رهانات الانتخابات المغربية 2026 في مواجهة التهديدات الهجينة المستجدة

- التضليل المعلوماتي والذكاء الاصطناعي كأدوات للتأثير الخارجي -

Stakes of the 2026 Moroccan Elections Against the new Hybrid Threats:
- Disinformation and Artificial Intelligence as Tools of Foreign Influence –

✍ **د. رضوان الوهابي**

أستاذ باحث في العلاقات الدولية

بالمعهد الجامعي للدراسات الإفريقية والأورومتوسطية والإيبيروأمريكية

جامعة محمد الخامس بالرباط - المغرب[1]

الملخص

تتناول هذه الورقة البحثية رهانات الانتخابات التشريعية المغربية المقبلة (شتنبر 2026) من منظور العلاقات الدولية، بالاستناد إلى الواقعية الجديدة بوصفها إطارا تفسيريا لتحليل أنماط التنافس الدولي على النفوذ. وتركز الدراسة على التضليل المعلوماتي المعزز بالذكاء الاصطناعي بوصفه أحد أدوات التهديدات الهجينة التي يوظفها الفاعلون الدوليون للتأثير في المسارات الانتخابية، ضمن سياق جيوسياسي أوسع يشمل الفضاءين المغاربي والإفريقي. وتنطلق الورقة من فرضية مفادها أن تصاعد التنافس بين القوى الكبرى، مقرونا بالتحول النوعي الذي يشكله الذكاء الاصطناعي التوليدي في بنية تهديدات التضليل المعلوماتي، يوفر بيئة مواتية لتكثيف التدخلات الخارجية عبر أدوات رقمية منخفضة الكلفة وعالية الأثر.

بعد ضبط الإطارين النظري والمنهجي وتحديد المفاهيم الرئيسية، تنظَّم الدراسة حول ثلاثة محاور: يرصد أولها تطور آليات التأثير الخارجي في الانتخابات، ويتناول ثانيها بالتحليل بعض الاستجابات الدولية الرئيسية، فيما يحاول ثالثها تطبيق هذه المقاربات على الحالة المغربية لاستخلاص رهانات الاستحقاق الانتخابي المقبل واقتراح توصيات داعمة للمرونة الانتخابية.

الكلمات المفتاحية: الانتخابات، التأثير الخارجي، التضليل المعلوماتي، الذكاء الاصطناعي، التهديدات الهجينة، السيادة التكنولوجية.

[1] البريد الإلكتروني: elouahhabi1@gmail.com

Abstract

This paper examines the stakes of Morocco's forthcoming legislative elections (September 2026) from an international relations perspective, employing the Neorealist theoretical framework to analyze patterns of international competition for influence. It focuses on AI-driven disinformation as one of the key instruments of hybrid threats deployed by international actors to shape electoral trajectories, situating these practices within a broader geopolitical context encompassing the Maghreb and Africa. The paper advances the hypothesis that the intensification of great-power rivalry, coupled with the qualitative transformation introduced by generative artificial intelligence in the structure of disinformation threats, creates a conducive environment for the expansion of foreign interference through low-cost, high-impact digital tools.

After establishing the theoretical and methodological frameworks and defining the study's core concepts, the analysis is organized around three main axes: first, tracing the evolution of mechanisms of external influence in electoral processes; second, examining selected major international responses to these challenges; and third, applying these approaches to the Moroccan case to identify the stakes of the upcoming electoral contest and to propose recommendations aimed at strengthening electoral resilience.

Keywords: Elections, Foreign Interference, Disinformation, Artificial Intelligence, Hybrid Threats, Technological Sovereignty.

مقدمة

شهد النظام الدولي المعاصر في العقد الأخير تحولات بنيوية عميقة، جعلت المشهد الجيوسياسي يتسم بتصاعد حدة التنافس بين كبار الفاعلين، وعلى رأسهم الولايات المتحدة الأمريكية التي تتركز استراتيجيتها للقرن الواحد والعشرين عموما، من جهة، في الحفاظ على موقع الزعامة العالمية التي تتمتع به وتدعيم مكانتها كمساهم رئيسي في الثورة العلمية التكنولوجية وقوة مسيطرة في العالم، ومن جهة ثانية، تحاشي ظهور أي منافس تصعب السيطرة عليه (أو على الأرجح اتحاد من المنافسين) يمكنه مع حلول منتصف القرن الحالي أن ينتزع الصدارة في السباق العالمي من أيدي زعماء الغرب ويؤسس عالما جديدا يتخلف فيه الغرب ولأول مرة منذ خمسمائة عام عن مقعد الزعامة.[1] وقد رافقت هذه التحولات البنيوية ثورة تكنولوجية غير مسبوقة في مجال الاتصال والمعلومات، أعادت رسم ملامح الصراع على النفوذ والتأثير، وأفرزت أشكالا جديدة من الحروب الهجينة التي تتخذ من الفضاء السيبراني ميدانا لها، لاسيما مع التطورات العلمية والابتكارات التقنية المتسارعة التي تعرفها نظم الذكاء الاصطناعي وتطبيقاتها المختلفة.

[1] أناتولى أوتكين، "الإستراتيجية الأمريكية للقرن الحادي والعشرين"، ترجمة: محمد نصر الدين الجبالى وأنور محمد إبراهيم، القاهرة: المجلس الأعلى للثقافة، الطبعة الأولى 2003، ص 268.

وفي أعقاب انتشار نظم الذكاء الاصطناعي التوليدي التي اجتاحت مجمل بقاع العالم، أصبحت مخاطر الاستخدام الخبيث أو التلاعب التي يمكن أن تنتج عنها، مخاطر جسيمة بما تشكله من تهديد، حقيقي وعلى المدى القصير، لحقوق الإنسان وتقويض للديمقراطية ولدولة القانون.

في خضم هذه التحولات، برز التدخل في الانتخابات من خلال توظيف التضليل المعلوماتي والذكاء الاصطناعي كأداتين استراتيجيتين يلجأ إليهما مختلف الفاعلين الدوليين، سواء أكانوا دولا أم فاعلين من غير الدول، وعلى رأسهم الشركات التقنية العابرة للحدود والشبكات الرقمية الانتهازية. وقد رصد تقرير المخاطر العالمية الصادر عن المنتدى الاقتصادي العالمي لعام 2024 ظاهرة المعلومات الخاطئة والتضليل المعلوماتي في الصدارة، بوصفها الخطر الأول الذي يتهدد الاستقرار العالمي على المدى القصير، وهو تصنيف أكده التقرير ذاته للعام 2025.[2]

ولا تقف المملكة المغربية، في سياق انتخاباتها التشريعية المرتقبة في الثالث والعشرين من شتنبر 2026، بمعزل عن هذه الديناميكيات الدولية؛ إذ تجمع فيها عوامل بنيوية تجعلها في قلب مناطق التنافس الدولي: موقعها الجيوسياسي الاستراتيجي بوصفها رابطا محوريا بين أوروبا وإفريقيا، وتوافر مصالح متنافسة لقوى إقليمية ودولية على أراضيها، فضلا عن سياقها الانتخابي الداخلي الذي يتسم بتراجع نسب المشاركة وضعف الثقة في المؤسسات السياسية. ويضاف إلى ذلك أن المغرب نفسه قد اتخذ خطوات تشريعية لتجريم نشر المعلومات المضللة في سياق الانتخابات.

من هذا المنطلق، يطرح هذا المقال الإشكالية الآتية: كيف تُشكّل متغيرات البيئة الدولية وديناميكيات التنافس على النفوذ رهانات الانتخابات المغربية 2026 في ضوء ظاهرة التأثير الخارجي من خلال التضليل المعلوماتي المعزز بالذكاء الاصطناعي؟

ويدور المقال حول ثلاث فرضيات إجرائية:

- كلما اشتد التنافس الدولي على النفوذ في منطقة ما، تصاعد احتمال توظيف العمليات الانتخابية فيها أداة لتحقيق مكاسب نسبية.

[2] رصد التقرير ارتقاء "المعلومات الخاطئة والتضليل المعلوماتي" (Misinformation and disinformation) بسرعة لتحتل المرتبة الأولى في ترتيب المخاطر التي سيواجهها العالم على المدى القصير (أي على مدى العامين المقبلين)، معتبرا إياه محركا لزعزعة الاستقرار الانتخابي، فقد مكنت الواجهات سهلة الاستخدام لنماذج الذكاء الاصطناعي واسعة النطاق بالفعل من حدوث انفجار في المعلومات المزيفة وما يسمى بالمحتوى "الاصطناعي". وقد تواصل هذا الخطر للعام الثاني تواليا. أنظر:

- World Economic Forum (WEF), "Global Risks Report 2024", Switzerland – Geneva: WEF, 19th Edition, 2024. pp. 5, 14-21.
- World Economic Forum (WEF), "Global Risks Report 2025", Switzerland – Geneva: WEF, 2025.

- يجسد الذكاء الاصطناعي التوليدي تحولا نوعيا في بنية تهديدات التضليل المعلوماتي، إذ يخفض تكلفة إنتاج المحتوى المزيف ويرفع مستوى استهدافه.
- يستلزم تعزيز السيادة الانتخابية المغربية في هذا السياق بناء منظومة دفاعية متكاملة تجمع بين المستويين التقني والمؤسسي.

يعالج هذا البحث هذه الإشكالية عبر منهج تحليلي مركب يمزج بين المنهج البنيوي المستمد من الواقعية الجديدة، ومنهج دراسة الحالة المطبق على السياق المغربي، إلى جانب تحليل المضمون للبيانات السياسية والتقارير الدولية ذات الصلة.

بعد ضبط الإطارين النظري والمنهجي وتحديد المفاهيم الرئيسية، تنقسم هذه الدراسة إلى ثلاثة محاور، يبرز أولها تطور آليات التأثير الخارجي في الانتخابات، فيما يلقي المحور الثاني الضوء على الإشكاليات التي واجهتها بعض التجارب الدولية الكبرى والاستجابات التي خلفتها، على أن تتم مقاربة الحالة المغربية واستشراف التدابير الكفيلة ببناء منظومة دفاع انتخابي سيادي.

الإطار النظري والمنهجي

يقع موضوع الدراسة، ألا وهو رهانات الانتخابات المغربية 2026 في مواجهة التهديدات الدولية الهجينة، في تقاطع دوائر متعددة بدءا من الحلقة الأوسع وهي حقل العلوم السياسية وضمنها دائرة العلاقات الدولية.

إن وضع المنهج الملائم لدراسة هذا الموضوع يتطلب استحضار المرجعيات النظرية للظاهرة المدروسة، بالاعتماد على أهم المنظورات المستعملة في حقل العلاقات الدولية في تحليل الموضوع. وهو ما يتصدى له الباحث من خلال استحضاره لمنظور الواقعية الجديدة.

تعد الواقعية الجديدة، ولاسيما الواقعية البنيوية، المنظور الملائم لمقاربة هذا الموضوع، بالنظر إلى كونها تقدم الأدوات اللازمة لتفسير التهديدات الدولية الهجينة موضوع البحث، ذلك أنه يرى العلاقات الدولية من زاوية "الفوضى الدولية" ويتميز بتحليله للبنية النظامية للنظام الدولي بوصفها المحدد الأساسي للسلوك الدولي.[3]

وتقوم هذه المقاربة على ثلاثة مرتكزات تحليلية راسخة: أولها مبدأ الفوضى بوصفه المنطق البنيوي للنظام الدولي، فغياب سلطة عليا فوق الدول يجعل كل وحدة سياسية تنزع نحو تعظيم أمنها الذاتي في مقابل وحدات منافسة؛ وثانيها منطق توازن القوى بوصفه محرك الاستراتيجيات الكبرى،

[3] Kenneth N. WALTZ, "Theory of International Politics", Reading: Addison-Wesley, 1979, pp. 88-99.

فالدول لا تسعى بالضرورة إلى تعظيم القوة المطلقة، بل إلى الحفاظ على وضعها النسبي في التوازن البنيوي للنظام؛[4] أما المرتكز الثالث فهو أولوية المكاسب النسبية على المكاسب المطلقة، وهو ما يفسر منطقيا توظيف الانتخابات الوطنية في دول أخرى أداة لتحقيق مكاسب نسبية في توازن القوى الإقليمي، إذ يعد التأثير في مخرجات الانتخابات ووصول حكومة صديقة أو إضعاف خصم محتمل من أهم أشكال التحسين النسبي لموازين القوى.

وإذا كان الواقعيون الجدد قد تمحور تحليلهم حول ميادين الصراع العسكري والتحالفات الاستراتيجية، فإن تطور مفهوم "الحرب الهجينة" (Hybrid Warfare) وما صاحبه من ثورة في تكنولوجيا المعلومات قد أعادا رسم ميادين التنافس الدولي، حيث باتت العمليات السيبرانية والمعلوماتية جزءا جوهريا من ترسانة الدول في تحسين أوضاعها النسبية.

وإذا كانت الواقعية الكلاسيكية قد ركزت على الوقائع المادية والقوة العسكرية كمرتكزات أساسية في التحليل، متجاهلة البعد الذي تمثله المعلومات وديناميات صناعة المعنى كأدوات لتشكيل الإدراك السياسي، فإن التحولات المعرفية التي جاءت بها المقاربات ما بعد الوضعية دفعت نحو فهم أكثر عمقا لدور السرديات والرؤى والصور في تشكيل السلوك الدولي، مما مهد لتحليل التضليل باعتباره أداة استراتيجية لإعادة تشكيل الإدراك السياسي وصياغة الواقع لصالح الفاعلين الدوليين.[5]

وهكذا يغدو التدخل الخارجي في الانتخابات، من منظور الواقعية الجديدة، شكلا متطورا من أشكال "الموازنة غير المتماثلة" (Asymmetric Balancing)؛ أي توظيف أدوات منخفضة التكلفة نسبيا لتحقيق مكاسب جيوسياسية كبيرة دون الانخراط المباشر في صراع عسكري مكلف. وفي ظل منطق الفوضى الدولية، تجد الدول الساعية إلى تغيير موازين القوى لصالحها حوافز بنيوية قوية للاستثمار في هذه الأدوات الهجينة.

وتكتسب التهديدات الهجينة أهمية تحليلية مضاعفة حين تقاربها الواقعية الجديدة من منظورها البنيوي؛ فهي لا تعدها مجرد أساليب قتالية مستحدثة، بل ترى فيها امتدادا وظيفيا لمنطق التنافس على المكاسب النسبية في نظام دولي يسوده الفوضى البنيوية. فمن منظور "والتز"، توفر التهديدات الهجينة للدول والفواعل المتنافسة أداة "موازنة غير متماثلة" بامتياز: تكاليفها المنخفضة

[4] جون ميرشايمر، "مأساة سياسات القوى العظمى"، ترجمة: مصطفى محمد قاسم، الرياض: جامعة الملك سعود، 2012، ص ص. 27-28.

[5] Anzera GIUSEPPE, Alessandra MASSA, "Using International Relations Theories to Understand Disinformation: Soft Power, Narrative Turns, and New Wars" in "Politics of Disinformation" (eds. Guillermo LÓPEZ-GARCÍA & al.), John WILEY & Sons, 2021, pp. 35–47. doi.org/10.1002/9781119743347.ch3.

نسبيا، وقدرتها على التملص من قواعد المواجهة المباشرة، وإمكانية إنكارها، تجعل منها خيارا استراتيجيا عقلانيا في حسابات الفاعلين الساعين إلى تحسين أوضاعهم في التوازن الجيوسياسي دون استنزاف موارد القوة الصلبة. وإذا أضفنا إلى ذلك ما أتاحه الذكاء الاصطناعي التوليدي من خفض تكلفة إنتاج المحتوى المضلل وتوسيع نطاقه واستهدافه بدقة ديمغرافية غير مسبوقة، تبين لنا أن هذه التهديدات تجمع اليوم بين كفاءة الأداة الاستراتيجية وفاعلية السلاح النفسي، مما يجعل المسارات الانتخابية، بما تنطوي عليه من هشاشة معلوماتية موسمية، هدفا مثاليا في حسابات التنافس الدولي على النفوذ.

الإطار المفاهيمي

يوفر الإطار المفاهيمي لهذه الدراسة إطارا للتفكير في الإشكالية المطروحة، حيث تبرز من خلال هذه الإشكالية بعض المفاهيم الرئيسية التي يتم تحديدها فيما يلي:

✓ مفهوم التهديدات الهجينة (Hybrid Threats)

لا يزال مفهوم التهديدات الهجينة يفتقر إلى تعريف جامع مانع في الأدبيات الأكاديمية للعلاقات الدولية، وهو ما يجعل تحديده المفاهيمي خطوة منهجية لا غنى عنها قبل توظيفه أداة تحليلية. وقد اقترح "فرانك هوفمان" (Frank Hoffman)، الذي يحسب له الفضل في تأصيل هذا المفهوم في عام 2007، تعريفا إجرائيا يحدده بوصفه توظيفا متزامنا ومتكاملا لطيف واسع من الأدوات العسكرية وغير العسكرية من قبل فاعل دولي (دولة كان أم من دون الدول)، بما يعسر الإسناد ويشوش حدود الصراع التقليدية.[6]

وقد استدعت بيئة ما بعد الحرب الباردة توسيع هذا المفهوم، إذ أدرج الاتحاد الأوروبي في وثيقة "الإطار المشترك لمواجهة التهديدات الهجينة" لعام 2016 تعريفا يقوم على دمج الأساليب التقليدية وغير التقليدية بما فيها التضليل المعلوماتي والضغط الاقتصادي والهجمات السيبرانية، في منظومة واحدة متناسقة تستهدف إضعاف إرادة الخصم مع البقاء تحت عتبة الحرب المعلنة رسميا.[7]

ويعرف "مركز التميز للتهديدات الهجينة" في "هلسنكي" التهديدات الهجينة بأنها "أنشطة ضارة يخطط لها وتنفذ بنية خبيثة. وتهدف إلى تقويض كيان مستهدف، كالدولة أو المؤسسة، من خلال

[6] Frank G. HOFFMAN, "Conflict in the 21st century: the rise of hybrid wars", Potomac Institute for Policy Studies, Arlington, Virginia, December 2007, p. 8.

[7] European Commission & High Representative of the Union for Foreign Affairs and Security Policy, "Joint Framework on countering hybrid threats: a European Union response", JOIN(2016) 18 final, 06/04/2016. The "EUR-Lex" website (Accessed: 02/04/2026): t.ly/iRiHz

طائفة متنوعة من الوسائل التي غالبا ما تستخدم بصورة متزامنة ومتكاملة. وتشمل هذه الوسائل التلاعب بالمعلومات، والهجمات السيبرانية، والتأثير الاقتصادي أو الإكراه الاقتصادي، والمناورات السياسية السرية، والدبلوماسية القسرية، أو التهديد باستخدام القوة العسكرية. ويشير مفهوم التهديدات الهجينة إلى نطاق واسع من الأنشطة الضارة ذات الأهداف المتباينة، بدءا من عمليات التأثير والتدخل وصولا إلى الحرب الهجينة."[8]

يقصد بالتهديدات الهجينة، إذن، ذلك النمط من التهديدات التي تتجاوز الحدود التقليدية بين أدوات القوة الصلبة والقوة الناعمة، وتقوم على توظيف متزامن ومتداخل لمجموعة من الوسائل بهدف التأثير في ميزان القوة بين الفاعلين الدوليين دون الاضطرار إلى خوض مواجهة عسكرية مباشرة.

وبالنسبة لخصائصها، يمكن القول بأن التهديدات الهجينة تدور حول أفكار عدم التماثل، وتعددية الأشكال، وعدم المساواة، وعدم المساءلة، والتصعيد، والقدرة على التكيف، وتعددية الأبعاد، والخبث، وعدم قابلية الكشف، والتدريج، والإساءة، والإخفاء، والسرية، والغموض، والانتهازية، وعدم الحزم، والاضطراب، والتلاعب، والتشويه، والإنكار، وعدم القابلية للسيطرة، والمعلومات المضللة، وعدم القانونية، والاغتصاب، واللاأخلاق، وغيرها.[9]

وتعد التهديدات الهجينة، وفقا للواقعية الجديدة، امتدادا طبيعيا لسعي القوى الدولية إلى تحقيق تفوق نسبي عبر استغلال الثغرات البنيوية في بيئة الدولة المستهدفة. وتشمل هذه التهديدات: استخدام الهجمات السيبرانية، وعمليات التأثير الإعلامي، والتضليل المعلوماتي، والضغوط الاقتصادية، وتوظيف الفاعلين غير الحكوميين، والحروب بالوكالة، وهي أدوات تستخدم بطريقة مركبة تهدف إلى إضعاف الدولة الخصم من الداخل، وتقويض ثقة مواطنيها في مؤسساتها، وإرباك قدرتها على اتخاذ قرارات سيادية مستقلة. ومن هذا المنظور، تصبح التهديدات الهجينة تعبيرا عن منطق القوة في النظام الدولي أكثر من كونها ظاهرة عابرة، لأنها تؤشر إلى تحول استراتيجي في طبيعة التنافس الدولي، حيث لم تعد الحروب التقليدية الوسيلة الوحيدة لإعادة تشكيل موازين القوى، بل أصبحت عمليات منخفضة الحدة وعالية التأثير تمارس في مناطق رمادية يصعب ضبطها أو

[8] حول تعريف مركز التميّز للتهديدات الهجينة في هلسنكي (Hybrid CoE) الذي يُعدّ المرجعية الأكثر تداولاً في الأدبيات الأوروبية الراهنة، أنظر:

The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), "Hybrid threats as a concept", the "Hybrid CoE" website (Accessed: 02/04/2026): t.ly/NxPQk

[9] Susana SANZ-CABALLERO, "The Concepts and Laws Applicable to Hybrid Threats, with a Special Focus on Europe", Humanities and Social Sciences Communications, Vol. 10, n° 360, 2023. doi.org/10.1057/s41599-023-01864-y

نسبها إلى فاعل محدد، بما يمنح القوى المؤثرة قدرة أكبر على المناورة وتحقيق مكاسب استراتيجية بتكلفة منخفضة وبتبعات سياسية محدودة.

انطلاقا من هذا التحديد للتهديدات الهجينة، يجدر القول بأن هذا البحث يستند إلى هذا المفهوم بوصفه الإطار التحليلي الأكثر ملاءمة لتشريح طبيعة المخاطر المحيطة بالانتخابات المغربية 2026، انطلاقا من مسوغ نظري وتجريبي موثق في أحدث تقارير دائرة العمل الخارجي الأوروبي (EEAS)، فقد كشفت هذه التقارير أن "التدخل الخارجي والتلاعب بالمعلومات" أو ما يعرف أوروبيا اختصارا بـ "FIMI" (Foreign Information Manipulation and Interference) تحول إلى "سلاح استراتيجي راسخ في صندوق أدوات السياسة الخارجية للجهات التهديدية"، ولا تعمل عمليات التلاعب بمعزل عن غيرها؛ بل تشكل جزءا من ترسانة هجينة أوسع تمزج بين التدخل الرقمي والإشارات الميدانية والأفعال القسرية، وعليه، فإنها لا تمثل تحديا اتصاليا فحسب، وإنما تعد مكونا من استراتيجية أشمل ذات تبعات سياسية وأمنية ملموسة،[10] كما أن الهدف الكامن وراءها لم يعد قاصرا على التأثير في نتيجة انتخابية بعينها، بل انزاح نحو غاية أشمل وأبقى أثرا: زعزعة الثقة في المؤسسات الديمقراطية على كل مستوياتها وتقويض تماسكها الداخلي بوصفها هدفا استراتيجيا بذاتها.[11] ويستدعي هذا التحول في طبيعة الهدف توظيف مفهوم "التهديدات الهجينة" لا مفهوم "التدخل الانتخابي" المتعارف عليه؛ إذ إن الهجينية تعبر بدقة أعلى عن طابع الدمج بين الأدوات العسكرية وغير العسكرية، والتقنية والمعلوماتية والنفسية، في ترسانة موحدة تشتغل في "المنطقة الرمادية" الواقعة بين السلم والحرب. فضلا عن ذلك، يؤطر مفهوم التهديدات الهجينة بما يتيح تفسير الكيفية التي تستغل بها الجهات التهديدية الأزمات الجيوسياسية الكبرى والأحداث العالمية الكبرى منصات لتوسيع نطاق عمليات التضليل بتكلفة منخفضة نسبيا وفاعلية تأثيرية مرتفعة. وهو النمط ذاته الذي يرجح انعكاسه على البيئة الانتخابية المغربية في ظل البيئة الجيوسياسية المتوترة التي تحيط بانتخابات 2026.

[10] The European External Action Service (EEAS), "4th EEAS Report on FIMI Threats: Dismantling the FIMI House of Cards", March 2026. pp. 7-8. The "EEAS" website (Accessed: 07/04/2026): t.ly/-fTLL

[11] Council of Europe Congress, "Foreign Interference in Electoral Processes at Local and Regional Levels", Report CG(2025)48-10, 26 March 2025. p. 10. The "Council of Europe" website (Accessed: 07/04/2026): t.ly/inRlY

✓ مفهوم التضليل المعلوماتي (Disinformation)

يعد هذا المفهوم من أكثر المفاهيم الأكاديمية حضورا في أدبيات الدراسات الأمنية وعلوم الاتصال السياسي في السنوات الأخيرة، غير أنه يظل في الوقت ذاته من أشد المفاهيم عرضة للاستعمال الفضفاض والخلط الاصطلاحي، مما يوجب تأصيلا مفاهيميا.

وتجدر الإشارة بهذا الصدد إلى التأصيل الذي أرساه "كلير واردیل" و"حسين درخشان" (Wardle Derakhshan) للهفي تقريرهما الصادر عام 2017 لحساب مجلس أوروبا والموسوم بـ "اضطراب المعلومات" (Information Disorder)، والذي انتهى إلى نبذ مصطلح "الأخبار الزائفة" (Fake News) بوصفه "غير كاف على نحو مؤسف لوصف الظاهرة المعقدة لتلوث المعلومات"، واستعاض عنه بتصنيف ثلاثي يشكل منذ صدوره المرجعية المفاهيمية الأكثر تداولا في الأدبيات الأكاديمية الدولية والوثائق المؤسسية على حد سواء.[12]

ويقسم هذا التصنيف الثلاثي ظواهر المعلومات الإشكالية إلى ثلاثة أنواع متمايزة وفق معياري الصحة والقصد معا: فـ "المعلومات الخاطئة" (Misinformation) هي معلومات كاذبة يروج لها دون قصد الإضرار، يقع فيها الناشر عادة ضحية للوهم لا شريكا في التدليس؛ أما "التضليل المعلوماتي" (Disinformation)فهو المعلومات الكاذبة أو المشوهة المنتجة والمنشورة بقصد إيقاع الضرر السياسي أو المالي أو المؤسسي أو الاجتماعي، وهو بذلك ينطوي على فاعلية إرادية محددة تفرق بين الخطأ والتضليل المتعمد؛ في حين تمثل "الإساءة المعلوماتية" (Malinformation) النوع الثالث وهي المعلومات الصحيحة في ذاتها، لكنها تستخدم بنية الإضرار عبر نقلها من دائرة الخصوصية إلى الفضاء العام، على نحو ما كشفه تسريب رسائل حملة "هيلاري كلينتون" الانتخابية في 2016.[13]

وإذا كان هذا التصنيف الثلاثي يتيح الدقة التحليلية على مستوى الفئات المفاهيمية، فإن الإشكالية المنهجية الجوهرية تكمن في صعوبة التطبيق الإجرائي؛ إذ يرى باحثون متخصصون كـ "تيم هايوارد" (Tim HAYWARD) أن الفصل بين التضليل المعلوماتي والمعلومات الخاطئة يستلزم توافر ثلاثة أطر معرفية متزامنة: إطار إبستيمولوجي للتحقق من زيف الادعاء، وإطار سلوكي لرصد

[12] Claire WARDLE, Hossein DERAKHSHAN, "Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking", Council of Europe Report DGI(2017)09, Strasbourg: Council of Europe, October 2017, pp. 5, 20. The "Council of Europe" website (Accessed: 05/04/2026): t.ly/URE1N

[13] ibid., pp. 5-6.

التنسيق المقصود في نشره، وإطار أمني لتحديد المخاطر المترتبة على انتشاره، وهذا التزامن التحليلي نادرا ما يكون متاحا في الزمن الفعلي لجريان الأزمة المعلوماتية.[14]

وقد أضافت دراسة نشرت في مجلة "Science" عام 2018، بعدا تجريبيا حاسما لفهم التضليل المعلوماتي، إذ كشفت أن الأخبار الزائفة تنتشر بصورة أوسع وأسرع وأعمق وأشمل من الأخبار الصحيحة في جميع التصنيفات المعلوماتية، وأن هذه الهوة تبلغ ذروتها في المحتوى السياسي المزيف دون سواه.[15] ويضيف هذا الاكتشاف التجريبي عمقا تفسيريا بالغا إلى فهم آليات اشتغال التضليل: فليس صدفة أن يكون المحتوى السياسي الأكثر تداولا هو الأكثر زيفا، إذ تحرك المعلومات المبتكرة والمفاجئة الاستجابات العاطفية كالخوف والاشمئزاز والصدمة بما يدفع إلى مشاركتها فيروسيا قبل أي تمحيص نقدي.

ومن منظور العلاقات الدولية تحديداً، يكتسب التضليل المعلوماتي بعدا استراتيجيا يتخطى دلالاته الاتصالية، إذ بات يوظف بوصفه "سلاحا جيوسياسيا" (Geopolitical Weapon) في يد الدول والفاعلين من غير الدول لتحقيق أهداف استراتيجية بكلفة أمنية ودبلوماسية منخفضة وبمستوى مرتفع من الإنكار المعقول.[16]

وتكشف ظاهرة التضليل المعلوماتي عن تآكل بنيوي حقيقي في الضمانات المؤسسية التقليدية، التي كانت تحصن المجتمعات، في العصر الرقمي، في ظل جهل مستمر بحدود الهشاشة الفردية والمؤسسية والمجتمعية أمام تدخل الفاعلين الخبيثين.[17] وفي هذا السياق، يصنف تقرير المخاطر العالمية للمنتدى الاقتصادي العالمي لعام 2024 ظاهرة التضليل المعلوماتي والمعلومات الخاطئة خطرا أول على الاستقرار العالمي على مدى سنتين، محددا بشكل خاص ارتباطها الوثيق بالانتخابات الكبرى في أكثر من دولة حول العالم، مما يرسخ وضعها بوصفها تهديدا بنيويا في منظومة المخاطر الدولية المعاصرة.[18]

---

[14] Tim HAYWARD, "The Problem of Disinformation: A Critical Approach", Social Epistemology, Vol. 39, No. 1, 2024, pp. 1-23. doi.org/10.1080/02691728.2024.2346127

[15] اعتمدت هذه الدراسة على تحليل أكثر من 126 ألف قصة منتشرة شارك في تداولها قرابة ثلاثة ملايين مستخدم، عبر منصة تويتر، من 2006 إلى 2017. أنظر:

Soroush VOSOUGHI, Deb ROY, Sinan ARAL, "The Spread of True and False News Online", Science, Vol. 359, No. 6380, March 9, 2018, pp. 1146-1151. doi: 10.1126/science.aap9559

[16] Christina NEMR, William GANGWARE, "Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age", Washington D.C.: Park Advisors, March 2019, pp. 1-3.

[17] David LAZER & al., "The Science of Fake News", Science, Vol. 359, No. 6380, March 9, 2018, pp. 1094-1096. doi: 10.1126/science.aao2998.

[18] World Economic Forum (WEF), "Global Risks Report ", 2024 & 2025, op. cit..

وعلى ضوء هذا التأصيل، يمكن تعريف التضليل المعلوماتي، إجرائيا لأغراض هذه الدراسة، بأنه كل فعل متعمد ومنظم لإنتاج معلومات كاذبة أو مشوهة أو منتزعة من سياقها، وتوزيعها بأساليب موجهة تستهدف التأثير في المعتقدات أو السلوك الانتخابي أو الثقة المؤسسية للجماعات، في خدمة أهداف سياسية أو جيوسياسية محددة. وتتمايز هذه الفاعلية التضليلية عن مجرد "الأخبار الخاطئة" العفوية بثلاثة معايير تحليلية جوهرية متكاملة: قصدية الإضرار، والتنسيق المنهجي في الإنتاج والتوزيع، والغاية الاستراتيجية التي تحرك العملية برمتها.

✓ مفهوم الذكاء الاصطناعي (Artificial Intelligence)

بالرغم من تعدد التعاريف التي أعطيت للذكاء الاصطناعي، فإن العديد من الباحثين يعتبرون بأن تعريف "جون مكارثي" وزملائه لهذا المفهوم في عام 1956 لازال يقدم العناصر الأساسية للذكاء الاصطناعي إلى الآن.[19] من وجهة نظر "مكارثي" وزملائه، كان الذكاء الاصطناعي يهدف في البداية إلى محاكاة كل واحدة من قدرات الذكاء المختلفة، بواسطة الآلات. وقد استند هذا النظام العلمي أساسا إلى افتراض أن جميع الوظائف المعرفية، ولاسيما التعلّم، والاستدلال، والحساب، والإدراك، والحفظ في الذاكرة، وحتى الاكتشاف العلمي أو الإبداع الفني، قابلة لوصف دقيق لدرجة أنه يمكن بناء آلة لمحاكاتها.[20]

ومع تطور المجال وتنوعه على مدى العقود التالية، زاد عدد المعاني المعطاة للذكاء الاصطناعي، ولا يوجد حاليا تعريف متفق عليه عالميا. وترتبط التعريفات المختلفة باختلاف المقتربات والحقول المعرفية التخصصية مثل علوم الحاسوب والهندسة الكهربائية وعلم الروبوتات وعلم النفس والفلسفة...[21]

وتعرف المادة 2 من "الاتفاقية-الإطار لمجلس أوروبا بشأن الذكاء الاصطناعي وحقوق الإنسان والديمقراطية ودولة القانون" أنظمة الذكاء الاصطناعي بأنها "أنظمة مؤتمتة تستنتج، لأغراض صريحة أو ضمنية، من المدخلات المستلمة، كيفية توليد نواتج مثل التنبؤات أو المحتوى أو التوصيات أو القرارات التي قد تؤثر على البيئات المادية أو الافتراضية. وتتمتع هذه الأنظمة المختلفة للذكاء

---

[19] Jaemin LEE, "Artificial Intelligence and International Law", Singapore: Springer Nature, 2022, p. 6.

[20] جان-غابريال غاناسيا، "الذكاء الاصطناعي: بين الأسطورة والواقع"، 2018/06/29، موقع "اليونسكو" على الإنترنت (آخر ولوج: 2026/04/05): t.ly/uSz_g

[21] The World Commission on the Ethics of Scientific Knowledge and Technology (COMEST), "Preliminary study on the ethics of Artificial Intelligence", 26/02/2019, p. 5. The "UNESCO Digital library" website (Accessed: 05/04/2026): t.ly/0CQaq

الاصطناعي بدرجات متفاوتة من الاستقلالية والقدرة على التكيف بعد دخولها الخدمة." وهو تقريبا نفس التعريف الذي تبناه قانون الذكاء الاصطناعي للاتحاد الأوروبي.

وبالنظر لما قد تنشأ عن توظيف أنظمة الذكاء الاصطناعي من أنماط مستجدة من التهديدات الهجينة، قد تتسبب في الإضرار بحقوق الإنسان، وتقويض سلامة العمليات الديمقراطية، وإضعاف مقتضيات دولة القانون، فقد حرص المجتمع الدولي على تطوير قواعد القانون الدولي التي تستهدف تحصين المجال الحقوقي والديمقراطي، وتدخل في هذا الإطار الاتفاقية-الإطار لمجلس أوروبا بشأن الذكاء الاصطناعي وحقوق الإنسان والديمقراطية ودولة القانون.

المبحث الأول: تطور آليات التأثير الخارجي في الانتخابات

لا يعد التأثير الخارجي في الانتخابات ظاهرة وليدة عصر الإنترنت، فقد رصدت جذوره في الحرب الباردة حين تنافست الولايات المتحدة والاتحاد السوفياتي على التأثير في انتخابات دول العالم الثالث.[22] بيد أن ما يميز الظاهرة في طورها الراهن هو التحول النوعي الذي أحدثته تكنولوجيا المعلومات؛ فبعد أن كانت تكلفة التأثير الخارجي مرتفعة وأدواته محدودة (التمويل السري، الدعاية التقليدية، شراء الأصوات...)، أصبح بمقدور جهات متعددة وبتكلفة منخفضة نسبيا التأثير في مشاعر ملايين الناخبين عبر أدوات رقمية متطورة.

يميز مجتمع الاستخبارات في الولايات المتحدة الأمريكية تمييزا جوهريا بين نمطين من الأنشطة الأجنبية[23]:

- **التأثير الانتخابي(Election Influence)**: وهو مفهوم واسع يشمل طيفا متنوعا من الأنشطة، العلنية والسرية على السواء، التي يُقصد بها التأثير في العملية الانتخابية، بما في ذلك توجيه تفضيلات الناخبين أو التأثير في المرشحين والأحزاب السياسية.
- **التدخل الانتخابي(Election Interference)**: وهو فئة أكثر تحديدا تندرج ضمن التأثير الانتخابي، وتستهدف الجوانب التقنية للعملية الانتخابية ذاتها، مثل أنظمة تسجيل الناخبين، وإجراءات الاقتراع، وفرز الأصوات، أو الإعلان عن النتائج.

[22] Dov H. LEVIN, "When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results". International Studies Quarterly, Vol. 60, Nº. 2, 2016, pp. 189–202. doi.org/10.1093/isq/sqv016

[23] "How the US Protects Elections from Foreign Interference", 01/09/2025, The "GovFacts" website (Accessed: 07/04/2026): t.ly/4G6a7

وتتوزع آليات التدخل الخارجي في السياق الانتخابي المعاصر على ثلاثة محاور وظيفية متكاملة، تميز بينها الأدبيات الأكاديمية المتخصصة:[24]

1. **محور الاستهداف المعلوماتي:** أي التأثير على بنية المعلومات والخطاب العام، ويشمل حملات التضليل المدارة عبر ربوتات وحسابات مزيفة على شبكات التواصل الاجتماعي، وصولا إلى توظيف تقنيات التزييف العميق (Deepfakes)؛

2. **ومحور الاستهداف المؤسسي:** أي التأثير على البنية التحتية الانتخابية عبر الهجمات السيبرانية، وهو الذي يستهدف البنية التحتية الانتخابية من خلال الهجمات السيبرانية على أنظمة التسجيل الانتخابي وقواعد البيانات؛

3. **ومحور الاستهداف التمويلي:** أي التمويل الأجنبي غير المشروع للأحزاب والمرشحين، والذي يسلك مسارات خفية (ما يعرف بـ "التزييف المصطنع للدعم الشعبي" أو "حرب الرأي العام المصطنع" "Astroturfing"...).[25]

وقد حذر تقرير مجلس أوروبا المتعلق بالتدخل الخارجي في الانتخابات المحلية والإقليمية من أن تطور التكنولوجيا والتوترات الجيوسياسية قد ضاعفت النطاق والتعقيد وعدد الفاعلين في هذه العمليات، مما يجعل الإسناد (Attribution) أكثر صعوبة من أي وقت مضى.[26]

انطلاقا من هذا الرصد لتطور آليات التأثير الخارجي في السياق الانتخابي المعاصر يمكن الوقوف على أداتين تشكلان ثورة في بيئة التهديدات الانتخابية: التضليل المعلوماتي والذكاء الاصطناعي.

المطلب الأول: التضليل المعلوماتي بوصفه سلاحاً جيوسياسياً

تحول التضليل المعلوماتي في السياق الجيوسياسي الراهن إلى سلاح استراتيجي دقيق يوظفه الفاعلون الدوليون، دولا كانوا أم شبكات منظمة، في خدمة أهداف جيوسياسية محددة، تتصدرها المؤسسات الديمقراطية والعمليات الانتخابية بوصفها أهدافا ذات مردود استراتيجي مضاعف. وفي هذا الإطار، تجادل الأدبيات المتخصصة بأن حملات التضليل المعلوماتي ذات الطابع الانتخابي تنطوي على هدفين متكاملين: هدف مباشر وآني يتمثّل في التأثير على اختيارات الناخبين وتوجيه سلوكهم

[24] Council of Europe Congress, op. cit.

[25] يقصد بالتزييف المصطنع للدعم الشعبي (Astroturfing) ممارسة اتصالية مضللة تخفى فيها الجهة الحقيقية الراعية للرسالة أو الحملة، مع تقديمها زيفا بوصفها تعبيرا عفويا عن دعم شعبي واسع. بموجبه تتم صناعة دعم شعبي زائف لقضية، أو سياسة، أو مرشح، أو منتج، بحيث يبدو الأمر وكأنه حراك شعبي عفوي (grassroots)، بينما يكون في الحقيقة منظما وممولا وموجها من جهة خفية مثل منظمة غير حكومية أو شركة أو جماعة ضغط أو حملة سياسية أو جهة دعائية.

[26] Council of Europe Congress, op. cit., par. b.

التصويتي نحو نتيجة بعينها، وهدف بعيد المدى وأعمق أثرا يتجلى في تآكل الثقة المجتمعية في العملية الانتخابية ذاتها وفي المؤسسات الديمقراطية الضامنة لها، وهو ما يترجم، في ضوء المنظور الواقعي الجديد، مكاسب نسبية مضاعفة للجهة المدبرة لتلك الحملات، إذ يكفيها الإضرار بالشرعية المؤسسية للخصم حتى حين يتعذر عليها تغيير نتيجة الاقتراع.

إن هذا التوجه الاستراتيجي ليس بالشيء الجديد، وتجدر الإشارة بهذا الصدد على سبيل المثال إلى المنظور الروسي للحرب المعلوماتية الذي يرجع عمره إلى قرن كامل، ويرفض أصلا الفصل المفاهيمي الغربي التقليدي بين الصراع العسكري والمنافسة السياسية-المعلوماتية؛ إذ يقوم على مسلّمة مفادها أن العنصر النفسي للصراع لا يقل في أهميته عن عنصره المادي، بل قد يتجاوزه في بعض الأحيان. ومن هذا المنطلق، فإن الاستراتيجيين الروس، وعلى خلفية الصراع حول تصورات النظام الدولي، يحثون على اتخاذ إجراءات تهدف في مرماها الأبعد إلى حرمان الخصوم من التماسك السياسي الداخلي اللازم للعمل بفاعلية على الصعيد الخارجي، وهو ما يجعل المجال السيبراني والفضاء المعلوماتي الرقمي بيئة طبيعية لتوسيع هذه الأنشطة واستثمار قابليتها للتخفي والإنكار، حيث يتيح ذلك الفضاء مجالا رحبا لبث الأفكار الهدامة وإثارة الانقسامات داخل الدولة المستهدفة عن بعد وبصورة فورية، في ظل توافر هامش من الإنكار يسمح بنفي التدخل في شؤون الخصم الداخلية.[27]

وقد أسهمت التحولات التكنولوجية العميقة المصاحبة للعولمة في إعادة رسم معادلات القوة الدولية ذاتها؛ إذ انتقل النظام الدولي نحو نموذج قوة معرفية-تكنولوجية متعددة المراكز، لم يعد فيه النفوذ محكوما بالقوة الصلبة وحدها. وفي هذا الإطار، يعاد توظيف مفهوم "القوة الناعمة" الذي صاغه جوزيف ناي (Joseph Nye) توظيفا هجوميا؛ إذ تتداخل حملات التضليل المعلوماتي مع الدعاية في شكلها المعاصر لتشكل أداة لتوجيه الرأي العام وإعادة هيكلة إدراك الخصوم والحلفاء على حد سواء، ليشمل الاستهداف الرقمي الدقيق منظومة المعتقدات السياسية للجمهور الأجنبي.[28]

---

[27] Lucas KELLO, "The virtual weapon : and international order", New Haven CT: Yale University Press, 2017, pp. 227-228.

ولتفاصل أكثر بهذا الشأن، أنظر أيضا مؤلف "توماس ريد" أسفله الذي يقدم تأريخا شاملا لتوظيف التضليل أداة استراتيجية من مرحلة الحرب الباردة، التي تطورت خلالها ما عرفت سوفياتيا باسم "الإجراءات النشطة" (active measures) وهي تشمل التضليل، والتأثير السياسي، واستخدام الواجهات والمنظمات الأمامية، والعمل السري لتشويه الخصوم أو إضعافهم، وصولا إلى مرحلة العمليات الرقمية المعاصرة، مبينا استمرارية العقيدة الروسية في نفي التدخل عبر الاستعانة بوسطاء محليين وشبكات موزعة.

Thomas RID, "Active Measures: The Secret History of Disinformation and Political Warfare", New York: Farrar, Straus and Giroux, 2020, pp. 3-18.

[28] أنظر:

=

وفي قلب هذه الديناميكية الجديدة تقع المنصات الرقمية الكبرى بوصفها فضاءات جيوسياسية مستقلة؛ فهي تعيد إنتاج علاقات القوة عبر آليات الإظهار والإخفاء والتحكم الخوارزمي، وتشكل البيئة الرمزية التي تدار فيها النقاشات العامة وتصنع فيها القناعات السياسية. وقد باتت "جيوسياسية المنصات" امتدادا وظيفيا للجيوسياسات التقليدية، توظّف فيها الدول قدراتها الرقمية، عبر الجيوش الإلكترونية والشبكات الآلية وبرامج التحليل الضخم للبيانات، لتعظيم نفوذها أو إرباك خصومها، مستغلة قابلية الفضاء المعلوماتي للتلاعب المتخفي والإنكار المعقول في آن واحد. وتبين الدراسات التحليلية أن الفاعلين الدوليين الساعين إلى توظيف التضليل سلاحا جيوسياسيا يعمدون تحديدا إلى توظيف فاعلين محليين وسطاء لإخفاء مصدر الرسائل الموجهة وإضفاء الطابع الأصيل والمحلي على المحتوى المنتج خارجيا، مما يعقد عملية الإسناد ويطيل أمد الانتشار الفيروسي للتضليل قبل الكشف عنه.[29]

المطلب الثاني: الذكاء الاصطناعي كعامل مضاعف في بنية التهديدات الانتخابية

إذا كانت التهديدات المعلوماتية الموجهة نحو العمليات الانتخابية تشكل ظاهرة راسخة في الأدبيات الأمنية المعاصرة، فإن دخول الذكاء الاصطناعي التوليدي (Generative AI) على خط هذه المعادلة لم يضف إليها تهديدا جديدا من حيث الجوهر، بقدر ما منحها قدرا غير مسبوق من القوة التسريعية والتكثيرية والانتشارية؛ فمن جهة أولى، نبّه مجلس أوروبا في تقريره الصادر عام 2025 المتعلق بالتدخل الخارجي في العمليات الانتخابية على المستويين المحلي والإقليمي إلى هذه الإشكالية، معترفا بأن الذكاء الاصطناعي "قد يمثل عاملا مضاعِفا محتملا" في منظومة التهديدات الانتخابية؛[30] ومن جهة أخرى، نبه التقرير السنوي الرابع لدائرة العمل الخارجي الأوروبي(EEAS) حول تهديدات التدخل الخارجي والتلاعب بالمعلومات(FIMI) الصادر عام 2026 بأن "الذكاء الاصطناعي يسرع عمليات (FIMI) بشكل متزايد، مما يجعلها أرخص وأسهل في التوسع".[31]

- Joseph S. NYE, "The Future of Power", New York: PublicAffairs, 2011, pp. 113-127.
- Joseph S. NYE, "How Sharp Power Threatens Soft Power", Foreign Affairs, 24/01/2018. The "Foreign Affairs" website (Accessed: 05/04/2026): t.ly/Hp-7F

[29] Christina NEMR, William GANGWARE, op. cit., pp. 1-3.

[30] ينبه التقرير بصراحة إلى ضرورة عدم المبالغة في التهويل المعلوماتي حول هذه المخاطر، مع الإقرار الصريح بالطابع المضاعِف المحتمل للذكاء الاصطناعي في بنية التهديدات الانتخابية. أنظر: Council of Europe Congress, op. cit., para. (c).

[31] EEAS, "4th EEAS Report on FIMI Threats: Dismantling the FIMI House of Cards", op. cit., p. 7.

يشكل الذكاء الاصطناعي، من هذا المنطلق، "سلاحا" جديدا تستخدمه الدول، ولكن أيضا جهات دولية أخرى، للتأثير على القضايا العالمية ومنها الانتخابات، وفقا لمصالحها من خلال إنشاء دعاية مستهدفة، أو تحليل البيانات المجمعة بكميات كبيرة، أو التلاعب بالفيديوهات... حيث يوفر الذكاء الاصطناعي إمكانية تحليل سلوكيات البشر ومزاجهم ومعتقداتهم بناء على البيانات المتاحة. إن الاستخدام الخبيث للذكاء الاصطناعي يدفعنا للتفكير في أحد أهم التأثيرات السلبية، خاصة التحول من الديمقراطية إلى الدكتاتورية.[32]

وتتجلى قدرات هذه التقنية على وجه التحديد في ثلاثة أبعاد بنيوية متمايزة ومتضافرة:

✓ خفض تكلفة إنتاج المحتوى المضلل وتوسيع نطاقه

يتمثل البعد الأول في تحول الذكاء الاصطناعي التوليدي إلى أداة للإنتاج الضخم للمحتوى المضلل بتكلفة تكاد تكون صفرية مقارنة بالأساليب التقليدية، بعد أن ظلت عقبة التكلفة المرتفعة لإنتاج المحتوى المزيف أحد أبرز العوامل المحبطة لجهات التضليل ذات الإمكانات المحدودة. لقد أتاحت نماذج اللغة الكبيرة (LLMs) وأدوات توليد الصور والصوت إنتاج كميات هائلة من المحتوى المضلل الموجه بدقة، وبتكلفة ضئيلة.[33]

وقد كشف تقرير صادر في أكتوبر 2025 أن المحتوى المولد بواسطة الذكاء الاصطناعي قد تجاوز من حيث الكم المحتوى المنتج بشريا بحلول نونبر 2024، ليبلغ نسبة 52% في مايو 2025.[34]

كما رصدت دراسة أكاديمية نشرت عام 2025 حول انتخابات البرلمان الأوروبي 2024، التي اعتبرت "ساحة اختبارية" لتهديدات الذكاء الاصطناعي الانتخابية، أن التعرض المبلغ عنه لمحتوى التضليل المولد بالذكاء الاصطناعي بلغ ذروته قبيل يوم الاقتراع مباشرة، مما يوحي بتوقيت استراتيجي محكم في نشره، وارتبط بتآكل ملحوظ في تصور المواطنين لنزاهة العملية الانتخابية.[35]

---

[32] Fatima ROUMATE, "Artificial Intelligence and the New World Order, New weapons, New Wars and a New Balance of Power", Switzerland: The Springer, 2024. p. 112.

[33] EEAS, "4th EEAS Report on FIMI Threats: Dismantling the FIMI House of Cards", op. cit., p. 7.

[34] European Parliament Research Service (EPRS), "Information Manipulation in the Age of Generative Artificial Intelligence", Briefing PE 779.259, Brussels: European Parliament, December 2025, p. 4. The "European Parliament" website (Accessed: 05/04/2026): t.ly/LKRnB

[35] Farooq AQSA & al., "Generative AI Generating Concerns: Citizens' Perspectives During the 2024 European Elections", The International Journal of Press/Politics, 2025. doi.org/10.1177/19401612251376060

✓ ظاهرة التزييف العميق وأزمة الثقة المعرفية

أما البعد الثاني فيكمن في ظاهرة التزييف العميق (Deepfakes) بوصفها الشكل الأكثر خطورة لتوظيف الذكاء الاصطناعي في السياقات الانتخابية؛ إذ أصبح بمقدور هذه التقنية توليد مقاطع مرئية ومسموعة لشخصيات سياسية حقيقية تبلغ من الإتقان مستوى لا يتمكن معه المتلقي العادي من تمييزها.

تولد تقنيات التزييف العميق إذن محتوى يبلغ من الواقعية مستوى يعجز عن تمييزه، مما يفضي إلى ما يسمى بـ "أزمة الثقة المعرفية" (Epistemic Crisis)؛ أي عجز الأفراد عن التمييز بين ما هو صحيح وما هو مزيف. وهو ما توثقه العديد من الحالات الدولية المقارنة التي تظهر حجم هذا الخطر بصورة ملموسة.[36]

وتحمل هذه الأزمة في طياتها خطرا مضاعفا، ليس فقط بسبب تصديق الزائف، بل أيضا بسبب الشك في الصحيح، حيث أن انتشار الوعي بوجود تقنيات التزييف ذاته يفضي إلى زعزعة الثقة في المحتوى الأصيل الموثوق بموازاة انتشار المزيف، مما يضاعف المكسب الاستراتيجي للجهات الموظفة لهذه التقنية.[37]

وقد كشف تقرير صدر في عام 2023 عن "حالة الوسائط المزيفة العميقة" أن محتوى فيديو التزييف العميق تضاعف على المستوى العالمي بنسبة تجاوزت 550% على الإنترنت منذ عام 2019.[38]

✓ الجيوش الإلكترونية والاستهداف النفسي-الانتخابي الدقيق في حرب "الرأي العام المصطنع"

يتجلى البعد الثالث في قدرة الذكاء الاصطناعي على الاستهداف النفسي-الانتخابي الدقيق؛ إذ تتيح نماذج اللغة الكبيرة (LLMs) إنتاج رسائل سياسية مصممة لاستهداف شرائح ديمغرافية بعينها برنين عاطفي مرتفع ولغة تنتمي إلى بيئتها الثقافية والاجتماعية المحلية، مما يخفي الطابع الخارجي لمصدر هذه الرسائل ويعزز تقبلها. وهذا ما دفع إلى التحذير من أن الأثر التراكمي لهذا القصف

[36] Raluca CSERNATONI, "Can Democracy Survive the Disruptive Power of AI?", 18/12/2024. The "Carnegie Endowment for International Peace (CEIP)" website (Accessed: 02/04/2026): t.ly/nhK-T

[37] Robert CHESNEY, Danielle CITRON, "Deep Fakes: A Looming Challenge for Privacy, Democracy and National Security", California Law Review, Vol. 107, 2019, pp. 1785-1786. doi.org/10.15779/Z38RV0D15J

[38] European Parliament Research Service (EPRS), op. cit., p. 4.

المعلوماتي الموجه بالذكاء الاصطناعي سيتجلى في تضخيم ارتباك الناخبين وتأجيج الشك تجاه العملية الانتخابية برمتها، حتى حين لا يتمكن من تغيير نتيجة الاقتراع بصورة مباشرة.[39]

وتعتمد الجهات المتدخلة بشكل متصاعد على شبكات حسابات آلية (Bots) وحسابات بشرية مدارة مركزيا لخلق وهم التوافق الاجتماعي حول قضايا ومرشحين بعينهم، وهو ما يعرف بـ "حرب الرأي العام المصطنع" (Astroturfing). وقد وظف هذا الأسلوب بصورة ممنهجة من طرف فريق "وكالة أبحاث الإنترنت"("IRA" Internet Research Agency) الروسي، الذي راكم خبرات تشغيلية متقدمة أفضت إلى عمليات تدخل موثقة في انتخابات أمريكية وأوروبية متعددة، جمعت بين الإعلانات الموجهة وإنتاج محتوى انقسامي محرض وتوزيعه عبر شبكات حسابات مزيفة تحاكي هوية المواطن المحلي الأصيل، وهو ما نبهت إليه تقارير لجنة الاستخبارات في مجلس الشيوخ الأمريكي وتحقيق المدعي الخاص "روبرت مولر" (Robert Mueller) على حد سواء.[40] ولا تقتصر خطورة (Astroturfing) على تأثيره المباشر في الرأي العام، بل تمتد إلى تأثيره الثانوي العميق المتمثل في زعزعة الثقة الاجتماعية في الخطاب الرقمي برمته؛ إذ حين يدرك المواطنون أن ما يبدو إجماعا شعبيا قد يكون مصطنعا، تتآكل قدرتهم على الاستناد إلى الفضاء الرقمي مرجعا موثوقا لقياس المزاج العام، وهو تآكل يربك ليس الناخبين وحدهم بل الأحزاب والمؤسسات المعنية بتفسير الرأي العام أيضا.[41]

وفي ضوء هذه المعطيات، يبرز مفهوم "التأثير الفيروسي المتأخر" (Delayed Viral Impact) بوصفه الإشكالية المنهجية الأعمق في مواجهة الذكاء الاصطناعي في السياقات الانتخابية، فالمحتوى المزيف الذي ينشر قبيل يوم الاقتراع مباشرة يشكل تهديدا استراتيجيا بالغا لأنه يفاجئ المنظومة

---

[39] Raluca CSERNATONI, op. cit.

[40] وثّق تقرير لجنة الاستخبارات قيام وكالة أبحاث الإنترنت (IRA) بخلق وإدارة صفحات اجتماعية وهمية وإعلانات موجهة استقطبت عشرات الملايين من التفاعلات الأمريكية. أنظر:

- U.S. Senate Select Committee on Intelligence (SSCI), "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election", Vol. 2: Russia's Use of Social Media, Washington D.C.: SSCI, 18/08/2020, pp. 4-11. The "SSCI" website (Accessed: 05/04/2026): t.ly/xXgjG

- Robert S. Mueller III, "Report on the Investigation into Russian Interference in the 2016 Presidential Election", Vol. I, Washington D.C.: U.S. Department of Justice, March 2019, pp. 14-35. The "U.S. Department of Justice" website (Accessed: 05/04/2026): t.ly/cSTiB

[41] Jon ROOZENBEEK & al., "Susceptibility to Misinformation about COVID-19 Around the World", Royal Society Open Science, Vol. 7, N°. 10, 2020.

الدفاعية في أضيق نوافذ الاستجابة الزمنية، وهو ما يرسخ الحاجة إلى استراتيجيات استباقية لا استجابية في منظومة الدفاع الانتخابي، وهي ثغرة تحتاج إلى إجابة سياسية وتقنية متكاملة سواء في التجارب الدولية الكبرى أو في الحالة المغربية استعدادا لاستحقاق شتنبر 2026.[42]

المبحث الثاني: بعض التجارب الدولية الكبرى: إشكالياتها وتدابير الاستجابة لها

باتت ظاهرة التدخل الخارجي في الانتخابات تشكل ركيزة تحليلية مركزية في أدبيات العلاقات الدولية المعاصرة؛ إذ تتقاطع فيها أسئلة السيادة والأمن والديمقراطية في آنٍ واحد. ولا يجوز تناول الرهانات الانتخابية المغربية في معزل عن هذا السياق الدولي المثبت، بل ينبغي قراءتها في ضوء ما كشفته التجارب الدولية الرائدة من إشكاليات وثغرات وما استجابت به من تشريعات ومنظومات دفاعية. وفيما يلي عرض وتحليل لتجربتين محوريتين: التجربة الأمريكية والتجربة الأوروبية.

المطلب الأول: التجربة الأمريكية: من صدمة 2016 إلى المنظومة المؤسسية لمكافحة التدخل

مثل التدخل الأجنبي في الانتخابات الرئاسية الأمريكية 2016 صدمة استراتيجية دفعت الحكومة الأمريكية إلى إعادة هيكلة جهاز أمن الانتخابات كليا. وقد شكلت الاستجابة الأمريكية لهذه الصدمة 2016 نموذجا مؤسسيا للتحول من منطق التفاعل إلى منطق البناء الهيكلي المنظم.

✓ صدمة التدخل الروسي في انتخابات 2016

شكلت انتخابات الرئاسة الأمريكية لعام 2016 نقطة تحول فارقة في فهم مخاطر التدخل الخارجي في العمليات الديمقراطية؛ إذ كشفت تحقيقات المدعي العام "روبرت مولر" (Mueller Robert)، الذي تم تصنيفه مستشارا مختصا (Special Counsel) في هذه القضية، عن عملية تدخل روسية ممنهجة تجمعت فيها أربعة محاور رئيسية: اختراق البنية التحتية الانتخابية عبر اختراق أجهزة الانتخابات في عدد من الولايات؛ وعمليات التأثير المعلوماتي التي نفّذتها "وكالة أبحاث الإنترنت" عبر إنشاء شبكة هائلة من الحسابات الزائفة؛ وسرقة وتسريب وثائق حملة هيلاري كلينتون؛ وحملات الاستقطاب الاجتماعي التي استهدفت تعميق الانقسامات القائمة أصلاً داخل المجتمع الأمريكي. وقد أكد تقرير لجنة الاستخبارات في مجلس الشيوخ (2020) أن العملية الروسية "سعت إلى استقطاب الأمريكيين على أسس مجتمعية وعقدية وعرقية، واستفزّت أحداثا حقيقية، وكانت جزءا من دعم سري لمرشح روسيا المفضل".[43]

[42] Farooq AQSA & al., op. cit..

[43] U.S. Senate Select Committee on Intelligence (SSCI), op. cit., pp. 4-11.

✓ الاستجابة المؤسسية الأمريكية وإعادة هيكلة منظومة الأمن الانتخابي

شكل التوجيه الرئاسي "PPD-41" الصادر في 26 يوليوز 2016 نقطة ارتكاز مبكرة في إعادة بناء الاستجابة الأمريكية تجاه التهديدات ذات الطابع السيبراني، وأسهم، من خلال وضع إطار منسق للجهود الفدرالية في مجالات التحقيق، والدعم التقني، والدعم الاستخباراتي، في تأسيس البنية التنظيمية التي اعتمدت عليها الولايات المتحدة لاحقا لمواجهة التدخل الأجنبي في العمليات الانتخابية.[44] فقد أوجدت الوثيقة هندسة تنسيقية واضحة عبر "فريق التنسيق الموحد السيبراني" وتحديد الوكالات القائدة، الأمر الذي وفر قاعدة تنظيمية يمكن البناء عليها في أعقاب تدخلات 2016، حين انتقل تركيز الحكومة إلى بلورة منظومة أمن انتخابي متخصصة. ومن هذا المنطلق، يعد التوجيه الرئاسي "PPD-41" حلقة تأسيسية في تطور الاستجابة المؤسسية الأمريكية، إذ مهدت لمرحلة ما بعد 2016 التي شهدت تعزيز سلطات وزارة الأمن الداخلي، وإنشاء وكالة الأمن السيبراني والبنية التحتية (CISA) عام 2018، وبناء منظومة دفاعية مكرسة لحماية البنية الانتخابية من التلاعب الأجنبي والتهديدات الهجينة المتنامية.

ويعتبر التصنيف المؤسسي الذي أقدمت عليه وزارة الأمن الداخلي في يناير 2017، بتصنيف البنية التحتية الانتخابية "بنية تحتية حيوية"، نقطة انطلاق أساسية أتاحت لهذه البنية الخضوع لحزمة حماية فيدرالية شاملة تشمل الرصد الدوري وتقييمات المخاطر وتبادل المعلومات الاستخباراتية.[45]

وقد ترتب على هذا التصنيف التأسيسي بناء منظومة مؤسسية بالغة التعقيد تتوزع على أربعة مستويات تنفيذية متمايزة تتكامل فيما بينها وظيفياً:

---

[44] حدد هذا التوجيه ثلاثة مسارات رئيسية تعمل بالتوازي:

- الاستجابة للتهديد (Threat Response): وتشمل التحقيق الجنائي، وإسناد الهجمات، وجمع الأدلة، وتحديد جهات التهديد.
- استجابة الأصول (Asset Response): وتتناول الدعم التقني للكيانات المتضرّرة، وتخفيف الثغرات، وتقليل الأضرار، وتقييم المخاطر القطاعية.
- الدعم الاستخباراتي :من خلال دمج التحليلات الاستخباراتية، وسد الفجوات المعرفية، ورفع الوعي بالتهديدات.

ويضاف إليها مسار رابع إذا كان المتضرّر وكالة فدرالية، يشمل استمرارية العمل، وإدارة المخاطر القانونية والإعلامية. أنظر:
The White House, "Presidential Policy Directive 41 (PPD-41): United States Cyber Incident Coordination", 26/07/2016. The "National Security Archive" website (Accessed: 07/04/2026): t.ly/6TPSG

[45] Lawrence NORDEN, "How the Federal Government Is Undermining Election Security", 14/04/2025. The " Brennan Center for Justice (BCJ)" website (Accessed: 05/04/2026): t.ly/okvAn

- **على مستوى التنسيق الاستراتيجي:** اضطلع مجلس الأمن القومي (NSC) بمهمة التنسيق بين مختلف أجهزة الدولة بما يضمن عمل وكالات الاستخبارات والأمن السيبراني وإنفاذ القانون والدبلوماسية في نسق واحد لا في صوامع منفصلة. وقد تمت مأسسة هذا الدور في عام 2018 بموجب القانون[46] الذي أنشأ منصب "منسّق مكافحة عمليات النفوذ الأجنبي الخبيث" ضمن هيئة موظفي المجلس، حيث يعينه الرئيس "مسؤولا عن تنسيق العمليات المشتركة بين الوكالات لمكافحة عمليات التأثير الأجنبي الخبيث" ويطلب منه إطلاع الكونغرس على مسؤوليات وأنشطة الموظفين مرتين على الأقل سنويا.[47]

- **على مستوى الاستخبارات والإنذار المبكر:** أسس مكتب مدير الاستخبارات الوطنية (ODNI) "مركز التأثير الأجنبي الخبيث" [48] (FMIC) ليبدأ عمله في 23 شتنبر 2022 بوصفه الجهة الحكومية الأمريكية الرئيسية لتجميع المعلومات الاستخباراتية المتعلقة بالتدخل الانتخابي وتحليلها وتوصيلها إلى صانعي القرار، مضطلعا بذلك بـ "خط الدعم الاستخباراتي" المنصوص عليه في "PPD-41"، وبمهمة إعداد التقييمات الرسمية ما بعد الانتخابية، التي تشكل الأساس القانوني لأي إجراءات لاحقة بموجب المرسوم التنفيذي EO 13848 الصادر عام 2018، والذي يلزم مدير الاستخبارات الوطنية بتقديم تقرير شامل حول التدخل الأجنبي في غضون 45 يوما من أي انتخابات، يفضي بدوره إلى آلية عقوبات إلزامية يشرف عليها وزيرا الخارجية والخزانة.[49]

- **على مستوى الدفاع السيبراني وحماية الأصول:** أنشئت وكالة الأمن السيبراني والبنية التحتية (CISA) عام 2018 لتضطلع بـ "خط الاستجابة الدفاعية" وفق "PPD-41"، مقدمة خدماتها التقنية طوعا ومجانا لمسؤولي الانتخابات في الولايات والمقاطعات المحلية، من بينها تقييمات الثغرات الأمنية ومسح الشبكات والاستجابة للحوادث والتدريب. وتدير الوكالة تبادل المعلومات على المستوى الوطني عبر "مركز تبادل المعلومات والتحليل للبنية التحتية الانتخابية" (EI-ISAC)، وقد أجرت الوكالة أكثر من 700 تقييم سيبراني للمقاطعات الانتخابية في عامي 2023 و2024 وحدهما.[50]

---

[46] Public Law 115–232—§1043(a)(2), 13/08/2018.

[47] "How the US Protects Elections from Foreign Interference", op. cit..

[48] Office of the Director of National Intelligence (ODNI), "Foreign Malign Influence Center (FMIC)", The "ODNI" website (Accessed: 02/04/2026): t.ly/iAmus

[49] "Executive Order 13848: Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election", 12/09/2018. The "American Presidency Project" website (Accessed: 07/04/2026): t.ly/IhtMr

[50] "How the US Protects Elections from Foreign Interference", op. cit..

- على مستوى الملاحقة القانونية والردع: اضطلعت وزارة العدل ومكتب التحقيقات الفيدرالي(FBI) بـ"خط الاستجابة التحقيقية الأمنية" وفق PPD-41؛ إذ أسس مكتب "FBI" عام 2017 فريق العمل الخاص بالتأثير الأجنبي (FITF) المعني بالتحقيق في عمليات التأثير وتعطيل أنشطة الخصوم وإسناد الهجمات إلى فاعليها وملاحقتهم قضائيا بالتنسيق مع قسم الأمن القومي في وزارة العدل.[51]

لقد أسفر هذا التراكم المؤسسي متعدد المستويات عن نتائج ملموسة؛ إذ أجمع مسؤولون أمنيون بارزون ومسؤولو البنية التحتية للانتخابات أن انتخابات 2020 كانت "الأكثر أمانا في تاريخ الولايات المتحدة".[52] بيد أن هذا المسار الدفاعي شهد انتكاسة في مطلع 2025 حين أقدمت الإدارة الأمريكية الجديدة على تجميد أنشطة مجموعة أمن الانتخابات في وكالة "CISA" وحلّ فريق عمل التأثير الأجنبي في مكتب "FBI"،[53] وهو ما وصفه خبراء أمن الانتخابات بأنه يعزز مباشرة قدرة الخصوم الأجانب على اختراق العملية الانتخابية الأمريكية.[54] ويجسد هذا المآل، بكل ما ينطوي عليه من مفارقة، الدرس المنهجي الأعمق الذي تقدمه التجربة الأمريكية: أن التحدي الحقيقي لأمن الانتخابات لا يكمن فحسب في بناء المنظومة الدفاعية التقنية والمؤسسية، بل يمتد ليشمل صون هذه المنظومة من التسييس الحزبي الداخلي الذي قد يفرغها من مضمونها حين تتحول إلى رهينة الصراع السياسي.

وهذا ما خلص له أيضا تقرير معهد الدراسات الأمنية للاتحاد الأوروبي (EUISS) بشأن الدروس المستخلصة من الانتخابات الأمريكية 2024، والتي حددها في خمسة دروس استراتيجية ذات قيمة

---

[51] Nikki FLORIS, "Securing America's Elections: Oversight of Government Agencies", Statement Before the House Judiciary Committee, 22/10/2019, The "Federal Bureau of Investigation (FBI)" website (Accessed: 07/04/2026): t.ly/R8Cne

[52] Stefan BECKET & al., "2020 election 'most secure in history', security officials say" – Sara COOK, "Election infrastructure officials: 2020 election was "most secure in American history", 13/11/2020. The "CBS News" website (Accessed: 05/04/2026): t.ly/oaTBP

[53] في 7 فبراير 2025، كشفت التقارير الصحفية أن المدعية العامة الأمريكية "بام بوندي" وجهت مكتب التحقيقات الفيدرالي لحل هذا الفريق وتقليص تطبيق "قانون تسجيل العملاء الأجانب"، مبررة قرارها بالتأكيد على ضرورة "تحرير الموارد لمعالجة الأولويات الأكثر إلحاحا، وإنهاء مخاطر المزيد من التسليح وإساءة استخدام سلطة الادعاء"، وذلك رغم سنوات من التحذيرات من وكالات الاستخبارات الأمريكية بأن عمليات التأثير الضارة الأجنبية التي تتعلق بالمعلومات المضللة تشكل تهديدا متزايدا وخطيرا. أنظر:

Ken DILANIAN, "Pam Bondi ends FBI effort to combat foreign influence in U.S. politics", 07/02/2025. The " nbcnews" website (Accessed: 07/04/2026): t.ly/QmLS3

[54] Jenna MCLAUGHLIN, "Efforts to Fight Foreign Influence and Protect Elections in Question under Trump", 11/02/2025. The "NPR" website (Accessed: 02/04/2026): t.ly/9jk2-

مرجعية للديمقراطيات الساعية إلى تحصين مساراتها الانتخابية؛ يتمثل أولها في استباق التضليل لا مجرد التفاعل معه، عبر نشر تقييمات تهديد دورية وتنبيهات عامة قبل يوم الاقتراع؛ ويتمحور الثاني حول تعزيز التنسيق المؤسسي البيني، إذ نسق مركز التأثير الأجنبي الخبيث (FMIC) عمل أكثر من عشرين وكالة فيدرالية في منظومة تحذير ودفاع متكاملة، أفضت إلى كشف الحملات الروسية وتفنيد مقاطع الفيديو المزيفة بصفة استباقية؛ أما الدرس الثالث فيتعلق بتوظيف آليات الإكراه والحوافز معا، حيث تجاوزت الاستجابة الحدود التقنية لتشمل تتبع التمويل الأجنبي الخفي وفرض العقوبات على الجهات المنفذة، مع إرساء نظام مكافآت لاستقطاب المعلومات الكاشفة لعمليات التدخل؛ ويتعلق الدرس الرابع بالتصدي لإساءة توظيف الذكاء الاصطناعي من خلال تدريب الكوادر المتخصصة على الكشف السريع عن محتوى التزييف العميق، وتعميق الشراكة مع شركات التكنولوجيا لتنظيم خوارزميات التضخيم؛ وينتهي التقرير بالدرس الخامس، وهو الأحد دلالة، إبعاد ملف أمن الانتخابات عن التجاذب الحزبي، وذلك أن صون الديمقراطية من التدخل الخارجي مشروطٌ بصون أجهزة الدفاع ذاتها من التدخل الداخلي.[55]

المطلب الثاني: التجربة الأوروبية في مواجهة التدخلات الهجينة المستجدة في الانتخابات: التحديات والاستجابة

يواجه الاتحاد الأوروبي تحديا هيكليا مركبا في مجال حماية انتخاباته؛ إذ تتوزع إدارة العمليات الانتخابية على سبعة وعشرين نظاما انتخابيا وطنيا مستقلا، مما يجعل التنسيق الدفاعي تجاه التهديدات الهجينة المستجدة أمرا بالغ التعقيد.

واستجابة لهذه التهديدات المتصاعدة، بنى الاتحاد الأوروبي منظومة متكاملة متعددة المستويات: على الصعيد التشريعي، وعلى الصعيد المؤسسي، وعلى صعيد التنسيق الاستخباراتي.

✓ التحديات البنيوية والظرفية

رصدت تقارير دائرة العمل الخارجي الأوروبي (EEAS) تصاعدا متواصلا في عمليات "التدخل الخارجي والتلاعب بالمعلومات" (FIMI) منذ عام 2015، حين تكشفت للمرة الأولى خيوط حملة التضليل الروسية في سياق التدخل العسكري في أوكرانيا.[56]

[55] Nad'a KOVALČÍKOVÁ, Giuseppe SPATAFORA, "The future of democracy: lessons from the US fight against foreign electoral interference in 2024", Brussels: EU Institute for Security Studies (EUISS), 17/12/2024. The "EUISS" website (Accessed: 07/04/2026): t.ly/BF9yf

[56] European External Action Service (EEAS), "Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI)", The "EEAS" website (Accessed: 07/04/2026): t.ly/WQAJq

وقد كشفت انتخابات البرلمان الأوروبي لعام 2024 عن تصاعد لافت في وتيرة التهديدات الهجينة المُوجَّهة نحو نزاهة العملية الديمقراطية ومصداقيتها. وتتصدر هذه التحديات ظاهرة "التدخل الخارجي والتلاعب بالمعلومات" (FIMI)، التي وثقها التقرير السنوي الثالث لدائرة العمل الخارجي الأوروبي (EEAS) في سياق تلك الانتخابات، كاشفا عن اثنين وأربعين حادثة مرتبطة بنشاط روسي في مجال (FIMI)رصد تصاعدها المتدرج في الأسابيع السابقة للاقتراع وبلغ ذروته إبان عملية الاقتراع بين السادس والتاسع من يونيو 2024، واستمر في مرحلة ما بعد الانتخابات بهدف التشكيك في مشروعية نتائجها.[57]

وتجلى في هذا السياق نمط تشغيلي منظم يميزه التقرير عن العمليات العشوائية: يقوم على إرساء البنية التحتية للتضليل مبكرا، ثم تصعيد الهجمات على المسار الديمقراطي وتكثيفها قبيل يوم الاقتراع، وتوظيف الاختراق السيبراني دعما للحملات المعلوماتية، قبل التحول في مرحلة ما بعد الانتخابات إلى تقويض الثقة في النتائج.[58] وقد رصد المرصد الأوروبي للإعلام الرقمي (EDMO) ارتفاعا ملحوظا في حجم التضليل المرتبط بالانتخابات الأوروبية من 5% في يناير 2024 إلى 15% في مايو من العام ذاته، مع تركيز السرديات المضللة على تقويض الثقة في تنظيم الانتخابات ومصداقية نتائجها، واستغلال قضايا التوتر الاجتماعي.[59]

ويكشف التقرير السنوي الرابع لدائرة العمل الخارجي الأوروبي (EEAS) حول تهديدات(FIMI) الصادر عام 2026، والمؤسس على رصد 540 حادثة موثقة طوال عام 2025 حول العالم شملت ما يزيد على عشرة آلاف وخمسمائة قناة في وسائل التواصل الاجتماعي والمواقع الإلكترونية، عن انتقال نوعي حاد في طبيعة هذه التهديدات: من عمليات معلوماتية نسبيا محدودة النطاق إلى منظومة هجينة بالغة التعقيد تتشابك فيها أبعاد سيبرانية وإعلامية ونفسية واقتصادية تستهدف صميم البنى الديمقراطية الأوروبية.[60]

---

[57] European External Action Service (EEAS), 3rd Annual Report on Foreign Information Manipulation and Interference (FIMI) Threats: Exposing the Architecture of FIMI Operations", March 2025. p. 10. The "EEAS" website (Accessed: 07/04/2026): t.ly/Zb53Q

[58] ibid.

[59] European Digital Media Observatory (EDMO), "Final Report Outputs and outcomes of a community-wide effort", 26/07/2024. p. 1. The "EDMO" website (Accessed: 07/04/2026): t.ly/kQJLL

[60] EEAS, "4th EEAS Report on FIMI Threats: Dismantling the FIMI House of Cards", op. cit., p. 7.

والإشكالية الهيكلية الجوهرية التي تفرضها هذه التهديدات على المنظومة الأوروبية أن الاتحاد يضم سبعا وعشرين منظومة انتخابية وطنية مستقلة، تتباين في ثقافتها الرقمية ومستوى قدراتها الدفاعية المؤسسية والتقنية وأطرها القانونية الناظمة للفضاء المعلوماتي، في حين أن التهديدات الهجينة تعمل بمنطق عابر للحدود، مما يفضي إلى فجوات في المناعة تشكل نقاط استهداف انتهازية بامتياز لعمليات (FIMI) التي تعمل أصلا على استغلال حالة الالتباس في واجهات الحرب-السلم والأمن الداخلي-الخارجي والمستوى الوطني-الأوروبي.[61]

وتبين معطيات التقرير الرابع أن العمليات الروسية استهدفت في عام 2025 عدة دول أروبية، مركزة بصفة خاصة على الاستحقاقات الانتخابية بوصفها "نوافذ انتهازية" استراتيجية، إذ إن ما يقارب نصف الحوادث المرصودة ارتبط ارتباطا مباشرا بأحداث سياسية كبرى كالانتخابات والاحتجاجات والأزمات الدولية، مؤكدا أن لحظات السعي المعلوماتي المكثف لدى الجمهور هي بالذات اللحظات التي تهيئ البيئة المثلى لتغلغل التضليل وانتشاره الفيروسي.[62] وقد جاء التوظيف المتصاعد للذكاء الاصطناعي في هذه العمليات ليضاعف خطرها الهيكلي؛ إذ ارتفع عدد حوادث (FIMI) الموثقة التي وظفت أدوات الذكاء الاصطناعي من 41 حادثة في عام 2024 إلى 147 في عام 2025، أي بنسبة نمو تبلغ 259% خلال سنة واحدة، في ما وصفه التقرير بتحول نحو التوظيف "الروتيني" للذكاء الاصطناعي في إنتاج المحتوى المضلل وتوزيعه بموارد أقل وقدرات أوسع.[63]

---

[61] فواجهة الحرب-السلم تجعل عمليات التضليل تشتغل في المنطقة الرمادية التي لا تبلغ عتبة الاستجابة العسكرية ولا تقتصر على الإطار الأمني المدني المعتاد؛ وواجهة الأمن الداخلي-الخارجي تعقد تحديد الجهة المختصة بالتصدي لعمليات التضليل ذات المصادر الأجنبية التي تستخدم وسطاء محليين تجعل تمييزهم عسيرا؛ وواجهة المستوى الوطني-الأوروبي تشكل فجوة تنسيقية حقيقية بين الاختصاصات السيادية للدول الأعضاء في تنظيم انتخاباتها وبين الحاجة الموضوعية إلى استجابة أوروبية موحدة تفترض قدرا من التنازل عن هذه السيادة في مجال الأمن المعلوماتي الانتخابي. وقد وثق التقرير الأوروبي الصادر عام 2025 حول انتخابات 2024 هذه الإشكالية بصورة لافتة حين أشار إلى أن المسؤوليات الرئيسية في تنظيم الانتخابات تبقى حكراً على الدول الأعضاء بموجب القانون الأوروبي، في حين أن التهديدات التي تواجه هذه الانتخابات باتت تتجاوز القدرة الفردية لكل دولة على التصدي لها منفردة، مما يعرّضها لفخ "المسؤولية المنقسمة" مسؤولية التنظيم وطنية بامتياز، ومسؤولية الحماية أوروبية بالضرورة. أنظر:

- The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), op. cit.
- European Commission (EC), "Report on the 2024 Elections to the European Parliament", COM(2025) 287 final, 06/06/2025, pp. 1-3. The "EC" website (Accessed: 02/04/2026): t.ly/utuZ7

[62] EEAS, "4th EEAS Report on FIMI Threats: Dismantling the FIMI House of Cards", op. cit., p. 10-11.

[63] Ibid., p. 14.

وتتكشف في هذا المشهد جملة من التحديات الهيكلية العميقة التي تعرقل الاستجابة الأوروبية الموحدة. يتمثل أبرزها في التفاوت الواسع بين الدول الأعضاء في القدرات الدفاعية المؤسسية والتقنية؛ إذ تواجه الدول الأصغر والأقل تجربة في مجال الأمن السيبراني ومكافحة التضليل ثغرات استهدافية أوسع بكثير مقارنة بنظيراتها الكبرى. وتنضاف إلى ذلك إشكاليات الفضاء الرقمي الجديد، لاسيما ما يرتبط منها بتوظيف الذكاء الاصطناعي في إنتاج "التزييف الرخيص" و"التزييف السطحي"، حيث رصدت منظمات المجتمع المدني 131 حالة موثقة لمحتوى ذكاء اصطناعي غير مصرح به خلال الحملة الانتخابية، وظف في نشر رسائل مضللة من قبل أحزاب سياسية في فرنسا وبلجيكا وإيطاليا.[64] وتبرز أيضا إشكالية ذات طابع بنيوي أعمق تتعلق بالتمويل السياسي الأجنبي الخفي في النظم الرقمية الجديدة، إذ تتعذر مراقبة التدفقات المالية عبر المنصات الرقمية وآليات التبرع الإلكترونية، مع غياب تشريعي جزئي لايزال يشكل فجوات في منظومة الرقابة.[65] وعلى صعيد التهديدات السيبرانية، وإن ظلت الحوادث الموثقة في انتخابات 2024 محدودة، إذ اقتصرت في معظمها على هجمات حجب الخدمة (DDoS) نفذتها مجموعات قرصنة موالية لروسيا، فإن خبراء الأمن ينبهون إلى أن هذه الحوادث قد تخفي عمليات اختراق أكثر تطورا وأصعب إسنادا.[66]

فضلا عن ذلك، رصد توظيف متصاعد للتضليل الهوياتي الجنساني (Gendered Disinformation)، يستهدف المرشحات والقياديات السياسيات بهدف دفعهن إلى مغادرة الفضاء السياسي، وهو ما وثقه المؤشر العالمي للتضليل في تقريره المتعلق بانتخابات البرلمان الأوروبي 2024.[67]

✓ منظومة الاستجابة الأوروبية

طور الاتحاد الأوروبي منظومة استجابة متعددة المستويات تجسد، لأول مرة في تاريخه، مقاربة تعتمد التنسيق المؤسسي الشامل بين مستويين: مستوى التحضير والوقاية، ومستوى الرصد والاستجابة الآنية.

على الصعيد التشريعي، فإن النظر في منظومة الاستجابة الأوروبية يحيلنا على نظامين قانونيين وقضائيين مستقلين ومختلفين: من جهة أولى الاتحاد الأوروبي الذي يقوم على أساس البناء

[64] European Commission (EC), "Report on the 2024 Elections to the European Parliament", COM(2025) 287 final, op. cit., p. 17.

[65] ibid., p. 20.

[66] Ibid., p. 19.

[67] Global Disinformation Index (GDI), "Gendered Disinformation in the European Parliamentary Elections", 10/06/2024. The "GDI" website (Accessed: 02/04/2026): t.ly/-vNsl

الاقتصادي لسوق واحدة ويهتم بتلبية متطلباته الاقتصادية؛ ومن جهة أخرى مجلس أوروبا الضامن لحماية الحقوق والحريات الأساسية.

فيما يخص الاتحاد الأوروبي، يعد قانون الخدمات الرقمية (DSA) الذي دخل حيز التنفيذ الكامل في فبراير 2024 العمود الفقري لهذه المنظومة، إذ يلزم المنصات الرقمية الكبرى (ذات أكثر من 45 مليون مستخدم) بإجراء تقييمات دورية للمخاطر المنهجية في مجالات الانتخابات والمحتوى غير القانوني وحقوق الإنسان، تحت طائلة غرامات تبلغ 6% من إجمالي إيراداتها السنوية.[68]

أما مجلس أوروبا فقد وضع في قلب منظومة الاستجابة الأوروبية "الاتفاقية-الإطار لمجلس أوروبا بشأن الذكاء الاصطناعي وحقوق الإنسان والديمقراطية وسيادة القانون" بوصفها المرجعية الدولية الملزمة الأولى من نوعها في مجال حوكمة الذكاء الاصطناعي.[69] وتتمحور أحكام هذه الاتفاقية حول مبدأ جوهري واحد: ضمان أن تكون أنشطة دورة حياة أنظمة الذكاء الاصطناعي، من التصميم إلى الاستخدام وحتى الإيقاف، متوافقة تماما مع حقوق الإنسان والمبادئ الديمقراطية وسيادة القانون، مع الإبقاء على الانفتاح أمام التقدم التقني والابتكار. وفي هذا الإطار تكتسب الاتفاقية أهمية مباشرة في السياق الانتخابي؛ إذ توجب على أطرافها صون شروط المشاركة العادلة في الفضاء العام وحق الأفراد في تكوين آرائهم بحرية دون تأثير مزيف من أنظمة الذكاء الاصطناعي، كما تشترط إخطار الأفراد حين يتعاملون مع أنظمة ذكاء اصطناعي لا مع بشر، وهي أحكام تشكل سياجا قانونيا دوليا مباشرا في مواجهة البوتات الانتخابية والتزييف العميق ذي الطابع السياسي. وقد أصدر البرلمان الأوروبي في 11 مارس 2026 موافقته على إبرام الاتحاد الأوروبي لهذه الاتفاقية رسميا، واصفا إياها في توصيته بأنها تجسد "إمكانية قيادة الثورة التكنولوجية على أساس القيم الديمقراطية".[70]

---

[68] Linda ROBINSON, "European Tech Law Faces Test to Address Interference, Threats and Disinformation in 2024 Elections", 22/05/2024. The "Council on Foreign Relations (CFR)" website (Accessed: 02/04/2026): t.ly/PQtwy

[69] اعتمدت هذه الاتفاقية الإطار من طرف مجلس وزراء مجلس أوروبا في 17 مايو 2024، وفتح باب التوقيع عليها في 5 سبتمبر 2024 بحضور الاتحاد الأوروبي والولايات المتحدة والمملكة المتحدة وعشرات الدول الأخرى، قبل أن تدخل حيز التنفيذ الدولي في الأول من نونبر 2025 إثر استيفاء عتبة التصديق المطلوبة (يبدأ نفاذها، وفق المادة 30 منها، في اليوم الأول من الشهر التالي لانقضاء فترة ثلاثة أشهر على التاريخ الذي أعربت فيه خمس دول موقعة، بما فيها ثلاث دول أعضاء في مجلس أوروبا على الأقل، عن موافقتها على الالتزام بهذه الاتفاقية). أنظر:

Council of Europe, "Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law", CETS N°. 225, Adopted 17/05/2024, Opened for signature 05/09/2024.

[70] European Parliament, "RECOMMENDATION on the draft Council decision on the conclusion, on behalf of the European Union, of the Council of Europe Framework Convention =

وعلى الصعيد التنظيمي، وظف قانون الخدمات الرقمية ("Digital Services Act "DSA") لأول مرة في سياق انتخابي شامل، إذ أصدرت المفوضية الأوروبية في أبريل 2024 مبادئ توجيهية تلزم مشغلي المنصات الكبرى بتقييم المخاطر المنهجية المتعلقة بالعمليات الانتخابية والحد منها، وإجراء اختبارات لسيناريوهات التضليل الانتخابي، في حين فتحت المفوضية تحقيقات رسمية ضد منصات "Meta" و"TikTok" و"X" بتهمة التساهل في التلاعب المنسق وانتهاكات قواعد الإعلانات الخادعة.[71]

وعلى الصعيد المؤسسي، أنشأت دائرة العمل الخارجي الأوروبي "إطار الاستجابة لمخاطر التدخل الخارجي والتلاعب بالمعلومات" (Response Framework to FIMI Threats) الذي يربط التحليل الاستخباراتي بآليات الاستجابة السريعة، وطورت "صندوقَي الأدوات" (Toolboxes)؛ أولهما مخصص للتهديدات الهجينة (EU Hybrid Toolbox)، وثانيهما خاص بالتدخل الخارجي والتلاعب بالمعلومات (FIMI Toolbox).[72]

وعلى صعيد آلية الأزمات الفورية، فعلت الرئاسة البلجيكية للمجلس الأوروبي في أبريل 2024 آليات الاستجابة السياسية المتكاملة للأزمات Integrated Political Crisis Response) ("IPCR"في وضع تبادل المعلومات، مما أتاح رؤية تنسيقية مباشرة بين المؤسسات الأوروبية والدول الأعضاء إزاء مؤشرات التدخل الأجنبي.[73]

وعلى صعيد الشبكات التحليلية والفحص الاستخباراتي، أسهم "المرصد الأوروبي للإعلام الرقمي" (EDMO) في رصد الفضاء المعلوماتي لانتخابات 2024 ميدانيا، مصدرا نشرات يومية وإنذارات مبكرة طوال الفترة الانتخابية.[74]

---

on Artificial Intelligence and Human Rights, Democracy and the Rule of Law", A10-0007/2026, 02/02/2026. The "European Parliament" website (Accessed: 02/04/2026): t.ly/TbA7L

[71] ibid.

[72] Council of the European Union, "Democratic resilience: Council approves conclusions on safeguarding electoral processes from foreign interference", 21/05/2024. The "Council of the EU" and the "European Council" website (Accessed: 02/04/2026): t.ly/OG8GG

[73] European Commission (EC), "Report on the 2024 Elections to the European Parliament", COM(2025) 287 final, op. cit., p. 2.

[74] أصدر المرصد "EDMO"، قبل انتخابات أوروبا لعام 2024، نشرات يومية اعتبارا من 8 أبريل 2024، يرفع فيها أحدث تهديدات التضليل وتقدم تحذيرات مبكرة. أنظر:

European Digital Media Observatory (EDMO), "EU Election Disinfo Bulletin", 2024. The "EDMO" website (Accessed: 02/04/2026): t.ly/cbw35

غير أن هذه الاستجابة المؤسسية لاتزال تعتريها ثغرات بنيوية، فعلى الرغم من غياب حوادث كبرى مخلة بسير الاقتراع، يقر التقرير الأوروبي بأن المقاربة التشريعية الرقمية لم تكن مكتملة التطبيق إبان استحقاق انتخابات البرلمان الأوروبي 2024، إذ لم تدخل الأحكام الأساسية للوائح الذكاء الاصطناعي (AI Act) والإعلان السياسي حيز التنفيذ إلا بعد الانتخابات،[75] أما "الاتفاقية-الإطار لمجلس أوروبا بشأن الذكاء الاصطناعي وحقوق الإنسان والديمقراطية وسيادة القانون" فتعاني من نقطتي ضعف موضوعيتين تحدان من أثرها المباشر: أولاهما استثناء الأنشطة المرتبطة بالأمن القومي من نطاق تطبيقها، مما يفتح مسارا للتحايل تحت ستار الدواعي الأمنية؛ وثانيتهما عدم استكمال الاتحاد الأوروبي إجراءات التصديق في المرحلة الراهنة، مما يبقي تطبيقها في النطاق الأوروبي رهينا باستكمال هذا المسار الجاري. وتبقى بذلك هذه الاتفاقية، رغم رمزيتها التأسيسية الرفيعة بوصفها أول معاهدة دولية ملزمة تتناول الذكاء الاصطناعي، في مرحلة "القانون في طور النشأة"، حاضرة بقوة على صعيد المعيارية الدولية، بينما لايزال تأثيرها التطبيقي المباشر رهينا باستكمال التصديقات وبناء آليات المتابعة والتنفيذ.

كما أثارت التدابير الطوعية للمنصات الرقمية، التي أبدت انضباطا متفاوتا في تطبيق التزاماتها المنبثقة عن إرشادات قانون الخدمات الرقمية (DSA) بخصوص الحد من المخاطر المنهجية عبر الإنترنت المرتبطة بالانتخابات، تساؤلات جدية حول مدى كفاية آليات الالتزام الطوعي في مواجهة تهديدات منهجية ذات طابع دولي.[76] وعلى صعيد الدول الأعضاء، رصد التقرير تباينا حادا في الإجراءات المتخذة: فبينما أعلنت خمس عشرة دولة عضو عن اتخاذ تدابير استباقية لحماية البيئة المعلوماتية، ظلّت الاستجابة في دول أخرى محدودة أو متأخرة.[77] ويختتم التقرير بدعوة صريحة إلى بناء "درع ديمقراطية أوروبية" (European Democracy Shield) كإطار استراتيجي جامع يتجاوز المقاربة التفاعلية نحو نموذج "الاستعداد الشامل"، وهو توجه يؤكد أن التجربة الأوروبية لاتزال في طور البناء المتسارع لا في طور الاكتمال والاستقرار، وهو الدرس الأكثر راهنية للحالة المغربية المقبلة على انتخاباتها التشريعية في خريف 2026.[78]

---

[75] يوضح تقرير المفوضية الأوروبية أن قانون الذكاء الاصطناعي (AI Act) دخل حيز التنفيذ رسميا في غشت 2024، ولم يكن مطبقا بالكامل إبان انتخابات البرلمان الأوروبي 2024. أنظر: European Commission (EC), "Report on the 2024 Elections to the European Parliament", COM(2025) 287 final, op. cit., p. 22.

[76] FIMI-ISAC, "Collective Findings Report on 2024 European Elections", October 2024, p. 17. The "FIMI-ISAC" website (Accessed: 02/04/2026): t.ly/PLp4z

[77] European Commission (EC), "Report on the 2024 Elections to the European Parliament", COM(2025) 287 final, op. cit., p. 16.

[78] Ibid., p. 29.

يتضح من مقارنة التجارب الدولية الكبرى أن ثمة قاسما مشتركا يجمعها؛ وهو أن جميعها تأخرت في التحرك وأجرت مراجعتها الاستراتيجية في أعقاب وقوع التدخل لا استباقا له. فالتجربة الأمريكية كانت رد فعل على صدمة 2016، والتجربة الأوروبية رد فعل على الكشف عن عمليات التضليل الروسية، والاتفاقية الإطار الأوروبية جاءت في أعقاب تصاعد القلق من الذكاء الاصطناعي التوليدي. وهذا النمط الاستجابي يشكل في حد ذاته درسا منهجيا بالغ الأثر: أن الديمقراطيات المتطورة تميل إلى التفاعل مع التهديد بعد وقوعه، وأن بناء الاستراتيجية الوقائية الاستباقية يعد الرهان المقبل للدول التي تُقبل على استحقاقات انتخابية في بيئة دولية متوترة، ومنها المملكة المغربية.

المبحث الثالث: الانتخابات المغربية المقبلة في مواجهة التأثير الخارجي

لا تقف المملكة المغربية، في سياق انتخاباتها التشريعية المرتقبة في 23 شتنبر 2026، بمعزل عن هذه الديناميكيات الدولية التي تم التطرق لها في المبحث السابق في مواجهة التهديدات الهجينة المستجدة، ولاسيما تلك التي يمثلها التضليل المعلوماتي ويدعمها الذكاء الاصطناعي؛ إذ تجمع فيها عوامل بنيوية تجعلها في قلب مناطق التنافس الدولي: موقعها الجيوسياسي الاستراتيجي بوصفها رابطا محوريا بين أوروبا وإفريقيا، وتوافر مصالح متنافسة لقوى إقليمية ودولية على أراضيها، فضلا عن سياقها الانتخابي الداخلي الذي يتسم بتراجع نسب المشاركة وضعف الثقة في المؤسسات السياسية.

ولعل وعي المغرب بهذه التحديات هو ما جعله يشرع في بناء منظومة استجابه لهذه التهديدات تجسدت من خلال اتخاذ خطوات على عدة مستويات: تشريعيا، وتنظيميا، وعلى صعيد التنسيق الاستخباراتي....

المطلب الأول: السياق الجيوسياسي الإقليمي والدولي والداخلي

يوجد الموقع الجيوسياسي الاستثنائي للمملكة المغربية بوصفها ملتقىً بين قارات ثلاث وحلقة وصل محورية بين أوروبا وإفريقيا والعالم العربي، سياقا دوليا بالغ التعقيد يجعل استحقاقها الانتخابي المرتقب حدثا يتجاوز حدوده الوطنية ليتحول إلى مؤشر استراتيجي تتقاطع حوله رهانات إقليمية ودولية متشعبة.

✓ المغرب في قلب التنافس الإقليمي والدولي

على صعيد التنافس الإقليمي، تشكل العلاقة مع الجزائر، التي أبقت حدودها مع المغرب مغلقة منذ 1994 وقطعت علاقاتها الدبلوماسية معه في غشت 2021، المحور البنيوي الأكثر تأثيرا في أمن

المنظومة الانتخابية المغربية. فقد وثق مجموعة الأزمات الدولية في تقريرها الصادر في نونبر 2024 أن التوترات بين البلدين امتدت من الدبلوماسية إلى الفضاء السيبراني، في ظل تحذيرات صريحة من أن "انتشار المعلومات المضللة على الإنترنت" يشكل أحد عوامل الخطر الرئيسية لتأجيج الأزمة المغربية-الجزائرية.[79]

ويضخم هذا الإطار التنافسي حدة المخاطر المحيطة بالعملية الانتخابية؛ إذ يتيح ملف الصحراء بوصفه مادة للتعبئة الرقمية أرضية خصبة للتنافس على السرديات السياسية التي تؤثر بصورة مباشرة في بيئة الرأي العام المغربي، في حين تجسد الانتخابات من منظور الواقعية الجديدة فرصة استراتيجية للجهات المتنافسة على النفوذ الإقليمي لإضعاف الشرعية المؤسسية للدولة المغربية في لحظة تجديد التفويض الشعبي، إذ يعزز إضعاف الثقة في المؤسسات الانتخابية المغربية موقف الأطراف المنازعة لمشروعية المواقف المغربية.

وعلى صعيد التنافس الدولي الأشمل، يقع المغرب في قلب بنية جيوسياسية يتشابك فيها اهتمام قوى من أقطاب متعددة؛ فالولايات المتحدة تعتبره حليفا استراتيجيا خارج "الناتو"، وقد اعترفت بسيادته على الصحراء عام 2020، كما سعت إدارة ترامب الثانية إلى دور وساطة بين الرباط والجزائر في مطلع عام 2026. وتتقاطع مع ذلك مصالح فرنسا التي أعلنت دعمها لمخطط الحكم الذاتي عام 2024 وأبرمت مع المغرب اتفاقيات استثمارية بقيمة 11.6 مليار دولار،[80] فضلا عن الصين التي تتوسع استثماراتها في المنظومة اللوجستية والبنية التحتية المغربية ضمن مبادرة الحزام والطريق.

ويفرز هذا التشابك الجيوسياسي متعدد الأقطاب منطقا بنيويا تؤطره الواقعية الجديدة بمفهوم "المكاسب النسبية" يحفز فاعلين إقليميين ودوليين متعددين على توظيف الفضاء المعلوماتي الانتخابي المغربي ساحة لتحسين أوضاعهم الاستراتيجية النسبية دون انخراط في مواجهة مباشرة مكلفة، ولتحقيق مكاسب جيوسياسية، حتى وإن تعارض ذلك مع مبادئ القانون الدولي المتعلقة بعدم التدخل.

في هذا السياق، تم رصد عدد من عمليات التضليل الإقليمية الموثقة، حيث وثقت تقارير منظمة "فريدوم هاوس" (Freedom House) وجهات رقابية أخرى حملات تضليل موجهة نحو المغرب، من بينها حملة إحدى المجموعات الإسرائيلية الخاصة، التي يطلق عليها اسم "فريق جورج" (Team

[79] International Crisis Group (ICG), "Managing Tensions between Algeria and Morocco", Report N° 247, 29/11/2024. The "ICG" website (Accessed: 02/04/2026): t.ly/WAX9-

[80] Hamza MEDDEB, "Economic Statecraft as Geopolitical Strategy: New Dimensions of Moroccan-Algerian Rivalry", 22/07/2025. The " Carnegie Endowment for International Peace (CEIP)" website (Accessed: 02/04/2026): t.ly/YO7W0

Jorge)، والتي استهدفت المشهد السياسي المغربي بوسم "هاشتاغات إلكترونية" مضللة تربط حركة "البوليساريو" بإيران وحزب الله.[81] وتنخرط هذه العملية في ما تسميه الأدبيات الأمنية "حرب الروايات" (Narrative Warfare)، وهي شكل من أشكال الصراع على النفوذ الجيوسياسي عبر السيطرة على تأطير المعلومات.

كذلك رصد تقرير لمعهد الدراسات الأمنية الإفريقية (ISS) الجنوب إفريقي تعرض المغرب، إلى جانب مصر ونيجيريا والسنغال، لشبكات دعاية إيرانية منظمة على المنصات الرقمية، فيما وثق "مركز إفريقيا للدراسات الاستراتيجية" التابع لوزارة الدفاع الأمريكية تعرض المغرب لحملة تضليل روسية. وخلص التقريران إلى أن حملات التضليل المعلوماتي الموجهة نحو إفريقيا، ولاسيما الروسية منها، تشتغل عبر أسلوب متطور يمزج بين المحتوى المختلق والانتقادات المشروعة للسياسات الغربية، مما يصعب كشفها ومواجهتها، ورصدا أن روسيا تعتمد "استراتيجية الامتياز" (Franchise Strategy) القائمة على توظيف فاعلين محليين من السكان ومؤثرين أفارقة مدفوعي الأجر لنشر المحتوى التضليلي، مما يجعل المحتوى يبدو أصيلا لا ممنهجا.[82]

وجدير بالذكر أن تقرير "مركز إفريقيا للدراسات الاستراتيجية" قد رصد بأن الانتخابات الإفريقية توفر فرصا رئيسية للتضليل، حيث يوظف البعض فرق عمليات تشويش المعلومات المرتزقة.[83]

وفي ضوء ذلك، فإن التنافس الجيوسياسي على الفضاء الإفريقي وشمال إفريقيا بين قوى روسية وغربية وإقليمية يشكل سياقا دوليا مواتيا لتوظيف هذه الأدوات استباقا للانتخابات المغربية 2026، وهو ما يؤكد أن المغرب بات هدفا ممنهجا في خريطة التنافس المعلوماتي الإقليمي والدولي.

---

[81] Freedom House, "Freedom on the Net 2023: Morocco Country Report", 2023. The "Freedom House" website (Accessed: 02/04/2026): t.ly/HCMeO

[82] أنظر:

- Kyle HIEBERT, "Foreign Interest in Africa Comes with Damaging Disinformation Tactics", 05/02/2025. The "Institute for Security Studies (ISS)" website (Accessed: 02/04/2026): t.ly/FdrYd
- مركز أفريقيا للدراسات الاستراتيجية، "خريطة موجة المعلومات المضللة في إفريقيا"، 2024/04/03، موقع "مركز أفريقيا للدراسات الاستراتيجية" على الإنترنت (آخر ولوج: 2026/04/04): t.ly/_xXcP

[83] كمثال على ذلك، وبحسب ما ورد، فقد نفذت إحدى المجموعات الإسرائيلية الخاصة، التي يطلق عليها اسم "فريق جورج"، حملات تضليل لتعطيل أكثر من 20 من الانتخابات الإفريقية منذ عام 2015. أنظر: مركز أفريقيا للدراسات الاستراتيجية، "خريطة موجة المعلومات المضللة في إفريقيا"، مرجع سابق.

✓ عوامل الهشاشة في السياق السياسي الداخلي المغربي

تتضافر في البيئة السياسية الداخلية المغربية عوامل هشاشة بنيوية تهيئ أرضا خصبة لاشتغال آليات التدخل الخارجي الهجين والتضليل المعلوماتي. يتمثل العامل الأول في أزمة الثقة السياسية الحادة؛ إذ أسفر استطلاع نُشر عام 2025 عن أن 91.5% من المستطلعين يصفون أداء الأحزاب السياسية بالضعف، في حين أكد 59.6% أن "الوعود الزائفة والتسويق الإعلامي الخادع" تقوّض الثقة في المؤسسات السياسية.[84]

ولا يمكن التقليل من أهمية هذه المعطيات في تقدير مناعة البيئة الانتخابية؛ إذ تشكل حالة انعدام الثقة المجتمعية في المؤسسات السياسية، وفق ما رصدته الأدبيات المتخصصة في تحليل نجاعة حملات التضليل، عامل ضعف استراتيجيا أمام الروايات المضللة التي تغذي الإحباط وتعزز العزوف، بما يخدم أهداف الجهات الراغبة في تفريغ الاستحقاق الانتخابي من مشروعيته الشعبية.[85] وهذا فضلا عن التوتر الذي أحاط بمسار إعداد قانون انتخابي جديد، بين مطالب الأحزاب الكبرى بتعزيز موقعها وعتبات انتخابية أعلى، وبين مطالب الأحزاب الصغيرة بضمان التعددية، مما يرجح استمرار حالة الاستقطاب السياسي الداخلي في مرحلة ما قبل الانتخابات.[86]

ويضاف إلى ذلك عامل العزوف الانتخابي، لاسيما في أوساط الشباب الذين يشكلون الشريحة الأكثر استخداما للمنصات الرقمية وبالتالي الأكثر عرضة للمحتوى المُضلِّل.

فضلا عن ذلك، تمثل التوترات المرتقبة بين الأحزاب المتنافسة في مرحلة ما قبل الانتخابات 2026، وما يصاحبها من ظاهرة "التسريبات والتسريبات المضادة"-Leaks and Counter) (Leaks،[87] نقطة دخول انتهازية لعمليات التدخل المعلوماتي الخارجي، وفق النمط نفسه الذي رصدته دراسات تحليلية في سياقات ديمقراطية مقارنة.

---

[84] نقلا عن تقرير جديد صادر عن المركز المغربي للمواطنة، بعنوان "الأحزاب السياسية المغربية وأزمة المصداقية"، والذي توصل إلى أن الأحزاب السياسية تصنف ضمن المؤسسات التي تواجه أزمة حادة في ثقة المواطنين. أنظر:
Mohamed ALAOUI, "Survey Reveals Widespread Distrust of Political Parties in Morocco", 22/09/2025. The "Arab Weekly" website (Accessed: 02/04/2026): t.ly/IsPBs

[85] Jon ROOZENBEEK & al., op. cit., p.2.

[86] Khadija TAOUIL, "Moroccan Political Parties Present Their Proposals for Electoral Code Reform", 16/08/2025. The "Atalayar" website (Accessed: 02/04/2026): t.ly/3zJsi

[87] "Analysts Warn of Political Tensions Ahead of Morocco's 2026 Legislative Elections", 10/11/2025. The "Hespress English" website (Accessed: 02/04/2026): t.ly/5M0r_

وعلى صعيد البيئة الإعلامية، تعاني المشهد الإعلامي المغربي من تركز يقيد تنوع مصادر المعلومات، في حين تتنامى نسبة استهلاك المحتوى الرقمي عبر منصات التواصل الاجتماعي، وهو ما يعظم من هشاشة البيئة المعلوماتية أمام حملات التضليل المنظم.

✓ جغرافيا التهديد: الفواعل المحتملون وأهدافهم المتوقعة

في ضوء الإطار الواقعي الجديد، يمكن استشراف خريطة الفواعل الدولية التي تمتلك حوافز بنيوية للتأثير في بيئة الانتخابات المغربية 2026 كما يلي:

1. **الفاعلون الإقليميون:** تمتلك الجزائر (ومعها البوليساريو) حوافز بنيوية واضحة لإضعاف مكانة الحكومة المغربية وتقويض ثقة المواطنين في المؤسسات، لاسيما في سياق ملف الصحراء. ومن المؤشرات الدالة بهذا الصدد ما تم رصده مرارا من حملات موجهة تعتمد على وسائل الإعلام الجزائرية ومجموعات ضغط إقليمية لبث روايات تشكك في مشروعية المؤسسات المغربية؛

2. **القوى الدولية الكبرى:** في ظل الصراع الجيوسياسي المتصاعد بين الغرب والصين وروسيا في القارة الإفريقية، وثقت مراكز بحثية عديدة أن مسرح الصراع امتد إلى شمال إفريقيا، وأن نشاط شبكات التضليل الروسية تصاعد تزامنا مع الاستحقاقات الانتخابية الإفريقية الكبرى. كما تمتلك قوى غربية حوافز انتقائية للتأثير في مسار الانتخابات المغربية لضمان استمرارية التوجهات التعاونية في ملفات الهجرة والأمن والإسلام السياسي....

3. **الفاعلون من غير الدول:** يبرز بهذا الخصوص ما شهده الفضاء السيبراني مؤخرا من عملية اختراق واسعة منسوبة لـ "هاكرز" جزائريين استهدفت موقعي وزارة الادماج الاقتصادي والمقاولات الصغرى والتشغيل والكفاءات وقاعدة بيانات الصندوق الوطني للضمان الاجتماعي (CNSS) وما تبعها من حملات تضليل، وكذا شبكات التضليل الإيرانية التي رصد نشاطها في المغرب ضمن منظومة استهداف دول شمال إفريقيا، إلى جانب شبكات التضليل كـ "Team Jorge" الموثقة في التقارير الدولية.

وبالتركيب بين خريطة الفاعلين المحتملين والسياق الانتخابي المغربي، يمكن رسم ثلاث نقاط استهداف محتملة:

1. التأثير في معادلة المشاركة الانتخابية، إذ يشكل رفع نسب العزوف الانتخابي أداة لإضعاف شرعية أي حكومة منتخبة، وهو هدف متاح تقنيا عبر حملات التثبيط المعلوماتي (Demobilization Campaigns)؛

2. التأثير في توجهات الرأي العام، حول ملف الصحراء والموقف من القضايا الكبرى، نظرا لما تحمله هذه الملفات من شحنة عاطفية وتأثير مباشر في خيارات الناخبين وفي الثقة في المؤسسات.

3. تضخيم خطاب الإحباط والإقصاء الاجتماعي في أوساط الشباب وساكنة الأحياء الشعبية، وهو الخطاب الأكثر قابلية للانتشار الفيروسي على منصات التواصل الاجتماعي.

المطلب الثاني: الاستجابة المغربية في ضوء الدروس الدولية

استجابة للتهديدات الهجينة المستجدة المتصاعدة، ولاسيما تلك التي يمثلها التضليل المعلوماتي ويدعمها الذكاء الاصطناعي؛ شرع المغرب في بناء منظومة دفاعية تجسدت من خلال اتخاذ خطوات على عدة مستويات: تشريعيا، تنظيميا، إعلاميا...

✓ على المستوى التشريعي

يعد تعديل المادة 51 من القانون التنظيمي 11-27 بشأن انتخاب أعضاء مجلس النواب استجابة تشريعية واعية لمخاطر التضليل الانتخابي، بما في ذلك من خلال الذكاء الاصطناعي، وإن أثار نقاشات جدية حول إشكاليات حرية التعبير.[88]

وقد سبق لوزير العدل المغربي "عبد اللطيف وهبي" أن حث البرلمان، في 8 يوليوز 2024، على الإسراع في وضع إطار قانوني ينظم استخدام الذكاء الاصطناعي قبل انتخابات 2026، مؤكدا أن هذا التشريع سيحمي المسار الديمقراطي الوطني من التلاعب الرقمي. وقد شدد الوزير، أمام البرلمان على أن الخطر لم يعد مقتصرا على الأخبار الزائفة، بل يتمثل في قدرة تقنيات الذكاء الاصطناعي على إنتاج محتوى مضلل يصعب على المواطنين التمييز بينه وبين الحقيقة، بما قد يؤدي إلى تشويه الخطاب العام أو المساس بالثوابت الدينية والسياسية.[89]

وقد سعت السلطات المغربية من خلال هذا التعديل إلى تشديد العقوبات على نشر المعلومات الكاذبة الوقائع المختلقة التي تضعف الثقة في المسار الانتخابي في إجراء يجسد الوعي الرسمي بأن

---

[88] تشير التقارير الصحفية بخصوص مجريات المسطرة التشريعية لإقرار القانون التنظيمي رقم 53.25 القاضي بتغيير وتتميم القانون التنظيمي رقم 27.11 المتعلق بمجلس النواب إلى أن وزارة الداخلية المغربية دافعت أمام البرلمان عام 2025 عن تعديل المادة 51 من القانون التنظيمي 11-27، لتجرم نشر الوقائع المختلقة التي تضعف الثقة في المسار الانتخابي، باستعمال وسائل الإعلام والتواصل الحديثة. وأكد وزير الداخلية المغربي أمام البرلمان أن الديمقراطيات حول العالم تواجه حملات تلاعب منظمة عبر شبكات التواصل الاجتماعي، وأن المغرب ملزم بحماية انتخاباته من التدخل الخارجي. أنظر:
"Morocco cites foreign interference risks in push to criminalis<qe election disinformation", 21/11/2025. The "Hespress English" website (Accessed: 02/04/2026): t.ly/tyC1M

[89] محمد عادل التاطو، "وهبي يستعجل تقنين الذكاء الاصطناعي لمواجهة تأثيره على الانتخابات المقبلة بالمغرب"، 2024/07/09، موقع "العمق المغربي" على الإنترنت (آخر ولوج: 2026/04/05): t.ly/j-B_U

حماية نزاهة الاقتراع لم تعد مسألة قانونية إجرائية بحتة، بل باتت رهانا سياديا حقيقيا يتصل بصميم الأمن الوطني في بعده المعلوماتي الجديد.

وقد تضمن النص الجديد للقانون التنظيمي رقم 53.25، القاضي بتغيير وتتميم القانون التنظيمي رقم 27.11 المتعلق بمجلس النواب والصادر في 16 يناير 2026، مقتضيات تروم تشديد العقوبات الحبسية والغرامات المالية المرتبطة بالمخالفات الانتخابية، حيث عاقب كل شخص أقدم، بأي وسيلة، بما في ذلك شبكات التواصل الاجتماعي أو شبكات البث المفتوح أو أدوات الذكاء الاصطناعي أو أي منصة إلكترونية أو تطبيق يعتمد على الإنترنت، على نشر أو إذاعة أو نقل أو بث أو توزيع أخبار زائفة أو إشاعات كاذبة أو غير ذلك من طرق التدليس، على تحويل أصوات الناخبين أو دفع ناخبا أو أكثر إلى الإمساك عن التصويت، بالحبس من سنتين إلى خمس سنوات وبغرامة من 50 ألفا إلى 100 ألف درهم (المادة 51).

تمثل هذه المقتضيات التشريعية من القانون التنظيمي رقم 53.25 الاستجابة التشريعية الأكثر مباشرة وخصوصية في ما يتعلق بالتضليل المعلوماتي الانتخابي. وتعد هذه المقتضيات من الناحية القانونية الأكثر تطورا في المنطقة المغاربية، لاسيما في تصريحها باسم صريح بتجريم توظيف "أدوات الذكاء الاصطناعي" في التضليل الانتخابي، مما يجعل المغرب في طليعة الدول التي أدمجت تقنيات الذكاء الاصطناعي في منظومتها التجريمية الانتخابية. غير أن فاعلية هذه المقتضيات في الردع الفعلي مرهونة بثلاثة شروط تشغيلية تظل موضع تساؤل: أولها قدرة الأجهزة القضائية على الإسناد (Attribution) الجنائي لعمليات التضليل الرقمي ذات المنشأ الخارجي في ظل الغموض التقني الذي يميز التضليل الهجين؛ وثانيها إشكالية الحدود الفاصلة بين حرية التعبير والمعلومات المجرمة، وهو توتر كامن في كل تشريع مناهض للتضليل رصده المراقبون الدوليون في سياق النقاشات البرلمانية التي أحاطت بتعديل المادة 51؛ وثالثها البعد الزمني المرتبط بالتضليل في "نافذته الفيروسية" أي تلك المرحلة الحرجة المحيطة بيوم الاقتراع ذاته، التي قد تقصر عن استيعاب زمن المسطرة القضائية.

وعلى الصعيد القانوني دائما، يشكل القانون رقم 05.20 المتعلق بالأمن السيبراني الصادر في 25 يوليوز 2020 والمرسوم التطبيقي له الصادر في 15 يوليوز 2021، أداة تشريعية محورية في منظومة حماية الفضاء الرقمي المغربي. يعرف القانون الأمن السيبراني في مادته الثانية بوصفه "مجموعة من التدابير والإجراءات ومفاهيم الأمن وطرق إدارة المخاطر والتكوينات وأفضل الممارسات والتكنولوجيات التي تسمح لنظام معلومات أن يقاوم أحداثا مرتبطة بالفضاء السيبراني"، ويحدد في مادته الأولى نطاق تطبيقه ليشمل نظم معلومات إدارات الدولة والجماعات الترابية والمؤسسات العمومية والبنيات التحتية ذات الأهمية الحيوية والمتعهدين التقنيين. والأكثر دلالةً في السياق الانتخابي هو أن هذا

القانون يرسي نظاما لحماية "البنيات التحتية ذات الأهمية الحيوية" يمكن توسيعه ليشمل البنية التحتية الانتخابية، كما يرسي ثلاثية الحماية المعلوماتية (السرية والنزاهة والتوافر) المكرسة في المادة الثانية، وهي ثلاثية ذات أهمية مباشرة في تحصين سجلات الناخبين ونتائج الاقتراع ضد أي تلاعب. ويتمم المرسوم التطبيقي رقم 2.21.406 هذا الإطار بتحديد كيفيات الإبلاغ عن حوادث الأمن السيبراني ومعالجتها، واشتراطات تأهيل مقدمي خدمات افتحاص نظم المعلومات، مما يرسي منظومة تأهيلية تضمن جودة الخدمات الأمنية المقدمة للبنيات الحيوية.[90]

بيد أن التحدي العملي يكمن في أن تحديد "البنيات التحتية ذات الأهمية الحيوية" يتم بموجب نصوص تنظيمية دون إيضاح صريح لما إذا كانت المنظومة الانتخابية مصنفة فيها، مما يثير تساؤلا مشروعا حول نطاق الحماية الفعلية الممنوحة لهذه المنظومة.

✓ على مستوى التنسيق الاستراتيجي والعملياتي

إن نجاح الاستجابة المغربية، وفق ما تقدمه التجارب المقارنة من دروس، تتوقف على إيجاد هيئة تنسيق انتخابي-سيبراني متخصص يماثل الفريق الاستخباراتي-الأمني الذي أطّر الاستجابة الأمريكية عبر مجلس الأمن القومي و"مركز التأثير الأجنبي الخبيث" "FMIC" ومكتب "FBI".

ويبدو أن المنظومة المغربية، ومن خلال اللجنة الاستراتيجية للأمن السيبراني، تتوفر على آلية تنسيقية واضحة وموحدة تجمع في تشكيلة واحدة، تحت رئاسة الوزير المنتدب لدى رئيس الحكومة المكلف بإدارة الدفاع الوطني، كلا من وزارة الداخلية المشرفة على العملية الانتخابية ومختلف الفاعلين المؤسساتيين من وزراء ورؤساء هيئات أمنية وعسكرية واستخباراتية، يمكنها أن تضطلع بهذا الدور.

يمثل إحداث اللجنة الاستراتيجية للأمن السيبراني بموجب القانون رقم 20-05 بتاريخ 25 يوليوز 2020 خطوة مؤسسة في بناء منظومة وطنية متكاملة لمواجهة التهديدات الهجينة المتصاعدة. فهذه اللجنة تضطلع بدور تنسيقي بين مختلف الفاعلين المؤسساتيين لتوحيد الرؤية الاستراتيجية، وضمان انسجام السياسات العمومية في مجال الحماية الرقمية. كما أنها تضع إطارا قانونيا وتنظيميا يتيح تعبئة الموارد التقنية والبشرية لمواجهة المخاطر الجديدة، وعلى رأسها التضليل المعلوماتي المدعوم بتقنيات الذكاء الاصطناعي. بهذا المعنى، يشكل وجود اللجنة آلية استباقية لتعزيز اليقظة الوطنية، وتطوير قدرات الرصد والتحليل، وصياغة خطط استجابة سريعة وفعالة، بما يرسخ قدرة المغرب على حماية فضائه السيبراني وصون نزاهة عملياته الديمقراطية أمام موجة التهديدات الهجينة.[91]

---

[90] أنظر النص الكامل للقانون رقم 05.20 المتعلق بالأمن السيبراني الصادر في 25 يوليوز 2020 والمرسوم التطبيقي له رقم 2.21.406 الصادر في 15 يوليوز 2021، على موقع "المديرية العامة لأمن نظم المعلومات" (آخر ولوج: 2026/04/04): t.ly/kOOXQ

[91] أنظر أدوار اللجنة على موقع "المديرية العامة لأمن نظم المعلومات" (آخر ولوج: 2026/04/04): t.ly/Ehk9S

وعمليا، يمثل إحداث "لجنة إدارة الأزمات والأحداث السيبرانية الجسيمة" بموجب المادة 36 من القانون رقم 05.20 ركيزة عملية في المنظومة المغربية للأمن السيبراني. هذه اللجنة، التي تترأسها المديرية العامة لأمن نظم المعلومات، وتضم ممثلين عن وزارة الداخلية وهيئات أمنية وعسكرية واستخباراتية، مما يمنحها طابعا تنسيقيا شاملا بين الفاعلين الأمنيين والعسكريين والاستخباراتيين في مختلف أجهزة الدولة، دورها الأساسي هو ضمان التدخل المنسق عند وقوع حوادث أو هجمات سيبرانية جسيمة، من خلال آليات الوقاية، الرصد، والتحكم في تداعيات الأزمات. وبهذا، تشكّل اللجنة أداة استجابة جماعية وسريعة، تعزز قدرة المغرب على مواجهة التهديدات الهجينة، بما فيها التضليل المعلوماتي المدعوم بالذكاء الاصطناعي، عبر تعبئة الموارد الوطنية وتوحيد القرار الاستراتيجي في لحظات الخطر.[92]

تؤسس إذن اللجنة الاستراتيجية البنية التحتية القانونية والمؤسساتية وتعمل على التحصين المسبق، بينما لجنة إدارة الأزمات تُفعّل هذه البنية عند وقوع تهديدات أو هجمات فعلية. وبهذا، يشكل عملهما معا منظومة متكاملة تجمع بين الوقاية الاستباقية والاستجابة التفاعلية، وهو ما يعزز قدرة المغرب على مواجهة التهديدات الهجينة، خاصة التضليل المعلوماتي المدعوم بالذكاء الاصطناعي.

وفي سياق يتسم بتصاعد التهديدات السيبرانية والتقادم التدريجي للحلول التقليدية، يخطو المغرب خطوة استراتيجية من خلال إحداث مركز الابتكار في الأمن السيبراني، وهو كيان ذو منفعة عامة يجسد إنشاؤه إرادة سياسية قوية لاستباق التهديدات الرقمية، وتعزيز السيادة التكنولوجية الوطنية، من خلال تشجيع بروز كفاءات محلية، وحلول مبتكرة، وتكامل بين القطاعين العام والخاص والقطاع الأكاديمي. ومن المأمول أن يُشكل، على المدى البعيد، فاعلا أساسيا في الذكاء الجماعي الوطني للاستجابة بفعالية للتحديات الراهنة والمستقبلية المرتبطة بأمن نظم المعلومات، وحماية البنيات التحتية الحيوية، والدفاع عن المعطيات الحساسة.[93]

✓ على المستوى التنفيذي

تعد المديرية العامة لأمن نظم المعلومات (DGSSI) التابعة لإدارة الدفاع الوطني، والمحدثة بموجب المرسوم رقم 2.11.509 بتاريخ 21 سبتمبر 2011، الجهاز الوطني المرجعي في مجال تأمين نظم المعلومات وحماية الفضاء السيبراني. وتضطلع المديرية بمهام محورية تشمل: صياغة السياسات

[92] نفس المرجع السابق.

[93] صدر القرار المشترك رقم 1148.25 المتعلق بالمصادقة على الاتفاقية المؤسسة لمركز الابتكار في الأمن السيبراني. ونشر في الجريدة الرسمية عدد 7407، بتاريخ 6 ماي 2025. أنظر موقع "المديرية العامة لأمن نظم المعلومات" (آخر ولوج: 2026/04/04): t.ly/-HIbN

والاستراتيجيات الوطنية للأمن السيبراني، وإرساء الأطر التشريعية والتنظيمية، وإجراء عمليات افتحاص نظم معلومات الإدارات والمؤسسات العمومية والبنى التحتية ذات الأهمية الحيوية، فضلا عن تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية (maCERT).

وفي سياق الاستحقاق الانتخابي 2026، تكتسب هذه المديرية دورا محوريا متوقعا في حماية البنية التحتية المعلوماتية الانتخابية، من منظومة سجلات الناخبين إلى أنظمة إدارة نتائج الاقتراع، وفق ما توجبه المادة 41 من القانون رقم 05.20 التي تخول أعوان السلطة الوطنية صلاحيات التحري اللازمة عند وقوع أي هجوم إلكتروني يمس بالوظائف الحيوية للمجتمع. وفي شتنبر 2025، عيّن الملك محمد السادس مديرا عاما جديدا لـ "DGSSI"، وهو اللواء "عبد الله بوطريك"، في ما يقرأ بوصفه دفعا بقيادة متجددة لتحسين أداء هذا الجهاز الاستراتيجي في مرحلة بالغة الحساسية.[94]

✓ على المستوى الإعلامي

يشكل إعلان وزارة الثقافة والشباب والتواصل المغربية عن إنشاء منظومة رصد إعلامي لمواجهة التضليل،[95] عنصرا محوريا من شأنه أن يسهم في بناء استجابة وطنية لحماية نزاهة الانتخابات أمام التهديدات الهجينة المستجدة المتصاعدة.

إن توجيه هذه المنظومة باتجاه متابعة تدفقات الأخبار والمحتوى الرقمي بشكل لحظي، ورصد الحملات الممنهجة التي تستهدف التشويش على العملية الانتخابية أو تقويض الثقة في المؤسسات، من خلال أدوات تحليل البيانات والذكاء الاصطناعي، قد يتيح التعرف المبكر على الأنماط التضليلية، سواء كانت محلية أو مدعومة من جهات خارجية، ومن ثم تنسيق الردود بين الإعلام العمومي والهيئات التنظيمية والأمنية. وبهذا، فهي لا تقتصر على كشف الأخبار الزائفة، بل تساهم في تحصين الرأي العام عبر التوعية الاستباقية، وتوفير أدلة موثوقة للهيئات القضائية والانتخابية، مما يعزز قدرة المغرب على حماية مساره الديمقراطي من حملات التضليل المعلوماتي المدعومة بتقنيات الذكاء الاصطناعي.

وينبغي القول، على الرغم من كل هذه التدابير، بأن ثمة هوة تفصل بين هذه التدابير والمنظومة الدفاعية الشاملة التي تستوجبها المرحلة. لاسيما عندما نعلم أن الانتخابات المغربية المرتقبة في 2026 تصادف مرحلة استثنائية يتوفر فيها رصيد تجريبي دولي مهم، فبعد انتخابات 2024 التي

---

[94] "الملك محمد السادس يعيّن مديراً جديداً لأمن نظم المعلومات في المغرب"، 2025/09/01. موقع "هسبريس" على الإنترنت (آخر ولوج: 2026/04/04): t.ly/HGrwL

[95] Disinformation Social Media Alliance (DISA), "Combating Disinformation in Morocco", 01/07/2025. The "DISA" website (Accessed: 02/04/2026): t.ly/-PtAa

أثبتت مواطن قوة وضعف المنظومتين الأمريكية والأوروبية في التصدي للتهديدات الهجينة المستجدة، يمتلك المغرب لأول مرة خريطة نسبيا محددة للأدوات الأكثر نجاعة والثغرات الأكثر خطورة.

وما يميز الحالة المغربية أن منظومة استجابتها الدفاعية المؤسسية التي تم إنشاؤها ليست متمحورة حول الشأن الانتخابي كما هو الشأن في التجربتين الأمريكية والأوروبية، ولكن نظام الحماية الذي ترسيه يمكن توسيعه ليشمل البنية التحتية الانتخابية باعتبارها "بنيات تحتية ذات أهمية حيوية".

وتكشف المقارنة مع التجربتين الأمريكية والأوروبية عن ثلاثة دروس إجرائية ذات أولوية مباشرة للحالة المغربية تستوجب أخذها بالاعتبار قبل شتنبر 2026:

- **أولها** أهمية الاستجابة الاستباقية من خلال "التفنيد المسبق"(Pre-bunking)، التي أثبتت الدراسات التجريبية، ولاسيما دراسة انتخابات البرلمان الأوروبي 2024، فاعليتها في الحد من انتشار التضليل الانتخابي قُبيل يوم الاقتراع مباشرة، مقارنة بالاستجابة التفاعلية التي تأتي بعد انتشار المحتوى المضلل؛[96]

- **وثانيها** أن الشراكة المؤسسية مع المنصات الرقمية الكبرى (Meta, Google, TikTok, X) المهيمنة على الفضاء المعلوماتي الانتخابي المغربي، على غرار ما فعله الاتحاد الأوروبي عبر قانون"DSA"، باتت شرطا بنيويا لا اختيارا سياسيا، حيث تتيح هذه الشراكة رصد الحملات المضللة بصورة منسّقة في الزمن الفعلي؛

- **وثالثها** أن التنسيق الاستخباراتي مع الشركاء الدوليين لمتابعة حوادث (FIMI)ذات الصلة بالفضاء الانتخابي المغربي يشكل الجسر الذي يحول الوعي بالتهديد إلى استجابة آنية منسّقة، لاسيما أمام محدودية القدرات الوطنية لكشف المحتوى المولد بالذكاء الاصطناعي والتزييف العميق. صحيح أن القانون التنظيمي 53.25 يجرم توظيف الذكاء الاصطناعي في التضليل الانتخابي، لكن التجريم وحده لا يستتبع تلقائيا امتلاك قدرات كشف تقنية فاعلة.

وإذا كان المغرب يمتلك اليوم منظومة تشريعية وطنية رصينة نسبيا قياسا على محيطه الإقليمي، فإن الجسر بين الوجود القانوني والفاعلية التنفيذية الآنية لايزال التحدي الأكثر إلحاحا في أفق انتخابات شتنبر 2026، وهو التحدي ذاته الذي يعد درسا محوريا تستخلصه الأدبيات المتخصصة في مجال الأمن الانتخابي المقارن.

[96] أثبتت الدراسة أن نهج التوعية الاستباقية يخفف من تأثيرات التضليل الانتخابي بصورة أكثر فاعلية من الاستجابة التفاعلية. أنظر: Farooq AQSA & al., op. cit.

خاتمة

في ختام هذه الورقة البحثية، يمكن القول بأن انتخابات المغرب 2026 ليست شأنا داخليا معزولا، بل هي حلقة تجري في سياق التنافس الدولي على النفوذ في المنطقة، في ضوء ما أبانه الإطار النظري الواقعي الجديد من آليات بنيوية تدفع الفاعلين الدوليين نحو توظيف الاستحقاقات الانتخابية لتحقيق مكاسب نسبية في موازين القوى.

وقد أثبتت الدراسة الفرضية الأولى بشأن العلاقة الطردية بين تصاعد التنافس الدولي في منطقة ما وتنامي احتمالات التدخل في انتخاباتها، إذ رصدنا حجم التنافس المتصاعد على الفضاء المغاربي من قبل قوى إقليمية ودولية متعددة. كما أثبتت الدراسة الفرضية الثانية المتعلقة بالتحول النوعي الذي أحدثه الذكاء الاصطناعي التوليدي في بيئة تهديدات التضليل المعلوماتي، من خلال تخفيضه لتكلفة الإنتاج ورفعه لدقة الاستهداف. وأما الفرضية الثالثة المتعلقة باستلزام التصدي لهذه التهديدات منظومة دفاعية متكاملة، فقد جاءت التوصيات المقترحة أسفله ترجمة عملية لها.

وفي المحصلة، يبدو أن رهان الانتخابات المغربية 2026 في بعده الأمني المعلوماتي ليس مجرد اختبار لنزاهة صناديق الاقتراع، بل اختبار لمدى قدرة المؤسسات الوطنية على حماية البيئة المعلوماتية المحيطة بهذه الصناديق في ظل بيئة دولية تصنف التضليل المعلوماتي للعام الثاني تواليا، الخطر الأول على الاستقرار الدولي في المدى القصير.

وهذا يعني أن الدولة المغربية يجب أن تكون قادرة على اختيار نظمها السياسية والاقتصادية دون أي تدخل أو تأثير من دول أخرى مثل استخدام الذكاء الاصطناعي للتأثير على الرأي العام وتغيير نتائج الانتخابات. لذلك، تعتمد السيادة التكنولوجية على أنواع أخرى من السيادة، على سبيل المثال، السيادة في الابتكار والعلم. السيادة التكنولوجية هي شرط للسيادة كمبدأ من مبادئ القانون الدولي وهي مفتاح لأنواع أخرى من السيادة (الاقتصادية، الزراعية، العلمية، الابتكار). وهذا يفسر السباق والمنافسة على الذكاء الاصطناعي والسيادة التكنولوجية.

استنادا إلى التحليل السابق، تقترح جملة من **التوصيات السياسية المنهجية** من أجل منظومة دفاع انتخابي سيادي، وزعت على ثلاثة مستويات متكاملة:

✓ المستوى التشريعي والمؤسسي

ينبغي للمغرب أن يطور إطارا قانونيا شاملا خاصا بالأمن المعلوماتي الانتخابي (Electoral Cybersecurity Framework)، يتجاوز التدابير التشريعية الراهنة نحو صياغة منظومة متكاملة تعالج التضليل المعلوماتي، وتمويل الحملات من مصادر أجنبية مجهولة، والهجمات السيبرانية على بنيتها التحتية. ويستدعي ذلك مراجعة منتظمة للإطار القانوني في ضوء التطورات المتسارعة في أدوات الذكاء الاصطناعي، مع الاستئناس بالتجارب الدولية الرائدة في هذا الشأن التي تم تناولها في هذه الدراسة.

كما توصي الدراسة بإنشاء هيئة مستقلة للأمن المعلوماتي الانتخابي تضم في عضويتها خبراء في العلاقات الدولية والأمن السيبراني وعلوم الاتصال، تكلف بمهام الرصد الدوري ووضع التقارير والتنسيق مع المنظومة الدولية لأمن الانتخابات.

✓ المستوى التقني والرقمي

في مواجهة التهديدات الرقمية المتصاعدة، توصي الدراسة بتعزيز الشراكة مع المنصات الرقمية الكبرى لوضع بروتوكولات استجابة سريعة لحملات التضليل المرتبطة بالانتخابات المغربية، واستثمار تجارب دولية كالتجربتين الأوروبية والأمريكية. ويمتد ذلك إلى الاستثمار في تطوير قدرات وطنية للكشف الآلي عن المحتوى المولد بالذكاء الاصطناعي، وإنشاء مختبر وطني للتحقق من المعلومات (Fact-Checking Lab) يعمل في زمن قريب من الزمن الفعلي خلال الفترة الانتخابية.

✓ المستوى الدبلوماسي والإقليمي

ينبغي للمغرب أن يفعّل الدبلوماسية الوقائية في هذا المجال من خلال بناء تحالفات إقليمية مع دول تشترك في مواجهة تهديدات التضليل الانتخابي، وإطار ثنائي ومتعدد الأطراف لتبادل المعلومات حول عمليات التدخل الخارجي الموثقة.

وتجدر الإشارة هنا إلى أن هذا الأمن الانتخابي يتجاوز بعده التقني ليمس صميم السيادة الوطنية بمفهومها الواقعي الجديد؛ إذ إن قدرة الدولة على حماية مسارها الانتخابي من التدخلات الخارجية تجسد قدرتها على صون وضعها النسبي في النظام الدولي، وحماية لمكانتها الجيوسياسية من أشكال التقويض الناعم المتصاعدة.

وختاما، يقترح هذا المقال جملة من مسارات البحث المستقبلي التي يمكن أن تثري هذا الحقل المعرفي الناشئ: أولها دراسة مقارنة لتجارب دول مغاربية وإفريقية في مجال التصدي لحملات التضليل

الانتخابي، وثانيها بحث تجريبي في أثر حملات التضليل على معدلات التصويت وسلوك الناخبين في السياق المغربي، وثالثها دراسة الفجوة بين المنظومة التشريعية الراهنة ومتطلبات أمن الانتخابات في عصر الذكاء الاصطناعي.

وأخيرا، فإن السيادة الانتخابية في القرن الحادي والعشرين لا تقاس فقط بنزاهة صناديق الاقتراع، بل أيضا بمتانة البيئة المعلوماتية المحيطة بها، أي بالسيادة التكنولوجية؛ فكما لا يمكن ضمان انتخابات نظيفة في ظل "الإفساد المالي"، لا يمكن ضمانها في ظل إفساد "المعلومات المضللة".

لائحة المراجع والمصادر

مراجع ومصادر باللغة العربية

- **الكتب والمساهمات**

- أناتولي أوتكين، "الإستراتيجية الأمريكية للقرن الحادي والعشرين"، ترجمة: محمد نصر الدين الجبالي وأنور محمد إبراهيم، القاهرة: المجلس الأعلى للثقافة، الطبعة الأولى 2003.
- جون ميرشايمر، "مأساة سياسات القوى العظمى"، ترجمة: مصطفى محمد قاسم، الرياض: جامعة الملك سعود، 2012.

- **المنشورات الإلكترونية بمواقع الإنترنت**

- جان-غابريال غاناسيا، "الذكاء الاصطناعي: بين الأسطورة والواقع"، 2018/06/29، موقع "اليونسكو" على الإنترنت (آخر ولوج: 2026/04/05): t.ly/uSz__g
- محمد عادل التاطو، "وهبي يستعجل تقنين الذكاء الاصطناعي لمواجهة تأثيره على الانتخابات المقبلة بالمغرب"، 2024/07/09، موقع "العمق المغربي" على الإنترنت (آخر زيارة: 2026/04/05): t.ly/j-B__U
- مركز أفريقيا للدراسات الاستراتيجية، "خريطة موجة المعلومات المضللة في إفريقيا"، 2024/04/03، موقع "مركز أفريقيا للدراسات الاستراتيجية" على الإنترنت (آخر ولوج: 2026/04/04): t.ly/__xXcP
- موقع "المديرية العامة لأمن نظم المعلومات" (آخر ولوج: 2026/04/04): t.ly/Ehk9S - t.ly/kOOXQ - t.ly/-HibN
- "الملك محمد السادس يعين مديرا جديدا لأمن نظم المعلومات في المغرب"، 2025/09/01. موقع "هسبريس" على الإنترنت (آخر ولوج: 2026/04/04): t.ly/HGrwL

- **الوثائق**

- القانون التنظيمي رقم 53.25 القاضي بتغيير وتتميم القانون التنظيمي رقم 27.11 المتعلق بمجلس النواب الصادر في 16 يناير 2026.

- القانون رقم 05.20 المتعلق بالأمن السيبراني الصادر في 25 يوليوز 2020 والمرسوم التطبيقي له رقم 2.21.406 الصادر في 15 يوليوز 2021.
- القرار المشترك رقم 1148.25 المتعلق بالمصادقة على الاتفاقية المؤسسة لمركز الابتكار في الأمن السيبراني، الجريدة الرسمية عدد 7407، بتاريخ 6 ماي 2025.

مراجع ومصادر باللغة الإنجليزية

- **الكتب والمساهمات**

- Anzera GIUSEPPE, Alessandra MASSA, "Using International Relations Theories to Understand Disinformation: Soft Power, Narrative Turns, and New Wars" in "Politics of Disinformation" (eds. Guillermo LÓPEZ-GARCÍA لله al.), John WILEY لله Sons, 2021, pp. 35–47.
- Christina NEMR, William GANGWARE, "Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age", Washington D.C.: Park Advisors, March 2019.
- Fatima ROUMATE, "Artificial Intelligence and the New World Order, New weapons, New Wars and a New Balance of Power", Switzerland: The Springer, 2024.
- Frank G. HOFFMAN, "Conflict in the 21st century: the rise of hybrid wars", Potomac Institute for Policy Studies, Arlington, Virginia, December 2007.
- Jaemin LEE, "Artificial Intelligence and International Law", Singapore: Springer Nature, 2022.
- John J. MEARSHEIMER, The Tragedy of Great Power Politics", New York: W.W. Norton, 2001.
- Joseph S. NYE, "The Future of Power", New York: PublicAffairs, 2011.
- Kenneth N. WALTZ, "Theory of International Politics", Reading: Addison-Wesley, 1979.
- Lucas KELLO, "The virtual weapon: and international order", New Haven CT: Yale University Press, 2017.

- Thomas RID, "Active Measures: The Secret History of Disinformation and Political Warfare", New York: Farrar, Straus and Giroux, 2020.

- المقالات والدراسات بالدوريات العلمية

- David LAZER et al., "The Science of Fake News", Science, Vol. 359, No. 6380, March 9, 2018, pp. 1094-1096. doi: 10.1126/science.aao2998.
- Dov H. LEVIN, "When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results". International Studies Quarterly, Vol. 60, No. 2, 2016, pp. 189-202. doi.org/10.1093/isq/sqv016
- Farooq AQSA لله al., "Generative AI Generating Concerns: Citizens' Perspectives During the 2024 European Elections", The International Journal of Press/Politics, 2025. The "Sage journals" website (Accessed: 02/04/2026): doi.org/10.1177/19401612251376060
- Jon ROOZENBEEK لله al., "Susceptibility to Misinformation about COVID-19 Around the World", Royal Society Open Science, Vol. 7, N° 10, 2020. dx.doi.org/10.1098/rsos.201199
- Joseph S. NYE, "How Sharp Power Threatens Soft Power", Foreign Affairs, 24/01/2018.
- Robert CHESNEY, Danielle CITRON, "Deep Fakes: A Looming Challenge for Privacy, Democracy and National Security", California Law Review, Vol. 107, 2019, pp. 1753-1820. doi.org/10.15779/Z38RV0D15J
- Soroush VOSOUGHI, Deb ROY, Sinan ARAL, "The Spread of True and False News Online", Science, Vol. 359, No. 6380, March 9, 2018, pp. 1146-1151. doi: 10.1126/science.aap9559.
- Susana SANZ-CABALLERO, "The Concepts and Laws Applicable to Hybrid Threats, with a Special Focus on Europe", Humanities and Social Sciences Communications, Vol. 10, N° 360, 2023. doi.org/10.1057/s41599-023-01864-y

- Tim HAYWARD, "The Problem of Disinformation: A Critical Approach", Social Epistemology, Vol. 39, No. 1, 2024, pp. 1-23. doi.org/10.1080/02691728.2024.2346127

- **الوثائق والتقارير الدولية**

- Claire WARDLE, Hossein DERAKHSHAN, "Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking", Council of Europe Report DGI(2017)09, Strasbourg: Council of Europe, October 2017.
- Council of Europe Congress, "Foreign Interference in Electoral Processes at Local and Regional Levels", Report CG(2025)48-10, 26/03/2025.
- Council of Europe, "Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law", CETS No. 225, Adopted 17/05/2024, Opened for signature 05/09/2024.
- European Commission لله High Representative of the Union for Foreign Affairs and Security Policy, "Joint Framework on countering hybrid threats: a European Union response", JOIN(2016) 18 final, 06/04/2016.
- European Commission (EC), "Report on the 2024 Elections to the European Parliament", COM(2025) 287 final, 06/06/2025.
- European Digital Media Observatory (EDMO), "Final Report Outputs and outcomes of a community-wide effort", 26/07/2024.
- European External Action Service (EEAS), 3rd Annual Report on Foreign Information Manipulation and Interference (FIMI) Threats: Exposing the Architecture of FIMI Operations", March 2025.
- European Parliament, "RECOMMENDATION on the draft Council decision on the conclusion, on behalf of the European Union, of the Council of Europe Framework Convention on Artificial Intelligence and

Human Rights, Democracy and the Rule of Law", A10-0007/2026, 02/02/2026.

- European Parliament Research Service (EPRS), "Information Manipulation in the Age of Generative Artificial Intelligence", Briefing PE 779.259, Brussels: European Parliament, December 2025.
- "Executive Order 13848: Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election", 12/09/2018.
- FIMI-ISAC, "Collective Findings Report on 2024 European Elections", October 2024.
- Freedom House, "Freedom on the Net 2023: Morocco Country Report", 2023.
- International Crisis Group (ICG), "Managing Tensions between Algeria and Morocco", Report No 247, 29/11/2024.
- Public Law 115–232—§1043(a)(2), 13/08/2018.
- Robert S. Mueller III, "Report on the Investigation into Russian Interference in the 2016 Presidential Election", Vol. I, Washington D.C.: U.S. Department of Justice, March 2019.
- The European External Action Service (EEAS), "4th EEAS Report on FIMI Threats: Dismantling the FIMI House of Cards", March 2026.
- The White House, "Presidential Policy Directive 41 (PPD-41): United States Cyber Incident Coordination", 26/07/2016.
- The World Commission on the Ethics of Scientific Knowledge and Technology (COMEST), "Preliminary study on the ethics of Artificial Intelligence", 26/02/2019.
- U.S. Senate Select Committee on Intelligence (SSCI), "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election", Vol. 2: Russia's Use of Social Media, Washington D.C.: SSCI, 18/08/2020.
- World Economic Forum (WEF), "Global Risks Report 2024", Switzerland – Geneva: WEF, 19th Edition, 2024.

- World Economic Forum (WEF), "Global Risks Report 2025", Switzerland – Geneva: WEF, 2025.

- **المنشورات الإلكترونية بمواقع الإنترنت**

- "Analysts Warn of Political Tensions Ahead of Morocco's 2026 Legislative Elections", 10/11/2025. The "Hespress English" website (Accessed: 02/04/2026): t.ly/5M0r_
- Council of the European Union, "Democratic resilience: Council approves conclusions on safeguarding electoral processes from foreign interference", 21/05/2024. The "Council of the EU" and the "European Council" website (Accessed: 02/04/2026): t.ly/OG8GG
- Disinformation Social Media Alliance (DISA), "Combating Disinformation in Morocco", 01/07/2025. The "DISA" website (Accessed: 02/04/2026): t.ly/-PtAa
- European Digital Media Observatory (EDMO), "EU Election Disinfo Bulletin", 2024. The "EDMO" website (Accessed: 02/04/2026): t.ly/cbw35
- European External Action Service (EEAS), "Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI)", The "EEAS" website (Accessed: 07/04/2026): t.ly/WQAJq
- Global Disinformation Index (GDI), "Gendered Disinformation in the European Parliamentary Elections", 10/06/2024. The "GDI" website (Accessed: 02/04/2026): t.ly/-vNsI
- Hamza MEDDEB, "Economic Statecraft as Geopolitical Strategy: New Dimensions of Moroccan-Algerian Rivalry", 22/07/2025. The " Carnegie Endowment for International Peace (CEIP)" website (Accessed: 02/04/2026): t.ly/YO7W0
- "How the US Protects Elections from Foreign Interference", 01/09/2025, The "GovFacts" website (Accessed: 07/04/2026): t.ly/4G6a7

- Jenna MCLAUGHLIN, "Efforts to Fight Foreign Influence and Protect Elections in Question under Trump", 11/02/2025. The "NPR" website (Accessed: 02/04/2026): t.ly/9jk2-
- Ken DILANIAN, "Pam Bondi ends FBI effort to combat foreign influence in U.S. politics", 07/02/2025. The " nbcnews" website (Accessed: 07/04/2026): t.ly/QmLS3
- Khadija TAOUIL, "Moroccan Political Parties Present Their Proposals for Electoral Code Reform", 16/08/2025. The "Atalayar" website (Accessed: 02/04/2026): t.ly/3zJsi
- Kyle HIEBERT, "Foreign Interest in Africa Comes with Damaging Disinformation Tactics", 05/02/2025. The "Institute for Security Studies (ISS)" website (Accessed: 02/04/2026): t.ly/FdrYd
- Lawrence NORDEN, "How the Federal Government Is Undermining Election Security", 14/04/2025. The " Brennan Center for Justice (BCJ)" website (Accessed: 05/04/2026): t.ly/okvAn
- Linda ROBINSON, "European Tech Law Faces Test to Address Interference, Threats and Disinformation in 2024 Elections", 22/05/2024. The "Council on Foreign Relations (CFR)" website (Accessed: 02/04/2026): t.ly/PQtwy
- Mohamed ALAOUI, "Survey Reveals Widespread Distrust of Political Parties in Morocco", 22/09/2025. The "Arab Weekly" website (Accessed: 02/04/2026): t.ly/IsPBs
- "Morocco cites foreign interference risks in push to criminalise election disinformation", 21/11/2025. The "Hespress English" website (Accessed: 02/04/2026): t.ly/tyC1M
- Nad'a KOVALČÍKOVÁ, Giuseppe SPATAFORA, "The future of democracy: lessons from the US fight against foreign electoral interference in 2024", Brussels: EU Institute for Security Studies

(EUISS), 17/12/2024. The "EUISS" website (Accessed: 07/04/2026): t.ly/BF9yf

- Nikki FLORIS, "Securing America's Elections: Oversight of Government Agencies", Statement Before the House Judiciary Committee, 22/10/2019, The "Federal Bureau of Investigation (FBI)" website (Accessed: 07/04/2026): t.ly/R8Cne
- Office of the Director of National Intelligence (ODNI), "Foreign Malign Influence Center (FMIC)", The "ODNI" website (Accessed: 02/04/2026): t.ly/iAmus
- Raluca CSERNATONI, "Can Democracy Survive the Disruptive Power of AI?", 18/12/2024. The "Carnegie Endowment for International Peace (CEIP)" website (Accessed: 02/04/2026): t.ly/nhK-T
- Stefan BECKET لله al., "2020 election 'most secure in history', security officials say" - Sara COOK, "Election infrastructure officials: 2020 election was 'most secure in American history' ", 13/11/2020. The "CBS News" website (Accessed: 05/04/2026): t.ly/oaTBP
- The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), "Hybrid threats as a concept", the "Hybrid CoE" website (Accessed: 02/04/2026): t.ly/NxPQk