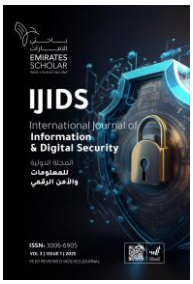


International Journal of Information & Digital Security
Vol 3 Issue 1 (2025)
Pages (37 - 50)

Available at
www.emiratesscholar.com

تحليل استراتيجي لتأثير الأمن السيبراني على البعد التكنولوجي للأمن القومي المصري

Wael Badawy
School of Artificial Intelligence, Egyptian Russian University, Cairo, Egypt ,Department of Data Science
wael@waelbadawy.com

ARTICLE HISTORY

Received: 19 November 2025.
Accepted: 30 November 2025.
Published: 24 December 2025.

PEER - REVIEW STATEMENT:

This article was reviewed under a double-blind process by three independent reviewers.

HOW TO CITE

Badawy, W. (2025). تحليل استراتيجي لتأثير الأمن السيبراني على البعد التكنولوجي للأمن القومي المصري. *International Journal of Information & Digital Security*, *3*(1), 37-50. https://doi.org/10.54878/bjabq755

ABSTRACT

يهدف هذا البحث إلى تحليل التأثيرات الاستراتيجية للأمن السيبراني على البعد التكنولوجي للأمن القومي في مصر، في ظل التحول الرقمي المتسارع والتزايد المستمر للتهديدات السيبرانية. ويوظف البحث نموذج PESTELISM لتحليل الأبعاد المؤسسية والقانونية والسياسية والبيئية والاجتماعية والتكنولوجية والابتكارية والعسكرية ذات الصلة بالأمن الرقمي. ويعتمد البحث على منهج تحليلي استشرافي مدعوم بإحصائيات وطنية ودولية وتقارير أمنية صادرة عن مؤسسات حكومية مثل الجهاز القومي لتنظيم الاتصالات (NTRA) والبنك المركزي المصري (CBE). تظهر نتائج البحث أن البعد التكنولوجي يعد من أكثر الأبعاد تأثرًا بالتحديات السيبرانية، لاسيما في ظل الاعتماد الكبير على حلول أجنبية للحماية الرقمية، ووجود فجوات في الجاهزية المؤسسية والاستجابة الطارئة. ويقترح البحث إنشاء مجلس وطني موحد للأمن السيبراني والذكاء الاصطناعي، إلى جانب تحديث التشريعات، وتحفيز الابتكار المحلي في أنظمة الدفاع الرقمي، وبناء ثقافة مجتمعية رقمية تضمن استدامة الأمن التكنولوجي الوطني.

Keywords: *الأمن السيبراني، الأمن القومي، التحول الرقمي، البنية التحتية التكنولوجية، الابتكار، الاستراتيجية PESTELISM، الوطنية.*

الأوروبية، والتقارير المحلية الصادرة عن الجهاز القومي لتنظيم الاتصالات والبنك المركزي المصري، إلى جانب مؤشرات الأمن السيبراني العالمية. وتتميز هذه الدراسة بمحاولة الربط بين النظرية والتطبيق، من خلال دراسة حالة مصر كنموذج لدولة نامية تخوض تجربة التحول الرقمي وتواجه تحديات الأمن السيبراني المتصاعدة. وتكمن مساهمة هذه الدراسة في أنها لا تكتفي بتشخيص المخاطر، بل تقدم رؤية استراتيجية قابلة للتنفيذ تركز على بناء قدرات وطنية في مجالات الابتكار السيبراني، وحوكمة البيانات، وتحديث الأطر القانونية، وإنشاء كيان مؤسسي موحد قادر على إدارة الأزمات الرقمية. كما تسعى الدراسة إلى تعزيز ثقافة الأمن السيبراني في المجتمع، باعتبارها جزءًا لا يتجزأ من بناء الأمن القومي التكنولوجي.

٢. أهداف البحث

تهدف هذه الدراسة إلى تحقيق الأهداف التالية:

- تحليل التأثيرات الاستراتيجية للأمن السيبراني على البعد التكنولوجي ضمن منظومة الأمن القومي المصري.
- تطبيق نموذج PESTELISM لرصد أوجه القصور والقوة في منظومة الأمن السيبراني المصري من منظور متعدد الأبعاد.
- تحديد التحديات المؤسسية والتشريعية والتقنية التي تواجه الأمن التكنولوجي في ظل تصاعد التهديدات الرقمية.
- اقتراح حلول استراتيجية تعزز من قدرة الدولة على بناء منظومة أمن رقمي متكاملة ومستدامة.
- المساهمة في تطوير فهم علمي وعملي لأهمية الأمن السيبراني كركيزة للأمن القومي في العصر الرقمي.

.أهمية البحث

تتجلى أهمية هذا البحث في كونه يتناول أحد أكثر أبعاد الأمن القومي تعقيدًا وحداثةً، وهو البعد التكنولوجي، الذي أصبح في مقدمة أولويات الدول في ظل التحول الرقمي العالمي. وتمثل مصر نموذجًا مهمًا لدولة نامية تواجه تهديدات سيبرانية متزايدة بالتوازي مع طموحاتها التنموية والتكنولوجية. ويأتي هذا البحث ليسد فجوة واضحة في الدراسات العربية المعنية بتحليل الأمن السيبراني من منظور شمولي، ويربط بين التحليل النظري والنطاق العملي باستعمال نموذج **PESTELISM** الذي يوفر أداة مرنة وشاملة لتحليل البيئة الأمنية الرقمية. كما يسهم البحث في إغناء السياسات العامة والتشريعات من خلال تقديم توصيات مدروسة ومبنية على معطيات واقعية.

١. المقدمة

شهد العالم في العقود الأخيرة تحولًا جوهريًا في مفهوم الأمن القومي، حيث لم يعد يقتصر على الحماية العسكرية والحدودية فقط، بل أصبح يشمل أبعادًا جديدة وأكثر تعقيدًا، من أبرزها الأمن السيبراني والأمن التكنولوجي. في هذا السياق، برزت التهديدات الرقمية كأحد أخطر التحديات التي تواجه الدول، خاصة في ظل الاعتماد المتزايد على النظم الرقمية، والانتقال السريع نحو الحكومة الذكية، والبنية التحتية المتصلة بالشبكات الرقمية والذكاء الاصطناعي. وقد أصبحت البنى التحتية الحيوية في الدول هدفًا رئيسيًا للهجمات السيبرانية، سواء كانت بنية اتصالات أو طاقة أو خدمات مالية أو نظم دفاعية، مما يجعل من الأمن السيبراني ضرورة استراتيجية لا غنى عنها لتعزيز صمود الدول في مواجهة هذه التهديدات الحديثة[١]. في الحالة المصرية، يواكب هذا التحول الرقمي جهود الدولة المستمرة ضمن "رؤية مصر 2030" التي تستهدف بناء اقتصاد رقمي تنافسي قائم على المعرفة. إلا أن هذه الجهود تصطدم بتحديات متصاعدة تتعلق بأمن الفضاء السيبراني، وتهديدات الاختراق، وسرقة البيانات، وتخريب الأنظمة، ما ينعكس بشكل مباشر على قدرة الدولة في حماية البنية التحتية الرقمية، وضمان استمرارية الخدمات الاستراتيجية. وتعد المؤسسات المالية والمصرفية، وقطاع الاتصالات، ومرافق الطاقة، من أكثر القطاعات عرضة لهذه التهديدات [٢٣]. وقد شهدت مصر خلال السنوات الأخيرة عدة حوادث سيبرانية تؤكد وجود ثغرات هيكلية في منظومة الحماية الرقمية، من بينها استهداف أنظمة البنوك، وحملات تصيد إلكتروني واسعة النطاق، بالإضافة إلى محاولات اختراق قواعد البيانات الحكومية. هذا الواقع يعكس الحاجة الملحة إلى وضع استراتيجية وطنية متكاملة للأمن السيبراني تأخذ في الاعتبار خصوصية السياق المصري، وتراعي التوازن بين التقدم التكنولوجي والحماية السيادية للبيانات والمعلومات [٤٥].

وفي ضوء ذلك، تبرز أهمية استخدام نموذج PESTELISM كإطار تحليلي استراتيجي يدمج بين الأبعاد السياسية والاقتصادية والاجتماعية والتكنولوجية والبيئية والقانونية والمؤسسية والعسكرية والابتكارية، لتقديم قراءة شاملة لتأثير الأمن السيبراني على البعد التكنولوجي للأمن القومي المصري. ويمنح هذا النموذج الباحث القدرة على تحليل عناصر القوة والضعف، والفرص والتحديات، بشكل منهجي يمكن من خلاله صياغة سياسات وتوصيات عملية تواكب المتغيرات المتسارعة على المستويين المحلي والدولي [٦٧]. تستند هذه الدراسة إلى منهج تحليلي استشرافي يستفيد من التقارير الدولية الصادرة عن الاتحاد الدولي للاتصالات (ITU)، ووكالة ENISA

المصرح به، والتدمير، أو التعطيل" [٦]. وقد توسّع هذا المفهوم في العقود الأخيرة ليُصبح عنصرًا رئيسيًا ضمن منظومة الأمن القومي، لا سيما مع تصاعد الهجمات الرقمية التي باتت تستهدف مؤسسات حيوية ومراكز صنع القرار [٧].

٢ الأمن القومي التكنولوجي

يشير الأمن القومي التكنولوجي إلى قدرة الدولة على تأمين بنيتها الرقمية والتقنية، والحفاظ على استقلالها السيادي فيما يتعلق بإدارة وتشغيل نظم المعلومات وشبكات الاتصال والبيانات الوطنية. ويشمل ذلك ضمان عدم اختراق مراكز التحكم الحيوية، مثل نظم الطاقة والمياه والمطارات والمصارف الرقمية، وهو ما يتطلب منظومة دفاع رقمي متكاملة ترتبط مباشرة بالمفهوم الأوسع للأمن القومي [٨].

٦.١.٣ المخاطر السيبرانية المرتبطة بالتحول الرقمي

رغم أهمية التحول الرقمي في دعم التنمية الاقتصادية وتطوير الخدمات الحكومية، إلا أن هذه النقلة النوعية في البيئة المعلوماتية تُعرض الدولة لمخاطر متزايدة. إذ تشير الإحصاءات إلى أن مصر شهدت في عام 2022 أكثر من 270 مليون محاولة هجوم سيبراني، استهدفت مؤسسات مصرفية، وهيئات حكومية، ومنشآت طبية [٩]. وقدّر تقرير صادر عن البنك المركزي المصري الخسائر الناتجة عن الهجمات السيبرانية في القطاع المصرفي المصري بأكثر من 320 مليون جنيه مصري خلال عام واحد فقط [١٠].

٦.١.٤ فجوات في الهيكل المؤسسي للأمن السيبراني

تُعاني البنية التنظيمية في مصر من تداخل في الأدوار وتعدد الجهات المسؤولة عن إدارة الأمن السيبراني، مثل الجهاز القومي لتنظيم الاتصالات (NTRA)، وزارة الاتصالات وتكنولوجيا المعلومات، وزارة الدفاع، ووزارة الداخلية. ويُلاحظ غياب كيان مركزي موحد قادر على إدارة الأزمات الرقمية والتنسيق الفوري بين هذه الجهات [١١]. كما أن محدودية التنسيق تؤثر سلبًا على سرعة الاستجابة للأزمات، وتُضعف القدرة على إصدار تحذيرات مبكرة أو التحكم في انتشار الهجمات.

٦.١.٥ ضعف الثقافة الرقمية المجتمعية

تلعب الثقافة الرقمية دورًا محوريًا في دعم أو إضعاف الأمن السيبراني. ووفقًا لدراسة مسحية أجرتها جامعة القاهرة بالتعاون مع المركز القومي للبحوث الرقمية عام 2023، تبين أن 82% من طلاب الجامعات لا يمتلكون معرفة كافية بأساسيات الأمن الرقمي، مثل طرق الحماية من التصيّد الإلكتروني أو استخدام

٤ .التساؤلات البحثية

ترتكز هذه الدراسة على التساؤلات التالية:

١ .ما مدى تأثر البعد التكنولوجي في الأمن القومي المصري بالتهديدات السيبرانية الحديثة؟

٢ .ما أبرز الفجوات المؤسسية والتشريعية التي تعيق بناء منظومة دفاع رقمي فعّالة في مصر؟

٣ .كيف يمكن لنموذج **PESTELISM** أن يُستخدم لتحليل بيئة الأمن السيبراني الوطني؟

٤ .ما السياسات والتوصيات المقترحة لتعزيز الأمن السيبراني التكنولوجي في مصر؟

٥ .منهجية البحث

يعتمد هذا البحث على المنهج التحليلي الاستشرافي الذي يجمع بين:

- التحليل الوصفي: لرصد الواقع الحالي لمنظومة الأمن السيبراني في مصر.
- التحليل الاستشرافي: لتوقع سيناريوهات التهديد المستقبلية واستجابة الدولة لها.
- دراسة الحالة: عبر التركيز على مصر كنموذج تطبيقي، وتحليل سياستها الوطنية في الأمن السيبراني.
- الإطار التحليلي :**PESTELISM** الذي يُستخدم لقراءة شاملة للبيئة الأمنية الرقمية عبر أبعاد متعددة (سياسية، اقتصادية، اجتماعية، تكنولوجية، بيئية، قانونية، مؤسسية، ابتكارية، وعسكرية).

وتعتمد الدراسة على مراجعة أدبيات علمية وتقارير محلية ودولية رسمية، من أبرزها تقارير الخاصة بالـ **NTRA**، **ITU**، **ENISA**، البنك المركزي المصري، ووثائق التشريعات القانونية المتعلقة بالأمن السيبراني.

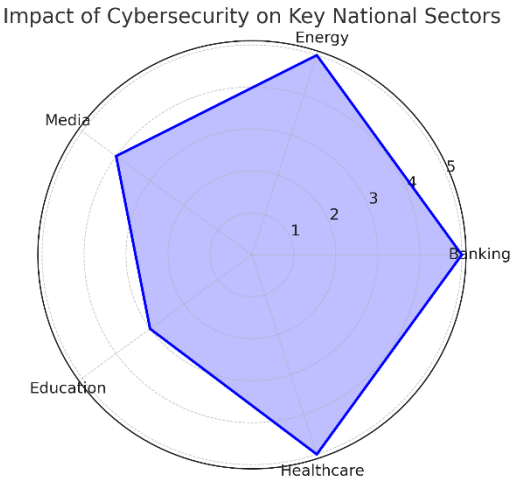
. الإطار المفاهيمي والنظري وتحليل المشكلة

٦.١. الإطار المفاهيمي وتحليل المشكلة

٦.١.١ مفهوم الأمن السيبراني

يُعرف الأمن السيبراني بأنه "مجموعة من الأدوات، السياسات، والضوابط المصممة لحماية الأنظمة الرقمية والشبكات والمستخدمين من الوصول غير

مؤسسي، ومجتمعي، وهو ما تسعى هذه الدراسة إلى تحليله وتفكيكه عبر النموذج المختار.



شكل (١) :يوضح تأثيرات الأمن السيبراني علي القطاعات المختلفه

المصدر: إعداد الباحث اعتمادًا على تحليل الوضع المؤسسي المصري (2025).

٦.٢ الإطار التحليلي لتأثير الأمن السيبراني على البعد التكنولوجي للأمن القومي المصري

٦.٢.١ أهمية البعد التكنولوجي في تكوين الأمن القومي

يمثل البعد التكنولوجي اليوم حجر الزاوية في منظومة الأمن القومي للدول الحديثة، فالبنية التحتية الرقمية، بما في ذلك شبكات الاتصالات، ونظم التحكم، ومراكز البيانات، أصبحت من الأصول الاستراتيجية التي لا تقل أهمية عن الأصول العسكرية أو الاقتصادية. وتشير دراسات حديثة إلى أن معظم الهجمات السيبرانية لا تهدف إلى التدمير الفوري فحسب، بل إلى زرع أبواب خلفية للتحكم طويل الأمد في الأنظمة الرقمية للدول [١٥].

٦.٢.٢ مظاهر الهشاشة في البيئة التكنولوجية المصرية

رغم جهود مصر في تطوير بنيتها الرقمية ضمن "رؤية مصر 2030"، لا تزال هناك تحديات جوهرية تعيق تحقيق السيادة التكنولوجية. من أبرزها:

- الاعتماد على برامج تشغيل أجنبية غير مفتوحة المصدر.
- غياب منصات وطنية متكاملة لإدارة الخدمات الرقمية الحساسة.

المصادقة الثنائية [١٢]. وهو ما يجعل المستخدم النهائي الحلقة الأضعف في سلسلة الدفاع الرقمي.

٦.١.٦ الحاجة إلى نموذج تحليلي شامل: نموذج PESTELISM

نظرًا لتعقيد الظاهرة الأمنية الرقمية، وارتباطها بتشابكات قانونية ومؤسسية وسياسية واجتماعية، فإن النماذج التقليدية مثل SWOT وPESTEL تصبح غير كافية لفهم السياق المصري. ومن هنا جاءت أهمية نموذج PESTELISM، الذي يُعد امتدادًا وتحسينًا لنموذج PESTEL، حيث يُضيف بُعدين إضافيين هما:

البعد العسكري/الأمني (Security/Military)

البعد الابتكاري (Innovation)

يُمكّن هذا النموذج من تحليل البيئة الرقمية من عدة زوايا، بدءًا من الإرادة السياسية، مرورًا بالتشريعات، وانتهاءً بالابتكار المحلي وقدرات الردع التكنولوجي [١٣]. وتوفر هذه المقاربة أداة فعالة لصنّاع القرار والباحثين لتقييم مخاطر الأمن السيبراني ووضع السياسات المناسبة للحد منها.

٦.١.٧ العلاقة الجدلية بين الأمن السيبراني والسيادة التكنولوجية

تظهر العلاقة الجدلية بوضوح في اعتماد المؤسسات المصرية على برمجيات وتطبيقات أجنبية تُدار خارج الإقليم، مثل أنظمة التشغيل الأمريكية ومنصات التخزين السحابي الأوروبية، مما يُهدد السيادة الرقمية في حالات الطوارئ السياسية أو العقوبات التكنولوجية [١٤]. كما أن غياب بنية تحتية مستقلة تُنتج أدوات الأمن السيبراني محليًا، يُعد من أبرز مظاهر هشاشة السيادة التكنولوجية الوطنية.

يسمح هذا النموذج برؤية تحليلية متعددة الزوايا، تساعد في فهم تداخلات الأمن السيبراني مع سياسات الدولة، ومواردها، وثقافتها الرقمية، وقدراتها المؤسسية والعسكرية.

إن المشكلة التي تتناولها هذه الورقة لا تتعلق فقط بوجود تهديدات رقمية، وإنما في **ضعف الردع الرقمي الاستباقي** في البيئة المصرية، وغياب منظومة متكاملة للوقاية والتحصين والتنبؤ. كما أن تعدد الجهات المسؤولة، وعدم وجود مركز وطني موحد للأمن السيبراني، يزيد من هشاشة الاستجابة لأي هجوم متزامن أو متعدد الجبهات. وبذلك، فإن التحدي الحقيقي ليس تقنيًا فقط، بل **سياسي، تشريعي،**

البنك المركزي المصري بأن عدد المحاولات الخبيثة لاختراق أنظمة الدفع زاد بنسبة 43% في الفترة من 2021 إلى 2023 [١٩]. كما أن بعض البنوك واجهت محاولات لسرقة بيانات العملاء من خلال تطبيقات مقلدة على الهواتف الذكية، وهو ما دفع الجهات الرقابية إلى إصدار تعليمات صارمة حول ضرورة تطوير حلول دفاعية تعتمد على الذكاء الاصطناعي والتحقق البيومتري.

٦.٢.٥ قصور في منظومة الإنذار المبكر والتكامل الوطني

من التحديات الأساسية التي تعاني منها المنظومة الرقمية في مصر هو غياب شبكة إنذار مبكر موحدة قادرة على تحليل الأنماط السيبرانية، وإصدار تحذيرات في الوقت الفعلي. وتعتمد معظم الجهات الحكومية حاليًا على آليات دفاعية غير مترابطة، ما يُعيق القدرة على كشف الهجمات المعقدة (APT attacks) التي تعتمد على التسلل البطيء والذكي إلى الأنظمة [٢٠] .

٦.٢.٦ نموذج PESTELISM

نموذج **PESTELISM** إطارًا تحليليًا موسعًا يُستخدم لفهم البيئة الاستراتيجية لأي دولة أو مؤسسة، من خلال تحليل العوامل الخارجية والداخلية التي تؤثر في القرار والسياسات العامة. يتميز نموذج **PESTELISM** إطارًا تحليليًا موسعًا يُستخدم لفهم البيئة الاستراتيجية لأي دولة أو مؤسسة، من خلال تحليل العوامل الخارجية والداخلية التي تؤثر في القرار والسياسات العامة. يتميز هذا النموذج بتكامله وشموليته مقارنة بالنماذج التقليدية مثل **PEST**أو **PESTEL**، حيث يُضيف إليه بُعدين حيويين هما: **الابتكار (Innovation)**، و**الأمن/العسكر (Security/Military)**، مما يجعله مثاليًا لتحليل قضايا متشابكة مثل الأمن السيبراني والتحول الرقمي الوطني.

. البعد السياسي (Political)

يركز على دور الإرادة السياسية والتوجهات الحكومية في دعم أو عرقلة قضايا التحول الرقمي والأمن القومي. يُحلل هذا البعد استقرار النظام السياسي، ومقدار الانخراط الرسمي في الخطط الرقمية، وطبيعة العلاقة بين صناع القرار والمؤسسات السيادية.

مثال تطبيقي: دعم القيادة السياسية المصرية لاستراتيجية الذكاء الاصطناعي يمثل قوة دفع مهمة في هذا البعد.

٢. البعد الاقتصادي (Economic)

- ضعف التكامل بين قواعد البيانات الحكومية المختلفة.
- تأخر تطبيق حلول الذكاء الاصطناعي في الأمن السيبراني المحلي [١٦].

كما أن مؤسسات التعليم العالي لا تزال تفتقر إلى برامج تخصصية محدثة في الأمن السيبراني، وهو ما يُفاقم من نقص الكفاءات المحلية في هذا المجال [١٧ ١٨].

٦.٢.٣ تحليل البعد التكنولوجي عبر نموذج PESTELISM

بالاستناد إلى نموذج PESTELISM، يمكن تحليل نقاط القوة والضعف في البعد التكنولوجي المصري كما يلي:

جدول ١ : تحليل نقاط القوة والضعف في البعد التكنولوجي المصري

البعد	نقاط القوة	نقاط الضعف
تكنولوجي	- تطوير البنية التحتية للإنترنت - مشاريع الحكومة الرقمية - مراكز البيانات الوطنية	- الاعتماد على حلول أجنبية - ضعف حماية البيانات في بعض القطاعات - بطء تحديث أنظمة التشغيل الحكومية
مؤسسي	- وجود جهاز منظم (NTRA) - دعم من وزارة الاتصالات	- تشتت الأدوار - غياب غرفة عمليات سيبرانية موحدة
قانوني	- صدور قوانين (مثل قانون مكافحة الجرائم الإلكترونية 175/2018)	- ضعف إنفاذ القوانين - غياب تشريع خاص بالذكاء الاصطناعي
عسكري	- تأسيس وحدات سيبرانية بالقوات المسلحة	- ضعف التكامل بين القدرات المدنية والعسكرية الرقمية
ابتكاري	- وجود بعض المبادرات البحثية	- غياب تمويل حكومي موجه للابتكار السيبراني المحلي

٤ دراسة حالة: الأمن السيبراني في القطاع المصرفي

تُعد المؤسسات المصرفية المصرية من أكثر القطاعات استهدافًا في الفضاء السيبراني. وأفاد

٧. بُعد الابتكار (Innovation)

يتناول القدرات الوطنية على تطوير حلول محلية في مجال الذكاء الاصطناعي والأمن السيبراني، ومدى دعم البحث العلمي، وحاضنات الابتكار، وريادة الأعمال التكنولوجية.

مثال تطبيقي: المسابقات التي تنظمها مصر في مجال الابتكار السيبراني يمكن أن تتحول إلى أدوات استراتيجية إذا أُدرجت ضمن منظومة وطنية.

٨. البعد الأمني/العسكري (Security/Military)

يُعد من أهم الأبعاد المضافة للنموذج، حيث يُعنى بتحليل جاهزية الدولة عسكريًا للتعامل مع حروب الجيل الخامس، ومدى دمج الذكاء الاصطناعي في إدارة الدفاع، وتحديث العقيدة العسكرية لتشمل الهجمات الرقمية.

مثال تطبيقي: قيام القوات المسلحة المصرية بإنشاء وحدات مختصة بالأمن السيبراني يعكس تطورًا في هذا المجال.

يمكّن نموذج **PESTELISM** الباحثين وصناع القرار من تحليل البيئة الرقمية والأمنية بشكل شامل ومتعدد الأبعاد، ويُعد أداة مثالية لبناء استراتيجيات ذكية للأمن القومي في زمن الرقمنة، لاسيما في دول مثل مصر التي تمر بتحول رقمي حرج.

٦.٢.٧ أهمية نموذج PESTELISM في تحليل الأمن السيبراني والتحول الرقمي

إن استخدام نموذج **PESTELISM** في تحليل السياسات الوطنية، لا سيما في مجالات معقدة مثل الأمن السيبراني والذكاء الاصطناعي، يُعد نقلة نوعية في الفكر التحليلي الاستراتيجي. فهو نموذج يجمع بين الرؤية الكلية للبيئة الخارجية والداخلية المحيطة بالدولة أو المؤسسة، ويساعد على فهم التفاعلات المتبادلة بين السياسة والاقتصاد والمجتمع والتكنولوجيا والقانون والبيئة، ويضيف إليها أبعادًا أصبحت اليوم ذات تأثير جوهري: الابتكار، والبنية المؤسسية، والأمن/العسكر.

ما يميز هذا النموذج عن غيره من النماذج التقليدية، مثل **SWOT** أو **PEST** أو حتى **PESTEL**، هو أنه لا يتوقف عند تحديد العوامل المؤثرة، بل يدفع باتجاه تحليل وظيفي متكامل يُمكّن الباحث أو صانع القرار من فهم نقاط القوة والضعف والفرص والتهديدات داخل بيئة ديناميكية سريعة التغير. وهذا التحليل المتعدد الأبعاد يُعد أداة حاسمة في تقييم جاهزية الدول لمواجهة

يرتبط هذا البعد بتحليل البنية الاقتصادية للدولة، ومدى ارتباط الاقتصاد الرقمي بمنظومة الأمن القومي. كما يدرس حجم الاستثمار في التكنولوجيا، والجاهزية الرقمية للقطاعات المالية، ومدى اعتماد الدولة على الاقتصاد غير النقدي.

مثال تطبيقي: توسّع مصر في الشمول المالي يفرض ضرورة وجود نظام سيبراني يحمي بيانات العملاء والمؤسسات.

٣. البعد الاجتماعي (Social)

يتناول هذا البعد سلوك الأفراد والمجتمعات، ومدى الوعي الرقمي، وثقافة الأمن السيبراني، ومدى استعداد المواطن للتعامل مع التكنولوجيا دون أن يكون عرضة للتضليل أو الاختراق.

مثال تطبيقي: ضعف الثقافة الرقمية بين الشباب المصري يشكل أحد أهم الثغرات في هذا البعد.

٤. البعد التكنولوجي (Technological)

يركز على الجاهزية التقنية، وتطور البنية التحتية الرقمية، واعتماد أنظمة الحماية، ومدى امتلاك الدولة لتقنيات الذكاء الاصطناعي وأدوات الدفاع السيبراني المحلية.

مثال تطبيقي: اعتماد مصر على حلول أجنبية للحماية الرقمية يُبرز خطرًا على الاستقلال السيبراني.

٥. البعد البيئي (Environmental)

يركز على التقنيات المستخدمة في إدارة الموارد البيئية، ومدى تأمين الأنظمة الذكية التي تُشغّل شبكات المياه والطاقة والنقل، ويُحلل المخاطر الناجمة عن اختراق هذه الأنظمة.

مثال تطبيقي: اختراق نظام ذكي لإدارة الكهرباء في مصر قد يؤدي إلى كوارث واسعة النطاق.

٦. البعد القانوني (Legal)

يتناول التشريعات والقوانين المتعلقة بالجرائم الإلكترونية، وحماية البيانات، والملكية الفكرية الرقمية، كما يحلل مدى مرونة القوانين وقدرتها على مواكبة التحولات التقنية.

مثال تطبيقي: قانون حماية البيانات في مصر لا يزال يحتاج إلى تفعيل أوسع لتطبيقه داخل المؤسسات.

يمثل البعد السياسي في النموذج أحد المفاتيح المركزية لفهم استراتيجية الأمن القومي الرقمي في مصر، حيث أظهرت السنوات الأخيرة انخراطًا مباشرًا من القيادة السياسية في دعم التحول الرقمي كأداة للحوكمة، وكعنصر جوهري من مشروع "الجمهورية الجديدة". وقد جاء هذا الدعم السياسي في صورة خطط حكومية معلنة، مثل الاستراتيجية الوطنية للذكاء الاصطناعي، وتشكيل المجلس الأعلى للتحول الرقمي، واعتماد رؤية رقمية واضحة في كافة الوزارات والهيئات. إلا أن هذا الدعم، رغم أهميته، ما زال يصطدم بعوائق تتعلق بالبنية التشريعية والتنفيذية، وضعف التنسيق بين الجهات، وغياب رؤية موحدة للأمن السيبراني كأولوية سيادية. كما أن التهديدات الرقمية العابرة للحدود تجعل من الدور السياسي للدولة أكثر تعقيدًا، خصوصًا في ظل تزايد الهجمات السيبرانية التي تتخذ من وسائل الإعلام منصات لبث الشائعات وتقويض الثقة العامة.

أما من الناحية الاقتصادية، فإن التحول الرقمي في مصر يُعد ركيزة أساسية لتحقيق النمو المستدام، خصوصًا مع الاتجاه الحكومي إلى توسيع قاعدة الشمول المالي، والتحول نحو الاقتصاد غير النقدي، وتبني المدن الذكية. ومع هذا، فإن البنية الرقمية الاقتصادية لا تزال تواجه تهديدات سيبرانية متكررة قد تؤدي إلى تعطيل أنظمة الدفع، أو اختراق قواعد البيانات المالية الحساسة، كما أن القطاع المصرفي، رغم كونه من أكثر القطاعات استعدادًا، إلا أنه ما زال معرضًا للاختراقات، وهو ما تشير إليه التقارير الصادرة عن البنك المركزي المصري والجهاز القومي لتنظيم الاتصالات. ومن الجدير بالذكر أن الأمن السيبراني الاقتصادي لا يقتصر على البنوك فقط، بل يشمل التجارة الإلكترونية، أنظمة الضرائب الرقمية، والاستثمارات الأجنبية، وكلها جوانب ترتبط بثقة المستخدم في المنظومة الرقمية للدولة.

فيما يتعلق بالبعد الاجتماعي، يمكن القول إن المجتمع المصري يعيش مرحلة انتقالية غير متوازنة في وعيه الرقمي، إذ يتزايد الاعتماد على وسائل التواصل الاجتماعي بشكل غير مسبوق، دون وجود ثقافة وقائية كافية لدى المستخدمين. وقد أظهرت عدة دراسات ميدانية أن نسبة كبيرة من الشباب المصري يستخدمون الإنترنت دون تمييز بين المعلومات الموثوقة والمضللة، مما يجعلهم هدفًا سهلًا للهجمات السيبرانية التي تستهدف النسيج المجتمعي، وتخلق حالة من البلبلة وعدم اليقين العام. كما أن عدم تكامل مؤسسات التعليم والثقافة في نشر الوعي الرقمي أدى إلى ضعف في المناعة المجتمعية ضد التضليل الرقمي وهندسة العقول عبر المحتوى الاصطناعي الذكي. وتزداد خطورة هذا الأمر في ظل انتشار محتوى "الديب فيك" والخطاب التهديدات السيبرانية والتكنولوجية، خصوصًا في ظل التحولات الجذرية التي يشهدها العالم بعد جائحة كوفيد-19، وصعود الذكاء الاصطناعي كأداة استراتيجية بحد ذاته.

٦.٢.٨ أهمية إضافة أبعاد الابتكار (I) والأمني/العسكري (SM)

أولًا: الابتكار (Innovation)

يُعد الابتكار أحد المحركات المركزية لأي استراتيجية أمنية رقمية ناجحة. فالاعتماد على حلول مستوردة في الأمن السيبراني أو الذكاء الاصطناعي يُضعف السيادة التقنية للدولة، ويجعلها عرضة للاختراق الخارجي أو التبعية البنيوية. ومن هنا، فإن دمج بُعد الابتكار ضمن النموذج يُبرز قدرة الدولة على إنتاج حلول محلية، وتطوير خوارزميات دفاعية، وبناء أدوات تنبؤ ذات سيادة، ما يُعزز الردع الرقمي الوطني.

مثال: مصر تمتلك طاقات بشرية واعدة في الذكاء الاصطناعي، ولكن غياب سياسات داعمة للابتكار يحول دون استثمار هذه القدرات في حماية الأمن القومي.

ثانيًا: الأمني/العسكري (Security/Military)

لا يمكن تحليل بيئة الأمن الرقمي دون النظر إلى القدرات الدفاعية والعسكرية للدولة، خصوصًا في ظل تطور حروب الجيل الخامس والسادس التي تعتمد على أدوات غير تقليدية، مثل الهجمات الموجهة على شبكات الكهرباء، أنظمة الاتصالات، أو البنية التحتية الحرجة. ولهذا، فإن دمج هذا البُعد في النموذج يُعطي صورة واقعية عن جاهزية الدولة لمواجهة التهديدات السيبرانية ذات الطبيعة السيادية.

مثال: تفعيل وحدات الأمن السيبراني داخل القوات المسلحة المصرية يعكس اعترافًا استراتيجيًا بأن الحرب في المستقبل لن تكون بالضرورة بالسلاح التقليدي، بل عبر خوادم وشيفرات وشبكات.

إن نموذج **PESTELISM** لا يُعد فقط أداة تحليل أكاديمية، بل هو بوصلة استراتيجية يمكن من خلالها رسم خريطة طريق عملية لتطوير الأمن السيبراني والحوكمة الرقمية في الدول. وإن إضافة أبعاد الابتكار والمؤسسات والدفاع السيبراني يجعل من هذا النموذج إطارًا مرنًا وقابلًا للتطبيق في واقع يتغيّر بسرعة ويفرض تهديدات مركّبة ومعقدة.

٦.٣ تحليل الواقع المصري من خلال نموذج PESTELISM

وفي الجانب المؤسسي، يتضح وجود تشتت واضح في توزيع المهام والاختصاصات بين الجهات المختلفة المعنية بالأمن السيبراني، إذ تعمل وزارة الاتصالات، وزارة الدفاع، وزارة الداخلية، والهيئات السيادية كل في مساره، دون وجود كيان وطني موحد قادر على التنسيق الشامل والتدخل السريع. كما أن الجهاز القومي لتنظيم الاتصالات، رغم جهوده الكبيرة، لا يمتلك صلاحيات سيادية تُمكِّنه من التعامل مع الأزمات العابرة للوزارات، وهو ما يخلق حالة من البطء المؤسسي في مواجهة التهديدات الرقمية المعقدة. وقد دعا العديد من الخبراء إلى إنشاء "مجلس سيادي وطني للأمن السيبراني"، تكون له سلطة تشريعية واستباقية، ويضم كافة الفاعلين من مؤسسات الدولة، إضافة إلى ممثلين عن القطاع الخاص والأوساط الأكاديمية.

وفيما يخص البعد الابتكاري، فإن مصر تمتلك إمكانيات بشرية متميزة في مجالات البرمجة، الذكاء الاصطناعي، والتحليل الرقمي، وقد ظهر ذلك في مشاركاتها الدولية في مسابقات الابتكار السيبراني، وتأسيس عدد من حاضنات الأعمال التقنية في الجامعات. إلا أن هذه القدرات تفتقر إلى حاضنة وطنية موحدة تستثمر هذه الطاقات في خدمة استراتيجية وطنية للابتكار في مجال الأمن الرقمي. إن الابتكار في السياق السيبراني لا يجب أن يُفهم فقط كمجال أكاديمي، بل كركيزة سيادية ذات بعد أمني، تتطلب تمويلًا حكوميًا مستقرًا، ومشاركة مجتمعية واسعة.

وأخيرًا، يُعد البعد الأمني والعسكري حجر الزاوية في أي استراتيجية للأمن القومي، وفي مصر، بدأت القوات المسلحة في السنوات الأخيرة في تطوير وحدات متخصصة بالأمن السيبراني، وتدريب كوادر عسكرية على تقنيات الحرب الرقمية. كما أن هناك إشارات إلى استخدام الذكاء الاصطناعي في مجال التخطيط العملياتي والرصد الاستراتيجي، إلا أن هذه الجهود لا تزال في مراحلها الأولى، مقارنةً بالسرعة التي تتطور بها تقنيات الحرب غير التقليدية. وتبقى الحاجة ملحة لدمج الذكاء الاصطناعي في المنظومة الدفاعية المصرية بشكل أوسع، سواء في الدفاعات السيبرانية أو في تحصين نظم القيادة والتحكم.

جدول ٢ تحليل نموذج PESTELISM للأمن القومي الرقمي في مصر

السياسي	دعم القيادة السياسية للتحول الرقمي؛ غياب استراتيجية موحدة للأمن السيبراني.

التحريضي، ما يفرض ضرورة إشراك الإعلام والتعليم في بناء بيئة اجتماعية محصنة رقميًا.

أما من الناحية التكنولوجية، فإن مصر حققت تقدمًا ملحوظًا في بناء بنية تحتية رقمية حديثة، من خلال التوسع في شبكات الألياف الضوئية، وإنشاء مراكز بيانات قومية، وتفعيل الهوية الرقمية. ومع ذلك، فإن هذا التقدم لا يصاحبه دائمًا تحديث دوري للأنظمة الأمنية، إذ تُظهر التقارير أن نسبة كبيرة من المؤسسات العامة لا تزال تستخدم أنظمة تشغيل قديمة أو غير مؤمنة بشكل كافٍ. كما أن معظم الحلول الأمنية المستخدمة مستوردة وليست محلية الصنع، مما يطرح تحديات تتعلق بالسيادة التكنولوجية، واستقلالية القرار الرقمي، خصوصًا في وقت بات فيه الأمن التكنولوجي يوازي الأمن العسكري من حيث الأهمية. إن الاعتماد على الذكاء الاصطناعي في قطاعات حساسة مثل الأمن القومي، الصحة، والبنية التحتية، دون امتلاك أدوات تقييم وطنية للمخاطر، يمثل فجوة تكنولوجية خطيرة تحتاج إلى تدخل عاجل.

وفيما يتعلق بالبعد البيئي، فإن توظيف التكنولوجيا الذكية في إدارة الموارد الطبيعية يُعد خطوة إيجابية نحو تحقيق الاستدامة، إلا أن غياب الحماية السيبرانية الكافية لهذه الأنظمة قد يؤدي إلى كوارث غير متوقعة. فقد باتت أنظمة الري الذكي، ومحطات تحلية المياه، وشبكات توزيع الكهرباء تعتمد على منصات رقمية متصلة بالإنترنت، مما يجعلها عرضة للاختراق، وهو ما قد يترتب عليه شلل في إدارة الموارد، وتهديد مباشر لحياة المواطنين. إن البيئة الرقمية ليست فقط معنية بحماية المعلومات، بل أيضًا بحماية الطبيعة، وهو ما يتطلب دمج الأمن البيئي الرقمي ضمن استراتيجية الأمن القومي، وليس كأمر ثانوي أو منفصل.

أما على الصعيد القانوني، فإن الإطار التشريعي المصري قد شهد تطورًا ملموسًا، خاصة بعد صدور قانون مكافحة الجرائم الإلكترونية وقانون حماية البيانات الشخصية. غير أن التطبيق العملي لهذين القانونين لا يزال يواجه صعوبات تتعلق بغياب الكفاءات القضائية المتخصصة في الجريمة الرقمية، وتضارب الصلاحيات بين الجهات الرقابية والتنفيذية. كما أن بعض المواد القانونية لم تُحدَّث لمواكبة التغير السريع في تقنيات الذكاء الاصطناعي، مما يجعل من الإطار التشريعي غير كافٍ لضمان الحماية الشاملة، سواء للفرد أو للمؤسسة أو للدولة. إن التشريع في عصر الذكاء الاصطناعي يجب أن يكون مرنًا، وقابلًا للتحديث المستمر، ومبنيًا على مقاربة تشاركية تضم القانونيين، التقنيين، والمجتمع المدني.

جدول ٤ الفجوات والتحديات المؤسسية في منظومة الأمن السيبراني المصرية

الفجوة الحالية	الدور المتوقع	الجهة المسؤولة
غياب الصلاحيات التنفيذية في الأزمات	التخطيط الرقمي والإشراف على الاستراتيجيات	وزارة الاتصالات
نقص الكوادر المدربة على التحقيق السيبراني	ضبط الجرائم الرقمية	وزارة الداخلية
غياب التكامل مع الجهات المدنية	حماية البنية العسكرية الرقمية	وزارة الدفاع
محدودية الصلاحيات العابرة للقطاعات	تنظيم القطاع التكنولوجي	NTRA
ضعف الدعم الفني وسرعة التحرك	الاستجابة للطوارئ السيبرانية	EG-CERT

المصدر: إعداد الباحث اعتمادًا على تحليل الوضع المؤسسي المصري (2025).

جدول ٥ مقارنة بين الوضع الحالي والمطلوب في 5 أبعاد رئيسية للأمن الرقمي

الوضع المطلوب	الوضع الحالي	البعد
قوانين متكاملة تتطور مع التكنولوجيا	تشريعات جزئية وغير مرنة	القانوني
تعليم رقمي مبكر ومناخ إعلامي توعوي	وعي رقمي منخفض وممارسات خطرة	الاجتماعي
الاقتصادي	نمو الشمول المالي؛ تهديدات مستمرة للبنوك والتجارة الإلكترونية.
الاجتماعي	ضعف الثقافة الرقمية؛ انتشار الهندسة الاجتماعية.
التكنولوجي	تقدم البنية التحتية؛ اعتماد على حلول أجنبية.
البيئي	أنظمة ذكية غير محصنة؛ هشاشة الأمن البيئي الرقمي.
القانوني	وجود قوانين جزئية؛ ضعف في آليات التنفيذ.
المؤسسي	تشتت المسؤوليات؛ غياب التنسيق الوطني.
الابتكاري	قدرات بشرية واعدة؛ غياب إطار وطني للابتكار.
الأمني والعسكري	وحدات متخصصة قيد التطوير؛ حاجة إلى دمج AI في العقيدة العسكرية.

المصدر: إعداد الباحث اعتمادًا على تحليل الوضع المؤسسي المصري (2025).

جدول ٣ المقترحات الاستراتيجية لتعزيز الأمن السيبراني في مصر

إنشاء مجلس وطني	كيان سيادي موحّد لإدارة الأمن السيبراني والذكاء الاصطناعي.
تحديث التشريعات	قوانين مرنة تغطي التهديدات الذكية والخوارزميات التنبؤية.
إدماج الثقافة الرقمية	تضمين الوعي السيبراني في المناهج التعليمية.
تمويل الابتكار المحلي	تحفيز حلول أمنية وطنية تدعم السيادة التكنولوجية.
تأمين البنية الذكية	تحصين نظم الكهرباء، المياه، والمواصلات الذكية.
تعزيز الشراكات	الانضمام لتحالفات سيبرانية إقليمية ودولية.

المصدر: إعداد الباحث اعتمادًا على تحليل الوضع المؤسسي المصري (2025).

. النتائج العامة

من خلال التحليل المفاهيمي والتطبيقي السابق، يُمكن استخلاص مجموعة من النتائج الأساسية التي توضّح التحديات والمخاطر والفرص في ملف الأمن السيبراني المرتبط بالبعد التكنولوجي للأمن القومي المصري:

تزايد حجم التهديدات الرقمية: تُظهر البيانات ارتفاعًا ملحوظًا في عدد الهجمات السيبرانية، سواء من حيث الكم أو النوعية، وبالأخص تلك التي تستهدف البنية التحتية الحيوية مثل المصارف والطاقة والمرافق الحكومية [٢١].

هشاشة سيادية في الأمن السيبراني: لا تزال مصر تعتمد بنسبة كبيرة على حلول تكنولوجية مستوردة، ما يُضعف سيادتها التقنية ويجعلها عرضة للابتزاز الرقمي في حالات الأزمات الجيوسياسية [٢٢].

فجوات مؤسسية وتشريعية: تتسم البيئة المؤسسية بالتداخل وعدم التكامل، كما أن التشريعات الحالية لا تواكب التطورات التقنية مثل الذكاء الاصطناعي، والتعلم الآلي، وتهديدات الفضاء السحابي [٢٣].

غياب كفاءة التنبؤ والوقاية: لا توجد بنية وطنية قوية للإنذار المبكر أو شبكات تحليل نمط الهجمات المعقدة، مما يجعل الاستجابة غالبًا متأخرة وردّ فعلية بدلًا من كونها استباقية [٢٤].

ضعف في تكوين رأس المال البشري السيبراني: لا يزال التعليم الجامعي والتقني في مصر غير قادر على تخريج عدد كافٍ من المختصين المؤهلين للعمل في وظائف الحماية الرقمية والتحليل الجنائي السيبراني [٢٥].

٨. مقترحات استراتيجية

استنادًا إلى النتائج والتحليل السابق، يمكن تقديم حزمة من المقترحات العملية ضمن استراتيجية وطنية شاملة لتعزيز الأمن السيبراني في بعده التكنولوجي:

أ. إنشاء مجلس وطني موحّد للأمن السيبراني

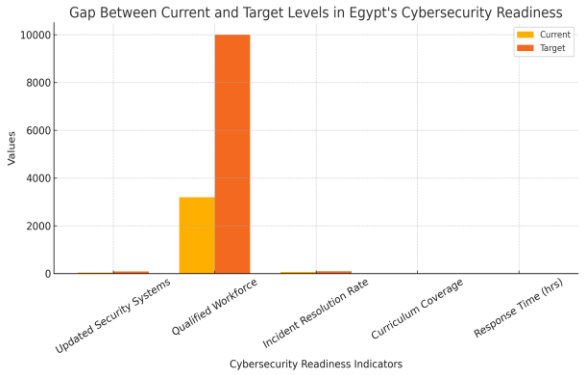
كيان سيادي مستقل يُشرف على التنسيق بين الجهات المعنية، ويُصدر تحذيرات فورية، ويضع سياسات موحّدة لحماية البنية الرقمية للدولة [٢١].

ب. تحديث التشريعات الرقمية

ضرورة إصدار قوانين جديدة تتعلق بـ:

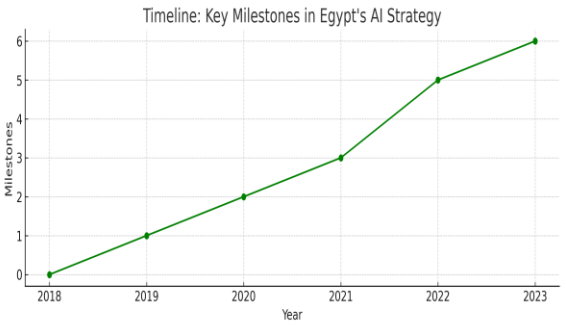
تنسيق مركزي موحد وشبكات اتصال داخلية	تشتت الأدوار والمؤسسات	المؤسسي
ربط الابتكار بالاستراتيجية الوطنية	مبادرات شبابية فردية	الابتكاري
سيادة تقنية وبنى تحتية وطنية	اعتماد كبير على أدوات أجنبية	التكنولوجي

المصدر: إعداد الباحث اعتمادًا على تحليل الوضع المؤسسي المصري (2025).



شكل (٢) :يوضح الفجوه بين الحالي والمستهدف في استعدادات الآمن السيبراني

المصدر: إعداد الباحث اعتمادًا على تحليل الوضع المؤسسي المصري (2025).



شكل (٣) : يوضح معدل الاداء بالنسبه للخطة المستهدفه

المصدر: إعداد الباحث اعتمادًا على تحليل الوضع المؤسسي المصري (2025).

جدول ٦ السيناريوهات المستقبلية للأمن السيبراني في مصر (2025-2030)

السيناريو	الملامح الأساسية	الاحتمالية	التأثير على الأمن القومي
سيناريو متفائل	إنشاء كيان وطني موحّد، تشريعات مرنة، تعليم رقمي شامل	متوسط	تعزيز الردع الرقمي
سيناريو واقعي	تحسين تدريجي في الأدوات والبنية والوعي	مرتفع	استقرار نسبي مع مخاطر مستمرة
سيناريو متدهور	استمرار التشظي وضعف الابتكار المحلي	ضعيف	تهديد مباشر للسيادة الرقمية

المصدر: إعداد الباحث اعتمادًا على تحليل الوضع المؤسسي المصري (2025).

جدول ٧ أبرز التهديدات الرقمية التي تواجه الأمن القومي المصري وتصنيفها

نوع التهديد	التصنيف	مثال واقعي	درجة الخطورة
هجمات الفدية (Ransomware)	تقني	محاولة تعطيل نظام مرفق صحي	مرتفعة
الهندسة الاجتماعية (Social Engineering)	بشري	رسائل احتيالية لسرقة بيانات بنكية	مرتفعة

الذكاء الاصطناعي وأمن البيانات الحساسة.

الخصوصية السيادية للبيانات الحكومية.

الحوسبة السحابية وأمن البنية الافتراضية [٢٧].

ج. تعزيز الابتكار المحلي

دعم الشركات الناشئة التي تعمل في تطوير أدوات الأمن السيبراني.

تمويل مراكز أبحاث متخصصة في الأمن الرقمي والابتكار السيبراني.

توفير حوافز ضريبية للاستثمارات في هذا القطاع [٢٨].

د. إدماج الأمن السيبراني في السياسات التعليمية

إنشاء مسارات أكاديمية متخصصة في الجامعات.

ربط المناهج التعليمية بالتدريب العملي باستخدام أدوات عالمية.

تقديم منح دراسية في مجال الحوسبة الآمنة وتحليل الثغرات [٢٩].

هـ. بناء شبكة إنذار مبكر وتكامل مؤسسي

تطوير منصة رقمية حكومية موحدة لمراقبة وتنبؤ التهديدات السيبرانية.

ربط قواعد البيانات الحكومية في منصة محمية وآمنة.

اعتماد بروتوكولات استجابة موحدة بين الوزارات والمؤسسات الأمنية [٣٠].

٩. خاتمة

يؤكد هذا البحث أن الأمن السيبراني لم يعد مجرد مسألة فنية بل يمثل عنصرًا حاسمًا في أمن الدولة وسلامة بنيتها السيادية، لا سيما في ظل بيئة رقمية متغيرة وتكامل تقني عالمي. ولأن البعد التكنولوجي يُعد خط الدفاع الأول في منظومة الأمن الوطني الحديث، فإن تجاهل تأمينه يُعد مخاطرة استراتيجية. ومن هنا، فإن تبني نهج شامل كـ **PESTELISM**، واستثمار الدولة في القدرات المحلية التشريعية والمؤسسية والتكنولوجية، يُعد ضرورة ملحّة لصياغة أمن قومي رقمي مستدام.

مرتفعة	11 ساعة	أقل من 4 ساعات	سرعة الاستجابة الوطنية للهجمات (بالساعات)

المصدر: إعداد الباحث اعتمادًا على تحليل الوضع المؤسسي المصري (2025)

جدول ٩ علاقة الأمن السيبراني بالأمن القومي عبر القطاعات الحيوية

مدى ارتباطه بالأمن القومي	تأثير الاختراق عليه	القطاع
حرج جدًا	فقدان الثقة، سرقة الأموال	القطاع المصرفي
حرج جدًا	شلل الخدمات، تهديد الحياة	قطاع الطاقة
عالي	تضليل الرأي العام	قطاع الإعلام
متوسط	ضعف الوعي المجتمعي الرقمي	قطاع التعليم
عالي جدًا	تهديد مباشر للسلامة العامة	القطاع الصحي

المصدر: إعداد الباحث اعتمادًا على تحليل الوضع المؤسسي المصري (2025).

جدول ١٠ تحليل PESTELISMلاستراتيجية الأمن السيبراني والذكاء الاصطناعي في مصر

البُعد	الملاحظات الرئيسية في السياق المصري	درجة الخطورة
السياسي	دعم سياسي قوي للتحول الرقمي؛ غياب كيان وطني موحد لإدارة الأمن السيبراني.	متوسطة
الاقتصادي	توسع الاقتصاد الرقمي والتمويل الإلكتروني؛ هشاشة أمام الاحتيال	مرتفعة
متوسطة	نشر إشاعات عبر منصات التواصل	إعلامي	التضليل الإعلامي الرقمي
عالية جدًا	تعطيل خدمات كهرباء أو مياه	استراتيجي	اختراق أنظمة البنية التحتية
متزايدة	التلاعب بقرارات الدولة أو المحتوى	تقني/سياسي	خوارزميات الذكاء الاصطناعي التخريبي

المصدر: إعداد الباحث اعتمادًا على تحليل الوضع المؤسسي المصري (2025).

جدول ٨ مؤشرات الأداء الرئيسية (KPIs)لتقييم جاهزية الأمن السيبراني الوطني

الفجوة	الوضع الحالي (2024)	القيمة المستهدفة	المؤشر
كبيرة	٤٢٪	٩٠٪	نسبة المؤسسات الحكومية ذات أنظمة أمن محدثة
كبيرة	3,200 شخص	10,000 شخص	عدد الكوادر المؤهلة في مجال الأمن السيبراني
متوسطة	٦٦٪	١٠٠٪	عدد الهجمات المُبلّغ عنها والمُعالجة سنويًا
كبيرة	المرحلة الثانوية فقط	كل المراحل	عدد المناهج التعليمية المتضمنة توعية رقمية

	السيبراني وسرقة البيانات المالية.	
الاجتماعي	مشاركة واسعة من الشباب في البيئة الرقمية؛ ضعف الوعي المجتمعي بالممارسات الرقمية الآمنة وانتشار التضليل.	مرتفعة
التكنولوجي	تطور في البنية التحتية (الألياف الضوئية، الحوسبة السحابية)؛ اعتماد مفرط على حلول أمنية أجنبية.	مرتفعة
البيئي	إدماج التكنولوجيا في إدارة الموارد (المياه، الكهرباء)؛ أنظمة عرضة للاختراق والتخريب الرقمي.	متوسطة
القانوني	صدور قوانين لحماية البيانات ومكافحة الجرائم الإلكترونية؛ تطبيق جزئي وبطيء، مع ضعف التحديث التشريعي.	متوسطة
المؤسسي	تشتت الأدوار بين الجهات؛ ضعف التنسيق وغياب منظومة استجابة وطنية موحدة.	مرتفعة
الابتكاري	توفر طاقات بشرية مبدعة في الذكاء الاصطناعي؛ عدم استثمارها بشكل ممنهج ضمن الرؤية الوطنية.	متوسطة
الأمني/العسكري	تطوير وحدات متخصصة داخل القوات المسلحة؛ حاجة ملحة لدمج الأمن السيبراني والذكاء الاصطناعي ضمن العقيدة الدفاعية.	مرتفعة

شرح درجات الخطورة: **منخفضة**: الأوضاع مستقرة وآليات الحماية فعالة. **متوسطة**: توجد جهود لكن بحاجة إلى تعزيز. **مرتفعة**: هناك ثغرات كبيرة أو هشاشة واضحة.

المصدر: إعداد الباحث اعتمادًا على تحليل الوضع المؤسسي المصري (2025).

قائمة المراجع

1. WEF, "Global Cybersecurity Outlook 2023," World Economic Forum, Davos, 2023.

2. ENISA, "Threat Landscape Report 2023," European Union Agency for Cybersecurity, Brussels, 2023.

3. National Telecom Regulatory Authority (NTRA), "Annual Cybersecurity Threats Report - Egypt," Cairo, 2023.

4. Central Bank of Egypt (CBE), "Financial Sector Cybersecurity Performance 2023," Cairo, Egypt, 2023.

5. EG-CERT, "Cyber Emergency Response Team Annual Report," Cairo, 2023.

6. A. Shires, "Cyber Sovereignty in Global Contexts," Journal of Strategic Studies, vol. 18, no. 2, pp. 45-67, 2020.

7. United Nations Institute for Disarmament Research (UNIDIR), "Digital Conflict Risks and Normative Challenges," Geneva, 2021.

8. Ministry of Communications and Information Technology, "Egypt's Digital Transformation Strategy," Cairo, 2022.

9. Cairo University and National Center for Digital Research, "Awareness Gaps in Cyber Hygiene among University Students," Cairo, 2022.

10. H. El-Sayed, "AI and Strategic Sovereignty in the Arab Region," Arab Journal of Digital Studies, vol. 11, no. 1, pp. 77-98, 2023.

11. Supreme Council for Cybersecurity, "Strategic Recommendations for National Coordination in Digital Defense," Cairo, 2024.

12. M. Soliman, "Cybersecurity Threat Modeling in Developing Countries," Information Security Journal, vol. 14, no. 3, pp. 120-135, 2023.

13 A. Abdelrahman, "Legal Gaps in Egyptian Data Protection Laws," Alexandria Law Review, vol. 39, no. 2, pp. 134-149, 2023.

14. Ministry of Defense (Egypt), "Military Doctrine and Cyber Integration Report," Cairo, 2024.

15. OECD, "Cyber Workforce and Talent Development in the MENA Region," Paris, 2023.

16. I. Al-Rashid, "Strategic Cyber Threats in the Middle East," Cyber Strategy Journal, vol. 7, no. 4, pp. 88-107, 2022.

17. A. M. Hassan and S. Badr, "Evaluating Cybersecurity Curriculum in Egyptian Universities," Journal of Digital Education, vol. 10, no. 3, pp. 55-70, 2023.

18. T. Khalil, "Innovation in Local Cyber Defense Startups: A Policy Gap Analysis," Cairo Economic Review, vol. 24, no. 2, pp. 12-29, 2022.

19. Central Bank of Egypt (CBE), "Annual Financial Technology and Risk Bulletin," Cairo, 2023.

20. ENISA, "AI for Threat Detection in Critical Infrastructure," European Union Agency for Cybersecurity, Brussels, 2023.

21. M. El-Kady, "Ransomware Threats and Industrial Espionage in Egypt," International Journal of Cyber Risk, vol. 9, no. 1, pp. 101-119, 2023.

22. Arab Digital Security Forum, "Sovereignty and Foreign Software Risks in Arab National Infrastructure," Amman, 2022.

23. NTRA, "Cybersecurity Governance Challenges in Egypt," Internal Policy Report, Cairo, 2022.

24. Global Risk Institute, "MENA Cyber Readiness Index 2023," Toronto, 2023.

25. ITU, "Measuring Digital Development: Facts and Figures 2023," International Telecommunication Union, Geneva, 2023.

26. A. El-Refai, "National Cybersecurity Councils: Global Models and Egyptian Needs," Cyber Policy Series, vol. 5, pp. 1-22, 2023.

27. Egyptian Parliament, "Draft Law on Artificial Intelligence Governance," Cairo, 2024.

28. Ministry of Planning and Economic Development, "Startups and Innovation Investment Report," Cairo, 2023.

29. Ministry of Higher Education and Scientific Research, "Cybersecurity Education Enhancement Program," Cairo, 2022.

30. EG-CERT, "Recommendations for National Cyber Alert System," Cairo, 2023.