مجلـــة العلـــوم التربـــوية والدراســـات الإنســـانيـــة
ISSN: 2709-0302 (online)
Humanities and Educational Sciences Journal
ISSN: 2617-5908 (print)

جرائم الأمن السيبراني في النظام السعودي(*)

الباحث/ محمد مشلوي يحيى الريثي

د/ عبد المجيد عبد الله القرني

الأستاذ المساعد بكلية العلوم الإدارية

جامعة نجران - السعودية

نشر ملخص رسالة ماجستير بعد اجازتها علميا من جامعة نجران في عام 1444هـ - 2023م.

*) تاريخ تسليم البحث 27/11/2024 تاريخ قبوله للنشر 2/1/2025
*) موقع المجلة: http://hesj.org/ojs/index.php/hesj/index

جرائم الأمن السيبراني في النظام السعودي

الباحث/ محمد مشلوي يحي الريثي

د/ عبد المجيد عبد الله القرني

الأستاذ المساعد بكلية العلوم الإدارية

جامعة نجران - السعودية

الملخص

الحمد لله والصلاة والسلام على أشرف خلق الله..... وبعد

قال تعالى: (وَإِنْ تَعُدُّوا نِعْمَةَ اللَّهِ لَا تُحْصُوهَا إِنَّ اللَّهَ لَغَفُورٌ رَحِيمٌ)[1].

لقد أنعم الله علينا بنعمة كثيرة، ومنها نعمة الاتصالات، وتقنية المعلومات، والحاسبات، والإنترنت في مختلف مجالات الحياة في عصرنا الحديث، لتقديم الخدمات، وتبادل المعلومات في مجال الاتصالات وأنظمة المعلومات، ومع هذا التقدم، وانتقال المجتمع من الواقع الفعلي المادي إلى الواقع السيبراني، شهدنا ظهور جرائم الأمن السيبراني، وتعديها على الفرد والمجتمع بشكل متزايد وملحوظ، لذا فقد أصبحت دراسة الأمن السيبراني واحدة من مستحدثات التطور التكنولوجي والرقمي الذي نعايشه في العالم مؤخرًا، حيث يشهد العالم المتقدم تطورًا كبيرًا لا يُمكننا بأي حال أن نَصِفُهَا، لذا أصبحت تلك الدراسات التكنولوجية في مجال الحوسبة الرقمية مقاصد الكثيرين من الدارسين المتميزين حول العالم، ولكن يوجد جانب آخر مظلم، لذلك التطور الرقمي الذي نشهده يُمكن أن يجعل كبار الدول، والشركات، والمؤسسات التجارية، والاقتصادية مهددة بالاختراق، ولعل من أسباب أهمية دراسة الأمن السيبراني حماية البيانات، والشبكات، والأنظمة الالكترونية من الهجمات، والاختراقات التي قد تودي بها وباستقرارها.

الكلمات المفتاحية: الجرائم، الأمن، سبراني.

(1) سورة النحل (18).

Cyber security crimes in the Saudi regime

Muhammad Mishlawi Yahya Al-Raithi

Dr. Abdul Majeed Abdullah Al-Qarni
Assistant Professor at the College of Administrative Sciences
Najran University - Kingdom of Saudi Arabia

Abstract

Praise be to God, and prayers and peace be upon the most honorable creation of God..... and after The Almighty said: (And if you count the blessings of God, you will not number them. Indeed, God is Forgiving, Merciful) God has blessed us with many blessings, including the blessing of communications, information technology, computers and the Internet in various fields of life in our modern era to provide services and exchange information and the tremendous development in the field of communications and information systems and with this progress and the transition of society from the actual physical reality to the cyber reality, we witnessed the emergence of cyber security crimes On the individual and society in an increasing and noticeable way, so the study of cybersecurity has become one of the innovations in the technological and digital development that we are experiencing in the world recently, as the developed world is witnessing a great development that we cannot describe in any way, so these technological studies in the field of digital computing have become the destinations of many Distinguished scholars around the world, but there is another dark side to that digital development that we are witnessing that can make major countries, companies, and commercial and economic institutions threatened with combustion. I would like to have a research project on security crimes in Seeb Rani in the Saudi system.

key words: crimes, Security, Sabrani.

مقدمة الدراسة:

ارتبطت الجريمة بالإنسان منذ بداية عيشه على وجه الأرض، ولا تزال الجريمة ظاهرة، وتُحاول التخفي خلف قناع التطور، لذلك تتبنى الدُّول استراتيجيات مختلفة للتعامل مع الجريمة وفقًا لطبيعتها وحجمها، ومن المؤكد أن أي دولة لا يُمكنها أن تتقدم، أو تتطور مع ارتفاع نسب الجريمة بها، لأن الجريمة تتعارض تمامًا مع التطور، والتنمية، فهي تتسبب في نتائج اجتماعية، واقتصادية سلبية على المجتمع(1).

وبخلاف تصور العديد من الكتاب والباحثين في مجال الجريمة الالكترونية، فإن ظاهرة انتشار التشريعات، والقوانين الوطنية للحد منها أخذت في الازدياد في الكثر من دول العالم، ولعل أبرز العوائق التي تواجه الحد من انتشار هذه الجريمة ضعف التعاون الدولي لمواجهة هذه الجرائم، والاكتفاء بسن قوانين وطنية محلية يقتصر أثرها داخل حدودها(2).

إن الجريمة السيبرانية في تزاد، والمجرمين يجرون عدة هجمات في جميع أنحاء العالم ذو تعليم عالي وخبراء لديهم معرفة عميقة بتكنولوجيا المعلومات، وهناك العديد من الجرائم السيبرانية مثل: قرصنة كلمة المرور نقل الأموال من حساب ضحية إلى حسابات أخرى وغيرها من الجرائم، ولمعالجتها فإن هناك حاجة لتنفيذ بعض القواعد واللوائح التي تحكم القضاء السيبراني(3).

مشكلة الدراسة:

تتمثل مشكلة الدراسة الحالية في الإجابة عن التساؤلات التالية:

1. ما الجانب الموضوعي والإجرائي لهذه الجرائم؟
2. ما خصائص وأنواع جرائم الأمن السيبراني؟
3. ماصور جرائم الأمن السيبراني؟
4. ما عقوبات جرائم الأمن السيبراني؟
5. ما هي طرق معالجة تلك الجرائم والحد منها؟

أهداف الدراسة: هدفت هذه الدراسة إلى:

1. معرفة مفهوم جرائم الأمن السيبراني في النظام السعودي، والجوانب الموضوعية من أركان وعقوبات.
2. توضيح طرق الاستدلال والتحقق والمحاكمة.
3. معرفة صور جرائم الأمن السيبراني، وعقوبات جرائم الأمن السيبراني.

---

(1) (Dashora, 2011, 240).

(2) الشهري، حسن بن أحمد، نحو قانون دولي موحد لمكافحة الجرائم المعلوماتية، مجلة دراسات وأبحاث جامعة الجلفة، ع1، 2009، ص 514.

(3) مانيطه، يوسف إسماعيل، نظرة عامة عن الجريمة الالكترونية في القضاء السيبراني، المجلة الليبية العالمية، جامعة بنغازي ــ كلية التربية بالمرج، ع32، 2017، ص 3 . 4.

أهمية الدراسة:

تأتي أهمية هذه الدراسة من أهمية موضوعها فهي تقدم جانب نظري عن متغيرات الدراسة، والعلاقة بينها قد تفيد المكتبة على المستوى المحلي والعربي، وتوجه انظار المسؤولين إلى أعمال جرائم الأمن السيبراني، وكيفية الحد منها، وخصوصًا مع هذا الانفتاح العالمي في شبكة المعلومات، وأيضًا قد تفيد باحثين آخرين للفائدة منها.

منهج الدراسة: استخدمت هذه الدراسة المنهج الاستنباطي (التحليلي)، والمنهج الوصفي لبيان مفهوم جرائم الأمن السيبراني وخصائصها، وتناول الجانب الموضعي والإجرائي، والرجوع إلى الأنظمة والقوانين حسب ما يقتضيه الأمر في معالجة مسائل البحث، ومن ثم تحليلها وشرحها، ولم أغفل الرجوع للتطبيقات العلمية.

الإطار النظري للدراسة:

معنى الجريمة السيبرانية في اللغة والاصطلاح:

الجريمة أصلها في اللغة من جرم والمصدر جُرم والفاعل للجريمة يقال له مُجرم، وتدل على المعصية والإثم والذنب. وفي لسان العرب: "الجرمةُ ما جُرِمَ وصُرم من البشر، يُقال: تجَرم ذلك القرن أي انقضى وانصرم، وأصله من الجرم القطع، والجرم: التعدي، والجرم: الذنب... وفي الحديث: "أعظمُ المسلمين في المسلمين جُرمًا من سأل عن شيء لم يُحرم عليه فحُرم من أجل مسألته"[1].

والجرم: الذنب، وقوله تعالى: (حَتَّى يَلِجَ الْجَمَلُ فِي سَمِّ الْخِيَاطِ وَكَذَلِكَ نَجْزِي الْمُجْرِمِينَ)[2].... المجرمون هنا الكافرون، لأن الذي ذكر من قصتهم التكذيب بآيات الله والاستكبار عنها"[3].

وفي المصباح المنير: "جَرَمَ جَرمًا من باب ضرب: أذنب واكتسب الإثم، وبالمصدر سُمي الرجلُ ــ ومنه بنو جَرْم، والاسم منه جُرْمٌ بالضم، والجريمة مثله، وأجرم إجرامًا كذلك، وجرمت النخل: قطعته، والجِرم بالكسر: الجسد والجمع: أجرامٌ، مثل حِمْل وأحمال، والجِرمُ أيضًا: اللون فيجوز أن يُقال نجاسٌ لا جِرْمَ لها....، وقولهم لا جَرَمَ.... هي في الأصل بمعنى لابُدَّ، ولا محالة، ثم كُثرن فحُولت إلى معنى القسم جَرَمَ.... وصارت بمعنى: حقًا ولهذا يُجاب باللام نحوُ: لا جَرَمَ لأفعلنَّ"[4].

إن الجريمة هي فعل ما نهى الله عنه، وعصان ما أمر الله به، أو بعبارة أعمّ، هي عصيان ما أمر الله به، وبالتالي فتعريف الجريمة يكون مرادفًا لتعريف الفقهاء لها بأنها إتيان فعل محرم معاقب على فعله، أو ترك فعل مأمور به معاقب على تركه، وذلك لأن الله تعالى قرر عقابًا لكل من يُخالف أوامره ونواهيه، وهو تعريف عام وليس بخاص، وبذلك تكون الجريمة والإثم والخطيئة بمعنى واحد، ولكن لأن الفقهاء ينظرون إلى المعاصي من ناحية سلطان القضاء

(1) البخاري كتاب الاعتصام رقم2789، مسلم كتاب الفضائل من حديث سعد بن أبي وقاص رضي الله عنه رقم 611.

(2) سورة الأعراف الآية (40).

(3) لسان العرب بتصرف، ابن منظور، جرم.

(4) المصباح المنير، الفيومي، جرم.

عليها، وما قرره الشارع من عقوبات دنيوية يخصصون اسم الجرائم بالمعاصي التي لها عقوبة ينفذها القضاء، وفي تعريف الجريمة بالمعنى الخاص، وهو الأمر المحظور الذي يكون فيه عقاب يقرره القضاء، وتكون الجريمة غير متلاقية مع معنى الشر الذي يقرره علماء الأخلاق أما تعريفها بالمعنى العام فإنه يتلاقى مع تعريف علماء الأخلاق للشر[1].

أما تعريف الجريمة في القانون منها:

1. أنها هي: "الفعل أو الترك الذي نص القانون على عقوبة مقررة له، فإنه بمقتضى ذلك القانون لا يعتبر الفعل جريمة إلا إذا كان ثمة نص على العقاب، ولا عقاب من غير نص".
2. وعرفت بأنها: "الإقدام على عمل يجرّمه القانون، أو الامتناع عن عمل يقضي به القانون مع كونه معاقبًا عليه"[2].
3. وعرفت بأنها: "كلُّ سلوك إنساني غير مشروع، إيجابًا كان أو سلبيًا عمديًا كان أم غير عمديٍ يرتب له القانون جزاءً جنائيًا "[3].

والجريمة السبرانية تُعد من الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطورها فكان بداية من مصطلح إساءة استخدام الكمبيوتر، مرورًا باصطلاح احتيال الكمبيوتر، والجريمة المعلوماتية، فاصطلاحات جرائم الكمبيوتر، والجريمة المرتبطة بالكمبيوتر، وجرائم التقنية العالية إلى جرائم الكاهرز، فجرائم الإنترنت إلى آخر المصطلحات الجرائم السيبرانية[4].

ولهذا فإننا نجد في كل مرة مع ظهور مصطلح جديد لجرائم الإنترنت يظهر لنا تعريفًا جديدًا ففقهاء القانون لم يستقروا على تعريف واحد، فنحن لا نستنكر ذاك أبدًا لأنه من الطبيعي جدًا أن يكون هاذ الاختلاف وهذا التنوع في المفاهيم والآراء، وذلك يرجع لحداثة جرائم الأمن السيبراني والاختلافات الثقافات والقوانين بين الدول، وأيضًا خشية في أن يحصروا المصطلح في نطاق ضيق أو مُحدد.

فقد عُرفت الجريمة السيبرانية عدة تعريفات منها:

الجريمة السيبرانية: كل عمل أو نشاط يحدث أضرارًا بمكونات الحاسب المادية المعنوية وشبكات الاتصال الخاصة به. أو هي كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع للتقنية المعلوماتية ويهدف إلى الاعتداء على الوال المادية أو المعنوية.

ويمكن القول أنها تلك الجرمة التي يتم ارتكابها عن طريق الحاسوب، سواءً أتم ذلك من خلال نظام أو شبكة، وتشكل الجريمة السيبرانية جميع الجرائم التي ترتكب في القضاء السيبراني[5].

---

(1) الجريمة والعقوبة في الفقه الإسلامي "الجريمة"، محمد أبو زهرة، دار الفكر العربي، 22.19.

(2) التشريع الجنائي الإسلامي مقارنًا بالقانون الوضعي، عبد القادر عودة، مؤسسة الرسالة، (1/67 . 68).

(3) الجريمة أحكامها العامة في الاتجاهات المعاصرة والفقه الإسلامي، عبد الفتاح خضر، ص 12.

(4) دكتور عبد العزيز بن غرام الله آل جار الله، جرائم الإنترنت وعقوباتها وفق نظام مكافحة الجرائم المعلوماتية السعودي (دراسة مقارنة) (ويليه آثار العولمة على مستخدمي الإنترنت، دار الكتاب الجامعي، الرياض، الطبعة الأولى 2017م، ص 70.

(5) الشهري، حسن بن أحمد، نحو قانون دولي موحد لمكافحة الجرائم المعلوماتية، مجلة دراسات وأبحاث جامعة الجلفة، ع1، 2009، ص 516.

وتعرف أيضًا بأنها كل فعل أو نشاط يتم بطريقة غير مشروعة من خلال الحاسوب أو الشبكات الحاسوبية، وتجدر الإشارة إلى أن منفذي الجريم الالكترونية تختلف أعمارهم مع اختلاف دوافعهم[1].

وهناك عدة مسميات للجريمة السيبرانية منها: الاحتيال المعلوماتي، الغش المعلوماتي، التعسف في استعمال الحاسب الآلي، الجرائم المرتبطة بالحاسب الآلي، جرائم الحاسب الآلي، جرائم المعلوماتية، احتيال الكمبيوتر، جرائم التقنية العالية، جرائم الهاكرز، الاختراقات، جرائم الإنترنت، جرائم الحاسب والإنترنت، الجرائم الاقتصادية المرتبطة بالكمبيوتر، جرائم أصحاب الياقات البيضاء[2].

إن تعريفات الهجمات السيبرانية القائمة، والمفاهيم ذات الصلة واسعة جدًا، إلا إن هناك اتجاهين ورئيسيين مختلفين في تعريف هذا النمط من الهجمات، وهما الاتجاه الضيق الذي يؤكد على موضوع الهجوم، والاتجاه الواسع الذي يتناول التهديدات المترتبة على الجرائم السيبرانية.

يعتبر مصطلح الأمن السيبراني مفهومًا جديدًا نوعًا، ما فقد ارتبط ظهوره بالثورة التكنولوجية التي عرفها البشر، ومع تزايد اعتماد الإنسان على وسائل التكنولوجيا، والاتصال وما واكبها من تحديات كبرى، ولعل أهمها مجابهة ما يطلق عليه اسم الفضاء السيبراني الذي يتم اعتباره على أنه مجال افتراضي لنظم الكمبيوتر وشبكات الإنترنت، وقد ظهر كمصطلح في ثمانيات القرن الماضي في إحدى روايات الخيال العلمي للكاتب الأمريكي ويليام جيبسون، والذي تم وصفه على أنه العصر الرقمي المتصف بالتطورات التكنولوجية وانعكاساتها على المجتمع الدولي، وتم التنبؤ على أنه مستقبل الحضارة الإنسانية وأساس التواصل، وهو ما حصل فعليًا من خلال تطورات الوقت الحالي.

وقد اختلفت التعريفات حول هذا المصطلح باختلاف طبيعة الدول، وكذا الاستراتيجية التي تعتمدها ومدى ارتباطها بعالم الرقمي، والتي ترتبط بمدى تفعيل الحكومة للنظم الالكترونية، وتوظيف شبكات المعلومات، ووسائل الاتصال السلكية واللاسلكية، والطبع توصيل الخدمات للمواطنين في مجالها المدني من جهة، واستخدم هذه التكنولوجيا في المجالات العسكرية، واستراتيجيات الدفاع من جهة أخرى.

يمثل الأمن السبراني تحديًا يتطور على الدوام، ومن اللازم متابعته باستمرار، نظرًا للتغير الدائم في طبيعة تكنولوجيا المعلومات والاتصالات، وقبل التطرق إلى تعريف الأمن السيبراني، لابد من تعريف أمن المعلومات: وهو السيطرة، والتحكم في البيانات، ونقلها، ونشرها، وحمايتها من المخاطر الداخلية والخارجية التي تهددها، ومن أنشطة الاعتداء عليها[3]، ويمكن تعريف الأمن السيبراني (Cyber security) بأنه الذي يُعنى بالحفاظ على أمن المعلومات وشبكات، وأجهزة الحاسب الآلي، ويُعد هذا المفهوم أحد أهم مفاهيم الحقبة القادمة[4].

(1) ملاك، قارة، الجريمة المعلوماتية في القطاع البنكي وأساليب مكافحتها إشارة لحالة الجزائر، مجلة جامعة الأمير عبد القادر للعلوم الإسلامية، جامعة الأمير عبدالقادر للعلوم الإسلامية، ع39، 2016، ص 414.

(2) الشهري، حسن بن أحمد، ص 516.

(3) الحانوتي، 2014، ص 190.

(4) مختار، 2015، ص 5.

كما يُشير الأمن السيبراني إلى الطرق التي تستهدف كشف، ومنع الهجمات على أي نظام حاسوبي، والمعلومات المتضمنة فيه، أو الوصول غير المصرح له، ويستهدف الأمن السيبراني، حماية البيانات، أو أي شكل من الأصول الرقمية المخزنة في حاسوب لأي جهة، أو في أي جهاز يحتوي على ذاكرة رقمية[1].

وهناك عدة تعريفات للأمن السيبراني من أهما ما يلي:

الأمن السيبراني هو: عالم افتراضي يتشابك مع العالم المادي يتأثر بشكل مترابط، وتقوم هذه العلاقة على نظرة تكاملية تحمل بين طياتها مزاي ومخاطر متعددة[2].

وهو مجموعة الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها، وبما يضمن تنفيذ التدابير والإجراءات المضادة للحماية[3].

أو هو عبارة عن مجموعة من الوسائل التنظيمية، والتقنية، والإدارية، والتي تستخدم في منع الاستخدامات غير المصرح به، وتوجه تلم الوسائل، والتقنيات للقضاء على سوء الاستغلال، والمحافظة على المعلومة الالكترونية، وتحصين نظم الاتصالات والمعلومات، وكل ذلك بهدف ضمان استمرارية عمل نظم المعلومات من خلال توفير الحماية لها والبيئة الملائمة، لتتمكن من القيام بدورها في الحفاظ على الأمن الرقمي والمعلوماتي[4].

استخدم مصطلح: الأمن السيبراني على المدى الطويل في إشارة إلى نوعين من الأنشطة فيما يتعلق بالفضاء السيبراني الأول هي الأنشطة الهجومية، والتي تشمل الحرب المتعلقة بالمعلومات، والجريمة السيبرانية، والإرهاب السيبراني، وأي الأنشطة التي تحتاج إلى مواجهة ومكافحة، ويتعلق السياق الثاني بالأنشطة الدفاعية المتصل بالمعلومات، وحماية المعلومات، والبنية التحتية الحيوية للمعلومات، ولابد من إضافة أن مفهوم البنية التحتية الحيوية يشير في جملة أمور إلى قطاعات المعلومات عن بعد والخدمات المالية والطاقة والنقل، أي المجالات التي تحدد الأداء السليم للبلد بأسره، وتدميرها أو عدم تنظيمها سوف يسبب ضررًا كبيرًا، وفي ضوء ذلك يُدرك بأن مصطلح "الأمن السيبراني يغطي الأنشطة التي تتجاوز نطاق الصيانة والحماية"[5].

---

(1) علي، 2017، ص 23 . 24.

(2) مانيطة، يوسف إسماعيل يوسف، نظرة عامة عن الجريمة الالكترونية في الفضاء السيبراني، المجلة الليبية العالمية، جامعة بنغازي، كلية التربية بالمرج، ع32، 2017، ص 8.

(3) سامي، بونيف محمد، دور الاستراتيجيات الاستباقية في مواجهة الهجمات السيبرانية: الردع السيبراني أنموذج، المجلة الجزائرية للحقوق والعلوم السياسية المركز الجامعي أحمد بن يحي الونشريس تيسمسيلت، معهد العلوم القانونية والإدارية، مج 4، ع7، 2019، ص 123 .124.

(4) هيئة التحرير: الأمن السيبراني: درع المملكة الواقي لحماية مصالحها الحيوية وبنيتها التحية الرقمية، مجلة الدبلوماسي، وزارة الخارجية . معهد سعود الفيصل للدراسات الدبلوماسية، ع 90 2018، ص 9.

(5) هيئة التحرير: الأمن السيبراني: درع المملكة الواقي لحماية مصالحها الحيوية وبنيتها التحية الرقمية، مجلة الدبلوماسي، وزارة الخارجية . معهد سعود الفيصل للدراسات الدبلوماسية، ع 90 2018، ص 9.

وبناءً على تلك التعريفات تظهر أهمية الأمن السيبراني، وتكمن أهميته في المحافظة على أمن الدول وسلامتها.

ولقد بات الأمن السيبراني مكونًا أساسيًا من مكونات أي تحول رقمي، حيث إن حماية البيانات والبنية التحتية ستكون مصدر قلق كبير للحكومة، والعامة، والقطاع الخاص، بسبب نمو الهجمات السيبرانية في العقد السابق، مما جعل من الضروري التعامل مع مثل هذه الهجمات، ومعالجتها بشكل مبتكر.

إن من الأمور التي أصبحت معلومة لدى القاصي والداني أن الأمن السيبراني أصبح يشكل جزءًا أساسيًا من أي سياسة أمنية وطنية، ذلك أن صُناع القرار في الولايات المتحدة، والاتحاد الأوروبي، وروسيا، والصين، والهند، وغيرها من الدول أصبحوا يصنفون مسائل الدفاع السيبراني/ الأمن السيبراني كأولوية في سياساتهم الدفاعية الوطنية، لاسيما بعد ما أصبحت الحروب السيبرانية أخطر ما يُهدد سيادة الدول والأفراد، حيث تستطيع أي دولة أو حتى محترف، أو محتال إلكتروني "قراصنة" في العالم أن تستغل ثغرات ونقاط ضعف[1].

ومن المعلوم أنه إبان الحرب الباردة لم تكن طموحات الدول إلا انعكاسًا لرغبة محلة في الأمن الذاتي بأقل الخسائر، فلما كانت سياسة البروباغندا العسكرية أحد وسائل المنع كان السباق نحو التسلح هدفًا، ففكرة التهديد والوعيد لم تكن يومًا وليدة الصدف، ولا عقيدة ذاتية بل أسلوب بشري ينعكس على مستوى الدول، وما عمليات الردع إلا أحد أنواع هذه الأساليب، وبانتقال الوسائل تنتقل الأهداف وجوبًا وتلازمًا، فاليوم الحديث لم يعد عن ما تمتلكه الدول من عدة وعتاد في حرب مماثلة ليتعدى لما بعده، فما القول بأن كل ما تستخدم الدولة في حماية أمنها قد يشكل خطرًا عليها إلا إشارة واضحة لجدلية الأمن والخطر، فمواطن الدولة ذاتها قد يكون تهديدًا لها[2].

وبالنظر لما يتعلق بضعف نظم الملاحقة الإجرائية التي تبدو قاصرة على استيعاب هذه الظاهرة الإجرامية الجديدة سواء على صعيد الملاحقة الجنائية في إطار القوانين الوطنية أم على صعيد الملاحقة الجنائية الدولية. إن كل ذلك يفرض على الدول ضرورة تضافر الجهود من أجل وضع آلية يتم من خلالها التصدي للجرائم التي يتم بثها عبر شبكة المعلومات الدولية، ويتحقق ذلك من خلال تطوير البنية التشريعية الجنائية في تلك الدول، والتركيز على البُعد القانوني الذي يُعد بالغ الأهمية في هذا المجال[3].

ومن أجل زيادة التكاتف بين الدول في تفعيل مجال الأمن السيبراني تأسس الاتحاد الدولي للاتصالات، وهو أحد أهم المؤسسات الدولية التي يقع على عاتقها بناء الثقة والأمن في استخدام المعلومات وتكنولوجيا الاتصالات، وخصوصًا بعد القمة العالمية لمجتمع المعلومات، ومؤتمر المندوبين المفوضين للاتحاد في عام 2010[4].

---

(1) هيئة التحرير: الأمن السيبراني، ص9.

(2) سامي، يونيف محمد، دور الاستراتيجيات الاستباقية في مواجهة الهجمات السيبرانية: الردع السيبراني أنموذج، المجلة الجزائرية للحقوق والعلوم السياسية، المركز الجامعي أحمد بن يحيى الونشريس تيسمسيلت، معهد العلوم القانونية والإدارية، مج4/ ع7، 2019، ص 122.

(3) المقصودي، محمد بن أحمد بن علي، الأمن السيبراني والجهود الدولية لمكافحة الجرائم عابرة القارات الأمن والحياة، جامعة، نايف العربية للعلوم الأمنية، مج 37، ع427، 2017، ص 102 . 106.

(4) مانيطة، إسماعيل يوسف، نظرة عامة عن الجريمة الالكترونية في الفضاء السيبراني المجلة الليبية العالمية، جامعة بنغازي ـــ كلية التربية بالمرج، ع32، 2017، ص 8

ومنذ ظهور الإنترنت، وبروز التكنولوجيا الالكترونية، والمعلوماتية في فجر الألفية الثالثة، أصبحت المجتمعات تسير بسرعة كبيرة نحو التغير في كافة المجالات، حيث أدت الأهمية المتزايدة للمعرفة إلى جانب العولمة والآثار المترتبة على التطور التكنولوجي في عصر الثورة الصناعية الرابعة إلى إيجاد عالم مختلف تمامًا[1].

وتعتبر الثورة الرقمية والتكنولوجية التي اجتاحت العالم خلال نهاية القرن الماضي وبداية القرن الحالي نتاجًا مباشرًا لجهود البشر على وجه الأرض، ممن كانوا يطمحون إلى الوصول إلى زمن تكون فيه الاتصالات متوفرة، وشاملة، وتكون فيه المعلومات متاحة للجميع في وقت قياسي وسريع[2].

إن ما سبق يحتم علينا أن نطور الأمن السيبراني ونحدث التكنولوجيا الخاصة به لتواكب التطور الكبير في كافة المجالات. لذلك يستلزم الأمر تطوير الأمن السيبراني للأسباب التالية:

1- يعتمد الوجود الاقتصادي الرقمي للبلد على الأداء الفعال للبنية التحتية الرقمية، وفي الفضاء السيبراني، فإن البلد ليس معزولًا، ولكنه مترابط مع بلدان أخرى، وجهات فاعلة في الفضاء السيبراني من خلال شبكات مترابطة للبنى التحتية للمعلومات، وبالتالي فإن البلد معرض لمخاطر يمكن التنبؤ بها، وأخرى لا يمكن التنبؤ بها.

2- كما أن لدينا جهات فاعلة ذات نويا مشروعة، فهناك أيضًا جهات فاعلة أخرى ذات نوايا غير مشروعة وخبيثة، داخل الشبكة العالمية للشبكات، توجد عيوب هيكلية حرجة يمكن استغلالها لأغراض خبيثة، ونوايا جنائية ضد البلد من أجل المساس بسرية نظم المعلومات الوطنية والبنية التحتية الحيوية للمعلومات، وسلامتها، وتوافرها، وإمكانية الوصول إليها، ومما ينعكس سلبًا على المواطن وبالتالي على الأمن الوطني.

3- توجد مواطن ضعف في الفضاء السيبراني يمكن استخدماها لاستغلال المصالح الاقتصادية الوطنية، وتشكل تهديدًا للأمن القومي على سبيل المثال:

- العمليات التخريبية.
- تزايد صناعة الجريمة السيبرانية.
- الممارسات الاحتيالية.
- وقوع الاستغلال عبر الإنترنت.
- إساءة استخدام وسال الإعلام ومواقع التواصل الاجتماعي، لشن حملات خبيثة ضد الدولة.
- الصراع والعنف المستمر من خلال الإنترنت.
- التخريب الاقتصادي من خلال حرمان المواطنين من الوصول إلى الخدمات الالكترونية الحكومية وغير الحكومية.

---

(1) استشراف مستقبل المعرفة: مؤسسة محمد بن راشد آل مكتوم للمعرفة والمكتب الإقليمي للدول العربية برنامج الأمم المتحدة الإنمائي، دار الغرير للطباعة والنشر، الإمارات، ص 3.

(2) حاج بشير، جيدور، أثر الثورة الرقمية والاستخدام المكثف لشبكات التواصل الاجتماعي في رسم الصورة الجديدة لمفهوم المواطنة: من المواطن العادي إلى المواطن الرقمي، دفاتر السياسة والقانون، ع15، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية، 2016، ص 733.

- التجسس الالكتروني والمنسق.
- التدخل الخبيث في أنظمة الكمبيوتر والأجهزة الرقمية الأخرى.
- القرصنة الالكترونية.
- سرقة الأصول الفكرية.
- الإرهاب الالكتروني.
- الجرائم المالية عبر الإنترنت.

كل هذه الأمور لا تنسجم مع سياسة الرفاهية لأي دولة، ولها الأثر الاقتصادي الذي يكون كفيل بتدمير أي دولة.

4- توفير الأمن للبنية التحتية الحيوية للمعلومات وغيرها من العناصر الحرجة في نظام المعلومات في ظل الوضع الراهن هو تحد وطني ضخم، ويحتاج الأمن الوطني إلى إطار متماسك للأمن السيبراني لتوفير نهج شامل إزاء المشهد الأمني الحالي والمستقبلي، لأن أمن الدول والتضاريس، والاقتصاد يسير بخطى سريعة، ويتجهان نحو تضاريس متحركة ومتنقلة رقميًا، فالجهات الفاعلة الحكومية وغير الحكومية المتورطة في الجرائم السيبرانية مجهزة تجهيزًا كافيًا بأدوات إلكترونية متطورة، تتسبب في أضرار ذات بُعد لم يسبق له مثيل، ومن شأن إدراج الأمن السيبراني في مجال الفضاء الالكتروني أن يُساعد البلد على الاستعداد، والاستجابة لهذه التهديدات الأمنية، والمساعدة على معالجة ضعف البلد في المجال الرقمي، فضلًا عن تعزيز قدرتنا على توفير تدابير مضادة بالاشتراك مع جهات فاعلة شرعية وغير حكومية أخرى، وهذا هو الأساس المنطقي الاستراتيجي لوضع السياسة الوطنية للأمن السيبراني في أي دولة من الدول المعنية بمسائل الأمن السيبراني خاصة بلادنا العربية[1].

5- التقدم في الأمن السيبراني ضروي لتنفيذ التكنولوجيات الرئيسية الأخرى.

تزداد أهمية الأمن السيبراني بسبب الاعتماد المتزايد لأنظمة الكمبيوتر على الإنترنت والشبكات اللاسلكية (واي فاي، بلوتوث، الحوسبة السحابية) لتخزين المعلومات وتبادلها وظهور إنترنت الأشياء، فقد أثبتت التجارب الحديثة أن معظم التكنولوجيات عرضة للاختراق بما في ذلك السيارات وأنظمة الإنذار والأجهزة الطبية القابلة للزرع والبنية التحتية العامة لأنظمة الطيران، والتطبيقات المصرفية الهاتفية، وتكنولوجيا المدن الذكية، وعمومًا يسمح استخدام أدوات الحماية المناسبة بتسريع تقديم الخدمات والتنفيذ السلس للعمليات.

6- الأمن السيبراني يقدم حلًا لأبرز التحديات الملحة التي تواجه المجتمعات، حيث يلعب الأمن السيبراني دورًا محوريًا في معالجة التحديات المستقبلية، نظرًا لاستخدامه كتكنولوجيا لإدارة الشبكات، فتقديم خدمات تكنولوجيا المعلومات والاتصالات بشكل أكثر أمانًا وسلاسة من خلال نظام أمن سيبراني فعال يُساعد في تحقيق عدد من أهداف التنمية المستدامة التي وضعتها الأمم المتحدة مثل: (تحسين إدارة استخدام المعدات وصيانتها، وزيادة الإنتاج الزراعي، وتوسيع نطاق الوصول إلى المعلومات المتعلقة بالتفاعل الاقتصادي بين المؤسسات الخاصة والعامة).

(1) استراتيجية الأمن السيبراني العراقي: مستشارية الأمن الوطني، أمانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات، ص 3.

7- إتاحة تكنولوجيا المعلومات والاتصالات للجميع بصورة آمنة وشفافة. إن انتشار تكنولوجيا المعلومات، والاتصالات، والترابط العالمي يوفر إمكانات كبيرة، لتسريع التقدم البشري، وردم الفجوة الرقمية، وتطوير مجتمعات المعرفة، مثله في ذلك مثل الابتكار العلمي والتكنولوجي في مجالات متنوعة مثل: الطب والطاقة، ومع ذلك ينبغي أن يكون بناء الثقة وتوفير الأمان في استخدام تكنولوجيات المعلومات والاتصالات من أجل التنمية المستدامة من الأولويات خاصة في ضوء التحديات المتنامية، بما في ذلك إساءة استخدام هذه التكنولوجيا للأنشطة المؤذية بدءًا بالتحرش وصولًا إلى الجريمة والإرهاب[1].

لذلك تسعى السياسات والاستراتيجيات الموضوعة للأمن السيبراني عمومًا إلى تحقيق مجموعة أهداف: **الهدف الأول**: هو أن تكفل حماية نظم المعلومات التي تقوم عليها الخدمات المهمة، ببساطة هذا الهدف يدعو إلى أساليب للحفاظ على استدامة ومرونة الخدمات الحيوية، وحماية البنية التحتية للمعلومات الحيوية.

الهدف الثاني: هو تعزيز مكافحة الجريمة السيبرانية، وزيادة الوعي العام، وتعزيز التعاون الدولي لمكافحة الجريمة السيبرانية. **والهدف الثالث**: هو تطوير قدرات الدفاع السيبراني الوطنية، مع التركيز بشكل خاص على مزامنة الاستعدادات، والإجراءات العسكرية الدولية، **والهدف الرابع**: هو إدارة تهديدات الأمن السيبراني المتطورة، ولتحقيق هذا الهدف تتحدد تدابير مثل تدريب وإعداد جيل مستقبلي من المهنيين في مجال الأمن السيبراني، وتطوير التعاقد الأمني الذكي على الإنترنت، **والهدف الخامس والأخير**: هو تطوير أنشطة مشتركة عبر قطاعات الدولة، وتشمل الإطارات القانونية، وسياسات الأمن السيبراني الدولية، والتعاون الدولي.

ويُعد أمن المعلومات الالكترونية عبر شبكة الإنترنت هو الهاجس الأكبر لمعظم منظمات الأعمال في العالم، لاسيما ونحن نعيش في عصر الحوسبة والمعلوماتية، والذي بات فيه التعامل التجاري مستندًا إلى تقنيات الحوسبة والاتصالات الحديثة، ومن الطبيعي أن يتزايد قلق منظمات الأعمال في ظل تزايد المخاطر الأمنية على أنظمة معلوماتها الالكترونية مثل: اختراق شبكات الإنترنت، ونشر برامج الفيروسات المختلفة من قبل جهات محترفة، فضلًا عن هواة العبث والتجسس، والمعروفون بالهاكرز، وما قد ينتج عن ذلك من خسائر مادية ضخمة، وإرباكات مختلفة في التعامل عبر شبكة الإنترنت، والأمر الذي يزيد المسألة تعقيدًا هو أن بعض الاختراقات الأمنية يرتكبها بعض الموظفين أنفسهم من خلال إساءة استخدام البريد الالكتروني والإنترنت لأغراضهم الشخصية، أو لصالح جهات خارجية[2].

دوافع اهتمام الدول بأبعاد الأمن السيبراني:

لقد أثارت تحديات الأمن السيبراني العديد من المخاوف المرتبطة بالأمن القومي في العديد من دول العالم، وهناك توجه سائد لدى العديد من الحكومات نحو تطوير وتطبيق سياسات جديدة للأمن السيبراني، ومراجعة

(1) استشراف مستقبل المعرفة: مؤسسة محمد بن راشد آل مكتوم للمعرفة والمكتب الإقليمي للدول العربية برنامج الأمم المتحدة الإنمائي، دار الغرير للطباعة والنشر، الإمارات، ص 12.

(2) الصمادي، 2005، ص 467.

السياسات الحالية (إن وجدت)، وبالنسبة لعدد من الدول، فإن سياسات الأمن السيبراني تتضمن استراتيجيات، ومعايير متعلقة بالأمن والعمليات في الفضاء السيبراني، ومجموعة من السياسات، والأنشطة المرتبطة بتقليل المخاطر، وردع الهجمات السيبرانية، والمشاركة الدولية، والاستجابة للحوادث، وتطبق هذه السياسات، والأنشطة في العديد من المجالات مثل: تنظيم العمليات عبر شبكات المعلومات، وتطبيق القانون، والدبلوامسية، والشؤون العسكرية، والمهمات الاستخباراتية، مما يُشير إلى الأهمية الكبرى لإجراءات الأمن السيبراني في تحقيق الأمن والاستقرار في البنى التحتية العالمية للمعلومات والاتصالات.

فإن ظاهرة جرائم الكمبيوتر والإنترنت، أو الجريمة الالكترونية ظاهرة إجرامية مستجدة نسبيًا تقرع في جنباتها أجراس الخطر، لتنبه مجتمعات العصر الراهن لهول الخسائر الناجمة عنها، باعتبارها تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة، فهي تطال الحق في المعلومات، وتمس الحياة الخاصة للأفراد، وتهدد والأمن القومي، وتشيع فقدان الثقة بالتقنية، لذا فإن إدراك ماهية جرائم الكمبيوتر والطبيعة الموضوعية لهذه الجرائم واستظهار خصائصها وحجم الخسائر عنها، وسمات مرتكبيها يتخذ أهمية استثنائية لسلامة التعامل مع هذه الظاهرة، ونطاق مخاطرها الاقتصادية، والأمنية، الاجتماعية، والثقافية[1].

فقد اعتمد الأفراد والمؤسسات التجارية على نظم المعلومات، لإدارة اعمالهم عبر العصور ففي القرن الثامن عشر 1800م، حيث كان الاقتصاد الزراعي هو السائد إذ يتم الاعتماد على نظم معلومات مثل: نظام الطقس ونظام التوقيت الزراعي، وخلافه لإدارة الأعمال الزراعية، وعند الانتقال إلى العصر الصناعي ظل الاعتماد على نظم المعلومات مستمرًا فتم الاعتماد على نظم أخرى مثل: نظم المشروع التي ترتكز على العمل، ونظم إنتاج المواد الخام، وحاليًا ونحن ندخل إلى عصر التكنولوجيا فإننا نعتمد على نحو متزايد على أنظمة تكنولوجيا المعلومات والاتصالات بشكل كبير جدًا[2]. وهناك العديد من الابعاد التي يمكن نعتمد عليها في الامن السيبراني منها:

- **البُعد العسكري:**

وهي عملية الحماية الأمنية للمعلومات من خلال بلورة أنظمة للدفاع السيبراني، وغالبًا ما تكون هذه الأنظمة، والاستراتيجيات ذات مستوى عالي من السرية.

وقد أصبح الفضاء السيبراني أحد النطاقات الرئيسة للعمليات العسكرية، مثل: النطاق البري، والبحري، والجوي، والفضائي، وتقوم العديد من الدول بزيادة نفقاتها على بناء وتعزيز إمكاناتها السيبرانية، وقد أصبح للفضاء السيبراني مكان هام في استراتيجيات الأمن القومي والاستراتيجيات العسكرية في العالم اليوم، ويرى العديد من الباحثين، لأن هذه التحولات العديدة تنذر ببدء ما يُطلق عليه "سباق التسلح الرقمي" والذي لا يزال حديث العهد، مما يجعل من الصعب تحديد قواعد المشاركة فيه، وقبل سنوات قليلة فقط، كانت فكرة استخدام الدول للوحدات الرقمية لإحداث الدمار في دول أخرى ضربًا من الخيال العلمي، أما اليوم، فقد أصبح ذلك أمرًا واقعًا يجب التعامل معه.

(1) البشير، 2012، ص 8.

(2) عبد العزيز، 2010، ص 427.

فلقد حدثت تغيرات جذرية في التصورات العامة لدى القادة العسكريين في مختلف دول العالم حول الأولويات القصوى للأمن القومي خاصة مع نشوء وتكون نوع جديد من التهديدات، وهي المخاطر الأمنية في القضاء السيبراني فمع تزايد الاعتماد على تكنولوجيا المعلومات والاتصالات في الحياة المعاصرة، تزايدت الثغرات الأمنية الموجودة في شبكات الاتصال، واحتمالية تعرض البنى التحتية الحيوية في مختلف القطاعات للهجمات الخبيث، وقد أجبرت هذه التغيرات الحكومات على إعادة تشكيل تصوراتها حول المخاطر الأمنية والآليات المتبعة للتصدي لها، وفي السنوات الأخيرة، زاد توجه المؤسسات العسكرية في دول العالم المختلفة نحو وضع استراتيجيات للتصدي للمخاطر الأمنية في الفضاء السيبراني، والتهديدات الأمنية السيبرانية لا تقتصر على مجرد الهجمات التي تستهدف استغلال الأفراد، أو إحداث الاضطرابات في المؤسسات، حيث إن الفرص والإمكانات التي يوفرها الفضاء السيبراني يتم استغلالها بشكل كبير من قبل العديد من الجهات، لتحقيق اهداف أكثر ضررًا، مثل نشر الفكر الهدام، وتجنيد العناصر، وممارسة العديد من أنشطة القرصنة المتفرقة، وسرقة الأموال لتمويل أنشطة معادية للدول المستهدفة والحصول على معلومات حساسة تمس أمنها القومي[1].

– البعد السياسي:

هو امتلاك الدولة الحق في حماية نظامها السياسي، ومصالحها ومصالح مواطنيها، وذلك من خلال اعتماد استراتيجيات داخلية متمثلة في إجراءات محلية، أو خارجية، من خلال العمل على التوافق الدولي لحماية الأمن السيبراني، وتضطلع القيادة السياسية العليا في أي دولة بتنظيم مؤسساتها المعلوماتية والأمنية، وتقويتها، لكي تحمي مصالحها الوطنية والقومية، كما تخطط لإدارة العمل السياسي، والاقتصادي، والعسكري عند الاستعداد لحرب محتملة، وتوجيه مؤسساتها للحصول على المعلومات عن قدرات الدول التي قد تكون مؤثرة، والاهتمام بنوايا العدو الحقيقية والمحتملة، لخدمة الأمن القومي لها، وتساعد تلك المعلومات على تهيئة قيادة الدولة في اتخاذ القرارات المناسبة، لإدارة الأزمة، وحلها، أو خوض الحرب بشكل فعال، أو إحباط الهجمات التي يشنها العدو.

وتعد الدوافع السياسية من أبرز المحاولات الدولية لاختراق شبكات حكومية في مختلف دول العالم، كما أن الأفراد قد يتمكنون من اختراق الأجهزة الأمنية الحكومية، وكذلك أصبحت شبكة الإنترنت مجالًا خصبًا لنشر أفكار العديد من الأفراد والمجموعات، ووسيلة للترويج لخبار وأمور أخرى قد تحمل في ثناياها مساسًا بأمن الدولة، أو بنظام الكم، أو قدحًا في رموز دولية أو سياسية، والإساءة لها بالذم والتشهير[2].

فهناك أمثلة كثيرة تدفع نحو الاهتمام بالبُعد السياسي للأمن السيبراني، كالتسريبات المختلفة للوثائق التي سببت مشكلات في علاقات الدول ببعضها البعض مما حتم على الدول إعادة النظر في سياستها الخارجية في ظل هذه التسريبات[3].

---

(1) العكلة، 2013، ص 363.

(2) البقمي، 2008، ص11.

(3) مختار، 2015، ص 7.

- **البُعد الاجتماعي:**

وتؤدي الجريمة السيبرانية إلى العديد من الآثار السلبية على المجتمع، حيث إنها تعتمد بصورة رئيسية على انتحال هوية الضحية في تعاملاته المالية والاجتماعية، وهذه الآثار لا تقتصر على الأفراد، ولكنها تمتد أيضًا إلى المنظمات والشركات، كما أن الحكومات من الأهداف الجذابة للأعمال الإجرامية السيبرانية، وهذه الجرائم تهدف بالأساس إلى إحداث العديد من الأضرار تجاه المجتمع ككل، وهذه الأضرار تستهدف تعطيل مصالح المواطنين في شبكات المواصلات، والطاقة، والشبكات المصرفية.

حيث إن مجتمع التكنولوجيا والإنترنت شبيه بالمجتمع الإنساني الذي يوجد فيه أطياف مختلفة من الناس أكثرهم الأسوياء، ولكن يوجد منهم ذوي الأخلاق السيئة، وهناك العديد من الأضرار، والآثار التي تسببها تكنولوجيا المعلومات، إن لم يُحسن استخدامها، وخصوصًا للأطفال والمراهقين، ويُمكن إجمال الأضرار والآثار السلبية في تسرب الأفكار الهدامة، والأديان، ووصولها إلى متناول الأبناء الصغار، ودخول بعض الأفراد إلى خصوصيات بعض الجهات الحكومية، أو البنكية، أو الأشخاص، والوصول إلى معلومات سرية قد لا يسمح بالوصول إليها بالطرق الشرعية[1].

والحقيقة أن ضرورة حماية أنظمة الكمبيوتر ليس الغرض منها حماية الجهاز كقيمة اجتماعية مستقلة، وإنما الغرض هو حماية المصالح العامة والمصالح الخاصة التي يحميها المجتمع والتي ترتبط باستعمال الحاسب الآلي، فالمعلومات المبرمجة ملك لصاحبها وبالتالي فإن حمايتها هي حماية للملكية من العبث بها في صورة استيلاء، أو اطلاع، أو إتلاف، وبالتالي فإن حماية نظام الكمبيوتر هي حماية للثقة العامة في المحررات[2].

- **البُعد الإعلامي:**

هناك أهمية كبرى لأخذ الاعتبارات الأمنية بعين الاعتبار عند التعامل مع الأثر الإعلامي للفضاء السيبراني، وذلك نظرًا لقدرة وسائل التواصل الاجتماعي (وهي أهم وسائل الإعلام في الفضاء السيبراني) على تحقيق أهداف مادية، ومعرفية بنجاح كبير، مقارنة بأي وسيلة لإعلامية أخرى، كما أن الفضاء السيبراني يتيح لواضعي المحتويات الإعلامية وتقديمها للجمهور بمختلف الصيغ مثل الكلمات، والصور، والملفات... إلخ.

وذلك بالإضافة إلى استخدام الأنماط التقليدية من الإعلام من خلال هذا الفضاء مثل القنوات التليفزيونية والإذاعية، وذلك مع وجود قدر أقل من الرقابة والتحكم، وبالإضافة إلى ذلك فإن من الجوانب الأخرى ذات الاعتبارات الأمنية المهمة هي قدرة وسائل التواصل الاجتماعي على التأثير على معتقدات وقرارات مستخدميها، وتاريخيًا تعتبر القدرة على التأثير في أذهان الجماهير من أهم العوامل المؤثرة ليس فقط في التأثير على سلوكيات أفراد المجتمع، ولكن أيضًا في التأثير في الرأي العام في أوقات الحروب[3].

---

(1) ابن عسكر، 2012، ص 6 . 7.

(2) غنام، 2010، ص 12.

(3) Crowell,2017. 11.

- **البُعد التعليمي والأكاديمي:**

يُعد البُعد التعليمي من أهم أبعاد الأمن السيبراني، نظرًا لأن التعليم هو الأساس في كل شيء، وهو الذي تنتقل منه الخبرات والمهارات، لتنتشر وتتمركز في المجتمع، لذا يقع على عاتق المؤسسات التعليمية مسؤولية كبيرة بشأن توعية الأفراد بالفضاء السيبراني، والأمن السيبراني، حيث إنه أصبح مصطلحًا كثير التردد، وله الكثير من المنافع، وأيضًا الكثير من المخاطر، فقد أصبحت المدارس تعتمد على الإنترنت بشكل كبير في تنفيذ الكثير من الأعمال. كما يُساعد التخزين الآمن لمعلومات وبيانات المدارس على استعادة قدراتها بسهولة ويُسر، وخاصة بعد الأزمات التي قد تمر بها المؤسسات التعليمية، إذا إن التخزين الآمن للبيانات والمعلومات يتيح لمتخذي القرارات استرجاع البيانات والمعلومات اللازمة لاستعادة النظام، حيث تظل بيانات أعضاء هيئة التدريس والطلاب، والنتائج النهائية للطلاب، وسجلات ميزانية المدرسة، وإمكاناتها من معامل وأجهزة، وتقارير أداء الإداريين والمعلمين، وعقود الشراكة بين المدارس وغيرها من الهيئات، وبروتوكولات التعاون وغيرها من السجلات، محفوظة بمأمن بعيدًا عن أي ضرر قد تكون الأزمة قد تسببت فيه[1].

وقد تكمن أهمية المؤسسات التعليمية في هذا الصدد في أنها تعتبر في طليعة المؤسسات المساهمة في معالجة قضايا الأمن السيبراني في العديد من المجتمعات، فعند النظر إلى الجهود التي تبذلها الدول لتعزيز الأمن في الفضاء السيبراني، فإن العديد من هذه الدول لا تطبق مبادرات أو استراتيجيات وطنية واضحة المعالم، ولكن الجزء الأكبر من هذه الجهود يأتي من جانب المؤسسات التعليمية، وتحديدًا الجامعات، وما يميز جهود المؤسسات التعليمية في هذا الصدد هي أنها لا تهتم فقط برفع مستوى كفاءة طلابها، مثال: (طلاب قسم علوم الحاسب الآلي) في التصدي للمخاطر المهددة للأمن السيبراني، بل إنها تركز أيضًا وبشكل أكبر على الرفع من مستوى الوعي العام لدى المجتمعات حول قضايا الأمن السيبراني، وتقوم المؤسسات التعليمية بنشر الوعي العام بين الأفراد العاديين من منطلق الاعتقاد بأن الخطوة الأولى للسيطرة على مصادر التهديد في الفضاء السيبراني تبدأ ببناء الوعي[2].

- **البعد الاقتصادي:**

تكمن أهمية البعد الاقتصادي للأمن السيبراني في أن معظم الهجمات السيبرانية الخبيثة تستهدف المصالح الاقتصادية للأفراد، حيث يعتبر الاستغلال المالي هو الدافع الأول للجريمة السيبرانية التي تستهدف الأفراد أو المؤسسات الصغيرة، وفي هذا النوع من الهجمات، يكون الهدف الرئيس هو الحصول على المعلومات المصرفية للضحايا من أجل سرقة الأموال من حسابات الضحايا، وتحويلها إلى حسابات خارجية، ويقوم القرصنة بتنفيذ هذه الهجمات باستخدام برامج للتجسس، وهذه البرامج تساعد في الحصول على المعلومات السرية من الجهاز الخاص بالضحية، مثل كلمات المرور في المواقع الالكترونية المختلفة، ويستطيع المجرمون السيبرانيون ممارسة أنشطتهم

(1) صقر، 2017، ص 401.

(2) Dlamini&Modise, 2012 , 104.

في دول خارجية بدون خوف من التعرض لانتقام من قبل الضحايا، أو الاعتقال من قبل السلطات القانونية وعادة ما يكون من الصعب تحديد منفذي الأعمال الإجرامية[1].

أركان جرائم الأمن السيبراني:

تتعدد أركان جرائم الأمن السيبراني منها الركن المادي، والركن المعنوي، والركن الشرعي، **فالركن المادي** وهو ارتكاب الجريمة سواءً كان فعلًا أو امتناعًا[2]، ويُعرف أيضًا بأنه النشاط المادي الذي يصدر عن الجاني متخذًا مظهرًا خارجيًا يتدخل من أجله القانون بتقري العقاب في هذا النشاط[3]، والركن المادي يتكون من ثلاثة عناصر:

العنصر الأول: السلوك الإجرامي: كأن يتحرك ها السلوك الإيجابي بحركة واحدة كالقتل بالرصاص بحركات متعددة كالمشاجرة التي تنتهي بالوفاة، وصوره متعددة كالسلوك الإجرامي الإيجابي، وذلك بمخالفته نصًا يُنهي عن الإتيان بهذا الفعل كسرقة بيت أو جهاز معين، وقد يكون هاذ السلوك سلبي لمخالفته نص يأمر بإتيان فعل معين، كامتناع دكتور من إعطاء الدواء لمريضه العاجز مما يؤدي لوفاته، وقد تكون في صورة معقدة كما في جريمة الإرهاب أو السطو المسلح، ويكون هذا السلوك الإجرامي بصورة بسيطة كما في جريمة القذف.

فالقانون الجنائي لا يعتد بزمان أو مكان وقوع الجريمة ولا يعول كثيرًا على الوسيلة التي ارتكبت بها الجريمة، أو وقع بها السلوك الإجرامي، إلا عند تقديره للظروف المشددة أو المخففة، فأهمية هذه الصور المجرمة والظروف المصاحبة لها تظهر مدى توافر القصد الجنائي، كما تُفيد تحديد الاختصاصات القضائية، والقوانين واجة التطبيق، ومدة التقادم فيها، وبدأ سريانها. وحين تتشابه الجرائم السيبرانية بالجرائم الأخرى فيُمكن تقسيمها وتكييفها بنفس قسيم الجرائم التقليدية[4].

العنصر الثاني: العلاقة السببية: وهذا العنصر له ثلاث نظريات:

النظرية الأولى: نظرية السبب الأقوى أو السبب المباشر: وهذه النظرية حصرت النتيجة في عامل واحد هو أقوى الأسباب، وهذا يؤدي بالجاني من الإفلات من العقاب، فهي لا تساوي بين الأسباب المساهمة في حصول الجريمة، بل تنظر إلى السبب الأقوى سواءً كان هو سلوك الجاني أو غيره.

النظرية الثانية: تعادل الأسباب: فهي متعادلة من حيث قوة أثرها في حصول النتيجة، وهي تساوي جميع العوامل التي تُساهم في إحداث النتيجة الإجرامية.

النظرية الثالث: السببية الملائمة: وهذا النظرية هي أنسب النظريات، ومضمونها أن الجاني يسأل عن النتائج المحتملة أو المتوقعة لفعله وذلك حسب المجرى العادي للأمور، ما لم يتدخل لقطع تلك العلاقة سببًا شاذًا أو غير مألوف.

---

(1) Geil, 2014 , 4

(2) التشريع الجنائي الإسلامي مقارنًا بالقانون الوضعي، عبد القادر عودة، ط5، 1968م. ص 110.

(3) عبد العزيز غرم الله آل جار الله، ص 85.

(4) عبد العزيز غرم الله آل جار الله، ص 88.

أما **الركن المعنوي** وهو العلم بعناصر الجريمة وإرادة ارتكابها[1]. ويُعرف أيضًا بأنه يكون الجاني مكلفًا مسؤولًا[2] والركن المعنوي له عنصرين أساسيين هما: العلم والإرادة. وذلك أن الركن المعنوي انعكاسًا لما في نفسية المجرم من قصد الجريمة وتوجه إرادته نحو تحقيق ذلك اركن المادي للجريمة، ولا يتحقق إلا بوجود هذين العنصرين فالركن المادي والركن المعنوي يرتبطان ببعض ارتباطًا قويًا.

العنصر الأول: العلم: ويشتمل عنصر العلم على عدة عناصر وهي:

1. العلم بحقيقة الفعل وخطورته وأنه يلحق ضررًا بالحق المعتدى عليه.
2. العلم بالوقائع.
3. العلم بموضوع الجريمة[3].

العنصر الثاني: الإرادة: ويشتمل على عنصرين أساسيين هما:

إرادة الفعل: وهي إثبات بأن الجاني قد اتجه إلى عمل يُمثل فعله خطرًا على الحق الذي يحميه القانون.

إرادة النتيجة: ليكتمل القصد الإجرامي، والركن المعنوي فلابد من إرادة الفعل وإرادة النتيجة، والقصد الإجرامي في الركن المعنوي له عدة صور منها: القصد العام والقصد الخاص، فالقصد العام وهو الهدف الفوري والمباشر للسلوك الإجرامي ويتحصر في حدود تحقيق الغرض من الجريمة أي لا يمتد لما بعدها بل يكون في حدود تلك الجريمة[4].

أما القصد الخاص وهو ما يتطلب توافره في بعض الجرائم فلا يكفي بمجرد تحقق الغرض من الجريمة بل هو أبعد من ذلك، أي أنه يبحث في نوايا المجرم[5].

في حين أن **الركن الشرعي** يمنع الجريمة ويُعاقب عليها. وهو:

1. أن يكون مقررًا موجودًا.
2. أن يكون ساري المفعول على الشخص والمكان والزمان.

ويُطلق عليه أيضًا الركن القانوني: أي لا جريمة ولا عقوبة إلا بنص القانون، ومن هنا وجود أي جريمة وفرض العقوبة عليها يعود إلى وجود نص قانوني، ثم وجود قانون العقوبات الذي يجرم الفعل، ويفرض العقوبة المناسبة على الجاني، ووجود الركن القانوني مهم جدًا وبصورة كبيرة في أي جريمة لا وجود لأي جريمة ولا عقاب على أي جريمة بوجود الركن القانوني أي الركن الشرعي.

وبناء على ما سبق يمكن أن نستنتج أن للجرائم السيبرانية صور كثيرة منها:

أولًا: الاعتداء السيبراني على حُرمة الحياة الخاصة.

---

(1) محمود أحمد القرعان، ص 35.

(2) التشريع الجنائي الإسلامي مقارنًا بالقانون الوضعي، عبد القادر عودة، ط5، 1968م. ص 110.

(3) عبد العزيز غرم الله آل جار الله، ص 95.

(4) محمود أحمد القرعان، ص 35.

(5) محمود أحمد القرعان، ص 36.

ثانيًا: الاعتداء على الحاسب الآلي كإتلاف البيانات والتلاعب بالمعلومات المخزنة داخل الحاسب الآلي والبرامج[1].

ثالثًا: الاستيلاء والاحتيال والنصب السيبراني، ويكون هذا الاستيلاء لغيره أو لنفسه على مال منقول أو على سند، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة، أو توقيع سند عن طريق الاحتيال[2].

رابعًا: الاعتداء على حقوق الملكية الفكرية، وذلك بنسخ وتقليد البرامج وإعادة إنتاجها وصنعها دون ترخيص، وهو اعتداء على الحقوق المالية والأدبية، وهذا ما يُسمى بالاعتداء على العلامات التجارية وبراءة الاختراع[3].

خامسًا: الاعتداء على الأمن، وذلك بالدخول غير المشروع إلى موقع الكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي، للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني، كإنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي، أو نشره لتسهيل الاتصال لقيادات تلك المنظمات أو أي من أعضائها، أو ترويج أفكارها أو تمويلها، أو نشر كيفية تصنيع المتفجرات والأجهزة الحارقة، أو أي اداة تستخدم في جميع الأعمال الإرهابية[4].

سادسًا: الاعتداء على الأخلاق والإتجار بالبشر وبالمخدرات.

سابعًا: الابتزاز والتهديد، وذلك بهدف الحصول على المال أو علاقة غير مشروعة كنشر صور أو معلومات صحيحة أو غير صحيحة عن المجني عليه.

ثامنًا: التنصت السيبراني، وذلك باستخدام برنامج المحادثة فيقوم المجرم بإقراء الضحية بأن هذا البرنامج يحتوي على ألعاب مثيرة، أو غير ذلك فيقوم الضحية باستقبال الملف، ويكون أيضًا باستخدام برنامج في جهاز الشخص المعتدى عليه الذي يُمكن من خلاله الاطلاع، والاستماع إلى المراسلات، والمحادثات الصادرة من الشخص المعتدى عليه، ويتم إدخال هذا الملف إلى جهاز المعتدى عليه عن طريق البريد الالكتروني، أو طريق مواقع مغرية يزورها المعتدى عليه فيقوم بتنزيل بعض البرامج ومنها برامج التنصت.

تاسعًا: السطو على البنوك، وذلك بتحويل الأموال من تلك الحسابات الخاصة بالعملاء إلى حسابات أخرى، وذلك بإدخال بيانات غير حقيقية، أو مسح أو تعديل البيانات الموجودة، بقصد اختلاس الأموال، أو إتلافها، أو نقلها، وتقوم هذه التقنية على الاستيلاء على الأموال بكميات صغيرة جدًا من الحسابات الكبيرة.

عاشرًا: الانتحال والتقرير السيبراني، وذلك بانتحال شخصية المواقع، ويكون باختراق الحاجز الأمني لهجوم يشنه المجرم على الموقع للسيطرة عليه، ومن ثم يقوم بتحويله كموقع بيني أو يحاول المجرم اختراق موقع لأحد مقدمي الخدمة المشهورين، أما انتحال الشخصية الفردية فيكون بسبب التنامي المتزايد لشبكة الإنترنت، والذي أعطى

---

(1) علي نعمة جواد الزرفي، الجريمة المعلوماتية الماسة بالحياة الخاصة دراسة مقارنة، المكتب الجامعي الحديث، بدون طبعة، 2019م، ص 38.

(2) نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية.

(3) غانم مرضي الشمري، الجرائم المعلوماتية، الدار الدولية، عمان، الطبعة الأولى، 2016 م، ص 52.

(4) عبد العزيز غرم الله آل جار الله، ص 85.

للمجرمين قدرة أكبر على جمع المعلومات للضحية المطلوبة، والاستفادة منها في ارتكاب الجرائم فتنتشر في شبكة الإنترنت الكثير من الإعلانات المشبوهة والتي تحاكي الطمع الإنساني في محاولة الاستيلاء على معلومات اختيارية من الضحية[1].

الاستدلال في الجريمة السيبرانية:

فالاستدلال هو مجموعة الإجراءات الأولية السابقة على تحريك الدعوى الجنائية، والتي تستهدف التحري عن الجرائم، والتثبت من وقوعها، وجمع معلومات كافية بشأنها، وإثبات الآثار التي تولدت عنها وجه يتيح لسلطة التحقيق التصرف في التهمة سواء بتحريك الدعوى الجنائية الناشئة عنها، أو بحفظ أوراقها وصرف النظر عنها، فهو إجمالًا بمثابة إعداد العناصر اللازمة للتحقيق في الجريمة[2].

حيث أناط نظام الإجراءات السعودي الجديد سلطة الضبط الجنائي لأشخاص معينين ومحددين، وذلك من خلال ما جاء في المادة (26)، حيث نص على ما يلي: يقوم بأعمال الضبط الجنائي بحسب المهمات الموكلة إليهم كلٌ من:

1. أعضاء هيئة النيابة العامة في مجال اختصاصاتهم.
2. مدير الشُرط ومعاونيهم في المدن والمحافظات والمراكز.
3. الضباط في جميع القطاعات العسكرية – بحسب المهمات الموكلة إليه في الجرائم التي تقع ضمن اختصاص كل منهم.
4. محافظي المحافظات ورؤساء المراكز.
5. رؤساء المراكب السعودية البحرية والجوية في الجرائم التي ترتكب على متنها.
6. رؤساء مراكز هيئة الأمر بالمعروف والنهي عن المنكر في حدود اختصاصاتهم.
7. الموظفين والأشخاص الذي خولو صلاحيات الضبط الجنائي بموجب أنظمة خاصة.
8. الجهات واللجان والأشخاص الذين يكلفون بالتحقيق بحسب الأنظمة[3].

وهناك أدوات حددتها المملكة العربية السعودية للإبلاغ عن الجرائم السيبرانية، وهي كالآتي:

1. الاتصال على الرقم 989.
2. التطبيق الالكتروني (كلنا أمن) على الأجهزة الذكية.
3. عن طريق الشرطة حسب الاختصاص المكاني.
4. البوابة الالكترونية لوزارة الداخلية (أبشر).
5. عن طريق إرسال بريد الكتروني لهيئة الاتصالات وتقنية المعلومات.

---

(1)https://www.citc.gov.sa/ar/mediacenter/awarenesscampaigns/pages/awar 6.aspx

(2) د. محمد حميد المزمومي، الوسيط في شرح نظام الإجراءات الجزائية السعودي، مركز النشر العلمي بجامعة الملك عبدالعزيز، جدة، الطبعة الثانية، 2019، ص 98.

(3) المادة (24) من نظام الإجراءات الجزائية الجديد لعام 1435هـ.

6. عن طريق البلاغ عن حادثة سيبرانية في موقع الالكتروني للهيئة الوطنية للأمن السيبراني.
7. هيئة الأمر بالمعروف أو النهي عن المنكر عن طريق الهاتف (1909).

التحقيق في جرائم الأمن السيبراني:

نصت المادة (65) من نظام الإجراءات الجزائية في المملكة العربية السعودية، يتم التحقيق مع المتهم في لنيابة العامة، وله الحق في توكيل محامي لحضور إجراءات التحقيق، وعلى المحقق القيام بالتحقيق في أي جريمة من الجرائم المنصوص عليها في اللائحة، ويُمكنه التحقيق في جرائم أخرى إذا اقتضت الحاجة لذلك[1].

يعتبر التحقيق هو المرحلة الألى للدعوى الجنائية التي تسبق المحاكمة، وتقوم به النيابة العامة بعد البلاغ عن القضية وإحالتها لها، إذ توجد بها دوائر متخصصة في التحقيق في الجرائم السيبرانية، تُسمى بدوائر المال، وتقوم هذه الدوائر باستجواب المتهم والتحقيق معه في الجريمة المنسوبة إليه.

وتتميز بأنها ذات طبيعة قضائية، ويُمكن مباشرتها بطريقة القهر والإجبار، بخلاف إجراءات الاستدلال التي تتميز بطبيعة إدارية، كما تتميز إجراءات التحقيق أيضًا بأن ما ينتج عنها من أدلة يمكن أن يعتمد عليها في إصدار أحكام القضاء الجنائي، بعكس إجراءات الاستدلال التي تكون مكملة لأدلة أخرى.

ومن إجراءات التحقيق جمع الأدلة من المعاينة، وندب الخبراء، والتفتيش، وضبط الأشياء، ومراقبة المحادثات وتسجيلها، وسماع الشهود، والاستجواب والمواجهة، ولا يلزم المحقق ترتيب معين عند مباشرة هذه الإجراءات وهي:

أولًا: المعاينة: والمعاينة هنا في التحقيق تعني إثبات مباشر ومادي لحالة شيء، أو شخص معين، ويكون ذلك من خلال الرؤية، أو الفحص المباشر للشيء، أو للشخص بوساطة من باشر الإجراء[2]، وعلى المحقق ضبط كل ماله علاقة بالجريمة، وإثبات حالة الأشخاص والأماكن والأشياء ذات الصلة بالجريمة، وقد يكون إثبات المعاينة مع الجرائم السيبرانية أمرًا صعبًا للفترة الزمنية التي قد تطول ما بين وقوعها واكتشافها، مما يؤدي بها إلى تلف البيانات، أو نقلها، أو إخفائها.

والمعاينة قد تكون إجراء تحقيق أو استدلال، ولا تتوقف طبيعتها على صفة من يجريها، بل على مدى ما يقتضيه إجراؤها من مساس بحقوق الأفراد وحرياتهم، فإذا جرت المعاينة في مكان عام كانت إجراء استدلال[3].

ثانيًا: ندب الخبراء: نصت المادة (66) من نظام الإجراءات الجزائية السعودي للمحقق أن يندب كتابة أحد الضبط الجنائي للقيام بإجراء معين أو أكثر من إجراءات التحقيق، عدا استجواب المتهم، ويكون للمندوب في حدود ندبه السلطة التي للمُحقق في هذا الإجراء، وإذا دع الحال إلى اتخاذ المحقق إجراء من الإجراءات خارج اختصاصه، فله أن يندب لذلك مُحقق الدائرة المختصة، أو رجال الضبط الجنائي بحسب الأحوال، ويجب على المحقق أن ينتقل بنفسه للقيام بهذا الإجراء إذا اقتضت مصلحة المحقق ذلك[4]، وللمحقق الاستعانة بالخبراء

(1) المادة (65) من نظام الإجراءات الجزائية الجديد لعام 1435هـ.
(2) سرور، أحمد فتحي، الوسيط في قانون الإجراءات الجنائية، ط6، ص 287.
(3) د. محمد حميد المزمومي، ص 165.
(4) المادة (66) من نظام الإجراءات الجزائية السعودي لعام 1435هـ.

المختصين لاستكمال إجراءات التحقيق، وهذا بالفعل ما تتطلبه طبيعة الجرائم السيبرانية الذي تقتضي معرفة تامة بنظم الحاسبات، ومهارة وتقنية فنية عالية، تمكنهم من مباشرة التحقيق في مجال الجرائم السيبرانية.

نصت المادة (50) من نظام الإجراءات الجزائية السعودي بما يلي:

1. للمُحقق تمكين الخبير من الاطلاع على الأوراق والمستندات المتعلقة بطلب الخبرة.
2. يكون ندب المحقق للخبير لإبداء رأيه في مسألة متعلقة بالتحقيق، وفقًا لم ورد في المادة (76) من النظام مكتوبًا، ويحدد في الندب المهمة المطلوب والمدة المحددة لإنجازها، ويخضع الخبير أثناء مباشرته مهمته لرقابة التحقيق.
3. يلتزم الخبير المنتدب بالمهمة المكلف بها.

ونصت المادة (51) من نظام الإجراءات الجزائية السعودي على الآتي:

1. يقدم الخبير عند إنجاز مهمته المطلوبة منه، وفقًا لما ورد في المادة (67) من النظام تقريرًا مؤرخًا وموقعًا منه يتضمن ملخصًا للمهمة، وإجراءات الكشف، والفحص والتحاليل الفنية التي باشرها.
2. تضم تقارير الخبرة، وجميع مرافقتها إلى ملف الدعوى.
3. عند تعداد الخبراء واختلافهم في الرأي عليهم أن يقدموا تقريرًا واحدًا يتضمن رأي كل واحد منهم[1].

ثالثًا: التفتيش: وهو إجراء من إجراءات التحقيق التي تؤدي إلى ضبط أدلة الجريمة بعد اكتشافها، ويشتمل التفتيش في الجرائم السيبرانية على ما يلي:

1. السجلات المثبتة لاستخدام نظام المعالجة الآلية للبيانات.
2. دفتر يومية التشغيل وسجل المعاملات.
3. السجلات الخاصة بعمليات الدخول إلى نظام المعالجة الآلية للبيانات وما يتعلق بها.
4. البيانات المسجلة في ذاكرة الحاسب أو في مخرجاته.

رابعًا: ضبط الرسائل ومراقبة المحادثات: نصت المادة (57) من النظام الأساسي للحكم بأنه لرئيس هيئة التحقيق والادعاء العام أن يأمر بضبط الرسائل، والخطابات، والموضوعات، والطرود، وله أن يأذن بمراقبة المحادثات الهاتفية وتسجيلها متى كان لذلك فائدة من ظهور الحقيقة من جريمة وقعت، على أن يكون الأمر أو الإذن مسببًا، أو مُحددًا بمدة لا تزيد عن عشرة أيام قابلة للتجديد وفقًا للتحقيق.

خامسًا: الشهادة: نصت المادة (66) على المحقق أن يثبت في المحضر البيانات الكاملة عن كل شاهد، وتدون تلك البيانات وشهادة الشهود وإجراءات سماعها في المحضر من غير تعديل، أو شطب، أو كشط، أو إضافة، ولا يعتمد شيء من ذلك إلا إذا صدق عليه المحقق، والكاتب، والشاهد، وتُعد الشهادة هي إجراء من إجراءات التحقيق.

سادسًا: الاستجواب: يُعد الاستجواب أحد الإجراءات المهمة من إجراءات التحقيق، التي تهدف إلى الوقوف على حقيقة التهمة من المتهم، أو إلى الدفاع منه بنفيها، أو الوصول إما إلى اعتراف أو غير ذلك، وللاستجواب نوعين هما:

(1) د. محمد حميد المزمومي، ص 168.

الاستجواب الحكمي: وهو مواجهة المتهم بغيره من الشهود، أو المتهمين في حكم الاستجواب.

الاستجواب الحقيقي: وهو توجيه التهمة إلى المتهم، ومناقشته تفصيليًا عنها، ومواجهته بالأدلة القائمة ضده[1].

المحاكمة في جرائم الأمن السيبراني:

تعتبر المحكمة الجزائية هي المحكمة المختصة في الجرائم الجنائية والجرائم السيبرانية، وتتألف من ثلاث دوائر متخصصة هي:

1- دوائر القضايا التعزيرية. 2- دوائر قضايا القصاص والحدود. 3- دوائر قضايا الأحداث.

كما أنها تختص بالفصل في جميع القضايا الجزائية.

الإثبات الجنائي في محاكمة جرائم الأمن السيبراني:

وهي تلك الأدلة الجنائية الرقمية التي تُضاف إلى وسائل الإثبات لإثباتها في المحاكم الجنائية السيبرانية[2].

وقد قضت المحاكم بإمكانية اعتماد الأدلة الجنائية الرقمية، وهي تلك الأدلة الغير ملموسة، وذلك للأسباب التالية:

1. وضوح الأدلة الرقمية، ودقتها في إثبات العلاقة بين الجاني والمجني عليه أو بين الجاني والسلوك الإجرامي.
2. إمكانية تعقب آثار الأدلة الرقمية، والوصول إلى مصادرها بدقة.
3. انتهاء العلم براي قاطع إلى صحة النتائج التي توصل إليها علوم الحاسب.
4. الأدلة الجنائية الرقمية يدعمها عادة رأي الخبير، وللخبرة في المواد الجنائية دورها في الكشف عن الأدلة، وفحصها، وتقييمها، وعرضها أمام المحاكم.
5. ارتباط الأدلة الجنائية الرقمية، وآثارها بالجريمة موضوع المحاكمة.
6. قيام الأدلة الرقمية على نظريات حسابية مؤكدة لا يتطرق إليها الشك، ممن قوى يقينيه الأدلة الرقمية.
7. الثقة التي اكتسبها الحاسوب والكفاءة التي حققتها النظم الحديثة للمعلوماتية في مختلف مجالات الحياة[3].

نصت المادة (24)، و (25) من نظام المرافعات الشرعية الصادر بالمرسوم الملكي ذي الرقم (م/1) وتاريخ 1435/1/22هـ، والمادة (128) من نظام الإجراءات الجزائية تكون المحاكمة وفقًا لنظام مكافحة الجرائم المعلوماتية الصادر بالمرسوم الملكي ذي الرقم (م/17) وتاريخ 1428/3/8هـ. وقد نصت المادة الخامسة من النظام المذكور عقوبة الجرائم السيبرانية الوطنية بكافة صورها أن عقوبتها السجن مدة لا تزيد عن أربع سنوات، وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين.

أما إذا كانت الجريمة السيبرانية جريمة عالمية فإما أن يكون المجرم سعوديًا أو غير سعودي. فإن كان سعوديًا فيكون اختصاصها للمحاكم الجزائية السعودية للمادة الرابعة والعشرين من نظام المرافعات الشرعية الصادر بالمرسوم

(1) د. محمد حميد المزمومي، ص 182

(2) خالد حسن أحمد لطفي، ص 128

(3) د. محمد الأمين البشري، الأدلة الجنائية الرقمية، المجلة العربية للدراسات الأمنية والتدريب، مجلد 17، العدد 33، ص 128.

الملكي ذي الرقم (م/1) وتاريخ 1435/1/22هـ، والمادة (128) من نظام الإجراءات الجزائية، وتكون المحاكمة وفقًا لنظام مكافحة الجرائم المعلوماتية الصادر بالمرسوم الملكي ذي الرقم (م/17) وتاريخ 1428/3/8هـ [1].

وإن كان غير سعودي فيخضع لقوانين العقوبات العالمية، ويُطبق في حقه الاتفاقيات المختصة بالتعاون الأمني والعدلي، على أنه يحق لكل دولة من حيث المبدأ محاكمة من ألحق بها الضرر على أراضيها ولو غيابيًا[2].

جهود المملكة العربية السعودية في مكافحة جرائم الأمن السيبراني:

أصدرت المملكة العربية السعودية أول قانون عربي يتطرق لمواجهة هذه الجرائم، تبعتها دولة الإمارات العربية المتحدة، ثم سلطنة عُمان جميع هذه القوانين مختصة في مكافحة جرائم المعلومات، وتُعد هذه القوانين نموذجية حيث تطرقت إلى غالبية الجرائم المعلوماتية، وتعتبر أول ثلاثة قوانين عربية تصدر بشكل مستقل لمواجهة الجرائم المعلوماتية[3].

فالمملكة العربية السعودية بذلت العديد من الجهود في مجال مكافحة الجرائم المعلوماتية، ومن تلك الجهود قيام المملكة بالمشاركة في مؤتمر القمة العالمي لمجتمع المعلومات، والجدير بالذكر أن المملكة العربية السعودية كانت أول دولة عربية سنت نظامًا خاصًا لمكافحة الجريمة الالكترونية تلتها الإمارات العربية المتحدة، وبعد ذلك سلطنة عمان[4].

سارعت المملكة العربية السعودية من خلال الجهات القانونية المعنية في البحث لمواجهة تلك الظواهر المستحدثة من الإجرام، وذلك بالبحث في كيفية الحماية لنظم المعلومات، وقعت المملكة العربية السعودية عل الاتفاقية الجديد للجريمة الالكترونية التي تم التصديق عليها في المملكة، حيث تهدف هذه الاتفاقية إلى التصدي لارتفاع الجرائم الالكترونية وإيجاد ونشر الفيروسات والقرصنة، وتداخل الأنظمة، والوصول غير المشرع للبيانات، واعتراضها وما شابه ذلك، كما أصدر المملكة العربية السعودية قانون للعقوبات بخصوص الجرائم المعلوماتية، يتألف من (16) فصلًا [5].

ولقد نص نظام مكافحة جرائم المعلوماتية السعودي في المادة السابعة على أنه: يعاقب بالسجن مدة لا تزيد على عشر سنوات، وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيًا من الجرائم المعلوماتية[6].

فتحت المملكة العربية السعودية المسارات الأكاديمية في تخصص الأمن السيبراني، وقد كان ذلك في غالب الجامعات، ومنها: جامعة الملك سعود، وجامعة الملك عبد العزيز، وجامع الأمير سلطان بن عبدالعزيز.

كما عاقبت المملكة العربية السعودية مرتكبي الجرائم السيبرانية بالمحاكم الشرعية:

---

(1) المادة (128) من نظام الإجراءات الجزائية السعودية.

(2) المادة (24 و25) من نظام المرافعات الشرعية.

(3) الشهري، 2009، ص 524.

(4) كمال وبوبكر، 2015، ص 211.

(5) Elnaim, 2013. 17.

(6) السلويلم، 2014، ص 63.

تختص النيابة العامة بالتحقيق والإعادة في قضـــايا الجرائم الســـيبرانية الوطنية، وكذا العالمية فإذا كان فاعلها ســعود، وبموجب المادة الثالثة من نظام هيئة التحقيق والادعاء العام الصــادر بالمرســوم الملكي ذي الرقم (م/56) وتاريخ 1409/10/24هـــــ. وتختص المحاكم الجزائية بســماع الدعاوى، والنظر في الأدلة، والبيانات، والحكم في دعاوى الجرائم السيبرانية الوطنية، وكذا العالمية إذا كان فاعليها سعودي، وبموجب المادة الثامنة والعشرون بعد المائة من نظام الإجراءات الجزائية الصادر بالمرسوم الملكي ذي الرقم (م/2) وتاريخ 1435/1/22هـ[1].

أنشأت المملكة العربية السعودية الهيئة الوطنية للأمن السيبراني:

حيث صدر بإنشائها الأمر الملكي الكريم ذي الرقم (6801) وتاريخ 1439/2/11هـــ، وقد نصت الفقرة الأولى من المادة الثانية من تنظيم الهيئة الوطنية للأمن السيبراني على أنها ترتبط بمقام الملك ـ يحفظه الله ـ كما نصت المادة السادسة من ذات التنظيم على أن تشكيلها وفق النحو الآتي:

رئيســها يُعين بأمر ملكي، وأعضــاؤها: رئيس أمن الدولة، ورئيس الاســتخبارات العامة، ونائب وزير الداخلية، ومساعد وزير الدفاع، ومحافظ الهيئة.

أقامت المملكة العربية السعودية الملتقيات والدورات والندوات وورش العمل المتعلقة بالأمن السيبراني:

من ذلك الهيئة الوطنية للأمن السيبراني، وما أقامته الجامعات المحلية: كجامعة شقراء بعنوان: دور الجامعات في تعزيز مفهوم الأمن الســـيبراني: التحديات والرؤى والتوجهات في تاريخ 2019/3/18م، وجامعة نايف العربية للعلوم الأمنية بعنوان الجرائم السيبرانية والأدلة الرقمية في تاريخ 2019/12/19م.

التوصيات في إعداد طُرق وسبل الوقاية من جرائم الأمن السيبراني:

1. تصميم قاعدة بيانات للجرائم السيبرانية بحيث تشمل كافة المتغيرات الخاصة بتلك الجرائم.
2. استخدام وسائل التقنية الحديثة لتأمين تناقل البيانات والمعلومات فيما بين المستفيدين والمخولين للوصول إليها.
3. تشــكيل لجنة من الفنيين الســعوديين المختصــين لمراقبة محتوى الأخلاقي، والســياســي، والعقائدي للألعاب المستوردة والبرمجيات الخبيثة، والتأكد من خلوها من الرسائل السياسية، أو المساس بالرموز الوطنية، والدينية للمملكة العربية السعودية.
4. تشكيل لجنة مختصة من الفنيين السعوديين لمراقبة محتوى التطبيقات الالكترونية، والبرامج الحكومية من خلال توظيف مختصين، وباحثين، إضافة إلى التشجيع على صناعة منصات حكومية لكوادر وطنية كي لا نكون رهينة لأي منصة دولية تفرض شروطها على تطبيقاتنا الوطنية.
5. إجراء المزيد من الدراســـات والبحوث حول الحروب الالكترونية الموجهة التي ثبت القيام بها من داخل المملكة العربية السعودية.
6. التوسع في تحليل لمعرفة الواقع الحالي، والتنبؤ بالمشاكل المستقبلية، وذلك باستخدام أدوات الذكاء الاصطناعي، ووضع خطط استباقية لمواجهة المشاكل المستقبلية.

(1) المادة (128) من نظام الإجراءات الجزائية السعودية.

7. العمل على تقليل الاعتماد على العنصر البشري، لما يُحتمل من الخطأ خاصة عند إدخال بيانات الجرائم السيبرانية.
8. تدريب أعضـــاء من النيابة العامة الســـعوديين المؤهلين قانونيًا على التقنيات البرمجية حتى يكونوا قريبين من مسارح الجريمة، وذلك لقدرتهم على استخدام الأدوات التقنية المناسبة أكثر من المتخصصين في الجرائم العامة.
9. رفع مستوى الوعي الأمني لدى جميع شـرائح المجتمع عن طريق الحملات الإعلامية المكثفة والحقائب التدريبية المتخصصة في هذا الشأن.

الخاتمة:

في الختام لابد من الوعي بأن الجرائم السيبرانية جرائم يصعب التحكم فيها، والتصدي لها، نظرًا لخصوصيتها باعتبارها جرائم عابرة للجغرافيا، وأيضًـــا باعتبار أن التطور المذهل في الجانب التكنولوجي، والالكتروني، والرقمي صعب هو الآخر من مهمة مكافحة هذه الجريمة.

وباعتبار أن الدولة كعضـــو في المجتمع الدولي لا تســـتطيع بمفردها مجابهة مثل هذه التحديات الصـــعبة، وعلى الرغم من تكاتف دول العالم في شـكل اتحادات جهوية، وإقليمية، وعالمية للتصـدي لهذه الجرائم السـيبرانية، إلا أن التحدي كان أكبر، والخسـائر في ارتفاع مسـتمر سـواء على المسـتوى القيمي، أو الشـخصـي، أو مختلف الخسـائر الاقتصادية، والتجارية الناجمة عن الأضرار التي تمس بخاصة اقتصاديات دول العلم.

ويُلاحظ عدم الاستقرار على مفهوم واحد للجرائم السيبرانية، ولعل السبب في ذلك يعود إلى أمكانية ظهور جرائم جديدة متصلة بالعالم الافتراضي وتدخل في نطاق هذه الجرائم.

كما يُلاحظ تعدد المصـطلحات المسـتخدمة للدلالة على الجرائم السـيبرانية، غير أن المهم هو أن تنصـب على هدف واحد يتمثل في اتخاذ التدابير الوقائية والإجرائية لمكافحتها، والحد من آثارها.

المصادر والمراجع:

القرآن الكريم.

كُتب اللغة:

مقاييس اللغة، ابن فارس، جرم. مختار الصحاح، الرازي، جرم. القاموس المحيط/ الفيروز آبادي، جرم.

لسان العرب بتصرف، ابن منظور، جرم. المصباح المنير، الفيومي، جرم.

كُتب الحديث:

صحيح البخاري كتاب الاعتصام رقم2789.

صحيح مسلم كتاب الفضائل من حديث سعد بن أبي وقاص رضي الله عنه رقم 611.

المراجع:

الشـــهري، حســـن بن أحمد، نحو قانون دولي موحد لمكافحة الجرائم المعلوماتية، **مجلة دراســـات وأبحاث جامعة الجلفة**، ع (1)، 2009.

مانيطه، يوســف إسماعيل، نظرة عامة عن الجريمة الالكترونية في القضـــاء الســـيبراني، **المجلة الليبية العالمية**، جامعة بنغازي ـ كلية التربية بالمرج، ع (32)، 2017.

الجريمة والعقوبة في الفقه الإسلامي "الجريمة"، محمد أبو زهرة دار الفكر العربي.

التشريع الجنائي الإسلامي مقارنًا بالقانون الوضعي، عبد القادر عودة، **مؤسسة الرسالة**.

الجريمة أحكامها العامة في الاتجاهات المعاصرة والفقه الإسلامي، عبد الفتاح خضر.

عبد العزيز بن غرام الله آل جار الله، جرائم الإنترنت وعقوباتها وفق نظام مكافحة الجرائم المعلوماتية السعودي (دراسة مقارنة) (ويليه آثار العولمة على مستخدمي الإنترنت، دار الكتاب الجامعي، الرياض، الطبعة الأولى 2017م.

ملاك، قارة، الجريمة المعلوماتية في القطاع البنكي وأساليب مكافحتها إشارة لحالة الجزائر، **مجلة جامعة الأمير عبد القادر للعلوم الإسلامية**، جامعة الأمير عبدالقادر للعلوم الإسلامية، ع (39)، 2016.

نعمة، أحمد عبيس، تكييف الهجمات السيبرانية في ضوء القانون الدولي، **مجلة الكوفة للعلوم القانونية والسياسة**، جامعة الكوفة، كلية القانون، مج (13)، ع (44)، 2020.

هيئة التحرير: الامن السيبراني: درع المملكة الواقي لحماية مصالحها الحيوية وبنيتها التحتية الرقمية، **مجلة الدبلوماسي**، وزارة الخارجية، معهد سعود الفيصل للدراسات الدبلوماسية، ع (90)، 2018.

أبو زيد، عبدالرحمن عاطف، الأمن السيبراني الوطن العربي: دراسة حالة المملكة العربية السعودية، آفاق سياسة، **المركز العربي للبحوث والدراسات**، ع(48)، 2019.

سامي، بونيف محمد، دور الاستراتيجيات الاستباقية في مواجهة الهجمات السيبرانية: الردع السيبراني أنموذج، **المجلة الجزائرية للحقوق والعلوم السياسية المركز الجامعي** أحمد بن يحي الونشريس تيسمسيلت، معهد العلوم القانونية والإدارية، مج (4)، ع (7)، 2019.

المقصودي، محمد بن أحمد بن علي، الأمن السيبراني والجهود الدولية لمكافحة الجرائم عابرة القارات الأمن والحياة، جامعة، نايف العربية للعلوم الأمنية، مج (37)، ع (437)، 2017.

خالد بن سعد الشايع، نجاحك هو معرفتك بالأمن السيبراني العميد.

استشراف مستقبل المعرفة: مؤسسة محمد بن راشد آل مكتوم للمعرفة والمكتب الإقليمي للدول العربية برنامج الأمم المتحدة الإنمائي، دار الغرير للطباعة والنشر، الإمارات.

حاج بشير، جيدور، أثر الثورة الرقمية والاستخدام المكثف لشبكات التواصل الاجتماعي في رسم الصورة الجديدة لمفهوم المواطنة: من المواطن العادي إلى المواطن الرقمي، دفاتر السياسة والقانون، ع15، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية، 2016

https://www.citc.gov.sa/ar/mediacenter/awarenesscampaigns/pages/awar(1).aspx .

Dashora,Kamini. 2011,Cyber crine in th society: problems and preventions.

Crowell,R. M(2017).SOME PRINCIPLES OF Cyber Warfare: Using Corbett to Understand war in th Early Twenty – First Century.University of London.Uk.

Dlamini&Modise,M (2012 , MARCH 22-23).Cyber Security Awareness Initiatives in South Africa : A Synergy Approach. 7th Inernational Conference on Information Warfare and Security. Seattle.USA.

Geil, a. p(2014). Cyber Securty ON The An Assessment of cyber security practices in the agriculture industry. Masyer of Science. Lllinois state University. USA.

Nagarathna, A.(2013). Combating cyber crime –exosting India Legal and institutional framework. The journal of Legal awareness,8(1).

Khan,Naasir , Khan.(2012)Taxonmy of Cyber Crimes and Legislation in Saudi Arabia.

Vivchar,O. L. & Oliynychuk, o.1.(2017). Modern trends of CYBERCRIME IN THE CONTEXT OF ECONOMIC SECURIT. Social and humanitarian aspects.9(25).

Ophardt, JONATHAN, A.(2010). Cyberwarfare and the crime of aggression: the need for individual accountability on tomorrows battlefield Duke haw and technology review,(3).