University of Benghazi

Faculty of Education Almarj

جامعة بنغازي

كلية التربية – المرج

ISSN 2518-5845

Global Libyan Journal

المجلة الليبية العالمية

العدد اثنان وسبعون/ ديسمبر / 2025

أثر التهديدات السِّيبْرَانِيَّة على السيادة الرقميَّة للدول

(الصين أنموذجاً)

د. توفيق صالح علي الحفار

أستاذ مشارك– قسم العلوم السياسيَّة

الأكاديمية الليبيَّة– بنغازي

أ. ونيسة علي بن غزي

عضو هيئة تدريس متعاون

بالجامعات الليبيَّة

ملخص الدراسة

هدفت الدراسة إلى تسليط الضوء على التجربة الصينية في حماية سيادتها الرقميَّة، وذلك انطلاقاً من المخاطر التي تشكلها التهديدات السيبرانية على الأمن القومي الصيني، خصوصاً فيما يتعلق بعملية اختراق المعلومات والبيانات الحساسة ذات الطابع الوطني، وفي هذا الإطار تم تعريف السيادة الرقمية وتوضيح أنواع التهديدات السيبرانية، كما تم وصف وتحليل تأثير التهديدات السيبرانية على السيادة الرقمية للصين، وكذلك تم استعراض أبرز السياسات والاستراتيجيات التي اتبعتها الصين لحماية سيادتها وتعزيز أمنها السيبراني، وقد توصلت الدراسة إلى نتيجة مفادها: إن الصين– رغم التحديات والمعوقات التي تواجهها– استطاعت من خلال السياسات والاستراتيجيات التي وضعتها رفع مستوى الأمان الرقمي وضمان استقلالية الفضاء الإلكتروني الوطني، مما جعلها أنموذجا يحتذى به في مواجهة التهديدات السيبرانية العالمية.

الكلمات المفتاحية:

التهديدات السِّيبْرَانِيَّة – الهجمات الإلكترونية– السيادة الرقمية– الأمن السيبراني– الأمن القومي– الصين.

University of Benghazi

Faculty of Education Almarj

جامعة بنغازي

كلية التربية – المرج

ISSN 2518-5845

Global Libyan Journal

المجلة الليبية العالمية

العدد اثنان وسبعون/ ديسمبر / 2025

Abstract

The study aimed to shed light on the Chinese experience in protecting its digital sovereignty, based on the risks posed by cyber threats to Chinese national security, especially with .regard to the process of hacking sensitive information and data of a national nature

In this context, digital sovereignty was defined and the types of cyber threats were clarified. The impact of cyber threats on China's digital sovereignty was also described and analyzed. The most prominent policies and strategies that China has followed to protect its sovereignty and enhance its cyber security were also reviewed. The study reached the conclusion that: Despite the challenges and obstacles it faces, China has been able, through the policies and strategies it has put in place, to raise the level of digital security and ensure the independence of national cyberspace, making it a role model in confronting global cyber threats.

Keywords: Cyber threats - cyber-attacks -Digital sovereignty - cybersecurity - national security - China.

المقدمة

أصبحت التكنولوجيا الرقمية – في عصر التحول الرقمي المتسارع – بمثابة العمود الفقري للدول الحديثة، حيث تمتد تأثيراتها إلى مختلف المجالات، بدءًا من الاقتصاد ووصولًا إلى الأمن القومي، ومع تزايد الاعتماد على التقنيات الرقمية، ظهرت التهديدات السيبرانية كواحدة من أخطر التحديات التي تواجه الدول في الحفاظ على سيادتها؛ فمفهوم سيادة الدول في عصر التكنولوجيا لم يعد كما هو متعارف عليه من قبل، حيث كانت سيادة الدول تقتصر على الأرض والمياه الإقليمية والمجال الجوي، ثم توسعت لتشمل العالم الرقمي الذي أصبح ميدانًا جديداً للصراعات والتنافس الدولي، وأصبحت الدول تخشى على سيادتها وأمنها القومي الذي بات قابلا للاختراق في ظل التهديدات الجديدة ذات الطبيعة السيبرانية، وتُعد الصين أنموذجًا مثيرًا للاهتمام في هذا السياق، كونها استطاعت تطوير سياسات وإستراتيجيات لتعزيز سيادتها الرقمية في مواجهة التحديات التي فرضها عليها التنافس العالمي على ملكية الفضاء السيبراني.

جامعة بنغازي
كلية التربية – المرج
ISSN 2518-5845
University of Benghazi
Faculty of Education Almarj
المجلة الليبية العالمية
Global Libyan Journal
العدد اثنان وسبعون/ ديسمبر / 2025

أولا/ الدراسات السابقة:

تم رصد بعض الأدبيات التي تطرقت لموضوع السيادة الرقمية والتهديدات السِّيبْرَانِيَّة من زوايا مختلفة، ولعل أبرز تلك الأدبيات يتمثل فيما يلي:

1- دراسة قدمها يحي ياسين مسعود بعنوان: "الحرب السِّيبْرَانِيَّة في ضوء قواعد القانون الدولي الإنساني" حيث تطرق الباحث لموضوع الهجمات السِّيبْرَانِيَّة أثناء النزاعات المسلحة، من خلال التعريف بأساليب ووسائل القتال أثناء الحروب التقليدية والحروب الحديثة، ومدى إمكانية تطبيق مبادئ وقواعد القانون الدولي الإنساني على الحروب الحديثة المتمثلة في الهجمات السِّيبْرَانِيَّة، وتوصل الباحث إلى نتيجة مفادها: إن. قواعد القانون الدولي الإنساني لم تشر إلى الهجمات السِّيبْرَانِيَّة أثناء النزاعات المسلحة، إلا أن شمولية العديد من قواعده يمكن أن تستوعب الكثير من التطورات ذات الصلة، دون انكار حقيقة التغيرات التي شهدتها طبيعة الحروب، ولعل الاستخدام المتزايد للفضاء السِّيبْرَانِي للأغراض العسكريَّة أحد أهم الأسباب التي تدعو إلى إعادة تنظيم قواعد وأحكام النزاعات المسلحة وصياغتها بالشكل الذي يتلائم مع طبيعة هذه الاستخدامات. وقد يبدو وضع مقاربات إنسانية متباينة بين الحروب التقليدية وحروب الفضاء(مسعود، 2018م)[1].

2- دراسة قدمها مصطفى حميل، بعنوان: السيادة الرقمية والتحول الرقمي: التحديات والحلول الهيكلية"، تناول الباحث في هذه الدراسة ظاهرة الثورة الرقمية الهائلة التي شهدها العالم في القرن العشرين، والتحولات نحو الاقتصاد الرقمي والسياسة الرقمية والدبلوماسية الرقمية، وصولاً إلى مفهوم الدول والمدن الرقمية، حيث ركز على مفهوم السيادة الرقمية كبديل للمفهوم التقليدي للسيادة، في ظل التهديدات والهجمات الإلكترونية مثل فيروسات "ستاكس نت" و"بوت نت" و"حصان طروادة"، وقد توصلت الدراسة إلى نتيجة مفادها: إن هذه الهجمات الإلكترونية التي استهدفت الحواسيب قد أدت إلى سرقة البيانات والمعلومات السرية للمستخدمين والشركات والمؤسسات الدفاعية والأمنية والاقتصادية في العالم(حميل،2022م)[2].

3- دراسة قدمتها فاطمة عوامر، بعنوان: "تأثير القوة السِّيبْرَانِيَّة على الاستراتيجيات الأمنية للدول الكبرى: دراسة حالة – الصين"، حيث استعرضت هذه الدراسة كيفية تأثير القوة السِّيبْرَانِيَّة على الاستراتيجيات الأمنية للدول الكبرى، مع التركيز على الصين، وقد تناولت

---

[1] يحي ياسين مسعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية، المجلد 4، العدد 4، 2018م.
[2] مصطفى حميل ، "السيادة الرقمية والتحول الرقمي: التحديات والحلول الهيكلية." **مجلة رقمنة للدراسات الإعلامية والاتصالية**، العدد 3 (31 ديسمبر 2022م).

University of Benghazi
Faculty of Education Almarj
جامعة بنغازي
كلية التربية – المرج
ISSN 2518-5845
Global Libyan Journal
المجلة الليبية العالمية
العدد اثنان وسبعون/ ديسمبر / 2025

الباحثة هذا الموضوع من خلال تحديد مفهوم القوة السِّيبْرَانِيَّة ومكوناتها المحلية والعالمية، وقد توصلت الدراسة إلى نتيجة مفادها: أن الصين دولة كبرى ومستهدفة سِيبْرَانِياً، وأن تعزيز قدراتها السيبرانية أصبح أمرا حتميا لحمايتها وتعزيز مكانتها الدولية، وأن وضع استراتيجية أمنية محكمة سيساهم في تعديل ميزان القوى العالمي(عوامر، 2018م)[3].

4– دراسة قدمتها إسراء شريف جيجان، بعنوان: "الأمن االسِّيبْرَانِي الصيني– دراسة في الدوافع والتحديات"،2021م)، تستعرض هذه الدراسة الحروب الإلكترونية أو الحروب السِّيبْرَانِيَّة التي تستهدف البنى التحتية والمنشآت والمؤسسات الحكومية والشبكات الصناعية والأبحاث، حيث توصلت الباحثة إلى نتيجة مفادها: إن التطور الذي تشهده الحروب السِّيبْرَانِيَّة يشكل في مجمله تحدي أمام الصين في مجال الأمن السيبراني، وإن تجاوزه يتطلب تعزيز الصين لقدراتها وقوتها السِّيبْرَانِيَّة عبر ما يسمى (جدار الحماية العظيم) حفاظا على مكانتها السياسية، والاقتصادية، والعسكرية، والأمنية، وذلك من خلال (جيجان، 2021م)[4].

التعقيب على الدراسات السابقة:

توضح الدراسات السابقة أن هناك اهتمامًا متزايدًا بموضوع السيادة الرقمية والأمن ا السِّيبْرَانِي، خاصة فيما يتعلق بالقوى الكبرى مثل الصين، ومع ذلك، يبرز من خلال مراجعة هذه الدراسات وجود بعض الفجوات البحثية التي تجنبت تلك الدراسات التعريج عليها، مثل التركيز على السياسات والاستراتيجيات التي اعتمدتها الصين لتعزيز سيادتها الرقمية، وآثار تطبيق تلك السياسات على مكانة الصين في العالم السِّيبْرَانِي، الأمر الذي سيتم معالجته من خلال هذه الدراسة.

ثانيا/ مشكلة الدراسة:

تعد السيادة الرقمية من المفاهيم الحديثة والمهمة التي تتعلق بقدرة الدول على التحكم في فضائها الإلكتروني وحماية مصالحها الرقمية، ومع ذلك تواجه الدول ومن بينها الصين تحديات كبيرة لمواجهة هذه التهديدات، التي قد تؤثر في الحفاظ على سيادتها الرقمية، الأمر الذي يطرح تساؤل رئيس التالي: كيف أثرت التهديدات السِّيبْرَانِيَّة على السيادة الرقمية للصين؟ وماهي الاستراتيجيات والسياسات التي اتبعتها الصين لتعزيز سيادتها الرقمية؟

---

[3] فاطمة عوامر"، **أثير القوة السِّيبْرَانِيَّة على الاستراتيجيات الأمنية للدول الكبرى: دراسة حالة - الصين"**،(جامعة قاصدي مرباح،الجزائر،2018م).

[4] إسراء شريف جيجان، "الأمن السِّيبْرَانِي الصيني"، **مجلة قضايا سياسية**، كلية العلوم السياسية، جامعة النهرين، العدد 65، 2021م.

وينبثق عن هذا التساؤل الرئيس عدة تساؤلات فرعية:

1. ما طبيعة التهديدات السِّيبْرَانِيَّة التي تواجه الدول في العصر الرقمي؟
2. كيف تطور مفهوم السيادة الرقمية في ظل التطورات التكنولوجية؟
3. ما هي الاستراتيجيات والسياسات التي اتبعتها الصين لتعزيز سيادتها الرقمية؟
4. إلى اي مدى كانت السياسات التي تبنتها الصين فعالة في مواجهة التهديدات السِّيبْرَانِيَّة التي تتعرض لها؟

ثالثا/ فرضية الدراسة:

تنطلق الدراسة من فرضية رئيسية مفادها :

(أثرت التهديدات السِّيبْرَانِيَّة سلباً على السيادة السيبرانية للصين، من خلال إضعاف قدرتها على حماية البيانات والمعلومات الحساسة مما دفعها الي تبني سياسات حديثة لتعزيز وحماية هذه السيادة).

رابعا/ أهمية الدراسة:

يمكن تقسيم أهمية الدراسة إلى أهمية علميةوأخرى عملية، حيث تبرز الأهمية العلمية للدراسة في تقديم إطار مفاهيمي ونظري حول السيادة الرقمية والتهديدات السِّيبْرَانِيَّة، وتوضيح حدود العلاقة بينهما، والاشكاليات التي تثيرها هذه العلاقة، في ظل فضاء إلكتروني متزاحم في ظاهره التنافس وفي باطنه الصراع، الأمر الذي سيشكل إضافة للمكتبات المحلية والعربية والدولية، ولمراكز الأبحاث ذات العلاقة بموضوع الدراسة.

أما الأهمية العملية، فتتمثل في استعراض وتحليل التجربة الصينية كنموذج يمكن أن تستفيد منه الدول الأخرى التي تعاني من الهجمات السِّيبْرَانِيَّة، خصوصا إذا ما استعرضنا أبرز السياسات التي اتخذها صانع القرار في الصين لحماية السيادة الرقمية لبلاده.

خامسا/ أهداف الدراسة:

تتمثل أهداف الدراسة فيما يلي:

1. تعريف التهديدات السِّيبْرَانِيَّة وتوضيح أنواعها.
2. وصف وتحليل تأثير التهديدات السِّيبْرَانِيَّة على السيادة الرقمية للدول.

3. دراسة آثار التهديدات السِّيبْرَانِيَّة على السيادة الرقمية للصين.
4. استعراض السياسات والاستراتيجيات التي اتبعتها الصين لحماية سيادتها الرقمية وتعزيز أمنها السِّيبْرَاني.

سادسا/ مفاهيم الدراسة:

1– التهديدات السيبرانية: يقصد بها تلك الهجمات التي تتم باستخدام آليات وشبكات الإنترنت وأجهزة الحاسوب الآلي، وتهدف إلى إلحاق الضرر بالأجهزة والشبكات الإلكترونية ذات الاتصال بالإنترنت، بهدف سرقة المعلومات والبيانات أو الاكتفاء بالاطلاع عليها أو تخريبها أو حتى تغيير مضمونها، وكل ذلك يهدف إلى إلحاق الضرر بالطرف الضحية1.

2– السيادة الرقمية: هي قدرة الدولة على فرض هيمنتها على بنيتها التحتية الرقمية، وتأمين بياناتها، وضمان استقلاليتها الرقمية في مواجهة التحديات الخارجية[5].

3– الأمن السِّيبْرَانِي: هو مجموعة السياسات والإجراءات والممارسات المصممة مسبقا بهدف حماية البنية التحتية والأنظمة الرقمية من التهديدات والهجمات الإلكترونية، كما يهدف التأكد من سلامة البيانات وسريتها[6].

سابعا / مناهج ومداخل الدراسة:

اعتمدنا في هذه الدراسة على المنهج الوصفي التحليلي لفهم ووصف واقع التهديدات السِّيبْرَانِيَّة، وتحليل تأثيرها على السيادة الرقمية، كما استخدمنا المدخل التاريخي لتتبع مراحل نشأة وتطور التهديدات السِّيبْرَانِيَّة، وتتبع السياسات الصينيَّة لحماية سيادتها الرقمية في هذا المجال.

ثامنا/ الحدود الزمنية والمكانية للدراسة:

تركز الدراسة على الفترة الزمنية من 2010 إلى 2024م، حيث شهدت هذه الفترة تطورات كبيرة في مجال التكنولوجيا والتهديدات السيبرانية، مع التركيز على السياسات والاجراءات المتبعة في الصين خلال هذه الفترة.

---

(5) عبدالحميد يوسف، **"السيادة الرقمية ومتطلبات الامن القومي"** ،(النهضة، بيروت ،2020م)،ص47.
(6) ناصر محمود، استراتيجيات الأمن السيبراني في مواجهة التهديدات المتزايدة، **مجلة الدراسات الاستراتيجية**، (المجلد 5، العدد2، 2021م)،ص25.

تاسعا/ أدوات ووسائل جمع البيانات:

ستعتمد هذه الدراسة في جمع البيانات على الوثائق والكتب والدوريات ورسائل الماجستير والدكتوراه والصحف وشبكة المعلومات العالمية.

عاشرا/ تقسيم الدراسة:

تم تقسيم الدراسة الى مطلبين:

المطلب الأول/ السيادة الرقمية والتهديدات السِّيبْرَانِيَّة (تأصيل نظري)

أولاً: السيادة الرقمية(مفهومها–تطورها–إبعادها)

ثانيا: التهديدات السِّيبْرَانِيَّة (مفهومها وأنواعها)

المطلب الثاني/ أثر التهديدات السِّيبْرَانِيَّة على السيادة الرقمية للصين وسبل معالجتها

أولاً: تأثير التهديدات السِّيبْرَانِيَّة السيبرانية على السيادة الرقمية في الصين

ثانياً: السياسات والإجراءات التي تبنتها الصين لمواجهة التهديدات السِّيبْرَانِيَّة وتعزيز سيادتها الرقمية

ثالثا: التحديات والآفاق المستقبلية.

المطلب الأول/ لسيادة الرقمية والتهديدات السيبرانية (تأصيل نظري)

شـكلت الثورة التكنولوجية والتحول الرقمي الملحوظ الذي باتت تعيش على وقعه دول العالم كافة، علامة فارقة في تاريخ الدول، خصوصا تلك التي كانت يوما ما يضرب بها المثل في حماية حدودها الجغرافية من الأخطار المحدقة بها على المستويين الإقليمي والدولي.

أولا/ السيادة الرقمية (مفهومها – تطورها– أنواعها):

1– مفهوم السيادة الرقمية:

تطور مفهوم السيادة الذي ظل مرتبط بالدولة التقليدية وقدرتها على تصريف شؤونها الداخلية والخارجية بطريقة مستقلة، إلى أن أصبحت العولمة والعولمة التكنولوجية عامل أساسي لتحقيق التنمية والرفاهية الاقتصادية والسبب الرئيسي في كل هذه

التغيرات التي تطبع الساحة الدولية ولعل أهمها ارتقاء دور فاعلين جدد مثل المنظمات الغير حكومية والشركات المتعددة الجنسيات والأفراد، الشيء الذي بإمكانه تفسير بروز مفاهيم جديدة في حقل العلاقات الدولية من قبيل السيادة الرقمية[7].

والواقع أن هذا التحول من سيادة تقليدية إلى سيادة رقمية، ما هو إلا نتاج لتمدد وكثرة استعمال الانترنت الشيء الذي جعل منه يتجاوز الحدود الجغرافية والواقعية للدول، هذا العبور للحدود الوطنية، مس بشكل واضح الحدود الإقليمية المادية، بعدها انفتحت الدولة على تكنولوجيات العالم والاتصال وتبنت التخزين المعلوماتي أو الإلكتروني للبيانات التي توجد في نطاقات تتحكم فيها دول أخرى بحكم أسبقيتها في مجال المعلومات، كما أن المجتمعات أصبحت تواجه تحديات متعددة نتيجة لتسارع وثيرة التحول الرقمي، وهذا أدى إلى استخدام مصطلح "السيادة الرقمية" بشكل واسع في وسائل الإعلام، بالرغم من كونه يحمل مجموعة متنوعة من الدلالات المفاهيمية، فالمفهوم الرقمي للسيادة يعد حديثًا نسبيًا ومميزا، ينشأ بشكل أساسي من مفهوم الأمن السيبراني الذي يعتبر أكثر تداولا، إذ يتعلق الأمن السيبراني بحماية البنية التحتية والعمليات المرتبطة بالإنترنت، في حين تتعامل السيادة الرقمية مع المعلومات والمحتوى المقدم عبر الإنترنت، مما جعل منها مفهوم غامض يثير جدلا كبيرا بين الأكاديميين وحتى السياسيين[8].

2- التطور التاريخي لمفهوم السيادة الرقمية:

ارتبط مفهوم السيادة تاريخيا بالدولة التقليدية التي مارست سيادتها في إطار حدودها الجغرافية، ومع ظهور الإنترنت وتوسعه، أصبحت هذه الحدود غير كافية لاحتواء التدفقات الرقمية للمعلومات والبيانات، وقد زاد تأثير الإنترنت مع انتشار تقنيات الاتصالات المتقدمة واعتماد الدول على الأنظمة الإلكترونية لإدارة شؤونها الداخلية والخارجية، كما ساهمت العولمة في زيادة الاعتماد على شبكات المعلومات والاتصالات، ومع ظهور فاعلين جدد مثل الشركات المتعددة الجنسيات والمنظمات غير الحكومية، تم تجاوز الهيئات الحكومية التقليدية، التي قل تأثيرها في المشهد الرقمي، الأمر الذي أدى إلى إعادة صياغة مفهوم السيادة ليشمل أبعاداً رقمية تتداخل مع الأطر التقليدية[9].

---

(7) فاطمة رومات، "**العلاقات الدولية وتحديات الذكاء الاصطناعي**"، المعهد الدولي للبحث العلمي، (الوطنية للنشر، مراكش، 2021م)، ص9.
(8) أحمد شحيرط، "تحديات الإنترنيت لسيادة الدول (السيادة الرقمية)"، **مجلة البحوث القانونية والاقتصادية**، المجلد الخامس، العدد 1 (الجزائر، 2022م): 305.
(9) فاطمة بيرم، السيادة الوطنية في ظل الفضاء السيبراني والتحولات الرقمية، **المجلة الجزائرية للأمن الإنساني**، (المجلد الخامس، العدد1، 2020م)، ص11.

وقد طال هذا التغير الذي طرأ على مفهوم السيادة التقليدية دولة الصين ومدى قدرتها على السيطرة على حدودها، وذلك بعد تسريبات إدوارد سنودن عام 2013م، التي كشفت تجسس الولايات المتحدة على أنظمتها، ما أدى إلى إصدار قانون الأمن السيبراني الصيني 2018م، وإنشاء "المجموعة القيادية المركزية للأمن السيبراني" عام 2014م، والتي تُعتبر الهيئة المسؤولة عن صياغة السياسات الأمنية للصين[10].

3- تعريف السيادة الرقمية:

السيادة الرقمية (Digital Sovereignty) هي قدرة الدولة على فرض سيطرتها الكاملة على فضاءها الإلكتروني، بما يشمل البنى التحتية الرقمية، وبيانات المواطنين، وسياسات الأمن السيبراني.

وتُعرِّف الصين هذا المفهوم بأنه "حق الدولة في تنظيم وتأمين شبكاتها وبياناتها دون تدخل خارجي"، وهو ما يعكس رؤيتها للإنترنت كـ"حدود سيادية إلكترونية" يجب الدفاع عنها بقوة[11].

4- أنواع السيادة الرقمية:

تشمل السيادة الرقمية ثلاثة أنواع تتمثل فيما يلي:

أ- السيادة التكنولوجية:

يشير هذا البعد إلى قدرة الدولة على تطوير واعتماد تقنيات محلية بدلاً من الاعتماد على الأنظمة والتقنيات الأجنبية، وتبرز أهمية السيادة التكنولوجية في تخفيض المخاطر المرتبطة بالتبعية التقنية، حيث أن تطوير حلول تكنولوجية داخلية يمكن أن يحمي الدولة من التأثيرات السلبية للتدخلات الخارجية، سواء على مستوى البرامج أو الأجهزة المستخدمة في البنى التحتية الرقمية[12] .

---

[10] الأمم المتحدة، اللجنة الاقتصادية والاجتماعية لغربي آسيا (السكوا)،2019م, نشرة التكنولوجيا من أجل التنمية في المنطقة العربية، آفاق عالمية وتوجهات إقليمية، بيروت ص93، تاريخ الدخول 22/2/2025 الساعة 05:20، عبر الرابط التالي: https://archive.unescwa.org/ar/publications

[11] أحمد شحيرط، "تحديات الإنترنيت لسيادة الدول (السيادة الرقمية)"، **مجلة البحوث القانونية والاقتصادية**، المجلد الخامس، العدد 1 (الجزائر، 2022م): ص305.

[12] سميرة شرايطية، "السيادة السيبرانية في الصين: بين الحماية والهيمنة، **مجلة الأمن والتنمية**، (دار الآمال، الجزائر، 2020م)، ص45 .

ب– سيادة البيانات :

تُعنى سيادة البيانات بحماية المعلومات الوطنية وتنظيم تخزينها وتداولها داخل الإطار الوطني، يشمل هذا البعد إصدار تشريعات تلزم الشركات والمؤسسات بتخزين البيانات الحساسة على أراضٍ وطنية، وبالتالي تقليل خطر تسريب المعلومات أو استغلالها من قِبل جهات خارجية، ويُعد هذا الإجراء ضروريًا لتعزيز الثقة في النظم الرقمية وحماية الخصوصية الوطنية، إذ تصبح البيانات جزءاً من الثروة الوطنية التي يجب حمايتها[13].

ج–السيادة التشريعية والتنظيمية:

يرتبط هذا البعد بضرورة وضع إطار قانوني وتنظيمي يضمن حماية الفضاء الرقمي وتنظيم استخدامه بما يخدم مصالح الدولة، إذ يتطلب التعامل مع التحديات السيبرانية صياغة قوانين وتشريعات متخصصة تُلزم الجهات العاملة في المجال الرقمي بإتباع معايير أمنية محددة، كما يتضمن هذا البعد إنشاء هيئات متخصصة تتابع تطبيق هذه القوانين وتعمل على تحديثها باستمرار لمواكبة التطورات التقنية المتسارعة، وتُعد السيادة التشريعية عنصرًا حيويًا لضمان استقرار النظام الرقمي، حيث تساعد في التصدي للتدخلات الخارجية وتنظيم العلاقة بين القطاعين العام والخاص في مجال التكنولوجيا[14].

ثانيا/ التهديدات السِّيبْرَانِيَّة (مفهومها وتطورها وأنواعها):

1– مفهوم التهديدات السِّيبْرَانِيَّة:

التهديدات السِّيبْرَانِيَّة تشير إلى أي محاولة متعمدة للوصول إلى نظم المعلومات الرقمية أو إلحاق الضرر بها، سواء كان ذلك من خلال سرقة البيانات أو تدميرها أو حتى استخدامها لأغراض غير مشروعة، وتُعد التهديدات السِّيبْرَانِيَّة من أخطر التحديات في العصر الرقمي، نتيجة لتزايد اعتماد الأفراد والمؤسسات والدول على النظم الرقمية في شتى المجالات، تهدف هذه الهجمات إلى تقويض الأمن السيبراني من خلال استغلال نقاط الضعف في الأنظمة الرقمية سواء كانت أجهزة أو شبكات أو برمجيات[15].

---

[13] عبد الله القيسي، **"تهديدات الأمن السيبراني: دراسة تحليلية في الهجمات الإلكترونية"**، (دار الفكر العربي، القاهرة، 2020م)، ص21.
[14] تقرير "الصين والطريق إلى القطبية السيبرانية"، **إندبندنت العربية**، 2025م، ص12.
[15] Hongfei Gu, Data, Big Tech, and the New Concept of Sovereignty (Beijing: Beijing Press, 2023), 78.

2- تطور التهديدات السِّيبْرَانِيَّة:

مع تزايد استخدام الإنترنت في التسعينيات، بدأ ظهور أولى التهديدات السِّيبْرَانِيَّة التي كانت تقتصر في البداية على الفيروسات والبرمجيات الضارة، ومع مرور الوقت تطور هذا النوع من التهديدات ليشمل أساليب متقدمة مثل هجمات حجب الخدمة (DDoS) والاختراقات المتقدمة(APT) ، التي تتطلب تقنيات متطورة لتنفيذها، وفي العقد الأخير أصبحت الهجمات السِّيبْرَانِيَّة أكثر تعقيدًا واستهدافًا، حيث ظهرت هجمات مدعومة من دول تستهدف المؤسسات الحكومية والتجارية الكبرى بهدف سرقة المعلومات أو تعطيل الأنظمة الحيوية[16].

3- أنواع التهديدات السِّيبْرَانِيَّة:

تنقسم التهديدات السِّيبْرَانِيَّة إلى عدة أنواع لعل أبرزها ما يلي:

أ-الفيروسات والبرمجيات الخبيثة:

الفيروسات هي برامج تصمم بهدف تدمير البيانات أو تدمير النظام من الداخل، أما البرمجيات الخبيثة، فهي تهدف إلى اختراق الأجهزة أو الشبكات لأغراض غير قانونية، مثل سرقة البيانات أو التجسس على الأنشطة الرقمية[17].

ب- هجمات حجب الخدمة(DDoS) :

تعد هذه الهجمات من أكثر الأساليب شيوعًا في تعطيل الخدمات على الإنترنت، حيث يتم إغراق الشبكة أو الخادم بطلبات غير قانونية مما يؤدي إلى توقف الخدمة، وتهدف هذه الهجمات إلى جعل النظام غير قادر على التعامل مع المستخدمين الشرعيين[18].

ج-الاحتيال الإلكتروني:

يشمل الاحتيال الإلكتروني أساليب مثل التصيد الاحتيالي (Phishing) التي يستخدمها المهاجمون لخداع الأفراد للحصول على معلومات سرية، مثل كلمات المرور أو تفاصيل الحسابات البنكية[19].

---

(16) أحمد زكريا، الأمن السيبراني والتهديدات الإلكترونية: دراسة في مفهوم وطرق الوقاية، **مركز دراسات الأمن السيبراني**، 2018م، ص9.
(17) سميرة شرايطية، **السيادة السيبرانية في الصين: بين الحماية والهيمنة**، مرجع سبق ذكره، ص48.
(18) سليمان المجالي، "مفاهيم الأمن السيبراني وتهديداته"، **مجلة دراسات الأمن السيبراني**، (العدد 12، عمان، 2020م)، ص 23.
(19) يوسف السمرة، "**التحديات الرقمية وأمن المعلومات في الوطن العربي**"، (جامعة الإمارات، العين، 2020م)، ص 32.

د– الهجمات المدعومة من دول:

تتضمن هذه الهجمات محاولات لاختراق نظم المعلومات الخاصة بالدول الأخرى، وغالبًا ما يحدث ذلك بهدف التجسس أو تقويض الاستقرار السياسي والاقتصادي، وتعد الهجمات الإلكترونية التي تستهدف البنية التحتية الحيوية مثل شبكات الكهرباء والمياه أحد أمثلة هذه الهجمات[20].

هـ – الاختراقات الموجهة(APT):

الهجمات المتقدمة الموجهة (APT) هي هجمات متخصصة تستهدف بشكل خاص الشركات الكبرى أو الحكومات، وتستخدم تقنيات متطورة بهدف جمع المعلومات الحساسة أو إحداث تأثيرات طويلة الأمد على الأنظمة المستهدفة[21].

المطلب الثاني

أثر التهديدات السيبرانية على السيادة الرقمية في الصين وسبل معالجتها

واجهت الصين تحديات جسيمة في حماية سيادتها الرقمية، لا سيما مع تزايد الهجمات الإلكترونية المنسوبة لجهات أجنبية، والتي تستهدف بنيتها التحتية الحيوية وسرقة أسرارها التكنولوجية، ومع ذلك، استطاعت الصين تحويل هذه التهديدات إلى دافع لتعزيز سيطرتها عبر سياسات صارمة، رغم ما يرافق ذلك من انتقادات دولية تتعلق بالحريات.

وسنستعرض في هذا المطلب التأثيرات السياسية، والأمنية، والاقتصادية، والاجتماعية لهذه التهديدات، إضافة إلى السياسات والاستراتيجيات التي اعتمدتها الصين لمعالجتها.

---

[20] خالد الشمري، "التهديدات السيبرانية: أساليب الوقاية والتصدي، **مجلة الأمن السيبراني**، (العدد 7، الرياض، 2019م) ، ص 58.

[21] WannaCry: The Ransomware Attack That Hit 150 Countries." BBC News, May 2017. https://www.bbc.com/news/technology-39920141

University of Benghazi
Faculty of Education Almarj
جامعة بنغازي
كلية التربية – المرج
ISSN 2518-5845
Global Libyan Journal
المجلة الليبية العالمية
العدد اثنان وسبعون/ ديسمبر / 2025

أولا/أثر التهديدات السِّيبْرَانِيَّة على السيادة الرقمية للصين:

شهدت الصين العديد من التهديدات والاختراقات السيبرانية التي طالت بنيتها الإلكترونية المتمثلة في شبكات الطاقة والمنظومات الحكومية ذات العلاقة بالنظام الأمني والمالي والاقتصـــادي والصـــحي والاجتماعي للدولة، الأمر الذي ترتب عليه عدة آثار لعل أبرزها ما يلي:

1-الآثار السياسية والأمنيَّة:

تتمثل الآثار السياسية والأمنية المترتبة عن التهديدات السيبرانية للسيادة الرقمية للصين فيما يلي:

أ- اختراق البنى التحتية الحيويَّة:

تعرضت شبكة الطاقة في شنغهاي عام 2022م لهجوم سيبراني تسبب في تعطيل الخدمات لعدة ساعات، مما أثر على قطاعات حيوية مثل النقل والصحة، ويُعتقد أن الهجوم استهدف أنظمة التحكم الصناعي (ICS) بهدف زعزعة الاستقرار الداخلي، وهو ما دفع الصـــين إلى تعزيز تشـــريعاتها الأمنية مثل قانون الأمن الســـيبراني لعام 2017م، الذي يفرض معايير صـــارمة لحماية البنى التحتية، وتُمثل الهجمات على الأنظمة الحكومية تهديدًا مباشـــراً لســـيادة الصـــين الرقمية، خاصـــةً مع تزايد الاعتماد على المنصـــات الإلكترونية مثل "AliPay" و "WeChat" الإدارة الخدمات العامة، وفي عام 2023م، كشـــفت تقارير عن محاولات اختراق لأنظمة التعرف على الوجوه في مشروع"Skynet"، مما أثار مخاوف حول انتهاك الخصوصية وتآكل الثقة في الأنظمة الرقمية.

ب- تهديد الأمن القومي:

تُصنف الصين الهجمات السيبرانية كـــ"أخطار وجودية"، خاصةً مع تزايد الاعتماد على التكنولوجيا الغربية في قطاعات مثل الرقائق الإلكترونية وأنظمة التشغيل؛ ففي عام 2024م كشفت تسريبات عن اختراق أنظمة البنك المركزي الصيني، مما أدى إلى تسرب بيانات مالية حساسة،وأدت هذه التهديدات إلى إنشاء "قوة الدعم المعلوماتي" العسكرية عام 2023م، وهي وحدة متخصصة في تنفيذ الهجمات السيبرانية المضادة لردع العدائيات الخارجية[22].

[22] "الصـــين أكبر هدف للهجمات الإلكترونية في العالم"، **العين الإخبارية**، 24 فبراير 2019م، https://al-ain.com/article/china-cyber-attack.

جامعة بنغازي
كلية التربية – المرج
ISSN 2518-5845
University of Benghazi
Faculty of Education Almarj
المجلة الليبية العالمية
Global Libyan Journal
العدد اثنان وسبعون/ ديسمبر / 2025

2–الآثار الاقتصادية والاجتماعية:

تتمثل الآثار الاقتصادية والاجتماعية المترتبة عن التهديدات السِّيبْرَانِيَّة للسيادة الرقمية للصين فيما يلي:

أ– الخسائر المادية:

تُقدَّر الخسائر السنوية للصين بسبب الهجمات السِّيبْرَانِيَّة بنحو 60 مليار دولار، وفقًا لتقارير وزارة الأمن السيبراني الصينية عام 2024م، وتشمل هذه الخسائر تكاليف استعادة الأنظمة المعطلة وتعويضات للمتضررين، ويمثل هجوم "WannaCry" عام 2017م الذي أصاب أنظمة المستشفيات الصينية، مما عطّل خدمات الطوارئ وأدى إلى خسائر فادحة في قطاع الصحة.

ب– تآكل الثقة في الخدمات الرقمية:

بعد سلسلة من الاختراقات، أظهر استطلاع أجرته "هيئة الإنترنت الصينية" عام 2024 أن 43% من المواطنين قللوا استخدامهم للخدمات الحكومية الإلكترونية خوفًا من انتهاك البيانات، كما أدت الهجمات على منصات التواصل مثل "Weibo" إلى انتشار الشائعات خلال الأزمات سياسية، مثل احتجاجات هونغ كونغ 2019م، مما زاد من حدة التوترات الداخلية[23].

ثانيا/ السياسات التي تبنتها الصين لمواجهة التهديدات السِّيبْرَانِيَّة وحماية سيادتها الرقمية:

في ظل تزايد التهديدات السِّيبْرَانِيَّة والتحول الرقمي السريع، اعتمدت الصين مجموعة من السياسات والإستراتيجيات المتكاملة لحماية سيادتها الرقمية، ويستند النموذج الصيني إلى تحديث الأطر القانونية والتشريعية، وتعزيز القدرات التقنية الوطنية، وتطبيق آليات رقابية دقيقة، بالإضافة إلى تبني التعاون الدولي لتبادل الخبرات، وفيما يلي أبرز تلك السياسات:

1– السياسات القانونية والتنظيمية:

أصدرت الصين قانون الأمن السيبراني في عام 2017م، والذي شكل حجر الأساس لتنظيم الفضاء الإلكتروني الوطني، وينص القانون على إلزام الشركات بتخزين البيانات الحساسة داخل الصين، وفرض ضوابط صارمة على نقل المعلومات إلى الخارج، وتمكين الجهات الحكومية من الرقابة المباشرة على الأنشطة الرقمية، كما شهدت السنوات التالية تحديثات تشريعية وإصدار قوانين مصاحبة، مثل

[23] نفس المرجع السابق.

قانون حماية البيانات الشـــخصـــية وقانون أمن البيانات (2019–2020م)، التي هدفت إلى تعزيز الأمن الرقمي وحماية المعلومات الوطنية[24].

2– إنشاء الهيكل التنظيمي والجهات الرقابية:

أنشـأت الصـين هيئات تنظيمية متخصـصـة مثل "المجموعة القيادية المركزية للأمن السِّيبْرَانِي" التي تأسـسـت عام 2014م، وهي الجهة المسؤولة عن تنسيق السياسات الرقمية بين مختلف الوزارات، ووضع معايير أمنية ملزمة للقطاعين العام والخاص، ورصد تطبيق الأطر التشريعية بشكل دوري[25].

3–تعزيز السيادة التكنولوجية:

أ– دعم البحث والتطوير في التقنيات الإستراتيجية:

تولي الصـــين اهتمامًا بالغًا بتطوير قدراتها التقنية من خلال تخصـــيص ميزانيات ضـــخمة للبحث والتطوير في مجالات الذكاء الاصطناعي والجيل الخامس وتقنيات الاتصالات، كما تدعم الشركات الوطنية الرائدة مثل "هواوي" و"زي تي إي"، وتشجع الابتكار المحلي لتقليل الاعتماد على التقنيات الأجنبية[26].

ب– التحول إلى الحلول والبرمجيات المحلية:

تعتبر إستراتيجية الصين في تطوير برمجيات وأنظمة تشغيل محلية مثل نظام "Kylin" خطوة رئيسية نحو تحقيق السيادة الرقمية، حيث يعمل هذا التحول على تقليل المخاطر الناجمة عن الاعتماد على الأنظمة الأجنبية، وتعزيز القدرة على مراقبة وتحديث النظم الرقمية داخلياً بما يتوافق مع المتطلبات الأمنية المحلية[27].

---

[24] الصين، قانون الأمن السيبراني، 2017م.
[25] "الرقابة على الإنترنت في الصين"، **صحيفة جلوبال تايمز**، 2021م.
[26] الحكومة الصينية، "قانون دعم الشركات الوطنية"، 2020م.
[27] تقرير "تحول النظم الرقمية في الصين: حالة نظام"Kylin، من مركز البحوث التقنية الصينية، بكين: 2020م.

4–سياسات حماية البيانات والخصوصية:

اعتمدت الصين تشريعات صارمة لحماية البيانات تتضمن مجموعة من القوانين تلزم المؤسسات بتخزين البيانات الحيوية ضمن الأراضي الوطنية، ووضع معايير أمان متقدمة لمنع تسرب البيانات واستخدامها لأغراض غير مشروعة، وتشير التقارير الرسمية إلى أن تطبيق هذه القوانين ساهم في رفع مستوى الثقة في الأنظمة الرقمية الوطنية وتحصينها ضد الهجمات السيبرانية[28].

5–الرقابة على التدفق الدولي للمعلومات:

تعمل الصين على تنظيم حركة البيانات الدولية عبر آليات رقابية متطورة تتيح للسلطات مراقبة تدفق المعلومات عبر الحدود، وتطبيق ضوابط تقنية وقانونية صارمة لضمان عدم استغلال البيانات الوطنية خارجيًا[29].

6–التعاون الدولي والإقليمي:

تسعى الصين إلى تعزيز حضورها الدولي في مجال الأمن السِّيبْرَانِي من خلال المشاركة الفعالة في منتديات الأمن السِّيبْرَانِي العالمية، والمساهمة في صياغة معايير تنظيمية دولية تتماشى مع مصالحها الاستراتيجية، أما على المستوى الإقليمي، تنفذ الصين مبادرات مثل "الحزام والطريق الرقمية" التي تهدف إلى تعزيز التعاون التقني مع الدول الشريكة، وتبادل الخبرات حول تطوير الأطر التنظيمية المشتركة في مجال الفضاء الرقمي[30].

ثالثا/ التحديات والآفاق المستقبلية:

على الرغم من النجاحات المحققة في مجال الأمن السِّيبْرَانِي، تواجه السياسات الصينية عدة تحديات، منها:

1– موازنة الرقابة والابتكار التقني:

تُعد موازنة الصين بين الرقابة الصارمة على الإنترنت وتعزيز الابتكار التكنولوجي من أكبر التحديات التي تواجهها في مجال الأمن السِّيبْرَانِي؛ فالرقابة المكثفة قد تؤثر على قدرة الشركات التكنولوجية على الابتكار والنمو، مما يحد من تطوير تقنيات جديدة.

[28] "التحديثات التشريعية"، وزارة الأمن السيبراني الصينية، 2022م.
[29] "الرقابة الصينية على تدفق البيانات عبر الحدود"، وزارة الأمن الوطني، 2019م.
[30] "الحزام والطريق الرقمية"، وزارة الخارجية الصينية، 2020م.

2- الصعوبات في التكيف مع القوانين الدولية:

تواجه الصين تحديات كبيرة في التنسيق بين تشريعاتها الوطنية مع المعايير الدولية مثل GDPR في الاتحاد الأوروبي، مما قد يعرقل التعاون الدولي في مجال الأمن السيبراني.

3- التوترات الجيوسياسية وتأثيرها على الأمن السِّيبرَانِي:

تصاعد التوترات بين الصين والدول الغربية، مثل الولايات المتحدة، قد يؤدي إلى زيادة التهديدات السيبرانية، مما يعقّد قدرة الصين على حماية سيادتها الرقمية.

4- تعزيز الكفاءات الرقمية المحلية:

في ظل التطورات المتسارعة للتقنيات العالمية، تجد الصين نفسها في تحدٍ مستمر لتعزيز الكفاءات المحلية في مجالات مثل الذكاء الاصطناعي والجيل الخامس، وذلك لتقليل الاعتماد على الخارج.

5- الاعتماد على الأنظمة المحلية في مواجهة الأنظمة الغربية:

تعتمد الصين على أنظمة تشغيل وبرمجيات محلية مثلKylin ، ولكن تظل هناك تحديات تتعلق بتنافس هذه الأنظمة مع الأنظمة الغربية من حيث الكفاءة والابتكار.

الخاتمة

تناولت هذه الدراسة في مطلبها الأول التأصيل النظري للسيادة الرقمية والتهديدات السِّيبْرَانِيَّة ، وذلك من خلال توضيح مفهوم السيادة الرقمية وتطورها وأبعادها، وكذلك تم التعرف على مفهوم التهديدات السِّيبْرَانِيَّة وأنواعها، وفي المطلب الثاني تم التعرض لأثر التهديدات السِّيبْرَانِيَّة على السيادة الرقمية للصين وسبل معالجتها، وذلك من خلال تسليط الضوء على تأثير التهديدات السِّيبْرَانِيَّة على السيادة الرقمية في الصين، وأبرز السياسات والإجراءات التي تبنتها الصين لمواجهة تلك التهديدات لتعزيز سيادتها الرقمية، كما تم استعراض أبرز التحديات التي تواجه الصين أثناء تأمينها لفضائها الإلكتروني.

من خلال ما سبق، لوحظ أن تجربة الصين في حماية سيادتها الرقمية، أظهرت مدى أهمية تبني استراتيجيات متكاملة تجمع بين الجوانب القانونية والتقنية والاقتصادية، مع دعم قوي من الهيكل التنظيمي والرقابي، إلا أنه على الرغم من النجاحات التي حققتها الصين في

مجال الأمن السيبراني، خصوصا فيما يتعلق بابتكار أنظمة تقنية محلية موازية للأنظمة العالمية، ما زالت هناك تحديات تتطلب تحديثاً مستمراً للأطر التشريعية التي تتماشى مع التطورات التكنولوجية العالمية بما لا يمس السيادة الرقمية للصين.

وقد توصلت الدراسة إلى النتائج التالية:

1- أظهرت الدراسة أن السيادة الرقمية أصبحت جزءًا أساسيًا من الأمن القومي، حيث تسعى الدول إلى حماية فضائها السيبراني وتعزيز استقلالها الرقمي.

2- بيّنت الدراسة أن التهديدات السِّيبْرَانِيَّة تشكل تحديًا حقيقياً لسيادة الدول، سواء من خلال الهجمات الإلكترونية أو استغلال البيانات، مما يستدعي تطوير سياسات أمنية صارمة.

3- كشفت الدراسة أن الصين اعتمدت استراتيجيات شاملة لحماية سيادتها الرقمية، شملت الإطار القانوني، وتطوير التكنولوجيا، وحماية البيانات، وتعزيز التعاون الدولي في المجال السيبراني.

4- رغم نجاح السياسات الصينية، لا تزال هناك تحديات تتعلق بالتوترات الجيوسياسية، والاعتماد على التكنولوجيا الأجنبية، والانتقادات المتعلقة بحرية الإنترنت وحقوق الأفراد.

5- أكدت الدراسة أن مواجهة التهديدات السِّيبْرَانِيَّة تتطلب تعاونًا دوليًا، حيث لا يمكن لأي دولة بمفردها حماية فضائها الرقمي بشكل كامل.

التوصيات:

1- ضرورة تطوير القوانين الوطنية التي تحمي البيانات والسيادة الرقمية، مع ضمان التوازن بين الأمن السيبراني وحقوق الأفراد.

2- يمكن للدول الأخرى الاستفادة من السياسات الصينية في تعزيز الأمن السِّيبْرَانِي، مع تكييفها وفقًا لاحتياجاتها الوطنية.

3- ينبغي للدول تقليل الاعتماد على الشركات الأجنبية في البنية التحتية الرقمية، وتعزيز الصناعات التقنية المحلية لضمان استقلالها السِّيبْرَانِي.

4- توصي الدراسة بإنشاء تحالفات سِيبْرَانِيَّة بين الدول لتعزيز تبادل المعلومات، وتطوير آليات مشتركة لمكافحة التهديدات السيبرانية، والتعاون في وضع معايير دولية للأمن الرقمي.

5- يجب تنفيذ برامج توعوية تهدف إلى تعزيز وعي الأفراد والمؤسسات بمخاطر التهديدات السِّيبْرَانِيَّة وأهمية حماية البيانات.

6- توصي الدراسة بزيادة الاستثمار في الأبحاث العلمية المتعلقة بالأمن السِّيبْرَانِي، والذكاء الاصطناعي، وتطوير أنظمة الدفاع السِّيبْرَانِي المتقدمة.

7- ينبغي على الحكومات أن توازن بين تعزيز الأمن الرقمي وحماية حرية التعبير، لضـــمان بيئة إلكترونية آمنة دون المســـاس بالحقوق الأساسية للمستخدمين.

إن تبني التوصيات الاستراتيجية المقترحة قد يُسهم في رفع مستوى الأمان الرقمي وضمان استقلالية الفضاء الإلكتروني الوطني، مما يجعل النموذج الصيني مرجعاً يُحتذى به في مواجهة التهديدات السِّيبْرَانِيَّة العالمية.

قائمة المراجع

أولًا/ الوثائق:

1- الحكومة الصينية، قانون دعم الشركات الوطنية لعام 2020م.

2- وزارة الأمن السِّيبْرَانِي الصينية، "التحديثات التشريعية" لعام 2022م.

3-وزارة الخارجية الصينية "الحزام والطريق الرقمية." 2020م.

4-مركز البحوث التقنية الصينية، تحول النظم الرقمية في الصين: حالة نظام .Kylin بكين، 2020م.

5-الأمم المتحدة، اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، نشرة التكنولوجيا من أجل التنمية في المنطقة العربية، 2019م.

6-وزارة الأمن الوطني الصينية، "الرقابة الصينية على تدفق البيانات عبر الحدود" 2019م.

7-الصين، قانون الأمن السيبراني لعام 2017م.

ثانيًا/ الكتب:

1- زكريا، أحمد، **الأمن السِّيبْرَانِي والتهديدات الإلكترونيَّة: دراسة في مفهوم وطرق الوقاية**، مركز دراسات الأمن السيبراني، 2018م.

2-القيسي، عبد الله، **تهديدات الأمن السِّيبِرَانِي: دراسة تحليلية في الهجمات الإلكترونية**.، القاهرة: دار الفكر العربي، 2020م.

3-Gu, Hongfei. Data, Big Tech, and the New Concept of Sovereignty. Beijing: Beijing Press, 2023.

ثالثًا/ الدوريات:

1-بيرم، فاطمة، "السيادة الوطنية في ظل الفضاء السِّيبْرَانِي والتحولات الرقمية "**المجلة الجزائرية للأمن الإنساني**، المجلد 5، العدد1، 2020 م.

2-جيجان، إسراء شريف، "الأمن السِّيبْرَانِي الصيني "، **مجلة قضايا سياسية**، كلية العلوم السياسية، جامعة النهرين، العدد 65 ،2021م.

3-حميل، مصطفى، "السيادة الرقمية والتحول الرقمي: التحديات والحلول الهيكلية"، **مجلة رقمنة للدراسات الإعلامية والاتصالية**، العدد 3 ،31 ديسمبر 2022م.

4-شحيرط، أحمد، "تحديات الإنترنت لسيادة الدول السيادة الرقمية"، **مجلة البحوث القانونية والاقتصادية**، المجلد 5، العدد 1، الجزائر، 2022م.

5- السمرة، يوسف، "التحديات الرقمية وأمن المعلومات في الوطن العربي"، مجلة **رؤية**، الإمارات، العين، 2020م.

6-شرايطية، سميرة، "السيادة السِّيبْرَانِيَّة في الصين: بين الحماية والهيمنة"، مجلة **الأمن والتنمية**، الجزائر،2020م.

7-الشمري، خالد، "التهديدات السِّيبْرَانِيَّة: أساليب الوقاية والتصدي"، مجلة **الأمن السيبراني**، العدد 7، الرياض، 2019م.

8-عوامر، فاطمة، "أثير القوة السِّيبْرَانِيَّة على الاستراتيجيات الأمنية للدول الكبرى: دراسة حالة – الصين"، **مجلة الأمن والتنمية**، الجزائر،2018م.

9-عيسى، ناصر محمود، "استراتيجيات الأمن السِّيبْرَانِي في مواجهة التهديدات المتزايدة"، مجلة **الدراسات الاستراتيجية**، المجلد 5، العدد 2،2021م.

10-المجالي، سليمان، "مفاهيم الأمن السِّيبْرَانِي وتهديداته"، **مجلة دراسات الأمن السيبراني**، العدد 12، عمان، 2020م.

11-يوسف، عبد الحميد، "السيادة الرقمية ومتطلبات الأمن القومي"، **مجلة النهضة**، بيروت 2020م.

رابعًا/ الصحف والإنترنت:

1. "الصين أكبر هدف للهجمات الإلكترونية في العالم"، العين الإخبارية، 24 فبراير 2019م- https://al-ain.com/article/china-cyber-attack.
2. "الرقابة على الإنترنت في الصين" صحيفة جلوبال تايمز، 2021م.
3. " الصين والطريق إلى القطبية السِّيبْرَانِيَّة "، إندبندنت العربية، 2025م.
4. "WannaCry: The Ransomware Attack That Hit 150 Countries." BBC News, May- 2017. https://www.bbc.com/news/technology-39920141.