مؤسسة إنكي للدراسات والبحوث
ENKI FOUNDATION FOR STUDIES AND RESEARCH

ورقة تحليلية

ستارلينك والسيادة الوطنية في العراق

بين التحولات الاستراتيجية وتحديات الأمن السيبراني

أ.م.د. عباس فاضل علوان

سلسلة إصدارات شبكة إنكي للبحث العلمي

تموز / يوليو ٢٠٢٦

بغداد • إصدارات مؤسسة إنكي للدراسات والبحوث

منظومات الإنترنت الفضائي في المدار الأرضي المنخفض

خلاصة الورقة

- يكسر الإنترنت الفضائي — وعلى رأسه ستارلينك — احتكار الدولة لبوابات النفاذ الدولية، ويخلق بنية تحتية موازية تعمل فوق الغلاف الجوي بعيداً عن الرقابة الوطنية التقليدية.
- يضع تجاوز «نقاط الاختناق» الوطنية مبدأ السيادة الرقمية أمام اختبار حقيقي: هل هي سيادة على الأرض والتراب فقط، أم سيادة على البيانات التي تمثل «النفط الجديد» في القرن الحادي والعشرين؟
- يجعل الفراغ التشريعي — وفي مقدمته غياب قانون جرائم المعلوماتية — التعامل مع هذه التقنيات في منطقة رمادية قانونية، وينذر بنشوء «جزر اتصالات» مستقلة خارج رقابة الدولة ومحاسبتها.
- يخلق تجاوز البيانات لمركز عمليات الشبكة الوطني (NOC) حالة «عمى استراتيجي» للأجهزة الاستخبارية، ويعرّض القرار السيادي للابتزاز الرقمي وأدوات «الردع الهجين» في لحظات الأزمات.
- تقدم الورقة خارطة طريق من خمس توصيات: «دستور رقمي» شامل، بوابة وطنية موحدة، توطين البيانات، «بروتوكول طوارئ سيادي» (زر الإيقاف الوطني)، والاستثمار في «المراقب التقني العراقي».

المقدمة

يواجه مفهوم السيادة الوطنية في مطلع العقد الثالث من القرن الحادي والعشرين تحدياً وجودياً يعيد تعريف حدود الدولة من المنظور الجغرافي التقليدي إلى المنظور السيبراني الافتراضي، حيث لم تعد الدفاعات الوطنية تقتصر على حماية الأرض والسماء والمياه، بل امتدت لتشمل (المجال الرابع) وهو الفضاء الرقمي الذي بات المحرك الأساسي للاقتصادات والجيوش الحديثة.

أما بخصوص العراق، الذي يسعى جاهداً لاستعادة استقراره وبناء مؤسساته السيادية بعد عقود من الحروب، يمثل دخول تقنيات الإنترنت الفضائي، وتحديداً دخول (ستارلينك - Starlink) وهي عبارة عن خدمة إنترنت فضائي يتم تشغيلها بواسطة أقمار صناعية في مدار أرضي منخفض، وهي تابعة لشركة (سبيس إكس - SpaceX) الأمريكية المملوكة لإيلون ماسك، ويمثل دخول هذه الخدمة للعراق انعطافة استراتيجية كبرى تضع الدولة أمام معضلة الموازنة بين الحاجة التنموية للاتصال السريع وبين مقتضيات الأمن القومي المعقدة.

إن هذه التقنية العابرة للحدود تكسر احتكار الدولة لبوابات النفاذ الدولية وتخلق بنية تحتية موازية تعمل فوق الغلاف الجوي بعيداً عن الرقابة الوطنية التقليدية، مما يثير تساؤلات حادة حول من يملك السيطرة الفعلية على تدفق البيانات الوطنية. هذا البحث يسعى لتشريح أبعاد هذا التحول، مستكشفاً كيف يمكن للعراق أن يبني سيادته الرقمية في ظل فضاء ترددي مفتوح، وكيف يمكن تحويل التهديدات السيبرانية الناشئة عن هذه المنظومات إلى فرص لتعزيز الحصانة الوطنية وضمان استقلال القرار العراقي في عالم رقمي لا يعترف بالحدود المادية ويعظم سرعة المعلومات.

«سنحلل في هذه الورقة التقاطعات المعقدة بين التطور التقني والسيادة الوطنية، لنرسم ملامح مستقبل الأمن السيبراني العراقي في فضاء الاتصالات، وسنقدم توصيات استراتيجية لصانع القرار في العراق»

أولاً: الثورة التقنية لمنظومات المدار الأرضي المنخفض

تستند منظومة ستارلينك إلى مفهوم تقني ثوري يعتمد على آلاف الأقمار الصناعية الصغيرة التي تسبح في المدار الأرضي المنخفض (Low Earth Orbit - LEO) مما يمنحها ميزة تنافسية متقدمة تتمثل في تقليل زمن تأخير استجابة البيانات وتوفير سرعات كبيرة تتجاوز قدرات البنية التحتية الأرضية المتهالكة في كثير من المناطق العراقية.

يتميز هذا النموذج التقني بأنه لا يقدم مجرد إنترنت سريع، بل يقدم (بنية تحتية موازية) لا تتقيد بحدود الدول أو بوابات النفاذ الحكومية، حيث يتم الاتصال مباشرة بين الصحن اللاقط لدى المستخدم والقمر الصناعي، الخطورة التقنية هنا تكمن في أن هذه المنظومات تعتمد على تشفير مغلق من المصنع إلى المستخدم مما يعني أن تدفق المعلومات يتم عبر (طريق مفتوح) فضائي لا يمر عن طريق الدولة أو نقاط السيطرة الوطنية، وهو ما يجعل مفهوم (الحدود الرقمية) العراقي في حالة انكشاف تام. بالنسبة للعراق حيث عانت مشاريع الفايبر الضوئي من التلكؤ والفساد والضغوط الأمنية، تبرز هذه الصحون البيضاء كبديل مغرٍ للأفراد والشركات لكنها في جوهرها تمثل انسحاباً تقنياً للدولة من قدرتها على إدارة (عنق الزجاجة) المعلوماتي، مما يغير مفاهيم الحرب المعلوماتية من مواجهة مع أنظمة أرضية إلى مواجهة مع

ترددات عابرة للغلاف الجوي لا تملك الدولة مفاتيح فك تشفيرها أو حتى القدرة الفنية على حجبها عند الضرورة القصوى.

ثانياً: تآكل مفهوم «حارس البوابة» والسيادة الرقمية

لقد استندت السيادة الوطنية تاريخياً إلى قدرة الدولة على التحكم في ما يدخل ويخرج من أراضيها، وفي العصر الرقمي تجسد هذا في مفهوم (حارس البوابة) الذي يراقب بوابات النفاذ الدولية للبيانات، ومع دخول ستارلينك يواجه العراق تحدياً مباشراً لمبدأ السيادة الرقمية (Digital Sovereignty) الذي يعني حق الدولة في فرض قوانينها على الفضاء الرقمي داخل حدودها الوطنية. إن قدرة الأقمار الصناعية على بث الإنترنت مباشرة إلى محطات الاستقبال الأرضية تتجاوز (نقاط الاختناق) التي كانت تستخدمها الحكومات العراقية المتعاقبة للسيطرة على الفضاء المعلوماتي أو فلترته أو حتى قطعه في حالات الطوارئ الأمنية، هذا التحول يعني أن الدولة قد تفقد قدرتها السيادية على حماية المواطنين من الهجمات الرقمية الموجهة أو منع تدفق المحتوى الذي قد يهدد السلم المجتمعي، إذ تصبح البيانات الوطنية رهينة لسياسات شركة خاصة عابرة للقارات تعمل وفق قوانين دولتها الأم وليس وفق المعايير العراقية.

يضع هذا (الاحتلال الرقمي) الافتراضي السيادة الوطنية أمام اختبار حقيقي (هل هي سيادة على الأرض والتراب فقط أم سيادة على البيانات التي تمثل النفط الجديد في القرن الحادي والعشرين)، إن الفشل في تنظيم هذا الملف يعني أن السيادة العراقية ستظل مجرد نص دستوري بينما يتم التحكم في الفضاء المعلوماتي الفعلي من غرف عمليات خلف المحيطات، السيادة في عصر الفضاء لم تعد تعني المنع المادي بل تعني القدرة على التنظيم والحوكمة في بيئة تقنية مفتوحة لا تطلب إذناً من الحدود البرية، مما يستدعي من العراق إعادة تعريف

حدوده الوطنية لتشمل كل بتّ (Bit) من المعلومات يعبر أجواءه وضمان أن تظل الولاية القضائية للدولة فاعلة على هذه الشركات حتى وهي تسبح في الفضاء الخارجي، وهو أمر يتطلب توازناً دقيقاً بين الانفتاح التكنولوجي وحماية الأمن القومي.

«السيادة في عصر الفضاء لم تعد تعني المنع المادي، بل القدرة على التنظيم والحوكمة في بيئة تقنية مفتوحة لا تطلب إذناً من الحدود البرية»

ثالثاً: الفراغ التشريعي ومعضلة قانون جرائم المعلوماتية

يعاني المشهد الرقمي في العراق من فجوة تشريعية كبيرة تجعل التعامل مع تقنيات مثل ستارلينك يجري في منطقة رمادية قانونية، حيث يفتقر العراق حتى الآن إلى قانون جرائم المعلوماتية (Information Crimes Law) الذي يحدد المسؤوليات والعقوبات بوضوح ويواكب التطورات المتسارعة، التشريعات الحالية التي يعود بعضها إلى فترات ما قبل الثورة الرقمية تقف عاجزة أمام تعقيدات الفضاء الترددي والجرائم السيبرانية العابرة للحدود.

يؤدي دخول أي خدمة إنترنت عابرة للحدود في ظل هذا الفراغ إلى نشوء (جزر اتصالات) مستقلة قد تستخدمها واجهات سياسية أو اقتصادية أو حتى مليشيات إلكترونية بعيداً عن رقابة الدولة ومحاسبتها.

الأزمة الحقيقية ليست في التقنية ذاتها بل في غياب إطار تنظيمي يلزم الشركات الأجنبية بالامتثال للمعايير الوطنية للخصوصية والأمن القومي، كما أن الاستراتيجية الوطنية للأمن الوطني العراقي (2025–2030) تؤكد في نصوصها على ضرورة السيادة على البيانات، لكن بدون نص قانوني ملزم يحدد شروط الترخيص والامتثال تبقى هذه التوجهات مجرد نصوص فاقدة لقيمتها لفقدانها الإلزام القانوني أمام الشركات الكبرى العابرة للحدود، إن العراق بحاجة ماسة إلى (دستور رقمي) يوحد الرؤية بين هيئة الإعلام والاتصالات ووزارة الاتصالات، ويضمن أن تكون التكنولوجيا أداة للتمكين لا ثغرة للهروب من طائلة القانون، مع ضرورة أن تتضمن التراخيص الممنوحة لهذه الشركات بنوداً تسمح للدولة بالوصول القانوني للبيانات في حالات الجرائم الكبرى والتهديدات الإرهابية، لضمان ألا يتحول التشفير الفضائي إلى غطاء للأنشطة المزعزعة للاستقرار.

رابعاً: التهديدات الأمنية وحالة «العمى الاستراتيجي» للأجهزة الاستخبارية

من منظور الأمن السيبراني (Cyber Security) يثير الاعتماد على شبكات فضائية خارجية مخاوف جدية تتعلق بالتجسس والمراقبة الخارجية، حيث إن تجاوز البيانات لمركز عمليات الشبكة الوطني (National Network Operation Center - NOC) يخلق ما يمكن وصفه بـ(العمى الاستراتيجي) للأجهزة الاستخبارية الوطنية، في هذه الحالة تصبح حركة البيانات الحساسة للمؤسسات الحيوية (مثل قطاعات الطاقة والمال والأمن) خارج نطاق الرؤية والقدرة على الرصد المبكر للهجمات أو الانحرافات المعلوماتية، هذا الانكشاف قد تستغله جهات خارجية لشن عمليات تخريبية صامتة أو نقل معلومات استراتيجية دون أثر رقمي يمكن تتبعه محلياً مما يحول سماء العراق إلى (ممر سيادي غير مرخص) للبيانات الحساسة.

كما أن التجربة في مناطق النزاع الدولية أثبتت أن الإنترنت الفضائي يمكن أن يتحول إلى أداة لـ(الردع الهجين - Hybrid Deterrence) حيث يمكن للجهة المزودة قطع الخدمة عن مناطق معينة أو تقييدها لدواعٍ جيوسياسية، مما يجعل القرار السيادي العراقي عرضة للابتزاز الرقمي في لحظات الأزمات الكبرى، إن حماية السيادة المعلوماتية تتطلب ليس فقط تأمين الأجهزة بل ضمان أن تظل مسارات البيانات تحت (الولاية القضائية العراقية) من خلال محطات أرضية تخضع للرقابة التقنية الوطنية، وبدون ذلك يظل العراق في حالة (انكشاف استراتيجي) يجعل من أمنه القومي رهينة لقرارات تتخذ في غرف عمليات تجارية بعيدة كل البعد عن المصلحة الوطنية العراقية، وهو ما يهدد قدرة الدولة على الاستجابة للأزمات الأمنية والسيبرانية بفاعلية واستقلالية تامة.

خامساً: التبعات الاقتصادية وتحدي توطين البيانات الوطنية

دخول ستارلينك للسوق العراقية يحمل في طياته تهديداً للشركات المحلية ومزودي الخدمة الوطنيين من خلال ما يعرف بـ(التسعير الافتراسي - Predatory Pricing) أو الهيمنة التقنية المطلقة، مما قد يؤدي إلى انهيار قطاع الاتصالات الأرضي الذي استثمر فيه العراق مليارات الدولارات لتطوير الشبكة الوطنية.

إضافة إلى أن استراتيجية الأمن السيبراني يجب أن تركز على مفهوم توطين البيانات (Data Localization) أي إلزام أي شركة أجنبية بتخزين بيانات المستخدمين العراقيين داخل مراكز بيانات سيادية تخضع للقانون العراقي وتقع داخل الحدود الجغرافية للبلاد، بدون هذا التوطين تتحول بيانات المواطنين من معاملات مصرفية واتصالات شخصية وسجلات حكومية إلى أصول رقمية تدار في خوادم خارج الحدود، مما يضعف السيادة الاقتصادية ويجعل الدولة العراقية

تابعة لمنظومات اقتصادية رقمية لا تملك السيطرة عليها أو القدرة على استثمار قيمتها المضافة، إن بناء اقتصاد سيبراني مستقل يتطلب تكامل الإنترنت الفضائي مع الشبكة الوطنية للألياف الضوئية، ليكون مكملاً لها في المناطق النائية والوعرة وليس بديلاً عنها يقوض ما تبقى من بنية تحتية وطنية ملموسة، وهو ما يستدعي فرض ضرائب سيادية ورسوم تنظيمية تضمن عدالة المنافسة وتوجه الأرباح نحو تطوير الكفاءات الرقمية العراقية بدلاً من خروجها بالكامل كرأس مال تقني للخارج.

سادساً: الدروس الإقليمية وتحدي «زر الإيقاف الوطني» في الأزمات

لقد تعاملت دول الجوار، مثل إيران مع ستارلينك كتهديد مباشر لسيادتها وتحدٍّ لمنظومتها الأمنية ولجأت إلى استراتيجيات تقنية وقانونية صارمة شملت التشويش المستهدف والشكاوى الدولية لدى الاتحاد الدولي للاتصالات لانتزاع اعتراف بعدم شرعية التشغيل غير المرخص فوق أراضيها، الدرس المستفاد للعراق هو أن مفهوم زر الإيقاف الوطني (National Kill Switch) الذي تملكه الدول عادة في الأزمات الكبرى لتقييد الاتصالات المهددة للأمن يختفي تماماً مع الإنترنت الفضائي غير المنظم الذي يعتمد على كوكبة أقمار لا تخضع للتحكم الأرضي المحلي، فإذا ما تعرضت البلاد لتهديد أمني كبير أو محاولة انقلابية تعتمد على التنسيق الرقمي المشفر عبر الفضاء لن تملك الحكومة القدرة الفنية على تقييد تلك الاتصالات التي لا تمر عبر بواباتها الوطنية مما يجعل الفضاء الرقمي ساحة مفتوحة للفوضى أو التدخلات الخارجية التي لا يمكن صدها بالوسائل التقليدية.

هذا التحدي يفرض على صانع القرار العراقي صياغة اتفاقيات تعاقدية تقنية صارمة تضمن للدولة حداً أدنى من السيطرة في ظروف الطوارئ، مع الاعتراف بأن السيادة في عصر الفضاء

تتطلب ذكاءً تنظيمياً قادراً على فرض الشروط السيادية قبل التشغيل الفعلي للخدمة، لضمان بقاء (مفتاح السيادة) في يد السلطات الوطنية العراقية وليس في يد مدير تنفيذي لشركة أجنبية.

الخاتمة

تأسيساً على التحليل الذي استعرضته هذه الورقة التحليلية تبرز حقيقة مفصلية مفادها أن السيادة الوطنية في العصر الرقمي لم تعد تقاس بمدى القدرة على حماية الحدود الجغرافية المادية، بل بمدى القدرة على حوكمة الفضاء الترددي الوطني والسيطرة على تدفقات البيانات.

إن دخول منظومات المدار الأرضي المنخفض وعلى رأسها ستارلينك يضع الدولة العراقية أمام اختبار (الاستقلال التقني) حيث لم يعد كافياً أن تملك الدولة الأرض وإنما بات من الضروري امتلاك (الولاية القضائية والتقنية) على كل بتّ (Bit) معلومات يعبر الأجواء السيادية، إن التحول من مفهوم الدولة الحارسة للبوابات المادية إلى مفهوم (الدولة الرقمية المنظمة) يتطلب تبني رؤية استراتيجية شاملة تفضي إلى (ويستفاليا رقمية - Digital Westphalia) حيث ترسم حدود المسؤولية والولاية فوق السحاب كما هي على الأرض، هذا الانتقال ليس مجرد خيار تكنولوجي إنما هو ضرورة وجودية لضمان ألا يتحول الانفتاح الرقمي إلى (انكشاف استراتيجي) يجعل من أمن البلاد القومي رهينة لخوارزميات أجنبية أو قرارات تجارية عابرة للقارات.

خارطة طريق

التوصيات الاستراتيجية لصانع القرار العراقي

وبناءً على مقتضيات الضرورة العلمية واحتياجات الأمن القومي العراقي، نضع أمام صانع القرار خارطة طريق استراتيجية تتجسد في التوصيات الآتية:

١ **سد الفراغ التشريعي بـ«دستور رقمي» شامل:** يجب على مجلس النواب العراقي الإسراع بتشريع (قانون جرائم المعلوماتية - Information Crimes Law) وقانون حماية البيانات الشخصية، على أن يتضمنا نصوصاً صريحة تنظم عمل مزودي الإنترنت الفضائي، ولا ينبغي التعامل مع ستارلينك كخدمة تجارية عابرة بل كبنية تحتية استراتيجية تتطلب تراخيص خاصة تفرض على الشركة الأم الامتثال للمعايير الوطنية للخصوصية والأمن القومي، مع منح الدولة الحق القانوني في الوصول إلى البيانات في حالات التهديدات الإرهابية وفق أوامر قضائية عراقية.

٢ **فرض «البوابة الوطنية الموحدة» شرطاً تشغيلياً:** تتمثل التوصية التقنية الأهم في إلزام أي مزود للإنترنت الفضائي بإنشاء محطات أرضية (Gateways) داخل الأراضي العراقية لضمان مرور حركة البيانات عبر مركز عمليات الشبكة الوطني (National Network Operation Center - NOC)، إن هذا الإجراء هو الكفيل الوحيد لإنهاء حالة (العمى الاستراتيجي) التي تعاني منها الأجهزة الاستخبارية إذا ما دخلت ستارلينك بدون سيطرة الدولة، حيث يتيح لها مراقبة التهديدات السيبرانية ومنع تحول الفضاء العراقي إلى ممر غير مرخص للبيانات الحساسة أو الأنشطة المزعزعة للاستقرار.

٣ **توطين البيانات واستعادة السيادة الاقتصادية:** على صانع القرار فرض سياسة توطين البيانات (Data Localization) التي تلزم الشركات الأجنبية بتخزين سجلات المستخدمين العراقيين ومعاملاتهم داخل مراكز بيانات سيادية مقامة على أرض العراق وتخضع للقانون المحلي، هذا الإجراء يحمي (النفط الجديد) للعراق من الاستغلال الخارجي ويمنع تحول

الاقتصاد الرقمي الوطني إلى مجرد تابع للمنظومات العالمية، كما يضمن حماية خصوصية المواطنين من سياسات المراقبة العابرة للحدود.

٤ **تفعيل «بروتوكول الطوارئ السيادي — زر الإيقاف الوطني»:** من الضروري تضمين الاتفاقيات التعاقدية مع شركات الأقمار الصناعية بنوداً تقنية تتيح للحكومة العراقية تفعيل مفهوم زر الإيقاف الوطني (National Kill Switch) في ظروف الأزمات الأمنية القصوى، إن السيادة في عصر الفضاء تعني امتلاك (مفتاح التحكم) في اللحظات الحرجة لضمان عدم استخدام الشبكات الفضائية كأداة للردع الهجين من قبل أطراف خارجية أو كقنوات اتصال مشفرة للجماعات الخارجة عن القانون بعيداً عن سيطرة الدولة.

٥ **الاستثمار في «المراقب التقني العراقي»:** توصي الورقة بضرورة تحويل العراق من (مستهلك تقني) سلبي إلى (مراقب فني) نشط عبر دعم المراكز البحثية والكوادر الشبابية المتخصصة في هندسة الفضاء والأمن السيبراني، إن السيادة الرقمية لن تتحقق بالمنع الذي بات مستحيلاً تقنياً، بل بالذكاء التنظيمي والقدرة على فحص الأنظمة والبرمجيات الداخلة للبلاد وتطوير خوارزميات وطنية قادرة على التفاعل مع شبكات المدار المنخفض بفاعلية وندية.

«الرهان الحقيقي للعراق لا يكمن في رفض التكنولوجيا مخافة الاختراق، بل في صياغة عقد سيادي جديد يبقي «مفتاح السيادة» بيد الدولة حصراً»

إن الرهان الحقيقي للعراق اليوم لا يكمن في رفض التكنولوجيا مخافة الاختراق، بل في صياغة عقد سيادي جديد يضمن تدفق المعلومات كشريان للتنمية مع بقاء (مفتاح السيادة) بيد الدولة حصراً، إن الطريق نحو الأمن السيبراني يبدأ من الوعي التقني الصارم ويمر عبر الحوكمة الذكية وينتهي ببناء حصانة وطنية شاملة تجعل من سماء العراق الرقمية درعاً حصيناً يحمي استقلال القرار الوطني في عالم لا يرحم الضعفاء تكنولوجياً.

مؤسسة إنكي للدراسات والبحوث — بغداد
سلسلة إصدارات شبكة إنكي للبحث العلمي
ENKI FOUNDATION FOR STUDIES AND RESEARCH