الحدود السيبرانية وأثرها في العلاقات الدولية: التحديات والاستقرار الإستراتيجي

خالد وليد محمود*

*معهد الدوحة، قطر

ملخص: تناقش هذه الدراسة «الحدود السيبرانية وأثرها في العلاقات الدولية: دراسة حول التحديات والاستقرار الإستراتيجي»، الدور المتزايد للفضاء السيبراني في إعادة تشكيل مفاهيم السيادة الوطنية والعلاقات بين الدول. في ظل التوسع الرقمي العابر للحدود، برزت تحديات جديدة تتعلق بكيفية حماية البنى التحتية الرقمية للدول، مع ضمان الحقوق الرقمية للأفراد. تستعرض الدراسة كذلك كيف أن غياب التوافق الدولي حول تنظيم الفضاء السيبراني يهدد الاستقرار الإستراتيجي، ويزيد من مخاطر الهجمات السيبرانية العابرة للحدود. كما تبحث في سبل تعزيز التعاون الدولي لتنسيق السياسات السيبرانية، وتحقيق توازن فعّال بين أمن الدول وحماية الخصوصية وحرية التعبير، بما يسهم في بناء نظام سيبراني أكثر استقرارًا وعدالة في سياق العلاقات الدولية الحديثة.

الكلمات المفتاحية: الحدود السيبرانية، العلاقات الدولية، التوسع الرقمي، السيادة.

Cyber Borders and their Impact on International Relations: Challenges and Strategic Stability

KHALED WALID MAHMOUD*

ORCID NO: 0000-0001-9357-7228

ABSTRACT: *This study, explores the growing role of cyberspace in reshaping concepts of national sovereignty and inter-state relations. Amid rapid digital expansion across borders, new challenges have emerged regarding how states can protect their digital infrastructure while safeguarding individual digital rights. The study examines how the absence of international consensus on cyberspace governance threatens strategic stability and increases the risks of cross-border cyberattacks. It also discusses ways to strengthen international cooperation and harmonize cyber policies to achieve a balanced approach between national security and the protection of privacy and freedom of expression—ultimately contributing to a more stable and equitable cyber order in the context of modern international relations.*

* Doha Institute, Qatar

Keywords: *Cyber Borders, International Relations, Digital Expansion, Sovereignty.*

رؤيـــة تركيـــة
2025-(2/14)
199 - 218

Received Date: 28 / 03 / 2025 • Accepted Date: 02 / 05 / 2025

DOI:10.36360/1560-014-002-010

في ظل التحولات السريعة التي يشهدها العالم اليوم، أصبح الفضاء السيبراني يشكل عنصرًا محوريًّا في تشكيل علاقات الدول والشعوب على المستويين المحلي والدولي. الثورة الرقمية التي بدأت منذ عقود أصبحت اليوم تُمثل تحولاً جذريًّا في كيفية تفاعل الدول والأفراد بعضهم مع بعض، حيث تجاوز الفضاء السيبراني الحدود التقليدية للمجالات السياسية والاقتصادية والاجتماعية. وقد فرض هذا التحول تحديات جديدة على مفهوم السيادة الوطنية، حيث أضحى الفضاء السيبراني ساحة شديدة التعقيد، لا تقتصر على المسائل التقنية فحسب، بل تمتد لتشمل قضايا أمنية، وسياسية، بل حتى حقوقية.

يُعَدّ الفضاء السيبراني بمثابة الشبكة العالمية التي تربط ملايين الأجهزة الرقمية عبر الإنترنت، وتُمكّن البشر من التفاعل بعضهم مع بعض ومشاركة المعلومات، بينما تظل هذه الشبكة بعيدة عن حدود الدولة أو الجغرافيا. إذ يعيد هذا الفضاء تعريف فكرة السيادة الوطنية التي كانت تدور حول الحدود الجغرافية المادية، في حين أن الحدود السيبرانية لا تتوقف عند هذه الحدود المادية، بل تمتد عبر الشبكات المتشابكة التي تمر عبر الدول المختلفة، وهذا يُثير تساؤلات عميقة حول كيفية تنظيم هذا الفضاء وحمايته.

إن إحدى القضايا البارزة التي تطرحها هذه التحولات هي مفهوم الحدود السيبرانية، التي تعكس محاولات الدول رسم حدودها في الفضاء السيبراني؛ لضمان حماية مصالحها الوطنية، وحماية البنى التحتية الرقمية، والمعلومات الحيوية، في وقت يشهد فيه هذا الفضاء نموًّا غير مسبوق. ويمثّل هذا الموضوع تحدّيًا معقدًا، حيث إن الفضاء السيبراني لا يعترف بالحدود الجغرافية التقليدية، وهو ما يضع الدول أمام ضرورة إعادة التفكير في سيادتها. فعلى الرغم من أن الفضاء السيبراني يتيح للدول القدرة على النمو والابتكار، إلا أنه في الوقت ذاته يُسهم في خلق تهديدات جديدة للأمن القومي.

وتتمثل التحديات الرئيسة في كيفية إيجاد التوازن بين حماية سيادة الدول في الفضاء السيبراني من جهة، وحماية حقوق الأفراد وحرياتهم في هذا الفضاء من جهة أخرى. ففي حين تسعى بعض الدول لتطبيق حدود سيبرانية صارمة لحماية مصالحها الداخلية وأمنها، فإن هذه الإجراءات قد تؤدي إلى انتهاك حقوق الأفراد في الوصول إلى المعلومات والتعبير عن آرائهم بحرية. وهذا يثير تساؤلات بشأن كيفية توازن حماية الأمن السيبراني مع الحفاظ على الحقوق الرقمية للأفراد وحرياتهم.

يشكّل الفضاء السيبراني اليوم ساحة من التحديات المستمرة على مستوى الدول والشركات والأفراد. ولا يمكن للمجتمع الدولي أن يتجاهل الآثار الجسيمة التي يمكن أن تترتب على غياب التنسيق الدولي الفعّال لحماية هذا الفضاء. فالأمن السيبراني ليس مجرد مسألة تقنية، بل قضية سياسية إستراتيجية تؤثر بشكل مباشر في استقرار الدول وتعاونها مع الدول الأخرى في شتى المجالات. من الهجمات السيبرانية العابرة للحدود إلى النزاعات الرقمية بين الدول الكبرى، يتعين على المجتمع الدولي وضع أطر عمل قانونية وأمنية مشتركة؛ لضمان استقرار الفضاء السيبراني، وتجنب تصاعد التوترات بين الدول.

من جهة أخرى، تبرز تحديات أخرى تتعلق بحقوق الإنسان في الفضاء السيبراني، تشمل حريات الأفراد في التعبير، وخصوصية البيانات، وحرية الوصول إلى الإنترنت. فعلى الرغم من أن الفضاء السيبراني يوفّر فرصًا هائلة للابتكار والبحث، فإن التهديدات المرتبطة بالرقابة الرقمية، وتجميع البيانات الشخصية، والانتهاك المحتمل للحقوق الرقمية، تتطلب من الدول التوصل إلى حلول قانونية فعّالة تحمي حقوق الأفراد، وتضمن لهم الأمان في عالم متصل بالإنترنت.

إن العلاقة بين الحدود السيبرانية واستقرار الفضاء السيبراني تمثّل عنصرًا أساسيًّا في نقاشات الأمن السيبراني العالمية. فغياب الاستقرار السيبراني يمكن أن يؤدي إلى تهديدات حقيقية للأمن والتنمية الاقتصادية والسياسية على المستوى العالمي. فالهجمات السيبرانية قد تعطّل البنية التحتية الحيوية، وهذا يتسبّب في تعطيل الخدمات الأساسية، مثل الكهرباء والمياه، ووسائل النقل، والاتصالات، وهذا يؤثر بشكل مباشر في استقرار الحكومات والشركات.

علاوة على ذلك، تفرض الطبيعة العابرة للحدود للتهديدات السيبرانية ضرورة التعاون الدولي بين الدول لتأمين هذا الفضاء. فالتنسيق بين الحكومات والمنظمات الدولية هو السبيل الوحيد للتصدي للهجمات التي قد تتجاوز حدود الدول وتؤثر في أمن العالم كلّه. إن تنسيق السياسات السيبرانية بين الدول، وتطوير آليات للرد على الهجمات السيبرانية العابرة للحدود- أصبحا ضرورة ملحة لضمان الاستقرار والأمن على مستوى العالم.

تهدف هذه الدراسة إلى تقديم تحليل شامل عن العلاقة بين الحدود السيبرانية والاستقرار الإستراتيجي في الفضاء السيبراني، وتحديد التحديات الأمنية والسياسية التي

يواجهها هذا الفضاء في سياق العلاقات الدولية، وتناقش سبل تعزيز التنسيق الدولي؛ لضمان استقرار الفضاء السيبراني وحماية الحقوق الرقمية في الوقت ذاته. ومن خلال هذا التحليل، سيتحقّق استكشاف الحلول الممكنة؛ لتحقيق توازن بين أمن الدول في الفضاء السيبراني وضمان حقوق الأفراد، مع تأكيد أهمية التعاون الدولي في بناء نظم حماية فعالة تسهم في تعزيز الاستقرار السيبراني.

في هذا الإطار، تطرح هذه الدراسة تساؤلاً حول كيفية تحقيق التوازن بين حماية سيادة الدول في الفضاء السيبراني وضمان استقرار هذا الفضاء بشكل يضمن حقوق الأفراد، مع تأكيد أن غياب الاستقرار السيبراني يشكل تهديدًا للأمن والتنمية العالمية.

الحدود السيبرانية: المفهوم والأبعاد الأمنية

يلقى موضوع الحدود السيبرانية Cyber Boundaries اهتمامًا كبيرًا بين أوساط الباحثين والأكاديميين ومراكز التفكير العالمية، وله حضور قوي في الأدبيات السياسية والعلاقات الدولية، وبدأت تطفو على سطح النقاش تساؤلات تتعلق بقدرة الدول على التحكم في البنية التحتية الرقمية الخاصة بها وبيانات مواطنيها، مثل: هل الحفاظ على الحدود الإقليمية والمفاهيمية المرتبطة بالمفهوم التقليدي للسيادة يتوافق مع فضاء سيبراني مترابط ومستقل؟

استطاع الواقع السيبراني فرض بعض المفاهيم المتعلقة بالجغرافيا من حيث الزمان والمكان والمحيط الجيوسياسي للدول، واستطاع أن يجعل الحدود الجغرافية تبدو في غاية الهشاشة والاختراق من طرف فاعلين افتراضيين يصعب تحديد هوياتهم ومعرفة الجهات والقوى أو الدول التي تدعمهم وتوفر لهم الملاذ.[1] وهنا يتضح بأنّ دولاً كثيرة تسعى إلى رسم حدودها السيبرانية لتكون متساوية مع حدودها الجغرافية؛ من أجل حماية أمن مؤسساتها التي تتعرض أحيانًا لتهديدات وهجمات سيبرانية، فضلاً عن قدرتها على حماية الخصوصية المعلوماتية للأفراد، وهذه الأخيرة أصبحت مكشوفة وعرضة للتهديد من طرف قراصنة المعلومات، في ظل «سيولة» مشهد حماية المعلومات الرقمية من الهجمات السيبرانية، والمخاوف من الجانب «المظلم» للإنترنت الذي يلقي بظلاله على العلاقات الدولية لحجب الفوائد الهائلة لتكنولوجيا المعلومات والاتصالات، بما يزعزع الاستقرار في النظام العالمي.[2]

أصبح الفضاء السيبراني Cyberspace وسيطًا لسوق عالمي يضم مجموعة من الأنشطة

السياسية التقليدية والجديدة، فالتوسع في استخدام الإنترنت يُعَدّ أحد أكثر التطورات التكنولوجية إثارة للاهتمام في أواخر القرن العشرين. هذه الظاهرة لم تغب عن انتباه الدول والخبراء الذين ينظرون إلى الفضاء السيبراني بصفته بعدًا جديدًا يضاف إلى الأبعاد الأربعة الأخرى التي تحدد السيادة الوطنية، وهي: المجال البري، والبحري، والجوي، والفضاء الخارجي.[3]

"في هذا الفضاء لا وجود للحدود الوطنية، فهناك حدود غير مرئية ترسمها شبكة الإنترنت على أسس سياسية واقتصادية وثقافية وإعلامية لتقيم عالمًا من دون دولة، ومن دون أمّة، ومن دون وطن"

في هذا الفضاء لا وجود للحدود الوطنية، فهناك حدود غير مرئية ترسمها شبكة الإنترنت على أسس سياسية واقتصادية وثقافية وإعلامية لتقيم عالمًا من دون دولة، ومن دون أمّة، ومن دون وطن.[4] فالفضاء السيبراني عمل على تشابك العلاقات بين الدول في إطار السياسات التحررية الاقتصادية والانفتاح والقدرة على تجاوز الحدود الدولية، وتخطيها، وبناء عليه، تكون سيطرة الدولة عليها أضعف من ذي قبل.[5] فالإنترنت تخطّى مفهوم الحدود الإقليمية، واخترقها، وهذا خلق مجالاً جديدًا للنشاط البشري يقوّض شرعية تطبيق القوانين القائمة على الحدود الجغرافية، ومن ثَمَّ جعل مسألة السيادة الوطنية في الفضاء السيبراني مطروحة بصفتها واحدة من التحديات التي تواجهها الدولة اليوم في عصر التكنولوجيا.[6]

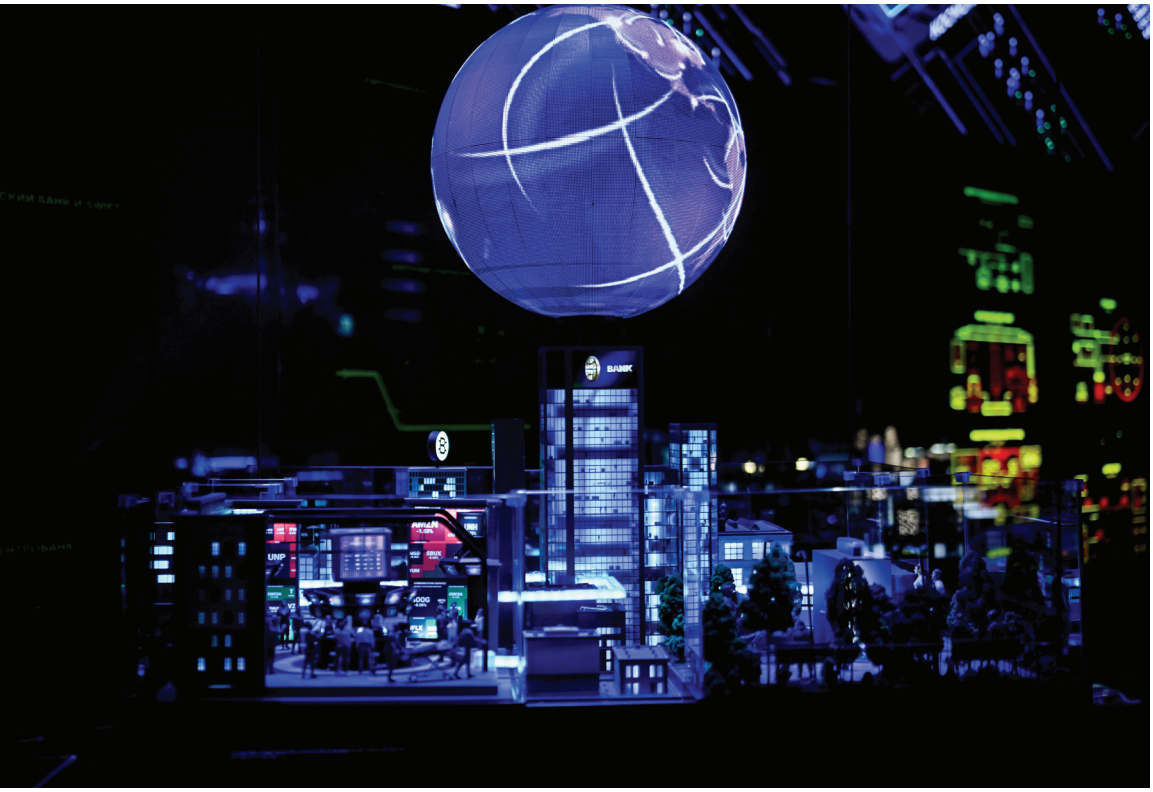
أدّى غياب الحدود في الفضاء السيبراني، إلى جانب طبيعة الهجمات السيبرانية وتجاوز التهديد طابعه التقليدي ليكون مصدرًا للتهديدات. كما يمثِّل ضعف الحدود التقليدية أحد أكبر التهديدات الأمنية للدولة، بوصفه ثغرة تستغلها جماعات الإجرام السيبراني، والفواعل من غير الدول، وخاصة مع بروز الشركات التكنولوجية العابرة للحدود الدولية، وتصاعد أخطار القرصنة والجريمة السيبرانية، إذ أتاح الفضاء السيبراني بهذا المعنى فرص الاختراق الذكي للحدود باستخدام التقنيات المتطورة، والبرامج الخبيثة، والفيروسات؛ لتهديد مصالح الدول وبناها التحتية.[7]

ومن المعلوم أن الحدود الجغرافية للدول هي حدود برية وبحرية وجوية، ولكن الآن استدعى الفضاء السيبراني الحديث عن الحدود السيبرانية أو الحدود الرقمية، مثل البث التلفزيوني والرقمي والوصول إلى الشبكات الوطنية للدول. إنّ الحدود الجغرافية يسهل الدفاع عنها ومراقبتها باستخدام تقنيات الرادار والاستشعار عن بُعد، ولكن الحدود السيبرانية يصعب التنبّؤ باختراقها، وخصوصًا أنه ليست لكل الدول قدرة على

امتلاك تكنولوجيا الدفاع اللازمة، فمن السهل الآن على أي قوات معادية اختراق أنظمة وخدمات حيوية والسيطرة عليها. ولكي نتصور خطورة هذا الاختراق، نتخيل أن جهات معادية استطاعت السيطرة على نظام تشغيل شبكة الكهرباء أو شركات الطيران أو مراكز تحكّم لبنى تحتية أخرى مثل البنوك، والمياه.[8]

تأسيسًا على هذا الكلام، نجد أن هناك تحولات مؤثرة عززت من حضور الدولة الوطنية في فرض سطوتها على الفضاء السيبراني داخل حدودها، من خلال استثمارها الرئيس في البنى التحتية، ووضع قواعد وقوانين لتنظيم المعلومات بحيث تكون الضامن الأخير لاستمرارية تدفق المعلومات والبيانات. فبعض الدول، مثل الصين وإيران تنظران مثلاً إلى التقنيات الرقمية بصفتها ساحة معركة شرسة للمنافسة العالمية، بسبب ما نتج منها من توترات جيوسياسية بعد فضائح وتسريبات «إدوارد سنودن»، والاستثمار في إمكاناتها؛ لبسط النفوذ على فضائها السيبراني من خلال «استعادة السيطرة» على تدفق بياناتها وحمايتها من عمالقة شركات التكنولوجيا العملاقة. وأصبح مدخل الحوكمة لشبكة الإنترنت معرضًا للخطر مع التوظيف السياسي والإستراتيجي من جانب قوى دولية لإخضاع شبكة الإنترنت لشبكة وطنيَّة تحت سيادتها الوطنية وجغرافيتها السياسية، وتظهر هنا دلالة سلبية تدور حول تعريف الحقوق والواجبات الرقمية للدولة، ويمكن أن يستغرق تجاوزها قطع الإنترنت وبناء جدران الحماية الكبرى والمراقبة وانتهاك الحريات. بينما يؤكد بعض أهل الشأن ضرورة استخدام أو قبول مصطلح «السيادة السيبرانية» انطلاقًا من حاجة الدول لحماية معلوماتها الحساسة في الفضاء السيبراني من هيمنة مزودي خدمة الإنترنت للحفاظ على سرية تدفق بياناتها وتوافرها وسلامتها- يرى آخرون في الواقع شرعنة للأنظمة السلطوية في بسط رقابتها على حرية الأفراد في الفضاء السيبراني وفق قوة القانون في حظر أو حجب أي موقع على الشبكة العنكبوتية؛ يمثل محتواه «تهديدًا على الأمن القومي».[9]

وقد سارعت بعض الدول، بعد تسريبات «سنودن»، إلى طرح مبادرات لإنشاء حدود سيبرانية على نحو مستقلّ تمامًا عن الفضاء السيبراني العالمي، وأعلنت عن رغبتها في إنشاء شبكة إنترنت وطنية، بعد تزايد عمليات التجسس وتسارعها، والتهديدات السيبرانية التي قامت بها الولايات المتحدة الأميركية، سواء ضد الخصوم أم الحلفاء، فضلاً عن تصاعد الهجمات السيبرانية ضد شبكات المرافق الحيوية، والتخوف من اختراق الشبكات العسكرية، وسرقة المعلومات الإستراتيجية، أو التحكم في الأنظمة العسكرية الإلكترونية التي تقوم بها دول وفواعل من غير الدول، وتوجهت دول من الاتحاد الأوروبي، ومجموعة البريكس،[10] نحو بناء شبكة داخلية للإنترنت.



في المقابل، قامت الصين بتبني موضوع حماية فضائها السيبراني المتمثل بالفضاء العالمي لبيئة المعلومات الذي يتألف من بيئة مترابطة من البنى التحتية لتكنولوجيا المعلومات، ومنها الإنترنت، وبسط سيطرتها القضائية على الفضاء السيبراني المتمثل بالإنترنت[11] من خلال إنشاء الجدار الناري العظيم Great Firewall of China للعمل على الحماية من التهديدات الإلكترونية وأمننة معلومات الإنترنت والشبكات الخاصة،[12] وسعت إيران إلى اعتماد نطاق السيبرانية وتوسيعها، وخصصت لذلك موارد هائلة؛ لإنشاء فضاء تتحكم فيه وطنيًّا. وتحاول الحكومة الإيرانية منذ سنوات تنفيذ خطة لفصل الإنترنت الداخلي عن الشبكة العالمية، إذ أفاد مركز البحوث التابع للبرلمان الإيراني في أيار/ مايو 2020 أنه جرى إنفاق نحو 190 تريليون ريال (أي ما يعادل 4.5 مليارات دولار) على إنشائها،[13] وهذا يخرج مثل هذه الدول شيئًا فشيئًا من دائرة الهيمنة والاحتكار الذي تمارسه الشركات الأميركية في هذا المجال.[14]

تسعى الدول إلى رسم حدودها السيبرانية من أجل حماية ما تستطيع حمايته، وتأمين مؤسساتها بمختلف أنواعها وتخصصاتها التي تتعرض لتهديدات وهجمات وجرائم

سيبرانية، في ظل «سيولة» المعلومات الرقمية، وازدياد ذكاء التهديدات السيبرانية، والمخاوف من الجانب «المظلم» للإنترنت الذي يلقي بظلاله على العلاقات الدولية لحجب الفوائد الهائلة لتكنولوجيا المعلومات والاتصالات، بما يزعزع الاستقرار في النظام العالمي.[15] وبناء عليه، تُرسَم الحدود السيبرانية من خلال مكوناتها، وهي البنية التحتية لشبكة الإنترنت (المعدات والمنافذ التي تقع على أرض جغرافية)، وأسماء النطاقات الحصرية وموقع الحوسبة السحابية والطاقة التي تمدّ شبكة الإنترنت والاتصالات وحركة مرور البيانات، ومن خلال هذه المكونات يمكن إنشاء بوابات للمعلومات ومراقبتها في التدفق عبر الحدود السيبرانية، رغم أن هذه الإجراءات ستخلق تحديات لخصوصية المستخدمين وحرية التعبير،[16] بالإضافة إلى تحدّيات تتعلق بالدولة نفسها التي ترغب بتوطين فضائها السيبراني والتحكم في شبكة الإنترنت.

تبدو الفجوة في المرافق السيبرانية الرئيسة المتّصلة بالبيانات بين البلدان المتقدّمة والنامية واضحة في الهيمنة على نظام الكابلات البحرية التي هي البنية التحتية الرئيسة التي تدعم الفضاء السيبراني العالمي. فأهمية هذه الكابلات يجعلها في صميم التوترات والتنافس الدولي ضمن مشهد «الصّراع الرقمي» بين الفواعل التي تمتلك الكابلات وتسيطر عليها، والأخرى الساعية لبسط السيادة على بيئتها الرقمية والسيطرة على التدفقات المعلوماتية على حدودها السيبرانية.[17]

من هذا المنطلق، أضعفت السيبرانية عامل الجغرافيا، وهو ما سمح بإنشاء فضاءات جديدة تختزل بداخلها كمية معلومات هائلة تخص أمنها الداخلي، ومثّلت معلومات الدولة الإلكترونية وضرورة حمايتها وتأمينها هاجسًا جديدًا في أي سياسة أمنية قد تتبناها هذه الدول، وقد نظر بعضها إلى هذا الأمر من منطلق السيادة بمفهومها الجديد، هذه الأخيرة التي تواجه تحديات عدة تنبع من الأنشطة عبر الفضاء السيبراني.

لم تظهر الحدود السيبرانية إلا بتخطي الإنترنت سيادة الدول وحدودها الواقعية التي ساعد فيها تطور الاتصالات الإلكترونية عبورها، وبعد أن أصبحت هناك حالة من التأثير الشبكي المتزايد بين الدولة وخارجها. إذ اتسع استخدام الأفراد، والجماعات، والدول والفواعل من غير الدول، مثل عمالقة شركات التكنولوجيا الحديثة التي تمتد قدرتها إلى السيطرة على البيانات والمعلومات والتفاعل في المجال السيبراني.[18]

إنّ مبدأ السيادة التامة والمطلقة للدولة على إقليمها بات مسألة نسبية لمصلحة سيادة مخترقة بعد أن تحدّى الإنترنت المهمّات التقليدية للدولة، وهي: ضمان الأمن الوطني، وتنظيم النشاط الاقتصادي، وفرض نمط من القيم في المجتمع.[19] كما أن للسيادة السيبرانية، في مجال السياسة دلالة إيجابية، تتمحور حول «استعادة السيطرة» من عمالقة التكنولوجيا والشركات العملاقة المهيمنة على الإنترنت، وفي الوقت نفسه، لها دلالة سلبية تترك تعريف الحقوق والواجبات الرقمية للدولة وحدها، ويمكن أن يستغرق تجاوزها قطع الإنترنت وجدران الحماية والمراقبة. والدلالة المزدوجة تفسح المجال للارتباك، إذ يخلط بعض المحللين بين السيادة السيبرانية والأمن السيبراني والاستقلالية، بينما يؤكد آخرون أن استخدام أو قبول مصطلح «السيادة السيبرانية» هو في الواقع تأييد للسلطوية «نموذج الصين» في الفضاء السيبراني.[20]

وبهذا نخلص إلى القول: إنّ الحدود السيبرانية تحدّد سلطة الدولة أو المؤسسة على الموارد السيبرانية التي تقع داخل حدودها. وتختلف الحدود السيبرانية من دولة إلى أخرى، وتتأثر بالتشريعات والقوانين المحلية، وبالعلاقات الدولية واتفاقيات الحماية السيبرانية الدولية. وبما أن الفضاء السيبراني لا يتميز بحدود جغرافية واضحة، فإنّ تحديد الحدود السيبرانية يتطلب تعاونًا دوليًّا قويًّا واستخدام التكنولوجيا للكشف عن الأنشطة السيبرانية غير المشروعة. وتتضمن الحدود السيبرانية الموارد السيبرانية جميعًا التي تنتجها أو تستخدمها، مثل قواعد البيانات والبرامج والأجهزة والأنظمة والشبكات، ويتعين على الدول والمؤسسات الحفاظ على أمن هذه الموارد وحمايتها من الهجمات السيبرانية غير المشروعة، ويتطلب ذلك تنفيذ سياسات وإجراءات أمنية فعَّالة وتحديثها دوريًّا، والتدريب المستمر للموظفين على السلوكيات الأمنية السيبرانية، وتوفير الموارد المالية والتقنية اللازمة لتحسين الأمن السيبراني.

المسؤولية العالمية لضمان الاستقرار في الفضاء السيبراني

إن المجال السيبراني المفتوح، وما يمثِّله من أخطار تؤثر في موازين القوى الدولية، يحتاج معه المجتمع الدولي إلى تعاون وتنسيق أمني للحد من هذه التهديدات، وتأمين حقوق الأفراد والمصالح الإستراتيجية للدول. فتحقيق الاستقرار الإستراتيجي في الفضاء السيبراني أصبح أمرًا ضروريًّا لضمان أمن الدول والمجتمعات، إذ إنَّ تصاعد التهديدات السيبرانية للأنظمة الحيوية والمؤسسات الحكومية والشركات الخاصة

جعلت من الضروري تطوير سياسات تعزِّز الاستقرار السيبراني، وتقدِّم حلًّا للتحديات الرقمية المتنوعة، إلى جانب ذلك يعزز البعد السياسي في الفضاء السيبراني أهمية السياسة السيبرانية. فالفضاء السيبراني لم يعد مقتصرًا على القضايا التقنية فحسب، بل أصبح أحد أهم القضايا العامة العالمية «المسيّسة».

أولًا: الاستقرار الإستراتيجي للفضاء السيبراني

تُعَدّ قضية تعزيز نظام سيبراني مستقر متوافق مع النظام الدولي الحالي من أكثر القضايا إلحاحًا بالنسبة للمجتمع الدولي. وهكذا أصبحت الحوكمة السيبرانية الدولية والحفاظ على الاستقرار السيبراني الإستراتيجي مجالين ناشئين في الدراسات الدولية.[21]

على مدى أكثر من جيل بقليل، أصبح الإنترنت والفضاء السيبراني ركيزة حيوية للتفاعلات الاقتصادية والاجتماعية والسياسية، وفتح الباب أمام مكاسب هائلة. لكن مع هذا القدر الكبير من الترابط والاعتماد المتبادل، يأتي الضعف والصراع، إذ تزايدت وتيرة الهجمات السيبرانية من جانب دولٍ أو قوًى غير تابعة لدولة بعينها، وهذا يهدّد استقرار العالم السيبراني.[22]

كما خلقت الأنشطة عبر الإنترنت بصفتها بيئة بلا حدود، تحدّيات بالنسبة إلى أمن الدول وسيادتها، وأوجدت تنافسًا دوليًّا، ولاسيّما بين الولايات المتحدة الأميركية والغرب من جهة وروسيا والصين من جهة أخرى، إذ تتنافس كل من هاتين الجهتين على فرض رؤيتها في حوكمة هذا الفضاء، وكيفية تشكيل القواعد الناظمة والمبادئ الدولية لإدارته. وبناء عليه، تنظيم التعامل مع التهديدات المحتملة فيه. كما ظهر الخلاف الدولي في إنشاء معايير الإنترنت الدولية، وبخاصة فيما يتعلق بالاختلاف بين تناول مفهوم «حوكمة الفضاء السيبراني» ومعالجته، إذ أصبحت حوكمة الفضاء السيبراني ترتبط على نحو متزايد بالسياسة الخارجية للدول.[23]

وبطبيعة الحال، بات الفضاء السيبراني يمثّل أحد أهم الأولويات في دراسات الحوكمة العالمية وساحة منافسة للقوى الكبرى. وفي الوقت الحالي، فإن إحدى أهم القضايا التي تواجه حوكمة الفضاء السيبراني على المستوى الدولي هي الحفاظ على الاستقرار الإستراتيجي؛ فمن دون هذا الاستقرار، لن يكون التطوير السلمي للفضاء السيبراني ممكنًا، وهذا سيهدد الاستقرار الإستراتيجي، ويضر في الحصيلة بالسلام والتنمية العالميين.[24]

تشير خيارات الاستقرار في الفضاء السيبراني إلى فضاء سيبراني مستقر، أو غير مستقر.[25] خلال وقت السلم، يمكن فهم الفضاء السيبراني المستقر على أنه توازن بين القوى الكبرى في القدرات السيبرانية، وإدارة الصراعات وآليات الحكم، فضلاً عن أمن الفضاء السيبراني الخاص بكل منها وتطويره. بمعنى آخر، بناءً على توازن القدرات السيبرانية بين القوى الكبرى، من الممكن تحقيق أمن الفضاء السيبراني وتطويره من خلال آليات إدارة الصراع والحوكمة. ومع ذلك، وخلافًا للأسلحة النووية التي يمكن قياسها من خلال مجموعة متنوعة من المؤشرات لتحديد القوة الوطنية لدولة ما، فإن تقييم القدرات السيبرانية أمر صعب للغاية، وهذا ما سنوضحه لاحقًا.[26]

يشير الفضاء السيبراني غير المستقر إلى حالة الحرب والصراعات السيبرانية. وبما أنه لا توجد سابقة لحرب سيبرانية واسعة النطاق، فإن المجتمع الدولي لم يتوصل إلى تفاهم حول ماهية الحرب السيبرانية والتأثيرات التي قد تولدها. حتى إن بعض العلماء يزعمون أنه لن يكون هناك ما يسمى «الحرب السيبرانية»؛ لأن الحرب لن تحدث في الفضاء السيبراني وحده، ولكن الهجمات السيبرانية ستُدمج بوسائل أخرى للهجوم في الفضاء المادي.[27] وفي هذه الحالة، قد تتصاعد حالات الطوارئ بسهولة إلى أزمات حادة، وهذا

يجعل الفضاء السيبراني المستقر غير مستقر. ولكن المعطيات تفيد بأن القوى الكبرى نفذت الهجمات السيبرانية بحذر شديد؛ لأنها لا تزال غير متأكدة من العواقب التي قد تترتب على الصراعات السيبرانية، وتخشى أن تأتي الهجمات السيبرانية بنتائج عكسية على نفسها بسبب تأثيرها غير المباشر.[28]

هناك ثمانية معايير يشير إليها جوزيف ناي، واقترحتها اللجنة العالمية بشأن استقرار الفضاء السيبراني، ويُمكن النظر إلى مثل هذه المعايير بأنها نقاط مرجعية مشتركة في المناقشات السياسية الجارية، ويصنفها كالآتي:[29]

1) هو عدم التدخل في الأساس العام للإنترنت.

2) لا ينبغي للدول والقوى غير التابعة لدول بعينها أن تدعم عمليات سيبرانية تهدف إلى تعطيل البنية التحتية التكنولوجية الضرورية لإجراء الانتخابات أو الاستفتاءات العامة أو التصديقات الشعبية.

3) لا يحق للدول والقوى غير التابعة لدول بعينها المساس بالسلع والخدمات في مراحل التطوير أو الإنتاج إذا كان قيامها بذلك يضر على نحو كبير باستقرار الفضاء السيبراني.

4) لا ينبغي للدول والقوى غير التابعة لدول بعينها أن تستولي على الموارد العامة بغرض استخدامها في صورة «شبكات روبوتية» (روبوتات إلكترونية مبنية على أجهزة الآخرين، ولكنها تُدار من دون علمهم أو موافقتهم).

5) ينبغي أن تنشئ الدول أطر عمل تتسم بالشفافية من الناحية الإجرائية، لتقييم ما إذا كانت ستكشف للعامة عن ثغرات أو عيوب في تكنولوجيا أو نظم المعلومات، ومتى يجب الكشف عنها.

6) ينبغي لمطوري ومنتجي السلع والخدمات التي يعتمد عليها استقرار الفضاء السيبراني تأكيد الجوانب الأمنية، واتخاذ خطوات معقولة لضمان خلو منتجاتهم من نقاط الضعف المهمة وتقليل العيوب عند اكتشافها وتوخي الشفافية فيما يتعلق بعملية الإنتاج.

7) ينبغي للدول أن تسنّ تدابير مناسبة، ومن ذلك القوانين والضوابط التنظيمية، لضمان الصحة الإلكترونية العامة.

8) لا ينبغي للقوى غير التابعة لدول بعينها أن تشارك في عمليات سيبرانية هجومية، ويجب على الأطراف الحكومية منع مثل هذه الأنشطة أو التصدي لها عند حدوثها.

بناءً على ما تقدّم، يبدو أن المبادرات المعنية في العمل نحو الاستقرار السيبراني آخذة في التوسع، لكن لغاية اليوم لا يوجد توافق دولي على القواعد الواجبة التطبيق، ولاسيما على سلوك الدول في هذا المجال، فالقانون الدولي، كما أشرنا، لا يحيط بكل القضايا المتعلقة بالفضاء السيبراني،[30] إلا أن هناك اهتمامًا دوليًّا ملحوظًا في تزايد الاتفاقيات الثنائية بين الدول، مثل دول أوروبية والصين وكندا وروسيا، وبمبادرات تعددية، مثل مساعي مجموعة العشرين ومنظمة شنغهاي للتعاون ومنظمة آسيان ومنظمة الدول الأميركية الساعية إلى إرساء اتفاق دولي بهذا الشأن، ورغم أن القانون الدولي يقدم القواعد القانونية والإرشادات التي يهتدي بها في وضع السياسات وحث الخطى للمضي قدمًا نحو بدء مفاوضات دولية، فإنّ كل ذلك لا يزال في إطار النقاش الحذر ويخضع للموازنة بين المصالح القومية للدول، وحقّها في الدفاع عن نفسها وبين الآثار الإنسانية التي قد تتسبب بها.[31]

إن المسؤولية العالمية المشتركة في الفضاء السيبراني تتجلى في الحاجة إلى تعاون دولي وتحالفات للحفاظ على الأمن والاستقرار في هذا المجال.[32] فالتحديات السيبرانية الحديثة تتطلب من فواعل الفضاء السيبراني جميعًا التعاون والتنسيق لمواجهتها وتجاوزها، لكن ما يبدو واضحًا إلى الآن أن «السلام السيبراني» الذي يجب أن يُبنَى على مسؤولية الدولة وسيادتها،[33] يبدو أقرب ما يكون اليوم إلى معادلة «السلام السيبراني السلبي» الذي يركز على «الردع» لا القدرة على معالجة الأنشطة الهجومية العدائية في هذا الجانب.

ثانيًا: البعد السياسي في الفضاء السيبراني

تمثّل السياسة السيبرانية Cyber Politics التفاعل الديناميكي بين القوى والمصالح السياسية في المجال السيبراني. ومع تزايد الترابط من خلال الإنترنت والتقنيات الرقمية، تزايدت أهمية السياسة السيبرانية على نحو كبير؛ لتشمل مجموعة واسعة من الأنشطة السياسية، بدءًا من العمليات السيبرانية التي ترعاها الدولة إلى المفاوضات الدولية بشأن معايير الأمن السيبراني وحماية الحقوق الرقمية.

كما أصبحت ظاهرة الفضاء السيبراني خلال السنوات الأخيرة، إحدى أهم القضايا العامة العالمية «المسيّسة»، وغدت أبعد من مسألة فنية في السياسات الدولية.[34] إذ أشارت نازلي شكري إلى أنَّ مجال الفضاء السيبراني الذي يتميز بسرعة الانتشار والسيولة، والقائم على شبكات الإنترنت، ومئات الملايين من الأجهزة التي تربطها بالمؤسسات

والشركات التي تعتمد على هذه الشبكة، وارتباطها بها، والخبرات الناتجة منها- قد رسّخ كل ذلك لواقع إنساني جديد، يمثل تحدّيًا للنظرية المعاصرة في العلاقات الدولية، وكذلك على مستوى السياسات والممارسات الفعلية. تتمثل هذه التحديات في الوقت، وقدرة التكنولوجيا على الاختراق، والارتباط، والتشبيك. ومن ثم، ظهر ما يُعرّف بالسياسة السيبرانية.[35]

شهد المجتمع الدولي في السنوات الأخيرة ظهور ثلاث مشكلات عامة عالمية كبرى، تتمثل في: الأزمة المالية، وتغير المناخ، وقضية تسييس الفضاء السيبراني Politicization of cyberspace، وباتت هذه الأخيرة أحد الموضوعات الرئيسة في أجندة السيناريوهات على مستوى العالم.[36]

يُحدِثُ الفضاء السيبراني تأثيرات في ديناميكيات السياسة الدولية وأنماطها الأوسع من خلال تمكين الجهات الفاعلة غير الدولية، وزيادة دور الفاعل المركزي وهو الدولة، إلى لاعب سياسي سيبراني على نحو متزايد.[37] وللتسييس السيبراني هنا معنيان، أحدهما يشير إلى العملية والآخر إلى النتيجة، فمن حيث تسييس القضايا الفنية، ثمة ثلاث مراحل من التطور يمكن الإشارة إليها، بدءًا من جعل القضايا التكنولوجية جزءًا لا يتجزأ من الأجندة الدولية، مرورًا بتوافق الدول في الآراء حول التعاون في مجال تكنولوجيا المعلومات والشبكات الحاسوبية، وهذا رفع من مستوى التعاون الفني إلى ذروة التعاون السياسي، وانتهاءً بالتعامل مع التكنولوجيا بصفتها قضية سياسية؛ لأنها انعكاس رئيس للقوة التنافسية بين الفواعل الدولية.[38]

يؤثر الفضاء السيبراني في مختلف مجالات الحياة، ومنها المجال السياسي، إذ يسهم عبر أدواته المختلفة في إعادة رسم البعد السياسي المحلي والعالمي، ويعمل على إعادة تشكيل الوعي والإدراك السياسي للأفراد والمجتمعات والدول على نحو مغاير عما كانت عليه،[39] واتجهت الدول والحكومات والقطاع الخاص نحو تأسيس مؤسسات بحثية تهتم بدراسة الفضاء السيبراني وكيفية توظيفه بالشكل الذي يسهم في تحقيق مصالحها السياسية والأمنية والاقتصادية... إلخ.[40]

ومن المظاهر الأساسية لتسييس هذا الفضاء، أن مضمونه أصبح مفاوضات بين الدول، وأن المنظمات الدولية ذات الصلة به بدأت تهتم تدريجيًّا بالمشكلة السيبرانية؛ فعلى الرغم مما تطرحه التكنولوجيا السيبرانية من تحديات عالمية استثنائية، فإن المبادئ والقواعد الدولية التي تحكم مسار استخدامها لا تزال موضع تشكيك، وتتطور بإيقاع بطيء.[41]

حاليًّا، هناك مئات ملايين الأشخاص حول العالم لديهم إمكانية الوصول إلى أجهزة الحاسوب والإنترنت، ويتزايد عدد المستخدمين ومستوى التفاعل وعمقه في الفضاء السيبراني كل لحظة، وفي مثل هذه الظروف، يؤدي الفضاء السيبراني دورًا مهمًّا في توجيه الرأي العام، وخلق الأولويات والمطالب، والدبلوماسية العامة، والتجسس، والتخريب، والردع والصراع، وأي شيء يمثّل فعليًّا الفضاء السياسي الحقيقي.

هذا يقودنا إلى القول: إنّه على الرغم من الدعوات العالمية التي تشدّد على أن الأمن السيبراني في منزلة تحدّ تواجهه الدول التي يجب أن تضمن سلام الفضاء السيبراني وأمنه عن طريق الحوار والتعاون المشترك، فإنّ تسييس هذا الفضاء وأدلجته لن يساعدا في تعزيزه، بل سيلحقان ضررًا بالثقة المتبادلة بين البلدان، (ولنا مثال واضح على عدم الثقة المتبادلة بين بكين وواشنطن، ولاسيّما فيما يتعلق بسرقة -أو المساعدة على سرقة- الملكية الفكرية عبر الفضاء السيبراني للإنترنت من أجل تعزيز الصناعات المحلية).[42]

باتت دول عديدة في العالم تحاول أن تخلق لنفسها مساحة آمنة في الفضاء السيبراني؛ كي تحافظ على أمنها القومي من ناحية، ولدعم نفوذها السياسي عالميًّا وسياساتها الخارجية من ناحية أخرى. وإنّ الأمن السيبراني Cybersecurity -بالإضافة إلى قدرته على تغيير ضوابط ومحددات بنية النظام الدولي، وفرض إعادة صياغة أو هندسة لقواعد اللعبة في العلاقات الدولية- أصبح حاجة ملحّة للدول، وهذا الأمر دفعها لـ»شرعنته وقوننته» رسميًّا؛ لصد التهديدات وبناء القدرات في أمن نظم المعلومات، وتحسين بيئتها السيبرانية، وفرض سيادتها من خلال حجب شبكة الإنترنت والاتصالات ونظام المعلومات والرسائل الإلكترونية، أو إلغائها، أو مصادرتها أو تعطيلها.[43] كما أن تحول الفضاء السيبراني إلى مجال عالمي مفتوح خلق اتجاهًا مضادًّا من طرف دول أخرى؛ في محاولة لضبط حركة التفاعلات بين الداخل والخارج، واستعادة وظيفة الدولة وسيطرتها على سيادتها السيبرانية في الأمن والدفاع في ظل تصاعد دور الفواعل من غير الدول.

وبهذا أضحت السياسة السيبرانية اليوم مصطلحًا يُستخدَم على نطاق واسع من قبل الأكاديميين والباحثين المهتمين بتحليل اتساع نطاق تأثير الإنترنت في الأنشطة السياسية والعلاقات الدولية، وأصبح البحث في هذا الجانب يأخذ زخمًا أكاديميًّا لتطوير التخطيط الإستراتيجي والقيادة في ساحات الإنترنت والبيانات الضخمة، بالإضافة إلى النقاش الدائر حول تأثير التحديات السيبرانية في الحكومات والمنظمات والمجتمعات عمومًا.[44]

بناء على ذلك، فإن المظهر الأساسي لتسييس الفضاء السيبراني أصبح مضمونَ مفاوضاتٍ بين الدول والمنظمات الدولية ذات الصلة التي بدأت تهتم تدريجيًّا بالمشكلة السيبرانية. لكن رغم ما تطرحه وتتيحه التكنولوجيا السيبرانية من فرص للتقدم والتطور وما تنطوي عليه من مخاطر وتحديات عالمية استثنائية، فإن المبادئ والقواعد الدولية التي تحكم مسار استخدامها لا تزال موضع تشكيك وتتطور بإيقاع بطيء؛ لذا فإن معالجة السياسة السيبرانية تكمن في إدارة ناجعة لمشهد حوكمة الفضاء السيبراني، وبذل جهد دولي شامل بمسؤولية مشتركة عبر جميع الفواعل واللاعبين فيه جميعًا.

وفي الختام، يظل موضوع الحدود السيبرانية أحد القضايا المركزية في السياسة الدولية المعاصرة؛ لما يحمله من أبعاد متشابكة تمسّ مفاهيم السيادة والأمن والتنمية. إذ فرضت الثورة الرقمية واقعًا جديدًا، تجاوز الحدود الجغرافية التقليدية، وخلق فضاءً افتراضيًّا يتطلب مقاربات أمنية وإستراتيجية مختلفة عما عرفته النظم السياسية سابقًا.

إنّ الفضاء السيبراني، بما يتضمنه من إمكانيات هائلة وتحديات عميقة، يدفع الدول إلى إعادة النظر في منظوماتها القانونية والأمنية، وإلى تطوير أدوات جديدة لحماية مصالحها الرقمية من جهة، وضمان حرية الأفراد وخصوصيتهم من جهة أخرى. ومع اتساع نطاق الهجمات السيبرانية، وتزايد الاعتماد على التكنولوجيا في القطاعات الحيوية، تتعاظم الحاجة إلى بناء أُطر تشاركية وتوافقات دولية لضبط هذا المجال وضمان استقراره.

ومن هنا، فإن حماية البنى التحتية الرقمية، وتأمين البيانات، والتصدي للتهديدات العابرة للحدود، ليست مسؤوليات محلية فحسب، بل هي مسؤولية جماعية تستوجب التعاون بين الدول، والمنظمات الدولية، وشركات التكنولوجيا الكبرى. كما أن تطوير قواعد حوكمة عادلة وشفافة للفضاء السيبراني بات ضرورة ملحّة لضمان الأمن الرقمي العالمي، وتعزيز الثقة بين الفاعلين الدوليين، وتحقيق توازن حقيقي بين الأمن والحرية.

وعليه، فإن تحقيق الاستقرار في الفضاء السيبراني يشكّل ركيزة أساسية في الحفاظ على النظام الدولي، ويتطلب رؤى إستراتيجية طويلة الأمد، تستند إلى الفهم العميق للطبيعة المتغيرة لهذا الفضاء، وإلى بناء منظومات دفاعية واستباقية تُسهم في بناء بيئة رقمية آمنة ومستدامة تُعزّز من فرص التنمية والتقدم الإنساني في العقود المقبلة.

الهوامش والمراجع:

1. Rob Sobers, 166 Cybersecurity Statistics and Trends, 8/7/2022, https://www.varonis.com/blog/cybersecurity-statistics, Accessed: 23/11/2022 .
2. خالد وليد محمود، سيادة الأوطان بين الرقمية والجغرافية، صحيفة الدستور، 2021/11/20، https://bit.ly/3OxujMd، تاريخ الزيارة: 2022/11/22.
3. علاء الدين فرحات وعمروس عمّارة، الفضاء السيبراني وتآكل مفهوم السيادة الوطنية، المجلة الجزائرية للدراسات السياسية، المدرسة الوطنية العليا للعلوم السياسية، العدد 2، 2021، ص. 163.
4. شهاب أحمد العنبكي، أثر العولمة على سادة الدولة في القانون الدولي: دراسة تحليلية مقارنة، ط 1، المكتبة القانونية، بغداد، 2015، ص. 140.
5. كاميران حسن، الجهود الدولية في مواجهة الجرائم السيبرانية، ط 1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2021، ص. 119.
6. Milton Mueller, Sovereignty and Cyberspace: Institutions and Internet governance, 2016, https://bit.ly/2WTCNat, Accessed: 9/12/2022.
7. علاء الدين فرحات وعمروس عمّارة، مرجع سبق ذكره، ص. 163.
8. علاء جراد، الحدود السيبرانية، الإمارات اليوم، 2021/4/27، https://bit.ly/3uEwDrL، تاريخ الزيارة: 2022/12/8.
9. خالد وليد محمود، السيادة السيبرانية، مرجع سبق ذكره، تاريخ الزيارة: 2022/12/12.
10. مجموعة بريكس تجمع خمس دول هي البرازيل، وروسيا، والهند، والصين، وجنوب إفريقيا.
11. كاميران حسن، مرجع سبق ذ كره، ص. 127.
12. أداة أساسية للحزب الشيوعي الصيني. وهو يتألف من سلسلة من التقنيات والقوانين التي تستخدمها الحكومة الصينية للرقابة والتحكم في المحتوى المتاح للمستخدمين في البلاد. من المعروف تاريخيًّا أن الصين إحدى أكثر الدول التي تخضع للرقابة الشديدة، إذ تنظم المحتوى على نسختها من الإنترنت، وهي جزء من عملية رقابة الإنترنت في الصين التي تهدف إلى الحجب المحليّ لعدد من مواقع الإنترنت الأجنبية، ومراقبة حركة البيانات من الإنترنت وإليه. تشمل آثار جدار الحماية العظيم: الحدّ من الوصول إلى مصادر المعلومات الأجنبية، وحجب أدوات الإنترنت الأجنبية (مثل: محرك بحث غوغل، أو فيسبوك)، وتطبيقات الهاتف الجوّال، والطلب من الشركات الأجنبية التكيّف مع التشريعات المحليّة ومنع مواطنيها من التعرض للأفكار والآراء التي تعدّها غير مقبولة. انظر: What Is the Great Firewall of China and How Does It Work, MUO, 1/11/2022, https://bit.ly/3Pg8dOQ, Accessed: 10/12/2022.
13. نائب إيراني: سننجز شبكة الإنترنت الوطنية بالتعاون مع الصين، العربية، 2020/9/1، https://bit.ly/3iHJGWC، تاريخ الزيارة: 2022/12/10.
14. خالد وليد محمود، السيادة السيبرانية، مرجع سبق ذكره، تاريخ الزيارة: 2022/12/13.

15. Thomas C. Wingfield, The law of information conflict: national security law in cyberspace, 1st edition, Aegis Research Corporation, USA, 2000, p. 14.

16. Anubha Gupta, Can Cyber Sovereignty Rein in Cyber Anarchy, ORF, 15/11/2022, https://bit.ly/3va7o0T, Accessed" 4/12/2022.

17. Dmitry V. Krasikov1, Nadezhda N. Lipkina, Sovereignty in Cyberspace: A Scholarly and Practical Discussion, Atlantis Press,7 December 2020, https://bit.ly/3uVNhmU, Accessed: 4/12/2022.

18. Nazli Choukri, "Cyberpolitics in International Relations," in Joel Krieger (ed.), The Oxford Companion to Theoretical Economics, New York: Oxford University Press, 2012, p. 267.

19. https://2u.pw/yBfZR

20. Trisha Ray, The Quest for Cyber Sovereignty Is Dark and Full of Terrors, ORF, 25/5/2020, https://bit.ly/3uXfNEK, Accessed: 5/12/2022.

21. Zhou Hongren, Strategic Stability in Cyberspace, China Quarterly of International Strategic Studies Vol. 5, No. 1, 2019, p. 81.

22. جوزيف ناي، ثمانية معايير لضمان الاستقرار في الفضاء السيبراني، بروجيكت سانديكيت، 4/12/2019، https://bit.ly/3uV8s8s
تاريخ الزيارة: 2022/12/15.

23. عادل عبد الصادق، صراع السيادة السيبرانية بين التوجهات الروسية والأميركية، المركز العربي لأبحاث الفضاء الإلكتروني، 2022/5/24،
https://bit.ly/3ULZuFg،
تاريخ الزيارة: 2022/12/13.

24. Samuele Dominioni, "Cyber Stability Conference: Towards a More Secure Cyberspace - 2021 Conference Report", UNIDIR, Geneva, Switzerland, 19 May 2022, https://bit.ly/41CW3pq, Accessed: 10/12/2022.

25. Zhou Hongren, op. cit., p. 86.

26. Trey Herr and Drew Herrick, "Understanding Military Cyber Operation," in Richard Harrison and Trey Herr, eds., Cyber Insecurity, Maryland: Rowman & Littlefield, 2016, p. 216.

27. Zhou Hongren, op. cit., p. 87.

28. Ibid.

29. جوزيف ناي، ثمانية معايير لضمان الاستقرار في الفضاء السيبراني، مرجع سبق ذكره، تاريخ الزيارة: 2022/12/15.

30. Louise Doswald-Beck, “Some Thoughts on Computer Network Attack and the International Law of Armed Conflict”, International Law Studies, volume 76, 2002, p. 163.

31. أنديرا عراجي، مرجع سبق ذكره، ص. 39.

32. محمد سعادي، أثر التكنولوجيا المستحدثة على القانون الدولي العام، دار الجامعة الجديدة، مصر، 2014، ص. 200.

33. خالد وليد محمود، البحث عن السلام السيبراني المنشود، الجزيرة نت، 2023/6/17، https://cutt.us/3XJWH، تاريخ الزيارة: 2023/10/20.

34. Nazli Choucri, David D. Clark, Integrating Cyberspace and International Relations: The Co-Evolution Dilemma, The MIT Press Cambridge, Massachusetts London, England, 2018, p. 4 .

35. Ibid, p. 5.

36. Brandon Valeriano, Cyber Politics, Risk Group, 1 October 2021, https://bit.ly/3tLz0Mv, Accessed: 22/12/2022.

37. Benjamin R. Banta, International Cyberpolitics, International Studies, International Studies Association, 28/9/2020, https://bit.ly/48wXx6P, Accessed: 19/12/2022.

38. Giancarlo Elia Valori, Cyberspace and world politics, Modern Diplomacy, 13/8/2021, https://bit.ly/3PBQXnw, Accessed: 19/12/2022.

39. Milton Mueller, Networks and States: The Global Politics of Internet Governance, Cambridge: MIT Press, 2010, p. 248.

40. باسم علي خريسان، مرجع سبق ذكره، ص. 18.

41. Nazli Choucri, Cyberpolitics in International Relations. International Political Science Review 21 (3), 2000, p. 243.

42. Dmitri Alperovitch, The Case for Cyber-Realism: Geopolitical Problems Don’t Have Technical Solutions, Foreign Affairs, January/February 2022, https://bit.ly/3WmlyHz, Accessed: 18/12/2022.

43. خالد وليد محمود، الأمن السيبراني، جريدة الوطن، 2021/10/16، https://bit.ly/3V4zLrP، تاريخ الزيارة: 2022/12/18.

44. خالد وليد محمود، السياسة السيبرانية كقضية عالمية، الجزيرة نت، 2023/1/17، https://cutt.us/o0yTR، تاريخ الزيارة: 2022/12/18.

TURKISH FOREIGN POLICY YEARBOOK 2023

Editors:
Burhanettin Duran
Kemal İnat
Mustafa Caner

setavakfitr setav setavakfi
www.setav.org · kitap@setav.org (0212) 395 11 00

SETA