

الفضاء السيبراني وتأكل مفهوم السيادة الوطنية

Cyberspace and the erosion of the concept of national sovereignty

فرحات علاء الدين¹، عمروس عمارة²¹ المدرسة الوطنية العليا للعلوم السياسية، Ferhat.alaeddine@enssp.dz² المدرسة الوطنية العليا للعلوم السياسية، doctoratenssp@gmail.com

تاريخ النشر: 2021/12/16

تاريخ القبول: 2021/11/10

تاريخ الاستلام: 2021/09/23

ملخص:

نحاول في هذا المقال فحص الإشكالية التي تبحث في مفهوم السيادة في الفضاء الإلكتروني، ووضع مناقشة تعترف بالواقع التاريخي للتطور التقني إلى جانب تغير طبيعة العدو وتجاوز التهديد طابعه التقليدي، كما يدرس إمكانيات إعادة بناء الكيانات ذات السيادة السياسية من أجل التوافق مع الطبيعة "الحرة" المتأصلة في العصر الرقمي.

تبعا لذلك، خلصت الدراسة إلى أنه وتحت تأثير العولمة بمختلف أبعادها ومظاهرها، ومع تطور تكنولوجيا الاتصالات وثورة المعلومات وانتشار استخدام الشبكة العنكبوتية عبر العالم، تلاشى عصر السيادة الوطنية المطلقة لصالح سيادة نسبية ومختزقة، واقتربت نحو التآكل شيئا فشيئا، بفعل وجود فضاء سيبراني يقابل الفضاء المادي التقليدي ويختلف عنه في خصائصه وتأثيره، هذا الفضاء المرن واللامحدود، وغير القابل للرقابة.

كلمات مفتاحية: الفضاء السيبراني، الحدود، السيادة الوطنية، الهجمات السيبرانية.

Abstract:

Throughout this article, we attempt to examine the problem of Sovereignty in Cyberspace and develop a discussion that acknowledges the historical existence of technical development, in addition to the change in the nature of the enemy and exceeding the threat of its traditional essence.

Furthermore, the article studies the possibilities of rebuilding the political sovereign entities to conform to the "free" nature inherent in the digital age.

Accordingly, the study concludes that, under the influence of globalization in its various dimensions and features, and with the development of communications technology, the revolution of the information and the spread of the use of the internet across the world, the era of absolute national sovereignty has vanished in favour of relative and penetrated sovereignty, and it is closer to erosion gradually. Thus, due to the existence of a cyberspace corresponding to the traditional physical space which is different in its properties and influence, it is flexible, unlimited and uncontrollable.

Keywords: Cyberspace; borders; national sovereignty; cyber attacks.

المؤلف المرسل: فرحات علاء الدين

1. مقدمة:

أصبحت الإنترنت وسيطاً لسوق عالمية ومنتدى لمجموعة من الأنشطة السياسية التقليدية والجديدة، فالتوسع في استخدام الإنترنت يعد أحد أكثر التطورات التكنولوجية والسياسية إثارة للاهتمام في أواخر القرن العشرين. هذه الظاهرة لم تغفل عن انتباه القادة السياسيين والباحثين الذين نظروا لبروز الفضاء السيبراني كبعد جديد يضاف للأبعاد الأربعة الأخرى التي تحدد السيادة الوطنية وهي: المجال البري، البحري، الجوي والفضاء الخارجي.

فعلى الصعيد الإستراتيجي، يعد الفضاء الإلكتروني مجالاً اجتماعياً وسياسياً وتكنولوجياً له خصائص فريدة مميّزتها طبيعته اللامركزية، ليشكل بذلك حضوره كمجال يقابل المجال المادي التقليدي ويتميز عنه بخصائص عديدة ومتنوعة، ويطرح تحديات بالنسبة لمفهوم السيادة الوطنية وإعادة تصور وتشكل سيادة الدولة في عصر الرقمنة.

فإذا كان مفهوم السيادة بمعناه التقليدي يتضمن سيطرة الدولة الكاملة على إقليمها والتحكم فيه، فإن ظهور الفضاء السيبراني بات يطرح نسبية هذا المفهوم مع غياب الحدود والتحول في طبيعة الصراعات. كما أن النظر إلى الفضاء الإلكتروني على أنه أحد المشاعات العالمية، وتحقيق التوازن بين سيادة الدولة والفضاء السيبراني، والمناقشة بين ذوي الحق السيادي" في وضع "السياسة العامة الدولية" للإنترنت والمجتمع التقني للإنترنت، يجعل المناقشات حول مفهوم السيادة في عصر السيبرانية أمراً معقداً للغاية بفعل التأثير المتزايد لسلطة الدولة على الإنترنت، وصعود مخاوف الأمن السيبراني، واستغلال الجيوش للفضاء الإلكتروني استغلالاً هجومياً، مما أدى إلى إحياء مطالب سيادية في الفضاء السيبراني. وانطلاقاً من ذلك جاءت فكرة هذا المقال ليتناول موضوع الفضاء السيبراني وتآكل مفهوم السيادة الوطنية، وسيتم في هذا الإطار معالجة الإشكالية الآتية:

إلى أي مدى يمكن للدول تشكيل مناطق ذات سيادة وطنية في الفضاء السيبراني ؟

هذه الإشكالية يتفرع عنها عدد من الأسئلة كما يلي:

- هل ينطبق مفهوم السيادة على الفضاء السيبراني؟
- هل الحفاظ على الحدود الإقليمية والمفاهيمية المرتبطة بالسيادة الوطنية يتوافق مع فضاء سيبراني مترابط ومستقل؟ إذا لم يكن كذلك، فهل البديل الافتراضي هو إعادة تفسير لقوة وسلطة الدول القومية؟

أما فرضية البحث فهي كالآتي:

- يرتبط تأثير الفضاء السيبراني في مفهوم السيادة الوطنية بمدى قدرة الدولة على تنظيم هذا الفضاء والتكيف مع ما يطرحه من تحديات.
- ويرمي هذا البحث إلى تحقيق مجموعة من الأهداف المعرفية ومن بينها:
- التعرف على تحولات الظاهرة الأمنية وأثر الفضاء الإلكتروني في ذلك.
- التعرف على جانب من خصائص الفضاء الإلكتروني بوصفه مجالاً إستراتيجياً خامساً.

- تشخيص ظاهرة تلاشي الحدود التقليدية في الفضاء السيبراني وبالتالي التعرف على تحديات الدولة في عصر الرقمنة وتقديم قراءة في تصور السيادة السيبرانية.

2. الفضاء السيبراني وإعادة فهم الحدود

تجاوز تأثير الفضاء السيبراني ما كان متوقعا في تصور الدول، فبعد أن اعتُبر مظهرا من مظاهر التطور التكنولوجي في عصر العولمة وتطوير أسلوب الحياة أصبح سلاحا ذو حدين، تمتد تأثيراته لتمس أمن الدول خاصة مع تحولات الظاهرة الأمنية وإعادة تعريف الحدود.

1.2 ملامح الظاهرة الأمنية المتعدية لحدود الدولة القومية

في هذا السياق الوطني والدولي المعولم والمهتز جيوسياسيا وجيوستراتيجيا تأكل المفهوم والواقع الكلاسيكي الويستفالي لـ "السيادة الوطنية"؛ وتنامي الأخذ بفكرة وواقع "السيادة المتقاسمة"، إما كواقع أو كإمكانية أو كحتمية، وهذا نظرا لتعرض مفهوم السيادة لهزات أمنية شاملة لعبت فيها العولمة الدور الأكبر، خاصة مع توسع نطاقات الظاهرة الأمنية والتفاعل الدائم بين الأبعاد الاقتصادية والتكنولوجية والإعلامية والاتصالية والسياسية والعسكرية والثقافية والمعرفية سواء بسواء (حجاج، 2013، صفحة 4). وجرى التشبث -بشكل كارثي- بفكرة العدو المركزي والتركيز على الدولة، وكلاهما كان أكثر معقولية خلال الحرب الباردة، إذ أن الهجوم المادي على الدول لم يعد له أي مبرر أو فائدة الآن، علاوة على النتائج العكسية التي يفرزها، في حين أن الأهمية المتزايدة للديناميات العابرة للحدود الوطنية، كما يلاحظ كارل كونيوتا، تعني في دالاتها أنه من المستحيل حصر مشاعر السخط والاستياء ضمن الصندوق الأسود للدولة الوطنية (كين د، 2008، صفحة 12).

في السنوات الأخيرة شهد العالم تزايدا ملحوظا في اتساع دائرة التهديدات الأمنية، والتي من شأنها أن تهدد أمن واستقرار الدولة القومية، كما يمكن لمتغير العولمة **Mondialisation** أن يجعل إفرازات هذه التحديات تتعدى الحدود الوطنية، جراء الانكشافية **La Vulnérabilité** التي خلفها التطور التقني المتسارع (منصوري، مارس 2016، الصفحات 155-166)، خاصة مع بروز المجال السيبراني كبعد

خامس، إلى جانب البر والبحر والجو والفضاء الخارجي، تسعى الدول لبسط سيادتها عليه، فبروزه كمساحة إستراتيجية خلف أيضا تهديدات تتجاوز في خطورتها التهديدات في المساحات التقليدية. هذا الفضاء، وفي إطار قدرته على استيعاب عدد أكبر من الفاعلين -حتى خارج إطار النظام السياسي- مع قدرته على توفير قدر كاف من المعلومات لهم، يقوم بتقليل المسافات وتخطي حواجز الدولة القومية المادية، فيما بينها. لذا فإن "جوزيف ناي" (Joseph Nye) يرى أن ما يوفره الفضاء الإلكتروني من مصادر قوة لمختلف الفاعلين على مختلف الأصعدة، يوسع من دائرة التهديدات الأمنية، والتي تنتج عن الأفعال العنيفة التي قد يمارسونها، وإن كان ذلك لا يعنى بالتأكيد تحقق المساواة الكاملة ما بين قدرات الدول، وقدرات الفاعلين من غير الدول، إنما يعنى بالأساس تقليص الفارق بينها في امتلاك القوة، والقدرة على إحداث العنف (شفيق، 2014، الصفحات 40-42)، وجراء هذه الفجوة الرقمية يبرز اضمحلال الحدود بين الداخل والخارج، أي أصبحت هناك حالة من التأثير الشبكي المتزايد بين الدولة وخارجها حيث اتسع استخدام الأفراد، والجماعات، والدول للتكنولوجيا الحديثة المرتبطة بالفضاء السيبراني (العبودي، 2019، صفحة 106).

2.2 الفضاء السيبراني: الفضاء الإستراتيجي الخامس:

تم تعريف "الفضاء الإلكتروني" بأنه "بجال عالمي داخل بيئة المعلومات، يتكون من شبكة مترابطة من البنى التحتية لتكنولوجيا المعلومات، بما في ذلك الإنترنت وشبكات الاتصالات وأنظمة الكمبيوتر والمعالجات ووحدات التحكم المضمنة"، كما يشار إليه بوصفه "ليس مكاناً مادياً، بل إنه يتحدى القياس في أي بُعد مادي أو متواصل في الفضاء الزمني، فهو مصطلح مختصر يشير إلى البيئة التي تم إنشاؤها عن طريق التقاء الشبكات التعاونية من أجهزة الكمبيوتر وأنظمة المعلومات والبنى التحتية للاتصالات التي يشار إليها عادة باسم شبكة الويب العالمية (Heinegg, 2012, pp. 7-19).

وجاء تعريفه في قاموس أكسفورد بوصفه "البيئة التي يتم عبرها إتمام عملية الاتصال عبر شبكة الكمبيوتر" (بري، 2019، صفحة 15، 22). كما عرفته الوكالة الفرنسية لأمن أنظمة الإعلام بأنه

"فضاء التواصل المشكّل من خلال الربط البيئي العالمي لمعدات المعالجة الآلية للمعطيات الرقمية" (بلفرد، 2016، ص 147). والفضاء الإلكتروني يتشكل من بنية مادية تشمل أجهزة الحاسوب ومصادر الكهرباء وألياف الاتصال والأقمار الصناعية، وأخرى تقنية معلوماتية (Tabansky, 2011, p.79)، إضافة إلى العامل البشري.

هذا وأصبح الفضاء السيبراني مجالاً حيوياً وجيوستراتيجياً تخاض فيه العديد من الحروب والهجمات الرقمية (عزت م.، 2017)، وذلك بالاعتماد على التطور التقني والثورة الرقمية الهائلة، ليصبح بعدا جديدا في الصراعات الدولية والحروب، وبعد أن كانت ساحات الحرب هي البر والبحر والجو والفضاء الخارجي، دخل الفضاء الإلكتروني على الخط ليصبح مجالا للصراع في القرن الـ 21 (عبد الغفار، 2016، صفحة 09)، بإمكانه أن يتحول إلى "سلاح إستراتيجي بيد الحكومات والأفراد، لاسيما أن الحرب السيبرانية أصبحت جزءا لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول" (عطية، صفحة 104). ويعد العمل العسكري في هذا الفضاء مظهرا للحروب الجديدة، ومعركة الغد هي حرب معلومات تدار في الفضاء السيبراني (أوستن لونج وآخرون، 2014، صفحة 17).

وبتحليل ديناميكيات الصراع السيبراني في هذا العصر نجد دوافعه سياسية وإستراتيجية، فقد يأخذ الشكل العسكري بتوظيف أسلوبي الهجوم والدفاع في هذا الفضاء، أو يكون في صورة ناعمة من خلال حرب الأفكار أو التنافس على عوامل القوة (زرزوقة، 2019، صفحة 1021). ومن أبعاد التحول الإستراتيجي في القوة ظهور الهجمات السيبرانية التي تمس أنظمة البيانات (اختراق، قرصنة، جوسسة، إلخ)، والحرب الإلكترونية التي تستخدم وتستهدف تكنولوجيا المعلومات، بالإضافة إلى تهديدات أمنية متعددة كالإرهاب الإلكتروني.

هذا واستطاع الفضاء السيبراني أن يتفوق على الفضاء المادي، لما يحمله من قنوات وبيانات جعلته قادرا في آن واحد على تجاوز رقابة الدولة (بري، 2019، ص 65). كما أنه يتميز بخصائص عديدة تجعله ينافس الفضاء المادي على الصعيد الإستراتيجي والأمني، من بينها المرونة وغياب الحدود، مما يتيح المجال للردع الإستراتيجي والهجوم على الخصم في صورة عابرة للحدود وبأقل تكلفة، مع نشر حالة من الخوف

لديه، بالإضافة إلى تداخل حالتي الحرب والسلم في هذا الفضاء مادامت المواجهة ليست عسكرية محضة بالمعنى التقليدي.

وكمثال على استخدام الفضاء الإلكتروني كساحة للصراع، كانت عملية "القنابل المعتمدة" نهاية القرن العشرين، أثناء قصف حلف الشمال الأطلسي (الناتو) لصربيا، مظهرا من مظاهر استخدام هذا الفضاء كبعد إستراتيجي جديد، حيث تسببت العملية في شلّ أنظمة الكمبيوتر الخاصة بوزارة الدفاع ليوغوسلافيا، بالإضافة إلى التشويش على الاتصالات (عبد الغفار، 2016، صفحة 14).

ومن الجهات التي تولي أهمية بالغة للفضاء السيبراني بعد الولايات المتحدة الأمريكية نجد الكيان الصهيوني، باعتبار أن ترسانة الأسلحة المتطورة قد تصبح عاجزة أمام القدرات السيبرانية لأطراف معادية له، وقام هذا الكيان بدوره بمهاجمة منشأة "نطنز" النووية الإيرانية في شهر ابريل 2021، مما تسبب في قطع التيار الكهربائي عن المنشأة (أبو عامر، 2021). ومع توسع استخدام الإنترنت عبر العالم لم يعد بالإمكان إغفال دور الفضاء السيبراني في تطوير أشكال الحروب المستقبلية، حتى أن البعض يرى أن الأسلحة السيبرانية تنافس السلاح النووي وتتفوق عليه من حيث مستوى التهديد والدمار الذي يمكن تحقيقه (Krepinevich, 2012, p.170).

في هذا الشأن يقول الباحث الأمريكي "جون روب" (John Robb) متحدثا عن حروب الجيل الخامس بأن "جنودها عبارة عن أفراد لا يرتدون الزي العسكري، وأنها حرب أفكار، وأنها تطلق دوامة من العنف، وتدار بأسلوب التدمير الفجائي لقوى الخصم معنويا ونفسيا، بإطلاق عملية من شأنها إشاعة الإحباط لدى الخصم، وأن ميدانها هو الفضاء الإلكتروني" (محمد علي، 2021، ص 21). ويشير ذلك إلى اختلاف طبيعة الصراع في الفضاء الإلكتروني، كما أن الخصوم غير متكافئة بالضرورة، فقد يكون العدو جماعة أو تنظيما إرهابيا يستهدف البنية التحتية للمعلومات أو منظومة القيم المجتمعية، أو حتى فردا خبيرا في قرصنة أنظمة البيانات الحساسة للدولة، مما يجعل حجم التهديد والهاجس الأمني في تزايد مستمر. وقد تكون المقولة التالية معبرة بالفعل عن حجم التطور والتحول في أبعاد الإستراتيجية العسكرية وانعكاس الفضاء السيبراني على أمن الدول: "إذا كان اكتشاف البارود قد غيّر من ملامح الخريطة الدولية

للحروب، فإن التحكم في مسارات الدولة الحديثة معلوماتياً أضحي قادراً على إصابة الدول الكبرى بالشلل والهزيمة من دون أن تُطلق عليها رصاصة واحدة" (وليد محمود، 2013).

3.2 الفضاء السيبراني وتهاوي الحدود التقليدية: الاختراق الذكي للحدود:

تُعرف الحدود بأنها "عملية قانونية وسياسية لتحديد المدى المكاني لسلطة الدولة" وأنها تمثل "فاصلاً واضحاً من السهل معرفته وتحديد مكانته بين نظامين أو دولتين مختلفتين" (غضبان، 2007، ص300). ولكن مفهوم الحدود بهذا المعنى عرف تحولاً خاصة مع الثورة في المجال التكنولوجي.

فالإنترنت تخطت مفهوم الحدود الإقليمية، واختزقتها مما يخلق مجالاً جديداً للنشاط البشري ويقوض جدوى - وشرعية - تطبيق القوانين القائمة على الحدود الجغرافية (Mueller، 2016)

من خصائص هذا الفضاء تلاشي الحدود التقليدية للدول، فبالتزامن مع حضور هذا الفضاء الجديد تحوّل العالم إلى ما يشبه القرية الكونية بفعل تأثير التطور التقني وثورة المعلومات، مما جعل المفاهيم التقليدية المتصلة بالزمان والمكان تتراجع تدريجياً، حيث أن "الزمن تكتفّ، والمكان تقلّص وتميّع، كما أن المسافات انحازت إلى الانحسار والانعدام، وهو ما عبّر عنه البعض بموت المسافات" (هروس، 2020). بالتالي، أصبح هناك هاجس أمني متجدداً يرتبط بانتشار التهديدات الأمنية العابرة للحدود، وما يفسر تغير رؤى الدول وتراجع المفاهيم التقليدية للأمن الذي مرده التغير في الظواهر الأمنية (برّي، ص80).

كما أن غياب الحدود في هذا الفضاء الإلكتروني، إلى جانب طبيعة العدو وتجاوز التهديد طابعه التقليدي، يعد مصدراً للمخاطر (SANS Institute, 2004, p.07). ويشكّل تهاوي الحدود التقليدية أكبر تهديد للدولة، باعتباره ثغرة تستغلها جماعات الإجرام السيبراني والفواعل من غير الدول، "خاصة مع بروز الشركات التكنولوجية العابرة للحدود الدولية وبروز أخطار القرصنة والجريمة الإلكترونية والجماعات الإرهابية" (عطية، 2019، صفحة 106). لقد أصبح التطور التقني وثورة المعلومات سلاحاً ذا حدين، وسمحت شبكة الإنترنت بإلغاء الحدود وتقليص المسافات، مما أتاح فرص الاختراق الذكي للحدود باستخدام التقنيات المتطورة والبرامج الخبيثة والفيروسات لتهديد مصالح الدول وبُناها التحتية.

ومن أشهر نماذج الاختراق الذكي للحدود عُرف برنامج "ستوكس نت" (Stuxnet) الذي تم تطويره في 2005، والذي استهدف المنشآت النووية لإيران بالتجسس والتخريب (سينجر، 2018، ص 08)، وكذلك فيروس "شمعون" الذي استهدف دولا وشركات كبرى (شركة رأس غاز القطرية، شركة أرامكو السعودية)، انطلاقا من مهاجمته للبيانات وتعطيل الخدمة، فأحدث العطب بحوالي 30 ألف جهاز حاسوب، وقد اكتشفته شركة Symantec في عام 2012 (عبد العظيم، 2020، ص 414).

ومن خلال خصائص الفضاء السيبراني وإمكانية التحرك بمرونة مع إمكانية التخفي وتزييف الهوية، تحولت فرضية تهاوي الحدود التقليدية -شيئا فشيئا- إلى واقع تحت تأثير العولمة بمختلف أبعادها، وهو ما يذكّر بمقولة عالم الاجتماع الأمريكي "دانيال بال" (Daniel Bell) حينما وصف الدولة في هذا العصر بأنها "أصغر من أن تتعامل مع المشكلات الكبرى، وأكبر من أن تتعامل بفعالية مع المشكلات الصغرى" (جندلي، 2010، صفحة 29). وفي هذا الصدد يُسجل عجز القانون الدولي عن توفير حماية وغطاء قانوني فعال في مواجهة التهديدات التي تمس الدول من خلال الفضاء السيبراني باستغلال حالة الانكشاف الحدودي فيه، كما لازالت التشريعات الوطنية قاصرة في مجال مواجهة أساليب الاختراق، مما يزيد حجم التهديد على صعيد أوسع ويؤثر بالتالي في مفهوم السيادة الوطنية.

3. واقع السيادة الوطنية في الفضاء السيبراني

مع حضور الفضاء الإلكتروني بجميع خصائصه وإيجابياته وسلبياته وتغلغله في كل نواحي الحياة، وجدت الدول نفسها في مواجهة تراجع المفاهيم والمدرجات التقليدية للأمن والسلطة والحدود والسيادة، مما جعل مسألة واقع السيادة الوطنية في الفضاء السيبراني مطروحة كواحدة من التحديات التي تواجهها الدولة اليوم في عصر التطور التكنولوجي والرقمنة.

1.3 أمن الدولة في عصر الرقمنة:

انطلاقا من العناصر التي تم تناولها آنفا، يمكن القول بأن أمن الدولة بات نسبيا، كمفهوم أولا وكظاهرة ثانيا، خاصة وأن الأمن في عصر العولمة والرقمنة لا يتوقف على الترسانة العسكرية فحسب في

ظل ظهور تهديدات ناعمة كالتحديات عبر الفضاء السيبراني ومن بينها ما يمس الهوية واستقرار المجتمعات. والدولة اليوم تعيش هاجس بلوغ الحد الأقصى من الأمن، ويقع على عاتقها بالتماشي مع ذلك تكييف سياساتها وإستراتيجياتها لاحتواء التهديدات غير التقليدية.

في هذا الإطار، من الضروري بالنسبة للأمن الوطني للدولة أن يراعي العناصر الآتية (الشهراني، 2006، الصفحات 70، 71):

- **النسبية:** فالأمن نسبي، والدولة لا تكون قادرة دوماً على تحقيقه دون الانخراط في التعاون الدولي.
- **المرونة:** بما يسمح له بمواكبة التحولات المستقبلية.
- **وضوح مصدر التهديد:** فمعرفة مصدر التهديد والتحدي، أو معرفة العدو، في الحاضر والمستقبل أمر ضروري لبناء الإستراتيجية.
- **التحكم الجيد والاستثمار في عوامل القوة على اختلافها.**

هذه العناصر أو الخصائص هي التي تجعل تصوّر الدولة لأمنها مطاطياً، مواكبا لكل التحولات والمستجدات، وإن كان الفضاء السيبراني يطرح إشكاليات أكبر تتعلق بغياب الحدود وتراجع مفهوم السيادة، والتعامل مع عدو مجهول الهوية أحياناً، خاصة وأن الفواعل في هذا الفضاء متنوعة (دولانية وغير دولانية في صورة أفراد وجماعات وتنظيمات عابرة للحدود الوطنية).

وقد تفتّنت الولايات المتحدة الأمريكية إلى حجم التهديد الذي يطرحه الفضاء السيبراني، فقامت بإدراجه في أجندة أمنها الوطني منذ 1996، وأشار الرئيس الأسبق "باراك أوباما" (Barac Obama) إلى أن التهديدات التي تأتي من خلال هذا الفضاء تطرح تحديات أمنية واقتصادية كثيرة (Tabansky, 2011, p.79)، وذلك بالنظر إلى أن معظم الخدمات والبنى التحتية والمعلومات والأنظمة المالية ترتبط بالإنترنت (بزي، 2019، صفحة 95). كما كيّفت الدول الأوروبية، على غرار إستونيا وفرنسا، رؤيتها الأمنية مع التهديدات الجديدة بعد أن عرفت إستونيا هجوماً إلكترونياً في سنة 2007 من مواقع حكومية وتضمّن حرمانها من الخدمة (بلفرد، 2016، صفحة 145).

جاء هذا أصبح أمن الدولة في عصر الثورة الرقمية شديد النسبية، وفي هذا السياق تناول الكاتبان "بنجامين ويتس" (Benjamin Wittes) و"غابرييلا بلوم" (Gabriella Blum)، في كتابهما "مستقبل العنف" نواحي تأثير التطور التكنولوجي وشبكة الإنترنت التي باتت "قادرة على إنتاج بيئة من الحرية غير المسؤولة"، كما أن التهديدات الجديدة المتصلة بالتكنولوجيا قد "نجمت في تحويل طبيعة العنف إلى نقطة أصبح فيها التمييز بين الحرب واللا حرب أقل وضوحاً" (عبد العليم، 2015). وهو ما يفرض على الدولة اليوم تحديثاً وتطويراً مستمراً لسياسات وآليات حفظ أمنها وتنظيم الفضاء السيبراني، مع تأكيد أهمية التعاون الدولي في مواجهة التهديدات التي يكون هذا الفضاء وسيلة فيها ومسرحاً لها.

2.3 تطبيق السيادة في الفضاء السيبراني:

تشكل السيادة عنصراً ومكوناً أساسياً من مكونات الدولة، إلى جانب الإقليم والشعب والسلطة السياسية والاعتراف الدولي. فمنذ نشأة الدولة القومية على إثر معاهدة "واستفاليا" التي أنهت حروب الثلاثين عاماً الدينية في أوروبا (1618-1648م)، أصبحت سيادة الدولة على إقليمها مبدأ مقدساً في العلاقات الدولية التي انحصرت مضمونها في ذلك الوقت في العلاقات بين الدول. ولكن هذا المبدأ شهد لاحقاً تحولات وانتقالات نحو النسبية نتيجة تحولات النظام الدولي وظهور مبادئ كالتدخل الإنساني على سبيل المثال.

ومع بداية عصر العولمة، توقع بعض الدارسين أن السيادة الوطنية لن تزول دفعة واحدة وإنما ستسير نحو التآكل التدريجي بصورة أعمق مما عرفته خلال القرن العشرين (غضبان، 2007، صفحة 359). هذا التآكل الذي لا يرتبط بالعولمة الاقتصادية والاختراق الثقافي لخصوصيات المجتمعات فحسب، ولكنه يرتبط أيضاً بإعادة فهم الحدود انطلاقاً من الفضاء السيبراني، بما يطرح إشكالية تطبيق سيادة الدولة داخله.

إن الإنترنت قد تحدت المهام التقليدية للدولة وهي: ضمان الأمن الوطني، تنظيم النشاط الاقتصادي وفرض نمط من القيم في المجتمع، لئتم بذلك تقويض السيادة (Peritt, 1998, p.427). وتقرن مسألة تطبيق السيادة في الفضاء السيبراني بعدة نقاط من بينها مدى قدرة الدولة على

فرض الانضباط وتنظيم النشاط في المجال السيبراني (بري، 2016، صفحة 116)، وهو مظهر من مظاهر السيطرة المحلية على التكنولوجيا (Ilves, Osula, 2020, p.27)، بمعنى سلطة ردع ورقابة حكومية تكون بالمرصاد لكل الأنشطة غير الاعتيادية، سواء على محركات البحث أو منصات التواصل الاجتماعي (فيسبوك، تويتر...). ولكن هذا يطرح في المقابل اختراق الخصوصية الفردية للمواطن. وبما أنه لا توجد حدود واضحة في هذا الفضاء كتلك التقليدية، تبقى مسألة تطبيق السيادة الوطنية نسبية وأقرب إلى التآكل حتى مع الجهود الوطنية والدولية المتواصلة. فمبدأ السيادة التامة والمطلقة للدولة على إقليمها برا وبحرا وجوا صار من الماضي، لصالح سيادة مختزقة بكافة الأشكال والطرق.

3.3 الانتقال من الصراع على السيادة الإقليمية إلى الفضاء السيبراني:

أدى ظهور شبكة الكمبيوتر العالمية إلى تدمير الرابط بين الموقع الجغرافي وقوة الحكومات المحلية لتأكيد السيطرة على السلوك عبر الإنترنت، إذ من المفروض أن تشكل السيطرة على الفضاء المادي والأشخاص والأشياء الموجودة فيه سمة مميزة لسيادة الدول، مما يتطلب سنّ آلية قانونية تعتمد - إلى حد كبير - على القدرة على ممارسة السيطرة المادية على منتهكي القانون وفرض عقوبات قسرية عليهم. لكن الجهود المبذولة للتحكم في تدفق المعلومات الإلكترونية عبر الحدود المادية - لرسم التنظيم المحلي والحدود المادية للفضاء السيبراني - من المرجح أن تكون عقيمة، على الأقل في البلدان التي تأمل أن تكون طرفا في التجارة العالمية. فمنفذو الهجمات الإلكترونية يمكنهم بسهولة الوصول إلى المعلومات وقنوات الاتصال، مما يعكس أن حجم الاتصالات الإلكترونية التي تعبر الحدود الإقليمية كبير جدًا مقارنة بالموارد المتاحة للسلطات الحكومية للسماح بمراقبة مجدية (Johnson, 1996, p. 1367).

واستجابة لتطورات الرقمنة، استثمرت الحكومات في القدرات الإلكترونية من أجل تأمين شبكات الدفاع الوطني والبنية التحتية. ونظرًا لأن القدرات الإلكترونية قللت بشكل كبير من التكاليف العسكرية والبشرية للحرب، وأصبح من السهل الوصول إليها، أصبحت كل من الحكومات والجهات الفاعلة غير الحكومية على استعداد متزايد لاستخدامها كأدوات هجومية. إن "الهجمات الإلكترونية يمكن أن تكون ضارة مثل الهجمات التقليدية (...)"، حيث أصبحت أكثر تكرارًا وأكثر تعقيدًا وأكثر تدميرًا" كما أبرز

الأمين العام لحلف الناتو ينس ستولتنبرغ *Jens Stoltenberg* في مؤتمر الدفاع الإلكتروني في لندن في ماي 2019، فخلال السنوات الماضية أعلنت دول مثل الولايات المتحدة وروسيا اعتماد عقيدة هجومية عبر الإنترنت، تحدد كيف ومتى ستستخدم الأسلحة السيبرانية (Cyber Weapons: The New Arms Race, 2019). في محاولة لتنظيم هذا المجال نظرا لتنامي التهديدات السيبرانية، تنوعها، وتوسع نطاقها خلال العقد الأخير، ويسرد الجدول التالي وقائع تبرز الصراع السيبراني الحالي.

الجدول 1: طيف من الهجمات السيبرانية.

السنة	اسم الهجوم السيبراني
1990	• هجمات حلف الناتو الالكترونية على يوغسلافيا واستهداف تعطيل شبكات الاتصالات
2006	• الحرب الالكترونية بين حزب الله وإسرائيل
2007	• الهجمات الالكترونية الروسية على استونيا
2008	• الهجمات الالكترونية الروسية على جورجيا
2010	• الهجمات الإسرائيلية الأمريكية ضد المنشآت النووية الإيرانية (فيروس ستاكسنت)
2012-2008	• المواجهات الالكترونية بين حماس وإسرائيل
2017-2012	• هجمات فيروس "شمعون" على المملكة العربية السعودية والتي استهدفت شركة أرامكو وبعض المنشآت الحيوية الحكومية
2015-2014	• هجمات فيروس "دوكو" على شبكة فنادق استضافت محادثات تتعلق بالملف النووي الإيراني
2016	• اتهام روسيا بالقرصنة الالكترونية في الانتخابات الأمريكية لدعم المرشح الجمهوري دونالد ترامب.
2021	• الهجوم الاسرائيلي على مفاعل "نطنز" النووي الإيراني
2021	• اتهام روسيا بشن هجمات الفدية Ransomware Attack على مؤسسات أمريكية

المصدر: علي عبد الرحيم العبودي، 2019، ص110. (بتصرف)

توفر الأحداث المبينة أعلاه سببًا إضافيًا لاستنتاج أن بيئة الأمن السيبراني الجيوسياسية الحالية هي بيئة صراع، تتميز بشكل مناسب بأنها سباق تسلح في المجال السيبراني الذي برز كحالة جديدة من أنماط الصراع وتأثيراته المختلفة في ظل حالة الاستقطاب بين الشرق والغرب، ودور الثورة الصناعية الرابعة في تراتبية القوة في النظام الدولي، دون إغفال الاتجاهات الجديدة للخلاف الروسي- الأمريكي حول السيادة السيبرانية، وهو ما انعكس على القضايا والإستراتيجيات التي ستؤثر حتماً على مستقبل الصراع السيبراني بين الدولتين من جهة، إلى جانب تأثير ذلك على الأمن الجماعي الدولي من جهة أخرى.

في هذا الشأن، أقرت الولايات المتحدة إستراتيجية جديدة للأمن السيبراني في عام 2018، اتخذت موقفاً أكثر شراسة من ذي قبل بخصوص الحرب السيبرانية، ذلك في مقابل تهديدات كل من الصين وروسيا، ودخلت الإستراتيجية حيز التنفيذ بعد قرار "ترامب" بإلغاء قواعد حدها سلفه "أوباما" للعمليات السيبرانية، مع الاتجاه للاستعداد للحرب السيبرانية من خلال بناء قوة أكثر فتكاً، وتوسيع التحالفات والشراكات، والرد بطريقة هجومية ودفاعية في حال قيام أي دولة بنشاط سيبراني ضدها، وذلك لن يتم بالضرورة في الفضاء السيبراني. كما أن فشل عملية ردع الأنشطة السيبرانية التي تشكل استخداماً للقوة ضد الولايات المتحدة أو حلفائها ستدفع إلى استخدام القوة المشتركة من القدرات العسكرية رداً على ذلك في المجال المادي. والاتجاه كذلك إلى تبني إستراتيجية قائمة على "الهجوم الدفاعي"، والتحرك إلى الإمام خارج الحدود واختراق شبكات الخصم، وتعزيز القدرات لجمع المعلومات الاستخباراتية والاستعداد للصراعات المستقبلية.

هذا وتسعى الدول، بشكل غير علني عكس مع تفرقه المعاهدات الدولية، إلى:

- توظيف الفضاء السيبراني لتحقيق أهداف خارجية والتدخل في الشؤون الداخلية من خلال دعم حركات معارضة سياسية أو مسلحة، سواء عبر تقديم الدعم التقني أو السياسي أو الإعلامي.

- التوجه لتوظيف الفضاء السيبراني لفرض العقوبات الدولية على السلوك، عبر منع تصدير تكنولوجيا عسكرية أو تجسسية أو قطع كابلات الانترنت الواصلة للدولة أو حجب مواقع مساندة للدولة في الداخل.
- تصعيد الأنشطة السرية والاستخباراتية وتوظيف برمجيات التجسس والرصد، والتحول من توجيه هجمات سيبرانية من الخارج إلى الداخل إلى توظيف عملاء الاستخبارات أو الدبلوماسيين المقيمين لشن هجمات من الداخل إلى داخل الدولة (عبد الصادق، 2019).

4.3 إعادة التفكير في السيادة السيبرانية:

على الرغم من التصنيف الصحيح للفضاء السيبراني كمجتمع عالمي، واعتباره من الناحية القانونية مجتمعًا مشتركًا، لا يخضع لسيادة دولة واحدة أو مجموعة دول، ونظرًا لخصائصه بوصفه محصنًا من الاستيلاء، فإن ممارسات الدول تقدّم أدلة كافية على أن الفضاء الإلكتروني، أو بالأحرى: مكوناته، ليست محصنة ضد السيادة ومن ممارسة الولاية القضائية (Heinegg, 2012, pp. 7-19).

ومع ذلك، فإن الإنترنت وشبكات الكمبيوتر لها مواقع مادية، تحت الولاية القضائية الإقليمية لدولة واحدة أو أكثر، والجهات الفاعلة فيه لديها جنسية، بغض النظر عما إذا كانوا أفرادًا أو شركات (Wrangle, 2020, pp. 67-105).

فمن ناحية، لقد مارست الدول، وستواصل ممارسة ولايتها القضائية الجنائية فيما يتعلق بالجرائم الإلكترونية، وتواصل تنظيم الأنشطة في الفضاء الإلكتروني. ومن ناحية أخرى، من المهم أن نأخذ في الاعتبار أن "الفضاء السيبراني يتطلب وجود بنية مادية". وعادة ما تكون المعدات المعنية موجودة داخل أراضي الدولة مملوكة من قبل الحكومة أو من قبل الشركات.

في هذا الصدد لا يمكن تفسير دمج المكونات المادية، أي البنية التحتية الإلكترونية الموجودة داخل أراضي الدولة، في "المجال العالمي" للفضاء الإلكتروني بأنه تنازل عن ممارسة السيادة الإقليمية. وفي ضوء البنية الحقيقية للفضاء السيبراني قد يكون من الصعب ممارسة السيادة. ومع ذلك، فإن المشاكل التقنية التي

ينطوي عليها الأمر لا تمنع الدولة من ممارسة سيادتها، ولا سيما سلطتها القضائية الجنائية، على البنية التحتية السيبرانية الواقعة في المناطق التي تغطيها سيادتها الإقليمية.

هذا ويستلزم التطبيق الأساسي لمبدأ السيادة الإقليمية على الفضاء السيبراني أن البنية التحتية السيبرانية الموجودة على الأرض، في المياه الداخلية، في البحر الإقليمي، أو في المجال الجوي الوطني، ومن حيث المبدأ، يحق للدولة ممارسة السيطرة عليها (أي على البنية التحتية الإلكترونية) وعلى الأنشطة الإلكترونية في تلك المناطق. ومع ذلك، لا يجوز استبعاد ممارسة السيادة من خلال القواعد العرفية أو التقليدية للقانون الدولي مثل حصانة المراسلات الدبلوماسية أو حقوق المرور البريء، والمرور العابر، والمرور في الممرات البحرية الأرخيبيلية (Heinegg, Ibid).

ولا يزال الحديث عن رغبة العديد من الدول في وضع قيود على الإنترنت مما ينهي عصر "الويب المفتوح" محلّ جدل واسع، ولا سيما مع انتشار الفكر "الطوباوي" السيبراني والفكر "التحرري" السيبراني الذي يرى أن الفضاء الإلكتروني غير قابل للحكم، ومن ثم يجب الحفاظ عليه باعتباره شبكة عالمية لامركزية.

انطلاقاً من هذا، فإن قدرة كل من الدول والشركات على إنشاء مناطق أو أقاليم في الفضاء السيبراني. يستلزم العديد من الأدوات كحجب ال IP، والبحث عن الكلمات الرئيسية لمراقبة المناقشات حول الموضوعات الحساسة، ومنع الوصول إلى مواقع الويب التي تعتبر تخريبية. وهو ما تم تطبيقه في العديد من الدول، كالجدار الناري العظيم في الصين، ونُظم الرقابة الحكومية الصارمة على الإنترنت في كوريا الشمالية لمواجهة ما يمكن أن نسميه بـ "الانكشافية السيبرانية"، ليتبلور بذلك نمط جديد من المجتمعات يمكن أن يطلق عليه "مجتمعات المراقبة".

وعلى الجانب الآخر، ستخلق الشركات الكبرى (مثل: جوجل، وآبل، ومايكروسوفت) مناطق في الفضاء السيبراني، من خلال ابتكار منتجات تحدد منطقة في الواقع الافتراضي والتي سيتعين على المستخدمين الآخرين المرور من خلالها، كما ستستخدم الشركات برامج إدارة الحقوق الرقمية، والتراخيص المحدودة، وملفات تعريف الارتباط، ومتطلبات التسجيل لإنشاء حدود تسمح بجمع البيانات، ومراقبة

المستخدمين. باختصار، سترغب الشركات في إعادة توطين الفضاء الإلكتروني لدعم أنشطتها الريادية. ويرجع ذلك جزئياً إلى موقف العديد من الشركات المتضارب تجاه السياسة والقانون. فمن ناحية، ستمتنع عادةً عن خرق القانون بشكل صريح لتقليل مخاطر العمل. ومن ناحية أخرى، ستعمل على تحدي الدولة بسبب العداء المتأصل في الشركات ضد ما تعتبره تدخلاً غير شرعي أو غير فعال للدولة والذي يجب الآثار التحريرية والتمكينية للتكنولوجيا (زيد، 2019).

4. خاتمة:

- ختاماً، لا يزال الشكل الويستفالي للسيادة مفهوماً مهماً تُبنى عليه السياسة والقوانين واللوائح والاتفاقيات والمعاهدات، وبالتالي فهو الأساس لتحديد سياسة وإستراتيجية الدول، لكن وتحت تأثير العولمة بمختلف أبعادها ومظاهرها، ومع تطور تكنولوجيا الاتصالات وثورة المعلومات تلاشى عصر السيادة الوطنية المطلقة لصالح سيادة نسبية ومختزقة، بفعل وجود فضاء مرن ولا محدود وغير قابل للرقابة يقابل الفضاء المادي التقليدي ويختلف عنه في خصائصه ودينامياته، فأصبحت فيه الحدود إلى حدٍّ ما سهلة الاختراق.

ونتيجة لذلك يمكن أن نبرز جملة استنتاجات نوجزها في التالي:

- بما أنه لا توجد حدود واضحة في الفضاء السيبراني كتلك التقليدية، تبقى مسألة تطبيق السيادة الوطنية نسبية وأقرب إلى التآكل حتى مع الجهود الوطنية والدولية المتواصلة. فمبدأ السيادة التامة والمطلقة للدولة على إقليمها برا وبحرا وجوا صار من الماضي، لصالح سيادة مختزقة بكافة الأشكال والطرق، وهو ما اتضح جليا في ظل ما شهدته تكنولوجيا المعلومات والاتصالات من تطور له إيجابياته وسلبياته.

- يمكن القول إن مبدأ السيادة الإقليمية والحق المترتب على ذلك لدولة ما في ممارسة ولايتها الإقليمية ينطبق على الفضاء السيبراني بقدر ما يتعلق الأمر بالبنية التحتية الإلكترونية داخل الإقليم.

- لقد تحدّت الإنترنت المهام التقليدية للدولة وهي: ضمان الأمن الوطني، تنظيم النشاط الاقتصادي وفرض نمط من القيم في المجتمع، ليتم بذلك تقويض السيادة نسبيا وتدرجيا.

- تعد قدرة الدولة على فرض الانضباط وتنظيم النشاط في المجال السيبراني نسبية على وجه العموم، وهو ما أثر في فرض السيادة السيبرانية بصورة تحتوي أنواع التهديدات كافة.
- في ظل انتشار الفكر "الطوباوي" السيبراني والفكر "التحرري" السيبراني يصبح الحديث عن وضع قيود على الإنترنت محل جدل واسع.

5. قائمة المراجع:

أولاً: باللغة العربية.

المؤلفات:

- برّي، محمود، (2019)، السيبرنيطيقا (السيبرانية): علم القدرة على التواصل والتحكم والسيطرة، منشورات المركز الإسلامي للدراسات الإستراتيجية، لبنان.
- عبد الغفار، فيصل محمد، (2016)، الحرب الإلكترونية، الجندارية للنشر والتوزيع، الأردن.
- غضبان، مبروك، (2007)، المدخل للعلاقات الدولية، دار العلوم للنشر والتوزيع، الجزائر.
- كين، ديفيد، (2008)، حرب بلا نهاية: وظائف خفية للحرب على الإرهاب، تر معين الإمام، ط 1، د.د.ن، المملكة العربية السعودية.
- لونج، أوستن، وآخرون، (2014)، الحروب المستقبلية في القرن الحادي والعشرين، منشورات مركز الإمارات للدراسات والبحوث الإستراتيجية، الإمارات العربية المتحدة.
- محمد علي، محمود، (2020)، إشكالية حروب الجيل الخامس، د.د.ن، مصر.

المقالات:

- بلقرد لطفي لمن، (2016)، الفضاء السيبراني: هندسة وفواعل، المجلة الجزائرية للدراسات السياسية، المجلد 3 (العدد الأول)، ص: 145-154؛
- جندلي، عبد الناصر، (2010)، إشكالية تكييف المنظور الواقعي للعلاقات الدولية مع التحولات الدولية لما بعد الحرب الباردة، مجلة المستقبل العربي، العدد 376، ص: 24-41؛

- زروقة إسماعيل، (2019)، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، المجلد 10 (العدد الأول)، ص: 1016-1031؛
- عادل زقاع، منصوري سفيان، (مارس 2016)، الجريمة المنظمة بمنطقة الساحل الإفريقي: بانوراما سوسيو-أمنية، مجلة العلوم الإنسانية والاجتماعية، العدد 23، ص: 155-166.
- عبد العظيم محمد عبد الجواد، أميرة، (2020)، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد 35، ص: 363-531.
- عطية إدريس، (2019)، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، المجلة الجزائرية للدراسات السياسية، المجلد الأول (العدد الأول)، ص: 100-123؛
- علي عبد الكريم العبودي، (2019)، هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين، مجلة قضايا سياسية، (العدد 57)، ص: 106.

الأطروحات:

- شفيق، نوران، (2014)، الفضاء الإلكتروني وأنماط التفاعلات الدولية، رسالة ماجستير، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة.
- الشهراني، محمد سعيد آل عياش، (2006)، أثر العولمة على مفهوم الأمن الوطني "دراسة مسحية على مجموعة من الأكاديميين في الرياض" استكمالا لنيل درجة الماجستير في القيادة الأمنية، قسم العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية.

المداخلات:

- حجاج، قاسم، (27-28 أوت 2013)، مدخل إلى تحليل نسقي للأسباب الهيكلية للهزات الأمنية الشاملة في المنطقة المغاربية-الساحلية، المؤتمر المغاربي الدولي حول التهديدات الأمنية للدول المغاربية في ضوء التطورات الراهنة: الرهانات والتحديات، الجزائر.

- سينجر، بيتر، (19 أوت 2015)، الإرهاب الإلكتروني: خرافات، وحقائق، وفيروس ستوكسنت، وتنظيم داعش، ووسائل الإعلام الاجتماعي، ومسرح المواجهة، مركز الإمارات للدراسات والبحوث الإستراتيجية، الإمارات العربية المتحدة؛

مواقع الانترنت:

- أبو عامر، عدنان، (2021)، هكذا تخوض إسرائيل جبهتها القتالية الجديدة عبر "الساير"، موقع

الجزيرة: <https://bit.ly/3f7M9Ew> (consulté le 05/05/2021)

- أبو زيد، هيدر، (2019)، السيادة الإلكترونية: اتجاهات تشكيل مناطق سيبرانية تحت سيطرة الدول والشركات، المستقبل للأبحاث والدراسات المتقدمة، المستقبل للأبحاث والدراسات المتقدمة:

<https://soo.gd/l9T4> (consulté le 23/05/2021)

- عبد العليم، أحمد، (2015)، تهديدات غير تقليدية: مستقبل العنف في ظل التطورات

التكنولوجية، المستقبل للدراسات والأبحاث المتقدمة:

<https://bit.ly/3o0aOip> (consulté le 28/05/2021)

- عبد الصادق، عادل، (2018)، صراع السيادة السيبرانية بين التوجهات الروسية والأمريكية، المركز

العربي لأبحاث الفضاء السيبراني

http://www.accronline.com/article_detail.aspx?id=29415

(consulté le 28/05/2021)

- عزت، محمود، الفضاء السيبراني وتحديات الأمن المعلوماتي العربي، موقع المجلة العربية:

<https://bit.ly/3bdJs33?Id=62> (consulté le 26/05/2021)

- هروس، حفيظ، (2020)، سلطة الافتراضي، مركز تكامل للدراسات والأبحاث:

<https://shortest.link/1682> (consulté le 02/05/2021)

- وليد محمود، خالد، (2013)، الهجمات عبر الإنترنت: ساحة الصراع الإلكتروني الجديدة، المركز

العربي للأبحاث ودراسة السياسات:

<https://bit.ly/3bdJs33> (consulté le 02/05/2021)

ثانيا: باللغة الأجنبية.

Reports:

- Krepinevich, Andrew, (2012), *Cyber Warfare : A Nuclear Option ?*, Center for Strategic and Budgetary Assessments (CSBA).
- SANS Institute, (2004), *Information Warfare : Cyber Warfare is the Future Warfare*.

Articles:

- Ilves, Luukas and Osula, Anna-Maria, (2020), *The Technological Sovereignty Dilemma and How New Technology Can Offer a Way Out ?*, *European Cybersecurity Journal*, Vol .06 (Issue 01), p-p : 24-35.
- Perritt, Henry, (1998), *The Internet as a Threat to Sovereignty ? Thoughts on the Internet's Role in Strengthening National and Global Governance*, *Indiana Journal of Global Legal Studies*, Vol.05 (Issue 02), p-p : 423-442.
- Tabansky, Lior, (2011), *Basic Concepts in Cyber Warfare*, *Military and Strategic Affairs*, Vol.03, (No.01), p-p : 75-92.
- Wrangle, Pål, *Sovereignty, belligerency and the new normal in cyberspace*, Submitted version of chapter published in Linda Bishai (ed.), *Law, Security and the State of Perpetual Emergency*, University of Stockholm, Palgrave, 2020, 67-105.

Web sites:

- Heinegg, Wolff Heintschel von, *Legal Implications of Territorial Sovereignty in Cyberspace*, 4th International Conference on Cyber Conflict, Faculty of Law Europa-Universität, Frankfurt (Oder), Germany, 2012, p-p :7-19 <https://soo.gd/uGln> (consolé le 09/05/2021)

- *Mueller, Milton, Sovereignty and Cyberspace: Institutions and Internet governance, 2016, <https://bit.ly/2WTCNat> (consulté le 07/09/2021)*