مجلة جامعة بني وليد للعلوم الإنسانية والتطبيقية
Bani Waleed University Journal of Humanities and Applied Sciences
تصدر عن– جامعة بني وليد – ليبيا
Website:https://jhas-bwu.com/index.php/bwjhas/index
ISSN 3005-3900 الصفحات (423 -442) المجلد الحادي عشر – العدد الخامس – 2026

The Impact of Cybersecurity and Artificial Intelligence on Reshaping Political Development and Sovereignty: A Foresight Study in International and Regional Relations

Khaled Omran Abdel Salam Al-Quraitli *
PhD Researcher at the School of Regional and International Strategic Studies, Libyan Academy, Tripoli, Libya
algritlt@gmail.com

أثر الأمن السيبراني والذكاء الاصطناعي في إعادة تشكيل التنمية السياسية والسيادة: دراسة استشرافية في العلاقات الدولية والإقليمية

خالد عمران عبد السلام القريتلى*
باحث دكتوراه بمدرسة الدراسات الاستراتيجية الإقليمية والدولية، الأكاديمية الليبية ، طرابلس ، ليبيا

Received: 14-06-2026	Accepted: 26-07-2026	Published: 04-08-2026
Copyright: © 2026 by the authors. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

الملخص:
تهدف هذه الدراسة إلى التقييم والاستشراف التحليلي لأثر المتغيرات التكنولوجية الحديثة ممثلة في الأمن السيبراني، وتطبيقات الذكاء الاصطناعي على إعادة تشكيل مقومات التنمية السياسية، ومفاهيم السيادة الوطنية في إطار العلاقات الدولية والإقليمية، وتستند الدراسة إلى أدوات التحليل الاستراتيجي، واقتراب بناء السيناريوهات لمعالجة الفجوة التخطيطية، والمفهومية الناجمة عن عجز الأطر النظرية التقليدية عن استيعاب حروب الجيل الخامس، والصراعات غير المتماثلة، والتهديدات الهجينة.
تسعى الدراسة إلى التأصيل الاستراتيجي لإدراج "السيادة السيبرانية، وحوكمة الذكاء الاصطناعي" كـ "مُحدد استراتيجي، وأزمة تنموية مستحدثة" تتفاعل مع الأزمات الكلاسيكية (الشرعية، الهوية، والمشاركة)، وتتوقع التقديرات الاستراتيجية للدراسة أن التفوق في معمارية الذكاء الاصطناعي، والأمن السيبراني أصبح يمثل ركيزة جوهرية في القوة الوطنية الشاملة، وأن الحفاظ على التنمية السياسية، والاستقرار الإقليمي يتطلب الانتقال من الأطر الأمنية الدفاعية التقليدية إلى صياغة استراتيجيات ردع سيبراني، وتكيف استراتيجي مرن.

الكلمات الدالة: التنمية السياسية ، الأمن السيبراني ، الذكاء الاصطناعي ، العلاقات الدولية والإقليمية.

Abstract
This study aims to assess and provide an analytical forecast of the impact of modern technological variables, specifically cybersecurity and artificial intelligence applications, on reshaping the foundations of political development and the concepts of national sovereignty within the framework of international and regional relations. The study employs strategic analysis tools and a scenario-building approach to address the planning and conceptual gaps

resulting from the inability of traditional theoretical frameworks to encompass fifth-generation warfare, asymmetric conflicts, and hybrid threats.
The study seeks to establish a strategic foundation for including "cyber sovereignty and AI governance" as a "strategic determinant and an emerging developmental crisis" that interacts with classic crises (legitimacy, identity, and participation). The study's strategic assessments anticipate that superiority in AI architecture and cybersecurity has become a fundamental pillar of comprehensive national power, and that maintaining political development and regional stability requires a shift from traditional defensive security frameworks to the formulation of cyber deterrence strategies and flexible strategic adaptation.

Keywords: Political development, cybersecurity, artificial intelligence, international and regional relations.

المقدمة:

تفرض التحولات الجيو-سياسية والتكنولوجية المتسارعة في البيئة الدولية والإقليمية المعاصرة واقعاً جديداً لإدارة القوة والتنمية؛ فلم تعد مرتكزات السيادة الوطنية والتنمية السياسية للدول تُقاس حصراً بالمعايير التقليدية كالموقع الجغرافي أو حجم الجيوش النظامية، بل أصبحت القدرات التكنولوجية والمنظومات السيبرانية جزءاً لا يتجزأ من عناصر القوة الوطنية الشاملة، وتُشكل التنمية السياسية في العلاقات الدولية والإقليمية صمام الأمان لتحقيق الاستقرار المؤسسي؛ حيث تُعزز قدرة الدولة على التكيف مع الأزمات والتحديات الإقليمية والدولية.

فإن صعود تطبيقات الذكاء الاصطناعي وتعاظم تهديدات الفضاء السيبراني عابر الحدود أديا إلى نقل موازين الصراع من الفضاء الفيزيائي إلى الفضاء الرقمي، مما فرض تحديات استراتيجية تمس جوهر "السيادة الوطنية" واستقلال القرار التنموي والسياسي. لقد أدى التوظيف الاستراتيجي للهجمات السيبرانية وعمليات التضليل الإعلامي الموجهة بواسطة الخوارزميات الذكية والتزييف العميق إلى تعميق أزمات التنمية السياسية الكلاسيكية؛ فلم تعد أزمة الشرعية السياسية أو أزمة الهوية الوطنية بمعزل عن الاختراقات السيبرانية عابرة الحدود. وبناءً عليه، تتناول هذه الدراسة أثر الأمن السيبراني والذكاء الاصطناعي في إعادة تشكيل التنمية السياسية والسيادة من منظور استراتيجي استشرافي في العلاقات الدولية والإقليمية.

إشكالية الدراسة تتمثل الإشكالية في وجود فجوة تخطيطية ومفهومية بين الأطر السياسية والسيادية الكلاسيكية في العلاقات الدولية وبين طبيعة التهديدات الجيو سياسية الناشئة عن الاستخدام الاستراتيجي للأمن السيبراني وتطبيقات الذكاء الاصطناعي. يترتب على هذه الفجوة انكشاف استراتيجي للدول وتفاقم أزمات التنمية السياسية، مما يُتيح للفاعلين من غير الدول والقوى الإقليمية والمنافسين الدوليين التأثير في الإرادة السياسية الوطنية واختراق السيادة دون الحاجة للمواجهة العسكرية التقليدية.

تساؤلات الدراسة كيف تؤثر التوظيفات الاستراتيجية للأمن السيبراني وتطبيقات الذكاء الاصطناعي في إعادة تشكيل مقومات التنمية السياسية والسيادة الوطنية؟ وما السيناريوهات الاستشرافية لمستقبل الاستقرار الإقليمي؟

التساؤلات الفرعية:

أ. ما المرتكزات النظرية والمنهجية لتفسير التحولات الرقمية في العلاقات الدولية؟ وكيف تُقاس القدرات التكنولوجية كعنصر في القوة الوطنية الشاملة؟

ب. كيف يُعيد الفضاء السيبراني صياغة مفاهيم السيادة الوطنية؟ وما دور الفاعلين من غير الدول والشركات التكنولوجية الكبرى في تقويض هذه السيادة؟

جـ. ما أثر الحروب غير المتماثلة وحروب الجيل الخامس على حماية البنى التحتية التنموية للدولة؟ وكيف تُحدد الفجوة الرقمية الاستراتيجية أنماط التبعية التكنولوجية وتؤثر على الاستقلال السياسي في التنافس الإقليمي والدولي؟

د. ما طبيعة الانعكاسات المباشرة للتضليل الإعلامي الموجه والتزييف العميق على أزمات الشرعية

والمشاركة والهوية الوطنية؟
هـ. ما الآليات المطلوبة لبناء عقيدة ردع سيبراني مرنة وصياغة استراتيجيات الأمن القومي الشامل لحماية التنمية السياسية؟
و. ما السيناريوهات المستقبلية للسيادة والتنمية الإقليمية بحلول عام 2035؟ وما خريطة الطريق الاستراتيجية للتعامل معها؟

أهمية الدراسة

الأهمية النظرية: الإسهام في تطوير أدبيات العلوم السياسية والعلاقات الدولية الإقليمية من خلال تقديم تأصيل نظري يربط بين نيو-واقعية العلاقات الدولية ومفهوم "القوة السيبرانية"، مع صياغة إطار تحليلي موسع ينظر للتكنولوجيا المتقدمة كعنصر محوري في معادلة التنمية السياسية والسيادة.
الأهمية التطبيقية الاستراتيجية: تزويد مراكز الفكر وصناع القرار ومؤسسات التخطيط القومي برؤية استشرافية شاملة تعتمد على تقييم المخاطر وبناء السيناريوهات، مما يُساعد في وضع استراتيجيات للردع السيبراني وحماية البُنى التحتية الحساسة والعملية السياسية التنموية.

أهداف الدراسة

أ. تحديد معالم التغير في البيئة الاستراتيجية الدولية والإقليمية المترتب على دخول الذكاء الاصطناعي والأمن السيبراني كأدوات للصراع والنفوذ.
ب. تفكيك أبعاد أزمات التنمية السياسية (الشرعية، الهوية، التغلغل، المشاركة) واختبار مدى تأثرها بالتهديدات الرقمية الحديثة.
جـ. التأصيل الاستراتيجي لمفهوم "السيادة الرقمية/السيبرانية" كشرط أساسي لتحقيق التنمية المستدامة والاستقلال السياسي في مواجهة هيمنة الشركات عابرة القارات.
د. تحليل تأثير الفجوة الرقمية الاستراتيجية بين الدول على موازين القوى الإقليمية والاستقلال التنموي.
هـ. صياغة سيناريوهات استشرافية مستقبلية وتقديم "خارطة طريق استراتيجية" للتعامل مع أزمات التنمية السياسية والسيبرانية حتى عام (2035).

فرضيات الدراسة توجد علاقة ذات دلالة استراتيجية بين امتلاك وتوظيف القدرات السيبرانية والذكاء الاصطناعي وبين القدرة على حماية السيادة الوطنية وتحقيق التنمية السياسية والمحافظة على الاستقرار الإقليمي.
الفرضية الأولى: غياب استراتيجيات الردع السيبراني والحوكمة الأخلاقية للذكاء الاصطناعي يؤدي إلى تفاقم أزمة الشرعية والمشاركة السياسية بسبب الحروب غير المتماثلة والتضليل الإعلامي.
الفرضية الثانية: اتساع الفجوة الرقمية الاستراتيجية يُعمق حالة التبعية التكنولوجية للدول النامية ويُضعف هامش المناورة السيادية في القرارات التنموية.
الفرضية الثالثة: بناء القدرات الذاتية والسيادة الرقمية الوطنية يُعزز من الاستقرار المؤسسي ويمكّن الدولة من التكيف مع سيناريوهات التهديد الإقليمي.

منهج الدراسة تعتمد الدراسة على:
المنهج التحليلي الاستراتيجي: لتحليل البيئة الأمنية والتنموية، ومعرفة أثر أدوات القوة التكنولوجية على مدخلات ومخرجات النظام السياسي والإقليمي.
اقتراب التخطيط القائم على السيناريوهات: لرسم المعالم المستقبلية واستشراف التحولات في التنمية والسيادة بحلول عام 2035.
اقتراب الردع والاستراتيجية غير المتماثلة: لفهم كيفية استخدام الفاعلين—كباراً وصغاراً—للثغرات التقنية لتحقيق أهداف جيوسياسية وتنموية.

المحور الأول: التنمية السياسية كمرتكز أساسي لبناء الاستقرار السياسي والإقليمي

تُمثل العلاقة بين التنمية السياسية والاستقرار السياسي والإقليمي إحدى أكثر القضايا محورية في أدبيات

العلاقات الدولية والدراسات الإقليمية المعاصرة. فبينما كان النظر التقليدي للعلوم السياسية يحصر التنمية السياسية في أبعادها الداخلية (كإعادة هيكلة المؤسسات وبناء الشرعية)، أثبتت التحولات الجيو-سياسية المتسارعة أن التنمية السياسية تشكل حجر الزاوية للمناعة الوطنية وقدرة الدولة على الصمود أمام التهديدات عابرة الحدود، وبالتالي ضمان الاستقرار في المحيط الإقليمي والدولي (بدران، 2011، ص 104).

أولاً: التنمية السياسية وبناء الاستقرار السياسي الداخلي يتحقق الاستقرار السياسي الداخلي عندما تمتلك الدولة القدرة على إدارة صراعاتها الاجتماعية والسياسية عبر أطر مؤسسية سلمية دون اللجوء إلى العنف أو الانكفاء نحو الفوضى. وتتداخل التنمية السياسية مع هذا الاستقرار من خلال ثلاثة متطلبات رئيسية:

شرعية المؤسسات وكفاءتها الوظيفية: إن التنمية السياسية الناجحة تعمل على نقل السلطة من أطرها الشخصية أو القبيلية أو النفعية الضيقة إلى مؤسسات عقلانية تتمتع بالشرعية والإنجاز (كيلاني، 2015، ص 152). إن قدرة الدولة على الاستجابة لمطالب مواطنيها بفاعلية يُقلل من احتمالات الانقسام العمودي ويُعزز من قيم المواطنة والاندماج الوطني (نافعة، 2016، ص 88).

إدارة التحديات والأزمات الهيكلية: تُمثل معالجة "أزمات التنمية السياسية" (كأزمة الهوية، والشرعية، والمشاركة، والتوزيع) الشرط الأساسي لمنع تحول التنافس السياسي إلى صراع صفري (محمد، 2018، ص 91). فعندما تُخفق التنمية السياسية في استيعاب التعبئة الاجتماعية المتزايدة، تنشأ حالة من الانحلال والاهتزاز المؤسسي تفتح الباب أمام الاضطرابات الداخلية (هنتنغتون، 1993، ص 73).

ترسيخ سيادة القانون وبناء الكتلة الوطنية: لا يُمكن التفكير في استقرار طويل الأمد دون استقلال السلطة القضائية وخضوع الجميع لحكم القانون؛ إذ يُساهم ذلك في خلق بيئة سياسية متوقعة ومستقرة تُقلل من فرص الاستقطاب الحاد وتضمن الاستمرارية الهيكلية لمؤسسات الدولة (رشاد، 2009، ص 210).

ثانياً: الانعكاسات الإقليمية للتنمية السياسية (من التنمية الوطنية إلى الأمن الإقليمي (في إطار العلاقات الدولية والإقليمية، لم تعد التنمية السياسية شأناً داخلياً محضاً، بل أصبحت متغيراً حاسماً في تشكيل معادلات التوازن والأمن الإقليمي عبر المستويات التالية:

ظاهرة "انتقال العدوى" والهشاشة عابرة الحدود: تؤكد أدبيات العلاقات الدولية الإقليمية أن تعثر التنمية السياسية ودخول الدولة في حالة من الفشل المؤسسي أو أزمات الشرعية يُحولها إلى "دولة هشّة" أو فراغ سياسي يُصادر استقرار جوارها الجغرافي (هلال ومجيب، 2017، ص 34). وصعود الجماعات المسلحة الفاعلة من غير الدول هي نتائج مباشرة للفشل التنموي السياسي الداخلي الذي يفيض على الإقليم (مركز الإمارات للدراسات والبحوث الاستراتيجية، 2019، ص 45).

بناء المناعة ضد التدخلات الخارجية: تُعد التنمية السياسية والمأسسة الصلبة الخط الدفاعي الأول للحفاظ على السيادة الوطنية؛ إذ إن الأنظمة السياسية التي تفتقر إلى الشرعية التنموية والمشاركة الشعبية تكون أكثر عرضة للاختراق الجيو-سياسي والارتهان للمشاريع الإقليمية والمحاور الدولية المتصارعة (البشري، 2005، ص 118). وعلى العكس، فإن التماسك التنموي الداخلي يمنح القرار السياسي الوطني استقلالية وقوة تفاوضية أمام القوى الإقليمية والدولية (حرب، 2014، ص 205).

الاعتماد المتبادل والسلام الإقليمي: تُشير دراسات التفاعلات الإقليمية إلى أن الدول التي تقطع شوطاً في التنمية السياسية وتأطير مؤسساتها تكون أكثر قدرة على الانخراط في ترتيبات أمنية واقتصادية إقليمية مستدامة (المعهد العربي للبحوث والدراسات الاستراتيجية، 2022، ص 112). إذ إن المؤسسات السياسية الكفء والرشيدة تمتلك رؤية استراتيجية قائمة على التعاون والاعتماد المتبادل بدلاً من افتعال الصراعات الخارجية لتصدير الأزمات الداخلية (المعهد العربي للبحوث والدراسات الاستراتيجية، 2022، ص 118).

ثالثاً: التنمية السياسية والاستقرار: رؤية استشرافية للبيئة الإقليمية المعاصرة في ظل التحولات التكنولوجية والجيو-سياسية المتسارعة، أصبح مفهوم الاستقرار السياسي والإقليمي ينطوي على أبعاد مستحدثة تتجاوز القوة العسكرية التقليدية:

السيادة الرقمية والمناعة الاستراتيجية: أصبحت التنمية السياسية المعاصرة تُقاس بمدى تطوير السلطة السياسية لقدراتها التنظيمية والتشريعية لمواجهة التهديدات السيبرانية والحروب الهجينة، وحماية البيئة

المعرفية والمعلوماتية للمجتمع من التضليل الخارجي (مركز الإمارات للدراسات والبحوث الاستراتيجية، 2019أ، ص 62).
المرونة المؤسسية في إدارة الأزمات الإقليمية: تتطلب البيئة الإقليمية المعقدة وجود مؤسسات سياسية تتمتع بـ "المرونة الاستراتيجية"، وهي القدرة على امتصاص الصدمات الإقليمية الخارجية (كالأزمات الاقتصادية، والتغيرات المناخية، والتنافس بين القوى الكبرى) دون أن يتفكك النظام السياسي الداخلي (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 140).
رابعاً: السيادة الرقمية والفضاء السيبراني (الحدود الجديدة للقوة (مَثَّلَ ظهور "الفضاء السيبراني" التحول الأكثر راديكالية واختباراً لمفهوم السيادة الوطنية في تاريخ العلاقات الدولية؛ حيث أوجد بيئة افتراضية لامركزية بلا حدود جغرافية، وتتسم بغياب الشفافية وصعوبة إسناد الهجمات (مركز الإمارات للدراسات والبحوث الاستراتيجية، 2019أ، ص 18).
طبيعة الفضاء السيبراني وتحدي الإقليمية: يتعارض الفضاء السيبراني في بنيته مع المنطق الوستفالي؛ فالشبكات السيبرانية والخوادم وتدفق البيانات تتجاوز الحدود الوطنية وتلتف على سيطرة الدولة الإقليمية (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 52). وقد أدى هذا الواقع إلى ظهور مفهوم "السيادة السيبرانية" أو "السيادة الرقمية"، والتي تُعرف بأنها قدرة الدولة واستقلاليتها في السيطرة على بنيتها التحتية الرقمية وبياناتها الوطنية والأنشطة السيبرانية داخل إقليمها (مركز الإمارات للدراسات والبحوث الاستراتيجية، 2019أ، ص 24).
صراع الأطر التنظيمية للسيادة الرقمية في العلاقات الدولية: ينقسم العالم اليوم حول إعادة تعريف السيادة في العصر الرقمي إلى اتجاهين رئيسيين:
الاتجاه السيادي المغلق (النموذج السيبراني الوستفالي): تقوده قوى كبرى تركز على فرض السيطرة الحكومية الكاملة على الإنترنت والبيانات، وتعتبر أي هجوم أو تحكم خارجي في الفضاء السيبراني الخاضع لها خرقاً لسيادتها الوطنية (المعهد العربي للبحوث والدراسات الاستراتيجية، 2022، ص 164).
الاتجاه المفتوح (النموذج الليبرالي العابر للحدود): يرى أن الإنترنت يجب أن يظل مساحة عالمية مفتوحة تديرها أطراف متعددة دون فرض سيطرة حصرية ومطلقة للدول (حرب، 2001، ص 278).
السيادة السيبرانية كمكون للسيادة القومية: لم تعد السيادة تقتصر على حماية الحدود البرية والبحرية والجوية، بل أصبحت "السيادة الجوية-السيبرانية" و"أمن البيانات الوطنية" مرتكزاً حيوياً لحماية مراكز القرار والأنظمة المالية والبنى التحتية الحيوية (كالطاقة والاتصالات) من الاختراقات الخارجية التي قد تُعطل أجهزة الدولة دون الحاجة لإطلاق رصاصة واحدة (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 78).

المحور الثاني: التكنولوجيا كعنصر مستحدث في معادلة القوة الوطنية الشاملة

أولاً: التكنولوجيا وإعادة تشكيل معادلة القوة الشاملة شهدت العقود الأخيرة تحولاً إبستمولوجياً أخرج المكون التكنولوجي من جلباب المقاربات التقليدية، ليتحول إلى مجال مستقل للقوة والسيادة:
الانتقال من "القوة الصلبة" إلى "القوة الرقمية والمستحدثة": لم تعد القوة العسكرية تُقاس بحجم الجيوش أو عدد الدبابات فقط، بل أصبحت تُقاس بمدى الذكاء الاصطناعي المُدمج وقدرات الحرب السيبرانية والاستطلاعات الفضائية وأنظمة القيادة والسيطرة الرقمية عابرة الحدود (مركز الإمارات للدراسات والبحوث الاستراتيجية، 2019أ، ص 55).
السيادة التكنولوجية والارتهان الجيو-سياسي: تؤكد أدبيات العلاقات الدولية المعاصرة أن العجز التكنولوجي يتسبب في ثغرة أمنية وسيادية عميقة؛ حيث تضطر الدول المفتقرة للبنية التكنولوجية إلى الارتهان للقوى المصنعة في تزويدها بالبنى التحتية، مما يجعل قرارها السياسي والأمني مكشوفاً ومخترقاً إقليمياً ودولياً (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 104).
ثانياً: مؤشرات قياس القوة السيبرانية والتكنولوجية وتأثيرها على وزن الدولة الإقليمية لم يعد تقييم وزن الدولة

ومكانتها في العلاقات الدولية والإقليمية يقتصر على المؤشرات التقليدية لحجم القوات المسلحة أو الناتج المحلي الإجمالي، بل فرضت الثورة الرقمية إدماج "القوة السيبرانية والتكنولوجية" بوصفها معياراً تحليلياً جديداً لقياس قدرة الدولة على التأثير والردع وصيانة قرارها السياسي والسيادي (بدران، 2011، ص 230). وتتوزع هذه القوة بين مؤشرات قياس كمية ونوعية تحدد درجة التفوق أو الهشاشة الجيو-سياسية للدولة.

ثالثاً: مؤشرات قياس القوة السيبرانية والتكنولوجية للدولة تعتمد المدارس الاستراتيجية والدراسات الدولية على مصفوفة مؤشرات مركبة لقياس القوة التكنولوجية والسيبرانية الشاملة للدولة، وتتنزل أهم هذه المؤشرات في المحاور التالية:

المؤشرات الهيكلية والبنية التحتية الرقمية: تقيس درجة امتلاك الدولة للبنى التحتية المتقدمة وسيادتها عليها؛ وتتضمن كفاءة شبكات الاتصالات وسرعتها، ومدى الاعتماد على مراكز البيانات الوطنية، وانتشار شبكات النطاق العريض، ونسبة النفاذ الرقمي للمؤسسات والمواطنين، بالإضافة إلى مستوى استقلالية الدولة في إدارة البنية التحتية للاتصالات بعيداً عن التحكم الخارجي (مركز الإمارات للدراسات والبحوث الاستراتيجية، 2019أ، ص 72).

المؤشرات الدفاعية والهجومية السيبرانية:

القدرة الدفاعية: وتتمثل في جدارات الحماية الوطنية للبنى التحتية الحيوية (كالشبكات المالية، محطات الطاقة، والمرافق العسكرية) ضد الاختراقات الخارجية، ووجود فرق وطنية متخصصة للاستجابة للطوارئ السيبرانية (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 122).

القدرة الهجومية والاستطلاع السيبراني: وتتعلق بامتلاك الدولة للقدرات التقنية والبرمجية لشن هجمات مضادة، وتخريب القدرات الرقمية للخصوم، وجمع المعلومات الاستخباراتية السيبرانية لإرباك البيئة الأمنية للطرف الآخر (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 128).

مؤشرات الابتكار والقدرة المعرفية الذاتية: وتُقاس بحجم الإنفاق الحكومي والخاص على البحث والتطوير التكنولوجي كنسبة من الناتج المحلي، وعدد البراءات والابتكارات المسجلة، ومدى توفر الكوادر البشرية الوطنية المؤهلة في مجالات الذكاء الاصطناعي وعلم البيانات والتشفير والأنظمة السيبرانية المتقدمة (رشاد، 2009، ص 185).

المؤشرات التنظيمية والتشريعية: وتشمل وجود استراتيجيات وطنية شاملة للأمن السيبراني، وأطر قانونية لحماية البيانات السيادية، وتنظيم الفضاء الرقمي بما يحفظ الحقوق الوطنية ويمنع اختراق الجبهة الداخلية (نافعة، 2016، ص 160).

رابعاً: تأثير القوة السيبرانية على وزن الدولة ومكانتها الإقليمية يُترجم امتلاك الدولة لمؤشرات مرتفعة في القوة السيبرانية والتكنولوجية إلى أدوات نفوذ جيوسياسي تُعزز من مكانتها في محيطها الإقليمي والدولي عبر الأبعاد التالية:

تعزيز ميزان الردع المتبادل: تسمح القدرات السيبرانية الهجومية والدفاعية للدولة بإيجاد "ردع غير متماثل"؛ حيث تستطيع الدول المتوسطة أو الصغيرة تقنياً تحييد التفوق العسكري التقليدي لقوى إقليمية أكبر منها عبر تهديد بنائها التحتية الحيوية واقتصادها الرقمي، مما يُعيد تشكيل موازين القوة الإقليمية (المعهد العربي للبحوث والدراسات الاستراتيجية، 2022، ص 182).

صيانة القرار السيادي والمناعة الاستراتيجية: تضمن القوة السيبرانية المستقلة حماية مراكز صنع القرار السياسي والعسكري من التجسس والتضليل الخارجي، وتُقلل من فرص ارتهان الدولة للتطبيقات والتقنيات المستوردة التي قد تُستخدم كـ "أبواب خلفية" للضغط السياسي والتجسس الاستراتيجي (مركز الإمارات للدراسات والبحوث الاستراتيجية، 2019أ، ص 89).

القيادة الاقتصادية والفاعلية الإقليمية: تتحول الدولة المسلحة تكنولوجياً إلى مركز ثقل إقليمي يُصدر الخدمات الرقمية والأمن السيبراني والحلول التقنية للدول المجاورة، مما يُكسبها أوراق ضغط وتأثير سياسي واقتصادي ناعم يُترجم إلى ثقل استراتيجي في التفاعلات الإقليمية (مركز الإمارات للدراسات والبحوث الاستراتيجية، 2019أ، ص 94).

المحور الثالث: الهجمات السيبرانية واستهداف البنى التحتية الحيوية

تُعرف البنى التحتية الحيوية بأنها القطاعات والأصول المادية والافتراضية التي يُؤدي شلُّها أو تدميرها إلى آثار كارثية على الأمن القومي والاقتصاد والصحة العامة للدولة (رشاد، 2009، ص 248).

أولاً: أنماط التهديد السيبراني الموجه للقطاعات الحيوية

تتعدد أنماط التهديدات السيبرانية الموجهة للقطاعات الحيوية وتتنزل في المحاور التالية:

استهداف منظومات التحكم الصناعي :تُعد منظومات "المراقبة والتحكم واكتساب البيانات (SCADA) " النواة التشغيلية لمحطات التوليد ومفاعلات الطاقة وشبكات المياه والمناطق النفطية. تُستهدف هذه المنظومات ببرمجيات خبيثة عالية التعقيد مثل الفيروسات الموجهة كـ Stuxnet وأحفادها للسيطرة على التشغيل المادي المباشر وإحداث أضرار مادية هائلة (المعهد العربي للبحوث والدراسات الاستراتيجية، 2022، ص 235).

شل القطاع المالي والأنظمة البنكية :تستهدف الهجمات السيبرانية شبكات التبادل المالي بين البنوك والمنصات الرقمية للبنوك المركزية عبر هجمات حجب الخدمة الموزعة (DDoS) أو برمجيات الفداء (Ransomware)، مما يؤدي إلى تجميد المعاملات التجارية وتدمير الاستقرار الاقتصادي القومي (مركز الإمارات للدراسات والبحوث الاستراتيجية، 2019أ، ص 145).

اختراق أنظمة الملاحة وسلاسل الإمداد :يتعمد مهاجمو الجيل الخامس زرع ثغرات برمجية في التحديثات البرمجية للموردين المعتمدين، مما يسمح باختراق شبكات الطيران والموانئ وشبكات الإمداد اللوجستي للمؤسسات العسكرية والدفاعية بشكل موازٍ (مركز الإمارات للدراسات والبحوث الاستراتيجية، 2019أ، ص 150).

ثانياً: التداعيات الجيو-سياسية والأمنية لاستراتيجيات استهداف البنى الحيوية

تخلق الهجمات السيبرانية على البنى الحيوية واقعاً أمنياً جديداً يُعيد صياغة موازين القوة الإقليمية والدولية:

تآكل خطوط الردع التقليدية :إن امتلاك الدولة لترسانة عسكرية تقليدية ضخمة لا يضمن حماية شبكات الكهرباء أو المستشفيات من هجوم سيبراني خاطف، مما يُجبر الدول على إنفاق أجزاء مضاعفة من ميزانياتها الدفاعية على الأمن السيبراني الوقائي (نافعة، 2016، ص 205).

تهديد التماسك المجتمعي والأمن الداخلي :ينتج عن انقطاع الخدمات الأساسية (الكهرباء، الإنترنت، الاتصالات، والخدمات المصرفية) حالة من الهلع الشعبي والفوضى، مما يُضعف الجبهة الداخلية للسيادة الوطنية ويُضغط على صانع القرار السيادي للقبول بإملاءات إقليمية أو دولية (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 182).

المحور الرابع: التداعيات الجيو-سياسية للفجوة الرقمية وحروب المعلومات

أبعاد الفجوة الرقمية بين الدول المتقدمة والدول النامية وآثارها الجيو-سياسية

تُعد "الفجوة الرقمية" إحدى أبرز صور اللاعدالة في العلاقات الدولية المعاصرة؛ إذ لم تقتصر آثارها على التفاوت الاقتصادي والاجتماعي، بل امتدت لتُشكل "لا تماثلاً هيكلياً" في توزيع القوة والنفوذ الاستراتيجي بين شمال عالمي متقدم يمتلك ناصية التقنية والمعرفة، وجنوب نامٍ يواجه مخاطر الارتهان والتبعية. ومع تحول الفضاء الرقمي والبيانات إلى محركات أساسية للنمو والأمن القومي، تحولت الفجوة الرقمية من مجرد تفاوت تقني إلى متغير جيوسياسي يُعيد إنتاج علاقات الهيمنة والاستتباع الإقليمي والدولي (بدران، 2011، ص 302).

أولاً: أبعاد ومظاهر الفجوة الرقمية الدولية

تتأسس الفجوة الرقمية بين الدول المتقدمة والدول النامية على مصفوفة من الأبعاد الهيكلية المركبة، ويمكن إيجاز أهمها في المحاور التالية:

فجوة البنية التحتية والوصول التكنولوجي :تتمثل في الاحتكار الشديد للدول المتقدمة لشبكات الاتصالات الأساسية ومراكز البيانات الفائقة، والسيادة على كابلات الألياف الضوئية العابرة للمحيطات ومحطات الحوسبة السحابية؛ في حين تعاني أغلب الدول النامية من ضعف التغطية وتهالك شبكات الاتصال والارتهان

للبنى التحتية الأجنبية لإدارة تدفقاتها المعلوماتية (مركز الإمارات للدراسات والبحوث الاستراتيجية، 2019أ، ص 220).

الفجوة المعرفية والابتكارية :تتجلى في التفاوت الهائل في حجم الإنفاق الحكومي والخاص على البحث والتطوير، ونسب امتلاك براءات الاختراع في المجالات المستقبلية (الذكاء الاصطناعي والتشفير). هذا التفاوت يمنح القوى المتقدمة القدرة على احتكار صناعة الخوارزميات وتحديد المعايير التقنية الدولية، بينما تكتفي الدول النامية بدور المستهلك والمسجل للحلول الجاهزة (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 260).

فجوة السيادة على البيانات والمعالجة :في اقتصاد المعرفة الرقمي، أصبحت "البيانات" هي النفط الجديد. تكمن الفجوة في قيام الشركات التكنولوجية الكبرى العابرة للقارات (المستقرة في الدول المتقدمة) باستخلاص البيانات الضخمة للمجتمعات النامية وتخزينها ومعالجتها خارج حدودها الوطنية، مما يحرم الدول النامية من قيمتها الاقتصادية ويجعل أمنها القومي مكشوفاً استخباراتياً (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 268).

ثانياً: الآثار الجيو-سياسية للفجوة الرقمية

يُترجم التفاوت الرقمي والتكنولوجي بين المجموعتين إلى تداعيات جيوسياسية تؤثر عميقاً في استقرار النظام الدولي والإقليمي وتوازناته:

تكريس التبعية الاستراتيجية و"الاستعمار الرقمي :"تؤدي الفجوة الرقمية إلى وقوع الدول النامية في مصيدة الارتهان التكنولوجي؛ حيث تضطر للاعتصام بالحلول والأنظمة البرمجية والدفاعية المزودة من القوى المتقدمة. هذا الارتهان يُتيح للدول الموردة فرض إملاءات سياسية واستخدام التقنية كأداة ضغط استراتيجي وابتزاز سياسي في الأزمات (المعهد العربي للبحوث والدراسات الاستراتيجية، 2022، ص 295).

توسع الفجوة الأمنية وضبط قدرات الردع :تجد الدول النامية نفسها عاجزة عن مجاراة التفوق السيبراني والعسكري للقوى الكبرى المعتمدة على الذكاء الاصطناعي والأنظمة المستقلة؛ مما يمنح القوى المتقدمة قدرة على اختراق الجبهات الداخلية للبلدان النامية وشل مرافقها الحيوية دون تكلفة عسكرية، وهو ما يُكسر مبدأ "التوازن الدفاعي" الإقليمي (رشاد، 2009، ص 315).

اتساع هامش التهميش في أطر الحوكمة الدولية :تستأثر الدول المتقدمة بصياغة القواعد والاتفاقيات الدولية المنظمة للفضاء الرقمي والأمن السيبراني، وتفرض معايير تخدم أهدافها الأمنية والاقتصادية، مما يُقصي مصالح الدول النامية ويُحجم قدرتها على صيانة أمنها وسيادتها الرقمية في المحافل الدولية (نافعة، 2016، ص 265).

المحور الخامس: التبعية الرقمية وأثرها على تقييد الاستقلال السياسي والقرارات التنموية

تُشكل "التبعية الرقمية" الامتداد المعاصر للتبعية الهيكلية التقليدية؛ حيث أدى الارتهان التقني المتزايد للتقنيات والأنظمة والتطبيقات الأجنبية إلى تحول الفضاء الرقمي إلى أداة ضغط استراتيجي غير متماثلة. ولم تعد التبعية تقتصر على استيراد الأجهزة والحلول البرمجية، بل تعدتها لتسلب الدولة المستهلكة قدرتها على إدارة مرافقها السيادية ومبادراتها التنموية بمعزل عن تأثير القوى والشركات التكنولوجية العابرة للحدود.

أولاً: مظاهر وآليات التبعية الرقمية في النظام الدولي

تتحقق التبعية الرقمية عبر شبكة معقدة من الآليات التقنية والاقتصادية التي تقيد قدرة الدول النامية والمتوسطة على الحركة الاستراتيجية:

الاحتكارية البرمجية والبنى التحتية المغلقة :تعتمد غالبية الدول على أنظمة تشغيل وحوسبة سحابية وخوارزميات معالجة مُحتكرة من عدد محدود من الشركات الاحتكارية التابعة للقوى العظمى. هذا الاحتكار يمنح القوى المُصنّعة قدرة التحكم في الوصول للبيانات، وفرض شروط الاستخدام، أو حتى إيقاف الخدمات الرقمية جزئياً أو كلياً في حالات الأزمات الجيو-سياسية (مركز الإمارات للدراسات والبحوث الاستراتيجية،

2019أ، ص 235).
الاستنزاف المالي والتدفق العكسي لرأس المال المعرفي :تؤدي التبعية الرقمية إلى نزيف مستمر للموارد المالية للدول النامية عبر دفع رسوم التراخيص والخدمات السحابية وشراء التجهيزات التقنية؛ بدلاً من توجيه تلك الموارد لبناء قدرات نووية أو تحفيز الابتكار المحلي، مما يُعزز الفجوة الاقتصادية بين الدول المبتكرة والمستوردة (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 275).
حرمان الدولة من "السيادة على البيانات :"تُخرج التبعية الرقمية عمليات تخزين البيانات الوطنية وتطويرها خارج الحدود السيادية، مما يُعرض بيئة القرار الداخلي لتنقيب البيانات والتجسس الرقمي، ويحرم الدولة من توظيف بياناتها الوطنية في بناء استراتيجيات تنموية مستقلة (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 282).
ثانياً: أثر التبعية الرقمية على تقييد الاستقلال السياسي
تتعدى التبعية الرقمية البعد التقني لتؤثر مباشرة على جوهر السيادة الوطنية واستقلالية القرار السياسي للدولة:
تحييد أوراق الضغط واستنزاف القرار السيادي :عندما تعتمد الدولة في أمنها ومرافقها المالية وشبكات إدارتها على التقنيات الأجنبية، تصبح خيارات سياستها الخارجية مكشوفة ومقيدة؛ إذ تُلوّح القوى الموردة للتقنية بسلاح "العقوبات الرقمية" أو إلغاء التراخيص التشغيلية في حال اتخاذ الدولة مواقف سياسية تعارض مصالح القوى المبتكرة (المعهد العربي للبحوث والدراسات الاستراتيجية، 2022، ص 310).
اختراق بيئة صنع القرار والتأثير على الجبهة الداخلية :تتيح التبعية الرقمية للفاعلين الخارجيين الوصول السلس إلى اتجاهات الرأي العام، وتوظيف المنصات الرقمية في شن حملات التضليل وإدارة العمليات النفسية، مما يُربك التماسك المجتمعي ويضغط على صانع القرار السياسي الداخلي للانصياع للضغوط الإقليمية والدولية (رشاد، 2009، ص 330).
ثالثاً: انعكاسات التبعية الرقمية على تعطيل القرارات التنموية تفرض التبعية الرقمية قيوداً مباشرة على مسارات التنمية المستدامة والتحديث المؤسسي في الدول المستوردة للتكنولوجيا عبر النماذج التالية:
فرض النماذج التنموية غير الملائمة: تضطر الدول التابعة لرسم خططها التنموية بناءً على المعايير والحلول التقنية الجاهزة والمستوردة، والتي قد لا تتوافق مع الأولويات الوطنية أو البيئة الاجتماعية والاقتصادية للبلد النامي، مما يخلق تشوهات تنموية ومشاريع غير مستدامة (نافعة، 2016، ص 280).
إعاقة التحول نحو "اقتصاد المعرفة": تُكرّس التبعية الرقمية نمط الاستهلاك السلبي للتقنية بدلاً من إنتاجها، مما يُضعف قطاعات البحث العلمي والابتكار المحلي، ويُؤدي إلى ظاهرة "هجرة العقول التقنية" نتيجة غياب البيئة الحاضنة للابتكار التكنولوجي المستقل (مركز الإمارات للدراسات والبحوث الاستراتيجية، 2019أ، ص 250).

المحور السادس: الذكاء الاصطناعي، التزييف العميق، والتحولات في مفهوم السيادة والشرعية السياسية
توظيف الذكاء الاصطناعي والتزييف العميق في ضرب الشرعية والتحول في المشاركة الرقمية أحدث التطور التسارعي في نماذج الذكاء الاصطناعي التوليدي والخوارزميات الشبكية نقلة نوعية في أدوات المشاركة والتأثير السياسي. وقد برزت تقنية "التزييف العميق" وأساليب "الهندسة الاجتماعية" بوصفها من أبرز الآليات المؤثرة في الحرب المعلوماتية والعمليات النفسية؛ نظراً لقدرتها على اصطناع المحتوى وتوجيه السلوك الجمعي، مما خلق تحولاً راديكالياً في البيئة الرقمية أثر مباشرة في ركائز "الشرعية السياسية" واستقرار بيئة المشاركة السياسية الرقمية (بدران، 2011، ص 335).
أولاً: الآليات التقنية للتزييف العميق وتأثيرها على ضرب الثقة في المؤسسات والشرعية السياسية تعتمد تقنية التزييف العميق على الشبكات العصبية الاصطناعية، وتحديداً "شبكات الخصومة التوليدية"، التي تقوم على تدريب نموذج برمجي محدد بواسطة نموذج خوارزمي آخر لتحسين جودة التزوير الرقمي للملامح والصوت والأفعال حتى تصل إلى درجة يصعب على الإدراك البشرى أو أدوات الفحص التقليدية تمييزها (مركز الإمارات للدراسات والبحوث الاستراتيجية، 2019أ، ص 265).

وتتجسد الآثار الاستراتيجية لهذه التقنية في تقويض الشرعية السياسية عبر المحاور التالية:
تآكل مفهوم "الثقة العامة": تعتمد الشرعية السياسية لأي نظام حكم على وجود حد أدنى من الثقة المتبادلة بين المواطن ومؤسسات الدولة. يُؤدي انتشار مقاطع التزييف العميق المفبركة للقيادات إلى خلق حالة من "العجز الإدراكي" لدى الرأي العام، حيث يصبح المواطن غير قادر على التمييز بين حقيقة القرارات السياسية والروايات المفبركة، مما يضرب الثقة في الخطاب الرسمي للدولة (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 295).
ظاهرة "دفاع الكاذب": تُوفر تكنولوجيا التزييف العميق منفذاً للنخب أو الفاعلين السياسيين للتنصل من التزاماتهم؛ إذ يمكن لأي مسؤول يتورط في خطابات أو قضايا فساد مثبتة بالصوت والصورة أن يدعي أن تلك التسجيلات ليست سوى "تزييف عميق" تم توليده بواسطة الذكاء الاصطناعي، مما يفقد أدلة المساءلة السياسية قيمتها، ويفرغ مبادئ الشفافية والشرعية من مضمونها (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 302).
استهداف النزاهة الانتخابية والعمليات الديمقراطية: تُستخدم مقاطع التزييف العميق كأدوات استباقية للتأثير في توجهات الناخبين خلال المواسم الانتخابية، عبر تسريب تسجيلات مفبركة لمرشحين في أوقات حرجة قبل الصمت الانتخابي، مما يحرم الطرف المستهدف من حق الرد الفعال، ويؤثر بشكل مباشر على نتائج التنافس السياسي ونزاهته (المعهد العربي للبحوث والدراسات الاستراتيجية، 2022، ص 330).
ثانياً: الهندسة الاجتماعية والمشاركة السياسية الرقمية: الفرص وتحديات الاختراق تُعبر "المشاركة السياسية الرقمية" عن التحول النفعي والتشاركي الذي أتاحته شبكات الاتصال والذكاء الاصطناعي للمواطنين للتعبير عن تطلعاتهم والتأثير في صنع القرار. غير أن هذا الفضاء المفتوح أصبح بدوره مسرحاً لتقنيات "الهندسة الاجتماعية" الموجهة، والتي تستهدف التلاعب بالنفسية الجمعية واختراق السلوك السياسي للمجتمعات (رشاد، 2009، ص 355).
يمكن تفكيك جدلية الفرص وتحديات الاختراق في المحاور التالية:
فرص المشاركة السياسية الرقمية وتعزيز التنمية السياسية:
توسيع الفضاء العام الرقمي: أتاحت التقنيات الرقمية منصات مفتوحة لتفعيل المشاركة السياسية غير التقليدية، وخفض تكلفة التعبير عن الرأي، وتسهيل الرقابة المجتمعية على الأداء الحكومي، وتشكيل جماعات الضغط الرقمية (نافعة، 2016، ص 310).
دعم التحول الديمقراطي والتفاعل المباشر: تُمكّن أدوات الذكاء الاصطناعي المؤسسات السياسية من تحليل الاتجاهات العامة وتطلعات المواطنين، مما يُعزز كفاءة القرارات التنموية، ويُقرب المسافة بين صانع القرار والشارع (نافعة، 2016، ص 318).
تحديات الاختراق عبر الهندسة الاجتماعية وتوجيه السلوك:
التلاعب النفسي والتوجيه الخوارزمي: تعتمد الهندسة الاجتماعية في الفضاء الرقمي على تحليل البيانات الضخمة لبناء أطياف وصور نفسية للمواطنين، واستغلال خوارزميات التوصية لتغذيتهم بمعلومات ومحتوى موجه يزرع الانقسام السياسي، أو يُوجه سلوكهم الانتخابي نحو غايات محددة دون إدراك منهم (مركز الإمارات للدراسات والبحوث الاستراتيجية، 2019أ، ص 285).
اختراق التماسك المجتمعي وصناعة الهلع: تُوظف أدوات التضليل الرقمي والهندسة الاجتماعية في شن عمليات نفسية تستهدف الفئات الهشة مجتمعياً، عبر إذكاء النزاعات الطائفية أو العرقية، وتحويل المشاركة الرقمية من أداة للبناء والتنمية السياسية إلى وسيلة للاستقطاب الراديكالي وإرباك الاستقرار الداخلي (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 312).
اختراق المؤسسات والبيئات السيادية: تُستغل أساليب الهندسة الاجتماعية (كالتصيد الاحتيالي المتقدم والموجه) لاختراق الحسابات السيادية للقيادات السياسية والأمنية، واستخدامها لنشر معلومات كاذبة أو تسريب بيانات استراتيجية تُخل بالأمن القومي (المعهد العربي للبحوث والدراسات الاستراتيجية، 2022، ص 342).

المحور السابع: أزمات الهوية والسيادة الرقمية

تُشكل التحولات الرقمية المتسارعة تحدياً بنيوياً لركائز الدولة الوطنية المعاصرة؛ إذ لم يعد التأثير التكنولوجي مقتصراً على الأبعاد العسكرية والأمنية، بل امتد ليمسّ النواة الصلبة لبناء الدولة والمتمثلة في "الهوية الوطنية" و"السيادة الوطنية". وفي ظل عولمة الاتصال وهيبة الفاعلين غير الحكوميين العابرين للحدود، برزت أزمات حادة تتعلق بتآكل الروافد الثقافية الوطنية واختراق التماسك المجتمعي، بالتوازي مع انكشاف الدولة أمام نفوذ الشركات التكنولوجية الاحتكارية التي باتت تُنافس أجهزة الحكم على ممارسة السلطة التنظيمية والرقابية (بدران، 2011، ص 348).

أولاً: اختراق الهوية الوطنية عبر المنصات الرقمية الدولية وتأثيرها على التماسك المجتمعي تُعبر الهوية الوطنية عن منظومة القيم واللغة والتاريخ والرموز الثقافية الموحدة للمجتمع، والتي تُشكل الحاضنة الأساسية للشرعية السياسية والتجانس الاجتماعي. ومع غلبة المنصات الرقمية الدولية وخوارزميات التواصل الاجتماعي العابرة للحدود، تعرضت الهويات الوطنية لأشكال غير متماثلة من التدفقات الثقافية والموجهات السلوكية التي فرضت تحديات مباشرة على الاستقرار الداخلي (مركز الإمارات للدراسات والبحوث الاستراتيجية، 2019أ، ص 295).

وتتجلى أبعاد هذا الاختراق وتأثيراته في المحاور التالية:

الاستعمار الثقافي واغتراب الوعي الجمعي: تعتمد خوارزميات التدفق والمعالجة في المنصات الرقمية الكبرى على معايير وقيم غربية وأحادية الثقافة، مما يُؤدي إلى تهميش الخصوصيات الثقافية واللغوية للدول النامية والمجتمعات المحافظة. ينجم عن هذا التدفق المستمر حالة من "الاغتراب الثقافي" لدى الفئات الشبابية، وتفكك الروابط مع الرموز الوطنية والتاريخية لبلدانهم لصالح قيم معولمة هجينة (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 320).

الاستقطاب الخوارزمي وتعميق الانقسامات المجتمعية: تستهدف خوارزميات التوصية والانخراط في المنصات الدولية تعظيم التفاعل الرقمي عبر تضخيم المحتوى الأكثر إثارة للجدل والمشاعر العاطفية الحادة. يُؤدي هذا النمط التشغيلي إلى تحفيز خطابات الكراهية، وتعزيز التعصب المذهبي والعرقي والمناطقي، وتحويل الفضاء الرقمي الداخلي من ساحة للتواصل إلى مصدر دائم لتفتيت التماسك المجتمعي (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 328).

تفكيك الرواية الوطنية الجامعة: فقدت المؤسسات الوطنية الرسمية (كالإعلام والتعليم) احتكارها لصياغة الرواية الوطنية وتوجيه الرأي العام، وقد سمحت المنصات الرقمية الأجنبية للفاعلين الخارجيين ولجماعات الضغط بضخ روايات بديلة ومضللة تُشكك في التاريخ الوطني والرموز السياسية، مما يحرم الدولة من مظلة التجانس التي تُسهم في استقرار نظامها السياسي وتنميتها الاجتماعية (المعهد العربي للبحوث والدراسات الاستراتيجية، 2022، ص 355).

ثانياً: أزمة السيادة السيبرانية في ظل هيمنة الشركات الاحتكارية والتكتلات التكنولوجية الكبرى تُعبر "السيادة السيبرانية" عن حق الدولة الحصري والسيادي في فرض سلطتها القانونية والرقابية والتنظيمية على البنى التحتية المعلوماتية والبيانات الوطنية والأنشطة الرقمية الواقعة ضمن حدودها، أو المتعلقة بمواطنيها. غير أن هذا المفهوم يواجه أزمة حقيقية نتيجة صعود التكتلات التكنولوجية الكبرى وتداخل صلاحياتها مع أدوار الدولة التقليدية.

تتجسد مظاهر أزمة السيادة الرقمية في المحاور التالية:

خصخصة السلطة السيادية ونشأة "السيادة التكنولوجية الموازية": تحولت شركات التكنولوجيا الكبرى (مثل شركات الحوسبة السحابية، وأنظمة التشغيل، ومنصات التواصل) إلى "فاعلين جيوسياسيين" يملكون صلاحيات تشريعية وتنظيمية موازية للسلطة السيادية للدول. فهي من يحدد قواعد النشر، ويعطل الحسابات الرئاسية والسيادية، ويُحيد التغطيات السياسية بناءً على شروط الخدمة الخاصة بها، ودون خضوع للقوانين الوطنية أو المحاكم الوطنية للدول المستضيفة (نافعة، 2016، ص 330).

الاحتكار الخوارزمي والتحكم في البيانات الضخمة: تعتمد التكتلات التكنولوجية الكبرى على سياسات جمع

واحتكار البيانات السلوكية والشخصية لمواطني الدول، وتخزينها في مراكز بيانات خارجية يخضع الوصول إليها للتشريعات الوطنية لدول المقر للشركات (غالباً الدول المتقدمة). هذا الاحتكار يُجرّد الدولة من سيادتها الوطنية على أصولها الرقمية، ويُعرض قرارها التنموي والأمني للتحكم والاستغلال الأجنبي (مركز الإمارات للدراسات والبحوث الاستراتيجية، 2019أ، ص 310).

العقوبات الرقمية وتسييس البنى التحتية: أظهرت الأزمات الجيو-سياسية المعاصرة تحول التكتلات التكنولوجية والشركات الاحتكارية إلى أداة تنفيذية للسياسات الخارجية للقوى العظمى؛ حيث أدى قطع الخدمات السحابية، وإلغاء تراخيص البرمجيات، وحظر منصات الدفع الرقمي عن دول أو مؤسسات معينة، إلى شلّ أجهزتها الإدارية والتنموية، مما يُبرز حجم الهشاشة الاستراتيجية الناجمة عن غياب "السيادة التكنولوجية الوطنية" (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 340).

المحور الثامن: أزمة التغلغل المؤسسي وتأمين البنية التحتية التنموية تُمثل "القدرة التغلغلية للمؤسسات" المعيار الأساسي لقدرة الدولة الوطنية على بسط سلطتها القانونية والخدمية داخل المجتمع ومجالها الحيوي (بدران، 2011، ص 362). وفي العصر الرقمي، انتقل هذا التغلغل من الوسائل التقليدية البيروقراطية إلى الفضاء السيبراني، ومنصات الحكومة الإلكترونية، والبيانات الضخمة. غير أن هذا التحول أفرز أزمة هيكلية تتمثل في تداخل الرقمنة الإدارية مع مخاطر الاختراق السيبراني، مما يجعل قدرة المؤسسات السيادية على تقديم الخدمات بأمان، وحماية سجلاتها الوطنية من الابتزاز والانكشاف، محط تهديد مباشر لاستقرار الدولة وخططها التنموية المستدامة (مركز الإمارات للدراسات والبحوث الاستراتيجية، 2019أ، ص 325).

أولاً: قدرة مؤسسات الدولة على التغلغل الرقمي وتقديم الخدمات السيادية بأمان يُقصد بالتغلغل الرقمي لمؤسسات الدولة قدرتها على استخدام تكنولوجيا المعلومات والاتصالات لربط القطاعات المجتمعية بشبكة الخدمات الحكومية الرسمية، وتيسير إدارة الموارد وتوزيعها بكفاءة. ومع تزايد اعتماد الحكومات على التحول الرقمي في تقديم الخدمات السيادية (كالتعليم، والصحة، والأمن، والسجل المدني، والضرائب)، باتت كفاءة وأمان هذه المنظومة تحديداً جوهرياً لاستمرار شرعية النظام السياسي (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 340).

وتتجلى أبعاد هذا المطلب في المحاور التالية:

إشكالية التوازن بين الشمول الرقمي والمخاطر الأمنية: تسعى الدول المعاصرة لتوسيع نطاق خدماتها الإلكترونية لتعزيز شرعيتها التنموية، غير أن التسرع في التغلغل الرقمي دون توفير بنية تحتية آمنة يعرض المؤسسات لهشاشة مفرطة، حيث تصبح النوافذ الخدمية المفتوحة للمواطنين نقاط دخول سهلة لعمليات التجسس والاختراق السيبراني الموجه (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 348).

ضعف القدرات المؤسسية والبنيوية في الدول النامية: تعاني مؤسسات الحكم في الدول النامية من تفاوت حاد في جاهزيتها الرقمية، وغياب المعايير الموحدة لأمن المعلومات، مما يفقدها السيطرة على أمن شبكاتها الداخلية، ويجعل تقديم الخدمات السيادية عرضة لشلل مفاجئ عند تعرضها لأبسط الهجمات الشبكية (المعهد العربي للبحوث والدراسات الاستراتيجية، 2022، ص 375).

تآكل الثقة في الخدمات السيادية الرقمية: عندما تتعرض الخدمات الحكومية الإلكترونية لاختراقات متكررة، أو تسريب لبيانات المراجعين، يؤدي ذلك إلى اهتزاز الثقة العامة في كفاءة وقدرة مؤسسات الدولة على حماية مواطنيها، مما يُفرغ التغلغل الرقمي من مضمونه التنموي والسياسي، ويُعيد الإنتاج لأزمات شرعية الحكم (رشاد، 2009، ص 390).

ثانياً: حماية السجلات الوطنية والنظم الاقتصادية-التنموية من الابتزاز والانكشاف السيبراني لا يقتصر خطر الفضاء السيبراني على شلل الخدمات اليومية، بل يمتد ليشكل تهديداً وجودياً للاستقرار الاقتصادي والوطني عبر استهداف "الأصول الاستراتيجية الحساسة" للدولة، وفي مقدمتها السجلات الوطنية الموحدة، وقواعد البيانات الاقتصادية والمصرفية (نافعة، 2016، ص 345).

وتبرز أبعاد هذا التهديد في المحاور التالية:

القيمة الاستراتيجية للسجلات الوطنية وقواعد البيانات الكبرى: تُمثل السجلات المدنية، وقواعد بيانات التعداد

السكاني، والمنظومات الضريبية والمالية العصب الحساس للدولة؛ إذ يعتمد عليها صانع القرار في التخطيط الاستراتيجي والتنموي. يؤدي انكشاف هذه السجلات أو اختراقها إلى فقدان الدولة السيطرة على أمنها الديموغرافي والاقتصادي (مركز الإمارات للدراسات والبحوث الاستراتيجية، 2019أ، ص 340).
برمجيات الفدية والابتزاز السيبراني المنظم: تتعرض النظم الاقتصادية والتنموية لموجات متصاعدة من هجمات برمجيات الفدية، حيث تقوم مجموعات قرصنة محترفة، أو شبكات مدعومة من دول إقليمية منافسة بتشفير قواعد البيانات الحكومية أو المصرفية الحيوية، والمطالبة بفدية مالية ضخمة، أو تنازلات سياسية مقابل استعادة البيانات، مما يُخضع الدولة لمنظومة ابتزاز استراتيجي مباشرة (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 358).
تهديد الخطط التنموية والاستثمارات الاستراتيجية: تؤدي الهجمات السيبرانية المستمرة على البنى التحتية الاقتصادية إلى تدمير المناخ الاستثماري، وتعطيل المشاريع التنموية الكبرى (كنظم إدارة الطاقة، والموانئ، وسلاسل التوريد)، مما يُكبد خزينة الدولة خسائر فادحة، ويعطل مسارات التحديث المؤسسي والتنمية السياسية المستدامة (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 365).

المحور التاسع: الاستجابات الاستراتيجية وبناء المناعة الرقمية

التخطيط الاستراتيجي وعقيدة الردع السيبراني لحماية التنمية والسيادة يفرض التحول العميق في طبيعة التهديدات الرقمية وانعكاساتها المباشرة على مكونات الشرعية والسيادة والتغلغل المؤسسي للدولة انتقالات استراتيجية حاسمة من نمط "الاستجابة الانفعالية" إلى نمط "التخطيط الاستباقي الشامل". فلم تعد حماية البنى التحتية والتنموية مجرد مهمة تقنية تعنى بها أقسام إدارات المعلومات، بل أضحت ركيزة جوهرية في "عقيدة الأمن القومي" تتطلب إعادة هيكلة القدرات الشاملة للدولة، وتطوير أطر مفاهيمية وعملياتية للردع والتكيف مع التهديدات المتقدمة التي يتيحها الذكاء الاصطناعي (بدران، 2011، ص 380).
أولاً: صياغة استراتيجيات الأمن القومي السيبراني لبناء القدرات الشاملة للدولة تُعبر "استراتيجية الأمن القومي السيبراني" عن الإطار الموجه الذي تُحدد من خلاله الدولة رؤيتها وأهدافها وأدواتها لحماية مجالها الحيوي الرقمي، وصيانة أصولها التنموية والسيادية، وضمان استمرارية وظائف مؤسساتها في أوقات السلم والأزمات (مركز الإمارات للدراسات والبحوث الاستراتيجية، 2019أ، ص 355).
وتتجسد المرتكزات الأساسية لبناء القدرات الشاملة للدولة في المحاور التالية:
مأسسة الحوكمة الرقمية والقيادة الموحدة: يتطلب بناء القدرات الوطنية إنشاء مظلة سيادية موحدة (كمجلس أعلى للأمن السيبراني، أو هيئة وطنية للأمن الرقمي) ترتبط برئاسة الدولة أو مجلس الوزراء؛ لضمان التنسيق العابر للقطاعات بين المؤسسات العسكرية والأمنية والمدنية والقطاع الخاص، والقضاء على حالة التشرذم التنظيمي التي تُشكل ثغرة نفاد للتهديدات العابرة للحدود (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 375).
تحصين البنى التحتية الحيوية والتنموية: تعتمد الاستراتيجية الوطنية على تحديد القطاعات الحيوية (كالشبكات الكهربائية، نظم إدارة المياه، القطاع المصرفي، والسجلات الوطنية) وإخضاعها لبروتوكولات أمنية صارمة، تعتمد على مبدأ "الدفاع عن بعد" وتطبيق نماذج "الثقة الصفرية" لضمان عدم انكشاف النظم التنموية للهجمات الشاملة (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 382).
تنمية رأس المال البشري وتوطين المعرفة الرقمية: لا يمكن بناء قدرات شاملة دون الاستثمار المكثف في الكوادر الوطنية، عبر تطوير المناهج التعليمية، وإنشاء مراكز التميز في الذكاء الاصطناعي والأمن السيبراني، وتشجيع البحث العلمي الوطني لتوطين التكنولوجيا، وتقليل الاعتماد الحرج على الخبرات والبرمجيات الأجنبية التي قد تحمل ثغرات سيادية مسبقة الصنع (رشاد، 2009، ص 410).
ثانياً: تطوير عقيدة الردع غير المتماثل والتكيف مع تهديدات الذكاء الاصطناعي يواجه مفهوم "الردع التقليدي" القائم على التهديد بالعقاب العسكري المتبادل تحديات جارية في الفضاء السيبراني؛ نظراً لصعوبة "إسناد الهجوم" وسرعة اختفاء المهاجمين. ومن ثم، برزت الحاجة إلى تطوير "عقيدة الردع غير المتماثل"،

والتكيف المرن مع بيئة التهديدات التوليدية المعززة بالذكاء الاصطناعي (المعهد العربي للبحوث والدراسات الاستراتيجية، 2022، ص 395).
وتبرز مقومات هذه العقيدة والتكيف الاستراتيجي في المحاور التالية:
أبعاد الردع غير المتماثل (بالسلب والإيجاب).
الردع بالمنع: يركز على رفع تكلفة الهجوم وجعله غير جدوى اقتصادياً أو سياسياً للمهاجم، عبر تعزيز "الصمود الرقمي" للبنى التحتية، بحيث تستطيع النظم امتصاص الهجمات السيبرانية والتعافي منها دون شلل وظائف الدولة (نافعة، 2016، ص 360).
الردع بالعقاب غير المتماثل: يتضمن تطوير قدرات سيبرانية هجومية ودفاعية تمكن الدولة من فرض تكاليف باهظة على الفاعلين المستهدفين (سواء كانوا دولاً أو شبكات) عبر ردود متعددة المجالات تمتد لتشمل العقوبات الاقتصادية، والعزل الدبلوماسي، والعمليات السيبرانية المضادة (نافعة، 2016، ص 368).
التكيف مع التهديدات المعززة بالذكاء الاصطناعي:
الدفاع السيبراني الذاتي والمبكر: تفرض هجمات الذكاء الاصطناعي (كالهجمات الخوارزمية الذاتية، والتصيد الموجه المعتمد على تحليل البيانات الكبيرة) الاعتماد على أنظمة دفاعية تعمل بالذكاء الاصطناعي لتشخيص أنماط التهديد وتكتيكاتها في أجزاء من الثانية، وتفعيل استجابات برمجية تلقائية قبل وقوع الضرر (مركز الإمارات للدراسات والبحوث الاستراتيجية، 2019أ، ص 372).
مواجهة التضليل والتزييف العميق الإستراتيجي: يتطلب التكيف العملياتي تطوير خوارزميات رصد وطنية ومتقدمة لكشف التزييف العميق والهندسة الاجتماعية فور ظهورها، وتفعيل أطر استجابة إعلامية وأمنية سريعة لحماية الثقة العامة، ومنع تحول الحملات الموجهة إلى أزمات استقرار سياسي (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 390).

المحور العاشر: الحوكمة الإقليمية والدولية للذكاء الاصطناعي والأمن السيبراني

تتطلب التهديدات الرقمية والتكنولوجية عابرة الحدود معالجةً تتجاوز حدود الأطر الوطنية الفردية؛ إذ إن الطبيعة الشبكية للفضاء السيبراني وتطبيقات الذكاء الاصطناعي تجعل من التعاون الدولي والإقليمي ضرورة استراتيجية لحماية الأمن والسلم الدوليين. وفي هذا السياق، تبرز إشكالية "الحوكمة الرقمية العالمية" كساحة تنافس جيوسياسي بين القوى العظمى للدفع باتجاه قواعد ومنظومات قانونية توازن بين الاستخدام التنموي للتقنية وضبط استخداماتها العسكرية والأمنية، وبناء تكتلات إقليمية قادرة على تحصين أمنها الجماعي السيبراني (بدران، 2011، ص 395).
أولاً: أطر القانون الدولي ومدونات السلوك المنظمة للاستخدام العسكري والتنموي للتقنية تُواجه المنظومة القانونية الدولية تحدياً بنيوياً في تكييف قواعد "القانون الدولي التقليدي" و"القانون الدولي الإنساني" مع الفضاء السيبراني وتطبيقات الذكاء الاصطناعي الفائقة. وتبرز المحاولات الدولية لصياغة أطر تنظيمية ومدونات سلوك تُحدد حدود الاستخدام المشروع والمسؤول للتقنية في السلم والحرب (مركز الإمارات للدراسات والبحوث الاستراتيجية، 2019أ، ص 380).
وتتجلى أبعاد هذا المطلب في المحاور التالية:
إشكالية إخضاع الفضاء السيبراني للقانون الدولي: يدور الجدل الأكاديمي والقانوني حول مدى انطباق ميثاق الأمم المتحدة (وتحديداً المادة 2 الفقرة 4 المتعلقة بحظر استخدام القوة، والمادة 51 المتعلقة بحق الدفاع الشرعي عن النفس) على الهجمات السيبرانية. وتتمثل العقبة الأساسية في تحديد "عتبة العمل الحربي" في الهجمات السيبرانية التي لا تؤدي لماديات ملموسة، ولكنها تُعطل البنى التحتية الحيوية أو المنظومات التنموية للدولة (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 405).
مدونات السلوك وقواعد "السلوك المسؤول للدول": سعت الجمعية العامة للأمم المتحدة عبر "فريق الخبراء الحكوميين" و"فريق العمل المفتوح العضوية" إلى صياغة معايير ومدونات سلوك غير ملزمة قانوناً، ولكنها ملزمة أدبياً وسيناريوياً. وتؤكد هذه المعايير على عدم جواز شن هجمات سيبرانية استراتيجية تستهدف البنى

التحتية التنموية الحيوية (المستشفيات، وسلاسل التوريد)، وضرورة تقديم المساعدة في التحقيقات السيبرانية العابرة للحدود (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 412).
تنظيم الاستخدام العسكري للذكاء الاصطناعي وأنظمة السلاح الذاتية: تتزايد المخاوف الدولية من دمج الذكاء الاصطناعي في منظومات الأسلحة الفتاكة ذاتية التشغيل، مما يُهدد بإبعاد العنصر البشري عن اتخاذ قرار القتل، ويخرق مبادئ التمييز والتناسب المسلم بها في القانون الدولي الإنساني. وتدفع الجهود الدولية الحالية نحو بناء المعاهدات والاتفاقيات الدولية لمنع الأتمتة الكاملة للقرارات العسكرية الاستراتيجية والنوايا الهجومية (المعهد العربي للبحوث والدراسات الاستراتيجية، 2022، ص 410).
ثانياً: آليات التعاون الإقليمي لبناء منظومات دفاعية وسيبرانية مشتركة نظراً للتفاوت الحاد في القدرات التكنولوجية بين الدول، تعتمد المقاربات الاستراتيجية الحديثة على "التحالفات السيبرانية الإقليمية" كخط دفاع متقدم لتعزيز القدرات الدفاعية الجماعية، وتبادل المعلومات حول التهديدات، وتوفير التضامن الاستراتيجي ضد الاختراقات السيبرانية والهندسة الاجتماعية الموجهة (رشاد، 2009، ص 430).
وتتجسد محاور وآليات التعاون الإقليمي في الآتي:
مراكز الاستجابة للطوارئ السيبرانية الإقليمية: يُمثل إنشاء شبكات ومراكز إقليمية مشتركة للاستجابة لطوارئ الحاسوب (كشبكة CERT التابعة للاتحاد الأفريقي، أو مبادرات مجلس التعاون الخليجي، وجامعة الدول العربية) آلية عملياتية حيوية لتبادل الإنذارات المبكرة حول الثغرات الأمنية والهجمات البرمجية فور اكتشافها، مما يمنح الدول الأعضاء قدرة على التعافي والتصدّي قبل اتساع رقعة الانكشاف (نافعة، 2016، ص 375).
التدريبات العسكرية والسيبرانية المشتركة: يتطلب بناء المنظومات الدفاعية المشتركة إجراء تمارين محاكاة سيبرانية إقليمية دورية ترفع من مستوى الجاهزية والتنسيق العملياتي بين وحدات الدفاع السيبراني للمؤسسات العسكرية والأمنية للدول المشاركة، واختبار كفاءة بروتوكولات الاتصال والاستجابة المشتركة للأزمات السيبرانية الشاملة (نافعة، 2016، ص 382).
مواجهة التهديدات غير المتماثلة وحماية الأمن التنموي الإقليمي: يُكّن التعاون الإقليمي من مواجهة مجموعات الجريمة المنظمة وشبكات القرصنة العابرة للحدود وحملات التضليل الرقمي الموجهة التي تستهدف الاستقرار الإقليمي برعايات أجنبية. كما يُوفر الإطار الإقليمي مظلة تفاوضية جماعية أقوى في مواجهة الشركات الاحتكارية والتكتلات التكنولوجية الكبرى، لفرض احترام السيادة الرقمية والخصوصية الوطنية لمواطني الإقليم (مركز الإمارات للدراسات والبحوث الاستراتيجية، 2019أ، ص 395).
المحور الحادي عشر: السيناريوهات المستقبلية للسيادة والتنمية وخارطة الطريق الاستراتيجية يُعد الاستشراف المستقبلي ركيزة حاسمة في تحليل التفاعلات المعقدة بين التحولات التكنولوجية المتسارعة ومستقبل الدولة الوطنية. وفي ضوء المعطيات والتحديات التي فككتها المباحث السابقة (بدءاً من التزييف العميق وأزمات الهوية، مروراً بالتغلغل المؤسسي والانكشاف السيبراني، وصولاً إلى استراتيجيات الردع والحوكمة الدولية)، يقدم هذا المبحث قراءة استشرافية لمستقبل السيادة والتنمية السياسية عبر سيناريوهين رئيسيين، ليخلص إلى وضع خارطة طريق استراتيجية تُشكل دليلاً موصى به لصناع القرار لإدارة الأزمات الرقمية والتنموية (بدران، 2011، ص 410).
أولاً: السيناريوهات المستقبلية للسيادة الرقمية والتنمية السياسية يعتمد التحليل الاستشرافي على مصفوفة التفاعل بين متغيرين حاسمين: مستوى الامتلاك الوطني للتكنولوجيا والبنية التحتية، وكفاءة حوكمة الأمن القومي السيبراني. وينتج عن التفاعل بين هذين المتغيرين مساران مستقبليان تمتد آثارهما للسنوات العشر القادمة (مركز الإمارات للدراسات والبحوث الاستراتيجية، 2019أ، ص 412).
السيناريو الأول (التآكل والانكشاف):
ارتهان القرار التنموي، وتفشي الاختراقات، وغياب السيادة الرقمية:
المعالم والخصائص: يفترض هذا السيناريو عجز الدولة عن مواكبة التحولات التكنولوجية، واستمرار الاعتماد الكلي والمطلق على البنى التحتية السحابية والخوارزميات والتطبيقات الأجنبية العابرة للحدود، مع

بطء مسارات التحول الرقمي الآمن في المؤسسات السيادية (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 430).
التداعيات على السيادة والتنمية: يؤدي تحقق هذا السيناريو إلى ارتهان القرار التنموي والسياسي للدولة للإرادة الخارجية ولضغوط الشركات التكنولوجية الاحتكارية. كما تتسارع فيه معدلات الانكشاف السيبراني، وتتعرض قواعد البيانات السكاني والاقتصادي للاختراق والابتزاز المستمر، مما يتسبب في تفكيك التماسك المجتمعي وتآكل شرعية النظام السياسي نتيجة الشلل المتكرر في الخدمات الحكومية والسيادية (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 438).
السيناريو الثاني (التكيف والسيادة الرقمية الذاتية):
امتلاك خوارزميات وبنى تحتية وطنية تحقق التوازن والاستقرار المعالم والخصائص: يفترض هذا السيناريو نجاح الدولة في صياغة وتنفيذ استراتيجية وطنية شاملة للأمن الرقمي، تشتمل على توطين مراكز البيانات الحيوية، وبناء الحوسبة السحابية السيادية، وتطوير نماذج ذكاء اصطناعي وخوارزميات وطنية مجهزة باللغة والخصوصية الثقافية للمجتمع (المعهد العربي للبحوث والدراسات الاستراتيجية، 2022، ص 435).
التداعيات على السيادة والتنمية: يُوفر هذا المسار مناعة استراتيجية تُمكن المؤسسات الوطنية من بسط تغلغلها الرقمي الآمن، وحماية السجلات الاستراتيجية من التجسس والابتزاز، كما يضمن استقلالية القرار السياسي والتنموي، ويعزز الثقة العامة بين المواطن ومؤسسات الحكم، مما يحول الفضاء الرقمي من مصدر تهديد إلى محرك رئيس للتنمية السياسية والاقتصادية المستدامة (المعهد العربي للبحوث والدراسات الاستراتيجية، 2022، ص 442).
ثانياً: خارطة الطريق الاستراتيجية: التوصيات والموجهات العامة لصناع القرار استناداً إلى ترجيح السيناريو الثاني (التكيف والسيادة الذاتية) بوصفه الهدف الإستراتيجي الحاكم لحفظ وجود الدولة، يقدم هذا المطلب خارطة طريق تنفيذية تتضمن موجهات عامة وتوصيات عملية موجهة لصناع القرار في مجالات الأمن القومي والتحول التنموي (رشاد، 2009، ص 455).
وتتوزع خارطة الطريق على أربعة محاور عملية:
المحور المالي والتنظيمي (مأسسة الحوكمة والسيادة).
إقرار تشريعات وقوانين حازمة وموحدة لحماية البيانات الشخصية الوطنية والسيادة السحابية، تُلزم الشركات الدولية بتخزين ومعالجة البيانات الحساسة داخل الحدود الوطنية.
تأسيس "مجلس أعلى للأمن السيبراني والذكاء الاصطناعي" يتمتع بصلاحيات سيادية لتنسيق السياسات الرقمية بين الأجهزة العسكرية والأمنية والقطاعات الخدمية والتنموية (نافعة، 2016، ص 390).
المحور التقني والبنيوي (توطين التكنولوجيا والصمود الرقمي).
الاستثمار العاجل في بناء مراكز بيانات سحابية سيادية ومحمية ضد الاختراقات الفيزيائية والشبكية.
تطوير خوارزميات وطنية موثوقة للتحقق من الهوية الرقمية، ورصد وتفكيك عمليات "التزييف العميق" والتضليل الإعلامي فور حدوثها وقبل انتشارها في الفضاء العام (مركز الإمارات للدراسات والبحوث الاستراتيجية، 2019أ، ص 428).
المحور البشري والاجتماعي (بناء المناعة والكوادر الوطنية).
إطلاق برامج تعليمية وتدريبية متقدمة لتأهيل كوادر وطنية متخصصة في الذكاء الاصطناعي والأمن السيبراني، مع إيجاد بيئة جاذبة لمنع العقول الوطنية من الهجرة.
إدماج مفاهيم "التفكير النقدي الرقمي" والأمن المعرفي في المناهج التعليمية والخطاب الإعلامي لبناء حصانة مجتمعية ضد تقنيات "الهندسة الاجتماعية" والاستقطاب الخوارزمي (المعهد العربي للبحوث والدراسات الاستراتيجية، 2021، ص 450).
المحور الدولي والإقليمي (الدبلوماسية الرقمية والتحالفات).
تفعيل "الدبلوماسية السيبرانية" للدفاع عن مصالح الدولة في المحافل الدولية الداعية لصياغة معاهدات ملزمة

تحظر استهداف البنى التحتية التنموية.
الانخراط الفاعل في تأسيس أطر وتحالفات سيبرانية إقليمية لتبادل المعلومات حول التهديدات وتحقيق الردع الجماعي غير المتماثل (نافعة، 2016، ص 398).

الخاتمة

أهم النتائج النظرية والتطبيقية للدراسة توصلت الدراسة إلى جملة من النتائج الأكاديمية والتطبيقية المركبة التي تُجمل أبعاد الظاهرة وتُثبت فرضيات البحث الرئيسة، ويمكن تصنيفها وفق المحورين التاليين:

النتائج النظرية :إعادة تشكيل أبعاد مفهوم السيادة: أثبتت الدراسة أن مفهوم "السيادة الوطنية" التقليدي القائم على الحدود الجغرافية والاحتكار الحصري لأدوات الإكراه البدني قد شهد تحولاً راديكالياً؛ حيث برز مفهوم "السيادة السيبرانية" بوصفه المُنظم الأساسي لقدرة الدولة على فرض سلطتها القانونية والرقابية على بياناتها الوطنية وبنيتها التحتية السحابية.

الشرعية السياسية في عصر الانكشاف الإدراكي: كشف التحليل النظري أن "الشرعية السياسية" لم تعد تعتمد فقط على المخرجات التنموية والأداء البيروقراطي، بل أصبحت محكومة بقدرة الدولة على تحصين البيئة الإدراكية لمواطنيها ضد تقنيات "التزييف العميق" والتضليل الخوارزمي الموجه، وتجنب السقوط في ظاهرة "دفاع الكاذب" التي تُقوض ثقة المجتمع في مؤسسات الحكم (بدران، 2011، ص 425).

بروز "الفاعلين التكنولوجيين غير الحكوميين" كقوى جيوسياسية: أظهر البحث أن التكتلات التكنولوجية الكبرى والشركات الاحتكارية العابرة للحدود باتت تمارس سلطات تنظيمية وسيادية موازية للدول، من خلال احتكار البيانات الضخمة والتحكم في الخوارزميات الحاكمة للمجال العام الرقمي (مركز الإمارات للدراسات والبحوث الاستراتيجية، 2019أ، ص 430).

النتائج التطبيقية والعملياتية :أزمة التغلغل الرقمي والانكشاف الاستراتيجي: كشفت الدراسة أن تسرع مؤسسات الدولة في تطبيق "الرقمنة الإدارية" والخدمات الحكومية الإلكترونية، دون بناء منظومة أمن سيبراني صلبة، أدى إلى خلق "هشاشة مؤسسية حادة" جعلت السجلات الوطنية الموحدة والأصول الاقتصادية والتنموية عرضة للهجمات المنظمة وبرمجيات الفدية والابتزاز الاستراتيجي.

قصور آليات الردع التقليدية: أثبت التحليل العملياتي أن أطر الردع التقليدية غير قادرة بمفردها على حماية الفضاء السيبراني نظراً لإشكالية "إسناد الهجوم"، مما يتطلب التحول نحو "عقيدة الردع غير المتماثل" القائمة على الردع بالمنع (الصمود الرقمي) والردع بالعقاب متعدد المجالات.

حتمية التحالفات الإقليمية والحوكمة الدولية: بين التطبيق العملي أن الدول النامية والإقليمية لا تستطيع تحقيق المناعة الرقمية منفردة؛ إذ يُعد الانخراط في التحالفات السيبرانية الإقليمية وصياغة أطر قانونية دولية ملزمة شرطين أساسيين لتأمين الاستقرار الجيو-سياسي وحماية التنمية المستدامة.

التوصيات

بناءً على النتائج التي أسفرت عنها الدراسة، تُقدم جملة من التوصيات التنفيذية الموجهة لصناع القرار والمؤسسات الأكاديمية والمراكز البحثية الاستراتيجية:

على صعيد المأسسة التشريعية والتنظيمية:

إقرار قانون موحد للسيادة الرقمية وحماية البيانات: إصدار تشريعات حازمة تُجبر المنصات والتكتلات التكنولوجية الدولية على توطين معالجة وتخزين السجلات والبيانات الوطنية داخل الحدود الإقليمية للدولة.

إنشاء هيكل سيادي موحد لحوكمة الفضاء الرقمي: تأسيس "مجلس أعلى للأمن السيبراني والذكاء الاصطناعي" يتبع قيادة الدولة مباشرة، ويتولى التنسيق الربطي بين القطاعات العسكرية والأمنية والمدنية والقطاع الخاص.

على صعيد التوطين التقني وبناء الصمود الرقمي:

بناء الحوسبة السحابية السيادية: الاستثمار العاجل في إنشاء بنية تحتية سحابية وطنية ومستقلة لتخزين الأصول المعلوماتية الحساسة وإدارتها بمعزل عن ضغوط الفاعلين الخارجيين.

تطـوير خوارزميـات الرصـد والاسـتجابة المبكـرة: دعـم إنتـاج أدوات برمجـة وطنيـة تعتمـد علـى الـذكاء الاصطناعي للتحقق الإشاري ورصد تقنيات التزييف العميق والهندسة الاجتماعية والتصدّي لها فور ظهورها في الفضاء العام.

على صعيد التنمية البشرية والمجتمعية:

تطوير رأس المال البشري المتخصص: إطلاق برامج أكاديمية وبحثية متقدمة لتأهيل النخب الوطنية في مجالات الأمن السيبراني والذكاء الاصطناعي، ووضع حوافز جاذبة للحد من هجرة الكفاءات العلمية.

تعزيز "الأمن المعرفي" للمجتمع: إدراج مفاهيم التفكير النقدي الرقمي والمواطنة الرقمية في المناهج التعليمية؛ لبناء مناعة مجتمعية ضد حملات الاستقطاب الخوارزمي والتضليل الإعلامي.

على صعيد التحالفات والدبلوماسية الرقمية:

تفعيل الدبلوماسية السيبرانية: المشاركة الفاعلة في صياغة المعاهدات الدولية لمنع تسييس التقنية وحظر استهداف البنى التحتية الخدمية والتنموية.

تأسيس المنظومات الدفاعية الإقليمية المشتركة: الانخراط في مراكز الاستجابة الإقليمية لطوارئ الحاسوب، وإجراء تدريبات سيبرانية مشتركة لتعزيز الردع الجماعي الإقليمي.

آفاق البحث المستقبلي تفتح هذه الدراسة آفاقاً بحثية واعدة أمام الباحثين في حقل العلاقات الدولية والعلوم السياسية لمواصلة تقصي الأبعاد التكنولوجية المتجددة، وتحديداً في محاور:

دراسة أثر دمج "أنظمة السلاح الذاتية التشغيل" المعززة بالذكاء الاصطناعي على استقرار معادلات التوازن الإقليمي.

دراسة تأثير "الشركات التكنولوجية الاحتكارية" كفاعلين جيوسياسيين جدد في إدارة النزاعات الدولية.

تطوير نماذج قياسية كمية لقياس "مؤشر السيادة الرقمية" ودوره في حماية التنمية السياسية بالدول النامية.

نسأل الله تعالى أن تكون هذه الدراسة قد قدمت إضافة علمية وازنة للمكتبة العربية والأكاديمية، وأن تشكل لبنة تُستضاء بها استراتيجيات حماية وطننا واستقراره السيادي والتنموي.

المراجع:

أولاً: الكتب

- البشري، طارق. (2002). إشكالية التنمية السياسية في الفكر العربي المعاصر. دار الشروق.
- بدران، عبد المنعم. (2018). التنمية السياسية وبناء الدولة: قراءات في الفكر السياسي المعاصر. مركز دراسات الوحدة العربية.
- رشاد، عبد الغفار. (2008). مناهج تحليل التنمية السياسية في العالم النامي: دراسة في النظريات والتطبيق. مكتبة الشروق الدولية.
- زايد، أحمد. (2005). التحديث والتنمية السياسية في العالم الثالث: رؤية نقدية في علم الاجتماع السياسي. الهيئة المصرية العامة للكتاب.
- أسامة، محمد. (2019). السيادة الوطنية في العصر الرقمي: تحديات الأمن السيبراني والذكاء الاصطناعي. دار النهضة العربية.
- كيلاني، موسى. (2010). نظريات التنمية السياسية المعاصرة: دراسة تحليلية مقارنة. دار الشروق للنشر والتوزيع.
- نافعة، حسن. (2012). إصلاح الدولة وأزمة الحكم في الوطن العربي: بين متطلبات الاستقرار واستحقاقات الديمقراطية. مركز دراسات الوحدة العربية.
- هنتنغتون، صامويل. (1993). النظام السياسي في مجتمعات متغيرة (سمية فلوع عبود، مترجم). دار الساقي.

ثانياً: الدوريات والمجلات العلمية

- القاسمي، خالد بن محمد. (2015). المأسسة والاستقرار السياسي في أطروحة هنتنغتون: دراسة نقدية. مجلة الدراسات السياسية والإستراتيجية، 8(2).
- المالكي، عبد الله. (2023). أزمة الشرعية والسيادة في الفضاء الافتراضي: دراسة تحليليّة جيوسياسية. مجلة السياسة الدولية، 58(231)، 45-78.
- المعهد العربي للبحوث والدراسات الاستراتيجية. (2022). التنافس الإقليمي والتنمية السياسية: دراسة في تحولات الجيو-بوليتيك المعاصر. المعهد العربي للبحوث والدراسات الاستراتيجية.

- المعهد العربي للبحوث والدراسات الاستراتيجية. (2023). التطور التكنولوجي والأمن القومي: أبعاد التنمية السياسية في البيئة الرقمية (دراسة موثقة). المعهد العربي للبحوث والدراسات الاستراتيجية.
- محمد، محمد علي. (2006). أزمات التنمية السياسية في الدول النامية: دراسة في أدبيات لوسيان باي. مجلة السياسة الدولية، (165).
- هلال، علي الدين، ومجيب، مي. (2017). التنمية السياسية في الوطن العربي: الأزمات والإمكانات. مجلة نهضة مصر للعلوم السياسية، 12(3).

ثالثاً: الرسائل والأطروحات الجامعية

- بوزيد، أحمد. (2022). القوة الناعمة والتنمية السياسية: دراسة استراتيجية في العلاقات الدولية المعاصرة [أطروحة دكتوراه غير منشورة]. جامعة الجزائر.
- حماد، رامي. (2025). الفجوة الرقمية وأثرها على التنمية السياسية والسيادة في منطقة الشرق الأوسط [رسالة ماجستير غير منشورة]. جامعة القاهرة.
- الشريف، طارق. (2024). حوكمة التكنولوجيا الحديثة وأثرها على التوازن الإقليمي والاستقرار السياسي [أطروحة دكتوراه غير منشورة]. جامعة عين شمس.
- طاهر، مصطفى. (2018). أزمات التنمية السياسية وبناء الدولة في الوطن العربي [رسالة ماجستير غير منشورة]. الجامعة الأردنية.
- عبد الله، خالد. (2021). الأمن السيبراني كأحد متطلبات حماية السيادة الوطنية في ظل التنافس الإقليمي [رسالة ماجستير غير منشورة]. جامعة الملك سعود.
- العتيبي، سعد. (2020). التحول الرقمي وأثره على المشاركة السياسية والشرعية في العلاقات الإقليمية [أطروحة دكتوراه غير منشورة]. كلية العلوم الاستراتيجية، جامعة نايف العربية للعلوم الأمنية.
- حرب، أسامة الغزالي. (2001). نظريات التحديث السياسي وإشكاليات التطبيق في الشرق الأوسط [أطروحة دكتوراه غير منشورة]. كلية الاقتصاد والعلوم السياسية، جامعة القاهرة.

رابعاً: التقارير الاستراتيجية

- مركز الإمارات للدراسات والبحوث الاستراتيجية. (2019). الدول الهشة وأثرها على الأمن الإقليمي والدولي (تقرير استراتيجي، سلسلة دراسات عالمية، العدد 98). مركز الإمارات للدراسات والبحوث الاستراتيجية.
- مركز الإمارات للدراسات والبحوث الاستراتيجية. (2021). التحديات الرقمية وأثرها على مفهوم السيادة والتنمية السياسية (تقرير استراتيجي، سلسلة دراسات عالمية، العدد 110). مركز الإمارات للدراسات والبحوث الاستراتيجية.

References:

First: Books

- Al-Bishri, Tariq. (2002). The Problematic of Political Development in Contemporary Arab Thought. Dar Al-Shorouk.
- Badran, Abdel Moneim. (2018). Political Development and State Building: Readings in Contemporary Political Thought. Center for Arab Unity Studies.
- Rashad, Abdel Ghaffar. (2008). Approaches to Analyzing Political Development in the Developing World: A Study in Theories and Applications. Al-Shorouk International Library.
- Zayed, Ahmed. (2005). Modernization and Political Development in the Third World: A Critical Perspective in Political Sociology. Egyptian General Book Organization.
- Osama, Mohamed. (2019). National Sovereignty in the Digital Age: Cybersecurity and Artificial Intelligence Challenges. Dar Al-Nahda Al-Arabiya.
- Kilani, Moussa. (2010). Contemporary Theories of Political Development: A Comparative Analytical Study. Dar Al-Shorouk for Publishing and Distribution.
- Nafaa, Hassan. (2012). State Reform and the Crisis of Governance in the Arab World: Between the Requirements of Stability and the Entitlements of Democracy. Center for Arab Unity Studies.
- Huntington, Samuel. (1993). Political Order in Changing Societies (translated by Sumaya Falou Aboud). Dar Al-Saqi.

Second: Scientific Journals and Periodicals

- Al-Qasimi, Khalid bin Muhammad. (2015). Institutionalization and Political Stability in Huntington's Thesis: A Critical Study. Journal of Political and Strategic Studies, 8(2).
- Al-Maliki, Abdullah. (2023). The Crisis of Legitimacy and Sovereignty in Cyberspace: A Geopolitical Analytical Study. Journal of International Politics, 58(231), 45-78.

- Arab Institute for Research and Strategic Studies. (2022). Regional Competition and Political Development: A Study in Contemporary Geopolitical Transformations. Arab Institute for Research and Strategic Studies.
- Moussa, A. M. (2026). The Legal Future of Artificial Intelligence Technology: A Study of the Impact of AI Technology on Civil Law. *Al-haq Journal for Sharia and Legal Sciences*, *13*(1), 403-413.
- Arab Institute for Research and Strategic Studies. (2023). Technological Development and National Security: Dimensions of Political Development in the Digital Environment (A Documented Study). Arab Institute for Research and Strategic Studies.
-
- Salem, M. A. (2026). Artificial Intelligence Crimes the Crime of Deep fake a model. *Al-haq Journal for Sharia and Legal Sciences*, *13*(1), 485-496.
- Muhammad, Muhammad Ali. (2006). Crises of Political Development in Developing Countries: A Study in the Literature of Lucien Pye. Journal of International Politics, (165).
- Hilal, Ali al-Din, and Mujeeb, Mai. (2017). Political Development in the Arab World: Crises and Potentials. Nahdet Misr Journal of Political Science, 12(3).

Third: University Theses and Dissertations

- Bouzid, Ahmed. (2022). Soft Power and Political Development: A Strategic Study in Contemporary International Relations [Unpublished PhD dissertation]. University of Algiers.
- Hammad, Rami. (2025). The Digital Divide and its Impact on Political Development and Sovereignty in the Middle East [Unpublished Master's thesis]. Cairo University.
- Al-Sharif, Tariq. (2024). Governance of Modern Technology and its Impact on Regional Balance and Political Stability [Unpublished PhD dissertation]. Ain Shams University.
- Taher, Mustafa. (2018). Crises of Political Development and State-Building in the Arab World [Unpublished Master's thesis]. University of Jordan
- Majid, S. A. (2026). Civil liability for damages caused by artificial intelligence. Al-haq Journal for Sharia and Legal Sciences, 13(1), 618-641.
- Abdullah, Khalid. (2021). Cybersecurity as a Requirement for Protecting National Sovereignty in Light of Regional Competition [Unpublished Master's thesis]. King Saud University.
- Al-Otaibi, Saad. (2020). Digital Transformation and its Impact on Political Participation and Legitimacy in Regional Relations [Unpublished PhD dissertation]. College of Strategic Sciences, Naif Arab University for Security Sciences.
- Khalleefah, A. B., Abdalqadir, M. A., & Salem, A. A. (2025). Towards a new theory of civil liability in the context of artificial intelligence systems and the challenges of reforming the traditional theory. Al-haq Journal for Sharia and Legal Sciences, 754-770.
- Harb, Osama Al-Ghazali. (2001). Theories of Political Modernization and the Problems of Application in the Middle East [Unpublished Doctoral Dissertation]. Faculty of Economics and Political Science, Cairo University.

Fourth: Strategic Reports

- Emirates Center for Strategic Studies and Research. (2019). Fragile States and Their Impact on Regional and International Security (Strategic Report, Global Studies Series, No. 98). Emirates Center for Strategic Studies and Research.
- Emirates Center for Strategic Studies and Research. (2021). Digital Challenges and Their Impact on the Concept of Sovereignty and Political Development (Strategic Report, Global Studies Series, No. 110). Emirates Center for Strategic Studies and Research.

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of **JLABW** and/or the editor(s). **JLABW** and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.