آليات مكافحة الجرائم السيبرانية
في المملكة العربية السعودية
"دراسة تحليلية"

د. رانا مصباح عبد المحسن عبد الرازق
أستاذ القانون الجنائي المساعد بقسم القانون
الكلية التطبيقية- جامعة الأميرة نورة بنت عبد الرحمن

(ISSN: 2537 - 0758)

آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية "دراسة تحليلية"

د. رانا مصباح عبد المحسن عبد الرازق

الملخص

تهدف الدراسة إلى التعرف على آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية، حيث تعد هذه الجرائم من الجرائم المستحدثة التي تمثل خطرًا وتهديدًا على أمن الفرد والمجتمع وعلى كافة الأجهزة الأمنية في الدولة. وقد أدى التطور السريع في مجال تقنية المعلومات والاتصالات وشبكة الإنترنت في العالم كله إلى ظهور أنماط جديدة من الجرائم جاءت عن طريق الاستغلال السَّيِّئ للتكنولوجيا، مما ترتب معه خلق ظاهرة إجرامية جديدة، وهي الجرائم المتعلقة بالحاسب الآلي والإنترنت، فظاهرة الجرائم السيبرانية تعتبر نتاج طبيعي لثورة الاتصالات والتكنولوجيا والتي أصبحت واسعة الانتشار، والتي تحدث عن طريق هجمات واختراقات وتسلل داخل النظم المعلوماتية بهدف تدميرها أو الحصول على معلومات سرية سواء عسكرية أو اقتصادية. لذلك سعت المملكة العربية السعودية لحماية مصالحها الوطنية من أي تهديدات أو مخاطر يشهدها الفضاء السيبراني، حيث قامت بإنشاء الهيئة الوطنية للأمن السيبراني بالأمر الملكي رقم٦٨٠١ بتاريخ ١١/ ٢/ ١٤٣٩هـ، لتكون هذه الهيئة هي الجهة المختصة في المملكة بالأمن السيبراني، ولحماية للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية والقطاعات الحكومية.

واعتمدت الدراسة على المنهج الوصفي التحليلي، واشتملت الدراسة على ثلاثة مباحث بيَّنت ماهية الجريمة السيبرانية، وبيان خصائصها، وصورها، وأركانها، والتعرف على دوافع وأساليب ارتكابها، والتعرف على جهود المملكة العربية السعودية في مكافحة الجرائم السيبرانية والتصدي لها. وقد توصلت الدراسة للعديد من توصيات التي ساهمت في الحد من الجرائم السيبرانية ومكافحتها.

الكلمات المفتاحية: الجريمة السيبرانية، الجريمة المعلوماتية، الأمن السيبراني، الفضاء السيبراني، أمن الفضاء المعلوماتي.

Mechanisms to Combat Cybercrime In K.S.A
An analytical Study

Dr. Rana Mosbah Abdel Mohsen Abdel Razek
Assistant Professor of Criminal Law- Law Department- Applied College- Princess Nourah bint Abdulrahman University

Abstract

The study aims to identify the mechanisms of combating cybercrime in the Kingdom of Saudi Arabia, as these crimes are among the new crimes that pose a threat and threat to the security of the individual and society and to all security agencies in the country. The rapid development in the field of information and communication technology and the Internet in the whole world has led to the emergence of new patterns of crimes that came through the bad exploitation of technology, which led to the creation of a new criminal phenomenon, namely, crimes related to the computer and the Internet. The phenomenon of cyber crimes is a natural product of the communications revolution. And technology, which has become widespread, and which occurs through attacks, penetrations and infiltration within information systems with the aim of destroying them or obtaining confidential information, whether military or economic. Therefore, the Kingdom of Saudi Arabia sought to protect its national interests from any threats or dangers in cyberspace, as it established the National Cyber Security Authority by Royal Order No. 6801 dated 2/11/1439 AH, so that this body would be the competent authority in the Kingdom in cybersecurity, and to protect the vital interests and security of the state national, infrastructure and government sectors.

The study relied on the descriptive analytical approach, and the study included three sections that showed the nature of cybercrime, clarifying its characteristics, images, and elements, identifying the motives and methods of committing it, and identifying the efforts of the Kingdom of Saudi Arabia in combating and addressing cybercrime. The study reached many recommendations that contributed to reducing and combating cyber crimes.

Keywords: cyber crime, information crime, cyber security, cyber space, cyber security.

(ISSN: 2537 - 0758)

١. موضوع الدراسة:

سعت المملكة العربية السعودية لتوفير كافة السبل لخدمة مواطنيها وتوظيف التقنيات الحديثة في خدمتهم، حيث كفلت المملكة أنظمة إلكترونية في كافة المعاملات الرسمية لتوفير خدمات فورية وميسرة، وتوفر للدولة قاعدة بيانات ضخمة، لذلك ظهرت الحاجة إلى ضرورة الحفاظ على أمن وسرية المعلومات ومكافحة طرق التسلل إليها، وذلك من خلال سن القوانين والأنظمة التي تختص بمكافحة الجرائم السيبرانية والتصدي لها.

٢. مشكلة الدراسة:

تكمن مشكلة الدراسة في مدى الخطورة التي تنتج عن إساءة استخدام الأنظمة المعلوماتية على نحو غير مشروع قصد الإضرار بمصالح الأفراد والمؤسسات والدول، فساهم التطور التقني في ظهور صورًا جديدة من الجرائم ومنها الجرائم السيبرانية. سعت المملكة العربية السعودية لاستخدام الأنظمة المعلوماتية في جميع أجهزة الدولة ومؤسساتها، لذلك أصبحت المملكة مستهدفة من قبل مجرمي الجرائم السيبرانية، نظرًا لأنها من أقوى عشرين دولةً اقتصادًا في العالم، مما جعل العديد من مؤسساتها وشركاتها هدفًا للهجمات السيبرانية التي يشنها قراصنة الإنترنت. فقد استهدفت الهجمات السيبرانية شركة أرامكو السعودية في عام ٢٠١٢م، وتتزايد الهجمات السيبرانية عليها، لذلك كان لا بد من وضع الأنظمة القانونية رادعة للتصدي للهجمات السيبرانية ومكافحتها.

وبناءً على ذلك تتمثل مشكلة الدراسة بصفة أساسية في التساؤل الرئيس الآتي:

ما هي آليات مكافحة الجرائم السيبرانية والتصدي لها؟

وينبثق من هذا السؤال الرئيس الأسئلة الفرعية الآتية:

- ما المقصود بمفهوم الجريمة السيبرانية، وخصائصها؟
- ما خصائص المجرم السيبراني؟
- ما دوافع ارتكاب الجرائم السيبرانية، وأساليبها؟
- ما صور الجرائم السيبرانية، وأركانها؟
- ما هي جهود المملكة العربية السعودية في مكافحة الجرائم السيبرانية؟

٣. أهداف الدراسة:

بناء على مشكلة الدراسة وتساؤلاتها تهدف الدراسة إلى الآتي:

- التعرف على مفهوم الجريمة السيبرانية، وخصائصها.
- التعرف على خصائص المجرم السيبراني.
- التعرف على دوافع ارتكاب الجرائم السيبرانية، وأساليبها.
- التعرف على صور الجرائم السيبرانية، وأركانها.
- التعرف على جهود المملكة العربية السعودية في مكافحة الجرائم السيبرانية.

٤. أهمية موضوع الدراسة:

تكمن أهمية دراسة هذا الموضوع من منطلق استخدام نظم المعلومات في جميع أجهزة الدولة ومؤسساتها، حيث استهدفت رؤية المملكة العربية السعودية ٢٠٣٠م التطوير الشامل للوطن وأمنه واقتصاده ورفاهية مواطنيه، ولقد كان ضمن مستهدفات الرؤية برنامج التحول الرقمي ٢٠٢٠م وتنمية البنية التحتية الرقمية، ولكن مع الاعتماد المتزايد على الأنظمة المعلوماتية، فقد يزيد من احتمالات الاعتداءات السيبرانية على الأنظمة الإلكترونية والمعلوماتية، لذلك كان لا بد من مكافحة الجرائم السيبرانية وقمعها من أجل المحافظة على أمن وسلامة كافة القطاعات المختلفة بالدولة.

٥. منهج الدراسة:

اعتمدت الدراسة على المنهج الوصفي التحليلي في تحديد ماهية الجريمة السيبرانية، وبيان خصائصها، وصورها، وأركانها، والتعرف على دوافع وأساليب ارتكابها، والتعرف على جهود المملكة العربية السعودية في مكافحة الجرائم السيبرانية والتصدي لها.

٦. حدود الدراسة:

- **الحدود الموضوعية:** اقتصرت الدراسة على التطرق إلى بيان تشريعات المملكة العربية السعودية فيما يتعلق بمكافحة الجرائم السيبرانية، وكذلك التعرف على ماهية الجرائم السيبرانية، وصورها، وأركانها.
- **الحدود الزمانية:** تم إجراء هذه الدراسة في الفصل الدراسي الثاني للعام الجامعي ١٤٤٣هـ- ٢٠٢٢م.
- **الحدود المكانية:** اقتصرت الدراسة على المملكة العربية السعودية.

٧. مصطلحات الدراسة:

- **الفضاء السيبراني:** هي الشبكة المترابطة من البنية التحتية لتقنية المعلومات، والتي تشمل الإنترنت وشبكات الاتصالات وأنظمة الحاسب الآلي والأجهزة المتصلة

(ISSN: 2537 - 0758)

بالإنترنت، إلى جانب المعالِجات وأجهزة التحكم المرتبطة بها. فهو عالم افتراضي[١].

- **الأمن السيبراني:** هو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها، وما تقدمه من خدمات، وما تحويه من بيانات، من أي اختراق، أو تعطيل، أو تعديل، أو دخول، أو استخدام أو استغلال غير مشروع[٢].
- **الهيئة الوطنية للأمن السيبراني:** هي هيئة حكومية مختصة في الأمن السيبراني في المملكة العربية السعودية، والمرجع الوطني في شؤونه، وتهدف إلى تعزيزه؛ حمايةً للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية[٣].
- **الهجوم السيبراني:** هو استغلال غير مشروع لأنظمة الحاسب، والشبكات، والمنظمات، التي يعتمد عملها على تقنية المعلومات والاتصالات الرقمية؛ بهدف إحداث أضرار. وتشمل أي نوع من الأنشطة الخبيثة التي تحاول الوصول غير المشروع أو تعطيل، أو منع، أو تدمير موارد النظم المعلوماتية، أو المعلومات نفسها[٤].

٨. الدراسات السابقة:

يعد موضوع مكافحة الجرائم السيبرانية من الموضوعات الهامة والحيوية، وعلى الرغم من وجود العديد من الدراسات السابقة التي تناولت موضوع الجرائم السيبرانية، إلا أنه لا توجد أي دراسة تناولت آليات مكافحة الجرائم السيبرانية من خلال التطرق لتشريعات والأنظمة القانونية في المملكة العربية السعودية، لذلك تختلف الدراسة الحالية عن الدراسات السابقة في أنها تطرقت لبيان طرق مكافحة الجرائم السيبرانية، وذلك من

---

[١]- تاريخ الاطلاع ٢٠٢٢/١/١، متاح على الموقع التالي:
https://www.citc.gov.sa/ar/Digitalknowledge/Pages/cyber-security.aspx

[٢]- تاريخ الاطلاع ٢٠٢٢/١/١، متاح على الموقع التالي:
https://nca.gov.sa/pages/glossary.html

[٣]- تاريخ الاطلاع ٢٠٢٢/١/١، متاح على الموقع التالي:
https://www.my.gov.sa/wps/portal/snp/agencies/agencyDetails/AC403

[٤]- تاريخ الاطلاع ٢٠٢٢/١/١، متاح على الموقع التالي:
https://nca.gov.sa/pages/glossary.html

خلال التعرض للبنيان القانوني والاتفاقيات التي انضمت إلى المملكة العربية السعودية بهذا الشأن، وبذلك تصبح الدراسة الحالية أعم وأشمل من الدراسات السابقة.

وفي السياق الآتي نستعرض الدراسات ذات الصلة بموضوع الدراسة العربية، والأجنبية، وسيتم الاعتماد على الترتيب الزمني من الأقدم للأحدث في عرض الدراسات.

أ- **الدراسات العربية:**

- **دراسة (أسامة مهمل، ٢٠١٨م) بعنوان "الإجرام السيبراني"**: هدفت هذه الدراسة إلى تعريف الجريمة السيبرانية وخصائصها وتحديد أنواعها، والمخاطر المترتبة عنها. وركزت هذه الدراسة على آليات مكافحة الجريمة السيبرانية في الجزائر ومدى كفاية القوانين الحالية لمواجهتها. وقد أوصت الدراسة ببعض توصيات منها: إدراج مقياس خاص بالقانون الجنائي السيبراني، ودمج جميع النصوص القانونية المتعلقة بهذه الجريمة سواء الموضوعية منها أو الإجرائية، وتنظيمها في قانون خاص بها.
- **دراسة (علي الشهري، ٢٠١٩) بعنوان "رؤية استراتيجية للحد من الجرائم الإلكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية"**: هدفت هذه الدراسة إلى تعريف الجرائم الإلكترونية وأسبابها، وأنواعها. وركزت هذه الدراسة على مخاطر الجرائم الإلكترونية، ووضع رؤية استراتيجية تحد من هذه الجرائم لتعزيز الأمن السيبراني في المملكة. وقد أوصت الدراسة ببعض توصيات منها: إصدار التشريعات والأنظمة التي تحد من الجريمة الإلكترونية، وإنشاء المحاكم المختصة في هذه الجرائم، وتطوير الأنظمة التقنية لرصد وملاحقة مرتكبي الجرائم الإلكترونية، وإلحاق العاملين في مجالات مكافحة الجرائم الإلكترونية والأمن السيبراني بدورات متخصصة في هذا المجال لرفع كفاءتهم.
- **دراسة (روان الصحفي، ٢٠٢٠م) بعنوان "الجرائم السيبرانية"**: هدفت هذه الدراسة إلى تعريف الجريمة السيبرانية والإطار القانوني للجريمة السيبرانية ودارسة الجوانب الموضوعية من أركان وعقوبات، وركزت هذه الدراسة على الجوانب الإجرائية من الاستدلال والتحقيق والمحاكمة في الجريمة السيبرانية. وقد أوصت الدراسة ببعض توصيات منها: إنشاء هيئة وطنية مختصة بالجرائم السيبرانية، واعتماد نظام ولائحة تنفيذية للهيئة، وانضمام هذه الهيئة كقطاع رسمي تحت وازرة العدل.
- **دراسة (زياد العتيبي، ٢٠٢١م) بعنوان "جرائم السيبرانية المرتكبة عبر الوسائط الرقمية"**: هدفت هذه الدراسة إلى تعريف الجريمة السيبرانية وخصائصها، وأركانها

(ISSN: 2537 - 0758)

والدافع من ارتكابها. وركزت هذه الدراسة على صور الجرائم السيبرانية. وتوصي الدراسة بضرورة إصدار المنظم السعودي نظامًا خاصًا بالإجراءات الجزائية الرقمية بما يواكب التحول الرقمي الذي تشهده المملكة.

ب- الدراسات الأجنبية:

ومن أهم الدراسات باللغة الإنجليزية التي تعرضت للجريمة السيبرانية في المملكة العربية السعودية بصفة خاصة نذكر ما يلي:

- **دراسة (Elnaim, B. M. E. December 2013)**: وقد تناولت هذه الدراسة الجريمة الإلكترونية في المملكة العربية السعودية، حيث هدفت هذه الدراسة إلى تحليل الجريمة الإلكترونية وقانون مكافحتها. وتوصلت الدراسة إلى أن الجرائم الإلكترونية آخذة في الارتفاع في جميع أنحاء المملكة، وتمثل الحماية من التهديدات الإلكترونية تحديًا إداريًا مستمرًا للمؤسسات في الدولة.
- **دراسة (Zayid, E. I. M., & Farah, N. A. A. March 2017)**: أجريت هذه الدراسة لاختبار وتقييم مخاطر الجرائم الإلكترونية والوعي في منطقة النماص. استهدفت الدراسة مجموعة من المستخدمين على دراية كبيرة باستخدام تطبيقات وخدمات التكنولوجيا الحديثة، وكذلك جميع المواد الدراسية لطلاب من جامعة بيشة، كلية العلوم والآداب، النماص. استخدمت الدراسة ١٦ متغيرًا مختلفًا. وأظهرت المخرجات أن الأسباب الكامنة وراء الجرائم الإلكترونية هي: الاستغلال الجنسي، والمالية، والسياسية، والثقافية، والشهرة. ومع ذلك، فإن شبكة التواصل الاجتماعي هي البوابة الأكثر انتشارًا لحدوث الجريمة الإلكترونية (معدل ٦٩.٦٪). بشكل عام، يعد برنامج مكافحة الفيروسات هو الأداة الوحيدة المستخدمة كأسلوب لمكافحة الجرائم الإلكترونية.
- **دراسة (Alqurashi, R. K., AlZain, M. A., Soh, B., Masud, M., & Al-Amri, J. 2020)**: تناولت هذه الدراسة الهجمات والتأثيرات السيبرانية: دراسة حالة في المملكة العربية السعودية، حيث تعد المملكة واحدة من أسرع الدول نموًا في الشرق الأوسط من حيث تقنيات الاتصالات مثل الإنترنت والهواتف المحمولة. في هذه الدراسة تم استكشاف تحديات الجرائم الإلكترونية في الشرق الأوسط وبالتركيز على السعودية كدراسة حالة. على وجه الخصوص، ركزت الدراسة على فحص تأثير استخدام الإنترنت والجرائم الإلكترونية على المراهقين في السعودية.

٩. خطة الدراسة:

تنقسم خطة الدراسة إلى ثلاثة مباحث رئيسة يسبقهما مقدمة وتنتهي بخاتمة، على النحو التالي:

المبحث الأول: ماهية الجريمة السيبرانية.

المبحث الثاني: صور الجرائم السيبرانية وأركانها.

المبحث الثالث: جهود المملكة العربية السعودية في مكافحة الجرائم السيبرانية.

المبحث الأول
ماهية الجريمة السيبرانية

تعد الجرائم السيبرانية من أخطر الجرائم شيوعًا خلال السنوات الأخيرة، نظرًا لإتاحة العديد من الوزارات والشركات والمؤسسات تطبيقاتها عبر شبكات الإنترنت، لاعتمادها على تقنية المعلومات والاتصالات التي أصبحت جزء لا يتجزأ في مجالات الحياة، وعلى الرغم من الإيجابيات التي تظهرها التقنية الإلكترونية من سهولة في سرعة الوصول والتواصل ونقل المعلومات، إلا أنها ساهمت في إحداث نوع جديد من الجرائم وهو ما يعرف بالجرائم السيبرانية. لذلك سينقسم هذا المبحث إلى المطالب التالية: المطلب الأول مفهوم الجريمة السيبرانية، المطلب الثاني خصائص الجريمة السيبرانية، المطلب الثالث خصائص المجرم السيبراني، المطلب الرابع دوافع ارتكاب الجرائم السيبرانية وأساليبها.

المطلب الأول
مفهوم الجريمة السيبرانية

تعتبر الجرائم السيبرانية من الجرائم المستحدثة؛ لذلك لم يستقر الفقهاء على وضع تعريف محدد للجرائم الناشئة في بيئة الحاسب الآلي أو الشبكة العنكبوتية، وبسبب نشأة وتطور ظاهرة الإجرام المرتبط بتقنية المعلومات، فيطلق عليها جرائم الإنترنت، أو الجريمة المرتبطة بالكمبيوتر، أو الجرائم المعلوماتية، أو جرائم الشبكة العنكبوتية، لذلك يصعب وضع تعريف ثابت ومحدد لهذه الجرائم نظرًا لحداثتها[٥].

وتعددت تعريفات الجريمة السيبرانية، فقد عرفها البعض بأنها "الجرائم التي تهدد الأمن السيبراني والتورط فيما ويسمى (بالجريمة السيبرانية)، وتتكون الجريمة السيبرانية

---

[٥]– وفاء لطفي، الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني، مجلة كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، المجلد ٢٣، العدد (١)، ٢٠٢٢م، ص ١٥٤.

(ISSN: 2537 - 0758)

أو الإلكترونية (Cybercrime)، من مقطعين هما: الجريمة (Crime) وتعني الأفعال الخارجة عن القانون، والسيبرانية (Cyber) تستخدم لوصف استخدام الحاسب الآلي في هذه الجرائم"[٦].

وعرفها البعض أيضًا بأنها "جرائم سيبرانية، أو جرائم الكمبيوتر، يتم استخدام الحاسب الآلي والإنترنت فيها كأداة لتحقيق أهداف غير مشروعة، مثل النصب والاحتيال، وانتهاك حقوق الملكية الفكرية، وانتهاك الخصوصية، والاتجار في المواد الإباحية للأطفال"[٧].

كما عرفها المنظم السعودي في الفقرة الثامنة من المادة الأولى من نظام مكافحة الجرائم المعلوماتية على أنها هي: "أي فعل يرتكب متضمنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام". وعرفت هيئة الاتصالات وتقنية المعلومات السعودية الجريمة السيبرانية في ورشة عمل بعنوان "الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت" المنعقد بتاريخ (٢٦/ ٤/ ٢٠١٨م) بأنها: "فعل غير قانوني مرتبط بالشبكة المعلوماتية، فهي جرائم العصر الرقمي"[٨].

وعرفها البعض الأخر بأنها "هي الهجوم عبر الفضاء الإلكتروني يهدف إلى السيطرة على مواقع إلكترونية أو بنى تحتية حساسة محمية بأنظمة إلكترونية لتعطيلها أو تدميرها أو الإضرار بها"، ويعد هذا التعريف من أفضل التعريفات التي تناولت ظاهرة الإجرام السيبراني[٩].

---

[٦]– أسامة مهمل، الإجرام السيبراني، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، ٢٠١٨م، ص ٢٥. **أنظر كذلك:**

Women" Halder. D., & Jaishankar. K. (2011) "Cybercrime and the Victimization of: Laws, Rights, and Regulations. Hershey, PA, USA, P.10.

[٧]– عبد السلام المايل، عادل الشربجي، الجريمة الإلكترونية في الفضاء الإلكتروني، مجلة آفاق للبحوث والدراسات، العدد (٤)، ٢٠١٩م، ص ٥. وأنظر كذلك:

Michael.A. Dennis. (2018)." Cybercrime", Selected by Britannica Academic, Encyclopedia Britannica, PP. 1-51.

[٨]– صالح الربيعة، الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت، هيئة الاتصالات وتقنية المعلومات، الرياض، ٢٠١٧م، ص ١٣.

[٩]– عبد العزيز آل جار الله، جرائم الإنترنت وعقوباتها وفقًا نظام مكافحة جرائم المعلوماتية السعودي، دار الكتاب الجامعي للنشر والتوزيع، الرياض، ط١، ٢٠١٧م، ص ٣٢. **وأنظر كذلك:**

ومن جانبنا نرى أنه مصطلح الجرائم السيبرانية (Cybercrime) مصطلح غير عربي، ولكنه أصبح متداول في الوقت الحاضر في العديد من المؤتمرات والندوات، مثال ذلك: ملتقى "الجرائم السيبرانية والأدلة الرقمية" الذي نظمته جامعة الأمير نايف العربية للعلوم الأمنية بمدينة الرياض في عام ٢٠١٩م، وكذلك اعتماد مصطلح الأمن السيبراني كتخصص جديد في العديد من الجامعات السعودية، لذلك يمكن تعريف الجريمة السيبرانية بأنها هي: "هجوم عبر الفضاء السيبراني قائم على التسلل عبر مواقع إلكترونية غير مصرح الدخول بها بهدف إتلاف البيانات المتوفرة فيها أو تدميرها أو تعطيلها أو التجسس عليها أو الاستحواذ عليها".

المطلب الثاني

خصائص الجريمة السيبرانية

تُعد الجرائم السيبرانية من الجرائم المستحدثة وسريعة التطور، لأنها تتطور تبعًا لتطور تقنية المعلومات، وهي تتميز عن غيرها من الجرائم التقليدية بالعديد من الخصائص، سنتناول سردها من خلال الفروع التالية:

الفرع الأول

جرائم ترتكب بواسطة الحاسب الآلي والأجهزة المحمولة الذكية:

تعتمد الجرائم السيبرانية في ارتكابها على جهاز الحاسب الآلي كوسيلة وموضوعًا للجريمة، وهذا ما يميزها عن الجرائم الأخرى، فالحاسب الآلي هو الأداة الرئيسية لارتكاب الجرائم السيبرانية، لذلك لا يستطيع المجرم السيبراني القيام بتنفيذ هجماته في بيئة سيبرانية إلا باستخدام أجهزة الحاسب الآلي المتصلة بشبكة الإنترنت وكذلك الأجهزة المحمولة الذكية، فارتكاب هذه الجريمة تتطلب توفر وسائل التقنية الحديثة التي لا بد أن يكون لدى المجرم المعرفة والدراية في كيفية التعامل معها[١٠].

Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). Cyber threats to health information systems: A systematic review. Technology and Health Care, 24(1), pp.1-9.

[١٠]– زياد العتيبي، جرائم السيبرانية المرتكبة عبر الوسائط الرقمية، المجلة الأكاديمية العالمية للدراسات القانونية، المجلد ٣، العدد (١)، ٢٠٢١م، ص٢. **وأنظر كذلك:**

(ISSN: 2537 - 0758)

الفرع الثاني
جرائم خفية يصعب اكتشافها وإثباتها

تتميز الجرائم السيبرانية بالخفاء؛ لأنها تقع في فضاء سيبراني لا حدود له، وفي الغالب لا يشعر بها المجني عليه كسرقة البيانات أو إرسال الفيروسات إلى جهازه، أو عن طريق نقل المعلومات بواسطة النبضات الإلكترونية في صيغة أوامر رقمية. ويصعب اكتشاف هذه الجرائم لأنها لا تترك أثرًا فوريًا مباشرًا، فأغلب الجرائم السيبرانية تكتشف بمحض الصدفة وبعد مدة طويلة وحينها يصعب إثباتها، كما أن التخلص من آثار الجرائم السيبرانية أمر في غاية البساطة، فهذه الجرائم تفتقر إلى الدليل التقليدي المادي كالبصمات؛ لأن الجرائم السيبرانية لا يمكن إثباتها إلا بدليل ذو طبيعة خاصة تنتمي إلى نفس الفضاء السيبراني التي تقع على الجريمة، والتي تحتاج إلى معرفة وإلمام ومهارة كافية في تقنية وعلوم الحاسب الآلي حتى لا يمكن اكتشافها وتتبعها[١١].

الفرع الثالث
جرائم عابرة للحدود الدولية

تتميز الجرائم السيبرانية بأنها جرائم عابرة للحدود، لأنها لا تنحصر في دولة معينة أو قارة معينة؛ نظرًا لأنها تتم في بيئة افتراضية لا حدود لها، وبالتالي يستطيع المجرم السيبراني تنفيذ هجماته في أي مكان وزمان دون أن يخضع لحرس الحدود (Dashora,K.2011,pp.240)، وهذا يشكل تحدي كبير في حقل الاختصاص القضائي والقانوني الواجب التطبيق من حيث الملاحقة والتحقق والضبط والتفتيش، لذلك يحتاج الأمر إلى عقد الاتفاقات الدولية والإقليمية لمكافحة الجرائم السيبرانية[١٢].

الفرع الرابع
جرائم صعبة الإثبات

تعتبر الجرائم السيبرانية من أصعب الجرائم إثباتًا لاسيما في حالة حدوثها بين دولة وأخرى، وصعوبة القبض على الجاني، وذلك يرجع إلى الاختلاف بين الدول والقوانين

Wall, D. (1999). Cybercrimes: New wine, no bottles. In Invisible crimes (pp. 105-139).

[١١]– محمود القرعان، الجرائم الإلكترونية، دار وائل النشر والتوزيع، عمان، ط١، ٢٠١٧م، ص ٤٥. وأنظر: عبيس الفتلاوي، الهجمات السيبرانية، منشورات زين الحقوقية، بيروت، ط١، ٢٠١٨م، ص ٥٥.

[١٢]– عبد العال الديربي، محمد إسماعيل، الجرائم الإلكترونية، المركز القومي للإصدارات القانونية، القاهرة، ط١، ٢٠١٢م، ص ٥٣.

فيما بينهم، التي تحكمها العلاقات الدولية والمعاهدات والاتفاقيات، والتي تتشابك في التعقيد الدولي، مما يضاعف من صعوبة اكتشافها أو ملاحقتها[١٣].

الفرع الخامس
جرائم ناعمة

تتسم الجرائم الناشئة عن استخدام الإنترنت بأنها ناعمة، نظرًا لأنها لا تتطلب ممارسة العنف، بل تعتمد على تخطيط منظم ومعرفة باستخدام الأجهزة الذكية، فهي عبارة عن أوامر رقمية تستولى على البيانات والمعلومات المخزنة في الأنظمة المعلوماتية أو تعديلها أو إتلافها أو التجسس عليها، وغيرها من الصور التي لا يمكن حصرها[١٤].

الفرع السادس
الجرائم السيبرانية من الجرائم المستحدثة

تعتبر الجرائم السيبرانية من الجرائم المستحدثة؛ نظرًا لارتباطها بوجود وسائل اتصال وأنظمة وتقنيات ذات طابع تكنولوجي حديث ومتطور[١٥].

الفرع السابع
جرائم سريعة التنفيذ

تتميز الجرائم السيبرانية بأنها ترتكب بسرعة فائقة وفي وقت قصير، وقد لا تتطلب الإعداد قبل التنفيذ.

الفرع الثامن
جرائم ترتكب عن بعد

فقد تحدث الجريمة السيبرانية بين شخص في دولة والأخر في دولة أخرى، فيمكن للجاني تنفيذ الجريمة وهو في دولة بعيدة عن دولة المجني عليه[١٦].

---

[١٣]– طاهر أبو القاسم، الجرائم المعلوماتية، صعوبات التحقيق فيها وكيفية مواجهتها، منشورات المنظمة العربية للتنمية الإدارية بجامعة الدول العربية، الشارقة، ط١ ٢٠١٩م.

[١٤]– تميم التميمي، الجرائم المعلوماتية في الاعتداء على الأشخاص، مكتبة القانون والاقتصاد، الرياض، ط١، ٢٠١٦م، ص ٦٦. وأنظر: عبد السلام المايل، وآخرون، مرجع سابق، ص١٠.

[١٥]– محمد المقصودي، الجرائم المعلوماتية، مجلة العربية للدراسات الأمينة، المجلد ٣٣، العدد (٧)، ٢٠١٧م، ص ١١٥.

(ISSN: 2537 - 0758)

المطلب الثالث
خصائص المجرم السيبراني

يتميز المتورطين في الجرائم السيبرانية بخصائص تميزهم عن غيرهم من المتورطين في الجرائم التقليدية، لذلك سنتناول أبرز هذه الخصائص من خلال الفروع التالية:

الفرع الأول
مهارة المجرم السيبراني في استخدام التقنية الحديثة لأنظمة المعلومات

يتمتع المجرم السيبراني بقدرة فائقة من الذكاء إذ يستغل مهاراته في اختراق الشبكات واستخدام الحاسب الآلي والمهارات الفنية بتقنية المعلومات، وقد يكون المجرم السيبراني من المتخصصين في معالجة البيانات الرقمية حيث أن آلية ارتكاب هذه الجريمة تشترط أن يتمتع المجرم بالصفات الفنية الخاصة في استخدام تقنية المعلومات، ولكن لا يشترط أن يكون المجرم السيبراني من المتخصصين في مجال الحاسب الآلي وتقنية المعلومات، لأن كثير من فئة الهاكرز اكتسبوا هذه المهارة الفنية كهواية من الآخرين أو من خلال الاطلاع والقراءة في الشبكة العنكبوتية[١٧].

الفرع الثاني
المجرم السيبراني على قدر عالي من الذكاء والابتكار

يتميز المجرم السيبراني بقدر عالي من الذكاء لتسخير تقنية المعلومات لاختراق الشبكات والتعمق في الفضاء السيبراني من خلال القدرة على التعامل مع أحدث وسائل التقنية، ولا يشترط في المجرم السيبراني أن يكون ذو مهارة عالية وإنما يكفي أن يكون لديه الإلمام الكاف في علوم تقنية الحاسب الآلي وكيفية اختراق الشبكات المحمية والقدرة على إخفاء جريمته[١٨].

---

[١٦]– محمد العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر والتوزيع، الإسكندرية، ٢٠٠٤م، ص ٧٨.

[١٧]– مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٩م، ص ٨٩.

[١٨]– حاتم بطيخ، تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات، مجلة الدراسات القانونية والاقتصادية، كلية الحقوق، جامعة مدينة السادات، المجلد ٧، العدد (١)، ٢٠٢١م، ص ٧٧.

الفرع الثالث
صعوبة الإمساك بالمجرم السيبراني

يحرص المجرم السيبراني دائما على إخفاء هويته وتدمير أي دليل يحتمل أن يستدل على شخصيه، بالإضافة إلى أن الجريمة تتم في الفضاء السيبراني الأمر الذي يزيد من صعوبة اكتشافها. ويطلق على مجرمي السيبراني مسمى ذوي الياقات البيضاء؛ لأنهم ينتمون إلى مناصب رفيعة المستوى وطبقات اجتماعية عليا تتصف بالثقافة والتعليم، بل إن بعضهم يتمتع بثقة الأشخاص المحيطين به.

الفرع الرابع
المجرم السيبراني عائد للإجرام

يتميز المجرم السيبراني عن المجرم التقليدي بأنه عائد للإجرام، لأنه يعود بارتكاب الجريمة مرة أخرى وبنفس الطريقة، فهو يكيف مهاراته الإجرامية في كيفية التعامل مع أجهزة الحاسب الآلي والتحكم في أنظمة الشبكات واختراقها عدة مرات، وقد تتعدد الدوافع لارتكابها في كل مرة يعود فيها[١٩].

المطلب الرابع
دوافع ارتكاب الجرائم السيبرانية وأساليبها

تختلف دوافع وأساليب المجرم السيبراني عن دوافع وأساليب المجرم التقليدي من حيث ارتكاب الجرائم، لذلك سنتناول أبرز هذه الدوافع والأساليب من خلال الفرعين التاليتين:

الفرع الأول
دوافع ارتكاب الجرائم السيبرانية

تقع الجرائم السيبرانية بسبب عدة دوافع فبعضها يرجع إلى دافع سياسي ومنها ما يرجع إلى دافع مالي ومنها ما هو دافع شخصي، لذلك سنتناول أهم الدوافع التي تدفع المجرم السيبراني إلى ارتكاب جريمته على النحو الآتي:

- **دافع سياسي:** يتم ذلك من خلال تخريب المواقع الحكومية أو التجسس عليها أو اختراق الحسابات الحكومية عبر منصات التواصل الاجتماعي لكتابة أخبار ومعلومات غير صحيحة بغرض إثارة الفتنة والرأي العام بين المواطنين.

[١٩]– روان الصحفي، الجرائم السيبرانية، المجلة الإلكترونية الشاملة، العدد (٢٤)، ٢٠٢٠م، ص ٢٣.

(ISSN: 2537 - 0758)

- **دافع الانتقام:** يرتكب بعض العاملين في مؤسسات أو شركات، بسبب ضغط العمل وضغط نفسي عليهم، فيقومون باختراق أنظمتها.
- **دافع مادي:** نجد أن الكسب المادي الناتج عن تلك الجرائم هو أهم الدوافع لارتكابها.
- **دافع ذهني:** تتسم الأنظمة المعلوماتية بالتعقيد وصعوبة الاختراق، وهذه الأمور تكون دافعًا للمجرم السيبراني إلى تحقيق الرغبة في الانتصار على الأنظمة المعلوماتية وهزيمتها عبر اختراقها والتحكم فيها[٢٠].

الفرع الثاني
أساليب المجرم السيبراني لارتكاب الجرائم السيبرانية

يستخدم المجرم السيبراني تقنية الاختراق للدخول على الأنظمة المعلوماتية والأمنية لتنفيذ جريمته، فيتم الاختراق عن طريق ثغرات في نظام الحماية الخاصة، وذلك عن طريق برنامجين هما: **الأول:** الخادم وهو متصل بجهاز المجني عليه إذ ينفذ المهام الموكلة إليه، **والثاني:** يوجد بجهاز المخترق ويسمى بالبرنامج المستفيد، ويمكن أن يكون عن طريق القصف السيبراني: وهو هجوم على شبكات المعلومات بحيث يسبب ضغط كبير على الموقع فيفقد قدرة الموقع على استقبال الرسائل من المستخدمين، وبالتالي يوقفه عن العمل، أو عن طريق الاختناق المروري السيبراني: وهو خنق الاتصالات لدى المجني عليه بحيث لا يمكنه تبادل المعلومات، أو عن طريق الأبواب الخلفية: وهي ثغرة يتركها مصمم النظام عمدًا للتسلل إليه وقت الحاجة. كما أن المجرم السيبراني يستخدم عدة برامج ومنها[٢١]:

- **حصان طروادة:** وهو عبارة عن برنامج صغير مختبئ يزرعه المبرمج داخل النظام الذي يصممه، ويؤدي مهماته بشكل خفي في إطلاق الفيروسات التي تقوم بإرسال البيانات عن طريق الثغرات الموجودة في النظام، أو تعطيل جهاز الكمبيوتر أو الشبكة، أو يمكن الجاني من التحكم عن بعد في النظام.

---

[٢٠]– عبد العال الديربي، وآخرون، مرجع سابق، ص ٦٥. أنظر: روان الصحفي، مرجع سابق، ص٢٨. وأنظر: زياد العتيبي، مرجع سابق، ص ٥.

[٢١]– عبد السلام المايل، وآخرون، مرجع سابق، ص ١٢. أنظر: محمد المقصودي، مرجع سابق، ص١٢٢. تميم التميمي، مرجع سابق، ص ٧٤.

- **فيروسات حجب الخدمات (Denial Of Service)**: هي عبارة عن برامج صغيرة تستخدم لتعطيل شبكات الخدمات، مثال ذلك: أن يقوم المهاجم بإرسال العديد من البيانات إلى أحد مواقع الإنترنت والتي تتسبب في ملئ وتعطيل هذه الأنظمة عن العمل، وقد يجعلها غير متاحة لأي مستخدم، ويستخدم هجوم حجب الخدمات الموزعة (DDoS) مجموعة من أجهزة الكمبيوتر، وتكون في أغالب الأحوال مخترقة عن طريق البرامج الضارة وتحت سيطرتهم، لإرسال البيانات إلى المستهدفين.
- **حقن SQL**: وهي عبارة عن أداة تُمكن الجاني من استغلال الثغرات للتحكم بقاعدة بيانات المجني عليه، وتوجد الكثير من قواعد البيانات المُصممة لتنفيذ أي أوامر مكتوبة في لغة الاستعلامات المركبة (SQL)، وتقوم العديد من مواقع الإنترنت بتجميع البيانات من المستخدمين، بإرسال هذه البيانات إلى قواعد بيانات (SQL)، مثال ذلك: سيقوم المخترق بكتابة بعض أوامر (SQL) في أحد نماذج المواقع التي تطلب بيانات شخصية، فربما تنفيذ قاعدة البيانات هذه الأوامر.
- **التعدين الخبيث (CryptoJacking)**: وهو عبارة عن هجوم يخترق جهاز الكمبيوتر الخاص بالمجني عليه واستخدامه لتعدين العملات الرقمية المشفرة، مثال ذلك: سيقوم الجاني بتثبيت أحد البرامج الضارة على جهاز الكمبيوتر الخاص بالمجني عليه لتنفيذ العمليات الحسابية المطلوبة[٢٢].

المبحث الثاني
صور الجريمة السيبرانية وأركانها

تعد الجرائم السيبرانية من الموضوعات المستجدة، لذلك يصعب وضع صور محددة للجرائم السيبرانية، نظرًا للتطور الهائل التي تشهدها هذه الجرائم، ولكن لا تختلف أركان الجريمة السيبرانية عن أركان أي جريمة تقليدية وأحكامها العامة، لذلك سينقسم هذا المبحث إلى المطالب التالية: المطلب الأول صور الجرائم السيبرانية، والمطلب الثاني أركان الجرائم السيبرانية، والمطلب الثالث الأحكام العامة في الجرائم السيبرانية.

---

[٢٢]– محمد العريان، مرجع سابق، ص ٩٤. أنظر: علي الشهري، رؤية استراتيجية للحد من الجرائم الإلكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية، رسالة دكتوراه، كلية العلوم الاستراتيجية، جامعة نايف العربية للعلوم الأمنية، ٢٠١٩م، ص ٤٥ وما بعدها. **وأنظر كذلك:**
Sausan. W. Brenner. (2010),"Criminal Threats from Cyberspace", Santa Barbra: greenwood publishing group, P12.

(ISSN: 2537 - 0758)

المطلب الأول
صور الجريمة السيبرانية

تتنوع صور الجرائم السيبرانية والتي يصعب حصرها في صور محددة؛ نظرًا لأنها جرائم مرتبطة بالتقنية المعلوماتية والتي تتطور تبعًا لتطور هذه التقنية، ووفقًا لنظام مكافحة جرائم المعلوماتية السعودي حيث نصت المادة السادسة على صور الجرائم بفقرتها الأولى: فمنها ما هو واقع على النظام العام أو القيم الدينية ومنها ما هو واقع على الآداب العامة والحياة الخاصة كالسب والشتم وإفشاء الأسرار وكذلك نشر الوثائق المعلوماتية السرية وإفشائها[٢٣]. لذلك سنتناول في هذا المطلب أكثر صور الجرائم السيبرانية انتشارًا من خلال الفروع التالية:

الفرع الأول
جرائم ضد الحكومات وكيانها الاقتصادي

يعد المساس بأمن الدولة الداخلي أو الخارجي، أو اقتصادها القومي من الجرائم الخطيرة التي تهدد كيان الدولة واستقرارها، فيستغل الجاني الفضاء السيبراني في المساس بأمن الدولة عن طريق الدخول غير المصرح به إلى المواقع الإلكترونية لنشر الفيروسات بهدف تدمير أومسح البرامج والملفات أوتعطيل أجهزة الكمبيوتر، وكذلك محاولة تنفيذ هجمات منظمة على البنوك والمواقع الإلكترونية للأجهزة الحكومية لاستهداف اقتصادها، بالإضافة إلى اختراق وتعطيل المواقع الإلكترونية الحكومية، وغير الحكومية، واختراق نظم حماية المعلومات والبوابات الإلكترونية.

ويستغل المجرم السيبراني تطور الأجهزة الحكومية التي تعتمد على التحول الرقمي وذلك بتنفيذ هجماته على الشبكات الحكومية بهدف سرقة بيانات معينة أو التأثير على اقتصاد الدولة من خلال تدمير الأجهزة بالفيروسات أو اختراق أنظمة البيانات والعبث في بيانات العملاء وتحويل الأموال. كما يهدف المجرم السيبراني إلى تعطيل الخدمات الحكومية الإلكترونية عن العمل وهو يعد من أخطر أنواع الجرائم السيبرانية[٢٤].

لذلك يعاقب المنظم السعودي بعقوبة السجن لمدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين، على الدخول غير

---

[٢٣]– غانم الشمري، الجرائم المعلوماتية، الدار العلمية الدولية، عمان، ط١، ٢٠١٦م، ص ٤٩.

[٢٤]– عبد العال الديربي، وآخرون، مرجع سابق، ص ٨٨. **وأنظر:** تميم التميمي، مرجع سابق، ص٩١.

المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرةً، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني". وذلك وفقًا لنص المادة السابعة من نظام مكافحة جرائم المعلوماتية.

الفرع الثاني
جرائم الإرهاب السيبراني

يجرم المنظم السعودي إنشاء مواقع إلكترونية لمنظمات إرهابية على الشبكة المعلوماتية، لبث الأفكار والمواد المعادية للدين الإسلامي، وإرسال الأوامر والتعليمات للمتعاونين معهم حول كيفية صنع القنابل والمتفجرات واستعمالها في عملياتهم الإرهابية، وتسهيل التواصل بين الإرهابيين، فالعديد من التنظيمات الإرهابية المسلحة تعلن عبر شبكة الإنترنت عن حاجتهم لتجنيد عناصر تساعدهم في تنفيذ أعمالهم الإجرامية، وعملياتهم انتحارية مستخدمة في ذلك الجانب الديني، وهو يعد من أخطر أنواع الجرائم السيبرانية[٢٥]. لذلك يعاقب المنظم السعودي بعقوبة السجن لمدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين، على إنشاء موقع لمنظمات إرهابية على الشبكة العنكبوتية أو أحد أجهزة الحاسب الآلي أو نشر لتسهيل الاتصال بقيادات الأجهزة الحارقة أو المتفجرات أو أي أداة تستخدم في الأعمال الإرهابية". وذلك وفقًا لنص المادة السابعة من نظام مكافحة جرائم المعلوماتية.

الفرع الثالث
جرائم الاعتداء على حرمة الحياة الخاصة

تتمثل جرائم الاعتداء على حرمة الحياة الخاصة في الجرائم الماسة بالحياة الشخصية من بيانات ومعلومات سرية للأفراد، فللحياة الخاصة حرمة، يحظر على الآخرين استباحتها، لا سيما بعد استخدام الهواتف المحمولة المزودة بالكاميرات أو ما في حكمها من التقنيات الحديثة، والتي يمكن بواسطتها اختراق أدق تفاصيل الحياة الخاصة للأشخاص[٢٦]، لذلك يعاقب المنظم السعودي على جرائم الاعتداء على حرمة

---

[٢٥]– علي الشهري، مرجع سابق، ٥٠ وما بعدها. وأنظر: تميم التميمي، مرجع سابق، ص ٩٤.

[٢٦]– فتوح الشاذلي، جرائم التعزير المنظمة في المملكة العربية السعودية، مكتبة الرشد، الرياض، ط٤، ٢٠٢٠م، ص ٣٠٢ وما بعدها.

(ISSN: 2537 - 0758)

الحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بكاميرا أو ما في حكمها بعقوبة السجن لمدة لا تزيد عن سنة وبغرامة لا تزيد على خمسمائة ألف ريال أو بإحدى هاتين العقوبتين وذلك وفقًا لنص المادة الثالثة من نظام مكافحة جرائم المعلوماتية.

الفرع الرابع
جرائم الاعتداء على حقوق الملكية الفكرية

يقصد بها الاعتداء على حقوق المؤلفين المبدعين، فهي التي تتم عن طريق انتهاك حقوق الملكية الفكرية لآخرين دون إذن أو تصريح مسبق منهم باستخدام أحد الأنظمة الحاسوبية، ويكون بالاعتداء على العلامات التجارية وبراءات الاختراع، وكذلك نسخ وتقليد البرامج وإعادة إنتاجها وصنعها دون ترخيص فهو اعتداء على الحقوق المالية والحقوق الأدبية[٢٧].

الفرع الخامس
جرائم السطو السيبراني على الأموال

يهدف الجاني في جرائم السطو السيبراني للاستيلاء على مال مملوك للغير، باستخدام وسيلة من وسائل تقنية المعلومات، فيقوم المجرم السيبراني بالسطو على أموال البنوك مستخدمًا لجهاز الحاسب الآلي للدخول عبر شبكة الإنترنت والوصول غير المصرح به إلى البنوك لتحويل الأموال من الحسابات الخاصة بالعملاء إلى حسابات أخرى، أو يقوم المجرم باختراق المواقع التجارية التي تقدم خدمة عرض السلع عن طريق الإنترنت، ثم يحصل على قواعد البيانات والمعلومات الخاصة بالزبائن المتعاملين مع هذه المواقع ، فيقوم المستخدم بتخزين معلومات بطاقته الائتمانية بحيث يستطيع الشراء في كل مرة من نفس الموقع دون الحاجة إلى إدخال بيانات بطاقته مرة أخرى، فيقوم المجرم باستغلال هذه الفرصة واختراق جهاز الضحية والحصول على بيانات البطاقة واستخدامها في الشراء دون علم المجني عليه، وتعد هذه الجرائم من أكثر الجرائم السيبرانية انتشارًا[٢٨].

---

[٢٧]– محمد الردفاني، تحقيقات الشرطة في مواجهة تحديات الجرائم السيبرانية، المجلة العربية للدراسات الأمنية، المجلد ٣١، العدد (٦١)، ٢٠١٤م، ص ١١٥. وأنظر: روان الصحفي، مرجع سابق، ص ٣٤.

[٢٨]– مدحت رمضان، مرجع سابق، ص ٩٨. وانظر: تميم التميمي، مرجع سابق، ص ٩٨.

لذلك يعاقب المنظم السعودي على جرائم الاستيلاء والنصب والاحتيال السيبراني بعقوبة السجن لمدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين. وذلك وفقًا لنص المادة الرابعة من نظام مكافحة جرائم المعلوماتية.

الفرع السادس
جرائم التنصت السيبراني

وهي جرائم ترتكب عن طريق الدخول غير المشروع إلى النظام المعلوماتي، وذلك من خلال إرسال برنامج التنصت إلى جهاز المجني عليه عن طريق البريد الإلكتروني أو عن طريق مواقع يزورها المجني عليه، فيقوم بتنزيل بعض البرامج ومنها برنامج التنصت، ويمكن من خلاله الاستماع إلى جميع المحادثات والاطلاع على جميع المراسلات الصادرة من المجني عليه[٢٩].

ويعاقب المنظم السعودي على جرائم التنصت السيبراني بعقوبة السجن لمدة لا تزيد عن سنة وبغرامة لا تزيد على خمسمائة ألف ريال أو بإحدى هاتين العقوبتين وذلك وفقًا لنص المادة الثالثة من نظام مكافحة جرائم المعلوماتية.

الفرع السابع
جرائم التهديد والابتزاز السيبراني

يقوم المجرم السيبراني في جرائم التهديد والابتزاز السيبراني بتهديد المجني عليه إما بنشر أخباره أو صوره أو معلومات صحيحة، وفي هذه الحالة لا يرغب المجني عليه لسبب ما ظهورها للآخرين، ويقوم المجرم بطلب مقابل حتى لا ينشرها سواء كان هذا المقابل مادي أو معنوي، ولذلك يعاقب المنظم السعودي على جرائم التهديد والابتزاز السيبراني بعقوبة السجن لمدة لا تزيد عن سنة وبغرامة لا تزيد على خمسمائة ألف ريال أو بإحدى هاتين العقوبتين. وذلك وفقًا لنص المادة الثالثة من نظام مكافحة جرائم المعلوماتية.

---

[٢٩]– روان الصحفي، مرجع سابق، ص ٣٧. وانظر: زياد العتيبي، مرجع سابق ٨.

(ISSN: 2537 - 0758)

الفرع الثامن

جرائم الاستغلال الجنسي، والممارسات الغير أخلاقية، والاتجار بالبشر، والاتجار بالمخدرات وترويجها عبر استخدام منصات التواصل الاجتماعي:

يقوم المجرم السيبراني بالاستغلال الجنسي للقاصرين عبر استخدام منصات التواصل الاجتماعي المتاحة على الشبكة العنكبوتية من خلال ارتياد المواقع الإباحية أو إنشاءها، وإرسال الكتابات والصور والرسومات الفاضحة، والمنافية للآداب العامة والأفلام الإباحية والإشارات التي يشارك بها[٣٠].

وتعد جرائم الاتجار بالبشر من أخطر الجرائم السيبرانية، حيث يقوم المجرم السيبراني بإنشاء مواقع إلكترونية على الشبكة المعلومات للترويج لتجارة الرقيق الأبيض، أو الأطفال، أو الأعضاء البشرية، كما تستغل المجرم هذه المواقع في ترويج أفعال الدعارة والدعاية لها، والممارسات الغير أخلاقية. ويمكن استخدام هذه المواقع لتقديم التسهيلات لمن يمارسون نشاط الاتجار في الجنس البشري، أي تقديم كل ما من شأنه مساعدتهم في تجارتهم غير المشروعة في الجنس البشري.

ويستغل الجاني الفضاء السيبراني في تسهيل التعامل مع المخدرات والمؤثرات العقلية، عن طريق إنشاء مواقع إلكترونية للاتجار بالمخدرات والمؤثرات العقلية، أو ترويجها، أو تسهيل التعامل بها[٣١].

لذلك يعاقب المنظم السعودي على إنشاء مواقع إلكترونية للاتجار بالجنس البشري، وإنشاء المواد والبيانات المتعلقة بالشبكات الإباحية، أو أنشطة الميسر المخلة بالآداب العامة أو نشرها أو ترويجها، أو نشره للاتجار بالمخدرات أو المؤثرات العقلية أو ترويجها أو طرق تعاطيها أو تسهيل التعامل بها، بعقوبة السجن لمدة لا تزيد على خمس سنوات وبغرامة لا تزيد عن ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين، وذلك وفقًا لنص المادة السادسة من نظام مكافحة جرائم المعلوماتية.

---

[٣٠]– أسامة العبيدي، جريمة الاستغلال الجنسي للأطفال عبر شبكة الانترنت، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة – كلية القانون، المجلد ٢٧، العدد (٥٣)، ٢٠١٣م، ص ٦٥. وأنظر: زياد العتيبي، مرجع سابق، ص ٨.

[٣١]– محمود عزت، الفضاء السيبراني وتحديات الأمن المعلوماتي العربي، المجلة العربية، العدد (٤٩)، ٢٠١٨م، ص ١٨.

الفرع التاسع
التصيد السيبراني

وقد يستغل مجرموا الفضاء السيبراني وسائل تقنية المعلومات لمحاولة خداع المجني عليه للكشف عن معلوماته السرية مثل كلمات السر الخاصة به أو معلومات حسابه المصرفي[٣٢] على سبيل المثال: فقد يستغل الجاني جائحة فيروس كورونا فرصة للتصيد وسرقة المعلومات الشخصية للمجني عليهم من خلال إرسال رسائل من حسابات وهمية تحت مسمى وزارة الصحة وتطلب منه الدخول إلى رابط غيري معروف تستهدف البيانات الشخصية، وقد نبهت وزارة الصحة وكذلك المركز الوطني الإرشادي للأمن السيبراني على من هذه الرسائل المشبوه وعدم فتح الروابط الإلكترونية مجهولة المصدر.

وتعتبر الخدمات اللوجستية (شركات الشحن) جزءًا لا يتجزأ من نظام التجارة الإلكترونية، حيث قام المجرمون بانتحال شخصية البريد السعودي لتنفيذ عمليات التصيد الخاصة بهم عن طريق إرسال رسائل نصية. ومع انطلاق حملة إحسان مؤخرًا وخلال شهر رمضان المبارك، تم استغلال الحملة واهتمام الناس بفعل الخير في هذا الشهر الفضيل لإطلاق حملات تصيديه، وفي هجوم آخر، يحاول المجرمون إقناع المستخدمين من خلال استخدام المواقع الأكثر شهرة في المملكة مثل موقع أبشر للخدمات الحكومية وإعادة توجيه المستخدمين إلى موقع مستنسخ حيث يمكنهم سرقة معلومات المستخدمين[٣٣].

المطلب الثاني
أركان الجريمة السيبرانية

لا تختلف أركان الجريمة السيبرانية عن أركان أي جريمة تقليدية، لذلك فلابد من توافر الأركان العامة للجريمة وهي الركن القانوني والركن المادي والركن المعنوي، **لذلك سنتناول هذه الأركان من خلال الفروع التالية:**

---

[٣٢]– زياد العتيبي، مرجع سابق، ص ٩. وأنظر كذلك:
Sausan. W. Brenner. (2010), "Criminal Threats from Cyberspace", Santa Barbra: greenwood publishing group,p20.

[٣٣]– تاريخ الاطلاع ١٠/ ١/ ٢٠٢٢م، متاح على الموقع التالي:
https://www.citc.gov.sa/ar/Pages/default.aspx

(ISSN: 2537 - 0758)

الفرع الأول
الركن القانوني

تنص القاعدة القانونية على أنه: "**لا جريمة ولا عقوبة إلا بنص قانوني**" لذلك جرم النظام السعودي الجريمة السيبرانية وصورها في نظام مكافحة جرائم المعلوماتية بموجب المرسوم الملكي رقم (١٧) لعام ١٤٢٨هـ، وتم وصف الجرائم وصفًا دقيقًا مع بيان العقوبات عليها.

الفرع الثاني
الركن المادي

يعرف الركن المادي بأنه: "هو إتيان الفعل المحظور سواء كانت الجريمة إيجابية أو سلبية أي ارتكاب فعل جرمه القانون أو الامتناع عن فعل أمر به القانون"، ويتمثل الركن المادي للجريمة في سلوك إرادي يترتب عليه نتيجة إجرامية تربطها بالسلوك الإجرامي رابطة سببية مادية، ومفاد ذلك أن الركن المادي يتكون من ثلاث عناصر وهما السلوك الإجرامي، والنتيجة الإجرامية والعلاقة السببية.

أولاً: السلوك الإجرامي:

يقصد بالسلوك الإجرامي: هو ما يتخذه الجاني من نشاط إنساني إرادي له مظهر خارجي مادي لابد من توفره لوقوع الجريمة سواء كان سلوكًا إيجابيًا أم سلبيًا، ونري أنه، تعد الجرائم السيبرانية من الجرائم الإيجابية ويتمثل ذلك في النشاط الإرادي الخارجي الذي يستخدم فيه الجاني أعضاء جسمه لإحداث الأثر الخارجي المحسوس للسلوك مكونًا لماديات الجريمة ومسببًا لما قد يترتب عليها من ضرر أو خطر، فمثلًا جريمة الدخول غير المصرح به إلى موقع إلكتروني لتغيير تصاميمه أو تدمره أو تعديله، أو التشهير به إلكترونيًا، فهذا النوع من الجرائم لا يتحقق إلا إذا قام الجاني بالدخول غير المشروع من دون مسوغ نظامي إلى الموقع الإلكتروني للمجني عليه سواء كانت ملكيته عائدةً لشخص أو مؤسسه أو شركة خاصة أو حكومية، فالسلوك الإجرامي له صوره متعددة وتختلف باختلاف نوع الجريمة المرتكبة، ففي الجرائم السيبرانية لابد من قيام الجاني بممارسة نشاط تقني والشروع فيه باستخدام جهاز الحاسب الآلي متصل بشبكة الإنترنت في بيئة رقمية[٣٤].

[٣٤]– أسامة مهمل، مرجع سابق، ص ٣٥. وأنظر: روان الصحفي، مرجع سابق، ص ٣٩.

ثانياً: النتيجة الإجرامية:

تُعرّف النتيجة الإجرامية بأنها هي: "الأثر القانوني المترتب على السلوك الإجرامي للجريمة"، فهي تتمثل في النتيجة التي توصل إليها الجاني بالدخول الغير مشروع تقنيًا باستخدام جهاز حاسب آلي إلى بيانات المجني عليه بهدف الاستيلاء على معلومات بنكية أو تدمير مواقع إلكترونية وذلك باستخدام برامج اختراق التي تمكنه من الدخول غر المصرح به وتحقيق نتيجة ضارة.

ثالثاً: العلاقة السببية:

تُعرف العلاقة السببية بأنها هي: "الرابطة التي تصل بين سلوك الجاني والنتيجة المترتبة عليه"، لذلك حتى تكتمل جميع عناصر الركن المادي للجريمة لابد من وجود علاقة سببية تربط بين السلوك الإجرامي وما تحققه من نتيجة إجرامية، فإذا انتفت العلاقة السببية التي تربط بين السلوك الإجرامي والنتيجة الإجرامية فلن تكون هناك مساءلة جنائية للمتهم، على سبيل المثال: في العلاقة المباشرة بين السلوك الإجرامي المتمثلة في اختراق الجاني مواقع إلكترونية لدولة ما بطريقة غير مشروعة وما تحقق من نتيجة ضارة بالدولة وهي الحصول على البيانات والمعلومات سرية غير مصرح له بالحصول عليها[٣٥].

الفرع الثالث
الركن المعنوي

يتكون القصد الجنائي للجريمة السيبرانية من عنصري العلم والإرادة كسائر الجرائم العادية، لذلك حتى يتوافر القصد الجنائي لدي الجاني لابد أن يكون عالمًا بأنّ الدخول إلكترونيًا على بيانات خاصة غير مصرح للاطلاع أو الحصول عليها هو أمر غير مشروع، أما فيما يخص الإرادة فلابد أن تتجه إرادة الجاني إلى ارتكاب الفعل المجرّم، وينفي القصد الجنائي لدي الجاني عندما يكون الدخول إلى قاعدة البيانات الرقمية عن طريق الخطأ، وبالتالي تنتفي المسؤولية الجنائية[٣٦].

---

[٣٥]– أسامة مهمل، مرجع سابق، ص ٣٩. وأنظر: روان الصحفي، مرجع سابق، ص ٤٢.

[٣٦]– محمد الردفاني، مرجع سابق، ص ١٢٠. وأنظر: روان الصحفي، مرجع سابق، ص ٤٤.

(ISSN: 2537 - 0758)

المطلب الثالث
الأحكام العامة في الجرائم السيبرانية

وردت الأحكام العامة للجرائم السيبرانية في نظام مكافحة جرائم المعلوماتية وهي التي تتعلق بالمساهمة الجنائية، والشروع في الجريمة السيبرانية، والظروف المشددة للعقاب، والإعفاء من العقاب، **سنتناول ذلك من خلال الفروع التالية:**

الفرع الأول
المساهمة الجنائية في الجرائم السيبرانية

قد ينفرد الجاني بارتكاب الجريمة، فيأتي وحده ركنها المادي وتنسب إليه سائر عناصرها، وقد يتعدد مرتكبوا الجريمة، فيطلق عليها المساهمة الجنائية، إذا تعدد المساهمون في جريمة واحدة، فإن أدوارهم تتفاوت في تحقيق هذه الجريمة، فمنهم من يأتي أعمالًا تنفيذية تسهم في تحقيق ماديات الجريمة، فيكون مساهمًا أصليًا، ومنهم من تنحصر مساهمته في أعمال غير داخله في الركن المادي للجريمة، وإنما تقتصر على أعمال ثانوية تابعة، فيكون مساهمًا تبعيًا، يطلق عليه وصف الشريك في الجريمة أو الشركاء إذا تعددوا. وحدد المنظم السعودي في نص المادة التاسعة من نظام مكافحة جرائم المعلوماتية على وسائل الاشتراك في الجريمة وهي ذاتها وسائل الاشتراك في أي جريمة أخرى، فسلوك الشريك يتمثل في الاتفاق على الجريمة، أو تحريضه على ارتكابها، أو مساعدة فاعلها لتمكينه من ارتكابها. ويعاقب المنظم على الاشتراك في الجريمة السيبرانية بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها، ويعاقب بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة لها إذا لم تقع الجريمة الأصلية"[٣٧].

يتضح لنا مما سبق، أنه ساوى المنظم السعودي في العقوبة بين الفاعل الأصلي والشريك، كما أنه يميز في العقاب بين نوعين من الاشتراك في الجريمة التامة والاشتراك في الجريمة غير التامة، فيتحقق الاشتراك في الجريمة التامة عندما تقع الجريمة بناءً على وسيلة من وسائل الاشتراك، أي على الاتفاق أو التحريض أو المساعدة، فيعاقب الشريك بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها، ويتحقق الاشتراك في الجريمة غير التامة في الاشتراك في جريمة لم تقع أي توقفت عند مرحلة الشروع، فيعاقب الشريك بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة لها إذا لم تقع الجريمة الأصلية.

---

[٣٧]– أسامة مهمل، مرجع سابق، ص ٥٨. وأنظر: فتوح الشاذلي، مرجع سابق، ص ٣٥٢ وما بعدها.

الفرع الثاني
الشروع في الجريمة السيبرانية

يقصد بالشروع في الجريمة: هو عدم اكتمال الركن المادي للجريمة بسبب عدم تحقق النتيجة الإجرامية التي كان يقصدها الجاني لأسباب خارجة عن إرادة الجاني، ويعني ذلك بدء الجاني في تنفيذ الجريمة لكنه أوقف أو خاب أثره لأسباب خارجة عن إرادته. مفاد ذلك أن الشروع قد يكون شروعًا ناقصًا، ويسمي بالجريمة الموقوفة، وفيها يبدأ الجاني في تنفيذ السلوك الإجرامي بقصد تحقيق النتيجة، لكنه لا يتمكن من إتمام السلوك لأسباب خارجة عن إرادته، مثال ذلك: أن يبدأ الجاني في الدخول غير المشروع إلى مواقع إلكتروني، لكنه يضبط قبل أن يتمكن من إتمام الدخول الذي كان يقصد منه إتلاف الموقع أو تعديله. كما قد يكون الشروع خائبًا، ويسمى بالجريمة الخائبة، مثال ذلك: أن يدخل الجاني موقع إلكتروني دخولاً غير مصرح به، ويقوم ببعض الأعمال التي كان يقصد منها إتلاف الموقع أو تعديله، لكنه لنقص خبرته في كيفية الإتلاف أو التعديل، لا يتحقق النتيجة الإجرامية، ففي الشروع الخائب يتم الجاني نشاط الإجرامي كاملاً، لكن تتخلف النتيجة التي كان يريدها لأسباب خارجة عن إرادته[٣٨]. ويعاقب المنظم السعودي على الشروع في الجريمة السيبرانية بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة".

الفرع الثالث
الظروف المشددة للعقاب في الجريمة السيبرانية

نصت المادة الثامنة من نظام مكافحة جرائم المعلوماتية على أسباب تشديد العقاب المقرر للجريمة، حيث نصت المادة على أنه "لا تقل عقوبة السجن أو الغرامة عن نصف حدها الأعلى إذا اقترنت أي جريمة منها بظروف من الظروف المشددة للعقاب، وهي إذا ارتكاب الجاني الجريمة من خلال عصابة منظمة، أو الصفة العمومية للجاني، أو بالتغرير بالقصر واستغلالهم، أو بتحقق حالة العود إلى الجريمة".

الفرع الرابع
الإعفاء من العقاب في الجريمة السيبرانية

نصت المادة الحادية عشرة من نظام مكافحة جرائم المعلوماتية على الإعفاء المقرر من العقاب المستحق عن الجريمة السيبرانية، والتي تقرر للمحكمة المختصة أن تعفي

---

[٣٨]– محمود القرعان، مرجع سابق، ص ٩٠. وانظر: محمد العريان، مرجع سابق، ص ١٠٤.

(ISSN: 2537 - 0758)

الجاني من العقوبة في حالة إبلاغه السلطة المختصة بالجريمة قبل العلم بها وقبل وقوع الضرر، إما في حالة إذا كان الإبلاغ بعد العلم بالجريمة، فيتعين على الجاني لاستفادة من الإعفاء أن يكون من شأن هذا الإبلاغ ضبط باقي الجناة في حال تعددهم، أو الأدوات المستخدمة في الجريمة. وثبوت حق المحكمة في إعفاء الجاني الذي بادر بالإبلاغ عن الجريمة من العقوبة المقررة لها. أما باقي الجناة في حالة المساهمة الجنائية لا يستفيدون من هذا الإعفاء، لأن موانع العقاب شخصية، لا يستفيد منها غير من تحقيق موجب الإعفاء بالنسبة له.

المبحث الثالث
جهود المملكة العربية السعودية في مكافحة الجرائم السيبرانية

احتلت المملكة العربية السعودية المرتبة الثانية عالميًا من بين ١٩٣ دولة في العالم، والمركز الأول على مستوى الوطن العربي والشرق الأوسط وقارة آسيا في المؤشر العالمي للأمن السيبراني GCI، الذي تصدره وكالة الأمم المتحدة المتخصصة في تكنولوجيا المعلومات والاتصالات– الاتحاد الدولي للاتصالات. وتعكس هذه المرتبة الجهود المبذولة في مجال الأمن السيبراني بالمملكة للوصول إلى فضاء سيبراني آمن وموثوق يمكّن النمو والازدهار.

وفي ضوء ذلك، سنتناول في هذا المبحث جهود المملكة في مكافحة للجرائم السيبرانية من خلال المطالب التالية: المطلب الأول لنظام مكافحة جرائم المعلوماتية، المطلب الثاني للهيئة الوطنية للأمن السيبراني، المطلب الثالث لشركة ريثيون العربية السعودية، المطلب الرابع الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ٢٠١٠م.

المطلب الأول
نظام مكافحة جرائم المعلوماتية

أدركت المملكة السعودية العربية خطورة الجرائم السيبرانية على المصالح الوطنية، وعلى القيم والتقاليد والعادات الإسلامية التي تسود في المجتمع السعودي، لذلك سارعت المملكة في إصدار نظامًا خاصًا لمكافحة جرائم تقنية المعلومات، حيث وافق مجلس الوزراء على نظام مكافحة جرائم المعلوماتية بموجب المرسوم الملكي رقم (١٧) لعام ١٤٢٨هـ، ويحتوي هذا النظام على ست عشرة مادة، يبدأ بالتعريفات في المادة الأولى، وتحديد أهداف النظام في المادة الثانية، ثم تتوالى النصوص الخاصة بالتجريم والعقاب وبعض القواعد الإجرائية.

وقد حدد المنظم السعودي في المادة الثانية من هذا النظام على أهداف للحد من وقوع الجرائم السيبرانية وهي على النحو التالي:-

- المساعدة على تحقيق الأمن المعلوماتي، عن طريق الحفاظ على سرية المعلومات التي تخص الدول والأفراد ويتم حفظها في الوسائط الإلكترونية.
- حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية، وهي حقوق للدولة ومؤسساتها وللأفراد.
- حماية المصلحة العامة، وحماية الأخلاق، والآداب العامة وحرمة الأديان، والحياة الخاصة للآخرين.
- حماية الاقتصاد الوطني، عن طريق تجريم عمليات الاختراق غير المشروع لشبكات المعلومات في المصارف والمؤسسات المالية.

المطلب الثاني
الهيئة الوطنية للأمن السيبراني

تسعى المملكة العربية السعودية لتكون ضمن مصاف دول العالم في الاقتصاد الرقمي من خلال الاستثمار في القطاعات التقنية، لذلك تحمل الهيئة الوطنية للأمن السيبراني على عاتقها حماية مصالح مستخدمي خدمات الاتصالات وتقنية المعلومات، وذلك من خلال إطلاق مبادرات تتماشى مع أفضل الممارسات العالمية في مجال الأمن السيبراني[٣٩].

١- الاستراتيجية الوطنية للأمن السيبراني وأهدافها:

وضعت الهيئة الوطنية للأمن السيبراني رؤية الاستراتيجية لتلبي أولويات المملكة وتطلعاتها، وتتضمن هذه الرؤية للوصول إلى فضاء سيبراني سعودي آمن وموثوق يمكّن النمو والازدهار، من خلال تعزيز حماية الأنظمة التقنية، وقدرتها على التصدي للهجمات السيبرانية. وتهدف الاستراتيجية الوطنية للأمن السيبراني إلى ستة أهداف رئيسية وهي على النحو التالي[٤٠]:

- حوكمة متكاملة للأمن السيبراني على المستوى الوطني.
- إدارة فعالة للمخاطر السيبرانية على المستوى الوطني.

---

[٣٩]- تاريخ الاطلاع ٢٠٢٢/١/١، متاح على الموقع التالي: https://nca.gov.sa/index.html

[٤٠]- تاريخ الاطلاع ٢٠٢٢/١/١، متاح على الموقع التالي:
https://nca.gov.sa/pages/strategic.html

(ISSN: 2537 - 0758)

- حماية الفضاء السيبراني.
- تعزيز القدرات الوطنية في الدفاع ضد التهديدات السيبرانية.
- تعزيز الشراكات والتعاون في الأمن السيبراني.
- بناء القدرات البشرية الوطنية وتطوير صناعة الأمن السيبراني في المملكة.

٢- الأطر والارشادات والبرامج والمبادرات للهيئة الوطنية للأمن السيبراني:

وقد أصدرت الهيئة الوطنية للأمن السيبراني عددًا من الضوابط والأطر والإرشادات والبرامج والمبادرات ذات العلاقة بالأمن السيبراني على المستوى الوطني بهدف حمايةً المصالح الحيوية للدولة وأمنها والقطاعات الحكومية المختلفة.

وتشتمل أهم هذه الأطر والإرشادات والبرامج والمبادرات التي أصدرتها الهيئة ما يلي:

- **الإطار المرجعي للأمن السيبراني:**

حرصت الهيئة الوطنية للأمن السيبراني على تصميم إطار مرجعي مبني على أفضل الممارسات المحلية والعالمية وأهم المستجدات والتحديات التي تواجه الأمن السيبراني، بحيث يعد نموذجًا متقدمًا يشمل الجوانب المختلفة للأمن السيبراني على مستوى الدول، ويحتوي هذا الإطار على ستة محاور رئيسية وهما: التكامل، التنظيم، التوكيد، الدفاع، التعاون، البناء.

- **الإطار الوطني للتعليم العالي في الأمن السيبراني:**

عملت الهيئة الوطنية للأمن السيبراني مع وزارة التعليم وهيئة تقويم التعليم والتدريب وعدد من الجامعات في المملكة على إعداد "الإطار السعودي للتعليم العالي في الأمن السيبراني" ليكون دليلًا إرشاديًا يمكن الاستفادة منه في إعداد وتطوير وتقييم واعتماد برامج التعليم العالي في الأمن السيبراني.

- **المركز الوطني الإرشادي للأمن السيبراني:**

تم إطلاق المركز الوطني الإرشادي للأمن السيبراني ليعمل على إصدار التنبيهات بآخر وأخطر الثغرات، كما يعمل على إطلاق حملات توعوية لرفع مستوى الوعي بالأمن السيبراني، بالتعاون مع المراكز الإرشادية الأخرى بالمملكة.

- **الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز:**

تم إطلاق الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز تحت مظلة اللجنة الأولمبية السعودية؛ للعمل على تقديم أنشطة وبرامج تساهم في زيادة وعي المجتمع

بالأمن السيبراني والبرمجة والدرونز، ودعم وتشجيع الشباب للاحتراف في هذا المجال. وسهّلت منصة مكافآت الثغرات وهي عبارة عن منصة إلكترونية تهدف إلى توظيف المهارات والخبرات للباحثين في الأمن السيبراني، من أجل اكتشاف الثغرات البرمجية في المواقع التقنية.

- **الأكاديمية الوطنية للأمن السيبراني:**

أطلقت هيئة الاتصالات وتقنية المعلومات بالتعاون مع صندوق تنمية الموارد البشرية مبادرة (هدف) لرفع مستوى القدرات الرقمية في مختلف مجالات التقنية الحديثة لمواكبة التحول الرقمي.

- **مبادرة حصين:**

أُطلِقت مبادرة حصين من أجل تعزيز الأمن السيبراني على المستوى الوطني، وتُعنى بحماية البريد الإلكتروني السعودي من الانتحال والاستخدام الغير مصرح به.

وجدير بالذكر أنه، شاركت الهيئة الوطنية للأمن السيبراني ممثلةً بالمركز الوطني الإرشادي للأمن السيبراني، في التمرين الافتراضي للأمن السيبراني الثامن تحت عنوان "التحكم في مخاطر الأمن الإلكتروني المصاحبة للعمل عن بعد"، بمشاركة ٢٥ دولة عربية وإقليمية، ويهدف هذا التمرين إلى تعزيز الجهود للتصدي للمخاطر والتهديدات السيبرانية المختلفة وطرق معالجتها.

كما وقَّعت الهيئة الوطنية للأمن السيبراني مذكرة شراكة إستراتيجية مع الشركة السعودية لتقنية المعلومات (سايت) لرعاية المنتدى الدولي للأمن السيبراني ٢٠٢٢م، وتأتي هذه المذكرة في إطار جهود المنتدى الدولي للأمن السيبراني ٢٠٢٢م الرامية إلى فتح المزيد من آفاق المعرفة حول موضوعات الأمن السيبراني. وتم عقد منتدى في فترة ٣١يناير حتى ٢ فبراير ٢٠٢٢م، في الرياض، تحت عنوان "إعادة التفكير في الترتيبات السيبرانية العالمية (Rethinking the Global Cyber Order) وأتاح هذا المنتدى الفرصة للمؤسسات الدولية لعقد شراكات جديدة، وإقامة حوارات هادفة حول القضايا الدولية للأمن السيبراني، وتعزيز التعاون، ومشاركة أفضل ممارسات الدول في كيفية معالجة التهديدات السيبرانية الحالية والمستقبلية[٤١].

---

[٤١]- تاريخ الاطلاع ٥/ ١/ ٢٠٢٢م، متاح على الموقع التالي: https://cert.gov.sa/ar//

(ISSN: 2537 - 0758)

المطلب الثالث

شركة ريثيون العربية السعودية Raytheon

شركة ريثيون العربية السعودية: هي شركة سعودية مختصة بأنظمة الدفاع والفضاء والأمن السيبراني، وتم تأسيسها بموجب اتفاقية تفاهم وقعتها شركة ريثيون الأمريكية ومع الشركة السعودية للصناعات العسكرية، وتتخذ الشركة من الرياض مقرًا لها، وتعمل هذه الشركة على توفير الخدمات الدفاعية العسكرية والسيبرانية، وتطبيق البرامج التي من شأنها العمل على تعزيز القدرات الدفاعية العسكرية والأمنية المختلفة للمملكة، وقدمت الشركة مجموعة من حلول الأمن السيبراني المتطورة، والدورات التدريبية في هذا المجال، وكذلك المعرفة والدعم التشغيلي اللازم في منطقة الشرق الأوسط.

وتم وقعت مذكرة تفاهم بين شركة «**أرامكو السعودية**» وشركة **Raytheon** عبر شركتها التابعة «**ريثيون العربية السعودية**»، لإطلاق مشروع مشترك لتطوير وتقديم خدمات وحماية الأمن السيبراني في المملكة العربية السعودية والمنطقة[٤٢].

المطلب الرابع

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ٢٠١٠م

وافق مجلسا وزراء الداخلية والعدل العرب في اجتماعهما المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بتاريخ ١٤٣٢/١/١٥هـ- ٢٠١٠/١٢/٢١م، وصدقت المملكة العربية السعودية على هذه الاتفاقية بتاريخ ٤ مارس٢٠١٢م، وتأتي أهمية هذه الاتفاقية في ظل تزايد الاختراعات التقنية في الهواتف الذكية وأجهزة الحاسوب التي يختفي وراءها مجرموا الاختراقات للمواقع الإلكترونية وارتكاب الجرائم من خلال تقنية الحاسوب.

وتحتوي اتفاقية مكافحة جرائم تقنية المعلومات على ٤٣ مادة، حيث نصت المادة الأولى منها على أنه: "تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات لدرء أخطار هذه الجرائم، حفاظًا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها"، ونجد في الفصل الثاني تفصيلًا للأفعال التي تعد مجرمة، أما الفصل الثالث منها فقد تم التعرض من خلاله إلى

---

[٤٢]- تاريخ الاطلاع ٢٠٢٢/١/٢٤م، متاح على الموقع التالي:
https://www.raytheon.com/ar/ksa/ourcompany

نطاق تطبيق الأحكام الإجرائية، وفي الفصل الرابع نصت على التعاون القانوني والقضائي، أما الفصل الخامس فتضمن أحكاما ختامية[٤٣].

تطبيقات على أمثلة للهجمات السيبرانية:

- **هجوم NotPetya:**

استُهدفت أوكرانيا عدّة مرّات بهجمات سيبرانية في السنوات الأخيرة، ومما يشار إليه الهجمات السيبرانية الأخيرة بتاريخ ٢٢ فبراير ٢٠٢٢م، والتي تسببت في أن بعض المواقع الإلكترونية الحكومية لم تعد متاحة بسبب تعرضها لهجوم سيبراني، وفي مايو عام ٢٠١٧م، طال هجوم معلوماتي بنى تحتية مهمّة، وعُرف هذا الهجوم باسم **NotPetya** هو عبارة عن برنامج من برامج الفدية الضارة بدأ في التداول عبر البريد الإلكتروني المتصيد في عام٢٠١٦م، وقام بتشفير نظام التشغيل في الأجهزة التي تم اختراقها، مما أدي إلى منع المستخدمين من الوصول إلى ملفاتهم الخاصة. وتم توجيه الاتهام إلى روسيا من قبل أوكرانيا بأنها هي وراء هجوم **NotPetya**، لكن روسيا أنكرت هذا الادعاء. وفي عام ٢٠١٥م، تتعرض أوكرانيا لهجوم سيبراني استهدف شبكتها الكهربائية[٤٤].

- **شركة أرامكو النفطية السعودية:**

واجهت شركة أرامكو السعودية في مايو ٢٠٢١م، عمليات ابتزاز سيبراني من قبل قراصنة، وتُعد شركة أرامكو أكبر شركة نفط في العالم من حيث القيمة السوقية، وقد تعرضت الشركة في عام ٢٠١٢م، لهجوم سيبراني تسبب في حذف محركات الأقراص الصلبة وتدمير أكثر من ٣٠ ألف جهاز حاسب آلي، وعُرف هذا الهجوم باسم فيروس شمعون. وفي عام ٢٠١٧م، انتشر فيروس آخر عطل أجهزة حاسبات في مشروع "صدارة"، المشترك بين أرامكو وشركة داو للكيماويات ومقرها ميشيغان، وصدرت تحذيرات حينها من أنه قد يكون نسخة أخرى من فيروس "شمعون"[٤٥].

---

[٤٣]- تاريخ الاطلاع ٢/ ١/ ٢٠٢٢م، متاح على الموقع التالي: www.arablegalnet.org

[٤٤]- تاريخ الاطلاع ٢٥/ ١/ ٢٠٢٢م، متاح على الموقع التالي:
https://arabic.cnn.com/tech/2017/10/25/bad-rabbit-ransomware-attack

[٤٥]- تاريخ الاطلاع ٢٢/ ١/٢٠٢٢م، متاح على الموقع التالي:
https://www.bbc.com/arabic/business-57928996

(ISSN: 2537 - 0758)

- **هجمات منصات قمة العشرين الرياض ٢٠٢٠ (G20 Riyadh 2020 summit):**

أعلنت هيئة البيانات والذكاء الاصطناعي **(SDAIA)** في المملكة العربية السعودية بأنها تعاملت مع عددً من التهديدات السيبرانية التي استهدفت منصات "**مجموعة العشرين**" أثناء انعقادها لأول قمة استثنائية افتراضية لقادة دول مجموعة العشرين بتاريخ ٢٦ مارس ٢٠٢٠م، والذي ترأسها خادم الحرمين الشريفين جلالة الملك "سلمان بن عبد العزيز" حفظه الله ملك المملكة العربية السعودية، لمناقشة مكافحة جائحة كورونا والحد من تأثيرها الإنساني والاقتصادي، وكما كشف المدير التنفيذي لأمن المعلومات في "**سدايا**" أنه تم التصدي لجميع الهجمات السيبرانية على منصة "**بروق**" من خلال أنظمة الحماية الخاصة بها(٤٦).

- **هجوم GitHub:**

تم اختراق الإصدار المتحكم في خدمة المضيف **GitHub** بهجوم حجب الخدمات في ٢٨ فبراير ٢٠١٨م، ورغم أن **GitHub** قد تعرض لعملية قطع اتصاله بالإنترنت بصورة متقطعة، ونجاحه في صد هذا الهجوم في وقت قصير، ولكن كانت لها الآثار الهائلة، فهجوم **GitHub** استغل أجهزة السيرفر التي تُشغل نظام التخزين المؤقت للذاكرة، والتي يمكنها إعادة مجموعات ضخمة للغاية من البيانات استجابةً للطلبات البسيطة(٤٧).

- **هجوم WannaCry:**

هو هجوم باستخدام برامج الفدية الضارة، وتم تثبيتها بشكل خاص في أجهزة الكمبيوتر بالمستشفيات التي تديرها هيئة الخدمات الصحية الوطنية البريطانية **(NHS)** في مايو ٢٠١٧م، فقد استغل إحدى الثغرات في **Microsoft Windows** واستخدم أداة استغلال الثغرات **EternalBlue**، وقد تمت اختراقها من إحدى المجموعات المخترقة التي تُطلق على نفسها اسم Shadow Brokers. وقامت

(٤٦)– تاريخ الاطلاع ٢٤/ ١/ ٢٠٢٢م، متاح على الموقع التالي:
https://www.independentarabia.com/node/1709010

(٤٧)– تاريخ الاطلاع ٢٢/١/ ٢٠٢٢م، متاح على الموقع التالي:
https://arabicprogrammer.com/article/37351066311/

شركة **Microsoft** بالفعل بتصحيح الثغرة قبلها بأسابيع قليلة، لكن لم يتم تحديث العديد من الأنظمة[٤٨].

- **Yahoo:**

تم اختراق نظام البريد الإلكتروني الخاص بشركة **Yahoo** في عام ٢٠١٣م، ولكن ظهرت تداعياته في أكتوبر ٢٠١٧م، وتسبب هذا الاختراق في سرقت كلمات المرور وعناوين البريد الإلكتروني المنسوخة[٤٩].

الخاتمة

استهدفت الدراسة مدى التعرف على آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية، فالجرائم السيبرانية هي ظاهرة إجرامية مستحدثة نسبيًا، ومع التزايد الهائل لأعداد الهجمات السيبرانية، وعمليات القرصنة، والاختراقات المتكررة للعديد من الدول، كان لابد من ضرورة وجود الأنظمة القانونية والتشريعات التي تساهم في حماية الدول من هذه الهجمات السيبرانية المختلفة.

النتائج:

- تُعد الجرائم السيبرانية من أخطر الجرائم شيوعًا خلال السنوات الأخيرة، نظرًا لإتاحة العديد من الوزارات والشركات والمؤسسات تطبيقاتها عبر شبكات الإنترنت.
- تعتبر الجرائم السيبرانية من الجرائم المستحدثة؛ لذلك لم يستقر الفقهاء على وضع تعريف محدد للجرائم الناشئة في بيئة الحاسب الآلي أو الشبكات العنكبوتية.
- تعتمد الجرائم السيبرانية في ارتكابها على جهاز الحاسب الآلي كوسيلة وموضوعًا للجريمة، وهذا ما يميزها عن الجرائم الأخرى.
- تتميز الجرائم السيبرانية بالخفاء؛ لأنها تقع في فضاء سيبراني لا حدود له، وفي الغالب لا يشعر بها المجني عليه كسرقة البيانات أو إرسال الفيروسات إلى جهازه.
- تتميز الجرائم السيبرانية بأنها جرائم عابرة للحدود؛ لأنها لا تنحصر في دولة معينة أو قارة معينة؛ نظرًا لأنها تتم في بيئة افتراضية لا حدود لها.

---

[٤٨]– تاريخ الاطلاع ٢٢/ ١/ ٢٠٢٢م، متاح على الموقع التالي:
https://me.kaspersky.com/resource-center/threats/ransomware-wannacry

[٤٩]– تاريخ الاطلاع ٢٠٢٢/١/٢٥م، متاح على الموقع التالي:
https://arabic.rt.com/it/902652-

(ISSN: 2537 - 0758)

- يتميز المتورطين في الجرائم السيبرانية بخصائص تميزهم عن غيرهم من المتورطين في الجرائم التقليدية.
- تتنوع صور الجرائم السيبرانية والتي يصعب حصرها في صور محددة؛ نظرًا لأنها جرائم مرتبطة بالتقنية المعلوماتية والتي تتطور تبعًا لتطور هذه التقنية.
- احتلت المملكة العربية السعودية المرتبة الثانية عالميًا من بين ١٩٣ دولة في العالم، والمركز الأول على مستوى الوطن العربي والشرق الأوسط وقارة آسيا في المؤشر العالمي للأمن السيبراني GCI.
- أدركت المملكة السعودية العربية خطورة الجرائم السيبرانية على المصالح الوطنية، لذلك سارعت المملكة في إصدار نظامًا خاصًا لمكافحة جرائم تقنية المعلومات.
- هدفت المملكة إلى تحقيق فضاء سيبراني سعودي أمن، من خلال إعداد خطط فاعلة لمواجهة الهجمات السيبرانية، وخصصت ميزانية مهولة لتحقيق أهداف خطتها الإستراتيجية للأمن السيبراني.

التوصيات:

بناءً على نتائج الدراسة السابقة، توصي الدراسة بما يلي:

- تطوير الأنظمة الخاصة بحماية البيانات المعلوماتية، ومراجعتها بصورة دورية لمواكبة سرعة التقدم التقني.
- إنشاء نيابة متخصصة للتحقيق في الجرائم السيبرانية، وتأهيل مأموري الضبط القضائي وتدريبهم للتعامل مع هذا النوع من الجرائم.
- إنشاء محاكم متخصصة للنظر في الجرائم السيبرانية.
- تشديد النصوص العقابية على الجرائم السيبرانية للتصدي لها.
- ضرورة عقد الاتفاقيات الدولية والإقليمية بين الدول لمكافحة الجرائم السيبرانية.
- تنمية البنية التحتية للأمن السيبراني داخل المملكة، للحد من عمليات الاختراق وتأمين البيانات المعلوماتية داخل المملكة والقطاعات الحكومية.
- ضرورة توعية أفراد المجتمع السعودي وخاصةً العاملين في القطاعات المختلفة، حول مخاطر عمليات الاختراقات والهجمات السيبرانية المختلفة، والتركيز على تعزيز الأمن السيبراني.

- ضرورة توعية الوالدين لما يقوم به الأطفال، وعدم مقدرتهم على السيطرة على كل ما تصل له أيديهم على الإنترنت، خاصة في حالة تنزيل البرامج المختلفة، التي قد تضر بالأجهزة.
- يجب نشر الوعي بين الشباب وخاصَّة الأطفال بمخاطر التعامل مع المواقع المشبوهة على الشبكات، وإشراك منظمات المجتمع المدني ببرامج التوعية والإرشاد بمخاطر الجرائم السيبرانية.
- إدراج مجال الأمن السيبراني ضمن المناهج التعليمية للمراحل الدراسية المختلفة بالمملكة.

المراجع

أولاً: المراجع العربية:

١- **الكتب:**

- تميم التميمي، الجرائم المعلوماتية في الاعتداء على الأشخاص، مكتبة القانون والاقتصاد، الرياض، ط١، ٢٠١٦م.
- صالح الربيعة، الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت، هيئة الاتصالات وتقنية المعلومات، الرياض، ٢٠١٧م.
- طاهر أبو القاسم، الجرائم المعلوماتية، صعوبات التحقيق فيها وكيفية مواجهتها، منشورات المنظمة العربية للتنمية الإدارية بجامعة الدول العربية، الشارقة، ط١ ٢٠١٩م.
- عبد العزيز آل جار الله، جرائم الإنترنت وعقوباتها وفقًا نظام مكافحة جرائم المعلوماتية السعودي، دار الكتاب الجامعي للنشر والتوزيع، الرياض، ط١، ٢٠١٧م.
- عبد العال الديربي، محمد إسماعيل، الجرائم الإلكترونية، المركز القومي للإصدارات القانونية، القاهرة، ط١، ٢٠١٢م.
- عبيس الفتلاوي، الهجمات السيبرانية، منشورات زين الحقوقية، بيروت، ط١، ٢٠١٨م.
- غانم الشمري، الجرائم المعلوماتية، الدار العلمية الدولية، عمان، ط١، ٢٠١٦م.
- فتوح الشاذلي، جرائم التعزير المنظمة في المملكة العربية السعودية، مكتبة الرشد، الرياض، ط٤، ٢٠٢٠م.

(ISSN: 2537 - 0758)

- محمد العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر والتوزيع، الإسكندرية، ٢٠٠٤م.
- محمود القرعان، الجرائم الإلكترونية، دار وائل النشر والتوزيع، عمان، ط١، ٢٠١٧م.
- مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٩م.
- نظام مكافحة الجرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/١٧ بتاريخ ١٤٢٨/٣/٨هـ.

٢- **البحوث ورسائل الماجستير والدكتوراه:**

- أسامة العبيدي، جريمة الاستغلال الجنسي للأطفال عبر شبكة الانترنت، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة- كلية القانون، المجلد ٢٧، العدد (٥٣)، ٢٠١٣م، ٥٧ -١٣٠.
- أسامة مهمل، الإجرام السيبراني، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، ٢٠١٨م.
- حاتم بطيخ، تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات، مجلة الدراسات القانونية والاقتصادية، كلية الحقوق، جامعة مدينة السادات، المجلد ٧، العدد (١)، ٢٠٢١م، ٥١- ١٠٢.
- روان الصحفي، الجرائم السيبرانية، المجلة الإلكترونية الشاملة، العدد (٢٤)، ٢٠٢٠م، ١- ٥٣.
- زياد العتيبي، جرائم السيبرانية المرتكبة عبر الوسائط الرقمية، المجلة الأكاديمية العالمية للدراسات القانونية، المجلد ٣، العدد (١)، ٢٠٢١م، ١- ٩.
- عبد السلام المايل، عادل الشربجي، الجريمة الإلكترونية في الفضاء الإلكتروني، مجلة آفاق للبحوث والدراسات، العدد (٤)، ٢٠١٩م، ١- ١٦.
- علي الشهري، رؤية استراتيجية للحد من الجرائم الإلكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية، رسالة دكتوراه، كلية العلوم الاستراتيجية، جامعة نايف العربية للعلوم الأمنية، ٢٠١٩م.
- محمد الردفاني، تحقيقات الشرطة في مواجهة تحديات الجرائم السيبرانية، المجلة العربية للدراسات الأمنية، المجلد ٣١، العدد (٦١)، ٢٠١٤م، ١١١- ١٢٥.
- محمد المقصودي، الجرائم المعلوماتية، مجلة العربية للدراسات الأمينة، المجلد ٣٣، العدد (٧)، ٢٠١٧م، ١٠١- ١٣١.

- محمود عزت، الفضاء السيبراني وتحديات الأمن المعلوماتي العربي، المجلة العربية، العدد (٤٩)، ٢٠١٨م، ١-٥٣.
- وفاء لطفي، الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني، مجلة كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، المجلد ٢٣، العدد (١)، ٢٠٢٢م، ١٥٢- ٢٠٥.

ثانياً: المراجع الإنجليزية:

- Chawki, M. (2005). A critical look at the regulation of cybercrime. IV (4) The ICFAI Journal of Cyberlaw.
- Dashora, K. (2011). Cyber crime in the society: Problems and preventions. Journal of Alternative Perspectives in the social sciences, 3(1).
- Dominic Carucci, David Overhuls & Nicholas Soares. (2011) "Computer Crimes", CRIM. L. REV. ,375.
- Halder. D., & Jaishankar. K. (2011) "Cybercrime and the Victimization of Women": Laws, Rights, and Regulations. Hershey, PA, USA.
- Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). Cyber threats to health information systems: A systematic review. Technology and Health Care, 24(1), pp.1-9.
- Michael.A. Dennis. (2018)." Cybercrime", Selected by Britannica Academic, Encyclopedia Britannica, PP. 1-51.
- Mayer. Jonathan. (2016) Cybercrime litigation, University of Pennsylvania Law Review, 164 U. Pa. L. Rev. 10521 -1453.
- Schjolberg, Stein .(2014) the History of Cybercrime: 2014-1976, Volume 9, Cybercrime Research Institute GmbH.
- Sausan. W. Brenner. (2010), "Criminal Threats from Cyberspace", Santa Barbra: greenwood publishing group.
- United Nations Office on Drugs and Crime (UNODC)F.(2013),"Comprehensive Study on Cybercrime". Vienna: United Nations.
- Wall, D. (1999). Cybercrimes: New wine, no bottles. In Invisible crimes (pp. 105-139). Palgrave Macmillan, London.

(ISSN: 2537 - 0758)

ثالثا: المواقع الإلكترونية:

- الهجمات السيبرانية على شركة أرامكو السعودية تاريخ الاطلاع ٢٢/ ١/٢٠٢٢م، متاح على الموقع التالي:
https://www.bbc.com/arabic/business-57928996
- موقع الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بتاريخ ٢١ ديسمبر ٢٠١٠م، تاريخ الاطلاع ٢/ ١/ ٢٠٢٢م، متاح على الموقع التالي:
www.arablegalnet.org
- موقع المركز الوطني الإرشادي للأمن السيبراني، تاريخ الاطلاع ٥/ ١/ ٢٠٢٢م، متاح على الموقع التالي: **//https://cert.gov.sa/ar**
- موقع الهيئة الوطنية للأمن السيبراني، تاريخ الاطلاع ٢٠٢٢/١/١، متاح على الموقع التالي:
https://nca.gov.sa/index.html
- شركة ريثيون العربية السعودية، تاريخ الاطلاع ٢٠٢٢/١/٢٤م، متاح على الموقع التالي: **https://www.raytheon.com/ar/ksa/ourcompany**
- موقع هيئة الاتصالات وتقنية المعلومات، تاريخ الاطلاع ١٠/ ١/ ٢٠٢٢م، متاح على الموقع التالي: **https://www.citc.gov.sa/ar/Pages/default.aspx**
- هجمات **منصات قمة العشرين ٢٠٢٠** الرياض، تاريخ الاطلاع ٢٤/ ١/ ٢٠٢٢م، متاح على الموقع التالي:
https://www.independentarabia.com/node/1709010
- **هجوم GitHub**، تاريخ الاطلاع ٢٢/١/ ٢٠٢٢م، متاح على الموقع التالي:
https://arabicprogrammer.com/article/37351066311/
- **هجوم WannaCry**، تاريخ الاطلاع ٢٢/ ١/ ٢٠٢٢م، متاح على الموقع التالي:
https://me.kaspersky.com/resource-center/threats/ransomware-wannacry
- هجوم على شركة **Yahoo الأمريكية**، تاريخ الاطلاع ٢٠٢٢/١/٢٥م، متاح على الموقع التالي: **https://arabic.rt.com/it/902652-.**