باب العلوم السياسية والقانونية:

1.العمليات السيبرانية وتأثيرها على تحولات السيادة في الفضاء السيبراني

Cyber Operations and Their Impact on Sovereignty Transformations in Cyberspace

بقلم الباحث: محمد محمود زيتون

طالب دكتوراه في جامعة بيروت العربية / كلية الحقوق والعلوم السياسية، فرع علوم سياسية

إشراف أ. د. إبراهيم شاكر

Muhammad Mahmoud Zaytoun

PhD student at Beirut Arab University / Faculty of Law and Political Science, Political Science Department

mzeitoun@outlook.com

تاريخ الاستلام: 2025/1/24 تاريخ القبول: 2/ 3/ 2025 تاريخ النشر: 25/3/ 2025

مستخلص البحث:

تتناول الدّراسة مفهوم العمليّات السّيبرانيّة وتأثيرها على تحوّلات السيّادة في الفضاء السيبراني، حيث كانت العمليّات السيادة السّيبرانيّة ركيزة أساسيّة للدّراسة، تناولت إطاراً نظرياً للسيادة والعمليات السيبرانية الفضاء السيبراني، وناقشت مفهوم العمليات السيبرانية وخصائصها وانواعها وتصنيف العمليّات السّيبرانيّة بما فيها الهجوميّة والدّفاعيّة في إطار عمليٍّ وأكاديميٍّ، وإبراز التّأثيرات التي تؤثّر على السّيادة السّيبرانية من انتهاكات وتدّخل سيبراني. وبعد فهم طبيعة المتغيّرات، اقترحنا قيام معاهدة تنظّم الفضاء السيبراني والعمليات السيبرانية، وبناء استراتيجيّة أمن سيبراني دوليّة للتّخفيف من أثر العمليّات السّيبرانيّة ولحماية سيادتها الرقمية.

كلمات مفتاحية: السيادة السيبرانية، العمليات السيبرانية، الفضاء السيبراني

Abstract:

The study addresses the concept of cyber operations and their impact on transformations in sovereignty within cyberspace. Cyber sovereignty served as a fundamental pillar of the study, which provided a theoretical framework for sovereignty and cyber operations within cyberspace. It discussed the concept, characteristics, and types of cyber operations, as well as the classification of cyber operations, including offensive and defensive ones, in both practical and academic contexts. The study highlighted the effects on cyber sovereignty, such as violations and cyber interference. After understanding the nature of these variables, the study proposed the establishment of a treaty to regulate cyberspace and cyber operations, along with the development of an international cybersecurity strategy to mitigate the impact of cyber operations and protect digital sovereignty

Keywords: Cyber sovereignty, cyber operations, cyberspace

مقدمة:

في هذا العصر المتسارع، أصبح فيه الفضاء السيبرانيّ أحد الميادين الحيويّة التي تُعاد فيه صياغة مفاهيم تقليديّة عديدة، كالسيادة التقليديّة، والقوّة، والامن القومي والوسائل القتالية. ونتيجةً للتطور التكنولوجي والتحولات الذي يشهده هذا الفضاء، اختزلت فيه الحدود الجغرافيّة والسياسيّة وأصبح الفضاء السيبراني مجالاً جديداً لامتدادات السيّادة ومصالح الدول، مما أدى الى ظهور السّيادة السيبرانيّة. إنّ تشابك الفضاء االسيبراني بين الواقع المادي والافتراضي وتوليف الامن السيبراني والعمليات السيبرانية مع القدرات العسكريّة والتكنولوجيّة والاقتصاديّة، حفّز الدول لامتلاك قدرات سيبرانيّة لعسكرة الفضاء السيبراني، والسيطرة على مقدرات الفضاء لتعزيز مكانتها والدفاع عن مصالحها، مما خلق تنافس في الرؤى بين القوى الكبرى كالولايات المتحدة والصين وروسيا حول مفهوم السيّادة السيبرانية ومسالة تدّفق البيانات. ومن جهة أخرى خلق تحديات حول تعريف مفهوم السيّادة السيبرانيّة في ظل تزايد العمليّات السيبرانيّة وتعقيد الفضاء السيبراني. ومع اشتداد تنوّع العملياّت السيبرانيّة وتزايد استخدامها في تحقيق المصالح، أصبحت أداة جذابة لتحقيق الأهداف العابرة للحدود وتتسابق الدول على توظيف العمليّات الدفاعيّة والهجوميّة في استراتيجيّاتها الوطنيّة ووحداتها العسكريّة.

وبناء على ما جاء، سنحاول من خلال هذه الورقة تقديم تعريفا موحداً للسيّادة السيبرانيّة، وخلق توازنًا بين حماية المصالح وضمان انفتاح الإنترنت وحقوق المستخدمين، لإذابة التناقض في وجهات النظر بين القوى الكبرى. والتركيز على مفهوم العمليات السيبرانيّة وخصائصها، للتشديد على ضرورة تبني استراتيجيّات للأمن السيبراني والتوّصل الى معاهدة رقميّة تنظّم الفضاء السيبرانيّ والأنشطّة السيبرانيّة.

أهمية الموضوع: تكمن أهمية البحث في تحليل مفهوم العلميات والسيادة السيبرانية، واستكشاف التحديّات التي تواجه الدول في الحفاظ على سيادتها السيبرانيّة، وأهمية دور العمليّات السيبرانية في زعزعة الاستقرار بين الدول، واستعراض تطورها كأداة مبتكرة للتأثير والتدّخل في شؤون الدول، وانتهاك السيادة، فضلاً عن كونها إحدى الوسائل

الحديثة في الصراعات الدولية.

أهداف البحث: تهدف الدراسة إلى تسليط الضوء على مفهوم السيادة السيبرانيّة، وتداعيات العمليات السيبرانية في الساحة الدولية.

إشكالية البحث: اصبحت العلميّات السيبرانيّة ظاهرة متنامية تلعب دوراً مزعزعاً في النظام الدوليّ المعاصر، خاصة بعدما أصبح الفضاء السيبراني ميدانًا جديدًا للصراع والتنافس بين الدول، والتباينات حول مفهوم السيّادة السيبرانيّة، وهنا تبرز إشكالية. كيف تؤثر العمليات السيبرانية على مفهوم السيادة في الفضاء السيبراني؟

منهجية البحث: سنتناول في هذا البحث المنهج الوصفي والتحليلي لتوصيف العمليات السيبرانية ومفاعليها على الدول، وتحليل التحولات التي طرأت على السيّادة السيبرانيّة كمجال جديد في الديناميكيّات الدوليّة في الفضاء السيبراني.

تصميم البحث:

المبحث الأول: الإطار النظري والمفاهيمي للسيّادة والعمليّات السيبرانيّة

المطلب الأول: مفهوم السيّادة السيبرانيّة في الفضاء السيبراني

المطلب الثاني:مفهوم العمليات السيبرانيّة وخصائصها

المبحث الثاني: أثر العمليّات السيبرانيّة على السيّادة السيبرانيّة

المطلب الأول: العمليّات السيبرانيّة وانتهاك السيّادة

المطلب الثاني: استراتيجيّات الدول لحماية سيادتها الرقميّة

المبحث الأول: الإطار النظري والمفاهيمي للسيّادة والعمليَات السيبرانيَة

السيّادة والعمليّات السيبرانيّة مفهومين ناشئين متضّادين في سياق العلاقات الدوليّة والفضاء السيبراني، لكنهما مرتبطين بالنمو الرقميّ. السيّادة السيبرانيّة تزداد تمدداً وتأثّراً، والعمليّات السيبرانيّة تزداد تعقيداً وتأثيراً، إلا إنّ مصطلح العمليات السيبرانيّة يشمل الحروب السيبرانيه والإرهاب السيبراني والهجمات السيبرانيه والجريمة السيبرانيه وسائر الأنشطة الخبثة، وكلها ترمي الى إحداث ضرر في العالم الحقيقي في الدول وشعوبها ويهدد السلام والامن الدوليين، بينما السيادة جاءت في البداية نتيجة لتطور الفكر الفلسفي عند توماس

هوبز وجان جاك روسو، ثم نتيجة للتفاعل المعقد بين التطورات السياسية والفكرية في أوروبا على مدار سنوات من الحرب وتطوّر الفكر والسلطة، مما أرسى مفهوم الدولة الحديثة والعلاقات الدولية، لتصبح السيّادة ناظمة للعلاقات الدولية قائمة على مبدأ المساواة وعدم التدّخل باي وسيلة. ولكن بسبب الترابط التكنولوجي والشبكي وظهور العمليات السيبرانية، وتنكّر المهاجمين وقدرتهم على شن عمليات سيبرانية عن بعد، أصبحت تؤثر على الثقة بين الدول، وتساهم في الصراعات السياسية والعسكرية والاجتماعية.

وانطلاقاً مما سبق، سنتناول في هذا المبحث مطلبين، الأول يبيّن مفهوم السيّادة السيبرانيّة في الفضاء السيبراني وجملة من التناقضات بين القوى الكبرى، والثاني يفصّل مفهوم العمليات السيبرانية وخصائصها نطاقها.

المطلب الأول: مفهوم السيّادة السيبرانيّة في الفضاء السيبراني

السيادة في مفهومها التقليدي، هي بأن الدولة في طابعها الداخلي هي سيّدة على اقليمها ذات سلطة مطلقة منفردة على كامل ارضها وشعبها، ولها حرية كاملة باختيار نظامها السياسي والاقتصادي والاجتماعي، وتضع الأنظمة والقوانين وتحتكر جميع قوانين الدولة والسلطات، بالإضافة الى الامن والسلاح ومواردها والاستثمار، وكل الوظائف الضرورية على الأقاليم البحرية، الجوية والبرية دون منازع. الطابع الخارجي للسيادة قائم على مبدأ مساواة السيادة بين الدول، ومبدأ عدم التدخل بالشؤون الدخيلة او عدم اللجوء الى استخدام القوة ضد أي دولة. ولكن بفضل الفضاء السيبراني والأنشطة الرقمية المتنوعة، تمّ توسع مفهوم السيادة ومصالح الدول، فلم تعد السيادة مقتصرة على الأرض والمجال الجوي والمياه الإقليمية، بل امتدَّ مفهوم السيادة ليشمل الفضاء السيبراني، كمجال تسعى فيه الدول إلى فرض سيطرتها على الأنشطة السيبرانية التي تتم داخل حدودها الافتراضية وخارجها.

1. **مفهوم السيادة السيبرانية:**

إن تزايد الاعتماد على التكنولوجيا في معظم المجالات جعلت من الفضاء السيبراني جزءاً لا يتجزأ من حياة البشريّة، وساهم في فرض تحولات على مفهوم السيادة التقليدية وعناصرها، فالرقعة الجغرافية أصبحت عالمية، والمصالح

تمّت رقمنتها، والافراد أصبحت أفراد رقميّة تعرف بـ (Netizen)، ومجالات السيادة أصبحت شبه رقميّة، كلّها ادّت إلى مفهوم السيادة السيبرانية، مفهوم تتنافس فيه الدول القومية والجهات الفاعلة على تملّك البيانات واستعمارها، واحتكار أدوات السيطرة الرقمية من صناعة التقنيات والخدمات الرقمية، او من خلال الانشطة المتمثلة بالعمليات السيبرانية.

على إثر هذه التحولات، قدمّت وكالة أنباء شينهوانت تفسيرا مهماً للسيادة السيبرانية تميّز بطابعين داخلي وخارجي: داخليًا تشير السيادة السيبرانية إلى التطوير المستقل والإشراف والمراقبة في إدارة شؤون الإنترنت الخاصة بالدولة، وخارجياً تشير السيادة السيبرانية إلى منع الإنترنت الخاص بالدولة من الغزو والهجوم الخارجي. رغم الاعتقاد، ان السيادة السيبرانية تشير إلى سيادة الفضاء السيبراني بدلاً من «السيادة على الإنترنت».[1] وكما يؤكّد ميثاق الأمم المتحدة سيادة الدول كمبدأ أساسي، وتتمتع كل دولة بالسيادة الكاملة والحصرية على أراضيها، بما في ذلك عمليات الفضاء السيبراني التي تنشأ من بنيتها التحتية الرقمية أو الموجّهة نحوها.[2] والسيادة السيبرانية في جوهرها، تشير إلى قدرة الدولة على السيطرة على الفضاء السيبراني داخل حدودها الجغرافية وحمايته من التهديدات الخارجية، بالإضافة إلى إدارة وتنظيم الأنشطة السيبرانية على أراضيها. وهذا التعريف ظهر على الرغم من أن مفهوم السيادة السيبرانية لم يتبلور أو يكتسب شكله النهائي بعد، بفضل التطورات الرقمية المستمرة، وما زال يشكل موضوعًا للنقاش بين المنظمات غير الحكومية التي تسعى للدفاع عن الحريات الرقمية.[3]

– السيادة السيبرانية وأبرز التحولات

الفضاء السيبراني هو مجال افتراضي يتكون من الشبكات الإلكترونية والبنية

1 Binxing Fang – Cyberspace Sovereignty–Springer Singapore, science press Beijing springer ,2018, 78.

2 – Cyber espionage and international law, available on internet, https://www.cyber–espionage.ch/Law.html, visited on 23–7–2024.

3– Gourley, Stephen K., "Cyber sovereignty. In Conflict and Cooperation in Cyberspace: The Challenge to National Security, eds. Panayotis A. Yannakogeorgos, and Adam B. Lowther ,Boca Raton: CRC Press, 2013, P.P.277–289.

التحتية الرقمية التي تربط الناس والأجهزة والبيانات في جميع أنحاء العالم، بما فيه الإنترنت، وأنظمة التحكم الصناعية، وأجهزة إنترنت الأشياء، والأنظمة العسكرية، أي هو المجال الذي تُمارس فيه السيادة السيبرانيّة، ولكن بسبب تفاعل الدول سيبرانيا وسياسيا فيما يتعلق بالأمن السيبراني ومواجهة التهديدات السيبرانية، وحماية الخصوصية والحرية والتنمية الرقمية، والحفاظ على الامن القومي وسلامة أصولها واستثماراتها. فأصبحت السيادة السيبرانية من أكثر المفاهيم تأثرا في الفضاء السيبراني خاصة بما يتعلّق بسلطة الانترنت وتدفّق المعلومات. وفي هذا السياق، لا بدّ من الإشارة، إلى أّن صبغة النظام السياسي الحاكم يلعب دورا كبيرا في التفاعل الرقمي وحوكمة الإنترنت والبيانات وآلية امتداد السيادة السيبرانية، على سبيل المثال الصين وروسيا عززا سلطتهما في إدارة التدفقات الرقميّة والانترنت التي تعبر بنيتهما التحتية خشية على أمنهما القومي من التجسس السيبراني والصناعي والسياسي، بما ينسجم مع مبادئهم السياسية تجاه ما يعتبرونهم أعداء تقليدين لهم.

ونتيجة لذلك، قامت روسيا والصين تبني مفهوم للسيادة السيبرانية يبرر مراقبة المحتوى الرقمي وتديق التدفقات خلافا لمفهوم السيادة لدى الدول التي تتبنى الليبرالية على رأسها الولايات المتحدة والدول الاوروبية. لذلك ظلت السيادة محل نزاع وغموض لتفسير ونشر المعنى الذي يناسب مصالح الدول وتدخلها، ولذلك قال بروس شاينر،[1] في كتابه البيانات وغولاياث(Data and Goliath)، إن حركة السيادة السيبرانية في بلدان مثل روسيا والصين والسعودية تلقت صدمة قوية بعد كشف التنصت الخطير الذي تمارسه وكالة الأمن القومي الأمريكية عليهم، وهذا ما اعطى تبرير للصين وروسيا والسعودية لإدارة نشاطاتهم الخاصة.[2]

لذلك أصبحت سيادة الدول في الفضاء السيبراني تتمحور حول تأثير الأمن السيبراني على مفهوم السيادة. بحيث أنّ الفضاء السيبراني ساهم في تعزيز سيادة الدولة من خلال مفهوم «السيادة السيبرانية»، والذي يتمثل في قدرة الدول

1 –بروس شاينر (Bruce، Schneier) خبير أمريكي في مجال الأمن المعلوماتي وحركة البيانات.

2 – Schneier ،Bruce, Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: W.W. Norton & Company, 2015,P. 78.

على فرض سيطرتها في الفضاء السيبراني عبر إنشاء مناطق ذات سيادة وطنية. يتم ذلك من خلال إجراءات، مثل قطع الإنترنت في أوقات الأزمات السياسية، والتحكم في البرمجيات والخوارزميات بتقنيات الذكاء الاصطناعي، وفرض الرقابة على المحتوى كما هو الحال في تركيا وتايلاند. لذلك لجأت بعض الدول إلى القرصنة الوطنية أو قوانين «توطين البيانات» ما يُعرف بـ «الأنطولوجيا الإقليمية»، التي تمنع نقل البيانات عبر الحدود، كاستخدام الدول أدوات حجب بروتوكول الإنترنت (IP) ومراقبة المناقشات حول المواضيع الحساسة، ومنع الوصول إلى مواقع معينة، واستخدام الصين للجدار الناري العظيم، وأنظمة الرقابة الصارمة في كوريا الشمالية. وهذه الإجراءات والتحولات تضع السيادة السيبرانية بين فكي الصراع والنفوذ بين القوى الكبرى حول مفهوم السيادة السيبرانية وتدفق البيانات والتدخل رقيما في شؤون الدول.

2.تناقضات الدول الكبرى حول مفهوم السيّادة السيبرانية وأبعادها السياسية

هناك ثلاثة تناقضات حول السيادة السيبرانية، تعرقلها السيطرة والتحكم والمصالح من جهة، وتحديات تخلقها العمليات السيبرانية من جهة اخرى، ويدور الجدال حول ثلاث جهات فاعلة رئيسية في الفضاء السيبراني: الدولة القومية، والمواطن، والمجتمع الدولي، وكل جهة تريد التركيز فقط على مصالحها الخاصة، وتتجاهل كل جهة فاعلة مصالح الطرفين الآخرين، الأمر الذي قادنا إلى الوضع الحالي، وهو الوضع الذي يصعب فيه التوصل إلى تسوية لتحقيق فهم السيادة السيبرانية وإدارة المصالح والتحكم فيها. إن الجهات الفاعلة التي تسبب التناقض بين السيادة السيبرانية وروح الإنترنت هما الدولة والمجتمع الدولي، وبين السيادة السيبرانية وحقوق الإنسان تقف الدولة والمواطن، وإنّ التناقض بين السيادة السيبرانية وحوكمة أصحاب المصلحة المتعددين يشمل الدولة، والمواطن، والمجتمع الدولي. مما جعل السيادة السيبرانية محوراً للجدال تجتزئها المصالح، تتراوح بين التشريعات المحلية والدولية والأنظمة الحاكمة والحوكمة وسياسات الامن السيبراني والعمليات السيبرانية وتتمثل في ثلاثة تناقضات على الشكل التالي:

– التناقض بين السيادة السيبرانية وروح الإنترنت: السيادة السيبرانية تشير إلى مبدأ أن الدول لها الحق في التحكم في الفضاء السيبراني داخل حدودها، بما في ذلك إدارة وتنظيم الإنترنت والسيطرة على البيانات والمعلومات التي تنتقل عبر شبكاتها،[1] وهذا قد يدفع كل دولة إلى إنشاء فضاء سيبراني منفصل خاص بها، مما يؤدي إلى تجزئة الإنترنت إلى أجزاء مختلفة تخضع لقوانين وسياسات مختلفة.

– التناقض بين السيادة السيبرانية وحقوق الإنسان: ويعكس هذا التناقض حقوق الانسان الرقميّة وسيادة البيانات والإنترنت على السيادة السيبرانيّة،[2] حيث يشهد هذا التناقض تفاوتًا في التعامل بين الدول الديمقراطية والدول ذات الأنظمة القمعيّة، وتستخدم ومعظم الحكومات تقنيات التجسس الرقمي لمراقبة نشاطات مواطنيها عبر الإنترنت، بما في ذلك مراقبة وسائل التواصل الاجتماعي والمنتديات. فتتدخل الدول باسم السيادة السيبرانية وحجّة امنها الوطني وتسن القوانين لمراقبة المحتوى وتقييد حرية التعبير وحجب المواقع، ومعاقبة الأفراد الذين يعبّرون عن آرائهم مثل اعتقال النشطاء والصحفيين، على سبيل المثال الصين تستخدم جدار الحماية العظيم (Great Firewall of China) لتنظيم الوصول الى الشبكة المحلية ومراقبة المحتوى وتقييد الوصول، وتبرره بحماية الأمن الوطني ومنع الجرائم السيبرانية وتنظيم البيانات.[3]

– التناقض بين السيادة السيبرانية وأصحاب المصلحة المتعددين في التحكم: يثير هذا التنتقض جدلاً حول نمط إدارة الإنترنت،[4] فالحكومات ترى أن لها الحق السيادي والطبيعي في تنظيم الفضاء السيبراني لحماية أمنها الوطني ومصالحها الاقتصادية، وأصحاب المصلحة المتعددين (القطاع الخاص، المجتمع المدني، الأكاديميين،منظمات دولية) يصرون على توزيع السلطة وكيفية إدارة الفضاء السيبراني والمشاركة في اتخاذ القرارات بشكل تشاركي وجماعي لتعزيز الشفافية والمساءلة

1- Hao Yeli, A Three-Perspective Theory of Cyber Sovereignty, PRISM Volume 7, No 2,P.3.

2 - Hao Yeli, ibid, P.3.

3 Baidu and CloudFlare Boost Users Over China's Great Firewall, available on internet https://www.benton.org/headlines/baidu-and-cloudflare-boost-users-over-chinas-great-firewall, visited 13-7-2024.

4- Hao Yeli, Ibid.,. P.3.

و مراعاة المصالح العالمية والمحلية على حد سواء، بينما الدول تحتكر سن القوانين لفرض سيطرتها الكاملة على سيادة الفضاء السيبراني ، من خلال القوانين والقيود الصارمة واللوائح التي تنظم استخدام الإنترنت ، وذلك يتعارض مع مبادئ الشفافية والتعاون. ويعوّق التجارة الإلكترونية العالمية ويؤثر على حرية تدفق البيانات.

وهذه التناقضات جاءت بناءً على اختلاف وجهات النظر بين الدول الكبرى، حول كيفية السيطرة على الفضاء السيبراني والمهيمنة على النظام الدولي القائم للحفاظ على وجودها ودورهم الدولي. وتوضيحا لوجهات النظر وضعنا في الجدول

ادناه رؤية كل دول للفضاء السيبراني وأدوات السيطرة على السيادة السيبرانية.

اختلاف وجهات النظر حول الفضاء السيبراني[1]		
القضية	الولايات المتحدة والمملكة المتحدة	روسيا والصين
الفضاء السيبراني	فوضوي	فضاء سيادي
التنظيم	دور مركزي للقطاع الخاص ولا حاجة ضرورية لتدخل الحكومات	دور مركزي للدولة وضرورة التدخل الحكومي
حوكمة الانترنت	مشاركة كافة أصحاب المصلحة (حكومة، قطاع خاص، أكاديمي، مجتمع مدني)	دور أساسي للدول ووضع قواعد ومنظمات جديدة للتعامل مع الظاهرة المستحدثة

–السيادة الخارجية: السيادة الخارجية هي مصدر حصانة الدولة مما يجعلها تمارس الأنشطة السيبرانية بحرية في علاقاتها الدولية وفي صياغة سياستها الخارجية. وتتبع السيادة الخارجية مبدا المساواة السيادية بين الدول كما هو معترف به في المادة 2 من ميثاق الأمم المتحدة،[1] ولها حرية الانخراط في أنشطة سيبرانية خارج أراضيها وفقًا للقانون الدولي فقط ، وبالانضمام الى اتفاقيات دولية تتعلق بالأنشطة السيبرانية وتقرير ما إذا كانت ستختار الانضمام إلى أنظمة معاهدات سيبرانية محددة أو إصدار تعبيرات

1 – Charter of the United Nations, available on internet, https://legal.un.org/repertory/art2.shtml , visited on 29-7-2024.

عن الرأي القانوني بشأنها لأي ممارسة سيبرانية معينة في دولة معينة، ولا تكون الدولة ملزمة بالموافقة على قواعد معاهدة معينة تحكم الأنشطة السيبرانية لأجهزتها أو مواطنيها أو السلوك الذي يجري في أراضيها السيادية. ويدعم الميثاق أن مشاركة الدولة في العمليات السيبرانية بحكم سيادتها الخارجية لا يخل بمعايير المعاهدات الملزمة أو القانون الدولي العرفي ويحرم انتهاك سيادة، والتدخل، واستخدام القوة.

2.2 المطلب الثاني: مفهوم العمليّات السيبرانيّة وخصائصها

أصبحت العمليّات السيبرانيّة أداة محوريّة في الاستراتيجيّات الأمنيّة والعسكريّة للدول والمنظمات الدوليّة، وسلاح استراتيجي بيد الدول إلى جانب قدراتها التقليدية، وأصبحت إحدى مكونات القوة الشاملة للدول. ويمكن تصنيفها إلى جزئين رئيسيين، العمليات الهجوميّة (OCO) وهي الأنشطة التي تستهدف اختراق الأنظمة والشبكات وتدمير البيانات، تعطيل الأنظمة الحيويّة. والعمليّات الدفاعيّة (DCO) التي تهدف إلى حماية الأنظمة والشبكات من تهديدات العمليات الهجومية، والكشف عنها، وتعزز الأمن السيبراني.

1. مفهوم العمليات السيبرانية أنواعها

العمليّات السّيبرانيّة (Cyber operations): يشار إليها أحيانًا باسم عمليّات الفضاء السّيبراني أو عمليّات شبكة الكمبيوتر (CNO) وهي جزءًا من الحروب الحديثة. فالعمليّات السّيبرانية هي مجموعة من الأنشطة (الهجوميّة والدّفاعيّة) تستخدم القدرات السّيبرانية في الفضاء السيبراني بهدف تحقيق أهداف محدّدة وتنفّذ في الفضاء السّيبراني أو من خلاله. ويتنوّع استخدامها في جمع المعلومات الاستخباراتيّة، وتعطيل أو تدمير الأنظمة والشّبكات الإلكترونيّة، لأغراض قوميّة أو سياسيّة واقتصادية، إلى جانب دورها الناشئ في الصّراعات الدّولية والعسكرية.[1] إلا انّ التقدم التكنولوجي لعب دورًا مزدوجًا في العمليات السيبرانية، من جهة الدفاع السيبراني، حيث ساهم الذكاء الاصطناعي وتعلّم الآلة في تحسين قدرة الأنظمة على اكتشاف التهديدات السيبرانية ومحاولات التسلل واصلاحها بسرعة أكبر ودقة عالية. ومن جهة

1- François Delerue, Cyber operations and international law, Cambridge University Press, United Kingdom ,2020, p.29.

الهجوم يستخدم الذكاء الاصطناعي في أكتشاف الثغرات وتسهيل عمل القراصنة في مهاجمة الاهداف. على سبيل المثال، التشفير يجعل البيانات أكثر أمانًا ويعزز قدرة الأنظمة على حماية المعلومات الحساسة، ولكن مؤخرًا شهدنا أكبر عملية سرقة للعملات المشفرة بتكوين(Bitcoin)، من خلال كسر جسر بلوك شاين(Block chain) ، على الرّغم من تميز البلوك شاين بتشفير معقد للغاية حيث يقوم بعملية تشفير تراكمية مع كل عملية مالية تحصل، ولكن تمّ اختراقه واستولى القراصنة 100 مليون دولار من شركة عملات رقمية.[1] لذلك سنناقش أنواع العمليات السيبرانية وآليات ونطاق عملها والتعقيدات التي تتميز بها، وأدواتها الهجومية والدفاعية.

وفي هذا السياق، نشير إلى أن مصطلح العمليات السيبرانية هو مصطلح أُتفق على استخدامه في المناقشات والنداءات الدولية والاممية مثل الأمم المتحدة، ومجلس حقوق الانسان واللجنة الدولية للصليب الأحمر، وهو مصطلح يشمل (الحرب السيبرانية، الهجمات السيبرانية، الحرب الصامتة، حرب الاصفار، وعمليات واجراءات الامن السيبراني وجميع العلميات الدفاعية والهجومية الى جانب جميع الأنشطة السيبرانية).[2]

– أنواع العمليات السيبرانية الهجومية وأسلحتها: تنقسم العمليات السيبرانية الى قسمين رئيسيين: العمليات السيبرانية الهجومية (Offensive Cyber Operations – OCO) تهدف إلى استهداف الأنظمة والشبكات لتحقيق أهداف عديدة، أهمها: تعطيل خدمات البنية التحتية للخصم ، وتدمير البيانات أو التلاعب بها، التجسس الرقمي وسرقة المعلومات. العمليات السيبرانية الدفاعية (Defensive Cyber Operations – DCO) ويقصد بها الامن السيبراني وتُركز على حماية الأنظمة والشبكات من التهديدات السيبرانية مثل إدارة ومعالجة الثغرات الأمنية ، كشف الهجمات ومنعها ، تصحيح الأنظمة، ويتضمن هاذين النوعين من عمليات أخرى كالعمليات الاستطلاعية والاستراتيجية والحركية لكشف عمليات التجسس

1– قراصنة يخترقون جسر «بلوك شاين» ويسطون على 100 مليون دولار من شركة عملات مشفرة، متوافر على الموقع الالكتروني، https://aja.me/bc98ib، تاريخ الزيارة 20-7-2024.

2 – العمليات السيبرانية أثناء النزاعات المسلحة، متوافر على الموقع الالكتروني، https://www.icrc.org/ar/law-and-policy/cyber-operations-and-information، تاريخ الزيارة 24-11-2025.

وجمع المعلومات الاستخباراتية ولكن كلها تندرج ضمن النطاق والهجومي والدفاعي . وتستخدمها الشركات الكبرى، والدّول، والاحلاف العسكريّة الدوليّة كالنّاتو، وبعض المجموعات الإرهابيّة او مجموعات القراصنة والافراد وتعتمد على مجموعة من الأسلحة السيبرانية او الأدوات والتّقنيّات المفصّلة في الجدول أدناه:

أدوات العمليات السيبرانية الهجومية والدفاعية[2]	
أدوات العمليات السيبرانية الهجومية Offensive cyber operations Tools	**أدوات العمليات السيبرانية الدفاعية** Defensive Cyber Operations Tools
برامج خبيثة Malware	نظام كشف التسلل Intrusion Detection System (IDS)
التصيّد الاحتيالي Phishing	نظام منع الاختراق Intrusion Prevention System (IPS)
هجمات حجب الخدمة /DoS DdoS	استخبارات التهديد Threat Intelligence
الهجمات المستمرة المتقدمة Advanced Persistent Threats	إدارة المعلومات الأمنية والأحداث Security Information and Event Management (SIEM)
حقن استعلام البيانات SQL Injection	الاستجابة للحوادث الامنية Incident Response (IR)
الرجل في الوسط Man-in-the-Middle (MitM)	منع تسرب البيانات Data Loss Prevention (DLP)
الهندسة الاجتماعية Social Engineering.	جدران الحماية (Firewalls)

2-خصائص العمليات السيبرانية: تتمتع العمليات السيبرانية الهجومية بخصائص لا تتميّز فيها العمليات العسكرية التقليدية، بحيث لا تستخدم أسلحة مادية مثل القنابل، والصواريخ، والدبابات، والجنود لتحقيق أهدافها. تستخدام أدوات وأكواد رقمية صامتة مثل البرمجيات الخبيثة، والفيروسات، من دون أصوات أو إراقة دماء، لكنها تتصف بالإنكار والجحود والغموض. لذلك سنسلط الضوء على بعض الخصائص الرئيسية للعمليات السيبرانية:[1]

التعقيد التقني Technical complexity:
من أسس العمليات السيبرانية الهجومية أن تكون معقّده بقدر تعقيد الخصم أو الهدف وربما أكثر حتى لا يتم فهمها أو التعامل معها بسرعة، حيث يستخدم المهاجمون أدوات وتقنيات متقدمة لتنفيذ الهجمات

1 – Jason Andress and Steve Winterfeld, Cyber Warfare. Techniques, Tactics and Tools for Security Practitioners, Syngress, second edition, 2014, p.p. 103-193.

تتطلب فهمًا عميقاً للأنظمة والشبكات المستهدفة.

الخفاء والتخفيSteganography and Stealth : من سمات الهجمات السيبرانية الأساسية تخفي وجودها، مما يجعل اكتشافها صعبًا. تم تصميم العديد من الهجمات الإلكترونية بحيث لا يمكن اكتشافها، مما يسمح للمهاجمين بالتسلل إلى الأنظمة وجمع المعلومات أو التسبب في أضرار دون أن يلاحظهم أحد، وغالبًا ما تظل غير مكتشفة لمدة طويلة، ويستخدم المهاجمون تقنيات مثل الجذور الخفية (Rootkits) والتشفير لإخفاء نشاطهم.

صعوبة الإسناد Difficulty in Attribution: إنّ التعقيدات التي تتمتع والخفاء بها العمليات السيبرانية وذلك نظرًا لاستخدام المهاجمين تقنيات التشفير وتقنيات التعتيم الأخرى، يكون من الصعب إسناد الهجمات السيبرانية إلى أفراد أو مجموعات محددة، مما يعقد جهود الاستجابة ويؤدي إلى تآكل الثقة بين الدول.

الاستهداف الانتقائي والتنوع Selective targeting and diversity: عند فحص الثغرات وتحديد نقاط الضعف يصادف المهاجمون أهدافا جديدة وسهلة الاستغلال، فتتغير استراتيجية فقد تكون الهجمات السيبرانية مستهدفة بشكل محدد أو عشوائي على أهداف معينة مثل الشركات أو الحكومات، بينما يمكن أن تصيب الهجمات العشوائية أي نظام ضعيف. فهي واسعة من الأساليب، من الفيروسات والديدان إلى الهجمات المعقدة مثل هجمات الرّجل في المنتصف وهجمات حجب الخدمة.

السرعة العالية: العمليات السيبرانية عبارة عن برامج وأكواد تنطلق بالفضاء محددة تتكيف مع سرعة الإنترنت، وهي تحدث بسرعة كبيرة، مما يسمح للمهاجمين بتنفيذ أهدافهم قبل اكتشاف الهجوم أو الاستجابة له.

العالمية Internationality: المهاجمون والعمليات السيبرانية ليست مقيدة بموقع جغرافي معين، يمكن للمهاجمين استهداف أنظمة في أي مكان في العالم مما يعزز تعقيد الدّفاعات المطلوبة للحماية ويعيق تحديد الهدف والاسناد.

التكلفة المنخفضة Low Cost: العمليات السيبرانية منخفضة التكلفة مقارنة بالأدوات التقليدية، فأحيانا تكون من تصرف فردي أو من جماعة يتخطى تطويرها الأسلحة المعروفة لأنها مفتوحة المصدر (open

resource –Lunix–kali). وتتوفر معظم الأدوات والتقنيات لتنفيذ الهجمات متاحة بسهولة على الإنترنت، فالعديد من الافراد العاديين أو المتدربين يمكنهم تحميل العديد من الأدوات ويقوموا بتجارب بدائية ويكون لها آثار واسعة.

الاستمرار Persistence: يمكن للعمليات السيبرانية المتقدمة أن تحافظ على وجودها في النظام المستهدف لمدّة طويلة، مما يسمح للمهاجم بجمع المعلومات أو تعطيل العمليات أو استخراج البيانات بمرور الوقت.

3–نطاق العمليات السيبرانية: العمليات السّيبرانية الهجومية لا تلتزم في نطاق جغرافي معيّن، فهي تستهدف أنظمة المعلومات، والبنية التّحتيّة وشبكات الكمبيوتر العالميّة والمحلّيّة، والبنية التحتية المدنية والعسكرية، وكل ألاصول ذات الوجه الرقمي. فهي عابرة للحدود وتتميز بالتأثير الواسع (Widespread impact)، لتميّزها بالمرونة على استهداف أيّ جهاز متّصل على شبكة الإنترنت ، حتى أصبحت تشكل خطرا على ، الاقتصاد، والأمن الوطني، وحتى الحياة اليومية للأفراد. على المستوى المحلي تستهدف أفراد أو منظمات أو بنية أساسية محددة داخل منطقة أو مدينة معينة، وعلى المستوى الدولي فهي واسعة النطاق تصل إلى شبكات بلدان متعددة وكيانات عالمية، مثل هجوم ببرامج الفدية الذي استغل مئات الآلاف من أجهزة الكمبيوتر في أكثر من 150 دولة، وأدّى إلى تعطيل مراكز الرّعاية الصّحيّة وغيرها من الخدمات. وفي هذا السياق، نشير إلى أنّ المهاجمين لا يهمهم القطاع أكثر ما يهمهم وجود الثّغرات والهجوم عليها واستغلالها ، وإنّ أغلب الدول التي تعتمد على التكنولوجيا في قطاعاتها هي الأكثر عرضة للعمليات السيبرانية الهجومية. وأهم القطاعات التي تأثرت بهجمات سيبرانية على مرّ عقدين:

– الخدمات الحكوميّة للدول: هي الأكثر استهدافًا خاصّة القطاعات المالية والأنظمة العسكرية والمؤسسات السّياسية، بما في ذلك الشركات المشغلة لهذه القطاعات وأبرز الأمثلة هجوم SolarWinds في 2020 إبان الانتخابات الأمريكية الذي استهدف سلسلة التوريد ممّا أدّى إلى اختراق

شبكات حكومية أمريكية بما في ذلك وزارة الخزانة ووزارة التجارة،[1] وهجوم OPM في الولايات المتحدة أدّى إلى سرقة بيانات شخصيّة حساسة لما يقرب من 22 مليون موظف حالي وسابق.[2]

-القطاعات الماليّة: هذا القطاع هو الأكثر استهدافا بعد القطاعات الحكومية ويهاجم من قبل جميع أنواع المخترقين لأسباب ماليّة، مثل استهداف البنوك والمؤسسات المالية وأنظمة الدفع، بهدف الاحتيال أو سرقة الأموال أو تعطيل الاستقرار المالي والاقتصادي. وأبرز الأمثلة الهجوم العالمي على النظام البنكي عام SWIFT 2015، مما أدّى إلى سرقة 81 مليون دولار من بنك بنغلاديش المركزي.[3]

-القطاعات الخاصة والشركات: يعتبر هذا القطاع مستنقعا مهما للمهاجمين خاصّة على المؤسسات الصناعية لسرقة الملكية الفكرية أو الأسرار التّجاريّة وأبرزها هجوم كبير على شركة Sony Pictures مما أدى إلى تسريب بيانات حساسة وأفلام لم تُصدر بعد ومعلومات شخصية عن الموظفين.[4]

-مراكز الرعاية الصحية: عادة تستهدف المستشفيات ومؤسسات البحث الطبي والرعاية الصحية، بهدف سرقة المعلومات الصحية الشخصية أو تعطيل الخدمات، مثل هجوم WannaCry Ransomware (2017) أدّى إلى تعطيل الرعاية الصحية وغيرها من الخدمات في بريطانيا وعلى الخدمات

1 - SEC sues SolarWinds over massive cyberattack, alleging fraud and weak controls, Available on internet,https://www.cnbc.com/2023/10/31/solar-winds-defrauded-investors-about-cybersecurity-sec-alleges.html, visited on 22-7-2024.

2 - US OPM Hack Exposes Data of 4 Million Federal Employees, Available on internet,https://www.trendmicro.com/vinfo/de/security/news/cyber-attacks/us-opm-hack-exposes-data-of-4-million-federal-employees, visited on 22-7-2024.

3 - Exclusive - SWIFT confirms new cyber thefts, hacking tactics, Available on internet,https://www.reuters.com/article/world/exclusive-swift-confirms-new-cyber-thefts-hacking-tactics-idUSKBN1412NS, visited on 22-7-2024.

4 - The Hack of Sony Pictures-What We Know and What You Need to Know ,Available on internet,https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/the-hack-of-sony-pictures-what-you-need-to-know, visited on 22-7-2024.

الصحية الوطنية (NHS). واختراق شركة التأمين الصحي Anthem لهجوم سيبراني أدّى إلى سرقة بيانات شخصية لحوالي 78.8 مليون شخص.[1]

– البنية الأساسية الحرجة: استهداف الخدمات الأساسية مثل شبكات الطاقة وأنظمة إمدادات المياه وشبكات النقل والاتصالات، أهمها الهجوم العربي (أوب إسرائيل) على محطّة تحلية المياه الإسرائيلية، وهجوم Stuxnet الشهير على منشآت إيران النووية،[2] مما أدى إلى تعطيل أجهزة الطرد المركزي المستخدمة في تخصيب اليورانيوم، هجوم على شبكة الطاقة الأوكرانية عام 2015 أدى إلى انقطاع التيار الكهربائي عن أكثر من 225,000 شخص في أوكرانيا.

– القطاع التعليمي: تتعرض الجامعات والمؤسّسات التّعليميّة لهجمات عديدة بهدف سرقة بيانات البحث أو تعطيل العمليات أو الوصول إلى المعلومات الشخصية للطلاب والموظفين أو التزوير وعادة تكون من المبتدئين والقراصنة، وأبرزها الهجوم على جامعة Maryland أدى إلى سرقة معلومات شخصية لأكثر من 300,000 طالب وموظف سابق. وهجوم ransomware على جامعة San Francisco،California في عام 2020 وتم دفع 1.14 مليون دولار للفدية لاستعادة الوصول إلى بيانات البحث الحساسة.[3]

– الهجمات على الأفراد: تطال الهجمات السيبرانية الافراد العاديّين لاستغلالهم وارتكاب جرائم بحقّهم واقتحام خصوصيّتهم مثل سرقة الهوية عبر التصيد الاحتيالي(Phishing)، والبرمجيات الخبيثة(Malware) ، وبرمجيات الفدية(Ransomware) وإجبارهم على الدفع مقابل استرجاع البيانات.

3. المبحث الثاني: أثر العمليّات السيبرانيّة على السيّادة السيبرانيّة

في ظل تصاعد العمليات السيبرانية في

1 – What was the WannaCry ransomware attack?, Available on internet,https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/,visited on 22-7-2024.

2 – Stuxnet explained- The first known cyberweapon, Available on internet,https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html,visited on 22-7-2024.

3- University of Maryland CISSM Cyber Attacks Database, Available on internet, hhttps://cissm.liquifiedapps.com/,visited on 22-7-2024.

الفضاء السيبراني، أصبحت العمليّات السيبرانيّة أحد التحديات الناشئة في العالم الرقمي، وخاصة على السيادة السيبرانية والعلاقات الدولية بسبب الانتهاكات التي تحدثها في العالم الواقعي على الأصول والخدمات الرقمية، وتهديد الامن القومي وزعزعة السلم والامن الدوليين، مما جعلها إحدى الاهتمامات الدولية بعد تداخلها في سياق صناعات الذكاء الاصطناعي ، لذلك سنتناول البعد القانوني والسياسي من خلال مطلبين، في الأول يناقش العمليات السيبرانية وانتهاك السيادة، بينما في الثاني سنحاول ان نظهّر استراتيجيات الدول لحماية سيادتها الرقمية ومواجهة العمليات السيبرانية.

1.3العمليّات السيبرانيّة وانتهاك السّيادة

هناك اتفاق متزايد بين الخبراء بأن العمليات السيبرانية تُعتبر انتهاكًا للسيادة، لكن ذلك يعتمد على طبيعة الهجمات وسياقها في إحداث الضرر في إختراق الأنظمة الحكومية، أو كيفية التدخل في الشؤون الداخلية، واستهداف البنية التحتية الحيوية، إلى جانب الاضرار بخدمات الاقتصاد الرقمي الدولي والمحلي. لذلك سنتناول في هذا المطلب أثر العمليات السيبرانية على أبعاد السيادة السيبرانية في الشق القانوني، وتقديم دراسة حالتين تبيّن أثر العمليات السيبرانية على السيادة السيبرانية والاستقرار السياسي.

1.البعد القانوني للسيادة في ظل العمليات السيبرانية:

العمليات السيبرانية تُعَدّ تحدياً كبيراً لسيادة الدول، خاصةً في سياق مبدأي عدم التدخل واستخدام القوة، هذان المبدآن يمثلان حجر الزاوية في العلاقات الدولية، ويشكلان أساساً للمبادئ القانونية والسياسية التي تحكم سلوك الدول في الساحة العالمية، وفقا للقانون الدولي والمواثيق الدولية، لا يجوز للدولة أن تجري عمليات سيبرانية تنتهك سيادة دولة أخرى، ولكن يمكنها قانونيا الرد بموجب ممارسة حق الدفاع عن النفس وتنطبق هذه القاعدة على العلاقات بين الدول، والإجراءات التي تتخذها الدول لا تشمل تصرفات الجهات الفاعلة غير الحكومية ما لم تكن هذه التصرفات منسوبة إلى دولة، لأن الدولة هي الشخصية القانونية الملزمة في ذلك. يقدم دليل تالين وهو كتاب رائد في العمليات السيبرانية، قواعد غير ملزمة حول السيادة والعمليات التي تنتهك السيادة، وقامت مجموعة الخبراء الدولية بتقييم شرعية العمليات السيبرانية

على قاعدتين مختلفين:

درجة التعدي على سلامة أراضي الدولة المستهدفة.

ما إذا كان هناك تدخل أو انتهاك لوظائف حكومية جوهرية.

الأولى تنطلق من فرضية مفادها أن الدولة تتحكم في الوصول إلى أراضيها السيادية، والثاني تنطلق من الحق السيادي للدولة في ممارسة وظائف الدولة داخل أراضيها. والقاعدة الأولى يتم تقيمها على ثلاثة مؤشرات: الضرر المادي، فقدان الوظيفة، والتعدي على سلامة الأراضي التي وقع فيها فقدان الوظيفة. لذلك أي عملية سيبرانية تؤدي الى ضرر مادي باي شكل من الاشكال فهي انتهاكا للسيادة مما يتناقض مع قدسية مبدأ السيادة، الذي يحمي بوضوح سلامة الأراضي من الانتهاك المادي. وأن مثل هذه العمليات قد تشكل أيضًا تدخلاً محظوراً، أو استخدامًا غير قانوني للقوة، أو هجومًا مسلحاً. وكما أقروا بالإضافة إلى الضرر المادي، فإن التسبب عن بعد في فقدان وظائف البنية الأساسية السيبرانية الموجودة في دولة أخرى يشكل في بعض الأحيان انتهاكاً للسيادة، على سبيل المثال، وبافتراض أن المسؤولية تقع على عاتق دولة، فإن فيروس شمعون الذي تطلب إصلاح أو استبدال آلاف الأقراص الصلبة لشركة النفط السعودية أرامكو في عام 2012 يشكل انتهاكاً لسيادة الدولة لأنه أدى الى فقدان وظائف المعدات أو العناصر المادية الأخرى التي تعتمد على البنية الأساسية المستهدفة من أجل التشغيل.

–البعد الخارجي للسيادة في سياق العمليات السيبرانية: البعد الخارجي للسيادة قائم على مبدأ المساواة وعدم التدخل، ومبدأ عدم التدخل هما مبدأ عدم اللجوء للقوة ومبدأ عدم التدخل في الشؤون الداخلية، ولكن يوفر الفضاء الإلكتروني للدول فرصاً للتدخل في الشؤون الداخلية أو الخارجية لدول أخرى، بسبب الترابط العالمي المتزايد والاعتماد المتزايد للدول على تكنولوجيا المعلومات. ولكن تحظر هذه قواعد في القانون الدولي التدخل باستخدام القوة بما في ذلك بالوسائل السيبرانية من قبل دولة واحدة في الشؤون الداخلية أو الخارجية لدولة أخرى، مستندة إلى مبدأ السيادة في القانون الدولي الذي ينص على المساواة السيادية للدول. ومبدأ الامتناع عن استخدام القوة أو التهديد باستخدام القوة،

تنص الفقرة 4 من المادة 2 من ميثاق الأمم المتحدة بامتناع أعضاء الجماعة الدولية جميعا في علاقاتهم الدولية عن التهديد باستعمال القوة، أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه أخر لا يتفق ومقاصد الأمم المتحدة.[1]

-مبدأ عدم التدخل: يتعرض مبدأ عدم التدخل لتحدي متزايد بسبب طبيعة العمليات السيبرانية، والتي يمكن أن تؤثر بشكل مباشر على الشؤون الداخلية للدول بطرق لا تستطيع أشكال التدخل التقليدية أن تفعلها، فمن خلال العمليات السيبرانية تتدخل الدول رقميّا في شؤون بعضها بين الدول القوة والضعيفة مثل روسيا واكرانيا وإستونيا دون الصراع او الاستخدام العسكري، وأيضا تحدث بين دول ذات عداء تاريخي طويل مثل روسيا والصين وامريكا، وتكون التدخلات مثل الحروب الباردة، فكل طرف يشن عمليات سيبرانية متعددة الاهداف تستهدف فيها الأنظمة الحكومية أو السياسية لدولة أو البنية التحتية أو الاستقرار الاجتماعي مثل التأثير على الانتخابات. على سبيل المثال الهجمات الروسية التي طالت الانتخابات البريطانية 2016، والامريكية في خريف2021 تزامنا مع انتخابات الرئاسية الامريكية، ووصفها آنذاك وزير الخارجية الامريكية بومبيو بأنه اجتياح رقمي على السيادة الامريكية، وردت كل من بريطانيا وامريكا على الانتخابات الروسية الأخيرة 2024 بعدد كبير من العمليات السيبرانية على نظام التصويت، وكان مصدره أميركا وبريطانيا، وأكدّ كوفاليف «هذه ليست المرة الأولى التي نسجل فيها هجمات على نظامنا... نرى أن معظم الخوادم التي تأتي منها الهجمات، تقع في الولايات المتحدة الأميركية والمملكة المتحدة.[2]

وتؤكد القواعد الدولية، أنّ أي تدخل من قبل أي دولة بوسائل إلكترونية في «الشؤون الداخلية أو الخارجية» لدولة أخرى يعتَبر انتهاكًا لمبدأ عدم التدخل وبالتالي على السيادة الوطنية،[3] وبالتأكيد سيكون له تداعيات على العلاقات الدولية بردود دبلوماسية ضد الدولة

1- يحي ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية، https://jlaw.journals.ekb.eg/article_45192_52d735c1a23cca2bf7dbbe56c4eb6846.pdf، متوفر بتاريخ 2/08/2024.

2 - روسيا: أكبر عدد هجمات سيبرانية على نظام التصويت جاء من أميركا وبريطانيا، متوافر على الموقع الالكتروني، https://tv.ara/wku28، تاريخ الزيارة 2024-108.

3 - مصدر سبق ذكرة

أو الكيان الذي قام بالهجوم، وقد تتخذ إجراءات دبلوماسية أو حتى عقوبات ضد الجهة المسؤولة وتهديدات امنية قد يؤدي إلى تصعيد النزاعات ويعزز من التوترات وتآكل الثقة بين الدول خاصة ان مسالة الاسناد للجهة المهاجمة لم يتم حسمها بعد مما يزيد من وتيرة التوترات بشكل أوسع.

-مبدأ استخدام القوة: السياق التقليدي يخضع مبدأ استخدام القوة في القانون الدولي في المقام الأول لميثاق الأمم المتحدة، الى تقييد استخدام القوة بالدفاع عن النفس أو الإجراءات التي أقرها مجلس الأمن التابع للأمم المتحدة.[1] وفي سياق العمليات السيبرانية، يواجه هذا المبدأ تعقيدات وتفسيرات جديدة بسبب الطبيعة الفريدة للصراعات والهجمات السيبرانية، لأن يمكن أن تتسبب العمليات السيبرانية أضرار مادية أو أذى اقتصادي أو تعطيل للبنية التحتية الحيوية تلزم تطبيق القواعد الدولية عليها كما أشرنا اليها سابقا.

1 - وفقًا للمادة 2(4) من ميثاق الأمم المتحدة، يُحظر على الدول استخدام القوة أو التهديد باستخدامها ضد سلامة أراضي أي دولة أو استقلالها السياسي. وتشمل الاستثناءات من ذلك استخدام القوة للدفاع عن النفس (المادة 51) أو الإجراءات التي أذن بها مجلس الأمن التابع للأمم المتحدة بموجب الفصل السابع من الميثاق.

-العمليات السيبرانية وعتبة القوّة: لا شك أنّ القوة السيبرانية مرتبطة بالعمليات السيبرانية وساهمت الى حد ما بتشكيل القوة السيبرانية وممارسة النفوذ، وتحقيق التفوق والتنافس الدولي. ولكن لهذه القوة عتبة، فلولا وجود الشبكات والانترنت ما وجدت، واذا تعطلت الكهرباء لم تعد شيئا وتتقوقع داخليا ولا تتخطى حدودها، لذلك هي تعمل ضمن اطارها ونطاقها، نعم لها جميع اوجه القوة التقليدية ولكنها ليست قوة بالمعنى المادي قادرة على أن تحل مكان قوة الردع التقليدية، ولكن من خلال شبكة الانترنت قادرة على ان تهدد استثمارات الدول الرقمية كالبيانات الضخمة و والذكاء الاصطناعي والتجارة الدولية وكل تقنية مرتبطة بالإنترنت محليا ودوليا، على سبيل المثال لو كانت الدبابات والاليات العسكرية تعمل على أنظمة سيارات تسلا فان القوة السيبرانية ستحل مكان القوة التقليدية. لذلك هي قوه لها عتبة على الرغم من الضرر المادي الذي تحدثه، ولكن التحدي هو تحديد متى تصل العملية السيبرانية إلى عتبة «الهجوم المسلح» الذي يبرر الاستجابة العسكرية التقليدية. وهذا ينطوي على تقييم شدة الهجوم، مثل ما إذا كان يتسبب في أضرار مادية كبيرة أو إصابات، وما إذا

كان يفي بعتبة الهجوم المسلح بموجب المادة 51 من ميثاق الأمم المتحدة، مما يثير تساؤلات حول ما إذا كان يشكل استخدامًا للقوة.

1-عمليات سيبرانية ذات ابعاد سياسية: العلميات السيبرانية التي تعتبر انتهاكًا للسيادة، هي تلك التي تؤثر بشكل مباشر أو غير مباشر على سيادة دولة ما، سواء من خلال استهداف البنية التحتية الحيوية (استهداف شبكات الطاقة أو الصحة)، أو التدخل في العمليات السياسية (التدخلات الانتخابية أو التجسس السياسي). على سبيل المثال لا الحصر:

أ-العمليات السيبرانية على البنية التحتية الحيوية:

العملية الروسية على شبكة الكهرباء في أوكرانيا عام 2015 الذي تسبب في انقطاع الكهرباء عن مئات الآلاف، والعملية الإسرائيلية 2010على منشآت أيرن النووية Stuxnetفي منشأة طنز وتسببت في تعطيل ما يقارب 1,000 جهاز طرد مركزي.

ب-التدخل في العمليات الانتخابية: التدخل الروسي في انتخابات الولايات المتحدة عام، 2016، 2020، 2024 واختراق قواعد بيانات للحزب الديمقراطي والجمهوري ونشر محتوى تضليلي.

د-عمليات التجسس السيبراني الروسي: على أنظمة SolarWinds التي استهدفت الوكالات الحكومية الأمريكية في 2020، لزعزعة الاستقرار السياسي التي ترافقت مع الانتخابات الامريكية.

هـ-عمليات تسبب ضررًا اقتصاديًا: الهجوم فيروس الفدية WannaCryعام 2017 الذي أثر على قطاعات متعددة بريطانيا والعالم.

وهناك هجمات تكون شديدة الأضرار ناتجة عن العمليات السيبرانية الهجومية تعتبر انتهاك للقانون الدولي والدولي الإنساني والسيادة السيبرانية وتهديدا للسلم والامن الدوليين على سبيل المثال عمليات تفجير البيجر في لبنان.

أ-دراسة حالة: العمليات السيبرانية على البنية التحتية الحيوية

2-عمليات سيبرانية ضد إستونيا 2007: سببّ نقل تمثال يخلد تضحيات جنود روس في الحرب العالمية الثانية، في عام 2007، شنت روسيا هجمات سيبرانية شاملة على إستونيا إثر نقل تمثال لجنود روس من الحرب العالمية

الثانية. الهجمات كانت من نوع «حجب الخدمة الموزعة (DDoS) ». واستهدفت مواقع حكومية وإعلامية، مما عرقل ولوج المواطنين إلى الخدمات البنكية والإلكترونية لعدة أيام، وأدى إلى شلل في البنية التحتية الرقمية لإستونيا. كانت الهجمات على مرحلتين:

- المرحلة الأولى 29-27 -نيسان-2007: كانت بسيطة وشعبية، بحيث بدأت الهجمات باستهداف المواقع الإلكترونية الحومية والاعلامية التي بثت أخبار عن حزب الإصلاح في إستونيا بنشر اعتذار رسمي مزور باللغة الروسية عن نقل التمثال والذي يبدو وكأنه صادر من رئيس الوزراء الأسيتونى.

- المرحلة الثانية من 30 نيسان إلى 18-2007: كانت أكثر تعقيداً باستخدام «Botnets» واستهدفت البنوك والبنية التحتية للإنترنت، ولقد فاق عدد طلبات الدخول الى هذه المواقع 400 ضعف المستوى الطبيعي.[1]

في المرحلتين الأثر كان معنوياً أكثر منه مادياً إذ لم ينتج عن الهجوم أي أثر تدميري على البنية التحتية الإلكترونية لإستونيا، إلا أنها سلطت الضوء على خطورة التهديدات الإلكترونية، ولا يرتقي الى حرب سيبرانية فهو أقرب الى نزاع او صراع سيبراني يؤدي الى توترات بين البلدين.

ب-دراسة حالة: التأثير السياسي للعمليات السيبرانية

-التأثير على نتائج الانتخابات الأمريكية: جاء هذا التدخل الروسي في الانتخابات الرئاسية الأمريكية 2016 عندما دعمت هيلاري كلينتون الاحتجاجات التي تلت الانتخابات الروسية في مارس 2012، مما أدى إلى احتجاجات ومعارضة داخلية وقمع من السلطات الروسية. رأت روسيا في دعم كلينتون لهذه الاحتجاجات محاولة لزعزعة الاستقرار السياسي في البلاد. في 2015، تم الكشف عن استخدام كلينتون لبريد إلكتروني خاص بدلاً من البريد الرسمي. استغلت روسيا هذه القضية وانتقمت من كلينتون عبر قرصنة ونشر رسائلها الإلكترونية للتشكيك في نزاهة الانتخابات الأمريكية، والتأثير على نتائجها لصالح دونالد ترامب. جاء

1- Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective, available on internet,https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf, visited 28-9-2024.

التدخل الروسي ضمن أنشطة متنوعة تهدف إلى التأثير على نتائج الانتخابات وتوجيه الرأي العام الأمريكي، وقد أثار جدلاً واسعاً وأدى إلى تحقيقات موسعة داخل الولايات المتحدة. واستخدمت روسيا قدراتها السيبرانية:

– حملات التضليل عبر وسائل التواصل الاجتماعي (Phishing& impersonation attack): استخدمت روسيا وسائل التواصل الاجتماعي لنشر معلومات مضللة ومحتويات مثيرة للانقسام بهدف زعزعة الثقة في العملية الديمقراطية الأمريكية، عملت مجموعات مثل «وكالة أبحاث الإنترنت(IRA)» الروسية على إنشاء حسابات مزيفة تهدف إلى التأثير على الناخبين ونشر الأخبار الكاذبة المؤيدة والمعادية وركزت هذه الحسابات على إثارة التوترات العرقية والدينية، ودعم دونالد ترامب والهجوم على هيلاري كلينتون.

– اختراق وتسريب البيانات (SQL Injection Attack) اخترق قراصنة روس شبكات الحزب الديمقراطي، بما في ذلك اللجنة الوطنية الديمقراطية(DNC) وحملة هيلاري كلينتون الرئاسية. ثم قاموا بتسريب هذه المعلومات عبر منصات مثل «ويكيليكس»، مما أضر بصورة الحزب الديمقراطي والمرشحة هيلاري كلينتون.

– الهجمات السيبرانية على البنية التحتية الانتخابية: حاولت جهات روسية اختراق أنظمة التصويت في بعض الولايات الأمريكية. فقد استخدم ضباط المخابرات العسكرية الروسية أيضًا رسائل بريد إلكتروني ضارة للوصول إلى شبكة كمبيوتر لجنة الحملة الانتخابية الديمقراطية في الكونجرس، قام المتسللون بتثبيت برامج ضارة سمحت لهم بالوصول إلى المزيد من أجهزة الكمبيوتر وسرقة آلاف رسائل البريد الإلكتروني والوثائق المتعلقة بالانتخابات. هذه المحاولات أثارت قلقاً كبيراً بشأن سلامة أنظمة التصويت وشفافية العملية الانتخابية.[1]

–الأهداف الروسية من التدخل: إضعاف الثقة في الديمقراطية الأمريكية وتقويض النظام الديمقراطي الأمريكي وإظهاره بمظهر غير مستقر. دعم مرشح مفضل (دونالد ترامب) بالاعتقاد أن ترامب يمكن أن يتبنى سياسات أكثر مرونة تجاه روسيا. والتأثير على السياسة الخارجية

1 – Hacking the Democratic National Committee, Available on internet, https://time.com/5565991/russia-influence-2016-election/ , visited 19-10-2024.

الأمريكية خصوصاً فيما يتعلق بالعلاقات بين البلدين وتخفيف العقوبات المفروضة على موسكو بعد ضمها شبه جزيرة القرم في 2014.[1]

2.3 المطلب الثاني: استراتيجيات الدول لحماية سيادتها الرّقمية

إنّ تعاظم العمليات السيبرانية أصبح ظاهرة مقلقة على مستوى العالم، ولا بدّ من تبني نهج متعدد الأبعاد في السياسات الامنية والتشريعات التي تركز على خفض حدة العلميات السيبرانية، فالمطلوب من الدول تحسين برامج الأمن السيبراني بأفضل الممارسات والمعايير الدولية في حماية البنية التحتية الحيوية، وتعزيز قدرة الدول على التحكم في بنيتها التحتية الإلكترونية ومنع انتهاك سيادتها، فإلى جانب بناء الاستراتيجيات السيبرانية ينبغي إبرام اتفاقيات دولية في مجال الأمن السيبراني الدفاعية لعزز التعاون الدولي لمواجهة الأنشطة السيبرانية العابرة للحدود، وتطوير أطر قانونية قوية تتماشى مع القانون الدولي وحقوق الإنسان وتضمن العلاقات وتعيد الثقة بين الدول على مبدا ويستفاليا ، لأن الفضاء السيبراني أخذاً بالتوسع والامتداد الى كل أركان الأصول البشرية، وعليه سنقترح مبادئ بناء استراتيجية أمن سيبراني تحمي البنية التحتية وتحمي سيادة الدول من الانتهاكات، وقيام ويستفاليا رقمي ينظّم العلاقات السيبرانية بين الدول .

1.تبني الدول استراتيجيات للأمن السيبراني : بعد أن اصبح الفضاء السيبراني مجالا فريدا للتهديدات السيبرانية ويؤثر على سيادة ومصالح الدول واستقرار العلاقات الدولية، فلن يكون كافيا أن تقوم الدول بإصلاح ثغراتها بنفسها او تسن قوانين وتشريعات رادعه تختلف بين دولة وأخرى، فلا بدّ من بناء استراتيجية للأمن السيبراني موحدة على صعيد دولي توّحد الجهود والتعاون بين الدول من أجل إرساء فضاء سيبراني آمن وتوفير بيئة سيبرانيّة مستقرة، مما يعزز الثقة بين الدول، ويدعم التجارة الدولية، ويحمي البنيّة التحتيّة الحيويّة وتمهّد الطريق لنظام عالمي يعتمد على التعاون في مواجهة التهديدات المشتركة بدلًا من التنافس.

1 - The Perfect Weapon: How Russian Cyberpower Invaded the U.S ,Available on internet , https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html , visited 19-10-2024.

ولإنجاح أي استراتيجية على صعيد محلي او دولي ينبغي إتباع منهج أو إطار مرن يساعد الدول في تنظيم الجهود وتحقيق الأمن السيبراني بشكل منهجي وشامل، ليكون أداة استراتيجية تدعم الدول والمؤسسات الدولية والشركات في مواجهة التهديدات السيبرانية المتزايدة، ترتكز على العديد من الجوانب تتضمنها أطر سيبرانيّة مبنيّة على تحليل البيئة الدولية وفهم المصالح الدوليّة، والاستفادة من الفرص المتاحة واستغلالها في خدمة الاستراتيجية، وتقييم المخاطر الناتجة عن الثغرات ومواطن الضعف، والبحث عن وسائل القوة الدولية المتوافرة بيد الدول والمؤسسات الدولية، واستخدامها في طُرق بناء الاستراتيجية لتحقيق الأهداف المنشودة. وعليه، لا بدّ من تعزيز التعاون الدولي وإنشاء آليات فعّالة لتبادل المعلومات الاستخباراتيّة حول التهديدات السيبرانيّة بين الدول، وتطوير معايير وبروتوكولات دولية موحّدة للأمن السيبراني تُفرض على جميع الدول، وتشكيل فرق استجابة دولية مشتركة للتعامل مع العمليات الهجوميّة. لا بدّ من تطوير القدرات الدفاعية والاستثمار في تقنيات الأمن السيبراني المتقدمّة مثل الذكاء الاصطناعي والتعلّم الآلي والاستفادة منه، والمساهمة في تدريب وتأهيل كوادر متخصصة في مجال الأمن السيبراني على المستوى الوطني والدولي، لتكون قادرة على حماية أمن البنى التحتية الحيوية والشبكات الحكومية. ويجب وضع إطار قانوني دولي لتعديل وصياغة معاهدات واتفاقيات دولية ملزمة لتنظيم الفضاء السيبراني على سبيل المثال وستفاليا رقمي، يساهم في ارساء السلام السيبراني في الفضاء السيبراني، كما يجب ان تتضمن الاستراتيجية تعديلات على بروتكولات القانون الدولي الإنساني وتحديد قواعد الاشتباك في حالة النزاع السيبراني بين الدول، ووضع آليات للمحاسبة ومعاقبة الجهات المتورطة في الهجمات السيبرانية، ووضع خطط طوارئ وطنية ودولية للتعامل مع الأزمات السيبرانية الكبرى. بالإضافة الى اشراك الجمعيّات الغير حكومية الدوليّة على زيادة الوعي والتثقيف الى جانب المناهج الدراسيّة واشراك القطاعين العام والخاص في إطلاق حملات توعية عالمية حول مخاطر الأمن السيبراني وطرق الحماية، وأن تعمل على مخاطر الجريمة السيبرانيّة وتجنّب اثارها خاصةً المؤسسات الماليّة والاقتصاد العالمي. إن تبني استراتيجيّة

أمن دولي شاملة تتضمن هذه الركائز ستساهم بشكل كبير في تعزيز قدرة المجتمع الدولي على مواجهة التحديات السيبرانية المتزايدة وحماية المصالح الحيوية للدول والمنظمات في العصر الرقمي.

2.صياغة وستفاليا رقمية للسيادة: إنّ امتداد مفهوم السيادة نحو السيبرانية وتطور مصالح الدول، أصبحت تؤكد أنّ العالم امتزج في العصر الرقمي ولا يمكن الانسلاخ عنه او العيش بدونه، لم تعد معه فكرة السيادة كما في القرن التاسع عشر، بل تغير مفهومها على نحو أنّ التهديدات التقليدية لم تعد تؤثر على امتداد السيادة الرقمية في الفضاء السيبراني، ونعني بذلك أنّ صارخ أو طائرة F16 لن تكون قادرة على إنزال او تدمير موقع انترنت. فمستقبل السيادة في العصر الرقمي أصبح في مفهوم رمادي في ثلاثة اتجاهات.

–الاتجاه الأول: هناك اتجاه بأن دور السيادة الوطنية تم تقليصه في نطاق العلاقات الدولية المتبادلة بسبب العديد من التطورات والأنشطة السيبرانية والفاعلين واستعمار البيانات.

–الاتجاه الثاني: هناك من يقول ان السيادة الوطنية التقليدية ما زال قائما، ولكنه بفضل التطورات في الفضاء الافتراضي تمددت السيادة وارتكزت على مفهوم الجغرافيا السياسة ومبدأ الحدود الشفافة الذي اثاره كارل هاوسهوفر (1869–1946) عن هيمنة الولايات المتحدة الامريكية كمفهوم جمهورية السيطرة دون الامبراطورية. ثم إحياء الحدود الشفافة في العالم الرقمي كل من «ألكسندر بيلينغتون» (Alexander Beller) و»مانويل كاستيلز» (Manuel Castells). حيث طور كاستيلز، في إطار دراسته حول العولمة والمجتمع الشبكي، فكرة أن الحدود الجغرافية التقليدية بين الدول قد أصبحت أقل أهمية في عصر العولمة بسبب تزايد تأثير التكنولوجيا الرقمية، التجارة العالمية، والأنشطة العابرة للحدود.

–الاتجاه الثالث: وهناك طيف آخر يرى اننا نعيش مرحلة جديدة من مراحل التغيير في هياكل بناء الدولة التقليدية، بحيث في الفضاء السيبراني تلجأ بعض الجماعات ذات القومية والثقافة الواحدة والتي تفتقر الى دولة رسمية تشملهم، يتكتلون بقوى سيبرانية ويمارسون من خلالها نوعا من السيادة الافتراضية، وهو

الأمر الذي ربما يكون له تأثير في اتجاه التأسيس الفعلي لدولتهم، مثل تأسيس الشبكة الكردية لأكراد سوريا، والعراق، وتركيا، وإيران كنوع من الاستقلال الافتراضي[1].

تبعاً لذلك،إنّ مفهوم الأمن والسيادة الوطنية ارتبط منذ القدم بعوامل تقليدية ذات صلة بالجغرافيا وحدود المجالات، وعلى أثره تبلور مفهوم الجغرافيا السياسية، وفي المقابل أدى الاندماج بالشبكة الدولية للاتصالات والمعلومات الى بلورة مفهوم مصطلح –السيادة الرقمية–او السيبرانية كمصطلح يُقصد به حق الدول السيطرة على بياناتها وبيانات مواطنيها وإعادة تدويرها في مجالات اخرى. فسيناريو انحسار السيادة مازال بعيدا، ولكن قد نشهد في السنوات القادمة تراجع سيادة الدول على أراضيها بسبب التحول الرقمي، وحاجات ومصالح الانسان ما زالت تتكتل رقميا وتزداد، فالتهديدات السيبرانية ستزداد وستتركز على مهاجمة النفط الرقمي للدول من بيانات ومعلومات وذكاء اصطناعي، بالإضافة الى الاحتلال الرقمي، واستعمار البيانات، والهيمنة والسيطرة على الذكاء الفريد والقرارات الدولية. فالسيادة القادمة ليس للجغرافيا السياسية بقدر ما ستكون للجغرافيا الافتراضية، وستتحول الأنظمة السياسية القادمة إلى حكومات إلكترونية، فيما يمكن أن يطلق عليه بنهاية السيادة الوطنية وبداية الدولة الكونية الافتراضية أو الرقمية.

من المفيد عند وضع تصورات نحو وستفاليا رقمية، إدراك أهمية قدرات الدول المشاركة، كيف حوّلت أميركا الاقتصاد العالمي إلى سلاح، وكيف حولت تدريجيا الشبكات العالمية لكابلات الألياف الضوئية وأجهزة التوجيه والمفاتيح ومراكز البيانات إلى أدوات للهيمنة. وتقدر شركة أمازون أن نحو 70% من حركة البيانات العالمية، وتدير سويفت منصة التعاملات المصرفية العالمية تمر عبر مراكز البيانات التي تتركز في شمال فيرجينيا.[2] وشركة هواوي والشركات الصينية الأخرى يؤكد على سيادة البيانات مع تمكين التشغيل البيني عبر الحدود بيئية بديلة للأجهزة

1 – أحلام نواري، تراجع السيادة الوطنية في ظل التحولات الدولية، دفاتر السياسة والقانون، العدد الرابع، 2011، ص 42.

2 – The Coming Digital Westphalia, available on internet, https://www.chinausfocus.com/peace-security/the-coming-digital-westphalia, visited 10-12-2024.

والبرامج والمعايير التي تقع خارج نطاق السلطات الأمريكية. وهذا يعطي أولوية للدول القومية في حوكمة وتشغيل أنظمة المعلومات والتكنولوجيا المرتبطة عالميا وإعادة بناء الأنظمة الرقمية، مع السيادة الوطنية كحجر الزاوية للهندسة المعمارية بأكملها، رغم هذا الاحتكار الطبيعي والاستلاء الرقمي. يجب أن تتميز وستفاليا الرقمية بخمسة دعائم رئيسية:

السيادة الرقمية (digital sovereignty): حرية الدول أن تحدد أنظمة حوكمة البيانات الخاصة بها، او إنشاء أنظمة بيئية رقمية تقع وتخضع لحكم حدود وطنية محددة او رقعة معينة مثل الشرق الأوسط، جنوب شرق اسيا، او تكتلات مثل البريكس او الاتحاد الأوروبي لعلها تجمع بين التصورات الغربية والتصورات الصينية الروسية وترسي استقرار في العلاقات الدولية وفضاء آمن.

المصدر المفتوح (Open source): دعم بنية الشريحة مفتوحة المصدر RISC-V، وإصلاح أنظمة المعلومات التي يقوم عليها العالم الرقمي والتخلي عن فكرة النظام الاقطاعي لأنظمة ويندوز وأن تكون الأنظمة شفافة ومتاحة لمجتمع أصحاب الجهات والدول. والتخلي عن استخدام الملكية الفكرية كحواجز أمام المشاركة الاجتماعية في تصميم وتنفيذ وتشغيل أنظمة البيانات، وتكون الأرضية مشتركة من خلال أنظمة التشغيل مفتوحة المصدر Linux، بهدف التوسع السريع والتشغيل البيني مع تطبيقات تم تطويرها على رأس هذه المنصات لتناسب احتياجات الدول ومتطلباتها.

الحقائق الجماعية (Collective truths): كان سائدا أنّ لكل قبيلة أو مجموعة ثقافية تفسيرها الخاص للحقائق. فمن خلال مشروع وستفاليا الرقمية، يمكن للجميع أن يلتقوا في عالم رقمي واحد ويتفقوا على حقائق مشتركة تحافظ على تماسك المجتمع على الإنترنت ويشترك فيها الجميع. وهذا كله يرتبط بمفهوم السيادة الرقمية التي تمنح التحكم في هذه المعلومات للأفراد أو الدول. ويعزز الوحدة والتماسك الاجتماعي وترتيب العلاقات بين الدول.

بيئات البيانات (Data Ecologies): هي عكس استعمار البيانات او الهيمنة على البيانات هو تنظيم البيانات بطريقة تضمن أن المصالح العامة تكون أهم من المصالح الخاصة لبعض الكيانات او الدول بمعنى أي ليس لأغراض ربحية أو لتحقيق مكاسب سياسية على حساب الدول

الاخرى. فاستخدامها فقط لخدمة البشرية في القرارات التي تخدم البشرية.

لذلك سنقترح بعض التصورات حول تحولات السيادة الذي يشهدها العالم، لتنظيمها وفقا لمبادئ وستفاليا وتكون قاعدة مشتركة ومرنة لإرساء سيادة سيبرانية آمنه، وتحفظ المبادئ الأساسية للسيادة الوطنية واحترام الحدود الإلكترونية بين الدول، وضمان تعاون الدول في التصدي للتهديدات السيبرانية العابرة للحدود مثل الهجمات والجرائم السيبرانية، والمشاركة الجماعية في تخزين البيانات وحمايتها، وتمتين العلاقات الرقمية وسد فجوات الثقة التي احدثتها العمليات السيبرانية.

أ-المبادئ العامة:

-تعريف السيادة السيبرانية: التأكيد على تعريف موحد للسيادة السيبرانية، وعلى قدرة الدولة على تنظيم، مراقبة، حماية البيانات، البنية التحتية الرقمية، والأنظمة الإلكترونية والاتصالات في الفضاء السيبراني الخاص بها ضمن حدودها، والقدرة على فرض سلطتها بسن القوانين والسياسات والاستثمارات المتعلقة بالفضاء السيبراني، على الشركات، الأفراد، والكيانات الأجنبية. وضمان حق كل دولة السيطرة على فضائها السيبراني وبياناتها الرقمية داخل حدودها ضمن إطار أبعاد السيادة الداخلي والخارجي.

-المساواة بين الدول في الفضاء السيبراني: اعتبار جميع الدول متساوية في حقوقها وواجباتها الرقمية، وحق الاستثمار، وحماية مصالحها، وأصولها.

-حل النزاعات الرقمية بالطرق السلمية: وضع آليات لحل الخلافات المتعلقة بالأمن السيبراني والجرائم الإلكترونية عبر الوسيلة الدبلوماسية الرقمية.[1]

-احترام الحدود الرقمية: الاعتراف بحدود افتراضية للدول في الفضاء السيبراني، وتحديد السيادة السيبرانية على أساس الحدود الإلكترونية التي تتخطى الحدود الجغرافية، وأن تشمل نطاقات البيانات والتكنولوجيا التي قد تتجاوز هذه الحدود، عبر تقسيم شبكي افتراضي للشبكة العالمية.

-احترام السيادة الوطنية: تسويغ مبدأ عدم التدخل بالوسائل السيبرانية في السيادة السيبرانية للدول الأخرى او عدم التدخل

1 - فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، الجمعية العامة للأمم المتحدة، البند ٩٣ من جدول الأعمال المؤقت، ص18.

في الشؤون الرقمية، والتأكيد أن القوانين والسياسات المتعلقة بالفضاء السيبراني لا تتجاوز حدود الدول أو تتعدى على بيانات ومعلومات مواطنيها دون موافقتهم. احترام حق كل دولة في تحديد سياساتها وقوانينها الخاصة بالإنترنت والتكنولوجيا دون تدخل خارجي.

خاتمة:

سلّطت هذه الدراسة الضوء على العمليات السيبرانية وتأثيرها على تحولات السيادة في الفضاء السيبراني، واجابت على الإشكالية كيف تؤثر العمليات السيبرانية على مفهوم السيادة في الفضاء السيبراني؟، وتمخّض عنها بأنّ العمليات السيبرانية تعتبر تحديًا لمفهوم السيادة السيبرانية في الفضاء السيبراني، وحيث أعادت تشكيل العلاقة بين الدول والفضاء السيبراني بطرق قائمة على وجهات وتناقضات مختلفة بين الدول الكبرى حول سيادة البيانات وحوكمة الانترنت وتدفق البيانات. وأظهرت مدى ضعف الأنظمة السيبرانية أمام العمليات السيبرانية العابرة للحدود، مما أدى إلى تعقيد الجهود المبذولة لحماية البيانات والبنية التحتية الحيوية. وفي هذا السياق، أصبح مفهوم السيادة السيبرانية ضرورة ملحة لتعزيز قدرة الدول على فرض سيطرتها الرقمية ضمن حدودها الافتراضية. ومع ذلك، تثير هذه الجهود تساؤلات حول التوازن بين حماية السيادة الوطنية وضمان انفتاح الإنترنت وحرية المعلومات. وبالتالي، فإن التعامل مع تحديات العمليات السيبرانية يتطلب استراتيجيات دولية متعددة الأطراف لتعزيز الأمن السيبراني والحفاظ على المبادئ الأساسية للفضاء الرقمي من خلال قيام معاهدة دولية أو تطوير وستفاليا ينظم الفضاء السيبراني والعمليات التي تجري من خلاله.

-استنتاجات:

-التكنولوجيا السيبرانيّة بما فيها العمليّات السيبرانيّة أثرت بشكل كبير على السيادة الوطنيّة ولعبت دوراً في تشكيل مفهوم السيّادة السيبرانيّة، ومكّنت بعض الدول لا سيّما الدول ذات الصبّغة السلطويّة والشيوعيّة الحق بإدارة تدفق البيانات، وحوكمة الإنترنت والفضاء السيبراني للتحكم في حدودها الرقمية وإدارة مواردها.

-استخدام العمليّات السيبرانيّة الهجوميّة والدفاعيّة على جانب القوّة السيبرانيّة في الصراعات السيبرانيّة، بحيث تستخدم

الدول العمليات الهجوميّة كأداة صلبة للتأثر على قدرات الخصم، وعمليات كقوة ناعمة لتعزيز صورة الدولة، نشر الثقافة، أو تحقيق أهداف دبلوماسية

-تبيّن أنّ العمليات السيبرانية بتطور متصاعد، وتمادى التأثير الى الأرواح البشرية بشكل مباشر أو غير مباشر، واكدّ ضرورة التعاون الدولي مع الشركات المحوكمة لمعايير التكنولوجيا والانترنت، على ضبط ثغرات تقنيات التكنولوجيا وسلاسل الامدادا والتوريد، وبناء أطر قانونية دولية تنظّم السلوك السيبراني لتخفف من تصعيد العمليات السيبرانية فيالنزاعات والصراعات في الفضاء السيبراني.

-الفضاء السيبراني مجال مرن ويتطور بشكل دراماتيكي، والاحداث فيه بديناميكية دائمة، فالعالم بحاجة الى اتفاقيات دولية تنظم هذ الفضاء حتى لا تمتد صراعات ومخاطر العمليات السيبرانية الى صِدام بين الدول التي لها عداء تقليدي، وخاصة إن الدول مستمرة في رقمنة مصالحها.

-التوصيات:

- ضرورة تبني استراتيجيات للأمن السيبراني تمتثل على أفضل المعايير الدولية وممارسات الامن السيبراني لمواجهة العمليات السيبرانية.

-التعاون دولي أصبح ضرورة ملحة للمجتمع الدولي لوضع أطر قانونية تعزز السيادة السيبرانية وتنظم التفاعلي الدولي مثل قيام وستفاليا رقمي.

قائمة المراجع:

أ-الكتب العربية:

1. أحلام نواري، تراجع السيادة الوطنية في ظل التحولات الدولية، دفاتر السياسة والقانون، العدد الرابع، 2011، ص 42.
2. عادل عبد الصادق، صراع السيادة السيبرانية بين التوجهات الروسية والأمريكية، المركز العربي للفضاء الإلكتروني، 2019.

ب-المواقع العربية:

1. روسيا: أكبر عدد هجمات سيبرانية على نظام التصويت جاء من أميركا وبريطانيا، متوافر على الموقع الالكتروني، https://ara.tv/28wku، تاريخ الزيارة 2024-108

2. يحيى ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية، https://jlaw.journals.ekb.eg/article_45192_52d735c1a23cca2bf7dbbe56c4eb6846.pdf

3. قراصنة يخترقون جسر «بلوك شاين» ويسطون على 100 مليون دولار من شركة عملات مشفرة، متوافر على الموقع الالكتروني، https://aja.me/bc98ib

ج-الكتب الأجنبية :

1. Binxing Fang - Cyberspace Sovereignty-Springer Singapore, science press Beijing springer ,2018, 78.
2. François Delerue, Cyber operations and international law, Cambridge University Press, United Kingdom ,2020, p.29.
3. Jason Andress and Steve Winterfeld, Cyber Warfare. Techniques, Tactics and Tools for Security Practitioners, Syngress, second edition, 2014, p.p. 103-193.
4. Gourley, Stephen K., "Cyber sovereignty. In Conflict and Cooperation in Cyberspace: The Challenge to National Security, eds. Panayotis A. Yannakogeorgos, and Adam B. Lowther ,Boca Raton: CRC Press, 2013, P.P.277-289.
5. Hao Yeli, A Three-Perspective Theory of Cyber Sovereignty, PRISM Volume 7, No 2,P.3.
6. Michael N Schmitt, ed., Tallinn Manual on the International Law Applicable to Cyber Warfare ,Cambridge University Press, 2017,p.11.
7. Schneier ،Bruce, Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: W.W. Norton & Company, 2015,P. 78.

هـ- المواقع الأجنبية:

8. Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective,https://ccdcoe.org/uploads/2018/10/Ottis2008_
9. Baidu and CloudFlare Boost Users Over China's Great Firewall, https://www.benton.org/headlines/baidu-and-cloudflare-boost-users-over-chinas-great-firewall.
10. Charter of the United Nations, available on internet, https://legal.un.org/repertory/art2.shtml.
11. Cyber espionage and international law, https://www.

17. The Coming Digital Westphalia, https://www.chinausfocus.com/peace-security/the-coming-digital-westphalia.

18. The Hack of Sony Pictures-What We Know and What You Need to Know ,https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/the-hack-of-sony-pictures-what-you-need-to-know.

19. The Perfect Weapon: How Russian Cyberpower Invaded the U.S , https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

20. University of Maryland CISSM Cyber Attacks Database, hhttps://cissm.liquifiedapps.com.

21. US OPM Hack Exposes Data of 4 Million Federal Employees,https://www.trendmicro.com/vinfo/de/security/news/cyber-attacks/us-opm-hack-exposes-data-of-4-million-federal-employees.

22. What was the WannaCry ransomware attack?,https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/.

cyber-espionage.ch/Law.html.

12. Exclusive - SWIFT confirms new cyber thefts, hacking tactics,https://www.reuters.com/article/world/exclusive-swift-confirms-new-cyber-thefts-hacking-tactics-idUSKBN1412NS.

13. Hacking the Democratic National Committee , https://time.com/5565991/russia-influence-2016-election/ .

14. JPMorgan suffers wave of cyber attacks as fraudsters get 'more devious,https://www.ft.com/content/cd287352-cb3b-48d8-a85b-668713b80962.

15. SEC sues SolarWinds over massive cyberattack, alleging fraud and weak controls,,https://www.cnbc.com/2023/10/31/solarwinds-defrauded-investors-about-cybersecurity-sec-alleges.html.

16. Stuxnet explained- The first known cyberweapon,https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html.