Naif Arab University for Security Sciences
Arab Journal for Security Studies
المجلة العربية للدراسات الأمنية
https://journals.nauss.edu.sa/index.php/ajss
AJSS

Security Response to Emerging Cyberattacks That Impact National Security

المواجهة الأمنية للاختراقات الإلكترونيَّة المُستحدثة المؤثرة على الأمن القومي

سعد مفلح حمود الصويلح
وزارة الداخلية، دولة الكويت

Saad Mefleh Humoud Alsuwaileh
Ministry of Interior, State of Kuwait

Received on 18 Feb. 2025; accepted on 15 Apr. 2025; available online 24 June 2025

Abstract

This study examines cybercrimes as a modern threat to national security, intensified by the digital revolution and rapid advancements in artificial intelligence (AI). It highlights how sophisticated cyberattacks—such as AI-driven financial fraud and Distributed Denial of Service (DDoS) attacks—target governments, corporations, and individuals, exploiting vulnerabilities in cyberspace's borderless and complex nature. Using descriptive and analytical methods, the research explores cyber breaches' impacts on national security and digital infrastructure, while evaluating countermeasures like quantum encryption and AI-based defenses. Key recommendations include strengthening national and international cybersecurity laws, integrating quantum computing and blockchain technologies, fostering technical expertise, and promoting preventive strategies that combine enhanced security protocols with public awareness campaigns. The study underscores the urgency of global collaboration, updated legislation, and innovative infrastructure protection to mitigate evolving cyber threats like social engineering and advanced persistent attacks.

Keywords: *security studies, cybersecurity, emerging crimes, cyber hacking, electronic infrastructure, security prevention*

المستخلص

تناولت الدراسة الجرائم السيبرانيَّة باعتبارها تهديدًا مستحدثًا للأمن القومي؛ نتيجة الثورة الرقمية والتطورات التقنية الهائلة للذكاء الاصطناعي؛ حيث تمثِّل الهجمات الإلكترونية تهديدًا جسيمًا للأمن القومي والدولي، مستهدفةً الحكومات والشركات والأفراد عبر تقنيات متطوِّرة يصعب تتبعها، وتبرز مشكلة الدراسة في البحث عن حلول أمنية سيبرانية وإعلامية لمواجهة جرائم سيبرانية حديثة كالاحتيال المالي المُوجه بالذكاء الاصطناعي وهجمات حجب الخدمة (DDoS)، التي تُعَدُّ جرائم عابرة للحدود مرتبطة بتعقيدات الفضاء السيبراني وتحدياته الأمنية، وتكمن أهمية الدراسة في تعزيز آليات حماية المجتمعات من مخاطر هذه الجرائم التي تهدد الأمن الوطني والاقتصادي. كما اعتمدت الدراسة المنهجَين الوصفي والتحليلي من خلال تناول صور الاختراقات الإلكترونية وتأثيرها على الأمن القومي والبنية التحتية الرقمية وآليات المواجهة الأمنية كالتشفير الكمي وتقنيات الذكاء الاصطناعي، وخلصت الدراسة إلى ضرورة تعزيز التشريعات الوطنية والدولية، وتعزيز أنظمة الأمن السيبراني والاستعانة بالحوسبة الكمومية، وبناء الكفاءات التقنية، وتبني إستراتيجيات شاملة تجمع بين الأمن الوقائي والتوعية المجتمعية، وتحديث القوانين لمواكبة التهديدات الناشئة، وتعزيز التعاون الدولي، ورفع الوعي بأخطار الهجمات السيبرانية، مع التركيز على حماية البنى التحتية الحيوية عبر تقنيات مبتكرة كالبلوك تشين.

الكلمات المفتاحية: الدراسات الأمنية، الأمن السيبراني، الجرائم المستحدثة، الاختراق الإلكتروني، البنية التحتية الإلكترونية، الأمن الوقائي

* Corresponding Author: *Saad Mefleh Humoud Alsuwaileh*
Email: saaad-78@hotmail.com

doi: 10.26735/GMHF2653

1. المقدمة

أصبحت الهجمات الإلكترونية تشكِّل تهديدًا كبيرًا للأمن الدولي، ولا سيما في خضم التطور التقني الهائل في ظل الثورة المعلوماتية، حيث تستهدف الحكومات والشركات والأفراد على حد سواء. وتُعدُّ هذه الهجمات حديثة العهد؛ نتيجة لاستخدام تقنيات متطورة؛ مما يزيد من تعقيدها وصعوبة تتبعها.

وعلاوة على أخطار الإرهاب التقليدي المعروفة، التي كانت أحد الأسباب الرئيسة في إيلاء أعضاء الجماعة الدولية - دولًا ومنظمات - الاهتمام الواسع بهذه الظاهرة، من حيث بيان صورها وأسبابها وتدابير مكافحتها، فقد أدَّى تسخير التنظيمات والجماعات الإرهابية للإنترنت؛ واختراق المؤسسات الحيوية بالدولة، وتعطيل الخدمات الحكومية الإلكترونية ومحطات الطاقة، وتدمير المواقع المعادية، إلى زيادة وعي الدول بأهمية وضرورة إصدار تشريعات وتبني تدابير دولية ووطنية أكثر فاعلية لمواجهة ظاهرة «الإرهاب السيبراني» (قادم، 2022، ص. 185).

مشكلة الدراسة

تتمثل المشكلة البحثية لهذه الدراسة في محاولة إيجاد الحلول الأمنية والإعلامية لمواجهة جرائم الاحتيال المالي والاختراقات الرقمية الموجهة بالذكاء الاصطناعي وهجمات منع الخدمة (DDoS) وذلك لكونها جريمة حديثة مرتبطة بكافة أوجه التكنولوجيا والفضاء السيبراني كواقع افتراضي بما يحويه من صعوبات مادية، سواء أكان في الجانب القانوني أو الجانب الأمني؛ ولكونها جريمة عابرة للقارات؛ حيث تزايد ارتكاب الجرائم السيبرانية من جراء تطور وسائل الاتصال وتكنولوجيا المعلومات؛ حيث تستهدف اختراقات وانتهاكات الرقمنة الإلكترونية وجمع المعلومات التي تستهدف الأجهزة الذكية المتصلة بالإنترنت، ومع التوسع في استخدام شبكة الإنترنت التي تجاوز عدد مستخدميها 5 بلايين مستخدم في 2025، فقد فرض هذا تعزيز المواجهة الأمنية للاختراقات الإلكترونية المستحدثة ومعالجة نقاط الضعف في منظومة الأمن السيبراني، مع تكثيف الجهود الإعلامية لحماية المجتمع (عبد العال، 2022، ص.67).

أهمية الدراسة

ترجع أهمية الدراسة إلى كشف طبيعة الجرائم السيبرانية التي تنفذها المنظمات الإجرامية عبر توظيف تقنيات الذكاء الاصطناعي لابتكار تطبيقات خبيثة، تُهدد أمن الأفراد والدول والبنية التحتية الرقمية؛ وذلك عبر استغلال التعقيدات التقنية لمنع التعقب أو الضبط؛ مما يفرض على المؤسسات الأمنية تطوير إستراتيجيات ردع ذكية لمراقبة الشبكات الدولية، ورصد السلوكيات غير الطبيعية التي تستهدف انتهاك الرقمنة والتطبيقات من خلال تعزيز الأمن السيبراني باستخدام تطبيقات الذكاء الاصطناعي والحوسبة الكمومية، بالإضافة إلى استخدام التكنولوجيا الناشئة «الحوسبة الكمومية» لعدم إلحاق الضرر بالمصالح العامة الرقمية وتعزيز المواجهة الأمنية؛ حيث يواجه العالم تحديات متزايدة في مجال الأمن الرقمي، مع تزايد التهديدات السيبرانية والانتهاكات الإلكترونية؛ مما يستدعي تبني إستراتيجيات فعَّالة للحماية والتصدي لهذه التحديات.

منهج الدراسة

ارتكزت الدراسة إلى منهجين: أحدهما وصفي، والثاني تحليلي، مشتملة على مباحث ثلاثة بيَّنت ماهية الجريمة السيبرانية، ومخاطرها وتأثيرها على الأمن، والتعرف على الآليات الحديثة لتأمين المعلومات، ومكافحة الجرائم السيبرانية والتصدي لها.

2. المبحث الأول: صور الاختراقات الإلكترونية المؤثرة على الأمن القومي

يُعدُّ الأمن السيبراني أداة إستراتيجية مهمة لكل من الحكومات والأفراد، خاصةً في ظل تحول الحرب السيبرانية إلى عنصر أساسي في التكتيكات الحديثة للصراعات والهجمات بين الدول. ويشمل الأمن السيبراني حماية المعلومات على أجهزة الحاسوب والشبكات، ويتضمن العمليات والآليات التي تهدف إلى تأمين المعدات والمعلومات والخدمات من أي تدخل غير مصرح به، أو تغيير أو تلف. ويمكن اعتبار تحديات الأمن السيبراني من أبرز التحديات التي تواجه الأمن القومي في القرن الحادي والعشرين؛ حيث إن المفهوم الحديث للأمن لا يقتصر على الجوانب العسكرية فحسب، بل يتناول جميع التهديدات التي قد تعوق الاقتصاد الرقمي، وتدفق المعرفة. وقد أسهمت تكنولوجيا المعلومات والاتصالات في تجاوز الحدود الجغرافيَّة والسياسيَّة والثقافيَّة بين الدول؛ مما يهدد السيادة الوطنية، خاصة في ظل حالات اختراق المواقع الحكومية والتجسس المعلوماتي (رمضان، 2021، ص.217).

2. 1 المطلب الأول: تعريف الجرائم الإلكترونية وأنواعها

تُعدُّ الجريمة الإلكترونية «السيبرانية» نوعًا متقدمًا من الجرائم العابرة للحدود؛ حيث يسهم تزايد نشاط جماعات الجريمة المنظمة في تعقيد هذه الظاهرة. وتحدث هذه الجرائم في الفضاء الإلكتروني الذي لا يعرف حدودًا، مما يتيح لمرتكبيها وضحاياهم التواجد في مناطق

جغرافية مختلفة. كما تمتد آثار هذه الجرائم لتشمل مجتمعات متعددة حول العالم؛ مما يبرز أهمية وضع استجابة سريعة وفعَّالة على الصعيدين الدولي والديناميكي (خليفة، 2017، ص.211).

تعريف مصطلح الفضاء السيبراني

لقد استخدم مصطلح الفضاء السيبراني لأول مرة وفقًا للبعض من قبل كاتب الخيال العلمي ويليام جيبسون (William Gibson) في رواية نشرها عام 1984 بعنوان (Neuromancer) وصف فيها الفضاء السيبراني بأنه شبكة من الحواسيب في عالم مليء بكائنات الذكاء الاصطناعي (آل جار الله، 2019، ص.79)، وفي وقت لاحق استعير هذا المفهوم لوصف شبكات الاتصالات وتقنيات الواقع الافتراضي الناتجة عن تشابك مئات الملايين من الحواسب وغيرها من مكونات البنية التحتية للإنترنت (Schwab)، يقول ويليام في روايته عن الفضاء السيبراني: إنه هلوسة توافقية يتعرض لها يوميًّا الملايين من المشغلين الشرعيين في كل دولة. تعقيد لا يمكن تصوره، تباينت فيه خطوط الضوء في الفضاء اللامركزي للعقل ومجموعات البيانات. (Desforges, 2021, pp. 67 - 81)

أنواع الجرائم السيبرانية

وكثيرة هي الأنواع التي تحتويها الجرائم الإلكترونية من الهجمات والاختراقات السيبرانية التي تشمل:

1. **الهجمات السيبرانية Cyber Attacks:** هي محاولة لإلحاق الضرر بنظام الكمبيوتر الخاص بشخص ما أو كيان ما أو المعلومات الموجودة عليه باستخدام الإنترنت.
2. **الاحتيال السيبراني:** تلك العمليَّة التي تستخدم فيها تقنيات الحاسوب للاحتيال على الأفراد أو المؤسسات، والحصول على المال أو المعلومات بشكل غير مشروع.
3. **الاختراق السيبراني:** عمليَّة الدخول إلى الأنظمة أو الشبكات الإلكترونية بشكل غير مشروع، والاستيلاء على المعلومات أو التلاعب بها أو تدميرها (Brundage, et al. 2018).
4. **التجسس السيبراني:** عملية توظيف تقنيات الحاسب الآلي؛ للحصول على المعلومات السرية أو الحساسة من الأنظمة السيبرانية أو الشبكات الإلكترونية، وذلك للاستخدام غير المشروع لهذه المعلومات وتعطيل الأنظمة.

ويتمثل ذلك فيما يأتي:

الجرائم ضد الإنسانية

- جُرم نشر وتوزيع المعلومات العنصرية بوسائل معلوماتية.
- جُرم تهديد أشخاص، (الأشقر، 2016، ص. 155).
- جُرم توزيع معلومات وظيفتها إنكار أو تشويه أو تبرير أعمال إبادة جماعية أو جرائم ضد الإنسانية، باستخدام الوسائل ذات الطابع الإلكتروني.
- جُرم المساعدة أو التحريض بالوسائل المتصفة بالإلكترونية على ارتكاب جرائم ضد الإنسانية (الدريني، 2021، ص. 310-345).

جرائم الاستغلال الجنسي للرقيق الأبيض

الجرائم التي تُظهرها الأفعال التي تتعلق باستغلال الرقيق في أعمال جنسية، والاتجار بهم وتشمل:

- الرسومات، أو الصور أو الكتابات، أو الأفلام أو الإشارات (محمد، 2021، ص. 58).
- الأعمال المنافية للآداب والوسائط الإباحية التي يكون أبطالها القاصرين، وتبث إلكترونيًّا.

الجرائم المعلوماتية ضد الدولة والسلامة العامة

تتضمن الأفعال الجرميَّة الناشئة عن المعلوماتيَّة التي تستهدف استقرار وأمن الدولة، وهي:

- تعطيل الأعمال الحكومية أو أعمال السلطة العامة باستعمال وسيلة معلوماتية.
- الإخفاق في الإبلاغ أو الإبلاغ عن قصد بشكل خاطئ عن جرائم المعلوماتية، والاطلاع أو الحصول على معلومات ليست متاحة للجميع، بواسطة الشبكة العنكبوتية.
- جرائم التعدي على البيانات المعلوماتية التي تمس الدولة، وتشمل الجرائم المتعلقة بالبيانات المعلوماتية تلك التي تستهدف المعلومات المخزنة، مثل: جرائم التعرض للاطلاع على البيانات، وجرائم اعتراض المعلومات. وتتضمن هذه البيانات كل ما يمكن تخزينه ومعالجته وتوليده ونقله عبر الحاسوب، مثل: الأرقام، والحروف والرموز وغيرها. كما تشمل هذه الجرائم أيضًا تعطيل الأجهزة وتدمير المعلومات المخزنة عليها باستخدام أي وسيلة متاحة للأفراد عبر الحاسوب أو الإنترنت.

الجرائم الواقعة على الأموال

- جرم الاختلاس أو سرقة أموال بوسيلة معلوماتية.
- أعمال التسويق والترويج غير المرغوب فيها؛ مما يؤثر على استقرار الاقتصاد الوطني واستقرار الدولة المالي.

- الاستيلاء على أدوات التعريف والهوية المُستخدمة في نظام معلوماتي، والاستخدام غير المشرع لها وجرم الاطلاع على معلومات سرية، أو حساسة أو إفشاؤها.

جرائم تُرتكب ضد الأفراد

ثمة جرائم عدة تنطوي تحت مظلة الجرائم السيبرانية تنفذ ضد الأفراد تتمثل فيما يأتي:

1. إساءة استعمال الأجهزة والبرامج المعلوماتية

تشمل هذه الجرائم كلَّ من قام بتقديم، أو إنتاج أو توزيع، أو حيازة جهاز أو برنامج معلوماتي، أو أي بيانات معلوماتية مُعدَّة، أو كلمات مرور أو رموز دخول، بهدف ارتكاب أي من الجرائم التي تتعارض مع القانون.

2. الجرائم التي تمس المعلومات الشخصية

تشمل الأفعال الجرمية المتعلقة بمعالجة البيانات الشخصية دون الحصول على تصريح أو ترخيص سابق يسمح بذلك، بالإضافة إلى إنشاء معلومات شخصية لأشخاص غير مخولين بالاطلاع عليها. وهذا يعدُّ انتهاكًا للخصوصية الفردية؛ حيث يمكن استغلال هذه المعلومات في عمليات التشهير والابتزاز. ويزداد الأمر سوءًا في ظل غياب قوانين واضحة تحمي الحياة الخاصة، باستثناء ما ورد في قانون الجرائم الإلكترونية الذي يتناول التعدي على المعلومات الشخصية وجرائم أنظمة المعلومات (القحطاني، 2021، ص. 16).

2. 2 المطلب الثاني: مخاطر الجرائم الإلكترونية وأثرها على الأمن القومي

يواجه الأفراد والمؤسسات والجهات الحكومية تحديات تتعلق بالقدرة على مواكبة التطورات السريعة والمستمرة في مجال التكنولوجيا، بالإضافة إلى التهديدات المتزايدة. كما تبرز قضايا الخصوصية وحماية البيانات كأمور حيوية؛ مما يستدعي أن يكون الجميع على دراية دائمة بتدابير الأمن السيبراني. ومن الضروري استخدام كلمات مرور قوية، وتحديث البرامج بشكل منتظم، وتطبيق تقنيات التشفير وغيرها من الوسائل الأمنية (السند، 2022، ص. 93).

تؤدي هذه التحديات إلى اختراق البيانات وسرقة المعلومات الشخصية، فضلًا عن الهجمات الإلكترونية التي تستهدف الشركات والمؤسسات، واستغلال الثغرات الأمنية في الأجهزة والشبكات. ولذا، يجب اتباع إجراءات أمنية صارمة وتحديث أنظمة الحماية بشكل مستمر، مع تكثيف الجهود المشتركة بين الحكومات والشركات والمستخدمين، والعمل على إيجاد حلول فعَّالة لمواجهة التحديات المتزايدة في هذا المجال (علي، 2021، ص. 215).

ونتناول تحديات الأمن السيبراني والجرائم المرتكبة عبر الوسائل الإلكترونية على النحو الآتي:

1. تبادل المعلومات الإرهابية ونشرها من خلال الشبكة الإلكترونية

ظهرت الجرائم المستحدثة مع بروز الإنترنت (Calder, 2014)، حيث أتاح هذا الفضاء للإرهابيين والمجرمين فرصة الالتقاء في بيئة معينة لتعلم أساليب الإجرام والإرهاب، وتبادل الآراء والأفكار والمعلومات. ورغم صعوبة ذلك في الواقع، فإن الشبكات الإلكترونية تسهل هذه العملية بشكل كبير (خليفة، 2020، ص. 60). إذ يمكن لعدة أشخاص الاجتماع في أماكن مختلفة، وفي أوقات محددة، والتواصل بعضهم مع بعض عبر الشبكة، كما يمكنهم أيضًا تجميع أتباع وأنصار من خلال نشر أفكارهم ومبادئهم عبر المواقع والمنتديات وغرف الحوار الإلكترونية (إبراهيم، 2021، ص. 19).

كما يستغل الإرهابيون البريد الإلكتروني لنشر أفكارهم والترويج لها، والسعي لزيادة عدد المتعاطفين معهم من خلال الرسائل الإلكترونية (رشيد، 2023، ص. 22). ومن خلال الشبكة الإلكترونية، تستطيع التنظيمات والجماعات الإرهابية نشر أفكارها المتطرفة والدعوة لمبادئها المنحرفة، والسيطرة على مشاعر الأفراد، واستغلال معاناتهم لتحقيق أهدافهم غير المشروعة التي تتعارض مع مصلحة المجتمع. ويستخدم الإرهابيون الإنترنت بشكل يومي لنشر أفكارهم الهدامة (بكر، 2018، ص. 95).

2. تأسيس المواقع الإلكترونية الإرهابية والإجرامية عبر الشبكات

يقوم الإرهابيون بإنشاء مواقع لهم وتصميمها على الشبكة الإلكترونية العالمية (الإنترنت) لبث أفكارهم الضالة، والدعوة إلى مبادئهم المنحرفة، ولتظهر قوة التنظيم الإرهابي، وللتعبئة الفكرية وتجنيد إرهابيين جدد، ولإعطاء التعليمات والتلقين الإلكتروني، والتدريب من خلال تعليم الطرق والوسائل التي تساعد على القيام بشن هجمات إرهابية (الفيل، 2022، ص. 74)، كما تم إنشاء مواقع إلكترونية إرهابية تهدف إلى توضيح كيفية تصنيع القنابل والمتفجرات والأسلحة الكيميائية الفتاكة، بالإضافة إلى شرح أساليب اختراق البريد الإلكتروني والمواقع الإلكترونية. كما تتضمن هذه المواقع معلومات حول تدمير المواقع والدخول إلى المواقع المحجوبة، وتعليم طرق نشر الفيروسات وغيرها من الأنشطة الضارة.

3. تدمير المواقع والبيانات الإلكترونية

تقوم الجماعات الإرهابية بتنفيذ هجمات إلكترونية عبر الشبكات المعلوماتية بهدف تدمير المواقع والبيانات الإلكترونية والأنظمة المعلوماتية؛ مما يؤدي إلى إلحاق الضرر بالبنية التحتية المعلوماتية وتدميرها. وتستهدف هذه الهجمات عادةً ثلاثة مجالات رئيسة: الأهداف العسكرية والسياسية والاقتصادية. وفي عصر ثورة المعلومات، تظل هذه الأهداف قائمة، حيث تركز الهجمات على مراكز القيادة والتحكم العسكرية، تليها مؤسسات الخدمات الأساسية؛ مثل: الكهرباء والمياه، ثم المصارف والبنوك والأسواق المالية، وذلك بغرض التأثير على إرادة الشعوب والمجتمعات الدولية (بوادي، 2023، ص. 123).

4. عطل شركة ميكروسوفت العالمية يوليو 2024 وتعطل المطارات حول العالم بسبب الاختراقات الإلكترونية والحوادث السيبرانية:

1. على الفور بعد وقوع العطل، تم إلغاء أكثر من 1000 رحلة جوية حول العالم؛ مما أدى إلى تراجع أسهم شركة كراود سترايك بأكثر من 20% في التداولات غير الرسمية في الولايات المتحدة، وهو ما يعكس خسارة تقدر بـ 16 مليار دولار من قيمتها السوقية.
2. يعود سبب هذا العطل التقني إلى تحديث قامت به شركة كراود سترايك للأجهزة المستخدمة لأنظمة مايكروسوفت، وبالتالي يتأثر به فقط مستخدم برمجيات مايكروسوفت وخدمات سترايك (عبد الصادق، ص. 18).
3. أن شركة كراود سترايك تتواصل مع عملائها بمختلف أنحاء العالم لحل أزمة الأعطال الحالية، مضيفًا أن سبب الأزمة تمثل في وجود الكثير من المؤسسات والشركات العالمية والبنوك والبورصات والمطارات التي تعتمد في أنظمتها على مايكروسوفت وخدمات سترايك.

5. تعطل البنية التحتية الرقمية وعطل كراود سترايك 2024

1. كانت أستراليا من أوائل الدول التي تأثرت، حيث توقفت الرحلات الجوية في مطار سيدني، وتعرضت أنظمة الدفع في المتاجر، بما في ذلك متاجر Woolworths، للخلل، بالإضافة إلى تأثير ذلك على مؤسسات مالية مثل: بنك أستراليا الوطني.
2. في ألمانيا، استؤنفت حركة الطيران جزئيًا في مطار برلين بعد حدوث تأخيرات في تسجيل الوصول نتيجة لخطأ فني. وفي إسبانيا، تم الإبلاغ عن عطل في جميع مطارات البلاد؛ حيث استمرت العمليات باستخدام الأنظمة اليدوية (القحطاني، ص. 126).
3. أعلن مطار شيفول في أمستردام عن تأخيرات بسبب انقطاع في تكنولوجيا المعلومات؛ مما أثر على الرحلات الجوية. كما ألغت الخطوط الجوية التركية 84 رحلة نتيجة لهذا العطل، وتمت الإشارة إلى أن الرحلات ستعود تدريجيًا إلى وضعها الطبيعي. (ابن عبد الله، 2024).

6. مخاطر السيطرة على تطبيقات الذكاء الاصطناعي

تعتمد المجتمعات الذكية على تقنيات الذكاء الاصطناعي، مثل: أنظمة الروبوتات في المصانع والمتاجر، بالإضافة إلى أنظمة الرد الآلي على العملاء، والسيارات ذاتية القيادة والطائرات بدون طيار. في حال تعرضت هذه الأنظمة للاختراق، قد نشهد تدفقًا للسيارات ذاتية القيادة في الشوارع، مما يؤدي إلى حوادث مميتة دون القدرة على تحديد الجاني الحقيقي. كما يمكن نظريًا السيطرة على جيوش من الطائرات بدون طيار والروبوتات وإعادة توجيهها لتنفيذ مهام تتعلق بالقتل والتدمير، مما يجعل اختراق هذه الأنظمة من أخطر التهديدات التكنولوجية التي قد تواجه البشرية.

2. 3. المطلب الثالث: أنواع الاختراقات الإلكترونية المؤثرة في الأمن الرقمي

أبرز التهديدات الإلكترونية السيبرانية

1. الاحتيال الإلكتروني وزيادة مواقع التصيد الاحتيالي: حيث قام مُرتكبو الجرائم السيبرانية بإنشاء مواقع مزورة ذات صلة بـ COVID-19 تهدف إلى استدراج الضحايا لفتح ملفات مُرفقة خبيثة أو النقر على وصلات إلكترونية احتيالية من أجل انتحال الهوية، أو النفاذ خلافًا للقانون إلى حسابات خاصة، وهو ما أكدته شركة Trend Micro ،(شركة يابانية مُتخصصة في مجال أمن تكنولوجيا المعلومات)، أن ما يقرب من مليون رسالة تطفلية مُوجهة مُنذ يناير 2020 كانت ذات صلة بكوفيد - 19، ومن ثم جمع المعلومات أو اختلاس ملايين الدولارات وتحويلها إلى حسابات غير مشروعة (INTERPOL.INT)
2. البرمجيات الخبيثة (برمجة انتزاع الفدية وهجمات تعطيل الخدمة DDoS): حيث قام مُرتكبو الجرائم السيبرانية ببث برمجيات خبيثة، مثل: برمجية انتزاع الفدية لتعطيل بنى تحتية ومُؤسسات حيوية، مثل: المستشفيات، بهدف منع البنى التحتية من الوصول إلى البيانات الحساسة أو تعطيل منظوماتها الكمبيوترية؛ مما يؤدي إلى تفاقم الأزمة.

وبحسب ما أُعلن حتى الآن عبر وكالات الأنباء تمثلت الهجمات السيبرانية في 2023 على النحو التالي:

اختراق القنوات التلفزيونية الحكومية الروسية

عطلت مجموعة أنونيموس الخدمات الإخبارية الروسية، واستبدلت مواقعها الإلكترونية برسائل مناهضة للحرب، وتعرضت قنوات Kommersant وIzvestia وFontaka وRBC الروسية للاختراق ، وفي مقطع فيديو تم تداوله على حسابات لنشطاء مجموعة أنونيموس، يُزعم أن المجموعة تمكنت من اختراق العديد من القنوات التلفزيونية الحكومية الروسية؛ حيث تم مقاطعة البث المباشر بالنشيد الوطني الأوكراني.

الابتزاز الإلكتروني للشركات والمؤسسات

يُعدُّ الابتزاز الإلكتروني أسلوبًا يتضمن تهديد الضحية بنشر صور أو مقاطع فيديو أو تسريب معلومات سرية تخصها، وذلك مقابل الحصول على أموال أو إجبار الضحية على القيام بأعمال غير قانونية لصالح المبتزين، مثل: الكشف عن معلومات سرية تتعلق بجهة العمل أو غيرها من الأنشطة غير المشروعة (عطوش، ص. 193). وغالبًا ما يتم استهداف الضحايا عبر البريد الإلكتروني أو منصات التواصل الاجتماعي المختلفة مثل: فيسبوك، وتويتر، وإنستغرام، نظرًا لشيوع استخدامها وانتشارها بين جميع فئات المجتمع.

كما يجب الإشارة إلى هجمات برنامج «WannaCry» الشهير، الذي أثر على أجهزة الكمبيوتر في البنوك ووكالات إنفاذ القانون والبنية التحتية ونظم الرعاية الصحية في عدة دول. بالإضافة إلى ذلك، يستهدف برنامج «Jaff» ضحاياه عبر البريد الإلكتروني الطفيلي، مطالبًا إياهم بدفع مبالغ مالية كبيرة بعملات رقمية. ويعرف الخبراء الابتزاز الإلكتروني بأنه أي فعل يهدف إلى إجبار الأفراد أو المؤسسات على دفع أموال مقابل استعادة الوصول إلى بياناتهم السيبرانية المسروقة أو المخترقة.

واستغلت القرصنة السرعة المتزايدة في تقدم التكنولوجيا والبرمجيات وشبكات الجيل الرابع والخامس من شبكات المحمول، بالإضافة إلى وجود الشبكة المظلمة، لتيسير جرائمها. وفي هذا السياق، يمكن تفصيل أسباب زيادة ظاهرة الابتزاز الإلكتروني على النحو الآتي:

- **تسريب أدوات الاختراق:** يتم تطوير برمجيات الاختراق للاستفادة من قبل الأجهزة الأمنية، ولكن بعض جماعات القرصنة قامت بتسريب هذه الأدوات، كما حدث مع مجموعة «Shadow Brokers»، التي نشرت برمجيات مصممة لاختراق أنظمة التشغيل من وكالة الأمن القومي الأمريكية، وتم استغلال هذه التسريبات في إنشاء برامج فدية مشهورة، مثل: «WannaCry» (IYU, 2023, pp 25-30).
- **العملات الرقمية:** تمثل العملات الرقمية مثل: البيتكوين تطورًا نوعيًا للقرصنة، حيث يصعب تتبع الصفقات التي تتم باستخدامها، وتفتقر إلى قوانين وجهات رقابية. كما أن ارتفاع قيمتها وتنوع استخداماتها يجعلها خيارًا مفضلًا لجرائم، مثل: غسل الأموال، والتحويلات المشبوهة، وتجارة الممنوعات، والتهرب الضريبي.
- وهناك عدة طرق يمكن استخدامها في الابتزاز الإلكتروني، من بينها (عبد الرازق، 2022، ص. 86).
- **التهديد بنشر معلومات حساسة:** يقوم المبتز بالحصول على معلومات خاصة أو حساسة عن الضحية، مثل: صور مخلة أو محادثات سرية، ويهدد بنشرها على الإنترنت أو مشاركتها مع الأشخاص المقربين من الضحية إذا لم يتم دفع مبلغ مالي أو تلبية مطالبه.
- **الاحتيال عبر البريد الإلكتروني:** يقوم المبتز بإرسال رسائل بريد إلكتروني مزيفة تدعي أنه تم العثور على معلومات حساسة عن الضحية، ويهدد بكشف هذه المعلومات إذا لم يتم دفع فدية.
- **هجمات الفدية (Ransomware):** يقوم المبتز بإصابة جهاز الضحية ببرنامج خبيث يشفر ملفاتها، ومن ثم يطلب دفع فدية مالية لفك التشفير واستعادة الملفات.
- **التشهير عبر وسائل التواصل:** يقوم المبتز بنشر معلومات مضللة أو مسيئة عن الضحية عبر وسائل التواصل الاجتماعي، بهدف إلحاق الأذى بسمعتها، أو إلحاق ضرر بحياتها الشخصية أو المهنية (Desforges, 2021, pp 67-81).

التهديدات الإلكترونية المؤثرة اقتصاديًّا

تشهد الجرائم الإلكترونية ارتفاعًا غير مسبوق في الخسائر المالية والتشغيلية، حيث يُتوقع أن تصل التكلفة العالمية للجرائم السيبرانية إلى 10.5 تريليون دولار سنويًّا بحلول عام 2025؛ مما يجعلها واحدة من أكثر التهديدات الاقتصادية خطورة. ووفقًا لتقرير IBM لعام 2024، بلغ متوسط تكلفة اختراق البيانات عالميًّا 4.88 مليون دولار، بزيادة 10% عن العام السابق؛ مما يعكس ارتفاع التكاليف التشغيلية والأضرار الناتجة عن هذه الهجمات. وقد أظهر تقرير FBI أن الجرائم الإلكترونية المبلغ عنها زادت بنسبة 22% بين عامي 2022 و2023،

بينما شهد الربع الثاني من عام 2024 زيادة بنسبة 30% في الهجمات مقارنة بالفترة نفسها من عام 2023، وفقًا لمؤسسة Check Point Research. (cobalt.io/blog/top-cybersecurity-statistics)

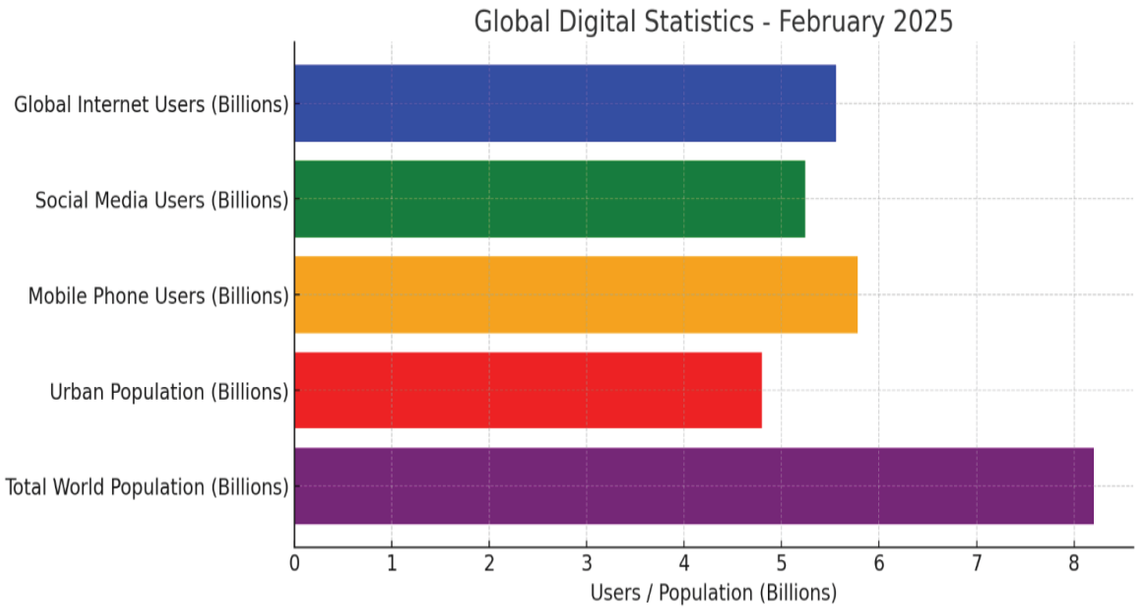
أما هجمات الفدية (Ransomware)، فقد طالت 59% من المؤسسات خلال العام الماضي، حيث بلغ متوسط تكلفة التعافي من هذه الهجمات 3.58 مليون دولار وفقًا لتقرير Sophos، في حين أن 63% من المهاجمين طلبوا فدية تتجاوز مليون دولار، و30% طلبوا أكثر من 5 ملايين دولار. كما أن القطاعات الأكثر تضررًا شملت الرعاية الصحية، والخدمات المالية، والصناعة، والتكنولوجيا، والطاقة، ووفقًا لتقرير Cybersecurity Ventures، فإن تكلفة هجمات الفدية قد تصل إلى 265 مليار دولار سنويًا بحلول عام 2031، مما يبرز خطورة هذا النوع من التهديدات. وفيما يتعلق بالتصيد الاحتيالي (Phishing)، فقد أصبح أكثر أساليب الهجوم شيوعًا عبر البريد الإلكتروني، حيث يمثل 33% من الحوادث الأمنية السحابية، مع استهداف علامات تجارية كبرى مثل: DHL وFedEx وFacebook وNetflix، وفقًا لتقرير Hornetsecurity. وتشير البيانات إلى أن 25% من هجمات اختراق البريد الإلكتروني للأعمال نجحت بسبب عدم استخدام المصادقة الثنائية (SpyCloud Ransomware De-fense Report2024).

وأدت التطورات في الذكاء الاصطناعي إلى زيادة التهديدات السيبرانية، حيث يعتقد 85% من خبراء الأمن السيبراني أن الذكاء الاصطناعي التوليدي يعزِّز قدرة المهاجمين، في حين تشير توقعات Gartner إلى أن 17% من الهجمات السيبرانية ستستخدم الذكاء الاصطناعي التوليدي بحلول عام 2027، كل هذه الأرقام تؤكد أن الخسائر الناجمة عن الجرائم السيبرانية ليست مجرد تكاليف مالية، بل تمتد إلى تعطيل العمليات التجارية، وإلحاق الضرر بالسمعة، وفرض غرامات تنظيمية باهظة؛ مما يجعل الأمن السيبراني أولوية قصوى للشركات والحكومات على حد سواء. كما هو موضح بالشكل رقم (1):

تطورات فيروسات الفدية وتأثيرها على الأمن القومي للدول والبنية التحتية الإلكترونية

تشهد الساحة العالمية اليوم انتشار نوع جديد من الإرهاب، يشبه انتشار النار في الهشيم، إنه إرهاب برامج الفدية (Ransomware)، الذي يلحق أضرارًا جسيمة بالأفراد والمؤسسات، ولكن دون أن يحظى بالاهتمام الكافي، وهذه البرامج تستخدم كأدوات ابتزاز إلكتروني لإجبار المستخدمين على دفع الأموال، وقد تحول استخدامها من استهداف الأفراد إلى استهداف الشركات.

وتشمل تكاليف برامج الفدية: تلف البيانات، ووقت التوقف عن العمل، وتعطيل الأعمال، والتحقيقات الجنائية، وإلحاق الضرر بالسمعة. ويكشف تقرير «Kaspersky Lab» لعام 2023 أن كل 40 ثانية كان يقع نشاط تجاري ضحية لهجمة برامج الفدية، مقارنةً بكل



شكل 1 ارتفاع مستويات الاختراقات الإلكترونية نسبة لعدد مستخدمي الإنترنت عالميًّا

Figure 1 *The rise in cyber breaches relative to the number of global Internet users*

دقيقتين في أوائل 2016. ويؤكد تقرير Cybersecurity Ventures أن هجمات الفدية تحدث على الشركات كل 14 ثانية بحلول نهاية 2019، وكل 11 ثانية في 2021. كما بلغت خسائر برامج الفدية في الولايات المتحدة 29.1 مليون دولار في 2024. (إبراهيم، ص. 33) بخلاف التعرض لهجمات البنية التحتية، وتعطل حركة الملاحة الجوية والمرافق المهمة والبنوك والمستشفيات ومحطات الطاقة.

3. المبحث الثاني: المواجهة الأمنية للاختراقات الإلكترونية

إن التطور النوعي في تكنولوجيا الاتصالات والإنترنت ومختلف الوسائط الإلكترونية أعطت أفراد المجتمع مجالًا واسعًا للاطلاع على المعلومات، وأدَّت إلى تغيير كبير في أسلوب حياتهم وتعاملهم بين الناس، كما أثر ذلك بشكل مباشر على حجم ونوع الجريمة، وعلى مشروعية الفعاليات عامة، ونتج عن ذلك نوع جديد من الجريمة أطلق عليها فيما بعد «الجريمة الإلكترونية» وهناك ضوابط حديثة يجب تناولها وتطبيقها في كافة الجهات الحكومية والاقتصادية لتعزيز الأمن السيبراني وزيادة الوعي الأمني الرقمي

وقد ارتأينا تقسيم ذلك المبحث إلى مطلبين، وفقًا لما يلي:

3. 1. المطلب الأول: الآليات الأمنية لمواجهة الجرائم الإلكترونية

تُعتمد اليوم آليات أمنية متكاملة ومتطورة لمواجهة الجرائم السيبرانية، تجمع بين التقنيات الذكية؛ مثل: الذكاء الاصطناعي لرصد الهجمات في الوقت الفعلي، وتحليل الأنماط المشبوهة، وتقنيات التشفير الكمي لمواجهة تهديدات الحواسيب الكمية، وأنظمة Zero Trust التي تفرض التحقق المستمر من هوية المستخدمين. إلى جانب ذلك، تعزز الدول الأطر التشريعية الصارمة، مثل: تحديث قوانين الجرائم الإلكترونية لملاحقة الابتزاز الرقمي والاختراقات، وتعزيز التعاون الدولي عبر مبادرات كشراكة دلهي للأمن السيبراني أو منصة الأمم المتحدة لمكافحة الجريمة السيبرانية. كما تُنشأ وحدات سيبرانية متخصصة (كالقيادة السيبرانية السعودية) لتعزيز الدفاع النشط، وتُدمج الشراكات بين الحكومات والقطاع الخاص لتأمين البنى التحتية الحيوية مثل: شبكات 5G والذكاء الاصطناعي في موازاة ذلك، وتُركّز الإستراتيجيات الحديثة على بناء الكفاءات البشرية عبر برامج تدريبية متخصصة، وحملات توعوية لمواجهة التصيد الاحتيالي، وتدريبات محاكاة؛ مثل: «Cyber Polygon» لاختبار الاستجابة للأزمات. ومع تصاعد الهجمات المُعقدة (كالبرمجيات الفدائية المُوجهة)، تظل المرونة والتكيف مع التهديدات الناشئة، مثل: التزييف العميق (Deepfake)، ركيزة أساسية في الحرب السيبرانية الحديثة.

تعريف مصطلح الأمن السيبراني

يشير الأمن السيبرانيCybersecurity إلى حماية نظم المعلومات (من أجهزة وبرامج وبنية تحتية مصاحبة) والبيانات المختزنة فيها، والخدمات التي توفرها، بحيث لا يصل إليها من ليس مرخصًا له بذلك. ويشمل ذلك الضرر المتعمد من جانب من يشغل النظام، والأذى العرضي الناجم عن عدم اتباع إجراءات الأمن (Meeuwisse, 2019, p524).

أهمية الأمن السيبراني

تنامت العلاقة بين الأمن والتكنولوجيا؛ مما أدَّى إلى ارتفاع احتمالية تعرض المصالح الإستراتيجية للدولة لتهديدات سيبرانية؛ مما يهدد بتحويل الفضاء السيبراني إلى وسيلة جديدة للصراع الدولي المتعدد الأطراف (عبد الصادق، 2022، ص. 32). كما أدَّت شبكات التواصل الاجتماعي دورًا بارزًا خلال الثورات العربية في بداية عام 2011، حيث أصبحت محورًا رئيسًا في تعزيز الاهتمام الدولي بأمن الفضاء السيبراني. وقد ظهرت محاولات للسيطرة على هذا الفضاء بعد تصاعد الاحتجاجات، حتى في الدول الأكثر ديمقراطية؛ مثل: بريطانيا والولايات المتحدة الأمريكية. وإذا كان الأمن القومي يعني حماية القيم الأساسية للمجتمع وغياب التهديدات التي قد تواجهه، فإن الفضاء السيبراني قد فرض إعادة تقييم مفهوم الأمن الذي يتعلق بمدى قدرة الدولة على حماية نفسها من خطر الهجمات، بالإضافة إلى اتخاذ تدابير لحماية المنشآت الحيوية للبنية التحتية من التهديدات الناتجة عن الاستخدام السيئ لتكنولوجيا الاتصال والمعلومات.

الأمن الوقائي المعلوماتي

تتنوع أساليب الحماية الأمنية المتعلقة بنظم المعلومات وتطبيقاتها الحديثة، بالإضافة إلى الشبكات المسؤولة عن نقل هذه المعلومات والبيانات. وتؤدي الشبكات دورًا حيويًّا في ربط الخوادم الرئيسة بالفرعية، وكذلك في ربط مراكز المعلومات وإداراتها بين مختلف القطاعات والمؤسسات الأمنية. وهذا يتطلب تأمين المعلومات بطرق متعددة لحماية سرية البيانات أثناء نقلها، بالإضافة إلى تعزيز الأمن الدفاعي عامة. حيث تعمل وحدات خاصة في الدولة على حماية موارد المعلومات الحكومية والعسكرية والأمنية، وضمان عدم وقوعها في الأيدي الخاطئة. وفي الوقت نفسه، تقوم هذه الوحدات بتطوير السياسات والإجراءات الأمنية المناسبة ونشرها على مختلف دوائر الدولة لتطبيقها. ومن بين تطبيقات الأمن السيبراني الوقائي (القرعان، 2021، ص.19):

تفعيل نظام إدارة المعلومات الأمنية (Security Information and Event Management System)

تُعدُّ الرقابة جزءًا أساسيًّا ومهمًّا جدًّا من منظومة الحماية الأمنية ودورة حياتها (Life-Cycle)، حيث تمكن الفريق الأمني من كشف الحوادث الأمنية ومحاولات الاختراق والتصدي لها، أو على الأقل اتخاذ إجراء أمني مناسب في مرحلة مبكرة؛ مما يقلل من أية خسائر مادية أو غير مادية محتملة، مقارنة مع تلك الخسائر التي قد تنجم في حال عدم القدرة على كشف الاختراق الأمني في مراحله المبكرة ومعالجته (Brenton, 2020, pp.510-513).

يعتمد مبدأ هذا النظام - باختصار - على تعزيز كفاءة مراقبة الأحداث والمعلومات الأمنية التي تصدر عن مختلف أنظمة تكنولوجيا المعلومات، بغض النظر عن نوعها، من خلال توفير الوقت والجهد وزيادة الدقة في كشف الحوادث الأمنية، أو حتى المؤشرات المحتملة لحدوثها. ويتم ذلك من خلال تجميع المعلومات في نظام مركزي وتحليلها للكشف عن أي أحداث مشبوهة، ثم عرضها على المحلل الأمني أو فريق المراقبة لاتخاذ الإجراءات المناسبة. في بعض الأحيان، يمكن لهذه الأنظمة أن تتخذ إجراءات وقائية بشكل تلقائي، مثل: تحديث نظام الجدار الناري (Firewall) أو نظام منع التسلل (IPS) لصد الهجمات أو الاختراقات عند حدوثها.

دور التشفير الكمومي للبيانات الرقمية وحماية الأمن القومي

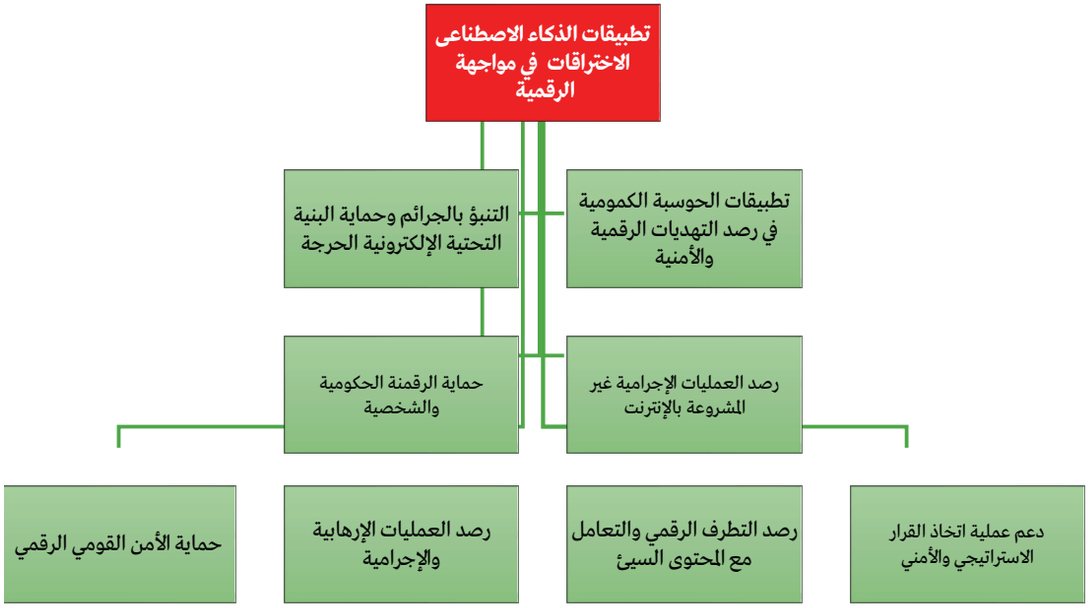
التشفير (The role of quantum cryptography) عملية استخدام صيغ رياضية معقدة لتشفير البيانات وجعلها غير قابلة للقراءة، ويُستخدم التشفير على نطاق واسع في التجارة عبر الإنترنت، والتمويل، وأنظمة الأمن القومي، ومن ثمَّ ستكون أجهزة الكمبيوتر الكمومية -بسرعاتها الكبيرة للغاية- قادرة على إجراء العمليات الحسابية لفك تشفير الرسائل بسرعة بمجرد اعتبارها آمنة، بالإضافة إلى أنها سيكون لديها القدرة على حل المعادلات الرياضية المعقدة بمعدلات أسرع بكثير من أجهزة الكمبيوتر التقليدية؛ مما يسمح بـ«كسر» التشفير، وهو ما يخلق تهديدًا جديدًا للبرامج والخدمات الحالية.

والتشفير الكمي يمثل أحد التطبيقات المتقدمة لتكنولوجيا الكم، حيث يعتمد على مبادئ ميكانيكا الكم لتوفير مستويات غير مسبوقة من الأمان في نقل البيانات. ويعمل هذا النوع من التشفير على إنشاء قنوات اتصال آمنة تعتمد على توزيع المفاتيح الكمومية (Quantum Key Distribution - QKD)، التي تجعل أي محاولة لاعتراض البيانات قابلة للكشف الفوري. وفيما يلي استعراض لأبرز تطبيقات التشفير الكمي: (موسى، 2022، ص. 79-80).

1. المعاملات المالية يؤدي التشفير الكمي دورًا حيويًّا في تأمين المعاملات المالية الحساسة التي تُجرى يوميًا على نطاق عالمي. من خلال إنشاء قنوات اتصال مشفرة وآمنة، تصبح المعلومات المالية مثل: بيانات البطاقات المصرفية وتحويلات الأموال محصنة ضد محاولات مجرمي الإنترنت لاختراقها. وهذه المزايا تجعل التشفير الكمي حلًّا مثاليًّا لحماية النظام المالي العالمي من التهديدات السيبرانية المتزايدة، وتعزيز ثقة المستخدمين في الخدمات الرقمية.
2. الاتصالات العسكرية والحكومية تُعدُّ الوكالات العسكرية والحكومية من أبرز الجهات المستفيدة من التشفير الكمي. وتستخدم هذه الجهات التكنولوجيا الكمومية لنقل المعلومات الحساسة والإستراتيجية بطرق آمنة تمنع أي تسريب أو اعتراض. ويتيح التشفير الكمي للمؤسسات الحكومية والعسكرية مواجهة تهديدات التجسس الرقمي بشكل فعَّال، حيث تُؤمن الاتصالات المتعلقة بالأمن القومي والعمليات الحساسة من أي اختراق؛ ما يعزِّز قدرة الدول على حماية مصالحها الحيوية.
3. إنترنت الأشياء (IoT): يمثل إنترنت الأشياء منظومة من الأجهزة المتصلة بالإنترنت، والتي تشمل كل شيء بدءًا من الأجهزة المنزلية الذكية، وصولًا إلى الأنظمة الصناعية. وتُعَدُّ هذه الأجهزة هدفًا شائعًا للهجمات السيبرانية بسبب محدودية قدراتها الحاسوبية وضعف مستويات الحماية التقليدية. باستخدام التشفير الكمي، يمكن تأمين قنوات الاتصال بين هذه الأجهزة وحمايتها من محاولات القرصنة. بالإضافة إلى ذلك، يسهم التشفير الكمي في تعزيز أمان أنظمة التحكم في المنشآت الصناعية الحيوية والبنية التحتية الذكية (خليفة، 2020، ص12).

وترجع أهمية التشفير الكمي عامةً إلى أنه يمثل مستقبل الأمان السيبراني في عصر تُصبح فيه البيانات أحد أهم الأصول. بفضل قدرته على تقديم حماية غير قابلة للكسر تقريبًا، ويمكن للتشفير الكمي أن يؤدي دورًا محوريًّا في تعزيز الأمن في القطاعات الحساسة مثل: البنوك، الصحة، الدفاع، البنية التحتية الحيوية. كما يُتوقع أن يشكل التشفير الكمي الأساس لأنظمة الاتصالات المستقبلية، حيث يضمن سرية المعلومات حتى في مواجهة الحوسبة الكمومية المتقدمة.

4. تأثير الحوسبة الكمومية على تأمين البنية التحتية الرقمية (البابلي، 2024، ص. 306) وذلك من خلال:



شكل 2 تطبيقات الذكاء الاصطناعي في مواجهة الاختراقات الرقمية

Figure 2 *Artificial intelligence applications in combating digital breaches*

- تعزيز التشفير وحماية البيانات من خلال تطوير أنظمة تشفير جديدة مقاومة للهجمات الكمومية، مثل: التشفير الكمي (Quantum Key Distribution - QKD)، الذي يضمن نقل المفاتيح السرية بين الأطراف بشكل آمن تمامًا، وهذه التقنيات يمكن أن تحمي الاتصالات السرية بين المؤسسات العسكرية والأمنية؛ مما يقلل من خطر التجسس أو الاختراقات.
- تأثير الحوسبة الكمومية على البنية التحتية الاقتصادية من خلال حماية الأنظمة المالية؛ حيث يمكن للحوسبة الكمومية أن توفر تشفيرًا متقدمًا لحماية الأنظمة المالية والبنوك من الهجمات السيبرانية، وهذا يشمل حماية المعاملات المالية والبيانات المصرفية الحساسة من الاختراقات.
- حماية البنية التحتية الحيوية، باستخدام الحوسبة الكمومية مثل: شبكات الطاقة والمياه والاتصالات التي تُعدُّ أساسية للأمن الاقتصادي، ومن ناحية أخرى، إذا تم اختراق هذه الأنظمة باستخدام تقنيات كمومية، فقد يؤدي ذلك إلى انهيار اقتصادي وأمني.
- تطوير أنظمة تشفير كمومية: يجب على الدول تطوير أنظمة تشفير مقاومة للهجمات الكمومية لحماية بياناتها الحساسة، وتعزيز التعاون الدولي في مجال البحوث الكمومية، ووضع معايير أمنية مشتركة يمكن أن تساعد في تقليل التهديدات، ويجب على الحكومات والقطاع الخاص الاستثمار في أبحاث الحوسبة الكمومية وتطبيقاتها الأمنية وبناء الوعي والتدريب من خلال الوعي بأهمية الحوسبة الكمومية وتدريب الكوادر الأمنية على التعامل مع التهديدات الكمومية.. ويوضح الشكل رقم (2) منظورًا لاستخدام الذكاء الاصطناعي في مواجهة الاختراقات الرقمية.

3. 2. المطلب الثاني: استخدام تقنيات الذكاء الاصطناعي لمواجهة الاختراقات الأمنية

الدفاع السيبراني في عصر الذكاء الاصطناعي والمجتمعات الذكية

يعتمد الأسلوب الدفاعي في مجال الأمن السيبراني على التعرف على أبرز أساليب الهجمات وتحديد توقعات واضحة لها. فقد تتعرض الشركات لفيروسات خبيثة تمسح جميع ملفاتها المهمة، أو لفيروسات من نوع «طروادة» التي تدخل النظام بشكل ودي عبر ملفات أو صور بعد كسب ثقة الضحية، كما هو الحال في قصة حصان طروادة الشهيرة. كما يمكن أن تتعرض لهجمات فيروس الفدية، الذي يقوم بتشفير جميع ملفات الضحية، ويطلب فدية لفك هذا التشفير، وغالبًا ما يكون المهاجم غير موثوق. بالإضافة إلى ذلك، قد تتعرض الشركات لهجمات ممنهجة تعطل حركة

خوادمها، والقائمة طويلة.

ولا شك أن الاستعداد لهذه الهجمات وتحديدها بدقة وبشكل مستمر يسهم بشكل كبير في التصدي لها وتقليل أضرارها. ومع ذلك، تُعتبر هجمات الـ Zero Day من أخطر الهجمات الإلكترونية في مجال الأمن السيبراني، حيث تكون نسبة نجاحها مرتفعة في معظم الأحيان. وهذه الهجمات جديدة ولم يتم التعرف عليها من قبل في النظام، ولا توجد طرق معروفة للتصدي لها، إذ تمثل ثغرة في النظام أو أسلوب هجوم مبتكر بالكامل (الجامع، 2019، ص.22).

على سبيل المثال، في المراحل الأولى لظهور إنترنت الأشياء، كانت المصانع تركز بشكل كبير على تطوير الأجهزة لتكون سهلة الاستخدام وفعَّالة في الأداء، مع إغفال الجانب الأمني. وقد استغل المخترقون هذا الضعف في الأجهزة، خاصة مع انتشارها الكبير وارتباطها بشبكات الواي فاي والخوادم؛ مما أدى إلى اختراقها واستخدامها في شن هجمات واسعة على شركات كبرى (فوزي، 2024، ص.52).

تطبيقات الذكاء الاصطناعي في صد عمليات الاحتيال ومكافحة الجريمة

- على الرغم من أن اكتشاف جرائم الإنترنت يتطلب عادةً فهم طبيعة الجريمة المستهدفة، فإن الذكاء الاصطناعي أصبح قادرًا على اكتشافها بشكل أفضل من البشر. فهو يستطيع رصد أنماط سلوكية يصعب على الإنسان ملاحظتها، كما يمكنه التدخل لإيقاف الأنشطة المشبوهة قبل أن تتفاقم. ويُستخدم التعلم الآلي في تحليل بيانات المحفظة لتحديد الأنماط؛ مما يسهم في تمييز التطبيقات الجيدة عن السيئة بدقة أكبر. ويعتمد الذكاء الاصطناعي على نسخة متطورة من الخوارزميات التي تعمل وفقًا لمبدأ التعلم العميق الذي يستند إلى هندسة الميزات التلقائية. وهذه الهندسة تحول البيانات الأساسية إلى ميزات يمكن للخوارزميات التعرف عليها، مثل: نبرة الصوت، وبصمة العين، وبصمة الإصبع، والنصوص المكتوبة. وبعبارة أخرى، فإنها قادرة على التعرف على الميزات التلقائية (السويدي، 2019، ص. 9).
- يستطيع النظام الذكي داخل البنوك والشركات العملاقة التجارية أن يميز الشخص الذي يستخدم بيانات مصرفية مسروقة للدخول إلى الحساب، فإن وجد أن الطريقة التي يستخدم الشخص بها الموقع لا تتفق مع الأنماط ذات الصلة بمالك المعلومات المسروقة، يُرسل رسالة تحذيرية على الفور، وبالمثل، إذا كان المستخدم مترددًا على غير عادته عند استخدام الموقع (عبد الكريم، ص42).
- يسهم الذكاء الاصطناعي بشكل كبير في الحد من عمليات التزوير والاحتيال، خصوصًا تلك التي تحدث عبر الإنترنت. لفهم كيفية أداء الذكاء الاصطناعي لهذه المهمة، ويمكن الإشارة إلى بعض ميزات الخوارزميات المستخدمة في كشف الاحتيال التي تعتمد على تحليل البيانات المدخلة وتحديد المعاملات غير الطبيعية باستخدام تقنيات التعلم الآلي التقليدية. (أبو بكر، 2020، ص. 57-60).

أهمية تطبيقات الذكاء الاصطناعي لتعزيز وحماية الأمن السيبراني

1. يعتمد الأسلوب الدفاعي في الأمن السيبراني على التعرف على أبرز أساليب الهجمات وتحديد توقعات دقيقة لها. قد تتعرض المؤسسات لفيروسات خبيثة تمسح جميع ملفاتها المهمة، أو لفيروسات من نوع «طروادة» التي تدخل النظام بشكل ودي عبر ملف أو صورة بعد كسب ثقة الضحية. كما يمكن أن تتعرض لهجمات من نوع «فدية» تشفر جميع ملفات الضحية وتطلب فدية لفك هذا التشفير، أو لهجمات ممنهجة تعطل حركة خوادم المؤسسات. وفقًا لـ (Villasenor, 2020, pp. 131-142)، تقوم أنظمة الذكاء الاصطناعي بالتعرف على الهجمات والتنبؤ بها وتحديدها بدقة. ويمكن استخدام التعلم الآلي لأتمتة عمليات كشف التهديدات والاستجابة السريعة لها؛ مما يعزز فاعليَّة الكشف عن التهديدات مقارنة بالأساليب البرمجية الأخرى (Akpan et al., 2020).
2. يوفر الذكاء الاصطناعي قدرة استثنائية على تحليل البيانات الضخمة بسرعة ودقة عالية. ويتيح ذلك للشركات والمؤسسات الأمنية والاستخباراتية مراقبة شبكاتها بشكل مستمر وتحليل التفاعلات والمعاملات للكشف عن أي سلوكيات مشبوهة أو غير عادية. على سبيل المثال، يمكن للخوارزميات المتطورة تحليل أنماط الاتصالات وتحديد الانحرافات، وعلى سبيل المثال، يمكن للخوارزميات المتطورة تحليل أنماط الاتصالات، وتحديد الانحرافات التي قد تشير إلى محاولة اختراق أو هجوم سيبراني (فوزي، ص. 75).
3. الذكاء الاصطناعي يمثل عنصرًا رئيسًا في تطور مجال الأمن السيبراني، حيث يوفر حلولًا ذكية لتحديد ومواجهة الهجمات والتهديدات السيبرانية. ويمكن لهذه التقنيات تحليل كميات كبيرة من البيانات لتحديد مصادر الخطر، وتقديم توصيات

لتعزيز الأمان. وعلاوة على ذلك، يمكن للذكاء الاصطناعي تحديث النظم الأمنية باستمرار لمواكبة أحدث أساليب الهجمات وتحديد العلاقات والعمليات الإجرامية وغير المشروعة (Alon-so, & et al. 2023).

البلوك تشين والأمن السيبراني

- تُعدُّ تقنية البلوك تشين نظامًا يتألف من دفاتر رقمية مشتركة تُستخدم لتسجيل المعاملات وتتبع الأصول ضمن شبكة غير مركزية. ومن أبرز التطبيقات التي تعتمد على هذه التقنية هي عملة البتكوين، التي تُعدُّ العملة الرقمية الأولى (Sulaiman, 2022).
- هناك عدة أنواع من شبكات البلوك تشين، منها الشبكة العامة والشبكة الخاصة. الشبكة العامة متاحة لجميع المشاركين؛ حيث يتمتع الجميع بصلاحيات متساوية في قراءة وكتابة المعاملات. وتتميز هذه الشبكة بعدم مركزيتها؛ إذ يسعى جميع الأعضاء إلى إثبات صحة المعاملات؛ مما قد يستغرق وقتًا طويلًا يتراوح بين 10 إلى 60 دقيقة؛ نظرًا لوجود عدد كبير من المشاركين. بالمقابل، تتيح الشبكة الخاصة صلاحيات قراءة وكتابة المعاملات لعدد محدد من المشاركين، بينما تظل غير مركزية. ومن بين التطبيقات المهمة للبلوك تشين نجد تطبيقات إدارة الهوية، والتصويت الإلكتروني، والعقود الذكية، وتسجيل الأصول، بالإضافة إلى العديد من التطبيقات في مجال الأمن السيبراني، وأخيرًا التطبيق اللامركزي لحماية البنى التحتية الرقمية (شفيق، ص. 20).

منصات الذكاء الاصطناعي للأمن السيبراني

كثيرة هي منصات الذكاء الاصطناعي للأمن السيبراني على النحو التالي:

- في حالة منصة Endpoint Protection: تعمل الإمكانات المتقدمة لتعلم الآلة والذكاء الاصطناعي، جنبًا إلى جنب مع شبكة جمع المعلومات العالمية (GIN)، وهي شبكة لبيانات التهديدات من «سيمانتك» تقوم بجمع بيانات عن بُعد من ملايين وحدات استشعار الهجمات، لاكتشاف التهديدات المحتملة قبل وقوعها، وكذلك تحديد الملفات ومواقع الويب التي يحتمل أن تكون مشكوكًا فيها، حتى تتمكن مؤسسات أمن المعلومات من اتخاذ إجراء قبل أن تتمكن من إلحاق الضرر (Matthijs, et al. 2021).
- الاستعانة بالحوسبة الكمومية في التأمين: تُعدُّ الحوسبة الكمومية واحدة من أكثر التقنيات الواعدة في تعزيز الأمن السيبراني وتأمين المعلومات؛ حيث توفر قدرات هائلة في معالجة البيانات وحل المشكلات المعقدة التي تتجاوز قدرات الحواسيب التقليدية.

3. 3. المطلب الثالث: التوعية الأمنية ضد المخاطر الرقمية المستحدثة

دور المؤسسات المعنية بالتوعية ضد أخطار شبكات التواصل الاجتماعي والاختراق الإلكتروني:

1. **المؤسسات الإعلامية:** لا شك أن الإعلام يؤدي دوره البارز في نفوس المشاهدين، وهذا منوط به مهمة أخلاقية، إذ يجب أن تؤدي هذه الوسائل على تنوعها المسموعة والمرئية والمطبوعة دورها في عملية التوعية والتثقيف للجمهور، وهنا يجب أن تكون هناك سياسة إعلامية تؤدي دورها الفاعل في توعية المواطنين بسبل التحايل (المطيري، ص. 115).

وبين الأمن ووسائل الإعلام علاقة وثيقة؛ حيث يعمل الإعلام بأشكاله المختلفة على دعم الأجهزة الأمنية على مستويات شتى، حيث إنه أداة أساسية للتوعية والوقاية من الجريمة ومخاطرها؛ حيث يقوم بتنظيم حملات توعية موجهة للأفراد والجماعات والمؤسسات، تساعد في بناء الوعي الرقمي والمعرفة السيبرانية بشأن قضايا الابتزاز الإلكتروني والاختراق الأخلاقي وسرقة الصفحات واختراقها وسرعة الحسابات المصرفية، ويمكّن الناس من فهم هذه القضايا وتحليلها؛ مما يسهم في اتخاذ الإجراءات المناسبة للتعامل معها (محمد، 2018، ص.20).

وتزداد أهمية وسائل الإعلام بشكل كبير في عصرنا الحالي نتيجة للتقدم التكنولوجي والتطور في مجال تبادل المعلومات، ويمكن للإعلام الحديث الوصول إلى جميع فئات المجتمع بفاعليَّة وحماية الأمان السيبراني على مستوى الأفراد والأسر والمجتمعات؛ لذلك يجب أن يؤدي الإعلام دورًا حيويًّا في توجيه الوعي، وتقليل معدلات الجريمة، بما في ذلك الجريمة الإرهابية والجريمة الرقمية عبر تطبيقات التواصل الاجتماعي (شفيق، 2016، ص.45).

ويمكن للباحث أن يسلط الضوء على دور الإعلام في مكافحة التطرف والعنف الرقمي ومخاطر الهندسة الاجتماعية التي تتخذ التواصل الاجتماعي كستار لها من خلال التنفيذ الجاد للنقاط التالية:

- **إعداد برامج إعلامية مستهدفة:** يجب تصميم برامج إعلامية مدروسة، تستهدف التعامل مع قضية الإرهاب في الوطن العربي بشكل خاص، ويجب أن تكون هذه البرامج قادرة على نقل رسائل إعلامية فعَّالة للأفراد والمجتمعات خاصة في المناطق الريفية.

- **برامج توعية وإرشاد موجهة:** يجب تضمين برامج إرشادية وتوعوية تستهدف مكافحة الهجمات السيبرانية الأسرية والاجتماعية الموجهة ضد أخطار تقنيات المعلومات والإنترنت والأفكار المتطرفة ضد سياسة الدولة والمجتمع. (الشهراني، 2020، ص.60-70).
- **دور المرأة:** من الضروري التأكيد على أهمية دور المرأة في نشر الوعي الإعلامي حول قضايا العنف الرقمي والإرهاب، خاصةً فيما يتعلق بالأسرة والأطفال، بالإضافة إلى قضايا الابتزاز الإلكتروني (المادي والجنسي) وسرعة الإبلاغ عن الحسابات الشخصية في تطبيقات التواصل الاجتماعي.
- **مواكبة التطورات التكنولوجية:** ينبغي إيلاء اهتمام خاص لمتابعة التطورات في مجال الجرائم المرتبطة بالميتافيرس والعوالم الافتراضية، وكذلك الهندسة الاجتماعية وغسل العقول والتنمر الإلكتروني. ومن المهم وضع خطط إعلامية وأمنية فعَّالة للتوعية بمخاطر هذه الظواهر (محمد، ص. 203).

2. **المنظمات غير الحكومية:** لا يمكن تجاهل الدور الذي يمكن أن تؤديه المنظمات غير الحكومية في مواجهة التأثيرات السلبية لمواقع التواصل الاجتماعي. ويمكن لهذه المنظمات تنظيم ندوات تثقيفية حول الاستخدام الآمن لهذه المواقع. كما يمكنها الاستفادة من منصات التواصل الاجتماعي نفسها للتواصل مع المواطنين بمختلف فئاتهم العمرية، حيث إن العديد من المنظمات غير الحكومية قد أنشأت صفحات على هذه المنصات لتوعية المجتمع.

دور المؤسسات المجتمعية والإعلامية في مواجهة التحديات الناجمة عن الاختراقات الإلكترونية

نحتاج إلى تعزيز الوعي في مجتمعنا لتمكين الجميع من فهم المخاطر، واتخاذ الإجراءات اللازمة. يُعدُّ تحقيق الوعي المجتمعي والأمني تجاه المخاطر المرتبطة بالمنصات الاجتماعية، مثل: تطبيقات التواصل الاجتماعي (كالتحايل الاجتماعي، والابتزاز الإلكتروني والأخلاقي، والتزييف الرقمي، وانتشار الشائعات)، أمرًا حيويًّا للحفاظ على سلامة الأفراد والمجتمعات. وعندما يكون الأفراد على دراية بخطورة هذه التقنيات، وكيفية استخدامها في تزوير المعلومات والصور والفيديوهات، يصبح بإمكانهم اتخاذ خطوات لتقليل المخاطر (ابن عبد العزيز، ص. 302).

تشمل إجراءات تعزيز الوعي المجتمعي والأمني مواجهة أخطار التزييف العميق وغيرها من التهديدات الناجمة عن البيئة الرقمية، بالإضافة إلى توفير التدريب والتعليم للأفراد والمؤسسات حول كيفية التعرف على هذه المخاطر والكشف عنها والتنبؤ بها. كما يجب أن تكون هناك جهود مستمرة لتوعية الأفراد والمجتمع. ويمكن أيضًا تقديم الدعم الفني للأفراد والمؤسسات لمساعدتهم في مواجهة هذه المخاطر وتعزيز الحماية الأمنية للأنظمة والبيانات والمعلومات (العيسوي، ص.11).

أدوات الأمان السيبراني للفرد والأسرة داخل المجتمع ضد أخطار التواصل الاجتماعي

وتشمل أساليب التوعية المجتمعية لمواجهة التزييف العميق ومخاطر الهندسة الاجتماعية والاحتيال الإلكتروني؛ حيث يُعدُّ الوعي والتعليم في مجال الأمن السيبراني من أقوى الأدوات لمواجهة التهديدات السيبرانية والهندسة الاجتماعية. ومن ثمَّ يجب على المستخدمين الالتزام بما يلي (شمس الدين، 2020، ص. 39):

1. تعزيز الأمان الشخصي والأمان السيبراني لحماية الأفراد من أخطار الابتزاز الأخلاقي والهندسة الاجتماعية، وللتصدي للهجمات السيبرانية والتزييف العميق.
2. التحقق من هوية الأشخاص والجهات التي تتواصل معها عبر منصات التواصل الاجتماعي، وتجنب الاتصال مع أشخاص غير معروفين.
3. تحديث الأجهزة والبرمجيات: تأكد من تحديث الأجهزة والبرمجيات والتطبيقات بانتظام للحفاظ على حمايتها من الثغرات والهجمات السيبرانية (James, 2017, pp109-110).
4. الإبلاغ عن الهجمات: إذا تعرضت لهجمات سيبرانية أو هندسة اجتماعية، قم بالإبلاغ عنها إلى الجهات المختصة أو منصة التواصل الاجتماعي المعنية.
5. الاستفادة من تقنيات مكافحة الاحتيال: استخدام تقنيات الكشف عن الاحتيال والتزوير العميق للحفاظ على السلامة المعلوماتية.

4. النتائج

يشهد العالم اليوم ثورة هائلة في مجال تكنولوجيا الحوسبة ومعالجة البيانات، تُعرف بصناعة المعلوماتية. وقد ظهرت فرص استثمارية جديدة تتمثل في مؤسسات وشركات ومشاريع فردية، حيث يركز بعضها على تصنيع الأجهزة الحاسوبية، بينما يركز البعض الآخر على تطوير البرمجيات بشكل عام، بالإضافة إلى وجود جهات متخصصة في إعداد الأطر الفنية اللازمة لتشغيل هذه الأنظمة.

ومن الضروري الالتزام باتخاذ تدابير أمنية وقانونية لتعزيز قدرة أجهزة العدالة الجنائية في مجال التحقيقات الرقمية. والتأكد من توافر الأدوات والتقنيات والمهارات المناسبة، مثل: الذكاء الاصطناعي، والبيانات الضخمة، والحوسبة عالية الأداء، ضمن السياسة الأمنية. ويُعدُّ هذا الأمر أولوية أساسية لتحقيق الأمن السيبراني ومكافحة الجرائم السيبرانية. كما يُعدُّ الاستثمار في مجال الأمن السيبراني وإقامة شراكات دولية مع الدول المتقدمة في هذا المجال أمرًا ضروريًّا لمشاركة معلومات التهديدات السيبرانية؛ مما يساعد في تحديد معالم التطور العالمي للفضاء السيبراني.

- تشهد التهديدات السيبرانية تصاعدًا غير مسبوق في التعقيد والتأثير، حيث تُقدَّر الخسائر العالمية الناجمة عنها بنحو 10.5 تريليون دولار سنويًّا بحلول عام 2025، وهو رقم يُنذر بتهديد وجودي للدول والمجتمعات. ولا تقتصر هذه الخسائر على الجرائم المالية التقليدية، بل تمتد إلى تعطيل البنى التحتية الحيوية كشبكات الطاقة والمستشفيات؛ ما يُهدد بانهيار الأنظمة الرقمية التي تُشكل عصب الاقتصاد الحديث. وتزداد الخطورة مع تركيز الهجمات على الشركات الصغيرة والمتوسطة، التي تفتقر إلى البنية الأمنية الكافية؛ مما يُعرِّض استقرار اقتصادات بأكملها للخطر.
- لمواجهة هذه التحديات، أصبح تطوير إطار عالمي عاجلًا ضرورة حتمية. ويتطلب ذلك تعزيز التعاون الدولي عبر منصات مشتركة لرصد الهجمات وتبادل المعلومات، ووضع تشريعات صارمة تلزم الشركات بحماية البيانات، كما في قانون GDPR الأوروبي، الذي فرض غرامة 1.2 مليار دولار على شركة Meta عام 2023. كما يجب توعية الأفراد والمؤسسات بمخاطر المشاركة العشوائية للبيانات، وتدريب الكوادر البشرية على التعامل مع التهديدات السيبرانية المتطورة.
- يرتبط الأمن السيبراني ارتباطًا وثيقًا بالسياسات العامة، التي تحدد القواعد والقوانين والإستراتيجيات اللازمة لضمان تحقيق هذا الأمن. وقد اعتمدت العديد من الدول حول العالم إستراتيجيات شاملة لمكافحة الجرائم المعلوماتية، والتصدي للتهديدات السيبرانية، وتعزيز البنية التحتية.
- لمواجهة المخاطر السيبرانية، من الضروري تحديد التصرفات التي قد تشكل مصادر حقيقية لهذه المخاطر، بما في ذلك الأفعال المسيئة والمضرة، وتحديد المسؤوليات المرتبطة بها. وتتعلق الجرائم السيبرانية باستغلال القاصرين في أنشطة جنسية والاتجار بهم، وهو ما يعرف بالاتجار بالبشر إلكترونيًّا.

كما تظهر آثار الجرائم السيبرانية على الأمن الوطني من خلال تنفيذ عمليات التجسس الإلكتروني على الشخصيات السياسية، أو تهديدهم بالقتل، أو اختراق المؤسسات الرسمية والحيوية للدولة؛ مما يؤدي إلى تدمير المصادر المعلوماتية المرتبطة بها.

- تُعدُّ السرقة والاحتيال الإلكتروني من أبرز المخاطر الناتجة عن الجرائم السيبرانية؛ حيث يتم استخدام الحواسيب والإنترنت لتدمير بعض الجوانب الاقتصادية، من خلال استغلال الموارد المتعلقة بالاقتصاد، والمال والأمن والاستقرار.

5. التوصيات

- تعزيز آليات المواجهة القانونية للاختراقات الرقمية الناتجة عن تطبيقات الذكاء الاصطناعي، وهذا يتطلب تبني إطار تشريعي متكامل يركز على تحديث القوانين المحلية والدولية لمواكبة التحديات الناشئة، مثل: تحديد المسؤولية القانونية عن الأضرار الناجمة عن أنظمة الذكاء الاصطناعي، وفرض معايير أمان صارمة على تصميمها وتشغيلها، وتجريم الاستغلال الخبيث لها في الهجمات الإلكترونية. ويجب أن تشمل هذه الآليات تعزيز التعاون الدولي عبر اتفاقيات تتيح تبادل الخبرات وتنسيق التحقيقات «قانون الذكاء الاصطناعي للاتحاد الأوروبي (GDPR) أنموذجًا».
- تتطلب الحماية الفعَّالة للمجتمعات من التهديدات السيبرانية المتطورة (مثل: هجمات الذكاء الاصطناعي التوليدي والتصيد الاحتيالي المُعزَّز تقنيًّا) والمخاطر الأخلاقية الناشئة (كالتحيّز الخوارزمي أو استغلال البيانات) تبني منهجية ديناميكية تجمع بين الذكاء الاصطناعي الأخلاقي والأمن السيبراني الاستباقي، عبر تعزيز البنى التحتية الرقمية بتشفير كمومي مقاوم وتأمين إنترنت الأشياء (IoT) بمعايير عالمية صارمة، مع دمج أنظمة ذكاء اصطناعي شفافة لاكتشاف الثغرات (Zero-Day) في الوقت الفعلي وتصحيحها آليًّا.
- على الصعيد المؤسسي، يجب تطبيق إطار حوكمة يراقب التطبيقات الأمنية والتنبئية لضمان العدالة، وتفادي الانتهاكات، مدعومًا بشراكات دولية لتبادل معلومات التهديدات ومحاربة الجرائم السيبرانية عبر الحدود، إلى جانب تمكين الأفراد عبر حملات توعوية مكثفة عن مخاطر التكنولوجيا الحديثة وتدريب كوادر متخصصة في الأمن السيبراني الأخلاقي، مع إنشاء آليات إبلاغ آمنة عن الثغرات

وتعويض الضحايا، لتحقيق توازن بين الابتكار التكنولوجي السريع وحماية الخصوصية والحقوق الأساسية في العصر الرقمي.

- اتخاذ إجراءات جديدة تتعلق بإجراء مراجعات دورية للأمن السيبراني، خاصة فيما يتعلق بالأبعاد الدولية المرتبطة بالأصول المشفرة؛ حيث إن هذه الأصول تتجاوز الحدود في تطبيقاتها وبنيتها التحتية، بالإضافة إلى سرعة تطورها وتعقيدها.
- تعزيز التعاون الدولي في مجال الأمن السيبراني؛ نظرًا للطبيعة العالمية للفضاء السيبراني، ودعم التنسيق بين الدول لمواجهة التهديدات السيبرانية وملاحقة مرتكبي الجرائم الإلكترونية.
- في ظل التطور المتسارع للحوسبة الكمومية وتطبيقاتها الثورية، أصبح لزامًا على المجتمعات تبني إستراتيجيات أمنية وأخلاقية متكاملة لمواجهة التهديدات السيبرانية المتطورة والمخاطر الناشئة عن استخدام الذكاء الاصطناعي. وتتمثل الخطوة الأولى في تعزيز البنية التحتية الرقمية عبر اعتماد تشفير ما بعد الكمومية كمعيار أساسي، لحماية البيانات الحساسة في القطاعات الحيوية كالطاقة والاتصالات؛ حيث تُهدد الحواسيب الكمومية بإبطال فاعليَّة خوارزميات التشفير التقليدية. إلى جانب ذلك، يمكن لشبكات توزيع المفاتيح الكمومية (QKD) أن توفر قنوات اتصال غير قابلة للاختراق بين الجهات الحكومية والعسكرية، مستفيدةً من قوانين الفيزياء الكمومية التي تجعل التنصت مستحيلًا دون اكتشافه. ولا تقتصر فائدة الحوسبة الكمومية على الدفاع فحسب، بل تمتد إلى تحليل أنماط الهجمات السيبرانية المعقدة بسرعة هائلة، مما يمكِّن من اكتشاف هجمات «Ze-ro-Day» في الوقت الفعلي، عبر خوارزميات كمومية قادرة على معالجة البيانات بأداء يفوق الحواسيب الكلاسيكية بملايين المرات.

الإفصاح عن تضارب المصالح

يعلن المؤلف أنه ليس له أي تضارب في المصالح للمقالة المنشورة.

الإفصاح عن تمويل البحث

يعلن المؤلف أن البحث المنشور لم يتلقَ أي منحة ماليَّة، من أي جهة تمويل في القطاعات الحكوميَّة، أو التجاريَّة، أو المؤسسات غير الربحية.

المراجع

المراجع العربية

إبراهيم، خالد حازم. (2023). دور الأجهزة الأمنية في الإثبات الجنائي في الجرائم المتعلقة بشبكة المعلومات الدولية، القاهرة: دار النهضة العربية.

إبراهيم، خالد ممدوح. (2021). حجية البريد الإلكتروني في الإثبات: دراسة مقارنة، القاهرة: دار الفكر العربي.

إعلان مونترو للمؤتمر الدولي لمفوضي حماية البيانات والخصوصية.

آل جار الله، عبد العزيز بن غرم الله. (2019). جرائم الإنترنت وعقوباتها وفق نظام مكافحة الجرائم المعلوماتية السعودي: دراسة مقارنة (ويليه آثار العولمة على مستخدمي الإنترنت)، ط1 الرياض: دار الكتاب الجامعي.

أبو بكر، خالد. (2020). تطبيقات الذكاء الاصطناعي في خدمة المصارف العربية، مجلة الدراسات المالية والمصرفية، م25(ع2)، الأكاديمية العربية للعلوم المالية والمصرفية، القاهرة، ص 57-60.

الجامع، موضي. (2019). تقرير المجموعة السعودية لأمن المعلومات، الرياض، السعودية، ص. 22.

خليفة، إيهاب. (2017). تنامي التهديدات السيبرانية للمؤسسات العسكرية، المستقبل للأبحاث والدراسات المتقدمة، مجلة اتجاهات الأحداث، أبو ظبي، الإمارات، ع22، ص.211.

____. (2020). مجتمع ما بعد المعلومات تأثير الثورة الصناعية الرابعة على الأمن القومي، القاهرة: دار العربي للنشر والتوزيع.

____. (2020). الحرب السيبرانية، الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، القاهرة: دار العربي للنشر والتوزيع.

____. (2020). القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت، القاهرة: دار العربي.

____. (2020). تحليلات الأمن السيبراني، القرصنة الإلكترونية مع انتشار «كورونا»، مركز المستقبل للبحوث والدراسات المتقدمة، أبو ظبي.

____. (2024). تطبيقات الذكاء الاصطناعي في مواجهة الشائعات وجرائم الإرهاب في البيئة السيبرانية، المنظمة العربية للعلوم الإدارية RADO، القاهرة: جامعة الدول العربية.

الدريني، أشرف محمد نجيب السعيد. (2021). جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات (دراسة تحليلية مقارنة)، مجلة روح القوانين، كلية الحقوق، جامعة طنطا، م33 (ع 95).

الدليل الإرشادي للحكومة الذكية. (2021) إصدار رقم 1، دولة الإمارات العربية المتحدة، ص 6 - 8.

رشيد، أحمد فخري. (2023). المواجهة الأمنية للجريمة المعلوماتية، بيروت: مكتبة السنهوري.

رمضان، شريف عبد الحميد حسن. (2021). الحرب السيبرانية ومدى ملاءمتها مع القانون الدولي الإنساني، بحث منشور بمجلة كلية الشريعة والأنظمة، جامعة الطائف، المملكة العربية السعودية، ص 217.

الروضان، وليد أحمد. (1439ه). ما الفرق بين أمن المعلومات والأمن السيبراني، صحيفة الجزيرة الإلكترونية، مؤسسة الجزيرة للصحافة والطباعة والنشر، العدد 16631.

السند، عبد الرحمن. (2022). الأحكام الفقهية للتعاملات الإلكترونية، المملكة العربية السعودية، الرياض: دار الرواق للطباعة.

السويدي، جمال سند. (2019). التغيير والأمن.. تعدد مصادر الخطر وآليات المواجهة الجديدة، آفاق المستقبل العدد 33، مركز الإمارات للدراسات والبحوث الإستراتيجية، أبو ظبي، الإمارات العربية المتحدة، ص 9.

شفيق، حسنين. (2016). «انعكاسات الإنترنت على الإعلام الأمني»، القاهرة: دار فكر وفن للطباعة والنشر والتوزيع.

الشهراني، سعد بن علي. (2020). الانحراف الفكري وأثره على الأمن الوطني والجماعي لدول مجلس التعاون لدول الخليج العربية، جامعة نايف العربية للعلوم الأمنية، الرياض.

عبد الرازق. رانا مصباح (2022). آليات مكافحة جرائم السيبرانية في المملكة العربية السعودية، العدد رقم 3، المملكة العربية السعودية.

عبد الصادق، عادل. (2022). القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، مجلة السياسة الدولية، العدد 188، مؤسسة الأهرام، مصر، ص 32.

عبد العال، جيهان أحمد. (2022)0 الجهود المصرية لمواجهة التحديات السيبرانية، مجلة الديمقراطية، مصر، م12(ع2)، 10 ص67.

عطوش، ضرغام جابر (2017) . جريمة التجسس المعلوماتي: دراسة مقارنة، القاهرة: المركز العربي للنشر والتوزيع.

علي، محمد بدر صابر. (2021). المخاطر الناتجة عن انتشار الشائعات الإلكترونية على مستخدمي مواقع التواصل الاجتماعي ومقترحات مواجهتها من منظور تنظيم المجتمع، أسيوط، كلية الخدمة الاجتماعية، مجلة دراسات في الخدمة الاجتماعية، ج1، ص 215.

فوزي، محمد. (2024). موسوعة الأمن السيبراني، أكاديمية شرطة الشارقة للعلوم الأمنية، معرض الشارقة للكتاب، الإمارات العربية المتحدة.

الفيل، علي عدنان. (2022). الإجرام الإلكتروني: دراسة مقارنة، بيروت: منشورات زين الحقوقية.

قادم، جميلة. (2022). الشائعات الإلكترونية ودوروها في تضليل الرأي العام - الفضاء السيبراني نموذجًا، جامعة الجزائر، كلية علوم الإعلام والاتصال، مجلة الرسالة للدراسات والبحوث الإنسانية، م 7(ع3)، ص 185.

القحطاني، عبدالله بن صالح، (2021). دراسات تربوية ونفسية، الناشر: جامعة الزقازيق، كلية التربية.

القرعان، محمود أحمد. (2021). الجرائم الإلكترونية، ط1، عمان: دار وائل للنشر والتوزيع.

محمد نبيل عبد الرؤوف، الأمن السيبراني (ضرورته، متطلبات تحققه)، مجلة كلية الدراسات العليا، أكاديمية الشرطة، (ع34).

محمد، علي محمد. (2018). «كوارث الإرهاب الإلكتروني بين الفلسفة القانونية وتطور الأمن التقني»، القاهرة: دار النهضة العربية.

المطيري، سلطان خلف. (2015). شبكات التواصل الاجتماعي وعلاقاتها بتحقيق الأمن المجتمعي، رسالة ماجستير كلية العلوم الإستراتيجية، قسم الدراسات الإقليمية والدولية، جامعة نايف العربية للعلوم الأمنية، ص 61.

موسى، مصطفى محمد. (2022). المراقبة الإلكترونية عبر شبكة الإنترنت، دراسة مقارنة بين المراقبة الأمنية التقليدية والإلكترونية، الكتاب الخامس، القاهرة: دار الكتب والوثائق القومية المصرية.

المراجع الأجنبية

Desforges, Alix. (2021). Representations of Cyberspace a Geopolitical Tool, Carin International Magazine, Vol. 152-153, Issue 1-2, pp. 67 - 81.

Alzahrani, Saleh and Pichappan. (2007) “An Empirical study of enabling security systems for Organizations”. Information technology & National Security Conference hold in Riuadh.

IYU (2023). Global Cybersecurity Index. Geneva: TU. Development Sector. ITU Publications. pp. 25 – 30.

Darko Galinec, Darko Moznik & Boris Guberina, (2017). “Cybersecuity and Cyber Defenc: National Level Stra-tegic Approach”, Automatika 58.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P, Garfinke B., & Amodei, D. (2018).

Brenton, Chris. (2020). Cameron Hunt, Network Security, Alameda,2020, pp. 510-513.

Sulaiman, Noor Suhani, Muhammad Ashraf Fauzi, Walton Wider, Jegatheesan Rajadurai, Suhaidah Hussain, and Siti Aminah Harun. 2022. “Cyber-Information Security Compliance and Violation Behaviour in Organisations: A Systematic Review” Social Sciences 11, no. 9: 386. https://doi.org/10.3390/socsci11090386 www.scopus.com

Top Cybersecurity Statistics for 2025:

The New Eyes of Surveillance. (23 Jan 2017). Artificial Intelligence and Humanizing Technology, https://www.wired.com/insights/2014/08/the-new-eyes-of-surveillance-artificial-intelligence-and-humanizing-technology/.

Meeuwisse, Raef. (March 2019). cybersecurity for beginners, p. 524.

https://www.cobalt.io/blog/top-cybersecurity-statistics-2025 (11/3/2025). The 2024 SpyCloud Ransomware De-fense Report:

https://spycloud.com/resource/2023-ransomware-defense-report/ (12/3/2025)

Calder, Alan. (February 2014). National Institute of Standards and Technology - Developing Security Plans for Federal Information Systems, Canada.