

²² Nicolas Colin et Henri Verdier, « Souveraineté numérique : la piste industrielle », paristechreview.com, 30 juin 2014 (www.paristechreview.com/2014/06/30/souverainete-numerique). Consulter le : 16-09-2024.

²³ محمد سعادي، أثر التكنولوجيا المستحدثة على القانون الدولي العام، دار الجامعة الجديدة، مصر، 2014، ص 240.

في مجالها السيبراني بما يضمن أنه يتبع ذات القواعد والمعايير والاعتبارات الموجودة في المجتمع".²⁴ ومن جهتها عرّفت لجنة التحقيق حول السيادة الرقمية التابعة لمجلس الشيوخ، في تقريرها الصادر عام 2019، السيادة الرقمية بأنها: "قدرة الدولة على التصرف في الفضاء السيبراني (...) وهو شرط ضروري للحفاظ على قيمنا، (...) ويتضمن، من ناحية، القدرة الذاتية على التقييم، واتخاذ القرارات، والعمل في الفضاء السيبراني، ومن ناحية أخرى، السيطرة على شبكاتنا واتصالاتنا الإلكترونية وبياناتنا".²⁵

وبالتالي تشير السيادة السيبرانية إلى قدرة الدول على التحكم في الفضاء الإلكتروني الذي يشمل البنية التحتية الرقمية والبيانات ضمن حدودها أو التي تؤثر على أمنها ومصالحها. تسعى الدول مثل الصين إلى تبني سيادتها السيبرانية من خلال تخصيص موارد ضخمة لصناعة الإلكترونيات والتحكم في هذا الفضاء، فمفهوم السيادة السيبرانية يتعلق بالتحكم الوطني في الفضاء الإلكتروني بما يخدم المصالح السياسية، الاقتصادية، الأمنية، والثقافية للدولة.

ثانياً: إشكالية الإقرار بسيادة الدول على فضاءها الرقمي

اختلف علماء السياسة حول تأثير الأمن السيبراني على سيادة الدولة. حيث يرى دانيال لامباش أن الفضاء السيبراني ساهم في تعزيز سيادة الدولة من خلال دعم ما يُعرف بـ "السيادة الإلكترونية" أو "السيادة على البيانات"، والتي تشير إلى فرض السيادة الوطنية في الفضاء السيبراني، بمعنى تشكيل مناطق ذات سيادة وطنية في هذا الفضاء. يعتمد هذا المفهوم على نظرية الممارسة والمفاهيم المزدوجة لإعادة التوطين، والمعروفة أيضاً بـ "الأنطولوجيا الإقليمية".

تتضمن الطرق التي تمارس من خلالها الجهات الفاعلة (مثل الدول) السيطرة على الفضاء السيبراني قطع الإنترنت في أوقات الأزمات السياسية، التحكم في التعليمات البرمجية والخوارزميات عبر تقنيات الذكاء الاصطناعي، وفرض رقابة صارمة على المحتوى، كما هو الحال في تركيا وتايلاند. بالإضافة إلى ذلك، تلجأ الدول إلى القرصنة الوطنية أو فرض قوانين "توطين البيانات" التي تمنع نقل البيانات عبر الحدود، كما في حالي روسيا والصين، مما يعكس قوة الدولة بشكل منتظم.

تتوفر العديد من الأدوات للدول التي تسعى لإعادة إنشاء أراضيها الوطنية في الفضاء السيبراني، مثل حجب بروتوكول الإنترنت (IP) ومراقبة الكلمات الرئيسية لمتابعة المناقشات حول الموضوعات

²⁴ مروة زين العابدين سعد، تأثير تغير مفهوم السيادة على الاختصاص القضائي في الجرائم السيبرانية. المجلة الدولية للفقه والقضاء والتشريع، نادي

قضاة مصر، مصر، المجلد 3، العدد 3، أكتوبر 2022، ص 703.

²⁵ Institut Inria, Souveraineté numérique : Quel rôle pour la recherche ?, in : <https://www.inria.fr/fr/souverainete-numerique-role-recherche>, 29 mars 2021. Consulter le : 18-09-2024.

الحساسة، ومنع الوصول إلى المواقع التي تعتبر تخريبية.²⁶ وقد تم تطبيق هذه الإجراءات في عدة دول، مثل "الجدار الناري العظيم" في الصين ونظم الرقابة الحكومية الصارمة على الإنترنت في كوريا الشمالية. ومع ذلك، يعتقد البعض أن الأمن السيبراني يحمل تهديدًا لسيادة الدولة بسبب عمليات الاختراق والهجمات السيبرانية، مثل هجمات وسطاء الظل والثغرات الإلكترونية التي تتجاوز حدود الدول.

تظهر إشكالية الاعتراف بالسيادة الرقمية للدول نتيجة المواقف السلبية التي تتبناها بعض الدول. فلم تعترف جميع الدول بعد بالسيادة الرقمية في الفضاء السيبراني، حيث تختلف السياسات والممارسات من دولة لأخرى. تعتبر بعض الدول، مثل الولايات المتحدة الأمريكية، أن الفضاء السيبراني هو من المشاعات العالمية، وبالتالي لا يمكن نقل السيادة إلى هذا الفضاء. في المقابل، لدى دول أخرى رؤية مغايرة، حيث ترى أن الأمر يتطلب السيطرة للحد من تأثيرات الفضاء السيبراني وانعكاساته على أمن الدولة،²⁷ حيث تتبنى الصين سياسة قوية للسيطرة على الفضاء السيبراني، مما يعكس تصورها للسيادة الرقمية، كما يركز الاتحاد الأوروبي على حماية البيانات من خلال اللائحة العامة لحماية البيانات (GDPR)، ويعتبر أن البيانات هي جزء من السيادة الوطنية. فهذه الدول تدرك أن الفضاء السيبراني يمكن أن يؤثر على أمنها الوطني، مما يدفعها إلى اتخاذ إجراءات أكثر صرامة للسيطرة على المعلومات والبنى التحتية، كما تسعى إلى وضع قوانين مختلفة لحماية البيانات والأمن السيبراني، مما يعكس وجهات نظرها حول السيادة الرقمية، حيث تؤدي هذه التشريعات، في بعض الأحيان، إلى صراعات قانونية بين الدول، خاصة فيما يتعلق بتبادل البيانات عبر الحدود.

وعلى الرغم من الحاجة المتزايدة للتعاون الدولي من أجل مواجهة التحديات السيبرانية العالمية، إلا أن هذا التعاون قد يكون معقدًا بسبب الاختلافات في السياسات الوطنية.، حيث تسعى الدول إلى السيطرة وفرض سلطتها القضائية على الإنترنت من خلال تنظيم فضاءها الإلكتروني، بهدف الحفاظ عليه. وتعكس هذه الجهود عزم الدول على مكافحة الأفعال التي تهدد ثقة وسلامة وأمن مجتمعات الافتراضي، خاصة مع تزايد الهجمات السيبرانية.

²⁶ Daniel Lambach, "The Territorialization of Cyberspace", International Studies Review, Vol 22, Issue 3, September 2020, PP 482–506.

²⁷ أنديرا عراجي، المرجع السابق، ص 112.

المبحث الثاني: واقع السيادة الرقمية في ظل الحروب السيبرانية

يمثل الحفاظ على السيادة الدولية تحديًا كبيرًا للدول في العصر الحديث، فمع تزايد الاعتماد على التكنولوجيا والأنظمة الرقمية، أصبح مفهوم السيادة الرقمية أكثر أهمية، حيث يتطلب من الدول حماية معلوماتها الوطنية والبنية التحتية الحيوية من التهديدات السيبرانية.

المطلب الأول: صور التعدي على السيادة الرقمية للدول

إن التعدي على السيادة الرقمية يشير إلى الانتهاكات التي تتعرض لها الدول في قدرتها على إدارة وحماية بياناتها الرقمية ومعلوماتها، حيث تتعدد صور التعدي على السيادة الرقمية للدول، ومن أبرزها:

أولاً: الهجوم الإلكتروني

يعني استخدام الطاقة الكهرومغناطيسية أو الأسلحة المضادة للإشعاع لمهاجمة الأفراد والمرافق بهدف إضعاف القدرة القتالية للعدو وتقليل استخدامه الفعّال للطيف المغناطيسي. تشمل هذه الهجمات التشويش والتضليل الكهرومغناطيسي. وعادةً ما تؤدي الخسائر الناتجة عن الهجوم الإلكتروني إلى خسائر مادية كبيرة، على عكس الحروب التقليدية التي تتضمن خسائر بشرية²⁸. ومن أمثلة الهجوم الإلكتروني تعطيل أنظمة الدعم اللوجستي لتقليل دعم للقوات المعادية وخفض فاعليتها، والتحكم في أنظمة توليد الكهرباء.

ثانياً: التجسس الإلكتروني انتهاك للسيادة الرقمية

يُعتبر التجسس الإلكتروني أحد أهم المراحل التمهيدية للعمليات الحربية السيبرانية، ويُعرف على أنه وسيلة لاعتراض غير مصرّح به لأنظمة الاتصالات والشبكات والبيانات بهدف الحصول على معلومات والتلاعب بها. ويُعد التجسس الإلكتروني من أولى أشكال التهديد التي تمس الأمن القومي الوطني، وتشكل خطراً على مصالح الدول والأفراد²⁹. كما يشير التجسس السيبراني إلى المحاولات المتعمدة لاختراق أجهزة الكمبيوتر والمواقع الإلكترونية الخاصة بالدولة المنافسة أو الخصم، بهدف سرقة معلومات سرية. يسعى هذا النوع من التجسس للحصول على قاعدة بيانات ضخمة تتعلق بالأنظمة والأسرار العسكرية والسياسية والأمنية

²⁸ محمد عاطف إمام إبراهيم، الفضاء الإلكتروني وأثره على الأمن القومي للدول: الحروب الإلكترونية نموذجاً، الدراسات البحثية، المركز الديمقراطي العربي، 23 أبريل 2022، <https://democraticac.de/?p=81775> تم الاطلاع بتاريخ: 10 سبتمبر 2024.

²⁹ كريم رقبولي ولخضر نويوة، الأمن السيبراني المتوسطي بين الواقع والرهانات الأمنية. مجلة طبنة للدراسات العلمية الأكاديمية. المجلد 2، العدد 2، 2019، ص 74.

والاقتصادية والصناعية. وتعتمد هذه العمليات بشكل كامل على وسائل وأنظمة الاتصال والتواصل التكنولوجي الحديثة داخل الدول.³⁰

في العصر الحالي، أصبح التجسس يتجاوز النطاق العسكري والحربي ليشمل مجالات متعددة مثل الاقتصاد، التكنولوجيا، السياسة، والصناعة. ورغم أن التجسس العسكري لا يزال يحتل مكانة هامة ويعتبر من أخطر أنواع التجسس، إلا أن طبيعة المعلومات المطلوبة اليوم قد تغيرت بشكل كبير. في الماضي، كانت المعلومات السرية تتمحور حول حجم الجيوش وتجهيزاتها، وكانت هذه المعلومات تعتبر بالغة الأهمية. أما الآن، فقد أصبحت هذه البيانات متاحة بشكل أوسع، حيث تُنشر في الصحف ووسائل الإعلام، وتُظهر الخرائط التي تمثل توزيع القوات في مناطق النزاع وتُناقش بشكل علني. التجسس الحديث يركز أكثر على المعلومات الدقيقة والمتقدمة، مثل التكنولوجيا العسكرية الحديثة، البيانات الاستراتيجية الاقتصادية، والمعرفة المتعلقة بالتطورات العلمية والصناعية. هذا التغيير يعكس التحولات الكبيرة في مفهوم الأمن القومي وأهمية المعلومات في العصر الرقمي.³¹

ثالثاً: الاختراق الإلكتروني

يتضمن اختراق الأنظمة للحصول على معلومات استخباراتية عن دولة أو منظمة، فهو نظام أو برنامج مصمم لاستغلال بيانات الخصم وإلحاق الضرر بها، بالإضافة إلى تعطيل نظامه الحاسوبي، بهدف التفوق عليه في المجالات الأمنية، العسكرية، والسياسية. تتم هذه العملية على مستويات متعددة، سواء كانت فردية، مؤسسية، أو على مستوى الدول. يأخذ الاختراق الإلكتروني أشكالاً متنوعة، لكنه يسعى في النهاية إلى الوصول إلى المعلومات الحيوية للخصم والاستيلاء عليها، من خلال استخدام أنظمة حاسوبية تستهدف البنية التحتية المعلوماتية للجهة المقصودة.³²

رابعاً: الهجمات على البنية التحتية الحيوية

قد تبدو هجمات الحرمان من الخدمة ذات ضرر نسبي ضئيل في الفضاء السيبراني للدول، لكنها قد تسبب تكاليف وخسائر مادية كبيرة إذا استمر انقطاع الخدمة لأسبوع كامل. وإذا استهدفت الهجمات البنية

³⁰ ينظر: شريفة كلاع، الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، جامعة الجلفة، المجلد 15، العدد 1، 2022، ص 295.

³¹ سامية بوشوشة، حياة سلماني، التجسس الإلكتروني وطرق مكافحته، مجلة العلوم الاجتماعية والإنسانية، جامعة تبسة، المجلد 16، العدد 1، 2023، ص 54.

³² علي محمد محمود، حروب الفضاء الإلكتروني وعلاقتها بحروب الجيل الخامس، دار المعارف، مصر، 2020، ص ص 55، 56.

التحتية، فإن الخسائر على أرض الواقع تكون هائلة، خاصة عند استهداف العمليات الصناعية والأنظمة الإدارية المرتبطة بها. على سبيل المثال، يمكن لمجموعة من الهاكرز التلاعب بالأنظمة الخاصة بالطاقة، مثل أنابيب نقل النفط والغاز، ومصانع إنتاج الوقود، ومحطات توليد الكهرباء³³.

بغض النظر عن العدد الدقيق للأنشطة والعمليات الإلكترونية التي تستهدف البنية التحتية الحيوية، فقد وقعت العديد من الحوادث الفعلية التي تبرز القلق المتزايد بشأن تأمين هذه البنية التحتية التي أصبحت مترابطة بشكل متزايد. على سبيل المثال، في أوائل عام 2020، أجبرت هجمات الجرائم الإلكترونية التي استهدفت مستشفى جامعة برنو في التشيك المستشفى على تعليق العمليات الجراحية المجدولة وتحويل المرضى إلى مرافق أخرى قريبة. وفي حادثة أخرى قبل أربع سنوات، أبلغت شركة توزيع الكهرباء الأوكرانية عن انقطاع في الشبكة دام عدة ساعات نتيجة هجوم إلكتروني استهدف أجهزة الكمبيوتر وأنظمة التحكم الإشرافي وجمع البيانات (SCADA)، مما تسبب في انقطاع التيار الكهربائي عن حوالي 225,000 عميل³⁴.

خامسا: القرصنة الإلكترونية

هي عملية الدخول غير المصرح بها إلى أجهزة الغير وشبكاتهم الإلكترونية تهدف إلى المساس بالسرية وخصوصية الأفراد، أو التأثير على سلامة المحتوى من خلال تغييره أو إتلاف³⁵. لا تقتصر القرصنة على المعلومات الشخصية للمواطنين فحسب، بل تتجاوز ذلك من خلال الكشف عن أسرار أمن الدول واختراق مواقع المؤسسات الحكومية والبريد الإلكتروني لبعض قادة الدول حول العالم، خاصة قادة تلك الدول التي عانت حروبا أهلية. فقد شهدت السنوات العشر الأخيرة تسريبات غير مسبوقة تتسم بالطابع السري وبأدق التفاصيل حول شخصيات دولية مستهدفة بهدف الإطاحة بها أو خلق مشاكل واضطرابات داخل الدول التي ينتمون إليها³⁶.

³³ نور الدين حامد علي إبراهيم، الفضاء السيبراني: المفاهيم والأبعاد، المجلة العلمية للبحوث والدراسات التجارية، جامعة حلوان، المجلد 38، العدد 2، 2024، ص ص 737، 738.

³⁴ Lee, Robert M., Michael J. Assante & Tim Conway. 2016. 'Analysis of the Cyber Attack on the Ukrainian Power Grid.' SANS & E-ISAC, 18 March. As of 21 October 2020: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, Accessed on: September 01, 2024.

³⁵ بعوني ليلي، التهديدات في الفضاء السيبراني وانعكاساتها على السيادة الرقمية: القرصنة الإلكترونية نموذجاً، مجلة ستراتيجيا، المعهد العسكري للوثائق والتقويم والاستقبالية، المجلد 8، العدد 2، 2021، ص 9.

³⁶ بعوني ليلي، المرجع نفسه، ص 18.

سادسا: الهجمات على الأنظمة العسكرية:

تستهدف أنظمة التحكم بالأسلحة، الأقمار الصناعية، أو أنظمة الاتصالات العسكرية لتعطيل العمليات الحربية، فالهجمات على العمليات العسكرية والحكومية تشمل استهداف الأنظمة بشكل يومي، وغالباً ما تكون جزءاً أساسياً منها للتجسس. هذه الهجمات تهدف إما للحصول على تصاميم الأسلحة، أو الحصول على معلومات سرية، أو لفهم طريقة تفكير العدو أثناء نشوب حرب، أو لمعرفة الخطط العسكرية وتمركز القوات. لذلك، أي شبكة متصلة بالإنترنت تكون عرضة للهجوم، وحتى تلك التي لا تكون متصلة قد لا تكون بمنأى عن الخطر. تعتمد الحكومات والجيش على هذه الشبكات في أوقات السلم، ولكن هذا لا يعني أن الاعتماد عليها في حالة الحرب آمن. في الواقع، قد تتقلب ميزة التكنولوجيا العسكرية المتقدمة للجيش الحديثة إلى كارثة في حال تعرضها لهجمات سيبرانية تؤدي إلى تعطيلها³⁷.

هذه بعض الصور التي تعكس الأشكال المختلفة للحرب السيبرانية التي تعتمد على التقنيات الرقمية للتأثير على الدول والمنظمات، حيث تعتبر هذه الصور تحدياً حقيقياً للسيادة الرقمية، وتتطلب استجابة فعالة من الحكومات لتعزيز الأمن السيبراني وحماية البيانات والمعلومات الحساسة.

المطلب الثاني: الآليات الدولية والإقليمية للحفاظ على السيادة الرقمية

تُعد السيادة مبدأً أساسياً من مبادئ القانون الدولي، وذلك وفقاً لتعريف واسع القبول الذي ورد في قرار التحكيم الدولي بشأن جزيرة بالماس لعام 1928. وفي هذا السياق، تؤكد التصريحات المتعددة الصادرة عن الأمم المتحدة، وحلف شمال الأطلسي، ومنظمة الأمن والتعاون في أوروبا، والاتحاد الأوروبي، بالإضافة إلى معظم الدول بشكل فردي، أن القانون الدولي ينطبق على الفضاء السيبراني. بناءً على ذلك، تُعتبر العمليات الهجومية السيبرانية التي تخترق سيادة الدول انتهاكاً صريحاً للقانون الدولي، وتترتب عليها "مسؤولية دولية"³⁸.

أولاً: تعزيز الحماية القانونية الدولية من أجل تحقيق الأمن السيبراني

تعد اتفاقية بودابست لعام 2001، والمعروفة أيضاً باسم اتفاقية الجريمة السيبرانية، أول معاهدة دولية تهدف إلى مكافحة الجرائم الإلكترونية، من خلال توفير إطار قانوني مشترك للدول الأعضاء لتنظيم وتنسيق جهودها في مواجهة الجرائم التي تحدث عبر الإنترنت. تم التوقيع على هذه الاتفاقية في بودابست، المجر، في 23 نوفمبر 2001، ودخلت حيز التنفيذ في 1 يوليو 2004. تدعو الاتفاقية إلى توحيد التشريعات

³⁷ نور الدين حامد علي إبراهيم، المرجع السابق، ص 737.

³⁸ مروة زين العابدين سعد، المرجع السابق، ص 707.

الوطنية المتعلقة بالجريمة السيبرانية، وتحديد الجرائم الإلكترونية، مثل الوصول غير المصرح به إلى أنظمة الكمبيوتر، الاحتيال الإلكتروني، والاعتداء على البيانات، والتعدي على حقوق الملكية الفكرية. وتتضمن الاتفاقية أيضًا إجراءات لتعزيز التعاون الدولي بين الدول الأعضاء لتسهيل تبادل المعلومات والمساعدة في التحقيقات والعمليات القانونية عبر الحدود³⁹.

تلعب اتفاقية بودابست دورًا مهمًا في تعزيز السيادة الرقمية من خلال توفير إطار قانوني دولي للتعامل مع الجرائم السيبرانية. ومع ذلك، هناك تحديات متعلقة بالسيادة الرقمية في سياق هذه الاتفاقية.

من جهة، تُسهم الاتفاقية في حماية السيادة الرقمية للدول من خلال توفير أدوات قانونية وإجرائية تساعد في التصدي للجرائم الإلكترونية التي قد تهدد أمنها الرقمي. الاتفاقية تُمكن الدول من تحديث تشريعاتها وممارساتها لتتماشى مع التطور التكنولوجي، وتعزز التعاون الدولي في مجال مكافحة الجرائم السيبرانية التي تتجاوز الحدود.

لكن من جهة أخرى، يُثار أحيانًا جدل حول مدى تأثير هذه الاتفاقية على السيادة الرقمية للدول، حيث أن الالتزام بتبادل المعلومات والتعاون مع دول أخرى قد يفرض تحديات تتعلق بحماية البيانات الوطنية وحقوق الخصوصية. بعض الدول قد ترى في هذه الاتفاقية تقييدًا لسيادتها الرقمية، خاصة إذا كانت تتطلب منها التعاون في قضايا تتعلق بأمنها القومي أو معلومات حساسة.

بالتالي، يمكن القول إن اتفاقية بودابست تمثل خطوة مهمة في تعزيز السيادة الرقمية من خلال حماية الفضاء السيبراني من الجرائم، لكنها تطرح أيضًا تحديات مرتبطة بتوازن التعاون الدولي وحماية السيادة الوطنية.

ثانياً: تدخل هيئة الأمم المتحدة من أجل حماية السيادة الرقمية

تلعب منظمة الأمم المتحدة دورًا متزايدًا في حماية السيادة الرقمية للدول من خلال جهود متعددة لتعزيز الأمن السيبراني والتصدي للتهديدات الرقمية. هذه الجهود تشمل عدة محاور، من أبرزها:

• تعزيز الأطر القانونية الدولية:

بدأ الاهتمام بالتصدي للأنشطة التي تخترق السيادة الرقمية على مستوى الأمم المتحدة خلال المؤتمر الثامن للأمم المتحدة للوقاية من الجريمة ومعاملة الجانحين، الذي انعقد في هافانا، كوبا، من 27 أغسطس

³⁹ ينظر: سليمان قطاف، عبد الحليم بوقرين، الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة الأغواط، المجلد 6، العدد 1، 2022، ص 337، 339.

إلى 7 سبتمبر 1990. في هذا المؤتمر، تبنت الجمعية العامة قرارًا بشأن التشريعات المتعلقة بالجريمة المعلوماتية. وقد أعقب هذا المؤتمر العديد من الأنشطة الهادفة إلى تعزيز الدفاع عن السيادة الرقمية للدول. في عام 1994، تكثفت الجهود في هذا المجال، وفي عام 2005، خلال المؤتمر الحادي عشر للأمم المتحدة للوقاية من الجريمة والعدالة الجنائية الذي انعقد في بانكوك، تايلاند، تبنت الأمم المتحدة إعلانًا يدعو إلى توحيد وتنسيق التشريعات المتعلقة بمكافحة الجريمة المعلوماتية. يعكس هذا الإعلان التزام المنظمة بمواجهة التهديدات التي تمس سيادة الدول في الفضاء السيبراني⁴⁰.

تعمل الأمم المتحدة على تطوير سياسات وأطر قانونية لتعزيز السيادة الرقمية، بما في ذلك مجموعة العمل المفتوحة التي أسستها في عام 2018 لتناول القضايا المتعلقة بالأمن السيبراني. تسعى هذه المجموعة إلى بناء مفاهيم دولية حول القوانين والمعايير التي تنظم الفضاء الرقمي.

• الحفاظ على السلم والأمن في الفضاء السيبراني:

عند استعراض العديد من الأمثلة على الهجمات السيبرانية التي استخدمت فيها أسلحة سيبرانية لأغراض هجومية أو دفاعية، مثل الهجمات على استونيا في عام 2007، ومفاعل نطنز في عام 2010، ودير الزور في عام 2010، وجورجيا في عام 2015، يتضح أن تأثيرها وتداعياتها على الأمن والسلم الدوليين تعادل ما يُستخدم في حالات العدوان أو الحروب التقليدية.⁴¹ لذلك تعمل الأمم المتحدة من خلال مؤسسات مثل مجلس الأمن الدولي على التصدي للتهديدات الرقمية التي قد تهدد السلم والأمن الدوليين، مثل الهجمات الإلكترونية التي تستهدف البنية التحتية الحيوية. في عام 2021، تم اعتماد عدة قرارات لتشجيع الدول على تعزيز تدابير الحماية السيبرانية.

• مكافحة الجرائم السيبرانية حفاظًا على السيادة الرقمية

تسعى الأمم المتحدة إلى وضع إطار شامل لمواجهة هذا النوع من الجرائم. وفي هذا السياق، قدمت مجموعة من القواعد الموضوعية والإجرائية للتصدي لهذه الجرائم، وقد جاء ذلك واضحًا في المؤتمر الثاني عشر للأمم المتحدة حول موضوع الجريمة والعدالة الجنائية الذي عُقد في سلفادور بالبرازيل في الفترة الممتدة من 12 إلى 16 أبريل 2008، حيث جاء في البند 40 من تقرير المؤتمر، التأكيد على أهمية بناء قدرات وطنية لمكافحة الجرائم الإلكترونية، بما في ذلك مراحل المنع والاكتشاف والتحقيق وملاحقة الجناة، وتعزيز

⁴⁰ أحمد شحيرط، مراد قريبيز، تحديات الأنترنت لسيادة الدول (لسيادة الرقمية)، مجلة البحوث القانونية والاقتصادية، المركز الجامعي آفلو، المجلد 5، العدد 1، 2022، ص 315.

⁴¹ وداد بوطالعة، منال بوكورو، صراع الفضاء السيبراني وتأثيره على السلم والأمن الدوليين - التهديدات والتحديات الجديدة وسبل المواجهة-، مجلة العلوم القانونية والاجتماعية، جامعة الجلفة، المجلد 7، العدد 4، 2022، ص 816.

الأمن في الفضاء السيبراني. كما أشار البند 42 من التقرير إلى أهمية التنسيق بين الدول في مجال مكافحة الجرائم الإلكترونية. تم التركيز على ضرورة تبادل المعلومات بشأن التشريعات الوطنية، وتعزيز التعاون والمساعدة التقنية، ودراسة التجارب الوطنية، وكذلك الإجراءات القانونية المتعلقة بالجرائم السيبرانية⁴².

بشكل عام، تسعى جهود الأمم المتحدة إلى تعزيز التعاون الدولي في حماية السيادة الرقمية للدول، مع التركيز على الأمن، حماية الخصوصية، وحقوق الإنسان في الفضاء السيبراني. كما تسعى الأمم المتحدة من خلال برامج مثل برنامج الأمم المتحدة الإنمائي إلى بناء القدرات التقنية للدول، لا سيما الدول النامية، لمساعدتها في تطوير أنظمة دفاع سيبرانية قوية، وحماية بنيتها التحتية من الهجمات الإلكترونية.

ثالثاً: التعاون الدولي من أجل وقف الانتهاكات الواقعة على السيادة الرقمية

في سياق البحث عن استراتيجية فعالة لتعزيز السيادة الرقمية للدول في الفضاء السيبراني، يمكن الإشارة إلى التقرير الصادر عن مؤسسة كارنيغي للسلام الدولي في نوفمبر 2020 بعنوان "استراتيجية دولية لزيادة حماية النظام المالي العالمي من التهديدات السيبرانية". رغم أن هذه الاستراتيجية تركز على القطاع المالي، إلا أنها يمكن أن تُطبق على مجالات أخرى، مثل السياسة والثقافة والمجتمع والاقتصاد والأمن العسكري. تهدف هذه الاستراتيجية إلى توحيد جهود الدول وتقليل تشتتها في مواجهة التهديدات في الفضاء السيبراني، وبالتالي تحقيق سيادة رقمية للدول بشكل جماعي. وعلى الرغم من ذلك، تظل مشكلة التعاون بين الدول في تنظيم الفضاء السيبراني قائمة بشكل ملحوظ، ويرتبط ذلك بانكفاء الدول على نفسها في تأمين فضائها السيبراني ضمن حدودها الجغرافية، بالإضافة إلى ارتفاع مستويات عدم الثقة بينها. حيث يرتبط الأمن السيبراني بالمصالح الحساسة للأمن القومي، مما يجعل التعاون متعدد الأطراف لتنظيم الفضاء السيبراني أمراً غير مفضل، رغم أنه ضروري⁴³.

رابعاً: إنشاء أطر قانونية وطنية

يقصد بذلك تطوير قوانين وطنية تتعلق بحماية البيانات، ومكافحة الجرائم الإلكترونية، وضمان الأمن السيبراني، مع التوافق مع المعايير الدولية، وتعد المنظومة التشريعية الصينية من أبرز النماذج في مجال حماية السيادة الرقمية حيث تبنت الصين عدة قوانين في هذا المجال أبرزها إقرار قانون جديد للإنترنت في الصين عام 2017 يُعرف باسم "قانون الأمن السيبراني الصيني"، ودخل حيز التنفيذ في 1 يونيو 2017.

⁴² آمال بيدي، جهود الأمم المتحدة في مكافحة الجريمة السيبرانية، مجلة البحوث في الحقوق والعلوم السياسية، جامعة تيارت، المجلد 8، العدد 1، 2022، ص ص 308، 308.

⁴³ عبد الغاني شرقي، التهديدات السيبرانية وإشكالية السيادة إعادة قراءة لسيادة واستقاليا، مجلة السياسة العالمية، جامعة بومرداس، المجلد 7، العدد 2، 2023، ص 284.

يهدف هذا القانون إلى تعزيز دور مكتب إدارة الفضاء الإلكتروني في الصين الذي أصبح الجهة المسؤولة عن مراقبة وتنظيم الإنترنت داخل البلاد. هذا القانون شدد الرقابة على الأنشطة الإلكترونية من خلال تطوير تقنيات متقدمة للمراقبة، مما أثر على مفاهيم الخصوصية على الإنترنت.

يخضع الإنترنت في الصين لرقابة صارمة من خلال "جدار الحماية العظيم (Great Firewall)"، وهو نظام تكنولوجي معقد طورته السلطات الصينية لإدارة والتحكم في الوصول إلى الإنترنت داخل البلاد.⁴⁴ هذا الجدار يمنع الوصول إلى آلاف المواقع الإلكترونية، بما في ذلك مواقع التواصل الاجتماعي الشهيرة مثل فيسبوك وتويتر، بالإضافة إلى العديد من محركات البحث مثل جوجل. الهدف من هذا النظام هو تقييد المعلومات المتاحة للمستخدمين الصينيين والحفاظ على السيطرة على المحتوى الرقمي داخل البلاد، مما يعزز السياسات الحكومية فيما يتعلق بالمراقبة والرقابة على الإنترنت.

وغيرها من القوانين التي أدت إلى جعل الصين رائدة في المجال الرقمي ومن بين إنجازاتها ما يعرف بطريق الحرير الرقمي الذي ظهر في عام 2015 كجزء من مبادرة الحزام والطريق الصينية، والتي تهدف إلى بناء بنية تحتية رقمية متقدمة وتعزيز التعاون الرقمي بين الصين والدول الأخرى. الفكرة مستوحاة من طريق الحرير القديم الذي كان يربط الصين بالعالم من خلال التجارة، ولكن النسخة الرقمية تهدف إلى تحقيق ذلك عبر التكنولوجيا والاتصالات، حيث تهدف الصين إلى تطوير استراتيجيات مشتركة لحماية البنية التحتية الرقمية من التهديدات السيبرانية وتعزيز الأمن الإلكتروني.⁴⁵

وعلى الرغم من اعتمادها سياسة حمائية دفاعية في المجال الرقمي تعتبر الصين منتهكة لحرية الوصول إلى المعلومات، حيث نشرت منظمة *Freedom House* تقريرها السنوي بعنوان "الحرية على شبكة الإنترنت 2018"، والذي يقيم حالة حرية الإنترنت في مختلف دول العالم. وفقاً للتقرير، احتلت الصين المرتبة الأولى بين الدول التي تفرض أكبر القيود على الإنترنت، مما يعكس استخدام الحكومة الصينية نموذجاً يحد من حرية الوصول إلى المعلومات. وذكر التقرير أن الصين كانت في طليعة الدول التي تنتهك النموذج الحر والمنفتح للإنترنت من خلال الرقابة الواسعة، حجب المواقع، ومراقبة الأنشطة الإلكترونية للمواطنين.

⁴⁴ عبد الغاني شرقي، المرجع السابق، ص 283.

⁴⁵ من أجل مزيد من المعلومات: نوران عمرو محمد رفع، أحمد إسماعيل أحمد حافظ، أثر الرقمنة على طريق الحرير - الآفاق و التحديات، مجلة المعهد العالي للدراسات النوعية، مجلة المعهد العالي للدراسات النوعية، المجلد 4، العدد 11، 2024.

خامساً: وضع استراتيجية للردع السيبراني

يتطلب تحقيق الوعي العالمي بحالة الفضاء السيبراني من حيث التهديدات والفاعلين. ينبغي أن تتضمن هذه الاستراتيجية أنظمة دفاعية سيبرانية فعالة لحماية جميع القطاعات المدنية والعسكرية، مع إعطاء الأولوية للدفاع عن البنية التحتية الأساسية. كما يجب امتلاك مجموعة واسعة من القدرات الهجومية السيبرانية المضادة لتعزيز قوة الدولة وفرض الردع قبل وأثناء وبعد الأزمات⁴⁶. وذلك من خلال رفع تكلفة الهجوم الإلكتروني للدولة المعتدية، من خلال إنشاء أنظمة دفاع إلكترونية معقدة وصعبة الاختراق، تتطلب وقتاً وجهداً كبيرين لاختراقها. كما ينبغي تطوير قدرات تتبع الهجمات الإلكترونية واكتشاف مصادرها، مما يؤدي في النهاية إلى التأثير على قرارات الخصم، وردعه عن شن هجمات إلكترونية ضد الدولة⁴⁷.

الخاتمة:

ختاماً يمكن القول أن السيادة الرقمية والحروب السيبرانية تمثلان أحد التحديات الكبيرة التي تواجه الدول في العصر الحديث، حيث تتزايد أهمية السيادة الرقمية في ظل التطور التكنولوجي السريع والاعتماد المتزايد على الفضاء الرقمي في مختلف جوانب الحياة، بما في ذلك الاقتصاد، والسياسة، والأمن. وتبرز الحروب السيبرانية كوسيلة جديدة للصراع، حيث تسعى الدول لتحقيق أهدافها الاستراتيجية من خلال استهداف البنية التحتية الرقمية، والبيانات الحساسة، والنظم الحيوية، مما يجعل الحفاظ على السيادة الرقمية عنصراً أساسياً في عصر المعلومات والتكنولوجيا. يجب على الدول أن تعزز استراتيجياتها للتأكد من أنها قادرة على حماية مصالحها الرقمية وضمان حقوق مواطنيها في الفضاء الرقمي. يتطلب ذلك التنسيق بين السياسات الوطنية والدولية لتحقيق بيئة رقمية آمنة ومزدهرة.

أولاً: النتائج

1. الحرب السيبرانية تمثل تهديداً مباشراً للسيادة الرقمية، حيث قد تسعى دولة ما إلى اختراق أو تعطيل الفضاء السيبراني لدولة أخرى بهدف تقويض سيادتها الرقمية.
2. الدول التي تتمتع بسيادة رقمية قوية تكون أكثر قدرة على حماية نفسها من الهجمات السيبرانية وتحديدًا على منع السيطرة أو التدخل الأجنبي في نظمها الرقمية.
3. الحروب السيبرانية قد تؤدي إلى تآكل هذه السيادة الرقمية، مما يُضعف قدرة الدولة على التحكم في بياناتها وأمنها الداخلي.

⁴⁶ نور الدين حامد علي ابراهيم، المرجع السابق، ص 726.

⁴⁷ شريفة كلاع، المرجع السابق، ص 306.

4. الحرب السيبرانية تُعتبر اختبارًا لقدرة الدول على الحفاظ على سيادتها الرقمية. إذ يتطلب ذلك من الدول تطوير دفاعات رقمية قوية وسياسات تضمن حماية مصالحها في الفضاء السيبراني.

5. يعد غياب التنظيم القانوني للهجمات السيبرانية التحدي الأكبر الذي يواجهه الفضاء الإلكتروني، فرغم وجود إرادة دولية على مستوى المفاوضات وقرارات مجلس الأمن. مع ذلك، لا يتم تطبيق هذه الإرادة بشكل فعال، خاصة من جانب القوى الكبرى المهيمنة في هذا المجال.

ثانيا: التوصيات

1. يجب على الدول الاستثمار في تطوير بنى تحتية قوية للأمن السيبراني تشمل تقنيات متقدمة، وأفضل الممارسات، وتدريب الكوادر البشرية لمواجهة التهديدات.
2. ينبغي على كل دولة وضع استراتيجيات وطنية شاملة تتضمن خطط استجابة للطوارئ السيبرانية، مع وضع إطار عمل قانوني يحدد كيفية جمع واستخدام وحماية البيانات الرقمية. يجب أن يركز هذا الإطار على حماية حقوق الأفراد ومؤسسات الدولة.
3. ضرورة تعزيز التعاون بين الدول لمشاركة المعلومات والموارد حول التهديدات السيبرانية، حيث يمكن أن يشمل التعاون تبادل البيانات حول الهجمات والتقنيات المستخدمة، مما يعزز القدرة على مواجهة التهديدات، ويسهم في تعزيز السيادة الرقمية.
4. اعتماد تقنيات حديثة للكشف عن التهديدات السيبرانية وتحليلها، مما يساعد على تحسين قدرة الدول على التفاعل مع الهجمات ومعرفة مصدرها.
5. سن تشريعات دولية فعالة تحمي الفضاء الرقمي وتعزز من قدرة الدول على الحفاظ على سيادتها.
6. يجب أن يكون هناك وعي مجتمعي بشأن أهمية حماية البيانات والخصوصية، إذ أن الوعي العام يمكن أن يلعب دورًا حيويًا في تعزيز السيادة الرقمية.