منطق الحوكمة في استراتيجيات الأمن القومي إدارة المخاطر المركبة في عالم متغير

أ.د. سهاد إسماعيل خليل*

يناقش البحث إشكالية محورية في الدراسات الاستراتيجية والأمنية تتمحور حول فكرة منطق الحوكمة في إدارة المخاطر في عالم متغير يتسم بالتعقيد والفوضة والغموض والتشابك بل يناقش الفكرة في ظل متغيرات دولية متسارعة بخطوات علمية وسياسية واقتصادية على حد سواء، فالانتقالات الموجية في التطور المعرفي والتكنولوجي انعكست بشكل مباشر على الإدارة الأمنية في الدول من حيث ترشيد القرار الأمني وبناء الاستراتيجيات الأمنية في مواجهات التهديدات والاخطار الناتجة عن هذا التطور مما اضفة تهديدات مركبة غير تقليدية تستدعي تطوير سيل الوقاية والمواجهة عبر بناء شبكات من التكامل المؤسسي والمعرفي وصياغة معادلات وفرضيات ومصفوفات بالاستعانة بتقنيات وتطبيقات الذكاء الاصطناعي في تحقيق الأهداف والمصالح الأمنية العليا للدولة في مجال مكافحة الإرهاب وتحقيق الامن والاستقرار.

الكلمات المفتاحية: حوكمة الامن ، شرعية الحوكمة، المخاطر المركبة ، التكامل المؤسسي، الذكاء الاصطناعي.

The Logic of Governance in National Security Strategies: Managing Complex Risks in a Changing World

Dr.suhad ismail khleel

This research addresses a pivotal problematic in Strategic and Security Studies, centering on the logic of governance in risk management within a volatile international environment characterized by complexity, turbulence, ambiguity, and systemic interdependence. The study examines this problematic against the backdrop of accelerating international transformations driven by concurrent scientific, political, and economic variables. The successive waves of cognitive and technological advancement have directly reshaped security governance in contemporary states, fundamentally affecting the rationalization of security decision-making and the formulation of security strategies in response to threats and risks emanating from this rapid development. Consequently, compound non-traditional threats have emerged, necessitating the development of prevention and counter-threat mechanisms through the construction of institutional and epistemic integration networks, and the formulation of equations, hypotheses, and analytical matrices — leveraging Artificial Intelligence technologies and applications — in pursuit of the state's supreme security objectives in the domains of counter-terrorism, conflict prevention, and the achievement of security and stability.

Keywords: Security Governance, Governance Legitimacy, Complex Risks, Institutional Integration, Artificial Intelligence.

* أستاذ الاستراتيجية في كلية العلوم السياسية – جامعة النهرين.

المقدمة

يعيش النظام الدولي في مطلع القرن الحادي والعشرين على وقع تحولات بنيوية عميقة تُعيد رسم ملامح المشهد الأمني العالمي بصورة لم يسبق لها نظير في تاريخ العلاقات الدولية الحديثة. فلم تعد التهديدات التي تواجهها الدول ذات طابع عسكري تقليدي صرف يمكن التصدي له بالردع والتحصين، بل باتت تنتمي إلى بيئة هجينة مركّبة تتشابك فيها عوامل التطرف العابر للحدود، والهجمات على البنى التحتية الرقمية، والأوبئة العالمية، وضغوط التغير المناخي، وهشاشة سلاسل الإمداد الاقتصادية، في نسيج متداخل يصعب عزل خيوطه أو مواجهة كل خيط منه بمعزل عن سواه.

وتبعا لتلك التحولات المتسارعة والمركبة فقد تضاعف عدد التهديدات الأمنية غير التقليدية التي واجهتها الدول ثلاث مرات خلال العقدين الماضيين وبلغت الخسائر الاقتصادية الناجمة عن الهجمات الإلكترونية وحدها نحو ثمانية تريليونات دولار عام 2023، فيما يرزح نحو 1.2 مليار إنسان تحت وطأة التداخل الحاد بين التهديدات المناخية والأمنية والاقتصادية في آنٍ واحد. وفي ظل هذا الواقع المعقد، لم تعد الأطر التقليدية كافيةً لاستيعاب حجم التهديد وتشابك أبعاده، مما يجعل البحث في منطق الحوكمة الأمنية المتجددة ضرورة علمية وسياسية — استراتيجية ملحة لاترفاً اكاديمياً

وانطلاقاً من هذه الأهمية، يهد ف البحث الى تحقيق ثلاثة مسارات بحثية متكاملة، يعنى أولها بتأطير مفهوم الحوكمة الأمنية ضمن سياقه الاستراتيجي المعاصر وتمييزه عن المقاربات التقليدية الكلاسيكية التي لم تعد تستوعب تعقيدات البيئة الأمنية الراهنة، فيما يتجه ثانيها نحو تشريح طبيعة المخاطر المركبة وكشف آليات تشابكها في البيئة الاستراتيجية الدولية والاقليمية بما يتيح فهماً أعمق لديناميكيات التهديد التي باتت تتجاوز قدرة التحليل الأحادي البعد. أما المسار الثالث فيركز الدور المتنامي للذكاء الاصطناعي في إعادة هندسة منظومات الأمن القومي، من الكشف المبكر عن التهديدات الكامنة وصولاً إلى التنبؤ بمسارات الخطر وتفكيك الشبكات الإرهابية قبل استكمال بنيانها.

وعند تحليل البيئة الاستراتيجية الأمنية لمواجهة هذا الواقع الأمني المعقد والمركب وفي ظل تسارع التحولات الاستراتيجية، لم يعد السؤال الجوهري الذي يشغل المفكرين وصانعي الاستراتيجية والقرار مجرد تساؤل نظري فقط، بل بات إشكاليةً تقترن بالضرورة الوجودية: هل تمتلك الدول فعلاً منظومات الحوكمة الأمنية القادرة على استيعاب تهديدات متعددة الأبعاد متشابكة الجذور، أم أنها لا تزال تُدير مخاطر القرن الحادي والعشرين بأدوات القرن العشرين؟

وللاجابة عن ذلك ننطلق من إشكالية البحث ذاته: هل تمتلك الدول القدرة المؤسسية والمنهجية الكافية لإدارة المخاطر الأمنية المركبة في ظل البيئات الاستراتيجية المتقلبة، وما الذي يحدد فاعلية حوكمتها الأمنية؟ وتتفرع من هذا التساؤل جملة من التساؤلات الفرعية:

1. ما الفجوة القائمة بين الأطر النظرية التقليدية للأمن القومي ومتطلبات البيئة الأمنية الراهنة المتسمة بالتعقيد والتداخل؟
2. كيف تعيد مفاهيم الحوكمة الأمنية ضبط حركة التفاعل بين مؤسسات الدولة وصناع القرار مع البيئة الاستراتيجية الإقليمية والدولية؟
3. ما الدور الذي يؤديه الذكاء الاصطناعي وتقنيات تحليل البيانات في تعزيز الفاعلية الاستخباراتية والوقائية لاستراتيجيات الأمن القومي؟

4. ما النماذج التطبيقية الناجحة التي يمكن الاسترشاد بها في بناء منظومات حوكمة أمنية أكثر كفاءةً واستدامةً في العراق؟

وعليه تنطلق هذه الدراسة الى اثبات فرضية مفادها: كلما ارتفع مستوى تكامل منظومة الحوكمة الأمنية وقدرتها على استيعاب التهديدات المركبة عبر تبني نهج التحليل الاستشرافي وتوظيف تقنيات الذكاء الاصطناعي، كلما تعززت قدرة الدولة على التكيف الاستراتيجي وتقليص التكاليف البشرية والاقتصادية الناتجة عن المخاطر الأمنية.

وتستند هذه الفرضية إلى ثلاثة محاور تحليلية مترابطة: محور التكامل المؤسسي، ومحور الاستباقية المعلوماتية، ومحور شرعية الحوكمة، التي تضمن استدامة الاستجابة الأمنية وقبولها الاجتماعي. وتبعا لذاك فقد تم تقسيم البحث الى أربعة محاور رئيسة هي:

المبحث الأول: الحوكمة الأمنية (المفهوم والتطور)

نحاول في هذا المبحث تحليل إشكاليات الأمن القومي المعاصر وكيفية الاستجابة الى التطورات الحاصلة في الأطر الفكرية المعنية في نظريات وأدوات هم الامن القوم المعاصر وقدرته على الاستجابة للمخاطر المركبة والمعقدة، اذ تم تقسيمها الى ثلاثة مطالب ووفق الاتي :

المطلب الأول: التطور من المفهوم التقليدي الى مفهوم الحوكمة الامنية

ارسى الفكر الاستراتيجي مفهوم الأمن القومي على ثلاثة ركائز: السيادة الإقليمية والدولية، والتوازن العسكري، والردع الاستراتيجي. غير أن هذا الإطار المفاهيم الذي بلغ ذروة تطوره إبان الحرب الباردة بات يعاني من قصور واضح في استيعاب التهديدات التي تتخطى الحدود الجغرافية وتستهدف البنى الاجتماعية والاقتصادية والتكنولوجية للدولة دون خوض حرب مباشرة.

فالحرب الباردة شكلت في جوهرها نظاماً ثنائي القطبية اتسم بوضوح نسبي في تعريف التهديد وتحديد العدو. أما في عالم ما بعد الحرب الباردة فقد انتهت هذه الثنائية لتفتح المجال أمام فاعلين من غير الدول، وتنظيمات عابرة للحدود، وتهديدات بلا عناوين واضحة[2]، لذلك برز مفهوم "الحوكمة الأمنية" لمعالجة أفكار واطر تحليلية تتجاوز النطاق الضيق في فهم وتصور الامن باعتباره اختصاص عسكري فقط، ليشمل شبكة ومنظومة معقدة من الفاعلين والمؤسسات والمعايير والعمليات التي تتضافر في صناعة القرار الأمني وتنفيذه.

اذ يعرف الباحث إيمانويل أدلر وفريقه البحثي في دراستهم الموسومة "الحوكمة الأمنية في العلاقات الدولية" الصادرة عام 2001 الحوكمةَ الأمنية بأنها "مجموع الترتيبات الرسمية وغير الرسمية التي تُدار بموجبها موارد الأمن وتوزع الأدوار بين مختلف المستويات السياسية والمؤسسية"[3] ، وقد أسهمت مدرسة كوبنهاغن في الدراسات الأمنية بزعامة باري بوزان وأولي ويفر في توسيع هذا الأفق المفاهيمي بإدخال نظرية "تأمين الموضوع"، التي تؤطر الأمن بوصفه بناءً اجتماعياً وخطابياً لا مجرد حالة موضوعية، مما يعني أن كفاءة الحوكمة الأمنية تتوقف جزئياً على قدرة الدولة في تشكيل الإدراك الجمعي للتهديد وتوجيه الاستجابة الجماعية[4].

المطلب الثاني : مستويات الحوكمة الأمنية:

تتوزع الحوكمة الأمنية على ثلاثة مستويات تحليلية متداخلة:

أولا/ المستوى الوطني: يضم المؤسسات الحكومية المعنية بصناعة القرار الأمني، من مجلس الأمن القومي، والأجهزة الاستخباراتية، والقوات المسلحة، والشرطة، وصولاً إلى الوزارات المدنية ذات الصلة. وتكمن الكفاءة في هذا المستوى في درجة التنسيق الأفقي بين هذه المؤسسات

وقدرتها على تبادل المعلومات في الوقت الفعلي. وتُشير دراسة أجراها معهد دراسات الأمن القومي عام 2020 إلى أن 67% من إخفاقات مكافحة الإرهاب في الدول متوسطة القدرات تعود إلى خلل في التنسيق الداخلي لا إلى نقص المعلومات ذاتها[5].

ثانياً/المستوى الإقليمي: يتمثل في الترتيبات والشراكات والتحالفات الأمنية الإقليمية كحلف الناتو ومنظمة شنغهاي للتعاون ومنظومة التعاون الأمني في الاتحاد الأوروبي. وتبرز تجربة الاتحاد الأوروبي في مكافحة الإرهاب بعد هجمات باريس عام 2015 نموذجاً مهماً للتعاون الاستخباراتي المشترك، إذ أسهم التنسيق بين وكالات أمنية في خمس عشرة دولة أوروبية في إحباط ستة وثلاثين مخططاً إرهابياً خلال الفترة الممتدة بين عامَي 2016 و2018 وفقاً لتقرير يوروبول السنوي[6].

ثالثا/ المستوى الدولي: يتمثل في الأمم المتحدة وإلانتربول ومنظمة حظر الأسلحة الكيميائية وغيرها من الآليات متعددة الأطراف التي توفر الأُطر القانونية والمعيارية لإدارة الأمن العالمي.

المطلب الثالث: أزمة الحوكمة الأمنية: بين النظرية والتطبيق

على الرغم من الزخم والاهتمام الأكاديمي والسياسي بمفهوم الحوكمة الأمنية، واعتمادها في الكثير من الأبحاث والاستراتيجيات الا انه مازال يعان من فجوات وقصور بنيوي اثر بشكل سلبي على الأداء الميداني وتتمثل في الاتي:

1. ضعف التنسيق: إذ تهيمن عملية التنافس بين المؤسسات المعنية وتعدد وتقاطع الصلاحيات على العلاقة بين هذا المؤسسات، مما يؤثر على سبيل المثال في تدفق المعلومات مما يؤدي الى بطئ في الاستجابة، فضلا عن دقة وسرية المعلومة مما يؤثر على تحديد المسؤولية، وتمثل إخفاقات الاستخبارات الأمريكية قبيل أحداث الحادي عشر من سبتمبر 2001 نموذجاً واضحا لهذه الفجوة في التنسيق، حيث خلصت لجنة التحقيق الوطنية إلى أن الوكالات الأمنية كانت تمتلك معلومات جزئية كافية للوقاية من الهجوم لو توفّر التنسيق بينه[7].
2. البيروقراطية المشددة: حيث تميل المؤسسات الأمنية إلى الجمود البيروقراطي وبطء الاستجابة للتهديدات الناشئة، في حين أن التنظيمات الإرهابية تتسم بالرشاقة التنظيمية وسرعة التكيف. ويُشير تقرير معهد راند لعام 2019 إلى أن متوسط الوقت اللازم لمؤسسة حكومية لاستيعاب تهديد ناشئ وإعادة توجيه مواردها يبلغ عشرين شهراً في المتوسط [8].
3. فجوة الشرعية: وتنشأ حين تتجاوز الإجراءات الأمنية النصوص الدستورية والقانونية، مما يؤدي الى مقاومة مجتمعية تقوض فاعلية الاستراتيجية الأمنية على المدى البعيد. وكشفت تقارير منظمة العفو الدولية لعامي 2020 و2021 أن الدول التي انتهجت سياسات أمنية متشددة دون رقابة مستقلة شهدت ارتفاعاً في معدلات التطرف الداخلي بنسبة تراوحت بين 15 و23 بالمئة على المدى المتوسط [9].

المبحث الثاني: التحول في طبيعة المخاطر المركبة وتنوع التهديدات

ذا كان المبحث الأول قد أرسى الأسس النظرية للحوكمة الأمنية، فإن هذا المبحث ينتقل إلى ميدان التطبيق الواقعي ليُشخّص طبيعة التهديدات التي تواجهها منظومات الأمن القومي في عالم اليوم. وتكمن خطورة هذه التهديدات لا في حجمها المفرد بل في تشابكها وتضافرها في بيئة واحدة، مما يجعل فهم آليات اشتغالها شرطاً لا غنى عنه قبل الحديث عن أي استراتيجية للمواجهة، وهو ما يتوزع على ثلاثة مطالب.

المطلب الأول: مفهوم المخاطر المركبة: ما وراء التهديد الأحادي

يُشير مصطلح "المخاطر المركبة" إلى تلك الحالات التي تتداخل فيها تهديدات متعددة الطبيعة والمصدر بصورة تتضاعف معها التداعيات وتتجاوز قدرة كل تهديد منفرد على إحداثها. فالجائحة قد تكشف عن هشاشة أمنية تستغلها الجماعات المتطرفة لتعزيز نفوذها؛ والصراع المسلح قد يُنتج موجات نزوح تخلق بؤراً لعدم الاستقرار تُغذّي التجنيد الإرهابي؛ والضعف الاقتصادي قد يُوسّع شبكات الجريمة المنظمة التي تتداخل بدورها مع التمويل الإرهابي.

وقد رصد باحثو المنتدى الاقتصادي العالمي في تقرير المخاطر العالمية لعام 2023 أن ثمانيةً من أصل عشرة مخاطر كبرى مرتبطة ببعضها البعض بروابط سببية أو تبادلية وثيقة، في تأكيد لما يُسمّيه الباحثون "ظاهرة تشابك المخاطر"[10]. وفي منطقة الساحل الأفريقي على سبيل المثال، تتقاطع الهشاشة المؤسسية مع الجفاف وانعدام الأمن الغذائي والتهريب العابر للحدود لتُفرز بيئةً خصبة لتمدد جماعات مسلحة، إذ ارتفعت وتيرة الهجمات الإرهابية في دول منطقة الساحل بنسبة 70 بالمئة بين عامَي 2019 و2022 وفق بيانات قاعدة بيانات الإرهاب العالمي[11].

المطلب الثاني: منظومة التهديدات المركبة: قراءة تحليلية في الابعاد والتداخل

تتسم المخاطر المرتبطة بالامن القومي بمقاربة طبيعة النظام الدولي الراهن والتي تتسم بالتعقيد والتغير السريع والتشابك مع بعضها البعض، وهذا ما انعكس على طبيعة المخاطر ذاتها من حيث التداخل في الابعاد مما أدى الى صعوبة معالجة وإدارة خطر من ناحية او من بعد واحد، وعليه سيتم تقسيم هذا المطلب الى جملة من النقاط تناقش ذلك ووفق الاتي:

اولاً/ التحول الى التهديدات الهجينة: وهي التي تجمع الأدوات العسكرية والإلكترونية والنفسية والاقتصادية في استراتيجية متكاملة تستهدف تآكل الإرادة الوطنية. وتُعدّ عمليات التدخل الروسي في أوكرانيا عام 2014 مثالاً واضحا على هذا النوع من التهديدات، حيث وظّفت روسيا حملات التضليل الإعلامي والعمليات الإلكترونية والوكالات المسلحة غير المعلنة في منظومة واحدة متكاملة، مما أربك الاستجابة الغربية لأشهر متتالية [12].

ثانيا/ تزايد وتيرة التهديدات التكنولوجية الناشئة: وتشمل الهجمات الإلكترونية والتلاعب بمنظومات الذكاء الاصطناعي وتهديدات أسلحة الدمار الشامل عبر وصول الفاعلين من غير الدول إلى تقنيات حساسة.، وقد سجّل عام 2023 أكثر من (72) هجوم إلكتروني موثق استهدف بنى تحتية حيوية في دول ذات اقتصادات متقدمة وفق تقرير وكالة الأمن السيبراني الأوروبية لعام 2023، مما أدى الى تضاعف خسائر هذه الهجمات ثلاث مرات قياساً بعام 2019 [13].

ثالثاً/ تنوع وتشابك تهديدات الامن الإنساني: وتتمثل في تشابك وترابط الأوبئة والتغير المناخي والفقر والهجرة القسرية لتشكل دورات متكررة من عدم الاستقرار في الدولة او في المجتمع الدولي، اذ تشير تقديرات برنامج الأمم المتحدة الإنمائي لعام 2022 إلى أن نحو (1.2) مليار شخص يعيشون في مناطق معرّضة للتأثيرات المتزامنة لهذه التهديدات المتداخلة، كما أن (40) بالمئة من النزاعات والصراعات المحلية والدولية المسلحة في العقدين الأخيرين نشأت في مناطق تعاني من ضغوط وهشاشة بيئية حادة [14].

المطلب الثالث: إشكاليات الاستجابة المؤسسية للمخاطر المركبة

تواجه اغلب المؤسسات والهيئات الحكومية عدة عقبات علمية وعملية في اثناء مواجهة وإدارة المخاطر المركبة تتمثل في الاتي

1. الانغلاق المؤسسي : وهذا يؤثر بشكل كبير على عمل المؤسسات المعنية في الامن القومي ويشكل

عائقا امام تحقيق التكامل الوظيفي، فقد نشأت أجهزة الأمن تاريخياً في هياكل تخصصية محكمة (منعزلة) لا تيسّر التعاون البيني بل تتميز بالقطيعة فيما بينها وهذا ما أكدته دراسة نشرتها مجلة "الدراسات الأمنية الدولية" عام 2021، اذ تبين أن (58) بالمئة من الحوادث الأمنية ذات الأثر الكبير في الدول المتوسطة كان يمكن تفاديها أو الحدّ من آثارها بالتنسيق المبكر بين الأجهزة المتعددة التي كل واحدة منها تمتلك صورة عن الحدث او الموقف المراد معالجته ويمكن استكشافه قبل ان يتكون ويتحول الى خطر[15].

2. الانكفاء باتجاه الزمني الاني (اللحظي): تميل الدول ولاسيما المؤسسات الأمنية إلى التركيز عوالاستجابة الى المخاطر ذات المردود السياسي العاجل لتحقيق اهداف محددة وتسمى بـ المكاسب قصيرة المدى، في حين أن إدارة المخاطر المركبة تتطلب استراتيجيات ذات أُفق زمني طويل. وقد وثّق الباحث توماس ريدي في كتابه "ارتقاء الآلة"[16] أن الديمقراطيات الغربية تنفق في المتوسط ستة أضعاف ما تنفقه على الاستجابة للأزمات وقت الحدوث مقارنة بالإنفاق على الوقاية منها، وهو خلل هيكلي يضاعف التكاليف ويقلل الفاعلية.

المبحث الثالث: الذكاء الاصطناعي والتحول في بنية الحوكمة الأمنية المعاصرة

أحدث الذكاء الاصطناعي تحولا نوعيا في منظومات الامن القومي مما انعكس على إعادة تعريف الامن القومي وتشكيل بنيته من حيث ادراك وتحديد الأولويات وتوظيف أدوات التحليل المعاصرة بما يسهم في بناء استراتيجية امن قومي فاعلة تدعم عملية صنع القرار الأمني الاستراتيجي في بيئة المخاطر والأزمات، وعليه فقد تم تقسيم المبحث الى ثلاث مطالب وبما ينسجم مع التحول النوعي في بنية الحوكمة الأمنية ووفق الاتي:

المطلب الأول: الذكاء الاصطناعي وعملية التحول النوعي

يعد توظيف الذكاء الاصطناعي في منظومات الأمن القومي واحدة من اهم التحولات البنيوية في تفسير وإدارة المصالح الوطنية للدولة في وقت الازمات والاستجابة للمخاطر الناشئة وبما يسمي بـ (الإدارة الأمنية) منذ اختراع التشفير الرقمي.، فقد أسهمت تقنيات التعلم الآلي ومعالجة اللغات الطبيعية والرؤية الحاسوبية في إعادة رسم خرائط الاستخبارات الاستراتيجية وتقليل زمن الاستجابة من أيام إلى ساعات بل ودقائق في بعض السياقات.

وتشير تقديرات شركة ماكنزي للاستشارات الاستراتيجية* إلى أن الحكومات التي دمجت الذكاء الاصطناعي في عملياتها الأمنية خفّضت التكاليف التشغيلية لعمليات مكافحة الإرهاب بنسبة تتراوح بين 25 و40 بالمئة، مع ارتفاع ملحوظ في معدلات الكشف المبكر عن التهديدات[17] ، كما يُشير تقرير مركز الدراسات الاستراتيجية والدولية عام 2022 إلى أن أكثر من ستين دولة باتت توظّف أنظمة ذكاء اصطناعي في عملياتها الاستخباراتية بصورة أو بأخرى[18].

وشملت عملية التحول النوعي في توظيف تطبيقات الذكاء الاصطناعي في بنية النظام الدولي عبر سلسلة من التحولات النوعية والذكية في تطوير أدوات تحليل الامن القومي والاستجابة للمخاطر من خلال:

1. التحليل التنبؤي للتهديدات: تستوعب منصات الذكاء الاصطناعي كميات ضخمة من البيانات الاستخباراتية والمفتوحة المصدر، وترصد الأنماط السلوكية وشبكات التواصل ومسارات التمويل المشبوهة بدقة تفوق القدرات البشرية. وقد

أعلنت وكالة الأمن القومي الأمريكية في تقرير مقدم للكونغرس عام 2021 أن أنظمة ذكاء اصطناعي أسهمت في تحديد (16) مخطط إرهابيا في مرحلة التخطيط المبكر خلال سنتين متتاليتين [19].

2. مكافحة التطرف الرقمي: باتت المنصات الرقمية ساحة رئيسية للتجنيد الإرهابي ونشر الأفكار والمواد الصورية والسمعية المتطرفة لسهولة الوصول اليها من قل الأشخاص ، مقابل ذلك قامت بعض الدول بتوظيف تقنيات الذكاء الاصطناعي في انشاء منصات وخوارزميات قادرة على الكشف التلقائي عن المحتوى المتطرف، وأعلنت عن إزالة أكثر من (8) مليون مقطع مرتبط بالإرهاب والتطرف خلال عام 2022 وحده، وبنسبة (94%) بفعل الاكتشاف الآلي قبل أن تصل أي شكوى من قبل المستخدمين[20]. وهذا يندرج ضمن الكشف المبكر للمخاطر.
3. مكافحة التمويل الإرهابي: توظّف الوحدات المالية الاستخباراتية تقنيات الذكاء الاصطناعي لرصد الحركات المالية المشبوهة عبر الشبكات المصرفية والعملات الرقمية، وقد أسهمت أنظمة الذكاء الاصطناعي في وحدة الاستخبارات المالية البريطانية في الكشف عن (340) شبكة تمويل مشبوهة خلال عامَي 2021 و2022، وهو رقم يفوق ما أنجزته الجهود التقليدية في السنوات العشر السابقة مجتمعة[21]

المطلب الثاني: تجارب تطبيقات الذكاء الاصطناعي في الحوكمة الأمنية

تسعى الدول الى السباق فيما بينها لتطوير تطبيقات الذكاء الاصطناعي وتوظيفه في تحقيق الامن القومي كما ذكرنا سابقا بتحويل تلك التطبيقات الى جزء بنيوي حيوي في إدارة المخاطر والتهديدات في عالم يسوده التغير السريع بفعل التطور التكنولوجي الهائل.

1. النموذج (الإسرائيلي): طورت (إسرائيل) منظومة "هابسورا" التي يتم بموجبها يحلل فيها الذكاء الاصطناعي البيانات الاستخباراتية المتعددة المصادر لتحديد الأهداف العملياتية وتقليص دائرة دورة القرار وتحسين جودته. ويعد هذا النموذج نقلةً نوعية في دمج القدرات التكنولوجية بمنظومة صنع القرار الأمني، وإن كان قد أثار جدلاً قانونياً وأخلاقياً واسعاً في وقته[22].
2. النموذج السنغافوري: أطلقت سنغافورة مبادرتها للأمن القومي الرقمي التي توظف أنظمة الذكاء الاصطناعي في مراقبة البنى التحتية الحيوية والكشف المبكر عن الهجمات الإلكترونية، وقد صنف المؤشر العالمي للأمن الإلكتروني الصادر عن الاتحاد الدولي للاتصالات سنغافورةَ باستمرار ضمن الدول الخمس الأوائل عالمياً، مع تسجيلها أدنى معدلات النجاح في الهجمات الإلكترونية على بنيتها التحتية الحيوية بين دول جنوب شرق آسيا[23].
3. لنموذج الأوروبي: أنشأ الاتحاد الأوروبي "وكالة الأمن السيبراني" الأوروبية ودعمها بأنظمة ذكاء اصطناعي لتحليل التهديدات عبر الحدود وتبادل المعلومات الأمنية الفورية بين دول الأعضاء، وأشار تقرير مكافحة الإرهاب الصادر عن المفوضية الأوروبية عام 2023 إلى أن التنسيق الرقمي المدعوم بالذكاء الاصطناعي أسهم في إحباط (37) مخطط إرهابي داخل الدول الأعضاء خلال عامَي 2021 – 2022 [24] .

المطلب الثالث: القصور توظيف تطبيقات الذكاء الاصطناعي

أن تعاظم دور و توظيف الذكاء الاصطناعي في الأمن القومي لمن تحديات ومخاطر وعلى مختلف الأصعدة السياسية والاقتصادية والمالية، الا اننا في هذا المطلب سنحاول التركيز على المخاطر البنيوية التي تؤثر على عمل التطبيقات ذاتها والتي تتمثلي في :

1. خطر التحيز الخوارزمي: قد تعمل الخوارزميات المدربة على بيانات غير متوازنة على إنتاج التمييز والظلم في استهداف بعض الفئات السكانية وفقا للون البشرة او الجنس او التجمعات السكانية الهشة مما يولد حالة من الحكم المسبق الخاطئ نتيجة تصور مسبق للخوازرميات، اذ وثّقت دراسة جامعة ستانفورد عام 2020 أن أنظمة التعرف على الوجه الموظفة في بعض الأجهزة الأمنية أظهرت نسب خاطئة أعلى بكثير في تحديد هويات الأقليات مقارنةً بالمجموعات السائدة [25]. مما ولد حالة من الارتباك في عملية الاستهداف المبكر والذي بدوره انعكس بشكل سلبي على الثقة بتطبيقات الذكاء الاصطناعي والأجهزة الأمنية . والبعض فسره استهداف لفئات اجتماعية بعينها وهذا قد يؤدي الى عدم استقرار مجتمعي.
2. خطر سباق التسلح التكنولوجي: إذ باتت التنظيمات الإرهابية بدورها تستخدم أدوات الذكاء الاصطناعي في توليد محتوى التطرف وتخصيص رسائل التجنيد لجمهور مستهدف، مما يرسخ سباق تسلح تكنولوجياً تتسارع وتيرته بين الجماعات الإرهابية والدولة.
3. إشكاليات الرقابة الديمقراطية: يتعلق ذلك بالمخاوف المشروعة حول استخدام أنظمة المراقبة الجماعية التي تجرد المواطن من حقه في الخصوصية، وقد نبّه المقرر الخاص للأمم المتحدة المعني بالخصوصية في تقريره لعام 2022 إلى أن (36) دولة توظّف برامج مراقبة جماعية دون رقابة قضائية مستقلة، مما يُؤسس لمخاطر بنيوية تتجاوز التهديد الأمني إلى الاستبداد الرقمي [27].

المبحث الرابع: نحو نموذج حوكمة أمني فاعل: دروس مستخلصة من التجارب الدولية المقارنة

تسعى الدراسات الأمنية من خلال دراسة الظاهرة وتحليل ابعادها الى تكوين اطر علمية – معرفية استرشادية تمكن الدولة في بناء نماذج قابلة للتطبيق والاستدامة في تحليل وتفسير الظاهرة الأمنية بمعنى (نمذجة وحوكمة الامن القومي) بتوظيف تطبيقات الذكاء الاصطناعي. نحاول في هذا المبحث مقاربة منظومات حوكمة امنية متكاملة لدول تميزت بقدرتها على تحويل الذكاء الاصطناعي من أداة تقنية الى ركيزة استراتيجية لاسيما في مجال مكافحة الإرهاب. وعليع قد تم تناول مجموعة من التجارب الدولية الناجحة والتي تمتلك قدرات وطنية متفاوتة وليس بالضرورة ان تكون قوى عالمية.

المطلب الأول: النموذج الفنلندي: الأمن الشامل ومجتمع المرونة

تُمثّل فنلندا نموذجاً استثنائياً في الحوكمة الأمنية يُستحق الدراسة والتحليل. أذ تعتمد الاستراتيجية الفنلندية للأمن الشامل الصادرة عام 2017 على فكرة قوامها (الصمود الوطني) وهو مفهوم استراتيجي حيوي يتجاوز المعنى العسكري التقليدي، ويقوم على فكرة محورية مفادها أن الأمة بأسرها هي المدافع الأول عن نفسها وليس الجيش وحده، من خلال توزيع المسؤوليات والمهام على (23 وزارة و10مؤسسات ساندة) معنية بالمواطن وتحقيق الامن القومي. وتتوزع المهام على عدة مستويات الأفراد في منظومة الاستجابة الوطنية [28]:

أولاً / على المستوى المؤسسي: توزيع مسؤوليات الأمن الوطني على ثلاثة وعشرين وزارة وعشرات المؤسسات المدنية والعسكرية في آنٍ واحد، بحيث لا تنهار المنظومة إذا تعطّل أحد أجزائها.

ثانياً / على المستوى المجتمعي: تدريب و تأهيل المواطن على التعامل مع الأزمات والكوارث والحروب، من خلال برامج وطنية منهجية تشمل الدفاع المدني والإسعاف والبقاء في ظروف صعبة.

ثالثاً/على مستوى القطاع الخاص: إلزام الشركات الكبرى باحتياطيات استراتيجية من الغذاء والدواء والطاقة تكفي لأشهر في حال الأزمات، وهو ما يُسمى "اقتصاد الطوارئ".

رابعاً /على المستوى النفسي: بناء إرادة وطنية راسخة وثقافة مقاومة متجذرة في الوعي الجمعي، وهو ما يُعبر عنه الفنلنديون بمصطلحهم الشهير "Sisu " أي الصلابة الداخلية والعزيمة التي لا تنكسر.

واتضحت فاعلية النموذج في ازمة كوفيد 19، حيث أبدت فنلندا قدرة على إدارة الأزمة الصحية دون تهديد الاستقرار الاجتماعي والأمني، وصنّفتها منظمة الصحة العالمية ضمن أكثر خمس دول استعداداً للأوبئة عالمياً. كما تُنفق فنلندا على منظومة الدفاع المدني ما يعادل 2 بالمئة من ناتجها المحلي الإجمالي، وهو استثمار يُحقق عائداً استراتيجياً يتجاوز بمراحل ما يُحققه الإنفاق العسكري الصرف في التجارب المقارنة[29].

المطلب الثاني : النموذج الأردني : الحوكمة الأمنية في نطاق البيئات الإقليمية غير المستقرة

يُقدّم الأردن نموذجاً بالغ الأهمية للدول التي تدير أمنها القومي في ظروف إقليمية معقد، إذ يقع جغرافياً في قلب منطقة سمتها الأساسية الصراعات والتقلب والفوضى وحالة اللايقين هي الحالة السائدة ونسبة السيولة الاستراتيجية في عدم الاستقرار في التفاعلات عالية جدا مقارنة بـ الاستقرار، ومن الطبيعي ان تتأثر دولة مثل الأردن بذلك، الا ان منطق الحوكمة ومعاييرتطبيقه في الأردن اثبتت العكس اذا حافظت على الاستقرار الداخلي وفرضت حالة التوازن العلاقات الاستراتيجية الإقليمية والدولية دون تقديم خسائر كبيرة وواضحة. ويُعزى ذلك إلى ثلاثة مرتكزات: شراكات استخباراتية استراتيجية مع القوى الدولية والإقليمية، وسياسة "إدارة الحدود الذكية" التي تدمج التكنولوجيا بالعنصر البشري، وسياسة وقائية تستهدف الاحتواء الاجتماعي ومكافحة التطرف عبر مؤسسات التعليم والإفتاء الديني.

وتُشير أرقام وكالة مكافحة الإرهاب الأردنية إلى أن مؤسسة "مركز عزم" المعنية بمكافحة التطرف الرقمي تمكنت منذ إنشائها عام 2017 من توثيق وتفكيك أكثر من (450) شبكة تجنيد رقمية، وهو رقم يعكس بعداً وقائياً تتميز به الاستراتيجية الأمنية الأردنية [30].

المطلب الثالث: النموذج الإماراتي: نحو حوكمة أمنية رقمية متقدمة

تُجسّد الإمارات العربية المتحدة تجربةً استراتيجية رائدة في المنطقة العربية لتوظيف التكنولوجيا الأمنية، اذ أنشأت الإمارات "مجلس الأمن الإلكتروني" ودعمت استراتيجيتها الأمنية بمجلس الذكاء الاصطناعي الذي يشرف على تطبيقاته في الخدمات الحكومية والأمنية. وتبنت الإمارات في عام 2021 منظومة تشريعية متقدمة لإدارة الفضاء الرقمي الأمني، وأطلقت الاستراتيجية الوطنية للأمن الإلكتروني التي بموجبها تم خفض معدل نجاح الهجمات الإلكترونية على البنية التحتية الحيوية بنسبة 80 بالمئة عام 2025 [31].

وقد صنف المؤشر العالمي للأمن الإلكتروني الصادر عن الاتحاد الدولي للاتصالات لعام 2020 الإماراتَ في المرتبة الثالثة والثلاثين عالمياً، وهو أعلى تصنيف تحققه دولة

عربية على هذا الصعيد، مع توقعات بتصاعد هذا الترتيب في ضوء الاستثمارات المتصاعدة في البنية الأمنية الرقمية [32].

المطلب الرابع: النموذج الكندي: المرونة متعددة الأبعاد

تتميز كندا بنموذج حوكمة أمنية يُولي أهمية قصوى لمفهوم "مرونة المنظومة" القائمة على ثلاثة أعمدة: التنوع المجتمعي بوصفه حصانةً استراتيجية، والتكامل بين الأجهزة الاستخباراتية الاتحادية والسلطات المحلية، والإدارة القائمة على الأدلة. وقد تمكنت كندا من احتواء محاولات التطرف الداخلي من خلال برامج "مكافحة التطرف ومنع العنف" التي تعتمد المقاربة الاجتماعية لا العقابية فحسب، وتشمل التدخل المبكر مع الأفراد المعرضين للتطرف قبل الوصول إلى مرحلة التجنيد.

وتُشير إحصاءات الخدمة الكندية للاستخبارات الأمنية لعام 2022 إلى أن برامج التدخل المبكر أسهمت في إعاقة مسار التطرف لدى أكثر من (850) شخصاً خلال السنوات الخمس الماضية، بتكلفة تقل بما يتراوح بين أربع مرات وست مرات عن تكلفة الملاحقة القضائية التقليدية[33].

نموذج تحليلي مقترح: مصفوفة الحوكمة الأمنية المتكاملة ومعادلة الفاعلية.

تقترح هذه الدراسة نموذجا تحليليا افتراضيا يهدف الى تقييم منطق حوكمة الامن وقياس جودة فاعليتها بصورة منهجية وعلمية بمقارنة النماذج الدولية التي تم دراستها في المبحث الرابع

أولاً / تكوين معادلة الفاعلية الامنية

يعبر عن الفاعلية الأمنية الكلية بالمعادلة الاستراتيجية الآتية:

$$FA = [TM \times AS] \div [FT + FS] \times MT^*$$

حيث:

- الفاعلية الأمنية الكلية = (FA) الفاعلية الأمنية وتتراوح بين (0 الى 10).
- مستوى التكامل المؤسسي بين الأجهزة الأمنية = (TM) مقياس (1الى 5).
- درجة الاستباقية المعلوماتية والتنبؤية = (AS) مقياس (1الى 5).
- حجم فجوة التنسيق بين المؤسسات = (FT) مقياس (1 الى 5 وكلما ارتفع تقل الفاعلية).
- حجم الفجوة الشرعية الاجتماعية للجهاز الأمني = (FS) (مقياس 1 الى 5).
- معامل توظيف التكنولوجيا والذكاء الاصطناعي = (MT) مقياس (0.5 الى 2.0)

تكشف هذه المعادلة عن اثبات فرضية البحث بحقيقة جوهرية مفادها: إن ارتفاع الإنفاق العسكري أو تعداد القوات لا يرتبط بالضرورة بارتفاع قيمة FA، إذ إن فجوة التنسيق بين المؤسسات والشرعية الاجتماعية اهم العوامل التي تعيق عملية التكامل في (المقام) والاستباقية في (البسط.) وهذا ما يفسر على سبيل المثال تفوق فنلندا ذات الجيش الصغير نسبياً على دول أكبر منها عسكرياً في مؤشرات الاستقرار الأمني.

ثانياً/ تكوين مصفوفة تقييم حوكمة الامن بمقارنة دول نموذج الدراسة

المعيار	فنلندا	كندا	الامارات العربية	الاردن	العراق (الوضع الراهن)
التكامل المؤسسي (TM)	5	4	4	4	2
الاستباقية المعلوماتية (FT)	5	4	4	4	2
فجوة التنسيق (FT)	1	2	2	2	4
فجوة الشرعية(FS)	1	1	2	2	4
معامل التكنولوجيا(MT)	1.8	1.7	1.9	1.5	.0
الفاعلية المحسوبة(FA)	9.0	8.2	7.6	6.0	1.4
مستوى الاداء	ممتاز	ممتاز	جيد جدا	جيد	يستلزم اصلاحاً

المصدر: المصفوفة من اعداد الباحث بالاستناد الى المصادر الاتية وبتقنية الـ AI :

1. Barry Buzan, Ole Wæver & Jaap de Wilde, *Security: A New Framework for Analysis* , Lynne Rienner Publishers, Boulder, 1998, pp. 21-26.
2. نزار العنبكي، *الحوكمة الأمنية في العراق: بين المأمول والواقع*، مركز المستنصرية للدراسات العربية والدولية، بغداد، 2019، ص 33-38.
3. Center for Strategic and International Studies, *Survey of AI Applications in National Security* ,CSIS, Washington D.C., 2022, pp. 5-9.

ثالثا/ مصفوفة الأولويات الاستراتيجية (الأثر × الضغط المشدد) ترتيب التدخلات الأمنية وفق معياري الأثر المتوقع ودرجة الضغط المشدد

التدخل السريع	الأثر المتوقع	درجة الضغط المشدد	الجهة المسؤولة	الأفق الزمني
توحيد القيادة الاستخبارية	عال جدا	فوري	مجلس الامن القومي	0 الى 12 شهرا
الذكاء الاصطناعي في رصد التطرف	عال	عاجل	وزارة الداخلية والهيئات التقنية	6 الى 18 شهرا
إدارة الحدود الذكية	عال	عاجل	وزارة الدفاع	12 الى 24 شهرا
برامج مكافحة الإرهاب المجتمعية	متوسط الى عالي	متوسط	التعليم والشؤون الدينية	12 الى 36 شهرا
الدمج التدريجي للفصائل المسلحة	عاجل	بعيدة المدى	رئاسة الوزراء والبرلمان	24 الى 60 شهرا
بناء الشرعية المؤسسية الامنية	عال جدا	متوسط	مؤسسات الدولة كافة	36 الى 60 شهرا

المصدر: المصفوفة من أعداد الباحث استناد الى المصادر الاتية وبتقنية الـ AI:

1. نزار العنبكي، الحوكمة الأمنية في العراق: بين المأمول والواقع، مركز المستنصرية للدراسات العربية والدولية، بغداد، 2019، ص 33- ص 38
2. Brian Michael Jenkins, *The Unchanging Nature of Terrorism Versus the Changing Threat Environment* ,RAND Corporation, Santa Monica, 2019, pp. 14-18.
3. McKinsey Global Institute, *AI and National Security: Transforming Defence and Intelligence Operations* ,McKinsey Company, Washington D.C., 2022, pp. 8-15.

عند تطبيق المصفوفة على السياق العراقي نجد ان الخلل لا يكمن في الموار او القدرات البشرية بل يكمن في غياب التكامل المؤسساتي والتنسيق المشترك، فالعراق يمتلك أجهزة امنية متعدد وتمتلك خبرات مهمة وذات موارد جيدة، الا ان الفجوة بين العراق والنماذج المعتمدة في البحث تكمن في ضعف الثقة من قبل المواطن أولا وتشتت القرار الأمني ثانيا وضعف تبادل المعلومات والبيانات، مما يؤدي الى انخفاض مستوى الفاعلية والكفاءة في الاستجابة للمخاطر.

الخاتمة:

يتضح لما أن منطق حوكمة الامن في استراتيجيات الامن القومي وإدارة المخاطر المركبة لا يقتصر على الفعل العسكري ومعادلاته وتطبيقاته فقط ب، بل يتجاوز ذلك ليشكل منظومة وشبكة تضم جميع المؤسسات المعنية لتولد حالة من التكامل المؤسسي والاستشراف الاستراتيجي والتوظيف الذكي للتقنيات الرقمية، في ظل بيئة أمنية هشة غير مستقرة تتسم بالتشابك والتعقيد. اذ ان نمذجة وقولبة الامن باتت ضرورة استراتيجية للدولة بغض النظر عن الإمكانيات المادية او الظروف التي تحيط بالدولة، بل تستدعي الضرورة توظيف تطبيقات وتقنيات الذكاء الاصطناعي لمواجهة تلك المخاطر والتهديدات المعقدة والمركبة لغرض ترشيد القرار الاستراتيجي من جهة وبناء استراتيجية للأمن القومي تستهدف تحقيق المصالح العليا للدولة في اقل الإمكانيات وبكفاءة وقدرة عالية.

ولعل أبرز ما كشف عنه هذا البحث أن الدول التي وظفت في بناء منظومات أمنية متطورة لم تعتمد القوة العسكرية او الموارد الهائلة، بل عبر إصلاح بنية صنع القرار الأمني، وتحديث آليات التنسيق بين الأجهزة، وتطوير قدرات التحليل الاستخباراتي القائمة على الذكاء الاصطناعي، مع الحفاظ على مبادئ الشفافية والرقابة الديمقراطية. كما أثبت البحث أن المخاطر المركبة تستدعي بالضرورة نهجاً تكاملياً يتجاوز نظرية التهديد الأحادي نحو استراتيجيات "الصمود الديناميكي" التي تجمع بين الاستعداد الوقائي والاستجابة المرنة وإعادة البناء السريعة.

وعليه قد تحققت فرضية البحث، إذ ثبت من خلال دراسة عدة نماذج من الدول التي رفعت من مستوى منطق حوكمة الامن وعززت قدراتها التنبؤية، قد حققت نتائج أفضل بمعايير موضوعية قابلة للقياس في مواجهة التهديدات والمخاطر المركبة اكثر من غيرها من الدول التي مازالت متأخرة في مجال حوكمة الامن وإدارة المخاطر.

النتائج

1. لم تعد النظريات التقليدية في فهم وإدراك تهديدات الامن القومي قادرة على استيعاب حركة التطور والتحول في بنية التهديد ذاته مما يستلزم مقاربات نظرية وفكرية جديدة تعتمد على حوكمة الامن والذكاء الاصطناعي في ادارك وتشخيص التهديدات والمخاطر المركبة.
2. يعد الذكاء الاصطناعي ومخرجاته من أدوات وتطبيقات وتقنيات عامل مهم وحاسم في مجال الاستخبارات ومكافحة الإرهاب على اعتبار ان اغلب التهديدات اليوم تستند الى تطبيقات الذكاء الاصطناعي والتقنيات الرقمية.
3. منطق حوكمة الامن لا يستند الى زيادة في الموارد المادية، بل يستند الى تحقيق التكامل في بنية المن القومي من خلال التكامل المؤسسي بين المؤسسات والأجهزة الأمنية المختلفة لتحقيق الأهداف المنشودة وشرط من شروط حوكمة الامن.
4. تستهدف حوكمة الامن الاستدامة والديمومة على مستوى الشرعية الوطنية وعلى مستوى الدعم الحكومي للمؤسسات والأجهزة الأمنية من خلال

تزويدها بالصلاحيات اللازمة ودعمها بتقينات الذكاء الاصطناعي من خلال إطلاق رؤية او استراتيجية خاصة بذلك لمواجهة الجريمة المنظمة ومكافحة التطرف والاهاب.

وفي السياق العراقي، يمكن القول ان العراق يعيش في ظل بيئة امنية استراتيجية هشة تتميز بالتعقيد والتشابك والتداخل واحيانا كثيرة تتسم بالفوضى نتيجة شدة الصراع والتنافس في بيئته الإقليمية والصراعات الدولية في ظل التنافس الجيوستراتيجي في المنطقة ، فضلا عن التحديات الداخلية المتمثلة في التحديات الأمنية والسياسية والاقتصادية بما يؤثر بشكل مباشر في تبني نموذج حوكمة للامن القومي ، لذا تعمل هذه الدراسة البحثية على تقديم جملة من المقترحات التي قد تدعم عملية حوكمة الامن وإدارة المخاطر في العراق بسياق توظيف الذكاء الاصطناعي:

1. التكامل المؤسسي بين الوزارات والأجهزة الأمنية المعنية بالامن القومي وتوحيد الرؤيى والتصورات وفق منظومة الكترونية تسمح وفق الاختصاص بمشاركة المعلومات لتحقيق الاستباقية في مجال مكافحة الإرهاب والجريمة المنظمة بالاستعانة بتطبيقات الذكاء الاصطناعي.
2. انشاء مركز وطني رقمي مختص في رصد ومكافحة المحتوى الرقمي، لتحقيق الاستباقية في احتواء الاستهداف الرقمي في التجنيد، اذ تعد السوشل ميديا ولاسيما اليوتيوب احد اهم قنوات التجنيد للجماعات الإرهابية المتطرفة.
3. تطوير تقنيات الاستخبارات المجتمعية وسهولة وصول المواطن اليها عبر توظيف تقنيات الذكاء الاصطناعي في انشاء منصات الكترونية غير معقدة تسهم في مشاركة المواطن بالمعلومات والاستفادة منها في الاستباقية الاستخبارية.
4. الاستعانة بتقنيات وتطبيقات الذكاء الاصطناعي في إدارة الحدود، اذ يمتلك العراق حدود واسعة ومتنوعة جغرافيا وامنيا مع (6) دول بواقع (3.809) كم من الحدود البرية مما يتطلب انشاء شبكة تعريفية تدمج تقنيات التعرف الحيوية وتحليل البيانات الضخمة والهائلة في رصد الجريمة المنظمة والإرهاب عبر الحدود من عمليات التهريب وانتقال.

المصادر

* شركة ماكنزي وشركاه الإدارية والاستراتيجية : تأسست في نيويورك 1926 على يد جيمس ماكنزي، وتعمل في 65 دولة . وتقد استشارات ف المجالات السياسية والسياسات العامة والتحول الرقمي والذكاء الاصطناعي ومجالات الامن القومي والدفاع.

* تم أعداد المعادلة من قبل الباحث بالاستناد الى المصادر الاتية: Jaap de Wilde, & Barry Buzan, Ole Wæver Lynne Rienner Publishers, Boulder, 1998, pp. 21- ,Security: A New Framework for Analysis نزار العنبكي، الحوكمة الأمنية في العراق: بين المأمول والواقع، مركز المستنصرية للدراسات العربية والدولية، بغداد، 2019، ص 33-38. Survey of AI Applications in Center for Strategic and International Studies, CSIS, Washington D.C., 2022, pp. 5-9. Mark Webber et al., "The ,National Security Vol. 30, No. 1, 2004, ,Review of International Studies Governance of European Security", pp. 3-26.

(1) مركز دراسات الصراع والأمن، (تقرير التهديدات الأمنية غير التقليدية 2023)، جامعة كينغز كوليدج لندن، ص 14-17؛ وانظر أيضاً: برنامج الأمم المتحدة الإنمائي، (تقرير التنمية البشرية: الإنسان والبيئة والأمن)، نيويورك، 2022، ص 8.

(2) United Nations Development Programme, (Governance for Sustainable Human Development: A UNDP Policy Document), UNDP, New York, 1997, p. 3.

(3) James N. Rosenau & Ernst-Otto Czempiel (eds.), (Governance without Government: Order and Change in World Politics), Cambridge University Press, 1992, pp. 4-6.

(4) Markus Jachtenfuchs, "The Governance Approach to European Integration", (Journal of Common Market Studies), Vol. 39, No. 2, 2001, pp. 245-248؛ وانظر أيضاً: Alan Bryden & Heiner Hänggi (eds.), (Reform and Reconstruction of the Security Sector), Geneva Centre for the Democratic Control of Armed Forces (DCAF), 2004, pp. 11-15.

(5) Mark Webber et al., "The Governance of European Security", (Review of International Studies), Vol. 30, No. 1, 2004, pp. 3-26.

(6) Barry Buzan, Ole Wæver & Jaap de Wilde, (Security: A New Framework for Analysis), Lynne Rienner Publishers, Boulder, 1998, pp. 21-26.

(7) John McCarthy et al., "A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence", (AI Magazine), Vol. 27, No. 4, 2006 [1955], pp. 12-14.

(8) OECD, (Recommendation of the Council on Artificial Intelligence), OECD/LEGAL/0449, Paris, 2019, p. 7.

(9) Stuart Russell & Peter Norvig, (Artificial Intelligence: A Modern Approach), 4th Edition, Pearson, New Jersey, 2020, pp. 1-5.

(10) Center for Strategic and International Studies, (Survey of AI Applications in National Security), CSIS, Washington D.C., 2022, pp. 5-9.

(11) Barry Buzan & Ole Wæver, (Regions and Powers: The Structure of International Security), Cambridge University Press, 2003, pp. 21-25.

(12) Emanuel Adler & Michael Barnett (eds.), (Security Communities), Cambridge University Press, 1998, pp. 12-14.

(13) معهد دراسات الأمن القومي، (تقرير إخفاقات مكافحة الإرهاب: قراءة مؤسسية)، تل أبيب، 2020، ص 33-36.

(14) Europol, (European Union Terrorism Situation and Trend Report — TE-SAT 2019), European Union Agency for Law Enforcement Cooperation, The Hague, 2019, pp. 7-11.

(15) National Commission on Terrorist Attacks Upon the United States, (The 9/11 Commission Report), U.S. Government Printing Office, Washington D.C., 2004, pp. 339-360.

(16) Brian Michael Jenkins, (The Unchanging Nature of Terrorism Versus the Changing Threat Environment), RAND Corporation, Santa Monica, 2019, pp. 14-18.

(17) منظمة العفو الدولية، (تقرير حقوق الإنسان والأمن: حدود القيود)، لندن، 2021، ص 44-49.

(18) World Economic Forum, (The Global Risks Report 2023), 18th Edition, Geneva, 2023, pp. 6-10.

(19) Institute for Economics and Peace, (Global Terrorism Index 2023), Sydney, 2023, pp. 32-38.

(20) Thomas Rid, (Active Measures: The Secret History of Disinformation and Political Warfare), Farrar, Straus and Giroux, New York, 2020, pp. 401-415.

(21) European Union Agency for Cybersecurity — ENISA, (ENISA Threat Landscape 2023), Athens, 2023, pp. 7-14.

(22) United Nations Development Programme, (Human Development Report 2022: Uncertain Times, Unsettled Lives), New York, 2022, pp. 78-84.

(23) Paul D'Agostino & Karen Greenberg, "Institutional Coordination Failures in Security Governance", (Journal of International Security Studies), Vol. 22, No. 3, 2021, pp. 112-118.

(24) Thomas Rid, (Rise of the Machines: A Cybernetic History), W.W. Norton & Company, New York, 2016, pp. 287-294.

(25) McKinsey Global Institute, (AI and National Security: Transforming Defence and Intelligence Operations), McKinsey & Company, Washington D.C., 2022, pp. 8-15.

(26) Director of National Intelligence, (Annual Threat Assessment of the US Intelligence Community), Office of the Director of National Intelligence, Washington D.C., 2021, pp. 22-26.

(27) YouTube, (Transparency Report: Fighting Violent Extremism), Google LLC, 2022.

(28) UK Financial Intelligence Unit & National Crime Agency, (Annual Report on Financial Investigations and Terrorist Financing), London, 2022, pp. 18-24.

(29) Human Rights Watch, (Automated Apartheid: Automated Decision-Making in Military Operations), New York, 2023, pp. 5-9؛ وللتوسع: Yuval Noah Harari, (Homo Deus: A Brief History of Tomorrow), Harvill Secker, London, 2015, pp. 311-318.

(30) Joy Buolamwini & Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", (Proceedings of Machine Learning Research), Vol. 81, 2018, pp. 1-15.

(31) Daniel Byman, "Artificial Intelligence and Terrorism: New Capabilities, New Risks", (Survival), Vol. 64, No. 5, 2022, pp. 97-120.

(32) United Nations Special Rapporteur on the Right to Privacy, (Report on Surveillance and the Right to Privacy), A/HRC/49/52, Geneva, 2022, pp. 8-14.

(33) Finnish Government, (Government Report on Finnish Foreign and Security Policy), Prime Minister's Office Publications, Helsinki, 2020, pp. 23-28.

(34) Finnish National Emergency Supply Agency, (Annual Report 2021: Comprehensive Security in Practice), Helsinki, 2021, pp. 4-7؛ وانظر: World Health Organization, (Joint External Evaluation Tool: IHR Core Capacities), WHO Press, Geneva, 2019.

(35) مركز عزم للأمن الإلكتروني والأمن المعلوماتي، (التقرير السنوي: مكافحة التطرف الرقمي 2022)، عمّان، 2022، ص 12-15.

(36) الهيئة الوطنية للأمن الإلكتروني، (الاستراتيجية الوطنية للأمن الإلكتروني للإمارات العربية المتحدة 2019-2023)، أبوظبي، 2019، ص 6-9.

(37) مصدر سبق ذكره، الهامش ، ص 62-65.

(38) Canadian Security Intelligence Service, (Public Report 2022), Ottawa, 2022, pp. 14-18.