علاقة الأمن السيبراني بالجرائم السيبرانية

The relationship of cybersecurity to cybercrime

الكاتب: حمزة المومني

أستاذ محاضر/ جامعة مؤتة

تاريخ الاستلام: ٢٠٢٣/٢/٢١ تاريخ القبول: ٢٠٢٣ /٢/٢٤ تاريخ النشر: ٢٠٢٤/٣/١٥

الملخص:

هدفت الدراسة الحالية إلى الكشف عن جرائم الأمن السيبراني والتي يتمثل في اختراق الأنظمة وسرقة المعلومات وتدميرها وتعطيلها والاحتيال والتجسس والإساءة والابتزاز وغيرها من الأنشطة الإجرامية التي تتم باستخدام التقنيات الحاسوبية والإلكترونية، وكما أنه هذه الجرائم تتسم بأنها تتم بشكل سريع ومن دون وجود أدلة مادية، مما يجعل من الصعب التحقيق فيها ومحاسبة المتسببين فيها، كما تشكل الجرائم السيبرانية تهديدًا خطيرًا للأمن السيبراني والاقتصاد الرقمي في جميع أنحاء العالم، وتتطلب جهودًا كبيرة للحد منها والحفاظ على الأمان والسلامة في الفضاء السيبراني.

لذلك يمكننا الرجوع إلى مثل هذه الدراسات والأدبيات السابقة والتي تمكننا من التعرف عليها والقيام بعلاجها أسهل صورة ممكنة، ويوصي الباحث بضرورة توفير دراسات تتحدث عن هذا الموضوع وبشكل أكثر دقة، كما يوصي الباحث المعنين بالاهتمام بمثل هذه الجرائم ومعرفة جميع الأسباب والعوامل التي تؤثر على أمنها.

الكلمات المفتاحية: الأمن السيبراني، وجرائم الأمن السيبراني.

Abstract

The current study aimed to detect cybersecurity crimes, which are represented by hacking systems, stealing information, destroying and disabling it, fraud, espionage, abuse, extortion, and other criminal activities that are carried out using computer and electronic technologies. These crimes are characterized by being carried out quickly and without the presence of physical evidence, which makes It is difficult to investigate and hold those responsible accountable. Cybercrimes pose a serious threat to cybersecurity and the digital economy around the world, and require significant efforts to reduce them and maintain security and safety in cyberspace.

Therefore, we can refer to such studies and previous literature, which enables us to identify them and treat them as easily as possible. The researcher recommends the necessity of providing studies that talk about this topic in a more precise manner. The researcher also recommends that those concerned pay attention to such crimes and know all the causes and factors that affect their security.

Keywords: cybersecurity, cybersecurity crimes.

المقدمة:

لقد ظهرت أساليب جديدة لإرتكاب الجريمة مع التطور الهائل للتكنولوجيا والمعلومات، فلم تعد الإعتداءات تستهدف المال والنفس فقط، بل أصبحت تمس المعلومات في البيئة الرقمية، فأصبح بإمكان المجرمين في الوقت الراهن ارتكاب أبشع الجرائم دون الانتقال من أماكنهم، وهذا الأسلوب الجديد لإرتكاب الجريمة أصبح يطلق عليه الإجرام السيبراني، ومن أجل فهم هذه الجريمة تم إعطاء تعريف لها في هذا الفصل وبيان أنواعها.

في ظل هذا التطور الهائل وما نتج عنه من ظهور تهديدات وجرائم سيبرانية أصبحت تشكّل تحدياً كبيراً للأمن القومي والدولي، أصبح من الضرورة دراسة الأمن السيبراني الذي يعمل على حماية البيانات والشبكات والأنظمة الالكترونية من الهجمات والاختراقات التي قد تودي بها وباستقرارها.

وللتعرف على مفهوم الجريمة السيبرانية وخصائصها وأنواعها، وبيان علاقتها بالأمن السيبراني خصص ثلاثة مباحث في هذا الفصل وهي:

المبحث الأول: مفهوم الجرائم السيبرانية وخصائصها

المبحث الثاني: أنواع الجرائم السيبرانية

المبحث الثالث: علاقة الأمن السيبراني بالجرائم السيبرانية

المبحث الأول: مفهوم الجرائم السيبرانية وخصائصها

يعد مصطلح الجرائم السيبرانية من المصطلحات الحديثة والتي تستخدم في جرائم الإنترنت الذي تعددت مصطلحاته، ونجد أن مصطلح الجرائم السيبرانية) crime cyber) هو مصطلح غير عربي، لكنه يتم تداوله واستخدامه في الوقت الحالي في تقنية المعلومات وهيئة الاتصالات.

أولاً: مفهوم الجريمة السيبرانية

وتعد هذه الجرائم أحد النتائج السلبية للتطور التكنولوجي، ونجد هذه الجرائم أخذت حيزاً كبيراً من الدراسات والأبحاث لتحديد مفهومها، فنجد العديد من الدراسات حاولت وضع تعريف للجرائم المرتكبة عبر الإنترنت، فتباينت هذه الجرائم في تسمياتها في مراحل تطورها(علي،٢٠١٩،ص:٢)، والتي ارتبطت بتطور تقنية المعلومات، فقد تسميها في بادئ الأمر " إساءة استخدام الكمبيوتر"، ثم "جرائم إحتيال الكمبيوتر"، ثم "الجريمة المعلوماتية"، "فجرائم الكمبيوتر" وبعدها، "جرائم التقنية العالية"، وبعدها"

جرائم الهاكرز" ثم "جرائم الإنترنت" وفي الوقت الحالي يتم تسميتها بالجرائم السيبرانية(cyber crime) (بونعارة، ٢٠١٥،ص:٣).

تعريف الجريمة السيبرانية لغوياً:

تعريف الجريمة لغة:

جاء تعريف الجريمة في اللغة لمعنيين وهما:

١- الذنب: بفتح أوله وسكون ثانيه، جمع ذنوب، الأثم والمعصية، ونقول جرم وأجرم، وأجتزم بمعنى واحد.

٢- الجناية: جنَى يجني، اجْنِ، جِنايةً، فهو جان، والمفعول مجنيّ للمتعدِّي جنَى الشخص: أي: أذنب، ارتكب جُرماً(لطفي،٢٠٢٠،ص:١٣).

تعريف السيبرانية لغة:

عرف قاموس أكسفورد كلمة (cyber) :"بأنها صفة لأي شيء يرتبط بتقنية المعلومات أو الواقع الافتراضي أو بثقافة الحاسوب" (الروضان، ١٤٣٩هـ).

تعريف الجريمة السيبرانية اصطلاحاً:

في كل مرة ظهر فيها مصطلح جديد لجرائم الإنترنت ظهر تعريفاً جديداً، فلم يستقر فقهاء القانون على تعريف واحد، فتنوعت المفاهيم والآراء، وذلك يرجع لحداثة الجرائم السيبرانية واختلاف الثقافات والقوانين بين الدول.

فمنهم من عرف الجرائم السيبرانية على أنها: نشاط إجرامي تستخدم فيه تقنية الحساب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المقصود"(القرعان،٢٠١٩، ص:٨).

وعرفها البعض على أساس محل الجريمة فقد عرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية على أنها: "الجرائم التي تلعب فيها البيانات والبرامج المعلوماتية دوراً رئيساً"(الدريبي،٢٠١٢، ص:٣٢).

وعرفها البعض بصياغة أخرى بأنها: الجرائم الناتجة عن استخدام التكنولوجيا والتقنية الحديثة المتمثلة في الكمبيوتر والإنترنت، بأعمال وأنشطة إجرامية تهدف إلى تحقيق عوائد جراء أعمال غير شرعية، يعاد ضخها في الاقتصاد الدولي عبر شبكة الإنترنت باستخدام النقود الإلكترونية(عبدالله،٢٠١٧،ص:٥).

https://scopmajd.com/ « ISI: (0.360) « ISSN (Online): 3005-2033

والبعض الآخر عرفها بأنها: " هي التي تتم بواسطة الحاسوب أو أحد وسائل التقنية الحديثة مع ضرورة توفر شبكة اتصال فيما بينهما" (مهمل،٢٠١٧، ص:٩).

ومنهم من عرفها بأنها: " السلوك غير المشروع أو المنافي للأخلاق أو غير المسموح به الذي يرتبط بالشبكات المعلوماتية العالمية، فهي جرائم العصر الرقمي التي تطال بالمال والمعرفة والثقة والسمعة وهي كلها تنفذ عن طريق التقنية (الربيعة،٢٠١٩، ص:٩).

ويرى بعض الخبراء أن الجرائم السيبرانية ليست التي يكون الحاسب أداة لإرتكابها، بل هي التي تقع عليه أو في نطاقه حيث يعرفون هذه الجريمة على أنها:" نشاط غير مشروع موجه لتغيير، أو نسخ أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحوله إلى طريقه"(رستم،٢٠٠٤، ص:٤٠٧).

ووضع البعض تعريف شامل للجريمة السيبرانية واعتبروا أن الجريمة السيبرانية هي الجريمة المرتكبة عبر الإنترنت حيث تم تعريفها على أنها:" الجريمة التي يستخدم فيها الحاسب الآلي كوسيلة أو أداة لإرتكابها، أو الجريمة التي يكون الحاسب الآلي نفسه ضحيتها"(حمديني،٢٠١٧، ص:٢).

ثانياً: خصائص الجريمة السيبرانية:

تختلف الجرائم السيبرانية عن الجرائم التقليدية التي ترتكب في العالم، لذلك تتسم الجرائم السيبرانية بخصائص جعلت منها ظاهرة إجرامية جديدة لم تكن من قبل ومن خلال هذا الفرع سوف يتم توضيح هذه الخصائص على النحو التالي:

١- جريمة ناعمة:

تتسم الجرائم السيبرانية بأنها ناعمة لخفتها، ولأنها متسترة في أغلبها، فالجاني من خلال هذه الجرائم يتمتع بقدرات فنية يتمكن من خلالها تنفيذ جريمته بدقة، كإرسال الفيروسات المدمرة وسرقة الأموال، والبيانات الخاصة والتجسس وغيرها من الجرائم، ويستفيد المجرمون من الشبكة في تبادل الأفكار، والخبرات الإجرامية فيما بينهم في مختلف مناطق العالم، ويتبادل المجرمين الخبرات في مجال القرصنة من أجل إرتكابهم لجرائمهم بعيداً عن أعين الأمن (بن صغير،٢٠١٥، ص:٨).

٢- جريمة عابرة للحدود:

لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر مختلف دول العالم بعد ظهور الشبكات، فالمقدرة التي تتمتع بها الشبكات في نقل المعلومات وتبادلها بين أنظمة تفصل بينها ألآف الأميال، جعلت من السهل إرتكاب الجريمة في أماكن متعددة من دول العالم (عبد المحمود،٢٠٠٧، ص:٥٢).

٣- صعوبة الوصول إلى دليل:

من الصعب الوصول إلى دليل في الجرائم السيبرانية على مرتكبيها، فتكون هذه البيانات والمعلومات المتداولة عبر شبكة الإنترنت على هيئة رموز يتم تخزينها في وسائط تخزين ممغنطة بلغة الصفر والواحد، ولا تقرأ هذه المعلومات إلا بواسطة الحاسب الآلي، والوقوف على الدليل الذي يمكن فهمه والتوصل عن طريقه إلى الجاني يكون أمراً صعباً، وخاصة إذا كان الجاني يسعى إلى إخفاء جريمتة (الكعبي،٢٠٠٩،ص:٣٧).

إن المعلومات والبيانات عبر شبكة الإنترنت تكون عبارة عن نبضات إلكترونية غير مرئية، مما يجعل أمر إخفاء الدليل ومحوه كلياً من قبل الفاعل أمرا في غاية السهولة، كما يسعى مرتكب الجريمة السيبرانية إلى إعاقة سلطات التحقيق في الوصول إلى الدليل بشتى الوسائل الممكنة كحذف البرامج أو وضع كلمات مرور ورموز سرية وتشفير المعلومات، فتزداد الأمور تعقيداً لدى أجهزة التحقيق، وسلطات الأمن(بن صغير، ٢٠١٥،ص:٨)، ومن بين صعوبات الوصول إلى الدليل أيضا هي قيام المواقع العالمية بإحاطة البيانات المخزنة على مواقعها بسياج من الحماية، لمنع التسلل، والوصول غير المشروع إليها لمراقبتها أو الإطلاع عليها أو لتدميرها(أرحومة، ٢٠١٠،ص:٣).

٤- تصادم التفتيش عن الأدلة مع الحق في الخصوصية المعلوماتية

يتم التفتيش في هذا النوع من الجرائم غالباً على نظم الكمبيوتر وقواعد البيانات وشبكات المعلومات، وقد يتجاوز التفتيش عن أدلة في بعض الجرائم إلى عدة أنظمة أخرى مرتبطة به، "نظراً لإنتشار التشبيك بين الحواسيب والشبكات الداخلية على مستوى المنشآت والشبكات المحلية والإقليمية والدولية على مستوى الدول، فيؤدي إمتداد التفتيش إلى نظم غير النظام محل الإشتباه فقد يمس الحق في خصوصية المعلومات لأصحاب النظم التي يمتد إليها التفتيش"(صغير،٢٠١٣، ص:٨).

٥- أقل عنفاً في التنفيذ:

إن جرائم السيبرانية لا تتطلب عنفاً أو مجهوداً كبيراً لتنفيذها، فهي يتم تنفيذها بأقل جهد ممكن مقارنة بالجرائم التقليدية التي تتطلب نوعاً من المجهود العضلي، والتي تتطلب ممارسة العنف والإيذاء كما هو الحال في جريمة القتل والإختطاف، أو في الكسر وتقليد المفاتيح في جريمة السرقة (المهيني،٢٠٠٠،ص:٢٠) ، وتتميز هذه الجرائم بأنها جرائم هادئة تحتاج إلى القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف لإرتكاب الأفعال غير المشروعة وتحتاج إلى الإنترنت مع وجود مجرم يتعامل مع الشبكة بخبرته وقدرته للقيام بجرائم مختلفة كالتجسس أو إختراق خصوصيات الغير وغيرها من الجرائم(صغير،٢٠١٣،ص:٩).

https://scopmajd.com/ « ISI: (0.360) « ISSN (Online): 3005-2033

٦- عدم قيام ضحايا الجريمة السيبرانية بتقديم الشكوى

من خصائص الجريمة السيبرانية، أنه لا يتم في أغلب الأوقات تقديم شكوى أو الإبلاغ عن الجريمة خوفاً من التشهير أو عدم إكتشاف الضحية لها، لذا تكتشف معظم جرائم الإنترنت بالمصادفة، أو بعد وقت طويل من إرتكابها،" لذلك أن الجرائم التي لم تكتشف هي أكثر بكثير من الجرائم التي تم كشفها، فالرقم مظلم وخطير بين حقيقة عدد الجرائم المرتكبة والعدد الذي تم إكتشافه" (حسين،٢٠٠٨، ص:٩).

٧- صعوبة ضبط الجرائم السيبرانية

يواجه رجال الشرطة القضائية، والمحققين، والقضاة أثناء تأديتهم لمهامهم صعوبات كبيرة تتعلق بإجراءات ضبط الجرائم المعلوماتية، وإضفاء الوصف القانوني المناسب والذي ينطبق على الوقائع المتعلقة بها، فيرجع ذلك إلى الطبيعة الخاصة لهذه الجرائم، فهي تتم في فضاء إلكتروني يتميز بالتغيير، والانتشار الجغرافي العابر للحدود، وصعوبة الوصول إلى دليل ملموس وتعود الصعوبة لعدة أسباب أبرزها:

- جريمة لا تترك أثراً بعد إرتكابها.
- تحتاج لخبرة فنية عالية للمحقق للتعامل معها.
- تعتمد على الخداع والإخفاء في ارتكابها.
- تحتاج لخبرة وذكاء مرتفع في إرتكابها.

٨- جريمة عن بعد:

تتسم الجرائم السيبرانية بأنها جرائم ترتكب عن بعد،" فيمكن للجاني تنفيذ جريمته وهو في دولة بعيدة كل البعد عن المجني عليه"(التميمي، ٢٠١٦، ص:١٦).

المبحث الثاني: أنواع الجرائم السيبرانية

أولاً: أنواع الجريمة السيبرانية

تتنوع الجرائم السيبرانية بحسب النظر إليها، فعند النظر إلى قصد الجاني يتم تقسيم هذه الجريمة إلى عمدية وغير عمدية، فالجريمة السيبرانية تتطلب المعرفة التخصصية بالكومبيوتر والإنترنت فهذا الأمر لا يتوافر عند جميع الأفراد في المجتمع، بل يتوافر عند الأفراد المتعلمين، والمتابعين باستمرار لكل ما هو جديد في وسائل الاتصالات الحديثة، وقد بدأت اصابع الإتهام والخوف اتجاه نحو المتعلمين بسبب ظهور إجرام على نحو عالي من التخصص والتقنية المتطلبة في مرتكب الجريمة السيبرانية حيث وصل الأمر إلى الإستعانة بالعلماء والخبراء من أجل إرتكاب الجريمة.

وتقع الجريمة السيبرانية في أغلبها بصورة عمدية يسبقها التفكير، والتخطيط في الحصول على المعلومات وإختراق الحاسوب والإنترنت من أجل تحقيق المنفعة أو الهدف المرسوم للجاني، فتكون هذه الجرائم للإستحواذ بغير حق على مبالغ نقدية من الأرصدة أو وسيلة لتدمير معلومات، أو وسيلة لمحو معلومات لمحاولة إزالة آثار الجريمة، أو استخدام الفايروسات للتدمير، وجرائم القذف أو السب أو التحريض على الفسق والفجور فكل هذه الجرائم تتطلب تخطيط وتفكير المجرب فهي بذلك جريمة عمدية. وتكون الجريمة غير عمدية إذا وقعت النتيجة الإجرامية بسبب خطأ الفاعل سواء كان هذا الخطأ إهمالاً أو رعونة أو عدم انتباه أو عدم مراعاة للقوانين والأنظمة والأوامر، فتكون الجريمة بصفة عامة غير عمدية إذا أراد الفاعل السلوك ولم تتجه إرادته للنتيجة الجرمية، فمن يقوم بالاعتماد على مهاراته في تلافي مشاكل الفايروسات وأدى ذلك لتدمير أجهزة الدائرة التي يعمل فيها نتيجة استخدامه جهاز الكومبيوتر العائد للدائرة بعمليات لحسابه الخاص تكون مسؤوليته هنا غير عمدية ، وكذلك الموظف الذي يستخدم أقراص مرنة خاصة به ولم يتأكد من خلوها من الفايروسات في أجهزة دائرته وأدت إلى نقل الفايروسات لهذه الأجهزة أو تسببت في تدميرها ، وغيرها من الحالات(السمحان،٢٠٢٠،ص:١٣).

ومن أبرز أنواع الجرائم السيبراني هي(الصحفي، ٢٠٢٠ ،ص:١٧):

١- جرائم التعدي على البيانات المعلوماتية:

هي الجرائم التي تقع على بيانات معلوماتية، وهي جرائم التعرض للبيانات المعلوماتية، والبيانات هي كل ما يمكن تخزينه ومعالجته، ونقله بواسطة الحاسب الآلي كالأرقام والحروف والرموز وما إليها.

٢- جرائم التعدي على الأنظمة المعلوماتية:

هي الجرائم التي تتعرض للبيانات المعلوماتية بطريقة غير مشروعة، والعمل على إعاقة عمل معلوماتي، ويتمثل النظام المعلوماتي في مجموعة البرامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات.

٣- جرائم التعدي على الملكية الفكرية للأعمال الرقمية:

هي الجرائم التي تقوم على وضع اسم مختلس على عمل ما، وتقليد إمضاء المؤلف أو ختمه، وتقليد عمل رقمي أو قرصنة البرمجيات، أو بيع أو عرض عمل مقلد أو وضعه في التداول، والاعتداء على أي حق من حقوق المؤلف أو الحقوق المجاورة.

https://scopmajd.com/ « ISI: (0.360) « ISSN (Online): 3005-2033

٤- جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية:

هي الجرائم التي تقوم على نشر وتوزيع المعلومات العنصرية بوسائل معلوماتية أو تهديد أشخاص أو التعدي عليهم بسبب انتهائهم العرقي، أو المذهبي أو لونهم أو توزيع معلومات بوسيلة إلكترونية من شانها تشويه أو تبرير أعمال إبادة جماعية أو جرائم ضد الإنسانية أو المساعدة أو التحريض بوسيلة إلكترونية على ارتكاب جرائم ضد الإنسانية

٥- الجرائم المعلوماتية ضد الدولة والسلامة العامة:

هي الجرائم التي تتضمن الأفعال الجرمية الناشئة عن المعلوماتية التي تطال الدولة وسلامتها وأمنها واستقرارها فتقوم على تعطيل الأعمال الحكومية أو أعمال السلطة العامة باستعمال وسيلة معلوماتي أو الحصول على معلومات سرية تخص الدولة من خلال شبكة الإنترنت أو باستعمال وسيلة معلوماتية، والعبث بالأدلة القضائية المعلوماتية أو إتلافها أو إخفائها، والأعمال الإرهابية التي ترتكب باستخدام شبكة الإنترنت أو أي وسيلة معلوماتية.

٦- جرائم تشفير المعلومات:

تشمل هذه الجرائم أفعال أو تصدير أو استيراد وسائل التشفير، وتوزيعها، وأفعال تقديم وسائل التشفير التي تؤمن السرية دون حيازة تصريح أو ترخيص من قبل المراجع الرسمية المختصة في الدولة، وبيع أو تسويق أو تأجير وسائل تشفير ممنوعة.

ثانياً: تصنيف مرتكبي الجرائم

يمكن تصنيف مرتكبي الجرائم السيبرانية إلى ثلاث مجموعات:

١- العاملون في مجال الأنظمة المعلوماتية:

إن النظام المعلوماتي هو مجال العمل الأساسي للعاملون في الأنظمة المعلوماتية، ونظرا للمهارات والمعرفة التقنية التي يتمتعون بها، فإنهم يقترفون بعض الجرائم المعلوماتية التي تحقق أهدافهم الشخصية، ومنها الكسب المادي، وتمثل هذه الفئة الغالبية العظمى من مرتكبي هذه الجرائم (عطوي،٢٠١٢، ص:١٣). ويتمتع المجرم السيبراني بالمهارة والمعرفة بتقنيات الحاسوب والإنترنت، فالبعض من مرتكبي هذه الجرائم هم من المتخصصين في مجال معالجة المعلومات، فيتمتع هذا المجرم بإحترافية كبيرة في تنفيذ جرائمه، فتنفيذ هذه الجرائم يتطلب الكثير من الدقة، والإحترافية بهدف التغلب على العقبات التي أوجدها المجرمون لحماية أنظمة المعلومات كما في حالة البنوك، والمؤسسات العسكرية، والمواقع الخاصة بالحكومة (رصاع،٢٠١٢،ص:٥١).

٢- الحاقدون

يرتكبون أفراد هذا الصنف أنشطتهم الإجرامية بدافع الرغبة في الإنتقام، وتتوفر لديهم أسباب للإنتقام من الشخص المستهدف في نشاطهم كالذين يقومون بإستخدام الكمبيوتر لمسح بعض المعلومات الخاصة بالشركة أو المؤسسة، كطريقة للإنتقام من المؤسسة لأسباب يعرفها مرتكبي هذا الفعل (جعفر،٢٠١٣،ص:١١٧).

٣- القراصنة:

هم المبرمجون من أصحاب الخبرة، يسعون إلى الدخول إلى الأنظمة المعلوماتية التي يكون غير مسموح لهم بدخولها، وكسر كل الحواجز الأمنية المحيطة بهذه الانظمة، ويمكن تصنيفهم إلى القراصنة الهاكرز ويكون هذا الصنف من هواة التكنولوجيا والحواسيب يرون في إختراق الأنظمة المعلومات تحدياً لقدراتهم وفضول التعمق في هذه الأنظمة وفي العادة لا يكون لهم أي أهداف أو دوافع تخريبية وراء أعمالهم، أما الصنف الثاني وهو القراصنة المحترفون ويعد هذا الصنف هو الأخطر على الإطلاق لأن المجرم يدرك أهدافه، وكيفية الوصول إليها مسبقاً، وذلك بإستخدام مهاراته و علم يطوره بإستمرار، فهدفه سحب الأموال من الأرصدة، و الوصول إلى أخطر المواقع وأكثرها حساسية وإختراقها و التلاعب بالبيانات، فلهذه الفئة ميول إجرامية خطيرة وواضحة، تفصح عن رغبتهم في إحداث التخريب والسرقة(مراد،د.ت،ص:٤٥).

ويستخدم المجرم السيبراني تقنية الاختراق لتنفيذ جريمته من خلال القدرة على الوصول إلى هدف معين عن طريق ثغرات في نظام الحماية الخاصة. ويستخدم المجرم السيبراني عدة برامج لتنفيذ جرائمه منها:

- القصف السيبراني: هو الهجوم على شبكة المعلومات، والتسبب بضغط كبير على الموقع فيفقد الموقع قدرته على استقبال الرسائل من العملاء، ويتوقف عن العمل تماماً.
- حصان طراودة: هو برنامج صغير يختبئ ببرنامج أخرى أكبر تؤدي مهامها من حلال شكل خفي في إطلاق الفيروسات التي تقوم بإرسال البيانات عن الثغرات الموجودة في النظام، وارسال كلمات المرور السرية الخاصة بالهدف.
- فيروسات الكمبيوتر: هي برامج صغيرة تستخدم لتعطيل شبكات الخدمات.
- الديدان: هي تكاثر من خلال نسخ نفسها عن طريق الشبكات ويكون هدفها الشبكات المالية كالبورصات.
- الأبواب الخلفية: هي ثغرة يتم تركها عن عمد من مصمم النظام للتسلل إليه وقت الحاجة.
- الإختناق المروري السيبراني: وهو سد وخنق الاتصالات لدى المستهدف حتى لا يتمكن من تبادل المعلومات.

https://scopmajd.com/ « ISI: (0.360) « ISSN (Online): 3005-2033

المبحث الثالث: علاقة الأمن السيبراني بالجرائم السيبرانية

أولاً: مفهوم الأمن السيبراني

يعتبر مفهوم الأمن السيبراني من المفاهيم الحديثة والمثيرة للإهتمام والدراسة فيعرف على أنه عبارة عن وسائل دفاعية تستخدم لكشف وإحباط المحاولات التي يقوم بها القراصنة"بينما يعرفه البعض على أنه: مجموعة من الوسائل التي من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات التي تستخدم في مواجهة القرصنة وكشف الفيروسات وتوقيفها، وتوفير الاتصالات المشفرة(جبور،٢٠١٢، ص:١٦)

يعرف البعض الأمن السيبراني على أنه: " عبارة عن مجموعة من الوسائل التقنية، والتنظيمية، والإدارية يتم استخدامها لمنع سوء استغلال المعلومات الإلكترونية، ونظم الاتصالات، والمعلومات وتعزيز سرية وخصوصية البيانات الشخصية، وحمايتها واتخاذ التدابير اللازمة لحماية المواطنين من المخاطر في الفضاء السيبراني"(العوادي،٢٠١٦،ص:٦)

وعرفه البعض بأنه: "مجموعة من الوسائل التي من شأنها الحد من الخطر الذي يهاجم البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة"(السمحان،٢٠٢٠،ص:٩-١٠).

ويعد مفهوم الأمن السيبراني مفهوم شامل وأوسع من أمن المعلومات، فالأمن السيبراني يهتم بأمن كل ما هو موجود على السايبر من غير أمن المعلومات، بينما أمن المعلومات يهتم بأمن المعلومات الفيزيائية " الورقية"، بينما الأمن السيبراني لا يهتم بذلك (المرجع السابق).

وهناك العديد من المفاهيم التي ترتبط بالأمن السيبراني ومن أهمها:

الفضاء السيراني: "هو المجال المادي وغير المادي الذي يتكون وينتج عن عناصر هي: الشبكات، البرمجيات، الكمبيوتر، أجهزة الكمبيوتر، المحتوى، معطيات النقل والتحكم، ومستخدمو هذه العناصر"(زروقة، ٢٠١٨ص:١٠١٧).

الردع السيبراني: "منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية".

الهجمات السيبرانية هي": عمليات سيبرانية تقوم بها الدولة أو مجموعات حكومية أو غير حكومية سواء كانت هجومية أو دفاعية، يهدف من خلالها التسبب بالإصهابة أو وفاة الأشخاص أو الإضهرار وتدمير الأهداف ضد خصم معين، وذلك عن طريق الدخول قصداً بطريقة غير مشروعة إلى جهاز حاسوبي أو منظومة معلوماتية أو موقع إلكتروني على الإنترنت"(الموصلي،٢٠١٠،ص:١٠).

ويرتبط أيضاً مفهوم الأمن السيبراني بالجريمة السيبرانية وسيتم ذكر العلاقة بينهما في هذا المبحث لاحقاً.

ثانياً: أهداف الأمن السيبراني وأبعاده

من أهداف الأمن السيبراني أيضاً(السمحان،٢٠٢٠، ص:١٢) :

- تعزيز حماية أنظمة التقنيات التشـغيلية على كافة الأصـعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحويه من بيانات.
- توفير بيئة آمنة موثوقة للتعاملات في مجتمع المعلومات.
- توفير المتطلبات الأزمة للحد من الجرائم الإلكترونية التي تستهدف المستخدمين.
- سد الثغرات في أنظمة أمن المعلومات.
- التصدي للبرمجيات الخبيثة ومقاومة ما تستهدفه من أحداث أضرار بالغة.
- اتخاذ مجموعة من التدابير اللازمة لحماية المواطنين من المخاطر في مجالات استخدام الإنترنت المختلفة.
- تدريب الأفراد على آليات جديدة لمواجهة التحديات الخاصة بإختراق الأجهزة التقنية بقصد الضرر بمعلوماتهم الشخصية سواء بالإتلاف أو بقصد السرقة.

يخص الأمن السيبراني جميع المسائل الاقتصادية، والاجتماعية والسياسية، والإنسانية، ويرتبط ارتباطاً وثيقاً بسلامة مصادر ثروة المعلومات في العصر الحالي لذا لا من التوقف عند أبعاد الأمن السيبراني، على أن نستعرضها كما يلي:

- الأبعاد العسكرية: إن أهمية الأمن السيبراني في هذا البعد تنشأ من خطورة الهجمات السيبرانية التي تؤدي إلى نشأة الصراعات المسلحة، والحروب، واختراقات الأنظمة للمنشأة النووية، فينتج عنها تهديدات لأمن الدول والحكومات وتؤدي هذه الهجمات إلى الكوارث، وتتراكم الأمثلة التي يمكن ذكرها في هذا المجال، لتوضيح الأبعاد العسكرية للأمن السيبراني، وخطورة الهجمات السيبرانية، حيث يمكن ذكر ما حصل في جورجيا، وكوريا الجنوبية، كمثال على بعض الهجمات السيبرانية التي ترجمت مادياً، باندلاع الصراعات المسلحة. ويمكن ذكر الهجمات التي حصلت على الولايات المتحدة حيث انقطع التيار الكهربائي فنتج عن آثار سلبية وطالت هذه الآثار ملايين الأشخاص والمؤسسات والمصالح(قورة،٢٠١٥).
- الأبعاد السياسية: تقوم الأبعاد السياسية في الأمن السيبراني على أساس حماية نظام الدولة السياسية من استخدام التقنيات في بث المعلومات والبيانات لزعزعة استقرار أمن الدول والحكومات، وتتمثل الأبعاد السياسية في الأمن السيبراني في حق الدولة على حماية أنظمتها، وواجبها في السعي لتحقيق استقرار وأمن شعبها في وقت تأثير التقنيات، وقد أصبح بإمكان

https://scopmajd.com/ « ISI: (0.360) « ISSN (Online): 3005-2033

المواطن، أن يتحول إلى لاعب أساسي، في اللعبة السياسية. فأصبح بإمكانه الإطلاع على مبررات القرارات السياسية، التي تتخذها الحكومة في دولة عبر الكم الهائل من المعلومات، التي يمكنه الوصول إليها عبر الإنترنت(البشري،٢٠١٤،ص:٣٣).

- الأبعاد الاقتصادية: يرتبط الأمن السيبراني ارتباطاً وثيقاً بالحفاظ على اقتصاد كل دولة فتتيح تقنيات المعلومات والاتصالات، تعزيز التنمية الاقتصادية لدول كثيرة، عبر إفادتها من فرص الاستخدام، التي تقدمها الشركات الدولية والكبيرة التي تبحث عن إدارة كلفة إنتاجها، بأفضل الشروط، إلا أن هذا يطرح مسائل عديدة منها ما يتعلق بحماية العمل وحماية المستهلك على شبكات الإنترنت. وقد دخل العالم العصر المالي الإلكتروني بعد إطلاق خدمات المحفظة الإلكترونية، وتزايد استخدام المصارف، والمؤسسات المالية، حيث تتنافس الشركات على إصدار التقريرات التي تسمح باستخدام آليات دفع آمنه للأفراد، وقد وضعت بعض الدول تشريعات خاصة بهذه الأموال للحد من بعض الجرائم الاقتصادية والمالية الخطيرة، كتبييض الأموال.
- الأبعاد القانونية: يترتب على النشاط الفردي والمؤسساتي والحكومي في الأمن السيبراني نتائج قانونية، تستدعي إيجاد قواعد خاصة لحل النزاعات التي تنشأ عنها فلا بد من مراعاة التحولات، التي رافقت ظهور مجتمع المعلومات، فقد تم إضافة حقوق جديدة غير الحقوق الأساسية، والحريات الإنسانية المعترف بها في الدساتير، والتشريعات الدولية، كحق النفاذ إلى الشبكة العالمية للمعلومات.

رابعاً: علاقة الأمن السيبراني بالجرائم السيبرانية

مع تطور التقنيات ووسائل تخزين المعلومات والاعتماد المجتمعي على البرمجيات أو أجهزة الحاسوب وشبكات الإنترنت، أصبح من الضروري على كل فرد من أفراد المجتمع معرفة المفاهيم الأساسية لمصطلح الأمن السيبراني ومن أهم هذه المفاهيم مصطلح الجريمة السيبرانية الذي يعد من أبرز المفاهيم التي تتعلق بسلامة المحتوى، وتأمينه من التلاعب ومحاسبة المخترقين.

أعتمدت المؤسسات في السنوات الأخيرة بشكل كبير على تقنية المعلومات في تنفيذ أعمالها وشكلت شبكات التواصل وسطاً تنساب فيه البيانات، وتخزن فيه المعلومات وبذلك تحتاج هذه المحتويات إلى حماية تصون عملها، وتضمن استمراريتها، ونظراً للجرائم السيبرانية التي تهدد سلامة البيانات والمعلومات المخزنة في الشبكات، وتعدد الأخطار التي تهدد استقرار تلك الشبكات و أمنها كالإصابة بالفيروسات والبرامج الضارة ومحاولات الاختراق لأغراض سرقة المعلومات أو التخريب أو التعديل، تأتي أهمية الأمن السيبراني لحماية مكونات شبكات المعلومات المادية والبرمجية بوضع أجهزة وبرامج الحماية في بوابات الشبكات لإدارة تلك الأجهزة والبرمجيات وسد الثغرات للتضييق على القراصنة والمنافسين والأعداء من التمكن، من اختراق أو سرقة أية بيانات من شبكات المعلومات(أبو حسين، ٢٠٢١،ص:٣٨).

في ظل التطور الهائل في وسائل الاتصال وأجهزة الاتصالات بلغ مستخدمي وسائل التواصل الاجتماعي في الفترة الأخيرة ما يتجاوز مليار ونصف مستخدم نشط (رستم،٢٠٠٩)، وفي ظل هذا التوسع الهائل في استخدام تكنولوجيا الاتصالات ارتفعت الرقابة ووسائل التجسس على مؤسسات الدولة، وعلى الأفراد، وهذا جعل حياة الأفراد وخصوصياتهم مخترقة بشكل كبير، وكثرت عمليات الجرائم الإلكترونية، وعمليات الابتزاز، ولم يعد يسلم المسؤول أو المواطن من هذه الجرائم.

ويهدف الأمن السيبراني إلى تعزيز حماية جميع ما يتعلق بالدولة إلكترونياً، كحماية الأنظمة الإلكترونية، وأنظمة تقنية المعلومات، وحماية جميع مكونات أنظمة التقنيات التشغيلية المحيطة بالمجتمع من أجهزة، وبرمجيات، فأصبحت هذه من أهم الأولوليات المهمة لدول العالم للحفاظ على بيانات مواطنيهم، وحفظ ممتلكاتهم وبياناتهم الإلكترونية، فقد أنشأت الدول الكليات والمعاهد ومراكز البحوث للتعمق في الأمن السيبراني حتى يتم معرفة كل شيء يقوم بتوفير الحماية للمواطنين، والمجتمعات، ومعرفة أهم ما يقوم به الأمن السيبراني وهو (أبو حسين،٢٠٢١،ص:٣٩):

- حماية شبكة المعلومات والاتصالات التي تلعب دوراً كبيراً في تدفق البيانات بين المواطنين والدولة من الأخطار التي إذا تعرضت لها كالتخريب أو التدمير أو الاختراقات التي حتماً قد تؤثر على الاتصالات وتقوم بقطعها، وتوقيف الخدمات، وسير العمل.
- "حماية شبكة المعلومات من أي هجوم، وكشف أهداف العدو والتعرف على طبيعة المهاجم، من خلال معرفة تكنيكاته وأساليبه المستخدمة، لكي يتم التصدي لهذا الهجوم بأسلوب علمي وتقني".
- تشفير التعاملات الإلكترونية من إختراق البيانات والتطبيقات لأن التشفير هو أحد أساليب الحماية التي يصعب فك رموزها.

ومن أجل إنجاز هذه المهمة يجب الحصول على أفضل وسائل التكنولوجيا، لحماية الأمن الوطني والبيئة المعلوماتية لكل المؤسسات، وبالإضافة لعمليات التدريب والتوعية لأفراد المجتمع، وهذا يتطلب تكاليف عالية لا تتحملها أي مؤسسات فردية، فكان من الضرورة إنشاء هيئات وطنية للأمن السيبراني، وتشريع قوانين تحمي المؤسسات والأفراد من الجرائم الإلكترونية.

https://scopmajd.com/ « ISI: (0.360) « ISSN (Online): 3005-2033

التحليل:

تناول هذا الفصل مفهوم الجريمة السيبرانية فهو أحد الجرائم المعاصرة التي أصبحت تشكل خطراً على الأفراد والمجتمعات وعلى أمن الدولة، فهي تتقدم بوتيرة سريعة باستخدام المجرمون لأحدث التقنيات في تنفيذ هجماتهم السيبرانية، لذا كان علينا مواكبة الجرائم السيبرانية والتعرف على طرق التصدي لهذه الجرائم المستحدثة بسن القوانين والأنظمة التي تختص بمكافحة الجرائم السيبرانية وفرض العقوبات على المجرمين. وتعرف الجريمة السيبرانية على أنها الجرائم الناتجة عن استخدام التكنولوجيا والتقنية الحديثة المتمثلة في الكمبيوتر والإنترنت، بأعمال وأنشطة إجرامية تهدف إلى تحقيق عوائد جراء أعمال غير شرعية، يعاد ضخها في الاقتصاد الدولي عبر شبكة الإنترنت باستخدام النقود الإلكترونية.

وتختلف الجرائم السيبرانية عن الجرائم التقليدية التي ترتكب في العالم ، فتتسم هذه بخصائص جعلت منها ظاهرة إجرامية جديدة لم تكن من قبل فتتسم هذه الجرائم بأنها بأنها ناعمة لخفتها، ولأنها متسترة في أغلبها، فالجاني من خلال هذه الجرائم يتمتع بقدرات فنية يتمكن من خلالها تنفيذ جريمته بدقة، ومن الصعب الوصول إلى دليل في هذ الجرائم على مرتكبيها، فتكون هذه البيانات والمعلومات المتداولة عبر شبكة الإنترنت على هيئة رموز يتم تخزينها في وسائط تخزين ممغنطة بلغة الصفر والواحد، ولا تقرأ هذه المعلومات إلا بواسطة الحاسب الآلي، ولا تتطلب هذه الجرائم عنفاً أو مجهوداً كبيراً لتنفيذها، فهي يتم تنفيذها بأقل جهد ممكن مقارنة بالجرائم التقليدية التي تتطلب نوعاً من المجهود العضلي، والتي تتطلب ممارسة العنف والإيذاء، وتتسم هذه الجرائم بأنها جرائم عابرة للحدود.

ومن أهم المفاهيم المرتبطة بالجرائم السيبرانية هو الأمن السيبراني الذي يعمل على حفظ وحماية المعلومات الموجودة على الشبكات، ويحرص على تقديم المعلومات الصحيحة ومن مصادر موثوقة للمستخدمين، وهذا يبث الأمن والطمأنينة في المجتمع، ويتيح للمستخدمين إضافة معلوماتهم الشخصية على الشبكة العالمية، ويعمل أيضاً على حماية الأمن في الدولة، وذلك لما يقدمه من حماية معلومات الأفراد والهيئات والمنظمات الموجودة في الدولة.

ويخص الأمن السيبراني جميع المسائل الاقتصادية، والاجتماعية والسياسية، والإنسانية، ويرتبط ارتباطاً وثيقاً بسلامة مصادر ثروة المعلومات في العصر الحالي، ومن أبرز أهدافه التصدي للجرائم السيبرانية ومقاومة ما تستهدفه من أحداث أضرار بالغة، واتخاذ مجموعة من التدابير اللازمة لحماية المواطنين من هذه الجرائم.

ومع تطور تكنولوجيا المعلومات والاتصالات، ووسائل تخزين المعلومات، واعتماد الأفراد على تقنيات الهواتف الذكية، وتبادل البيانات بطرق مختلفة إضافة، وتطور أساليب المخترقين، أصبح من الضروري على كل فرد من أفراد المجتمع معرفة المفاهيم الأساسية لمصطلح الأمن السيبراني، فهو من المفاهيم التي تتعلق بسلامة المحتوى وتأمينه من التلاعب ومحاسبة المخترقين.

المراجع:

ابن منظور، محمد بن مكرم بن علي، لسان العرب، المؤلف: محمد بن مكرم بن منظور المصري, الناشر: دار صادر -بيروت, الطبعة الأولى, عدد الأجزاء: ١٥.

أبو حسين، حنين جميل (٢٠٢١)، الإطار القانوني لخدمات الأمن السيبراني، رسالة ماجستير في القانون، كلية الحقوق، جامعة الشرق الأوسط.

أرحومة، موسى مسعود (٢٠١٠) ، الإشكاليات الإجرامية التي تثيرها الجريمة المعلوماتية عبر الوطنية" ، مداخلة مقدمة ضمن فعاليات المؤتمر المغاربي الأول الذي نظمته أكاديمية الدراسات العليا بطرابلس، الموسوم بعنوان: المعلوماتية والقانون.

البشـــري، محمد أمين (٢٠١٤)، التحقيق في الجرائم المســـتحدثة، الرياض: جامعة نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث.

البداينة، ذياب موسى (٢٠١٤)، " الجرائم الإلكترونية المفهوم والأسباب "، ورقة علمية مقدمة في الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، كلية العلوم الإستراتيجية، الأردن.

الزرفي، علي نعمة جواد (٢٠١٩)، الجريمة المعلوماتية الماسة بالحياة الخاصة دراسة مقارنة، المكتب الجامعي الحديث، بدون طبعة .

العوادي، أوس جميد غالب (٢٠١٥) الأمن المعلوماتي السيبراني، مركز البيان للدراسات والتخطيط.

السمحان، د. مني عبد الله (٢٠٢٠)، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، جامعة المنصورة، العدد١١١.

الصـحفي، روان بنت عطية الله (٢٠٢٠)، الجرائم السيبرانية، المجلة الإلكترونية الشاملة متعددة التخصصـات، المملكة العربية السعودية، العدد٢٤.

الكعبي، محمد عبيد (٢٠٠٩) ، الجرائم الناشـئة عن الإسـتخدام غير المشـروع لشـبكة الإنترنت، الطبعة الثانية، دار النهضة العربية، القاهرة.

المحمود، عباس أبو شـــامة (٢٠١٧)، " عولمة الجريمة الاقتصـــادية "، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض.

بونعارة، ياسمينة (٢٠١٥)، " الجريمة الإلكترونية "، مجلة المعيار، جامعة الأمير عبد القادر كلية أصول الدين، المجلد الثاني، العدد ٣٩.

بن صـــغير، د المؤمن (٢٠١٥)، " الطبيعة الخاصـــة للجريمة المرتكبة عبر الإنترنت في التشـــريع الجزائري والتشـــريع المقارن "، مداخلة مقدمة ضمن فعاليات الملتقى الوطني الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة محمد خيضر بسكرة، الموسوم بعنوان: الجريمة المعلوماتية بين الوقاية والمكافحة.

حمديني، ابتســـام. (٢٠١٧)" أســـلوب التحقيق في الجرائم الإلكترونية كآلية لمكافحتها "، مداخلة مقدمة ضـــمن فعاليات الملتقى الدولي الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة برج بوعريريج، الموسوم بعنوان: إلجرام السيبراني المفاهيم والتحديات.

جبور، منى الأشـــقر (٢٠١٢)، الأمن الســـيبراني: التحديات ومســـتلزمات المواجهة"، المركز العربي للبحوث القانونية والقضائية.

صـــغير، يوســـف. (٢٠١٣)، الجريمة المرتكبة عبر األنترنت، مذكرة ماجســـتير، جامعة مولود معمري تيز ي وزو، كلية الحقوق والعلوم السياسية، قسم الحقوق.

رستم، هشام محمد فريد (٢٠٠٤)، " الجرائم المعلوماتية أصول التحقيق الجنائي الغني واقتراح إنشاء آلية حربية موحدة للتدريب التخصـــصـــي"، الطبعة الثالثة، بحوث مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات المتحدة كلية الشـــريعة والقانون، المجلد الثاني.

زروقة، إسماعيل. (٢٠١٨)، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية،جامعة محمد بو ضياف المسيلة، الجزائر، المجلد١٠،العدد١.

عطوي، مليكة. (٢٠١٢)، الجريمة المعلوماتية، حوليات جامعة الجزائر، العدد٢١ .

عبابنة، محمود أحمد (٢٠٠٩)، جرائم الحاسوب وأبعادها الدولية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان.

قورة، نائلة عادل (٢٠١٥)، جرائم الحاسب الأقتصادية، رسالة دكتوراه منشورة، ط١ ،دار النهضة العربية، القاهرة.

مهمل، سامة (٢٠١٧) ، الإجرام السيبراني ، رسالة ماجستير ، كلية الحقوق والعلوم السياسية ، جامعة محمد بوضياف.