الاتجاهات العالمية الحديثة لبحوث ودراسات جرائم الذكاء الاصطناعي والأمن السيبراني في مواقع ومنصات الاعلام الرقمي: رؤية مستقبلية

Recent Global Trends in Research and Studies on Artificial Intelligence Crimes and Cybersecurity in Digital Media Sites and Platforms: A Future Vision

أ. د. مجدي عبد الجواد الداغر

Prof. Dr. Magdy Abdel Gawad Al-Dagher

جامعة المنصورة ـ مصر

Mansoura University - Egypt

مستخلص

يشهد العالم تطوراً متسارعاً في تقنيات الذكاء الاصطناعي وتطبيقاته، مما أدى إلى بروز تحديات أمنية جديدة تتعلق بجرائم الذكاء الاصطناعي والأمن السيبراني، خاصة على منصات الإعلام الرقمي. يتناول هذا البحث الاتجاهات العالمية الحديثة في بحوث ودراسات هذه الجرائم، مع تسليط الضوء على آليات الاستخدام غير المشروع للذكاء الاصطناعي في التضليل الإعلامي، والهجمات السيبرانية، والانتهاكات الرقمية للخصوصية. كما يناقش البحث استراتيجيات المواجهة والتشريعات الدولية المستحدثة، ودور المؤسسات الإعلامية والتقنية في بناء بيئة رقمية أكثر أماناً. ويستعرض البحث نماذج تحليلية وتنبؤية حول مستقبل التهديدات السيبرانية وآفاق الذكاء الاصطناعي في هذا المجال، مع تقديم رؤية مستقبلية تسعى إلى مواءمة التطور التكنولوجي مع الحماية القانونية والأخلاقية. ويخلص البحث إلى ضرورة تبني نهج عالمي موحّد للتصدي لتلك التحديات ضمن إطار تكاملي يراعي الأمن، والشفافية، وحقوق الأفراد في الفضاء الرقمي.

الكلمات المفتاحية: اتجاهات البحوث الحديثة، جرائم الذكاء الاصطناعي، الأمن السيبراني، منصات الاعلام الرقمي.

Abstract

The world is witnessing rapid development in artificial intelligence technologies and applications, leading to the emergence of new security challenges related to AI crimes and cybersecurity, particularly on digital media platforms. This research examines recent global trends in research and studies on these crimes, highlighting the mechanisms of the illicit use of AI in media disinformation, cyberattacks, and digital privacy violations. It also discusses counter-strategies, emerging international legislation, and the role

of media and technology institutions in building a safer digital environment. The research presents analytical and predictive models on the future of cyber threats and the prospects of AI in this field, while presenting a future vision that seeks to align technological development with legal and ethical protection. The research concludes with the necessity of adopting a unified global approach to address these challenges within an integrated framework that takes into account security, transparency, and individual rights in the digital space.

Keywords: Modern research trends, AI crimes, cybersecurity, digital media platforms.

مقدمة

تُعد الجريمة - التقليدية – والذكية- من الظواهر السلبية التي تهدد كيان المجتمع، وتعمل على الإضرار بمصالح أفراده، فيما يكتسب السلوك الإجرامي في ضوء المتغيرات العالمية - ثورة الاتصالات والمعلومات- أبعاداً جديدة، حيث تطورت الظاهرة الاجرامية وزادت معدلاتها وتنوعت صورها، واستحدثت أشكال جديدة منها، كما تنوعت اساليب ارتكابها وبيئاتها، الأمر الذي أدى إلى تزايد الاضرار الناجمة عنها.[١]

ومع تنامى التقنية الحديثة ظهرت تطبيقات الذكاء الاصطناعي وتحليل البيانات الضخمة وإنترنت الأشياء والمدن الذكية، والتي تزايد معها تأثيرات تلك التقنيات من ناحية المزايا والمخاطر على حد سواء، حيث تبرز أهمية معرفة المخاطر التي تشكلها تلك الوسائل والتطبيقات والتي تتطور بشكل ملحوظ يوما بعد أخر، والتي تضم أخطار متنوعة من بينها الجرائم الذكية، ومخاطر التأثير على قيم المجتمع وأخلاقياته.[٢]

وتعد الجرائم الذكية مصطلحًا واسعًا يشمل أشكالاً أخرى من الجرائم الالكترونية، يأتي من بينها جرائم الحاسب Computer Crimes، وجرائم الإنترنت، Internet Crimes، وجرائم الاتصال المباشر Online Crimes، وجرائم التكنولوجيا الجديدة، New Technology Crimes، وجرائم التكنولوجيا العالية، Hi Tech Crimes، وكذلك يمتد التوصيف ليشمل عالم الجناة، فهناك مجرمو الإنترنت cyber-criminals، والمتنمرون عبر الإنترنت cyber-bullies، والقراصنة الرقميون digital pirates، واللصوص الرقميون digital thieves، والمتسللونhackers ، والمخترقون Crackers وغيرهم .[٣]

وتختلف الجرائم الذكية كثيرا عن الجرائم التقليدية من حيث طبيعتها ونطاقها ووسائلها وأدلتها، فقد أدى التطور السريع في مجال تقنية المعلومات والاتصالات وشبكة الإنترنت إلى ظهور أنماط جديدة من الجرائم جاءت عن طريق الاستغلال السيئ للتكنولوجيا الحديثة، مما ترتب عليه خلق ظاهرة إجرامية جديدة تتم عن طريق هجمات واختراقات وتسلل داخل النظم المعلوماتية، إما بغرض تدمير

(1) G. Technology, "Trends in Cybercrime in 2022 and Beyond," 2021. [Online]. Available: https://blog.govnet.co.uk/technology/trends-in-cybercrime-in-and-beyond.

(2) AGG, "Cybercrime trends 2022," 2020. [Online]. Available: https://aag-it.com/the-latest-2022-cyber-crime-statistics/.

(3) Axelrod, The Evolution of Cooperation, A second generation computer forensic analysis system, Digital investigations, New York: Basic Books Inc, 1984, pp. 34-42.

تلك النظم أو الحصول على معلومات سرية سواء عسكرية أو اقتصادية، الأمر الذي ينبه بوجود مخاطر على الصعيد الدولي والوطني، فلابد من إيجاد سبل للتصدي لهذه الظاهرة.
وتتسم الجرائم الذكية بطابع سرية الهوية وأنها لا تترك سوى القليل من الأثر، بالإضافة إلى ذلك لا تقف امام الجرائم الذكية أي قيود إقليمية أو زمنية، ويمكن أن تسبب أضراراً فورية لعدد لا يحصى من الضحايا.
وتتمثل الخطورة التي تتميز بها هذه النوعية من الجرائم في كونها سهلة الارتكاب بسبب الاستخدام السيئ للتطبيقات الحديثة، إضافة إلى أن مرتكبي هذا النوع من الجرائم ليسوا مجرمين عاديين، بل يتسمون بالفطنة والذكاء والمهارة في التعامل مع البرامج الحديثة وغيرها، وقد أثار التحري والبحث والتحقيق في الجرائم الذكية معوقات وعراقيل في استخلاص الأدلة التي تثبت وقوعها وتدين مرتكبيها كونها تختلف عن الأدلة التقليدية في الجرائم العادية.
وفى إطار ذلك حرصت حكومات العديد من الدول في العالم ومؤسساتها الأمنية على تطوير أنظمة مكافحة الجرائم والتي يأتي من بينها جرائم الذكاء الاصطناعي، وذلك بإدخال نصوص تشريعية عقابية وإجرائية تتلاءم مع ظاهرة الجرائم الذكية، وسن تشريعات خاصة ومستقلة.
وقد اهتم الباحثون بدراسة الأسباب والعوامل المؤثرة في انتشار الجرائم بأنماطها المختلفة، بالإضافة إلى إثارة بعض القضايا التي شغلت الساحة العالمية وذلك في ضوء مواجهة التطورات والتغيرات الاجتماعية والاقتصادية والسياسية والاخلاقية التي شهدها العالم وما طرحته من انحرافات سلوكية ومشكلات اجتماعية تمثل خطراً يهدد أمن المجتمع واستقراره، الأمر الذى فرض على الحكومات والمؤسسات الكبرى الاهتمام بالأمن السيبراني ودوره في الحد من ظاهرة الجرائم عبر المنصات الرقمية، ومن هنا تهتم الدراسة بالتعرف على الاتجاهات العالمية الحديثة لبحوث جرائم الذكاء الاصطناعي والأمن السيبراني في مواقع ومنصات الاعلام الرقمي.

المبحث الأول: منهجية البحث

مشكلة الدراسة وأبعادها:

تساهم تطبيقات الذكاء الاصطناعي في تبسيط التعرف على الأنماط، مثل اكتشاف نمط تكرار في نص ما في رسائل البريد الإلكتروني أو نمط محدد في ملف صوتي، كما توفر أدوات الذكاء الاصطناعي أدوات حسابية يمكن أن تساعد في بناء أدلة ذات صلة إحصائية، الأمر الذي يقلل من الأخطاء، ويحسن من فهم بعض النتائج في عملية التعرف على الأنماط والتكرار في البيانات الضخمة يشمل ذلك التعرف على أنماط الصور، حيث يحاول النظام التعرف على أجزاء مختلفة من الصور أو الأشخاص وأنواع أخرى من التعرف تطبيقات الذكاء الاصطناعي في مجال إعادة بناء مسرح الجريمة ، حيث يعمل الخبراء على تفسير كيفية حدوث الجريمة من خلال عدد من المعطيات والنتائج للأدلة المرفوعة من مسرح الجريمة حتى يتمكنوا من تحديد نوع الجريمة والتعرف على الجاني وكيفية حدوث الجريمة.
وتسعى الدراسة إلى رصد الاتجاهات الحديثة في تلك الدراسات من حيث مجالات الاهتمام البحثي، وتحليل ونقد أهم نتائجها وتوصياتها، وكذلك التعرف على أهم الأطر المعرفية والنماذج والأطر النظرية التي انطلقت منها، وتحديد المناهج البحثية وأدوات جمع البيانات التي اعتمدت عليها، ومن ثم تقديم رؤية مستقبلية بحثية في هذا المجال الجديد، وذلك عبر استخدام التحليل من المستوى الثاني بشقيه الكمي والكيفي للدراسات العلمية المنشورة عالميا.

ومن هنا تتبلور مشكلة الدراسة في التعرف على الاتجاهات العالمية الحديثة لبحوث ودراسات جرائم الذكاء الاصطناعي والأمن السيبراني في مواقع ومنصات الاعلام الرقمي.

أهمية الدراسة:

تبرز أهمية الدراسة في الاستفادة من نتائجها وإثراء البحث العلمي المتعلق بجرائم الذكاء الاصطناعي والأمن السيبراني في مواقع ومنصات الاعلام الرقمي، لتقديمها مؤشرات معرفية لما تم تناوله من قضايا وموضوعات بحثية، وما يتطلب الاهتمام بدراسته في البحوث المستقبلية.

كما تعد الدراسة من البحوث التوثيقية التي ترصد اتجاهات الباحثين خلال فترة زمنية حديثة مما يمثل إضافة علمية للمكتبة الإعلامية العربية، حيث يمكن الاستفادة من نتائج وتوصيات دراسات وبحوث جرائم الذكاء الاصطناعي التي تم تحليلها في التعرف على كيفية مواجهة تلك الجرائم مستقبلاً.

كما تكمن أهمية الدراسة الحالية في كونها تتعلق بالإعلام الرقمي وارتباطه بالأمن السيبراني الذي يؤثر بدوره بطريق مباشر نحو الاستقرار وإيجاد حلول إيجابية لتوفير بيئة خصبة تتحلى بالأمن والسلام وتتجه نحو تحقيق امن الأفراد والدول واستقرارها، ومكافحة التهديدات والجرائم التي تصاحب استخدامات الذكاء الاصطناعي.

أهداف الدراسة:

- رصد الدراسات التي تناولت جرائم الذكاء الاصطناعي والأمن السيبراني.
- التعرف على الموضوعات الى تناولت جرائم الذكاء الاصطناعي والأمن السيبراني.
- التعرف على النماذج والأطر النظرية التي انطلقت منها تلك دراسات جرائم الذكاء الاصطناعي والأمن السيبراني.
- تحديد المناهج والأدوات البحثية التي اعتمدت عليها دراسات جرائم الذكاء الاصطناعي والأمن السيبراني.
- مقارنة نتائج الدراسات التي تناولت جرائم الذكاء الاصطناعي والأمن السيبراني.
- تقديم رؤية مستقبلية في مجال جرائم الذكاء الاصطناعي يمكن الاستفادة منها في قضايا بحثية جديدة.

تساؤلات الدراسة:

- ما حجم الاهتمام بدراسات جرائم الذكاء الاصطناعي والأمن السيبراني في مجال الاعلام الرقمي؟
- ما المجالات التي تناولتها الدراسات الخاصة بجرائم الذكاء الاصطناعي والأمن السيبراني؟
- ما الموضوعات التي تناولتها دراسات جرائم الذكاء الاصطناعي والأمن السيبراني؟
- ما الأطر المنهجية التي طبقتها الدراسات الخاصة جرائم الذكاء الاصطناعي والأمن السيبراني؟
- ما الأطر النظرية التي انطلقت منها تلك الدراسات الخاصة جرائم الذكاء الاصطناعي والأمن السيبراني؟
- ما أهم النتائج التي توصلت إليها دراسات جرائم الذكاء الاصطناعي والأمن السيبراني؟
- ما التوجهات البحثية المستقبلية دراسات وبحوث جرائم الذكاء الاصطناعي والأمن السيبراني؟

مفاهيم ومصطلحات الدراسة:

مفهوم الجريمة الالكترونية: الجريمة الإلكترونية هي المخالفات التي ترتكب ضد الأفراد أو الجماعات باستخدام منصات الاتصال (مثل غرف الدردشة والبريد الإلكتروني والموبايل، وتكمن خطورة هذه الجرائم في كونها سهلة الارتكاب وصعبة الإثبات وتتخطى الحدود الإقليمية للدولة لتمتد إلى جميع دول العالم كونها متصلة مع بعضها البعض عبر شبكة لا حدود لها.

مفهوم الأمن السيبراني: يعرف الأمن السيبراني بأنه حماية الأنظمة والشبكات والبرامج والموقع الجغرافي من الهجمات الرقمية ومن أي مشكلة أو عائق أو هجمات إلكترونية تحول دون أداء عملها،

حيث تهدف الهجمات الإلكترونية عادة إلى الوصول إلى المعلومات الحساسة بهدف تغييرها أو إتلافها أو ابتزاز الأموال من المستخدمين. [١]

مفهوم الذكاء الاصطناعي: الذكاء الاصطناعي هو علم يهتم بصناعة آلات تقوم بتصرفات يعتبرها الإنسان تصرفات ذكية، بواسطة برنامج يفكر بنفس الطريقة التي يفكر بها الإنسان الخبير، وهو أحد علوم الحاسب الآلي الحديثة التي تبحث عن أساليب متطورة لبرمجته للقيام بأعمال واستنتاجات تشابه الأساليب التي تنسب لذكاء الإنسان. [٢]

أسباب اختيار موضوع الدراسة:

- أن تطور الاعلام الرقمي صاحبة تطور في نوعية الجرائم، وهو ما ساهم في ظهور جرائم لم تكن موجودة من قبل.
- تنامى جرائم تطبيقات الذكاء الاصطناعي مؤخراً والتي من بينها جرائم الروبوتات الآلية
- تعدد القطاعات التي تأثرت بجرائم الفضاء الإلكتروني من بينها قطاع الإعلام وشبكات وأنظمة الاتصالات.
- الحاجة إلى دراسات تعزز من الوعي الإعلامي بمخاطر الجرائم الذكية في المجتمعات العربية.
- الحاجة إلى تدشين قوانين وتشريعات رادعة تسهم في الحد من جرائم الإنترنت والفاعلين بها.
- اهتمام قادة الدول والمنظمات الدولية والإقليمية بقضايا الأمن السيبراني والجرائم الذكية.
- تزايد أخطار ومهددات الأمن السيبراني على أمن الأفراد والدول، بما في ذلك الدول الكبرى ذاتها.

نوع الدراسة:

تعد الدراسة من الدراسات الوصفية التحليلية، حيث تهتم برصد وتوصيف وتحليل الاتجاهات البحثية الحديثة وتطور التناول العلمي لظاهرة جرائم الذكاء الاصطناعي والأمن السيبراني بمختلف جوانبها.

منهج الدراسة: وتعتمد الدراسة على أسلوب تحليل المستوى الثاني بشقيه الكمي والكيفي للدراسات العربية والأجنبية التي تناولت جرائم الذكاء الاصطناعي والأمن السيبراني في الإطار الزمني من عام ٢٠٢٠ وحتى عام ٢٠٢٤

بالإضافة الى تحديد الموضوعات التي تناولتها وأطرها المنهجية والنظرية البحثية محل الاهتمام وهي جرائم الذكاء الاصطناعي والأمن السيبراني، وتحديد أهداف مراجعة الدراسات المنشورة حول هذه القضايا، وجمع المعلومات منها، والتصنيف والتحليل الكيفي لتلك المعلومات وتفسيرها، والتحليل الكمي للمؤشرات المعرفية والنظرية والمنهجية للدراسات، ورصد النتائج والتوصيات والخروج برؤى مستقبلية.

أداة جمع البيانات:

تمثلت أداة جمع البيانات في تحليل المحتوى من أجل تحديد البيانات الأساسية للدراسة، وعدد الباحثين المشاركين فيها، وسنة نشرها، والدولة التي تم التطبيق عليها، والاتجاه البحثي التي تناولته، والإطار المعرفي أو النظري الذي انطلقت منه، والمنهج البحثي الذي طبقته، وأهم نتائج الدراسة وتوصياتها.

(1) S. Morgan, "Official Cyber Crime Report," Cybersecurity Ventures, 2022

(2) Chan-Olmsted, S. M. (2019). A Review of Artificial Intelligence Adoptions in the Media Industry. International Journal on Media Management, 21(3–4), 193–215. Doi:10.1080/14241277.2019.1695619

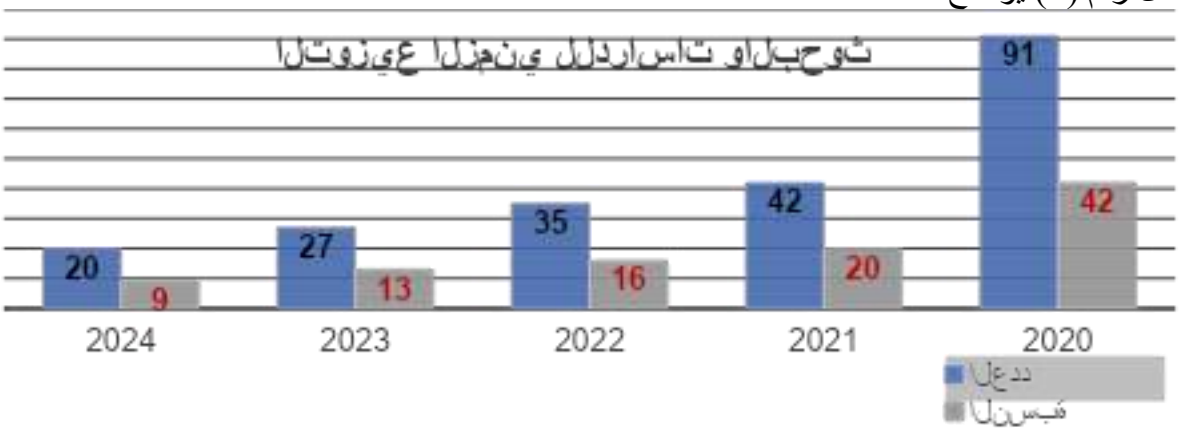
مجتمع وعينة الدراسة:

تمثل مجتمع الدراسة في الدراسات العربية والأجنبية المنشورة في دوريات علمية محكمة ورسائل الماجستير والدكتوراة المنشورة وغير المنشورة، والتي تناولت جرائم الذكاء الاصطناعي والأمن السيبراني، في الفترة من عام ٢٠٢٠ وحتى نهاية عام ٢٠٢٤، وقد بلغ إجمالي الدراسات والبحوث التي توصل اليها الباحث (٢١٥) دراسة، فيما تحددت معايير اختيار العينة عبر استخدام كلمات مفتاحية عربية وإنجليزية هي:

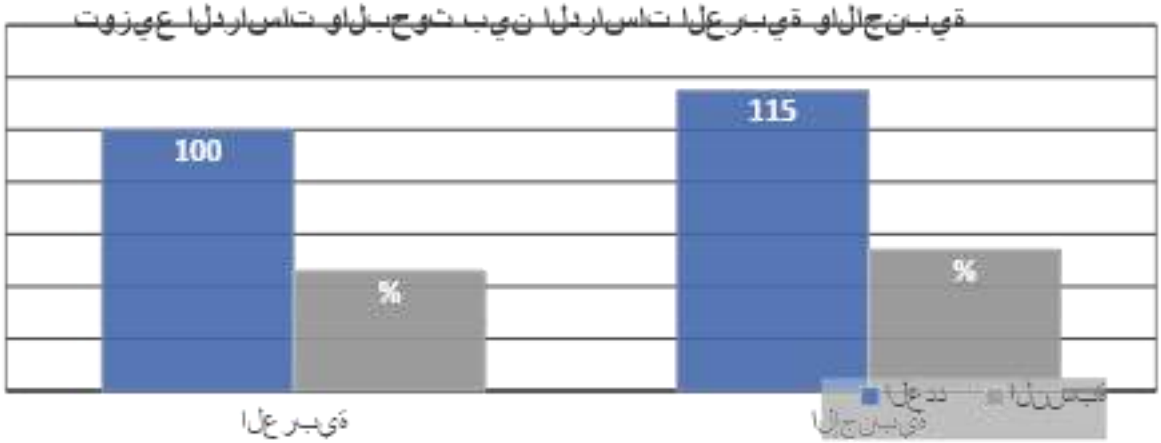
Cyber Security, Cyber Terrorism, Deepfakes, Digital Media, Cyberspace , Robot Crimes, national security, Dark Web Crimes

فيما شملت مصادر البحث، المصادر العربية التالية: دار المنظومة، ودار المنهل، وبنك المعرفة المصري، ومركز الأهرام للدراسات السياسية والاستراتيجية، وعلى المستوى الدولي جاءت المصادر التالية: SAGE، ProQuest، Scopus database، Academic Search Complete database، Google، Google Scholar.

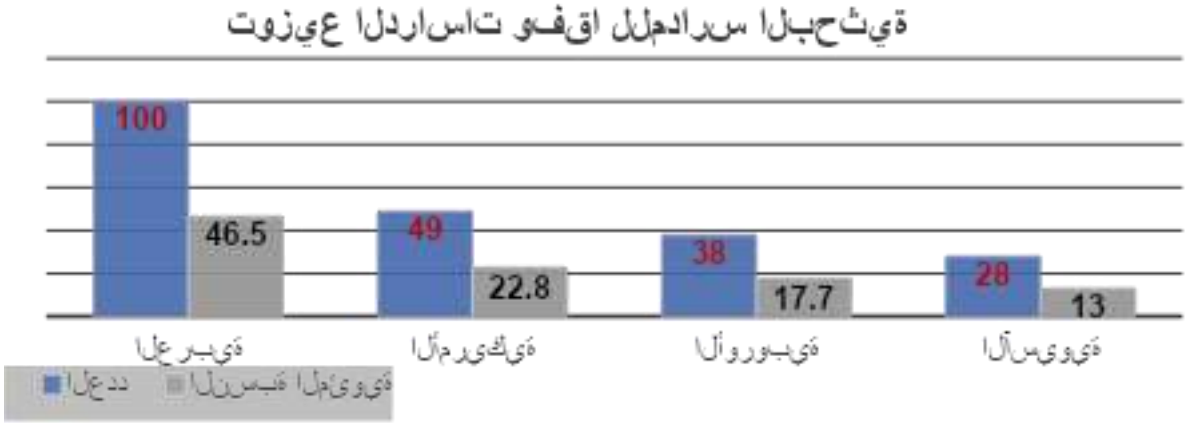
الشكل رقم (١) يوضح



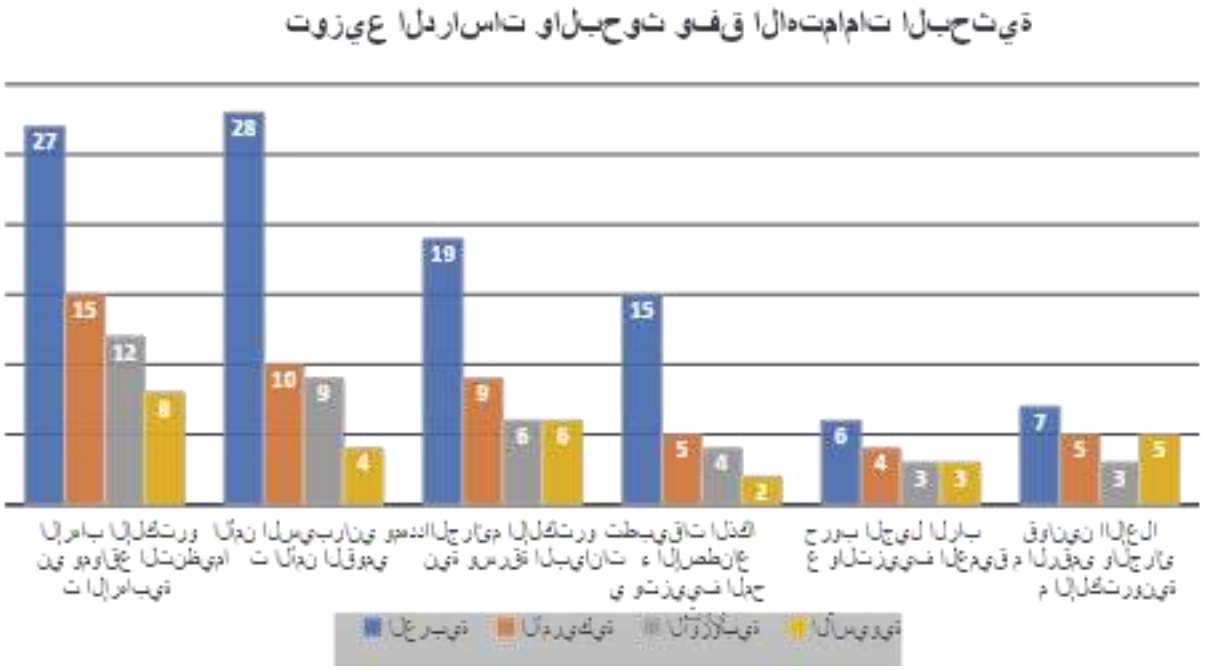
الشكل رقم (٢) يوضح



الشكل رقم (٣) يوضح



الشكل رقم (٤) يوضح



المبحث الثاني الإطار المعرفي لدراسات وبحوث جرائم الذكاء الاصطناعي والأمن السيبراني:

يعبر مفهوم الأمن السيبراني عن تطبيقات عبر أجهزة الكمبيوتر أو الشبكات، لحماية البيانات، والأمن السيبراني نعني به الإجراءات الواجب اتخاذها من الأجهزة الأمنية للحفاظ على سرية المعلومات الإلكترونية، ومنع الاختراقات الفيروسية من أجل ضمان وصول المعلومات الحاسوبية إلى الجهات المختصة في الوقت المناسب، وضمان عدم وقوعها في أيدي غير حليفة للدولة...).

والأمن السيبراني هو حماية الأجهزة الرقمية وقنوات الاتصال الخاصة بها للحفاظ على استقرارها واعتماديتها وخلوها من الخطر أو التهديد. عادةً ما يجب أن يكون مستوى الحماية المطلوب كافيًا لمنع الوصول غير المصرح به، أو التدخل الذي يمكن أن يؤدي إلى أضرار شخصية، مهنية، تنظيمية، مالية أو سياسية، كما أن الأمن السيبراني يتعلق بحماية ما هو أكثر من أجهزة الكمبيوتر، فهو يتجاوز مجرد حماية كل التكنولوجيا في الحقيقة، الأمن السيبراني يتعلق بحماية الأشخاص الذين يعتمدون بشكل مباشر أو غير مباشر على أي شيء إلكتروني. [١]

مجالات الأمن السيبراني:

تعددت مجالات الأمن السيبراني وتطورت، ومن أمثلة المجالات التي تندرج تحت مظلة الأمن السيبراني: [٢]

- أمن الشبكات: يتضمن ذلك حماية الشبكات المادية والسيرفرات " servers " وجميع الأجهزة المتصلة بها، والسماح للمستخدمين المصرح لهم فقط إلى الشبكة وعدم التعرض لحدوث سلوكيات مشبوهة داخل الشبكة أو أي اختراقات.
- أمن التطبيق: يرتبط هذا النوع بتأمين التطبيقات الموجودة على الشبكة بهدف الحفاظ عليها من أي تهديدات من شأنها التركيز على تدمير تلك التطبيقات التي تمثل العمود الفقري للشبكة وخاصة الشركات التي تعمل على تطوير وبيع التطبيقات والخدمات السحابية الحديثة، ويتم استخدام خدمة سحابية كبيرة مثل Microsoft ٣٦٥ كنوع من أنواع التأمين للتطبيقات الموجودة على الشبكة لكنها تحتاج لتخصيص إعدادات الأمان من خلال الإعدادات الافتراضية.
- أمن المعلومات: يختص هذا النوع من التأمين بأمن المعلومات وحماية بيانات الخاصة بالشركات إضافة الى البيانات التي يتم جمعها من العملاء وذلك من منطلق الحفاظ على خصوصية وسرية البيانات والامتثال للوائح والقوانين المنظمة للخصوصية، حيث أن الشركات لابد لها من الالتزام وتطبيق معايير أمن المعلومات، في حين ان الشركات التي تخل عن هذه المعايير تتعرض لعقوبات خاصة إذا كان الإهمال يؤدي إلى اختراق المعلومات التعريفية للأشخاص. لذا فإن الشركات التي تعمل في مجال الأمن السيبراني تعمل تامين جمع البيانات وتخزينها ونقلها، وتطبيق وسائل الحماية الكافية التي تضمن تشفير البيانات وحمايتها من التعرض للانتهاك.

---

(1) Ulusoy, Ş. & Atar, Ö. (2020). Reflection of social media addiction on family communication processes. Adam Academy Journal of Social Science, 10(2), 425-445. https://www.proquest.com/scholarly-journals/reflection-social-media-addiction-on-family/docview/2581938797/se-2

(2) James, P. & Kur, J. (2020). Parental Mediation of Children's Risky Experiences with Digital Media. The Journal of Society and Media, 4(2), 298-318. https://www.researchgate.net/publication/350816418

- الأمن السحابي: يتميز العصر الحديث بما يسمى Cloud Computing) الحوسبة السحابية (تلك التقنية التي أصبحت منتشرة وواسعة الاستخدام في مجالات شتى ومن أهم تطبيقاتها " التخزين السحابي "، ويلعب الأمن السحابي دور فعالاً في حماية البيانات المُخزنة من الاختراق أو الحذف أو التشوية، كما يقوم الأمن الحاسوبي بعمل الدعم وتوفير كل الحماية للمكونات والبيانات التي تدخل في عملية الحوسبة السحابية بما يضمن عدم الدخول إلى [١] ..Cloud Computing

- أمن العمليات: يعد أمن العمليات Operation Security واحد من أهم أعمدة الامن السيبراني وهو جزء لا يتجزأ من الاستراتيجية الشاملة للأمن السيبراني. ويتضمن على جميع العمليات المختلفة التي من شأنها تعريف الخطوات والإجراءات التي ينبغي فعلها لصد العمليات العكسية التي تتم من قبل الأشخاص الذين يسعون للوصول إلى البيانات الحساسة بطرق غير مصرح بها.

- أمن المستخدم النهائي : و يقصد به أمان النقاط النهائية أو الطرفية End Points) (في النظام والمرتبطة بحماية الأجهزة المتصلة بالنظام ويتم استخدامها من قبل المستخدمين بطريقة مباشرة أنفسهم ويعد أمان المستخدم النهائي أمرًا في منتهى الأهمية والحيوية حيث أن معظم الهجمات الإلكترونية دائما وأبداً تبدأ برسالة عبر بريد إلكتروني للتمكين من التصيد الاحتيالي ، لذا يجب الاحتياط وزيادة التدريب بالوعي لأمن المستخدمين وتنمية المهارات لدى المستخدمين في التعامل واكتسابهم طرق اكتشاف رسائل البريد الإلكتروني المخادعة. هذا بخلاف حماية الأجهزة والتحقيق من أمن الكلمات المرورية المعقدة وحساسيتها. [٢]

- أمن إدارة الهوية والوصول: يمثل أمن إدارة الهوية والوصول واحدة من أكثر المجالات أهمية التي يعنى بها الأمن السيبراني. وتشمل مجموعة القوانين والقواعد إضافة فضلاً عن الممارسات التي تتم على الشبكة وتضمن وصول الأشخاص المستخدمين المصرح لهم من خلال (System Administrator) الى المعلومات الصحيحة المطلوبة وذلك في الوقت المناسب والزمان المناسب وللأسباب الصحيحة.[٣]

- أمن إنترنت الأشياء: لقد انتشرت تقنية إنترنت الأشياء بصورة واسعة في الفترة الأخيرة وتغلغلت في نواحي كثيرة من مجالات البيئة الرقمية التي تغطى جميع مجالات الحياة المعاصرة فهي تعد واحدة من أفضل التقنيات الواعدة للغاية التي تنمو بطريقة سريعة، وهذه التقنية تعتمد على استخدام Smarting Devices وربطها بالإنترنت مثل الغسالة أو الثلاجة أو أي أجهزة منزلية أخرى. ويكون دور IOT Security التي تعد جزء من الامن السيبراني حماية البيانات وتأمين

(1) Alanazi, N. (2018). A Study of The Influence of Social Media Communication Technologies on Family Relationships In The Kingdom of Saudi Arabia. Journal of humanities and Social Sciences, 2(8), 107-136. https://search.mandumah.com/Record/941373

(2) Sarker, G. (2022). An Interlinked Relationship between Cybercrime & Digital Media. International Journal for Multidisciplinary Research (IJFMR), 4(6), 1-5. https://www.ijfmr.com/papers/2022/6/1051.pdf

(3) Cain, J. & Imre, I. (2022). Everybody wants some: Collection and control of personal information, privacy concerns, and social media use. New Media & Society, 24(12), 2705–2724. https://08113e081-1104-y-https-doi-org.mplbci.ekb.eg/10.1177/14614448211000327

جميع الأجهزة المتصلة بالشبكة والقيام بصد أي هجمات أو انتهاكات على الشبكة تتم على الأجهزة المنزلية التي يتم التحكم بها من خلال من قبل إنترنت الأشياء IOT__

- أمن الأجهزة المحمولة : تعد الهواتف الذكية أكثر الوسائل أو الأجهزة التي تقع عرضة للهجمات السيبرانية، ويكون مستخدمها في خطر خاصة عند تنزيل التطبيقات جديدة وغير معروفة بموجب نظام تشغيل خاص بالهاتف، فضلًا عن مستقبلات وعدسات وأجهزة استشعار متعلقة به، وينطوي كل هاتف ذكي على عيوب محتملة تسمى أحيانًا أخطاء برمجية، بالإضافة إلى أخطاء من المستخدم ذاته حينما يفتح رابطا أو رسالة غير آمنة؛ مما يسمح للقراصنة بالسيطرة على الهاتف وإحداث خلل في أمن الهاتف وخصوصيته، ومن الممكن أن تجعل نظام التشغيل ينهار أو يتصرف على نحو غير متوقع عند استقبال رسالة تنطوي على خداع ما، أو ملفات تحتوي على برامج خبيثة. فقد أصبحت تلك الأجهزة مرصد ومطمع للهجمات والانتهاكات الإلكترونية من قبل الأشخاص ذوي الأغراض السيئة. وعند حدوث أي هجوم أو انتهاك تتأثر تلك الأجهزة وتتعطل جميع التطبيقات المرتبطة بها. لذا يلعب أمن الأجهزة المحمولة دوراً حيويا في حماية وتأمين تلك الأجهزة وتعزيز الأمن الخاص بها. من خلال مجموعة من الممارسات والقواعد التي ينفذها عدد من المتخصصين. [١]

أبعاد الأمن السيبراني

يتضمن الأمن السيبراني أنظمة تهدف إلى الحفاظ على الاستقرار والأمان من جميع التهديدات السيبرانية، ويتضمن الأمن المتكامل الجوانب التي تسهم في تعزيز نظام الأمن السيبراني، وذلك وفق الأبعاد التالية: [٢]

- البعد العسكري: يهدف الأمن السيبراني إلى الحفاظ على قدرة الوحدات العسكرية على التواصل عبر الشبكات العسكرية، وهو ما يسهل من عملية تبادل المعلومات بين قادة الوحدات، وقد تُعد نقطة ضعف، خاصة إذا لم تكن آمنة، حيث يمكن أن يؤدي تدمير قواعد البيانات العسكرية أو الابتزاز عليها إلى تعطيل الاتصالات بين وحدات القيادة والوحدات العسكرية، بالإضافة إلى خطر فقدان السيطرة على بعض الأسلحة مثل الطائرات بدون طيار والصواريخ الموجهة والأقمار الصناعية وغيرها.

- البعد الاقتصادي: نظراً لاستخدام أجهزة الحاسب في تشغيل الصناعات وتطويرها، حيث ترتبط جميعها ببعضها البعض من خلال شبكات مؤمنة لضمان الأمن السيبراني، وهو أمر يتعلق بشكل خاص بالقطاع المالي.

- البعد الاجتماعي : وفق إحصاءات ٢٠٢٤م يوجد أكثر من ٤ مليار مستخدم للإنترنت حول العالم، حيث يستخدم أكثر من ٢.٦ مليار شخص مواقع شبكات التواصل الاجتماعي والتي تحظى بأعلى معدلات التفاعل البشري، مما يتيح فرصاً واسعة لمشاركة الأفكار والتجارب الناجحة، لكنها في المقابل تكشف أيضاً عن أخلاقيات الأفراد، فصعوبة الرقابة على محتوى الإنترنت ليست مجرد خطر على المجتمعات، بل تعرض أيضاً المعلومات الشخصية لاستخدامات غير مشروعة من جهات خارجية، مما يهدد السلم الاجتماعي في البلدان، نتيجة فقدان الأمن السيبراني الاجتماعي.

---

(1) Nadia Al-Mutairi. (2022). The Impact of Intensive Use of Social Networking in Increasing Cyber Bullying Among Secondary School Female Students in Riyadh in the Kingdom of Saudi Arabia. (https://search.mandumah.com/Record/1243898

(2) El-Tarabishi, M. & Elsayed, M. (2020). The Impact of Cyberbullying on Private High School Teenagers in Cairo Governorate. 30 , 2-31. https://search.mandumah.com/Record/1140511

- البعد السياسي: بعيداً عن تسريبات الوثائق السرية والامتيازات التي غالباً ما تؤدي إلى أزمات دبلوماسية بين الدول، فإن التدخل السيبراني لروسيا في الانتخابات الأمريكية هو أهم دليل على الحاجة إلى الأمن السيبراني وأهميته في البعد السياسي.
- البعد القانوني: يتطلب التطور التكنولوجي السريع الامتثال للتشريعات من خلال تحسين الأطر القانونية للتعامل مع الأنشطة القانونية وغير القانونية على الإنترنت، حيث تعتبر الجرائم الإلكترونية في الغالب جرائم سيبرانية. بعض الدول تفتقر إلى تشريعات صارمة للتعامل مع هذه الظواهر.

الجهود الدولية في مجال الأمن السيبراني:[1]

- نداء باريس للثقة والأمن في الفضاء السيبراني: تم إطلاق نداء باريس في ١٢ نوفمبر ٢٠١٨ خلال منتدى باريس للسلام، ويهدف إلى تعزيز المبادرات المتعلقة بالقضايا الناشئة، التي لم يتم تنظيمها بشكل كافٍ بعد، من خلال العمل مع مجموعة متنوعة من الجهات الفاعلة، بما في ذلك الدول والشركات والجمعيات المهنية ومنظمات المجتمع المدني، يقترح النداء رؤية لتنظيم الفضاء السيبراني والمبادئ الرئيسية المرتبطة به، لا سيما منع فشل الأمن والامتناع عن استخدام بعض الممارسات التي قد تضر باستقرار الفضاء السيبراني.
- المنتدى العالمي لبناء القدرات في الفضاء السيبراني: يعزز المنتدى (GFCE) الذي تأسس سنة ٢٠١٥، التعاون الدولي في بناء القدرات السيبرانية من خلال ربط الاحتياجات والموارد والخبرات، ومن خلال إتاحة المعرفة العملية، ويركز المنتدى حاليًا على ثلاث مجالات تضم تنسيق المشاريع والمبادرات الإقليمية والعالمية لبناء القدرات السيبرانية، تبادل المعرفة والخبرات، وتلبية الاحتياجات الفردية لبناء القدرات السيبرانية.
- الاتفاقيات مع حلف الشمال الأطلسي : اعترف الناتو بالفضاء السيبراني كأحد مجالات العمليات في عام ٢٠١٦ إلى جانب المجالات التقليدية الأخرى كالجو والبر والبحر، يتيح هذا الاعتراف لقادة الناتو العسكريين حماية المهام والعمليات بشكل أفضل من التهديدات السيبرانية، بما في ذلك الاعتماد على القدرات السيبرانية الوطنية للحلفاء، وتكون إجراءات الناتو في الفضاء السيبراني دفاعية ووفقًا للقانون الدولي يتفق الحلفاء على أن الجميع سيستفيدون من فضاء سيبراني يستند إلى القواعد ويكون قابلًا للتنبؤ به، مفتوحًا، حراً وآمنًا.
- الحوار السيبراني الأمريكي الأوروبي : شمل الحوار السيبراني الأمريكي الأوروبي عام ٢٠٢٣ تبادلات حول الدفاع السيبراني، وحدد المزيد من الإجراءات لتعزيز التعاون والتصدي للأنشطة الإلكترونية الخبيثة، تسعى الولايات المتحدة والاتحاد الأوروبي إلى تعاون إقليمي أوسع مع الدول في أمريكا اللاتينية ومنطقة المحيطين الهندي والهادئ وإفريقيا، لتعزيز سلوك الدول المسؤول من خلال العمل الدبلوماسي والمشاركة، ولتعزيز الأمن السيبراني والمرونة لمواجهة هذه التحديات، تبادلت الولايات المتحدة والاتحاد الأوروبي، التحديثات بشأن عدة أولويات رئيسية تم تحديدها في البيان المشترك الصادر في يناير ٢٠٢٣، وشملت هذه الأولويات أمن المنتجات الرقمية

(1) Huang, J., et al. (2021). Cyberbullying in social media and online games among Chinese college students and its associated factors. International Journal of Environmental Research and Public Health, 18(9), 1-12. https://doi.org/10.3390/ijerph18094819

والمعايير السيبرانية ذات الصلة، مرونة البنية التحتية الحيوية وتأثير فرص التقنيات الناشئة، والتعاون بين الوكالات السيبرانية . [1]

- التعاون السيبراني الأمريكي الياباني: عقد الحوار الإلكتروني التاسع بين اليابان والولايات المتحدة في واشنطن العاصمة في ٢٦ يونيو ٢٠٢٤، وبناءً على ضرورة مواصلة الجهود الحكومية الشاملة من قبل كل من "اليابان " و"الولايات المتحدة"، ناقش المشاركون القضايا المتعلقة بالتعاون الياباني الأمريكي في مجال الأمن السيبراني، بما في ذلك السياسات السيبرانية المحلية، والتعاون السيبراني الثنائي في العمليات، والتعاون الدولي والإقليمي وبناء القدرات.

- الاتفاقية السيبرانية الأمريكية الأسترالية: في إطار جهود وزارة الدفاع الأمريكية وتعزيز الشراكات في الفضاء الإلكتروني، أطلقت الولايات المتحدة وأستراليا أول اتفاقية من نوعها لتطوير مجال تدريب افتراضي مشترك على الفضاء الإلكتروني، وقد قعت الدولتان على مشروع القدرات التدريبية السيبرانية في ٣ نوفمبر ٢٠٢٠، وهي اتفاقية دولية ثنائية تمكن قيادة الفضاء الإلكتروني الأمريكية من دمج ملاحظات قوات الدفاع ا لأسترالية، ضمن ما يسمى بـ" بيئة التدريب السيبراني المستمرة ، وهي منصة تدريب على المهام الدفاعية ال واقعية عبر حدود الشبكات ، واستخدامها وتطويرها المشترك سيجعلها تتطور باستمرار ويعزز الجاهزية في الإجراءات السيبرانية.

وظائف الذكاء الاصطناعي في الأمن السيبراني

يشير مصطلح الذكاء الاصطناعي إلى محاكاة الإنسان ذكاء في الآلات المصممة للتفكير والتصرف مثل البشر. وهذا يشمل مجموعة واسعة من التقنيات بما في ذلك الآلات تعلم، التعلم العميق والشبكات العصبية ومعالجة اللغة الطبيعية. تمكن هذه التقنيات الآلات من أداء المهام التي تتطلب عادةً الذكاء البشري، مثل التعرف على الأنماط والتعلم من الخبرة واتخاذ القرارات.

ويمتلك الذكاء الاصطناعي قدرة فائقة على تحليل البيانات الضخمة. يمكنه التعرف على الأنماط والتهديدات الأمنية بسرعة وآلية. هذا يساعد الشركات في اكتشاف المخاطر واتخاذ الإجراءات المناسبة في الوقت المناسب.

ويساهم الذكاء الاصطناعي في تحسين كفاءة العمليات الأمنية. إنه يقلل من الأخطاء البشرية بشكل كبير. الآلات تنفذ المهام بدقة وموثوقية أكبر من البشر.

ويتيح الذكاء الاصطناعي اكتشاف التهديدات الأمنية بسرعة فائقة. كما يمكّن من تنفيذ إجراءات الاستجابة الفورية. هذا يساعد في الحد من الأضرار المحتملة وحماية البيانات الحساسة بشكل فعال.

ويمكن للمؤسسات الاستفادة من أحدث الأدوات القائمة على الذكاء الاصطناعي لاكتشاف التهديدات بشكل أفضل وحماية أنظمتها وموارد بياناتها. لكن يمكن لمجرمي الإنترنت أيضًا استخدام التكنولوجيا لشن هجمات أكثر تعقيدًا.

أهمية الذكاء الاصطناعي في الأمن السيبراني:

تكمن أهمية الذكاء الاصطناعي بالأمن السيبراني، في قدرته على توفير اكتشاف متقدم للتهديدات، وأتمتة الاستجابات، والتكيف مع التهديدات المتطورة، والتعامل مع تحليل البيانات على نطاق واسع.

ومع استمرار تطور التهديدات السيبرانية، أصبح دمج الذكاء الاصطناعي في استراتيجيات الأمن السيبراني، ضروريًا على نحو متزايد لضمان دفاعات قوية وفاعلة.

---

(1) Aljasir, S. & Alsebaei, M. (2022). Cyberbullying and cybervictimization on digital media platforms: The role of demographic variables and parental mediation strategies. Humanities & Social Sciences Communications, 9(1), 1-9. https://doi.org/10.1057/s41599-022-01318-x

ويتيح الذكاء الاصطناعي اكتشافًا أكثر تعقيدًا ودقة للتهديدات، منها يمكن لخوارزميات التعلم الآلي تحليل مجموعات كبيرة من البيانات وتحديد الأنماط والاختلافات والتهديدات المحتملة في الوقت الفعلي. (١)

كما يسمح هذا النهج الاستباقي بالكشف المبكر عن التهديدات الناشئة؛ بما في ذلك الهجمات المعقدة وغير المرئية من قبل، بالإضافة إلى كشف التهديدات والوقاية منها، خاصة وأن أغلب أنظمة الأمن التقليدية تعتمد على التوقعات المحددة مسبقاً فقط، ما يضعها في مرمى التهديدات بشكل غير مسبوق، بينما خوارزميات التعلم الآلي للذكاء الاصطناعي تكشف عن بيانات سريعة للتهديدات السيبرانية الناشئة، مما يوفر دفاعاً استباقياً لهذه الهجمات. كما يتفوق في التحليل السلوكي وتحديد الثغرات التي تشير إلى الخرق الأمني المحتمل، إضافة إلى أتمتة التدابير الأمنية ما يزيد من سرعة الاستجابة لأي هجوم. وفي الوقت ذاته يمكن التعامل مع الذكاء الاصطناعي كعدو محتمل للأمن السيبراني، لاستعانة منفذو الهجمات الإلكترونية بأنظمة ذكاء اصطناعي في تهديد البنية التحتية للمؤسسات، إضافة إلى أن البيانات التي تتناولها خوارزميات الذكاء الاصطناعي قد تكون متحيزة ضد أفراد أو مجموعات وفقاً لعوامل ديموغرافية أو ثقافية، ما يؤدي إلى تحليلات خاطئة من قبل هذه الخوارزميات. كما أن دخول الذكاء الاصطناعي في الأمن السيبراني يهدد دور العنصر البشري في هذا المجال، ويزيد المخاوف من انتهاك خصوصية الأفراد أثناء جمع المعلومات عنهم. (٢)

دور الذكاء الاصطناعي في تعزيز الأمن السيبراني

يلعب الذكاء الاصطناعي دورًا مهمًا في الأمن السيبراني. إنه يساعد الشركات على التعامل مع البيانات الضخمة بكفاءة. كما يمكّنها من كشف التهديدات الأمنية والاستجابة لها بسرعة. (٣)

- التحليلات السلوكية: يتفوق الذكاء الاصطناعي في التحليلات السلوكية، التي تتضمن تحليل أنماط سلوك المستخدم وأنشطة الشبكة، حيث يمكن لأنظمة الذكاء الاصطناعي اكتشاف الانحرافات أو الحالات الشاذة التي قد تشير إلى تهديد أمني. ويساعد ذلك في تحديد التهديدات الداخلية.
- الاستجابة التلقائية للحوادث: يسهل الذكاء الاصطناعي، أتمتة عمليات الاستجابة للحوادث. مع القدرة على التعلم من البيانات التاريخية والتكيف مع المعلومات الجديدة، يمكن لأنظمة الذكاء الاصطناعي الاستجابة للحوادث الأمنية بسرعة وفاعلية، كما يمكن أن تساعد الاستجابات التلقائية في التخفيف من تأثير الهجوم، وتقليل الوقت المستغرق لتحديد الاختراق الأمني واحتوائه ومعالجته.
- التدابير الأمنية التكيفية: يمكّن الذكاء الاصطناعي أنظمة الأمان من التكيف والتطور بناءً على مشهد التهديدات المتغير، ونظرًا لأن التهديدات السيبرانية أصبحت أكثر تعقيدًا، يمكن للذكاء

(1) Chadha, K., et al. (2020). Women's Responses to Online Harassment. International Journal of Communication, 14, 239-257. https://ijoc.org/index.php/ijoc/article/view/11683

(2) Mberia, H. & Kamaku, M. (2018). Social Sites Accessibility and the Rise of Sexual Harassment among Teenagers in Kenya. International Journal of Recent Research in Social Sciences and Humanities, 5(1), 64-72.

(3) Meier, A. & Reinecke, L. (2021). Computer-Mediated Communication, Social Media, and Mental Health: A Conceptual and Empirical Meta-Review. Communication Research, 48(8), 1182-1209. https://journals.sagepub.com/doi/pdf/10.1177/0093650220958224

الاصطناعي أن يتعلم ويحدث خوارزمياته باستمرار للبقاء في صدارة المخاطر الناشئة، وتعتبر هذه القدرة على التكيف أمرًا بالغ الأهمية في ضمان دفاعات قوية للأمن السيبراني.

- تحليل البيانات على نطاق واسع: يولّد الأمن السيبراني، كميات هائلة من البيانات من مصادر مختلفة؛ بما في ذلك السجلات وحركة مرور الشبكة وأنشطة المستخدم، ويمكن للذكاء الاصطناعي التعامل مع هذه البيانات وتحليلها على نطاق واسع، وتحديد الأنماط والاتجاهات التي قد تشير إلى وجود تهديد أمني، وتعد القدرة على معالجة البيانات الضخمة أمرًا ضروريًا للأمن السيبراني الفاعل في بيئات اليوم المترابطة والمعتمدة على البيانات.

- تقليل الإيجابيات الكاذبة: يمكن أن يساعد الذكاء الاصطناعي، في تقليل عدد النتائج الإيجابية الخاطئة في التنبيهات الأمنية، وغالبًا ما تولد أنظمة الأمان التقليدية إنذارات كاذبة، ما يؤدي إلى إرهاق التنبيه، وربما تجاهل التهديدات الحقيقية، وتساعد قدرة الذكاء الاصطناعي، على وضع البيانات في سياقها وفهم أنماط السلوك العادية في التمييز بين التهديدات الحقيقية والإنذارات الكاذبة.

- المراقبة المستمرة والتعلم التكيفي: يتيح الذكاء الاصطناعي المراقبة المستمرة للشبكات والأنظمة، ما يوفر رؤى في الوقت الفعلي حول المخاطر الأمنية المحتملة، بالإضافة إلى ذلك، يمكن لأنظمة الذكاء الاصطناعي التعلم من الأنشطة الجارية، والتكيف مع التغيرات في البيئة، وتحديث فهمها للسلوك الطبيعي بمرور الوقت.

- الكفاءة والسرعة: يمكن للأتمتة أن تعزز كثيرًا سرعة وكفاءة عمليات الأمن السيبراني. يمكن للأنظمة الآلية تحليل كميات هائلة من البيانات بسرعة، واكتشاف التهديدات، والاستجابة للحوادث على نحو أسرع من الطرق اليدوية، وتعتبر هذه السرعة أمرًا بالغ الأهمية في مشهد التهديدات السيبرانية سريع التطور.

- الحد من الخطأ البشري: تساعد الأتمتة على تقليل مخاطر الأخطاء البشرية، وهو عامل شائع في حوادث الأمن السيبراني، ويمكن للأنظمة الآلية أن تتبع باستمرار بروتوكولات الأمان المحددة مسبقًا، ما يقلل من احتمالية الأخطاء التي قد تؤدي إلى ثغرات أمنية.

- المراقبة والاستجابة السريعة: تتيح تدابير استخدام الذكاء الاصطناعي في الأمن السيبراني المراقبة المستمرة للشبكات والأنظمة، ما يوفر دفاعًا استباقيًا ضد التهديدات المحتملة. يصعب الحفاظ على هذه اليقظة المستمرة يدويًا، خصوصًا في بيئات تكنولوجيا المعلومات الكبيرة والمعقدة.

- قابلية التوسع: يمكن للأنظمة الآلية التوسع بسهولة للتعامل مع حجم كبير من البيانات ومهام الأمان المتنوعة، وتعد قابلية التوسع هذه ضرورية للمؤسسات ذات البنى التحتية المعقدة وحجم كبير من حركة مرور الشبكة. [1]

- المهام الروتينية والمتكررة: تعتبر الأتمتة مناسبة تمامًا للتعامل مع المهام الروتينية والمتكررة، ما يسمح لمحترفي الأمن السيبراني من البشر بالتركيز على الجوانب الأمنية الأكثر تعقيدًا واستراتيجية، ويؤدي ذلك إلى تحسين الرضا الوظيفي والاستفادة من الخبرة البشرية؛ حيث تشتد الحاجة إليها.

- توفير حماية استباقية: يمكن للذكاء الاصطناعي والتعلم الآلي، تحليل بيانات الشبكة والأنظمة؛ للتنبؤ بالهجمات الإلكترونية ومنعها قبل وقوعها. وهو ما يُعرف باسم الأمن السيبراني الاستباقي، فعلى سبيل المثال، يمكن لنظام أمان مدعوم بالذكاء الاصطناعي تحديد السلوكيات الضارة للمستخدمين قبل أن يتمكنوا من إلحاق الضرر بالنظام.

---

(1) Others, J. L. (2012). Cyber Security Policy guidebook (01 ed.). New Jersey, united states of america: Published by John Wiley & Sons, Inc.

- تحسين التحقيقات في مجال الأمن السيبراني: يمكن استخدام الذكاء الاصطناعي والتعلم الآلي، لتحليل البيانات من أجل جمع الأدلة والتعرف على الجناة في جرائم الإنترنت، وهذا يساعد في تسريع التحقيقات وزيادة فرص الإدانة، وعلى سبيل المثال، يمكن استخدام التعلم الآلي لتحديد أنماط الاتصالات التي تشير إلى النشاط الإجرامي عبر الإنترنت.

تحديات تطبيقات الذكاء الاصطناعي في الأمن السيبراني:

على الرغم من فوائد الذكاء الاصطناعي في مجال الأمن السيبراني له أيضًا بعض التحديات أهمها: (١)

- البيانات المتحيزة: يمكن أن تكون خوارزميات الذكاء الاصطناعي والتعلم الآلي، متحيزة إذا تم تدريبها على بيانات غير دقيقة أو غير كاملة.
- التهديدات الداخلية: أحيانًا يتم استخدام تقنيات الذكاء الاصطناعي والتعلم الآلي من قبل المحتالين لشن هجمات أكثر تعقيدًا.
- المخاوف الأخلاقية: تثير بعض تقنيات الذكاء الاصطناعي، مثل التعرف على الوجه، مخاوف أخلاقية بشأن الخصوصية، وعمومًا الذكاء الاصطناعي والتعلم الآلي، أدوات قوية يمكن استخدامها لتحسين الأمن السيبراني كثيرًا.

طرق تطبيق أنظمة الذكاء الاصطناعي في الأمن السيبراني: (٢)

- حماية حسابات المستخدمين من خلال تأمين كلمات المرور باستخدام تقنيات مثل: التعرف على الوجه واختبار Captcha والماسحات الضوئية لبصمات الأصابع.
- كشف ومنع هجمات التصيد من خلال استخدام حلول الذكاء الاصطناعي لتحليل محتوى البريد الإلكتروني، والكشف عن العلامات الشائعة للتصيد الاحتيالي.
- استخدام تقنيات التعلم الآلي، لتحسين أمان الشبكات وتحديد الحوادث الأمنية المحتملة.
- إدارة نقاط الضعف والحماية من الهجمات الإلكترونية، باستخدام تحليل الأنشطة في الوقت الفعلي.
- تحليل السلوكيات للكشف عن التهديدات السيبرانية المتطورة وتحديد نقاط الضعف المحتملة.
- اكتشاف ومعالجة التهديدات السيبرانية الداخلية من خلال تحليل سلوك المستخدم.
- تطبيق الذكاء الاصطناعي لأمن نقاط النهاية لتحديد السلوك غير الطبيعي واكتشاف التهديدات المعروفة.

أهداف الذكاء الاصطناعي في الأمن السيبراني:

يساعد الذكاء الاصطناعي في الأمن السيبراني، متخصصي الأمن من خلال فهم أنماط البيانات المعقدة، وتقديم النصائح المفيدة، والسماح بحل المشكلات تلقائيًا، فهو يسهل اكتشاف المخاطر

(1) Ferris, A., et al. (2021). Applying the uses and gratifications model to examine consequences of social media addiction. Social media + Society, 7(2), 1-16. https://doi.org/10.1177/20563051211019003

(2) Mieczkowski, H., et al. (2020). Priming effects of social media use scales on well-being outcomes: The influence of intensity and addiction scales on self-reported depression. Social media + Society, 6(4), 1-15. https://doi.org/10.1177/2056305120961784

المحتملة، ويساعد في اتخاذ القرارات، ويسرع الاستجابة للحوادث، ويمكن لدور الذكاء الاصطناعي أن يعزز معلومات التهديد التي تم جمعها لمنع الجرائم السيبرانية. (١)

- التعامل مع البيانات الضخمة: حيث يتم تنفيذ العديد من الأنشطة على المنصات المختلفة، مما يعني نقل كميات كبيرة من البيانات بين المستخدمين، وتُظهر هذه العمليات التحديات التي يواجهها محللو الأمن السيبراني في التحقق من كل شيء وتقييم مخاطر محتملة، ويعد الذكاء الاصطناعي الخيار المثلى لاكتشاف هذه التهديدات التي تنشأ خلال الأنشطة اليومية، بفضل قدرته على مراقبة حركة المرور وتحليل نشاط الخادم بدقة وتحديد المخاطر المحتملة بشكل تلقائي.

- توقع التهديدات المستقبلية: تعتبر كمية البيانات التي يتعامل معها محللو الأمن السيبراني تحديًا في التنبؤ بالتهديدات المستقبلية، إلا أن الذكاء الاصطناعي يستطيع معالجة حجم كبير من البيانات في وقت واحد، مما يمكّن من الكشف المبكر عن الأنشطة الضارة. بفضل تحديد الإجراءات الوقائية والتهديدات المحتملة، يمكن تقليل الوقت المهدور والموارد البشرية، ويساعد في البقاء يقظًا من خلال اتخاذ خطوات لحماية المؤسسة.

- تقليل وقت اكتشاف التهديد: يمكن للذكاء الاصطناعي فحص كميات هائلة من البيانات في وقت واحد للكشف عن التهديدات السيبرانية، مما يعزز الأمن بشكل كبير. وبحسب استطلاع، أفاد ٥٦% من المؤسسات بأنها تعاني من ضغط شديد بسبب تحليل تهديدات يشغل المحللين السيبرانيين، وأبلغ ٢٣% منهم أنهم غير قادرين على التحقق من التهديدات بشكل فعال.

- التقليل في التكاليف: يعاني العديد من المؤسسات من تأثيرات مالية جسيمة نتيجة انتهاكات البيانات كل عام، وهذا أمر لا يمكن تجاهله أو التوقف عن مواجهة المجرمين. وفقًا للدراسات، توضح الفروقات الكبيرة في توفير التكاليف بنسبة ٨٠% للمؤسسات التي تعتمد على تقنيات الذكاء الاصطناعي في أمنها السيبراني، حيث يتم تقديم خدمات بتكلفة ٢.٩ مليون دولار مقابل ٦.٧١ مليون دولار لمن لا يستخدمون هذه التقنيات. (٢)

تحديات تطبيق الذكاء الاصطناعي في الأمن السيبراني

يبدأ عمل الذكاء الاصطناعي في مجال الأمن السيبراني؛ عندما تتوفر يتوفر نظام لجمع البيانات الرقمية حول جميع تعاملات الأفراد داخل المؤسسة. ويجب أن تكون تلك الأنظمة ضد الاختراق، وقد لوحظ مؤخراً؛ أن الشركات الكبرى وحتى الصغيرة والمتوسطة تنتج كميات هائلة من السجلات والبيانات، ولكن من لديه القدرة لمراجعة كل هذه السجلات؟

يقول بندر السلمي، إن أهمية الذكاء الاصطناعي، برزت من قدرته على مراجعة كم هائل من السجلات، والتأكد من سلامتها، في دقائق قليلة. وأضاف أنه على سبيل المثال في فرنسا تضاعفت الهجمات لأنظمة الحاسب ٣ أضعاف منذ جائحة كورونا، مشيراً إلى أن ذلك يؤكد أن الاستفادة من جميع سجلات الوصول والمصادر من الأفراد أو الكيانات، أمر مهم وحاسم في عملية تحقيق منظومة الأمن السيبراني.

مجالات الذكاء الاصطناعي في الأمن السيبراني: (٣)

١. كشف التهديدات الجديدة.

---

(1) Dutot, V. (2020). A social identity perspective of social media's impact on satisfaction with life. Psychology & Marketing, 37(6), 759-772. https://doi.org/10.1002/mar.21333

(2) Walker, b. (2019). Cyber Security: Comprehensive Beginners Guide to Learn the Basics and Effective Methods of Cyber Security. Australia: Independently Published

(3) Adam, H. (2021). The Excessive Use of social media and its Relationship to Insomnia Among Female Students in Hail University.

٢. محاربة ومنع روبوتات الإنترنت.
٣. حماية فعالة للأجهزة الطرفية المتصلة.
٤. كشف التسلل والوقاية منه.
٥. الحماية من البرامج الضارة.
٦. الكشف عن الغش.
٧. مراقبة وإدارة الهوية والوصول.
٨. منع البريد الضار.

استراتيجيات تفعيل الذكاء الاصطناعي

أشار بندر السلمي إلى أنه خلال رسالة الدكتوراة خاصته؛ قد ناقش سلوك الفيروسات، وكيف يقوم الذكاء الاصطناعي بتحليل هذا السلوك، وبناء أنظمة خاصة بشكل أتوماتيكي لتحجيم نشاط الفيروسات، والقضاء عليها. وقد لخص «السلمي» خطوات تفعيل الذكاء الاصطناعي في مجال الأمن السيبراني لدى المؤسسات في عدة خطوات، كالتالي: [١]

١. إنشاء منصة بيانات متكاملة.
٢. تحديد الحالات عالية التأثير والأهمية.
٣. بناء منظومة الأمان والأتمتة والاستجابة.
٤. تفعيل دور الخبراء والمحللين السيبرانيين.
٥. إنشاء منظومة لإدارة البيانات وأنظمة الذكاء الاصطناعي.

ما الذي يهدد الذكاء الاصطناعي؟

بيتم استخراج بيانات قيمة من الذكاء الاصطناعي، ومهما بلغ ذكاء الخوارزميات، فهناك حدود لها، حيث تستهدف الهجمات السيبرانية حديثا، اختراق خوارزميات الذكاء الاصطناعي. ويؤكد بندر السلمي إلى أن زيادة دقة البيانات مع دعم الخصوصية، يساعد على بناء أنظمة لها خصوصية عالية، حيث يتم حماية البيانات وتحصينها، دون انتهاك خصوصية المستخدمين أو الموظفين.

وأضاف بندر السلمي، أن مع ظروف جائحة كورونا، صار من الضروري والملّح أن تكون لدينا أنظمة ذكاء اصطناعي قوية في دعم الأمن السيبراني، خاصة مع انتشار ثقافة العمل عن بعد، وزيادة حجم إنتاج الملفات الرقمية عبر الإنترنت. وأشار «السلمي» إلى أن في كندا وأمريكا على سبيل المثال، قد زادت ميزانية كل دولة بثلاثة أضعاف تقريبا، لدعم تطبيقات الذكاء الاصطناعي في الأمن السيبراني.

تحديات تفعيل الذكاء الاصطناعي في المؤسسات: [٢]

١. نمذجة الشبكات واسعة النطاق.
٢. تطور وتقدم الهجمات السيبرانية.
٣. جودة وموثوقية البيانات.

(1) Peng Wang, Mei Su, Jingyi Wang. (2021). Organized crime in cyberspace: How traditional organized criminal groups exploit the online peer-to-peer lending market in China. The British Journal of Criminology. Volume 61. Issue 2. Pp. 303–324.

(2) Park, A. F. (2022): Mapping the public voice of development natural langue processing of social
media text data, Asian development bank, p.125.

٤. الحفاظ على الخصوصية.
٥. اكتشاف التهديدات النادرة.
٦. تقليل معدل الخطأ لأنظمة الذكاء الاصطناعي.
٧. تقليل تهديدات نماذج الذكاء الاصطناعي.

التطبيقات الحالية للذكاء الاصطناعي في الأمن القومي: [١]

لقد أصبحت التكنولوجيا الرقمية جزءًا لا يتجزأ من جوانب مختلفة من الأمن الوطني، حيث توفر قدرات تحويلية في مجالات المراقبة والأمن السيبراني والأنظمة المستقلة والخدمات اللوجستية ومن التطبيقات التالي.

- التعرف على الوجه: تُستخدم أنظمة التعرف على الوجه المدعومة بالذكاء الاصطناعي على الحدود والمطارات والأماكن العامة لتحديد التهديدات المحتملة وتعزيز الأمن. يمكن لهذه الأنظمة معالجة وتحليل كميات هائلة من البيانات في الوقت الفعلي، مما يحسن أوقات الاستجابة.
- التعرف على الأنماط: تستطيع خوارزميات الذكاء الاصطناعي اكتشاف الأنماط أو السلوكيات غير المعتادة التي قد تشير إلى وجود تهديد أمني. وهذا مفيد بشكل خاص في مراقبة الحشود الكبيرة أو البنية التحتية الحيوية. [٢]
- التحليل الجيو مكاني: يقوم الذكاء الاصطناعي بتحليل صور الأقمار الصناعية لتحديد التغييرات أو الشذوذ التي قد تشير إلى مخاطر أمنية. يمكن أن يشمل هذا اكتشاف الإنشاءات غير المصرح بها أو تحركات القوات أو التغيرات البيئية.
- كشف التهديدات: تراقب أنظمة الذكاء الاصطناعي حركة الشبكة وتحدد الشذوذ الذي قد يشير إلى هجمات إلكترونية. وتتعلم خوارزميات التعلم الآلي من الحوادث السابقة لتحسين دقة الكشف.
- الاستجابة للتهديدات: تساعد الذكاء الاصطناعي في أتمتة الاستجابة للتهديدات السيبرانية، مما يقلل الوقت المستغرق للتخفيف من حدة الهجمات والحد من الأضرار. ويشمل ذلك عزل الأنظمة المتضررة وبدء التدابير المضادة.
- التحليل التنبئي: يمكن للذكاء الاصطناعي التنبؤ بالتهديدات السيبرانية المحتملة من خلال تحليل الأنماط والاتجاهات، مما يسمح باتخاذ تدابير استباقية.
- تحليل البيانات في الوقت الفعلي: يمكن للذكاء الاصطناعي معالجة كميات هائلة من البيانات في الوقت الفعلي، وتحديد الاتجاهات والأنماط التي قد لا تكون واضحة على الفور للمحللين البشريين.
- التحليلات التنبؤية: تستطيع خوارزميات الذكاء الاصطناعي التنبؤ بالتهديدات والسيناريوهات المحتملة استنادًا إلى البيانات التاريخية، مما يتيح اتخاذ إجراءات وقائية. على سبيل المثال، يمكن للذكاء الاصطناعي التنبؤ بحركات العدو أو تحديد احتمالات وقوع هجمات إلكترونية. [٣]
- أنظمة دعم القرار: تساعد الأنظمة المدعومة بالذكاء الاصطناعي القادة على وضع الاستراتيجيات والتخطيط من خلال محاكاة السيناريوهات والنتائج المختلفة.

---

(1) siau,k.& wang, w. Artificial intelligence ethics: ethics of AI and ethical AL. Journal of Database
Management (JDM) &1(2). 2020.
(2) States, u. d. (2023). joint Statement on the United States-European Union 9th Cyber Dialogue in Brussels. Brussels: Office of the Spokesperson. Retrieved from: https://n9.cl/ppy73
(3) Cywreck, B. (2024, 03 04). Top 10 Cybersecurity Powerhouses: Ranking the Global Defenders in 2024. Retrieved 08 28, 2024, from https://n9.cl/7posi

- المراقبة المتقدمة: يمكن لأنظمة المراقبة المعتمدة على الذكاء الاصطناعي مراقبة وتحليل البيانات من مصادر متعددة، مثل صور الأقمار الصناعية، وموجزات الفيديو، ووسائل التواصل الاجتماعي، للكشف عن الشذوذ والتهديدات المحتملة.
- الأمن الإلكتروني: تعمل الذكاء الاصطناعي على تحسين تدابير الأمن السيبراني من خلال تحديد التهديدات وتحييدها بسرعة. يمكن لنماذج التعلم الآلي اكتشاف الأنشطة غير المعتادة في حركة المرور على الشبكة، مما يقلل من الوقت اللازم للاستجابة للهجمات السيبرانية.
- الردود الآلية: يتيح الذكاء الاصطناعي آليات الاستجابة الآلية، مما يسمح باتخاذ إجراءات فورية للتخفيف من حدة التهديدات دون تدخل بشري.
- مشاركة البيانات وتحليلها: تسهل الذكاء الاصطناعي معالجة وتحليل كميات هائلة من البيانات الاستخباراتية المشتركة بين البلدان الأعضاء، مما يحسن سرعة ودقة اكتشاف التهديدات.
- العمليات المشتركة: تدعم تقنيات الذكاء الاصطناعي العمليات الأمنية المشتركة، مما يتيح استجابات منسقة للتهديدات العالمية، مثل الإرهاب والهجمات الإلكترونية.

مجالات تطبيقات الذكاء الاصطناعي:[1]

- الطائرات بدون طيار والطائرات بدون طيار: تستطيع المركبات الجوية غير المأهولة المزودة بالذكاء الاصطناعي القيام بمهام الاستطلاع وتوصيل الإمدادات ومهاجمة الأهداف بأقل قدر من التدخل البشري. وتُستخدم في أدوار قتالية وغير قتالية مختلفة.
- الروبوتات: يمكن نشر الروبوتات التي تعمل بالذكاء الاصطناعي في مهام مثل التخلص من القنابل ومهام البحث والإنقاذ والمراقبة. تعمل هذه الروبوتات على تقليل المخاطر التي يتعرض لها الأفراد من البشر. ويهدف مشروع Maven، الذي أطلقته وكالة مشاريع الأبحاث الدفاعية المتقدمة (DARPA) التابعة لوزارة الدفاع الأمريكية، إلى دمج الذكاء الاصطناعي في الاستخبارات العسكرية لتحليل كميات هائلة من لقطات الفيديو.
- الصيانة الوقائية: تتنبأ الذكاء الاصطناعي بفشل المعدات قبل حدوثه، مما يسمح بالصيانة في الوقت المناسب وتقليل وقت التوقف عن العمل. وهذا يضمن أن الأصول الحيوية تعمل دائمًا.
- تحسين سلسلة التوريد: تعمل خوارزميات الذكاء الاصطناعي على تحسين طرق الإمداد وإدارة المخزون، مما يضمن حصول القوات العسكرية على الإمدادات اللازمة عندما وأينما تحتاج إليها.

تحديات ومخاطر الذكاء الاصطناعي في الأمن القومي

ورغم أن الذكاء الاصطناعي يقدم فوائد عديدة في مجال الأمن الوطني، فإنه يطرح أيضا تحديات ومخاطر كبيرة. وتشمل هذه التحديات المخاوف الأخلاقية والقانونية، وإساءة استخدام الذكاء الاصطناعي في الأسلحة ذاتية التشغيل، والثغرات في الأمن السيبراني. وفهم هذه التحديات أمر بالغ الأهمية لتطوير استراتيجيات قوية للتخفيف من المخاطر وضمان الاستخدام المسؤول للذكاء الاصطناعي. [2]

(1) Peng Wang, Paul Joosse, Lok Lee Cho. (2020). The Evolution of Protest Policing in a Hybrid Regime. The British Journal of Criminology. Volume 60. Issue 6. Pp. 1523–1546.

(2) Pete Fussey, Bethan Davies& Martin Innes. (2021). 'Assisted' facial recognition and the reinvention of suspicion and discretion in digital policing. The British Journal of Criminology. Volume 61. Issue 2. pp. 325

- صنع القرار المستقل: تثير أنظمة الذكاء الاصطناعي التي تتخذ قرارات مستقلة، وخاصة في سيناريوهات القتال، مخاوف أخلاقية بشأن المساءلة ومن المسؤول عن اتخاذ نظام الذكاء الاصطناعي قرارًا خاطئًا يؤدي إلى فقدان الأرواح أو الدمار غير المقصود؟
- التحيز والإنصاف: يمكن لخوارزميات الذكاء الاصطناعي أن تعمل على إدامة التحيزات الموجودة في البيانات التي يتم تدريبها عليها، بل وحتى تضخيمها. وقد يؤدي هذا إلى استهداف أو تحديد هويات غير عادلة، مما يثير قضايا أخلاقية خطيرة.
- سياسة اهتمامات: يمكن لتقنيات مراقبة الذكاء الاصطناعي أن تنتهك حقوق الخصوصية الفردية، مما يؤدي إلى حالة مراقبة حيث يتم مراقبة المواطنين باستمرار.
- غياب الرقابة البشرية: يمكن للأسلحة المستقلة أن تعمل دون تدخل بشري، مما قد يؤدي إلى سيناريوهات غير متوقعة وغير قابلة للسيطرة.
- تصعيد الصراع: إن نشر أنظمة الأسلحة الهجومية المتقدمة قد يخفض من عتبة المشاركة في الصراع، حيث تعمل هذه الأنظمة على تقليل المخاطر التي يتعرض لها الجنود البشر، مما قد يؤدي إلى المزيد من الأعمال العسكرية المتكررة والعدوانية.
- مخاطر الانتشار: هناك خطر يتمثل في إمكانية انتشار الأسلحة المستقلة إلى جهات غير حكومية أو دول مارقة، مما يؤدي إلى زيادة عدم الاستقرار العالمي.
- الهجمات العدائية: تتضمن الهجمات المعادية التلاعب بأنظمة الذكاء الاصطناعي من خلال تزويدها ببيانات مضللة، مما يدفعها إلى اتخاذ قرارات غير صحيحة. وهذا أمر مثير للقلق بشكل خاص في مجال الأمن السيبراني والأنظمة المستقلة.
- أمن البيانات: تتطلب أنظمة الذكاء الاصطناعي كميات هائلة من البيانات، والتي يجب حمايتها. وقد يؤدي المساس بهذه البيانات إلى تدريب أنظمة الذكاء الاصطناعي على معلومات خاطئة أو متحيزة، مما يقوض فعاليتها.

المبحث الثالث: محاور دراسات وبحوث جرائم الذكاء الاصطناعي والأمن السيبراني

الاتجاه البحثي الأول: الدراسات البحوث التي تناولت الأمن السيبراني:

دراسة أسماء جابر (٢٠٢٤) [١] والتي هدفت إلى تقديم تحليل المخاطر الاجتماعية للجرائم والهجمات والهجمات السيبرانية على الأمن الرقمي ورصد آليات وجهود الدولة المصرية في ضوء رؤية مصر ٢٠٣٠، وتوصلت الدراسة الى عدد من النتائج أهمها : أن الأمن الرقمي يعد ضرورة ملحة فرضها التطور التكنولوجي ومنظومة التحول الرقمي لضمان سلامة وأمن المعلومات وتكنولوجيا الاتصالات، كما بينت النتائج أن معظم دول العالم تعرضت للعديد من الجرائم والهجمات السيبرانية التي استهدفت القطاعات الحيوية في المجتمع، ومن ثم قامت بإصدار القوانين المختلفة من أجل التغلب على التهديدات والأخطار الناجمة عنها.

دراسة نجوان عاصم (٢٠٢٣) [٢]، والتي هدفت إلى التعرف على الأبعاد الاجتماعية والاقتصادية للجريمة السيبرانية، وتحليل التحديات والتهديدات التي تواجه الأمن القومي المصري نتيجة الجريمة

---

(١) أسماء على جابر، (٢٠٢٤) الانعكاسات والمخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمي وآليات المواجهة في ضوء رؤية مصر ٢٠٣٠، الاكاديمية العسكرية للدراسات العليا والإستراتيجية مج ٢، ع٤ ، ص١٠٣.

(٢) نجوان أحمد عاصم عبد الجواد، (٢٠٢٣)، الجريمة السيبرانية وتأثيرها على الأمن القومي المصري: دراسة سوسيو تحليلية، جامعة الفيوم - كلية الآداب مجلة كلية الآداب، مج ١٥، ع١، ص ٢١٤٩

السيبرانية، واستخدمت الدراسة منهج المسح وأداة الاستبيان بالتطبيق على عينة قوامها ٥٠٠ مفردة من طلاب جامعة الفيوم ، وتوصلت الدراسة الى عدد من النتائج أهمها : أن الجريمة السيبرانية تزداد بشكل مباشر عن طريق الإيميلات الإلكترونية وذلك بإرسال بعض الإيميلات الوهمية التي تحمل الفيروسات التي تساعد على الاختراق، لسرقة المعلومات والأموال وتعطيل الأنظمة الحيوية، وأنه يوجد العديد من الطرق لتجنب الاختراق أبرزها هو استخدام كلمات مرور قوية لكل حساب، كما توصلت النتائج الى أن الأبعاد الاجتماعية والاقتصادية للجريمة السيبرانية هي الفقر والأمية الرقمية والبطالة والتهميش الاجتماعي والسياسي للفرد والفضول الزائد الذي يعاني منه، فيلجأ الفرد إلى إثبات ذاته عن طريق انتهاك خصوصية الغير.

دراسة شيماء صالح (٢٠٢٣) [١] والتي سعت نحو التعرف على الأبعاد المختلفة للتهديدات السيبرانية وكيف يمكن أن تؤثر على الأمن الوطني من خلال الهجمات السيبرانية التي تنفذها التنظيمات الإرهابية. كما توضح كيف تستغل هذه التنظيمات التطور في وسائل الاتصال والمعلومات لتحقيق أهدافها، وما هي الجهود الدولية المبذولة للتصدي لهذه التهديدات، واعتمدت الدراسة على المنهج الوصفي واداة تحليل المضمون، وتوصلت الدراسة الى عدد من النتائج أهمها : أن التهديدات السيبرانية ضد العراق في تزايد مستمر، وهى عادة تستهدف البنية التحتية الحيوية للدولة بما في ذلك المؤسسات الحكومية والمالية، وأن التنظيمات الإرهابية تستخدم التكنولوجيا الحديثة ووسائل الاتصال المتطورة لتنفيذ هجماتها السيبرانية، مما يزيد من تعقيد المواجهة معها.

دراسة شيرين عبد الحفيظ (٢٠٢٣) [٢] والتي هدفت إلى التعرف على دور الإعلام الرقمي في تعزيز الأمن السيبراني، ودوره في التهديدات والجرائم الالكترونية، واعتمدت الدراسة على منهج المسح واداة الاستبيان بالتطبيق على عينة قوامها (٦٤) مفردة من الإعلاميين، وتوصلت الدراسة الى عدد من النتائج أهمها: أن الإعلام الرقمي له دور كبير في تعزيز الأمن السيبراني بدرجة مرتفعة، وأن الإعلام الرقمي يلعب دور كبير في مقاومة التهديدات والجرائم السيبرانية بدرجة مرتفعة.

دراسة (اية فرج ٢٠٢٢ ([٣] والتي سعت نحو التعرف على دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي بالجامعات السعودية، وقد استخدمت الباحثة المنهج الوصفي واداة الاستبيان بالتطبيق على٣٥٢ مفردة من أعضا هيئة التدريس بجامعة الأمير سطام بن عبد العزيز، وتوصلت نتائج الدراسة الى أن دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي من وجهة نظر عينة الدراسة كانت بدرجة متوسطة بالنسبة للاستبيان ؛ بينما حصل محور الدواعي المجتمعية لتعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي للجامعة على متوسط (٣.٧٢)،كما توصلت النتائج لعدم وجود فروق ذات دلالة إحصائية لمتغير الكلية والرتبة العلمية، بينما كانت هناك فروق تعزى لمتغير سنوات الخبرة .

(١) شيماء تركان صالح، (٢٠٢٣). الأمن الوطني العراقي والتهديدات السيبرانية... الإرهاب السيبراني نموذجا. كلية العلوم السياسية، جامعة النهرين.

(٢)شيرين عبد الحفيظ، (٢٠٢٣). دور الإعلام الرقمي في تعزيز الأمن السيبراني ومكافحة التهديدات والجرائم السيبرانية. المجلة العلمية لبحوث العلاقات العامة والإعلان، جامعة القاهرة ـ كلية الإعلام، عدد ٢٥، ص٢٠١.

(٣) اية عمر فرج. (٢٠٢٢)، دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي – جامعة الأمير سطام بن عبد العزيز نموذجا، مجلة جامعة سوهاج الدولية التربوية

دراسة أماني حمدي قرني (٢٠٢٢) [١]والتي هدفت الى التعرف على دور مواقع الإعلام الرقمي في حماية الأمن السيبراني، وتكونت العينة من صفحات ومواقع الإعلام الرقمي التي تناولت القضايا المتعلقة بالأمن والجرائم السيبرانية، واعتمدت الدراسة على المنهج الوصفي التحليلي، وأظهرت النتائج أن قضيتي اختراق الحسابات والاستخدامات الإيجابية جاءت في الترتيب الأول، وجاء موضوع جرائم إلكترونية دولية في الترتيب الثاني.

دراسة عادل عبد الصادق ،(٢٠٢٢([٢]التي تناولت الإرهاب السيبراني والأمن القومي في بيئة متغيرة ومدى ارتباط الظاهرة بالتطور التقني من جهة وتحول المصالح الاستراتيجية إلى الفضاء السيبراني ، وأثر انعكاس الفضاء الإلكتروني بتغير طبيعة وخصائص الأمن والقوة والصراع الدولي ، كما أبرزت الدراسة العلاقة التاريخية بين التكنولوجيا والإرهاب وارتباط الرقمنة والإرهاب، وقد توصلت الدراسة الى أن التطوير في التطبيقات الرقمية يؤدى الى هجرة المواقع الإلكترونية والمنتديات وغرف الدردشة والمدونات والتركيز على تطبيقات الشبكات الاجتماعية والهواتف الذكية. كما أظهرت نتائج الدراسة الممارسات الإلكترونية الإرهابية ذات الطابع الرقمي عبر الفضاء الإلكتروني.

كما سعت دراسة موسى بن تغري، (٢٠٢٠(([٣]نحو إيجاد الحلول نحو تطوير قواعد وتشريعات القانون الدولي الإنساني لكي تتم مواءمتها مع النزاعات والحرب السيبرانية، وقد توصلت الدراسة إلى نتيجة في غاية الأهمية وهي أن الحرب السيبرانية تمثل حرب حقيقية وليست خيالية ويمكن تطبيق قواعد القانون الدولي الإنساني عليها، كما أظهرت الدراسة من خلال نتائجها أن الهجمات السيبرانية تشكل نزاعات مسلحة حقيقية في ثوبها الجديد والغير المألوف وتكون قابلة لتطبيق القانون الدولي الإنساني عليها.

وهدفت دراسة (أسماء أبو زيد، ٢٠٢١ [٤]الى التعرف على إطار استراتيجيات خطاب صحافة التكنولوجيا العربية تجاه الأمن السيبراني في مصر والسعودية من خلال القيام بعمل الرصد والتحليل بموقع صحيفتي (اليوم السابع المصرية وعكاظ السعودية)، وقد اعتمدت الدراسة على المنهج الوصفي الى جنب مع منهجي التحليلي المقارن والمنهج المسحي وكان من أبرز نتائج الدراسة تأكيدها على ضرورة الاحتياج للأمن السيبراني فهو ضرورة دفاعية في غاية الأهمية

وسعت دراسة (منال حسن، ٢٠٢١ [٥] نحو الكشف عن الفاعلية لبرنامج تدريبي مقترح لتنمية الوعي بجوانب الأمن السيبراني في التعليم عن بعد لدى معلمات العلوم بالمرحلة الابتدائية بالمملكة العربية السعودية، وقد استخدمت الدراسة المنهج التجريبي. وتمثلت أداة الدراسة في مقياس تم تصميمه من قبل الباحثة لمعرفة الوعي بجوانب الأمن السيبراني في التعليم عن بعد، بالتطبيق على عينة قوامها (٣٢) معلمة من مجتمع الدراسة الممثل في المعلمات لمادة العلوم لدى المرحلة الابتدائية، وتوصلت نتائج الدراسة الى وجود فرق ذي دلالة إحصائية عند مستوى (٠.٠٥) بين متوسطي درجات

---

(١) أماني حمدي. (٢٠٢٢). دور مواقع الإعلام الرقمي في حماية الأمن السيبراني: دراسة تحليلية لعينة من المواقع الخاصة بالأمن السيبراني. جامعة القاهرة ـ كلية الإعلام، المجلة المصرية لبحوث الإعلام، ع٨٠ ص ١٠٦.

(٢) عادل عبد الصادق. (٢٠٢٢)، الإرهاب السيبراني والأمن القومي في بيئة متغيرة، مؤسسة الأهرام، مجلة السياسة الدولية، مج)٠٤(، ع)٢٢٤(، ص ص .٢٧٤-٢٧٧ ـ

(٣) موسى بن تغري. (٢٠٢٠)، الحرب السيبرانية والقانون الدولي الإنساني، مجلة الاجتهاد القضائي، مجلد ١٢ص ٤٥

(٤) أسماء أحمد أبو زيد، (٢٠٢١)، استراتيجيات خطاب صحافة التكنولوجيا العربية تجاه الأمن السيبراني، المجلة المصرية لبحوث الرأي العام، مج (٢٠)، ع (٢(.

(٥) منال حسن محمد إبراهيم. (٢٠٢١)، الوعي بجوانب الأمن السيبراني في التعليم عن بعد، المجلة العلمية لجامعة الملك فيصل ـ العلوم الإنسانية والإدارية، مج (٢٢)، ع (٢)، ص .٣٠٠

المعلمات في التطبيقين القبلي والبعدي لمقياس الوعي لصالح التطبيق البعدي مما يؤكد على فاعلية البرنامج التدريبي المقترح

كما هدفت) [١] (Ameen et al.2021الى معرفة مدى امتثال الموظفين للأمن السيبراني وسياساته، وقد طبقت الدراسة على عينة من مجتمع الموظفين متعددة الثقافات والجنسيات مثل الولايات المتحدة والمملكة المتحدة، والإمارات العربية المتحدة، واستخدمت الدراسة منهج المسح واداة الاستبيان بالتطبيق على عينة قوامها ٣٧٣٢ مفردة، وقد توصلت الدراسة من خلال نتائجها على ضرورة الاستخدامات الآمنة للهواتف الذكية لدى الموظفين في العمل مع مراعاة الاختلافات الثقافية والمعرفية بين الجنسيات المختلفة وكذلك التحذير من التهديدات والجرائم السيبرانية عبر الهواتف الذكية.

كما سعت دراسة Moskal،[٢] (2020) نحو الكشف أهمية تعزيز ثقافة الأمن السيبراني في الجامعات الأمريكية وقد اعتمدت الدراسة على منهج المسح واداة الاستبيان بالتطبيق على عينة من الجامعات الأمريكية بلغ قوامها (٣٢٢) جامعة أمريكية لمعرفة درجة الاهتمام بتدريس الأمن السيبراني، وقد أوضحت الدراسة تصور تطبيقي لإنشاء مركز متخصص للعمل على التدريب وزيادة الوعي التثقيفي للأمن السيبراني والمخاطر السيبرانية لدى طالب بالجامعات الأمريكية.

وهدفت دراسة مالك بن فهد الغبيوي، (٢٠٢٠ [٣]الى التعرف على الأمن السيبراني ودوره في الحد من تهديدات الأمن الفكري، واعتمدت الدراسة على منهج المسح واداة استبيان، وتوصلت الدراسة من خلال نتائجها الى اتفاق عينة الدراسة على خطورة التهديدات والجرائم الفكرية للأمن السيبراني والاتجاه نحو توظيف الأدوات التكنولوجية الحديثة لتعزيز دور الأمن السيبراني بالمملكة العربية السعودية.

وكشفت دراسة [٤] (2020) Jemin Justin Lee et al عن وسائل منع الجريمة قبل وقوعها من خلال استخدام تصميم نظام (CPTED) وتم تطبيقه على عينة بلغ قوامها ١٠٠مفردة من طلاب الدراسات العليا، وتم استخدام تحليل عامل مخاطر المعلومات الكمية (FAIR)، وقد توصلت الدراسة من خلال النتائج ان علم المورفولوجيا في البيئة الافتراضية له تأثير مباشر في انتشار الجريمة، كما أكدت نتائج الدراسة أن جميع اللاعبين يصبحوا في لعبة بابجي رهن لقواعد اللعبة ارتكاب أعمال عنف وذلك طبقا حتى يتثنى لهم استكمال مراحل اللعبة

(1) Ameen، A.، Tarhini، B.، Shah، M.، Madichie، D.، Paul، J. and Choudrie، J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. Computers in Human Behavior، 114(n/a)، doi.org/10.1016/j.chb.2020.106531

(2) Moskal. E (2020) ، A Model of Establishing Cyber Security Center of Excellence. Information Systems Education Journal، Vol. (13) ، No. (6) ، PP 97- 102

(٣) مالك بن فهد الغبيوي، (٢٠٢٠) الأمن السيبراني ودوره في الحد من تهديدات الأمن الفكري، رسالة ماجستير، قسم الدراسات الاستراتيجية، جامعة نايف العربية للعلوم الأمنية

(4) Jemin Justin Lee ، Myong-Hyun Go ، Yu-Kyung Kim ، Minhee Joo.)2020(، A Multi-Component Analysis of CPTED in the Cyberspace Domain، Free PMC article، Vol. (20)، No. (14)، DOI: 10.3390/s20143968

وسعت دراسة [١] Roden Judah A. (2020) لتقديم تحليلات متكاملة عن الألعاب الإلكترونية المدعمة بالفيديو وأثارها على القائمين بممارسة تلك الألعاب، وتعرضت الدراسة لتاريخ صناعة الألعاب الإلكترونية والمراحل التاريخية عبر الفترات الزمنية التي مرت بها تلك الألعاب الإلكترونية وما أحدثته التطورات التكنولوجية الحديثة للأجهزة والبرمجيات من تحديثات سريعة ومتلاحقة لهذه الألعاب وكذلك علاقتها بالتغيرات الثقافية للمجتمع وارتباط التغيرات الثقافية والمجتمعية بالأمن المعلوماتي.

واهتمت دراسة [٢] Nyinkeu et al (2019) بالتعرف على مفهوم الأمن السيبراني الذي يجب غرسه لدى طلاب تكنولوجيا المعلومات بالجامعات، حيث قام الباحثون بإجراء مقابلات مباشرة مع مجموعة المبحوثين من طلاب الجامعات، وقد توصلت الدراسة من خلال نتائج استجابات عينة المبحوثين عن ضعف معرفة مفهوم الأمن السيبراني، وأكدت النتائج على ضرورة أهمية تعزيز مفهوم الأمن السيبراني كما أكدت الدراسة على أهمية التمييز بين الأمن السيبراني وأمن الشبكات.

وكشفت دراسة (٢٠١٨[٣](Bustard عن الانتهاكات والاخلاقيات المرتبطة بالأمن السيبراني، كما سعت نحو معرفة أثر تعلم الطلبة أخلاقيات الأمن السيبراني، وقد طبقت الدراسة على عينة من طلاب الدراسات العليا، حيث تم عمل إعداد استبيان لقياس مدى قبول وتحقيق الرضا من قبل عينة الدراسة لتلك الوحدة وتقبلهم لتعلم الأخلاقيات والتصدي للهجمات الإلكترونية من خلال الأمن السيبراني، وقد توصلت الدراسة من خلال نتائجها بأن عينة الدراسة لديها الرضا والقبول لتعلم الأخلاقيات المرتبطة بالأمن السيبراني بدرجة كبيرة، كما أكدت الدراسة على ضرورة التوعية للتصدي للهجمات والانتهاكات السيبرانية .

الاتجاه البحثي الثاني: دراسات تناولت تأثير الجرائم الذكية على قيم المجتمع وأخلاقياته:

أكدت دراسة ([٤] Golam Sarker (2023 ارتباط العلاقة بين الإعلام الرقمي والجرائم الإلكترونية، وتناولت الأنواع الشائعة للجرائم الإلكترونية التي يتم ارتكابها على وسائل التواصل الاجتماعي من قرصنة وسرقة هوية وابتزاز وتحرش واحتيال وتنمر، وأوصت بضرورة إجراء تعديلات على قوانين تكنولوجيا المعلومات لمنع تلك الجرائم الإلكترونية.

واهتمت دراسة (علواش كهينة (٢٠٢٢) [٥] بمخاطر الجريمة الإلكترونية عبر مواقع التواصل الاجتماعي وآثارها المتعددة، والانعكاسات السلبية لها بالتعدي على خصوصية الأفراد وتهديد أمن المعلومات وسلامة المجتمعات والدول.

---

(1) Roden Judah A. (2019) Video Game Industry Analysis: History، Growth، and Architecture، Master Thesis، Lamar University، The Faculty of the College of Graduate Studies

(2) Nyinkeu، N.، Anye، D.، Kwededu، L. & Buttler، W. (2018). Cyber education outside the cyber space: the case of catholic university institute of Buea. International journal of technology in teaching and learning. Vol. (14) ، No. (2) ، PP: 90-98

(3) Bustard، J. (2018). Improving student engagement in the study of professional ethics: concepts and an example in cyber security. Scientific engineer ethics. No. (24) ، pp: 683-692

(4) Sarker, G. (2022). An Interlinked Relationship between Cybercrime & Digital Media. International Journal for Multidisciplinary Research (IJFMR), 4(6), 1-5. https://www.ijfmr.com/papers/2022/6/1051.pdf

(٥) علواش كهينة (٢٠٢٢) مخاطر الجريمة الإلكترونية عبر مواقع التواصل الاجتماعي "بين اختراق الخصوصية وآليات المواجهة". مجلة دراسات عربية، جامعة الجزائر.

واشارت دراسة (سليمان تعمري (٢٠٢٢) [١] إلى أن زيادة الإقبال على استخدام مواقع التواصل الاجتماعي تؤدي دوراً مهما في انتشار الجرائم الإلكترونية في المجتمع، وأوصت بضرورة وجود عقوبات رادعة على مرتكبي الجرائم الإلكترونية للحد من تلك الجرائم.

اهتمت دراسة سمية حوداسي (٢٠٢٢) [٢] بإبراز الدور الذي تلعبه مواقع التواصل الاجتماعي بين نشر وتنمية الوعي السياسي والاجتماعي من خلال تكريس ثقافة المشاركة، وبين تأثيرها السلبي على استقرار الدول والمجتمعات العربية من خلال نشر ثقافة العنف والتطرف الإرهابي وإثارة الفتن ونشر الفوضى، وأشارت نتائج الدراسة إلى استخدام تنظيم داعش لهذه المواقع ونجاحه في تجنيد العديد من الشباب من خلالها نتيجة لتأثيرها الواسع على كل فئات المجتمع.

أما دراسة طارق ميرغني (٢٠٢٢) [٣]في سعت نحو التعرف على أساليب توظيف التنظيمات الإرهابية لوسائل التواصل الإلكتروني والإعلام الجديد من خلال تجنيد الشباب والأطفال وتهديد الأمن الفكري، إضافةً إلى استخدام الألعاب الإلكترونية كوسيلة للتواصل بجانب التدريب العسكري عبر الواقع الافتراضي، وقدمت الدراسة عدداً من الاستراتيجيات لمكافحة الأفكار الهدامة وإبراز الحقائق والقيم الصحيحة للعقيدة الإسلامية.

فيما هدفت دراسة هبة الله محمود (٢٠٢٢) [٤] التعرف على مستوى إدراك الشباب السعودي لتوظيف تنظيم داعش الإرهابي لوسائل الإعلام الرقمي الجديد لخدمة مصالحه وتحقيق أهدافه، وأظهرت أن أكثر الاستمالات التي يستخدمها التنظيم لجذب الشباب هي الاستمالات العاطفية تليها العقلية ثم النفسية.

وسعت دراسة (صفاء رجب (٢٠٢١)[٥] نحو الكشف عن علاقة استخدام طلاب الجامعة لوسائل الإعلام الجديد ودرجة تعرضهم لجرائم الإعلام الإلكتروني؛ إلى أن جريمة الاعتداء على الحق في الحياة الخاصة كانت الأعلى في التعرض لها عبر تلك الوسائل، وأن أسباب ارتكاب جرائم الإعلام الإلكتروني تمثلت في الشهرة والرغبة في جذب الأضواء والفساد الأخلاقي.

وتوصلت دراسة عبد النبي النوبي (٢٠٢٢) [٦] الى أن مواقع التواصل الاجتماعي تساهم في نشر العنف والتطرف، وأن المنظمات الإرهابية تستغل تلك المواقع لتجنيد المراهقين، وأوصت بضرورة

---

(١) سليمان تعمري. (٢٠٢٢) زيادة الإقبال على استخدام مواقع التواصل الاجتماعي وانعكاسها على الجرائم الإلكترونية في المجتمع الفلسطيني: دراسة من وجهة نظر طلبة الجامعات الفلسطينية في محافظة بيت لحم. المجلة العلمية لكلية الآداب، جامعة أسيوط، ٣١

(٢) سمية حوداسي(٢٠٢٢) جدلية دور مواقع التواصل الاجتماعي: بين نشر الوعي السياسي والاجتماعي وثقافة العنف والتطرف الإرهابي في المجتمع العربي. مجلة جيل الدراسات السياسية والعلاقات الدولية، 06 https://search.mandumah.com/Record/902447،.23

(٣) طارق ميرغني. (٢٠٢٢) توظيف التنظيمات الإرهابية لوسائل التواصل الإلكتروني: دراسة وصفية للمخاطر وكيفية المواجهة. مجلة القلزم للدراسات الإعلامية، ٨ ١٢٧١٣٢٨/https://search.mandumah.com/Record

(٤) هبة الله محمود (٢٠٢٢) إدراك الشباب لتوظيف التنظيمات الإرهابية لوسائل الإعلام الرقمي الجديد: داعش أنموذج ا: دراسة ميدانية على عينة من الشباب السعودي. مجلة مستقبل العلوم الاجتماعية، ٢

(٥) صفاء رجب. (٢٠٢٢) استخدام طلاب الجامعة لوسائل الإعلام الجديد وعلاقته بدرجة تعرضهم لجرائم الإعلام الإعلام الإلكتروني: دراسة ميدانية. مجلة البحوث في مجالات التربية النوعية، جامعة المنيا، ٨٤

(٦) عبد النبي النوبي. (٢٠٢٢) دور مواقع التواصل الاجتماعي في نشر العنف والتطرف: دراسة تطبيقية على عينة من المستخدمين بمنطقة جازان جنوب المملكة العربية السعودية. مجلة العربي للدراسات الإعلامية، ٣ https://search.mandumah.com/Record/1129262

توعية المجتمع بخطورة استغلال المنظمات الإرهابية لمواقع التواصل الاجتماعي، وأن يعمل قادة المجتمع على التبصير بخطورة تلك المنظمات.

كما أشارت دراسة (٢٠٢٠) [١] Abeer Fayed إلى أن الترويج الإلكتروني للإرهاب من خلال الشبكات الاجتماعية يلعب دور اً رئيسيا في تجنيد الشباب من قبل الإرهابيين، وأوصت بضرورة الترويج المضاد، واختراق هذه المواقع واستغلال الثغرات في هذه الجماعات الإرهابية، ووضع برنامج وطني شامل لمواجهتها.

كما سعت دراسة شريفة كلاع (٢٠٢٠) [٢] نحو التعرف على ظاهرة تجنيد الشباب في الجماعات الإرهابية من خلال استخدام شبكات التواصل الاجتماعي، وذلك بالتركيز على بيان أسباب استخدامها والكيفية التي يتم تجنيد واستقطاب الشباب من قبل تلك الجماعات، وقدمت الدراسة تصور اً للآليات التي يمكن من خلالها مواجهة ظاهرة تجنيد الشباب في الجماعات الإرهابية،

وأكدت دراسة ([٣] Nurzali Ismail (2020أن استغلال وسائل التواصل الاجتماعي لنشر الدعاية والتطرف العنيف أصبح قضية خطيرة، مشيرة إلى أن اتجاهات الشباب نحو هذا التطرف كانت معتدلة، وأن الحجج المقدمة والفائدة المتصورة وسهولة الاستخدام هي عوامل يمكنها التأثير على تلك الاتجاهات.

فيما توصلت دراسة عبد الله الدراوشة (٢٠٢٠) [٤] إلى كثرة التحديات في مواجهة مواقع التطرف على شبكات التواصل الاجتماعي من وجهة نظر طلبة الجامعات وفي مقدمتها التحديات الأمنية تليها التحديات الفكرية ثم التحديات القانونية.

أما دراسة لطفي الزيادي (٢٠٢٠) [٥] فقد تناولت الحرب الإعلامية وكيفية استخدامها من قبل المنظمات الإرهابية لبث أفكارها المتطرفة واستقطاب الشباب، وقامت بتحليل الاستراتيجية الاتصالية والإعلامية لما يسمى بتنظيم الدولة الإسلامية داعش، وأشارت إلى تحكمه كليا في العملية الاتصالية واستخدامه الرمزية والمرجعيات الدينية لتبرير أعماله الإجرامية وإضفاء نوع من المصداقية عليها.

بينما اهتمت دراسة (أكرم الربيعي (٢٠٢٠) [٦] بالتعرف على الأساليب الإلكترونية لغسيل الدماغ التي تتبعها التنظيمات الإرهابية وتحديداً تنظيم داعش في تجنيد الشباب والمراهقين، فضلا عن كيفية

---

(1) Abeer Fayed. (2020). The Role of Electronic Promotion of Terrorism Through Social Networks in the Spread of Terrorists Recruiting the Youth: Applied to the Kingdom of Saudi Arabia. Global Journal of Economics and Business, Refaad, 5(1), 109-125.

(٢) شريفة كلاع. (٢٠٢٠) ظاهرة تجنيد الشباب في الجماعات الإرهابية من خلال استخدام شبكات التواصل الاجتماعي. مجلة مدارات سياسية، ٨
٧٣٣٧٣/٣/٢/٤٢٩/https://www.asjp.cerist.dz/en/downArticle

(3) Ismail, N., et al. (2020). Understanding Malaysian youth's social media practices and their attitude towards violent extremism. Intellectual Discourse, 30(1), 5-33. https://www.proquest.com/scholarly-journals/understanding-malaysian-youths-social-media/docview/2701144939/se-2

(٤) عبد الله الدراوشة. (٢٠٢٠) التحديات الأمنية والفكرية والقانونية في مواجهة مواقع التطرف على شبكات التواصل الاجتماعي من وجهة نظر طلبة الجامعات الأردنية. مجلة العلوم الاجتماعية، جامعة الكويت،

(٥) لطفي الزيادي (٢٠٢٠) أساليب الحرب الإعلامية في المنظمات الإرهابية وآليات التصدي لها: دراسة نظرية تحليلية على "تنظيم الدولة الإسلامية". مجلة العلوم الإنسانية والاجتماعية، ٨
٩٤١٠٩٣/https://search.mandumah.com/Record

(٦) أكرم الربيعي وسعد إبراهيم (٢٠٢٠) ظاهرة بروز غسيل الدماغ الإلكتروني مع ظهور التنظيمات الإرهابية: دراسة في توظيف تنظيم الدولة الإسلامية "داعش" للتقنيات الرقمية في تجنيد الشباب والمراهقين. المجلة الدولية

توظيف التقنيات الرقمية في عملية غسيل الدماغ، وكشفت الدراسة عن وجود علاقة طردية موجبة بين التعرض للمواقع الإلكترونية الإعلامية الخاصة بالتنظيمات الإرهابية وظهور هذه العلامات على الشباب.

اما دراسة محمد جمال (٢٠٢٠) [١] فقد قدمت تصوراً لبرنامج مقترح من منظور الممارسة العامة في الخدمة الاجتماعية لتوعية الشباب بأخطار وأضرار التطرف الفكري عبر مواقع التواصل الاجتماعي وذلك لحمايتهم من الوقوع داخل دائرة التطرف،

أما دراسة محي الدين المدني (٢٠٢٠) [٢] فقد تناولت الإرهاب الإلكتروني واستخدام التنظيمات الإرهابية لمواقع التواصل الاجتماعي ونجاحهم في تجنيد العديد من الشباب، وفي مقدمتها تنظيم داعش الذي أسس لنفسه قاعدة أساسية على تلك المواقع، وقد قامت الدراسة بصياغة استراتيجية مقترحة للتصدي للإرهاب ومكافحة الأفكار المتطرفة عبر الشبكات الاجتماعية ترتكز على آليات المواجهة والتشريعات اللازمة.

أما دراسة سعيد القحطاني (٢٠٢٠) [٣] فقد أظهرت أهمية توظيف وسائل الإعلام الجديد ذاتها لتوعية الطلاب بمخاطر التطرف الفكري، وذلك من خلال التأكيد على أهمية المحافظة على العقيدة الإسلامية، وعرض الأفكار الصحيحة للطلاب عن حياة الفرد والمجتمع، وتحذير الطلاب من التيارات الفكرية الضالة عبر هذه الوسائل، وتوجيه الطلاب للسلوكيات المحمودة.

اما دراسة هيام الهادي (٢٠٢٠) [٤] فقد أوضحت أن أكثر أنواع الجرائم الإلكترونية انتشاراً عبر وسائل الإعلام الرقمي من وجهة نظر المراهقين هي الهجوم المتعلق بطلب فدية أو أموال من الآخرين وانتحال وسرقة هوية الأشخاص والاحتيال ونشر مواد إباحية والترصد والتحرش الإلكتروني وتشويه السمعة.

كما أظهرت دراسة حفيظة البراشدية (٢٠٢٠) [٥] تأكيد خبراء أمن المعلومات على وجود علاقة بين بعض الجرائم الإلكترونية وإساءة استخدام معلومات المستخدمين في الفيسبوك، وأن أبرز دوافع تلك

للإعلام والاتصال الجماهيري، الجامعة الخليجية، ٠ ١٠٨٤١٧٢/https://search.mandumah.com/Record

(١) محمد جمال. (٢٠٢٠) تصور مقترح لتنمية وعي الشباب بمخاطر التطرف الفكري عبر مواقع التواصل الاجتماعي: دراسة من منظور الممارسة العامة في الخدمة الاجتماعية. الأعمال الكاملة للمؤتمر العلمي الأول: مواجهة التحديات السياسية والاقتصادية في الأطر الإقليمية والدولية، كلية الدراسات الاقتصادية والعلوم السياسية جامعة بني سويف، ٨
https://search.mandumah.com/Record/910240

(٢) محي الدين المدني (٢٠٢٠) دور وسائل التواصل الاجتماعي في تفشي ظاهرة الإرهاب والتطرف في ضوء استراتيجية مقترحة للمواجهة. المجلة الدولية أبحاث في العلوم التربوية والإنسانية والآداب واللغات،
https://search.mandumah.com/Record/1083925

(٣) سعيد القحطاني (٢٠٢٠) استخدامات الإعلام الجديد في توعية الطلاب بمخاطر التطرف الفكري: دراسة مسحية على معلمي المرحلة الثانوية بمدارس مدينة الرياض. مجلة البحوث الإعلامية، كلية الإعلام – جامعة الأزهر،
https://search.mandumah.com/Record/1032753

(٤) هيام الهادي. (٢٠٢٠) تعرض المراهقين للجرائم الإلكترونية عبر وسائل الإعلام الرقمي وتأثيرها على إدراكهم للأمن الاجتماعي المصري. المجلة العربية لبحوث الإعلام والاتصال، جامعة الأهرام الكندية، ٣١

(٥) حفيظة البراشدية (٢٠٢٠) الفيسبوك والجرائم الإلكترونية في عُ مان: هل هنا علاقة؟ مجلة دراسات المعلومات والتكنولوجيا، ٨ https://search.mandumah.com/Record/١١٤١٧٣٥

الجرائم هي الحصول على المال أو الحصول على مواد حميمة أو سرقة البيانات والمعلومات الخاصة للانتفاع بها أو التشهير.

ومن جانبها أكدت دراسة ليلى بن برغوث (٢٠٢٠) [١]أن الخصوصية الرقمية محاصرة بأدوات ووسائل ذكية كأنظمة الذكاء الاصطناعي والحوسبة السحابية والبيانات الضخمة، وأن مواقع التواصل الاجتماعي المختلفة تساهم في تهديد خصوصية البيانات بدرجات مختلفة حسب شهرتها وضخامة مشتركيها ونوع الشركات التجارية والسياسية التي تتعامل معها.

كما كشفت دراسة عائشة كريكط (٢٠٢٠) ([٢]عن التحديات والمخاطر التي تواجه خصوصية المستخدمين للإعلام الرقمي والتي تتمثل في إساءة استخدام البيانات الخاصة بهم في أغراض تجارية أو سياسية وغيرها، بالإضافة إلى حفظ المواقع الإلكترونية المختلفة لمعلومات المستخدمين أثناء التصفح، وعالمية المعلومات وغياب المركزية ما يفتح المجال للاحتيال والتجسس الإلكتروني وتزوير المعلومات،

وأشارت دراسة شيرين كدواني (٢٠٢٠) [٣] إلى أن إعدادات الخصوصية التي توفرها مواقع التواصل الاجتماعي لا تحمي المستخدم إلا من بقية الأعضاء، ولكنها لا تمنع بياناته عن مالكي الخدمة الذين يجنون الأرباح من جمع تلك البيانات وبيعها لأغراض مختلفة مع التبرير بأن ذلك يسهم في بقاء استخدام تلك المواقع مجاناً.

وأشارت دراسة سمير الجمل (٢٠٢٠) [٤]إلى وجود آثار سلبية لمواقع التواصل الاجتماعي على القيم الثقافية، والدينية، والأخلاقية، والاجتماعية.

كما أظهرت دراسة عونية صوالحة وكوثر سلامة (٢٠٢٠) [٥] أن هناك تأثير لاستخدام مواقع التواصل الاجتماعي على تغيير القيم الاجتماعية لدى طلبة الجامعة، وكان هذا التأثير السلبي بدرجة متوسطة.

كما أثبتت دراسة محمد عقوب (٢٠٢٠) [٦]وجود تأثير لاستخدام شبكات التواصل الاجتماعي على منظومة القيم لدى الشباب الجامعي، وأن أكثر الآثار السلبية تتمثل في حالة التشتت التي تخلقها عملية التواصل عبر تلك المواقع حتى الانفصال عن الواقع

---

(١) ليلى بن برغوث. (٢٠٢٠) الخصوصية المعلوماتية على مواقع التواصل الاجتماعي في ظل التوجه الحتمي نحو المتاهة الافتراضية: التحديات، الانتهاكات، الانعكاسات. مجلة الإعلام والمجتمع، ٥ https://www.asjp.cerist.dz/en/downArticle/496/5/2/181088

(٢) عائشة كريكط. (٢٠٢٠) حق الخصوصية لمستخدم الفضاء الرقمي: المخاطر والتحديات. مجلة الحقيقة للعلوم الاجتماعية والإنسانية، ٠٢ https://www.asjp.cerist.dz/en/downArticle/٤٩/٢/١٨/٩٥٢٢٩

(٣) شيرين كدواني (٢٠٢٠) ضوابط حماية الحق في الخصوصية عبر مواقع التواصل الاجتماعي: دراسة تحليلية. تحليلية. مجلة البحوث الإعلامية، كلية الإعلام جامعة الأزهر، ٦١

(٤) سمير الجمل ومحمد الكرم (٢٠٢٠) الآثار السلبية لاستخدام مواقع التواصل الاجتماعي على عدد من القيم: دراسة ميدانية على طلبة جامعة الاستقلال في أريحا. شؤون اجتماعية، ٣٣ https://search.mandumah.com/Record/١٠٥٤٦٢٦

(٥) عونية صوالحة وكوثر سلامة (٢٠٢٠) استخدام مواقع التواصل الاجتماعي وأثره على القيم الاجتماعية لدى لدى طلبة جامعة عمان الأهلية. المجلة التربوية، جامعة سوهاج، ٦٦ https://search.mandumah.com/Record/٩٩٠١١٨

(٦) محمد عقوب (٢٠٢٠) استخدام شبكات التواصل الاجتماعي وآثارها على منظومة القيم لدى الشباب الجامعي: دراسة مطبقة لعينة من الشباب الجامعي. مجلة جامعة الزيتونة، ٨٣ https://search.mandumah.com/Record/٩٦٥٠٤٩

وهدفت دراسة جمعية بوكبشة (٢٠٢٠)[١] الى الكشف عن تأثير وسائل التواصل الاجتماعي على التغير القيمي لدى الشباب، حيث أشارت إلى أن القيم الأخلاقية والجمالية كانت الأكثر تداولا في تلك الوسائل ولها تأثير إيجابي على الشباب، وأن نوعية المنشورات تحدد قابلية هذا التغيير.

وأوضحت دراسة مها فتحي (٢٠٢٠) [٢] وجود تأثير لمستويات تعرض الشباب لفيديوهات التيك توك عبر هواتفهم الذكية على إدراكهم للقيم الاجتماعية في المجتمع.

وأشارت دراسة حنان السيد (٢٠٢٠) [٣]إلى المخاطر المتعددة الناتجة عن إساءة استخدام موقع الفيسبوك وتأثيراته السلبية على النسق القيمي للشباب، وتغير الاهتمامات لدى مستخدميه والتي تتعارض مع الدين والثقافة وتهدم قيم المجتمع.

أما دراسة هالة العصامي (٢٠٢٠) [٤] فقد حددت المشكلات الأخلاقية التي يواجهها المجتمع المصري جراء استخدام موقع التواصل الاجتماعي الفيسبوك، وتوصلت إلى منظومة قيم خلقية لازمة لمجابهة السلوكيات الأخلاقية الدخيلة على المجتمع مكونة من قيم خلقية كبرى هي (الصدق، المسؤولية، الأمانة، الوفاء، التسامح، اجتناب سوء الظن (،

كما هدفت دراسة شهرزاد سوفي (٢٠٢٠) [٥]بحث مظاهر الاستخدام القيمي واللاقيمي لموقع الفيسبوك، وتوصلت إلى أنه كلما كان المستخدم مشبعا بالقيم والتي مصدرها الدين الإسلامي والمحتوى مقترناً بها كان الاستخدام قيمي ا لموقع الفيسبوك وكلما ابتعد المستخدم والمحتوى عنها حدث العكس.

وكشفت دراسة ليلى الخياط (٢٠٢٠) [٦] عن الدور السلبي لمشاهدة الأطفال لليوتيوب في تغيير القيم الاجتماعية لهم من وجهة نظر أولياء الأمور، وأن أهم تلك السلبيات إهدار وقت كبير أمام الشاشة، وضعف قدرتهم على تنظيم وقت النوم، وعزلهم عن التواصل الاجتماعي مع من حولهم.

ودراسة شمس الهدى وخالد لعلاوي (٢٠٢٠) [١] فقد خلصت إلى أن موقع اليوتيوب يؤثر سلبا على القيم الأخلاقية لطفل ما قبل المدرسة ويعمل على هدم القيم الأصيلة، وعدم اهتمام مضامين البرامج

---

(١) جمعية بوكبشة (٢٠٢٠) وسائل التواصل الاجتماعي والصراع القيمي لدى الشباب: دراسة ميدانية على عينة من طلبة جامعة حسيبة بن بوعلي. المجلة الدولية للاتصال الاجتماعي، ١ mandumah.com/Record/1281888https://search

(٢) مها فتحي. (٢٠٢٠) تأثير تعرض الشباب لفيديوهات التيك تو عبر هواتفهم الذكية على إدراكهم للقيم الاجتماعية في المجتمع. المجلة المصرية لبحوث الرأي العام، كلية الإعلام ٨١ ١١٨٠٩٣٤/https://search.mandumah.com/Record

(٣) حنان السيد. (٢٠٢٠) أثر استخدام موقع التواصل الاجتماعي "الفيسبوك " Facebook على النسق القيمي لدى طلاب كلية التربية النوعية جامعة الإسكندرية. المجلة العلمية لجمعية إنسيا التربية عن طريق الفن، ٠٤ https://search.mandumah.com/Record/1001542

(٤) هالة العصامي (٢٠٢٠) منظومة القيم الخلقية الإسلامية البعد الغائب في مواقع التواصل الاجتماعي: الفيسبوك نموذجاً. المجلة التربوية، جامعة سوهاج، ٣٤ ١٠٤٨٨٠٥/https://search.mandumah.com/Record

(٥) شهرزاد سوفي (٢٠٢٠) الشباب الجزائري وموقع التواصل الاجتماعي الفيسبوك: دراسة في مظاهر الاستخدام القيمي واللاقيمي للموقع. مجلة العلوم الإنسانية، جامعة أم البواقي، ١ ٩٣٧٣٣٠/https://search.mandumah.com/Record

(٦) ليلى الخياط. (٢٠٢٠) استخدام اليوتيوب وعلاقته بتغيير القيم الاجتماعية لدى أطفال الكويت من وجهة نظر أولياء الأمور: دراسة ميدانية. المجلة التربوية، جامعة الكويت، ٣٤ ١٠٧٢٤٢٣/https://search.mandumah.com/Record

الموجهة له بالتنشئة على تلك القيم بقدر اهتمامها بالتسلية لغرض تجاري، بالإضافة إلى عدم ملاءمتها لقيم المنطقة العربية.

وتوصلت دراسة آمنة الكيلاني (٢٠٢٠)[٢] إلى تأثيرات الإعلام الاجتماعي السلبية على الأسرة العربية، ودوره في تفكك الأسرة وتبديل هويتها الوطنية بهويات وافدة، بالإضافة إلى تراجع دور الأسرة في التنشئة الاجتماعية والتربية وفق معايير المجتمع.

أما دراسة إبراهيم محمد (٢٠٢٠) [٣]فقد تناولت تأثير شبكات التواصل الاجتماعي في التنشئة الاجتماعية للشباب في المجتمعات الخليجية، وأظهرت أن من أهم العوامل التي تبعد الشباب عن دائرة التأثر الإيجابي بمؤسسات التنشئة الاجتماعية المعتادة بينما تقربهم أكثر من الوقوع ضمن دائرة التأثير السلبي لتلك الشبكات؛ تراجع دور مؤسسات التنشئة الاجتماعية التقليدية، فضلاً عن أنهم في إطارها يتحركون بحرية في نطاق مجتمع افتراضي بعيداً عن المجتمع الواقعي.

وأشارت دراسة لمياء محسن (٢٠٢٠)[٤] إلى دور مواقع التواصل الاجتماعي بالتفكك الأسري في المجتمع، حيث يعد الانشغال عن الأسرة وقضاء وقت طويل على مواقع التواصل الاجتماعي؛ أبرز أسباب سوء العلاقة الزوجية على مستوى الأسرة المصرية، كما تتمثل أسباب المشكلات الأسرية الناجمة عن استخدام الزوجين لتلك المواقع في التجاوز الأخلاقي في التعامل مع الجنس الآخر، وإخبار الأصدقاء على مواقع التواصل ما يحدث معهما في حياتهما الخاصة،

وأظهرت دراسة مساعد الجويان (٢٠٢٠) [٥]وجود علاقة طردية بين الآثار السلبية لاستخدام مواقع التواصل الاجتماعي وانتشار مظاهر التفكك الأسري، وأن من أبرز مظاهر هذا التفكك عدم اهتمام أفراد الأسرة بالقضايا والمشاكل الداخلية التي تخص أفرادها، وبروز مظاهر الأنانية.

كما أظهرت دراسة (٢٠٢٠) [٦] Najwa Albeladi (2020) التأثير السلبي للاستخدام المفرط للمراهقين لوسائل التواصل الاجتماعي على العلاقات الأسرية، وارتباط المستويات المنخفضة من التعبير الأسري والمستويات الأعلى من الصراع الأسري بإدمان تلك الوسائل، وأوصت الدراسة بضرورة تنفيذ استراتيجيات وساطة أبوية مختلفة للتحكم في استخدام وسائل التواصل الاجتماعي وتنظيمها وحماية أطفالهم من الآثار السلبية لها.

---

(١) شمس الهدى وخالد لعلاوي (٢٠٢٠) مواقع التواصل الاجتماعي وانعكاساتها على القيم الأخلاقية لطفل ما قبل المدرسة: دراسة تحليلية لمحتوى اليوتيوب المقدم للأطفال. مجلة العلوم الإنسانية، ٣٠ https://search.mandumah.com/Record/١٠٦٤٧٣٨

(٢) آمنة الكيلاني (٢٠٢٠) الإعلام الاجتماعي وأثره على الأسرة العربية من منظور اجتماعي وثقافي. كتاب أعمال المؤتمر الدولي المحكم: التفكك الأسري الأسباب والحلول ٢٢ ٢٣ مارس لبنان، ٠٥٦ ٠٤٠

(٣) إبراهيم محمد (٢٠٢٠) وسائل الإعلام الحديثة في التنشئة الاجتماعية للشباب في المجتمعات الخليجية، ش مجلة الباحث في العلوم الإنسانية والاجتماعية، ٠٨ https://search.mandumah.com/Record/١٠٨٣٧٦٩

(٤) لمياء محسن (٢٠٢٠) دور مواقع التواصل الاجتماعي في التفكك الأسري: دراسة ميدانية. مجلة البحوث الإعلامية، كلية الإعلام جامعة الأزهر، ٥٥ https://search.mandumah.com/Record/١١٠٢١٧٤

(٥) مساعد الجويان وسليم القيسي (٢٠٢٠) الآثار السلبية المترتبة على استخدام وسائل التواصل الاجتماعي وعلاقتها بالتفكك الأسري في المجتمع الكويتي. مجلة التربية، جامعة الأزهر، ٠٢٦ https://search.mandumah.com/Record/١٠٨٥٥٤٢

(6) Albeladi, N. & Palmer, E. (2020). The Role of Parental Mediation in the Relationship between Adolescents' Use of Social Media and Family Relationships in Saudi Arabia. Journal of Information Technology Management, 12(2), 163-183

وتناولت دراسة (KAYA-NANI Gamze (٢٠٢٠ [١] مخاطر الإعلام الرقمي وتأثيراته السلبية على الحياة اليومية للأسرة فيما يتعلق بتربية الأطفال، وأشارت إلى استخدام الآباء العديد من استراتيجيات الوساطة الأبوية لمواجهة تلك المخاطر إلا أنهم بحاجة لمزيد من التثقيف حولها.

وأظهرت دراسة (٢٠٢٠) [٢] (Şebnem Ulusoyأن إدمان وسائل التواصل الاجتماعي يؤثر سلبا على التواصل داخل الأسرة، كما يتم تضمين تلك الوسائل أيضا في الوقت الذي يقضيه أفراد الأسرة.

كشفت دراسة (أيمن خليل وفهد الخريف (٢٠٢٠)[٣] عن معاناة نسبة كبيرة من الأسر السعودية من ظاهرة الخرس الأسري نتيجة لانتشار استخدام شبكات التواصل الاجتماعي، حيث أن أكثر من نصف حجم العينة يقرون بقلة التفاعل وتقلص العلاقات الاجتماعية والحوارية بين أفراد الأسرة، بالإضافة إلى أن نسبة متوسطة من الأسر تعاني من الخرس أو الصمت الزوجي الذي يعد من أهم مظاهر الخرس الأسري في المجتمع.

كما توصلت دراسة وفاء محمد (٢٠٢٠) [٤]الى وجود علاقة بين استخدام مواقع التواصل الاجتماعي وانتشار ظاهرة الخرس الزوجي في مدينة سوهاج المصرية، واختلف الخرس الزوجي باختلاف كل من المستوى التعليمي والعمر ومدة الزواج والمهنة، وأوصت الدراسة بتنظيم دورات لتوعية الأزواج على حسن استخدام مواقع التواصل الاجتماعي. ورغم اتفاق أغلب الأدبيات على التأثيرات السلبية للإعلام الرقمي ووسائل التواصل الاجتماعي على العلاقات الأسرية والتنشئة الاجتماعية في السعودية.

الاتجاه البحثي الثالث: دراسات تناولت علاقة الذكاء الاصطناعي بالأمن السيبراني

هدفت دراسة Dambe et al.،[٥] (2023) إلى الكشف عن دور الذكاء الاصطناعي تحسين الأمن السيبراني حيث تواجه المؤسسات عددًا متزايدًا من الهجمات السيبرانية المتطورة ، وقد برز الذكاء الاصطناعي كحل واعد لهذا التحدي، حيث يمكنه أتمتة عمليات الأمن السيبراني، وتحديد التهديدات والاستجابة لها في الوقت الفعلي، وتقديم رؤى حول نقاط الضعف المحتملة، بالإضافة إلى أن الذكاء

---

(1) KAYA, G., (2020). Digital Parenting: Perceptions on Digital Risks. Kalem http://www.kalemacademy.com/Cms_Data/Contents/KalemAcademyDB/Folders/SayiMakaleleri/~contents/BMLJGDM7UFRFGAHS/10-23863kalem-2018-96.pdf 131-157.

(2) Ulusoy, Ş. & Atar, Ö. (2020). Reflection of social media addiction on family communication processes. Adam Academy Journal of Social Science, 10(2), 425-445. https://www.proquest.com/scholarly-journals/reflection-social-media-addiction-on-family/docview/2581938797/se-2

(٣) أيمن خليل وفهد الخريف (٢٠٢٠) شبكات التواصل الاجتماعي والخرس الأسري في المجتمع السعودي، (المجلة العلمية لجامعة الملك فيصل العلوم الإنسانية والإدارية)، ٨١ ١٠٤٠١٣٩/https://search.mandumah.com/Record

(٤) وفاء محمد. (٢٠٢٠) مواقع التواصل الاجتماعي والخرس الزوجي: دراسة ميدانية على عينة من الأزواج بمدينة سوهاج. مجلة علوم الإنسان والمجتمع، ٠١ ١٢٣٤٨١٩/https://search.mandumah.com/Record

(5) Dambe, S., Gochhait, S., & Ray, S. (2023, November). The Role of Artificial Intelligence in Enhancing Cybersecurity and Internal Audit. In 2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE) (pp. 88-93). IEEE.

الاصطناعي يمتلك القدرة على تبسيط إجراءات التدقيق الداخلي، وتحسين الدقة، وزيادة الرؤية في عمليات المنظمة، وتوصلت الدراسة نتائج إلى أن الذكاء الاصطناعي هو أداة قوية يمكنها تعزيز الوضع الأمني للمؤسسة بشكل كبير وضمان الامتثال للمتطلبات التنظيمية.

هدفت دراسة (Dambe et al.،[1] (2023 إلى استكشاف كيف يمكن للذكاء الاصطناعي تحسين الأمن السيبراني وممارسات التدقيق الداخلي. في وقتنا الحالي، تواجه المؤسسات عددًا متزايدًا من الهجمات السيبرانية المتطورة وتبحث بنشاط عن طرق جديدة لحماية معلوماتها وأنظمتها الحساسة. وقد برز الذكاء الاصطناعي كحل واعد لهذا التحدي، حيث يمكنه أتمتة عمليات الأمن السيبراني، وتحديد التهديدات والاستجابة لها في الوقت الفعلي، وتقديم رؤى حول نقاط الضعف المحتملة. بالإضافة إلى ذلك، يمتلك الذكاء الاصطناعي القدرة على تبسيط إجراءات التدقيق الداخلي، وتحسين الدقة، وزيادة الرؤية في عمليات المنظمة. تناقش هذه الورقة التقنيات المختلفة التي تعمل جنبًا إلى جنب مع الذكاء الاصطناعي لتحسين الأمن السيبراني وممارسات التدقيق الداخلي. تشير نتائج هذا البحث إلى أن الذكاء الاصطناعي هو أداة قوية يمكنها تعزيز الوضع الأمني للمؤسسة بشكل كبير وضمان الامتثال للمتطلبات التنظيمية.

ودراسة Zeadally et al.،[2] (2020) التي هدفت التعرف على قدرات الذكاء الاصطناعي في تحسين الأمن السيبراني، حيث أصبح الأمن السيبراني مجالًا سريع التطور بسبب زيادة التهديدات والجهود المستمرة التي يبذلها المتسللون للتغلب على تطبيق القانون، بمرور الوقت، قام مجرمو الإنترنت بتحسين أساليبهم، على الرغم من أن دوافعهم الأولية للقيام بالهجمات الإلكترونية ظلت ثابتة إلى حد ما، وتوصلت الدراسة الى ان التطورات التكنولوجية في مجال التشفير والذكاء الاصطناعي، وخاصة التعلم الآلي والتعلم العميق، لديها القدرة على تمكين المتخصصين في مجال الأمن السيبراني من مكافحة التهديدات الديناميكية التي يقدمها الخصوم.

وهدفت دراسة Alhayani et al.،[3]) (2021 إلى التعرف على مدى فعالية تقنيات الذكاء الاصطناعي في التخفيف من مخاوف الأمن السيبراني في العراق، بالتطبيق على العاملين في قطاع تكنولوجيا المعلومات. واستخدمت الدراسة منهج المسح واداة الاستبيان بالتطبيق على عينة مكونة من ٤٦٨ مفردة، واظهرت النتائج عدم وجود علاقة ذات دلالة إحصائية بين تطبيقات الذكاء الاصطناعي ومخاطر الأمن السيبراني.

واظهرت دراسة (Tao et al.،[4] (2021 أن الذكاء الاصطناعي يساعد في مخطط سوق الأمن السيبراني المؤسسات في مراقبة الهجمات السيبرانية وتحديدها والكشف عنها وصدها من أجل الحفاظ على خصوصية بياناتها، وان زيادة الوعي العام، والتحسينات التكنولوجية، وإنفاذ القانون، وحجم المعلومات المجمعة من العديد من المصادر، كلها جعلت من الضروري استخدام حلول

(1) Dambe, S., Gochhait, S., & Ray, S. (2023, November). The Role of Artificial Intelligence in Enhancing Cybersecurity and Internal Audit. In 2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE) (pp. 88-93).

(2) Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. Ieee Access, 8, 23817-23837.

(3) Alhayani, B., Mohammed, H. J., Chaloob, I. Z., & Ahmed, J. S. (2021). Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. Materials Today: Proceedings, 531(10.1016).

(4) Tao, F., Akhtar, M. S., & Jiayuan, Z. (2021). The future of artificial intelligence in cybersecurity: A comprehensive survey. EAI Endorsed Transactions on Creative Technologies, 8(28), e3-e3.

موثوقة ومعززة للأمن السيبراني في جميع الصناعات. إن الأنظمة السيبرانية ذات قدرات الذكاء الاصطناعي مدفوعة بارتفاع وتيرة ومستوى الهجمات السيبرانية، حيث أدى العدد المتزايد من الهجمات الإلكترونية إلى جعل الشركات تدرك الحاجة إلى تأمين بياناتها، وأن الغرض من معظم الهجمات الإلكترونية هو الربح.

وهدفت دراسة (Alhayani et al.،[1]) (2021 إلى دراسة مدى فعالية تقنيات الذكاء الاصطناعي في التخفيف من مخاوف الأمن السيبراني في العراق. وقد تم جمع البيانات من قبل الباحث من العاملين في قطاع تكنولوجيا المعلومات. استخدمت هذه الدراسة عينة مكونة من ٤٦٨ شخصًا، وأجرت التحليل العاملي التأكيدي، والصلاحية التمييزية، وتحليل النموذج الأساسي، وتقييم الفرضيات. وباستثناء النظام الخبير الذي لم يظهر أي علاقة ذات دلالة إحصائية بين الذكاء الاصطناعي والأمن السيبراني، فقد وجد أن القيم P لجميع المتغيرات ذات دلالة إحصائية. وكانت المشاكل الأساسية هي حجم العينة، وإمكانية الوصول، والمنطقة الجغرافية، وعدد أقل من المتغيرات.

وبيّنت دراسة (Tao et al.،[2]) (2021 أنه يساعد الذكاء الاصطناعي في مخطط سوق الأمن السيبراني المؤسسات في مراقبة الهجمات السيبرانية وتحديدها والكشف عنها وصدها من أجل الحفاظ على خصوصية بياناتها. إن زيادة الوعي العام، والتحسينات التكنولوجية، وزيادة أدوات الاستخبارات وإنفاذ القانون، وحجم المعلومات المجمعة من العديد من المصادر، كلها جعلت من الضروري استخدام حلول موثوقة ومعززة للأمن السيبراني في جميع الصناعات. إن الأنظمة السيبرانية ذات قدرات الذكاء الاصطناعي مدفوعة بارتفاع وتيرة ومستوى الهجمات السيبرانية. أدى العدد المتزايد من الهجمات الإلكترونية واسعة النطاق في جميع أنحاء العالم إلى جعل الشركات تدرك الحاجة إلى تأمين بياناتها. يتم تحفيز هؤلاء المجرمين الإلكترونيين من خلال المصالح الجماعية المتطرفة غير العلمانية، وسرقة المعلومات العابرة للحدود الوطنية، والتنافس بين المنافسين، والتحركات المتخذة لتحقيق مكاسب مالية وتشويه سمعة الآخرين. الغرض من معظم الهجمات الإلكترونية هو الربح.

وأوضحت دراسة (Zeadally et al.، [3]) (2020 أنّ على مدى السنوات العشر الماضية، أصبح الأمن السيبراني مجالًا سريع التطور وظهر في الأخبار بشكل متكرر بسبب زيادة التهديدات والجهود المستمرة التي يبذلها المتسللون للتغلب على تطبيق القانون. بمرور الوقت، قام مجرمو الإنترنت بتحسين أساليبهم، على الرغم من أن دوافعهم الأولية للقيام بالهجمات الإلكترونية ظلت ثابتة إلى حد ما. إن قدرة أنظمة الأمن السيبراني التقليدية على تحديد وإيقاف عمليات الاختراق الجديدة آخذة في التضاؤل. إن التطورات التكنولوجية في مجال التشفير والذكاء الاصطناعي، وخاصة التعلم الآلي والتعلم العميق، لديها القدرة على تمكين المتخصصين في مجال الأمن السيبراني من مكافحة التهديدات الديناميكية التي يقدمها الخصوم. هنا، ندرس كيف يمكن للذكاء الاصطناعي أن يعزز

(1) Alhayani, B., Mohammed, H. J., Chaloob, I. Z., & Ahmed, J. S. (2021). Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. Materials Today: Proceedings, 531(10.1016).

(2) Tao, F., Akhtar, M. S., & Jiayuan, Z. (2021). The future of artificial intelligence in cybersecurity: A comprehensive survey. EAI Endorsed Transactions on Creative Technologies, 8(28), e3-e3

(3) Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. Ieee Access, 8, 23817-23837.

حلول الأمن السيبراني من خلال الإشارة إلى مزاياه وعيوبه. نتحدث أيضًا عن الاتجاهات المحتملة للدراسة المستقبلية حيث يتم تطوير مناهج الذكاء الاصطناعي في الأمن السيبراني عبر مجموعة متنوعة من قطاعات التطبيقات.

وجدت دراسة (Li، 2018)[1] أنّ الذكاء الاصطناعي والأمن السيبراني لديهما العديد من التفاعلات المختلفة متعددة التخصصات. فمن ناحية، يمكن تطبيق تكنولوجيا الذكاء الاصطناعي، مثل التعلم العميق، على الأمن السيبراني لبناء نماذج ذكية لتصنيف البرامج الضارة، واكتشاف التسلل، واستشعار التهديدات الذكية. ومع ذلك، ستواجه نماذج الذكاء الاصطناعي مجموعة متنوعة من التهديدات السيبرانية، مما سيعطل عملية التعلم وصنع القرار وأخذ العينات. لذلك، من أجل منع التعلم الآلي العدائي، والحفاظ على خصوصية التعلم الآلي، والتعلم الموحد الآمن، وما إلى ذلك، تتطلب نماذج الذكاء الاصطناعي تقنيات متخصصة في الدفاع والحماية في مجال الأمن السيبراني. نحن ندرس العلاقة بين الذكاء الاصطناعي والأمن السيبراني بناءً على العاملين المذكورين أعلاه. أولاً، نقدم نظرة عامة على الجهود البحثية الحالية المتعلقة باستخدام الذكاء الاصطناعي لمواجهة الهجمات الإلكترونية، بما في ذلك استخدام كل من حلول التعلم العميق الراسخة وتقنيات التعلم الآلي التقليدية. بعد ذلك، سندرس الهجمات المضادة التي قد يكون الذكاء الاصطناعي عرضة لها، ونحلل سماتها، ونصنف استراتيجيات الحماية المناسبة. وأخيرًا، نلخص الأدبيات الحالية حول تطوير أنظمة الذكاء الاصطناعي الآمنة، مع التركيز على جوانب بناء شبكات عصبية مشفرة وتنفيذ التعلم العميق الموحد الآمن.

المبحث الرابع: الرؤية النقدية لدراسات جرائم الذكاء الاصطناعي والأمن السيبراني:

دراسات المدرسة الأمريكية:

ركزت على القضايا ذات الطابع التقني مثل: الأمن السيبراني، والجرائم المرتبطة بالعملات الرقمية المشفرة، وتطبيقات الإعلام الرقمي في مجال الإرهاب الإلكتروني بالإضافة إلى التحليل التقني للسلوك الإجرامي، والتهديدات السيبرانية على أمن الدول والأفراد والمؤسسات الأمنية

دراسات المدرسة الاوربية:

اهتمت بقضايا الأمن السيبراني وموضوعات الإرهاب الإلكتروني وعمليات التزييف اللين والعميق وحروب الجيل الرابع والخامس، وجرائم الذكاء الاصطناعي، وجرائم ابتزاز الأطفال والفتيات القاصرات

دراسات المدرسة الأسيوية:

ركزت على أساليب الجرائم الإلكترونية والاستخدام السلبي للإنترنت، وجرائم الاحتيال والنصب وسرقة البطاقات الائتمانية ومخاطر الأمن السيبراني وتداعيات ذلك على الأمن القومي للدول الأسيوية والعالم

دراسات المدرسة العربية:

اهتمت بالقضايا المجتمعية والأخلاقية مثل: الجرائم المتعلقة بانتهاك الخصوصية والتشهير والنصب والتنمر والتحرش والابتزاز وبث الكراهية والاحتيال وانتهاك الملكية الفكرية عبر وسائل التواصل الاجتماعي.

---

(1) Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering, 19(12), 1462-1474.

الجرائم التي ركزت عليها المدارس البحثية:
جرائم عامة مثل (القرصنة – الاحتيال الإلكتروني – السرقة الالكترونية – التجسس السيبراني – الإرهاب السيبراني)، وجرائم متخصصة مثل الجرائم (السياسية – الاقتصادية – الجنائية – المالية – المرأة والطفولة – ذوي الاعاقات،) وكذلك جرائم ذكية مثل الجرائم المتعلقة بتزييف المحتوى بالذكاء الاصطناعي وتطبيقاته التوليدية
الرؤية النقدية للأطر النظرية والمنهجية:
في دراسات المدرسة الأجنبية:
- تميزت الدراسات الأجنبية بالديناميكية العالمية والبعد التقني، حيث يتم تناول الجرائم السيبرانية كجزء من ظاهرة عالمية تشمل الاقتصاد والسياسة والجغرافيا.
- تركز الدراسات الأجنبية على التحليل التقني العميق، والاعتماد على النظريات المرتبطة بالشبكات والأنظمة، مما يجعلها أكثر شمولية في الطرح والمعالجة.
- الدراسات الأجنبية تُظهر مرونة في تبني أطر نظرية من تخصصات متعددة مثل التكنولوجيا، والاقتصاد، والسياسة، وعلم النفس، والجغرافيا والتاريخ ....
- تستخدم الدراسات الأجنبية نظريات تقنية متطورة، مثل نظرية الأمن السيبراني الاستباقي، لفهم استراتيجيات الدفاع والهجوم في الوقت نفسه.
- تتبني الدراسات الأجنبية أطر نظرية عالمية مثل الأنظمة المعقدة والحوكمة الدولية لدراسة التنسيق بين الدول لمكافحة الجرائم السيبرانية وتعزيز الأمن السيبراني
في دراسات المدرسة العربية:
- تأثرت الدراسات العربية بالسياقات الاجتماعية والثقافية والمحلية، مما يجعلها تركز على قضايا مثل التأثير على الأسرة والشباب والأخلاق العامة.
- ترتبط الدراسات العربية بقضايا مثل الأمية الرقمية، ضعف التشريعات، وتأثير الجرائم السيبرانية على البنية الاجتماعية.
- تُظهر الدراسات العربية ميلًا إلى استخدام النظريات الاجتماعية والإنسانية لتفسير الظاهرة.
- تعتمد الدراسات العربية غالبًا على النظريات الاجتماعية والإنسانية أكثر من النظريات التقنية المتقدمة.
- هناك نقص واضح في دمج الأطر التكنولوجية الحديثة في تحليل الجرائم السيبرانية في الدراسات العربية.
- تميل الدراسات العربية إلى تفسير الجرائم السيبرانية من منظور أخلاقي أو قانوني فقط، مع ضعف التركيز على التحليل العلمي والتقني للبنية التحتية الرقمية.

❖ تعليق الباحث:

يلاحظ الباحث أن النظريات المشتركة في المدرستين تجمعان بين الأبعاد الاجتماعية والتقنية لفهم الظاهرة من منظور شامل، مما يُبرز أهمية التعاون البحثي الدولي في مواجهة الجرائم السيبرانية. ودعم الأمن السيبراني على كافة مستوياته.
الدراسات الأجنبية:
- تعتمد بشكل كبير على المناهج الكيفية والتحليل الإحصائي.
- تجمع بين المناهج التقنية والقانونية لتقديم رؤى شاملة.
- تحليل البيانات الضخمة (Big Data) لتحديد الأنماط الإجرامية.

- النماذج التجريبية والمحاكاة لتحليل احتمالات وقوع الجرائم.
- استخدام تكنولوجيا التعلم العميق (Deep Learning) لفهم وتوقع الأنماط الإجرامية.

الدراسات العربية:

- تركز على المناهج الوصفية والتحليلية لشرح الظواهر السيبرانية في سياقات مجتمعية.
- تعتمد غالبًا على تحليل الدراسات السابقة والتشريعات والقوانين.

تستخدم أدوات تحليل المضمون والاستبانة والمقابلة لجمع البيانات.

المبحث الرابع: المستقبلية لبحوث جرائم الذكاء الاصطناعي والأمن السيبراني

- سعت معظم الدراسات والبحوث التي تم تحليلها إلى توصيف المخاطر والتأثيرات السلبية للإعلام الرقمي وفقا للاتجاهات البحثية التي انطلقت منها، وكانت المحاولات البحثية لتقديم حلول أو برامج محددة لمواجهة تلك المخاطر محدودة للغاية، لذلك فإن البحوث المستقبلية تحتاج إلى زيادة الاهتمام بطرح آليات تنفيذية يمكن من خلالها مواجهة مخاطر الإعلام الرقمي.
- كانت أغلب البحوث العربية فردية مما يتطلب توجيه الاهتمام بإجراء بحوث جماعية يمكن أن تجمع بين تخصصات الإعلام وعلم النفس والاجتماع في بحوث بينية مشتركة لدراسة تأثيرات ومخاطر الإعلام الرقمي مما يثري المكتبة الإعلامية العربية.
- كشف التحليل النقدي عن عدم استفادة عدد كبير من الدراسات العربية من الأطر النظرية والاكتفاء بتأصيلها معرفيا فقط، مما يتطلب أن تقوم البحوث العربية المستقبلية بالتوظيف الأمثل للأطر النظرية والاستفادة منها في صياغة واختبار فروضها ومناقشة نتائجها، بالإضافة إلى بناء الأطر النظرية والمفاهيمية لتصنيف مخاطر الإعلام الرقمي، وذلك لتسهيل فهم واستخدام وسائل الإعلام الجديد ومواقع التواصل الاجتماعي بشكل أفضل، وهنا يجب التوجه لاستخدام أطر ونماذج نظرية حديثة لمواكبة التطور المستمر في الإعلام الرقمي، ومحاولة استحداث نماذج نظرية تتوافق مع السياق الثقافي والبيئة الاجتماعية في الدول العربية.
- يلاحظ أن الدراسات الوصفية كانت الأكثر استخداما في الدراسات والبحوث التي تم تحليلها، مما يتطلب اعتماد البحوث العربية مستقبلاً على الدراسات التجريبية والاستشرافية المستقبلية، مع أهمية الدمج بين الأساليب الكمية والكيفية في دراسة مخاطر الإعلام الرقمي للتعمق في تفسير الظاهرة.
- كما يلاحظ تصدر منهج المسح المناهج البحثية المستخدمة في الدراسات والبحوث، تلاه المنهج التحليلي، مما يستلزم التنوع في المناهج المستخدمة في الدراسات العربية مستقبلاً، وتوظيف مناهج معاصرة تتناسب مع خصائص وسائل التواصل الاجتماعي، مثل المنهج الاثنوجرافي الذي يسمح للباحثين بدراسة التفاعل الاجتماعي في سياقات الاتصالات الرقمية الحديثة، بالإضافة إلى القيام ببحوث تجريبية مركزة، واستخدام المنهج الكيفي ومنهج التحليل النقدي من المستوى الثاني ومنهج دراسة الحال، مع تفعيل أدوات جمع البيانات المناسبة لتلك المناهج من ملاحظة واختبارات تجريبية وتحليل خطاب ومقابلات متعمقة ومجموعات نقاش مركزة، وذلك للوصول إلى نتائج أكثر عمقا، ويجب توجيه الاهتمام نحو توظيف أداة التحليل الشبكي وأدوات تحليل البيانات الضخمة Big data للتعامل مع الكم الهائل من البيانات على المنصات الرقمية.
- كما ركزت الدراسات والبحوث التي تم تحليلها على الشباب كونهم الأكثر استخداما لوسائل التواصل الاجتماعي، إلا أنه يجب توجيه الاهتمام البحثي لفئات أخرى كالأطفال وكبار السن وغيرها، بالإضافة إلى الجمهور العام من مستخدمي المنصات الرقمية.

أجندة البحوث المستقبلية في مجال جرائم الفضاء الإلكتروني والأمن السيبراني

يمكن اقتراح الأجندة التالية للقضايا البحثية التي يمكن معالجتها في الدراسات المستقبلية في هذا المجال:

- دراسة استخدام تطبيقات الذكاء الاصطناعي لتطوير خوارزميات قادرة على: التنبؤ بالجرائم السيبرانية قبل وقوعها.
- البحث في توحيد التشريعات الخاصة بالجرائم السيبرانية عالميًا لتجنب الثغرات القانونية وإجراء بحوث حول آليات التعاون الدولي لتتبع المجرمين عبر الحدود.
- دراسة دور المنظمات الدولية مثل الأمم المتحدة في وضع سياسات لحوكمة الأمن السيبراني في العالم.
- البحث في تقنيات الجيل الخامس مثل: الحوسبة الكمومية وتأثيرها على تشفير البيانات والتحديات السيبرانية المرتبطة بالواقع الافتراضي والواقع المعزز في المؤسسات الإعلامية.
- دراسة الأنواع الجديدة من الجرائم السيبرانية التي قد تظهر مع تطور التكنولوجيا مثل: الهجمات السيبرانية باستخدام الروبوتات، والجرائم المتعلقة بتزييف البيانات باستخدام الذكاء الاصطناعي (مثل التزييف العميق - Deepfake). والتلاعب بتقنية Chat Gpt)
- دراسة استراتيجيات تعزيز الثقافة السيبرانية لدى الاعلاميين عبر تطوير برامج تعليمية تركز على تدريب الاعلاميين على حماية أنفسهم من مرتكبي الجرائم الالكترونية وكيفية التعامل مع التهديدات والمخاطر المستقبلية.
- دراسة العلاقة بين الجرائم السيبرانية والحروب الإلكترونية عبر تطوير استراتيجيات دفاع وطنية لحماية الدول من الهجمات السيبرانية المنظمة.
- التركيز في الدراسات المستقبلية على فهم الدوافع النفسية والاجتماعية لمرتكبي الجرائم السيبرانية، ودراسة الفئات الأكثر عرضة للجرائم السيبرانية وكيفية حمايتها.
- البحث في استخدام تقنيات المحاكاة (Simulation) لتوقع آثار الجرائم السيبرانية، وتطوير أبحاث تعتمد على التجارب الميدانية والدراسات التطبيقية.
- دراسة القضايا الأخلاقية المتعلقة بجمع البيانات وتحليلها، ووضع سياسات تضمن خصوصية الأفراد أثناء البحث في الجرائم السيبرانية.
- التركيز على البحوث متعددة التخصصات، حيث تتطلب الجرائم السيبرانية أبحاثًا تجمع بين مختلف المجالات مثل: الاعلام والتكنولوجيا والقانون وعلم النفس والاجتماع.
- دراسة المعايير المهنية والأخلاقية في انتاج محتوى الجرائم الالكترونية عبر المنصات الرقمية وعلاقتها بمصداقية المحتوى لدى الجمهور.
- إعداد بحوث جماعية حول قوانين وسياسات تنظيم الأمن السيبراني بالمؤسسات الإعلامية الرقمية. في المنطقة العربية.

❖ مقترحات وتوصيات الدراسة:

- تحديث القواعد القانونية الإجرائية لمواكبة التطور السريع والمستمر للجرائم الإلكترونية.
- الاستفادة من خبرات الدول الرائدة في مجال مكافحة الجرائم الإلكترونية والقبض على المجرمين وإبرام اتفاقيات ثنائية وإقليمية ودولية في مجال البحث والتحري والتحقيق.

- التعاون الدولي في مجال ضبط الجرائم المعلوماتية لا سيما في مسائل المساعدة القانونية المتبادلة.
- إنشاء هيئات متخصصة في كشف وضبط الجرائم السيبرانية وفي ملاحقة الجناة.
- تشريع قوانين موضوعية تتعلق بمواجهة العراقيل والعوائق التي تحول دون تمكن المكلف بالتحقيق الجنائي من الوصول إلى فك غموض الجرائم المعلوماتية والقبض على المجرمين.
- سن نصوص قانونية خاصة تتعلق بجرائم الحاسب الآلي وآليات البحث والتحري والتحقيق عن الجرائم الإلكترونية مستقلة عن قانون العقوبات وقانون الإجراءات الجزائية وقانون الوقاية من الفساد ومكافحته.
- ضرورة التكاتف والتكامل بين الأجهزة الأمنية ووسائل الإعلام لوضع استراتيجية متكاملة لمواجهة التنظيمات الإرهابية، وصنع سياسة إعلامية محورها قضية تنمية الوعي الفكري بين الشباب ودعم دور مؤسسات التنشئة الاجتماعية، وتفعيل التشريعات والقوانين لتشمل عقوبات صارمة تتناسب مع جريمة التطرف على شبكات التواصل الاجتماعي، وتفعيل دور المؤسسات التعليمية والمجتمع المدني لمواجهة التطرف، ووضع سياسات تنموية لمواجهة الفقر والبطالة لأنهما من العوامل الأساسية المؤدية للتطرف.
- ضرورة إخضاع تطبيقات التواصل الاجتماعي إلى الرقابة من خلال تفعيل أداة الرقابة الذاتية والأبوية، إلى جانب تنشئة الأطفال والمراهقين على التربية الإعلامية التي تغرس فيهم الوعي وتحقق السلامة المجتمعية، وإعداد دورات تدريبية متخصصة لإكساب الشباب مهارات التواصل الآمن عبر شبكات التواصل الاجتماعي، وتشجيعهم على الاستفادة من جوانبها الإيجابية.
- ضرورة تشكيل فريق عمل من جهات رسمية مختلفة تقوم بإعداد خطة تنفيذية تحتوي على برامج وأنشطة وفعاليات، للتوعية باستخدام وسائل التواصل الاجتماعي لمختلف شرائح المجتمع والحد من آثارها السلبية ومتابعة تنفيذها وتقييمها باستمرار، ووضع سياسات رقابية واضحة من قبل الجهات الرسمية لإيجاد وسائل فاعلة للتقليل من الآثار السلبية لمواقع التواصل الاجتماعي على الأسرة وحظر المواقع المشبوهة.
- ضرورة الاهتمام بالتربية الإعلامية فيما يخص الإعلام الجديد لتثقيف الجمهور لمعرفة حقه في الخصوصية الرقمية وكيفية حماية بياناته، وضرورة سن قوانين ومواثيق إعلامية جديدة تناسب تطورات الوسائل الإعلامية الجديدة، واتخاذ الإجراءات اللازمة التي تحمي خصوصية المجتمعات والأفراد من انتهاكات الخصوصية عبر مواقع التواصل الاجتماعي، وإطلاق حملات توعية للجمهور حول كيفية التعامل بشكل قانوني مع مواقف انتهاك الخصوصية، وإطلاق حملات توعية خاصة للمرأة حول الاستخدام الآمن للإعلام الرقمي حتى لا تقع فريسة لعمليات الابتزاز الإلكتروني.
- ضرورة إصدار المزيد من التشريعات والقوانين الرادعة فيما يتعلق بجرائم التنمر الإلكتروني وتشديد العقوبات على المتنمرين، وإنشاء أقسام شرطة خاصة بتلك الجرائم، ووضع استراتيجيات من شأنها أن تساعد في الحد من انتشار هذه الظاهرة، والاهتمام بالأمن السيبراني بتثقيف الشباب والجيل الناشئ عن حدود الحريات في الفضاء الإلكتروني من خلال نشر الأفلام التسجيلية والبرامج التثقيفية والإعلانات التوعوية.

❖ المصادر والمراجع:

1. Abeer Fayed. (2020). The Role of Electronic Promotion of Terrorism Through Social Networks in the Spread of Terrorists Recruiting the Youth: Applied to the Kingdom of Saudi Arabia. Global Journal of Economics and Business, Refaad, 5(1), 109-125.

2. Adam, H. (2021). The Excessive Use of social media and its Relationship to Insomnia Among Female Students in Hail University.

3. AGG, "Cybercrime trends 2022," 2020. [Online]. Available: https://aag-it.com/the-latest-2022-cyber-crime-statistics/.

4. Alanazi, N. (2018). A Study of The Influence of Social Media Communication Technologies on Family Relationships In The Kingdom of Saudi Arabia. Journal of humanities and Social Sciences, 2(8), 107-136. https://search.mandumah.com/Record/941373

5. Albeladi, N. & Palmer, E. (2020). The Role of Parental Mediation in the Relationship between Adolescents' Use of Social Media and Family Relationships in Saudi Arabia. Journal of Information Technology Management, 12(2), 163-183

6. Alhayani, B., Mohammed, H. J., Chaloob, I. Z., & Ahmed, J. S. (2021). Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. Materials Today: Proceedings, 531(10.1016).

7. Aljasir, S. & Alsebaei, M. (2022). Cyberbullying and cybervictimization on digital media platforms: The role of demographic variables and parental mediation strategies. Humanities & Social Sciences Communications, 9(1), 1-9. https://doi.org/10.1057/s41599-022-01318-x

8. Ameen، A.، Tarhini، B.، Shah، M.، Madichie، D.، Paul، J. and Choudrie، J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. Computers in Human Behavior، 114(n/a)، doi.org/10.1016/j.chb.2020.106531

9. Axelrod, The Evolution of Cooperation, A second generation computer forensic analysis system, Digital investigations, New York: Basic Books Inc, 1984, pp. 34-42.

10. Bustard، J. (2018). Improving student engagement in the study of professional ethics: concepts and an example in cyber security. Scientific engineer ethics. No. (24) ، pp: 683-692

11. Cain, J. & Imre, I. (2022). Everybody wants some: Collection and control of personal information, privacy concerns, and social media use. New Media & Society, 24(12), 2705–2724. https://08113e081-1104-y-https-doi-org.mplbci.ekb.eg/10.1177/14614448211000327

12. Chadha, K., et al. (2020). Women's Responses to Online Harassment. International Journal of Communication, 14, 239-257. https://ijoc.org/index.php/ijoc/article/view/11683

13. Chan-Olmsted, S. M. (2019). A Review of Artificial Intelligence Adoptions in the Media Industry. International Journal on Media Management, 21(3–4), 193–215. Doi:10.1080/14241277.2019.1695619

14. Cywreck, B. (2024, 03 04). Top 10 Cybersecurity Powerhouses: Ranking the Global Defenders in 2024. Retrieved 08 28, 2024, from https://n9.cl/7posi

15. Dambe, S., Gochhait, S., & Ray, S. (2023, November). The Role of Artificial Intelligence in Enhancing Cybersecurity and Internal Audit. In 2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE) (pp. 88-93). IEEE.

16. Dambe, S., Gochhait, S., & Ray, S. (2023, November). The Role of Artificial Intelligence in Enhancing Cybersecurity and Internal Audit. In 2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE) (pp. 88-93).

17. Dutot, V. (2020). A social identity perspective of social media's impact on satisfaction with life. Psychology & Marketing, 37(6), 759-772. https://doi.org/10.1002/mar.21333

18. El-Tarabishi, M. & Elsayed, M. (2020). The Impact of Cyberbullying on Private High School Teenagers in Cairo Governorate. 30 , 2-31. https://search.mandumah.com/Record/1140511

19. Ferris, A., et al. (2021). Applying the uses and gratifications model to examine consequences of social media addiction. Social media + Society, 7(2), 1-16. https://doi.org/10.1177/20563051211019003

20. G. Technology, "Trends in Cybercrime in 2022 and Beyond," 2021. [Online]. Available: https://blog.govnet.co.uk/technology/trends-in-cybercrime-in-and-beyond.

٢١. https://search.mandumah.com/Record/1001542

٢٢. https://search.mandumah.com/Record/1032753

٢٣. https://search.mandumah.com/Record/1083925

٢٤. https://search.mandumah.com/Record/1129262

٢٥. https://search.mandumah.com/Record/910240

٢٦. https://www.asjp.cerist.dz/en/downArticle/496/5/2/181088

27. Huang, J., et al. (2021). Cyberbullying in social media and online games among Chinese college students and its associated factors. International Journal of Environmental Research and Public Health, 18(9), 1-12. https://doi.org/10.3390/ijerph18094819

28. Ismail, N., et al. (2020). Understanding Malaysian youth's social media practices and their attitude towards violent extremism. Intellectual Discourse, 30(1), 5-33. https://www.proquest.com/scholarly-journals/understanding-malaysian-youths-social-media/docview/2701144939/se-2

29. James, P. & Kur, J. (2020). Parental Mediation of Children's Risky Experiences with Digital Media. The Journal of Society and Media, 4(2), 298-318. https://www.researchgate.net/publication/350816418

30. Jemin Justin Lee ، Myong-Hyun Go ، Yu-Kyung Kim ، Minhee Joo.)2020(، A Multi-Component Analysis of CPTED in the Cyberspace Domain، Free PMC article، Vol. (20)، No. (14)، DOI: 10.3390/s20143968

31. KAYA, G., (2020). Digital Parenting: Perceptions on Digital Risks. Kalem http://www.kalemacademy.com/Cms_Data/Contents/KalemAcademyDB/Folders/SayiMakaleleri/~contents/BMLJGDM7UFRFGAHS/10-23863kalem-2018-96.pdf 131-157.

32. lhayani, B., Mohammed, H. J., Chaloob, I. Z., & Ahmed, J. S. (2021). Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. Materials Today: Proceedings, 531(10.1016).

33. Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering, 19(12), 1462-1474.
34. Management (JDM) &1(2). 2020.
35. Mberia, H. & Kamaku, M. (2018). Social Sites Accessibility and the Rise of Sexual Harassment among Teenagers in Kenya. International Journal of Recent Research in Social Sciences and Humanities, 5(1), 64-72.
36. media text data, Asian development bank, p.125.
37. Meier, A. & Reinecke, L. (2021). Computer-Mediated Communication, Social Media, and Mental Health: A Conceptual and Empirical Meta-Review. Communication Research, 48(8), 1182-1209. https://journals.sagepub.com/doi/pdf/10.1177/0093650220958224
38. Mieczkowski, H., et al. (2020). Priming effects of social media use scales on well-being outcomes: The influence of intensity and addiction scales on self-reported depression. Social media + Society, 6(4), 1-15. https://doi.org/10.1177/2056305120961784
39. Moskal. E (2020) ، A Model of Establishing Cyber Security Center of Excellence. Information Systems Education Journal، Vol. (13) ، No. (6) ، PP 97- 102
40. Nadia Al-Mutairi. (2022). The Impact of Intensive Use of Social Networking in Increasing Cyber Bullying Among Secondary School Female Students in Riyadh in the Kingdom of Saudi Arabia. (https://search.mandumah.com/Record/1243898
41. Nyinkeu، N.، Anye، D.، Kwededu، L. & Buttler، W. (2018). Cyber education outside the cyber space: the case of catholic university institute of Buea. International journal of technology in teaching and learning. Vol. (14) ، No. (2) ، PP: 90-98
42. Others, J. L. (2012). Cyber Security Policy guidebook (01 ed.). New Jersey, united states of america: Published by John Wiley & Sons, Inc.
43. Park, A. F. (2022): Mapping the public voice of development natural langue processing of social
44. Peng Wang, Mei Su, Jingyi Wang. (2021). Organized crime in cyberspace: How traditional organized criminal groups exploit the online peer-to-peer lending market in China. The British Journal of Criminology. Volume 61. Issue 2. Pp. 303–324.
45. Peng Wang, Paul Joosse, Lok Lee Cho. (2020). The Evolution of Protest Policing in a Hybrid Regime. The British Journal of Criminology. Volume 60. Issue 6. Pp. 1523–1546.
46. Pete Fussey, Bethan Davies& Martin Innes. (2021). 'Assisted' facial recognition and the reinvention of suspicion and discretion in digital policing. The British Journal of Criminology. Volume 61. Issue 2. pp. 325
47. Roden Judah A. (2019) Video Game Industry Analysis: History، Growth، and Architecture، Master Thesis، Lamar University، The Faculty of the College of Graduate Studies
48. S. Morgan, "Official Cyber Crime Report," Cybersecurity Ventures, 2022
49. Sarker, G. (2022). An Interlinked Relationship between Cybercrime & Digital Media. International Journal for Multidisciplinary Research (IJFMR), 4(6), 1-5. https://www.ijfmr.com/papers/2022/6/1051.pdf

50. Sarker, G. (2022). An Interlinked Relationship between Cybercrime & Digital Media. International Journal for Multidisciplinary Research (IJFMR), 4(6), 1-5. https://www.ijfmr.com/papers/2022/6/1051.pdf
51. siau,k.& wang, w. Artificial intelligence ethics: ethics of AI and ethical AL. Journal of Database
52. States, u. d. (2023). joint Statement on the United States-European Union 9th Cyber Dialogue in Brussels. Brussels: Office of the Spokesperson. Retrieved from: https://n9.cl/ppy73
53. Tao, F., Akhtar, M. S., & Jiayuan, Z. (2021). The future of artificial intelligence in cybersecurity: A comprehensive survey. EAI Endorsed Transactions on Creative Technologies, 8(28), e3-e3.
54. Tao, F., Akhtar, M. S., & Jiayuan, Z. (2021). The future of artificial intelligence in cybersecurity: A comprehensive survey. EAI Endorsed Transactions on Creative Technologies, 8(28), e3-e3
55. Ulusoy, Ş. & Atar, Ö. (2020). Reflection of social media addiction on family communication processes. Adam Academy Journal of Social Science, 10(2), 425-445. https://www.proquest.com/scholarly-journals/reflection-social-media-addiction-on-family/docview/2581938797/se-2
56. Ulusoy, Ş. & Atar, Ö. (2020). Reflection of social media addiction on family communication processes. Adam Academy Journal of Social Science, 10(2), 425-445. https://www.proquest.com/scholarly-journals/reflection-social-media-addiction-on-family/docview/2581938797/se-2
57. Walker, b. (2019). Cyber Security: Comprehensive Beginners Guide to Learn the Basics and Effective Methods of Cyber Security. Australia: Independently Published
58. Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. Ieee Access, 8, 23817-23837.
59. Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. Ieee Access, 8, 23817-23837.
٦٠. إبراهيم محمد (٢٠٢٠) وسائل الإعلام الحديثة في التنشئة الاجتماعية للشباب في المجتمعات الخليجية، ش مجلة الباحث في العلوم الإنسانية والاجتماعية، ٠٨ https://search.mandumah.com/Record/١٠٨٣٧٦٩
٦١. أسماء أحمد أبو زيد، (٢٠٢١)، استراتيجيات خطاب صحافة التكنولوجيا العربية تجاه الأمن السيبراني، المجلة المصرية لبحوث الرأي العام، مج (٢٠)، ع (٢).
٦٢. أسماء على جابر، (٢٠٢٤) الانعكاسات والمخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمي وآليات المواجهة في ضوء رؤية مصر ٢٠٣٠، الاكاديمية العسكرية للدراسات العليا والإستراتيجية مج ٢، ع٤، ص١٠٣.
٦٣. أكرم الربيعي وسعد إبراهيم (٢٠٢٠) ظاهرة بروز غسيل الدماغ الإلكتروني مع ظهور التنظيمات الإرهابية: دراسة في توظيف تنظيم الدولة الإسلامية "داعش" للتقنيات الرقمية في تجنيد الشباب والمراهقين. المجلة الدولية للإعلام والاتصال الجماهيري، الجامعة الخليجية، ٠ https://search.mandumah.com/Record/١٠٨٤١٧٢
٦٤. أماني حمدي. (٢٠٢٢). دور مواقع الإعلام الرقمي في حماية الأمن السيبراني: دراسة تحليلية لعينة من المواقع الخاصة بالأمن السيبراني. جامعة القاهرة - كلية الإعلام، المجلة المصرية لبحوث الإعلام، ع٨٠ ص ١٠٦.
٦٥. آمنة الكيلاني (٢٠٢٠) الإعلام الاجتماعي وأثره على الأسرة العربية من منظور اجتماعي وثقافي. كتاب أعمال المؤتمر الدولي المحكم: التفكك الأسري الأسباب والحلول ٢٢ ٢٣ مارس لبنان، ٠٥٦ ٠٤٠
٦٦. اية عمر فرج. (٢٠٢٢)، دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي – جامعة الأمير سطام بن عبد العزيز نموذجا، مجلة جامعة سوهاج الدولية التربوية
٦٧. أيمن خليل وفهد الخريف (٢٠٢٠) شبكات التواصل الاجتماعي والخرس الأسري في المجتمع السعودي، (المجلة العلمية لجامعة الملك فيصل العلوم الإنسانية والإدارية)، ٨١ https://search.mandumah.com/Record/١٠٤٠١٣٩

٦٨. جمعية بوكبشة (٢٠٢٠) وسائل التواصل الاجتماعي والصراع القيمي لدى الشباب: دراسة ميدانية على عينة من طلبة جامعة حسيبة بن بوعلي. المجلة الدولية للاتصال الاجتماعي، ١ mandumah.com/Record/1281888https://search
٦٩. حفيظة البراشدية (٢٠٢٠) الفيسبوك والجرائم الإلكترونية في عُمان: هل هنا علاقة؟ مجلة دراسات المعلومات والتكنولوجيا، ٨ ١١٤١٧٣٥/https://search.mandumah.com/Record
٧٠. حنان السيد. (٢٠٢٠) أثر استخدام موقع التواصل الاجتماعي "الفيسبوك " Facebook على النسق القيمي لدى طلاب كلية التربية النوعية جامعة الإسكندرية. المجلة العلمية لجمعية إنسيا التربية عن طريق الفن، ٠٤
٧١. سعيد القحطاني (٢٠٢٠) استخدامات الإعلام الجديد في توعية الطلاب بمخاطر التطرف الفكري: دراسة مسحية على معلمي المرحلة الثانوية بمدارس مدينة الرياض. مجلة البحوث الإعلامية، كلية الإعلام – جامعة الأزهر،
٧٢. سليمان تعمري. (٢٠٢٢) زيادة الإقبال على استخدام مواقع التواصل الاجتماعي وانعكاسها على الجرائم الإلكترونية في المجتمع الفلسطيني: دراسة من وجهة نظر طلبة الجامعات الفلسطينية في محافظة بيت لحم. المجلة العلمية لكلية الآداب، جامعة أسيوط، ٣١
٧٣. سمية حوداسي(٢٠٢٢) جدلية دور مواقع التواصل الاجتماعي: بين نشر الوعي السياسي والاجتماعي وثقافة العنف والتطرف الإرهابي في المجتمع العربي. مجلة جيل الدراسات السياسية والعلاقات الدولية،
٧٤. سمير الجمل ومحمد الكرم (٢٠٢٠) الآثار السلبية لاستخدام مواقع التواصل الاجتماعي على عدد من القيم: دراسة ميدانية على طلبة جامعة الاستقلال في أريحا. شؤون اجتماعية، ٣٣ ١٠٥٤٦٢٦/https://search.mandumah.com/Record
٧٥. شريفة كلاع. (٢٠٢٠) ظاهرة تجنيد الشباب في الجماعات الإرهابية من خلال استخدام شبكات التواصل الاجتماعي. مجلة مدارات سياسية، ٨ ٧٣٣٧٣/٣/٢/٤٢٩/https://www.asjp.cerist.dz/en/downArticle
٧٦. شمس الهدى وخالد لعلاوي (٢٠٢٠) مواقع التواصل الاجتماعي وانعكاساتها على القيم الأخلاقية لطفل ما قبل المدرسة: دراسة تحليلية لمحتوى اليوتيوب المقدم للأطفال. مجلة العلوم الإنسانية، ٣٠ ١٠٦٤٧٣٨/https://search.mandumah.com/Record
٧٧. شهرزاد سوفي (٢٠٢٠) الشباب الجزائري وموقع التواصل الاجتماعي الفيسبوك: دراسة في مظاهر الاستخدام القيمي واللاقيمي للموقع. مجلة العلوم الإنسانية، جامعة أم البواقي، ١ ٩٣٧٣٣٠/https://search.mandumah.com/Record
٧٨. شيرين عبد الحفيظ، (٢٠٢٣). دور الإعلام الرقمي في تعزيز الأمن السيبراني ومكافحة التهديدات والجرائم السيبرانية. المجلة العلمية لبحوث العلاقات العامة والإعلان، جامعة القاهرة - كلية الإعلام، عدد ٢٥، ص٢٠١.
٧٩. شيرين كدواني (٢٠٢٠) ضوابط حماية الحق في الخصوصية عبر مواقع التواصل الاجتماعي: دراسة تحليلية. مجلة البحوث الإعلامية، كلية الإعلام جامعة الأزهر، ٦١
٨٠. شيماء تركان صالح، (٢٠٢٣). الأمن الوطني العراقي والتهديدات السيبرانية... الإرهاب السيبراني نموذجا. كلية العلوم السياسية، جامعة النهرين.
٨١. صفاء رجب. (٢٠٢٢) استخدام طلاب الجامعة لوسائل الإعلام الجديد وعلاقته بدرجة تعرضهم لجرائم الإعلام الإلكتروني: دراسة ميدانية. مجلة البحوث في مجالات التربية النوعية، جامعة المنيا، ٨٤
٨٢. طارق ميرغني. (٢٠٢٢) توظيف التنظيمات الإرهابية لوسائل التواصل الإلكتروني: دراسة وصفية للمخاطر وكيفية المواجهة. مجلة القلزم للدراسات الإعلامية، ٨ ١٢٧١٣٢٨/https://search.mandumah.com/Record
٨٣. عادل عبد الصادق. (٢٠٢٢)، الإرهاب السيبراني والأمن القومي في بيئة متغيرة، مؤسسة الأهرام، مجلة السياسة الدولية، مج)٠٤(، ع)٢٢٤(، ص ص .٢٧٤-٢٧٧ -
٨٤. عائشة كريكط. (٢٠٢٠) حق الخصوصية لمستخدم الفضاء الرقمي: المخاطر والتحديات. مجلة الحقيقة للعلوم الاجتماعية والإنسانية، ٠٢ ٩٥٢٢٩/٢/١٨/٤٩/https://www.asjp.cerist.dz/en/downArticle
٨٥. عبد الله الدراوشة. (٢٠٢٠) التحديات الأمنية والفكرية والقانونية في مواجهة مواقع التطرف على شبكات التواصل الاجتماعي من وجهة نظر طلبة الجامعات الأردنية. مجلة العلوم الاجتماعية، جامعة الكويت،
٨٦. عبد النبي النوبي. (٢٠٢٢) دور مواقع التواصل الاجتماعي في نشر العنف والتطرف: دراسة تطبيقية على عينة من المستخدمين بمنطقة جازان جنوب المملكة العربية السعودية. مجلة العربي للدراسات الإعلامية، ٣

٨٧. علواش كهينة (٢٠٢٢) مخاطر الجريمة الإلكترونية عبر مواقع التواصل الاجتماعي "بين اختراق الخصوصية وآليات المواجهة". مجلة دراسات عربية، جامعة الجزائر.
٨٨. عونية صوالحة وكوثر سلامة (٢٠٢٠) استخدام مواقع التواصل الاجتماعي وأثره على القيم الاجتماعية لدى طلبة جامعة عمان الأهلية. المجلة التربوية، جامعة سوهاج، ٦٦ https://search.mandumah.com/Record/٩٩٠١١٨
٨٩. لطفي الزيادي (٢٠٢٠) أساليب الحرب الإعلامية في المنظمات الإرهابية وآليات التصدي لها: دراسة نظرية تحليلية على "تنظيم الدولة الإسلامية". مجلة العلوم الإنسانية والاجتماعية، ٨ https://search.mandumah.com/Record/٩٤١٠٩٣
٩٠. لمياء محسن (٢٠٢٠) دور مواقع التواصل الاجتماعي في التفكك الأسري: دراسة ميدانية. مجلة البحوث الإعلامية، كلية الإعلام جامعة الأزهر، ٥٥ https://search.mandumah.com/Record/١١٠٢١٧٤
٩١. ليلى الخياط. (٢٠٢٠) استخدام اليوتيوب وعلاقته بتغيير القيم الاجتماعية لدى أطفال الكويت من وجهة نظر أولياء الأمور: دراسة ميدانية. المجلة التربوية، جامعة الكويت، ٣٤ https://search.mandumah.com/Record/١٠٧٢٤٢٣
٩٢. ليلى بن برغوث. (٢٠٢٠) الخصوصية المعلوماتية على مواقع التواصل الاجتماعي في ظل التوجه الحتمي نحو المتاهة الافتراضية: التحديات، الانتهاكات، الانعكاسات. مجلة الإعلام والمجتمع، ٥
٩٣. مالك بن فهد الغبيوي، (٢٠٢٠) الأمن السيبراني ودوره في الحد من تهديدات الأمن الفكري، رسالة ماجستير، قسم الدراسات الاستراتيجية، جامعة نايف العربية للعلوم الأمنية
٩٤. محمد جمال. (٢٠٢٠) تصور مقترح لتنمية وعي الشباب بمخاطر التطرف الفكري عبر مواقع التواصل الاجتماعي: دراسة من منظور الممارسة العامة في الخدمة الاجتماعية. الأعمال الكاملة للمؤتمر العلمي الأول: مواجهة التحديات السياسية والاقتصادية في الأطر الإقليمية والدولية، كلية الدراسات الاقتصادية والعلوم السياسية جامعة بني سويف، ٨
٩٥. محمد عقوب (٢٠٢٠) استخدام شبكات التواصل الاجتماعي وآثارها على منظومة القيم لدى الشباب الجامعي: دراسة مطبقة لعينة من الشباب الجامعي. مجلة جامعة الزيتونة، ٨٣ https://search.mandumah.com/Record/٩٦٥٠٤٩
٩٦. محي الدين المدني (٢٠٢٠) دور وسائل التواصل الاجتماعي في تفشي ظاهرة الإرهاب والتطرف في ضوء استراتيجية مقترحة للمواجهة. المجلة الدولية أبحاث في العلوم التربوية والإنسانية والآداب واللغات،
٩٧. مساعد الجويان وسليم القيسي (٢٠٢٠) الآثار السلبية المترتبة على استخدام وسائل التواصل الاجتماعي وعلاقتها بالتفكك الأسري في المجتمع الكويتي. مجلة التربية، جامعة الأزهر، ٠٢٦ https://search.mandumah.com/Record/١٠٨٥٥٤٢
٩٨. منال حسن محمد إبراهيم. (٢٠٢١)، الوعي بجوانب الأمن السيبراني في التعليم عن بعد، المجلة العلمية لجامعة الملك فيصل - العلوم الإنسانية والإدارية، مج (٢٢)، ع (٢)، ص .٣٠٠
٩٩. مها فتحي. (٢٠٢٠) تأثير تعرض الشباب لفيديوهات التيك تو عبر هواتفهم الذكية على إدراكهم للقيم الاجتماعية في المجتمع. المجلة المصرية لبحوث الرأي العام، كلية الإعلام ٨١ https://search.mandumah.com/Record/١١٨٠٩٣٤
١٠٠. موسى بن تغري. (٢٠٢٠)، الحرب السيبرانية والقانون الدولي الإنساني، مجلة الاجتهاد القضائي، مجلد ١٢ص ٤٥
١٠١. نجوان أحمد عاصم عبد الجواد، (٢٠٢٣)، الجريمة السيبرانية وتأثيرها على الأمن القومي المصري: دراسة سوسيو تحليلية، جامعة الفيوم - كلية الآداب مجلة كلية الآداب، مج ١٥، ع١، ص ٢١٤٩
١٠٢. هالة العصامي (٢٠٢٠) منظومة القيم الخلقية الإسلامية البعد الغائب في مواقع التواصل الاجتماعي: الفيسبوك نموذجاً. المجلة التربوية، جامعة سوهاج، ٣٤ https://search.mandumah.com/Record/١٠٤٨٨٠٥
١٠٣. هبة الله محمود (٢٠٢٢) إدراك الشباب لتوظيف التنظيمات الإرهابية لوسائل الإعلام الرقمي الجديد: داعش أنموذج اً دراسة ميدانية على عينة من الشباب السعودي. مجلة مستقبل العلوم الاجتماعية، ٢
١٠٤. هيام الهادي. (٢٠٢٠) تعرض المراهقين للجرائم الإلكترونية عبر وسائل الإعلام الرقمي وتأثيرها على إدراكهم للأمن الاجتماعي المصري. المجلة العربية لبحوث الإعلام والاتصال، جامعة الأهرام الكندية، ٣١
١٠٥. وفاء محمد. (٢٠٢٠) مواقع التواصل الاجتماعي والخرس الزوجي: دراسة ميدانية على عينة من الأزواج بمدينة سوهاج. مجلة علوم الإنسان والمجتمع، ٠١ https://search.mandumah.com/Record/١٢٣٤٨١٩