الترميز الدولي / ISSN (P) :2710-2653 تاريخ استلام البحث : ٢٠٢٦/٦/١٧
ISSN (E) :2960-253X / تاريخ قبول البحث : ٢٠٢٦/٨/١٦
رقم الايداع الوطني / 2375 /2019 تاريخ النشر : ٢٠٢٦/٩/٣٠

جدلية السيادة في ظل تحديات الألفية الثالثة: التحدي الرقمي أنموذجا

The dialectic of sovereignty under the challenges of the third millennium: the digital challenge as a model

أ.م.د. صفاء ابراهيم جاسم الموسوي

Dr. Safaa Ibrahim Jassim Al-Mousawi

جامعة الأمين / كلية القانون

Al-Amin University / Faculty of Law

safaa@alameen.edu.iq

IRAQI
Academic Scientific Journals
https://iasj.rdd.eedu.iq/journals/journal/view/229

الملخص:

في الألفية الثالثة، أصبح الفضاء الألكتروني وأدواته المتعددة كالأنترنت ونحوها وسيلة لا غنى عنها لجميع البلدان والشعوب، ومع التطور الهائل في هذا الميدان والخدمات الجليلة التي تقدمها في شتى الميادين ، برزت الى الواجهة تحديات تتعلق بالأمن السيبراني للدول والشركات والأفراد، مما دعا هذه الأطراف الى وضع استراتيجيات أمنية ، وبناء أنظمة حماية خاصة بالفضاء السيبراني للحد من هذه الأنتهاكات ، مؤسسة بذلك بعدا جديدا في مفهوم السيادة التقليدي الا وهو "السيادة السيبرانية" ، والتي تعد قيمة أمنية عليا للدول وأمنها القومي، والأساس لكل الأنشطة المقابلة للتهديدات السيبرانية الخارجية.

(**الكلمات المفتاحية:** الدولة، السيادة، التحدي الرقمي، الألفية الثالثة، الامن السيبراني)

Synopsis:

In the third millennium, cyberspace and its various tools such as the internet and so on have become an indispensable means for all countries and peoples, and with this tremendous development in this field and the great services it provides in various fields, challenges related to the cybersecurity of states, companies and individuals have come to the fore, which called on these parties to develop security strategies and build special protection systems in cyberspace to reduce these violations, thus establishing a new dimension in the traditional concept of sovereignty, which is "cyber sovereignty", which expresses a high security value for states and their national security, and the basis for all activities corresponding to external cyber threats.

(Keywords: state, sovereignty, Digital Challenge, third millennium, cyber security)

المقدمة:

تواجه السيادة الوطنية للدول في الألفية الثالثة تحديات كبيرة في ظل ثورة الأتصالات والمواصلات الحديثة والتي بدأت تهدد وبشكل جدي مفهوم السيادة الويستفالي القديم للدول الوطنية والذي تعرض للنقد بشكل جدي من قبل العديد من المختصين والذين جادلوا بأن أن المفهوم القديم الذي أسس لفكرة الدول القومية ذات السيادة قد اصبح من الماضي ، حيث بات تحققه اكثر صعوبة اليوم في ظل التحديات الجديدةالمعاصرة.

أهمية البحث: تكمن اهمية البحث في ضرورة اعادة قراءة السيادة في ظل التحديات المختلفة الجديدة ومن ابرزها التحدي الرقمي، فمع التحولات الجديدة الهائلة على مستوى العالم وسرعة التواصل بين المجموعات والافراد تلاشى دور الزمان والجغرافيا ، وتراجعت سيطرة الحكومات على حركة المعلومات والأموال والأفكار عبر الحدود ، مما يستدعي وضع معالجات سريعة ونوعية لمواجهة هذا التحدي والسيطرة عليه.

أشكالية البحث: يعتبر التحدي الرقمي وما ينجم عنه من تزايد خطر التهديدات الأمنية للهجمات السيبرانية واختراق المنظومة الرقمية الالكترونية للدولة من قبل اطراف وافراد خارجيين من ابرز التحديات التي تواجه سيادة الدول في القرن الحالي، مما يتطلب وضع استراتيجيات فعالة لمواجهة هذا الخطر وحماية سيادة الدولة. وتتمثل أهم محاور البحث بالآتي:

١- الأطار النظري لمفهوم السيادة في ظل التحديات الحالية.

٢- تحديات الألفية الثالثة وسيادة الدول.

٣- حتمية السيادة الرقمية والمستقبل.

فرضية البحث: ان التحدي الرقمي لا يؤثر على سيادة الدول الوطنية التي تستطيع التكيف مع التحدي من خلال المرونة والأبتكار والقدرة على تطويع التكنولوجيا والأستفادة من الخبرات الوطنية والدولية في هذا المجال.

منهجية البحث: أعتمد البحث على المنهج الأستقرائي بصورة رئيسة، مع الأستعانة أيضا بعدد من المقتربات البحثية الأخرى كالمقترب الوصفي والتحليلي والتأريخي حيثما دعت الحاجة الى ذلك.

هيكلية البحث: أشتمل البحث على المقدمة وثلاث مباحث والخاتمة التي تضمن عددا من الاستنتاجات والتوصيات.

المبحث الأول: الأطار النظري لمفهوم السيادة في ظل التحديات الحالية

لا يخفى على الباحث، ان المفهوم الكلاسيكي العام لسيادة الدول هو نتاج معاهدة ويستفاليا ١٦٤٨م، حيث تعرف بأنها: "السلطة العليا والحصرية في أدارة الأمور داخل ولاية قضائية معينة" (Wenhong،2019) ، وتحتوي هذه السلطة ضمن مقوماتها الأساسية على ثلاث ركائز هي الشعب والأقليم والنظام السياسي، (حنون ، ٢٠١٩) ، وبذلك فأن " السيادة هي السلطة العليا للدولة التي لا يسمو عليها شئ ولا تخضع لأحد" ، ومن خصائصها" الأصالة والشمول والدوام وعدم القابلية للتجزئة فضلا عن عدم جواز التنازل عنها لأنها ملازمة لسلطة الدولة" (بدوي، ١٩٧١).

ومع التطور السريع للتكنولوجيا في العصر الحديث، وتحول الشبكة الى "نظام عصبي" تعتمد عليه الدول ذات السيادة على نطاق واسع في أدارة شؤونها الأقتصادية

والأجتماعية والسياسية والعسكرية لأغراض التحكم والسيطرة والتنميةالشاملة،وقد رافق ذلك التطور المهم للتكنولوجيا تحديات في الوقت نفسه لسيادة الدول، تمثلت بالتجسس والمراقبة واختراق الشبكات الرسمية، وسرقة المعلومات وأسرار الدولة المهمة من قبل دول وشبكات وفواعل أخرى من غير الدول. (**Wenhong** , 2019)

لقد اصبحت حياة الانسان اكثر ارتباطا بالعالم الافتراضي والاجهزة الالكترونية، وشرعت التكنولوجيا بالتأثير في مجمل نواحي الحياة، فضلا عن أعادتها لتشكيل الانظمة السياسية والعلاقات الدولية بصور وأسباب جديدة ومختلفة. (بيرم ، ٢٠٢٠)

ومن خلال دراسة السياق التأريخي للقوة وتحولاتها عبر أشكال مختلفة ومتعددة عبر التأريخ، كالقوة الصلبة ، والقوة الناعمة، والقوة السيبرانية، والقوة الذكية ، نجد ان القوة السيبرانية تمثلت بالقدرة على السيطرة من خلال "استخدام الفضاء الألكتروني للتأثير في الأحداث المتعلقة بالبيئات التشغيلية الأخرى وذلك عبر أدوات ألكترونية تشمل التحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الألكترونية، وبواسطة المهارات المدربة للتعامل مع هذه الوسائل". (بوكابوس ، ٢٠١٩)

ومن هنا أصبح مفهوم القوة الحديثة لا يعترف بمنطق النظام الدولي الكلاسيكي المتعارف عليه منذ الحرب العالمية الاولى، حيث ان كل من تمكن من أمتلاك القوة [سواء احدى أو بعض صورها ، وبغض النظر عن كونه دولة أم دون ذلك، فأنه سيتمكن عندها من منافسة الآخرين من الدول وغيرها. (الحراري، ٢٠١٥)

وعلى هذا الأساس اصبحت التكنولوجيا الرقمية وما يتفرع عنها من عالم افتراضي وفضاء سيبراني، بعدا جديدا في العلاقات الدولية، حيث يصنفه البعض كبعد خامس جديد في هذا المجال. (الدباغ ، ٢٠٢٦)

ونظرا للأختلاف الواسع في استغلال واستخدام الفضاء الالكتروني من قبل المستخدمين في شتى المجالات الأيجابية والسلبية، فأن الأفراد والشركات والدول وشبكاتها الألكترونية قد تصبح فريسة سهلة للأستخدامات السلبية ، وللهجمات التخريبية على مؤسساتها المختلفة، ومع عدم القدرة على تحديد مصدر هذه الهجمات على وجه التحديد في الغالب، فأن ذلك قد يؤدي الى خلق حالة من الفوضى وعدم الاستقرار في العلاقات الدولية.(عباس ، ٢٠٢١)

ومن هنا تعرف **السيادة الرقمية** بأنها: "**بسط سيطرة الدولة على فضائها الرقمي وتحكمها بالأنترنت وفرض ولايتها القضائية عليه من خلال التنظيم القانوني لأستخداماته ومكافحة آثاره السلبية التي تهدد أمن واستقرار الدولة والمجتمع على السواء**". (حسين، ٢٠٢٦ ، ص١٨)

ومن المعروف ان الفضاء السيبراني يتمتع بعدد من الصفات والخصائص، حيث لا يتضح فيه الأرتباط الاقليمي بشكل واضح بسبب طبيعته الأفتراضية، مما يجعل من الصعب معه تطبيق مبدأ السيادة الأقليمية. (شرقي، ٢٠٢٣)

وعلى هذا الأساس، يمكن الأشارة الى ثلاثة مبادئ أساسية يستند اليها "مفهوم السيادة الرقمية" ، هي: (Broeders & Berg, 2020)

١- **المبدأ الأول:** وهو من المبادئ المستقرة في القانون الدولي العام، بأن الحكومات الوطنية تتمتع بحقوق سيادية على دولها أمام حكومات الدول الأخرى بموجب أختصاصها المكاني.

٢- **المبدأ الثاني:** بحكم الواقع تفرض الحكومات الوطنية سيادتها على جميع القوى والجهات الفاعلة في الفضاء الرقمي سواء اكانت رسمية أم غير رسمية، محلية أم أجنبية، وتفرض عليها سيطرتها السياسية.

٣- **المبدأ الثالث:** أن ادارة الأنترنت يجب أن تكون بالتساوي بين الدول، حيث لا يمكن ان تستحوذ دولة ما على أدارته وتسعى للهيمنة الرقمية على حساب باقي الدول.

لقد أظهرت الأحداث المتزايدة في الساحة الدولية، مثل الأتهامات المتبادلة بين الولايات المتحدة وروسيا الأتحادية بشأن الأدعاء بتدخل الأخيرة في الأنتخابات الرئاسية الأميركية لعام ٢٠١٦م وغيرها كثير، الصورة الواضحة والتعبير الدقيق عن أحتدام الصراع السيبراني بين الدول الكبرى ، وعلى الرغم من الأعتقاد السائد بأن الأنترنت قوة جبارة وليس لها حدود، الا أن هذا الأعتقاد غير صحيح، فبالرجوع الى العلماء المختصين في هذا المجال، فأنهم يشيرون الى أمكانية السيطرة بشكل كبير على الهجمات السيبرانية ، وحماية البنى التحتية السيبرانية للدولة بشكل كامل ، ومن خلال التشريعات القانونية أيضا يمكن رسم مسار التكنولوجيا وضبطه في حدود هذه التشريعات. (عبد الرحمن ، ٢٠٢٥)

ولعل اخطر ما يمكن ان يظهر في مجال التحدي الرقمي والذكاء الأصطناعي هو السباق في التسلح بين الدول، حيث يشهد العالم اليوم تنافسا محموما بين الدول الكبرى في هذا المجال.(حسين، ٢٠٢٦)

ويمكن التحقق من شدة التنافس بين الدول الكبرى في المجال الرقمي وتطبيقات الذكاء الأصطناعي وتوظيفها في المجال العسكري، من خلال الأطلاع على الميزانيات

الضخمة المرصودة في هذا المجال، حيث "أزدهر سوق الذكاء الأصطناعي في المجال العسكري ليصل الى ٢٣.٦٨ مليار دولار اميركي خلال السنوات ٢٠٢٢-٢٠٢٧، وبمعدل نمو سنوي يبلغ ٣٠.٦٧% ، وتقدر قيمة الذكاء الأصطناعي في الصناعات العسكرية عالميا ب ٩.٢ مليار دولار اميركي عام ٢٠٢٣، مع توقع وصولها الى ٣٨.٨ مليار دولار اميركي حتى عام ٢٠٢٨، وبمعدل نمو سنوي قدره ٣٣.٣% خلال المدة ٢٠٢٣-٢٠٢٨، ويأتي هذا النمو مدفوعا بعوامل عديدة ابرزها التركيز المتزايد على تطوير أنظمة الليزر العسكرية عالية الدقة، وزيادة الأستثمارات في تطوير الحلول التي تدعم الذكاء الأصطناعي لتعزيز القدرات العسكرية". (الحسيني وسعدي، ٢٠٢٥)

ولعل من أخطر أنظمة الذكاء الأصطناعي العسكرية اليوم هي أنظمة استهداف الأشخاص وتصفيتهم والتي تعد من صنف الجرائم الدولية الخطيرة التي تستهدف سيادة الدول بشكل مباشر، مثل **منصة "مافن"** الرقمية المستخدمة من قبل الجيش الأميركي لتحليل بيانات ساحة المعركة وتحديد الأهداف المعادية ، وهذه المنصة لا تعتمد على مصدر بيانات واحد وأنما عدة عناصر، وبدلا من وجود ٨-٩ أنظمة ، يتم دمجها في أداة تصور مرئي واحدة تتيح تحديد الهدف وتدميره بثلاث نقرات فقط. (موقع روسيا اليوم، ٢٠٢٦)

ويستعرض (**رونن بريجمان**) في كتابه **Rise and kill first** كيف تسيطر اسرائيل على خصومها عبر عمليات تجسس طويلة ومعقدة عبر مجموعة من الأساليب والوسائل الألكترونية التي توظف التكنولوجيا والذكاء الأصطناعي، من قبيل: (قناة الجزيرة ، ٢٠٢٦)

١- السيطرة على برمجيات كاميرات الشوارع والبنايات والمراقبة على المدى الطويل للمسؤولين والقوى الأمنية في دولة العدو.

٢- السيطرة على انترنت الأشياء (الأجهزة المنزلية، الساعات الذكية، أجهزة السيارات) وتحويلها الى وسائل تجسس.

٣- توظيف الذكاء الأصطناعي عن طريق برمجيات تجسس حديثة مثل (لافندر ، كوستل ، وأين أبي؟) وتحليل البيانات للوصول الى الأهداف بدقة.

٤- الربط بين الفضاء السيبراني والمادي (هنا تراقب الخوارزميات أي تبدل في السلوك للضحية وتعطي الأشارة للمركز بسرعة)

حيث أدى استخدام هذه التطبيقات الى تحول جوهري في طبيعة الحروب، وأختراق الأجهزة والمؤسسات الرسمية وغير الرسمية للدول الأخرى مما يهدد أمنها القومي بشكل مباشر.

المبحث الثاني: تحديات الألفية الثالثة وسيادة الدول

يعتبر مفهوم السيادة من المفاهيم الأساسية التي أرتكز عليها المفهوم الحديث للعلاقات الدولية، حيث أرتبط الى حد ما بأسم الفيلسوف الفرنسي "جان بودان" ، الذي تكلم فيه وحدد مدلوله بشكل دقيق، وعلى الرغم من الأنتقادات التي وجهت اليه كمفهوم مطلق ، الا أنه ظل محاطا بهالة من القدسية والمكانة الرفيعة لدى الدول.(ميرل، ١٩٨٦)

وبذلك فقد أنعكست التطورات الدولية الكبرى على تطور مفهوم السيادة من حالة الأطلاق الى حدود النسبية، فالأنتقال من طور العزلة الى مساحة التضامن التي بدأت تتسع وتزداد من خلال العلاقات التعاونية لمواجهة الأعباء المتزايدة، رسخ مفهوم

الأعتماد المتبادل الذي أخذت فيه كل دولة تساهم بقدر معين في تحقيق مصالح المجموعة الدولية. (نعمة، ١٩٧٨)

ويرى بعض المختصين ان السيادة قد تحولت من مبدأ فلسفي عند "بودان" (١٥٣٠-١٥٩٦) ، الى مبدأ وظيفي في معاهدة وستفاليا ١٦٤٨ ، ومن ثم تحول لاحقا الى مبدأ قانوني في معاهدة فيينا عام ١٨١٥، والتي جعل ارتباطها وثيقا بالقانون الدولي العام ، اذ أصبح أنتهاك سيادة اي دولة هو انتهاك مباشر للقانون الدولي نفسه. (لحسيني وسعدي، ٢٠٢٥)

وقد أعتبر "بطرس غالي" الأمين العام الأسبق للأمم المتحدة، بأنه: "على الرغم من ان أحترام سيادة الدولة ووحدة أراضيها لا يزال محوريا، ولكن مبدأ (السيادة المطلق) المعروف منذ قرون لم يعد قائما الآن ، ومن الضروري أعادة النظر في مفهوم السيادة لا من أجل أضعاف جوهرها الذي له أهمية حاسمة في الأمن والتعاون الدوليين ، وأنما بقصد الأقرار أنها يمكن أن تتخذ أكثر من وظيفة، ويمكن أن تتعدد صورها، وأن تسهم في حل المشاكل سواء داخل الدول أو فيما بينها". (غالي، ١٩٩٣، ص١١)

ان سيادة الدول اليوم تتعرض الى تحديات غير مسبوقة بسبب العولمة والتقدم التكنولوجي ، وتشمل تلك التحديات تآكل السيطرة الأقليمية وزيادة التدخلات الخارجية، والهيمنة السيبرانية التي تتجاوز سلطة الحكومات الوطنية وتهدد أمنها واستقرارها بشكل كبير، ولعل من أبرز الأمثلة على هذه التحديات والتهديدات التي تؤثر بشكل جدي على سيادة الدول ، هي ما يأتي: (افشين، ٢٠١٧)

اولا: العولمة والإعتماد المتبادل: ويشتمل على عدد من التأثيرات المتمثلة ب**التأثير الأقتصادي ، الهيمنة الثقافية.**

ثانيا: التكنولوجيا والفضاء السيبراني: ومن ابرز صور هذه التهديدات هي:السيادة العالمية الرقمية، النشاط العالمي المرتكز على الذكاء الأصطناعي والأتمتة.

ثالثا: الأمن والتهديدات غير التقليدية: والتي تبرز في صور الأرهاب والعصابات العالمية،الجريمة المنظمةوالأوبئة.

رابعا: التغير المناخي وادارة الموارد الطبيعية: ويتمثل هذا التهديد بعدد من الصور ، منها: **الكوارث البيئية، الصراع على الموارد.**

خامسا: التدخل الخارجي والنزاعات الجيوسياسية: ومثالها الواضح:حروب الوكالة،العقوبات الأقتصادية.

سادسا: الحركات الأنفصالية والصراعات الداخلية.

سابعا: الهجرة واللجوء.

ثامنا: الأسلحة النووية والتسلح.

تاسعا: الشعبوية والاستقطاب السياسي.

ومن خلال ما تقدم، يمكن ان يثور سؤال حول أكثر هذه التحديات تأثيرا على سيادة الدول من غيرها في الألفية الثالثة؟ ، وللإجابة على ذلك، وبعد الدراسة والتحليل فأن التحدي الأكثر تأثيرا هو التحدي السيبراني والناتج عن التداخل العميق بين العولمة والتكنولوجيا، وللأسباب الآتية: (عبد السلام ، ٢٠٢٦)

- **ان الفضاء السيبراني لايعترف بالحدود.**
- **السرعة:** تكون الهجمات الالكترونية سريعة وخاطفة وتتفوق على اي رد حكومي مقابل.

- **اللامركزية:** من الممكن ان تقوم بها دول او مؤسسات خفية او قراصنة افراد ولا تحتاج الى جيوش تقليدية ومعدات عسكرية.
- **التأثير الشامل:** يمكن شل الدولة بشكل كامل عبر هجوم الكتروني على بنيتها التحتية مثل هجوم ("نوت بيتا" على اوكرانيا في ٢٠١٧).
- **خطر الأعتماد على البنية التحتية الرقمية:** وذلك بسبب انه اذا تعرضت انظمة الطاقة ، البنوك، الشبكات الحكومية، وغيرها لأي هجوم فقد تنهار سيادة الدولة فعليا دون الحاجة الى الهجوم العسكري.
- **التحكم بالبيانات من قبل الشركات:** فشركات التكنولوجيا الكبرى مثل (كوكل ، فيسبوك ، امازون.... الخ) هي التي تتحكم في بيانات المواطنين اكثر من الحكومات مما يهدد بإضعاف السيطرة الحكومية الوطنية.

وتشير المعلومات الصادرة من المؤسسات الدولية الى تزايد خطورة تجنيد التكنولوجيا والفضاء السيبراني في الصراعات السياسية بين الدول ، فقد ارتفعت وتيرة االحوادث السيبرانية الخطرة في العقود الأخيرة ، ومن الأمثلة الواقعية على ذلك، هو تعرض الولايات المتحدة (أقوى دولة في العالم) الى هجوم الكتروني أطلق عليه اختراق solar wind والذي نسب في حينها الى روسيا، مما يكشف ان القوى العظمى نفسها ليست بمنأى عن هذه التهديدات. (حمد قدورة، ٢٠٢٥)

وفي هذا السياق ، فقد تحول سباق التسلح العالمي بين القوى الكبرى الى سباق تسلح رقمي أيضا، فالأسلحة ذاتية التشغيل بالكامل ، والطائرات المسيرة بدون طيار ذات الكلف المنخفضة نسبيا ، واسلحة الليزر وغيرها ، "غيرت معادلة الردع من القدرات

العسكرية التقليدية الباهظة ، لتتحول الى ما يمكن وصفه بالأستدامة الخوارزمية". (عبد السلام ، ٢٠٢٦ ، ص٣٣٢)

وبلغة الأرقام ، فقد بينت الدراسات الأخيرة الصادرة من جهات دولية ، الى ان "الخسائر العالمية الناتجة عن عن الهجمات الألكترونية والأرهاب السيبراني تقدر بنحو ١٠.٥ تريليون دولار اميركي خلال عام ٢٠٢٥، مقارنة بثلاثة تريليون دولار في عام ٢٠١٥" ، وقد أكدت دراسة أعدها "فريق دولي من الباحثين" عام ٢٠٢٤ على أنشاء اول "**مؤشر رقمي للجرائم الألكترونية**" في العالم ، حيث يصنف هذا المؤشر الدول حسب مستوى التهديد الصادر عنها بالجرائم الألكترونية الأساسية، وهي: الهجمات والابتزاز الالكتروني، سرقة البيانات ، غسيل الأموال ، عمليات الأحتيال ، جرائم المنتجات والخدمات التقنية، ويوضح الجدول رقم (١) أدناه أعلى عشرين دولة الأكثر خطورة في القيام بالهجمات السيبرانية ودرجة المؤشر لها. (ندزانا ، ٢٠٢٥)

ومن خلال ما تقدم، فأن محاولة الدول تحصين نفسها من الهجمات السيبرانية للدول الأخرى تصبح واقعا لا مفر منه، ويمكن الاستدلال على ذلك من ضخامة الميزانيات المرصودة للأمن السيبراني ، حيث تحتل الولايات المتحدة المرتبة الاولى في عداد الدول المستثمرة في هذا المجال وبرأسمال يصل الى ٨٥.٦٨ مليار دولار عام ٢٠٢٥، تليها الصين والمملكة المتحدة ثم باقي الدول، وكما يتضح ذلك من الجدول رقم (٢) أدناه:

جدول رقم (١): الدول الأكثر خطورة كمصدر للهجمات السيبرانية لعام ٢٠٢٤

شكل رقم (.) يوضح تصنيف الدول الأكثر خطورة كمصدر للهجمات السيبرانية لعام 2024

المصدر/ من اعداد الباحث بناء على بيانات مؤشر الجرائم الالكترونية.

المصدر: (Oxford University, 2024)

جدول رقم (٢) : ميزانية الأمن السيبراني لعدد من الدول لغاية عام ٢٠٢٥

ت	اسم الدولة	٢٠٢٢ / مليار $	٢٠٢٣ / مليار $	٢٠٢٤ / مليار $	٢٠٢٥ / مليار $
١	الولايات المتحدة	٦٤.٨٦	٧١.٧٩	٧٨.٣١	٨٥.٦٨
٢	الصين	١١.٢	١٢.٠٥	١٣.٧١	١٣.٧١
٣	المملكة المتحدة	٨.٧٤	٩.٤٤	١٠.٦٣	١١.٨٦
٤	اليابان	٨.٥٢	٩.٣١	١٠.١	١١.١٣
٥	المانيا	٥.٩٩	٦.٦٧	٧.٢٩	٨.٠٣
٦	فرنسا	٤.٦٠	٥.٠٩	٥.٥٥	٦.٠٩
٧	استراليا	٣.٤٥	٣.٦٣	٣.٨٧	٤.٢٣
٨	روسيا الاتحادية	٣.٣٥	٣.٥٦	٣.٨٨	٤.٢٣
٩	كندا	٣.٢٣	٣.٣٤	٣.٦٨	٤.٠٨
١٠	كوريا الجنوبية	٢.٨٥	٣.١٠	٣.٤١	٣.٧٦
١١	الهند	٢.١٧	٢.٥٢	٢.٨٩	٣.٣١
١٢	المكسيك	٢.٠٢	٢.٤٨	٢.٧٢	٢.٩٦
١٣	اندونيسيا	١.٩٢	٢.١٢	٢.٤٠	٢.٧٢
١٤	السويد	١.٢٥	١.٣٥	١.٤٦	١.٦٠
١٥	اسرائيل	٨٠١ مليون $	٨٦٨ مليون $	٩٥٧ مليون $	١.٠٥

المصدر : (عبد السلام، ٢٠٢٦، ص٣٣٣)

المبحث الثالث : حتمية السيادة الرقمية والمستقبل

بعد أن اصبح الفضاء السيبراني ميدانا مفتوحا للتنافس الشديد بين الدول حيث تتقاطع مفاهيم السيادة والنفوذ والأمن بشكل حاد، أمست الحاجة شديدة (للسيادة الرقمية) كضرورة حتمية للدول لغرض البقاء والأستمرار في ظل هذا الواقع الجديد، وفي تحقيق هذا السبيل تعتبر (الحوكمة السيبرانية)[1] أداة جيوسياسية مهمة للدول في تحقيق سيادتها الرقمية في ظل هذا التنافس الصفري. (سعد ، ٢٠٢٢) ، **ومن النماذج التي نقدمها في هذا المبحث والتي تعتبر كدراسة حالة لدولة حققت (السيادة الرقمية) لها، والتي تستحق الدراسة والتحليل واستخلاص النتائج** ، هي:

اولا: تجربة الولايات المتحدة الأميركية (مبدا أنفتاح الأنترنت وأدوات النفوذ السيادي المستترة): (الدباغ، ٢٠٢٦)

تستند التجربة الأميركية في الحوكمة السيبرانية الى المبادئ المعلنة عن حرية الأنترنت وتدفق المعلومات كقيم عليا ثابتة، ودعت الى ترسيخ مفهوم أصحاب المصلحة العالمية من خلال أدارة لامركزية للشبكة العنكبوتية بعيدا عن سيطرة الحكومات، ومما يميز التجربة الأميركية بشكل واضح في هذا المجال:

- في الوقت الذي لا يوجد قانون فدرالي موحد لحماية البيانات في الولايات المتحدة ، الا ان صاحب القرار الاميركي يدفع الحلفاء بأتجاه صياغة معايير دولية تعزز حماية المعلومات والخصوصية وحرية التعبير والحد من رقابة الحكومات.

[1] الحوكمة : هي الترجمة المختصرة الرائجة لمصطلح (Corporate Governance)، أما الترجمة العلمي للمصطلح فهي: (اسلوب ممارسة السلطات للأدارة الرشيدة).

- يعكس النهج المتقدم محاولة الموازنة بين حماية الحقوق ودعم الابتكار الرقمي في نفس الوقت.
- تستبطن التجربة الاميركية ادوات نفوذ سيادي مستترة، فتحكمها بالبنية التحتية للشبكة العالمية جعل لها اليد العليا في التحكم في تدفق البيانات العالمي، فضلا عن اعتراضها لكم هائل من الاتصالات الدولية، (بحسب تسريبات سنودن)[٢] ، وهو ما بات يشكل قلقا من هذه الهيمنة لدى الكثير من الأوساط في داخل وخارج الولايات المتحدة.

ثانيا: تجربة الصين (الجدار السيبراني العظيم وتقليل التبعية التكنولوجية): (عبد الرحمن، ٢٠٢٥)

- **الأمن السيبراني:** تتلخص تجربة الصين في قيامها بأنشاء نظام (الجدار الناري العظيم Great fire wall) لحجب المواقع الأجنبية مثل كوكل Google وفيسبوك Facebook وتعزيز منصات محلية مثل Baidu و We chat، وقد قامت الصين في سبيل تعزيز هذه التكنولوجيا المحلية بأستثمار مليارات الدولارات في تطوير شركات تكنولوجيا محلية مثل هواوي Huawei للأجهزة وشركة سميك Smic لصناعة الرقائق من اجل تقليل الأعتماد على الغرب.
- **القوانين الصارمة:** فرضت الصين قانونا صارما يلزم الشركات الأجنبية العاملة في الصين بتخزين بيانات المواطنين الصينيين داخل البلاد مثل شركة آبل التي أنشأت لها مركز بيانات Guizhou.

[٢] مثلت هذه التسريبات حدثا مهما في تأريخ الحوكمة السيبرانية، ففي عام ٢٠١٣ قام الموظف السابق في وكالة الامن القومي الاميركي بتسريب الاف الوثائق السرية للوكالة الى الاعلام، والتي أحتوت على معلومات صادمة عن برامج الرقابة والتنصت على المكالمات والرسائل، مثل برنامج PRISM الذي يقوم بجمع بيانات المستخدمين.

- **النتيجة:** نجحت الصين جزئيا في حماية سيادتها الرقمية، والحفاظ على الأستقرار الداخلي وتوسيع النفوذ، لكنها لازالت تعاني تحديات في التكنولوجيا المتقدمة مثل أشباه الموصلات بسبب عقوبات الولايات المتحدة.

ثانيا: تجربة روسيا الأتحادية (قانون الأنترنت السيادي Sovereign Internet Law): (بيرم، ٢٠٢٠)

في عام ٢٠١٩ أقرت جمهورية روسيا الأتحادية (قانون الانترنت السيادي) الذي يتيح لها ما يأتي:

- **عزل شبكتها عن العالم الخارجي** في حال تعرضها لهجمات الكترونية او عقوبات.
- **أنشاء بنية تحتية DNS محلية** لتجنب الأعتماد على الخوادم الأميركية.
- **فرض قيود على شركات مثل كوكل وميتا (فيسبوك)** لصالح منصات محلية مثل VKONTAKTE .
- **بالنسبة للتحدي لايزال النظام ليس كاملا** والعديد من الروس ما يزالوا يستخدمون VPN للوصول الى المحتوى الأجنبي.

ثالثا: تجربة الأتحاد الأوربي (اللائحة العامة لحماية البيانات GDPR) : (علي، ٢٠٢١)

تقدم تجربة الأتحاد الأوربي في الحوكمة السيبرانية نموذجا مستقلا يوازن بين الدعوة الى حرية الأنترنت من جهة، والحفاظ على السيادة الرقمية من جهة أخرى، وأعتماد مقاربة خاصة تستند الى أعتبار الخصوصية حقا من حقوق الأنسان الذي يحظى بالأولوية في العصر الرقمي ، لذا فرض الأتحاد الأوربي منذ عام ٢٠١٨ **مجموعة من**

القوانين التي تلزم الشركات العالمية لحماية بيانات المواطنين الأوربيين وذلك من خلال :

- **كل شركة تعمل في نطاق اوربا** مثل فيسبوك او امازون فعليها ان تخزن بيانات المواطنين الاوربيين داخل دول الاتحاد او تلتزم بشروط صارمة.
- في حال مخالفة الشركة تصل الغرامات الى نسبة ٤% من ايرادات الشركة العالمية (كانت غرامة شركة امازون عام ٢٠٢١ هي بحدود ٧٤٦ مليون يورو)
- اقرار قانون الذكاء الأصطناعي لعام ٢٠٢٤، والذي يحد من التطبيقات ذات المخاطر العالية، ويحد من قيود المراقبة الجماعية.
- **النتيجة** : أصبح الأتحاد الأوربي أقليما رائدا في مجال البيانات رغم أنتقادات الشركات العالمية.

رابعا: تجربة الهند: سياسة (صنع في الهند made in INDA): (عريبي، ٢٠٢٥)

نجحت الهند في ترسيخ مكانتها الرقمية عالميا وخاصة في مجال الذكاء الأصطناعي ، حيث تتفوق في مجال الرقمنة على دول متقدمة كالمملكة المتحدة واليابان ، وتعتبر من الدول المصدرة للقوة الناعمة الى الدول الأخرى، ولا تقاس قدرتها هنا على أنتاج خوارزميات متقدمة فقط لغرض جذب الأستثمارات الأجنبية، بل يتعدى ذلك الى أمكاناتها في تبني تشريعات متوازنة، وتصميم وتنفيذ سياسات عامة تحقق الحوكمة السيبرانية، وتضمن المنافسة العادلة في نفس الوقت. ولغرض مواجهة كلا من الصين والولايات المتحدة قامت الهند بما يأتي:

- تحقيق الريادة في مجال الذكاء الأصطناعي المسؤول، من خلال تحقيق التكامل بين الذكاء الأصناعي GPAI بما يتفق مع مبادئ التعاون الاقتصادي OECD ، والذي مهد لتعزيز مكانتها عالميا كشريك موثوق به من قبل الدول الأخرى.
- تحفيز الابتكار وريادة الاعمال، حيث شجعت الهند تصنيع الهواتف محليا مثل شركة Reliance Jio التي طورت هاتفا رخيصا بنظام تشغيل هندي.
- تعمل على أنشاء نظام دفع رقمي محلي UPI بدلا عن أنظمة Visa و Master Cart.
- حظر عشرات التطبيقات الصينية مثل TIK TOK و PUBG لأسباب أمنية.

التحدي: لا زالت الهند تعتمد في استيراد الرقائق الالكترونية على الصين وتايوان.

خامسا: تجربة أيران (المواجهة مع العقوبات الأقتصادية): (الهاشمي، ٢٠٢٦)

تمثل التجربة الأيرانية في السيادة الرقمية نموذجا فريدا لكيفية تعامل دولة وهي تواجه عقوبات اقتصادية لأكثر من اربعة عقود مع تقنيات الأتصال الحديثة العابرة للحدود، فهي تقدم تجربة تستند الى قراءة علمية دقيقة تفهم الأتصال كمعادلة شاملة تحكمها الفيزياء كما تحكمها السياسة في نفس الوقت، حيث أثبتت التجربة الايرانية ان "السيطرة على المجال الجوي لم يعد حكرا على الطائرات والرادارات فقط، بل يمتد الى الفضاء الكهرومغناطيسي بوصفه بعدا سياديا لا يقل أهمية عن الجغرافيا ، فالقدرة على تحييد منظومة اتصالات فضائية متقدمة دون مواجهة مع الاقمار الصناعية تكشف مستوى تكنولوجي متقدم في فهم الطيف الترددي وادارة الأشارة ، ودمج الأدوات الفيزيائية في الأطر الأمنية والقانونية".

ومن خلال الرؤية المتقدمة لكوادرها العلمية والفنية، وفي ظل استمرار العقوبات الدولية، أنجزت الجمهورية الاسلامية منذ قيام الثورة في عام ١٩٧٩م ولغاية الوقت الحاضر المشاريع الآتية:

١- استحداث شبكة اتصالات محلية معزولة (نظام SEPAH) للحد من تأثير قطع الانترنت.

٢- استحداث عملة وطنية رقمية (الريال الرقمي) لتجنب العقوبات على التحويلات الدولية.

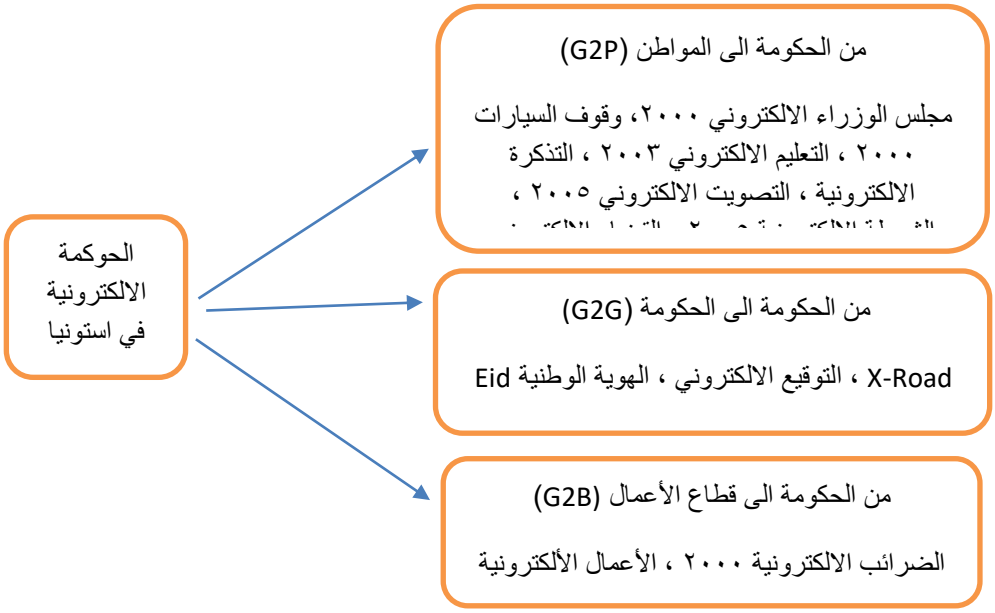
٣- تطوير شبكة تجارية دولية بديلة بالتعامل مع روسيا والصين عبر مقايضة النفط بالسلع.

التحدي: لا يزال الاقتصاد الايراني يعاني من العقوبات الدولية.

سادسا: تجربة إستونيا: الحكومة الالكترونية والمواطنة الرقمية: (خليفي و لطرش، ٢٠٢٥**)**

كان الدافع الى تطبيق الحوكمة السيبرانية في استونيا، هو تعرضها لأكبر هجوم سيبراني منظم عام ٢٠٠٧ ، حيث دفعها ذلك الى تشجيع الاستثمارات في حقل التكنولوجيا من أجل تدريب الموظفين ودعم الشركات الاستونية المختصة في هذا المجال ، مما جعلها من أكثر الدول تقدما في المجال الرقمي من خلال تطبيقها تجربة فريدة كان لها عدد من المخرجات النوعية والكمية والتي يبينها الشكل رقم (١) أدناه:

شكل رقم (١)



المصدر : من أعداد الباحث بالأعتماد على الموقع الالكتروني:

النتيجة: تثبت استونيا ان الدول الصغيرة يمكن ان تحافظ على سيادتها الرقمية عبر الابتكار.

ويمكن ان نخلص من خلال استقراء التجارب السابقة الى النتائج الآتية:

١- ان الدول الكبرى مثل الصين وروسيا الاتحادية تعتمد على العزلة الجزئية وبناء أنظمة بديلة.

٢- الدول المتوسطة مثل الهند والاتحاد الأوربي وايران تستخدم القوانين لحفظ وفرض سيادتها.

٣- الدول الصغيرة مثل استونيا تعتمد المرونة والابتكار.

وبالنتيجة فأن "حتمية السيادة السيبرانية" للدول اليوم ، تعتبر خط الصد الأول لحماية أمنها القومي، وباستثناء الولايات المتحدة (بسبب الأختلاف بين الدول الكبرى على ادارة الأنترنت بين استقلال الدول وحدها بأدارته أو بأشراك القطاع الخاص والشركات وكافة أصحاب المصلحة) ، يمكن أعتبار النموذج الصيني محققا لأعلى قدر من السيادة السيبرانية، وذلك بسبب تحكمها الكبير في الأقتصاد والأنترنت، على الرغم من ان ذلك له أكلاف اجتماعية واقتصادية وسياسية باهظة. (زيتون، ٢٠٢٥)

وحيث أن القوة في العلاقات الدولية تظل هي المحور الأساس للنظام الدولي (كما يرى الواقعيون) في ذلك على خلاف الليبراليين الذين يقولون بقدرة القوانين والمؤسسات على الحد منها، فالسؤال الذي يمكن ان يثار أيضا في هذا المقام ، **هو هل أن القوة السيبرانية هي أمتداد لمفهوم القوة التقليدي، أم أنها نوع آخر من القوة يحكمها منظور جديد آخر؟** ، ويميل هنا عدد من المختصين الى تأييد الفرض الأخير بسبب كونها قوة ذات مزايا فريدة، فهي غير مرئية، صعوبة تحديد الجهة التي تقف خلفها، غير مدمرة بالضرورة، مما يجعل منها قوة مثالية في الحروب اللاتماثلية، والحروب غير المباشرة. (الرخاوي، ٢٠٢٦)

وهناك سؤال آخر يتفرع على ما تقدم، هو: ما هي الحلول التي يمكن ان تتبعها الدول حاليا ومستقبلا لمواجهة هذا التحدي والسيطرة عليه؟ ، والجواب: بعد الدراسة والأطلاع على عدد من تجارب الدول المختلفة في هذا المجال والتي قدمها البحث آنفا ، فأنه يمكن أن نخلص الى ان التوجه العالمي لحل هذه الإشكالية يقوم على حزمة من الإجراءات السريعة والمهمة وعلى أكثر من صعيد، والتي تتضافر مع بعضها للحد من هذا التحدي وضبط آثاره، ولعل من أبرزها:

أولا: على الصعيد الوطني:

- تعزيز الأمن السيبراني الوطني عبر التشريعات الداخلية ذات العلاقة وبناء القدرات الفنية والعلمية وتدريب الكوادر الوطنية لرفع كفاءتهم في هذا الأختصاص.
- ابرام المعاهدات والأتفاقيات الدولية لضبط وتنظيم استخدام على التكنولوجيا.
- تقليل الأعتماد على التكنولوجيا الأجنبية من خلال تطوير انظمة محلية بديلة.

ثانيا : على الصعيد الأقليمي :

السعي الى تشكيل التحالفات الدولية السيبرانية مثل التحالف الغربي five Eyes ، وحلف الناتو (المادة ٥ من المعاهدة التي تعتبر الهجوم على اي عضو هجوما على الجميع) ، والأتفاق الصيني الروسي في المجال السيبراني لعام ٢٠١٥ والذي يعزز السيادة السيبرانية عبر منظمة شنغهاي للتعاون، وتحدد هذه التحالفات بشكل عام المعالم الأساسية لتعزيز المنظومات السيبرانية الدفاعية والهجومية للدول المنضوية تحت لوائها لتشكل حالة من الردع أمام الدول الأخرى.

ثالثا: على الصعيد الدولي:

يعتبر أقرار الأتفاقية الدولية الشاملة لمكافحة الجريمة السيبرانية من قبل الجمعية العامة للأمم المتحدة في ٢٠٢٤/١٢/٢٤ خطوة مهمة في مجال التعاون بين الدول الأطراف في مجال مكافحة الجريمة السيبرانية ، وضمان تعاون قضائي بين الدول لحماية الضحايا من المدنيين وحماية حقوق الأنسان، وتجميد العائدات الأجرامية، وتحديد قواعد الاستخدام والمسؤولية الدولية ، ووسائل المراقبة والمسائلة ، وآليات التنفيذ ، فضلا عن تحديد الهيئة الدولية المختصة بالمتابعة والمراقبة والتنفيذ. وقد بلغ عدد

الدول الموقعة على الاتفاقية لحد الآن قرابة الستين دولة من دول العالم. (الجزيرة ، ٢٠٢٥)

لكن أقرار هذه الأتفاقية لوحدها ليس كافيا في هذا المجال، وأنما يجب تعزيزه بأتفاقيات دولية أخرى تهتم بالجوانب الأضافية التي تخص الفضاء السيبراني كالأدارة ، التشريعات ، التعاون الفني وتبادل الخبرات ، التعاون القضائي ، الأتفاق على آليات موحدة لتحديد المسؤولية الدولية ... الخ، بل يذهب بعض الباحثين الى أهية ادراج الجرائم الارهابية السيبرانية الدولية في النظام الأساس للمحكمة الجنائية الدولية وأعتبارها ضمن الجرائم التي تخضع للأختصاص الموضوعي. (مراد ، ٢٠٢٥)

وختاما ، نستطيع القول ان التحديات المختلفة لسيادة الدول في العقود الأخيرة ومنها التحدي الرقمي ، لا يؤثر بالنتيجة على سيادتها ، فالسيادة الوطنية للدول ستظل باقية ما دامت الدول باقية ومستمرة، وهذا البقاء للسيادة ينبع من مرونتها وقدرتها على التكيف والتأقلم مع هذه التحديات.

الخاتمة:

اولا: الاستنتاجات:

١- شكلت التطورات الحاصلة في الساحة الدولية في العقود الأخيرة، تحولا كبيرا في مفهوم السيادة من حالة الأطلاق الى حدود النسبية.

٢- عزز الأنتقال من حالة العزلة السابقة التي رافقت المفهوم الكلاسيكي القديم الى حالة التضامن التي بدأت تتسع وتزداد من خلال العلاقات التعاونية لمواجهة الأعباء المتزايدة من رسوخ مفهوم الأعتماد المتبادل الذي أخذت فيه كل دولة تساهم بقدر معين

في تحقيق مصالح المجموعة الدولية، وهو ما يشير الى مرونة في التعامل الدولي والأنتقال من فكرة السيادة المطلقة الى التنازل عن جزء منها لصالح الجماعة الدولية.

٣- يعتبر التحدي الرقمي من أخطر التحديات التي يمكن ان تواجه سيادة الدول ، حيث تشير المعلومات الصادرة من المؤسسات الدولية الى تزايد خطورة تجنيد التكنولوجيا والفضاء السيبراني في الصراعات السياسية بين الدول.

٤- سجلت العقود الأخيرة ارتفاعا في وتيرة االحوادث السيبرانية الخطرة ، حيث لم تسلم منها حتى القوى العظمى نفسها والتي لم تكن بمنأى عن هذه التهديدات، حيث مثل انعدام السيطرة على الفضاء السيبراني والتبعية الرقمية التهديد الأكبر لسيادة الدول اليوم لأنه يضرب قلب الأمن والأقتصاد دون الحاجة الى غزو تقليدي.

٥- اصبح الفضاء السيبراني اليوم ساحة مفتوحة للتنافس الدولي الشديد، حيث تتقاطع فيها مفاهيم السيادة والنفوذ والأمن ، وقد فرضت (السيادة الرقمية) نفسها كمفهوم حتمي للدول للبقاء والتكيف والأستمرار مع هذا الواقع الجديد ، حيث تمثل فيها (الحوكمة السيبرانية) أداة جيوسياسية مهمة تسعى الدول الكبرى من خلالها الى ترسيخ عقيدتها واستراتيجيتها في تحقيق سيادتها الرقمية في ظل هذا التنافس الصفري، خاصة في ظل وجود تجارب ريادية لبعض هذه الدول في هذا المجال ، والتي يمكن ان تكون دليلا يحتذى به في هذا المجال من قبل الدول الأخرى.

ثانيا: التوصيات:

١- تعزيز الأمن السيبراني الوطني، من خلال تشريع قوانين وطنية لتنظيم استخدام التكنولوجيا، وانشاء المؤسسات المختصة بذلك ، وتدريب الكوادر لرفع مستوى الكفاءة والمهارة، مع زيادة التخصيصات المالية لدعم هذه الأنشطة المهمة.

٢- عدم الأعتماد الكلي على التكنولوجيا الأجنبية المستوردة ، والسعي لتطوير انظمة محلية بديلة بأعتبارها استراتيجية وطنية مهمة في تحقيق "السيادة السيبرانية" لأي دولة، ويمكن الأستفادة من الدول التي لها تجارب ملهمة في هذا المجال والتي مر ذكر بعضها في البحث.

٣- التعاون وبناء الشراكات مع الدول المتقدمة في مجال الامن السيبراني بالنسبة للدول التي تسعى لبناء استراتيجية وطنية محلية في الامن السيبراني الخاص بها، والاستفادة في مجال الخبرات والتدريب والتعاون المستدام في هذا المجال.

٤- السعي لبناء شبكة من التحالفات القوية بين الدول (ذات التوجهات السياسية المتقاربة) في مجال الأمن السيبراني بهدف تعزيز الأمن والسلم والتنمية في العالم.

٥- تفعيل الأتفاقيات الدولية كأتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية ، واتفاقية بودابست لعام ٢٠٠١ ، من خلال تحسين وتحديث التشريعات الوطنية أعتمادا على المبادئ والنصوص الواردة في تلك الأتفاقيات.

المصادر:

١- أفشين، أل، ٢٠١٧ ، تقهقر سيادة الدول في ظل التحولات الدولية، شؤون استراتيجية، العدد ٢.

٢- بدوي، ث، ١٩٧١، القانون الدستوري وتطور الأنظمة الدستورية في مصر، دار النهضة العربية.

٣- بوكابوس، و ، ٢٠١٩ ، تحول القوة في العلاقات الدولية: دراسة في انتقال القوة من التقليدية الى الحديثة، الحرب الباردة الثانية: تغير الجغرافيا وتعدد الفواعل، ط١، المركز الديمقراطي العربي للدراسات الاستراتيجية ، برلين ، المانيا.

٤- بيرم ، ف ، ٢٠٢٠ ، السيادة الوطنية في ظل الفضاء السيبراني والتحولات الرقمية: الصين أنموذجا، المجلة الجزائرية للأمن الأنساني ، المجلد ٥، العدد ٢.

٥- الجزيرة ، ابرز بنود اتفاقية الامم المتحدة لمنع الجريمة السيبرانية ، Aljazeera.net

٦- الحراري، خ ، ٢٠١٥ ، مفهوم القوة في العلاقات الدولية ، مطبعة الأهرام ، مصر.
٧- حنون ، ح، ٢٠١٩، القانون الدستوري ، مكتبة السنهوري، بغداد.
٨- خليفي ، هـ و لطرش، ص ، ٢٠٢٥ ، الحوكمة الالكترونية: دراسة حالة استونيا كنموذج متقدم ومدى استفادة الجزائر منه ، مجلة نماء للأقتصاد والتجارة ، المجلد ٩ ، العدد ١.
٩- الدباغ، ن ، ٢٠٢٦ ، الحوكمة السيبرانية: المفهوم والتنافسية الدولية، مجلة حمورابي، العدد ٥٧.
١٠- الرخاوي، ك ، ٢٠٢٦ ، السيادة الرقمية: استخدام القوة في الفضاء السيبراني بين القانون الدولي والواقع الاستراتيجي ، foulabook.com.
١١- زيتون، م ، ٢٠٢٥ ، العمليات السيبرانية وتأثيرها على تحولات السيادة في الفضاء السيبراني،AJSP
١٢- سعد، م ، ٢٠٢٢ ، تأثير تغير مفهوم السيادة على الأختصاص القضائي في الجرائم السيبرانية ، المجلة الدولية للفقه والقضاء والتشريع.
١٣- شرقي، ع ، ٢٠٢٣ ، التهديدات السيبرانية واشكالية السيادة، مجلة السياسة العالمية، المجلد ٧، العدد ٢.
١٤- عباس، و ، ٢٠٢٦ ، سباق التسلح بالذكاء الأصطناعي وتأثيره على الأستقرار الأستراتيجي في النظام الدولي، مجلة الجمعية العراقية للعلوم السياسية، العدد١٨.
١٥- عبد الرحمن، ف ، ٢٠٢٥ ، السياسة الرقمية الصينية: قراءة في التشريعات الوطنية لتأمين السيادة الرقمية، سياسات وتجارب مقارنة ، متاح على الرابط الألكتروني: https://www.democraticac.de
١٦- عبد السلام، ب ، ٢٠٢٦ ، التحول العالمي نحو استخدام تقنيات الذكاء الأصطناعي في الصراعات السياسية وانعكاساته على الأمن السيبراني المصري، مجلة البحوث المالية والتجارية.
١٧- عريبي، ز ، ٢٠٢٥ ، معركة الاحتكار في الهند: كيف يعيد الذكاء الأصطناعي صياغة قوانين المنافسة الرقمية، مركز حمورابي للبحوث والدراسات الأستراتيجية.

١٨- علي، م ، ٢٠٢١ ، السيبرانية والحوكمة: بين ممارسة السيادة وحقوق الأنسان: قضايا ونظرات، مركز الحضارات للدراسات والبحوث، القاهرة ، العدد ٢١.

١٩- غالي، ب، ١٩٩٣ ، نحو دور أقوى للأمم المتحدة ، مجلة السياسة الدولية، مركز الدراسات السياسية والاستراتيجية بالأهرام ، العدد١١١.

٢٠- قدورة ، ح ، ٢٠٢٥، أزمة السيادة الأقليمية في القرن الحادي والعشرين ، متاح على الرابط الألكتروني: https://www.democraticac.de

٢١- لحسيني، ح و سعدي، خ، ٢٠٢٥، الأمن السيبراني وحماية البنية التحتية الرقمية: المغرب أنموذجا، رسالة ماجستير، كلية العلوم القانونية والسياسية، جامعة بن طفيل.

٢٢- محمد رضا، م ، ٢٠٢١ ، الجيوش الالكترونية: ضحايا بلا دماء، ط١، دار امجد للنشر والتوزيع.

٢٣- مراد، م ، ٢٠٢٥ ، الحماية الجنائية الدولية في مواجهة الجرائم السيبرانية وآلياتها، مجلة الباحث العربي، مجلد ٦، العدد ٢.

٢٤- موقع روسيا اليوم، Arabic.rt.com

٢٥- ميرل، م ، ١٩٨٦، سوسيولوجيا العلاقات الدولية، دار المستقبل العربي، القاهرة.

٢٦- ندزانا ، ج، ٢٠٢٥، دور الذكاء الاصطناعي في منع الصراعات وادارتها في افريقيا، أفروبوليسي.

٢٧- نعمة، ع ، ١٩٨٨، السيادة في ضوء التنظيم الدولي المعاصر، بيروت.

٢٨- الهاشمي، ن ، ٢٠٢٦ ، السيادة الرقمية في عصر المدار المنخفض: التجربة الأيرانية في تحييد الأتصال الفضائي ، أقلام ، المرجع الألكتروني للمعلوماتية، ns1.almerja.com

29- Dennis Broeders & Bibi van den Berg, Governing cyber space: Behavior, Power and Diplomacy, The Netherlands Universiteit Leiden.

30- Oxford University, World-first "Cybercrime Index" ranks countries by cybercrime threat level, 10 Apr 2024, See: https://www.ox.ac.uk/news/10-4-2024

31- Xu Wenhong, CHALLENGES TO CYBER SOVEREIGNTY AND RESPONSE MEASURES, I.O.R, Chinese academy of social sciences, 2019.