الجريمة السيبرانية وتأثيرها على الأمن القومي المصرى: دراسة سوسيو تحليلية

نجوان أحمد عاصم عبد الجواد*
naa06@fayoum.edu.eg

ملخص

هدفت الدراسة إلى التعرف على الأبعاد الاجتماعية والاقتصادية للجريمة السيبرانية ، وتحليل التحديات والتهديدات التي تواجه الأمن القومي المصري نتيجة الجريمة السيبرانية ،وكيف أثرت الجريمة السيبرانية على بروز أنماط جديدة من الصراع القومي المصري، وما هى استراتيجية جمهورية مصر العربية في مواجهة الجريمة السيبرانية ؟ ، استخدمت الدراسة منهج المسح الاجتماعي على عينة طبقية عددها ٥٠٠ مفردة من شباب جامعة الفيوم من كليات عملية ونظرية وباستخدام أداة الأستبيان ، ومن أهم النتائج التي توصلت إليها الدراسة:

- توصلت الدراسة إلى أن الجريمة السيبرانية تزداد بشكل مباشر عن طريق الايميلات الإلكترونية وذلك بإرسال بعض الايميلات الوهمية التي تحمل بعض 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 .
- توصلت نتائج الدراسة أن الأبعاد الاجتماعية والاقتصادية للجريمة السيبرانية هي الفقر والأمية الرقمية والبطالة والتهميش الاجتماعي والسياسى للفرد والفضول الزائد الذى يعانى منه ، فليجأ الفرد إلى إثبات ذاته عن طريق انتهاك خصوصية الغير، فالجرائم السيبرانية تمتاز بخصوصيات تميزها عن غيرها من الجرائم حيث أنها ترتكب في بيئة افتراضية ولاتترك أثراً مادياً ، في صعب إكتشافها.
- توصلت نتائج الدراسة إلى أنه من التهديدات المحتملة للجريمة السيبرانية الاختراق الإلكترونى والتجسس السيبراني من خلال إستغلال الثغرات الأمنية فى البنية التحتية السيبرانية للوصول إلى معلومات حساسة وسرية وأمنية حول الحكومات والشركات

* مدرس بقسم علم الاجتماع – كلية الأداب – جامعة الفيوم

والمؤسسات الحيوية ، وقد تستخدم تلك المعلومات فى التأثير على القرارات الوطنية والتجسس الصناعي.

- توصلت نتائج الدراسة أنه من التهديدات المحتملة للجريمة السيبرانية التي تهدد الأمن القومي المصرى الحروب السيبرانية فقد تقوم دولة أو جماعة إرهابية بهجمات بغرض الإضطرار بالبنية التحتية للبلاد ، وقدرتها العسكرية والاستخباراتية والاقتصادية ، وذلك يؤثر على الأمن القومي.
- توصلت نتائج الدراسة أنه من ضمن التهديدات التي تواجه الأمن القومي المصرى نتيجة الجريمة السيبرانية التطرف الإلكتروني وتأثيره على الأنظمة السياسية للبلاد حيث سوء استخدام مواقع التواصل الاجتماعي والمنصات الرقمية لنشر الأفكار المتطرفة لتأثيرها على الرأى العام والعملية السياسية فى مصر ، واستغلال الجماهير وقوة الوسائط الاجتماعية لتحقيق أهداف سياسية لإثارة الفتن والإنقسامات داخل الشعب .
- توصلت نتائج الدراسة إلى أنه من ضمن الاستراتيجيات المتبعة لمكافحة الجريمة السيبرانية استراتيجية التعاون الدولي لأن الجريمة السيبرانية عابرة للحدود ، فلابد من تبادل المعلومات والخبرات حيث تكون المساعدات القانونية عابزة للدول لحل أى مشكلة.
- توصلت نتائج الدراسة إلي أنه من ضمن الاستراتيجيات المتبعة لمكافحة الجريمة السيبرانية استراتيجية تعزيز التدريب والتأهيل : حيث لابد من توفير تدريب مناسب للكوادر الأمنية بحيث يكون لديهم الخبرات الكافية للتعامل مع التهديدات السيبرانية لجمع الأدلة الرقمية حول أى جريمة وتحليلها بالطريقة المناسبة .
- توصلت نتائج الدراسة أنه من ضمن الاستراتيجات المتبعة لمكافحة الجريمة السيبرانية استراتيجية الإجابة السريعة وتطوير خطة الطوارئ للهجمات السيبرانية ، فلابد من وجود خطط للطوارئ والاستعدادت اللأزمة لإستعادة البيانات ، وإصلاح الأنظمة المتضررة ، وتحديد المسؤليات والإجراءات وتقديم المساءلة .

الكلمات المفتاحية: الجريمة السيبرانية – الأمن القومي – الفضاء السيبراني

مقدمة :

شهد المجتمع العالمي بالفترة الأخيرة تطورات على مستوى تكنولوجيا المعلومات، وشبكات الإنترنت، صاحب ذلك تطور ملحوظ في نشاطات الجريمة الإلكترونية، والتهديدات الأمنية التي تستهدف المجال السيبراني ضمن الفضاء الإلكتروني في إطار ما يسمى بالحرب الإلكترونية، مما حتم على دول العالم على اختلاف مستوياتها الاقتصادية والاجتماعية التعاون البيني في سبيل البحث عن استراتيجيات وميكانيزمات فعالة كفيلة بالتصدي لهذا النوع من التهديدات التي على تعمل تحطيم البنية الإلكترونية التحتية للدول ومنظوماتها[١]

فالجريمة السيبرانية هي أحد التحديات التي تواجه الأمن القومي في العديد من البلدان فتشمل مجموعة واسعة من الأنشطة الإجرامية غير المحدودة بالحدود الجغرافية مثل القرصنة الإلكترونية ، وغسيل الأموال ، والإرهاب الدولي ، فالجرائم السيبرانية تلحق الدمار بالاقتصاد العالمي والأمن القومي والاستقرار الاجتماعي والمصالح الفردية،و تركز الجهود الحالية للدول على التخفيف من تهديدات الجرائم السيبرانية في المقام الأول باتخاذ التدابير التقنية اللأزمة . [٢]

فاتخاذ التدابير التقنية المناسبة لمحاربة مثل تلك الجرائم أحد أهم الأسلحة الاستراتيجية التي تمتلكه الدول في عصر الثورة الرقمية حاليًا [٣] ، حيث أنه أعلى تحدى يواجه الأمن القومي المصري في العصر الحديث ، نظراً للمخاطر المصاحبة لها باعتبار أن

[١] - بلى سمير_.(٢٠٢٣) ، التهديدات الأمنية السيبرانية : دراسة فى انعكاسات الحرب الالكترونية على الأمن القومي للدول وإستراتيجيات المقاومة ، مجلة الرسالة للدراسات والبحوث الانسانية (٨)٢ ،ص ١٨٩

2- Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., ... & Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities and Social Sciences Communications*, *10*(1), 1-10.

3- Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of cyber security. *International Journal of Advanced Research in Computer and Communication Engineering*, *7*(11), 125-128.

المفهوم الحديث للأمن لايشتمل فقط على الأمن العسكري ، بل يشمل أمن الفرد والمؤسسة والأسرة والدولة على جميع المستويات ومن أهمها أمن المعلومات [١] ، الأمر الذى يضع السيادة الوطنية لأي دولة على المحك ، خاصة مع زيادة التجسس الإلكتروني على بعض الدول حيث أسقطت تكنولوجيا المعلومات والاتصالات مفهوم الحدود الجغرافية، السياسية والثقافية فيما بينها.[٢]

فالأمن السيبراني والجريمة السيبرانية من المفاهيم الجديدة التي يمكن من خلالها الوقوف على التحديات الحديثة التي تواجه الأمن القومي في عصر المنصات الرقمية خصوصاً أن الفرد هو الذي يمكن أن يحدد من خلال تصرفاته وأفعاله وثقافته المعنى الحقيقي للأمن، كما يبدو له، وهنا يتسع معنى الأمن ليتضمن جوانب معرفية عديدة، وداخلة تطرح أسئلة كثيرة، من نوعية: الأمن لمن؟ ولماذا؟ وما الشروط التي تحقق الأمن؟، فالحرب السيبرانية تستغرق وقتاً طوبلاً بين الدول لأنها بدون معدات عسكرية، وافتراضية .[٣]

مشكلة الدراسة :

في ظل تنامي التهديدات والمخاطر العالمية المعاصرة، وتنوع مصادرها الخارجية وداخل حدود الدول ذاتها واتساع دوائر تأثيراتها السلبية على النظم السياسية والاجتماعية، وعلى حياة الشعوب، تم التوسع في رصد محاور القضايا الأمنية واتجهت الدراسات الأمنية على الصعيد الأممي ولدى المنظمات الدولية ورجال البحث

1- Alarab Muhammad..(2016). Securing The Future: An Egyptian National Security Strategy, Issues in international Security, Spring,P3

[٢] -طاله لاميه (٢٠٢٠)، التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومى للدول واستراتيجيات مكافحاتها ،مجلة معالم للدراسات القانونية والسياسية ، (٤)٢ ،ص ٥٦

3- Adil Rasool.(2017) "Crimes and Laws Related to Internet users: an Overview," *SSRG International Journal of Economics and Management Studies*, vol. 4, no. 3, pp. 6-10,

الأكاديمي والتنموي إلى التوسع في مفهوم الأمن القومي حيث أصبح مفهوم الأمن القومي يضم زخم من القضايا الاقتصادية والاجتماعية والسياسية والثقافية المتشابكة [١]

فالعالم العربي يشهد تغيرات واسعة وحراكاً سياسياً واجتماعيا هامًا، فالأحداث التي شهدتها كل من تونس ومصر و سوريا، و التي أدت لإسقاط النظام تتّم عن وجود تدخل خارجي عبر الوسائط الإعلامية من جهة و تزايد الاختراق المرن للأمن الوطني للدول وأثرها على زعزعة الاستقرار الداخلي للدول من جهة ثانية، فالأنظمة السياسية تعرف مدى أهمية تكنولوجيا الاتصال ، فالإعلام الاجتماعي بطابعه الشبكي أصبح يشكل نمطاً جديداً من أشكال التنظيم الجماعي، فهو يساهم في تشكيل فضاء يمارس من خلاله كل أشكال الجرائم الإلكترونية التي أصبحت أخطر أنواع الجرائم التي ترتكب عبر الشبكة الدولية للمعلومات، ويتضح ذلك من خلال النظر إلى فداحة الخسائر التي يمكن أن تسببها عملية واحدة ناجحة تندرج تحت مفهومه. [٢]

فالجرائم السيبرانية تتسم بطابع سرية الهوية ولاتترك سوى القليل من الأثر، بالإضافة إلى ذلك لا تقف أمام الجرائم السيبرانية أي قيود إقليمية أو زمنية، ويمكن أن تسبب أضراراً لعدد لا يحصى من الضحايا، ويجدر الاشارة أن قضية أمن المعلومات قد تجاوزت مفهومها التقني لتشمل الأبعاد الأمنية والدفاعية والاستراتيجية، فضلا عن أنها أصبحت جزءًا لا يتجزأ من خطط الأمن القومي لأى دولة والمواثيق الدفاعية للتحالفات العسكرية.

كما أنها باتت محل اهتمام دائم في ظل التطور التكنولوجي المذهل الذي بقدر ما يحمله للعالم من فرص فإن في طياته مخاطر جمة،[٣] ، الذى من شأنه أن يرسخ أزمة

---

[١] - العدوى، محمد أحمد ،٢٠١٠" ،الأمن الأنسانى ومنظومة حقوق الإنسان"، فى: أحمد مجدى حجازى(تحرير)، المواطنة وحقوق الإنسان فى ظل المتغيرات الدولية الراهنة، القاهرة، الدار المصرية السعودية للطباعة والنشر والتوزيع، ص ١٤١ .

[٢]- قرني، أماني حمدي، خطاب & ,إيمان عبد المنعم. (٢٠٢٢). دور مواقع الإعلام الرقمي في حماية الأمن السيبراني .*المجلة المصرية لبحوث الأعلام*..687-657 ,(80) *2022* ,

[٣] - الماحى، & .,اسامه صلاح محمود. (٢٠٢٣). الجرائم المعلوماتية المهددة للأمن القومى المصرى .*مجلة البحوث القانونية والاقتصادية-المنوفية*(1)*57* ،ص ص104-63

عدم ثقة بين المواطنين ، كأزمة الانتخابات الأمريكية عام ٢٠١٦الذى كلفت الولايات المتحدة الأمريكية ما يزيد عن ٣٥ مليون دولار أمريكي، ووجه البعض أصابع الاتهام إلى روسيا ، وتدمير البنية التحتية للدولة وتهديد القيم والأخلاق وغيرها من المخاطر الاجتماعية، ويعتبر عام ٢٠١٨ هو عام الاختراقات الامنية ، حيث شهد العالم كله خلال عام ٢٠١٨ ارتفاعاً كبيراً في عمليات اختراق أنظمة الأمن الإلكتروني وبالتالي تسريب بيانات الملايين من المستخدمين ، ومن ثم حاجة دول العالم الماسة إلى تشريعات دولية واضحة ومحددة بشأن مواجهة الإرهاب السيبراني[١]. **ومن هنا يأتي السؤال الرئيسي للبحث :. وهو إلى أي مدى تؤثر الجريمة السيبرانية على الأمن القومي المصري؟**

ويتفرع منه عدة تساؤلات فرعية وهي :

١- ما الجريمة السيبرانية ؟، وما أنواعها؟

٢- ما الأبعاد الاجتماعية والاقتصادية للجريمة السيبرانية ؟

٣- ما التحديات والتهديدات التي تواجه الأمن القومي المصري نتيجة الجريمة السيبرانية ؟

٤- كيف أثرت الجريمة السيبرانية على بروز أنماط جديدة من الصراع القومي المصري؟

٥- ما استراتيجية جمهورية مصر العربية في مواجهة الجريمة السيبرانية وأمن المعلومات ؟

أهمية الدراسة :

ـ مما لاشك فيه أن العالم أصبح بعاني من مشكلات اجتماعية أفرزتها البيئة الرقمية، مثل الغزو الثقافي الرقمي، والجريمة السيبرانية، والابتزاز

[١] -فوزى إسلام (٢٠١٩)، الامن السيبرانى : الأبعاد الأجتماعية والقانونية : تحليل سيوسولوجى ، المجلة القومية الأجتماعية ، طنطا، مج ٥٦، ع ٢، ص ٩٩

الإلكتروني ،وفي ضوء هذه البيئة المتغيرة ، تأتى هذه الدراسة محاولة لدراسة هذه المشكلات ، واتخاذ الإجراءات والتشريعات المناسبة لمجابهة تقنية المعلومات ضد جميع أشكال الجريمة السيبرانية ، وهذا مادعت إليه حاجة البحث في الوقت الراهن لنشر بعض التوصيات للمختصين بوضع السياسات الاجتماعية بالمجتمع المصري للوقوف على كيفية مكافحة الجريمة السيبرانية ورفع الوعى السيبراني لدى المواطنين، وإنشاء مجتمع قائم على المعرفة الرقمية والذى من شأنه ينعكس على البيئة الواقعية في ظل خطة مصر للتنمية المستدامة ٢٠٣٠ ،ويمكن أن يثري ذلك الدراسات المختصة في علم الاجتماع الرقمي، بسبب قلة بعض الدراسات المصرية التى تناولت تأثير الجريمة السيبرانية على الأمن القومي المصرى بعد جائحة كوفيد-١٩ حيث زاد معدل الاعتماد على الإنترنت وهو ماتتناوله الدراسية الحالية.

ومن هذه الأهمية تنطلق أهداف الدراسة :

أهداف الدراسة :

١- التعرف على ماهية الجريمة السيبرانية، وأنواعها.

٢- التعرف على الأبعاد الاجتماعية والاقتصادية للجريمة السيبرانية .

٣- التعرف على التحديات والتهديدات التي تواجه الأمن القومي المصري نتيجة الجريمة
السيبرانية .

٤- التعرف على استراتيجية جمهورية مصر العربية في مواجهة الجريمة السيبرانية وأمن المعلومات .

مفاهيم الدراسة :

١- الأمن السيبراني :

يعتبر مفهوم الأمن السيبراني من المفاهيم الحديثة نسبياً ، حيث ارتبط ظهوره بالثورة التكنولوجية ومع تزايد اعتماد الفرد عليها في كل شيء، أصبح الأمن السيبراني أحد أكبر التحديات التي تواجهها المؤسسات في الوقت الحاضر.[١]

يختلف تعريف الأمن السيبراني حسب طبيعة كل دولة حيث هناك من يعرفه على عالم افتراضي يتشابك مع العالم المادي يؤثر ويتأثر به بشكل معقد، في مثل لدى بعض الدول البعد الخامس للحرب القومية .[٢]

ويعرف على أنه" أمن الشبكات والأنظمة المعلوماتية، وأي بيانات تتعلق بالأجهزة المتصلة على الإنترنت، وعليه فهو المجال الذي يتعلق بإجراءات ومقاييس ومعايير الحماية المفروض اتخاذها أو الالتزام بها لمواجهة التهديدات، ومنع التعديات ".[٣]

المفهوم الإجرائي للأمن السيبراني : هي كل ما تتخذها الدولة من إجراءات وقوانين وممارسات واتفاقيات دولية لرفع الوعي الرقمي لدى المواطنين لحماية خصوصيتهم الثقافية والمعلوماتية على شبكة الإنترنت ، وحماية الفضاء الإلكتروني ضد أي معتدي.

٢- الفضاء السيبراني

صاغ ويليام جيبسون مصطلح "الفضاء السيبراني" لأول مرة عام ١٩٨٢ " للإشارة إلى واقع افتراضي تم إنشاؤه بواسطة الكمبيوتر، ومع ذلك ، أصبح المصطلح شائعًا في عام ١٩٨٤ ، بعد استخدامه من قبل جيبسون من الناحية اللغوية ، فيعد الفضاء

1- Hubbard, D. W., & Seiersen, R. (2023). *How to measure anything in cybersecurity risk*. John Wiley & Sons.p8

٢- شلوش ، نورة. ٢٠١٨. القرصنة الإلكترونية في الفضاء السيبراني "التهديد المتصاعد لأمن الدول". مجلة مركز بابل للدراسات الإنسانية، (٨)، ٢، ص١٨٥.206-185 .

٣-طالة، لامية. ٢٠٢٠. التهديدات و الجرائم السيبرانية : تأثيرها على الأمن القومي للدول و استراتيجيات مكافحتها. معالم للدراسات القانونية و السياسية، (٤) ٢،ص ٦٠.

السيبراني كلمة مركبة ، وهو المصطلح الذي يصف تخليقًا بين الإنسان والآلة ينتج عنه ربط جسم الإنسان بجهاز متقدم عالي التقنية، فالفضاء السيبراني مصطلح يتميز بالقدرة على التواجد الافتراضي والتفاعل بين الناس من خلال "الرموز والحقائق الاصطناعية" [١]

٣- **الجريمة السيبرانية** :الجريمة السيبرانية هي إحدى الجرائم المعاصرة التي أصبحت تمثل خطراَ على الفرد وأمن المجتمع، حيث أنها تتقدم بوتيرة سريعة؛ حيث يستخدم المجرمون أحدث تقنيات الرقمية في تنفيذ هجماتهم السيبرانية [٢]، فاختلفت تعريفات مصطلح "القرصنة" على مر العقود ، فهذا المفهوم يتعلق بالأشخاص الذين يحصلون على وصول غير مصرح به إلى أنظمة المعلومات بما في ذلك شبكات الكمبيوتر. واقتحام نظامه ، حيث يعتبر تجاوز أذونات الشبكة شكلاً من أشكال التعدي على الشخص الأخر.[٣]

فتتكون الجريمة الإلكترونية أو الافتراضية Cyber Crimes من مقطعين هما الجريمة Crime، والإلكترونية Cyber، ويستخدم مصطلح الإلكترونية لوصف فكرة جزء من الحاسب،أو عصر المعلومات ، أما الجريمة فهي السلوكيات والأفعال الخارجة عن القانون[٤] ،والجرائم الإلكترونية هي المخالفات التي ترتكب ضد الأفراد بدافع الجريمة ولإيذاء سمعة الضحية أو أذى مادي أو عقلي للضحية بطريقة مباشرة أو غير مباشرة باستخدام شبكات الاتصال من الإنترنت [٥]

1-Kemmerer, R. A. (2003, May). Cybersecurity. In *25th International Conference on Software Engineering, 2003. Proceedings.* (pp. 705-715). IEEE.

[٢] -عطية روان (٢٠٢٠) ، الجرائم السيبرانية ،المجلة الالكترونية الشاملة متعددة التخصصات ، السعودية ، مج ٣ع ٢٤ ، ص ١

3- McQuade III, S. C. (Ed.). (2008). *Encyclopedia of cybercrime*. Bloomsbury Publishing USA.p.12

4-Goni, O., Ali, M. H., Alam, M. M., & Shameem, M. A. (2022). The Basic Concept of Cyber Crime. *Journal of Technology Innovations and Energy*, *1*(2), 16-24.

5 - موسى دياب(٢٠٢٤) ، الجرائم الالكترونية : المفهوم والأسباب، ورقة علمية منشورة فى الملتقى العلمى الجرائم المستحدثة فى ظل المتغيرات والتحولات الاقليمية والدولية ، كلية العلوم الاستراتيجية ، عمان ، ص ١

المفهوم الإجرائي للجريمة السيبرانية : هي أفعال وممارسات قد تكون مستجدة على السلوك البشري ولكنها خارج القانون ، فمرتكبيها يتميزون بمعرفتهم الشديدة والمهارية بالكمبيوتر وشبكة الإنترنت .

٤- **الأمن القومي** :يعد مفهوم الأمن القومي مفهوم يتسم بالغموض لأنه يخضع باستمرار إلى ظروف وعوامل خارجة وداخلية تؤثر عليه تأثيراً مباشراً ، فالأمن القومي كما يعتبره علي الدين هلال "هو مفهوم شامل ، ليس مسألة حماية للحدود وحسب، ولا قضية إقامة ترسانة من السلاح،أنه يجمع كل المتطلبات وغيرها، فهو قضية مجتمعية تشمل الكيان الاجتماعي بكافة جوانبه لتأمين كيان الدولة ضد الأخطار التي تهددها داخلياً وخارجياً،وتأمين مصالحها وتحقيق أهدافها وغايتها القومية [١]

المفهوم الإجرائي للأمن القومي: هو حماية الفضاء الإلكتروني، وحماية المؤسسات والشركات وأي بيانات ضد أي معتدى هو المفهوم التي اعتمدت عليه الباحثة في هذا البحث.

الدراسات السابقة :

١- **دراسة سمير بلي : التهديدات الأمنية السيبرانية : دراسة في انعكاسات الحرب الإلكترونية على الأمن القومي للدول واستراتيجيات المقاومة ،٢٠٢٣ [٢]**

هدف الدراسة: هدفت الدراسة إلى بحث في طبيعة التهديدات الأمنية السيبرانية التي تواجه المنظومات المعلوماتية للدول، وذلك من خلال التطرق لمفاهيم الأمن السيبراني

[١] - أبو سعود، ، و عباس طاهر. (٢٠٢٠). ارتباطات الأمن المعلوماتي بالأمن القومي، مجلة الدراسات الحقوقية، مج٧، ع٢ ، 221 - 204 هاني مطر منصور

[٢] -بلى سمير_.(٢٠٢٣) ، التهديدات الأمنية السيبرانية : دراسة فى انعكاسات الحرب الالكترونية على الأمن القومي للدول وإستراتيجيات المقاومة ، مجلة الرسالة للدراسات والبحوث الانسانية (٨)٢ ،ص ١٨٩

وخصائصه، والاستراتيجيات الوطنية والدولية التي عملت عليها الدول والحكومات بهدف التصدي للحرب الإلكترونية لتحقيق أمنها السيبراني.

منهجية الدراسة :استخدمت الدراسة منهج الوصفي التحليلي ومنهج دراسة الحالة في دراسة الأوضاع الراهنة من حيث خصائصها وعلاقتها بالعوامل المؤثرة، كما استخدمت الدراسة أداة المقابلة بمقابلة عدد من الخبراء القانونيين والدوليين لدراسة الاستراتيجيات الدولية التي عملت عليها الحكومات بهدف التصدي للحرب السيبرانية.

نتائج الدراسة :

- أدت شمولية التهديدات الأمنية السيبرانية إلى قيام المجتمع الدولي بما فيه الدول والحكومات والمنظمات المختلفة، بالتعاون وتنسيق الجهود لابتكار ميكانيزمات مضادة من أجل التصدي للانعكاسات السلبية المصاحبة للحرب الإلكترونية .
- أكدت الدراسة أن الأمن القومي لأي دولة يرتبط ارتباطا وثيقاً بالأمن المعلوماتي لها وذلك يرجع إلى مختلف التهديدات التي يطرحها التطور التكنولوجي.
- إن الجريمة السيبرانية تتمثل في سرقة المعلومات والبيانات العسكرية وتدميرها في بعض الأحيان إن تتطلب الأمر.

٢- <u>دراسة قادي نور الهدى ،الجريمة السيبرانية وآليات مكافحتها: مواجهة تحديات الأمن السيبراني٢٠٢٣</u>[١]

هدف الدراسة: هدفت الدراسة إلى دارسة موضوع الجريمة السيبرانية باعتبارها من بين المواضيع القانونية الحديثة التي ظهرت تزامناً مع ظهور وانتشار الثورة التكنولوجية التي أثرت وبدرجة كبيرة على جميع مناحي الحياة الاقتصادية والاجتماعية والإدارية.

[١] - نور الهدى قادرى (٢٠٢٣) ،الجريمة السيبرانية وإلىات مكافحتها: مواجهة تحديات الأمن السيبرانى، المجلة الجزائرية للحقوق والعلوم السياسية ، مج ٨ ، ع ١ ،ص ٣٢١

ونظرًا لطابع الخصوصية التي تتميز بها الجرائم السيبرانية باعتبارها أنها من بين الجرائم التي يصعب اكتشافها وإثباتها أمام القضاء.

منهجية الدراسة :استخدمت الدراسة منهج تحليل المضمون باستخدام أداة تحليل المضمون لدراسة الأوضاع الراهنة من حيث خصائصها وإشكاليتها وعلاقتها بالعوامل المؤثرة، كما استخدمت الدراسة أداة تحليل المضمون لبعض الاستراتيجيات القانونية التي عملت عليها الحكومات بهدف التصدي للحرب الإلكترونية.

نتائج الدراسة: أكدت نتائج الدراسة أنه تتميز الجريمة السيبرانية بأنها يصعب اكتشافها وإثباتها أمام القضاء، كما أنها من الجرائم العابرة للحدود لاتعترف بالحدود الزمانية والمكانية.

- أكدت الدراسة أنه لاتوجد تسمية موحدة للجريمة السيبرانية، فهناك من يطلق عليها الجريمة الإلكترونية، وآخرون يطلقون عليها بانها الجريمة التي تتم عبر الإنترنت.
- أكدت الدراسة أنه لابد من تعزيز عنصر التعاون الدولي قضائياً وإجرائياَ في مجال مكافحة الجرائم المعلوماتية.

٣- دراسة ربيعي حسين وسمر محمود، الحروب السيبرانية – المخاطر واستراتيجيات تحقيق الأمن السيبراني الدولي والخارجي ٢٠٢٢[١]

هدف الدراسة : هدفت الدراسة إلى تحديد مفهوم الحرب السيبرانية كأحدث شكل من أشكال الحروب القائمة بين الدول داخل الفضاء السيبراني: الذي أصبح مصدر تهديد فعلي لأمن الدول و المجتمعات بصفة مشتركة و منفردة ، من خلال إتاحته لكل الأعمال العدائية ذات الطابع الإلكتروني ضد أي كان دون تمييز ، بالإضافة إلى

[١] - حسين ربيعى وأخرون (٢٠٢٢)، الحروب السيبرانية : المخاطر وإستراتيجيات تحقيق الأمن السيبرانى الدولى والخارجى، المجلة الجزائرية للأمن الانسانى ،مج ٧،ع ٢٢، ص ١٧٢

التطرق إلى الجهود الدولية التي تسعى إلى إرساء قواعد تحقق وتحافظ على الأمن السيبراني العالمي باعتباره إرثا مشتركاً.

منهجية الدراسة :استخدمت الدراسة منهج الوصفي التحليلي والاستقرائي،واعتمد الباحثان على مراجعة الأدبيات النظرية المتعلقة بالظاهرة، وجمع المعلومات والبيانات الدقيقة جداً عن الظاهرة ثمّ قاما بدراستها وتحليل هذه المعلومات، التي توصلهما إلى تفسيرات دقيقة وحلول منطقية.

نتائج الدراسة :

- توصلت الدراسة إلى أن الفضاء السيبراني هو أحد العناصر الاستراتيجية التي تعتمد في مجال تحقيق لأمن القومي نظراً لحجم التهديدات التي يحتويها
- كما توصلت الدراسة أن الحروب السيبرانية في مراحلها الأولى وصورها البسيطة ، يمكن أن تأول إلى أكثر حدة وخطورة مستقبلاً متعلق ذلك بدرجة التطور التي ستؤول إليها النظم المعلوماتية .
- كما توصلت نتائج الدراسة أيضاً أنه أغلب الدول العظمى أصبحت الدول المسيطرة في مجال العالمي عكس الدول النامية لا نجد لها أثراً في هذا المجال.

٤-دراسة **توب شولا أكينيتون ،الفقر والجرائم الإلكترونية والأمن القومي في نيجيريا ٢٠٢١**[1]

هدفت الدراسة إلى التعرف على الأبعاد الاجتماعية للجرائم الإلكترونية وتأثيرها على الأمن القومي النيجيري ، استخدمت الدراسة منهج المسح الاجتماعي على عينة من الشباب النيجيري بلغ عددهم ٣٠٠ مفردة من سن ٢٠-٣٥ عاماً.

1-Akinyetun, T. S. (2021). Poverty, Cybercrime and National Security in Nigeria. *Journal of Contemporary Sociological Issues*, *1*(2),p 86-109.

وتوصلت الدراسة إلى أن الفقر هو المحرك الرئيسي للجرائم السيبرانية في نيجيريا، وأن الجرائم السيبرانية تشكل تهديدًا خطيرًا للأمن القومي، ويظهر أنه مع انتشار الفقر والحرمان وعدم المساواة، يلجأ العديد من الشباب النيجيري إلى الجريمة الإلكترونية ، كما أن الجرائم الإلكترونية تقوض الأمن القومي من خلال تعريض الأفراد للعنف والتجسس الإلكتروني والمطاردة الإلكترونية والتلاعب.

٥-دراسة نورتون روز فولبريت ، الانتشار الفيروسي: تصاعد مخاطر الجرائم السيبرانية في ظل جائحة كوفيد -١٩ ،٢٠٢٠[1]

هدف الدراسة : هدفت الدراسة إلى الإجابة على التساؤل الآتي وهو كيف تسبب وباء مثل كوفيد -١٩ في تعرض الشركات لمزيد من المخاطر كعمليات كالاحتيال الإلكتروني ، والهجمات الإلكترونية ، والسلوك الاحتيالي .

منهجية الدراسة : استخدمت الدراسة منهج المسح الاجتماعي، باستخدام أداة الاستبيان على عينة من موظفي من بعض الشركات التي تعرضت للهجوم السيبراني في ظل جائحة كوفيد ١٩

نتائج الدراسة : توصلت نتائج الدراسة إلى أن :

- أن الجريمة السيبرانية تزداد بشكل مباشر عن طريق الإيميلات الإلكترونية وذلك بإرسال بعض الإيميلات الوهمية التي تحمل بعض الفيروسات التي تساعد على الاختراق .
- أنه نتيجة جائحة كوفيد ١٩ توقفت التعاملات المادية المباشرة وأصبحت عن طريق الإنترنت مما ساعد بعض المخترقين على اختراق بعض أنظمة الشركات للاستيلاء على أموالها.

1- NORTON ROSE FULBRIGHT . (2020) .Going Viral: Heightened Cyber and Corporate Crime Risks in the COVID-19 Pandemic. Norton Rose Fulbright,.p1:8

- توصلت الدراسة أيضاً إلى أنه ظهرت بعض البرامج تساعد على الاختراق مثل برامج الفدية والتي ساعدت المحترقين الوصول إلى بيانات العملاء بكل سهولة .

٦-دراسة أوفي في كتوريا آن ريتشاردسون ، الجريمة السيبرانية والأمن القومي : نيوزيلندا نموذجاً،٢٠١٥[1]

هدف الدراسة : هدفت الدراسة التعرف على العلاقة بين الجريمة الإلكترونية والأمن القومي التي أصبحت تتزايد مع تقدم التكنولوجيا ، خصوصاً أنها أصبحت المشكلة الرئيسية للقرن الحادي والعشرين ، وكذلك التعرف على التحديات المتعلقة بالإبلاغ والمقاضاة الجنائية للجرائم المتعلقة بالجرائم الإلكترونية .

استخدمت الدراسة أداة المقابلة باستخدام منهج دراسة الحالة على حالتين تعرضت لهم دولة نيوزيلندا وهم اختراق النظام الإلكتروني لشركة الاتصالات الوطنية النيوزيلندية ، وكذلك موقع الويب الخاص بالبرلمان النيوزيلندي .

توصلت نتائج الدراسة إلى أنه :

- لم يعد الهجوم العسكري هو الطريق الوحيد لتقويض أي أمة ، بل أصبح الهجوم الإلكتروني بديل للهجوم العسكري ، وأقل تكلفة ، ولايعرض أي دولة للخسائر في أرواح مواطنيه .
- أصبحت الصلة بين الجريمة الإلكترونية والأمن القومي سائدة بشكل متزايد، حيث طورت التكنولوجيا القدرة الجنائية على إحداث ضرر وإزعاج للأفراد وكذلك للبنية التحتية الحيوية للأمة من خلال تقويض أدواتها الحيوية والهجوم على الأنظمة الإلكترونية لأي مؤسسة.

1-Richardson, S. V. A., & Gilmour, N. (2015). Cybercrime and national security: A New Zealand perspective. *The European Review of Organised Crime (EROC)*, *1*(1), 51-70.

- مع زيادة الجرائم السيبرانية في نيوزيلندا ، اعتمدت نيوزيلندا الاستراتيجية الوطنية للأمن السيبراني عام ٢٠١١، وإدخال تشريعات وطنية على القانون النيوزيلندي لمحاسبة أي مرتكب لمثل هذه الأفعال.

رؤية نقدية للدراسات السابقة :

- لا يوجد إطار نظري شامل يساعد الباحثين في توصيف وتفسير تأثير الجريمة السيبرانية على الأمن القومي ، وبالتالي فقدت قدرتها على تقديم نتائج و تفسيرات شاملة ودقيقة حول تأثير الجريمة السيبرانية على الأمن القومي.
- عدم التركيز بشكل كافي على التدابير الوقائية والحماية: حيث ركزت بعض الدراسات على وصف الجريمة السيبرانية وتأثيرها على الأمن القومي ، ولم تركز على التدابير الوقائية والحماية التي يمكن اتخاذها للحد من الجريمة السيبرانية وتعزيز الأمن القومي.
- عدم توافر بيانات كافية : حيث كان من الصعوبة الوصول إلي بيانات كافية وموثوقة حول الجرائم السيبرانية وتأثيرها على الأمن القومي ، لأنه عادة توجد قيود فى التلبيغ عن الجرائم السيبرانية، ولايوجد نظام فعال لجمع البيانات الكافية حول مثل هذه الجرائم .
- يوجد إنحياز للعينة المستخدمة فى بعض الدراسات ، مما أدى إلى قلة تمثيل للعينة ، أو خصب العينة فى التهديدات السيبرانية التي تؤثر على الأمن القومي ، وذلك بسبب وجود قيود وصعوبة فى الوصول إلي بيانات حقيقة أو عينات ممثلة .
- قلة المصداقية والدقة : عانت بعض الدراسات السابقة فى حمع البيانات وتمثليها وتحليلها ، حيث كان هناك نقص فى تعريف نطاق الجربمة السيبرانية

بشكل صحيح مما أثر على استنتاجات صحة النتائج مثل دراسة(**دراسة نورتون روز فولبريت**).

نظريات الدراسة :

١- **نظرية تشكيل البنية لتحليل أركان وأبعاد الجريمة السيبرانية** تعد نظرية التشكيل البنائي لدى أنتوني جيدنز محاولة للتوفيق بين البنية والفعل في فهم المجتمع الإنساني ، حيث أن البناءات الاجتماعية تتأسس من خلال الفعل البشرى، فيؤمن جيدنز أن للفعل الاجتماعي أهمية بالغة في تشكيل البنية الاجتماعية، كما يعترف بالمقابل بدور البنية الاجتماعية في تغيير شكل الأفعال والممارسات وإعادة إنتاجها، فالأفراد يكونون المجتمعات، والمجتمعات بالمقابل تعيد إنتاج الأفراد من خلال الممارسات الاجتماعية المنتظمة عبر الزمان والمكان، فلابد من ضرورة الإقرار بأننا نحن الذين ننشط في صياغة البنية الاجتماعية وإعادة صياغتها في آن معًا من خلال التفكير والسلوك البشري، وهذا يعني أن المجتمعات الإنسانية في حالة مستمرة من التباين والتشكيل، وتعد فكرة النتائج غير المقصودة إحدى ركائز مدخل جيدنز، ويقصد بذلك أن أفعال الناس لها نتائج مقصودة بصفة مستمرة. وهذه النتائج تصبح شروط تلك الشروط غير معروفة للفعل وتغذية مرتدة، وتحول تلك الشروط دون جهود السيطرة عليها. ومع ذلك يبذل الفاعلون قصارى جهدهم بصفة مستمرة لوضع تلك النتائج غير المقصودة تحت السيطرة.[١]

فالعالم اليوم يمر بتغيرات متلاحقة ، حتى وقف المتخصصون في العلوم الإنسانية أمام هذه التغيرات وقفات متأنية لأنهم يدركون مدى تأثيرها على ثقافة المجتمع وأصبحوا يطلقون على هذه التغيرات مسميات باسم " عالم عدم " " مجتمع المخاطر" "

[١] - محمد حسام الدين (٢٠٢٠) نظرية التشكيل البنائي لدى أنتوني جيدنز (محاولة للتوفيق بين البنية والفعل في فهم المجتمع الإنساني) دراسة تحليلية – نقدية. .(مجلة العلوم الإنسانية و الإجتماعية.(7)4 ،، ص ص29-51

إمبرطورية الفوضى ، ونتج عن هذه التغييرات في ما يعرف بجيل المنصة ،وهو المصطلح الأكثر حداثة في سلسة تطور المجتمع الافتراضي.

ذلك المجتمع الذى ينطلق من فرضية أساسية مفادها أن مفهوم الثقافة_الرقمية بالشكل الحالي لا يستخدم بدقة، فالعديد ينظر إليه على أنه يتشكل من الممارسات التي يقوم بها الأفراد عبر وسائل التواصل الاجتماعي، إلا أن هذه المفاهيم تُحمل الثقافة ما لا تستوعبه، فالحقيقة لا توجد ثقافة رقمية واحدة في العالم الرقمي، وهو المدخل الذي يعتمد عليه التحليل الراهن في فهم ثقافة الشباب المصري في ظل العالم الرقمي، فلا يمكن أن ننظر إلى الثقافة الرقمية من منظور أنها ثقافة واحدة.[١]

تلك الثقافة التي يتقمص فيها الفرد شخصيته الافتراضية وتبدأ الذات الوهمية بالتضخم على حساب الذات الحقيقية ، وفي تلك الشخصية يستخدم الأنسان لغة الفرانكو وهو الأمر الذى ينذر باختفاء اللغة العربية وهي اللغة القومية للبلاد مما يؤثر على أمنها الاجتماعي وهو مؤشر على ضعف الانتماء واختفاء الهوية ، وتتمثل مخاطر الفضاء السيبراني أيضاً في المخدرات الرقمية التي أصبحت منتشرة في الوقت الحالي التي تؤثر على الذبذبات الطبيعية للدماغ ، كما يسمح الفضاء السيبراني للأفكار والمعتقدات المتطرفة سواء دينية أو سياسية بالانتشار في صور متعددة وماكرة ، بحيث يتم الترويج لها عبر بعض المواقع التي يرتادها الشباب ، مما يوقعهم في براثن هذه الأفكار الهدامة لبناء المجتمع ، وتصبح جزء من مكونهم الفكري والثقافي بحيث يتوجه سلوكهم إلى سلوك معادٍ للمجتمع ،ويأتي من مخاطر الفضاء السيبراني كذلك تنامي ظاهرة الإرهاب الإلكتروني حيث الهجوم على الحسابات والمواقع الإلكترونية ، والأنظمة المعلوماتية وهي هجمات تهدد حسابات الأفراد والشركات، وتصبح بياناتهم

[١] -زايد أحمد (٢٠٢٣) ، التحولات القيمية والثقافية فى المجتمع ..إلى أين ؟ ، تحرير ومراجعة شيرين جابر ، مكتبة الأسكندرية مركز الدراسات الأستراتيجية ، ص٥٩

عرضة للتسريب والتهديد والتلاعب مما يؤثر على أمنهم وسلامتهم الاجتماعية والأسرية والاًقتصادية مما يوضع السلامة الأمنية للبلاد على المحك ، ويصل مخاطر الفضاء السيبراني إلى ذروته عندما يطلع الشباب على ويعايشون تجارب حية للانتحار الأخرين مما يؤثر سلباً عليهم وهو مؤشر على تصدير أزمة ثقة .[١]

فحسب نظرية جيدنز أن البنية ليست معوق لأى فعل اجتماعي بل تشكله ، ولكن باعتبار أن الفاعل مشارك بشكل أساسي في إنتاج البنية ، حيث يقوم الفاعلون من خلال أنشطتهم الروتينية والمستمرة والمكررة نتيجة إحساسهم بأن العالم باقٍ على ما هو عليه ،وأن الأمور تسير بهذا الشكل نتيجة إحساسهم بالأمن الوجودي فكل تلك الممارسات تساهم في تشكيل البنية وكذلك تقوم البنية بتشكيلهم،لأننا الناس يتصرفون وفق أنماط سلوكية منتظمة حيث إنهم يعيشون في عالم اجتماعي له دلالاته الثقافية وظواهره الاجتماعية.[٢]

وفي ضوء ذلك هذه المقولات التي تنطلق منها نظرية تشكيل البنية عند جيدنز:

- أن البناءات الاجتماعية تتأسس من خلال الفعل البشرى، فيؤمن جيدنز أن للفعل الاجتماعي أهمية بالغة في تشكيل البنية الاجتماعية.
- أن البنية ليست معوق لأى فعل اجتماعي بل تشكله ، ولكن باعتبار أن الفاعل مشارك بشكل أساسي في إنتاج البنية.

ومما سبق نرى أن سلبيات المجتمع السيبراني وتأثيرها على بناء المجتمع والأمن القومي للبلاد تتمثل في تدنــي المستوى القيمي ، فالمحتويات غير المشروعة لها تأثير سلبي على أخلاقيات الشباب ،وعلى ارتفاع نسبة الممارسات الإجرامية

[١] - الصغير، أحمد حسين. (٢٠١٩). مخاطر المجتمع الافتراضي على الأبناء: دراسة نقدية .المجلة التربوية، ج٦٨ ، ص ص68 - 57

٢ - حسين، رامي محمد. (٢٠٢٣). نظرية التشكيل البنائي لدى أنتوني جيدنز: السياق - المفاهيم - الفرضيات الأساسية .مجلة كلية الآداب والعلوم الإنسانية، ع٤٥ ،ص 203

كالإباحية، والترويج للإرهاب والأفكار المتطرفة، وقضايا تمس الأمن القومي، وعليه لا بد من بناء مجتمع مدرك لمخاطر الفضاء السيبراني، قادر على التعامل مع هذه المخاطر ومدرك للعواقب التي يمكن أن تترتب على التعرض لسلامة الأفراد والمؤسسات بالبلاد.

٢-**نظرية مجتمع المخاطر:** منذ فجر التاريخ كان كل شيء يحدث باسم الأمن، حتى المغامرات التكنولوجية الكبرى، ومنها القنبلة النووية، كانت تتحقق من أجل الإنسان وأمنه، فكثيراً مامورسالعنف من أجل مناخ آمن، حتى الأسرة- هذه المنطقة التي تعد الأكثر أمنا وأماناً، يحيط بأفرادها أكثر أنواع العنف الرمزي قساوة وشدة ،فالخطاب الأمني في مجتمع المخاطر أصبح خبزا يومياً يروج له كسلعة استهلاكية وأصبح يقدم للإنسان على أساس أنه مصدر راحة وسعادة. [١]

فخطاب المخاطر العابر للقارات غير من سلوكيات الأفراد الذين اقتنعوا بأن المستقبل أصبح غير واضح ، وملئ بالتحديات التي تأتى من الأنسان لأخيه الأنسان نتيجة العدوان البشرى والذى أطلق عليه توامس هوبس " زمن الحرب الكل ضد الكل "، حيث أصبح مؤشر حساسية المخاطر يحتل مكانة أساسية في الخطاب الأمني والسياسي لعديد من الدول في جميع أنحاء العالم ، فأصبح العالم يعيش حالة من الخوف والقلق من بمايسمى من مخاطر المدينة ، والمجتمع الهش .[٢]

فالمشكلات الاجتماعية حينما تترك لفترة من الزمن دول حل ، ذلك من شأنه يجعل مشكلات أخرى تطفو على سطح المجتمع ، ومن ثم تعمل هذه المشكلات على

[١] -البوعزيزى محسن (٢٠١٧) ، تساؤلات حول صناعة الأمن والتهديدفى مجتمع المخاطر،مجلة الدراسات المالية والمصرفية ، الأكاديمية العربية للعلوم المالية والمصرفية ، مركز البحوث المالية والمصرفية ، مج ٢٥ ،ع ٢ ، ص ١

[٢] - الحسن ايت الحسن (٢٠٢١) ،مجتمع المخاطر – فوبيا – تحضر المخاطر، مجلة جيل للعلوم الانسانية والاجتماعية ، مركز جيل البحث العلمى ، ع ٧٥،ص ٥

استقرار وتماسك المجتمع ، في عمل ذلك على خطورة اجتماعية على الأمن الإنساني للبلاد[١]

فمعظم التغيرات التي حدثت في المجتمع يعتبر مصدرها العولمة وتكنولوجيا الاتصال، ولقد كان ذلك له تأثير– حيث عجزت منظومات القيم المجتمعية الضامنة للأمن عن احتواء أي تطرف أو سلوك إجرامي يرتكبه الفرد بسبب التقدم التكنولوجي ، فالإدراك الثقافي للمخاطرة وهو مصطلح هام في نظرية أولريش بيك عن مجتمع المخاطر و يقصد بهذا المصطلح أن لكل مجتمع نظرته وتقييمه للمخاطر التي تواجهه وكذا الدرجة التي يمنحها كل مجتمع للخطر، فقد تكون بعض المخاطر عند بعض المجتمعات كبيرة وصعبة ، حيث أنه تمخض عن مجتمع المخاطر مصطلحات حديثة، كمجتمع المعلومات، والمجتمع الرقمي، ذلك المجتمع الذى أوقع على البلاد ما يسمى المسؤولية الاحترازية المشتركة والهدف من ذلك هو كيف أن المجتمعات الحديثة تقاطع مخاطر التكنولوجيا وتحديد المسؤوليات الثقافية لكل فرد في المجتمع ومؤسساته حتى يمكن اتخاذ قرار بشأن سلوك أو قانون يحقق التغلب على أي اضطراب ممكن يحدث بسبب انعكاسية التحديث التي فرضها المجتمع الرقمي على الأفراد ، فمظاهر انعكاسية التحديث وماتحمله الثورة الرقمية يؤثر على الخصوصية الثقافية للأفراد وضرب للهوية الاجتماعية في مقتل ،فالتحليل السوسيولوجي لأى ظاهرة لابد أن ينبع من السياق الاجتماع والثقافي التي تتواجد فيه الظاهرة [٢]،حيث أن المخاطر تعتمد على القرارات التي يتم إنتاجها صناعيًا، وبهذا المعنى فهي انعكاس للنظم السياسية .[٣]

[١] -أحمد فيصل (٢٠١٥)، المخاطر الاجتماعية ، المعهد العربى للتخطيط، ، الكويت ، مج ١٣ ، ع ١٢٤، ص ٢

[٢] - مرابط أحلام (٢٠٢٣) ، تمثلات المخاطر بين التراث السوسيولوجي والخلفية الثقافية،مجلة آفاق للبحوث والدراسات، المركز الجامعى المقاوم الشيخ أمود بن مختار إيليزى ، مج ٦، ع ١، ص ص٣٧٩-٤٠٧

3-Beck, U. (1992). *Risk society: Towards a new modernity* (Vol. 17). sage.p.128

ومما سبق نرى أن الأمن القومي للبلاد يشهد مخاطر عديدة نتيجة الثورة الرقمية التي يشهدها المجتمع من خلال عدم الحفاظ على الخصوصية الثقافية للأفراد والاستيلاء على بعض المعلومات الرقمية للمؤسسات والأفراد ، فتستخدم الثورة الرقمية من قبيل الذكاء الاصطناعي لتتبع المشكلات الاجتماعية وتشخصيها والدفاع عن حقوق الأنسان، إلا أنه يمكن أيضاً استخدام هذه التكنولوجيا لانتهاك هذه الحقوق ،فنشأت دراسة المخاطر من الاحتياجات العملية للمجتمعات الصناعية لتنظيم التكنولوجيا وحماية مواطنيها من المخاطر الطبيعية والتكنولوجية.[١]

ماهية الأمن السيبراني وأنواع الجريمة السيبرانية : لقد تعرض المجتمع الإنساني طوال السنوات الماضية للمخاطر نتيجة لعملية التحديث التي عملت على تغير الأنظمة الاقتصادية والاجتماعية، كما أن النظرة المستقبلية للعلم والتكنولوجيا غير مستقرة فكثيرا ما تنجم عنها معرفة متناقضة حول وجود المخاطر المعاصرة وتركز على دراسة المخاطر الناتجة عن التهديدات التكنولوجية ،فلابد من الدراسة والتحليل لتلك المفاهيم واستنباط ما يفيد الأمن القومي للبلاد ،لأن الأمن القومي لأي دولة له أبعاد ممتدة عبر الحدود الدولية والقارية:

١-**ماهية الأمن السيبراني** :هو كل الممارسات التقنية التي تقوم بحماية الشبكات والأجهزة والمعلومات من أي نوع من أنواع الاختراقات أو الهجمات الإلكترونية ومع تطور طرق الاختراق والهجمات الإلكترونية أصبح من الضروري أن تتطور كذلك وسائل الحماية ضد هذه الهجمات.[٢]

1- Traulsen, Janine & Bissell, Paul. (2010). (7) The risk society. International Journal of Pharmacy Practice. 11. P. 251 - 258

2- Salih, Azar & Abdulrazzaq, Maiwan. (2023). Cyber security: performance analysis and challenges for cyber attacks detection. Indonesian Journal of Electrical .Engineering and Computer Science. 31. p1763.

٢-**أنواع الجرائم السيبرانية:** تستخدم الهندسة الاجتماعية أشكال عديدة في الحصول على المعلومات الحساسة والبيانات الشخصية، كما تعتمد هذه الأساليب على استغلال الجوانب النفسية والاجتماعية للأفراد والتلاعب بهم، وقد يظهر الأشخاص الاختلافات بين سلوكهم في الفضاء السيبراني بالمقارنة مع سلوكهم في العالم المادي، ويرتكبون بعض الجرائم ما يرتكبوها في الحيِّز المادي بحكم وضعهم ومكانتهم، ومن بين أنواع الهندسة الاجتماعية الشائعة في ارتكاب الجرائم السيبرانية :

أ-**الجريمة المادية:**تتم من خلال أضرار مادية تقع على المستهدف من عمليات النصب التي تتم ومنها السرقة الإلكترونية كالاستيلاء على ماكينات الصرف الآلي والبنوك، وإنشاء صفحة إنترنت مماثلة لموقع أحد البنوك الكبرى، والرسائل البريدية الواردة من مصادر مجهولة بخصوص طلب المساهمة في تحرير الأموال من الخارج مع الوعد بنسبة من المبلغ.[١]

ب- الجريمة الثقافية: تتم من خلال استيلاء المجرم على الحقوق الفكرية ونسبتها له بدون موافقة الضحية مثل قرصنة البرمجيات من خلال نسخ لبرامج إحدى الشركات العالمية على أسطوانات وبيعها للناس بسعر أقل، وكذا التعدي على القنوات الفضائية بالإضافة لجريمة نسخ المؤلفات العلمية والأدبية.

ج-الجريمة السياسية الاقتصادية: تستخدم المجموعات الإرهابية الاتصالات وبث الأخبار المغلوطة، وتحويل بعض الأموال مع الاستيلاء على المواقع الحساسة وسرقة المعلومات ونشر الفيروسات والأفكار الخاطئة بين الشباب.[٢]

1- Osman Goni, Md. Haidar Ali, Showrov, Md. Mahbub Alam, & Md. Abu Shameem. (2022). The Basic Concept of Cyber Crime. Journal of Technology Innovations and Energy, 1(2),p 29

2- جاب الله، حكيمة. (٢٠٢١). انعكاسات الجريمة السيبرانية على البيئة الرقمية: دراسة في إلمات واستراتيجيات مكافحتها .حوليات جامعة الجزائر ١، مج٣٥، ع٣ ، ص 649

د-الجريمة الجنسية: تشمل الابتزاز والتغرير والاستدراج ،وهي من أهم الجرائم التي انتشرت بشكل كبير في البيئة الرقمية كانت نتيجة انتشار التطبيقات التكنولوجية المختلفة بالإضافة للبعد الإنساني، فتفاعل الإنسان مع هذه الآليات الجديدة أوجد مشكلات وجرائم لم تكن معروفة من قبل فالإقبال الكبير على استخدام التكنولوجيات الحديثة بشكل عام و الإنترنت بشكل خاص أدى لبروز مظاهر تميز البيئة الرقمية منها التحديات الفكرية والاجتماعية والإعلامية والسياسية والاقتصادية.[١]

أسباب انتشار الجريمة السيبرانية: مع انتشار شبكة الإنترنت وأصبح الفضاء السيبراني لبعض الدول من الصعب السيطرة عليه، أصبحت أجهزة المخابرات كل دولة تسعى لاستغلال هذه الشبكات في حروبها الدولية بواسطة التغلغل في ها والسيطرة عليها أو تعطيلها أو نفي البيانات أو إتلافها أو التحكم فيها لإخضاع دولة العدو رغبة الفرد التشهير بالآخرين أو غيرها من الأسباب تشمل

أولاً: الدوافع السياسية : يصعب في الفضاء السيبراني تحديد هوية مرتكبي الجريمة السيبرانية في أغلب الهجمات الإلكترونية ، وبخاصة إذا ما اتسمت بدرجة عالية من التعقيد. فكلما زادت درجة تعقيد الهجوم الإلكتروني، زادت صعوبة تحديد هوية مرتكبي الجريمة ، و تحديد الدوافع الكامنة وراءه، لذلك نجد أن كافة الدول التي وجهت إليها اتهامات بشن هجمات الكترونية كروسيا في حالتي استونيا و جورجيا، و الولايات المتحدة واسرائيل في حالة ستاكنست، قد نفت تمامًا أية صلة لها بتلك الهجمات حيث عجزت الدولة المتعرضة للهجوم عن تقديم أدلة تثبن إدانة أي دولة بعينها أو تحميلها المسؤولية ونتيجة لذلك تستطيع الدول أن تحقق أهدافها السياسية باستخدام الأسلحة الإلكترونية بدلاً من القوى العسكرية.[٢]

[١] هلال منال .(٢٠١٤) تكنولوجيا الاتصال والمعلومات، ط١ ،دار أسامة، الأردن،ص .٣٧٤

[٢] -عدنان بهاء(٢٠١٩) ،انتقال التهديدات من الواقع إلى العالم الأفتراضى ،مجلة جامعة بابل للعلوم الأنسانية ، العراق ،مج ٢٧،ع ٤، ص ٤٧٦

ثانياً: الدوافع الفكرية والمادية :.تتمثل هذه الدوافع في المتعة والرغبة في إثبات الذات وفهم القرصنة حيث تكون هذه الدوافع مجرد شغف قد يكون لحظي لتسلية وقت الفراغ لدى بعض الشباب، حيث يميل بعض الشباب إلى القرصنة والرغبة في ارتكاب هذه الجرائم بدافع الرغبة في إظهار تفوقهم على وسائل التكنولوجيا الحديثة[١] ،وقد تدفع حاجة البعض إلى تحقيق الثراء السريع عن طريق إتاحة الاطلاع على معلومات معينة أساسية ذات أهمية خاصة لمن يطلبها. [٢]

رابعاً: الدوافع الاجتماعية والاقتصادية : يحدث السلوك الإجرامي نتيجة الصراعات النفسية والاجتماعية التي تحدث بسبب الفشل والإحباط وعدم تحقيق الأهداف في الحياة فتتفاعل هذه العوامل مع الحياة الاجتماعية التي يعيشها الأنسان فينتج عنها فرد مضطرب نفسياً واجتماعيا ، ومن بين العوامل التي لها دور مهم في ارتكاب الفرد لأى جريمة البطالة ،والفقر ،والتهميش السياسي والاجتماعي ، حيث إن الفرد يشعر بعدم الأمان لعدم وجود دخل ثابت يوفر له حياة كريمة، حيث أن المتغيرات الاقتصادية والأزمات التي يعيشها المجتمع لها تأثير مباشر على حياة وسلوك الفرد داخل المجتمع ، كما أن تفكك الروابط الأسرية أيضا لهاً دخل مباشر في ذلك لعدم وجود رقابة في بعض من الأحيان من الآباء على الأبناء ،[٣] وفي هذا السياق تأتي

[١] - محمد على وفاء (٢٠٢١). الأبعاد الاجتماعية للجرائم الإلكترونية: دراسة تحليلية لمضمون عينة من القضايا في محكمة سوهاج .مجلة كلية التربية في العلوم الإنسانية والأدبية، مج٢٧، ع٣ ،ص ٤٥٤

[٢] - طعبة سعاد(٢٠٢٢) ،الجريمة الألكترونية :تفعيل لإلبات القانون من أجل تحقيق العدالة ،مجلة الحقوق والعلوم الانسانية ، مجلة الحقوق والعلوم الانسانية، ١٥(٣) ، ص ٢٢٩

[٣] - العطيان، تركي بن محمد. (٢٠٠٦). البطالة وعلاقتها بالسلوك الإجرامي: دراسة نظرية على المجتمع السعودي .المجلة العربية للدراسات الأمنية، مج ٢١، ع ٤١ ، .403 - 341

العولمة كعامل رئيسي أيضاَ في ارتكاب الفرد لأى جريمة، حيث خلقت العولمة جيلاً جديداً من الجرائم الإلكترونية عابرة للقارات تعتمد على تكنولوجيا الشبكات .[١]

المخاطر الاجتماعية للجريمة السيبرانية وتأثيرها على الأمن القومي المصري : إن تطور الأمن القومي أفرز أبعاداَ وتحديات جديدة للمفهوم، حيث أفرزت هذه التحديات العديد من التهديدات ومن بين هذه التهديدات أصبح التهديد الإلكتروني واحداً من أهم التحديات.

فالتهديد الإلكتروني أصبح يؤثر بقوة على الأمن القومي للدول _على الأقل_ في الوقت الراهن، إذا أصبحت السياسات الأمنية للدول تتضمن التركيز على مفاهيم أمنية جديدة مثل: الحرب الإلكترونية ، الجريمة السيبرانية ، جرائم الإنترنت، القرصنة الإلكترونية . اختراق الأجهزة القومية للمؤسسات العسكرية، وتهديد القيم والأخلاق، وتصدير أزمة عدم ثقة لجيل ومجتمع **كامل**[٢]**،ونتناول المخاطر الاجتماعية فيما يلى:**

١- **زيادة معدل الجرائم السيبرانية وتحديات الأمن السيبراني :**

لقد أحدثت شبكة الإنترنت وأجهزة الكمبيوتر والهواتف المحمولة وغيرها من أشكال التكنولوجيا ثورة في كل جانب من جوانب الحياة البشرية على مدى العقود العديدة الماضية، بما في ذلك كيفية التواصل، وإجراء المعاملات المصرفية عبر الإنترنت، والتسوق، والحصول على الأخبار والترفيه ، وقد خلقت هذه التطورات التكنولوجية أيضًا فرصًا لا تعد ولا تحصى للمجرمين لارتكاب أشكال مختلفة من الجريمة السيبرانية ،وغالبًا ما يشار إلى الجرائم عبر الإنترنت على أنها جرائم إلكترونية[٣] ، حيث تمتاز

1-Chareonwongsak, K. (2002). Globalization and technology: how will they change society?. *Technology in Society*, *24*(3),p 191.

[٢] - عجيل فاطمة. (٢٠١٩) ، التهديدات الإلكترونية والأمن القومى ، جامعة محمد بوضياف ، رسالة ماجستير منشورة ، الجزائر، ص ٢

3-Bossler, A. M., & Berenblum, T. (2019). Introduction: new directions in cybercrime research. *Journal of Crime and Justice*, *42*(5),p 495-499.

الجرائم السيبرانية بخصوصيات تميزها عن غيرها من الجرائم حيث أنها ترتكب في بيئة افتراضية ولاتترك أثراً ماديًا، ويمكن أن يؤدى ذلك في سقوط بيانات أي دولة في الدول المعادية لها [١].

ومن أبرز الأمثلة الدالة على ذلك هجوم الفدية الذى وصفته وزارة العدل الأمريكية بأنه نموذج عمل جديد للجريمة السيبرانية وتشير التقارير الدولية إلى أن فيروس الفدية تسبب في خسائر مالية تفوق الخمسة مليارات دولار أثناء عام ٢٠١٧ ومن أمثلة الهجوم الإلكتروني ما أصاب شبكة الكهرباء الأوكرانية والذى تسبب في بقاء أُوكرانيا لساعات في الظلام. وبذا، تخطت الحروب الإلكترونية والهجمات السيبرانية حاجز البيانات والمعلومات والمواقع الإلكترونية لتصل للبنية التحتية والأنظمة الحيوية مثل المفاعلات النووية وأنظمة الكهرباء والأنظمة الطبية والنقل وغيرها من القطاعات التي تُعد ركائز أساسية للدول مثل الهجوم السيبراني التي حدث لشركة أرامكو السعودية حيث كلفها تغيير ٥٠ألف قرص صلب لأجهزتها الحاسوبية، ولم تستطع استخدام الإنترنت لمدة خمسة أشهر تقريبا مما يرفع مستوى الخطورة على الدول ومن أشهر الاختراقات أيضًا، ما حدث من سرقة حسابات شركة ياهو حيث بلغ عدد الحسابات المسروقة ثلاثة مليارات حساب، وكذلك اختراق إكيفاكس في عام ٢٠١٧حيث تأثر ٥،١٤٥مليون عميل، ومما يزيد الأمر تعقيداً، ظهور ما يسمى بالويب العميق والمعروف باسم الويب المظلم وهي شبكة خفية تستخدم في تعزيز الأنشطة الإجرامية الشنيعة [٢] ، وذلك يتطلب وضع النصوص القانونية لمواجهة مثل ذلك الجرائم المستحدثة فكان وضع النصوص القانونية كان وليد جدل فقهي بحيث

1- Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. *International journal of engineering sciences & Emerging technologies*, *6*(2), p142

[٢] - فوزى إسلام (٢٠١٩)، الامن السيبرانى : الأبعاد الأجتماعية والقانونية : تحليل سيوسولوجى ، مرجع سابق ، ص ١١٠

تشمل القوانين هذه القيم من الجرائم المستحدثة [١] ، فتولد أمام الدول بما يسمى بتحديات الأمن السيبراني وهي كالتالي:

- **التجسس والقرصنة السيبرانية:** وغالبًا ما يستهدفان المؤسسات والشركات وفي حالات نادرة بعض المؤسسات الحكومية القيام بعمليات قرصنه المواقع من خلال إغراقها بالبيانات الإلكترونية ، أو تعطيل الحواسيب الخادمة.[٢]
- **الإرهاب السيبراني:** ويقع في المستوى الثالث ويعبر عن الهجمات غير الشرعية التي ينفذها فاعلون غير حكوميون ضد أجهزة الكمبيوتر والشبكات والمعلومات المخزنة.
- **الحرب السيبرانية:** وهي المستوي الأخطر للنزاع في الفضاء السيبراني وتهدف التأثير علي الإرادة السياسية للهدف المستهدف،وكذلك التأثير في ما يتعلق بالقيادة العسكرية ، فالدول النامية تعانى من معضلة حماية سيادتها وتأمين حدودها وخاصة الافتراضية- وفي هذا الإطار يعتبر الفضاء الافتراضي (السيبيراني) أحد أهم العوامل المؤثرة في بناء منظومة الأمن بالنسبة للدولة؛ لما يشكله من مجال مفتوح لتزايد التهديدات وانعدام الاستقرار.[٣]

٢-**استهداف الأمن القومي وتدمير البنية التحتية للدولة** :يفضل التقدم التكنولوجي في السنوات الأخيرة، أصبحت البنية التحتية الحيوية أكثر أهمية في الحياة الاجتماعية الحديثة، وتعد الإدارة الآمنة والفعالة للبنية التحتية علامة على التطور الاجتماعي للدولة، فضمان أمن البنية التحتية لأى دولة أمر ضروري للأمن القومي، حيث أصبح

١ -بن علية بن جدو(٢٠٢٢)، تحديات الأمن السيبرانى لمواجهة الجريمة الألكترونية ، المجلة الجزائرية للامن الأنسانى ، مج٧،ع ٢، ص ٣٠٥

2 –محارب محمد.(٢٠١٣) ،حرب في الفضاء الالكتروني:اتجاهات وتاثيرات علي اسرائيل ، ،نابلس،العراق ،ص٨٦

3- إسماعيل عبد الكريم .(٢٠٢٢) ،تأثير الفضاء الأفتراضى على الأمن القومى ، مجلة البحوث والدراسات ، جامعة قاصدى مرباح ، الجزائر، مج١٩،ع١، ص ١٤٤

الاعتماد على الشبكة العنكبوتية من أي وقت مضى أمر ضروري لابد منه ، ويعتمد أمن البنية التحتية بشكل كبير على تقنيات الشبكات؛ وبناءً على ذلك، فإن توفير الأمن السيبراني للبنية التحتية الحيوية للدولة يعد مرادفًا للأمن القومي، فحماية البنية التحتية ومكافحة الهجمات السيبرانية أمر بالغ الأهمية للحفاظ على الحياة اليومية، لأنه يضمن توفير الخدمات العامة والأساسية [١]

فالحديث عن توزيع المقدرات الاقتصادية في الفضاء السيبراني، أمرا يرتبط بتدفقات البيانات كأساس للاقتصاد العالمي، ومع التسارع الحالي لرقمنة المؤسسات العالمية، مدعومًا بالاعتماد السريع للتقنيات المتطورة مثل تلك الخاصة بالحوسبة السحابية وتحليلات البيانات، زادت أهمية البيانات كمدخل للصناعات، وهذا ليس فقط لصناعات المعلومات، ولكن أيضًا للصناعات التحويلية والتقليدية الأخرى. فيرتبط توزيع المقدرات الاقتصادية على الساحة الدولية بامتلاك البيانات. هذا ويرتبط استخدام الإنترنت ارتباطًا وثيقًا بالتنمية الاقتصادية، فارتفاع معدل انتشار الإنترنت إلى حد كبير يرجع إلى مجموعة من مقاييس النجاح الاقتصادي، فتحقيق الوصول الشامل لا يتطلب إصلاحات في قطاع الاتصالات فحسب، بل يتطلب أيضًا سياسات لمساعدة الأفراد والشركات على تحقيق أقصى استفادة من الإنترنت.

ومن ثم فهناك علاقة بين شبكة المعلومات الدولية والتنمية الاقتصادية، فالاقتصاد الرقمي قد يكون مدخلا لبناء قوى اقتصادية كبيرة لبعض الكيانات الدولية الفاعلة؛ كالدول، والشركات متعددة الجنسيات، والمنظمات الدولية الحكومية وغير الحكومية، في ظل بنية معلوماتية تستند عليها بنية الاقتصادات الرقمية، وفي المقابل هي ساحة لزيادة القدرات الاقتصادية لوسطاء الظل والجماعات الإرهابية عبر الإنترنت المظلم وفي ظل سرية المقدرات السيبرانية، لا يمكن الوقوف على التوزيع الكلي للموارد

1- Daricili, A. B., & Celik, S. (2022). National Security 2.0: The Cyber Security of Critical Infrastructure. *PERCEPTIONS: Journal of International Affairs*, *26*(2), 259-276.

الاقتصادية للفاعلين على مستوى النظام الدولي، فيوفر الفضاء السيبراني منصات وفرص اقتصادية ممتازة لتنمية اقتصاديات الوحدات الفاعلة في النظام الدولي عبر ساحة الاقتصاد الرقمي، وما يوفره من سد الفجوات في التنقل والتجارة والابتكارات والتمكين الاقتصادي، والحد من الفقر، فساعد الفضاء السيبراني على دعم تغير بنية النظام الدولي، عبر تغير هيكل توزيع القوى بمعناها التقليدي، فبالنظر للنظام الدولي الحالي الذي تهيمن عليه الولايات المتحدة الأمريكية كقوى عظمى وحيدة في العالم، يمكن القول أنها لم تعد قادرة على القيادة داخل الفضاء السيبراني رغم ما تمتلكه من مقدرات عسكرية هائلة. فتتعرض الولايات المتحدة الأمريكية إلى هجمات سيبرانية متكررة تمثل تهديدا لأمنها القومي، بل وتحديًا كبيرًا أمام صانع القرار الأمريكي.[١]

ففي ظل اهتمام الإدارات الأمريكية المتلاحقة بالتسليح والاهتمام بالتفوق العسكري، كان الأمن السيبراني محل جدلاً فيري آدامز أن "التفوق العسكري الساحق والميزة الرائدة في تكنولوجيا المعلومات، جعلت الولايات المتحدة الدولة الأكثر عرضة للهجمات الإلكترونية "، كالهجوم الذي تعرضت له الولايات المتحدة الأمريكية عام ١٩٩٨ فقد تعرضت لسرقة الأف المستندات السرية والعقود والتشفير والمواد الحساسة، ولم تسفر التحقيقات التي امتدت على مدار خمسة سنوات إلا عن تحديد عناوين بروتوكول الإنترنتIP لأجهزة الحاسوب التي قامت بالهجمة، وتم تحديد هويتها الروسية، ولكن دون إمكانية إدانة الدولة الروسية فمن غير الواضح ما إذا كانت هذه الهجمات ترعاها الدولة، لكن الحكومة الأمريكية لم تستطع التأكد من براءة روسيا، مما أدى إلى مزيد من عدم الثقة والشك، وفي ١٣ ديسمبر ٢٠٢٠ تعرضت ما لا يقل عن ٦ وكالات حكومية أمريكية للاختراق بفعل برنامج خبيث أصاب آلاف الشركات فيما

[١] - جمال الدين، هبة. (٢٠٢٣). الأمن السيبراني والتحول في النظام الدولي. *مجلة كلية الاقتصاد والعلوم السياسية*، ٢٤ (١)، ص ص ١٨٩-٢٣٠.

يبدو أنها واحدة من أكبر عمليات الاختراق التي تم الكشف عنها، حيث استطاع متسللين النفاذ إلى البريد الإلكتروني الخاص بوزارتي الخزانة، والتجارة الأمريكيتين مما سبب مشاكل كثيرة تخطت حدود الدولة الامريكية ذاتها. [١]

وخلال ماسبق يمكن أن نجد أن كل المؤسسات والمنظمات تبنت استراتيجية "العمل من المنزل" بين عشيةٍ وضحاها، بسبب جائحة كورنا "كوفيد -١٩" وما سببته من حدوث اضطراب غير مسبوق، وتغيير لاحق على الصعيد العالمي، ودون إشعار مسبق، تحول ٩٦٪ من الموظفين إلى العمل الكامل من المنزل مقارنةً بنسبة ٤% فقط من الموظفين قبل أن تبدأ جائحة كورونا "كوفيد-١٩"، وخلال تلك الفترة واجه مسؤولي تكنولوجيا أمن المعلومات العديد من التحديات الهائلة في مهمتهم لتوفير روابط آمنة للقوى العاملة المشتتة مع الحفاظ على الحماية الكافية ضد الهجمات الإلكترونية [٢] ،فالتعامل مع هذه التحديات يتطلب مرونة تامة لأن هذه التحديات تدمر البنية التحتية لأى دولة لأن التهديد الإلكتروني والجريمة السيبرانية له عدة خصائص وأشكال من أهمها :

أ- **<u>أشكال الجرائم السيبرانية والتهديد الإلكتروني :</u>**

- التجنيد والتبعية والدعاية والإعلان وجمع التمويل.
- تهديد البنية الإلكترونية للدول وتعطل شبكة الاتصال.
- مهاجمة نظم التحكم في الطيران لإحداث تصادم سواء بالطائرات ،أو قطارات السكك الحديدية.
- التلاعب بالبيانات الشخصية وتهديد أمن المواطنين
- تعطيل البنوك وعمليات التحويل المإلى .

١- المرجع السابق، ص ص ١٨٩-٢٣٠.

2-Tonge, A. M., Kasture, S. S., & Chaudhari, S. R. (2013). Cyber security: challenges for society-literature review. *IOSR Journal of computer Engineering*, *2*(12),p 67-75.

- تعديل ضغط الغاز عن بعد لضغط أنابيب الغاز لتعطيلها.
- التلاعب في نظم السلامة للمصانع الكيماوية لإحداث أضرار كارثية بالمواطنين.
- السيطرة على شبكات الربط الكهربائي المتصلة بالإنترنت عبر الأنظمة

ب- خصائص الجريمة السيبرانية والتهديد الإلكتروني :تتطور الجريمة السيبرانية بوتيرة غير مسبوقة وعادة ما تسمى بالجرائم الناعمة لأن مرتكبيها يتميزون بخصائص عديدة منها :

- أن الإرهاب الإلكتروني لايحتاج إلى عنف ولكن مايتطلبه هو حاسب شخصى متصل بالإنترنت
- صعوبة اكتشاف مرتكبي الجرائم الإلكترونية نظراً لتغيير عنوان IP Address الخاص بهم.
- أن مرتكبي الجريمة عادة مايكونون في غاية الثقافة في المجال ذاته .
- أن الإرهاب الإلكتروني ومرتكبى الجريمة السيبرانية عادة مايكونون عابرين للقارات ،ولا يكونون مقتصرين على دول بعينها .[١]

يتضح مماسبق أن لابد للدولة أن تتخذ إجراءات جادة لحماية أمنها السيبراني ضد أي عدو لأن الأمن السيبراني أشمل وأعم من أمن المعلومات ، فالأمن السيبراني يعد اللبنة الأساسية ودعامة من دعائم الأمن القومي الذى يضمن إستقرار المجتمعات ، والحفاظ على وجودها فلابد من أن الدولة تشرع بعض القوانين التي تدخل في سياقها أي تطور للجريمة يضمن التصدي لمرتكبي مثل هذه الجرائم .

حيث أن الاعتماد الكبير للدول والمحتمعات على التطبيقات والتقنيات الرقمية السيبرانية في كافة المجالات ، وضع كافة مقومات الأمن القومي لأى دولة في سلسة التنقيات

[١] - عجيل فاطمة. (٢٠١٩) ، التهديدات الإلكترونية والأمن القومى ، مرجع سابق ص ص ١٠٥-١٠٧

السيبرانية ووسطائها الذكية والمتطورة ، فلابد من توفير كافة التدابير الوقائية ضد أي هجوم سيبراني، تكون هذه التدابير قائمة على الأتفاقيات الدولية ، والقوانين الوطنية .[١]

٣-تهديد القيم الاجتماعية وتصدير أزمة عدم الثقة بين المواطنين :

لاشك أن العولمة ظاهرة العصر وسمته ، والوقوف في وجهها ومحاولة تجنبها والعزلة عنها إنما هو خروج على العصر وتخلف وراءه ، فمسايرة ومواكبة التحولات والتغيرات الاجتماعية والاقتصادية أمر لابد منه [٢].

فانهيار القيم الاجتماعية مسألة هامة في علم الاجتماع لأنها عنصر أساسي في بناء المجتمع وموجه أساسي لسلوك أعضاءه لأنها تحقق وحدة الفكر داخل المجتمع ،فوسائل الإعلام لها قدرة هائلة في التأثير على مختلف شرائح المجتمع ، والعمل على تغيير قيمهم فتقنيات الأتصال المتطورة تشكل أهم إلىات العولمة في تنمية القيم، وتكريس منظومة قيمية معينة.[٣]

حيث أن معظم البلدان الصناعية كانت نهاية الحرب الباردة بالنسبة لهم بمثابة تغيير في التركيز من الاستعداد للحرب إلى التركيز المتزايد على ضعف المجتمع المدني وسلامته، ولمواجهة التهديدات الجديدة والمخاطر المتغيرة، كان هناك حاجة إلى مفاهيم تحليلية جديدة كالسلامة المجتمعية وهو مفهوم يمكن تعريفه بأنه: "قدرة المجتمع على الحفاظ على الوظائف الاجتماعية الحيوية، وحماية حياة وصحة المواطنين وتلبية متطلبات المواطنين الأساسية في مجموعة متنوعة من حالات التوتر". ويهدف إلى أن

[١] - مصطفى أحمد(٢٠٢٢) ، دمج الأمن السبيرانى فى منظومة الأمن القومى : الأمن السبيرانى والأمن القومى، مجلة إدارة الاعمال ، جمعية إدارة الأعمال العربية ، مصر ،ع ١٧٨ ، ص ص ٥٠-٥٢

[1]- تريكي، حسان(٢٠١٥)، "عولمة الجريمة: الواقع والتحديات الأمنية الجديدة."مجلة دراسات وأبحاث ع١٩،ص ٧٠

[٣] توانا فريدون حسين، & أمير خداكرم محمد. (٢٠٢٣). العولمة الثقافية وعلاقتها بالقيم الاجتماعية من منظور أساتذة الجامعة دراسة ميدانية في جامعة السليمانية. *مجلة جامعة بابل للعلوم الانسانية*، ٣١ (٢)، ص ص ١-١٨.

يكون نهجًا منظمًا لفهم المشكلات الاجتماعية والتخفيف منها والاستجابة لها مثل الضغوط والخسائر غير العادية، أو التدخلات في الأنظمة المعقدة والمعتمدة على بعضها البعض، أو انعدام الثقة في المؤسسات الاجتماعية الحيوية.

ولا تقتصر التهديدات المستقبلية للمجتمع على قطاعات أو مجالات محددة، ولكنها تنبع من التفاعلات المعقدة بين العوامل الاقتصادية والتكنولوجية والاجتماعية والثقافية،وبالتإلى فإن التحديات الرئيسية لتحسين السلامة المجتمعية ستكون القدرة على تنسيق وتنظيم وتعيين أدوار واضحة لمختلف الجهات الفاعلة على المستويات الدولية والوطنية والمحلية، وترتبط السلامة المجتمعية بمجالات أخرى متعلقة مثل الأمن القومي والتنمية المستدامة والأمن البشري وإدارة الحوادث ومع ذلك، فإن السلامة المجتمعية هي قضية سياسية حساسة تحتوي على معضلات وخيارات قيمية يصعب تصورها أو حلها على أنها مشكلات علمية بحتة.[١]

يتضح من مماسبق أن أهم القيم الاجتماعية التي تصدرها الجريمة السيبرانية على السطح ومن شأنها تصدير أزمة عدم الثقة بين الأفراد: الفضول، والتقليد الأعمى لدى بعض الشباب، وضعف الرقابة الأسرية، وانبهار المجرمين بالتقنية الحديثة، وانتهاك الخصوصية .

حيث أظهرت نتائج بعض الدراسات أن من أهم المعوقات التي تحد من فاعلية مواجهة الجرائم الإلكترونية هي: سهولة محو الدليل أو تدميره في زمن قصير جداً، وقلة المتخصصين الجنائيين في مجال الجرائم الإلكترونية، وقلة خبرة المحققين في هذا المجال، وضعف وعي المواطنين بالطرق السليمة والآمنة عند استخدام الحاسوب، ومن أهم الحلول المقترحة لمواجهة مثل هذه الجرائم الإلكترونية هي: الرقابة الأسرية

[1]- Olsen, O. E., Kruke, B. I., & Hovden, J. (2007). Societal safety: Concept, borders and dilemmas. *Journal of contingencies and crisis management*, *15*(2)p, 69-79 .

والمجتمعية ، والحرص على تحديث أنظمة الحماية، والامتناع عن تنزيل أي ملف من مصادر غير معروفة، وعدم الإفصاح عن كلمة السر، وإصدار قانون رادع للجميع.[١]

استراتيجية جمهورية مصر العربية في مواجهة الجريمة السيبرانية وأمن المعلومات

:في إطار جهود الدولة لدعم الأمن القومي وتنمية المجتمع المصرى ووفقًا للمادة ٣١ من الدستور المصري التي تنص على أن أمن الفضاء المعلوماتي جزء أساسي من الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه ، على النحو الذى ينظمه القانون " ، ومع تزايد التهديدات والتحديات المستقبلية في المجال السيبراني والمجتمع الرقمي ولرصد ومجابهة المخاطر والتهديدات المتزايدة، وإنطلاقًا من الأهداف التي دعت إلي إنشاء المجلس الأعلى لتأمين البني التحتية للاتصالات والمعلومات (المجلس الأعلى للأمن السيبراني ، تم إعداد وثيقة تتضمن عددا من البرامج التي تدعم الأهداف الاستراتيجية للأمن السيبراني، كما توضح توزيع الأدوار بين الجهات الحكومية والقطاع الخاص ومؤسسات الأعمال والمجتمع المدني وما ستقوم به الدولة من إجراءات للتقدم نحو تحقيق تلك الأهداف ، بما يدعم التحول نحو اقتصاد رقمي متكامل يحقق طموحات المواطنين في تنمية اجتماعية واقتصادية شاملة ويحمي مصالحهم، ويحافظ علي مصالح الدولة العليا ويسهم في نهضتها وازدهارها ورخائها[٢]

١-الجنفاوي، خ. م.، & خالد مخلف. (٢٠٢٠). العوامل المؤدية للعودة إلى الجريمة وفقاً لتوجهات العاملين في أقسام الخدمة الاجتماعية في المؤسسات الإصلاحية في الكويت. *مجلة كلية الخدمة الاجتماعية للدراسات والبحوث الاجتماعية*، *١٨* (العدد ١٨ الجزء الثانى)، ص ص ١٥-٥٢.

٢ - مركز المعلومات ودعم إتخاذ القرار (٢٠٢١) ، رئاسة مجلس الوزراء، جمهورية مصر العربية، المجلس الأعلى للأمن السيبرانى ،الأستراتيجية الوطنية للأمن السيبرانى ، ص ص ١-٩

شكل (١)
أهم البرامج الاستراتيجية فى المرحلة الحالية (٢٠١٧-٢٠٢١)

الإجراءات المنهجية للدراسة :

١-**نوع الدراسة** :تعد هذه الدراسة من الدراسات الوصفية التي تهدف إلى وصف العلاقة الارتباطية بين الجريمة السيبرانية وتأثيرها علي الأمن القومي، والتعرف على مظاهر وإشكالات الجريمة السيبرانية وتأثير ذلك أيضاً علي الأمن القومي.

٢-**منهج الدراسة** : تعتمد الدراسة الحالية علي منهج المسح الاجتماعي؛ فمنهج المسح الاجتماعي أحد المناهج العلمية المُستخدمة للتعرف على بيانات ومعلومات دقيقة، ويكون ذلك من خلال التواصُل المباشر، أو عبر البريد العادي، أو الوسائل الإلكترونية الحديثة.

٣-**طريقه المسح الاجتماعي بالعينة** : تعتمد هذه الدراسة علي منهج المسح الاجتماعي بالعينة وذلك من خلال عينه عشوائيه بسيطه من خلال التطبيق علي بعض من كليات جامعة الفيوم وتم اختيار بعض الكليات النظرية والعملية والتطبيقية

حيث تم تقسيم جامعة الفيوم إلى كليات نظرية، و عملية ،وتطبيقية وتم التطبيق في البعض الكليات الممثلة لكل فئة.

٤-**أدوات ومصادر جمع البيانات:** اعتمدت الدراسة علي الاستبيان كأداه لجمع البيانات من الطلاب ومحاوله اكتشاف مدي وعي الطلاب عن علاقه الجريمة السيبرانية بالأمن القومي ، والتعرف على إشكالات الجريمة السيبرانية وتأثير ذلك على الأمن القومي المصرى ،والتعرف على الاستراتيجيات والقوانين التي شرعتها الدولة لمواجهة الجريمة السيبرانية ،ويتكون الاستبيان من أربعه اقسام رئيسيه يحتوي كل منها علي عدد من الاسئله حيث تناول القسم الاول للاستبيان البيانات الاساسيه للمبحوثين بينما تناولت الاقسام الثلاثة الأخرى أبعاد ومؤشرات الجريمة السيبرانية وتأثيرها على الأمن القومي .

وقد مر الاستبيان بعدد من الخطوات حتي وصل إلى صياغته النهائية حيث قامت الباحثة بإعداد الأستبيان في صورته الأوليه ثم قامت باختبار الصدق والثبات للاستمارة، وذلك عن طريق تجربه الاستبيان علي عدد من المبحوثين بطريقه عشوائيه ببعض الكليات لاختبار الأسئلة ومدي تقبل المبحوثين لتلك الأسئله ،ثم قامت الباحثة بصياغه الاستبيان في صورته النهائيه بعد التعديلات حيث قامت الباحثة بتوزيع ٥٢٠ استماره علي المبحوثين في بعض من كليات الجامعة وكان العائد منها ٥٠٠ استماره حيث تم استبعاد(٢٠ استمارة) نظراً لوجود بعض الأسئلة لم تم إجابتها من قبل المبحوثين ،فكان عدد الاستمارات الصحيحة التي تم تحليلها (٥٠٠)استماره.

٤-**مجالات الدراسة** : أ-**المجال البشري** :يتمثل المجال البشري للدراسه باختيار الباحثة عينه مكونه من(٥٠٠) طالب من بعض كليات جامعة الفيوم منها الكليات النظرية والعملية والتطبيقية.

ب-**المجال الجغرافي** :تم التطبيق في جامعه الفيوم في بعض الكليات

- الكليات العمليه (هندسه ،علوم،طب)
- الكليات النظرية (تربية ،خدمه اجتماعيه) ،ويأتي السبب في اختيار هذه الكليات من الباحثين:
- لتوافر بعض الأصدقاء في هذه الكليات يسهلون للباحثة تطبيق الاستمارة .
- يوجد وحدة للخدمات الإلكترونية في بعض الكليات فيمكن قياس وعى الطلاب بأهمية موضع الدراسة وسؤالهم عن دورها في رفع الوعي الرقمي لهم.

٥-**خطوات العمل الميداني** :مرت الدراسة بعدد من الخطوات بدايه من اختيار محل الدراسة وعمل استماره الاستبيان وتحكيمها واختبارها انتهاءاً بالتحليل الاحصائي لإستماره الاستبيان واستخلاص النتائج وفي ما يلي سوف :

- اختيار الكليات التي ستقوم الباحثة بالتطبيق فيها.
- إعداد استماره الأستبيان وإجراء التعديلات .
- تطبيق اختبار قبلي pre-test لاستماره الاستبيان وتعديل بعض الأسئلة .
- تطبيق استماره الاستبيان علي عينه الدراسة من الكليات التي تم اختيارها كما أشار الباحثة إليها من قبل حيث بلغ عدد مفردات العينة ٥٠٠ مفردة.
- تفريغ الاستمارات باستخدام الجداول الإحصائية وتحليلها بواسطة برنامج SPSS.

٦-**أسإلب التحليل والتفسير**

- تفريغ الجداول وتحليلها عن طريق برنامج SPSS وربطها بالمقولات النظريه المستخدمة في نظريات الدراسة .
- تحليل الجزء الميداني وربطه بنتائج الدراسات السابقة التي رجعت إليها الدراسة باستخدام المعامل الإحصائى ANOVA أو تحليل التباين هو اختبار يستخدم

لتحديد الاختلافات بين نتائج البحث من ثلاث عينات أو مجموعات غير مرتبطة أو أكثر .

٧-**خصائص عينه الدراسة:** جاءت العينة في هذه الدراسة عينة متعددة المراحل أو عينة طبقية وانقسمت عمليه إختيار العينة إلى مرحلتين:

المرحله الأولى : تم تقسيم جامعة الفيوم إلى طبقتين كليات عملية، وكليات نظرية ، **والمرحلة الثانية** :تم اختيار عينة عشوائية قوامها ٥٠٠ مفردة من كل الكليات العملية والكليات النظرية.

٨-**صعوبات الدراسة الميدانية:** واجهت الباحثة بعض الصعوبات خلال الدراسة الميدانية وتتمثل هذه الصعوبات في :أ -توزيع الاستمارات وخوف بعض المبوحثين بالإجابة على بعض أسئلة الاستبيان كلها: وذلك بسبب عدم موافقة بعض الأشخاص على ملئ الإستمارة بسبب حساسية الموضوع ووجود بهض الأسئلة المتعلقة بحياتهم الشخصية ، وإذا كانوا تعرضوا للاختراق أم لا، ولكن تم التعلب على هذه النقطة بتوضيح الباحثة لأفراد العينة أن معلومات هذه الاستمارة تستخدم لأغراض البحث العملي وليس لأي شي اَخر.

جدول (١)
الفروق بين كليات جامعة الفيوم من حيث تعرض شباب الجامعة للاختراق الرقمي

الاستجابات	كلية الهندسة		كلية الخدمة الاجتماعية		كلية الطب		كلية العلوم		كلية التربية		الجملة	ANVO		
	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	القيمة	الدلالة
نعم	87	87.00	٦٣	72.00	٧٢	63.00	74	74.00	72	72.00	368	73.60	3.90	*0.00
لا	13	13.00	37	37.00	٢٨	٢٨,00	26	26.00	28	28.00	132	26.40		
Total	100	100.00	100	100.00	100	100.00	100	100.00	100	100.00	500	100.00	د.ح = ٤	

(ن=٥٠٠)

يتضح من الجدول السابق أن أفراد مجتمع الدراسة في معظم الكليات التي تم التطبيق بها بنسبة ٧٣,٦%، مقابل ٢٦,٤% تعرضوا للإختراق الرقمي وذلك يتفق مع دراسة نورتون روز فولبريت الذين توصلوا في نتائج دراستهم إلى أن الجريمة السيبرانية تزاد بشكل مباشر عن طريق الايميلات الإلكترونية وذلك بارسال بعض الايميلات الوهمية التي تحمل بعض الفيروسات التي تساعد على الاختراق .

وذلك يتفق مع المقولة النظرية التي تنطلق منها نظرية مجتمع المخاطر التي ترى أن خطاب المخاطر العابر للقارات غير من سلوكيات الأفراد الذين اقتنعوا بأن المستقبل أصبح غير واضح ، وملئ بالتحديات التي تأتى من الأنسان لأخيه الأنسان نتيجة العدوان البشرى والذى أطلق عليه توامس هوبس " زمن الحرب الكل ضد الكل "، حيث أصبح مؤشر حساسية المخاطر يحتل مكانة أساسية في الخطاب الأمنى والسياسى لعديد من الدول في جميع أنحاء العالم ، فأصبح العالم يعيش حالة من الخوف والقلق من بمايسمى من مخاطر المدينة والمجتمع .[١]

أما على مستوى الكليات فقد كانت هناك فروق ذات دلالة إحصائية بين الكليات باستخدام مقياس ANOVA حيث أن قيمة ANOVA(0.00)هو مستوى دال إحصائياً عند مستوى معنوية (٠.٠٥)، وقد كانت هذه الفروق لصالح كلية الهندسة

[١] - الحسن ايت الحسين ،مجتمع المخاطر – فوبيا – تحضر المخاطر، مرجع سابق ، ص ٥

جدول (٢)

الفروق بين كليات الدراسة من حيث نوعية الاختراق الذى تعرض له أفراد مجتمع الدراسة

نوعية الاختراق	كلية الهندسة		كلية الخدمة الاجتماعية		كلية الطب		كلية العلوم		كلية التربية		الجملة		ANOVA	
	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	القيمة	الدلالة
أ-اختراق جنسى	66	18 %	41	11.1%	32	8.7%	31	8.4%	54	14.7%	224	60.8 %	*9.747	0.000
ب- اختراق مادى	16	4.3 %	21	5.7%	22	5.9%	43	11.6%	27	7.3%	129	35 %	*6.012	
ج-اختراق شخصى	3	0.82 %	17	4,6%	6	1.6%	21	5.7%	19	5.2%	66	17.9 %	*5.979	
د-انتحال الشخصية	2	0.5 %	4	1.1%	3	0.82%	2	0.5%	13	3.5%	24	6.5 %	*4.887	0.001
هـ- نشر الفي روسات	2	0.5 %	2	0.5%	6	1.6%	5	1.3%	15	4.1%	30	8.1 %	2.075	0.083
د- غير مبين	-	-	-	-	1	0.3%	-	-	3	0.82%	4	1.1 %	2.158	0.073

(يمكن للمبحوث اختيار أكثر من إجابة على هذا السؤال حيث ن=٣٦٨).

يتضح من الجدول السابق أن نوعية الاختراق الذى تعرض لها أفراد مجتمع الدراسة الذى تعرضوا بها كان اختراق جنسى بنسبة 60.8%، يليها في المرتبة الثانية اختراق مادى بنسبة 35%، يليها في المرتبة الثالثة اختراق شخصى بنسبة 17.9%.

أما على مستوى الكليات فهناك فروق ذات دلالة إحصائية بين كليات الدراسة في ما يتعلق بنوعية الاختراق الذى حدث لهم تمثل في الاختراق الجنسى والشخصى وانتحال الشخصية حيث أن مستوى دلالة ANOVA(0.00)هو مستوى دال إحصائياً عند مستوى معنوية (٠.٠٥)، وترجع الفروق في الاختراق الجنسي لصالح كلية الهنسة حيث سجلت كلية الهندسة أعلى نسبة وهي ١٨% ،وربما يرجع ذلك أن طلاب كليات الهندسة يستخدمون أجهزة الحاسب الشخصى بنسبة مرتفعة ولساعات كثيرة وذلك يتفق مع دراسة قادى نور الهدى الذى توصل في نتائج دراسته أن الجريمة السيبرانية تتميز بأنها يصعب إكتشافها وإثباتها أمام القضاء، كما أنها من الجرائم العابرة للحدود لاتعترف بالحدود الزمانية والمكانية.

فحسب نظرية جيدنز أن البنية ليست معوق لأى فعل اجتماعي بل تشكله ، ولكن باعتبار أن الفاعل مشارك بشكل أساسي في إنتاج البنية ، حيث يقوم الفاعلون من خلال أنشطتهم الروتينية والمستمرة والمكررة نتيجة إحساسهم بأن العالم باقٍ على ما هو عليه ،وأن الأمور تسير بهذا الشكل نتيجة إحساسهم بالأمن الوجودي فكل تلك الممارسات تساهم في تشكيل البنية وكذلك تقوم البنية بتشكيلهم،لأن الناس يتصرفون وفق أنماط سلوكية منتظمة حيث أنهم يعيشون في عالم اجتماعي له دلالاته الثقافية وظواهره الاجتماعية[١]

جدول (3)
الفروق بين كليات مجتمع الدراسة من حيث الإجراءات التي قام بها الأفراد لمواجهة هذا الاختراق

الإجراءات المتبعة عند التعرض للاختراق	كلية الهندسة		كلية الخدمة الاجتماعية		كلية الطب		كلية العلوم		كلية التربية		الجملة		ANOVA	
	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	القيمة	الدلالة
أ-إغلاق الحساب الإلكتروني والتكتم على الموضوع	64	17.4%	46	15.2%	46	12.5%	45	12.2%	35	9.5%	246	66.8%	9.9*2	0.00
ب- تبليغ الجهات المختصة	15	4.1%	14	2.5%	14	3.8%	23	6.25%	29	7.9%	90	24.5%		
ج- إبلاغ الأسرة	-	-	3	0.3%	3	0.8%	1	0.02%	10	2.7%	16	4.3%		
غير مبين	8	2.1%		1.6%			3	0,08%			17	4.6%	دح=٤	

(يمكن للمبحوث اختيار أكثر من إجابة على هذا السؤال حيث ن=٣٦٨).

يتضح من الجدول السابق أن الإجراءات المتبعة التي إتخذها أفراد العينة عند تعرضهم للأختراق هو إغلاق الحساب الإلكتروني والتكتم على الموضوع بنسبة

[١]- حسين، رامي محمد. (٢٠٢٣). نظرية التشكيل البنائي لدى أنتوني جيدنز: مرجع سابق ،ص 203

٦٦.٨% ، ،يليها في المرتبة الثانية تبيلغ الجهات المختصة بنسبة ٢٤.٥%، يليها في المرتبة الثالثة إبلاغ الأسرة بنسبة ٤.٣% .

أما على مستوى الكليات فقد كان هناك فروق ذات دلالة إحصائية بين في ما يتعلق بالإجراء المتبع عند تعرضهم للإختراق وهو غلق الحساب الإلكتروني والتكتم على الموضوع بنسبة ١٧.٤% دلالة ANOVA(0.00)هو مستوى دال إحصائياَ عند مستوى معنويا (٠.٠٥)

وفي ضوء المقولة التي تنطلق منها نظرية تشكيل البنية عند جيدنز:أن البناءات الاجتماعية تتأسس من خلال الفعل البشرى، فيؤمن جيدنز أن للفعل الاجتماعي أهمية بالغة في تشكيل البنية الاجتماعية، فطبيعة المجتمع المصري من حيث ثقافته وعاداته عند حدوث أي مشكلة أن أفراده يميلون إلى التكتم على تلك الموضوعات وعدم الخوض فيها نظراً لخطورة الموضوع .

جدول (٤)

الفروق بين كليات الدراسة من حيث كيفية تأثير الجريمة السيبرانية على الأمن القومي

أوجه التأثير	كلية الهندسة		كلية الخدمة الاجتماعية		كلية الطب		كلية العلوم		كلية التربية		الجملة		ANOVA	
	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	القيمة	الدلالة
أ-تدهور الحالة الأمنية	47	66.2%	33	45.2 %	53	61.6 %	25	39.7 %	40	55.6%	198	54.2%	3.12 *	0.02
ب-تدهور الحالة الأقتصادية للدولة	22	31.0%	36	49.3 %	29	33.7 %	34	54.0 %	19	26.4%	140	38.4%		
ج-إحتلال الدولة	2	2.8%	3	4.1%	4	4.7%	4	6.3 %	13	18.1%	26	7.1%		
غير مجاب		0.0%	1	1.4%							1	0.3%		
الجملة	71	100.0 %	73	100 %	86	100	63	100 %	72	100%	365	100%	د.ح= ٤	

(ن =٣٦٥)

يتضح من الجدول السابق أن الجريمة السيبرانية لها تأثير على الأمن القومي حيث رأت عينة الدراسة أن ذلك يتمثل في تدهور الحالة الأمنية للبلاد بنسبة ٥٤.٢% ويلها

في المرتبة الثانية تدهور الحالة الاقتصادية بنسبة ٣٨.٤%، يليها في المرتبة الثالثة احتلال الدولة بنسبة ٧.١%، وذلك يتفق مع دراسة ربيعى حسن الذى توصل في نتائج دراسته إلى أن الفضاء السيبراني هو أحد العناصر الاستراتيجية التي يعتمد عليها فى الخبراء في مجال تحقيق الأمن القومي للبلاد نظراً لحجم التهديدات التي يحتويها، فالجرائم السيبرانية يمكن أن تؤدي إلي صراع دولي.[1]

أما على مستوى كليات الدراسة فقد كانت هناك فروق ذات دلالة إحصائية بين الكليات باستخدام مقياس ANOVA حيث أن قيمة ANOVA(0.00)هو مستوى دال إحصائياً عند مستوى معنوية (٠.٠٥) .

ويوضح الجدول السابق أن الفروق الذى سجلها معامل ANOVA من حيث الكيفية التي تؤثر بها الجريمة السيبرانية على الأمن القومي وترجع هذه الفروق إلى كلية الهندسة بنسبة ٦٦,٢% ، وربما يرجع ذلك طبيعة الكلية من حيث المناهج الذى يدرسونها فهم أكثر دراية بالمخاطر التي تتعرض لها البلاد عند تعرضهم لهذا الموقف.

1- Grabosky, P. (2013). Organised crime and the internet: Implications for national security. *The RUSI Journal*, *158*(5), 18-25.

جدول (٥)
الفروق بين كليات الدراسة من حيث أسباب أنتشار الجريمة السيبرانية من وجهة نظر مجتمع الدراسة

أسباب الجريمة السيبرانية	كلية الهندسة		كلية الخدمة الاجتماعية		كلية الطب		كلية العلوم		كلية التربية		الجملة		ANOVA	
	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	القيمة	الدلالة
أ-الرغبة في تعلم القرصنة	33	46.2%	22	31%	19	26.4 %	29	33.7 %	25	39.7%	128	%35,1	3.12 *	0.02
ب-بدافع الأبتزاز	3	4,1%	47	66.2 %	40	55.6 %	53	66.2 %	34	54.0%	177	48.8%		
ج-بدافع الشهرة	36	49,3%	2	2.8%	13	18.1 %	4	4.7 %	4	6.3%	59	%16.1		
غير مجاب	-	-		-	-	-	-	-				%		
الجملة	72	100%		100 %		100	86	100.0%	63	100%	365	100%	د.ح= ٤	

(ن =٣٦٥)

يتضح من الجدول السابق أن ارتكاب الفرد للجريمة السيبرانية له أسباب قد يكون بدافع الأبتزاز بنسبة ٤٨,٨% ويلها في المرتبة الثانية بدافع الرغبة في تعلم القرصنة بنسبة ٣٥.١%، يليها في المرتبة الثالثة بدافع الشهرة بنسبة ١٦.١%.[١]

أما على مستوى كليات الدراسة فقد كانت هناك فروق ذات دلالة إحصائية بين الكليات باستخدام مقياس ANOVA حيث أن قيمة ANOVA(0.00)هو مستوى دال إحصائياً عند مستوى معنوية (٠.٠٥) .

ويوضح الجدول السابق أن الفروق الذى سجلها معامل ANOVA من حيث السبب في ارتكاب الجريمة السيبرانية في الرغبة في تعلم القرصنة وترجع هذه الفروق إلى كلية الهندسة بنسبة ٤٦,٢% ، وربما يرجع ذلك قد تكون هواية عند بعض طلاب خصوصاً قسم اتصالات، وذلك يتفق مع دراسة سمير بلى الذى توصل في نتائج

[١] -تمور نوال (٢٠١٢) ، كعفاءة أعضاء هيئة التدريس و أثرها على جودة التعليم العالي: دراسة حالة ،كلية العلوم الاقتصادية و علوم التسيير، جامعة، منتوري قسنطينة الجزائر، رسالة ماجستير منشورة ، ص ص ١٦٢-١٧٣

دراسته إلى أن الأمن القومي لأى دولة يرتبط ارتباطا وثيقاً بالأمن المعلوماتى لها وذلك يرجع إلى لمختلف التهديدات التي يطرحها التطور التكنولوجي.

حيث أن تكنولوجيا المعلومات والاتصالات توفر بشكل فوري الوسائل والدوافع والفرص للجرائم السيبرانية، ولكن بعدها الثقافي والاجتماعي والنفسي الناجم ثقافية عن العولمة هي السبب الجذري فى ارتكاب مثل هذه الجرائم .

ولا يمكن للجرائم السيبرانية أن تركز فقط على الدفاعات التكنولوجية أو المتعلقة بالبنية التحتية

ولكن يجب أن تعالج هذه التطورات العالمية فى إطار سياقي اجتماعي وثقافي وبنائي ، بينما الفهم العلمي والوعي السياسي بهذه القضايا لا يزال محدودا.[١]

جدول (٦)

الفروق بين كليات الجامعة من حيث وجود استراتيجية وطنية في مصر لرفع الوعى الإلكتروني

الاستجابات	كلية الهندسة		كلية الخدمة الاجتماعية		كلية الطب		كلية العلوم		كلية التربية		الجملة		ANOVA	
	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	القيمة	الدلالة
نعم	81	81%	72	72%	83	83%	68	68%	66	66%	370	74%	*3.2	0.01
لا	19	19%	27	27%	15	15%	32	32%	32	32%	125	25%		
غير مجاب	-		1	1%	2	2%	-	-	2	2%	5	1%		
الجملة	100	100%	100	100%	100	100%	100	100%	100	100%	500	100%	د.ح = 4.00	

(ن =٥٠٠)

يتضح من الجدول السابق أن أغلب عينة الدراسة رأت أنه يوجد استراتيجية في مصر لرفع الوعى الإلكتروني بنسبة ٧٤% مقابل ٢٥ % رأت غير ذلك ، حيث أنه لم تقم أنظمة المعلومات بتصميم مستويات أمنية كافية بعد، حيث إن الأمن المعلوماتى

1- Riaz, A., & Riaz, A. (2015, November). Causes and consequences of cybercrimes: An exploratory study of Pakistan. In *2015 First International Conference on Anti-Cybercrime (ICACC)* (pp. 1-5). IEEE.

المحقق من خلال المرافق التقنية محدود ويجب دعمه بإدارة وأساليب ، وتشريعات قانونية مناسبة.[1]

أما على مستوى الكليات فقد كانت هناك فروق ذات دلالة إحصائية بين كليات الدراسة باستخدام مقياس ANOVA حيث أن قيمة ANOVA(0.00)هو مستوى دال إحصائياً عند مستوى معنوية (٠.٠٥) .

جدول (٧)
الفروق بين الكليات من حيث الكيفية التي تعمل بها الأستراتيجية الوطنية لرفع الوعى الإلكتروني

الكيفية التي تعمل بها الاستراتيجية	كلية الهندسة		كلية الخدمة الاجتماعية		كلية الطب		كلية العلوم		كلية التربية		الجملة		ANOVA	
	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	القيمة	الدلالة
أ -بعمل ندوات توعية لرفع الوعى الرقمي لدى الشباب.	57	68.7%	29	43.9%	46	63.9%	46	56.8%	25	36.8%	203	54.9%	*5.31	0.00
ب-بعمل دورات تدريبة .	21	25.3%	25	37.9%	21	29.2%	17	21.0%	35	51.5%	119	32.2%		
ج- بعمل اعلانات قصيرة للتوعية الرقمية .	4	4.8%	10	15.2%	4	5.6%	6	7.4%	7	10.3%	31	8.4%		
د- بتوفي ر تقنيات معززة للجريمة السيبرانية .	1	1.2%	1	1.5%	0	0.0%	5	6.2%	-	-	7	1.9%		
هبتوعية الأباء لحماية أبنائهم	-	-	1	1.5%	-	-	2	2.5%	-	-	3	0.8%		
و- بتعزيز دور مباحث الإنترنت	-	-	-	-	-	-	5	6.2%	1	1.5%	6	1.6%		
غير مجاب	-	-	-	-	1	1.4%	-	-	-	-	1	0.3%		
الجملة	83	100.0%	66	100.0%	72	100.0%	81	100.0%	68	100.0%	370	100.0%	د.ح = ٤	

(ن=٣٧٠)

1- Yildirim, E. (2016). The importance of information security awareness for the success of business enterprises. In *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity*, Springer International Publishing. *July 27-31, 2016, Walt Disney World®, Florida, USA* (pp. 211-222).

يتضح من الجدول السابق أن الاستراتيجية الوطنية التي تعمل بها لرفع الوعى الإلكتروني لدى المواطنين هي عمل ندوات للتوعية، ورفع الوعى الرقمي بنسبة ٥٤,٩٥% يليها في المرتبة الثاني بعمل دورات تدريبية بنسبة ٣٢,٢% ،وذلك يرجع إلى أن مفهوم الثقافة_الرقمية بالشكل الحالي لا يستخدم بدقة، فالعديد ينظر إليه على أنه يتشكل من الممارسات التي يقوم بها الأفراد عبر وسائل التواصل الاجتماعي

أما على مستوى الكليات فقد كانت هناك فروق ذات دلالة إحصائية باستخدام مقياس ANOVA حيث أن قيمة ANOVA(0.00)هو مستوى دال إحصائياً عند مستوى معنوية (٠.٠٥) .

ويوضح الجدول السابق أن الفروق الذى سجلها معامل ANOVA من حيث الأستراتيجية الوطنية التي تعمل بها البلاد لرفع الوعى الإلكتروني كانت لصالح كلية الهندسة بنسبة ٦٨,٧% وربما يرجع ذلك خريجي وطلاب كليات الهندسة متخصصين في المجال ذاته فهم أكثر دراية بأكثر فاعلية إيجابية تؤثر في عقول كثير من المواطنين .

جدول (٨)

الفروق بين كليات مجتمع الدراسة من حيث حماية البيانات الشخصية على شبكة الإنترنت

الأستجابات	كلية الهندشة		كلية الخدمة الاجتماعية		كلية الطب		كلية العلوم		كلية التربية		الجملة		ANOVA	
	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	القيمة	الدلالة
نعم	94	94.0%	86	86.0%	73	73.0%	89	89.0%	89	89.0%	431	87.2%	*7.12	0.00
لا	1	1.0%	13	13.0%	25	25.0%	11	11.0%	11	11.0%	61	12.2%		
غير مبين	5	5.0%	1	1.0%	2	2.0%	-	-	-	-	8	1.6%		
الجملة	100	100.0%	100	100.0%	100	100.0%	100	100.0%	100	100.0%	500	100.0%	د.ح = ٤	

(ن=٥٠٠)

يتضح من الجدول السابق أن أفراد مجتمع الدراسة يميلون إلى حفظ بياناتهم على شبكة الإنترنت بنسبة ٨٧,٢% ، مقابل ١٢,٢% من أفراد العينة رأوا غير ذلك وبتفق

ذلك مع نظرية مجتمع المخاطر التي ترى أن الأمن القومي للبلاد يشهد مخاطر عديدة نتيجة الثورة الرقمية التي يشهدها المجتمع من خلال عدم الحفاظ على الخصوصية الثقافية للأفراد والاستيلاء على بعض المعلومات الرقمية للمؤسسات والأفراد ، فتستخدم الثورة الرقمية من قبل الذكاء الأصطناعى لتتبع المشكلات الاجتماعية وتشخصيها والدفاع عن حقوق الأنسان، إلا أنه يمكن أيضاً استخدام هذه التكنولوجيا لانتهاك هذه الحقوق ،فنشأت دراسة المخاطر من الاحتياجات العملية للمجتمعات الصناعية لتنظيم التكنولوجيا وحماية مواطنيها من المخاطر الطبيعية والتكنولوجية.[١]

أما على مستوى الكليات فقد كانت هناك فروق ذات دلالة إحصائية باستخدام مقياس ANOVA حيث أن قيمة ANOVA(0.00)هو مستوى دال إحصائياَ عند مستوى معنوية **(٠.٠٥) ، وكانت هذه الفروق لصالح كلية الهندسة .**

1- Janine Morgall Traulsen and Paul Bissell ,opcit,p251

جدول (٩)
الفروق بين أفراد مجتمع الدراسة من حيث الأجرءات التي يقومون بها لحماية بيناتهم من الاختراق

أهم الأجراءات التي يتخذها أفراد مجتمع الدراسة لحماية بياناتهك	كلية الهندسة		كلية الخدمة الاجتماعية		كلية الطب		كلية العلوم		محافظة الفي وم		الجملة		ANOVA	
	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	القيمة	الدلالة
أ –بكلمة مرور قوية	9	12.3%	3	3.5%	1	1.1%	11	12.4%	40	44.9%	64	14.8%	*27.18	
ب- تجنب تخوين ملفات هامة على كمبيوتر العمل	4	5.5%	8	9.3%	4	4.3%	44	49.4%	32	36.0%	92	21.3%	*27.28	
ج –عدم مشاركة البيانات الشخصية على مواقع التواصل الاجتماعي	7	9.6%	15	17.4%	14	14.9%	39	43.8%	9	10.1%	84	19.5%	*12.35	0.00
د- استخدام تطبيق مكافح للفي وٌوسات .	8	11.0%	31	36.0%	44	46.8%	31	34.8%	26	29.2%	140	32.5%	*6.25	
هـ الأنتباه إلى أذونات التطبيق	28	38.4%	55	64.0%	49	52.1%	17	19.1%	32	36.0%	181	42.0%	*10.6	
و- أنتيه لشبكة أمان الواى فاى	48	65.8%	31	36.0%	28	29.8%	8	9.0%	24	27.0%	139	32.3%	*16.15	
ر عمل تحديث للرامج من فترة لأخرى	3	4.1%	3	3.5%	4	4.3%	1	1.1%	6	6.7%	17	3.9%	0.96	0.43

(ن = ٤٣١)

يوضح الجدول السابق أن أهم الإجراءات التي يتخذها أفراد مجتمع الدراسة لحماية بياناتهم من الاختراق هي الإنتباه إلى أذونات التطبيقات بنسبة ٤٢% ، يليها في المرتبة الثانية استخدام تطبيق مكافح للفي روسات بنسبة ٣٢,٥%، يليها في المرتبة الثالثة الأنتباه لشبكة الواى فاى حيث قد تكون مخترقة بنسبة ٣٢,٢%، ويليها في المرتبة الرابعة تجنب تخزين ملفات هامة على الكمبيوتر بنسبة ٢١,٣% ،وربما يرجع ذلك أن معظم التغيرات التي حدثت في المجتمع يعتبر مصدرها العولمة وتكنولوجيا الاتصال، ولقد كان ذلك له تأثير– حيث عجزت منظومات القيم المجتمعية الضامنة للأمن عن احتواء أي تطرف أو سلوك إجرامى يرتكبه الفرد بسبب التقدم التكنولوجي أما على مستوى الكليات فقد كانت هناك فروق ذات دلالة إحصائية كانت لصالح كلية

الهندسة باستخدام مقياس ANOVA حيث أن قيمة ANOVA(٠.٠٠٠)هو مستوى دال إحصائياَ عند مستوى معنوية (٠.٠٥) .

جدول (١٠)

الفروق بين كليات الدراسة من حيث أشكال الجريمة السيبرانية

أشكال الجريمة السيبرانية	كلية الهندسة		كلية الخدمة الاجتماعية		كلية الطب		كلية العلوم		كلية التربية		الجملة		ANOVA	
	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	القيمة	الدلالة
أ-سرقة المعلومات والبيانات العسكرية.	47	52.8%	39	45.3%	19	26.0%	29	30.9%	36	40.4%	171	39.7%		
ب-سرقة المعلومات أو إتلافها وتدميرها إلكترونياً .	33	37.1%	26	30.2%	24	32.9%	41	43.6%	21	23.6%	151	35.0%		
ج- التجسس الإلكتروني	5	5.6%	11	12.8%	11	15.1%	13	13.8%	11	12.4%	56	13.0%	*7.27	0.00
د-الحرمان من خدمة الإنترنت.	2	2.2%	5	5.8%	9	12.3%	6	6.4%	10	11.2%	33	7.7%		
هـ- الإرهاب السيبراني.	2	2.2%	3	3.5%	10	13.7%	4	4.3%	9	10.1%	28	6.5%		
غير مبين		0.0%		0.0%		0.0%	1	1.1%	2	2.2%	3	0.7%		
الجملة	89	100%	86	100%	73	100%	94	100%	89	100%	431	100%		
د.ح = ٤														

(ن =٤٣١)

يتضح من الجدول السابق أن أفراد العينة في الكليات رأت أن أشكال الجريمة السيبرانية هي سرقة المعلومات والبيانات العسكرية بنسبة ٣٩,٩% يليها في المرتبة سرقة المعلومات وإتلافها الكترونياً بنسبة ٣٤,٤% ويتفق ذلك مع دراسة أوفي في كتوريا آن ريتشاردسون الذى توصل في نتائج دراسته إلى لم يعد الهجوم العسكري هو الطريق الوحيد لتقويض أي أمة ، بل أصبح الهجوم الإلكتروني بديل للهجوم العسكري ، وأقل تكلفة ، وأمن ولايعرض أي دولة للخسائر في أرواح مواطنيه ، وأنها أصبحت الصلة بين الجريمة الإلكترونية والأمن القومي سائدة بشكل متزايد ، حيث طورت التكنولوجيا القدرة الجنائية على إحداث ضرر وإزعاج للأفراد وكذلك للبنية التحتية الحيوية للأمة من خلال تقويض أدواتها الحيوية والهجوم على الأنظمة الإلكترونية لأى مؤسسة .

أما على مستوى الكليات فهناك فروق ذات دلالة إحصائية بين الكليات باستخدام مقياس ANOVA حيث أن قيمة ANOVA(0.00)هو مستوى دال إحصائياً عند مستوى معنوية (٠.٠٥) .

جدول (١١)
الفروق بين كليات الدراسة من حيث أهم المقترحات التي تتخذها الدولة لحماية فضائها السيبراني من الاختراق

أهم المقترحات للحماية من الاختراق	كلية الهندسة		كلية الخدمة الاجتماعية		كلية الطب		كلية العلوم		كلية التربية		الجملة		ANOVA	
	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	القيمة	الدلالة
أ- تأمين البنية التحتيةالإلكترونية	41	41.0%	26	26.0%	18	18.0%	11	11.0%	58	58.0%	154	30.8%	*19.07	0.00
ب-التعاون بين الدول في هذا المجال .	49	49.0%	41	41.0%	30	30.0%	25	25.0%	45	45.0%	190	38.0%	*4.49	
ج- استخدام الأسالى ب التوعوية في هذا المجال	21	21.0%	31	31.0%	24	24.0%	27	27.0%	20	20.0%	123	24.6%	1.09	0.36
د- تفعيل العقوبات القانونية والدولية التي تخص هذا الإطار.	18	18.0%	31	31.0%	24	24.0%	25	25.0%	15	15.0%	113	22.6%	2.27	0.06
هـ-تنظيم مؤتمرات دولية في هذا المجال .	20	20.0%	26	26.0%	25	25.0%	36	36.0%	19	19.0%	126	25.2%	*2.45	0.05
م- القدرة على الأنتقام التي تتطلب وجود إلى ات للرد على الهجمات بما يمنع الطرف الأخر من الهجوم	19	19.0%	19	19.0%	21	21.0%	35	35.0%	10	10.0%	104	20.8%	*5.08	0.00
ن-توافر نسخة احتياطى من المعلومات الهامة للدولة	12	12.0%	11	11.0%	11	11.0%	20	20.0%	13	13.0%	67	13.4%	1.23	0.30
و- تفعيل العقوبات الاقتصادية التي ترتكب مثل هذا الفعل	4	4.0%	2	2.0%	14	14.0%	14	14.0%	13	13.0%	47	9.4%	*4.00	0.00
ل – تفعيل الأتفاقيات الدولية في هذا المجال	7	7.0%	8	8.0%	15	15.0%	5	5.0%	8	8.0%	43	8.6%	1.83	0.12
ي- عمل برامج في الجماعات تخص هذا الشأن	17	17.0%	7	7.0%	7	7.0%	3	3.0%	9	9.0%	43	8.6%	*3.47	0.01

(ن=٥٠٠)

يتضح من الجدول السابق أن أفراد العينة في كليات الدراسة رأت أن التعاون بين الدول في هذا المجال هي من أهم الإجراءات التي يمكن أن تتخذها الدولة لتأمين فضائها السيبراني ضد أي معتدي وذلك بنسبة ٣٨% ، يليها في المرتبة الثانية تأمين البنية التحتية الإلكترونية بنسبة ٣٠.٨% وذلك يتفق مع دراسة ربيعى حسن الذى

توصل في نتائج دراسته إلى أنه أغلب الدول العظمى أصبحت هي الدول المسيطرة في مجال الأمن السيبراني العالمى عكس الدول النامية والضعيفة لا نجد لها أثراً في هذا المجال، فعليه لابد من التعاون بين الدول لمواجهة مثل هذه الجرائم .

أما على مستوى الكليات فقد كانت هناك فروق ذات دلالة إحصائية بين الكليات باستخدام مقياس ANOVA حيث أن قيمة ANOVA(0.00)هو مستوى دال إحصائياً عند مستوى معنوية (٠.٠٥) .

نتائج الدراسة :

-توصلت الدراسة الحالية إلى العديد من النتائج الميدانية أهمها:

١-ماهية الجريمة السيبرانية ،وأنواعها:

- توصلت الدراسة إلى أن الجريمة السيبرانية هي الأفعال الخارجة عن القانون ولكن يصعب إكتشافها ، وأن حماية المعلومات الشخصية هو المعنى المرادف للأمن السيبراني.
- توصلت الدراسة إلى أن الجريمة السيبرانية تزداد بشكل مباشر عن طريق الايميلات الإلكترونية وذلك بإرسال بعض الايميلات الوهمية التي تحمل بعض الفيروسات التي تساعد على الاختراق والحصول على المعلومات .
- توصلت الدراسة إلى أن أنواع الجريمة السيبرانية قد تكون جنسية أو مادية أو إقتصادية .
- توصلت الدراسة إلى أن الجريمة السيبرانية قد ترتكب بدافع مادى ، أو بدافع الرغبة في الأبتزاز الطرف الأخر ، أو الرغبة في تعلم القرصنة .
- توصلت الدراسة إلى أن الأسباب الاجتماعية والاقتصادية التي قد تدفع الشباب إلي إرتكاب مثل هذه الجرائم هو الفقر ، والبطالة ،والرغبة فى الشهرة وإثبات الذات أمام الأهل .

- توصلت الدراسة إلى أن الأفراد الذين اخترقت حساباتهم تعرضوا إلى إبتزاز مادى وأنه يوجد عدد افراد من الاسرة لديهم درايه بالامن السيبراني لذلك لم يتم اختراقهم
- توصلت نتائج الدراسة إلى أن سرقة الهوية علي الإنترنت من أهم مظاهر الجريمة السيبرانية
- توصلت نتائج الدراسة إلى أن عدد قليل من الافراد هم من يستخدمون برامج الحماية وان برنامج الحماية المتداول بين الافراد هو برنامج Anti-Virasplus
- توصلت الدراسة إلى أنه يوجد العديد من الطرق لتجنب الاختراق أبرزها هو استخدام كلمات مرور قوية لكل حساب وأن الفئة الأكثر استخدام للانترنت هي فئة الشباب.

٢- التحديات والتهديدات التي تواجه الأمن القومي المصري نتيجة الجريمة السيبرانية وبروز أنماط جديدة من الصراع القومي :

- توصلت نتائج الدراسة إلى أنه من التهديدات المحتملة للجريمة السيبرانية الاختراق الالكترونى والتجسس السيبراني من خلال إستغلال الثغرات الأمنية فى البنية التحتية السيبرانية للوصول إلى معلومات حساسة وسرية وأمنية حول الحكومات والشركات والمؤسسات الحيوية ، وقد تستخدم تلك المعلومات فى التأثير على القرارات الوطنية والتجسس الصناعي.
- توصلت نتائج الدراسة إلى أنه من ضمن التهديدات التي الأمن القومي المصرى نتيجة الجريمة السيبرانية قد يكون هناك هجمات إلكترونية كبرى غير محدودة النظاق على الشبكة التحتية للبلاد مثل شبكة لإنترنت والنقل والكهرباء فتعطل تلك الهجمات من الخدمات الإقتصادية والاجتماعية للبلاد ويدخل ذلك من نظاق الأمن القومي.

- توصلت نتائج الدراسة أنه من التهديدات المحتملة للجريمة السيبرانية التي تهدد الأمن القومي المصرى الحروب السيبرانية فقد تقوم دولة أو جماعة إرهابية بهجمات بغرض الإضطرار بالبنية التحتية للبلاد ، وقدرتها العسكرية والاستخباراتية والاقتصادية ، وذلك يؤثر على الأمن القومي.
- توصلت نتائج الدراسة أنه من ضمن التهديدات التى توجه الأمن القومى المصري القرصنة الإلكترونية وذلك بإستخدام البرامج الخبيثة والروابط الوهمية وتهديد الحكومات والشركات والأفراد للتصيد الإحتيالي لسرقة المعلومات والأموال وتعطيل الأنظمة الحيوية .
- توصلت نتائج الدراسة أنه من ضمن التهديدات التي تواجه الأمن القومي المصرى نتيجة الجريمة السيبرانية التطرف الإلكتروميو وتأثيره على الأنظمة السياسية للبلاد حيث سوء استخدام مواقع التواصل الاجتماعي والمنصات الرقمية لنشر الأفكار المتطرفة لتأثيرها على الرأى العام والعملية السياسية فى مصر ، واستغلال الجماهير وقوة الوسائط الاجتماعية لتحقيق أهداف سياسية لإثارة الفتن والإنقسامات داخل الشعب .
- توصلت الدراسة إلى أن الجرائم السيبرانية تمتاز بخصوصيات تميزها عن غيرها من الجرائم حيث أنها ترتكب في بيئة افتراضية ولاتترك أثراً مادياَ ، في صعب إكتشافها.
- توصلت نتائج الدراسة إلى أن الدول النامية تعانى من معضلة حماية سيادتها وتأمين حدودها وخاصة الافتراضية.
- توصلت نتائج الدراسة إلى أن اختراق أمن المعلومات له تأثير كبير علي الأمن القومي في وٌدى ذلك إلى تدهور الحالة الامنية والاقتصادية للبلاد.

- توصلت نتائج الدراسة إلى أن الأمية الرقمية تساهم في انتهاك خصوصية الفرد وتمنعهم من استخدام مواقع التواصل الاجتماعي.
- توصل الدراسة إلى أن التهديد الإلكتروني أصبح يؤثر بقوة على الأمن القومي للدول _على الأقل_ في الوقت الراهن، إذا أصبحت السياسات الأمنية للدول تتضمن التركيز على مفاهيم أمنية جديدة مثل: الحرب الإلكترونية ، الجريمة السيبرانية ، جرائم الإنترنت، القرصنةالإلكترونية . اختراق الأجهزة القومية للمؤسسات العسكرية.

ثالثاً:التعرف على استراتيجيات مكافحة الجريمة السيبرانية :

- توصلت نتائج الدراسة أنه من ضمن الاستراتيجيات المتبعة لمكافحة الجريمة السيبرانية استراتيجية تعزيز التوعية والتثقيف بأهمية الأمن السيبراني والمخاطر المحتملة ، وتوجيه الجهود حول الممارسات الأمنة ، والحذر من البريد الإلكتروني المشبوه والبرامج الخبيثة ، والروابط الضارة .
- توصلت نتائج الدراسة أنه من ضمن الاستراتيجيات المتبعة لمكافحة الجريمة السيبرانية تعزيز التشريعات والقوانين : حيث أنه لابد من أن تتبني الحكومات قوانين فعالة على أن تكون لها إجراءات لمكافحة الاختراق ومعاقبة كل من يتسبب فى اختراق الأنظمة والاحتيال الإلكتروني والتلاعب بالبيانات.
- توصلت نتائج الدراسة أنه من الاستراتيجيات المتبعة لمكافحة الجريمة السيبرانية تعزيز القدرات التقنية للبلاد لمكافحة الجريمة السيبرانية بحيث أن تكون قادرة عن الكشف عن الهجمات ، والوقاية منها ، بحيث أن تشمل تطوير الأنظمة الاختراق ، وتقنية الإجابة السريعة وتحليل البيانات ورصد الشبكات وحل أى مشكلة طارئة حيث أن الهجمات السيبرانية تمثل مخاطر أمام المجتمع الدولى لما لها أثار على الفرد والدولة .

- توصلت نتائج الدراسة إلى أنه من ضمن الاستراتيجيات المتبعة لمكافحة الجريمة السيبرانية استراتيجية التعاون الدولي لأن الجريمة السيبرانية عابرة للحدود ، فلابد من تبادل المعلومات والخبرات حيث تكون المساعدات القانونية عابزة للدول لحل أى مشكلة.
- توصلت نتائج الدراسة إلي أنه من ضمن الاستراتيجيات المتبعة لمكافحة الجريمة السيبرانية استراتيجية تعزيز التدريب والتأهيل : حيث لابد من توفير تدريب مناسب للكوادر الأمنية بحيث يكون لديهم الخبرات الكافية للتعامل مع التهديدات السيبرانية لجمع الأدلة الرقمية حول أى جريمة وتحليلها بالطريقة المناسبة .
- توصلت نتائج الدراسة أنه من ضمن الاستراتيجات المتبعة لمكافحة الجريمة السيبرانية استراتيجية الإجابة السريعة وتطوير خطة الطوارئ للهجمات السيبرانية ، فلابد من وجود خطط للطوارئ والاستعدادت اللأزمة لإستعادة البيانات ، وإصلاح الأنظمة المتضررة ، وتحديد المسؤليات والإجراءات وتقديم المساءلة .

التوصيات والرؤى المستقبلية للدراسة

ثانياً: توصيات الدراسة

توصلت هذه الدراسة إلى أن يوجد علاقة وثيقة بين الجريمة السيبرانية والأمن القومي حيث تمثل المعضلة الأساسية لبعض الدول النامية حماية فضائها ، وخاصة الإلكتروني ، فلابد من جماية أمن معلومات الأفراد الذي يحمي كل ما يتعلق بهم علي الإنترنت ويحمي خصوصيتهم من الانتهاك والاختراق ويتحقق ذلك من خلال بعض توصيات توصي بها الدراسة وهي :

١. توصي الدراسة بأهمية الوعي الرقمي للفرد ويتحقق ذلك من خلال عدة طرق من أهمها الندوات والمحاضرات ووسائل الإعلام بكافة أشكالها واستضافة الشخصيات العلمية للتوعية بذلك.

٢. تعزيز الدورات التدريبية المقدمة للأساتذة الجامعيين والعاملين في سلك التربية والتعليم في مجال الوعي الرقمي والاستخدام الآمن للإنترنت.

٣. تغليظ العقوبات في الجرائم التي تقع على شبكات التواصل الاجتماعي لسرعة تداولها واتساع نطاقها ومن أهمها الجرائم الإلكترونية والقرصنةالإلكترونية

٤. زيادة التعمق في الفضاء السيبراني في مجال علم الإجتماع الرقمي من خلال المواطنة الرقمية، والغزو الثقافي السيبراني، العولمة الثقافية في عصر المعلومات، مخاطر العالم الافتراضي، قانون المعاملات الإلكترونية والتجارة الإلكترونية

٥. ضرورة إصدار قانون بشأن حماية الخصوصية يتيح إلى ات المراقبة من خلال استحداث تقنية لإنذار المسئولين بسوء استخدام مما يعطيهم الحق في التدخل والرقابة.

٦.توصي الدراسة بزيادة التعمق في الفضاء السيبراني في مجال علم الاجتماع الرقمي من خلال دراسة المفاهيم التالية المواطنة الرقمية، والغزو الثقافي السيبراني ، والعولمة الثقافية في عصر المعلوماتية، مجتمع المخاطر المعلوماتى، مخاطر العالم الافتراضي، والتحول لمجتمع المعرفة.

مراجع الدراسة

أولاً: المراجع العربية :

١ – أبو سعود، ، و عباس طاهر. (٢٠٢٠). ارتباطات الأمن المعلوماتي بالأمن القومي .مجلة الدراسات الحقوقية، مج٧، ع٢ .

٢ – الحسن ايت الحسن (٢٠٢١) ،مجتمع المخاطر – فوبيا – تحضر المخاطر، مجلة جيل للعلوم الانسانية والاجتماعية ، مركز جيل البحث العلمى ، ع ٧٥.

٣ – الصغير، أحمد حسين. (٢٠١٩). مخاطر المجتمع الافتراضي على الأبناء: دراسة نقدية .المجلة التربوية، ج٦٨ .

4– العدوى، محمد أحمد ،٢٠١٠" ،الأمن الإنساني ومنظومة حقوق الإنسان"، في: أحمد مجدى حجازى (تحرير) ، المواطنة وحقوق الإنسان في ظل المتغيرات الدولية الراهنة، القاهرة، الدار المصرية السعودية للطباعة والنشر والتوزيع،.

5 – العطيان، تركي بن محمد. (٢٠٠٦). البطالة وعلاقتها بالسلوك الإجرامي: دراسة نظرية على المجتمع السعودي .المجلة العربية للدراسات الأمنية، مج ٢١، ع ٤١

٦ – الماحى، & .,اسامه صلاح محمود. (٢٠٢٣). الجرائم المعلوماتية المهددة للأمن القومي المصري .مجلة البحوث القانونية والاقتصادية–المنوفية(1)57 ،

٧– بلى سمير_.(٢٠٢٣) ، التهديدات الأمنية السيبرانية : دراسة في انعكاسات الحرب الإلكترونية على الأمن القومي للدول واستراتيجيات المقاومة ، مجلة الرسالة للدراسات والبحوث الانسانية (٨)٢ ،

٨ – بلى سمير_.(٢٠٢٣) ، التهديدات الأمنية السيبرانية : دراسة في انعكاسات الحرب الإلكترونية على الأمن القومي للدول واستراتيجيات المقاومة ، مجلة الرسالة للدراسات والبحوث الانسانية (٨)٢ ،

٩– جمال الدين، هبة. (٢٠٢٣). الأمن السيبراني والتحول في النظام الدولي. مجلة كلية الاقتصاد والعلوم السياسية، ٢٤(١)

١٠– تمور نوال (٢٠١٢) ، كعفاءة أعضاء هيئة التدريس و أثرها على جودة التعليم العإلى: دراسة حالة ،كلية العلوم الاقتصادية و علوم التسيير، جامعة، منتوري قسنطينة الجزائر، رسالة ماجستير منشورة.

١١- حسين ربيعى وأخرون (٢٠٢٢)، الحروب السبيرانية : المخاطر واستراتيجيات تحقيق الأمن السيبراني الدولى والخارجى، المجلة الجزائرية للأمن الانسانى ،مج ٧،ع ٢٢.
١٢ – حسين، رامي محمد. (٢٠٢٣). نظرية التشكيل البنائي لدى أنتوني جيدنز: السياق – المفاهيم – الفرضيات الأساسية .مجلة كلية الآداب والعلوم الإنسانية، ع٤٥ .
١٣- طعبة سعاد(٢٠٢٢) ،الجريمة الإلكترونية :تفعيل لإلىات القانون من أجل تحقيق العدالة ،مجلة الحقوق والعلوم الانسانية ، مجلة الحقوق والعلوم الانسانية، ١٥(٣) .
١٤ – عجيل فاطمة. (٢٠١٩) ، التهديداتالإلكترونية والأمن القومي ، جامعة محمد بوضياف ، رسالة ماجستير منشورة ، الجزائر.
١٥- فوزى إسلام (٢٠١٩) ، الامن السيبراني: الأبعاد الاجتماعية والقانونية: تحليل سيوسولوجى ، مرجع سابق ، ص ١١٠
١٦ – محمد حسام الدين (٢٠٢٠) نظرية التشكيل البنائي لدى أنتوني جيدنز (محاولة للتوفيق بين البنية والفعل في فهم المجتمع الإنساني) دراسة تحليلية – نقدية٠ .(مجلة العلوم الإنسانية و الاجتماعية.(7)4 ,
١٧- محمد على وفاء (٢٠٢١). الأبعاد الاجتماعية للجرائمالإلكترونية : دراسة تحليلية لمضمون عينة من القضايا في محكمة سوهاج .مجلة كلية التربية في العلوم الإنسانية والأدبية، مج٢٧، ع٣ .
١٨ – مرابط أحلام (٢٠٢٣) ، ثمثلات المخاطر بين التراث السوسيولوجي والخلفية الثقافية،مجلة آفاق للبحوث والدراسات، المركز الجامعي المقاوم الشيخ أمود بن مختار إيليزى ، مج ٦، ع ١،.
١٩- مصطفي أحمد(٢٠٢٢) ، دمج الأمن السيبراني في منظومة الأمن القومي : الأمن السيبراني والأمن القومي، مجلة إدارة الاعمال ، جمعية إدارة الأعمال العربية ، مصر ،ع ١٧٨ .
٢٠- هلال منال .(٢٠١٤) تكنولوجيا الاتصال والمعلومات، ط١ ،دار أسامة، الأردن.
٢١-٠جيلإلى شويرب(٢٠٢٣) ،مفهوم الحروب السبيرانية والأمن السيبراني ،مجلة الحقوق والحريات ،مج ١١، ع١ .
٢٢-أحمد فيصل (٢٠١٥)، المخاطر الاجتماعية ، المعهد العربى للتخطيط، ، الكويت ، مج ١٣ ، ع ١٢٤.

٢٣ –البوعزيزى محسن (٢٠١٧) ، تساؤلات حول صناعة الأمن والتهديدفي مجتمع المخاطر،مجلة الدراسات المإلبة والمصرفية ، الأكاديمية العربية للعلوم المإلبة والمصرفية ، مركز البحوث المإلبة والمصرفية ، مج ٢٥ ،ع ٢ .

٢٤ –بن علية بن جدو(٢٠٢٢)، تحديات الأمن السيبراني لمواجهة الجريمة الإلكترونية ، المجلة الجزائرية للامن الإنساني ، مج٧،ع ٢،

٢٥–توانا فريدون حسين، & أمير خداكرم محمد. (٢٠٢٣). العولمة الثقافية وعلاقتها بالقيم الاجتماعية من منظور أساتذة الجامعة دراسة ميدانية في جامعة السليمانية. مجلة جامعة بابل للعلوم الانسانية، ٣١(٢)،

٢٦– جاب الله، حكيمة. (٢٠٢١). انعكاسات الجريمة السيبرانية على البيئة الرقمية: دراسة في إلبات واستراتيجيات مكافحتها .حوليات جامعة الجزائر ١، مج٣٥، ع٣ .

٢٧ –زايد أحمد (٢٠٢٣) ، التحولات القيمية والثقافية في المجتمع ..إلى أين ؟ ، تحرير ومراجعة شيرين جابر ، مكتبة الأسكندرية مركز الدراسات الأستراتيجية .

٢٨–طاله لاميه (٢٠٢٠)، التهديدات والجرائم السبيرانية: تأثيرها على الأمن القومي للدول واستراتيجيات مكافحاتها ،مجلة معالم للدراسات القانونية والسياسية ، (٤)٢ .

٢٩––عدنان بهاء(٢٠١٩) ،انتقال التهديدات من الواقع إلى العالم الافتراضي ،مجلة جامعة بابل للعلوم الإنسانية ، العراق ،مج ٢٧،ع ٤.

٣٠ –عطية روان (٢٠٢٠) ، الجرائم السبيرانية ،المجلةالإلكترونية الشاملة متعددة التخصصات ، السعودية ، مج ٣ع ٢٤ .

٣١ –فوزى إسلام (٢٠١٩)، الامن السيبراني : الأبعاد الاجتماعية والقانونية : تحليل سيوسولوجى ، المجلة القومية الاجتماعية ، طنطا، مج ٥٦، ع ٢.

٣٢– قرني، أماني حمدي، خطاب & ,إيمان عبد المنعم. (٢٠٢٢). دور مواقع الإعلام الرقمي في حماية الأمن السيبراني .المجلة المصرية لبحوث الأعلام (٨٠)

٣٣– مركز المعلومات ودعم اتخاذ القرار (٢٠٢١) ، رئاسة مجلس الوزراء، جمهورية مصر العربية، المجلس الأعلى للأمن السيبراني ،الأستراتيجية الوطنية للأمن السيبراني ، ص ص ١–٩

٣٣– نور الهدى قادرى (٢٠٢٣) ،الجريمة السبيرانية وإلبات مكافحتها: مواجهة تحديات الأمن السيبراني، المجلة الجزائرية للحقوق والعلوم السياسية ، مج ٨ ، ع ١ ..

٣٤ –محارب محمد.(٢٠١٣) ،حرب في الفضاء الإلكتروني:اتجاهات وتاثيرات علي اسرائيل ، ،نابلس،العراق .

٣٥- إسماعيل عبد الكريم .(٢٠٢٢) ،تأثير الفضاء الافتراضي على الأمن القومي ، مجلة البحوث والدراسات ، جامعة قاصدى مرباح ، الجزائر، مج١٩،ع١،

٣٦ –شلوش ، نورة. ٢٠١٨. القرصنةالإلكترونية في الفضاء السيبراني "التهديد المتصاعد لأمن الدول". مجلة مركز بابل للدراسات الإنسانية،. (٨)، ٢.

٣٧–الجنفاوي & خالد مخلف. (٢٠٢٠). العوامل المؤدية للعودة إلى الجريمة وفقاً لتوجهات العاملين في أقسام الخدمة الاجتماعية في المؤسسات الإصلاحية في الكويت. مجلة كلية الخدمة الاجتماعية للدراسات والبحوث الاجتماعية، ١٨(العدد ١٨ الجزء الثانى).

٣٨ تريكي، حسان(٢٠١٥)، "عولمة الجريمة: الواقع والتحديات الأمنية الجديدة."مجلة دراسات وأبحاث ع١٩.

٣٩–طالة، لامية. ٢٠٢٠. التهديدات و الجرائم السيبرانية : تأثيرها على الأمن القومي للدول و استراتيجيات مكافحتها. معالم للدراسات القانونية و السياسية،. (٤) ٢.

٤٠–موسى دياب(٢٠٢٤) ، الجرائمالإلكترونية : المفهوم والأسباب، ورقة علمية منشورة في الملتقى العلمى الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية ، كلية العلوم الاستراتيجية ، عمان .

ثانياً: المراجع الأجنبية:

1-Adil Raoul. (2017) "Crimes and Laws Related to Internet users: an Overview," *SSRG International Journal of Economics and Management Studies*,4 (3).

2- Hubbard, D. W., & Seers, R. (2023). *How to measure anything in cyber security risk*. John Wiley & Sons.

3- Olsen, O. E., Kruk, B. I., & Hoyden, J. (2007). Societal safety: Concept, borders and dilemmas. *Journal of contingencies and crisis management, 15*(2)

4- Salah, Aznar & Abdulrazzaq, Maiwan. (2023). Cyber security: performance analysis and challenges for cyber attacks detection. Indonesian Journal of Electrical Engineering and Computer Science. 31.

5-Akinyetun, T. S. (2021). Poverty, Cybercrime and National Security in Nigeria. *Journal of Contemporary Sociological Issues*, *1*(2).

6-Bossler, A. M., & Berenblum, T. (2019). Introduction: new directions in cybercrime research. *Journal of Crime and Justice*, *42*(5),

7-Kemmerer, R. A. (2003, May). Cyber security. In *25th International Conference on Software Engineering, 2003. Proceedings.* IEEE.

8-Richardson, S. V. A., & Gilmour, N. (2015). Cybercrime and national security: A New Zealand perspective. *The European Review of Organized Crime (EROC)*, *1*(1),

9- Chen, S., Halo, M., Ding, F., Jiang, D., Dong, J., Zhang, S., & Ago, C. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities and Social Sciences Communications*, *10*(1), 1-10.

10- Das, S., & Kayak, T. (2013). Impact of cybercrime: Issues and challenges. *International journal of engineering sciences & Emerging technologies*, *6*(2),

11- NORTON ROSE FULBRIGHT. (2020) .Going Viral: Heightened Cyber and Corporate Crime Risks in the COVID-19 Pandemic. Norton Rose Fulbright,

12- Osman Gone, Md. Haidar Ali, Showrov, Md. Mahbub Alam, & Md. Abu Shameem. (2022).

13-Beck, U. (1992). *Risk society: Towards a new modernity* (Vol. 17). sage.

14- McQuade III, S. C. (Ed.). (2008). *Encyclopedia of cybercrime*. Bloomsbury Publishing USA.

15- Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of cyber security. *International Journal of Advanced Research in Computer and Communication Engineering*, *7*(11)

16- Traulsen, Janine & Bissell, Paul. (2010). (7) The risk society. International Journal of Pharmacy Practice. 11.

17-Goni, O., Ali, M. H., Alam, M. M., & Shameem, M. A. (2022). The Basic Concept of Cyber Crime. *Journal of Technology Innovations and Energy*, *1*(2),

18- Alarab Muhammad..(2016). Securing The Future: An Egyptian National Security Strategy, Issues in international Security, Spring,

19-Chareonwongsak, K. (2002). Globalization and technology: how will they change society?. *Technology in Society*, *24*(3),p 191.

20-Daricili, A. B., & Celik, S. (2022). National Security 2.0: The Cyber Security of Critical Infrastructure. *PERCEPTIONS: Journal of International Affairs*, *26*(2),

21-Tonge, A. M., Kasture, S. S., & Chaudhari, S. R. (2013). Cyber security: challenges for society-literature review. *IOSR Journal of computer Engineering*, *2*(12).

22-The Basic Concept of Cyber Crime. Journal of Technology Innovations and Energy, 1(2),

23-Riaz, A., & Riaz, A. (2015, November). Causes and consequences of cybercrimes: An exploratory study of Pakistan. In 2015 First International Conference on Anti-Cybercrime (ICACC) IEEE

24- Yildirim, E. (2016). The importance of information security awareness for the success of business enterprises. In Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity, July 27-31, 2016, Walt Disney World®, Florida, USA .Springer International Publishing.

Abstract

The study aimed to identify the social and economic dimensions of cybercrime, analyze the challenges and threats facing Egyptian national security as a result of cybercrime, how did cybercrime affect the emergence of new patterns of Egyptian national conflict, and what is the strategy of the Arab Republic of Egypt in confronting cybercrime? The study used a social survey approach on a stratified sample of 500 individuals from Fayoum University youth from practical and theoretical faculties, using a questionnaire tool. Among the most important results reached by the study:

-The study found that cybercrime increases directly through electronic emails by sending some fake emails that contain some viruses that help in penetration, to steal information and money and disrupt vital systems, and that there are many ways to avoid hacking, the most prominent of which is the use of strong passwords for each account. .

-The results of the study found that the social and economic dimensions of cybercrime are poverty, digital illiteracy, unemployment, social and political marginalization of the individual, and the excessive curiosity that he suffers from. So the individual resorts to proving himself by violating the privacy of others. Cybercrimes are

characterized by characteristics that distinguish them from other crimes, as they are committed in an environment It is virtual and does not leave a physical trace, making it difficult to detect.

-The results of the study concluded that potential threats to cybercrime include electronic hacking and cyberespionage through exploiting security vulnerabilities in the cyber infrastructure to access sensitive, confidential, and security information about governments, companies, and vital institutions. This information may be used to influence national decisions and industrial espionage.

-The results of the study found that one of the potential threats to cybercrime that threatens Egyptian national security is cyberwars. A state or a terrorist group may carry out attacks for the purpose of compromising the country's infrastructure, and its military, intelligence, and economic capabilities, and this affects national security.

-The results of the study found that among the threats facing Egyptian national security as a result of cybercrime is electronic extremism and its impact on the country's political systems, where the misuse of social networking sites and digital platforms to spread extremist ideas to influence public opinion and the political process in Egypt, and

exploiting the masses and the power of social media to achieve goals. Politically to stir up strife and divisions within the people.

-The results of the study concluded that among the strategies used to combat cybercrime is the strategy of international cooperation, because cybercrime crosses borders, so information and experiences must be exchanged, as legal aid is crucial for countries to solve any problem.

-The results of the study concluded that among the strategies used to combat cybercrime is the strategy of enhancing training and qualification: appropriate training must be provided to security personnel so that they have sufficient experience to deal with cyberthreats to collect digital evidence about any crime and analyze it in the appropriate manner.

-The results of the study found that among the strategies used to combat cybercrime is a quick response strategy and the development of a contingency plan for cyberattacks. There must be contingency plans and the necessary preparations to recover data, repair damaged systems, define responsibilities and procedures, and provide accountability.

Keywords: cybercrime – national security – cyberspace