نموذج مطور لتصنيف مستويات التهديدات السيبرانية واستراتيجيات التصدّي الفعالة: من منظور الأمن القومي الليبي

د. طارق رمضان زنبو *
Zanpou@yahoo.com

أ. رنا عبد الرحمن محمد قباصة*
r.gabbasa@zu.edu.ly

المستخلص:

يهدف هذا البحث إلى تقديم نموذج شامل لتصنيف مستويات التهديدات السيبرانية، مع ربط كل مستوى باستراتيجيات تصدّي فعالة، ففي ظل التطور المتسارع للتهديدات السيبرانية تواجه المؤسسات تحديات كبيرة في تقييم هذه التهديدات وتحديد أولويات الاستجابة لها بفعالية، هذه الدراسة تبرز الفجوة في الأدبيات الحالية والمتمثلة في الافتقار إلى إطار موحد ومنهجي يربط بشكل ديناميكي مستويات التهديد باستراتيجيات الاستجابة المناسبة، وتعتمد الدراسة منهجية وصفية تحليلية ومنهج بناء النموذج، حيث يتم تحليل الأدبيات السابقة لتحديد المكونات الأساسية للتهديدات السيبرانية ومعايير تصنيفها، ثم يتم تصميم نموذج مقترح يقدم تصنيفاً هرمياً للتهديدات (منخفض، متوسط، عالٍ، عالٍ جداً، حرج)، ويربطها بإجراءات اكتشاف ومعالجة محددة. تناقش الدراسة فعالية النموذج في تحسين قدرة المؤسسات على تقييم المخاطر السيبرانية وترشيد تخصيص الموارد، مع الأخذ في الاعتبار التحديات المرتبطة بالتنفيذ وديناميكية التهديدات. توصي الدراسة المؤسسات بتبني إطار عمل منهجي لإدارة التهديدات، والاستثمار في استخبارات التهديدات السيبرانية، وتطوير خطط استجابة متدرجة، وتوفير تدريب مستمر للموظفين، كما تقدم الدراسة توصيات للباحثين المستقبليين لإجراء تحقق عملي لفاعلية النموذج وتطوير أدوات آلية لدعمه، حيث تساهم هذه الدراسة في بناء أساس نظري متين يمكن أن يعزز مرونة الأمن السيبراني في مواجهة التحديات المتزايدة.

الكلمات المفتاحية: أمن سيبراني، تهديدات سيبرانية، تصنيف التهديدات، استراتيجيات التصدي، إدارة المخاطر السيبرانية، نموذج مقترح.

---

* د. طارق رمضان زنبو، مدير المركزِ القومي للبحوث والدراسات العلمية، رئيس اللجنة العلمية بالمركز.
* أ. رنا عبد الرحمن محمد قباصة، عضو هيئة التدريس بقسم تحليل البيانات بكلية الاقتصاد، جامعة الزاوية.

Abstract:

This study aims to propose a comprehensive model for classifying cyber threats levels, linking each level with effective countermeasures. In light of the rapid evolution of cyber threats, organizations face significant challenges in assessing these threats and prioritizing their responses effectively. This study highlights a gap in current literature, which is the lack of a unified and systematic framework that dynamically links threats levels with appropriate response strategies. The study adopts a descriptive-analytical methodology and a model-building approach, where previous literature is analyzed to identify the basic components of threats and their classification criteria. Then, a proposed model is designed to provide a hierarchical classification of threats (low, medium, high, very high (critical) and links them to specific detection and treatment procedures. The study discusses the model's effectiveness in improving organizations' ability to assess cyber risks and rationalize resource allocation, considering the challenges associated with implementation and the dynamic nature of threats. The study recommends that organizations to adopt a systematic framework for threat management, invest in cyber threats intelligence, develop tiered response plans, and provide continuous training for employees, It also offers recommendations for future researchers to practically verify the model and develop automated tools to support it. This study contributes to building a solid theoretical foundation that can enhance cybersecurity resilience in the face of increasing challenges.

Keywords: Cybersecurity, Cyber Threats, Threat Classification, Countermeasures, Cyber Risk Management, Proposed Model.

مقدمة

يشهد عالمنا اليوم تحولاً رقمياً غير مسبوق، خاصة مع النمو المتواصل للاتصالات وتبادل البيانات عبر الإنترنت، وأصبحت أنظمة المعلومات والاتصالات العمود الفقري لأي منظمة أو مؤسسة، ومع ازدياد الاعتماد على التكنولوجيا كجزء لا يتجزأ من حياتنا، أدى ذلك إلى ظهور تحديات أمنية معقدة تُعرف **بالتهديدات السيبرانية**، والتي تستهدف سرقة البيانات، وتعطيل العمليات، والتجسس الصناعي، ولم تعد هذه التهديدات مجرد حوادث فردية عابرة، بل تحولت إلى عاصفة رقمية حقيقية قادرة على زعزعة الاستقرار، وتكبد خسائر فادحة، وحتى تهديد للأمن القومي والاستقرار الاقتصادي؛ إن مشهد الهجمات السيبرانية يتغير بلمح البصر، فما كان يشكل تهديداً بالأمس قد لا يكون هو نفسه اليوم، وما يبدو بسيطاً قد يخفي وراءه تعقيدات هائلة؛ هذا التطور المستمر، من البرمجيات الخبيثة المتطورة إلى حملات التصيد الاحتيالي شديدة الإتقان، يجعل من التصنيف الدقيق لمستويات التهديد أمراً حيوياً،

فكيف يمكننا وضع استراتيجيات دفاعية فعالة إذا لم نفهم قوة وطبيعة الهجوم الذي نواجهه؟ وكيف يمكننا توجيه جهودنا الاستباقية وتخصيص مواردنا الثمينة في عالم يتسم بالغموض والسرعة؟

من هنا، تبرز الحاجة الملحة لتطوير نموذج يصنف مستويات التهديدات السيبرانية، لا يكون مجرد أداة نظرية، بل دليلاً عملياً يمكن للمؤسسات والأفراد على حد سواء الاعتماد عليه؛ لن يقتصر هذا النموذج على مجرد فهم التهديدات، بل سيمتد ليشمل استراتيجيات تصدٍّ مبتكرة وفعالة تتناسب مع كل مستوى من مستويات التهديد؛ فالهدف هو بناء درع رقمي حصين، يمكن من خلاله ليس فقط مقاومة العواصف السيبرانية، بل توقعها والاستعداد لها، وتحويل التحديات إلى فرص لتعزيز أمننا الرقمي وحماية مقدرات الأمة والأمن القومي الليبي في هذا الفضاء المتشابك.

2. مشكلة الدراسة:

في ظل التطور المتسارع للتهديدات السيبرانية وتعقيداتها المتزايدة، والذي ألقى بظلاله على قدرة المؤسسات على تقييم هذه التهديدات وتحديد أولويات التصدّي لها بفعالية، فإنه على الرغم من الجهود المبذولة لتطوير آليات دفاعية واستراتيجيات أمنية، لا يزال هناك قصور واضح في تطوير نموذج شامل ومعياري لتصنيف مستويات التهديدات السيبرانية يراعي التطور المستمر لهذه التهديدات، فغالباً ما تعتمد المؤسسات على تصنيفات مبسطة أو غير متكاملة، لا تمكنها من التمييز الدقيق بين التهديدات المختلفة بناءً على شدتها، وتأثيرها المحتمل، وتعقيدها؛ يؤدي هذا القصور بدوره إلى صعوبة في تحديد الأولويات الأمنية وتخصيص الموارد بكفاءة، واتخاذ قرارات وقائية واستباقية فعالة، فالاستجابة لتهديد عالي الخطورة بنفس مستوى الاستجابة لتهديد بسيط قد يؤدي إلى استنزاف الموارد، أو على النقيض، التقليل من شأن أي تهديد قد تكون له عواقب كارثية.

بناءً عليه، تتمحور مشكلة هذه الدراسة في "الافتقار إلى إطار عمل تصنيفي موحد وديناميكي لمستويات التهديدات السيبرانية، يقترن باستراتيجيات تصدٍّ واضحة ومحددة لكل مستوى، هذا الافتقار يعيق القدرة على الاستجابة الفعالة للتهديدات، ويحد من إمكانية الوقاية الاستباقية من المخاطر السيبرانية المتنامية والمتطورة باستمرار".

بناءً على ما سبق، تتمحور مشكلة الدراسة في الإجابة على **التساؤل الرئيسي التالي:**

"كيف يمكن تطوير نموذج لتصنيف مستويات التهديدات السيبرانية، وتحديد استراتيجيات التصدّي الفعّالة المرتبطة بكل مستوى، بما يساهم في تعزيز القدرة على إدارة المخاطر السيبرانية بشكل استباقي وموجه؟".

3. أهداف الدراسة:

تهدف هذه الدراسة إلى تحقيق مجموعة من الأهداف الرئيسية التي تسهم في بناء نموذج مقترح لتصنيف مستويات التهديدات السيبرانية واستراتيجيات التصدّي لها، يمكن تلخيص هذه الأهداف كما يلي:

- تحديد وجمع المكونات الأساسية للتهديدات السيبرانية، وذلك عبر تحليل الأدبيات المتخصصة لتحديد أبرز العناصر التي تسهم في تحديد مستوى خطورة التهديد، مثل نوع الهجوم، الجهة المهاجمة، الأهداف المحتملة، والتأثير المتوقع.
- تطوير نموذج نظري يوفر تصنيفاً واضحاً ومتدرجاً للتهديدات السيبرانية، يمكن الاعتماد عليه لتقييم المخاطر بشكل دقيق.
- اقتراح مجموعة من استراتيجيات التصدّي الوقائية والاستجابية التي تتناسب مع كل مستوى من مستويات التهديد المصنفة، وذلك لتقديم خارطة طريق عملية لإدارة الأمن السيبراني.
- بناء قاعدة معرفية ومفاهيمية يمكن أن تفتح المجال أمام دراسات وأبحاث مستقبلية أكثر تخصصاً في مجال الأمن السيبراني، وتطوير أدوات عملية لتطبيق النموذج المقترح.

4. أهمية الدراسة:

تنبع أهمية الدراسة من الحاجة الملحة لمعالجة الثغرات الحالية في إدارة الأمن السيبراني، وتقديم حلول عملية تساهم في تعزيز مرونة الأنظمة الرقمية وقدرتها على الصمود أمام الهجمات المتزايدة، ويمكن تلخيصها في النقاط التالية:

الأهمية العلمية:

- تسعى الدراسة إلى سد فجوة علمية واضحة في الأدبيات العلمية المتعلقة بتصنيف التهديدات السيبرانية، بشكل ديناميكي وشامل يربط بين التصنيف والاستراتيجيات العملية للتصدّي، مما يفتح آفاقاً لدراسات مستقبلية في هذا المجال.

- تسهم الدراسة في تقديم نموذج تصنيفي مبتكر لمستويات التهديدات السيبرانية، مما يمكّن الجهات المعنية (المؤسسات الحكومية، الشركات الخاصة، وحتى الأفراد) من فهم طبيعة التهديدات التي تواجهها بشكل أعمق وأكثر دقة، وتصنيفها بناءً على معايير واضحة وشاملة.

الأهمية العملية:

- تسعى الدراسة إلى تحسين كفاءة الاستجابة الأمنية للحوادث من خلال ربط كل مستوى من مستويات التهديد باستراتيجيات تصدٍّ فعالة ومحددة، سيوفر النموذج المقترح خارطة طريق واضحة للاستجابة السريعة والفعّالة للهجمات السيبرانية، وتقييم مستوى التهديد (مثل مؤشرات الشدة والتكرار)، مما يمكّن فرق الأمن السيبراني من تحديد أولويات الاستجابة بدقة، ويحد من الأضرار المحتملة.
- سيمكن النموذج المقترح صانعي القرار من تخصيص الموارد الأمنية (تقنية، مادية، بشرية) بشكل أكثر كفاءة وفعالية، وتوجيهها نحو التهديدات الأكثر خطورة أو ذات الأولوية القصوى، بدلاً من التوزيع العشوائي الذي قد يؤدي إلى هدر الموارد أو ضعف الحماية في نقاط حرجة؛ تشير البيانات إلى أن 60% من الاختراقات يمكن تجنبها بوجود تصنيف استباقي[1].
- يقدم النموذج المطور إطاراً موحداً يمكن تطبيقه للقطاعات المختلفة، مما يسهل التعاون في مواجهة التهديدات السيبرانية العابرة للحدود.

5. فرضية الدراسة:

بناءً على مشكلة الدراسة وأهدافها، يمكن صياغة الفرضية الرئيسية للدراسة على النحو التالي:

"إن تطوير نموذج نظري شامل لتصنيف مستويات التهديدات السيبرانية، والذي يحدد بوضوح استراتيجيات التصدّي الفعالة المرتبطة بكل مستوى، سيمكن المؤسسات من تحسين قدرتها على تقييم المخاطر السيبرانية بشكل فعّال واستباقي، وبالتالي تعزيز صمودها الأمني في مواجهة الهجمات المتطورة".

---

(1) Ahmed, Ali, Saad Khan, and Abdullah Al-Ghamdi. "A Proposed Classification Model for Cyber Threats Based on Severity and Impact." Journal of Cybersecurity Research 5, no. 2 (2019): 123–35.

6. الإطار النظري (المفاهيم الأساسية):

لفهم أعمق للنموذج المقترح لتصنيف مستويات التهديدات السيبرانية واستراتيجيات التصدّي الفعّالة، من الضروري استعراض المفاهيم الأساسية التي تشكل ركيزة هذه الدراسة، تضع هذه المفاهيم الإطار النظري الذي يُبنى عليه التحليل والتصنيف.

تعريف الأمن السيبراني (Cybersecurity):

الأمن السيبراني هو نظام أو مجموعة من التقنيات والسياسات والممارسات المصممة لحماية الأنظمة والشبكات والأجهزة والبرامج والبيانات من الهجمات الرقمية أو التلف أو الوصول غير المصرّح به، يتضمن ذلك تطبيق تدابير لحماية البنية التحتية الرقمية وتأمين البيانات الحسّاسة، سواء كانت تتعلق بمعلومات شخصية أو مالية أو حكومية[1].

يهدف الأمن السيبراني إلى ضمان سرية وتكامل وتوافر المعلومات والأنظمة (CIA Triad)، وهو ما يُعد حجر الأساس في أي بيئة رقمية آمنة.

تعريف التهديد السيبراني (Cyber Threat):

التهديد الأمني السيبراني هو أي خطر أو نشاط ضار، يهدف إلى سرقة البيانات أو الأموال، وإلحاق الضرر بنظام أو شبكة، أو تخريب البيانات أو أنظمة الكمبيوتر، أو تعطيل العمليات التجارية الحيوية والحياة الرقمية بشكل عام؛ يمكن أن تتراوح التهديدات السيبرانية من محاولات اختراق بسيطة إلى هجمات معقدة ذات دوافع إجرامية أو سياسية أو اقتصادية، وتتسم هذه التهديدات بالديناميكية والتطور المستمر، مما يتطلب استراتيجيات دفاعية مرنة ومتجددة[2].

---

(1) Al-Hawari, Mohammad, Majdi Al-Rousan, and Ahmad Al-Shami. "A Classification of Cyber Threats Based on Attack Nature and Targeted Objectives." International Journal of Computer Science and Network Security 18, no. 10 (2018): 123-30.

(2) Hussain, Ahmad, Muhammad A. Khan, and Rashid Ahmad. "Cyber Threat Intelligence: Challenges and Solutions." Journal of Information Security and Applications 40 (2018): 147-57.

تعريف الهجمات السيبرانية (Cyberattack):

هي أي هجوم ضار أو محاولات خبيثة لاختراق أنظمة المعلومات والاتصالات بهدف الوصول غير القانوني إلى البيانات، وتعطيل العمليات الرقمية، أو إتلاف المعلومات، يقوم بها قراصنة، أو جواسيس شركات، أو جماعات إرهابية، أو دول، أو حتى موظفين داخليين .Kontaxis, G.et (2016)[1].

فبينما يمثل التهديد إمكانية الخطر، فإن الهجوم السيبراني هو الفعل العملي لتنفيذ التهديد؛ وتتنوع الهجمات السيبرانية بشكل كبير لتشمل هجمات الفدية (Ransomware)، وهجمات حجب الخدمة الموزعة (DDoS)، والتصيد الاحتيالي (Phishing)، واستغلال ثغرة أمنية معينة، والبرمجيات الخبيثة (Malware)، وهجمات الهندسة الاجتماعية[2].

الفرق بين التهديد السيبراني والهجوم السيبراني:

التهديد السيبراني غير نشط (Potential) قد يكون موجوداً دون أن يتحول إلى فعل ضار، أما الهجوم فهو نشط (Active)، فالهجوم السيبراني هو التنفيذ الفعلي لاستغلال التهديدات لاختراق الأنظمة أو سرقة البيانات أو تعطيل الخدمات، وكمثال على ذلك:

- وجود ثغرة في نظام تشغيل **(تهديد)** واستغلال هذه الثغرة من قبل هاكر لسرقة بيانات **(هجوم)**.
- إمكانية وصول موظف داخلي إلى بيانات حسّاسة **(تهديد)** وقيام الموظف بتسريب أو ببيع البيانات **(هجوم)**، بالتالي، التهديد السيبراني يشير إلى الخطر المحتمل، بينما الهجوم السيبراني هو التنفيذ الفعلي لهذا الخطر.

إدارة المخاطر السيبرانية (Cyber Risk Management):

(1) Kontaxis, Georgios, Michalis Polychronakis, and Evangelos P. Markatos. "A Taxonomy of Cyber Threats for Critical Infrastructures." In Proceedings of the 11th International Conference on Critical Information Infrastructures Security (CRITIS 2016), 1–15. Springer, 2016.

(2) Al-Shammari, Fahad, and Ahmad Al-Mubarak. "Evaluating the Effectiveness of Cybersecurity Strategies in Protecting Critical Infrastructure in GCC Countries." Journal of Information Security 15, no. 4 (2021): 301–15.

تُعرف إدارة المخاطر السيبرانية بأنها: "العملية المنهجية لتحديد، تقييم، ومعالجة، ومراقبة المخاطر المرتبطة بالتهديدات السيبرانية"، تتضمن هذه العملية فهم الأصول الرقمية، وتحديد التهديدات ونقاط الضعف، وتقدير احتمالية وقوع الهجوم وتأثيره، ثم اتخاذ الإجراءات اللازمة لتقليل هذه المخاطر إلى مستوى مقبول؛ وتهدف الإدارة الفعالة للمخاطر السيبرانية إلى تمكين المؤسسات من اتخاذ قرارات مستنيرة بشأن استثماراتها في الأمن السيبراني[1].

استراتيجيات التصدّي (Countermeasures/Response Strategies):

تشير استراتيجيات التصدّي إلى الإجراءات والخطوات المتخذة للتعامل مع التهديدات والهجمات السيبرانية، سواء كان ذلك وقائياً (قبل وقوعها)، أو أثناءها (استجابياً)، أو بعدها (تعافياً)، تشمل هذه الاستراتيجيات مجموعة واسعة من التدابير التقنية مثل: جدران الحماية، وأنظمة كشف الاختراق، والإجراءات الإدارية مثل: وضع سياسات وتدريب أمني، وخطط تشغيلية للاستجابة للحوادث والتعافي من الكوارث[2].

تهدف هذه الاستراتيجيات إلى تقليل تعرض الأنظمة للخطر، واكتشاف الهجمات مبكراً، واحتوائها، واستعادة العمليات الطبيعية في أسرع وقت ممكن.

7. أهداف الأمن السيبراني:

يمكن ابراز أهم أهداف الأمن السيبراني فيما يلي:

1. الحفاظ على سرية البيانات: يشير مفهوم الحفاظ على سرية البيانات إلى منع الكشف غير المصرّح به عن المعلومات، وضمان عدم وصولها إلى أشخاص غير مخوّلين، مع تمكين المستخدمين المُعتمدين من الوصول إليها بشكل آمن، ولتحقيق هذا الهدف في الأمن السيبراني، تُستخدم الأدوات والآليات التالية[3]:

(1) Smith, John, and Alice Jones. "The Impact of Artificial Intelligence on Evolving Cyber Threats and Defense Strategies." AI in Cybersecurity Journal 2, no. 1 (2023): 1–15.

(2) Ahmad. Khan and Ahmad. "Cyber Threat Intelligence: Challenges and Solutions." 147–57.

(3) المصدر: المؤسسة العامة للتدريب التقني والمهني، بدون تاريخ.

- **التشفير**: وهو تقنية تحويل البيانات إلى صيغة غير قابلة للقراءة باستخدام خوارزميات ومفاتيح سرية، لا يمكن فك تشفير البيانات إلا باستخدام المفتاح المناسب، مما يضمن حماية المعلومات الحسّاسة مثل: بيانات البطاقات الائتمانية أو المراسلات الخاصة، أو المعلومات الاستخبارية.
- **مراقبة الوصول**: هي مجموعة من القواعد والإجراءات التي تحدد صلاحية الوصول إلى الأنظمة أو الموارد المادية والافتراضية، يتم منح الامتيازات بناءً على بيانات اعتماد المستخدم (مثل اسم المستخدم أو رقم الجهاز).
- **المصادقة**: هي عملية التحقق من هوية المستخدم قبل منحه صلاحية الوصول إلى البيانات أو الأنظمة المحمية، وتشمل أمثلة المصادقة: كلمات المرور، والبصمة الحيوية، والتحقق بخطوتين.
- **التفويض**: هو آلية تقييم صلاحية المستخدم أو النظام للوصول إلى موارد محددة (مثل الملفات أو قواعد البيانات)، بعد التحقق من هويته، بناءً على سياسات التحكم في الوصول.
- **الأمن المادي**: هو حماية الأصول الملموسة مثل المباني والمعدات والموظفين من الوصول غير المصرّح به، مما يساهم بشكل غير مباشر في حماية البيانات المخزنة على قواعد البيانات.

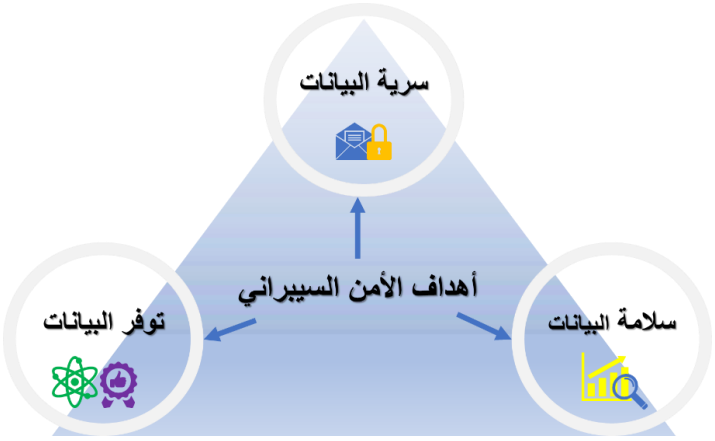
2. **الحفاظ على سلامة البيانات**: يهدف هذا الجانب إلى ضمان دقة وموثوقية البيانات، ومنع التعديلات غير المصرّح بها، الأدوات المستخدمة لتحقيق سلامة البيانات تشمل:

- **النسخ الاحتياطي**: هو عملية نسخ البيانات بشكل دوري إلى موقع آمن لاستعادتها في حال فقدان النسخ الأصلية أو تلفها.
- **تدقيق المجموع**: هو تقنية للتحقق من سلامة الملفات أو البيانات المنقولة عبر حساب قيم رقمية فريدة (Checksums) ومقارنتها لاكتشاف أي تغييرات.
- **تصحيح الأخطاء التلقائي**: هو آليات تسمح باكتشاف التعديلات غير المصرّح بها وإصلاحها تلقائياً باستخدام رموز تصحيح الأخطاء.

3. **ضمان توفر البيانات**: يعني هذا المبدأ ضمان إتاحة البيانات والخدمات للمستخدمين المصرّح لهم في الوقت المناسب وبشكل موثوق، الأدوات الداعمة لضمان توفر البيانات تشمل:

- **الحماية المادية للبنية التحتية:** هو ضمان استمرارية عمل الأنظمة عبر تأمين مراكز البيانات والشبكات من الأعطال أو الكوارث.
- **تكرار البيانات والأنظمة:** هو إنشاء نسخ احتياطية متعددة للموارد الحرجة لضمان استمرارية الوصول حتى في حال حدوث أعطال.

ويمكن توضيح أهم أهداف الأمن السيبراني في الشكل التالي:



شكل رقم (1): يوضح أهداف الأمن السيبراني

المصدر: من إعداد الباحِثَيْنِ.

8. أهمية الأمن السيبراني:

تتجلى أهمية الأمن السيبراني في جوانب متعددة، يمكن إيجازها فيما يلي:

أ- **حماية البيانات:** يشمل الأمن السيبراني التدابير اللازمة لحماية البيانات الحساسة، سواء كانت شخصية، حكومية، صناعية، أو حقوق ملكية فكرية، من الوصول غير المصرح به والاستغلال الضار من قبل المهاجمين المتخصصين.

ب- **حماية البنية التحتية الحيوية:** تلعب حلول الأمن السيبراني دوراً حيوياً في حماية البنى التحتية الحيوية، مثل: المستشفيات، والمؤسسات المالية، والمؤسسات الأمنية والعسكرية، التي يعتمد عليها المجتمع بأكمله من التهديدات الإلكترونية.

ج- **الحد من المخاطر الفردية:** يساهم الأمن السيبراني في تقليل المخاطر التي يتعرض لها الأفراد، مثل سرقة الهوية، والابتزاز الإلكتروني، والتي قد تتسبب في أضرار جسيمة لحياتهم.

د- **ضمان استمرارية الأعمال:** يضمن الأمن السيبراني استمرارية الأعمال والخدمات من خلال حماية الأنظمة والشبكات من الهجمات الإلكترونية التي قد تعطل العمليات وتؤدي إلى خسائر مالية وسمعة.

هـ- **الامتثال للوائح:** ممارسات الأمن السيبراني تفرض على المؤسسات الامتثال للوائح، فجميع المؤسسات بحاجة إلى حماية أصولها، وضمان أمن وخصوصية معلومات عملائها، ولذلك يجب عليها الالتزام بالامتثال للوائح في مجال الأمن السيبراني، باتخاذ عدة تدابير مثل: التقييمات الأمنية المنتظمة، وتدريب الموظفين على أفضل الممارسات الأمنية، واستخدام التكنولوجيا الآمنة مثل جدران الحماية والتشفير.

بالتالي أصبح الأمن السيبراني ضرورة حتمية لجميع القطاعات، بدءاً من الحكومات والمؤسسات المالية وصولاً إلى الشركات الصغيرة والأفراد؛ يشمل نطاق الأمن السيبراني حماية البنية التحتية الحيوية، وأنظمة التحكم الصناعي، والشبكات الحكومية، والبيانات الشخصية، والملكية الفكرية.

9. الأمن السيبراني في البيئة الليبية:

- **مفهوم الأمن السيبراني في البيئة الليبية:**

يُعرَّف الأمن السيبراني في ليبيا بأنه "مجموعة الإجراءات والتقنيات التي تهدف إلى حماية الشبكات الوطنية، والبيانات الحكومية، ومقدمي الخدمات الأساسية، من الهجمات الرقمية التي قد تعرض وحدة الوطن واستقراره للخطر؛ برز هذا المفهوم بقوة في العقدين الأخيرين من الزمن في ليبيا، حيث أظهرت تجربة قطع الإنترنت وإغلاق شبكات الاتصالات أن التحكم المركزي في البنية التحتية للاتصالات أصبح أداة لتقييد الحريات السياسية والعامة.

- **الأمن السيبراني والأمن القومي الليبي:**

يُعدّ الأمن السيبراني جزءاً لا يتجزأ من الأمن القومي الليبي، نظراً لتزايد الاعتماد على التكنولوجيا الرقمية في إدارة الدولة وتقديم الخدمات العامة، فالأمن القومي هو المفهوم الذي يشير إلى "قدرة الدولة على حماية نفسها من التهديدات الداخلية والخارجية"، كان هذا يشمل الحماية العسكرية والدبلوماسية

والاقتصادية، وفي القرن الحادي والعشرين، توسع تعريف الأمن القومي ليشمل أبعاداً جديدة، أبرزها البعد السيبراني.

تتضمن عناصر الأمن القومي الحديثة ما يلي[1]:

- **الحماية العسكرية:** الدفاع عن الحدود والمصالح الوطنية.
- **الاستقرار الاقتصادي:** ضمان النمو والازدهار الاقتصادي.
- **الاستقرار السياسي:** الحفاظ على أنظمة الحكم الرشيد والمؤسسات الديمقراطية.
- **الأمن السيبراني:** حماية البنية التحتية الرقمية الحيوية والمصالح الوطنية في الفضاء السيبراني.

تواجه البلاد تحديات أمنية معقدة، تشمل التهديدات السيبرانية هجمات على البنية التحتية الحيوية مثل: شبكات الكهرباء والاتصالات، والمؤسسات الحكومية والمالية، بالإضافة إلى محاولات التدخل في العمليات السياسية والانتخابية، هذه التهديدات لا تقتصر على جهات داخلية، بل تمتد لتشمل تهديدات خارجية من دول أو منظمات تسعى لزعزعة الاستقرار أو التأثير على السياسات الوطنية وفقاً لتقارير وكالة الأنباء الليبية خلال سنتي 2024، 2025.

وقد أكد السيد "عبد الحكيم عنيبة"، مدير المركز الليبي للمنظومات الإلكترونية والبرمجيات وبحوث الطيران، على الدور المحوري للأمن السيبراني في حماية أسرار الدولة ومعلوماتها الحّساسة، مشدّداً على ضرورة نشر الوعي بين المسؤولين والموظفين للتعامل مع الاختراقات المحتملة.

ليبيا تواجه تحديات كبيرة في بناء منظومة سيبرانية فعّالة، أبرزها غياب خطط أمنية متكاملة لحماية الاستثمارات الرقمية، مما يؤدي إلى خسائر مادية وتشغيلية كبيرة، تشمل التهديدات المتنوعة "هجمات الفدية الإلكترونية، وهجمات حجب الخدمة الموزعة (DDoS)، فضلًا عن الهجمات الموجهة ضد البنية التحتية الحيوية".

في ضوء هذه التحديات، أصبح تطوير القدرات الوطنية في مجال الأمن السيبراني أولوية استراتيجية، يتطلب ذلك:

(1) حسن، أحمد طارق. "الأمن السيبراني وتداعياته على الأمن القومي المصري" مجلة كلية التربية، جامعة عين شمس، 2024.

- **إنشاء مؤسسات متخصصة:** يجب تأسيس جهات متخصصة في الأمن السيبراني.
- **وضع استراتيجية وطنية شاملة:** لا بد من تطوير خطة وطنية متكاملة لمواجهة التهديدات السيبرانية.
- **بناء القدرات البشرية والتقنية:** من الضروري الاستثمار في الكوادر البشرية وتطوير التقنيات اللازمة.
- **تعزيز التعاون الدولي:** يجب تعزيز التعاون الدولي وتبادل المعلومات حول التهديدات السيبرانية وأفضل الممارسات.
- **الأمن السيبراني والاقتصاد الليبي:**

يُمثل الأمن السيبراني عاملاً حاسماً في حماية الاقتصاد الليبي وتعزيز نموه المستدام، خاصة في ظل التوسع المتسارع للتحول الرقمي، وتزداد أهمية هذا الدور بازدياد المخاطر السيبرانية التي تهدد الاستقرار الاقتصادي وتؤثر على مسارات النمو، ويبرز القطاع المصرفي والمالي والأمني كأكثر القطاعات عرضة للتهديدات السيبرانية، حيث يمكن للهجمات الناجحة أن تتسبب في خسائر مالية جسيمة وتؤدي إلى فقدان الثقة في النظام العام للدولة، مما يؤثر سلباً على سلامة المعاملات والعلاقات واستقرار السوق.

وفي ضوء هذه المعطيات، يواجه الاقتصاد الليبي تحدياتِ إضافية نابعة من الاعتماد الكبير على قطاع النفط والغاز، الذي يُعد هدفاً استراتيجياً للهجمات السيبرانية، وقد تؤدي الهجمات على أنظمة التحكم الصناعي في المنشآت النفطية إلى توقف الإنتاج وخسائر اقتصادية فادحة، مما يجعل تأمين هذه المنشآت الحيوية ضرورة اقتصادية وأمنية قصوى. كما يؤثر مستوى الأمن السيبراني بشكل مباشر على جاذبية ليبيا للاستثمارات الأجنبية، حيث يبحث المستثمرون عن بيئات آمنة ومستقرة لاستثماراتهم؛ لذا، فإن تطوير القدرات السيبرانية وإنشاء إطار تنظيمي قوي يعزز الثقة في الاقتصاد الليبي ويحفز الاستثمارات الاجنبية، خاصة في قطاعات التكنولوجيا والخدمات المالية؛ وتشير الدراسات إلى أن المصارف التجارية الليبية تدرك أهمية تطبيق الأمن السيبراني المحاسبي لحماية البيانات المالية

الحساسة، وتعزيز الثقة والمصداقية، وتقليل المخاطر، وضمان الامتثال للمعايير الأمنية[1]، ومع ذلك، تواجه هذه المصارف تحديات وعقبات كبيرة في التطبيق الفعّال لهذه المعايير.

ولمواجهة هذه التحديات، تُوصي الدراسات بضرورة تنظيم برامج تدريبية دورية لموظفي المصارف لتعزيز وعيهم بأحدث التهديدات السيبرانية وأفضل الممارسات الأمنية، والاستثمار في تقنيات الأمن السيبراني المتطورة، وتحديث الأنظمة بشكل مستمر لمواكبة التطورات التكنولوجية والمخاطر الجديدة، كما يُعد تعزيز التعاون بين المصرف المركزي والجهات الحكومية لتبادل المعلومات والخبرات في هذا المجال أمر بالغ الأهمية لدعم الجهود المشتركة نحو تحقيق أمن سيبراني فعّال.

10. الأمن السيبراني وأمن المعلومات والاتصالات:

غالباً ما تُستخدم مصطلحات الأمن السيبراني وأمن المعلومات وأمن الاتصالات بالتبادل، ولكن هناك فروق دقيقة ومهمة بينها:

- **أمن المعلومات (Information Security):** يُعد أمن المعلومات المظلة الأوسع التي تهدف إلى حماية المعلومات بجميع أشكالها، سواء كانت رقمية أو ورقية أو مرئية أو سمعية، يركز أمن المعلومات على ضمان سرية وسلامة وتوافر المعلومات (CIA Triad) بغض النظر عن وسيلة تخزينها أو نقلها[2]. يشمل ذلك حماية الوثائق المهمة، والتحقق من هوية الأشخاص المصرح لهم بالوصول، ومواجهة التهديدات الداخلية والخارجية، ومراقبة أمن البيانات.
- **الأمن السيبراني (Cybersecurity):** يُعد الأمن السيبراني جزءاً من أمن المعلومات، ويركز بشكل خاص على حماية الأنظمة والشبكات والأجهزة والبرامج والبيانات الرقمية من الهجمات الإلكترونية في الفضاء السيبراني، يهدف إلى حماية كل ما هو متصل بالإنترنت والإلكترونيات، مثل أجهزة الكمبيوتر،

(1) التائب، عقيلة محمد، وجمعة عمر السائح. "أهمية تطبيق الأمن السيبراني المحاسبي في المصارف التجارية الليبية: دراسة تطبيقية على المصارف التجارية العاملة في مدينة سرت." مجلة الدراسات الاقتصادية 8، 1. (2025).

(2) القاسم، أحمد سالم سعد، وأحمد محمد سالم حسين. "واقع مخاطر أمن نظم المعلومات المحاسبية الإلكترونية بالمصارف التجارية الليبية العاملة بمدينة البيضاء"، 25–55. مركز السنابل للبحث وتطوير الموارد البشرية ومركز بيان للهندسة المالية والإسلامية، 2017.

وأنظمة السيارات، والطائرات المسيرة؛ يشمل ذلك إعداد كلمات مرور قوية، وتحديث البرامج، ومعرفة التطبيقات المشبوهة، والتأكد من الروابط الآمنة.

- **أمن الاتصالات (Communication Security)**: يركز أمن الاتصالات على حماية المعلومات أثناء نقلها عبر الشبكات والقنوات المختلفة، يشمل ذلك تقنيات التشفير لضمان سرية البيانات أثناء الإرسال، وآليات التحقق من الهوية لضمان أن المرسل والمستقبل هما من يدعيان، وحماية البنية التحتية للاتصالات من الهجمات التي قد تعطل الخدمة أو تتجسس على البيانات.

بالتالي فإن أمن المعلومات هو المفهوم الشامل لحماية البيانات، والأمن السيبراني هو جزء منه يركز على الحماية في البيئة الرقمية، بينما أمن الاتصالات يضمن سلامة المعلومات أثناء انتقالها، وتعمل هذه المجالات الثلاثة معاً بشكل متكامل لتوفير حماية شاملة للأصول الرقمية والمعلوماتية للمؤسسات والأفراد.

في ليبيا ووفقاً لتقارير وكالة الأنباء الليبية سنة 2025، يشهد المشهد الرقمي تحولاً متسارعاً، مما يجعل الأمن السيبراني ضرورة ملحة لحماية البنية التحتية الحيوية والمؤسسات والبيانات، ومع ذلك، تواجه البلاد تحديات فريدة بسبب الظروف السياسية والاقتصادية التي تؤثر على قدرتها على تطوير دفاعات سيبرانية فعالة.

قبل عام 2011، كانت جميع قنوات الإنترنت تصبّ في بوابة واحدة مملوكة لشركة Libyan Technology (LTT) & Telecom، وهي شركة تابعة مباشرة للدولة، ما جعلها هدفاً سهلاً للاختراق وللإغلاق الشامل، وخلق وضع هش يتسم بما يلي:

أ- الاعتماد الكامل على بوابة إنترنت واحدة.

ب- غياب تكرار الشبكات والمسارات البديلة (Redundancy) في المنطقة الشرقية والغربية.

ج- استخدام أنظمة مراقبة أجنبية (Amesys Eagle وZTE ZXMT) سمحت بالتنصت على 98% من حركة الإنترنت الواردة والصادرة.

د- الرقابة المركزية على تدفق المعلومات.

هـ- عدم وجود استراتيجية واضحة لتنويع البنية التحتية.

ومواجهةً لهذه الهشاشة الرقمية برزت الحاجة إلى إطار تنظيمي وتشريعي فاعل، وقد شهدت السنوات الأخيرة ظهور عدة مؤسسات وهيئات تهدف إلى معالجة هذه الثغرات، من أبرزها:

أ- **الهيئة الوطنية لأمن وسلامة المعلومات (NISSA)**: تأسست عام 2013، وهي الجهة الحكومية الرئيسية المسؤولة عن حماية البنية التحتية للمعلومات والاتصالات في ليبيا، تعمل الهيئة على وضع السياسات والمعايير، مراقبة الشبكة الوطنية، وتقديم الحلول الأمنية.[1]

ب-**الفريق الليبي للاستجابة لطوارئ الحاسب (Libya-CERT)**: يعمل تحت مظلة الهيئة الوطنية لأمن وسلامة المعلومات، وهو مسؤول عن منع واكتشاف وتخفيف التهديدات السيبرانية على المستوى الوطني.

ج-**التشريعات والقوانين المنظمة :لا** تزال ليبيا في طور تطوير إطار قانوني شامل للأمن السيبراني، صدر قانون مكافحة الجرائم الإلكترونية في عام 2021، لكنه واجه انتقادات لكونه فضفاضاً، وقد يستخدم لتقييد الحريات، وفي عام 2024، أصدرت وزارة الاقتصاد والتجارة قرارات لتنظيم نشاط مزاولة خدمات الأمن السيبراني، مما يعكس اهتماماً متزايداً بتقنين هذا القطاع.

أدركت الحكومة الليبية أن الفضاء السيبراني أصبح مسرحاً للصراع الجيوسياسي، فأطلقت مشروع تطوير البنية التحتية للاتصالات (2022 – 2025) بالتعاون مع الاتحاد الدولي للاتصالات (ITU) لتأمين الشبكة الوطنية ضد:

- هجمات البرمجيات الخبيثة على أنظمة الكهرباء والمياه.
- التنصت على الاتصالات الدبلوماسية والأمنية والعسكرية.
- التضليل الإعلامي الذي يهدد اللحمة الاجتماعية.

إلا أن الطريق لا يخلو من معوقات، حيث برزت تحديات جسيمة مثل:

- **ضعف البنية التحتية والتشريعات:** تواجه ليبيا تحديات كبيرة تتمثل في الافتقار إلى استراتيجيات أمنية متكاملة وتشريعات محدثة لحماية البيانات والبنية التحتية الرقمية.

(1) https://www.coe.int/en/web/octopus/-/libya.

- **الهجمات السيبرانية** :تتعرض المؤسسات الليبية، بما في ذلك قطاع الاتصالات الحيوي، لهجمات سيبرانية مستمرة مثل هجمات حجب الخدمة (DDoS)، هجمات الفدية، والتصيد الإلكتروني.
- **نقص الوعي والكوادر**: لا يزال الوعي بأهمية الأمن السيبراني منخفضاً لدى الكثير من المسؤولين والموظفين، مما يجعله أحياناً وظيفة ثانوية رغم المخاطر الكبيرة.
- **تقرير الأمن السيبراني 2024**: كشف تقرير صادر عن الهيئة الوطنية لأمن وسلامة المعلومات عن نقاط ضعف حرجة في الدفاعات الرقمية لـ 37 مؤسسة حكومية، مع وجود 73 ثغرة أمنية، 68.5% منها عالية الخطورة، و55% من هذه الثغرات لم يتم معالجتها.

على الرغم من تلك التحديات، فهناك جهود حثيثة لتحسين الأوضاع الأمنية الرقمية، حيث أطلقت الهيئة الوطنية لأمن وسلامة المعلومات "**الاستراتيجية الوطنية للأمن السيبراني**" في فبراير 2023 لمساعدة المؤسسات على حماية بياناتها، كما تحرز ليبيا تقدماً في المؤشر العالمي للأمن السيبراني (GCI) الصادر عن الاتحاد الدولي للاتصالات، حيث انتقلت إلى المستوى الثالث من النضج.

عليه يمكن القول أن العلاقة بين أمن المعلومات والأمن السيبراني وأمن الاتصالات في ليبيا هي علاقة ضرورة حتمية يفرضها الواقع الرقمي المتنامي، ورغم أن الإطار التنظيمي والتشريعي لا يزال في طور النضوج، فالجهود التي تبذلها الهيئات المختصة مثل الهيئة الوطنية لأمن وسلامة المعلومات تضع الأساس لمستقبل رقمي أكثر أماناً في البلاد.

11. الأمن السيبراني والمجتمع الليبي:

يمتد تأثير الأمن السيبراني إلى جميع جوانب المجتمع الليبي، من الأفراد والأسر إلى المؤسسات التعليمية والصحية والخدمية، وقد شهد هذا التأثير تحولاً كبيراً بعد عام 2011، مما أسفر عن واقع جديد يتسم بفرص وتحديات متزامنة.

قبل عام 2011م، كان الوضع الرقمي في ليبيا يتسم بـ:

- **انتشار محدود للإنترنت**: كانت نسبة انتشار الإنترنت بين الأسر لا تتجاوز 14%؛ لذا بقيت التأثيرات المباشرة على الحياة اليومية محدودة.

- **ضعف التقنية في التعليم:** لم تُدمج التقنيات الرقمية بشكل واسع في المؤسسات التعليمية، وبالتالي لم تكن أي هجمات سيبرانية على البنية التعليمية ذات أثر مالي أو اجتماعي كبير علناً.
- **بيئة رقمية مغلقة:** مع سيطرة تامة على تدفق المعلومات والوصول إلى المحتوى الرقمي.

بعد عام 2011 شهدت ليبيا تحولاً كبيراً في المشهد الرقمي، فمع تزايد استخدام الإنترنت والهواتف الذكية في ليبيا، يتعرض المواطنون لمخاطر سيبرانية متنوعة، مثل سرقة الهوية، والاحتيال الإلكتروني، وانتهاك الخصوصية، حيث:

- ارتفعت نسبة انتشار الإنترنت إلى 54% بحسب تقارير الاتحاد الدولي للاتصالات، ما جعل المنازل تعتمد على الإنترنت للتعلم عن بُعد، العمل الحر، وشراء السلع الأساسية.
- زيادة الاعتماد على الخدمات الرقمية في: التعليم، الصحة، التجارة، والخدمات الحكومية.
- تزايد التهديدات السيبرانية: مع زيادة الاعتماد على الفضاء الرقمي، برزت تحديات أمنية جديدة.

هذا التحول الرقمي السريع أدى إلى خلق واقع جديد يتسم بفرص كبيرة من ناحية، وتحديات جسيمة من ناحية أخرى، فبينما أصبحت التحديات الرقمية متاحة بشكل أوسع، برزت تحديات أمنية جديدة في ليبيا أبرزها: نقص الوعي بالمخاطر السيبرانية بين المواطنين، وضعف البنية التحتية للاتصالات في بعض المناطق، وغياب التشريعات الشاملة لحماية البيانات والخصوصية، وعدم وجود خطط أمنية متكاملة لحماية الاستثمارات الرقمية. هذه التحديات تتطلب جهوداً مجتمعية شاملة تشمل التوعية والتثقيف، وتطوير البنية التحتية، وسن القوانين المناسبة.

في المقابل، يمكن أن يساهم تعزيز الأمن السيبراني في تحسين جودة الحياة للمواطنين الليبيين من خلال توفير خدمات رقمية آمنة وموثوقة (كالخدمات الحكومية الإلكترونية)، والتعليم الإلكتروني الآمن، وتطوير خدمات الصحة الرقمية الموثوقة، كما يمكن أن يفتح المجال أمام فرص عمل جديدة في مجال الأمن السيبراني والتكنولوجيا.

عليه، يتطلب تعزيز الأمن السيبراني في ليبيا جهوداً متكاملة تشمل:

- تطوير استراتيجيات وطنية شاملة للأمن السيبراني.
- تحديث التشريعات والقوانين لحماية البيانات والخصوصية.

- تعزيز البنية التحتية للاتصالات وتكنولوجيا المعلومات.
- تنظيم برامج توعوية مستدامة لكافة فئات المجتمع.
- تعزيز التعاون بين المؤسسات الحكومية والقطاع الخاص والمجتمع المدني.

12. الآثار الاقتصادية والاجتماعية للهجمات السيبرانية وانقطاعات الإنترنت في ليبيا:

الآثار الاقتصادية:

• تتجاوز الخسائر الناجمة عن الهجمات السيبرانية وانقطاعات الإنترنت مجرد انعدام الاتصال، لتمس صميم الاقتصاد الوطني والأمن المعيشي للمواطن، فمن الناحية الاقتصادية، تُقدَّر خسائر الهجمات السيبرانية المباشرة على مؤسسات القطاع النفطي الليبي وحدها بحوالي 750 مليون دولار سنوياً وفقاً لتقرير (Oxford Economics, 2024)، نتيجة تعطيل الإنتاج، وعمليات الابتزاز الإلكتروني، وتكاليف استعادة أنظمة التحكم.

أما على مستوى الأسرة، فإن كل انقطاع للإنترنت يُكلِّف الأسرة متوسطة الدخل خسائر ما بين (15–25 ديناراً شهرياً)، أي تقريباً (3–5% من دخلها)، ناجمة عن:

• **تعطل مصادر الدخل:** خاصة مع اعتماد الكثيرين على العمل عبر المنصات الرقمية والتجارة الإلكترونية.

• **التهديد للأمن الغذائي:** حيث أدى تعطل خدمات الدفع الإلكتروني ومنصات بيع المواد الغذائية إلى عرقلة وصول السلع الأساسية، وتساهم الفوضى الناتجة في ارتفاع أسعارها بسبب اضطراب سلاسل التوريد، مما أدى إلى زيادة تكلفة سلة الحد الأدنى للإنفاق بنسبة 14% خلال أزمة 2022.

• **خسائر في القطاع التجاري:** تعطل عمليات البيع والشراء وتحويل الأموال، مما يضرب النشاط الاقتصادي في الصميم.

الآثار الاجتماعية:

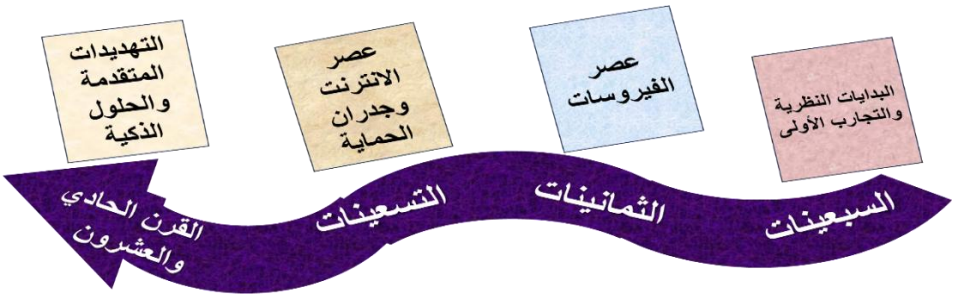
امتدت تأثيرات الانقطاعات لتعطيل الخدمات الأساسية التي يعتمد عليها المواطنون يومياً، مما زاد من حدة الأزمة الإنسانية، حيث:

- **في القطاع الصحي:** أدى انقطاع الإنترنت في عام 2011 إلى تعطيل خدمات الرعاية الصحية عن بُعد، وعدم القدرة على الوصول إلى السجلات الطبية الإلكترونية، وإعاقة تنسيق جهود الإغاثة الطارئة، خاصة في المناطق النائية، مما هدد حياة المرضى الذين يعتمدون على المراقبة المستمرة، ما دفع المجتمع المدني لإنشاء شبكات VSAT ممولة من الجاليات الليبية في الخارج لتأمين الاتصالات الإنسانية[1].
- **في القطاع التعليمي:** توقف التعلم عن بُعد بشكل مفاجئ، مما حرم ملايين الطلاب من استكمال تعليمهم وعمَّق الفجوة التعليمية.
- **عزلة مجتمعية:** فقدان الآلاف المهاجرين مع عائلاتهم لأوطانهم، مما زاد من الشعور بعدم الاستقرار النفسي والاجتماعي، وعطّل قدرات الاقتصاد الليبي.

وهكذا، لم يعد الأمن السيبراني ترفاً تقنياً، بل أصبح رهيناً بالأمن الاقتصادي والاجتماعي والإنساني في ليبيا، حيث تتداخل حماية الفضاء الإلكتروني بشكل مباشر مع حماية مقومات الحياة الأساسية.

13. التطور التاريخي للأمن السيبراني:

لم يظهر الأمن السيبراني بشكله الحالي دفعة واحدة، بل هو نتيجة لتطور مستمر يواكب التقدم التكنولوجي وظهور تهديدات جديدة، يمكن تلخيص هذا التطور حسب تقرير الآفاق العالمية للأمن السيبراني 2025، في مراحل رئيسية كما يوضحها الشكل التالي:



شكل رقم (2): يوضح التطور التاريخى للأمن
المصدر: من إعداد الباحِثيْنِ

(1) التائب، السائح. "أهمية تطبيق الأمن السيبراني المحاسبي في المصارف التجارية الليبية.

- **فترة السبعينات (البدايات النظرية والتجارب الأولى):**

تكمن الجذور الفكرية للأمن السيبراني في بداية السبعينات من القرن الماضي، مع عمل عالم الرياضيات "جون فون نيومان" الذي وضع الأساس النظري للبرامج ذاتية التكاثر، في عام 1971، شهدت شبكة ARPANET أول تطبيق عملي لهذا المفهوم مع برنامج "الزاحف (Creeper)"، الذي لم يكن ضاراً بل كان مجرد تجربة، رداً على ذلك، ابتكر "راي توملينسون" برنامج "الحصاد (Reaper)" لإزالته، والذي يُعتبر أول برنامج لمكافحة الفيروسات ذاتي النسخ.

- **فترة الثمانينات (عصر الفيروسات):**

شهدت هذه الفترة ظهور فيروسات أكثر تعقيداً مع انتشار الحواسيب الشخصية، في عام 1986 ظهر فيروس "برين" (Brain) الذي يُعتبر أول فيروس يصيب أجهزة الكمبيوتر الشخصي، ولم يكن يهدف إلى إحداث دمار كبير بل كان يهدف إلى تتبع النسخ المقرصنة من البرامج، وفي عام 1988 تسببت دودة "موريس (Morris Worm)" في إصابة حوالي 10% من أجهزة الكمبيوتر المتصلة بالإنترنت آنذاك، مما أظهر هشاشة الشبكات المتصلة، دفعت هذه الأحداث إلى ظهور صناعة مكافحة الفيروسات وظهور برامج تجارية مثل "Ultimate Virus Killer".

- **فترة التسعينات (عصر الإنترنت وجدران الحماية):**

مع الانتشار الواسع للإنترنت، تحولت التهديدات السيبرانية من استهداف الأجهزة الفردية إلى استهداف الشبكات بأكملها، مما أدى إلى الحاجة لتقنيات حماية جديدة، في هذه المرحلة، برزت تقنية جدران الحماية (Firewalls)، التي بدأت كأنظمة بسيطة لتصفية الحزم، وتطورت مع ابتكار جيل "شفيد"، مؤسس شركة Check Point، لجدار الحماية الحديث القائم على "فحص الحالة" في عام 1993، وهو ما غيّر طريقة تأمين الشبكات بشكل جذري.

- **القرن الحادي والعشرون: التهديدات المتقدمة والحلول الذكية:**

شهد هذا القرن احترافية الجريمة السيبرانية، وظهور هجمات معقدة ذات دوافع مالية وجيوسياسية، من أبرزها، هجمات برامج الفدية (Ransomware) مثل هجوم (WannaCry) في عام 2017 الذي

أثر على مئات الآلاف من الأجهزة، وهجمات سلسلة التوريد مثل هجوم (SolarWinds) في عام 2020، الذي كشف عن هشاشة الاعتماد على برامج الطرف الثالث.

ولمواجهة هذه التهديدات، تطورت الدفاعات بشكل كبير:

- **الذكاء الاصطناعي (AI):** أصبح يُستخدم لتحليل كميات هائلة من البيانات واكتشاف التهديدات المتقدمة بشكل استباقي وأتمتة المهام الأمنية.
- **الأمن السحابي:** مع انتقال الأعمال إلى السحابة، ظهر مفهوم "نموذج المسؤولية المشتركة" الذي يقسم المسؤولية الأمنية بين مزود الخدمة والعميل.
- **البعد الجيوسياسي:** أصبح الأمن السيبراني جزءاً لا يتجزأ من الأمن القومي، مع وجود هجمات ترعاها الدول بهدف التجسس أو تعطيل البنية التحتية، مما يجعل الفضاء السيبراني ساحة جديدة للصراع.

هذا التطور المستمر يُظهر أن الأمن السيبراني ليس مجرد مجموعة من الإجراءات الثابتة، بل هو مجال ديناميكي يتطلب يقظة دائمة وتكيفاً مستمراً مع التحديات والابتكارات الجديدة.

14. الدراسات السابقة:

تناولت العديد من الدراسات السابقة جوانب مختلفة من التهديدات السيبرانية، بما في ذلك تصنيفها واستراتيجيات التصدّي لها، تأتي هذه الدراسة كمحاولة لتطوير هذه الجهود البحثية من خلال تقديم إطار عمل متكامل يسهم في سد الفجوات القائمة، مما يحدث إضافة نوعية إلى الأدبيات الحالية، فيما يلي عرض لثمانية دراسات سابقة ذات صلة، مرتبة من الأقدم إلى الأحدث:

أجرى Kontaxis et al (2016)، دراسة هدفت إلى تطوير نموذج لتصنيف التهديدات السيبرانية للبنى التحتية الحيوية، حيث اعتمدت الدراسة على منهجية تحليل التهديدات الخاصة بالبنى التحتية الحيوية واقتراح نموذج تصنيفي، توصلت الدراسة إلى تحديد أنواع التهديدات التي تستهدف البنى التحتية الحيوية وتقديم إطار لتصنيفها، وأوصت بضرورة التركيز على التهديدات الموجهة للبنى التحتية الحيوية وتطوير استراتيجيات دفاعية مخصصة.

كما اجرى Hussain et al (2018)، دراسة هدفت إلى استعراض التحديات والحلول المتعلقة باستخبارات التهديدات السيبرانية (CTI)، واعتمدت الدراسة على مراجعة منهجية للأدبيات المتعلقة بـ

CTI، أظهرت النتائج تحديد التحديات الرئيسية في جمع وتحليل ومشاركة استخبارات التهديدات، وتقديم حلول مقترحة لتحسين فعاليتها، وأوصت بتحسين آليات جمع وتحليل ومشاركة استخبارات التهديدات لتعزيز الأمن السيبراني.

أيضا أجرى Al-Hawari et al (2018)، دراسة هدفت إلى تقديم تصنيف للتهديدات السيبرانية بناءً على طبيعة الهجوم والأهداف المستهدفة، وبناء شجرة تصنيفية لفهم الأنواع المختلفة للتهديدات، اعتمدت الدراسة على تحليل الأدبيات وبناء تصنيف هرمي، وتوصلت إلى توفير إطار مبدئي لتصنيف التهديدات، لكنه يفتقر إلى ربط التصنيفات بمستويات خطورة محددة أو استراتيجيات تصدّي مفصلة، وأوصت بضرورة ربط التصنيفات باستراتيجيات تصدّي محددة.

كما قدم Ahmed et al (2019) دراسة هدفت إلى اقتراح نموذج تصنيفي يعتمد على مستويات الخطورة وتأثير التهديد على البنية التحتية الرقمية، مع التركيز على ربط كل مستوى باستراتيجيات دفاعية متخصصة، اعتمدت الدراسة على تطوير نموذج تصنيفي بناءً على تحليل المخاطر، وأظهرت النتائج فاعلية هذا النموذج في تحسين استجابة المؤسسات للتهديدات المختلفة، وأوصت بأهمية تطوير نماذج تصنيفية ديناميكية تأخذ في الاعتبار التطور المستمر للتهديدات.

وقام **Aldawood and Al-Zahrani (2020)** بدراسة تناولت تحليل التهديدات السيبرانية التي تواجه المؤسسات التعليمية في المملكة العربية السعودية، وتقديم استراتيجيات للتخفيف منها، اعتمدت الدراسة على دراسة حالة ومسح للمؤسسات التعليمية، وتوصلت إلى تحديد أبرز التهديدات التي تواجه القطاع التعليمي، مثل التصيد الاحتيالي والبرمجيات الخبيثة، وتقديم توصيات لتعزيز الأمن السيبراني في هذا القطاع، وأوصت بضرورة توعية المستخدمين وتطبيق سياسات أمنية صارمة في المؤسسات التعليمية.

كما أجرى **Al-Shammari and Al-Mubarak (2021)** دراسة هدفت إلى تقييم فعالية استراتيجيات الأمن السيبراني في حماية البنية التحتية الحيوية في دول مجلس التعاون الخليجي، اعتمدت الدراسة على مراجعة أدبيات وتحليل مقارن للاستراتيجيات المتبعة، وتوصلت إلى تحديد نقاط القوة

والضعف في الاستراتيجيات الحالية، وتقديم توصيات لتحسين التعاون الإقليمي وتبادل المعلومات، وأوصت بتعزيز التعاون الإقليمي وتبادل المعلومات الاستخباراتية لمواجهة التهديدات السيبرانية المشتركة. وقام **Smith and Jones (2023)** بدراسة تأثير الذكاء الاصطناعي على تطور التهديدات السيبرانية واستراتيجيات الدفاع، اعتمدت الدراسة على تحليل اتجاهات الذكاء الاصطناعي في الأمن السيبراني، وأظهرت النتائج أن الذكاء الاصطناعي يزيد من تعقيد الهجمات، ولكنه يقدم أيضاً أدوات قوية للدفاع، والحاجة إلى نماذج دفاعية تتكيف مع التهديدات المدعومة بالذكاء الاصطناعي، وأوصت بالاستثمار في البحث والتطوير في مجال الذكاء الاصطناعي للدفاع السيبراني، وتطوير أطر عمل لتقييم التهديدات المدعومة بالذكاء الاصطناعي.

كما قام كلا من التائب، وعلي مفتاح والسائح، وجبريل عمر (2025) بدراسة أهمية تطبيق الأمن السيبراني المحاسبي في المصارف التجارية الليبية العاملة في مدينة سرت، هدفت الدراسة إلى تقييم مستوى الوعي بأهمية تطبيق الأمن السيبراني المحاسبي في المصارف التجارية الليبية العاملة في مدينة سرت، وتحديد التحديات التي تواجهها هذه المصارف في تطبيقه، بالإضافة إلى استكشاف مدى اهتمام المصرف المركزي والمصارف التجارية بتعزيز هذا الجانب، واعتمدت الدراسة على المنهج الوصفي التحليلي، حيث تم جمع البيانات الأولية عبر استبانة صممت خصيصاً لهذا الغرض، وتم تحليل البيانات باستخدام برنامج SPSS وتوصلت الدراسة للنتائج التالية:

1. أن موظفي المصارف يدركون أهمية تطبيق الأمن السيبراني المحاسبي.
2. وجود تحديات وعقبات كبيرة تواجه تطبيق نظم الأمن السيبراني في المصارف التجارية بمدينة سرت.
3. هناك اهتمام ملحوظ من المصرف المركزي والمصارف التجارية بتعزيز الأمن السيبراني المحاسبي، خاصة في مجالات: حماية البيانات المالية الحساسة، وتعزيز الثقة والمصداقية، وتقليل المخاطر المالية والتشغيلية، وضمان الامتثال للمعايير الأمنية والقانونية.

وقدمت الدراسة توصيات أهمها: تنظيم دورات وورش عمل دورية لموظفي المصارف، والاستثمار في تقنيات الأمن السيبراني المتطورة، وتحديث الأنظمة بشكل مستمر، وتعزيز التعاون مع المصرف المركزي والجهات الحكومية لتبادل المعلومات والخبرات.

أوجه التشابه والاختلاف بين الدراسات السابقة والدراسة الحالية:

تتشابه الدراسة الحالية مع الدراسات السابقة في تناولها لموضوع التهديدات السيبرانية وأهمية تصنيفها، كما تتفق مع دراسة Ahmed et al. (2019) في التركيز على ربط مستويات التهديد باستراتيجيات دفاعية محددة، كما تتشابه مع دراسة Al-Hawari et al. (2018) في بناء إطار تصنيفي هرمي للتهديدات، والتركيز على تصنيف التهديدات السيبرانية مثل دراسة Kontaxis et al., 2016؛ كما اعتمدت الدراسة الحالية منهجية تحليلية وصفيّة مشابهة لدراسات (Hussain et al., 2020; Alqahtani & Abukari, 2020) لاستخلاص المعايير والاستراتيجيات، ومع ذلك، تختلف الدراسة الحالية عن الدراسات السابقة في تقديمها لنموذج شامل يربط بشكل ديناميكي بين تصنيف التهديدات واستراتيجيات التصدّي، بينما ركزت معظم الدراسات السابقة على جانب واحد فقط؛ كما تتميز الدراسة الحالية بتقديم إطار عمل متكامل يمكن تطبيقه عبر قطاعات مختلفة، وقدمت الدراسة مصفوفة عملية تربط كل تهديد بإجراءات اكتشافه ومعالجته (انظر الجدول 1)، بينما اقتصرت بعض الدراسات السابقة على قطاعات محددة مثل التعليم أو البنية التحتية الحيوية.

15. منهجية الدراسة:

اعتمدت الدراسة على المنهج الوصفي التحليلي ومنهج بناء النماذج، وذلك عبر:

- **تحليل الأدبيات السابقة:** من خلال مراجعة عدد من الدراسات والمصادر المعتمدة في مجالات تصنيف التهديدات واستراتيجيات التصدي.
- **تحديد معايير التصنيف:** من حيث الخطورة (تأثير مالي/ تشغيلي)، والتعقيد (تقني/ غير تقني)، والانتشار (سرعة/ نطاق).
- **تصميم النموذج المقترح:** من خلال أربع مستويات هرمية (منخفض، متوسط، عالي، حرج)، ومصفوفة ربط بين التهديدات واستراتيجيات التصدي.

16. النموذج المقترح لتصنيف مستويات التهديدات السيبرانية:

تقدم هذه الدراسة نموذجاً شاملاً لتصنيف مستويات التهديدات السيبرانية، يهدف إلى توفير إطار عمل منهجي يمكن المؤسسات من تقييم التهديدات بدقة، وتحديد استراتيجيات التصدّي المناسبة؛ يعتمد

النموذج على تصنيف هرمي للتهديدات إلى أربعة مستويات رئيسية، مع ربط كل مستوى باستراتيجيات وقائية واكتشافية واستجابية محددة.

- **معايير تصنيف مستويات التهديدات السيبرانية:**

يستند النموذج المقترح على مجموعة من المعايير الأساسية لتصنيف التهديدات السيبرانية، والتي تشمل شدة التأثير المحتمل على المؤسسة، ومستوى التعقيد التقني للتهديد، وسرعة انتشاره، ومدى صعوبة اكتشافه ومعالجته، كما يأخذ النموذج في الاعتبار طبيعة الجهة المهاجمة ودوافعها، والأصول المستهدفة وحساسيتها، والزمن المطلوب للتعافي من الهجوم.

- **مستويات التصنيف واستراتيجيات التصدّي:**

يوضح الجدول التالي النموذج المقترح لتصنيف مستويات التهديدات السيبرانية واستراتيجيات التصدّي المرتبطة بكل مستوى:

جدول رقم (1): نموذج مقترح لتصنيف مستويات التهديدات السيبرانية واستراتيجيات التصدي

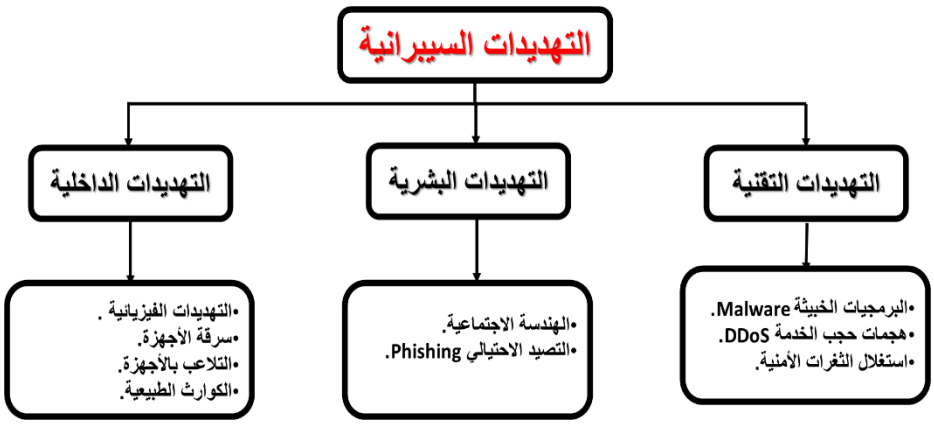
مستوى التهديد	الوصف	خصائص التهديد	استراتيجيات الوقاية	استراتيجيات الاكتشاف	استراتيجيات الاستجابة
منخفض	تهديدات بسيطة ذات تأثير محدود.	– هجمات آلية غير موجهة. – تأثير محدود على العمليات. – سهولة الاكتشاف والمعالجة.	– تحديث أنظمة التشغيل والبرامج. – استخدام برامج مكافحة الفيروسات. – تدريب أساسي للمستخدمين.	– أنظمة مكافحة الفيروسات. – مراقبة السجلات الأساسية. – تنبيهات النظام التلقائية.	– إزالة البرمجيات الخبيثة. – إعادة تشغيل الأنظمة. – توثيق الحادث.
متوسط	تهديدات موجهة بتأثير متوسط.	– هجمات مستهدفة جزئياً. – تأثير على بيانات غير حرجة. – تتطلب مهارات تقنية متوسطة.	– تطبيق سياسات أمنية متقدمة. – استخدام جدران الحماية. – المصادقة ثنائية العوامل.	– أنظمة كشف التسلل (IDS). – مراقبة حركة الشبكة. – تحليل السلوك الشاذ.	– عزل الأنظمة المتأثرة. – تحليل الحادث. – استعادة البيانات من النسخ الاحتياطية.

عالٍ	تهديدات متقدمة بتأثير كبير.	– هجمات مستهدفة ومعقدة. – تأثير على البيانات الحساسة. – استخدام تقنيات متطورة.	– أنظمة إدارة معلومات الأمن (SIEM). – اختبار الاختراق الدوري. – تدريب متقدم للموظفين.	– استخبارات التهديدات السيبرانية. – تحليل السلوك المتقدم. – فرق الاستجابة للحوادث.	– تفعيل خطة الاستجابة للطوارئ. – التحقيق الجنائي الرقمي. – إبلاغ الجهات المختصة.
حرج – عالٍ جداً	تهديدات كارثية بتأثير شامل.	– هجمات دولة أو جماعات إرهابية. – تهديد الأمن القومي. – تعطيل شامل للخدمات الحيوية.	– الأمن السيبراني التكيفي. – الشراكة مع الجهات الأمنية. – خطط استمرارية الأعمال.	– مراكز العمليات الأمنية المتقدمة. – التعاون مع وكالات الأمن القومي. – المراقبة المستمرة 7/24.	– تفعيل خطط الطوارئ الوطنية. – التنسيق الدولي. – التحقيق على مستوى الدولة.

المصدر: من إعداد الباحِثَيْنِ

- **مخطط تصنيف فئات التهديدات السيبرانية:**

يمكن تمثيل فئات التهديدات السيبرانية الرئيسية في المخطط التالي:



شكل رقم (3) يوضح تصنيف فئات التهديدات السيبرانية

المصدر: من إعداد الباحِثَيْنِ

17. استخبارات التهديدات السيبرانية:

تعتبر استخبارات التهديد السيبراني (CTI) حجر الزاوية في استراتيجيات التصدي الفعالة، وتُعرف CTI بأنها: "عملية جمع وتحليل ونشر المعلومات حول الهجمات المحتملة أو الحالية بهدف تزويد صانعي القرار بالأدوات والمعلومات اللازمة لمنع التهديدات واكتشافها والاستجابة لها"، وتتكون CTI من أربعة أنواع رئيسية[1]:

أ. **الاستخبارات الاستراتيجية:** توفر رؤى عالية المستوى حول المشهد الأمني الأوسع ودوافع الخصوم على المدى الطويل، وتساعد في مواءمة استراتيجيات الأمن السيبراني مع الأهداف التجارية.

ب. **الاستخبارات التكتيكية:** تركز على الإجراءات الفورية ومؤشرات الاختراق (IOCs) لمساعدة فرق الأمن على التعرف على التهديدات النشطة والاستجابة لها بسرعة.

ج. **الاستخبارات التقنية:** تتضمن معلومات مفصلة عن آليات الهجوم، مثل تحليل البرامج الضارة ونقاط الضعف، مما يساعد في تطوير آليات دفاعية وتحسين الوضع الأمني.

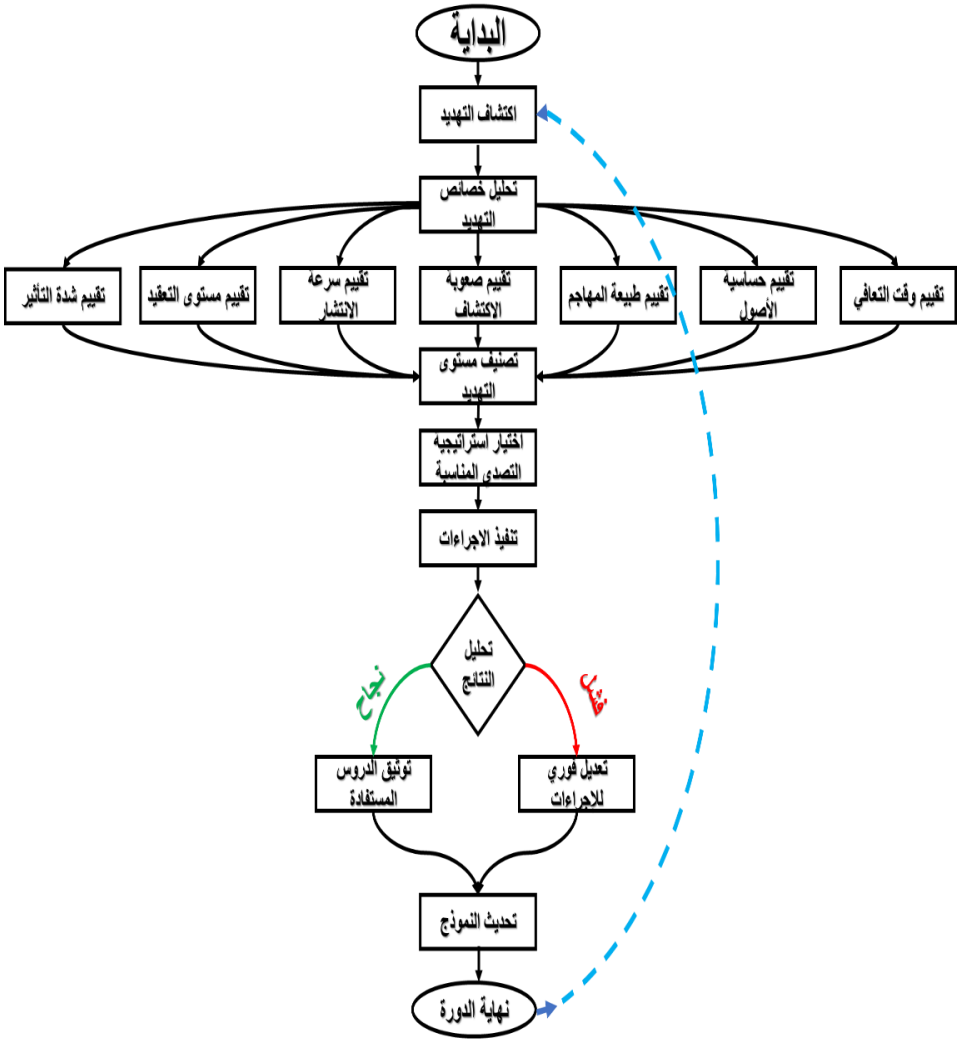
د. **الاستخبارات التشغيلية:** تركز على التكتيكات والحملات قصيرة المدى للخصوم، وتوفر معلومات سياقية لدعم اتخاذ القرارات الفورية وتحسين قدرات الاستجابة للحوادث.

إن فهم هذه الأنواع من الاستخبارات السيبرانية يمكن أن يعزز بشكل كبير قدرة المؤسسات على اتخاذ تدابير استباقية وتطوير استراتيجيات تصدي مرنة، تتضمن استراتيجيات التصدي الفعالة: استخدام كلمات مرور قوية، وتفعيل المصادقة متعددة العوامل، وتحديث البرامج بانتظام، واستخدام برامج مكافحة الفيروسات، وتوخي الحذر من الروابط المشبوهة، والنسخ الاحتياطي للبيانات، واستخدام الشبكات الافتراضية الخاصة (VPN).

(1) https://www.exabeam.com/ar/explainers/cyber-threat-intelligence/4-types-of-cyber-threat-intelligence-and-using-them-effectively.

18. المخطط الانسيابي للنموذج المقترح:

يوضح المخطط التالي العملية المنهجية لتطبيق النموذج المقترح بشكل دوري في تصنيف التهديدات وتحديد استراتيجيات التصدّي، يبدأ باكتشاف التهديد وينتهي بتحديث النموذج بناء على الدروس المستفادة:



شكل رقم (4): المخطط الانسيابي للنموذج المقترح

المصدر: من إعداد الباحِثَيْنِ

شرح تفصيلي للمراحل بالنموذج المطور:

أ-اكتشاف التهديدات السيبرانية: من خلال الآليات التالية: أنظمة كشف التسلل (IDS/IPS)، ومراقبة السجلات الأمنية (SIEM) ، وتقارير الثغرات الأمنية وتحليل السلوك الشبكي (UEBA)، ثم يتم كتابة تقرير أولي عن مؤشرات الهجوم (IoCs).

ب-تحليل خصائص التهديدات السيبرانية: الجدول التالي (رقم 2) يوضح تحليل خصائص التهديد السيبراني، حيث يقيم الفريق الأمني كل تهديد بناء على هذه المعايير، ويتم الإجابة على أسئلة التقييم من قبل الفريق الأمني، ثم تعطي نقاط (مثلاً باستخدام مقياس من 1 إلى 10 لكل معيار)، وتضرب النقاط بأوزانها المعيارية المحددة مسبقاً (حيث يصنف التهديد باستخدام أوزان معيارية[1] مستمدة من مراجع الأمن السيبراني الرائدة)، ثم تجمع النقاط لاحقاً لتصنيف مستوى التهديد (منخفض/ متوسط/ عالٍ/ حرج).

جدول رقم (2): معايير تقييم خصائص التهديدات السيبرانية

ت	المعيار	أسئلة (معايير) التقييم
1	**شدة التأثير**	ما حجم الضرر المالي/التشغيلي/القانوني؟ هل توجد تأثيرات على السمعة؟
2	**مستوى التعقيد**	ما درجة تقدم الأدوات المستخدمة؟ هل يتطلب هجومًا متعدد المراحل؟
3	**سرعة الانتشار**	هل ينتشر عبر الشبكة تلقائيًا؟ ما معدل الإصابة المتوقع؟
4	**صعوبة الاكتشاف**	هل يستخدم تقنيات التخفّي؟ هل يتجنب أنظمة الكشف التقليدية؟
5	**طبيعة المهاجم**	هل هي جهة فردية/منظمة/دولية؟ ما الدوافع (مالية، تجسس، تخريب)؟
6	**حساسية الأصول**	هل المستهدف بنى تحتية حرجة؟ هل البيانات مسربة حساسة (شخصية/أمنية)؟
7	**زمن التعافي**	ما متوسط وقت الإصلاح؟ هل يتطلب استعادة نسخ احتياطية كاملة؟

المصدر: من إعداد الباحِثَيْنِ

(1) الأوزان المعيارية:

- شدة التأثير (1.5): NIST Cybersecurity Framework (NIST, 2018).
- التعقيد (1.2): MITRE ATT&CK Matrix (MITRE, 2023).
- حساسية الأصول (1.4): PCI DSS v4.0 (PCI SSC, 2022).

ج- تصنيف مستوى التهديدات السيبرانية:

بعد جمع النقاط المرجحة، تصنف التهديدات السيبرانية إلى أحد المستويات كما في الجدول التالي:

جدول رقم (3): تصنيف مستوى التهديدات السيبرانية [1]

مجموع النقاط	المستوى	الوصف
1003-	**منخفض**	تأثير محدود (لا يعطل العمليات الأساسية ولا يؤثر على الأهداف الاستراتيجية).
31-55	**متوسط**	تأثير ملحوظ (قابل للإدارة، لكنه لا يهدد الوظائف الحيوية).
56-75	**مرتفع**	تهديد كبير (يؤثر على الوظائف الحيوية ويتطلب تدخلًا فورياً).
76-100	**حرج**	تهديد وجودي (يهدد بانهيار النظام أو الخدمة الحيوية، ويتطلب إجراءات طارئة).

د- استراتيجيات التصدّي للتهديدات السيبرانية المبنية على التصنيف:

بعد التصنيف يتم اختيار استراتيجية التصدي للتهديدات السيبرانية من الجدول التالي:

جدول رقم (4): استراتيجيات التصدي للتهديدات السيبرانية.

المستوى	الإجراءات الوقائية	الإجراءات الاستجابية	أدوات التنفيذ
منخفض	- تحديثات التصحيحات. - تدريب المستخدمين.	- عزل الاجهزة المصابة. - مسح البرمجيات الخبيثة.	أنظمة AV ، جدران النار الأساسية.
متوسط	- تقسيم الشبكة. - سياسات الوصول الصارمة.	- تنشيط خطة الاستجابة للحوادث. - تحليل الذاكرة.	أنظمة EDR ، SOAR، تقنيات التجزئة
مرتفع	- أنظمة كشف التسلل المتقدمة – التشفير .	- إيقاف الأنظمة الحرجة. - التنسيق مع الجهات الحكومية.	أنظمة XDR، نظير الدفاع الإلكتروني (CDR)

المصدر: من إعداد الباحِثَيْنِ

(1) المصدر: من إعداد الباحِثَيْنِ بناء على ممارسات دولية معتمدة ودراسات سابقة في إدارة المخاطر وتصنيف التهديدات.
ISO 31000:2018;NIST SP 800-30 Rev.1; NIST SP 800-37 Rev.2; WEF,2023,2025.

هـ- تحليل النتائج ومراقبة الفعالية وتقييمها:

هذه المرحلة هي الأكثر ديناميكية في النموذج، حيث تتضمن تحسيناً مستمراً لاستجابة المؤسسة للتهديدات، هدفها قياس مدى نجاح استراتيجيات التصدي للتهديدات السيبرانية باستخدام مؤشرات أداء رئيسية التي تتضمن:

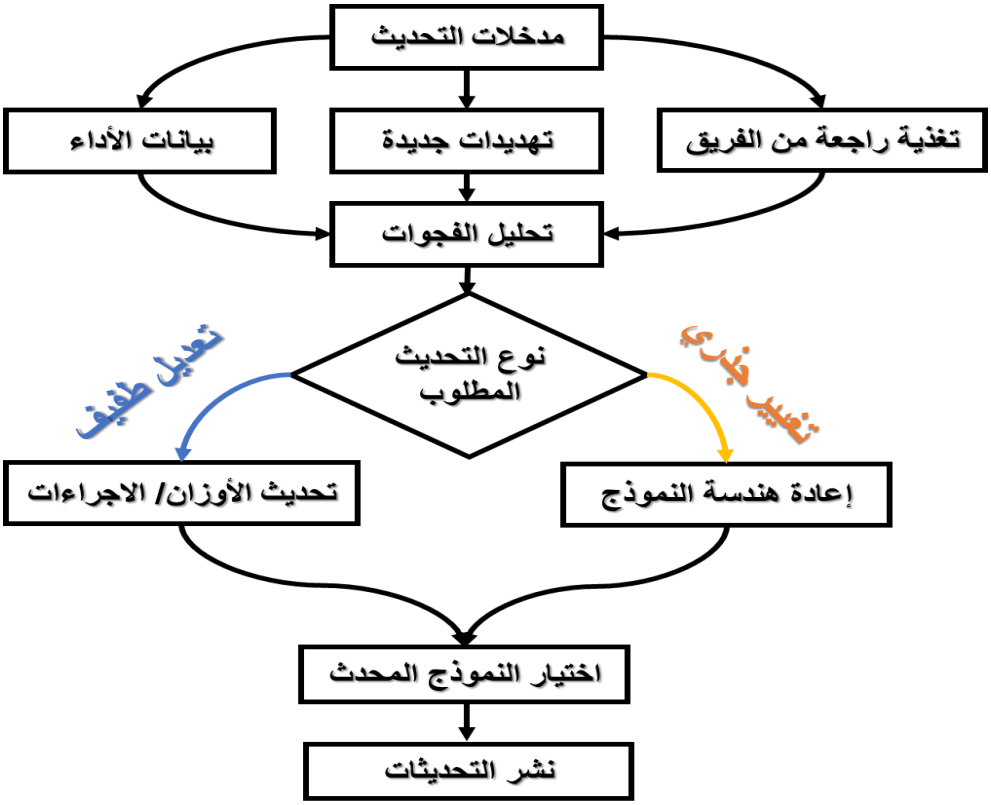
(متوسط وقت الاحتواء (MTTD) ونسبة التهديدات المصنفة بشكل صحيح، وتكلفة التعافي من الحوادث، ومستوى رضا المستخدمين عن فعالية الاستجابة).

فبعد تطبيق استراتيجيات التصدي للتهديدات السيبرانية يتم تحليل النتائج عبر مقارنة الأداء الفعلي بالأهداف المحددة مسبقاً مثل: (وقت الاستجابة، ودقة التصنيف)، وفي حال وجود فجوات يتم البحث عن أسبابها، كتأخر فريق الاستجابة، أو نقص التدريب، بينما يدرس نجاح الاستجابة لمعرفة العوامل المؤثرة مثل: (كفاءة وفعالية أنظمة EDR، أو فعالية الخطط الموضوعة)، ثم تستخلص الدروس المستفادة لتحديث النموذج سواء عبر تعديل معايير التصنيف أو تحسين استراتيجيات التصدي المستقبلية.

و- تحديث النموذج:

يخضع النموذج لتحديث دوري بناء على تحليل بيانات الأداء والتهديدات الناشئة والتغذية الراجعة من الفرق، فهذه المرحلة تضمن أن النموذج يتطور باستمرار لمواكبة التهديدات السيبرانية الجديدة، ونقاط الضعف المكتشفة في الاستجابات السابقة، والتغيرات في بيئة المؤسسة الأمنية والاقتصادية، فجميع الدراسات السابقة، وإن اختلفت في تفاصيلها، إلا أنها تؤكد على الحاجة الملحة لوجود أطر عمل فعّالة لإدارة الأمن السيبراني، فعلى على سبيل المثال، ركزت دراسة Kontaxis et al. (2016) على البنى التحتية الحيوية، بينما تناولت دراسة Aldawood and Al-Zahrani (2020) المؤسسات التعليمية، مما يبرز التنوع في تطبيقات الأمن السيبراني.

ويمكن توضيح هذه المرحلة بالمخطط الانسيابي التالي الذي يوضح كيفية تحويل البيانات الخام (المدخلات) إلى تحسين فعلية (مخرجات) عبر عدة مراحل أساسية.



شكل رقم (5): المخطط الانسيابي لآلية التحديث الديناميكية للنموذج

المصدر: من إعداد الباحِثَيْنِ

يوضح هذا الشكل أن عملية تحديث النموذج تمر بمراحل متسلسلة تبدأ بجمع البيانات من مصادر متعددة، وتنتهي بنشر تحسينات قابلة للقياس، حيث تضمن هذه الآلية بقاء النموذج متوافقاً مع أحدث التهديدات السيبرانية.

مميزات النموذج:

أ. **الديناميكية:** تحديث تلقائي بناءً على دروس الحوادث السابقة.

ب. **المرونة:** قابلية تعديل أوزان المعايير حسب طبيعة نشاط المؤسسة.

ج. **التكامل:** الربط المباشر بين التصنيف واستراتيجيات العمل.

د. **القياسية:** استخدام مقاييس كمية لتقليل الذاتية والارتجالية في التقييم.

هـ. **الامتثال:** يدعم معايير الأيزو NIST CSF27001.

و. **نصيحة التطبيق:** استخدم منصات مثل Splunk أو IBM QRadar أو استخدام أداة مثل Micrisoft Threat Modeling Tool لأتمتة جمع بيانات التقييم، مع بناء "محرك تصنيف" مخصص يحسب النقاط تلقائياً بناءً على مدخلات الفريق الأمني.

19. النتائج والتوصيات والمقترحات:

نتائج الدراسة:

لقد أظهرت هذه الدراسة أن تقديم نموذج شامل لتصنيف مستويات التهديدات السيبرانية وربطها باستراتيجيات تصَدّ فعّالة يمثل خطوة حاسمة نحو تعزيز الأمن السيبراني للمؤسسات الأمنية والاقتصادية، فمن خلال التحليل النظري للأدبيات السابقة حول موضوع الدراسة، تم التوصل إلى النتائج الرئيسية التالية:

1. تبين أن التصنيف الهرمي للتهديدات السيبرانية (منخفض، متوسط، عالٍ، حرج، عالٍ جداً) يوفر إطاراً واضحاً لتقييم المخاطر، مما يسهل على المؤسسات فهم طبيعة التهديدات التي تواجهها.
2. أوضحت الدراسة أن ربط كل مستوى من مستويات التهديد السيبرانية باستراتيجيات تصدّي محددة (وقائية، اكتشافية، استجابية) يعزز من كفاءة الاستجابة الأمنية ويقلل من الهدر في الموارد.
3. أظهر النموذج المقترح قدرته على التكيف مع التطور المستمر للتهديدات السيبرانية، مما يجعله أداة عملية يمكن تحديثها بانتظام لتواكب التحديات الجديدة.
4. يساهم النموذج في دعم صانعي القرار من خلال توفير رؤية واضحة للمخاطر المحتملة والإجراءات اللازمة للتعامل معها، مما يؤدي إلى اتخاذ قرارات أكثر استنارة وفعالية.

توصيات الدراسة:

بناءً على النتائج التي تم التوصل إليها، يوصي الباحثان بما يلي:

1. يجب على المؤسسات الأمنية والاقتصادية تبني نموذج تصنيفي شامل للتهديدات السيبرانية، مثل النموذج المقترح في هذه الدراسة، لضمان تقييم موحد ومنهجي للمخاطر والتهديدات السيبرانية.

2. الاستثمار في برامج استخبارات التهديدات السيبرانية (CTI) لتعزيز قدرة المؤسسات الأمنية والاقتصادية على التنبؤ بالتهديدات السيبرانية واكتشافها مبكراً، ويجب الاستثمار في أدوات وتقنيات CTI، وتدريب الفرق الأمنية والاقتصادية على تحليل البيانات الاستخباراتية.
3. يجب على المؤسسات الأمنية والاقتصادية تطوير خطط استجابة سريعة للحوادث تتناسب مع مستويات التهديد السيبرانية المختلفة، لضمان استجابة سريعة وفعّالة لكل نوع من أنواع الهجمات.
4. يعتبر العنصر البشري خط الدفاع الأول، لذا يجب توفير برامج تدريب وتوعية مستمرة للموظفين حول أحدث التهديدات السيبرانية والممارسات الأمنية الجيدة.
5. يوصي الباحثان بإجراء دراسات حالة وتجارب لاستخلاص نتائج ومؤشرات من تجارب عملية للتحقق من فعالية النموذج المقترح في بيئات حقيقية، وقياس تأثيره على تحسين برامج الأمن السيبراني.
6. تطوير أدوات برمجية تعتمد على الذكاء الاصطناعي والتعلم الآلي لدعم تطبيق النموذج المقترح، مثل أنظمة تصنيف التهديدات الآلية، وأنظمة توصية باستراتيجيات التصدّي للتهديدات السيبرانية.

مقترحات الدراسة:

تقترح هذه الدراسة مجموعة من المجالات للبحث والدراسات المستقبلية:

1. يمكن تطوير النموذج ليشمل تقييم الثغرات الأمنية وربطها بمستويات التهديدات السيبرانية، مما يوفر رؤية أكثر شمولية للمخاطر السيبرانية.
2. يمكن للباحثين تطوير أدوات برمجية أو أنظمة ذكاء اصطناعي لدعم تطبيق النموذج المقترح، مثل أنظمة تصنيف التهديدات التلقائية أو أنظمة التوصية باستراتيجيات التصدّي.
3. أيضا يمكن إجراء دراسات متخصصة لتقييم تأثير تطبيق النموذج المقترح في قطاعات أخرى وتكييفه ليناسب احتياجات هذه القطاعات.
4. إجراء أبحاث مستقبلية حول تأثير التهديدات الناشئة، مثل تلك المرتبطة بالحوسبة الكمومية وإنترنت الأشياء (IoT)، على النموذج المقترح وتكييفه معها.
5. اقتراح وتطوير مقاييس أداء كمية لتقييم فعالية استراتيجيات التصدّي المطبقة، مما يتيح للمؤسسات قياس العائد على الاستثمار في الأمن السيبراني.

قائمة المراجع:

أولاً/ الكتب والدوريات العربية:

- القاسم، أحمد سالم سعد، وأحمد محمد سالم حسين. "**واقع مخاطر أمن نظم المعلومات المحاسبية الإلكترونية بالمصارف التجارية الليبية العاملة بمدينة البيضاء .**" في المؤتمر العلمي الدولي الأول حول التحوط وإدارة الخطر بالصناعة المالية الإسلامية، 25–55. مركز السنابل للبحث وتطوير الموارد البشرية ومركز بيان للهندسة المالية والإسلامية، 2017.
- حسن، أحمد طارق. "**الأمن السيبراني وتداعياته على الأمن القومي المصري.**" مجلة كلية التربية، جامعة عين شمس، 2024.
- يوسف، عقيلة عمر عقيلة. "ت**قييم تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية الليبية: دراسة وصفية.**" المجلة العلمية للدراسات التجارية والبيئية 15، 1. (2024).

ثانياً/ التقارير والمنشورات:

- الهيئة الوطنية لأمن وسلامة المعلومات. **الإعلان عن إطلاق الاستراتيجية الوطنية للأمن السيبراني.** فبراير 2023. https://www.coe.int/en/web/octopus/-/libya
- الهيئة الوطنية لأمن وسلامة المعلومات. **تقرير الأمن السيبراني لعام 2024.**

https://www.coe.int/en/web/octopus/-/libya

ثالثاً/ أطروحات ورسائل جامعية:

- جامعة سبها، "**تأثير الأمن السيبراني على الاقتصاد الليبي**"، تاريخ الوصول: سبتمبر 10، 2025.

.https://journal.su.edu.ly/index.php/esj/article/view/3264

- التائب، عقيلة محمد، وجمعة عمر السائح. "**أهمية تطبيق الأمن السيبراني المحاسبي في المصارف التجارية الليبية: دراسة تطبيقية على المصارف التجارية العاملة في مدينة سرت.**" مجلة الدراسات الاقتصادية 8، 1. (2025).

https://doi.org/10.37375/esj.v8i1.3264

رابعاً/ مصادر إلكترونية وقانونية:

- **الاقتصاد الليبي بعد 2011: خرائط المقدرات والتحديات.**

Mediterranean Center for Strategic Studies. 11 أغسطس 2023

https://mediterraneancss.uk/2023/08/10/libyan-economy./

- المؤسسة العامة للتدريب التقني والمهني. "**دبلوم الأمن السيبراني: أساسيات الأمن السيبراني.**" أكاديمية التعلم. تاريخ الوصول: سبتمبر 10، 2025.

https://drive.google.com/file/d/1m4o265lxVJvv2Y9vUlzvllDHXHQKLWl1/view.

- **ليبيا ما قبل وبعد 2011: انهيار دخل المواطن لأقل من النصف.**

Sky News Arabia. 2 أغسطس 2022

https://www.skynewsarabia.com/amp/middle-east/1552317

- عبد الله، وآخرون. "**الهجمات السيبرانية المتكررة تقلق المؤسسات المالية في ليبيا.**" اندبندنت عربيا. 2024.

https://www.independentarabia.com/node/566346.

- وكالة الأنباء الليبية "لانا". "**الأمن السيبراني والمجتمع الليبي.**" تاريخ الوصول: سبتمبر 10، 2025.

https://lana.gov.ly/post.php?lang=ar&id=324291

- وكالة الأنباء الليبية. "**الأمن السيبراني في ليبيا: تحديات تواجه المؤسسات الحكومية.**" 17 يناير 2025.

https://lana.gov.ly/post.php?lang=ar&id=324291.

- وزارة الاقتصاد والتجارة، حكومة الوحدة الوطنية. قرار رقم (333) لسنة 2024م **بشأن تنظيم نشاط مزاولة خدمات الأمن السيبراني.** 2024.
- "**أربع أنواع من استخبارات التهديد وكيفية استخدامها بشكل فعال.**" Exabeam. تاريخ الوصول: سبتمبر 10، 2025.

https://www.exabeam.com/ar/explainers/cyber-threat-intelligence/4-types-of-cyber-threat-intelligence-and-using-them-effectively.

خامساً/ المراجع الاجنبية:

- Al-Hawari, Mohammad, Majdi Al-Rousan, and Ahmad Al-Shami. "A Classification of Cyber Threats Based on Attack Nature and Targeted Objectives." **International Journal of Computer Science and Network Security** 18, no. 10 (2018): 123–30.
- Ahmed, Ali, Saad Khan, and Abdullah Al-Ghamdi. "A Proposed Classification Model for Cyber Threats Based on Severity and Impact." **Journal of Cybersecurity Research** 5, no. 2 (2019): 123–35.
- Al-Shammari, Fahad, and Ahmad Al-Mubarak. "Evaluating the Effectiveness of Cybersecurity Strategies in Protecting Critical Infrastructure in GCC Countries." **Journal of Information Security** 15, no. 4 (2021): 301–15.
- Aldawood, Abdulaziz, and Saeed Al-Zahrani. "Cyber Threats Facing Educational Institutions in Saudi Arabia and Mitigation Strategies." **International Journal of Cybersecurity** 8, no. 3 (2020): 210–25.
- Brown, Laura. "The CIA Triad in Modern Cybersecurity." **Security Journal** 12, no. 4 (2018): 201–15.
- Davis, Mark. "Understanding Cyber Threats." **Cyber Defense Review** 7, no. 1 (2019): 45–58.
- Green, Paul. "Threat vs. Attack: Differentiating Concepts in Cybersecurity." **Digital Forensics Journal** 9, no. 2 (2017): 87–99.

- Hussain, Ahmad, Muhammad A. Khan, and Rashid Ahmad. "Cyber Threat Intelligence: Challenges and Solutions." **Journal of Information Security and Applications** 40 (2018): 147–57.
- Kontaxis, Georgios, Michalis Polychronakis, and Evangelos P. Markatos. "A Taxonomy of Cyber Threats for Critical Infrastructures." In **Proceedings of the 11th International Conference on Critical Information Infrastructures Security (CRITIS 2016)**, 1–15. Springer, 2016.
- Smith, John, and Alice Jones. "The Impact of Artificial Intelligence on Evolving Cyber Threats and Defense Strategies." **AI in Cybersecurity Journal** 2, no. 1 (2023): 1–15.
- Smith, Thomas, and Laura Jones. "AI-Driven Cyber Threats and Adaptive Defenses." **IEEE Transactions on Cybersecurity** 15, no. 2 (2023): 200–215.
- CrowdStrike. **Global Threat Report**. 2025. https://www.crowdstrike.com.
- Cybersecurity & Infrastructure Security Agency (CISA). "Cyber Attacks." Accessed September 10, 2025. https://www.cisa.gov/topics/cyber-attacks.
- ENISA. "Cybersecurity Strategies." Accessed September 10, 2025. https://www.enisa.europa.eu/topics/national-cyber-security-strategies.
- Europol. **Internet Organized Crime Threat Assessment (IOCTA)**.2023. https://www.europol.europa.eu/cms/sites/default/files/documents/europol_iocta_2023.pdf.
- Gartner. "Cybersecurity Trends 2023." Accessed September 10, 2025. https://www.gartner.com/en/articles/top-cybersecurity-trends-2023.
- Global Cybersecurity Index (GCI). **Global Cybersecurity Outlook Report 2025**. Accessed September 10, 2025.
- International Telecommunication Union. **National Cybersecurity Strategy Guide for Libya**. ITU Publications, 2022.
- National Cyber Security Centre (NCSC). "Cyber Security Guidance." Accessed September 10, 2025. https://www.ncsc.gov.uk/guidance.

- National Institute of Standards and Technology (NIST). **Cybersecurity Framework**. 2022. https://www.nist.gov/cybersecurity/framework.
- Oxford Economics. **The Economic Impact of Cyberattacks on Libya's Energy Sector**. Oxford: Oxford Economics, 2024.
- Scott-Railton, John. **Cyber Technology and Threats in the 2011 Libyan Revolution**. AD1148875. Defense Technical Information Center, 2025.
- SANS Institute. "Understanding Cyber Threats." Accessed September 10, 2025. https://www.sans.org/cyber-security-training/understanding-cyber-threats/.
- World Economic Forum. **The Global Risks Report 2025**. 20th ed. https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf.
- International Organization for Standardization. **ISO 31000:2018 – Risk Management–Guidelines**.2018. https://lpm.uinsuka.ac.id/media/dokumen_akademik/011_20191007_ISO%2031000.2018%20-%20Risk%20Management%20-%20Guidelines.pdf.
- ISACA. **COBIT 2019 Framework: Governance and Management Objectives**. 2023. https://www.isaca.org/resources/cobit.
- ISO/IEC. **ISO/IEC 27001:2022 – Information Security Management Systems – Requirements**. 2022.
- Kaspersky. "Types of Cyberattacks." Accessed September 10, 2025. https://www.kaspersky.com/resource-center/definitions/types-of-cyber-attacks.