الحوكمة السيبرانية: المفهوم والتنافسية الدولية

م.م نورا رياض الدباغ
مركز الدراسات الإستراتيجية والدولية / جامعة بغداد
noura.r@cis.uobaghdad.edu.iq
https://doi.org/10.61884/hjs.v14i57.703

ملخص :

الحوكمة السيبرانية بوصفها أداة جيوسياسية فاعلة في التنافس الدولي المعاصر، بعد تحول الفضاء الرقمي من مجال تقني إلى ساحة تنافس على النفوذ والسيادة وإعادة تشكيل موازين القوة، ويحلل البحث نماذج الحوكمة التي تطرحها الولايات المتحدة والصين والاتحاد الأوروبي، ويقارن بين منطلقاتها السياسية والتنظيمية، كما يقيّم موقع المنطقة العربية ضمن هذا التنافس، مُبرزاً تحديات التبعية التقنية وضعف التنسيق، يقترح مساراً استراتيجياً عربياً لتعزيز السيادة الرقمية والحضور الدولي.

الكلمات المفتاحية: الحوكمة السيبرانية، السيادة الرقمية، الأمن السيبراني.

Cyber Governance: Concept and International Competitiveness

Asst. Lecturer Noura Riyadh Al-Dabbagh
Center for Strategic and International Studies / University of Baghdad
Email: noura.r@cis.uobaghdad.edu.iq

ABSTRACT

This cyber governance as an effective geopolitical instrument in contemporary international competition, following the transformation of cyberspace from a purely technical domain into an arena for contestation over influence, sovereignty, and the reconfiguration of power balances. The research analyzes the cyber governance models advanced by the United States، China،

and the European Union, comparing their political and regulatory foundations. It further assesses the position of the Arab region within this competitive landscape, highlighting challenges related to technological dependency and weak regional coordination. The study proposes a strategic Arab pathway aimed at strengthening digital sovereignty and enhancing international presence.

KEYWORDS: Cyber Governance, Digital Sovereignty, Cybersecurity

المقدمة:

أضحى الفضاء السيبراني ساحةً محورية للتنافس الدولي، بعد انتقاله من مجال تقني إلى فضاء تتقاطع فيه مفاهيم السيادة والأمن والنفوذ، إذ يُستخدم مفهوم التنافس في هذا البحث للدلالة على تنافس إستراتيجي صفري يقوم على فرض المعايير واحتواء الخصوم والتحكم بتدفقات البيانات لا على التعاون المتكافئ، وفي هذا السياق، برزت الحوكمة السيبرانية بوصفها أداة جيوسياسية تسعى القوى الكبرى فيها إلى ترسيخ رؤاها، بين نموذج الإنترنت المفتوح الذي تقوده الولايات المتحدة، ونموذج السيادة الرقمية الذي تدفع به الصين، والمقاربة التنظيمية الأوروبية القائمة على حماية الخصوصية والحقوق، وفي المقابل، لا تزال الجهود العربية متفرقة ومحدودة التأثير في ظل غياب إطار موحّد للسياسات الرقمية، مما يضعف القدرة على حماية المصالح الإستراتيجية، ومن هنا، يهدف هذا البحث إلى تحليل الحوكمة السيبرانية وأبعادها الدولية، مع التركيز على التنافس بين القوى الكبرى وتحديات المنطقة العربية.

أهمية البحث:

تأتي أهمية البحث من تحليل الحوكمة السيبرانية بوصفها أداة جيوسياسية في التنافس الدولي، مع إبراز تباين نماذج القوى الكبرى وانعكاسها على السيادة الرقمية،كما يسلّط الضوء على واقع الدول العربية، مبيناً أثر غياب التنسيق في تعميق التبعية التقنية وإضعاف حماية المصالح الإستراتيجية في الفضاء السيبراني.

هدف البحث:

يهدف البحث إلى مقارنة نماذج الحوكمة السيبرانية التي تطرحها القوى الكبرى، وبيان آثار التنافس الدولي في تشكيل قواعد السيادة الرقمية، مع تشخيص التحديات البنيوية التي تواجه المنطقة العربية في هذا السياق.

إشكالية البحث:

كيف تُوظَّف الحوكمة السيبرانية بوصفها أداة للتنافس الدولي على النفوذ والسيادة الرقمية في ظل غياب إطار دولي موحّد، وما انعكاس ذلك على موقع وقدرة المنطقة العربية في النظام السيبراني العالمي؟

فرضية البحث:

إن تباين نماذج الحوكمة السيبرانية التي تعتمدها القوى الكبرى يعكس طبيعة التنافس الدولي على النفوذ والسيادة الرقمية، وأن غياب إطار عربي موحّد للحوكمة السيبرانية يُسهم في تعميق التبعية التقنية ويحدّ من قدرة المنطقة العربية على التأثير في قواعد النظام السيبراني العالمي.

منهجية البحث:

يرتكز البحث على المنهج التحليلي لرصد تطور مفهوم الحوكمة السيبرانية وأبعاده الدولية، وعلى المنهج المقارن للمقارنة بين النماذج المختلفة التي تطرحها القوى الكبرى.

المبحث الأول

المفهوم النظري للحوكمة السيبر انية و أبعاده الدولية

شهد الفضاء السيبراني تحولاً من مجال تقني إلى ساحة ترتبط بالأمن والسيادة والنفوذ الدولي، ما أفرز الحاجة إلى الحوكمة السيبرانية، ومع تصاعد التهديدات الرقمية، غدا تنظيم هذا الفضاء مطلباً دولياً لحماية البنى التحتية والبيانات وحقوق الأفراد، لتتبلور الحوكمة السيبرانية بوصفها إطاراً لإدارة التفاعلات الرقمية وأداة لإعادة تشكيل موازين القوة في النظام الدولي.

المطلب الأول: تطور مفهوم الحوكمة السيبر انية

بدأت الحوكمة السيبرانية تتبلور بوصفها مفهوم أكاديمي وبحثي منذ سبعينيات القرن العشرين، مع ظهور مصطلحات تقنية جديدة مثل: الفيروسات وحصان طروادة، التي أثارت النقاشات الأولى حول التهديدات الرقمية، وفي منتصف الثمانينيات، انتقل الأمن السيبراني من إطار نظري إلى واقع عملي، خصوصاً بعد حادثة اختراق (ماركوس هِس) عام (١٩٨٦) لأنظمة حكومية أمريكية، من بينها حواسيب عسكرية، ومثّل هذا الهجوم نقطة تحوّل مؤسسية، دفعت الحكومات والشركات إلى تبنّي إجراءات أولية لمواجهة المخاطر السيبرانية[١] وفي أواخر الثمانينيات، تبلورت صناعة الأمن السيبراني بوصفه مجال تجاري منظم، كان الرئيس الأمريكي رونالد ريغان أول رئيس عالج مشكلة التهديدات السيبرانية بالمعنى الحالي، إذ طُرحت برامج مضادات الفيروسات التجارية لأول مرة عام (١٩٨٧)، هذا التطور عكس إدراكاً عالمياً بأن التهديدات الرقمية لم تعد مجرد إحتمالات، بل واقع يتطلب أدوات تقنية ومؤسسية وقانونية، وهو ما وضع اللبنة الأولى لجدل حول (الحوكمة السيبرانية) بوصفها موضوع أكاديمي وإستراتيجي مستمر حتى اليوم [٢].

أثر مفهوم (حوكمة الأمن السيبراني) أو ما يُعرف بـ (حوكمة الإنترنيت) على أنظمة الإدارة في العالم وبرز إلى الواجهة بوصفه إنعكاساً لما يجري في الفضاء الإلكتروني [٣]. وتطور الأمن

---

(١) «تأريخ الأمن السيبراني – ذكريات وبعض الحنين – الجزء الثاني»، موقع روبودين، ١٢ شباط ٢٠٢٤، تم الوصول إليه في ٧ شباط ٢٠٢٥، https://robodin.com/cybersecurity-history-part٢/

(2) Serkan Savaş and Süleyman Karataş ,"Cyber Governance Studies in Ensuring Cybersecurity: An Overview of Cybersecurity Governance،" International Cybersecurity Law Review 3 (2022): 13, https://doi.org/10.1365/s43439-021-00045-4

(3) Kamil Tarhan ،"Historical Development of Cybersecurity Studies: A Literature Review and Its Place in Security Studies" Przegląd Strategiczny ,International Islamic University Malaysia ,Issue 15 (2022): 395.

السيبراني في ثمانينيات وتسعينيات القرن العشرين مع الانتشار الواسع للإنترنت وشبكات الحاسوب، إذ انصبّ التركيز في بدايته على الحلول التقنية كجدران الحماية وبرامج مكافحة الفيروسات، ومع تصاعد التهديدات، بدأت المؤسسات والحكومات بإدراك الحاجة إلى أطر تنظيمية وسياسات وقائية، وهو ما تجسّد في إنشاء فريق الاستجابة لحالات الطوارئ الحاسوبية (CERT) عام (١٩٨٨) من قبل وزارة الدفاع الأمريكية، لاحقاً، اتجهت الدول إلى تقنين ممارسات الأمن السيبراني، وكان من أبرزها قانون (جرام–ليتش–بليلي) لعام (١٩٩٩)، الذي ألزم المؤسسات المالية بتطبيق معايير صارمة لحماية بيانات العملاء[١].

على الرغم من الجهود الدولية المبكرة، عجزت الأمم المتحدة عن بلورة إطار واضح يحدّد المسؤولية السيادية للدول في الفضاء السيبراني، وقد تجلّى ذلك في فشل مجموعة الخبراء الحكوميين عام (٢٠١٧) في التوصل إلى توافق بشأن قواعد السلوك السيبراني، بما عكس عمق الانقسام بين القوى الكبرى، و في أعقاب ذلك، طرحت روسيا عام (٢٠١٩) مبادرة داخل الجمعية العامة أدت إلى إنشاء مجموعة عمل مفتوحة العضوية، أنهت أعمالها عام (٢٠٢١) بإصدار تقرير توافقي أكد مبادئ احترام القانون الدولي، وتعزيز الشفافية، وبناء الثقة بين الدول[٢]. يعكس ذلك بوضوح تحول الفضاء السيبراني إلى ساحة تنافس دولي محتدم، تسعى فيها الدول إلى ترسيخ رؤاها الخاصة لمعايير الحوكمة السيبرانية بما يخدم مصالحها الإستراتيجية، وبذلك، غدت الحوكمة السيبرانية جزءاً لا يتجزأ من التنافس الجيوسياسي العالمي، على غرار مجالات التسليح والطاقة [٣].

إن النظر إلى الحوكمة السيبرانية بوصفها أداة لتنظيم الفضاء الرقمي العالمي يعكس التعامل مع الإنترنت والبنية المعلوماتية بوصفها مجال تنافس بين الدول على صياغة القواعد والمعايير بما يخدم قيمها ومصالحها، وفي هذا السياق، سعت الأمم المتحدة عام (٢٠٢٤) إلى بلورة الميثاق الرقمي العالمي (Global Digital Compact) بهدف إرساء مبادئ مشتركة لحوكمة

(1) CIO Hub ,"The Evolution of Cybersecurity Governance" (March 2021 https://ciohub.org/post/2021/03/the-evolution-of-cybersecurity-governance/

(2) Saeme Kim ,"Roles and Limitations of Middle Powers in Shaping Global Cyber Governance" The International Spectator 57, no. 3 (2022): 31,https://doi.org/10.1080/03932729.2022.2097807

(٣) خالد وليد محمود، الفضاء السيبراني وتحولات القوة في العلاقات الدولية (بيروت: المركز العربي للأبحاث ودراسة السياسات، ٢٠٢٥)، ص٩٣.

التكنولوجيا الرقمية تراعي انفتاح الإنترنت وأمنه وشمولية الاستفادة منه[١]، و كذلك أُنشئ منتدى حوكمة الإنترنت (IGF) بوصفه محفلاً سنوياً متعدد الأطراف للنظر في قضايا إدارة الإنترنت عالمياً[٢].

لغوياً: مصطلح الحوكمة في الأصل مشتق من مفردة يونانية تعني (توجيه السفينة)، إصطلاحياً: الحوكمة هي الترجمة المختصرة الرائجة لمصطلح (Corporate Governance)، أما الترجمة العلمية للمصطلح هو (أسلوب ممارسة السلطات للإدارة الرشيدة)[٣]، فعندما يتعلق الأمر بأمن المعلومات و الشبكات فإن عملية توجيه الموارد تتم عن طريق التنسيق بين الحكومات مع القطاع الخاص وصولاً الى المنظمات الدولية،[٤] و بالتالي تشير حوكمة الأمن السيبراني إلى مكون الحوكمة الذي يعالج إعتماد الموسسة على البيانات الرقمية و المعلومات في الفضاء السيبراني، و لأن تدفق البيانات و المعلومات منتشر بشكل كبير بين العوالم السيبرانية فالحوكمة في سياقها السيبراني تعتمد على أمن أنظمة المعلومات [٥].

يُقصد بمفردة سيبرانية لغوياً كل ما هو مرتبط بشبكات الحاسب الآلي بمختلف أنواعها مثل: شبكةالإنترنت أو بالإتصالات الإلكترونية[٦]، أما مصطلح السيبرانية بوصفها تخصُّص علمي تهتم بحماية سيادة الدولة وشبكات المعلومات الخاصة بها، و تشمل بحكم تعريفها:

(1) Anita Gurumurthy, Nandini Chami, and Amay Korjan "A Southern Agenda for Global Digital Governance," in Future of Global Governance: Perspectives from Global South, ed. Global Policy Watch and Social Watch (Global Policy Watch، 2024), accessed July 21,2025,https://www.globalpolicywatch.org/futureofglobalgovernance/index/f-a-southern-agenda-for-global-digital-governance/

(٢) المركز الإفريقي لمعلومات الشبكة (AFRINIC)، «حوكمة الإنترنت»، تم الدخول إليه في ٢١ تموز ٢٠٢٥، text:~:#https://www.afrinic.net/ar/internet-governance=منتدى٪٢٠حوكمة٪٢٠الإنترنت

(٣) كريم عادل عبيد، إستراتيجيات الحوكمة الرقمية وتطبيقاتها الذكية – الجزء الأول (ليبيا: دار البيان للنشر والتوزيع والإعلان، ٢٠٢٢)، ص٢٣.

(4) Michel van Eeten, Hans De Bruijn، Mirjam Kars, and Haiko Van Der Voort, "The Governance of Cybersecurity: A Framework for Policy," International Journal of Critical Infrastructures Vol. 2, no. 4 (United Kingdom, 2006): 359.

(5) Deb Bodeau et al, Cyber Security Governance: A Component of MITRE's Cyber Prep Methodology, Technical Report (MITRE Corporation، September 2010), 1.

(٦) محمد أحمد لبيب أحمد، وهيثم محمد بهاء القاضي، ومستشار مصطفى أحمد كمال، «دور الاتفاقيات الدولية والإقليمية في مجال الأمن السيبراني وموقف الدولة المصرية منها،» مجلة JGPCC، المجلد ١، العدد ١ (أيلول ٢٠٢٤): ص١٢٨.

أمن الشبكات والأنظمة المعلوماتية والبيانات والمعلومات والأجهزة المتصلة بالإنترنت بشكل عام، و تُعرف أيضاً بأنها: النشاط الذي يؤمّن حماية الموارد البشرية والمالية المرتبطة بتقنيات الإتصالات والمعلومات، وتتضمن مواجهة التهديدات والأخطار التي تتعرَّض لها الشبكات السيبرانية من هجمات ومحاولات إختراق خصوصية المعلومات والبيانات الحيوية بالنسبة للمؤسسة أو للدولة التي تتعرَّض للهجوم أو للإختراق السيبراني، وإستغلال هذه المعلومات والبيانات بما يُهدّد سيادة الدولة أو إستقلالية ومصالح المؤسسة المعنية [١].

تُفهم الحوكمة السيبرانية في بعدها السياسي بوصفها توظيفاً منظماً لتكنولوجيا المعلومات والاتصالات لتعزيز التفاعل بين الدولة والمجتمع، ورفع كفاءة الإدارة العامة وتحسين تقديم الخدمات الرقمية، ومع تصاعد التهديدات السيبرانية، تجاوز هذا المفهوم الإطار التقني ليغدو نموذجاً تعاونياً قائماً على الشراكة والمسؤولية المشتركة بين الدولة والفاعلين الآخرين، بما يضمن حماية الفضاء الرقمي وصون الصالح العام وحقوق الأفراد، ويظل نجاح هذا النموذج مشروعاً بالحد من المخاطر السيبرانية، عبر تعاون مؤسسي منظم يقوم على الشفافية والمساءلة والالتزام بالمعايير الدولية [٢].

تُفهم الحوكمة السيبرانية في بعدها السياسي بوصفها توظيفاً منظماً لتكنولوجيا المعلومات والاتصالات لتعزيز التفاعل بين الدولة والمجتمع، ورفع كفاءة الإدارة العامة وتحسين تقديم الخدمات الرقمية

تقوم الحوكمة السيبرانية على تعدد الفاعلين المنخرطين فيها، وتشمل الحكومات، والمنظمات الدولية، والشركات، ومنظمات المجتمع المدني، فضلاً عن المستخدمين، إذ تضطلع الحكومات بوضع الأطر القانونية والتنظيمية وتعزيز الأمن السيبراني، بينما تسهم المنظمات الدولية في صياغة المعايير المشتركة وتقديم الدعم، وتتحمل الشركات مسؤولية تطوير الحلول التقنية الآمنة، في حين تعمل منظمات المجتمع المدني على رفع الوعي والمتابعة الرقابية، ويبقى للمستخدمين دور أساسي في تبنّي الممارسات الرقمية الآمنة بما يعزز حماية الفضاء السيبراني[٣].

(١) محمد جمال علي، «السيبرانية والحوكمة: بين ممارسة السيادة وحقوق الإنسان،» قضايا ونظرات: تقرير ربع سنوي، مركز الحضارات للدراسات والبحوث، القاهرة، العدد ٢١ (٢٠٢١): ص٤٤.

(٢) منال السيد، «آليات تطبيق الحوكمة الرقمية في القطاع الحكومي: دروس مستفادة من الخبرة الدولية»، مجلة كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، العدد ٣ (٢٠٢٤): ص٢٦٧.

(٣) يوسف مناصرة، «التوفيق بين حوكمة الإنترنت والأمن السيبراني للدول»، مجلة صوت القانون، العدد ٩ (٢٠٢٣): ص٣٢٥.

المطلب الثاني: فواعل ونماذج الحوكمة السيبرانية

أضحت الحوكمة السيبرانية أداة فاعلة لفرض النفوذ والتحكم في تدفق البيانات عبر الحدود، مما أوجد توتراً متصاعداً بين مبدأ السيادة الرقمية وفكرة الإنترنت المفتوح، وفي هذا السياق، تؤدي الولايات المتحدة دوراً محورياً في صياغة سياسات الفضاء السيبراني وفق نموذج الحوكمة متعدد أصحاب المصلحة، الذي يشرك القطاع الخاص والمجتمع المدني والخبراء التقنيين، ويرتكز على حرية الإنترنت وحماية الحقوق الأساسية، ولا سيما حرية التعبير وتدفق المعلومات[١]، في المقابل سعت الدول إلى تبني إستراتيجيات السيادة الرقمية التي تُعنى ببسط سيطرة الدولة على البنية التحتية الرقمية والبيانات ضمن حدودها[٢]،إذ تجلّت هذه نزعة لدى قوى كبرى مثل: الصين و روسيا، عبر تبنّي قوانين صارمة لفرض قيود محلية على حركة البيانات والبنية التحتية الرقمية ضمن نطاقها الوطني[٣].

من جانب أخر، الشركات التقنية العالمية باتت هي الأخرى جهات حاكمة فعلياً في الفضاء السيبراني، بمعنى أنها تمارس نفوذاً يتجاوز الدولة فيما يُسمى بـ (حوكمة المنصات) أي أن سياساتها الداخلية وخوارزمياتها ترسم قواعد النظام الرقمي العالمي إلى حد كبير. مثل: شركات وادي السيليكون (*) مثل: غوغل (Google)، ميتا (Meta/Facebook)، آبل (Apple)، مايكروسوفت (Microsoft)، أمازون (Amazon)على الجانب الأمريكي، وشركة هواوي (Huawei) على الجانب الصيني التي أصبحت محوراً للتنافس الأمريكي-الصيني في مجال البنى التحتية لشبكات الجيل الخامس، كل تلك الشركات تمتلك منصات وبنى تحتية رقمية حاسمة، ما يخوّلهم وضع معايير تقنية وسلوكيات إستخدام تُفرض بحكم الأمر الواقع على

(1) Ho Ting Hung, "Exploring China's Cyber Sovereignty Concept and Artificial Intelligence Governance Model: A Machine Learning Approach," Journal of Computational Social Science 8, no. 1 (2025): 24, https://doi.org/10.1007/s42001-024-00346-8.

(٢) مصطفى مجدي، «السيادة السيبرانية ومستقبل الإنترنت»، مسار، ١٦ شباط ٢٠٢٢، تاريخ الاطلاع ١٧ تموز ٢٠٢٥، https://masaar.net/ar/السيادة-السيبرانية-ومستقبل-الإنترنت/

(3) Diba Aalami Harandi, "International Legal Frameworks on Cybersecurity and Data Protection Law," Denver Journal of International Law & Policy, January 7, 2025, accessed July 21, 2025, https://djilp.org/international-legal-frameworks-on-cybersecurity-and-data-protection-law/

مليارات المستخدمين عبر الحدود [١].

تحولت المنظمات الدولية المعنية بوضع معايير الفضاء السيبراني إلى ساحات تنافس غير مباشر بين القوى الكبرى، تسعى كل منها إلى ترسيخ رؤيتها الخاصة للحوكمة، فلم تعد هذه المنظمات محايدة تقنياً، بل أصبحت محافل لتنازع الشرعية السيبرانية، وفي هذا الإطار، يُعدّ الاتحاد الدولي للاتصالات (ITU) منصة تفضّلها الدول الداعمة لمشاريع السيادة الرقمية، مثل الصين وروسيا، عبر مقترحات كمشروع (New IP) الذي يمنح الدول صلاحيات موسعة للتحكم بالشبكات وتدفقات البيانات،و في المقابل، تدافع الولايات المتحدة وحلفاؤها عن نموذج الحوكمة التشاركية متعددة أصحاب المصلحة، الذي تجسّده المؤسسة المعنية بإدارة أسماء وأرقام الإنترنت (ICANN)، بوصفه نموذجاً ليبرالياً قائماً على إدارة تقنية مستقلة بعيداً عن الهيمنة الحكومية المباشرة[٢].

وعليه، تتبلور ثلاثة نماذج متباينة للحكم الرقمي تمثلها القوى الدولية الكبرى: الولايات المتحدة والصين والإتحاد الأوروبي، إذ يعالج كل أنموذج مجموعة مبادئ مختلفة للحوكمة السيبرانية، والمنطقة العربية في هذا السياق، لا تمثل أنموذجاً مستقلاً للحوكمة السيبرانية، بل ساحة تفاعل وتأثر بين هذه المقاربات المتنافسة [٣]:

---

(١) (*) أُطلق إسم وادي السيليكون (Silicon Valley) على البقعة الجنوبية من خليج سان فرانسيسكو؛ لأن المنطقة كانت مركزاً رئيسياً لصناعة أشباه المُوصلات، التي تعتمد بشكل أساسي على عنصر السيليكون في تصنيع الترانزستورات والدوائر المتكاملة. لعب دور السيليكون الحيوي في الثورة التقنية وبروز الشركات المتخصصة فيه دوراً أساسياً في إختيار الإسم الإقتصادي والتكنولوجي للمكان في البداية. إحتضن الوادي شركات متخصصة في تصنيع الشرائح الإلكترونية، وهو ما جعله قلب الثورة التكنولوجية في الولايات المتحدة، مع مرور الوقت توسع النشاط ليشمل الحواسيب، والبرمجيات، ثم لاحقاً الإنترنت والتطبيقات الرقمية الكبرى و شركاتها. للمزيد من التفاصيل أنظر:
Don Hoefler, "Who Named Silicon Valley?،," Computer History Museum Blog, January 7, 2015، https://computerhistory.org/blog/who-named-silicon-valley/

(3) Moore, G.J. Huawei, Cyber-Sovereignty and Liberal Norms: China's Challenge to the West/Democracies. J OF CHIN POLIT SCI 28, 154 (2023). https://doi.org/10.1007/s11366-022-09814-2

(2) Wolfgang Kleinwächter, "Internet Governance Outlook 2023: Will Digital Coop-Frontation' Become the 'New Normal'?," CircleID, January 11, 2023، accessed July 21, 2025, https://circleid.com/posts/20230111-internet-governance-outlook-2023-will-digital-coop-frontation-become-the-new-normal/

(٣) أحمد صلاح علي، «قوانين الخصوصية وحوكمة البيانات.. ساحة صراع بالذكاء الاصطناعي في ظل الحرب الباردة الجديدة»، الجزيرة نت، ٤ أيار ٢٠٢٥، تاريخ الاطلاع ١٧ تموز ٢٠٢٥، https://www.aljazeera.net/tech/٢٠٢٥/٥/٤/قوانين-الخصوصية-وحوكمة-البيانات-ساحة.

أ- **الأنموذج الأمريكي:** يرتكز النموذج الأمريكي التقليدي للحوكمة السيبرانية على مبدأ انفتاح الإنترنت وحرية تدفق المعلومات بوصفهما قيماً عليا، ومنذ تسعينيات القرن الماضي، قادت الولايات المتحدة ترسيخ نهج تعدد أصحاب المصلحة عالمياً، القائم على إدارة لامركزية للشبكة وبعيدة عن السيطرة الحكومية المباشرة، وقد انعكس ذلك في دعم حرية التعبير ومعارضة القيود السيادية على الإنترنت، انطلاقاً من قناعة بأن الإنترنت المفتوح يخدم المصالح الإستراتيجية والاقتصادية الأمريكية، وهو ما أتاح لشركات وادي السيليكون الهيمنة على الاقتصاد الرقمي العالمي[١]. و على الرغم من غياب قانون فدرالي شامل لحماية البيانات والخصوصية في الولايات المتحدة، يدفع البيت الأبيض وحلفاؤه باتجاه صياغة معايير دولية تعزز حرية التعبير وتداول المعلومات مع الحد من الرقابة الحكومية، ويعكس هذا النهج سعياً إلى الموازنة بين دعم الابتكار الرقمي وحماية الحقوق، بوصفه امتداداً لمنظومة الحوكمة السيبرانية التي أسستها واشنطن عبر كيانات تشاركية مفتوحة، مثل المؤسسة المعنية بإدارة أسماء وأرقام الإنترنت (ICANN)، بما يعزز إدارة دولية غير خاضعة للهيمنة الحكومية المباشرة [٢]. غير أن هذا الأنموذج الأمريكي ليس خالياً من أدوات النفوذ السيادي المستترة؛ فإمتلاك الولايات المتحدة لنصيب الأسد من البنية التحتية الأساسية للإنترنت ومنصاته مكنها ضمنياً من التأثير في تدفق البيانات العالمي، وقد أثبتت تسريبات سنودن (Snowden Leaks) (*) أن واشنطن إستغلت موقعها المهيمن لإعتراض كم هائل من الإتصالات الدولية، ما عدّه خصومها دليلاً على هيمنة سيبرانية أمريكية خلف ستار الإنترنت الحر الذي تدعيه[٣].

(1) CEPA (Center for European Policy Analysis), "US U-Turn Undermines Free, Open Internet," CEPA, May 8, 2024, accessed July 21, 2025, https://cepa.org/article/us-u-turn-undermines-free-open-internet

(2) Wolfgang Kleinwächter, "Developments in the Internet Governance Environment: October toDecember 2024" DENIC Blog, January 30, 2025, accessed July 22, 2025, https://blog.denic.de/en/developments-in-the-internet-governance-environment-october-to-december-2024/.

(*) تُعد تسريبات سنودن (Snowden Leaks) من أبرز الأحداث المفصلية في تأريخ الحوكمة السيبرانية، في حزيران عام (٢٠١٣)، سلّم سنودن وهو موظف سابق في وكالة الأمن القومي الأمريكية (NSA) آلاف الوثائق السرية إلى الصحافة، كاشفاً عن برامج مراقبة واسعة النطاق تقودها الوكالة، من بينها برنامج (PRISM) الذي يتيح جمع بيانات المستخدمين من شركات وادي السيليكون. **للمزيد من التفاصيل أنظر:**
Electronic Privacy Information Center (EPIC)، EPIC v. DOJ – PRISM، accessed July 21، 2025، https://epic.org/documents/epic-v-doj-prism/

(٣) مجدي، مرجع سابق.

ب- **الأنموذج الصيني:** تروّج الصين لنموذج حوكمة سيبرانية قائم على سيطرة الدولة، يمنح الحكومات صلاحية التحكم الكامل بمحتوى الإنترنت داخل حدودها الوطنية، وتعمل بكين على تصدير هذا النموذج عبر دعم دول أخرى بتقنيات الرقابة المستوحاة من (الجدار الناري العظيم)، بما يسهم في إعادة توجيه المعايير الدولية نحو فضاء سيبراني مركزي خاضع للسلطة الحكومية بدل النموذج المفتوح. كما سعت الصين إلى إضفاء شرعية دبلوماسية على هذا التوجه عبر مبادرات مثل: (بناء مجتمع ذي مستقبل مشترك في الفضاء السيبراني)، التي تؤكد أولوية دور الدولة في إدارة الإنترنت [١]، فالصين توكد على وجهتي نظر: من جهة، يجب أن تكون الدولة قادرة على المطالبة بالسيادة الرقمية في الفضاء السيبراني، ومن جهة أخرى، لا ينبغي للدولة التدخل في سيادة الدول الأخرى.

تروّج الصين لنموذج حوكمة سيبرانية قائم على سيطرة الدولة، يمنح الحكومات صلاحية التحكم الكامل بمحتوى الإنترنت داخل حدودها الوطنية

إذ يتميز أنموذج الحوكمة السيبرانية الصيني بالتحكم الصارم في المعلومات والبيانات، لتحقيق أربعة أهداف رئيسة [٢]:

أ- **الحفاظ على الإستقرار الداخلي:** تسعى بكين إلى الحفاظ على الإستقرار الإجتماعي والسياسي عبر السيطرة المشددة على تدفق المعلومات، ومنع إنتشار المحتوى الذي تعده ضاراً أو مزعزعاً لذلك الإستقرار[٣].

ب- **تقليل نقاط الضعف:** يهدف النموذج الصيني إلى تقليص نقاط الضعف في بنيته التحتية الرقمية وحماية أنظمته من الهجمات السيبرانية الخارجية، وتنطلق بكين من تصور يعد الفضاء السيبراني مائلاً لصالح الولايات المتحدة، بما يتيح لها، عبر الشركات الأميركية ذات الحضور الواسع ومنصات التواصل الاجتماعي، جمع البيانات وممارسة أنماط مختلفة من المراقبة، وهو ما يدفع الصين إلى تعزيز التحكم والسيادة على فضائها الرقمي[٤].

(1) Dakota Cary, Community Watch: China's Vision for the Future of the Internet, Global China Hub (Atlantic Council), December 4,2023 , accessed July 22, ,2025 https://www.atlanticcouncil.org/in-depth-research-reports/report/community-watch-chinas-vision-for-the-future-of-the-internet/.

(2) Tarhan, op. cit., 407.

(3) Noah Berman, Lindsay Maizland, and Andrew Chatzky, "Is China's Huawei a Threat to U.S. National Security?," Council on Foreign Relations, February 8, 2023, accessed July 21, 2025, https://www.cfr.org/backgrounder/chinas-huawei-threat-us-national-security

(4) Cary, op. cit.

ج- **ضمان الإستقلالية التكنولوجية:** تسعى الصين إلى تحقيق الاكتفاء الذاتي التكنولوجي للحد من اعتمادها على التقنيات الأجنبية وتعزيز سيادتها الرقمية، وترتكز هذه الإستراتيجية على مبادرة (طريق الحرير الرقمي) ضمن مشروع (الحزام والطريق)، التي تهدف إلى بناء بنية تحتية رقمية عالمية تقودها الصين، وفي هذا الإطار، تستثمر بكين بكثافة في كابلات الاتصالات البحرية وشبكات الجيل الخامس ومراكز البيانات في الدول النامية، بما يرسّخ اعتمادها على التكنولوجيا الصينية ويمنحها نفوذاً متزايداً على المفاصل الرقمية العالمية[١].

د- **توسيع النفوذ:** في تصدير نموذجها وتقنياتها، إذ تسعى الصين إلى توسيع نفوذها في صياغة المعايير والقواعد العالمية للحوكمة السيبرانية، مستندة إلى الدور المحوري لشبكات الجيل الخامس في إعادة تشكيل موازين القوة الرقمية، وتؤدي شركة هواوي (Huawei) دوراً مركزياً في هذا التوجه عبر الابتكار التكنولوجي وتعزيز الحضور الصيني عالمياً، في مقابل اعتماد الولايات المتحدة على أدوات القيود الاقتصادية والتقنية لاحتواء هذا الصعود[٢].

ج- **أنموذج الإتحاد الأوروبي:** يقدّم الاتحاد الأوروبي نفسه بوصفه طريقاً ثالثاً في الحوكمة السيبرانية، يوازن بين انفتاح الإنترنت وحماية السيادة الرقمية، عبر سيادة القواعد والمعايير بدلاً من السيطرة الشمولية أو الفوضى السوقية، انطلاقاً من مقاربة تعد الخصوصية حقاً أساسياً من حقوق الإنسان في العصر الرقمي[٣]، وينبع هذا النهج من إدراك مخاطر ترك الفضاء السيبراني دون حوكمة معتدلة، مع استمرار دعم الاتحاد لمبدأ الإنترنت المفتوح وحوكمة متعددة الأطراف، ضمن تصور «الإنترنت ذي القواعد» الذي يصون الحقوق ويحمي المصالح الأوروبية[٤]، يواصل الإتحاد الأوروبي تبني تشريعات رائدة لتنظيم التقنيات الناشئة، أبرزها: قانون الذكاء الاصطناعي لعام (٢٠٢٤) الذي يصنّف التطبيقات وفق مستويات المخاطر ويقيّد الاستخدامات عالية الخطورة، مثل المراقبة الجماعية، ورغم غياب شركات تقنية عملاقة تضاهي النفوذ الأميركي أو الصيني، يوظّف الاتحاد ثقله التنظيمي لفرض ضوابط وغرامات على شركات التكنولوجيا، خاصة الأميركية، في قضايا الاحتكار وانتهاك

(1) Air Marshal Anil Khosla, "The Digital Silk Road: Implication of China's Techno-Political Strategy," Life of Soldiers, February 20, 2025, accessed July 22, 2025, https://55nda.com/blogs/anil-khosla/2025/02/20/605-the-digital-silk-road-implication-of-chinas-techno-political-strategy/

(٢) إيهاب خليفة, «نماذج دولية لتمكين رقمي وسبل الاستفادة منها لمكافحة كورونا,» الملف المصري, العدد ٧٠ (٢٠٢٠): ١٧–٢٨.

(٣) علي, مرجع سابق.

(4) Cary, op. cit.

الخصوصية، ويتسم النهج الأوروبي بالتركيز على التنظيم القانوني الشامل، كما تجسّده اللائحة العامة لحماية البيانات (GDPR) وقانون المرونة السيبرانية، الهادف إلى تعزيز أمن المنتجات الرقمية قبل طرحها في الأسواق[١].

المبحث الثاني

التنافسية الدولية والإقليمية في الحوكمة السيبرانية

لم تعد الحوكمة السيبرانية إطاراً تنظيمياً تقنياً، بل غدت مجالاً للتنافس الإستراتيجي بين القوى الكبرى على قواعد إدارة الإنترنت والبيانات، بما يعكس انتقال التنافس الدولي إلى الفضاء الرقمي عبر التحكم بالبنية التحتية والمعايير، وفي هذا السياق، تتباين نماذج الحوكمة بين الولايات المتحدة والصين والاتحاد الأوروبي، فيما تواجه المنطقة العربية تحديات التبعية التقنية مقابل السعي إلى تعزيز الاستقلالية الرقمية.

المطلب الأول: المشاريع التنافسية الدولية للحوكمة السيبرانية

١- **مبادرة (الشبكة النظيفة) الأمريكية (Clean Network Initiative):** أُطلقت المبادرة في الولاية الأولى لإدارة ترامب في آب (٢٠٢٠) بوصفها جهداً إستراتيجياً يهدف إلى حماية البنية التحتية للاتصالات والتكنولوجيا في الولايات المتحدة وحلفائها من التهديدات الأمنية، ولا سيما المرتبطة بالصين. وجاءت المبادرة استجابة لمخاوف تصاعد النفوذ الصيني على البنية التحتية الرقمية عالمياً، خاصة في شبكات الجيل الخامس [٢]، وتأتي هذه المبادرة في سياق تنافس جيو-سياسي أوسع حول الحوكمة السيبرانية، إذ تسعى الولايات المتحدة إلى فرض معاييرها وقيمها الديمقراطية في مواجهة النماذج السائدة للسيطرة على الإنترنت والبيانات لإحتواء النفوذ الصيني [٣]، وتتمحور الأهداف الرئيسية للمبادرة حول حماية أصول الأمة، بما في ذلك خصوصية المواطنين والمعلومات الحساسة للشركات. يمكن تلخيص هذه

(1)European Union, "Data Protection and Online Privacy," Your Europe, published online (about 3.6 years ago), accessed July 22, 2025, https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.htm

(2)United States Department of State, "Building a Clean Network: Key Milestones," State.gov (archived), accessed July 22, 2025, via archived content at 2017–2021.state.gov (timeline page listing expansion milestones e.g. Brazil as 50th member on November 10, 2020) https://2017-2021.state.gov/building-a-clean-network-key-milestones/

(3) David P. Fidler, "The Clean Network Program: Digital Age Echoes of the 'Long Telegram'?" Council on Foreign Relations, October 5, 2020, accessed July 22, 2025, https://www.cfr.org/blog/clean-network-program-digital-age-echoes-long-telegram.

الأهداف في عدة نقاط منها: معالجة التهديد طويل الأمد الذي تشكله الأنظمة المنافسة على خصوصية البيانات والأمن وحقوق الإنسان، وبناء تحالف عالمي من الدول والشركات التي تلتزم بمجموعة مشتركة من المبادئ في تبني التكنولوجيا المتوافقة مع الرؤية الأمريكية، وذلك بهدف تعزيز النمو الإقتصادي والأمن القومي؛ في سياق ما يُوصف بأنه حرب باردة تكنولوجية جديدة بين واشنطن وبكين [1].

جدول يبين الدول المطبقة للحوكمة المطبقة في مبادرة الشبكة النظيفة

الفئة	الجهات الفاعلة الرئيسية في مبادرة الشبكة النظيفة	الأهمية الإستراتيجية
الدول	جمهورية التشيك، النرويج، بولندا، إستونيا، رومانيا، الدنمارك، اليونان، نيوزيلندا، اليابان، أستراليا، (إسرائيل)، لاتفيا، والمملكة المتحدة	تشكيل تحالف ديمقراطي لتوحيد المعايير الأمنية ومواجهة النفوذ التكنولوجي الصيني.
الشركات	أوراكل (Oracle)، إتش بي (HP)، سيسكو (Cisco)، في إم وير (VMware)، نيك (NEC)، فوجيتسو (Fujitsu)، سوفت بانك (SoftBank)	توفير بدائل تكنولوجية موثوقة للشركات الصينية، مما يضمن أمان سلاسل التوريد.
المنظمات	حلف الناتو، الإتحاد الأوروبي، منظمة التعاون الإقتصادي والتنمية (OECD)، مبادرة البحار الثلاثة	توفير أطر سياسية ودبلوماسية لتعزيز التعاون وتنسيق السياسات الأمنية.

الجدول من عمل الباحثة بالعودة إلى المصدر:
Gallagher، Jill C. Undersea Telecommunication Cables: Technology Overview and Issues for Congress. CRS Report R47237. Washington، DC: Congressional Research Service، September 13، 2022، 17. https://crsreports.congress.gov/product/pdf/R/R47237

إلا أن تلك المبادرة ليست الوحيدة في إطار الحوكمة السيبرانية الأمريكية، إذ أطلقت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية (CISA) مبادرة (الخطة الإستراتيجية الدولية للفترة ٢٠٢٥–٢٠٢٦) تأتي هذه الخطة إستجابةً لطبيعة التهديدات السيبرانية العابرة للحدود،

(1) Krach Institute for Tech Diplomacy, "Strategy," Tech Statecraft, accessed July 22, 2025, https://techdiplomacy.org/tech-statecraft/strategy/

و تعتمد المبادرة على أدوات حوكمة سيبرانية تشمل: تكثيف تبادل معلومات التهديد مع الشركاء الدوليين، وبناء قدرات الشركاء الدوليين عبر التدريب والتمارين السيبرانية المشتركة، ودعم تطوير معايير أمنية عالمية، وذلك بالتعاون الوثيق مع جهات حكومية أمريكية أخرى مثل: وزارة الأمن الداخلي و وزارة الخارجية، مما يعني إن المبادرة مثلت تحولاً في الإستراتيجية الإمريكية من المواجهة المباشرة مع الصين إلى نهج الحوكمة السيبرانية التعاونية مع الشركاء الدوليين[1].

ليس ذلك فحسب لمواجهة التحدي الصيني، تقود الولايات المتحدة جهوداً لتشكيل توازن خارجي عبر بناء شبكة من التحالفات الإستراتيجية والتكنولوجية، وتهدف هذه الإستراتيجيات إلى تقييد وصول الصين إلى التقنيات الحيوية **كما هو موضح في الجدول أدناه:**

المبادرة	الأعضاء الرئيسيون	الأهداف المشتركة
الحوار الأمني الرباعي (QUAD)	الولايات المتحدة، الهند، اليابان، أستراليا	تعزيز الأمن السيبراني، وضع معايير للذكاء الإصطناعي؛ لمواجهة التهديدات الصينية.
(AUKUS) أوكوس	الولايات المتحدة، أستراليا، المملكة المتحدة	التعاون في التقنيات الناشئة والمتقدمة مثل: الذكاء الإصطناعي والقدرات السيبرانية؛ لمواجهة النفوذ الصيني في منطقة المحيطين الهندي والهادئ.
تحالف الرقائق (Chip 4/Fab 4)	الولايات المتحدة، اليابان، تايوان، كوريا الجنوبية	تنسيق الجهود لإعادة هيكلة أشباه الموصلات العالمية؛ لتقليل الإعتماد على الصين وحماية الملكية الفكرية.
مجلس التجارة والتكنولوجيا (TTC)	الولايات المتحدة و الإتحاد الأوروبي	تنسيق السياسات المتعلقة بالتكنولوجيا والتجارة، بما في ذلك ضوابط التصدير على التقنيات الناشئة؛ لمواجهة التحديات التي تفرضها الصين.
المصدر	E. A. Rasheed، "Cyber Security in International Conflict: US China Cyber Competition and Its Impact on India،" Journal of Social Sciences Review 5، no. 2 (2025): 156–160، https://doi.org/10.62843/jssr.v5i2.549	

(1) Cybersecurity and Infrastructure Security Agency (CISA), "2025-2026 CISA International Strategic Plan," CISA.gov, accessed July 22, 2025, https://www.cisa.gov/2025-2026-cisa-international-strategic-plan

٢- **المبادرة العالمية لأمن المعلومات الصينية (Global Initiative on Data Security – GIDS):** طرحت الصين في أيلول من العام (٢٠٢٠) هذه المبادرة بوصفها رداً مباشراً على مبادرة الحوكمة السيبرانية الأمريكية المتمثلة بـ(الشبكة النظيفة)[١]. قدمت الصين فيها مجموعة مبادئ أساسية منها: إحترام سيادة كل دولة على بياناتها الرقمية، والإمتناع عن المراقبة الجماعية وجمع المعلومات الشخصية دون إذن، وضمان خلو المنتجات التكنولوجية من معايير التجسس الخفية التي قد تُستغل للوصول غير المشروع إلى المعلومات[٢]، وتهدف المبادرة الصينية في بعدها السياسي إلى تقديم الصين بوصفها فاعلاً داعماً للأمن الرقمي وتعزيز الاستثمارات في مجالي التكنولوجيا والاتصالات، في سياق سعيها لموازنة النفوذ الأميركي في صياغة قواعد الفضاء السيبراني، وتنتقد بكين ما تصفه بالنهج الأميركي الأحادي في قضايا أمن البيانات، وعدت مبادرة (الشبكة النظيفة) شكلاً من أشكال التنمّر الدولي، وترتبط بهذه المبادرة دول عدة، من أبرزها كازاخستان ولاوس وباكستان وسوريا وروسيا، وفي موازاة ذلك، واصلت الصين تطوير قدراتها الهجومية السيبرانية بوتيرة متسارعة، مع اتهامات دولية بتورط جهات مرتبطة بالدولة في عمليات تجسس سيبراني وحملات تضليل، إلى جانب اعتماد استراتيجية (الإندماج المدني–العسكري) التي توظّف التقنيات المتقدمة، بما فيها الذكاء الاصطناعي لأغراض عسكرية سيبرانية[٣].

تهدف المبادرة الصينية في بعدها السياسي إلى تقديم الصين بوصفها فاعلاً داعماً للأمن الرقمي وتعزيز الاستثمارات في مجالي التكنولوجيا والاتصالات، في سياق سعيها لموازنة النفوذ الأميركي في صياغة قواعد الفضاء السيبراني،

تُعد (خطة العمل لحوكمة الذكاء الاصطناعي العالمية ٢٠٢٥) من أبرز مبادرات الصين في إطار الحوكمة السيبرانية، وقد قُدمت بوصفها أداة منافسة مباشرة للرؤية الأمريكية، وأُطلقت

(1) Nigel Cory and Zhiwei Chen, "China Unveils New Framework To Stimulate Cross-Border Data Flows: Risk or Opportunity for Multinational Companies," Crowell & Moring LLP – Client Alert, January 13, 2025, https://www.crowell.com/en/insights/client-alerts/china-unveils-new-framework-to-stimulate-cross-border-data-flows-risk-or-opportunity-for-multinational-companies/

(2) Marek Wąsiński and Damian Wnukowski, "U.S. Tightens Policy Towards China Amidst the COVID-19 Pandemic," PISM Bulletin no. 148 (1578), 13 July 2020, p. 2.

(3) Reuters, "China unveils global data security initiative, says some countries bullying others," Reuters, September 8, 2020, https://www.reuters.com/article/technology/china-unveils-global-data-security-initiative-says-some-countries-bullying-othe-idUSKBN25Z064/

الخطة في مؤتمر الذكاء الاصطناعي العالمي في شنغهاي، وتهدف إلى تعزيز التعاون الدولي في تطوير وتنظيم تقنيات الذكاء الاصطناعي، مع التأكيد على احترام سيادة الدول ودعم أهداف التنمية الأممية [١].

ثالثاً: قانون البيانات الأوروبي (Data Act): صدر هذا القانون في كانون الثاني عام (٢٠٢٤) بوصفه حجر زاوية في استراتيجية الاتحاد الأوروبي للبيانات وتحقيق رؤيته الرقمية، وجاء استجابة لهيمنة الشركات التقنية الكبرى، ولا سيما الأميركية، على البيانات، ويهدف إلى صياغة نهج أوروبي يوازن بين دعم الابتكار القائم على البيانات وحماية الحقوق والمنافسة العادلة، عبر تنظيم إتاحة البيانات ومشاركتها بشكل آمن، وضمان حماية الخصوصية والأسرار الصناعية، فيقوم هذا النهج على نموذج هجين يجنّب احتكار الشركات أو هيمنة الدولة، محققاً توازناً بين الحقوق الخاصة والصالح العام[٢].

امتداداً لقانون البيانات، أقرّ الاتحاد الأوروبي قانون الذكاء الاصطناعي (EU AI Act) في آذار (٢٠٢٤) بوصفه إطاراً قانونياً شاملاً لتنظيم تقنيات الذكاء الاصطناعي. يندرج القانون ضمن إستراتيجية أوروبية تهدف إلى جعل أوروبا مركزاً عالمياً للذكاء الاصطناعي يضع الإنسان وحقوقه في صلب التطوير التقني، ويركز على ضبط الاستخدامات عالية الخطورة وحظر التطبيقات المخالفة للقيم الأوروبية، بما يعزز الثقة والأمان، ويحمي الخصوصية والكرامة الإنسانية، ويدعم الابتكار، مميزاً النهج الأوروبي عن النموذجين الأميركي والصيني [٣].

المطلب الثاني: تحديات الحوكمة السيبرانية في المنطقة العربية

تواجه الدول العربية تحديات مركبة تتعلق بالسيادة الرقمية ومكانتها في الفضاء السيبراني العالمي، في ظل ضعف التخطيط للحوكمة السيبرانية وغياب إطار إقليمي موحّد ينظم السياسات الرقمية، مما أدى إلى تشتت الجهود وتباين الإستراتيجيات الوطنية، ويؤدي غياب آليات الدفاع السيبراني الجماعي والتنسيق الأمني المتبادل إلى جعل بعض الدول عرضة

(1) Liang Zheng, "Solidarity, Inclusiveness and a Future for All: Understanding China's Global AI Governance Action Plan," Xinhua – English Column, August 15, 2025, https://english.news.cn/20250815/2266c491e6774b49a79ca147de174891/c.html

(2) Sean Fleming, "What Is Digital Sovereignty and How Are Countries Approaching It?," World Economic Forum – WEF Stories, January 10, 2025, https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/

(3) European Parliament, "Digital Agenda for Europe," Fact Sheets on the European Union, updated March 31, 2025, https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe.

للهجمات الإلكترونية، وفي هذا السياق، أنشأت جامعة الدول العربية في أيلول (٢٠٢٣) مجلساً وزارياً للأمن السيبراني في محاولة لتعزيز التنسيق وتوحيد الجهود الإقليمية[١]، و يعكس ذلك إدراكاً متزايداً لدى الدول العربية بأهمية التحرك المشترك في مجال الحوكمة السيبرانية، غير أن المبادرات القائمة ما تزال متفرقة ومحدودة، بما يعيق تحقيق تماسك إستراتيجي إقليمي فعّال، وتزداد هذه الإشكالية مع استمرار التبعية التقنية لشركات أجنبية في البنية التحتية والخدمات الرقمية، مما يثير مخاوف تتعلق بالسيادة الرقمية، خاصة في ظل اعتماد بعض الدول الخليجية، مثل الإمارات، على معدات شركات صينية كهواوي في شبكات الاتصالات ومراكز البيانات[٢].

وبالمثل، تسيطر شركات أمريكية كبرى مثل: مايكروسوفت (Microsoft) وأمازون (Amazon) في المنطقة، إذ بادرت هذه الشركات مؤخراً إلى بناء مراكز بيانات ضخمة في السعودية وغيرها؛ لتلبية الطلب المحلي، فهذه التبعية تجعل أمن الدول العربية التقني رهناً لسياسات ومصالح مزودي التكنولوجيا الأجانب، وتضعها أمام معادلة صعبة في الموازنة بين العروض الصينية والأمريكية المتنافسة. ورغم سعي بعض الدول إلى إشتراط توطين البيانات والبنية التحتية داخل حدودها لزيادة السيطرة (كما فعلت السعودية بالضغط على الشركات لنقل مقارها الإقليمية إلى الرياض) فإن الواقع يبين أن القدرات الذاتية والتقنية العربية ما زالت غير كافية للإستغناء عن الخبرات والمنتجات الأجنبية في المدى المنظور[٣]، فضلا عن عن تباين الجهود بين دول الخليج وبقية الدول العربية، فهناك فجوة واضحة بين دول الخليج العربي ودول عربية أخرى فيما يتعلق بقدرات الحوكمة السيبرانية والأمن الرقمي، فقد إستثمرت دول الخليج الغنية خصوصاً السعودية والإمارات وقطر فضلاً عن عُمان والبحرين في بناء أطر وطنية متقدمة

(١) أحمد أبو المعاطي, «الأمن السيبراني العربي... فضاءات مُستباحة واستراتيجيات غائبة!», العروبة ٢٢, ٢٨ حزيران/يونيو ٢٠٢٥, تاريخ الاطلاع ٢٢ تموز/يوليو ٢٠٢٥, https://ourouba٢٢.com/article/٦١٦١/الأمن-السيبراني-العربي-فضاءات-مستباحة-واستراتيجيات-غائبة.

(2) Elizabeth Dwoskin, Ellen Nakashima, and Nitasha Tiku, "How the Authoritarian Middle East Became the Capital of Silicon Valley," The Washington Post, May 14, 2024, accessed July 22, 2025, https://www.washingtonpost.com/technology/2024/05/14/middle-east-ai-tech-companies-saudi-arabia-uae/

(3) Elizabeth Montalbano, "AWS to Invest $5.3 Billion to Build Data Centers in Saudi Arabia to Bolster Tech in the Region," CIO, March 5, 2024, accessed July 22, 2025, https://www.cio.com/article/1311730/aws-to-invest-5-3-to-build-data-centers-in-saudi-arabia-to-bolster-tech-in-the-region.html

للأمن السيبراني، بما في ذلك إنشاء هيئات متخصصة وسنّ تشريعات حديثة وإستراتيجيات شاملة، مما إنعكس في تصدرها مراكز متقدمة عالمياً في مؤشرات الأمن السيبراني[١].

ملكية البيانات تمثل هاجساً متزايداً، إذ أن جزء كبير من بيانات المواطنين والمؤسسات العربية مخزّن لدى خوادم تديرها شركات أجنبية، مما يثير تساؤلات حول التحكم بالبيانات وحماية خصوصيتها. وقد دفع ذلك بعض الدول للمطالبة بتخزين البيانات محلياً وإنشاء مراكز بيانات وطنية؛ لضمان سيادتها الرقمية على المعلومات الحساسة[٢].

لا تزال العديد من الدول العربية تعاني من قصور في البنية التحتية الرقمية الأساسية، ولا سيما في قدرات التصدي للهجمات ومراكز الاستجابة للطوارئ السيبرانية، مع اعتماد واسع على معدات أجنبية قد تنطوي على ثغرات أمنية ومخاطر تدخل خارجي، ويواكب ذلك ضعف التمثيل العربي في المحافل الدولية المعنية بالفضاء السيبراني، إذ لم تتحول المبادرات الفردية إلى تأثير فعلي في صياغة السياسات الرقمية العالمية، وبقي الحضور العربي في النقاشات الأممية محدوداً ومتبايناً[٣]، ويؤدي غياب رؤية عربية موحّدة إلى إضعاف القدرة التفاوضية وحماية المصالح الرقمية، مما يبرز الحاجة إلى تنسيق المواقف، وتعزيز البنية التحتية المحلية، وتبني دبلوماسية سيبرانية نشطة لضمان موقع أكثر فاعلية في النظام السيبراني الدولي[٤].

(١) أمنية, «أهمية الإنفاق على الأمن السيبراني», Umniah – TheΛLog, تاريخ الاطلاع ٢٢ تموز ٢٠٢٥, https://www.umniah.com/ar/explore-theΛlog/أهمية-الإنفاق-على-الأمن-السيبراني/

(2)Elizabeth Montalbano, "AWS to Invest $5.3 Billion to Build Data Centers in Saudi Arabia to Bolster Tech in the Region," CIO, March 5, 2024, accessed July 22, 2025, https://www.cio.com/article/1311730/aws-to-invest-53--to-build-data-centers-in-saudi-arabia-to-bolster-tech-in-the-region.html

(3) Ibid.

(4) Ibid.

الخاتمة:

خلص البحث إلى أن الحوكمة السيبرانية لم تعد إطاراً تقنياً محايداً، بل تحولت إلى أداة جيوسياسية مركزية في التنافس الدولي على النفوذ والسيادة الرقمية، حيث تتباين نماذج القوى الكبرى بين مقاربة الإنترنت المفتوح، وسيادة الدولة، والتنظيم القائم على القواعد، ويبيّن البحث أن هذا التنافس لا يقتصر على البنى التحتية والتقنيات، بل يمتد إلى صياغة المعايير والقيم الحاكمة للنظام الرقمي العالمي، وفي المقابل، يكشف ضعف التنسيق وتشتت السياسات الرقمية عن هشاشة الموقع العربي، بما يعمّق التبعية التقنية ويحدّ من القدرة على التأثير في قواعد الحوكمة السيبرانية. وبذلك، يستنتج البحث أن تعزيز السيادة الرقمية العربية يتطلب إطاراً إقليمياً موحّداً، ودبلوماسية سيبرانية نشطة، وتطوير قدرات ذاتية تُمكّن من حضور أكثر فاعلية في النظام السيبراني الدولي.

قائمة المصادر:

أولاً: المصادر العربية

أ- الكتب العربية والمترجمة:

١- خالد وليد محمود. الفضاء السيبراني وتحولات القوة في العلاقات الدولية. بيروت: المركز العربي للأبحاث ودراسة السياسات، ٢٠٢٥.

٢- كريم عادل عبيد. إستراتيجيات الحوكمة الرقمية وتطبيقاتها الذكية – الجزء الأول. ليبيا: دار البيان للنشر والتوزيع والإعلان، ٢٠٢٢.

ب- مقالات ودراسات علمية

١- أحمد أبو المعاطي. «الأمن السيبراني العربي... فضاءات مُستباحة واستراتيجيات غائبة!» العروبة ٢٢، ٢٨ حزيران ٢٠٢٥. تاريخ الاطلاع ٢٢ تموز ٢٠٢٥. https://ourouba٢٢.com/article/٦١٦١-الأمن-السيبراني-العربي-فضاءات-مستباحة-واستراتيجيات-غائبة

٢- أحمد صلاح علي. «قوانين الخصوصية وحوكمة البيانات.. ساحة صراع بالذكاء الاصطناعي في ظل الحرب الباردة الجديدة.» الجزيرة نت، ٤ أيار ٢٠٢٥. تاريخ الاطلاع ١٧ تموز ٢٠٢٥. https://www.aljazeera.net/tech/٢٠٢٥/٥/٤/قوانين-الخصوصية-وحوكمة-البيانات-ساحة

٣- إيهاب خليفة. «نماذج دولية لتمكين رقمي وسبل الاستفادة منها لمكافحة كورونا.» الملف المصري ٧٠ (٢٠٢٠): ١٧–٢٨.

٤- مصطفى مجدي. «السيادة السيبرانية ومستقبل الإنترنت.» مسار، ١٦ شباط ٢٠٢٢. تاريخ الاطلاع ١٧ تموز ٢٠٢٥. https://masaar.net/ar/السيادة-السيبرانية-ومستقبل-الإنترنت/

٥- محمد أحمد لبيب أحمد، وهيثم محمد بهاء القاضي، ومصطفى أحمد كمال. «دور الاتفاقيات الدولية والإقليمية في مجال الأمن السيبراني وموقف الدولة المصرية منها.» مجلة JGPCC ١، عدد ١ (أيلول ٢٠٢٤): ١٢٨.

٦- محمد جمال علي. «السيبرانية والحوكمة: بين ممارسة السيادة وحقوق الإنسان.» قضايا ونظرات: تقرير ربع سنوي، مركز الحضارات للدراسات والبحوث، العدد ٢١ (٢٠٢١).

٧- منال السيد. «آليات تطبيق الحوكمة الرقمية في القطاع الحكومي: دروس مستفادة من الخبرة الدولية.» مجلة كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، العدد ٣ (٢٠٢٤).

٨- يوسف مناصرة. «التوفيق بين حوكمة الإنترنت والأمن السيبراني للدول.» مجلة صوت القانون، العدد ٩ (٢٠٢٣).

ج- تقارير ومنظمات

١- AFRINI (المركز الإفريقي لمعلومات الشبكة). «حوكمة الإنترنت.» تم الدخول ٢١ تموز ٢٠٢٥. https://www.afrinic.net/ar/internet-governance

٢- أمنية. «أهمية الإنفاق على الأمن السيبراني.» Umniah – TheΛLog. تاريخ الاطلاع ٢٢ تموز ٢٠٢٥. https://www.umniah.com/ar/explore-theΛlog/أهمية-الإنفاق-على-الأمن-السيبراني/

ثانياً: المصادر الأجنبية

1- Deb Bodeau et al. Cyber Security Governance: A Component of MITRE's Cyber Prep Methodology. Technical Report. MITRE Corporation، September 2010.

2- Eeten, Michel van, Hans De Bruijn, Mirjam Kars, and Haiko Van Der Voort. "The Governance of Cybersecurity: A Framework for Policy." International Journal of Critical Infrastructures 2, no. 4 (2006).

3- Moore، G. J. Huawei, Cyber-Sovereignty and Liberal Norms: China's Challenge to the West/Democracies. Journal of Chinese Political Science 28 (2023). https://doi.org/10.1007/s11366-022-09814-2

4- Savaş, Serkan، and Süleyman Karataş. "Cyber Governance Studies in Ensuring Cybersecurity: An Overview of Cybersecurity Governance." International Cybersecurity Law Review 3 (2022). https://doi.org/10.1365/s43439-021-00045-4

5- Tarhan، Kamil. "Historical Development of Cybersecurity Studies: A Literature Review and Its Place in Security Studies." Przegląd Strategiczny, Issue 15 (2022). International Islamic University Malaysia.

6- Gurumurthy, Anita, Nandini Chami, and Amay Korjan. "A Southern Agenda for Global Digital Governance." In Future of Global Governance: Perspectives from Global South، ed. Global Policy Watch and Social Watch. Global Policy Watch, 2024. Accessed July 21، 2025. https://www.globalpolicywatch.org/futureofglobalgovernance/index/f-a-southern-agenda-for-global-digital-governance/

7- Harandi, Diba Aalami. "International Legal Frameworks on Cybersecurity and Data Protection Law." Denver Journal of International Law & Policy, January 7, 2025. Accessed July 21, 2025.

https://djilp.org/international-legal-frameworks-on-cybersecurity-and-data-protection-law /

8- Ho Ting Hung. "Exploring China's Cyber Sovereignty Concept and Artificial Intelligence Governance Model: A Machine Learning Approach." Journal of Computational Social Science 8، no. 1 (2025). https://doi.org/10.1007/s42001-024-00346-8

9- Rasheed، E. A. "Cyber Security in International Conflict: US China Cyber Competition and Its Impact on India." Journal of Social Sciences Review 5, no. 2 (2025). https://doi.org/10.62843/jssr.v5i2.549

10- Cybersecurity and Infrastructure Security Agency (CISA). 2025–2026 CISA International Strategic Plan. CISA.gov. Accessed July 22, 2025. https://www.cisa.gov/2025-2026-cisa-international-strategic-plan

11- European Parliament. "Digital Agenda for Europe." Fact Sheets on the European Union, March 31, 2025. https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe

12- European Union. "Data Protection and Online Privacy." Your Europe. Published online about 3.6 years ago. Accessed July 22, 2025. https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.htm

13- United States Department of State. "Building a Clean Network: Key Milestones." State.gov (archived). Accessed July 22, 2025. https://2017-2021.state.gov/building-a-clean-network-key-milestones/

14- Berman, Noah, Lindsay Maizland، and Andrew Chatzky. "Is China's Huawei a Threat to U.S. National Security?" Council on Foreign Relations, February 8, 2023. Accessed July 21, 2025. https://www.cfr.org/backgrounder/chinas-huawei-threat-us-national-security

15- Cary, Dakota. Community Watch: China's Vision for the Future of the Internet. Global China Hub, Atlantic Council, December 4, 2023. Accessed July 22، 2025. https://www.atlanticcouncil.org/in-depth-research-reports/report/community-watch-chinas-vision-for-the-future-of-the-internet/

16- Don Hoefler. "Who Named Silicon Valley?" Computer History Museum Blog، January 7, 2015. https://computerhistory.org/blog/who-named-silicon-valley/

17- Electronic Privacy Information Center (EPIC). EPIC v. DOJ – PRISM. Accessed July 21, 2025. https://epic.org/documents/epic-v-doj-prism/
18- Elizabeth Dwoskin, Ellen Nakashima, and Nitasha Tiku. "How the Authoritarian Middle East Became the Capital of Silicon Valley." The Washington Post, May 14, 2024. Accessed July 22, 2025. https://www.washingtonpost.com/technology/2024/05/14/middle-east-ai-tech-companies-saudi-arabia-uae/
19- Elizabeth Montalbano. "AWS to Invest $5.3 Billion to Build Data Centers in Saudi Arabia to Bolster Tech in the Region." CIO، March 5, 2024. Accessed July 22, 2025. https://www.cio.com/article/1311730/aws-to-invest-5-3-to-build-data-centers-in-saudi-arabia-to-bolster-tech-in-the-region.html
20- Fidler David P. The Clean Network Program: Digital Age Echoes of the "Long Telegram"? Council on Foreign Relations, October 5, 2020. Accessed July 22, 2025. https://www.cfr.org/blog/clean-network-program-digital-age-echoes-long-telegram
21- Kleinwächter, Wolfgang. "Developments in the Internet Governance Environment: October to December 2024." DENIC Blog, January 30, 2025. Accessed July 22, 2025. https://blog.denic.de/en/developments-in-the-internet-governance-environment-october-to-december-2024/
22- Kleinwächter, Wolfgang. Internet Governance Outlook 2023: Will Digital Coop-Frontation' Become the "New Normal"? CircleID, January 11، 2023. Accessed July 21, 2025. https://circleid.com/posts/20230111-internet-governance-outlook-2023-will-digital-coop-frontation-become-the-new-normal/
23- Reuters. China Unveils Global Data Security Initiative, Says Some Countries Bullying Others. Reuters, September 8, 2020. https://www.reuters.com/article/us-china-security-data/china-unveils-global-data-security-initiative-says-some-countries-bullying-others-idUSKBN25Z06L/
24- Sean Fleming. What Is Digital Sovereignty and How Are Countries Approaching It? World Economic Forum (WEF), January 10, 2025. https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/