

تحديات السيادة الوطنية في مواجهة الفواعل التكنولوجية العابرة للقارات - دراسة حالة
منظومة "ستارلينك"

Challenges to National Sovereignty in the Face of Transnational
Technological Actors: A Case Study of the "Starlink" System

وادي أحمد¹

¹ جامعة الجزائر 3، ouadi.ahmed@univ-alger3.dz

تاريخ النشر: 2026/10/15

تاريخ القبول: 2026/09/28

تاريخ الاستلام: 2026/04/22

ملخص:

تتناول هذه الدراسة إشكالية التحول في مفهوم السيادة الوطنية للدولة القومية أمام تغول الفواعل التكنولوجية العابرة للحدود، مع التركيز على منظومة "ستارلينك" (Starlink) التابعة لشركة "SpaceX" كنموذج تطبيقي. تهدف الدراسة إلى تفكيك أبعاد "التآكل الرقمي" للسيادة بفعل تكنولوجيا الإنترنت الفضائي التي تتجاوز الرقابة الحكومية والحدود الجغرافية التقليدية. اعتمدت الدراسة على المنهج الوصفي التحليلي لتشخيص الخصائص الوظيفية لهذه المنظومات وتحليل تداعياتها على الاستقلال الاستراتيجي والأمن القومي للدول.

خلصت الدراسة إلى مجموعة من النتائج، أبرزها أن الفواعل التكنولوجية الكبرى تحولت إلى "كيانات فعالة" تزاخم الدولة في وظائفها الأساسية، وأن الحدود الوطنية أصبحت حدوداً "رقمية" تتطلب فلسفة حوكمة جديدة تقوم على "السيادة الاستراتيجية" و"مبدأ الوقاية السيادية". وتوصي الدراسة بضرورة توطين البنية التحتية المعلوماتية وتحديث الأطر القانونية الوطنية لضمان الامتثال التقني للشركات العابرة للقارات، بما يحفظ توازن القوى بين السلطة السياسية والسطوة التكنولوجية.

كلمات مفتاحية: السيادة الوطنية؛ الفواعل التكنولوجية؛ ستارلينك؛ الأمن القومي؛ السيادة الرقمية.

Abstract:

This study examines the shifting concept of national sovereignty in the face of burgeoning transnational technological actors, focusing on the Starlink satellite system by SpaceX as a primary case study. The research aims to deconstruct the "digital erosion" of state sovereignty caused by satellite internet technology, which bypasses government censorship and traditional geographical borders. Utilizing a **descriptive-analytical approach**, the study diagnoses the functional characteristics of these systems and analyzes their implications for national security and strategic autonomy.

The findings indicate that major technological actors have evolved into "functional entities" competing with states for authority. Consequently, national borders have become "digital-programmatic" boundaries, necessitating a new governance philosophy based on "Strategic Sovereignty" and the "Sovereign Precaution Principle." The study recommends localizing information infrastructure and updating national legal frameworks to ensure the technical compliance of multinational corporations, thereby preserving the balance of power between political authority and technological influence.

Keywords: National Sovereignty; Technological Actors; Starlink; National Security; Digital Sovereignty.

المؤلف المرسل: وادي أحمد ، ouadi.ahmed@univ-alger3.dz

مقدمة:

شهدت البيئة الدولية في العقدین الأخيرین تحولات بنیویة متسارعة ساهمت فی إعادة تشکيل موازين القوى وأنماط النفوذ، حيث لم تعد الدولة القومية الفاعل المهيمن الوحيد على التفاعلات الجيوسياسية. فقد أنتجت الثورة الرقمية المعاصرة نمطاً جديداً من الفواعل العابرة للحدود التي تستمد قوتها من الامتلاك الحصري للتكنولوجيا الفائقة والقدرات المالية الضخمة، مما مكنها من مزاحمة الدول في وظائفها السيادية. وفي هذا السياق، تبرز منظومة ستارلينك (Starlink) التابعة لشركة SpaceX

كنموذج راديكالي لهذه الفواعل، حيث تطرح تحديا مباشرا للمفهوم التقليدي للسيادة الوطنية القائم على نظرية السيطرة الإقليمية.

إن السيادة، التي تبلورت تاريخيا حول السلطة المطلقة للدولة داخل حيزها الجغرافي، تواجه اليوم حالة من التآكل الرقمي والسيولة السيادية؛ إذ تعمل شبكات الأقمار الاصطناعية المدارية على خلق مساحات تواصلية عابرة للرقابة الوطنية، ومتحللة من القيود التشريعية المحلية، مما يجعل من مفهوم الحدود مفهوما افتراضيا بقدر ما هو فيزيائي ومادي.

تتمحور إشكالية الدراسة حول التساؤل الجوهرى التالي : إلى أي مدى تساهم تكنولوجيا الإنترنت الفضائي (نموذج ستارلينك) في إعادة صياغة مفهوم السيادة الوطنية للدولة القومية، وما هي تداعيات هذا التحول على الأمن القومي والاستقلال الاستراتيجي للدول في ظل هيمنة الشركات التكنولوجية الكبرى؟ وينبثق عن هذا التساؤل مجموعة من الأسئلة الفرعية:

1. كيف تغلغلت المنظومات التقنية العابرة للحدود في الوظائف السيادية للدولة ؟
2. ما هي التهديدات التي تفرضها شبكات الأقمار الاصطناعية على الدول ؟
3. ما هي أهم الآليات المتاحة للدول لاستعادة سيادتها الرقمية في مواجهة تغول الفواعل التكنولوجية العابرة للحدود؟

تكتسب هذه الدراسة أهميتها من خلال سد الفجوة المعرفية المتعلقة بتحويلات مفهوم السيادة في الأدبيات السياسية المعاصرة، وفي كونها أيضا تلامس واقعاً استراتيجياً تواجهه الدول (ومنها الجزائر) في كيفية التعامل مع شركات التكنولوجيا الكبرى، وضرورة تطوير أطر قانونية وإدارية تحمي البنية التحتية المعلوماتية الوطنية من الاختراق أو التبعية للخارج.

تتمحور أهداف هذه الدراسة بداية بتفكيك طبيعة العلاقة بين الدولة والشركات التكنولوجية الكبرى كقوى دولية صاعدة ، مع تحليل مخاطر تجاوز البوابات الوطنية للإنترنت وانعكاساتها على الأمن السيبراني . كما تسعى لاستشراف مستقبل الدولة القومية في ظل التعددية القطبية التكنولوجية ، وصولاً إلى تقديم رؤى عملية لصناع القرار لمواجهة التكنولوجيات المزعزعة وضمان الأمن القومي الرقمي .

اعتمدت الدراسة على المنهج الوصفي التحليلي، كونه الأنسب لتشخيص وتحليل ظاهرة تداخل التكنولوجيا مع السيادة كمفهوم سياسي وقانوني يرتبط بالدولة. حيث تم استخدام الجانب الوصفي لرصد الخصائص التقنية والوظيفية لمنظومة ستارلينك وسياقات ظهورها في البيئة الدولية، بينما تم توظيف الجانب التحليلي لتفكيك أبعاد النزاع بين السلطة السياسية والسلطة التكنولوجية، مع تحليل حالات دراسية واقعية (مثل ردود أفعال بعض الدول مع ستارلينك) لاستخلاص النتائج وتعميمها على الإطار النظري للسيادة، وصولاً إلى بناء رؤية نقدية لمستقبل الدولة في العصر الرقمي .

المحور الأول : الإطار النظري و المفاهيمي للسيادة في العصر الرقمي

أولاً : تطور مفهوم السيادة (من الاقليم المادي الى الاقليم الافتراضي) :

يعد ظهور مفهوم السيادة تاريخياً إلى القرن السادس عشر، حيث تطور عبر قرون عبر اسهامات فكرية سياسية لمفكرين أمثال جون بودان، توماس هوبز، وجون لوك. وقد ارتبطت السيادة بمبدأ "دولة الحق" والقدرة على تقرير المصير، وهي تتسم بكونها سلطة مطلقة، دائمة، ولا تقبل التجزئة أو التنازل عنها طالما ظلت الدولة قائمة.¹ ومع ذلك، فإن التحول نحو "العملة الرقمية" أحدث إعادة بناء جوهري في هذا المفهوم، حيث أدى التقارب التكنولوجي إلى تقليص صلاحيات الدولة القومية لصالح فواعل دولية وشركات عابرة للحدود، مما أفقد السيادة التقليدية بعض مبررات وجودها في مواجهة التدفق الكبير والسريع للبيانات والمعرفة عبر الحدود دون عوائق قانونية أو تقنية.

تُعرف السيادة الرقمية بأنها قدرة الدولة على التحكم في فضاءها الرقمي والأنظمة الرقمية التي تدعم المجتمع، بشكل مستقل، بما في ذلك البنية التحتية، البيانات، والخوارزميات.² بحيث تظهر "السيادة الرقمية" اليوم كمفهوم مثير للجدل، يقع في قلب المنافسة بين الدول القومية، التكتلات الإقليمية،

والشركات الكبرى، وينقسم الباحثون في مقاربتهم لهذا المفهوم إلى مدرستين رئيسيتين : المدرسة المؤسسية التي تعتبر السيادة وظيفة لقدرة الدولة على فرض إرادتها على إقليمها، والمدرسة البنائية التي ترى السيادة مورداً خطابياً يُستخدم في الصراعات السياسية للسيطرة على الشبكات الرقمية.³

ثانيا : أبعاد وتحديات السيادة الرقمية في السياسة الدولية وأهم التحديات المرتبطة بها :

تتجاوز السيادة الرقمية مجرد التحكم في المحتوى، فهي تمتد لتشمل ثلاث طبقات أساسية: الطبقة المادية (البنية التحتية والأقمار الصناعية)، طبقة الشفرة (المعايير والبروتوكولات)، وطبقة المعلومات (البيانات والمحتوى). إن الدول التي تفتقر إلى التكنولوجيا المحلية تجد نفسها في حالة "تبعية تكنولوجية"، حيث تصبح قدرتها على ممارسة سيادتها رهينة لقرارات الشركات المزودة للتكنولوجيا، مما يجعل الأمن القومي عرضة للاختراق أو العزل بقرار خارجي، اقتصادي أو سياسي.⁴

وتتجلى السيادة الرقمية في السياسة الدولية، في مجموعة من الأشكال تتمثل في:⁵

- سيادة البيانات : تعني التحكم في تدفق وتخزين البيانات الشخصية والوطنية المجمعة داخل الإقليم.
- سيادة الأمن السيبراني : حماية البنية التحتية الحرة من الهجمات والاختراقات ومختلف التهديدات.
- السيادة التكنولوجية : وهي قدرة الدولة على تطوير وامتلاك البنية التحتية والعتاد التكنولوجي.
- السيادة التشريعية : وهي القدرة على سن وإنفاذ القوانين في الفضاء الرقمي.

إن هذا يشير الى أن السيادة الرقمية تعني أيضا القدرة على اتخاذ القرارات الاستراتيجية، وصياغة التشريعات، وإنفاذ القانون في الفضاء الرقمي. إلا أن ذلك قد يواجهه جملة من التحديات والتي تتمثل عادة في:

- الهيمنة الاحتكارية للشركات الكبرى على الرقائق والبرمجيات.
- التخزين السحابي العابر للحدود وصعوبة فرض القوانين المحلية على البيانات
- التهرب القانوني للشركات العابرة للقارات واستخدام بروتوكولات مشفرة، والاعتماد على أنظمة اتصالات فضائية أجنبية.

المحور الثاني : صعود الفواعل التكنولوجية: "ستارلينك" كفاعل سياسي غير دولاتي

لم يعد مفهوم "الفاعل الدولي" يقتصر على الدول أو المنظمات الحكومية الدولية، فقد أدى تراكم القوة التكنولوجية والمالية إلى توسعه ليشمل الشركات متعددة الجنسيات، لما تملكه من وسائل النفوذ والتأثير أصبحت تضاهي الدول الكبرى. وتعد شركة "سبيس إكس" (SpaceX)، بقيادة إيلون ماسك، تجسيدا لهذا التحول، حيث لم تعد مجرد شركة للصناعات الفضائية، بل تحولت إلى مزود عالمي للبنية التحتية الاستراتيجية عبر منظومة "ستارلينك".⁶ إن قدرة هذه المنظومة على توفير الإنترنت في أي نقطة على كوكب الأرض تجعلها أداة تتحدى احتكار الدول لوسائل الاتصال، وقد تجلّى ذلك بوضوح خلال الحرب الروسية الأوكرانية الأخيرة .

أولاً: الخصوصيات التقنية كمحدد قوة لمنظومة ستارلينك على الصعيد الدولي :

تعتمد قوة "ستارلينك" على التكامل العمودي الفريد لشركة SpaceX، فهي تصنع الأقمار الصناعية، وتطلقها باستخدام صواريخها الخاصة (9 Falcon)، وتدير الشبكة الأرضية والبرمجيات، مما يقلل التكلفة بشكل هائل ويمنحها ميزة تنافسية لا يمكن للدول القومية مجاراتها بسهولة، مع سرعة تدفق تصل إلى 610 ميغابت/ثانية، وزمن تأخير (latency) يصل إلى 20 مللي/ ثانية.⁷ وبحلول عام 2025، وصلت القيمة السوقية للشركة إلى حوالي 800 مليار دولار، مع تطلعات للوصول إلى 1.5 تريليون دولار في نهاية عام 2026.⁸ مما يضع هذه الشركة في مصاف أكبر الاقتصاديات في العالم ويمنح مؤسسها نفوذاً سياسياً عالمياً يتجاوز حدود المال والأعمال، وهنا يبرز دور الفرد كأحد الفواعل الهامة أيضاً في العلاقات الدولية.

ثانياً: التوظيف الاستراتيجي لـ Starlink في الصراع الروسي الأوكراني :

ساهمت الحرب الأوكرانية-الروسية في طرح جملة من التحولات في دراسة الأثر المتنامي للفواعل التكنولوجية على السيادة الوطنية للدول وعلى مسرح العمليات العسكري على المستوى العالمي. ففي الأيام الأولى لهذه الحرب في فبراير 2022، استهدفت الهجمات الروسية البنية التحتية للاتصالات الأوكرانية، بما في ذلك الأبراج الأرضية وشبكات الأقمار الصناعية التقليدية (مثل Viasat)، مما أدى إلى

شلل شبه كامل في قدرات القيادة والسيطرة الأوكرانية.⁹ ذلك دفع بالحكومة الأوكرانية بطلب تدخل "ستارلينك" ليوفر خدمة الأنترنت والاتصالات، تعمل على تمكين القوات المسلحة من استعادة الاتصال وتنسيق العمليات الدفاعية على كل الإقليم الأوكراني.

لقد مكنت "ستارلينك" الجيش الأوكراني من الاعتماد على الشبكة وفق ما يسمى "الحرب المرتكزة على الشبكة" (Network-Centric Warfare)، حيث ساهم ذلك في تحقيق الصمود النفسي والاجتماعي وتعزيز قدرات الجيش على مختلف المستويات التي نذكر منها :¹⁰

- ربط الجنود في الخنادق بمراكز القيادة الخلفية وبمنصات الاستطلاع الجوي بشكل مباشر.
- تعزيز قدرات الاستخبارات والمراقبة والاستطلاع (ISR) من خلال النقل السريع للبيانات والصور عالية الدقة من الطائرات بدون طيار (الدرونز).
- تنسيق نيران المدفعية لتوجيه الضربات الدقيقة عبر برمجيات متصلة بالإنترنت الفضائي.
- توجيه قوارب انتحارية مسيرة (درونز بحرية) لضرب الأسطول الروسي في البحر الأسود.

رغم كل ما قدمته منظومة "ستارلينك" للنظام الأوكراني في ظل تطور وتيرة الحرب و حدتها، إلا أن صانع القرار الأوكراني وجد نفسه مرتعناً لإرادة "إيلون ماسك" الشخصية وتفسيراته لاتفاقيات الاستخدام، عندما رفض ماسك تفعيل الخدمة في شبه جزيرة القرم لدعم هجوم أوكراني خوفاً من التصعيد النووي، أظهر ذلك أن "السيادة الوطنية" للدولة في حالة الحرب قد تصبح مقيدة بقرارات "فاعل تكنولوجي" غير خاضع للمساءلة الديمقراطية أو الالتزامات الدولية التقليدية.¹¹ هذا التداخل بين الأهداف التجارية والاعتبارات الجيوسياسية يطرح تساؤلات حول قدرة الدول على الاعتماد على شركات خاصة في أمنها القومي.

ثالثاً : منظومة ستارليك بين الفرص و التحديات القانونية والتنظيمية في الفضاء الخارجي

تواجه المنظومة القانونية الدولية الحالية صعوبات وتحديات جمة في مواكبة وتيرة الابتكار في مشاريع "الكوكبات الضخمة" أو ما يسمى أيضا "بالجموعات الساتلية الضخمة" (Megaconstellations) وهو ما يمثل في نفس الوقت فرصة لهذه الأخيرة في التوسع وفرض نفسها كفاعل دولي هام ينازع الدول في سيادتها على إقليمها، ويمكن اختصار هذه التحديات في عنصرين رئيسيين يتعلقان بـ :

1. قصور الاتحاد الدولي للاتصالات (ITU)

يعتمد الاتحاد الدولي للاتصالات على نظام "الأولوية للتسجيل الأول"، مما يتيح للشركات الكبرى فرصة استغلال هذا النظام عبر حجز كميات ضخمة من الترددات من خلال تقديم العديد من الطلبات، حتى وإن لم تُستغل تلك الطلبات بالكامل، رغم الإتحاد يوصي الأعضاء "بالسعي نحو الحد من عدد الترددات ومن استعمال الطيف إلى أدنى ما يلزم لتأمين الخدمات الضرورية بصورة مرضية"،¹² هذا الواقع يعرقل جهود الدول النامية في تطوير برامج فضائية مستقلة. إضافة إلى ذلك، فإن الافتقار إلى آليات إنفاذ فعالة داخل الاتحاد يعزز تحديات تحقيق "سيادة الطيف الترددي" للدول، ليظل هذا المفهوم نظرياً أمام التحولات التقنية التي تفرضه المنظومات العابرة للقارات.

2. الفجوات في معاهدة الفضاء الخارجي لعام 1967

تعتبر معاهدة الفضاء الخارجي لعام 1967 (OST)، الدستور الأساسي للفضاء، وقد صيغت في سياق المنافسة بين الدول (الولايات المتحدة والاتحاد السوفيتي)، ولم تتوقع ظهور شركات خاصة تمتلك عشرات الآلاف من الأقمار الصناعية. تركز المعاهدة على مبدأ "عدم التملك" للفضاء الخارجي وأنه "تراث مشترك للبشرية"، لكن ما يفرضه الواقع هو أن منظومة "ستارلينك" تفرض وجودها في الفضاء عبر احتلال المدارات والترددات المحدودة. وبموجب المادة السادسة من المعاهدة، تتحمل الدول المسؤولية الدولية عن الأنشطة الوطنية في الفضاء، سواء كانت حكومية أو غير حكومية،¹³ هذا ما يضع الولايات المتحدة في موقف المسؤولية عن تصرفات SpaceX، وهو ما قد يؤدي إلى تصعيد دبلوماسي أو قانوني في حال وقوع حوادث فضائية.

المحور الثالث: مخاطر منظومة ستارلينك على خصوصيات الأفراد وأمن وسيادة الدول

تجاوزت SpaceX مرحلة توفير الإنترنت المدني لتنتقل إلى بناء بنية تحتية مخصصة للأمن القومي الأمريكي تُعرف باسم "ستارشيلد" (Starshield) هذه المنظومة مصممة لاستضافة حمولات حكومية مشفرة وتوفير قدرات مراقبة واستطلاع (ISR) متقدمة لصالح وكالات الاستخبارات، مثل مكتب

الاستطلاع الوطني الأمريكي (NRO) بالنسبة للدول العربية، يمثل هذا التطور تحديا هاما بالنسبة لمسألة السيادة، بحيث يصعب الفصل تقنيا وشكليا بين النسخة المدنية (Starlink) والنسخة الاستخباراتية (Starshield)،¹⁴ إضافة الى ذلك هناك مجموعة هامة من المخاطر على مختلف المستويات نذكر منها :

أولا : مخاطر منظومة ستارلينك على الصعيد التقني والسياسي

لم تعد "البيانات الوصفية" (Metadata) مجرد بيانات هامشية غير مهمة، بل أصبحت الوسيلة الإستخباراتية الأكثر قيمة في حروب الجيل الخامس. فمن خلال منظومة مثل (ستارلينك)، يمتلك المشغل القدرة على رصد البصمة الرقمية للدولة المستضيفة عبر تتبع مواقع المحطات وسجلات التشغيل.¹⁵ هذا الانكشاف المعلوماتي يمنح القوى المهيمنة تفوقا في رسم الخرائط الأمنية والاجتماعية، مما يحول البيانات الوصفية من أداة تنظيمية إلى سلاح استراتيجي يستخدم في التوجيه الدقيق للضربات السيبرانية والعمليات العسكرية ويتضح ذلك جليا من خلال :

- **التدخل التقني والبنوي :** تشير التقارير إلى أن تعطل "ستارلينك" قد يؤدي أحيانا إلى تعطل أجزاء من "ستارشيلد"، مما يثبت عدم وجود عزل فيزيائي تام بين المنظومتين.¹⁶
- **تجاوز الرقابة الوطنية:** تسمح المنظومة للمستخدمين بالاتصال المباشر بالإنترنت دون المرور عبر بوابات الدولة (Gateways)، مما يبطل مفعول أنظمة الرقابة والأمن القومي المحلية ويسمح بتدفق معلومات قد تكون ضارة أو محرّضة.¹⁷
- **القدرة على التعطيل الانتقائي:** يتجاوز خطر الهيمنة التقنية مجرد التجسس ليصل إلى "التحكم الوظيفي" في البنية التحتية للدولة، بحيث يمكن للمشغل عزل مناطق جغرافية كاملة معلوماتيا، مما يؤدي إلى شلل في التواصل بين المنشآت الحيوية في لحظات التأزم الاستراتيجي.¹⁸ إن استغلال هذه القدرة على التدخل من قبل الفاعلين من غير الدول (Non-State Actors) يعيد تعريف مفهوم "الحدود الوطنية" للدولة، إذ لم تعد الحدود تُرسم على الأرض فقط، بل أصبحت تدار عبر لوحات تحكم برمجية قادرة على تمييز فاعلية الدولة داخل حدودها الجغرافية.

ثانيا : الآثار الاقتصادية والاجتماعية على الدول المضيفة

رغم ما توفره منظومة "ستارلينك" من مزايا أساسا تتعلق بتعزيز التنمية البشرية والتعليم والصحة، من خلال مساهمتها في سد الفجوة الرقمية إلى جانب تقديم خدمات تمثل حلا مثاليا للمناطق الريفية والنائية، والتي فشلت الدول في توصيل الخدمات إليها، إلا أن تداعياتها الجيوسياسية تتجاوز الأبعاد التقنية لتمتد إلى العمق الهيكلي للاقتصاد الكلي والنسيج الاجتماعي للدول، حيث تُشكل هذه المنظومات تحديا وجوديا لمزودي خدمات الإنترنت المحليين ضمن نطاق الدولة، والذين يمثلون رافداً حيوياً للسيادة المالية للدولة.¹⁹ إن تدفق خدمات الإنترنت الفضائي بتسعير وآليات تنافسية، وبمعزل عن الحاجة لاستثمارات ضخمة في البنية التحتية، من شأنه أن يحدث حالة من العزوف الاستثماري عن مشاريع الشبكات الأرضية كالألياف البصرية، مما يهدد استدامة القطاع التكنولوجي المحلي ويُضعف قدرة الدول، على بناء استقلال رقمي قائم على قواعد مادية وطنية. وعليه يمكن حصر أهم آثارها السلبية على المستوى الاقتصادي والاجتماعي في :

- **نزيف العملة الصعبة:** يتم دفع اشتراكات المنظومة مباشرة للشركة الأم خارج الحدود، مما يمثل خروجاً لرؤوس الأموال دون استفادة الاقتصاد المحلي من الضرائب أو الرسوم التنظيمية.²⁰
- **الأمن السيبراني والجرائم:** يسهل الإنترنت الفضائي غير الخاضع للرقابة تنفيذ أنشطة غير قانونية، مثل غسيل الأموال، تجارة البشر، والتنسيق بين الجماعات الإرهابية، بعيداً عن أعين السلطات المحلية.²¹

ثالثا : ردود الفعل الدولية تجاه مخاطر الأمن القومي الفضائي :

أدى صعود "ستارلينك" إلى استنفار القوى الكبرى، وعلى رأسها الصين وروسيا، اللتان تريان في المنظومة أداة للهيمنة العسكرية الأمريكية في الفضاء. حذرت الصين الأمم المتحدة من مخاطر الاصطدام بين أقمار "ستارلينك" ومحطة الفضاء الصينية (Tiangong)، معتبرة أن الافتقار إلى التنظيم الدولي الفعال يزيد من احتمالية سباق تسلح في الفضاء الخارجي.²² وقد انتهجت على إثر ذلك مجموعة من الدول إجراءات مماثلة، ويمكن عرضها في :

1. الرد الصيني: مشروع "آلاف الأشعة" : أطلقت الصين مشروع "قوان وانغ" (Guowang) ومشروع "آلاف الأشعة" (Qianfan) لبناء كوكبات فضائية تضم أكثر من 15,000 قمر صناعي بحلول عام 2030. يهدف هذا التحرك إلى كسر الاحتكار الأمريكي للمدارات المنخفضة وتوفير بديل تقني للدول الحليفة للصين في آسيا وأفريقيا وأمريكا اللاتينية، مما يعزز مفهوم "السيادة التكنولوجية" الصينية وحماية الأمن القومي الفضائي.²³

2. الرد الروسي : تبنت روسيا استراتيجية مضادة لإزالة تهديدات الفضاء الخارجي خصوصاً تحييد منظومة ستارلينك خلال النزاعات الإقليمية، بحيث تركز هذه الاستراتيجية على مسارين: الأول تقني عسكري عبر تطوير واختبار أسلحة مضادة للأقمار الصناعية (ASAT) قادرة على التدمير الفيزيائي أو التعطيل الحركي، والثاني سيبراني يعتمد على تقنيات التشويش الإلكتروني والهجمات البرمجية لتعطيل إشارات المنظومة فوق مناطق العمليات. يمثل هذا الرد الروسي تحولاً في العقيدة العسكرية نحو "حرب الفضاء"؛ حيث لم تعد السيطرة على الأرض كافية دون تحييد "السيادة الرقمية الفضائية" للخصوم والفاعلين من غير الدول.²⁴

3. الاتحاد الأوروبي: تعد مبادرة "IRIS2" (البنية التحتية للمرونة والترابط والأمن عبر الأقمار الاصطناعية) الرد الاستراتيجي للاتحاد الأوروبي الرامي إلى كسر الهيمنة التقنية لشركات الفضاء الأمريكية مثل "ستارلينك". يهدف هذا المشروع إلى بناء منظومة اتصالات فضائية توفر إنترنت عالي السرعة وخدمات اتصالات مشفرة وآمنة للجهات الحكومية والعسكرية، مما يضمن الاستقلال الاستراتيجي لأوروبا في حالات الأزمات. ومن خلال الاعتماد على تقنيات التشفير الكمي وشبكات المدار الأرضي المنخفض (LEO)، تسعى هذه المبادرة إلى تأمين البنية التحتية الحيوية بعيداً عن تقلبات السياسات الخارجية والتبعية التكنولوجية للفاعلين من غير الدول، وهو ما يعيد صياغة مفهوم السيادة الرقمية في الفضاء الخارجي كضرورة أمنية وقومية لا تقبل التجزئة.²⁵

4. الرد البرازيلي : تُعد الأزمة القانونية بين الفضاء البرازيلي ومنصتي (X) و (Starlink) نموذجاً حياً لتضارب المصالح بين الدولة الوطنية والشركات العابرة للقارات، حيث عكس قرار المحكمة العليا البرازيلية بفرض غرامات مالية باهظة وتجميد الأصول المصرفية لشركة "ستارلينك" تحولاً

استراتيجيا في آليات إجبار العمالقة التكنولوجيين على الامتثال للسيادة القانونية المحلية. وتبرز هذه المواجهة كسابقة قضائية تؤكد أن "الفضاء الرقمي" ليس منطقة معزولة عن القانون، بل هو خاضع لولاية القضاء الوطني، خاصة في القضايا المتعلقة بمكافحة التضليل الإعلامي وحماية المؤسسات الديمقراطية، مما يعيد الاعتبار لمفهوم "السيادة الرقمية" في مواجهة نفوذ الشركات غير المقيدة²⁶.

المحور الرابع : استراتيجيات حماية السيادة الوطنية في مواجهة التهديدات التكنولوجية

في ظل التحولات التقنية المتسارعة، لم يعد الأمن القومي يتحقق بالحظر الرقمي، بل عبر "السيادة المتكيفة". هذا المفهوم يسعى، كما تشير الدراسات الحديثة، إلى معالجة الخلل في موازين القوى العالمية حيث تفرض القوى المهيمنة نماذج حوكمة قد تسلب دول الجنوب قدرتها على الابتكار المستقل، مما يفرض على الدولة الحديثة ممارسة سيادتها من خلال حوكمة ذكية تستوعب هذه التناقضات الدولية²⁷. بناءً على العديد من الدراسات القانونية المعاصرة، تبرز ضرورة تبني مبدأ "الوقاية السيادية"، لإخضاع كافة مكونات البنية التحتية لبروتوكولات التدقيق والرقابة الوطنية، واعتبار أي وسيط تكنولوجي يرفض الخضوع للنظام العام التي تفرضه الدولة بمثابة تهديد محتمل لا يمكن دمج وقبوله ضمن كيانه ومنظومتها الشاملة.²⁸ وضمن هذا السياق يتطلب توفير مجموعة من الشروط يتمثل أهمها في :

1. بناء البدائل الوطنية : تشجيع الاستثمار التكنولوجي في البنية التحتية الوطنية لتقليل الاعتماد على المزودين الخارجيين.
2. تطوير الأطر التنظيمية : وذلك مواكبة للتجارب الدولية الرائدة، مثل قانون حماية البيانات الأوروبي (GDPR) ، والذي يعد كوسيلة فعالة لفرض شروط الدولة على الشركات العالمية في المجال الرقمي والتكنولوجي.
3. توطين البيانات عبر المخطات الأرضية (Gateways) : اشتراط مرور حركة البيانات عبر بوابات وطنية تسمح للدولة بممارسة حقها القانوني في الرقابة والأمن السيبراني وضمان تخزين البيانات محلياً.²⁹
4. الإفصاح الإلزامي بالخصائص والمواصفات التقنية : إلزام الشركات المزودة بتقديم تفاصيل دقيقة

حول طبقات الشبكة، مراكز التحكم، وسياسات جمع البيانات الوصفية قبل منح أي ترخيص.

30

5. صلاحية التعطيل الانتقائي: تضمين شروط في التراخيص تمنح الدولة الحق (عبر أوامر قضائية) في

طلب تعطيل أجهزة محددة أو في مناطق معينة لحماية الأمن القومي.³¹

إن السيادة الحقيقية في العصر الرقمي لا تُبنى فقط بالمنع والقوانين، بل بامتلاك القدرة على الابتكار والمنافسة. وعليه فإن الاستثمار في التعليم التقني المتقدم، وتطوير برمجيات محلية، وبناء تحالفات إقليمية في هذا المجال يمثل الضمانة الوحيدة للخروج من دائرة الخضوع والتبعية لإرادة الفواعل التكنولوجية العابرة للقارات، وتحقيق السيادة الرقمية المنشودة.

خاتمة :

تخلص هذه الدراسة من خلال تحليل حالة منظومة "ستارلينك" إلى أن السيادة الوطنية تشهد تحولات بنيوية في ظل تلاشي الثنائيات التقليدية بين الفضاء المحلي والفضاء العالمي، والقطاعين المدني والعسكري. لقد أضحت الفواعل التكنولوجية العابرة للحدود، وفي مقدمتها شركة (SpaceX)، تمارس أدوارا تتجاوز الطابع التجاري لتتحول إلى فواعل دولية وظيفية تعيد صياغة موازين القوى الأمنية والاستراتيجية دوليا .

إن ملامح النظام الدولي الناشئ تشير إلى حالة من "التعددية القطبية التكنولوجية"، حيث يمتد الصراع بين القوى الكبرى للهيمنة على التدفقات المعلوماتية والبيانات. وفي هذا السياق، تظل القدرة السيادية للدولة مرتبطة بمدى نجاحها في تأسيس حوكمة رقمية تفرض سيادة القانون الوطني، وتوطن القدرات التقنية الذاتية. وعلى هذا فإن منظومة "ستارلينك" لا تمثل سوى الجيل الأول من التهديدات التكنولوجية التي ستعيد تعريف الحدود القومية لتصبح حدودا رقمية وخوارزمية، مما يستوجب تبني فلسفة سياسية وإدارية جديدة تدرك أن مصادر القوة في القرن الحادي والعشرين باتت ترهّن بالسيطرة على الفضاء والمعلوماتية كأدوات موازية للقوة الصلبة التقليدية.

- ¹ - جمال بن مرار. مفهوم السيادة الوطنية في ظل العولمة. *مجلة مدارات سياسية*. سبتمبر، 2017، المجلد 1، 2، ص 21-24.
- ² - أمينة إيجر. السيادة الرقمية في العالم المعوم : التحديات والحلول الهيكلية. *مجلة الدراسات القانونية والسياسية*. جوان، 2024، المجلد 10، 02، ص 75.
- ³ - **Mauro, santaniello**. Attributes of Digital Sovereignty: A Conceptual Framework. *GEOPOLITICS*. 2026, Vol. 31, 2, pp. 789-793. <https://doi.org/10.1080/14650045.2025.2521548>.
- ⁴ - **سنوسي, علي**. السيادة الرقمية والاستقلال التكنولوجي بين تحديات الظروف الوطنية والدولية. *المجلة الجزائرية للحقوق والعلوم السياسية*. 2024, Vol. 9, 2, ص 250.
- ⁵ - **Gábor, Hulkó, János, Kálmán et András, Lapsánszky**. The politics of digital sovereignty and the European Union's legislation: navigating crises. *Frontiers in Political Science*. 05 fevrier 2025, Vol. 7, pp. 01-09. <https://doi.org/10.3389/fpos.2025.1548562>. p 3.
- ⁶ - **Hasan, Khaled**. Big Tech, Social Media, and American Foreign Policy: The Role of Elon Musk and Donald Trump in Shaping Global Politics. *International Journal of Social Science and Human Research*. 3 mars 2025, 08, pp. 1867-1872. <https://ijsshr.in/v8i3/Doc/64.pdf>. p1870.
- ⁷ - **Jiajie, Yan et yu, nanping**. The U.S. Starlink Project and Its Implications from the Perspective of International and National Security. *csis interpret*. [En ligne] 14 septembre 2024. [Citation : 12 mars 2026.] <https://interpret.csis.org/translations/the-u-s-starlink-project-and-its-implications-from-the-perspective-of-international-and-national-security/>.
- ⁸ - **regolith**. SpaceX set a \$800 billion valuation and is considering a 2026 IPO at \$1.5 trillion. *Regolith*. [En ligne] 17 decembre 2025. [Citation : 12 mars 2026.] <https://regolith.com/news/spacex-ipo-valuation-800b-70>.
- ⁹ - **Fahmi, Ramadan; Wijitrnanto, Fajar; Esthithama, Wanodya; Nurahman, Arip; Hamdani, Nizar Alam**. Starlink in the context of critical infrastructure protection and strategic consequences in cyber warfare. *Advanced Research in Intelligence and National Security*. 25 avril 2025, Vol. 2, 1, p169-170.

¹⁰ - **BOJOR, Laviniu; PETRACHE, Tudorică; CRISTESCU, Cristian.**

EMERGING TECHNOLOGIES IN CONFLICT: THE IMPACT OF STARLINK IN THE RUSSIA – UKRAINE WAR. *Revista Academiei Forțelor Terestre*. 2024, Vol. 114, 2, pp. 185–194.

https://www.armyacademy.ro/reviste/rev2_2024/Bojor_Petrache_Cristescu_RAFT_2_2024.pdf, pp89–91.

¹¹ - **الفرزلي, إيلي**. خديعة "ستارلينك" غداً في مجلس الوزراء: من ينقذ السيادة الرقمية والمال العام؟ <https://legal-agenda.com/>. [En ligne] 04 08 2025. [Citation : 15 03 2026.]

¹² - **International Telecommunication Union**. Radio Regulations 2020. *ITU-The UN Agency for Digital Technologies*. [En ligne] 1, 2020. [Citation : 18 avril 2026.] Articles 9&11. <https://www.itu.int/pub/R-REG-RR-2020>.

¹³ - **منال بوكورو**. النظام القانوني الدولي للفضاء الخارجي. *مجلة العلوم الإنسانية*. ديسمبر, 2018, المجلد 29, 4, ص393.

¹⁴ - **خلادي, سارة**. تحديات الأمن القومي في ظل عسكرة الفضاء الخارجي: القوى الفضائية الصاعدة والفاعلون من غير الدول. *مجلة الدراسات الاستراتيجية والعسكرية*. مارس, 2023, Vol. 5, 18, ص95.

¹⁵ - **الشريف, مصطفى كامل**. ستار شيلد: عندما يتحوّل الإنترنت الفضائي في ستار لنك إلى بنية استخباراتية *iTach*. *Danmark – Strategic Studies Center – ITSSC*. [En ligne] 13 01 2026. <https://itach.dk/starshield-starlink/>.

¹⁶ - المرجع نفسه.

¹⁷ - **بن مرار**, مرجع سابق, ص ص27-29.

¹⁸ - **amoore, louise**. *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others*. Durham : Duke University Press, 2020, pp27–29.

¹⁹ - **عبد الكريم أبو حاتم**. الآثار السلبية لمشروع "ستارلينك" على الأمن الوطني للدول. **يمني برس**. [متصل] 19 09 2024. <https://www.yemenipress.net/archives/351822> [تاريخ الاقتباس: 10 04 2026]

²⁰ - نفس المرجع السابق.

²¹ - **عادل, عبد الصادق**, **العلاقات الدولية والفضاء الإلكتروني: دراسة في النظرية والتطبيق**. القاهرة : المركز العربي لأبحاث الفضاء الإلكتروني, 2016, ص ص181-184.

²² - **satnews**. Beijing Warns UN of 'Safety and Security' Risks from Starlink

Expansion. *satnews*. [En ligne] 02 janvier 2026. [Citation : 10 avril 2026.]

<https://satnews.com/2026/01/02/beijing-warns-un-of-safety-and-security-risks-from-starlink-expansion/>.

²³ – **satnews**. Beijing Warns UN of ‘Safety and Security’ Risks from Starlink Expansion. *satnews*. [En ligne] 02 janvier 2026. [Citation : 10 avril 2026.] <https://satnews.com/2026/01/02/beijing-warns-un-of-safety-and-security-risks-from-starlink-expansion/>.

²⁴ – **العربي، محمد**. تسليح السماء : جيوسياسات الفضاء الخارجي [auteur du livre]. مصطفى ربيع. دراسات خاصة . أبوظبي : المستقبل للأبحاث والدراسات المتقدمة. 2022 , ص 7-16.

²⁵ – **المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات**. أمن أوروبا . الاستقلال الفضائي الأوروبي، وتداعياته على السياسات الدفاعية. *europarabct - ECCI*. [متصل] 28 جانفي, 2026. [تاريخ الاقتباس: 11 افريل, 2026]. <https://www.europarabct.com/?p=114247>

²⁶ – **Hillebrand, michael n**. The Sky’s Not the Limit: Navigating Starlink’s Impact on Global. *SMU Science and Technology Law Review*. 2025, Vol. 28, 1, pp. 364-378. <https://doi.org/10.25172/smustr.28.1.10.p367-368>.

²⁷ – **Mamo, Daniel Samuel**. International Organizations and Adaptive Sovereignty in 21st Century Global Governance: Possibilities and Challenges. *Science Futures*. 30 Janvier 2026, Vol. 2, 2, p 171.

²⁸ – الشريف، مرجع سابق.

²⁹ – **Aya Ali Kaj & co**. Digital Sovereignty and the Political Economy of Technology: A Comparative Study of U.S. and China Perspectives. *OxJournal*. [En ligne] 17 09 2025. [Citation : 12 avril 2026.] <https://www.oxjournal.org/digital-sovereignty-and-the-political-economy-of-technology/>.

³⁰ – الشريف، مرجع سابق.

³¹ – نفس المرجع السابق.