

التحول الرقمي وأثره في تطوير منظومة اتخاذ القرار الأمني

عمر احمد محمد الانصاري

باحث قانوني في العلوم القانونية والجنائية / قطر

law.mohzheee@gmail.com

المستخلص:

تناولت هذه الدراسة التحول الرقمي وأثره في تطوير منظومة اتخاذ القرار الأمني، انطلاقاً من التطور المتسارع في استخدام التقنيات الرقمية داخل المؤسسات الأمنية، وما أتاحه ذلك من إمكانات جديدة في التعامل مع المعلومات والمواقف الأمنية. وهدفت الدراسة إلى بيان مفهوم التحول الرقمي في المجال الأمني ومقوماته، وتحديد دور التقنيات الرقمية في توفير المعلومات ودعم القرار، ثم بحث أثر هذا التحول في سرعة القرار الأمني ودقته، وفي القدرة على التنبؤ بالمخاطر وتعزيز الاستجابة الأمنية. واعتمدت الدراسة على المنهج الوصفي التحليلي من خلال عرض المفاهيم والأدوار الأساسية للتحول الرقمي وتحليل انعكاساته على عملية اتخاذ القرار الأمني. وتوصلت الدراسة إلى أن التحول الرقمي يساهم في تطوير القرار الأمني من خلال تحسين التعامل مع المعلومات، وتقليل الوقت اللازم للوصول إلى القرار، ودعم دقته، فضلاً عن تعزيز القدرة على رصد مؤشرات المخاطر والاستعداد لها. كما خلصت إلى أن نجاح التحول الرقمي لا يتوقف على توافر التقنيات، وإنما يرتبط بجودة البيانات، وتكامل الأنظمة، وكفاءة العنصر البشري، وحماية المعلومات، واستمرار الرقابة البشرية على مخرجات التقنيات الرقمية.

الكلمات المفتاحية: التحول الرقمي، اتخاذ القرار الأمني، التقنيات الرقمية، المعلومات الأمنية، التنبؤ بالمخاطر، الاستجابة الأمنية.

Digital Transformation and Its Impact on Developing the Security Decision-Making System

Omar Ahmad Mohammad Al-Ansari

Legal Researcher in Legal and Criminal Sciences /Qatar

law.mohzheee@gmail.com

Abstract:

This study **examines** Digital Transformation and Its Impact on the Development of the Security Decision-Making System, against the backdrop of the rapid adoption of digital technologies by security institutions and their growing role in processing security-related information and situations. It aims to clarify the concept of digital transformation in the security field and its main components, examine the role of digital technologies in providing information and supporting security decision-making, and assess their impact on the speed and accuracy of security decisions, as well as on the ability to anticipate risks and strengthen security responses. The study adopts a **descriptive-analytical approach** to examine the main dimensions of digital transformation and analyze its implications for the security decision-making process. The findings indicate that digital transformation contributes to the development of security decision-making by improving the collection, processing, and use of information, reducing the time required to reach decisions, and enhancing their accuracy. It also strengthens the ability to identify risk indicators and improve preparedness and response. However, the effectiveness of digital transformation depends not only on the availability of technological solutions, but also on data quality, system integration, human expertise, information security, and continued human oversight of digital outputs.

Keywords: Digital Transformation; Security Decision-Making; Digital Technologies; Security Information; Risk Prediction; Security Response.

المقدمة:

كان التطور المتسارع في تقنيات المعلومات والاتصالات في عصرنا الراهن من الفواعل الأساسية في أبرز التحولات التي تشهدها المؤسسات المعاصرة، بحكم ما أتاحتها هذا التطور من إمكانات متقدمة في جمع البيانات ومعالجتها وتحليلها وتبادلها. ولم يعد التحول الرقمي مقتصرًا على تحويل الإجراءات التقليدية إلى إجراءات إلكترونية، وإنما امتد أثره إلى أساليب العمل المؤسسي، وآليات إدارة المعلومات، وتحديد الأولويات، والتعامل مع المخاطر، وصولاً إلى التأثير في عملية اتخاذ القرار ذاتها. ويكتسب هذا التحول أهمية خاصة في المجال الأمني؛ لأن العمل الأمني يقوم بصورة أساسية على توافر المعلومات الدقيقة في الوقت المناسب، وتحليلها بصورة تسمح بتقدير الموقف واتخاذ القرار الملائم والاستجابة السريعة للتهديدات والمخاطر. وفي هذا السياق، أسهم التحول الرقمي في إحداث تغيير واضح في مصادر المعلومات الأمنية وطرق التعامل معها؛ إذ أتاحت التقنيات الحديثة إمكانية جمع البيانات من مصادر متعددة وربطها وتحليلها بصورة أسرع من الوسائل التقليدية. كما أتاحت استخدام أدوات التحليل الرقمي والأنظمة الذكية إمكانات أوسع في اكتشاف الأنماط والمؤشرات المرتبطة بالتهديدات الأمنية، بما يساعد في توفير معلومات أكثر ملاءمة لاحتياجات صانع القرار. ومن ثم، لم تعد قيمة المعلومات الأمنية مرتبطة بكمها فقط، وإنما أصبحت مرتبطة كذلك بسرعة الوصول إليها، وجودتها، وإمكانية تحليلها والاستفادة منها في الوقت المناسب ومع ذلك، فإن الاستفادة من التحول الرقمي في اتخاذ القرار الأمني لا تتحقق بمجرد إدخال التقنيات الحديثة إلى المؤسسات الأمنية، وإنما تتطلب توافر مجموعة من المقومات التي تضمن جودة المعلومات وإمكانية الاعتماد عليها، فضلاً عن قدرة العاملين على استخدام الأدوات الرقمية وفهم مخرجاتها. كما أن الاعتماد المتزايد على الأنظمة الرقمية يفرض ضرورة التعامل مع التحديات التي قد تؤثر في موثوقية المعلومات أو سلامة الأنظمة أو دقة النتائج التي تقدمها الأدوات الرقمية. ومن ثم، فإن دراسة أثر التحول الرقمي في القرار الأمني ينبغي ألا تقتصر على بيان مزايا التكنولوجيا، وإنما تمتد إلى بحث مدى إسهامها الفعلي في تحسين القرار الأمني وتطوير كفاءته.

تتبع أهمية هذا الموضوع من أن اتخاذ القرار يمثل أحد العناصر الأساسية في العمل الأمني، إذ تتوقف عليه كيفية تحديد الأولويات، وتوزيع الموارد، والتعامل مع المخاطر، واختيار أساليب الاستجابة المناسبة. وكلما ارتفعت جودة القرار الأمني وسرعته ودقته، ازدادت قدرة المؤسسة الأمنية على أداء وظائفها بكفاءة. وفي المقابل، فإن ضعف المعلومات أو تأخرها أو عدم القدرة على تحليلها قد يؤدي إلى اتخاذ قرارات غير ملائمة لطبيعة الموقف الأمني. ومن هنا تبرز أهمية التحول الرقمي باعتباره وسيلة يمكن أن تسهم في تحسين البيئة المعلوماتية التي يستند إليها القرار الأمني.

أهمية البحث: تتحدد أهمية البحث في جانبين رئيسيين:

أولاً: الأهمية العلمية

تتمثل في تناول العلاقة بين التحول الرقمي واتخاذ القرار الأمني، باعتبارها من الموضوعات التي تجمع بين التطور التقني ومتطلبات العمل الأمني. كما يسهم البحث في توضيح الكيفية التي يمكن من خلالها توظيف التقنيات الرقمية في دعم القرار، والتمييز بين مجرد استخدام التكنولوجيا وبين توظيفها بصورة تؤدي إلى تطوير فعلي في عملية اتخاذ القرار.

ثانياً: الأهمية العملية

تتمثل في إمكانية الاستفادة من نتائج البحث في تطوير آليات العمل الأمني، وتحسين سرعة الحصول على المعلومات وتحليلها، وتعزيز دقة التقدير الأمني، ودعم القدرة على التعامل مع المخاطر بصورة أكثر كفاءة واستباقية.

أهداف البحث: يهدف البحث بصفة أساسية إلى بيان أثر التحول الرقمي في تطوير منظومة اتخاذ القرار الأمني، وذلك من خلال تحقيق مجموعة من الأهداف، أهمها:

1. بيان مفهوم التحول الرقمي في المجال الأمني ومقوماته الأساسية.
2. توضيح دور التقنيات الرقمية في توفير المعلومات اللازمة لدعم القرار الأمني.
3. بيان أثر التحول الرقمي في سرعة اتخاذ القرار الأمني ودقته.

4. توضيح مدى إسهام الوسائل الرقمية في تعزيز القدرة على التنبؤ بالمخاطر والاستجابة لها.
5. تحديد أهم الجوانب التي يمكن من خلالها توظيف التحول الرقمي في تطوير منظومة اتخاذ القرار الأمني.

إشكالية البحث وأسئلته:

يفرض التحول الرقمي على المؤسسات الأمنية إعادة النظر في الأساليب التقليدية لجمع المعلومات ومعالجتها والاستفادة منها في اتخاذ القرار، بعد أن أتاحت التقنيات الرقمية إمكانيات واسعة في سرعة الحصول على المعلومات وربطها وتحليلها. غير أن امتلاك هذه التقنيات لا يعني بالضرورة تحقق التطوير في منظومة اتخاذ القرار الأمني، إذ يرتبط ذلك بمدى توافر مقومات التحول الرقمي، وقدرة التقنيات المستخدمة على توفير معلومات دقيقة وملائمة، ومدى انعكاسها فعلياً على سرعة القرار ودقته والقدرة على التنبؤ بالمخاطر والاستجابة لها. ومن ثم، تتمثل إشكالية البحث في التساؤل الرئيس الآتي: **إلى أي مدى يسهم التحول الرقمي في تطوير منظومة اتخاذ القرار الأمني، من خلال دوره في دعم القرار وتحسين سرعته ودقته وتعزيز القدرة على التنبؤ بالمخاطر والاستجابة لها ؟** ويتفرع عن هذا التساؤل تساؤلات فرعية، هي:

1. كيف يُسهم التحول الرقمي في دعم اتخاذ القرار الأمني من خلال مقوماته والتقنيات الرقمية المستخدمة في توفير المعلومات اللازمة لصانع القرار؟
2. ما المقصود بالتحول الرقمي في المجال الأمني، وما أهم مقوماته؟
3. ما دور التقنيات الرقمية في توفير المعلومات ودعم القرار الأمني؟

منهج البحث:

يعتمد البحث على **المنهج الوصفي التحليلي**، من خلال عرض مفهوم التحول الرقمي وبيان أهم عناصره المرتبطة بالعمل الأمني، ثم تحليل دوره في دعم عملية اتخاذ القرار، وبيان أوجه تأثيره في سرعة القرار ودقته والقدرة على التنبؤ بالمخاطر والاستجابة لها. كما

يستفيد البحث من التطبيقات والدراسات المرتبطة بالتحول الرقمي في المجال الأمني؛ بهدف الوصول إلى تصور واضح لطبيعة الأثر الذي يمكن أن يحدثه التحول الرقمي في منظومة اتخاذ القرار الأمني، ويقتضي ذلك التركيز على العلاقة بين الوسائل الرقمية وعملية اتخاذ القرار، دون تحويل البحث إلى دراسة تقنية بحتة؛ إذ تظل الغاية الأساسية هي تحليل أثر هذه الوسائل في كفاءة القرار الأمني، ومدى قدرتها على تحسين المعلومات التي يستند إليها صانع القرار، وتسريع التعامل مع المواقف والمخاطر الأمنية.

الإطار النظري

المطلب الأول: التحول الرقمي ودوره في دعم اتخاذ القرار الأمني:

أصبح التحول الرقمي أحد المرتكزات المهمة لتطوير العمل الأمني، لما يتيح من إمكانيات في جمع المعلومات الأمنية وتخزينها ومعالجتها وتحليلها وتبادلها بسرعة وكفاءة، بما يعزز قدرة المؤسسات الأمنية على بناء قرارات تستند إلى معلومات أكثر دقة وتكاملاً. ولا يقتصر أثر التحول الرقمي على إدخال التقنيات الحديثة في العمل الأمني، وإنما يمتد إلى تطوير الآليات التي يعتمد عليها صانع القرار في فهم الموقف الأمني وتقديره واختيار الاستجابة المناسبة له ومن ثم، يقتضي تحديد أثره في القرار الأمني أولاً بيان المقصود بالتحول الرقمي في المجال الأمني وأهم المقومات التي يقوم عليها، وذلك في الفرع الأول: مفهوم التحول الرقمي في المجال الأمني ومقوماته، ثم بيان كيفية توظيف التقنيات الرقمية في توفير المعلومات اللازمة لصنع القرار، وذلك في الفرع الثاني: دور التقنيات الرقمية في توفير المعلومات ودعم القرار الأمني.

الفرع الأول: مفهوم التحول الرقمي في المجال الأمني ومقوماته:

لم يعد مفهوم التحول الرقمي محصوراً في مجرد استخدام الحاسوب أو تحويل الوثائق الورقية إلى ملفات إلكترونية، بل أصبح يمثل توجهاً أشمل نحو إعادة تنظيم العمل داخل المؤسسات، وتطوير طرق أداء المهام والوصول إلى المعلومات واستثمارها. فالتحول الرقمي يعني توظيف التقنيات الحديثة والبيانات بصورة تتيح تحسين الأساليب القائمة وابتكار وسائل

جديدة لإنجاز الأعمال وتقديم الخدمات. وتعزفه منظمة التعاون الاقتصادي والتنمية بأنه الأثر المترتب على استخدام التقنيات الرقمية والبيانات في الأنشطة الجارية والأنشطة المستحدثة، بما يؤدي إلى تغيير جوهري في طريقة أداء المؤسسات لوظائفها وخدماتها (OECD، 2020) ومن ثم، فإن التحول الرقمي لا يُختزل في الجانب التقني وحده، بل يتصل أساساً بكيفية دمج هذه التقنيات في بيئة العمل لتحقيق نتائج أكثر فاعلية وجودة.

علاوة على ذلك، أصبح التحول الرقمي يكتسب أهمية خاصة في المجال الأمني، إذ يقوم العمل الأمني أساساً على المعلومات وسرعة الحصول عليها ودقة تحليلها. فالجهات الأمنية تواجه باستمرار أحداثاً ووقائع ومخاطر متغيرة، وقد تُضطر في بعض الحالات إلى جمع بيانات من مصادر متعددة خلال فترة زمنية وجيزة، ثم تنظيمها وربطها وتحليلها لتكوين صورة دقيقة عن الموقف. ومن هذا المنطلق، يمكن تعريف التحول الرقمي في المجال الأمني بأنه توظيف التقنيات الرقمية والبيانات في مختلف مراحل العمل الأمني؛ بدءاً من جمع المعلومات وتسجيلها وحفظها، مروراً بربطها وتحليلها وتبادلها بين الجهات المختصة، وصولاً إلى استخدام نتائجها في تقدير الموقف ودعم عملية اتخاذ القرار.

تزداد أهمية البيانات في المجال الأمني نظراً لارتباط القرار الأمني بطبيعة المعلومات المتاحة لدى الجهة المختصة. فقد تشمل هذه البيانات حوادث سابقة، أو بلاغات، أو معلومات ميدانية، أو مؤشرات مرتبطة بمخاطر محددة. وعندما تُحفظ البيانات بطريقة منظمة وقابلة للبحث والربط، يصبح من السهل الاستفادة منها عند دراسة موقف أمني جديد. وقد أكدت منظمة التعاون الاقتصادي والتنمية أن القطاع العام الرقمي يعتمد بشكل متزايد على البيانات باعتبارها أصلاً استراتيجياً يمكن المؤسسات من فهم التغيرات والتنبؤ بالاحتياجات وتحسين الاستجابة لها. (OECD، 2020) وهذا يوضح أن البيانات لم تعد مجرد ناتج للعمل الإداري، بل أصبحت مورداً أساسياً يسهم بصورة مباشرة في رفع كفاءة المؤسسة وتحسين أدائها.

يقوم التحول الرقمي في المجال الأمني على عدد من المقومات التي لا يمكن فصل بعضها عن بعض. ويأتي في مقدمة هذه المقومات البنية التقنية التي توفر الوسائل اللازمة

لجمع البيانات وتخزينها ومعالجتها وربط الأنظمة المختلفة. ولا يكفي أن تمتلك كل جهة أمنية نظاماً إلكترونياً خاصاً بها، إذا كانت هذه الأنظمة تعمل بصورة منفصلة ولا تسمح بتبادل المعلومات عند الحاجة. فالفائدة الحقيقية تظهر عندما تكون الأنظمة قادرة على التواصل وتبادل البيانات وفق ضوابط محددة، بما يساعد الجهات المختصة على الوصول إلى المعلومات التي تحتاج إليها دون تعطيل أو تأخير.

وبالإضافة إلى ما تقدّم، تعدّ قابلية الربط والتكامل بين الأنظمة من الركائز الأساسية في بناء البيئة الرقمية الأمنية. فوجود قواعد بيانات وأنظمة متعددة قد يكون مفيداً، لكن هذه الفائدة تظل محدودة إذا تعذر الوصول إلى البيانات أو تبادلها بين الوحدات والجهات ذات الصلة. ولهذا تؤكد منظمة التعاون الاقتصادي والتنمية على أهمية التكامل والتنسيق وتطوير القدرات اللازمة لدعم التحول الرقمي في القطاع العام. وفي المجال الأمني، يكتسب هذا الجانب أهمية مضاعفة؛ إذ قد تتطلب بعض المواقف جمع معلومات من أكثر من مصدر قبل الوصول إلى تقدير دقيق للموقف ولا يمكن أن ينجح التحول الرقمي من دون كوادرات بشرية مؤهلة. فوجود الأنظمة والبرامج لا يكفي إذا كان العاملون لا يمتلكون القدرة على استخدامها أو فهم النتائج التي تقدمها. كما أن التعامل مع البيانات الأمنية يتطلب قدرًا من المعرفة بطريقة إدخال المعلومات واسترجاعها وتحليلها، إلى جانب القدرة على التعامل مع المشكلات التي قد تظهر أثناء استخدام الأنظمة الرقمية. ولذلك تؤكد منظمة التعاون الاقتصادي والتنمية أهمية المهارات والقدرات البشرية إلى جانب الأدوات التقنية والأطر التنظيمية والقانونية عند تنفيذ التحول الرقمي في المؤسسات العامة. (OECD، 2020) ومن المقومات الأساسية للتحول الرقمي أيضاً الأمن الرقمي وحماية المعلومات. فكلما زاد اعتماد المؤسسة الأمنية على الأنظمة الإلكترونية، أصبحت حماية هذه الأنظمة والبيانات الموجودة فيها مسألة أكثر أهمية. وقد تتعرض المعلومات لمحاولات اختراق أو تغيير أو حذف أو وصول غير مصرح به، وهو ما قد يؤثر في سلامة العمل الأمني وفي الثقة بالمعلومات التي يعتمد عليها القرار. ولذلك لا يمكن الفصل بين التحول الرقمي وحماية الأنظمة

والبيانات، بل يجب أن تكون الحماية جزءاً من عملية التحول منذ مرحلة تصميم النظام واستخدامه. (OECD، 2020)

وفي هذا السياق، يؤكد إطار المعهد الوطني الأمريكي للمعايير والتكنولوجيا للأمن السيبراني (NIST) أهمية التعامل مع المخاطر الرقمية من خلال منظومة تشمل الحوكمة وتحديد المخاطر والحماية والكشف والاستجابة والتعافي. (Rigopoulos، 2024) ويعني ذلك أن حماية المعلومات لا تقتصر على منع الاختراق فقط، وإنما تشمل كذلك اكتشاف المخاطر والتعامل معها والحد من آثارها واستعادة القدرة على العمل عند وقوع حادث أمني. وهذا الأمر له أهمية خاصة في المؤسسات الأمنية؛ لأن توقف نظام معلومات أو فقدان بيانات مهمة قد يؤثر بصورة مباشرة في القدرة على التعامل مع الموقف ومن هذا المنطلق، فإن القيمة الأساسية للتحول الرقمي في المجال الأمني تظهر في قدرته على تحسين تدفق المعلومات ودعم تقدير الموقف ومساعدة متخذ القرار على التعامل مع المخاطر في الوقت المناسب. فكلما كانت المعلومات أكثر دقة وتنظيماً وسهولة في الوصول والتحليل، أصبح القرار الأمني قائماً على أساس أفضل. ومن هنا تبرز العلاقة المباشرة بين التحول الرقمي وتطوير منظومة اتخاذ القرار الأمني، وهي العلاقة التي تمثل مدخلاً أساسياً لبحث دور التقنيات الرقمية في توفير المعلومات وتحليلها ودعم القرار الأمني. (منظمة التعاون الاقتصادي والتنمية، 2015).

الفرع الثاني: دور التقنيات الرقمية في توفير المعلومات ودعم القرار الأمني:

أصبحت المعلومات من العناصر الأساسية التي يقوم عليها العمل الأمني، لأن سلامة القرار الأمني ترتبط إلى حد كبير بمدى توافر المعلومات اللازمة عن الموضوع محل الدراسة، ومدى دقتها وحدائتها وإمكانية الوصول إليها في الوقت المناسب. فالمسؤول الأمني لا يستطيع تقدير موقف معين بصورة سليمة إذا كانت المعلومات المتاحة أمامه ناقصة أو متفرقة أو يصعب التحقق منها، ولذلك لم يعد جمع المعلومات وحفظها أمراً منفصلاً عن عملية اتخاذ القرار، وإنما أصبح جزءاً من مراحل العمل التي تسبق القرار وتساعد على تكوين الأساس الذي يقوم عليه. (منظمة التعاون الاقتصادي والتنمية، 2015)، (الطماوي

(1998). والأمر الملاحظ، أنه مع تطور التقنيات الرقمية تغيرت بصورة جذرية الطريقة التي تُدار بها المعلومات الأمنية. فلم تعد البيانات تجمع وتُحفظ في ملفات وسجلات منفصلة كما كان الحال في الأساليب التقليدية، بل أصبحت تُدمج في أنظمة رقمية متقدمة تتيح تخزينها وتنظيمها والبحث فيها وربط عناصرها وتحليلها عند الحاجة. وهذا التحول لا يعني أن التقنية أصبحت بديلاً عن المسؤول الأمني، وإنما غدت أداة داعمة تمكنه من الوصول إلى المعلومات بسرعة أكبر وبصورة أكثر تنظيماً، مما يوفر له أساساً أكثر متانة عند دراسة الموقف واتخاذ القرار المناسب. (Möller، 2023)

ومن هذا المنطلق، يمكن القول إن دور التقنيات الرقمية في دعم القرار الأمني يبدأ قبل لحظة اتخاذ القرار نفسها، وذلك من خلال تهيئة المعلومات التي يحتاج إليها صانع القرار. فكلما كانت المعلومات منظمة ومتاحة وقابلة للتحليل، أصبح من الأسهل على المسؤول فهم الموقف وتحديد عناصره الأساسية. أما إذا كانت المعلومات موزعة بين مصادر مختلفة أو محفوظة بطريقة يصعب الوصول إليها، فإن ذلك قد يؤدي إلى تأخير القرار أو الاعتماد على معلومات غير مكتملة. (OECD ، 2019)

وتبدأ هذه العملية من جمع المعلومات من مصادر متعددة. فقد تحتاج الجهات الأمنية إلى التعامل مع معلومات ميدانية، وبيانات واردة من الجهات المختصة، وسجلات سابقة، وبلاغات، وتقارير، وغيرها من المصادر التي تختلف طبيعتها بحسب الموضوع محل الدراسة. وتساعد التقنيات الرقمية على إدخال هذه المعلومات في أنظمة يمكن حفظها وتنظيمها والرجوع إليها عند الحاجة. كما تتيح إمكانية التعامل مع حجم أكبر من البيانات مقارنة بالوسائل التقليدية، وهو أمر مهم في ظل تزايد كمية المعلومات التي ترتبط بالعمل الأمني. (OECD ، 2019)

وتزداد أهمية ذلك بسبب أن المعلومة الأمنية قد تتعلق بشخص أو مكان أو واقعة أو نشاط أو سلوك أو حادث معين، وقد تكون مرتبطة بمعلومات أخرى لا تظهر أهميتها عند النظر إليها بصورة منفردة. لذلك فإن جمع المعلومات داخل بيئة رقمية منظمة يساعد على الاحتفاظ بها وإمكانية الرجوع إليها في مراحل لاحقة، كما يسهل مقارنتها بالمعلومات الجديدة

التي تصل إلى الجهة الأمنية. وقد اتجهت بعض الدراسات الأمنية العربية إلى بحث رقمنة دعم اتخاذ القرار باعتبارها جزءاً من برامج التحول الرقمي في الخدمات والأعمال الأمنية. (الخريجي، 2022).

ولا تقتصر وظيفة التقنيات الرقمية على جمع المعلومات فحسب، بل تمتد لتشمل تنظيمها وتصنيفها بما يضمن الاستفادة القصوى منها. فالمعلومات التي تصل إلى الجهة الأمنية غالباً ما تكون كثيرة ومتنوعة، وقد تأتي في صور مختلفة، مما يجعل قيمتها محدودة إذا لم تُرتب وفق معايير واضحة تسمح بالوصول إليها واستخدامها عند الحاجة. وهنا تبرز أهمية قواعد البيانات والأنظمة الرقمية التي توفر آليات متقدمة لتصنيف المعلومات بحسب موضوعاتها ومصادرها وتواريخها، وربط العناصر ذات الصلة ببعضها البعض. إن هذا التنظيم لا يسهل عملية البحث والاسترجاع فحسب، بل يرفع أيضاً من جودة التحليل الأمني، ويمنح المسؤول أساساً أكثر دقة وموثوقية عند تقدير الموقف واتخاذ القرار المناسب. (OECD، 2019)

وتظهر أهمية التنظيم في أن صانع القرار لا يحتاج عادة إلى جميع البيانات الموجودة في النظام، وإنما يحتاج إلى المعلومات المرتبطة بالموقف الذي يتعامل معه. ولذلك فإن تنظيم المعلومات يساعد على الوصول إلى البيانات المطلوبة دون إضاعة وقت طويل في البحث بين معلومات لا ترتبط بالموضوع. كما أن التصنيف الجيد يسهل تحديث البيانات وتصحيحها، ويقلل من احتمال الاعتماد على معلومات قديمة أو غير مرتبطة بالموقف محل الدراسة. (OECD، 2019)

كما تؤدي التقنيات الرقمية دوراً مهماً في ربط المعلومات بين الأنظمة والجهات المختصة، وذلك في حدود الصلاحيات والإجراءات القانونية والتنظيمية المعتمدة، فقد تكون بعض المعلومات موجودة لدى جهة معينة، بينما توجد معلومات أخرى مرتبطة بها لدى جهة مختلفة. وفي هذه الحالة قد لا تظهر الصورة الكاملة إلا بعد جمع المعلومات ذات الصلة ومقارنتها. ويساعد التكامل بين الأنظمة الرقمية على الحد من بقاء المعلومات في قواعد منفصلة، ويجعل الوصول إليها والاستفادة منها أكثر سهولة.

ولا يعني تبادل المعلومات بين الجهات أن يكون الوصول إليها مفتوحاً دون ضوابط، وإنما يجب أن يتم وفق قواعد تحدد من يملك صلاحية الاطلاع عليها واستخدامها، وبما يضمن حماية المعلومات الأمنية. فالغرض من الربط بين الأنظمة هو تحسين العمل وتوفير المعلومات للجهة التي تحتاج إليها، وليس التوسع غير المنضبط في تداولها. وتعد هذه المسألة من الجوانب المهمة في رقمنة دعم اتخاذ القرار؛ لأن الهدف من الرقمنة لا يقتصر على تحويل المعلومات إلى صورة إلكترونية، وإنما يتصل بقدرتها على الانتقال داخل منظومة العمل واستخدامها في الوقت المناسب.

وتفيد هذه الإمكانيات في مساعدة المسؤول الأمني على الوصول إلى المعلومات ذات الصلة، واكتشاف بعض الأنماط أو العلاقات التي قد لا تكون واضحة عند التعامل مع كل معلومة بصورة منفردة. ومع ذلك، فإن استخدام الأنظمة الرقمية في التحليل لا يعني أن نتائجها تكون صحيحة في جميع الحالات، إذ تظل جودة النتائج مرتبطة بدقة البيانات التي تدخل إلى النظام، وبطريقة تصميم النظام والآليات التي يعتمد عليها في معالجة المعلومات. ولهذا فإن نتائج التحليل الرقمي تحتاج إلى قراءة ومراجعة قبل الاعتماد عليها في اتخاذ القرار. (Möller, 2014)

وفي هذا الإطار، برزت تطبيقات الذكاء الاصطناعي باعتبارها من الأدوات الحديثة التي يمكن الاستفادة منها في التعامل مع البيانات والمعلومات الأمنية. وتسمح بعض تطبيقاتها بمعالجة كميات كبيرة من البيانات واستخلاص مؤشرات أو أنماط قد تساعد في فهم موضوع معين. وقد تناولت جامعة نايف العربية للعلوم الأمنية تطبيقات الذكاء الاصطناعي في المجالات الأمنية والعسكرية، وأشارت إلى استخداماته في جمع المعلومات وتحليلها وفي عدد من الوظائف المرتبطة بالعمل الأمني. (الخريجي ويوسف، 2022)

وتكمن أهمية الذكاء الاصطناعي في هذا المجال في قدرته على مساعدة العاملين في التعامل مع حجم كبير من المعلومات خلال وقت قصير، إلا أن ذلك لا يعني الاعتماد عليه بصورة مطلقة. فالمعلومات الأمنية تحتاج إلى التحقق من مصدرها وسلامتها، كما أن نتائج الأنظمة الذكية تتأثر بالبيانات التي تعتمد عليها. وإذا كانت البيانات ناقصة أو غير دقيقة،

فقد تنعكس هذه المشكلات على النتائج التي يقدمها النظام. لذلك تظل المراجعة البشرية ضرورية، خاصة عندما تكون النتائج مرتبطة بقرار أمني له آثار مهمة. وتؤدي التقنيات الرقمية كذلك دوراً في عرض المعلومات أمام صانع القرار. فبعد جمع المعلومات وتنظيمها وتحليلها، تبرز الحاجة إلى تقديمها بطريقة واضحة تساعد المسؤول على فهمها، ويمكن عرض المعلومات في شكل تقارير إلكترونية أو قواعد بيانات أو لوحات معلومات أو خرائط وصور رقمية، بحسب طبيعة الموضوع والهدف من استخدامها. ولا تكمن أهمية هذه الوسائل في شكل العرض فقط، وإنما في قدرتها على ترتيب المعلومات وإظهار العناصر المهمة أمام المسؤول بصورة تسهل قراءتها ومقارنتها. (OECD، 2019) فبدل أن يواجه صانع القرار عددًا كبيرًا من البيانات غير المرتبة، يمكن للنظام الرقمي أن يساعد في تقديم المعلومات ذات الصلة بالموقف في صورة أكثر وضوحًا. وقد يسمح ذلك بمقارنة المعلومات الحالية بالمعلومات السابقة، أو متابعة تطور موقف معين، أو تحديد بعض المؤشرات التي تستدعي الانتباه. وبذلك تتحول المعلومات من مجرد بيانات محفوظة داخل النظام إلى مادة يمكن الاستفادة منها عند تقدير الموقف ويجب في هذا السياق التمييز بين توفير المعلومات ودعم القرار من جهة، واتخاذ القرار من جهة أخرى. فالتقنيات الرقمية تستطيع جمع البيانات وتنظيمها وربطها وتحليلها وعرض نتائجها، لكنها لا تتحمل المسؤولية عن القرار الأمني في ذاته. فالقرار يظل من اختصاص الشخص أو الجهة التي منحها القانون أو التنظيم سلطة اتخاذها، وهي التي تقوم بتقدير الموقف والموازنة بين المعلومات المتاحة والاعتبارات الأمنية والقانونية والعملية. (Möller, 2023)، ويكتسب هذا التمييز أهمية خاصة في العمل الأمني؛ لأن القرار قد يتطلب مراعاة ظروف لا يمكن للنظام الرقمي أن يقدرها بصورة كاملة، فقد تكون هناك اعتبارات ميدانية أو قانونية أو إنسانية أو عملية لا تظهر بصورة واضحة في البيانات الموجودة داخل النظام. ومن ثم، فإن استخدام التقنية يجب أن يكون في إطار دعم المسؤول الأمني وليس إلغاء دوره. وكلما كانت المعلومات التي توفرها التقنية أكثر دقة وتنظيمًا، كان بإمكان المسؤول أن يستفيد منها بصورة أفضل عند ممارسة اختصاصه. كما أن سرعة الوصول إلى المعلومات تعد من أهم الجوانب التي تظهر فيها قيمة التقنيات

الرقمية. ففي بعض المواقف الأمنية، قد يكون الوقت عنصرًا مؤثرًا في القرار، وقد يؤدي التأخر في الوصول إلى معلومة مهمة إلى تقليل القدرة على التعامل مع الخطر، وتساعد الأنظمة الرقمية على تقليل الوقت اللازم للبحث عن المعلومات واسترجاعها ومقارنتها، وهو ما يمكن أن ينعكس على سرعة الاستجابة للمواقف الأمنية. غير أن السرعة لا ينبغي أن تكون على حساب الدقة، لأن القرار السريع القائم على معلومات غير صحيحة قد يؤدي إلى نتائج غير مسبوقة (OECD، 2019)، يمكن اعتبار توفير المعلومات وتحسين طريقة التعامل معها من أهم صور إسهام التحول الرقمي في تطوير العمل الأمني. فالتقنية تساعد على جعل المعلومة أسرع وصولاً، وأكثر تنظيماً، وأسهل في التحليل والعرض، بينما يبقى تقدير الموقف واتخاذ القرار من اختصاص الإنسان المسؤول. ومن هنا يمهّد هذا الدور لدراسة الآثار المباشرة للتحول الرقمي على منظومة اتخاذ القرار الأمني، وبخاصة ما يتعلق بسرعة القرار ودقته، وتحسين القدرة على مواجهة المخاطر، وهي المسائل التي يتناولها المطلب الثاني.

المطلب الثاني:

أثر التحول الرقمي في تطوير منظومة اتخاذ القرار الأمني:

لا تقتصر أهمية التحول الرقمي في المجال الأمني على توفير المعلومات وتنظيمها وتحليلها، وإنما تظهر قيمته بصورة أوضح في مدى انعكاس هذه الإمكانيات على جودة القرار الأمني وفاعليته

فكلما أمكن الاستفادة من المعلومات الرقمية بصورة أفضل، ازدادت قدرة المؤسسة الأمنية على التعامل مع المواقف المختلفة واتخاذ القرارات المناسبة في الوقت الملائم. ولا يقاس هذا الأثر بمجرد استخدام التقنيات الحديثة، وإنما بما تحدثه فعلياً من تحسين في أداء منظومة اتخاذ القرار؛ سواء من جهة سرعة الوصول إلى القرار ودقته، أو من حيث القدرة على استشراف المخاطر والتعامل معها بصورة أكثر استعداداً. ومن ثم، يتناول الفرع الأول: أثر التحول الرقمي في سرعة ودقة القرار الأمني

لبيان مدى إسهام التقنيات الرقمية في تحسين القرار من حيث الوقت والدقة، ثم يتناول الفرع الثاني: أثر التحول الرقمي في التنبؤ بالمخاطر وتعزيز الاستجابة الأمنية؛ لبيان دور هذه التقنيات في الانتقال من التعامل مع الخطر بعد وقوعه إلى الاستعداد له والتعامل معه بصورة أكثر فاعلية. كما هو مبين في الأسفل.

1- الفرع الأول: أثر التحول الرقمي في سرعة ودقة القرار الأمني:

يُقاس نجاح القرار الأمني بمدى قدرة الجهة المختصة على التعامل مع الموقف في الوقت المناسب، وبمدى استناده إلى معلومات صحيحة ومرتبطة بالموضوع الذي صدر بشأنه القرار. فالقرار الأمني لا يعتمد فقط على سلطة الشخص الذي يُصدره، وإنما يحتاج كذلك إلى معلومات تساعده على فهم الموقف وتحديد ما يقتضيه من إجراءات. وكلما كانت المعلومات متاحة في الوقت المناسب، ومنظمة وقابلة للتحقق، أصبح من الأسهل على المسؤول الأمني تقدير الموقف واختيار الإجراء المناسب.

ولا مرأى من القول، إنّ التحول الرقمي الذي نعيشه في الوقت الراهن أثر تأثيراً واضحاً في البيئة التي يُتخذ فيها القرار الأمني؛ حيث لم يعد المسؤول يعتمد بالدرجة نفسها على الإجراءات الورقية أو على انتقال المعلومات عبر القنوات التقليدية، بل أصبح يعمل في إطار مؤسسي يسمح بتداول البيانات والنتائج بين المستويات المختصة بسرعة أكبر وبصورة أكثر تنظيماً. وقد بينت الدراسات المعنية برقمنة دعم اتخاذ القرار أن إدماج التقنيات الرقمية في بنية العمل المؤسسي لا يُعدّ مجرد إضافة تقنية، وإنما يمثل إعادة صياغة لآليات القرار؛ بحيث تصبح هذه التقنيات جزءاً من العملية ذاتها، وليست أدوات منفصلة تُستخدم إلى جانب الإجراءات التقليدية. (الخريجي، 2022) بالإضافة إلى ذلك، تظهر إحدى النتائج المباشرة للتحول الرقمي في المجال الأمني في **تقليص الوقت اللازم للوصول إلى القرار**. فالأنظمة الرقمية ساعدت على اختصار العديد من الخطوات التي كانت تستغرق وقتاً أطول في الأساليب التقليدية، خاصة عندما يتطلب الموقف الرجوع إلى أكثر من مصدر أو جهة. كما أن انتقال المعلومات إلكترونياً بين المستويات المختصة يقلل من الفاصل الزمني بين ظهور الموقف الأمني ووصول البيانات إلى المسؤول المعني، مما يتيح إمكانية البحث

والاسترجاع والمراجعة دون الحاجة إلى انتظار انتقال الملفات أو المراسلات الورقية. ومع ذلك، فإن قيمة هذه السرعة تظل مشروطة بالدقة، إذ إن القرار السريع القائم على معلومات غير صحيحة قد يقود إلى نتائج غير مناسبة. (OECD، 2019) وتزداد أهمية عامل الوقت في العمل الأمني بسبب طبيعة بعض المواقف التي تتغير بصورة سريعة. فقد تتغير الظروف خلال فترة قصيرة، وقد تظهر معلومات جديدة تؤثر في تقدير الموقف، ولذلك فإن تأخر المعلومة قد يؤثر في قيمة القرار حتى لو كانت المعلومة نفسها صحيحة، ومن هنا يساعد التحول الرقمي على جعل القرار أقرب زمنياً إلى الواقعة التي يتعامل معها، ويمنح المسؤول فرصة أفضل للاستجابة للموقف قبل أن تتغير عناصره الأساسية.

وقد أكدت منظمة التعاون الاقتصادي والتنمية أن ربط البيانات والأنظمة وتحديث الإجراءات الرقمية يمكن أن يساهم في جعل المؤسسات الحكومية أكثر سرعة وقدرة على الاستجابة، مع المحافظة على جودة العمل والمساءلة. (OECD، 2026) ويعني ذلك، أن السرعة المطلوبة في القرار الأمني ليست هدفاً مستقلاً عن الجودة، وإنما ينبغي أن تتحقق السرعة مع المحافظة على سلامة المعلومات والإجراءات التي يقوم عليها القرار أما الأثر الثاني للتحول الرقمي فيتعلق بدقة القرار الأمني فالقرار الدقيق لا يتوقف على كثرة المعلومات المتاحة، وإنما يرتبط بمدى صلتها بالموضوع محل القرار، وحدائتها، وإمكان التحقق من مصدرها. وقد يكون لدى المسؤول عدد كبير من البيانات، ولكنها لا تساعده في اتخاذ القرار إذا كانت قديمة أو غير منظمة أو لا تتعلق بالموقف الذي يدرسه، ولذلك فإن القيمة الحقيقية للتحول الرقمي تظهر في قدرته على تحسين نوعية المعلومات التي تصل إلى المسؤول وطريقة عرضها أمامه وتساعد الأنظمة الرقمية في هذا الجانب من خلال توفير البيانات ذات الصلة بصورة أكثر تنظيماً، وإتاحة إمكانية البحث والمقارنة والرجوع إلى المعلومات السابقة قبل اعتمادها. كما تسمح هذه الأنظمة بتحديث البيانات بصورة مستمرة، وإضافة المعلومات الجديدة إلى السجلات القائمة، وهو ما يقلل من احتمال الاعتماد على معلومات قديمة لم تعد تعكس الوضع الأمني القائم غير أن الاستفادة من هذه القدرات تظل مرتبطة بجودة البيانات التي يعتمد عليها النظام وبسلامة طريقة استخدامه. فإذا كانت

البيانات ناقصة أو غير دقيقة، فإن النتائج التي يقدمها النظام قد تتأثر بذلك. ولذلك لا يمكن التعامل مع المخرجات الرقمية باعتبارها صحيحة بصورة مطلقة، وإنما يجب أن تخضع للمراجعة والتقييم من جانب المسؤول المختص. وتؤكد منظمة التعاون الاقتصادي والتنمية أن استخدام البيانات في القطاع العام يمكن أن يساعد على اتخاذ قرارات قائمة على أدلة أفضل، مع ضرورة وجود أطر مناسبة لحوكمة البيانات تضمن جودتها وأمنها وإمكان الاعتماد عليها (OECD,N,D) وتبرز أهمية ذلك بصورة أكبر في القرارات الأمنية التي تتعامل مع معلومات متغيرة ففي هذه الحالات لا تكفي صحة المعلومة في وقت سابق، وإنما يجب أن تكون المعلومات المستخدمة في القرار قريبة قدر الإمكان من الوضع القائم وقت اتخاذه، فالمعلومات الأمنية ليست ثابتة دائماً، وقد تظهر بيانات جديدة تؤثر في فهم الموقف أو تغير تقدير درجة الخطر.

ويساعد التحول الرقمي على متابعة هذه التغيرات من خلال تحديث قواعد البيانات وإضافة المعلومات الجديدة بصورة أسرع، مما يسمح للمسؤول بمراجعة تقديره للموقف عندما تظهر معطيات جديدة. وبذلك يصبح القرار الأمني أكثر ارتباطاً بالواقع المتغير، ولا يبقى قائماً على معلومات تم جمعها في وقت سابق دون مراجعة مدى استمرار صلاحيتها كما يسهم التحول الرقمي في تحسين الاتساق بين مستويات القرار الأمني فعندما تعمل الوحدات والجهات المختلفة داخل بيئة رقمية مترابطة، يمكن للمستويات الإدارية المختلفة أن تعتمد على معلومات مشتركة ومحدثة بدل أن يعمل كل مستوى اعتماداً على مجموعة مختلفة من البيانات. وهذا الأمر يقلل من احتمال وجود اختلاف في المعلومات بين المستويات المختلفة، ويساعد على جعل القرارات المتعاقبة أكثر ارتباطاً ببعضها ببعض وتشير إحدى الدراسات حول رقمنة دعم اتخاذ القرار إلى أهمية بناء مستودعات رقمية موحدة وربط الجهات المشاركة، بما يخدم عمليات اتخاذ القرار في المستويات التشغيلية والإدارية والتنظيمية والاستراتيجية. (الخريجي، 2022) وتظهر أهمية ذلك في أن القرار الأمني قد يبدأ من مستوى ميداني، ثم ينتقل إلى مستويات إدارية أعلى، وقد يحتاج كل مستوى إلى المعلومات نفسها مع إضافة ما يخص اختصاصه من تقدير وتحليل.

(OECD، 2020) ومع ذلك، لا ينبغي النظر إلى التحول الرقمي باعتباره ضماناً تلقائياً لسرعة القرار ودقته. فقد يؤدي النظام الرقمي إلى نتائج عكسية إذا كانت البيانات غير صحيحة، أو كانت الأنظمة غير مترابطة، أو لم يمتلك العاملون المهارات اللازمة لاستخدامها. كما أن كثرة البيانات لا تعني بالضرورة جودة القرار، لأن وجود معلومات كثيرة دون تنظيم أو تحليل مناسب قد يصعب على المسؤول تحديد المعلومات المهمة من بين المعلومات الأقل أهمية وقد تظهر مشكلة أخرى عندما يكون الاعتماد على المخرجات التقنية أكبر من اللازم. فالنظام الرقمي يقدم نتائج بناءً على البيانات التي تدخل إليه والآليات التي يعمل بها، ولذلك لا ينبغي التعامل مع نتائجه باعتبارها حقيقة نهائية لا تحتاج إلى مراجعة. وتظل الخبرة البشرية ضرورية لفهم الظروف المحيطة بالموقف، والتحقق من المعلومات، وتحديد مدى ملاءمة النتائج للحالة التي يتعين اتخاذ القرار بشأنها. ولهذا تؤكد الأدبيات الدولية الحديثة أن التحول الرقمي الفعال يحتاج إلى جانب التكنولوجيا إلى حوكمة جيدة للبيانات، وكفاءات بشرية، وأطر تنظيمية، وآليات لقياس النتائج (OECD، 2026).

كما أن سرعة القرار لا تعني دائماً أن القرار الأفضل هو القرار الأسرع، فقد تتطلب بعض القرارات الأمنية قدراً من الوقت للتحقق من المعلومات ومراجعة البدائل المتاحة. ولذلك فإن القيمة التي يضيفها التحول الرقمي تتمثل في تقليل الوقت غير الضروري، وليس في إلغاء الوقت اللازم للتفكير والتقدير والتحقق. وهذه نقطة مهمة حتى لا تتحول الرغبة في سرعة القرار إلى سبب في إضعاف دقته. وعليه، يمكن القول إن التحول الرقمي يسهم في تطوير القرار الأمني من خلال تقليل التأخير، وتحسين جودة المعلومات، وتسهيل تحديثها، والحد من بعض الأخطاء، وتحسين التنسيق بين مستويات العمل الأمني. غير أن هذه المزايا لا تتحقق بصورة تلقائية، وإنما تحتاج إلى أنظمة مترابطة، وبيانات موثوقة، وعاملين مؤهلين، وضوابط واضحة لاستخدام التقنية. وفي جميع الأحوال، يبقى المسؤول الأمني هو صاحب الدور الأساسي في تقدير الموقف واختيار الإجراء المناسب، بينما تؤدي التقنيات الرقمية دوراً مساعداً يوفر له المعلومات والأدوات التي تمكنه من أداء هذه المهمة بصورة أفضل.

2- الفرع الثاني: أثر التحول الرقمي في التنبؤ بالمخاطر وتعزيز الاستجابة الأمنية :

لا يقتصر أثر التحول الرقمي في المجال الأمني على التعامل مع الخطر بعد وقوعه، وإنما يمتد إلى محاولة التعرف عليه قبل تحوله إلى واقعة فعلية، من خلال الاستفادة من البيانات المتاحة وتحليلها للكشف عن المؤشرات التي قد تدل على احتمال وقوع خطر أمني. وبذلك أصبح العمل الأمني أكثر قدرة على الانتقال من رد الفعل إلى الاستعداد المبكر، خاصة في الحالات التي تترك فيها المخاطر مؤشرات يمكن ملاحظتها من خلال تحليل البيانات والمعلومات المتوفرة.. (OECD، 2019) وتقوم فكرة التنبؤ بالمخاطر الأمنية على جمع البيانات السابقة والبيانات المتاحة في الوقت الحاضر، ثم تحليلها لاستخلاص أنماط أو مؤشرات يمكن أن تساعد في تقدير احتمال وقوع حدث أمني في المستقبل. وقد ساهم تطور تقنيات الذكاء الاصطناعي والتحليل الرقمي في زيادة قدرة الأجهزة الأمنية على التعامل مع كميات كبيرة من البيانات، وربط المعلومات القادمة من مصادر مختلفة، وهو ما يصعب تحقيقه بالوسائل التقليدية في الوقت نفسه وبالمسرة ذاتها. (OECD، 2019) وتظهر أهمية ذلك بصورة خاصة عندما تكون البيانات موزعة بين أكثر من مصدر، كبيانات البلاغات الأمنية، وسجلات الحوادث، وبيانات المراقبة، والمعلومات الميدانية وغيرها. فربط هذه البيانات وتحليلها قد يكشف علاقات أو أنماطاً لا تظهر عند النظر إلى كل مجموعة من البيانات بصورة منفصلة. ومن هنا يمكن للتقنيات الرقمية أن تساعد في تحديد بعض الأماكن أو الأوقات التي قد ترتفع فيها احتمالات وقوع أنشطة إجرامية أو مخاطر أمنية معينة.. (OECD، 2025)

ولا يعني التنبؤ الأمني أن النظام يستطيع معرفة ما سيقع بصورة مؤكدة، وإنما يقدم تقديراً احتمالياً يقوم على البيانات المتاحة والأنماط التي ظهرت في الماضي أو في الوقت الحاضر. ولذلك يجب التعامل مع نتائج التحليل التنبؤي باعتبارها مؤشرات تساعد متخذ القرار، وليست حقائق نهائية يجب التعامل معها باعتبارها أمراً محققاً، وتزداد أهمية هذا الأمر لأن التنبؤ الذي يعتمد على بيانات تاريخية قد يتأثر بجودة هذه البيانات ومدى اكتمالها ومدى صلاحيتها لتمثيل الظروف الحالية. (كامل، 2025) ودراسة (عضيبات ،

2023) وقد أصبح استخدام الذكاء الاصطناعي في المجالات الأمنية من الموضوعات التي تحظى باهتمام متزايد، لما توفره تطبيقاته من إمكانيات في تحليل البيانات ومتابعة الأنماط ورصد المؤشرات المرتبطة بالجرائم والمخاطر الأمنية (أبو منصور، 2023) وتبرز أهمية هذه التطبيقات في قدرتها على التعامل مع حجم كبير من المعلومات خلال فترة قصيرة، بما يساعد الجهات الأمنية على تكوين صورة أكثر وضوحاً عن الموقف واتخاذ الإجراءات المناسبة في الوقت الملائم. (OECD، 2025)

ولا تقتصر قيمة التنبؤ بالمخاطر على معرفة احتمال وقوع الخطر، بل تمتد إلى الاستعداد له. فإذا أظهرت البيانات وجود مؤشرات تستدعي الانتباه في منطقة أو وقت معين، أمكن للجهة الأمنية إعادة توزيع بعض مواردها، أو زيادة وجودها الميداني، أو تعزيز المراقبة، أو اتخاذ إجراءات وقائية قبل تفاقم الوضع. وبذلك يصبح القرار الأمني قائماً بدرجة أكبر على تقدير مسبق للمخاطر، وليس فقط على التعامل معها بعد وقوعها.. (OECD، 2019)

كما تساعد البيانات الآنية في تحسين هذا النوع من القرارات، لأن الوضع الأمني قد يتغير بسرعة، وقد تصبح المعلومات التي كان القرار قائماً عليها غير كافية بعد فترة قصيرة. ولذلك فإن الاستفادة من تقارير الحوادث، وبيانات المراقبة، وأجهزة الاستشعار، وغيرها من مصادر البيانات بصورة مستمرة، تسمح بتحديث التقديرات والتوصيات وفقاً للتغيرات التي تحدث على أرض الواقع. وهذا الأمر يساعد على جعل الاستجابة الأمنية أكثر مرونة وقدرة على التكيف مع تطور الموقف. (OECD، 2025)

ويظهر أثر ذلك كذلك في توجيه الموارد الأمنية إلى الأماكن أو الحالات التي تحتاج إليها بدرجة أكبر. فبدلاً من توزيع الموارد بصورة ثابتة، يمكن استخدام نتائج تحليل البيانات في تحديد الأولويات، وتوجيه الدوريات، وتحديد المناطق التي تحتاج إلى مزيد من المتابعة، بما يساعد على تحقيق استخدام أفضل للإمكانيات المتاحة. غير أن ذلك لا يعني أن التنبؤ الرقمي يحل محل التقدير الأمني، وإنما يوفر للجهة المختصة معلومات إضافية تساعد في تحديد كيفية التصرف.. (OECD، 2019)

ومع ذلك، فإن الاعتماد على التقنيات الرقمية في التنبؤ بالمخاطر يثير بعض المسائل التي ينبغي عدم إغفالها. فنتائج التحليل لا تكون أفضل من البيانات التي يعتمد عليها النظام؛ فإذا كانت البيانات ناقصة أو غير دقيقة أو متحيزة، فقد تؤدي النتائج إلى تقديرات غير سليمة. كما أن الاعتماد المفرط على مخرجات النظام قد يؤدي إلى التعامل مع التوقع باعتباره حقيقة مؤكدة، وهو ما قد يؤثر في سلامة القرار الأمني. ولذلك تؤكد الأدبيات الحديثة أهمية اختبار الأنظمة الرقمية والتحقق من نتائجها، مع الإبقاء على الرقابة والتقدير البشري في عملية اتخاذ القرار. (OECD، 2025)

ومن ثم، فإن القيمة الحقيقية للتحويل الرقمي لا تتمثل في القدرة على التنبؤ بالمخاطر بصورة يقينية، وإنما في تحسين قدرة الأجهزة الأمنية على اكتشاف المؤشرات المبكرة، وتحليلها، وتقدير مستوى الخطر، ثم الاستعداد له واتخاذ الإجراءات المناسبة في الوقت الملائم. ويؤدي ذلك إلى تعزيز الجانب الوقائي في العمل الأمني، ويمنح متخذ القرار أساساً معلوماتياً أفضل عند تحديد الأولويات وتوزيع الموارد واختيار أسلوب الاستجابة. وبذلك يمكن القول إن التحويل الرقمي ساهم في تطوير مفهوم الاستجابة الأمنية، فلم تعد الاستجابة مرتبطة فقط بوقوع الحادث، وإنما أصبحت تبدأ في مرحلة سابقة من خلال رصد المؤشرات وتحليل البيانات وتقدير المخاطر المحتملة. ومع ذلك، تبقى هذه التقنيات وسيلة لدعم القرار الأمني وليست بديلاً عن المسؤول البشري، لأن القرار النهائي يظل بحاجة إلى تقدير الظروف المحيطة بالواقعة ومراعاة الجوانب القانونية والعملية والإنسانية التي قد لا تستطيع الأنظمة الرقمية تقديرها بصورة كاملة.

الخاتمة:

خلصت الدراسة إلى أنّ التحويل الرقمي أصبح عنصراً مؤثراً في تطوير منظومة اتخاذ القرار الأمني، ليس لمجرد إدخال التقنيات الحديثة في العمل الأمني، وإنما لما توفره هذه التقنيات من إمكانيات لتحسين التعامل مع المعلومات والاستفادة منها في تقدير المواقف الأمنية. وقد أظهرت الدراسة أن قيمة التحويل الرقمي ترتبط بمدى توظيفه داخل منظومة

القرار، وجودة البيانات والقدرات البشرية والتنظيمية التي تحيط به وفي ضوء ذلك، توصلت الدراسة إلى النتائج والتوصيات الآتية:

أولاً: النتائج:

1. أثبتت الدراسة أن التحول الرقمي في المجال الأمني يتجاوز مجرد استخدام الوسائل الإلكترونية؛ إذ يقوم على تكامل البنية التقنية والبيانات والموارد البشرية والأمن الرقمي، بما يجعل التقنية جزءاً من منظومة العمل الأمني وآلية دعم القرار .
2. تبين أن التقنيات الرقمية تعزز دعم القرار الأمني من خلال تحسين دورة المعلومات، ابتداءً من الحصول عليها وتنظيمها وربطها وتحليلها، وصولاً إلى إتاحتها للمسؤول المختص في صورة تساعد على تقدير الموقف، مع بقاء القرار النهائي مرتبطاً بالتقدير البشري وصاحب الاختصاص .
3. يسهم التحول الرقمي في تقليل الوقت اللازم لاتخاذ القرار وتحسين دقته، من خلال الحد من التأخير في تداول المعلومات والإجراءات، وإتاحة بيانات أكثر ارتباطاً بالموقف الأمني وقابلة للتحديث والمراجعة .
4. يوفر التحول الرقمي أساساً أفضل للتعامل الاستباقي مع المخاطر الأمنية، من خلال استخدام أدوات التحليل الرقمي والذكاء الاصطناعي لاكتشاف المؤشرات والأنماط التي قد تساعد في تقدير احتمالات الخطر والاستعداد له، دون أن تجعل هذه التقنيات التنبؤ بالمخاطر أمراً يقينياً .
5. يتوقف أثر التحول الرقمي على القرار الأمني على عوامل تتجاوز توافر التقنية نفسها؛ وفي مقدمتها جودة البيانات، وكفاءة المستخدمين، وتكامل الأنظمة، وحماية المعلومات، ووجود رقابة بشرية على مخرجات الأنظمة الرقمية .

ثانياً: التوصيات:

1. وضع إطار مؤسسي متكامل للتحويل الرقمي في العمل الأمني يربط بين البنية التقنية والبيانات والموارد البشرية واحتياجات اتخاذ القرار، بدل التعامل مع كل عنصر بصورة منفصلة .
2. تطوير قواعد البيانات والأنظمة الأمنية بما يسمح بتكاملها وتحديثها المستمر، مع وضع معايير واضحة لجودة البيانات ودقتها وسلامتها قبل استخدامها في اتخاذ القرارات الأمنية .
3. التوسع المنضبط في استخدام تقنيات التحليل الرقمي والذكاء الاصطناعي في دعم التنبؤ بالمخاطر، مع اعتبار مخرجاتها مؤشرات مساعدة لا بديلاً عن التقدير والمسؤولية البشرية .
4. رفع كفاءة العاملين في مجال اتخاذ القرار الأمني من خلال التدريب المستمر على استخدام التقنيات الرقمية وقراءة مخرجاتها وتقييم مدى ملاءمتها للموقف الأمني .
5. تعزيز حماية الأنظمة والبيانات الأمنية من خلال ضوابط واضحة للوصول إلى المعلومات وتداولها واستخدامها، وإجراء اختبارات دورية للأنظمة الرقمية للتأكد من سلامتها وقدرتها على مواجهة المخاطر الإلكترونية .
6. اعتماد آليات دورية لقياس أثر التحويل الرقمي على القرار الأمني، بحيث لا يقتصر تقييم التحويل على عدد الأنظمة والتطبيقات المستخدمة، وإنما يقاس بمدى إسهامه الفعلي في تحسين سرعة القرار ودقته والقدرة على الاستعداد للمخاطر والاستجابة لها .

المراجع:

أولاً: المراجع العربية:

1. الطماوي، محمد سليمان (1998) *النظرية العامة للقرارات الإدارية*، القاهرة: دار الفكر العربي. طبعات متعددة.

2. عبد الله، عبد الغني بسيوني (1998)، *القرار الإداري بين النظرية والتطبيق*، القاهرة: دار النهضة العربية.
3. عبد الله، محمد عبد الفتاح (2015)، *إدارة المعلومات الأمنية: مدخل تنظيمي وتقني*، القاهرة: مكتبة النهضة المصرية، 2015.
4. الخريجي، عبد الله إبراهيم عبد الله. (2022) *رقمنة دعم اتخاذ القرار كنواة لبرامج التحول الرقمي في خدمات الحج وأعماله*. مجلة البحوث الأمنية، 31(83). كلية الملك فهد الأمنية، مركز الدراسات والبحوث.
5. أبو منصور، حسين يوسف. (2020). *الذكاء الاصطناعي وأبعاده الأمنية*. أوراق السياسات الأمنية. الرياض: جامعة نايف العربية للعلوم الأمنية .
<https://doi.org/10.26735/SKHN3682>
6. كامل، عبد الرحمن. (2025). *استخدام الذكاء الاصطناعي في مجالات الأمن والمراقبة: تحليل الممارسات الدولية واستشراف التحديات المستقبلية*. المجلة العربية للدراسات الأمنية، 41(1)
<https://doi.org/10.26735/CXSD7939>
7. عضيبات، أنس عدنان، وأبو عيادة، هبة توفيق. (2023). *تفعيل دور تطبيقات الذكاء الاصطناعي في آلية رصد الجرائم: تصور مقترح*. المجلة العربية للدراسات الأمنية، 39(2)
<https://doi.org/10.26735/BNZJ6179>

ثانياً: المراجع الأجنبية :

1. Möller, Dietmar P. F. & Vakilzadian, H. (2023). *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Applications, and Best Practices*. Advances in Information Security, Vol. 103. Springer Nature Switzerland.
2. Rigopoulos, K., Quinn, S., Pascoe, C., Marron, J., Mahn, A., & Topper, D. (2024). *NIST Cybersecurity Framework 2.0: Resource & Overview Guide* (NIST Special Publication 1299). National Institute of Standards and Technology.
3. Organisation for Economic Co-operation and Development (OECD). (2015). *Recommendation of the Council on Digital*

- Security Risk Management for Economic and Social Prosperity*. OECD Legal Instruments, OECD/LEGAL/0415.
4. Organisation for Economic Co-operation and Development (OECD). (2019). *The Path to Becoming a Data-Driven Public Sector*. OECD Publishing, Paris.
 5. Organisation for Economic Co-operation and Development (OECD). (2019). *Artificial Intelligence in Society*. OECD Publishing, Paris.
 6. Organisation for Economic Co-operation and Development (OECD). (2020). *The OECD Digital Government Policy Framework: Six Dimensions of a Digital Government* (OECD Public Governance Policy Papers, No. 2). OECD Publishing, Paris.
 7. Organisation for Economic Co-operation and Development (OECD). (2025). *Governing with Artificial Intelligence: AI in Law Enforcement and Disaster Risk Management*. OECD Publishing, Paris.
 8. Organisation for Economic Co-operation and Development (OECD). (2026). *Digital Government Outlook 2026*. OECD Publishing, Paris.
 9. Organisation for Economic Co-operation and Development (OECD). (n.d.). *Digital Government*. OECD Publishing.