رؤى عالمية

العدد 32، أغسطس 2024

البيانات الضخمة:
كيف تغيرت قواعد اللعبة العالمية في مجال الأمن القومي؟

المستقبل
للأبحاث والدراسات المتقدمة

تحرير:

مصطفى ربيع

رئيس برنامج المؤشرات وتحليلات البيانات
المستقبل للأبحاث والدراسات المتقدمة

مع بداية حقبة الألفينيات، أتاح التقدم التكنولوجي في قدرات كل من البرمجيات والأجهزة الحاسوبية، للعديد من المنظمات المهتمة بالبيانات، آفاقاً جديدة من زاوية القدرة على جمع ومعالجة المزيد من البيانات والاستخلاص الأعمق للمعلومات والرؤى منها، وقد مكن من ذلك أيضاً؛ الانفجار الهائل في كم البيانات القابلة لتوليدها من مصادر متعددة لجمع البيانات مثل: شبكة الإنترنت وشبكات التواصل الاجتماعي والأجهزة المتصلة بالإنترنت التي تعرف بإنترنت الأشياء وغيرها.

ومن هنا ظهر مفهوم «البيانات الضخمةBig Data » كأحد المفاهيم التي ما زالت قيد التشكل، والتي جرى استخدامها لوصف الكميات الهائلة وغير المُنظمة من البيانات المُنتجة من مصادر متعددة وغير القابلة لجمعها في قاعدة بيانات ارتباطية واحدة، مثل: المعاملات اليومية للأفراد على الإنترنت وعلى شبكات ووسائل التواصل الاجتماعي، وكذلك البيانات التي تُنتجها الأجهزة المتصلة بإنترنت الأشياء ككاميرات المراقبة العامة، وغيرها من مصادر البيانات[1]. وتشير التوقعات إلى ارتفاع هائل في حجم ونسبة البيانات الضخمة من إجمالي البيانات بالعالم، لتصل إلى نحو 200 ألف إكسابايت[2] في عام 2026؛ بما يشكل نحو 90% من إجمالي البيانات بالعالم، وتشير التوقعات ذاتها إلى أن نحو 45% من هذه البيانات حساسة للغاية ولكنها غير محمية[3].

وعلى الجانب الآخر، ارتبط بظهور البيانات الضخمة مفهوم ثانٍ، وهو «تحليل البيانات الضخمةBig Data Analytics»؛ والذي يُعبر عن القدرة على عملية المعالجة المنهجية لكميات كبيرة ومعقدة من البيانات؛ بهدف استخلاص معلومات ورؤى ذات صلة بالبيانات التي تمت معالجتها، وذلك عبر اكتشاف الاتجاهات والارتباطات والأنماط المشتركة لهذه البيانات؛ ما يسهم في مساعدة المُحللين على اتخاذ قرارات قائمة على هذه البيانات. وتتطلب الحالة المُعقدة لهذه البيانات، الاعتماد في تحليلها/ معالجتها على التقنيات الأكثر تقدماً والقائمة على الذكاء الاصطناعي مثل تعلم الآلة.

هذا الكم الهائل والمعقد من البيانات الضخمة، والاتساع في انتشار التكنولوجيات المرتبطة بها وبخاصة الذكاء الاصطناعي وتعلم الآلة، وما تفرضه هذه التكنولوجيات من حالة ترابط رقمي شديدة التعقيد، تغطي حيوات الأفراد بنمط شبه كامل في كلا العالمين الواقعي والرقمي، دفع العديد من مؤسسات وأصحاب الرؤى والخبرات العالمية إلى الجدال بالتأثيرات العميقة للبيانات الضخمة في المجتمع ككل. ليس ذلك على المستويات الإيجابية والفرص فحسب، ولكن على مستوى التهديدات التي قد تفرضها إتاحة وإمكانية الوصول إلى هذا الكم من البيانات، على أمن الأفراد، بل وعلى الأمن القومي للدولة ككل.

المحتويات:

البيانات الضخمة:

كيف تغيرت قواعد اللعبة العالمية في مجال الأمن القومي؟

يشير مفهوم «الأمن القومي National Security» إلى القدرة على حماية الدولة ومواطنيها ومصالحهم، والدفاع عنهم ضد المخاطر الداخلية والخارجية، والتي قد تتراوح ما بين مخاطر جيوسياسية أو اقتصادية أو أية مخاطر أخرى[4]. ومن ثم تستعرض هذه الورقة الرؤى التي قدمتها مراكز الفكر والدراسات، والخبراء العالميين وتقييماتهم وتجاربهم، حول التأثيرات التي قد تخلفها استخدامات وتطبيقات البيانات الضخمة في الوقت الحالي، في مجال الأمن القومي للدول، بمعنى؛ إلى أي مدى تحقق هذه البيانات حماية الدول ومواطنيها ومصالحهم؟ وإلى أي مدى أيضاً يمكن لهذه البيانات والتكنولوجيات المرتبطة بها وتطبيقاتها أن تهدد الأمن القومي وتفرض مخاطر جديدة على مواطنيها ومصالحهم؟

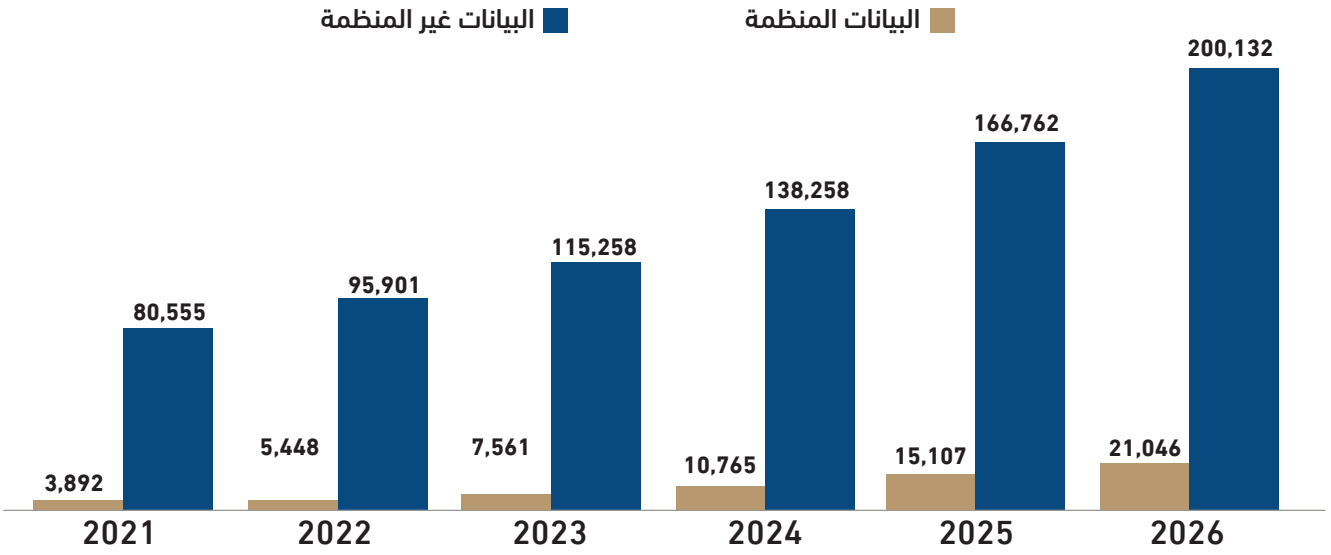
تحولات أمنية في عصر البيانات الضخمة:

يناقش «معهد لووي Lowy Institute»، كيف يُغير نشوء البيانات الضخمة والتكنولوجيات المرتبطة بعملية معالجتها، النظرة إلى الأمن القومي للدول ومواطنيها، وذلك بالتطرق إلى هيمنة ثلاثة ملامح بارزة لهذه البيانات على حياة المواطنين، على النحو التالي[5]:

1- تحويل المواطنين إلى بيانات رقمية: يشير المعهد إلى أن خطورة البيانات الضخمة ليست في حجمها نفسه، بقدر ما تعبر عنه أو تحمله هذه البيانات عن المواطنين؛ لافتاً إلى أن هذه البيانات هي وببساطة ترجمة للتصرفات والعادات اليومية للأفراد، مثل: اهتماماتهم التي يبحثون عنها على مُحركات البحث على الإنترنت، وحجم وأنواع مشترياتهم، وسجلات تطور لياقاتهم البدنية، وهي البيانات التي صارت جميعها مُتاحة وقابلة للاستحواذ عليها عبر تكنولوجيات مُدمجة على هواتفهم المحمولة بشكل أساسي؛ إذ وصل المعدل اليومي العالمي للوقت الذي يقضيه الفرد في استخدام الإنترنت إلى نحو 6 ساعات و40 دقيقة يومياً[6].

وما يثيره المعهد هنا، أن هذه الحالة من شمولية البيانات الضخمة لكافة جوانب الحياة اليومية للفرد؛ تُمكن الشركات التي تجمع هذه البيانات من معالجتها/ تحليلها، والوصول إلى استخلاصات حول تفضيلات أصحابها وطريقة تفكيرهم وحالتهم النفسية، بل والتفاصيل الحميمية والعاطفية لكل منهم، وذلك دون دراية من المستخدم في كثير من الحالات. فعلى سبيل المثال، فإن إحدى شركات البيانات وهي «أكسيوم» تمتلك وحدها نحو 3000 نقطة من البيانات للفرد الواحد لنحو 500 مليون شخص حول العالم. باختصار، أدت البيانات الضخمة إلى انفجار كبير في كمية المعلومات الشخصية التي صار من الممكن معرفتها وجمعها عن الأفراد.

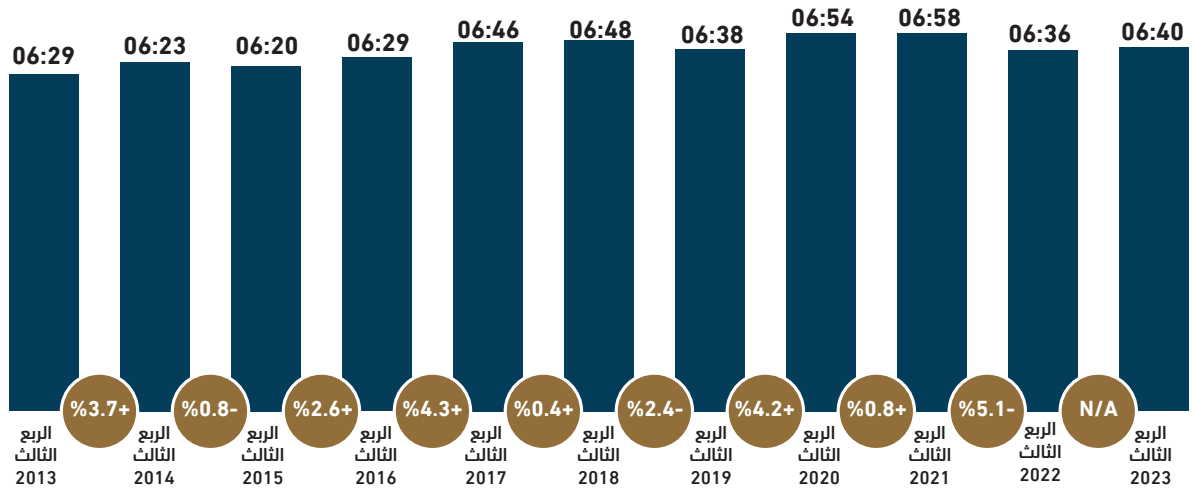
شكل (1): توقعات بحجم البيانات حول العالم (بالإكسابايت)، عن الفترة (2021 - 2026)



Source: IDC WW Global DataSphere and Global Storage Sphere Structured and Unstructured Data Forecast, 2022-2026

شكل (2): متوسط الوقت (بالساعات والدقائق) الذي يقضيه مستخدم الإنترنت

(الفئة العمرية من 16 حتى 64 سنة) في استخدام الإنترنت لليوم الواحد



Source: Digital 2024: Global Overview Report, DataReportal, published on January 31, 2024, access date July 27, available on the following link: https://datareportal.com/reports/digital-2024-global-overview-report

2- الاتصالية والاعتمادية بين الإنسان والآلة: الملمح الثاني الذي يطرحه المعهد، هو الارتفاع في حالة الاتصالية والاعتمادية اليومية الشديدة من المواطنين على الأجهزة المتصلة بالإنترنت، مثل: الهواتف المحمولة وأجهزة الكمبيوتر وغيرها من الأجهزة المتصلة بالإنترنت، والتي من المتوقع وصول عددها إلى نحو 30 مليار جهاز في عام 2027[7]. التغير الجديد في حالة الأمن القومي سواء على مستوى حماية الأفراد أم الدولة ككل، والذي تطرحه هذه الحالة من الاتصال، هو أن تصرفات المواطنين اليومية لم يعد ممكناً فصلها عن هذه الأجهزة المُولدة للبيانات باستمرار، كما أنها صارت مرئية ومتعقبة أو مُراقبة بشكل لحظي من الجهات التي تجمع البيانات من هذه الأجهزة.

3- احتكار قدرات جمع وتحليل البيانات الضخمة: الملمح الأخير الذي ناقشه المعهد، هو أن هناك عدداً محدوداً من الشركات العالمية، ومنها (جوجل، مايكروسوفت، فيسبوك، أمازون)، هي المُحتكرة والقادرة على توفير البنية التحتية الأساسية لتدفقات البيانات الضخمة وكذلك القدرات التحليلية لهذه البيانات، والتي تقوم عليها التطبيقات والمنصات الأخرى. وهو ما يمنح هذه الشركات مصدراً فريداً للقوة والتأثير وسط جميع الفاعلين بمن فيهم الحكومات نفسها التي تطلب مساعدة هذه الشركات لبناء بنيتها التحتية المعلوماتية؛ أي أن هذا العدد القليل من الشركات بات يعرف عن المواطنين وعاداتهم وتفضيلاتهم، على نحو أكبر بكثير، من أية جهة استخباراتية حكومية حول العالم.

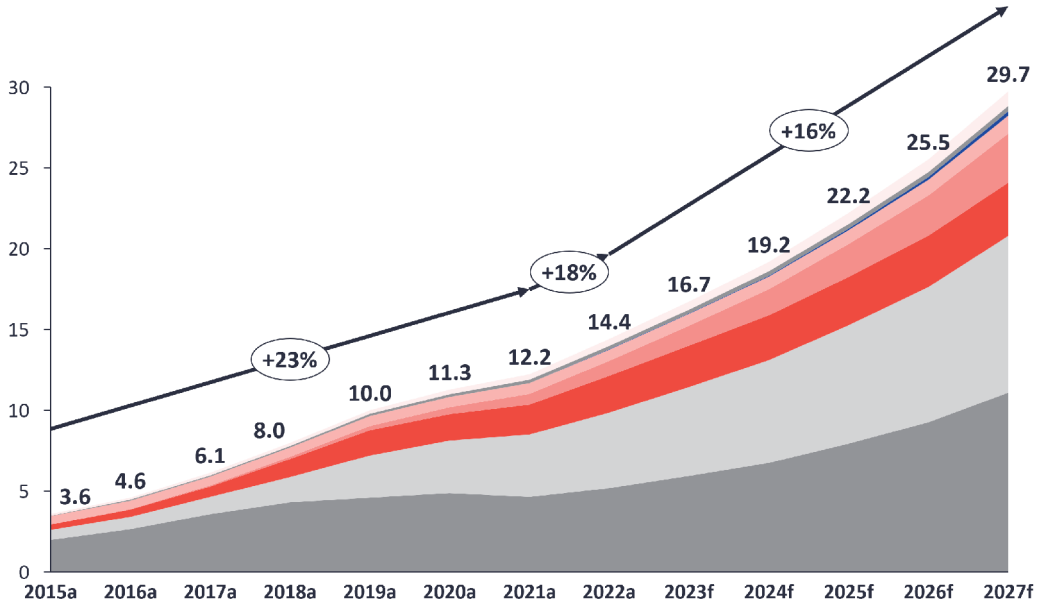
إمكانات متعددة لصنع القرار:

اتصالاً بما سبق، يؤكد «**المعهد الأسترالي للسياسات الاستراتيجية ASPI**» أن النُخب القائمة على الأمن القومي للدول في حاجة إلى مراجعة مواقفها نحو إمكانات توظيف البيانات الضخمة والتكنولوجيات المرتبطة بها، لخدمة مهام تحقيق الأمن القومي، ولاسيما أن هنالك عدداً من المهام الأساسية تتعلق بالأمن القومي هي التي تحتم هذا الاتجاه، ومنها[8]:

1- التكامل المعلوماتي: يستشهد المعهد بهجوم الحادي عشر من سبتمبر الإرهابي الشهير لعام 2001 ضد مركز التجارة العالمي بالولايات المتحدة الأمريكية، للإشارة إلى أن أشد الانتقادات خطورة التي تم اكتشافها وتوجيهها إلى مجتمع الأمن القومي الأمريكي حينها، أن جهاز الاستخبارات الأمريكي كان لديه وبشكل مُسبق مجموعة من البيانات المرتبطة بمنفذي الهجوم، وفي الوقت ذاته؛ فإن جهات إنفاذ القانون الأمريكية كانت تمتلك هي الأخرى مجموعة من البيانات ذات صلة بالحادث، ولو أن هذه المؤسسات كانت قد تمكنت وقتها من مشاركة هذه البيانات معاً وتحليلها بشكل كُلي؛ لظهرت لديها مؤشرات للإنذار المُبكر بالتخطيط لهجمات سبتمبر.

وبالتطرق إلى ما قد توفره البيانات الضخمة من مساعدة على هذه الحالة، يلفت المعهد هنا وعلى سبيل المثال، إلى مشروع (EMBERS) الذي طورته الحكومة الأمريكية، بالاعتماد على تكنولوجيات البيانات الضخمة

شكل (3): توقعات بعدد الأجهزة المعتمدة على الإنترنت (IOT) النشطة والمتصلة بالإنترنت عالميًا (بالمليار)



المصدر: شركة (IoT Analytics GmbH)

التي تجمع البيانات يومياً من مصادر متعددة مثل: التقارير الحكومية والمنشورات على موقع (X)؛ ليتولى المشروع إصدار تنبؤات بالتهديدات المحتملة للأمن القومي؛ كتحديد الأماكن التي من المحتمل أن تشهد احتجاجات أو أوبئة أو احتقاناً بين سكانها؛ وهو ما ألمح إليه المعهد؛ كأحد التطبيقات التي تم تطويرها فيما بعد بناءً على تكنولوجيات البيانات الضخمة؛ لخدمة التكامل بين البيانات والمعلومات التي تجمعها الجهات المسؤولة عن الأمن القومي من مصادر متعددة.

2- **تحليل كميات ضخمة من البيانات:** ينتقل المعهد إلى تحدٍّ آخر؛ وهو ضخامة المعلومات المُكلفة بجمعها المؤسسات الأمنية العاملة على الأمن القومي؛ مُشيراً إلى أنه وعلى سبيل المثال، قد قامت الطائرات الأمريكية من دون طيار في عام 2010 بتسجيل فيديوهات داخل العراق وأفغانستان بلغ إجمالي عدد ساعاتها 24 سنة ميلادية، ولكن العقبة حينها لم تكن توفير ذاكرة إلكترونية لتخزين هذه البيانات، ولكن كيف يمكن تحليلها في ظل محدودية عدد المُحللين البشريين المتاحين في ذلك الوقت؛ وهو ما قلل حينها من القيمة الاستخباراتية لهذه البيانات التي تم جمعها وتخزينها بالفعل. حتى إن أحد الرتب العسكرية حينها علق على هذه المسألة بانها ستكون بمثابة «سباحة بين الكاميرات وغرق داخل البيانات».

وفي هذا الصدد، يشير المعهد إلى ظهور نماذج عدة الآن مبنية على تكنولوجيات «تعدين البيانات الضخمة Data-Mining» التي تدمج ما بين تعلم الآلة والخوارزميات؛ بهدف تجميع البيانات والوصول بسهولة وسرعة إلى الارتباطات الناشئة بينها وغير الظاهرة للمحللين البشريين.

ولكن، وعلى جانب آخر، يشير «**المعهد الملكي للشؤون الدولية Chatham House**» البريطاني، في إحدى الدراسات الصادرة عنه، إلى أنه ولو كانت تكنولوجيات البيانات الضخمة قادرة على إنجاز الأنشطة الاستخباراتية التقليدية، وهي جمع المعلومات ومعالجتها وتحليلها، بل ومضاعفة حجم ومصادر البيانات القابلة لجمعها ومعالجتها؛ إلا أن القدرات الذهنية والإبداعية البشرية لا بد وأن تتولى مسؤولية الحُكم واتخاذ أية قرارات نهائية تتصل بالأمن القومي.

ويعود ذلك إلى أن البيئة الأمنية وإن كانت على المدى البعيد، تتضمن توقعات حتمية الحدوث تُدلل عليها الرؤى الناتجة عن تحليل البيانات المتاحة في الوقت الحالي، إلا أنه وعلى المدى القصير، قد تتعرض البيئة ذاتها إلى تغيرات وأحداث فجائية شديدة الخطورة، وفي الحالة الأخيرة ليس ممكناً استبدال الخبراء الأمنيين والاستراتيجيين القادرين على التحسب لهذه المفاجآت وتوقعها بالتكنولوجيا، فعلى سبيل المثال، لا يمكن التعرف على النيات التي يضمرها قادة الدول والحكومات قبل

حدوثها عبر التكنولوجيا، ولكن الخبرة والعقلية البشرية أقرب إلى توقع هذه النيات[9].

كما نبهت «مؤسسة كارنيغي للسلام الدولي» هي الأخرى إلى أن إحدى تبعات الاعتماد على نماذج العمل الآلية لتحليل البيانات الضخمة في صناعة قرارات الأمن القومي، هي إطالة الوقت المطلوب لعملية صناعة واتخاذ هذه القرارات، وذلك لسبب رئيسي، هو أن هذه النماذج سوف تُنتج كماً كبيراً من التحليلات وتتطرق إلى مجالات متشعبة ومتداخلة مع القرار محل النقاش، والانعكاس المباشر لهذا لدى صناع القرار البشريين هو حاجتهم لزمن أطول لمناقشة هذه الأبعاد الجديدة وما تطرحه من أسئلة حول تبعات هذا القرار؛ ومن ثم لن يتم اتخاذ القرار بشكل نهائي قبل الوصول إلى إجابات حول هذه الأسئلة[10].

المخاطر بين الاختراق والتسليع:

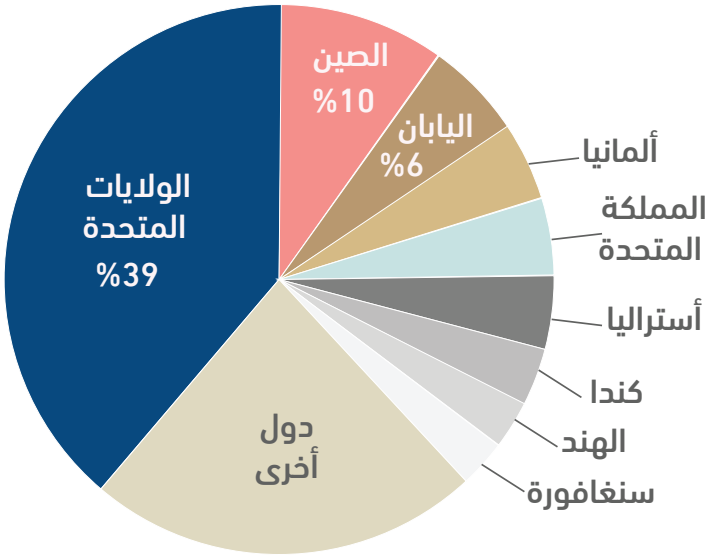
في تقييم خطورتها الأمنية والاستراتيجية، لفتت إحدى الدراسات الأكاديمية[11] إلى أن البيانات هي رابع أهم وأكبر مورد في العالم بعد الطاقة والموارد الطبيعية والمعلومات، وهي الفضاء الرابع في العالم بعد الأرض والبحار والجو، ومن هذا المنظور؛ اهتمت عدد من الدراسات وتحقيقات الصحافة الأمريكية جنباً إلى جنب مع مراكز الفكر والبحوث الأوروبية، بتقييم المخاطر الواردة عن حالة التنافس الاستراتيجي بين القوى الكبرى العالمية على البيانات الضخمة، ولاسيما الصين والولايات المتحدة الأمريكية، على الأمن القومي لهذه الدول وغيرها، وذلك على النحو التالي:

1- **تبعية البيانات:** أشارت مجلة «آفاق الأعمال والاقتصاد والإدارة»، وهي واحدة من المجلات العلمية الماليزية البارزة، في إحدى دراساتها[12] إلى أن بيانات ضخمة للدول من جميع أرجاء العالم تتدفق إلى الولايات المتحدة؛ إذ تستأثر واشنطن وحدها باستضافة نحو 40% من مراكز البيانات والشركات التي تقدم خدمات الحوسبة السحابية[13].

وهو ما تراه الدراسة ظاهرة أطلقت عليها «تبعية البيانات»؛ أي قيام الدولة بتخزين بياناتها داخل سيرفرات أو حوسبة سحابية تقع داخل دولة أخرى؛ وهو ما بإمكانه أن يهدد السيادة الوطنية لهذه الدولة؛ نظراً لما تقدمه هذه البيانات من قوة استراتيجية وتنافسية قابلة لاستخدامها من الدولة الحائزة لهذه البيانات ضد الدولة المستهدفة بهذه البيانات.

2- **شن الهجمات:** من المخاطر التي لفتت إليها أيضاً مجلة «FINBE»، هي أن استحواذ دولة معادية على بيانات مواطنين أو مرافق دولة أخرى، يسهل من استهدافها بهجمات شاملة شديدة الدقة، ولو امتلكت إحدى الدول على سبيل المثال، البيانات الجينية والصحية لمواطني دولة أخرى؛ فإن تحليل هذه البيانات يُمكن من شن هجمة بيولوجية من جانب واحد تجاه مواطني هذه الدولة.

شكل (4): توزيع أهم مواقع مراكز البيانات السحابية وبيانات الإنترنت (%) على الدول المستضيفة



المصدر: Homeland Security Research Corporation HSRSC

وبقدر أكبر من التفصيل، فقد استهدفت دراسة منشورة بمجلة «المعلومات الحكومية» ربع السنوية والصادرة عن كلية كوبنهاغن الدنماركية للأعمال[14]، تقييم الآثار المتوقعة لبناء عدد من المستشفيات بالقطاع الصحي بدولة الصين، لنموذج يعتمد على تكنولوجيات تعلم الآلة لتشخيص الأمراض المزمنة عبر الذكاء الاصطناعي، والذي تم تصميمه عبر تسجيل بيانات ضخمة لتاريخ الحالات المرضية المشابهة بالدولة، ثم استخدام تقنيات تعلم الآلة في تشخيص أية حالات جديدة عبر مقارنة بياناتها الحالية بالبيانات التاريخية.

وتشرح الدراسة أن أبرز المخاطر المرتبطة بهذا المشروع، هي أن شركة (IBM) التي توفر هذه التكنولوجيات للمشروع هي شركة أمريكية وليست صينية، مُعلقة أن جمع وتخزين وامتلاك كم هائل من البيانات حول المرضى الصينيين من طرف غير وطني يُعرض الأمن القومي الصيني للخطر، مع احتمالية تسرب واستغلال هذه البيانات في إنتاج خطط لشن حرب بيولوجية على الشعب الصيني؛ بل ووصفت الدراسة هذا الاحتمال باعتباره خطراً وجودياً على الدولة والشعب الصيني ككل.

3- **التجسس:** في عام 2021، نشرت صحيفة «الواشنطن بوست» الأمريكية تحقيقاً راجعت فيه وثائق منشورة مثل: عقود وعطاءات، تتعلق بـ300 مشروع بدأت بها الحكومة الصينية منذ عام 2020، وقد استنتج التحقيق تضمن هذه المشروعات لأوامر مباشرة بتصميم برمجيات تقوم مهمتها على جمع البيانات عن مواطنين ونخب دول أجنبية ومن مصادر مثل: فيسبوك وتويتر وغيرها من شبكات التواصل الاجتماعي الغربية.

الوثائق ذاتها كشفت أن جهات حكومية وعسكرية صينية تتجه إلى شراء برمجيات أكثر تعقيداً؛ هدفها تعدين بيانات المستخدمين على فيسبوك وتويتر؛ لتأسيس قاعدة بيانات للأكاديميين والصحفيين والسياسيين الأجانب، وأكد أحد العاملين الصينيين لدى هذه الجهات لواشنطن بوست، أن الغرض هو تعرف حكومة بكين على الأشخاص الذين يكتبون محتوى مُعادياً للحكومة الصينية على وسائل التواصل الاجتماعي في الغرب. الصحيفة علقت على هذا التحقيق، بأن بكين تعكف أيضاً من وخلال الاستحواذ على هذه البيانات، على تصميم شبكة من نظم الإنذار المُبكر حول ظهور أية توجهات جديدة «Trends» مُعادية لمصالحها في الغرب[15].

4- **تسليع البيانات:** أشار تقرير نشره «مجلس العلاقات الخارجية»، إلى نمط آخر من التهديدات التي تشكلها البيانات الضخمة على الأمن القومي، وهو «تسليع البيانات»، مدللاً عليه بالإجراءات الحمائية التي اتخذتها كل من إدارتي ترامب وبايدن التالية لتقليص الواردات الأمريكية من السيارات الكهربائية صينية المنشأ، نظراً لما تمثله من تهديد سيبراني صيني للأمن القومي الأمريكي.

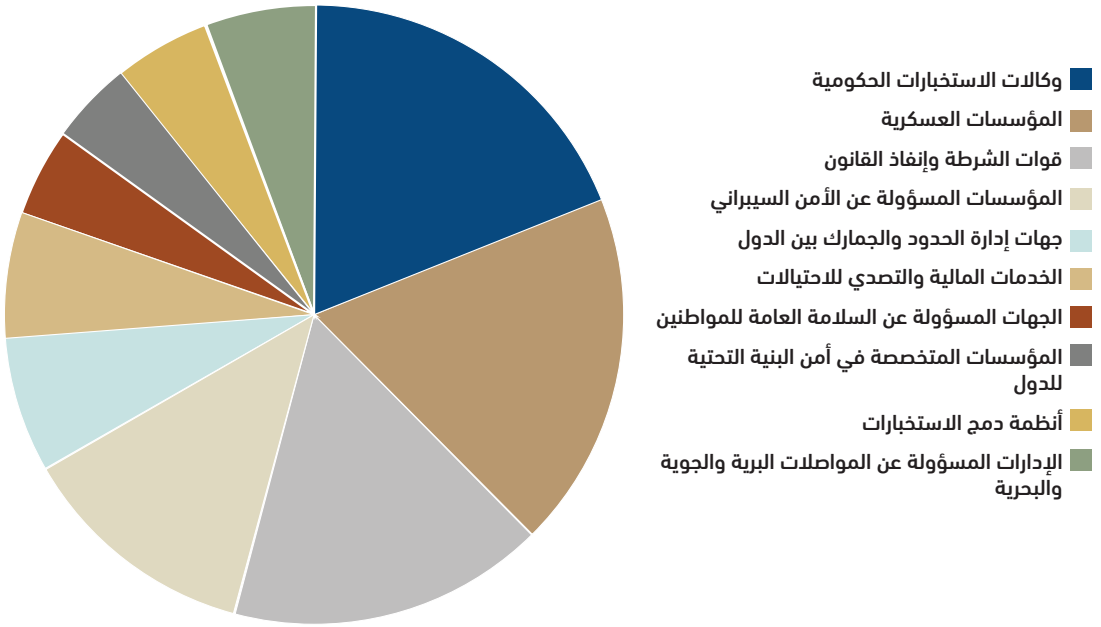
التفصيل الذي أورده التقرير، أشار إلى أن هذه المركبات تحوي حواسب آلية تقوم بجمع ونقل كميات ضخمة من البيانات غير القابلة لتعقبها والرقابة عليها بشكل كبير من الحكومة الأمريكية، وذلك إما لصالح الشركة المُصنعة، أو تقوم ببيعها إلى أطراف ثالثة بمقابل. ومن السوابق لمثل هذه العمليات، إقرار شركة «جنرال موتورز» للسيارات، بأنها قامت بجمع بيانات حول مستخدمي سياراتها وقامت ببيعها إلى شركات أخرى متخصصة في تجارة البيانات، مثل: المواعيد والمسافات والأوقات المستغرقة لكل رحلة وسرعة القيادة وأنماط تعامل المستخدمين مع مكابح السيارة.

التعليق الذي أورده وزير التجارة الأمريكي في يناير 2024 حول تخوفاتهم من المركبات الصينية كان نصه: «لسنا في حاجة إلى محاولة تصور التهديد الخطر الذي تمثله السيارات المتصلة بالإنترنت وتجمع البيانات على الأمن القومي الأمريكي»، وأضاف التقرير أن هذه التخوفات تقوم بشكل رئيسي على تجميع هذه المركبات لبيانات ضخمة حول البنية التحتية بالولايات المتحدة مثل: حالة الطرق وأماكن وتوزيع محطات الشحن الكهربائي للمركبات، فضلاً عن البيانات الشخصية للمواطنين[16].

نموذج الاستخدام الأمريكي:

أحد التقارير الفريدة حول استخدامات البيانات الضخمة في مجال الأمن القومي، أصدرته «شركة بحوث الأمن القومي» الأمريكية تحت عنوان «البيانات الضخمة وتحليلات البيانات في الأمن القومي وإنفاذ القانون»، وقد اهتم التقرير بشكل أساسي بتقدير حجم استخدام البيانات الضخمة في المجالات الرئيسية بالأمن القومي خلال الفترة (من عام 2021 – حتى عام 2026).

شكل (5): توقعات سوق استخدامات البيانات الضخمة وتحليلات البيانات (%) في قطاعات الأمن الداخلي والأمن الوطني والسلامة العامة في الفترة (2019 - 2026)



المصدر: Synergy Research Group

وبتركيز التقرير على 19 دولة ومنطقة حول العالم، وهي (الولايات المتحدة الأمريكية، ألمانيا، فرنسا، المملكة المتحدة، إيطاليا، إسبانيا، أستراليا، الصين، الهند، نيجيريا، كندا، جنوب إفريقيا، اليابان، البرازيل، المكسيك، كولومبيا، دول مجلس التعاون الخليجي، كينيا)، وصل إلى نتيجتين رئيسيتين. الأولى، هي أن سوق استخدامات البيانات الضخمة في الأمن القومي داخل هذه الدول، وخلال الفترة المحددة، سوف تشهد زيادة بنسبة 12% حتى تصل قيمتها إلى 17.3 مليار دولار.

والنتيجة الثانية أنه ومن بين 10 مجالات أساسية للأمن القومي حددها التقرير، ستأتي بالمركز الأول استخدامات وكالات الاستخبارات الحكومية للبيانات الضخمة وتحليلاتها، وبعدها المؤسسات العسكرية، ثم قوات الشرطة وإنفاذ القانون، وتليها المؤسسات المسؤولة عن الأمن السيبراني، وخامساً جهات إدارة الحدود والجمارك بين الدول، ثم الخدمات المالية والتصدي للاحتيالات المرتبطة بها. وفي المراكز اللاحقة، تأتي الجهات المسؤولة عن السلامة العامة للمواطنين، والمؤسسات المتخصصة في أمن البنية التحتية للدول، والإدارات المسؤولة عن المواصلات البرية والجوية والبحرية للدولة[17].

وبالتطرق بشكل مُفصل لأحد تطبيقات البيانات الضخمة من جانب الحكومات في مجال الأمن القومي، فقد شرح كل من السيد/ توم هوشيك، القائم بأعمال مساعد وزير الخارجية الأمريكية بمكتب عمليات الصراع والاستقرار، والسيد/ بريان كين، مدير برامج التحليل والتخطيط والتعلم بالمكتب ذاته، في مقال مشترك لهما على موقع «The Hill» الأمريكي، وشاركته وزارة الخارجية الأمريكية على موقعها أيضاً[18]، كيفية استخدام الولايات المتحدة لتحليلات البيانات الضخمة في الحفاظ على الأمن القومي الأمريكي. ويشير المسؤولان إلى أن مكتبهما قد بدأ منذ العام 2013 في استخدام تحليلات البيانات الضخمة؛ من أجل مساعدة واشنطن والدول الحليفة لها، على مواجهة التطرف والعنف وتحقيق الاستقرار داخل وخارج الولايات المتحدة.

ويشرح المقال أن نموذج العمل الأمريكي قد قام على تطوير ثلاث خطوات رئيسية لجمع وتحليل البيانات الضخمة:

1- التنسيق بين أجهزة جمع البيانات والمعلومات: البداية هي رسم خطوط التنسيق والتكامل بين مصادر ومؤسسات جمع البيانات والمعلومات، ممثلة في المؤسسات الأمريكية العاملة بالخارج وهي السفارات الأمريكية، والبعثات التابعة لهيئة التنمية الأمريكية (USAID) وبعثات القوات الخاصة التابعة لوزارة الدفاع، إلى جانب المؤسسات الأم الوطنية في واشنطن وهي وزارات الدفاع والخارجية وهيئة (USAID).

2- **تكامل البيانات الاستخباراتية مع قواعد البيانات حول مناطق الصراع:** في مرحلة ثانية، يقوم مكتب العمليات بجمع البيانات المُحدثة التي يُرسلها المختصون والدبلوماسيون الأمريكيون من كل دولة حول العام بشأن حوادث الصراع أو التوتر أو الإرهاب هنالك، ثم يدمجها مع قواعد البيانات المتوفرة لدى المؤسسات الثلاث بواشنطن حول هذه الدول مثل: (حوادث الصراع التاريخية لكل دولة، الاتجاهات السياسية لمواطنيها، التركيبة الديمغرافية، مستويات الدخول)؛ وذلك بهدف توليد تحليلات جديدة تربط بين هذه البيانات والمعلومات مجتمعة، وصولاً إلى صياغة توقعات بالمناطق التي توشك على اندلاع صراع جديد أو ستنشأ بها منظمات أو جماعات إرهابية.

3- **تصميم شبكات بالفاعلين وسُبل حل الصراعات:** في مرحلة جديدة تالية، يتم تصميم خريطة لمناطق التوتر والفاعلين داخلها، وتحديد درجات الاتصال بين الجماعات المختلفة المنتشرة بكل منطقة، ودرجة قوة كل جماعة، وعبر المزيد من المعالجات للبيانات، يتم استخلاص بيانات حول القادة المؤثرين بكل منظمة، وقياس نسبة ميل كل جماعة للتفاوض ونوعية الشروط التي قد تفرضها، ثم توليد تحليلات أخرى حول مدى ملاءمة هذه الشروط مع أهداف وغايات السياسة الأمريكية؛ ويكون الهدف من المعالجة في هذه المرحلة، هو التوصل لسُبل حل الصراع.

بنهاية المقال، يؤكد المسؤولان الأمريكيان أن الاعتماد على تحليلات البيانات الضخمة في مجال الدفاع والأمن القومي بالنسبة للحكومة الأمريكية، قد غير قواعد اللعبة، فالقاعدة الآن هي الاستكشاف والتشخيص المبكر للصراعات قبل اندلاعها، بدلاً من انتظار حدوثها ثم إرسال قوات عسكرية بغرض إخمادها؛ وهو ما عبر عنه وزير الدفاع الأمريكي الأسبق جيمس ماتيس بتعبير آخر: «كلما أنفقنا في وزارة الخارجية وأدواتها الدبلوماسية؛ سوف يوفر لنا ذلك نفقات وزارة الدفاع».

متطلبات بناء القدرات:

في إحاطة قدمها بنيامين جنسين، أحد كبار الزملاء الباحثين لدى **«مركز الدراسات الاستراتيجية والدولية CSIS»** الأمريكي أمام لجنة في مجلس الشيوخ الأمريكي متخصصة بالشؤون الاستخباراتية، أكد أن تكنولوجيات البيانات الضخمة، ممثلة في الذكاء الاصطناعي، ولاسيما تقنية تعلم الآلة ستكون بمثابة مورد أساسي لبناء قدرات الدولة الأمنية لكل من الردع وشن الحروب في القرن الحادي والعشرين، وأن النموذج الأمثل لبناء نماذج تحليل بيانات الأمن القومي القائمة على هذه التكنولوجيات، لا بد وأن يتضمن ثلاثة ملامح أساسية، وهي:

1- **نخبة متخصصة في علوم البيانات:** لا بد وأن تضمن أجهزة الاستخبارات والدفاع لكل دولة، نخبة من كبار العاملين والرتب العسكرية بها، الذين تكون لديهم دراية وعلم وفهم لعلوم البيانات.

2- **بيروقراطية رشيقة:** فرق العمل نفسها العاملة داخل هذا النموذج، يجب ألا تخضع لسياسات البيروقراطية الحكومية الهيراركية والكابحة للابتكار؛ بل تتسم برشاقة العدد والمرونة في صنع القرار وإجراء التجارب الجديدة.

3- **الوصول إلى البيانات:** إتاحة وصول فرق العمل والمتخصصين العاملين داخل هذا النموذج إلى مراكز البيانات دون عوائق، وبما يسمح لهم بإجراء التدريبات المستمرة لما يقومون ببنائه من نماذج حتى تكتسب قدرات تعلم الآلة؛ بل وإطلاعهم على التحديثات باستمرار.

ولفت بنيامين إلى أن تردد أو فشل أي من الحكومات في توفير هذه المتطلبات للمؤسسات القائمة على حماية الأمن القومي لديها؛ يعني ببساطة تنازل هذه الدولة عن المبادرة والسبق، وتعرضها للمبادرة من خصومها[19].

وعلى الجانب الآخر، أعد كل من **«مركز جامعة جورج تاون للأمن والتكنولوجيات الناشئة -CSET-»** و**«مركز السياسات غير الحزبية»** الأمريكيين، ورقة مشتركة تضمنت مجموعة توصيات لدعم استراتيجية الأمن القومي الأمريكي، حول تكنولوجيات البيانات الضخمة وبخاصة الذكاء الاصطناعي، وتضمنت أبرز هذه التوصيات ما يلي[20]:

1- **التدرب على بناء الثقة بين متخذ القرار والآلة:** تؤكد الورقة أن الهدف الأساسي لبناء وتطوير نماذج العمل القائمة على التكنولوجيا، داخل مؤسسات الأمن القومي؛ هو صقل ودعم الذكاء البشري عبر بناء فريق عمل يقوم على التعاون بين ثنائية (الإنسان والآلة)، منوهة بأن الثغرة الأساسية المناهضة لهذه الثنائية، هي انخفاض ثقة العنصر البشري في قرار الآلة، وبخاصة خلال اللحظات الحرجة التي تحتاج إلى حلول سريعة لأزمة خطرة وطارئة.

وبناءً عليه، توصي الورقة المسؤولين عن إدارة فرق العمل داخل أجهزة الأمن القومي، ولاسيما المؤسسات العسكرية؛ بالاستثمار في إجراء بحوث تركز وبشكل واضح على عامل الثقة في التفاعلات ما بين العنصرين البشري والآلي، وكيف يُمكن للفرد الأمني أثناء الأوقات الضاغطة والخطرة التدرب على كيفية قياس مقدار الثقة المناسب الذي يجب منحه في نظام قائم على الذكاء الاصطناعي، قبل الاعتماد عليه في اتخاذ القرارات.

2- **بناء القدرات:** تقييم الدولة لحجم المواهب البشرية المتاحة لديها والقادرة على فهم وإدارة التكنولوجيات المرتبطة بالبيانات الضخمة، وقدرتها كذلك على تصميم النظم والمناهج التعليمية القادرة على إنتاج المزيد من المواهب في تخصصات مثل: الهندسة وعلوم الحاسبات والعلوم الطبيعية، بجانب قدرة الأطر القانونية والتقنية الحاكمة لحماية أمن البيانات وخصوصية المواطنين، هي جميعها عوامل تندرج تحت بند بناء القدرات للدول، والتي يحتاج صانعوا القرار إلى التخطيط لها، وألا تتعرض أية منظومة أو نموذج عمل قائم على التكنولوجيا إلى مخاطر عدم الاستدامة مع نقص هذه الموارد والقدرات.

وبالإضافة إلى ما سبق، كانت أبرز التوصيات التي قدمها تقرير صادر عن **«مركز بيلفر للعلوم والشؤون الدولية»** الأمريكي إلى الحكومات حول تضمين تكنولوجيات البيانات الضخمة في بناء استراتيجيات الأمن القومي؛ هي العمل على الاستثمار في تيسير نقل التكنولوجيا بين القطاعين الخاص والحكومي، بجانب تحسين آليات نقل البرمجيات التجارية إلى الأنظمة الحكومية؛ إذ أكد التقرير أنه ومهما استحوذت الحكومات على مواهب بشرية وقدرات تكنولوجية؛ فإن شركات القطاع الخاص سوف تُحرز المزيد من التطورات التكنولوجية مع الوقت وفي المستقبل؛ ومن ثم ستحتاج الحكومات إلى مواكبتها باستمرار ونقلها إلى أنظمة عملها.

ومن الآليات التي اقترحها التقرير؛ هي قيام الحكومات بتأسيس «شركة خارجية» تعمل كقطاع خاص، وتكون مهمتها هي نقل التكنولوجيات الجديدة إلى الحكومات[21]، وعلى سبيل المثال، فقد أسست وكالة الاستخبارات الأمريكية (CIA) في عام 1999 شركة (IQT) كشركة خاصة تستثمر برأسمال مغامر في القطاع الخاص وباستقلالية عن الحكومة الأمريكية؛ ومهمتها الأساسية التي تأسست من أجلها هي تسريع نقل التكنولوجيا بين القطاع الخاص والحكومة الأمريكية وحلفائها؛ بهدف دعم كل من الأمن القومي والازدهار الاقتصادي لهذه الدول[22].

ختاماً، إن الأفراد حول العالم في الوقت الحالي يقضون وقتاً كبيراً من يومهم في استخدام شبكات الإنترنت؛ ما يسمح بإنتاج نحو 200 ألف إكسابايت من البيانات؛ أي ما يساوي 40 مرة من حيث الحجم لمقدار الكلمات التي تحدث بها البشر على مر التاريخ. والجديد في الأمر، أن هذه البيانات هي وصف لمشاعرهم واحتياجاتهم، والمثير أيضاً للاهتمام أن تكنولوجيات الذكاء الاصطناعي، ولاسيما تقنية تعلم الآلة باتت قادرة الآن على معالجة هذا الكم الهائل من البيانات، وترجمة هذه المعالجة في صورة توقعات تُجيب عن سؤال ما الذي سيحدث في المستقبل؟ بل وما الذي يمكن صناعته من سياسات للتعامل مع المستقبل على النحو الأمثل؟

بدأت حكومات الدول في استخدام البيانات الضخمة لحماية أمنها القومي، عبر بناء نماذج تكنولوجية تضخ بها البيانات، وتستخرج منها الرؤى حول ما الذي سيحدث في المستقبل من صراعات؟ وكيف يمكن إنهاؤها؟ وبالإضافة إلى ذلك، فمن المتوقع أن يزيد اعتماد مؤسسات الأمن القومي على البيانات الضخمة بمرور الوقت.

وقرابة 45% من البيانات الضخمة حول العالم هي بيانات شديدة الحساسية وغير محمية، ونحو 40% منها أيضاً مُخزن لدى مراكز بيانات لشركات مقرها الولايات المتحدة الأمريكية، والتي لديها القدرة على نقل هذه البيانات الخاصة بدول أو شعوب معينة وبيعها إلى طرف ثالث. كما أثبتت التحليلات أن الحكومة الصينية مهتمة وبشكل كبير بجمع كميات هائلة من البيانات الضخمة عن مواطني ونخب الدول الغربية والولايات المتحدة، وذلك عبر تطوير برمجيات تستخرج هذه البيانات من شبكات التواصل الاجتماعي، أو عبر المنتجات الصينية التي يستخدمها مواطنو هذه الدول مثل السيارات صينية المنشأ التي بمقدورها تصوير المواطنين والبنية التحتية بالدولة التي تسير بها هذه السيارة، والخصائص الخاصة بكل من المواطنين والبنى التحتية للدول.

تؤشر الدلائل على أن البيانات الضخمة صارت جزءاً من التنافس الاستراتيجي بين القوى الكبرى، ولاسيما الولايات المتحدة والصين، وأن كلاً منهما يسعى للاستحواذ على القدر الأكبر من هذه البيانات أو الشركات المتحكمة بها؛ وتؤكد الرؤى التي قدمتها مراكز الأبحاث العالمية، أن هذه الممارسات تجسد مخاطر على الأمن القومي لهذه الدول وغيرها من دول العالم، فامتلاك الولايات المتحدة لنحو 40% من هذه البيانات يفرض حالة من التبعية لصالحها، والممارسات الصينية يمكن أن تهدد حقوق المواطنين في الخصوصية، إلى جانب التهديد الاستراتيجي بإمكانية استخدام هذه البيانات في استهداف المواطنين أو البنى التحتية لهذه الدول بدرجة عالية من الدقة بهجمات متنوعة وشاملة قائمة على هذه البيانات.

ومن ثم فإنه لا مفر من مبادرة كل دولة للقيام بالآتي:

1- بناء القدرات للدولة في مجال البيانات الضخمة؛ بالاستحواذ على مواهب بشرية مدربة، وتطوير تعليم تكنولوجي، وتحسين الأطر القانونية والأمنية لحماية البيانات، ما يخلق بيئة أكثر تمكيناً وتحفيزاً.

2- النخب الأمنية العاملة على الأمن القومي، لا بد وأن تكون على دراية تكنولوجية، وقادرة على الوصول إلى البيانات، ورشيقة الحجم بيروقراطياً كي تتمكن من العمل والتدرب واتخاذ القرار بحرية.

3- المزيد من الانفتاح والاتصال والتعاون من الحكومات مع شركات القطاع الخاص، فالأخيرة هي الأكثر جرأة على الاستثمار في التكنولوجيا واستحداث المزيد من التقنيات.

المصادر:

1- Big data, **Cambridge Dictionary**, access date July 25, available on the following link: https://dictionary.cambridge.org/fr/dictionnaire/anglais/big-data

2- One Exabyte means 1,000,000,000,000,000,000 byte, and it equals about one fifth of the words people have ever spoken.
One Zettabytes means 1,000,000,000,000,000,000,000 byte.
Source: Data Volumes, **University of Delaware**, access date August 2, 2024, available on the following link: https://www.eecis.udel.edu/~amer/Table-Kilo-Mega-Giga---YottaBytes.html

3- Eric Burgener & John Rydning, High Data Growth and Modern Applications Drive New Storage Requirements in Digitally Transformed Enterprises, **International Data Corporation (IDC)**, July 2022, P 3.

4- Kim R. Holmes, What Is National Security?, **The Heritage Foundation**, access date July 26, available on the following link: https://www.heritage.org/sites/default/files/2019-10/2015_IndexOfUSMilitaryStrength_What20%Is20%National20%Security.pdf

5- Miah Hammond-Errey, Big data and national security: A guide for Australian policymakers, **Lowy Institute**, published on February 1, 2022, access date July 27, available on the following link:
https://www.lowyinstitute.org/publications/big-data-national-security-guide-australian-policymakers

6- Digital 2024: Global Overview Report, **DataReportal**, published on January 31, 2024, access date July 27, available on the following link: https://datareportal.com/reports/digital-2024-global-overview-report

7- Satyajit Sinha, State of IoT 2023: Number of connected IoT devices growing 16% to 16.7 billion globally, **IoT Analytics**, published on May 24, 2023, access date July 27, available on the following link: https://iot-analytics.com/number-connected-iot-devices/

8- Miah Hammond-Errey, Big data and national security: A guide for Australian policymakers, **Lowy Institute**, published on February 1, 2022, access date July 27, available on the following link:
https://www.lowyinstitute.org/publications/big-data-national-security-guide-australian-policymakers

9- Damien Van Puyvelde et others, Beyond the buzzword: big data and national security decision-making, Chatham House: **International Affairs** (93:6), 2017.

10- Christopher S. Chivvis & Jennifer Kavanagh, How AI Might Affect Decision making in a National Security Crisis, **Carnegie Endowment for International Peace**, published in June 17, 2024, access date August 2, 2024, available on the following link: https://carnegieendowment.org/research/2024/06/artificial-intelligence-national-security-crisis?lang=en

11- Xuan Liu, The Study on National Security in Big Data Era, **Frontiers in Business, Economics and Management**, Vol. 5, No. 3, 2022.

12- Xuan Liu, **ibid**.

13- Microsoft, Amazon and Google Account for Over Half of Today's 600 Hyperscale Data Centers, **Synergy Research Group**, published on January 26, 2021, access date July 28, available on the following link:
https://www.srgresearch.com/articles/microsoft-amazon-and-google-account-for-over-half-of-todays-600-hyperscale-data-centers

14- Sun, T. Q & Medaglia, R, Mapping the Challenges of Artificial Intelligence in the Public Sector:
Evidence from Public Healthcare, **Government Information Quarterly**, 2019, 36(2).

15- Cate Cadell, China harvests masses of data on Western targets, documents show, **Washington post**, published on December 31, 2021, access date July 28, available on the following link: https://www.washingtonpost.com/national-security/china-harvests-masses-of-data-on-western-targets-documents-show/2021/12/31/3981ce9c-538e-11ec-8927-c396fa861a71_story.html

16- Kat Duffy and Kyle Fendorf, In the Age of AI, Personal Data Security Is National Security, **Council on Foreign Relations**, published on April 1, 2024, access date July 29, 2024, available on the following link: https://www.cfr.org/article/age-ai-personal-data-security-national-security

17- Big Data & Data Analytics Market in National Security & Law Enforcement: 2020-2026, **Homeland Security Research Corporation (HSRSC)**, published in January 2021, access date July 30, 2024, available on the following link: https://hsrc.biz/reports/big-data-data-analytics-homeland-security-public-safety-global-market/

18- Tom Hushek & Brian Keane, Using Data Analytics To Promote American Security, **the Hill**, published in Aug 17, 2017, access date July 30, 2024, available on the following link: https://thehill.com/blogs/pundits-blog/homeland-security/346879-how-data-is-playing-a-key-role-in-american-security/

19- Benjamin Jensen, Addressing the National Security Implications of AI, **Center for Strategic & International Studies**, published on 19 September, 2023, access date July 24, 2024, available on the following link:
https://www.csis.org/analysis/addressing-national-security-implications-ai

20-Artificial Intelligence and National Security, **Bipartisan Policy Center**, published in June 2020, access date July 24, 2024, available on the following link: https://bipartisanpolicy.org/download/?file=/wp-content/uploads/2020/07/BPC-Artificial-Intelligence-and-National-Security_Brief-Final-1.pdf

21-Stephen Coulthart and Ryan Riccucci, **The Belfer Center for Science and International Affairs**, Improving Big Data Integration and Building a Data Culture for U.S. Border Security, published on March 2021, access date July 29, 2024, available on the following link: https://www.belfercenter.org/sites/default/files/files/publication/HSP8-draft2.pdf

22- IQT, access date July 29, 2024, available on the following link: https://www.iqt.org/about

عن المستقبل:

"المستقبل للأبحاث والدراسات المتقدمة"، هو مركز تفكير Think Tank مستقل، تأسس في 2014/4/4، في أبوظبي، بدولة الإمارات العربية المتحدة، للمساهمة في تعميق الحوار العام، ومساندة صنع القرار، ودعم البحث العلمي، فيما يتعلق باتجاهات المستقبل، التي أصبحت تمثل مشكلة حقيقية بالمنطقة، في ظل حالة عدم الاستقرار وعدم القدرة على التنبؤ خلال المرحلة الحالية، بهدف المساهمة في تجنب "صدمات المستقبل" قدر الإمكان.
ويهتم المركز بالاتجاهات التي يمكن أن تساهم في تشكيل المستقبل، على المدى القصير، خاصة الأفكار غير التقليدية والظواهر "تحت التشكيل"، مع التطبيق على منطقة الخليج، من خلال رصد وتحليل الاحتمالات الممكنة، للتفاعلات القائمة والتيارات القادمة، وتقدير البدائل المتصورة للتعامل معها، باستخدام مناهج التفكير المتقدمة، عبر أنشطة علمية تجمع بين الأكاديميين والممارسين، والشخصيات العامة، من داخل الإمارات وخارجها.

أنشطة المركز:

مجلة اتجاهات الأحداث: دورية أكاديمية فصلية، تهتم بتحليل اتجاهات المستقبل على المدى القصير، بما يتضمنه من تيارات وتطورات، متعددة الأبعاد، وذات تأثيرات استراتيجية، وذلك في مجالات اهتمام برامج المركز.

تقديرات المستقبل: تقديرات تصدر يومياً لتغطية أبرز التطورات الإقليمية والدولية المؤثرة على منطقة الشرق الأوسط.

بوابة المستقبل: موقع إلكتروني أكاديمي، يقوم بنشر تحليلات يومية، باللغتين العربية والإنجليزية، حول أهم الأحداث والتطورات الجارية في المنطقة والعالم، ويغطي الموقع إنتاج المركز المطبوع وأنشطته المختلفة، من لقاءات عامة وحلقات نقاشية، ويقدم خدمات علمية تتعلق بعروض الكتب والدراسات، وقواعد البيانات والخرائط السياسية.

تقرير المستقبل: نشرة يومية تتضمن أبرز التقديرات والتحليلات التي ينتجها باحثو المركز، أو ما ينشر على موقعه الإلكتروني أو الدورية التي تصدر عن المركز، وغيرها من الأنشطة والإصدارات، وترسل عبر البريد الإلكتروني.

دراسات المستقبل: سلسلة دراسات أكاديمية تصدر كل شهرين، وتركز كل دراسة على قضية واحدة تمثل ظاهرة صاعدة على المستوى الاستراتيجي تتسم بالتعقيد وتعدد الأبعاد، وتهيمن على الجدل العام في الشرق الأوسط والعالم.

دراسات خاصة: سلسلة دراسات غير دورية تركز على الظواهر الصاعدة، والمؤشرات المركبة والأفكار غير التقليدية، والاتجاهات القادمة التي ترتبط بالعالم قيد التشكل.

التقرير الاستراتيجي: تقرير يصدر سنوياً عن المركز، ويركز على الاتجاهات الرئيسية طويلة المدى التي تشكلت في الشرق الأوسط من خلال تفاعلات العام السابق، والتي يتوقع أيضاً أن تكون الأكثر تأثيراً في حالة الإقليم خلال العام التالي.

مؤشرات المستقبل: تقرير غير دوري يرصد ويُحلل أبرز المؤشرات وقواعد البيانات واستطلاعات الرأي العالمية والإقليمية.

رؤى عالمية: تهدف إلى عرض أبرز ما يُنشر في مراكز الفكر والمجلات والدوريات البحثية الغربية، من أفكار غير تقليدية واتجاهات صاعدة في مختلف المجالات السياسية والأمنية والاقتصادية وغيرها.

ملفات المستقبل: سلسلة ملفات تجميعية تصدر بشكل غير دوري، وتتناول أهم الأحداث والتحولات الإقليمية والدولية، التي تشغل اهتمام الجمهور وتتصدر نقاشات المجال العام وقت صدورها.

فعاليات المستقبل: ينظم المركز عدة فعاليات مثل (اللقاءات العامة، وحلقات النقاش، والدورات التدريبية).