

الإستراتيجية المصرية في مكافحة التهديدات والجرائم السيبرانية -دراسة للواقع والرهانات-

Egypt's Strategy in Combating Cyber Threats and Crimes – A study of the Reality and Challenges-



د. أمينة بوبصلة

جامعة أحمد بوقرة بومرداس (الجزائر)

a.boubesla@univ-boumerdes.dz

تاريخ النشر: 2025/12/28

تاريخ القبول: 2025/12/17

تاريخ الارسال: 2025/10/01

ملخص:

تسعى الدراسة إلى البحث عن موضوع غاية في الأهمية، ألا وهو موضوع التهديدات السيبرانية ;الجرائم السيبرانية التي أضحت اليوم تشكل خطرا و تهديدا حقيقيا للأمن القومي للدول و الامن السيبراني. و عليه تعالج هذه المداخلة الإستراتيجية المصرية في مواجهة التهديدات السيبرانية –دراسة للواقع و الرهانات-و هذا من خلال مجموعة من النقاط أهمها البحث عن العلاقة بين الجريمة السيبرانية و الهجوم السيبراني في سياق الأمن السيبراني، بعدها نتطرق إلى أنواع و أنماط التهديدات و الهجومات السيبرانية التي يتعرض لها الأمن السيبراني المصري، بعدها نحاول الإلمام بالجهود التي قامت بها دولة مصر من اجل مواجهة التهديدات السيبرانية من خلال التشريعات القانونية أو البرامج و الآليات، و في الأخير تسعى إلى تبيان الرهانات و التحديات التي تواجه الأمن القومي المصري في ظل التهديد السيبراني.

الكلمات المفتاحية: الجريمة السيبرانية، الأمن السيبراني، الإستراتيجية، مصر، الرهانات.

تصنيف جال: k00.

Abstract:

The study seeks to examine a topic of utmost importance, namely cyber threats; cyber crimes that today pose a real danger and threat to national security and cyber security. This paper addresses Egypt's strategic response to cyber threats – a study of the reality and the stakes – through a series of points, the most important of which is the relationship between cybercrime and cyber attacks in the context of cyber security. We then address the types and patterns of cyber threats and attacks to which Egyptian cyber security is exposed. We then attempt to understand the efforts made by the Egyptian state to counter cyber threats through legal legislation, programmers and mechanisms. Finally, we seek to highlight the stakes and challenges facing Egyptian national security in light of cyber threats.

key words:

Cybercrime, cybersecurity, strategy, Egypt, stakes

JEL classification: k00.....

مقدمة:

شهد العالم في السنوات الماضية الكثير من التطورات المتسارعة في الفضاء السيبراني، و مازلنا نشهد رقمنة في مختلفة جوانب الحياة و الخدمات و ابتكار تكنولوجيا جديدة، و مع كل مرحلة تطويرية في قطاع الاتصالات و تكنولوجيا المعلومات نشهد كذلك تحديات جديدة.

إن قضية الأمن السيبراني أصبحت موضوع اهتمام بشكل متزايد خلال الفترة الماضية لا سيما بعد جائحة كوفيد19 التي اضطرت العديد من القطاعات الاعتماد على تكنولوجيا المعلومات و الاتصالات بشكل اكبر من ذي قبل. بدأت تظهر العديد من الأبعاد في هذا السياق، معظمها ذات طبيعة عابرة للحدود الجغرافية للدول كالأخبار الزائفة و أخلاقيات الفضاء السيبراني و الدبلوماسية السيبرانية و السيادة الرقمية، دلالة على تنامي التهديدات و التحديات السيبرانية التي ستواجه الدول الوطنية و مصر كغيرها من الدول عملت على اتخاذ إجراءات و استراتيجيات لمواجهة التحديات و التهديدات الأمنية السيبرانية التي يمكن أن تشكل تهديدا مباشرا لأمنها القومي.

أسباب و دوافع اختيار الموضوع: يندرج الدافع الأساسي في اختيار الموضوع هو نتيجة التطور و التحول الرقمي الحاصل في العلاقات الدولية، حيث اتجهت معظم دول العالم لوضع استراتيجيات و برامج من شأنها مجابهة التهديدات و الهجمات السيبرانية، و هذا بسبب انتشار الجرائم السيبرانية على نطاق واسع و هو ما يهدد الأمن السيبراني للدول.

كذلك التحول الرقمي الذي أصبح من الضرورات على الدول ان تتجه نحوه و هذا من لتوفير خدمات الكترونية متكاملة، و هو ما يستدعي توفير بيئة متينة للبنية التحتية لحماية البيانات الشخصية و الحكومية.

الإشكالية: سعت الدراسة إلى الإجابة على تساؤل رئيس يتمحور حول كيفية مواجهة مصر للتهديدات السيبرانية لحماية أمنها السيبراني؟

منهج التحليل المعتمد: انطلاقا من المقدمة، سنحاول من خلال هذه الدراسة بإتباع منهجي وصفي تحليلي، فالمنهج الوصفي الذي يستند إلى وصف الظاهرة المراد دراستها أما المنهج التحليلي من خلاله سنحاول تحليل الإستراتيجية المصرية لمواجهة الجرائم السيبرانية.

الفرضيات المعتمدة: و للمساهمة في الإجابة عن الإشكالية يمكن طرح الفرضية التالية:

إن تبني مصر لاستراتيجيات و برامج شاملة من شأنه أن يحد من التهديدات السيبرانية و مواجهة الجرائم السيبرانية.

أهداف المقال:

تهدف الدراسة إلى إبراز توجهات النظام المصري من خلال وضع إستراتيجية وطنية شاملة من أجل الحد من الهجمات السيبرانية في الفضاء الإلكتروني و الافتراضي، و ذلك بالاعتماد على أساليب و آليات و برامج جديدة تساهم في مكافحة الجرائم السيبرانية و الحد من التهديدات الإلكترونية سواء على مستوى الأفراد، الشركات او الحكومات.

- إبراز أهمية التشريعات و البرامج المتخذة من طرف مصر و جهودها المبذولة من أجل بناء منظومة أمنية واضحة المعالم لمواجهة و الحد من التهديدات السيبرانية.
- كذلك التحول الرقمي الذي أصبح من الضرورات على الدول أن تتجه إلى توفير خدمات الكترونية متكاملة، و هو ما يستدعي توفير بيئة متينة للبنية التحتية لحماية البيانات الشخصية و الحكومية.
- تقسيم العمل: لمعالجة هذه الموضوع تم تقسيم الدراسة إلى أربع محاور:
- مدخل مفاهيمي -الجريمة السيبرانية و الهجوم السيبراني، الأمن السيبراني.
- أنماط و مصادر خطورة التهديدات السيبرانية في دولة مصر.
- واقع الأمن السيبراني في مصر بالنسبة الى العالم "بالأرقام"
- جهود دولة مصر لمواجهة التهديدات السيبرانية-التشريعات القانونية، البرامج، الاستراتيجيات-
- الرهانات و التحديات التي تواجهها مصر لمستقبل آمنا سيبرانيا.
- نتائج الدراسة.

1. مدخل مفاهيمي-الجريمة السيبرانية، الهجوم السيبراني، الأمن السيبراني-

إن مفهوم الجرائم السيبرانية هو إحدى المفاهيم الحديثة التي أصبحت تعبر عن تلك الجرائم التي تقع او تكون مرتبطة بما يسمى بجرائم الفضاء الالكتروني او السيبراني و المتصل بتطور التقنيات المعلوماتية. إن الجرائم السيبرانية تعد من الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطورها، فكانت بداية من مصطلح إساءة استخدام الكمبيوتر، مرورا بمصطلح احتيال الكمبيوتر، والجريمة المعلوماتية، فاصطلاحات جرائم الكمبيوتر إلى جرائم الهاكرز، فجرائم الإنترنت، إلى آخر المصطلحات الجرائم السيبرانية.

1.1 تعريف الجريمة السيبرانية: فإننا نجد في كل مرة مع ظهور مصطلح جديد لجرائم الإنترنت يظهر لنا تعريفا جديدا، ففقهاء القانون لم يستقروا على تعريف واحد وذلك يرجع لحدثة الجرائم السيبرانية و الاختلافات الثقافية والقوانين بين الدول، فمنهم من عرف الجرائم السيبرانية: بأنها هي التي تتم بواسطة الكمبيوتر أو أحد وسائل التقنية الحديثة، و البعض الآخر عرفها: "بأنها نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود". (حميدة، 2021، صفحة 341)

يتكون مصطلح الجريمة الإلكترونية من جزئين: الجريمة والالكترونية. وهو يجمع بين الفكرة العامة للجريمة وطابعها الإلكتروني. الجريمة هي خرق للمعايير والضوابط التي يحددها المجتمع، وتسبب ضرراً للفرد والمجتمع، ويحدد القانون العقوبات التي تحمي المجتمع وتمثل الهيئة الاجتماعية عقابا او جزاء جنائيا. (سلام، 2020، صفحة 66)..

والجريمة الإلكترونية لها مسميات عدة منها: جرائم الحاسوب والإنترنت ، -جرائم التقنية العالية او بالجريمة الإلكترونية او الجريمة السيبرانية.....

2.1 مفهوم الهجوم السيبراني: الهجوم السيبراني هو محاولة غير شرعية من شخص أو جهة ما لاختراق نظام معلومات شخص آخر أو مؤسسة. غالبًا ما يسعى المهاجم للحصول على شيء مفيد من خلال تعطيل شبكة الضحية. ومع تزايد الجرائم السيبرانية كل عام، يحاول البعض استغلال الثغرات الأمنية في أنظمة الأعمال، وغالبًا ما يبحث المهاجمون عن فدية: حيث تسببت 53% من الهجمات الإلكترونية في أضرار تصل إلى 500,000 دولار أو أكثر. كما يمكن أن تأتي التهديدات السيبرانية بدوافع خفية، حيث يسعى بعض المهاجمين إلى محو الأنظمة والبيانات كنوع من التحدي.

(ماهو الهجوم الإلكتروني: ما التهديدات الإلكترونية الشائعة)، كما يعرف على أنه هو الاستغلال المتعمد لأنظمة الحاسب الآلي، والشبكات، والجهات التي يعتمد عملها على تقنية المعلومات والاتصالات الرقمية؛ بهدف إحداث الأضرار. و الهجمات الأكثر انتشاراً هي:

***هجمة تعطيل الخدمة (DoS):** هي محاولة لتعطيل النظام، وجعل خدماته غير متوافرة؛ عن طريق إرسال طلبات كثيرة من أكثر من مصدر في الوقت نفسه.

***التصيد (Phishing):** محاولة الحصول على معلومات حساسة مثل أسماء المستخدمين وكلمات المرور أو تفاصيل بطاقة الائتمان، غالباً لأسباب ونوايا ضارة وخبيثة، وذلك بالتنكر على هيئة جهة جديرة بالثقة.

***هجمة الاعتراض (Man in the Middle):** هي اعتراض المهاجم للاتصال بين طرفين عن طريق التنصت بهدف الاطلاع على البيانات أو تغييرها.

***البرمجيات الضارة (Malware):** برنامج يُصيب الأنظمة بطريقة خفية (في الغالب) لانتهاك سرية أو سلامة ودقة أو توافر البيانات أو التطبيقات أو نظم التشغيل. (ماهو الهجوم السيبراني، الهيئة الوطنية للأمن السيبراني، المملكة العربية السعودية، :، 2020).

3.1 مفهوم التهديدات السيبرانية: هذه هجمات تُنفذ باستخدام آليات وشبكات إلكترونية، كالإنترنت وأجهزة الحاسوب، بهدف إتلاف أجهزة أو شبكات إلكترونية أخرى أو سرقة المعلومات التي تحتويها. هذا يعني أن الطبيعة "الإلكترونية" للتهديدات تشير إلى كلّ من أداة الهجوم - الآليات المستخدمة - والطبيعة الإلكترونية للهدف. يمكن أن تتعرض الأهداف الإلكترونية لهجمات غير إلكترونية، كالهجمات الحركية أو الفيزيائية أو الكهرومغناطيسية، والتي قد تلحق بها الضرر أو حتى تُعطّلها. ومن المهم أيضاً ملاحظة أن التهديدات السيبرانية لا تستهدف الأفراد مباشرةً، بل تؤثر على الفضاء الإلكتروني، الذي أصبح جزءاً أساسياً من حياتهم. إنها تؤثر على الأنظمة والشبكات والأجهزة التي يستخدمها الأفراد والتي تعتمد عليها الدول، مما يؤثر على أسلوب الحياة نفسه بطرق تُهدد أمن الأمة بأكملها. ومع ذلك، فهي ليست موجهة ضد الأفراد، كما هو الحال مع الأسلحة التقليدية، التي يُمكن استخدامها للقتل المباشر.. (شفيق، 2020).

أما أنواع التهديدات السيبرانية فهي:

-التهديدات التي يتصدى لها الأمن السيبراني وهي 3 فئات:

***الجرائم الإلكترونية** تشمل أفراداً أو جماعات يهاجمون الأنظمة لتحقيق مكاسب مالية أو لتعطيلها.

***غالبًا ما تتضمن الهجمات الإلكترونية جمع معلومات ذات دوافع سياسية.**

- *يهدف الإرهاب الإلكتروني إلى إضعاف الأنظمة الإلكترونية وإثارة الذعر والخوف. كيف يسيطر المجرمون على أنظمة الحاسوب؟ إليك بعض الطرق الشائعة المستخدمة لتهديد الأمن السيبراني* :
- * البرمجيات الخبيثة: تُعد البرمجيات الخبيثة من أكثر التهديدات الإلكترونية شيوعًا. وهي برامج يُنشئها مجرمو الإنترنت أو القراصنة لتعطيل أو إتلاف جهاز كمبيوتر مستخدم شرعي. تنتشر البرمجيات الخبيثة غالبًا عبر مرفقات بريد إلكتروني غير مرغوب فيها أو تنزيلات تبدو شرعية. يمكن لمجرمي الإنترنت استخدامها لتحقيق الربح أو في هجمات إلكترونية ذات دوافع سياسية. هناك عدة أنواع من البرمجيات الخبيثة - :الفيروسات: برنامج يتكاثر ذاتيًا، يهاجم الملفات وينتشر في جميع أنحاء نظام الحاسوب، مُصيَّبًا إياها ببرمجيات خبيثة - .أحصنة*أحصنة طروادة: نوع من البرمجيات الخبيثة يتخفى في صورة برامج شرعية. يخدع مجرمو الإنترنت المستخدمين لتنزيل أحصنة طروادة على أجهزة الكمبيوتر الخاصة بهم، حيث تُلحق الضرر أو تجمع البيانات.
- * برامج التجسس: برنامج يُسجل نشاط المستخدم سرًا ليتمكن مجرمو الإنترنت من استغلال المعلومات. على سبيل المثال، يمكن لبرامج التجسس اعتراض بطاقات الائتمان.
- *برامج الفدية: برمجيات خبيثة تُشفّر ملفات وبيانات المستخدم، وتهدد بحذفها ما لم تُدفع فدية .
- *برامج الإعلانات: برمجيات إعلانية تُستخدم لنشر البرمجيات الخبيثة .
- *شبكات الروبوتات: شبكات من الحواسيب المُصابة ببرمجيات خبيثة، يستخدمها مجرمو الإنترنت لتنفيذ مهام عبر الإنترنت دون موافقة المستخدم. حقن لغة الاستعلامات الهيكلية (SQL) حقن لغة الاستعلامات الهيكلية (SQL) هو نوع من الهجمات الإلكترونية يُستخدم للسيطرة على قاعدة بيانات وسرقة بيانات منها. يستغل مجرمو الإنترنت ثغرات أمنية في التطبيقات المعتمدة على البيانات لحقن برمجيات خبيثة في قاعدة البيانات عبر أوامر SQL خبيثة، مما يتيح لهم الوصول إلى معلومات حساسة موجودة فيها.
- *التصيد الاحتيالي: يتضمن التصيد الاحتيالي مهاجمة مجرمي الإنترنت للضحايا برسائل بريد إلكتروني تبدو وكأنها أصلية ومن شركة قانونية، مطالبين بمعلومات سرية. يُستخدم هذا النوع من هجمات الهندسة الاجتماعية غالبًا لسرقة بيانات المستخدمين، بما في ذلك بيانات تسجيل الدخول وأرقام بطاقات الائتمان. يحدث ذلك عندما يخدع مهاجم، متظاهرًا بأنه جهة موثوقة، الضحية لفتح بريد إلكتروني أو رسالة فورية أو رسالة نصية. تنتشر هذه الهجمات على فيسبوك ومواقع التواصل الاجتماعي الأخرى، حتى باستخدام روابط وصفحات مزيفة تتطلب بيانات تسجيل دخول أو استخدام خدمة معينة. يحصل المهاجم في النهاية على هذه المعلومات ويستخدمها للسيطرة على الحسابات .
- *هجوم الوسيط: نوع من التهديدات الإلكترونية يعترض فيه مجرم الإنترنت الاتصالات بين شخصين لسرقة البيانات. على سبيل المثال، على شبكة واي فاي غير آمنة، يمكن للمهاجم اعتراض البيانات المنقولة بين جهاز الضحية والشبكة. (بدون مؤلف، 2021). و عليه ما هي أهداف التي يحققها الأمن السيبراني للدول في ظل تنامي التهديدات السيبرانية؟ و تتمثل في:
- ضمان توافر استمرارية عمل نظم المعلومات.

- اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حدٍ سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة، مع تعزيز حماية وسرية وخصوصية البيانات الشخصية و حماية الأنظمة التشغيلية من أي محاولات للولوج بشكل غير مسموح به لأهداف غير سليمة.

إن هدف الأمن السيبراني هو القدرة على مقاومة التهديدات المتعمدة وغير المتعمدة والاستجابة والتعافي، وبالتالي التحرر من الخطر أو الأضرار الناجمة عن تعطيل أو إتلاف تكنولوجيا المعلومات والاتصالات أو بسبب إساءة استخدام تكنولوجيا المعلومات والاتصالات. وهذا يتطلب حماية الشبكات وأجهزة الكمبيوتر، والبرامج والبيانات من الهجوم أو الضرر أو الوصول غير المصرح به، وبعبارة أخرى فإنه لا يعني أكثر من حماية البيانات. (حرشاي، 2017، صفحة 7)

4.1 الجريمة السيبرانية والهجوم السيبراني في سياق الأمن السيبراني:

عمومًا، بالطريقة التقليدية، ان مرتكبي الجريمة السيبرانية هم أفراد وليست دول. لقد تغير هذا الفهم بشكل ذاتي لأننا لم نشهد فقط تهديدات في أشكال حملات خاصة بهدف مالي أو ابتزاز للمعلومات من مجرمي الأنترنت، ولكن هويات أفراد من هذه الجماعات تهاجم لأسباب جغرافية سياسية.

إن التمييز بين الجريمة السيبرانية والهجوم السيبراني أمر بالغ الأهمية، فإننا ندرك أنه من الصعب في كثير من الأحيان معرفة ما إذا كان الحدث السيبراني واحدًا أو آخر (أو كلاهما)، في وقت وقوع الحدث - ويرجع ذلك جزئيًا إلى أن هوية الفاعل والقصد قد لا يكون واضحًا. ونظرًا للغموض الذي يحيط بهذا الأمر، يوصى برد فعل عاجل ومناسب على الجرائم السيبرانية أو الهجوم السيبراني. (مصر و الأمن السيبراني، مصر، 2023).

2. أنماط ومصادر خطورة التهديدات السيبرانية في جمهورية مصر

على الرغم من المزايا الإيجابية للفضاء الرقمي، إلا أنه يتضمن بعض المخاطر، حيث هو مكان لعدد من الأفراد الخطيرين، بالإضافة إلى وقوع جرائم قانونية مثل الشتم والكذب وخرق الخصوصية، في هذا الإطار، تواجه مصر مجموعة من التهديدات الإلكترونية، والتي يمكن تلخيصها في النقطة التالية من خلال تقديم مختلف أنواع وأساليب التهديدات الإلكترونية في مصر.

1.2 أنماط وأنواع التهديدات السيبرانية في مصر:

- جذب الجماعات المتطرفة للشباب المصري من خلال وسائل التواصل الاجتماعي: تستخدم الجماعات المتطرفة بفضل أداوتها الرقمية، مجموعة من التقنيات الحديثة لاستقطاب الشباب عبر الشبكات الاجتماعية و تقوم بترتيب حملات دقيقة و موجهة كما تهدف للاستفادة من جميع الوسائل التكنولوجية للتأثير في الشباب المصري و على جميع الفئات العمرية و الاجتماعية.

كما تسعى هذه الجماعات لتقديم أهدافها بشكل يجذب انتباه الشباب، مثل إنشاء فيديوهات بجودة عالية كما أن معظم أعضاء هذه التنظيمات يمتلكون حسابات شخصية على تويتر و فايسبوك و يستخدمون فيها قدرتهم على التأثير.

لقد تمكن تنظيم الدولة الاسلامية المعروف بداعش من استقطاب عدد من الشباب المصريين، و من ابرزهم اسلام يكن و صديقه محمود الغندور، بعد ان قام التنظيم بذبح 21 مصرياً قبطياً في فبراير 2015، اشاد الغندور بافعال اعضاء التنظيم، و هدد الجيش المصري بسبب قصفه لبعض مواقع التنظيم.

-التحريض و نشر الاخبار الكاذبة التي تهدد امن المجتمع: منذ 2011، شهدت مصر العديد من التغيرات والاضطرابات التي جعلتها ارضا خصبة لانتشار الشائعات. و قد ساهمت وسائل التواصل الاجتماعي في نشر الكثير من هذه الشائعات، فعلى سبيل المثال، الشائعات التي انتشرت بعد 30 جوان 2013 كانت نتيجة فعالة لنشر الرسائل التحريضية غير الصحيحة عبر هذه المنصات. (شريف، 2025).

-ارتفاع مستويات الجرائم الرقمية: شهدت مصر بعد ثورة 25 يناير 2011 تصاعد في الجرائم الالكترونية، خاصة مع تراجع الامن، حيث تتنوع اهداف مرتكبي الجرائم الرقمية في البلاد، سواء كانت للانتقام او التجسس او لابتزاز او تشويه السمعة. و تتعدد انواع و اشكال هذه الجرائم، مثل سرقة البريد الالكتروني و اختراق حسابات على وسائل التواصل الاجتماعي، بالاضافة الى الاحتيال و انتحال الشخصية. و من الجدير بالذكر ان مصر تعمل على اصدار تشريع شامل لمعاقبة مرتكبي الجرائم الالكترونية. (شريف، 2025).

2.2 العناصر الرئيسية لخطورة التهديدات السيبرانية في مصر: ترجع خطورة التهديدات السيبرانية إلى ثلاث عناصر رئيسية هي:

- استنادها إلى تقنيات متقدمة ومتطورة غالبا ما تكون تلك التقنيات حكرا على دول معدودة وشركات كبرى، كما أن كثير من تلك التقنيات سرية وغير متاحة للتصدير، وقد تحتوي النسخ المتاحة منها للتصدير على أبواب خلفية أو ثغرات تجعلها مصدرا لتهديدات إضافية .
 - سرعة وسهولة انتشارها حيث أن نشر الفيروسات الخبيثة أو شن هجمات إعاقة الخدمات وغيرها من الأخطار السيبرانية يمكن أن يحدث بسرعة فائقة وسهولة في ظل انتشار واتساع نطاق استخدام شبكات الاتصالات وتكنولوجيا المعلومات، ونظرا لسهولة شن الهجمات وبث الفيروسات عبر الحدود من أي مكان وبأرخص التكاليف، كما يصعب وقد يستحيل تعقب مصدر تلك التهديدات والأخطار في الوقت المناسب لتداركها والتغلب عليها.
 - اتساع نطاق تأثيرها سواء من حيث التأثير المباشر أو غير المباشر على البنى التحتية وما قد يتبعه من أضرار أو خسائر فادحة، وكذلك من حيث إمكانية الأضرار بمصالح الجهات العامة والخاصة والتأثير على جموع كبيرة من المواطنين (آلاف أو ملايين) بصورة مفاجئة وفي وقت قصير وعن بعد.
- (الإستراتيجية الوطنية للأمن السيبراني 2017-2021، صفحة 08).

إن غياب الوعي المجتمعي بالتهديدات والهجمات السيبرانية و ضعف التمويل اللازم لحماية البنية التحتية الرقمية، إضافة إلى صعوبة التنبؤ بالمخاطر وتوقعها وتجنبها و نقص عدد المختصين والتقنيين الذين يمتلكون المهارات اللازمة في مجال الأمن السيبراني كما ان ضعف الدور الإعلامي في التوعية بالجرائم التي

تهدد الأمن السيبراني ومحاربة الشائعات والأخبار المضللة و غياب الثقافة الرقمية للاستخدام الآمن والأمثل لإدارة البيانات بشكل فعال من قبل معظم أفراد المجتمع.

يجعل من الفضاء الافتراضي مفتوحا و هو ما يسهم في التطور السريع للجرائم السيبرانية و التكلفة التكنولوجية المرتفعة لحماية الأمن السيبراني، كما أن تطور أسلحة المجرم المعلوماتي واعتماده على تقنية عالية في التعامل مع التقنية المعلوماتية و العولمة الرقمية تؤدي إلى صعوبة التعرف على منفذي تلك الهجمات بسهولة و إلى السرعة في إتلاف الأدلة ومحو آثارها من قبل مرتكبي الجرائم السيبرانية مع وجود في بعض الأحيان جهات خارجية تتربص بالأمن القومي (سيداحمد، 2021، الصفحات 1794-1795) للدولة، و هو ما يجعل هذه الأخيرة تتخذ إجراءات و تتبنى برامج و سياسات من اجل حماية أمنها القومي و السيبراني .

3. واقع الأمن السيبراني في مصر بالنسبة إلى العالم "بالأرقام"

اظهر مؤشر الأمن السيبراني الذي أصدره الاتحاد الدولي للاتصالات، ان مصر احتلت المركز الثالث و العشرين في عام 2020 بين 182 دولة، محققة 95.45 درجة في حين كانت الولايات المتحدة في المقدمة بدرجة كاملة تبلغ 100، تلتها المملكة المتحدة في المركز الثاني بدرجة 99.54 وجاءت المملكة السعودية في المركز نفسه. كما وقد أشار التقرير أن مصر قامت بخطوات مهمة لتعزيز الأمن السيبراني، من بينها وطنية للأمن السيبراني تغطي الفترة 2017 إلى 2021، بالإضافة إلى إنشاء المركز الوطني للاستعداد لطوارئ الحاسبات والشركات. كما احتلت مصر أيضا الرتبة الأولى عالميا في كفاءة قطاعي الانترنت والهاتف في عام 2021، وفقا لمؤشر المعرفة العالمي.

من المهم الإشارة إلى أن الاتحاد الدولي للاتصالات المرتبط بالأمم المتحدة ينتج مؤشر الأمن السيبراني العالمي بشكل منتظم كل عامين، يعتمد هذا المؤشر على تقييم الدول من مئة نقطة وفق خمسة معايير، ومن هذه المعايير السياسات التنظيمية و القوانين ، البنى التحتية والمؤسسية و تنمية المهارات البشرية، وتوفر الكفاءات التقنية و الفنية المطلوبة. (مصر و الأمن السيبراني، مصر، 2023).

إن تحليل الموقف الراهن ومنظومة الأمن المصري السيبراني، وحصر نقاط القوة والضعف والتهديدات والفرص وتمثلت نقاط القوة في جهود الدولة المصرية في الحفاظ على الأمن السيبراني من خلال وجود إستراتيجية فعالة لإدارة مخاطر أمن المعلومات، ووجود إستراتيجية وطنية للأمن السيبراني والسعي لإرساء حوكمة الأمن السيبراني الذي يستهدف الاستقرار الاجتماعي والسياسي والاقتصادي، ولذلك تم افتتاح أقسام وتخصصات أكاديمية الأمن السيبراني في الجامعات مع زيادة الاهتمام ببحوث الأمن السيبراني وتطوير الإجراءات للمواجهة فضلا عن وجود هيئة وطنية تتولى الدفاع وتعزيز ودعم الفرق الفنية والتقنية المتخصصة في التقنية المعلوماتية وإصدار قانون للحماية المعلوماتية ووجود مركز للاستجابة الطارئة للآزمات السيبرانية ووجود قانون لمكافحة جرائم تقنية المعلومات إلا أنه لا تزال هناك نقاط ضعف متمثلة في غياب الوعي المجتمعي بالتهديدات والهجمات السيبرانية وضعف التمويل اللازم

لحماية البنية التحتية الرقمية ونقص المختصين والتقنيين المؤهلين وغياب الثقافة الرقمية للاستخدام الآمن.

ولكن لا تزال الفرصة سانحة باستغلال التطور التكنولوجي في تطوير عمليات الردع ووجود تعاون دولي للمواجهة وزيادة الوعي العالمي بالهجمات والتهديدات السيبرانية وإمكانية تحقيق التنسيق الدولي لمواجهة تهديدات الفضاء المفتوح ومخاطر الغزو الفكري. (السيد، 2021، صفحة 499)

4. جهود دولة مصر لمواجهة التهديدات السيبرانية-التشريعات القانونية، البرامج، الاستراتيجيات-

1.4 التشريعات والآليات القانونية للحد من انتشار الجرائم السيبرانية: لقد أبدت مصر استعدادها في مجال الأمن السيبراني عام 2017، حيث أصدر الاتحاد الدولي للاتصالات تقرير مؤشر قياس استعداد الدول في هذا المجال من أجل دفع المزيد من الجهود في مجال اعتماد الأمن السيبراني وتكامله على نطاق عالمي، حيث تصدرت المرتبة 14 من بين 193 دولة من دول كما جاءت في المرتبة الثانية عربيا فيما يتعلق بمستويات الالتزام بالأمن السيبراني بعد سلطنة عمان التي جاءت في المركز الرابع عالميا، و الأولى عربيا. أكد التقرير على أن مصر لديها استعداد قوى في مجال الأمن السيبراني من خلال هيكلية بنية تحتية وتبنيها استراتيجيات وطنية في هذا المجال، كما عقدت اتفاقيات عديدة دعت من خلالها لتبادل الخبرات ونشر ثقافة الوعي بالأمن السيبراني من خلال تبنيها سياسات وطنية، كما أن لديها الكثير من المبادرات والمبادرات والملتقيات والمنتديات وتدشين مؤتمرات واتفاقيات في مجال الأمن السيبراني، (اسلام، 2019، صفحة 161) إضافة إلى اتخاذها لقوانين تشريعية من أجل الحد من استغلال الإنترنت بشكل سيء و حماية لأمنها السيبراني. وقعت مصر مجموعة من الاتفاقيات و المعاهدات الدولية المرتبطة بأمن الانترنت، كما تم وضع قوانين تهدف إلى تنظيم هذا المجال، من بين هذه القوانين نجد قانون الملكية الفكرية رقم -82- لعام 2022، و قانون الاتصالات رقم -10- لعام 2003، و قانون التوقيع الالكتروني و لائحته التنفيذية رقم -15- لعام 2004، بالإضافة إلى ذلك، تم الأخذ ببعض مواد قانون الطفل رقم -12- لعام 1996 و تعديلاته بالقانون رقم -126- لعام 2008، مثل المادة 116 مكرر(أ) التي تتعلق بتجريم استغلال الأطفال و الاعتداء عليهم عبر الانترنت. هناك أيضا قانون المحاكم الاقتصادية رقم -120- لعام 2008، و كذلك يتم الاعتماد على بعض مواد قانون العقوبات رقم -58- لعام 1937، و قانون الإجراءات الضريبية رقم -150- لعام 1950 المعدل، و قانون الأحوال المدنية رقم -143- لعام 1994، حيث تجرم المادة 72 من قانون الأحوال المدنية أي محاولة للاطلاع أو الحصول على البيانات المخزنة على الحواسيب أو محاولة التصرف فيها، كما توضح المادة العقوبات الناتجة عن هذه الأفعال، و من الجدير بالذكر انه قد تم إعداد مسودة لقانون شامل خاص بأمن الانترنت قانون الأمن السيبراني، ولكنه لم يبحث بعد. (شريف، 2025).

2.4 الأطر التنظيمية لمواجهة الجريمة السيبرانية:

-الإطار التنظيمي والتنفيذي: وضع الإطار التنظيمي وإنشاء منظومة وطنية لحماية أمن الفضاء السيبراني وتأمين البنية التحتية للاتصالات وتكنولوجيا المعلومات ونظم وقواعد البيانات والمعلومات القومية وبوابات الخدمات الحكومية والمواقع الحكومية على الانترنت، وذلك بإعداد وتنفيذ ما يعرف بفرق الاستعداد والاستجابة لطوارئ الحاسبات والشبكات، في القطاعات الحيوية على المستوى الوطني، انطلاقاً من التجربة الرائدة في قطاع الاتصالات وتكنولوجيا المعلومات تكون هذه الفرق مسئولة عن أعمال المتابعة الأمنية لشبكات الاتصالات والمعلومات الوطنية والحاسب المتصلة بها، وعن التعامل مع أية أخطار سيبرانية تهددها أو هجمات سيبرانية توجه إليها، وعن التوعية والإعداد لمواجهةها.

- البحث العلمي والتطوير وتنمية صناعة الأمن السيبراني: تشجيع ودعم وتنمية البحث العلمي والتطوير ودعم التعاون بين الجهات البحثية والشركات الوطنية، خاصة في مجال تحليل البرمجيات الخبيثة. المتقدمة، ومجال تحليل الأدلة الرقمية، وفي مجال حماية وتأمين نظم التحكم الصناعية، ومجال تطوير أجهزة وأنظمة تأمين النظم والشبكات، ومجال التشفير والتوقيع الإلكتروني، ومجال حماية البنية التحتية للاتصالات وتكنولوجيا المعلومات، ومجال تأمين الحواسيب السحابية وحماية قواعد البيانات الكبرى ومجال تقنيات الذكاء الاصطناعي وانترنت الأشياء.

- تنمية الكوادر البشرية والخبرات اللازمة لتنفيذ منظومة الأمن السيبراني في مختلف القطاعات، بالتعاون والشراكة مع القطاع الخاص والجامعات ومؤسسات المجتمع المدني.

- التوعية المجتمعية: وضع وتنفيذ خطط وحملات للتوعية المجتمعية بالفرص والمزايا التي تقدمها الخدمات الإلكترونية المؤمنة للأفراد والمؤسسات، وبأهمية الأمن السيبراني لحماية تلك لخدمات من المخاطر والتحديات التي قد تواجهها، فضلاً عن حماية الخصوصية وإطلاق برامج حماية الأطفال والنشء على الانترنت.

أما آلية التنفيذ فقد أنشئت مصر المجلس الأعلى لتأمين البنية التحتية للاتصالات وتكنولوجيا المعلومات (المجلس الأعلى للأمن السيبراني): تبنت وزارة الاتصالات وتكنولوجيا المعلومات الدعوة لتشكيل مجلس أعلى لحماية البنية التحتية للاتصالات وتكنولوجيا المعلومات المجلس الأعلى للأمن السيبراني (يتبع مجلس الوزراء يرأسه وزير الاتصالات وتكنولوجيا المعلومات، وتمثل فيه الأطراف المعنية بالأمن القومي وإدارة وتشغيل البنية التحتية في القطاعات الحيوية والمرافق العامة، وذوي الخبرة في القطاع الخاص والجهات البحثية والتعليمية. حيث يتولى المجلس وضع إستراتيجية وطنية للأمن السيبراني ولمواجهة الهجمات السيبرانية، كما. يتولى الإشراف على تنفيذ تلك الإستراتيجية، مع ضرورة تحديثها تمشياً مع التطورات التقنية المتلاحقة. وقد بدأ المجلس عمله التمهيدي في يناير 2015، وقام رئيس مجلس الوزراء اعتماد تشكيل المكتب التنفيذي للمجلس ولجنته الفنية وتوصيف مهامه في جوان 2016. (الإستراتيجية الوطنية للأمن السيبراني 2017-2021، صفحة 10).

-فريق التعامل مع حوادث امن الحاسوب الذي يعرف ايضا باسم فريق الاستجابة لحالات الطوارئ الحاسوبية، هو مجموعة من المحترفين الذين يقومون بتلقي و تحليل و التعامل مع الحوادث الامنية

المتعلقة بالحواسيب. يمكن ان تكون هذه الفرق محدودة جغرافيا او متخصصة في مجالات معينة، ويشرف عليها اما مؤسسات حكومية او خاصة او كليهما. تلعب فرق التعامل مع حوادث امن الحاسوب دورا مهما في تبادل المعلومات لضمان الامان. حيث تسعى لتعزيز مستوى الامان المعلوماتي على مستوى الدولة، و تحمي البنية التحتية لتكنولوجيا المعلومات من المخاطر و التهديدات و الهجمات الالكترونية، و تقدم دعما تقنيا مبنيا للجهات الحكومية، و مع ذلك، و على الرغم من ان فرق التعامل مع حوادث امن الحاسوب تقوم بعمل رائع في العادة، فانها غالبا ما تعاني من نقص في التمويل، المعدات، العاملين. (المبادئ التوجيهية المتعلقة بآمن البنية التحتية للإنترنت في الدول العربية، ملخص تنفيذي،).

-نظمت مصر معرض معرض امن و مؤتمر امن المعلومات و الأمن السيبراني في 13-14 جوان 2022، جاء هذا المؤتمر تحت شعار الامن السيبراني في أوقات الأزمات بدعم من عدة وزارات و بمشاركة شركات كبيرة مثل " دل تكنولوجيا، أي فاينانس، مايكروسوفت، سيسكو، هواوي، انتل، اورانج، البنك التجاري الدولي، ستار لينك، سايشيلد، كاسبرسكي، بروف بوينت، سايبير فورس، سيتريكس، الكان تيلكوم، فيكسد جروب، فيس بوينت، فيكتوري لينك، " و تم تناول مواضيع حيوية في المؤتمر من خلال لقاءات و جلسات تفاعلية بين الجهات الحكومية و الشركات المصرية و الدولية الرائدة في مجال امن المعلومات، خلال الجلسات تم مناقشة موضوع الجيل الخامس من الحروب، و الذي يتناول الحرب السيبرانية، و ذلك في محاضرة خاصة ألقاها ممثل عن القوات المسلحة المصرية للمرة الأولى. كما تم طرح موضوعات تتعلق بالأمن السيبراني و المرونة الالكترونية، بالإضافة إلى جلسات تناولت الأمن السيبراني و الخدمات البنكية المفتوحة و الرقمية. (مصر و الأمن السيبراني، مصر، ، 2023).

3.4 إستراتيجية مصر في مكافحة الجرائم السيبرانية-رؤية مصر 2030:-

بسبب تزايد حجم التهديدات و الهجمات الالكترونية، بدأت مصر في تحسين قدراتها في الهجوم و الدفاع لمواجهة المخاطر المتعلقة بالحرب الالكترونية، بالإضافة إلى ذلك، تستثمر البلاد في تطوير البنية التحتية التكنولوجية و زيادة جاهزيتها للاستعداد للحرب الالكترونية، و هذا يظهر من خلال تبنيها لرؤية إستراتيجية مستقبلية لأمنها السيبراني تعرف برؤية مصر 2030.

أما بخصوص ركائز الرؤية الإستراتيجية فقد بدأت الرؤية الإستراتيجية و بنيت على عدة اسس و التي تشمل:- الرؤية المستقبلية لمصر 2030، التي تهدف الى تحقيق الاستقرار و التنمية المستدامة و ضمان الامن السيبراني و الاستراتيجي.

-المادة 31 من الدستور المصري، التي تنص على ان حماية الامن الالكتروني يعتبر من الامن القومي.
-الاستراتيجية لعام 2020 التي اعلنت عنها وزارة الاتصالات و تكنولوجيا المعلومات، و التي تركز على ثلاثة اهداف رئيسية: الانتقال الى مجتمع رقمي، و تعزيز صناعة تكنولوجيا المعلومات و الاتصالات، و تحويل مصر الى قطب و مركز رقمي عالمي. (سيداحمد، 2021، الصفحات 1795-1796)

أما أهداف الرؤية الإستراتيجية: وقد كانت من ضمن أهداف الرؤية الإستراتيجية
- تعزيز سياسات الأمن السيبراني، من خلال توفير الحماية الفعالة للبنية الحيوية التحتية

- تفعيل دور الإعلام في التوعية بمخاطر الفضاء السيبراني، خاصة في مجال التوعية بمخاطر وتهديدات الفضاء السيبراني.
- ضمان تحقيق التكامل والتعاون بين القطاعات والأجهزة لمواجهة المخاطر وتحقيق الاستجابة السريعة في مواجهة الأزمات السيبرانية.
- الاهتمام بدعم الوعي في مجال الأمن السيبراني بما يتوافق مع التطور التكنولوجي المتلاحق في الحوسبة السحابية. (السيد، 2021، صفحة 498).
- البرامج الإستراتيجية في المرحلة 2014-2021:
- برنامج لتطوير الإطار التشريعي الملانم لأمن الفضاء السيبراني و مكافحة الجرائم السيبرانية و حماية الخصوصية، و حماية الهوية الرقمية.
- برنامج تطوير منظومة وطنية متكاملة لحماية امن الفضاء السيبراني و تأمين البنى التحتية للاتصالات و تكنولوجيا المعلومات.
- برنامج لحماية الهوية الرقمية (برنامج المواطنة الرقمية) و تفعيل البنى التحتية اللازمة لدعم الثقة في التعاملات الالكترونية بوجه عام و في الخدمات الحكومية الالكترونية بوجه خاص.
- برنامج لإعداد الكوادر البشرية و الخبرات اللازمة بتفعيل منظومة الأمن السيبراني في مختلف القطاعات.
- برنامج للتوعية المجتمعية بالفرص و المزايا التي تقدمها الخدمات الالكترونية للأفراد و المؤسسات والجهات الحكومية، و بأهمية الأمن السيبراني لحماية تلك الخدمات من المخاطر و التحديات التي قد تواجهها.
- (الإستراتيجية الوطنية للأمن السيبراني 2017-2021، صفحة 12).
- في اطار جهود الدولة لدعم الامن القومي و تنمية المجتمع المصري، و مع تزايد التهديدات و التحديات المستقبلية في المجال السيبراني و المجتمع الرقمي و لرصد و مجابهة المخاطر و التهديدات المتزايدة، و التزاما بالمادة 31 من الدستور المصري الصادر عام 2014، ثم الدعوة الى انشاء المجلس الاعلى لتأمين البنى التحتية للاتصالات و المعلومات " المجلس الاعلى للامن السيبراني" التابع لرئاسة مجلس الوزراء و وزير الاتصالات و تكنولوجيا المعلومات. و اما تقوم به الدولة المصرية من اجراءات للتقدم نحو تحقيق تلك الاهداف لمواجهة الاخطار السيبرانية.
- و يعد اعلان شركة Treand Micro المتخصصة في امن المعلومات بانه تم معالجة اكثر من 12 مليون تهديد الكتروني في مصر في النصف الاول من عام 2020، و اشارت الى انه تم اكتشاف اكثر من 235 الف هجوم برمجيات خبيثة في مصر، و تم العثور على اكثر من 6.8 مليون تطبيق خبيث للهواتف المحمولة.
- كما اسهمت "تريدن مايكرو" في تحديث و ايقاف من 740.000 هجمة عبر البارمج الضارة، و كذلك صد و ايقاف اكثر من 1600 هجمة عبر البرامج الضارة التي استهدفت مواقع بنكية و مصرفية، بالاضافة الى ذلك اظهر التقرير تحولا في الاستراتيجيات التي يستخدمها مجرمو الانترنت، الذين حولوا تركيزهم خلال النصف الاول من عام 2020 نحو استغلال اثار فيروس كورونا -كوفيد19-، تفتقت المخاطر التي تتعرض لها الشركات بسبب الثغرات الامنية الناتجة عن العمل عن بعد. و من اصبحت الشبكات المنزلية في مصر

المصدر الرئيسي لاستقطاب مجرمي الانترنت الذين يستهدفون الانظمة و الاجهزة و الشبكات. (عبد العال، 2022، الصفحات 277-281)

-استراتيجية الوطنية للأمن السيبراني 2022-2026:

تهدف الى مكافحة التحديات و المخاطر العالمية الناجمة عن التهديدات السيبرانية و ذلك من خلال مجموعة من الخطوات التي تدعم لجهود الدولة الامن القومي، و تنمية المجتمع المصري تم اصدار الاستراتيجية الوطنية للأمن السيبراني التي تهدف الى مكافحة الاخطار السيبرانية و ذلك من خلال رصد و مواجهة التهديدات و التحديات المستقبلية في مجال الامن السيبراني و المجتمع الرقمي بما يساهم في تحقيق تنمية اجتماعية و اقتصادية شاملة، و حماية المواطنين من المخاطر في الفضاء السيبراني، و الحفاظ على مصالح الدولة العليا، و هذا ما اكده الدكتور "عمرو طلعت" وزير الاتصالات و تكنولوجيا المعلومات على ضرورة مواكبة الاستراتيجية للأمن السيبراني 2022-2026 لكافة المستجدات و احدث التكنولوجيات و التقنيات في مجال الامن السيبراني حتى تصبح قادرة على التصدي للتحديات و المخاطر العالمية الناجمة عن التهديدات السيبرانية، على النحو الذي يدعم جهود الدولة في بناء مصر الرقمية و التي يتم من خلالها رقمنة الخدمات الحكومية و تبني المعاملات الرقمية. (عبد العال، 2022، صفحة 281).

5. الرهانات و التحديات التي تواجهها مصر لمستقبل أمنها سيبرانيا.

لم تقتصر إنجازات مصر على التصنيف العالمي فحسب، بل برزت أيضاً على المستوى الإقليمي والدولي. ففي عام 2024، حصلت مصر على المركز الثاني في مسابقة "سايردريل" الدولية التي أقيمت في دبي تحت رعاية الاتحاد الدولي للاتصالات، متفوقة على دول مثل إيطاليا وتركيا والهند. كما أن تصنيف مصر في الفئة الأولى إلى جانب دول مثل الولايات المتحدة واليابان والإمارات يؤكد ريادتها في المنطقة العربية. تأثير الإنجاز على التحول الرقمي يأتي هذا التقدم في إطار رؤية مصر للتحول الرقمي، حيث تسعى الدولة إلى بناء "مصر الرقمية" من خلال رقمنة الخدمات الحكومية وتعزيز البنية التحتية التكنولوجية. وقد ساهمت هذه الجهود في تحسين ترتيب مصر في مؤشرات أخرى، مثل: المركز الأول إفريقياً في سرعة الإنترنت الثابت، بعد أن كانت في المركز 40 قبل ست سنوات. تقدم 49 مركزاً في مؤشر جاهزية الحكومة للذكاء الاصطناعي، مما يعكس التزام مصر بمواكبة التقدم التكنولوجي.

على الرغم من هذا الإنجاز، تواجه مصر تحديات مستمرة مع تزايد التهديدات السيبرانية العالمية، مثل البرمجيات الخبيثة، الاحتيال الإلكتروني، والهجمات على البنية التحتية الحيوية. ومع ذلك، فإن استثمار مصر في تطوير الكوادر البشرية، تحديث التشريعات، وتعزيز التعاون الدولي يضعها في موقف قوي لمواجهة هذه التحديات. كما يتوقع الخبراء استمرار تحسن ترتيب مصر في المستقبل مع التوسع في تطبيقات التحول الرقمي وزيادة الاستثمارات في الأمن السيبراني. (ترتيب مصر في الأمن السيبراني: إنجاز عالمي يعكس الريادة الرقمية، 2025)

6.الخاتمة:

نستنتج مما سبق أن الأمن السيبراني في مصر قد تجسد في عدة ممارسات لحمايته و التغلب أو الحد من المخاطر و التهديدات التي قد تنتج عنه كالتحديات الاجتماعية و الأمنية.

و عليه عمدت مصر إلى تبني سياسات تراوحت بين الأمنية و اطر قانونية و أخرى تنظيمية دون أن ننسى تهيئة بنية إعلامية و تقنية لتوعية الرأي العام المصري بخطر تهديد الأمن السيبراني و القومي المصري.

كما يبرز دور مصر في تجسيد الأمن السيبراني من خلال استحداث مركز الطوارئ و إنشاء المجلس الأعلى للأمن السيبراني الذي يخضع لوزارة الاتصالات، إضافة إلى غرفة صناعة تكنولوجيا المعلومات و الاتصالات و مركز معلومات بمجلس الوزراء، كل هذا سينعكس على تحقيق الأمن السيبراني و القومي لمصر.

و في الأخير إن خطورة الجرائم و التهديدات السيبرانية كبيرة جدا، خاصة إذا لم يتم السيطرة عليها، فالقضاء عليها أو الحد منها يتطلب تنفيذ سياسات و آليات لازمة للتقليل من مخاطرها، باعتبار أن هذه الجريمة في تطور دائم و تحديث كبير و جب على مصر تكثيف و تنسيق التعاون المشترك مع كل الجهات الفاعلة و هذا للحفاظ على أمنها القومي مع تعزيز رؤيتها المستقبلية رؤية 2030.

6.قائمة المراجع:

- الاتحاد الدولي للاتصالات،(2006)، " دليل الأمن السيبراني للبلدان النامية".
- الإستراتيجية الوطنية للأمن السيبراني 2017-2021، جمهورية مصر العربية: رئاسة مجلس الوزراء، المجلس الأعلى للأمن السيبراني.
- المبادئ التوجيهية المتعلقة بأمن البنية التحتية للإنترنت في الدول العربية، ملخص تنفيذي، تاريخ الاسترداد 2025/09 /13، من [@internet.society.org](http://internet.society.org)
- أميرة محمد محمد سيداحمد، (جولية، 2021)، استراتيجيات مكافحة الجرائم الالكترونية في العصر المعلوماتي تعزيزا لرؤية مصر 2030: دراسة استشرافية، مجلة البحوث الإعلامية، العدد58، الجزء 04، الصفحات 1794-1795.
- بدون مؤلف. (2021/09/04). "ماهو الأمن السيبراني و أنواع التهديدات السيبرانية"، تاريخ الاسترداد 2025, 09 10 <https://www.howtechs.net>
- جيهان احمد عبد العال، الجهود المصرية لمواجهة التحديات السيبرانية، مجلة في البحوث الاعلامية، المجلد13، العدد02، 277-281.
- راضية حميدة، (ديسمبر , 2021)، "الجريمة الالكترونية عبر مواقع التواصل الاجتماعي...نحو تفعيل دور الأمن السيبراني المعلوماتي"، مجلة الإعلام و المجتمع، المجلد05، العدد02، صفحة 314.
- سميرة بارة، (جولية , 2017)، " الدفاع الوطني و السياسات الوطنية للأمن السيبراني في الجزائر: الدور و التحديات"، المجلة الجزائرية للأمن الإنساني، العدد04، الصفحات 258-259.

- صالح بن علي بن عبد الرحمن الربيعه، (2017)، "الأمن الرقمي و حماية المستخدم من مخاطر الانترنت"، المملكة العربية السعودية: هيئة الاتصالات و تقنية المعلومات.
- عنترة بن مرزوق، محي الدين حرشاي، (06 06, 2017)، "الأمن السيبراني كبعد جديد في السياسة الدفاعية للجزائر"، تاريخ الاسترداد 2025/09/12، من www.manifest.univ-ourgladz.dz
- فوزي اسلام، (ماي، 2019)، "الأمن السيبراني: الأبعاد الاجتماعية و القانونية تحليل سوسيولوجي"، المجلة الاجتماعية القومية، المجلد56، العدد02، صفحة 161.
- لامية طالة، كهيبة سلام، (2020)، " الجريمة الالكترونية: بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الاجتماعي"، مجلة الرواق للدراسات الاجتماعية و الإنسانية، المجلد06، العدد02، صفحة 66.
- ماهو الهجوم الالكتروني: ما التهديدات الالكترونية الشائعة، (بلا تاريخ)، تاريخ الاسترداد 2025/09/10، www.cisc.com
- ماهو الهجوم السيبراني، الهيئة الوطنية للأمن السيبراني، المملكة العربية السعودية، (16 02, 2020). تاريخ الاسترداد 2025/09/10، من المركز الوطني الإرشادي للأمن السيبراني: www.cert.gov.sa
- مصر و الأمن السيبراني، مصر، (11 06, 2023). تاريخ الاسترداد 2025/09/11، من الهيئة العامة للاستعلامات: www.sis.gov.eg
- منى الأشقر جبور، (2012)، "الأمن السيبراني: التحديات و مستلزمات المواجهة"، جامعة الدول العربية: المركز العربي للبحوث القانونية والقضائية، اللقاء السنوي الأول للمتخصصين في امن و سلامة الفضاء السيبراني.
- نهى مجدي محمد السيد، (ديسمبر، 2021)، "الأمن السيبراني و علاقته بالمضمون الإعلامي في ظل رؤية مصر 2030"، المجلة العربية لبحوث الإعلام و الاتصال، العدد35، صفحة 498.
- نورالدين فلاك، (08 12, 2021)، " التهديدات السيبرانية عبر الفضاء الأزرق وتأثيرها على الأمن القومي للدول"، تاريخ الاسترداد 2025/09/12، من جريدة الشعب الالكترونية.
- نوران شريف، (بلا تاريخ)، معضلة السيطرة: تهديدات الأمن السيبراني في مصر.. هل الرقابة هي الحل؟، تاريخ الاسترداد 2025/09/10، من المركز الإقليمي للدراسات الإستراتيجية، مجموعة الخدمات البحثية: <https://rsgleb.org>
- نوران شفيق، (20 01, 2020)، " أشكال التهديدات الإلكترونية ومصادرها"، تاريخ الاسترداد 2025/09/10، من المركز الأوروبي لدراسات مكافحة الإرهاب و الاستخبارات، وحدة الدراسات و التقارير: <https://www.europarabct.com>