أكاديمية التعلم
Academy Of Learning

الجريمة الإلكترونية ومخاطرها

Electronic crime and its risks

دبلوم الأمن السيبراني

تحت إشراف
المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

❖ الأهداف التفصيلية للمقرر

بنهاية هذا المقرر سيكون المتدرب قادراً وبكفاءة على أن:

- يذكر مفهوم الجرائم الإلكترونية.
- يشرح التطور التاريخي للجرائم الإلكترونية.
- يصنف أنواع الجرائم الإلكترونية.
- يحدد دوافع الجرائم الإلكترونية.
- يعدد أنماط المجرم الإلكترونية.
- يدرك دور الحاسب الآلي في الجرائم الإلكترونية.
- يربط العلاقة بين الإنترنت والجرائم الإلكترونية.
- يبين العوامل التي ساعدت على انتشار الجرائم الإلكترونية.
- يحدد مخاطر الجرائم الإلكترونية.
- يلم بقوانيين الجرائم الإلكترونية وتشريعاتها.

❖ فهرس الكتاب

الفصل الأول

الجرائم الإلكترونية وتطورها

في هذا الفصل سوف نتعرف على المواضيع التالية:

- مفهوم الجريمة الإلكترونية والتطور التاريخي لها
- أنواع الجرائم الإلكترونية
- أدوات الجرائم الإلكترونية
- خصائص الجرائم الإلكترونية
- خصائص المجرم الإلكتروني
- أنماط المجرم الإلكتروني
- أهداف الجرائم الإلكترونية
- دوافع الجرائم الإلكترونية

- **أمن المعلومات**

لقد تعددت التعاريف الرسمية لأمن المعلومات وفيما يأتي أهمها:

فأمن المعلومات Information Security هو ممارسة العمل الذي يتمثل في حماية المعلومات الخاصّة من السرقة، أو الإفشاء، أو التخريب وإدخالها في وضع الأمان والمحافظة عليها، وتقتضي حماية المعلومات في هذا التعريف حماية محيطها ومالكها أيضا.

- **مكونات امن المعلومات**

عند ذكر كلمة امن المعلومات وجرائم الحاسوب فأن ما يتبادر الى الذهن غالباً هو كشف معلومات كأن يجب أن تبقى سرا، والحقيقة أن الحفاظ على سرية المعلومات لا يعدو أن يكون جانبا واحدا من جوانب الأمن، **أما المتخصصون فيرون لأمن الحاسوب والمعلومات مكونات ثلاثة على درجة واحدة من الأهمية، وهذه المكونات هي:**

1 - سرية المعلومات (Data Confidentiality):

وهذا الجانب يشمل كل التدابير اللازمة لمنع اطلاع غير المصرح لهم على المعلومات الحساسة أو السرية، **ومن أمثلة المعلومات التي يحرص على سريتها:** المعلومات الشخصية – الموقف المالي لشركة ما قبل إعلانه – المعلومات العسكرية.

2 - سلامة المعلومات (Data Integrity):

لا يعنينا هنا أن نحافظ على سرية المعلومات، ولكن ما يهمنا هنا هو اتخاذ التدابير اللازمة لحماية المعلومات من التغيير، وهناك أمثلة متعددة لهذا المطلب، فقد تنشر جهة ما قوائم أسماء المقبولين ممن تقدموا بطلبات للعمل لديها، وكما نرى فأننا عندما نتحدث عن أمن هذه القوائم نعني حمايتها من التغيير فمن المحتمل أن يقوم شخص ما بحذف بعض الأسماء، وإدراج أسماء أخرى بدلاً منها، مسببا كثيرا من الإرباك للناس والحرج للجهة المعنية، أو ممكن تغيير مبلغ التحويل من ١٠٠ ريال الى ١٠٠٠٠ ريال.

3 - ضمان الوصول الى المعلومات والموارد الحاسوبية (التوفر) (Availability):

أن الحفاظ على سرية المعلومات وسلامتها امر مهم ولا ريب، لكن هذه المعلومات تصبح بدون قيمة إذا كأن من يحق له الاطلاع عليها لا يمكنه الوصول إليها، أو أن الوصول إليها يحتاج وقت طويل، ويتخذ المهاجمون وسائل شتى لحرمان المستفيدين من الوصول إلى المعلومات، ومن هذه الوسائل حذف المعلومات نفسها أو مهاجمة الأجهزة التي تخزن المعلومات فيها وشلها عن العمل.

- **الجرائم الإلكترونية وتطورها**

من يمتلك المعلومات يمتلك مفاتيح المستقبل فهي ثروة لا يستهان بها ومصدر قوة سياسية واقتصادية لمن يُحسن جمعها واستثمارها وحمايتها ومعيار يُقاس به مدى تطور تحضر الشعوب وقد أضفى تطور الحاسب الآلي ودخوله في شتى مجالات الحياة السياسية والاقتصادية والاجتماعية على المعلومات قيمة مضافة ، أن تطور تكنولوجيا المعلومات وما صاحبه من تأثير إيجابي على المعلومات التي تحولت من طبيعتها التقليدية إلى الطبيعة المستحدثة والاستفادة منها في مجالات الحياة المختلفة لكنها أصبحت عُرضة بواسطة نفس التكنولوجيا للاختراقات بصور وأشكال مختلفة ومتعددة مما استحدث نوعاً جديدا من الجرائم ومنها الجرائم الإلكترونية التي أصبحت تمثل خطراً كبيراً على الأفراد والمؤسسات و بياناتهم وارتكاب جرائم بوسائل إلكترونية حيث تعاني المجتمعات والأفراد من اختراق للحقوق والخصوصيات الإلكترونية فهي ظواهر إجرامية ينتج عنها حجم مخاطر وخسائر التي يمكن أن ينتج عنها خسائر للمجتمع ككل على المستويات الاقتصادية والاجتماعية والثقافية والأمنية ، الأمر الذي دفع الدول والمؤسسات إلى العمل على الحد من هذه الجرائم التي تلحق الضرر بالأفراد من خلال التوعية والوسائل الأمنية وغيرها من الطرق.

اعتباراً لطبيعة الجريمة الإلكترونية العابرة للحدود وإمكانية ارتكابها من أي مكان في العالم لإحداث نتائجها في مكان أخر وسرعة وسهولة إخفاء أدلتها، والتداخل في دوائر الاختصاص المكاني لمباشرة الإجراءات القانونية ، إضافة إلى تعقيدات التحقيق فيها وضبط أدلتها ومرتكبيها ، كل ذلك يجعل دراستها ومواجهتها في المجتمع الخليجي أو غيره من المجتمعات أمراً لا ينفصل عن التعرف بشكل عام على ماهيتها ومفهومها وأسبابها وتطوراتها ودوافعها وآثارها والجهود الدولية والإقليمية لمواجهتها ، والحد منها فهي مشكلة عالمية تتأثر بها منطقة الخليج العربي بقدر معين مثل بقية أقاليم و دول العالم.

❖ مفهوم الجريمة الإلكترونية Cybercrime والتطور التاريخي لها

هناك صعوبة في تحديد بداية معينة لنشوء الجرائم الإلكترونية حيث إن الحواسيب الإلكترونية كأنت موجودة منذ فترة بعيدة، ولكن تختلف عما هي عليه الحواسيب الحالية سواء من حيث الشكل أو السرعة أو الدقة، والتطور الحالي يُعتبر نتاج لتطور كبير عبر سنين عديدة.

البعض يرجع حدوث أول جريمة متصلة بالحاسوب إلى عام ١٨٠١ م عندما أقدم صاحب مصنع للنسيج في فرنسا على تصميم لوحة إلكترونية وكأنت أول نموذج للوحة الحاسوب الحالي لتقوم هذه اللوحة بتكرار مجموعة من الخطوات المستخدمة لحياكة أنواع النسيج، الأمر الذي أثار مخاوف بعض العاملين في المصنع من تأثير تلك اللوحة على وظائفهم مما دفعهم إلى تخريب تلك اللوحة.

بينما يرجع البعض الأخر البداية الحقيقية لظاهرة الجرائم الإلكترونية إلى عام ١٩٥٨ م حينما بدأ معهد ستأنفورد الدولي للأبحاث في الولايات المتحدة الأمريكية يرصد حالات ما سمي في ذلك الحين بإساءة استخدام الحاسوب بصورة منظمة .

- **تطور الجرائم الإلكترونية**

مرت الجرائم الإلكترونية بتطور تاريخي تبعا لتطور التقنية واستخداماتها وقد مرت بثلاث مراحل هي:

١. المرحلة الأولى

تتمثل في انتشار استخدام الحواسيب في الستينيات والسبعينيات ومع تزايد استخدام الحواسيب الشخصية في السبعينات ظهر عدد من الدراسات المسحية والقانونية التي اهتمت بجرائم الحاسب وعالجت عدداً من قضايا الجرائم الفعلية وبدأ الحديث عنها بوصفها ظاهرة إجرامية لا مُجرد سلوكيات مرفوضة.

أبرز جريمة هي جريمة سرقة بنك مينيسوتا الأمريكي عام ١٩٦٦ م والتي اعتبرت أول سرقة إلكترونية تقع على بنك وبعد ذلك توالت بعض المقالات الصحفية في الظهور متناولة بعض الحالات التي أطلق عليها في هذا الوقت جرائم الحاسوب Computer Crime.

رغم استمرار تطور ظاهرة الجريمة الإلكترونية خلال السبعينيات إلا أن الحالات التي سجلت في تلك الفترة الزمنية كانت قليلة وقد تعود أسباب تلك القلة إلى كون مكمن الخطر كأن داخلياً ويكاد أن يكون خطراً ينحصر بين العاملين على الأنظمة الحاسوبية نفسها حيث كانوا هم فقط من يستطيعون الوصول إلى تلك الأنظمة بصورة مباشرة ولم يكن هناك اتصال بتلك الأنظمة من العالم الخارجي كما أن سبب قلتها أيضا يعود إلى عدم الإبلاغ عن الكثير من تلك الجرائم لكون الشركات والوكالات كأنت تحرص على عدم اهتزاز الثقة بها وبأنظمتها الحديثة وأعقبت تتلك الحقبة الزمنية إجراء دراسات و مقالات صحفية بشأن الجريمة الإلكترونية من قبل الباحثين الصحفيين.

وفي السبعينيات أيضا شهد العالم بداية لظهور بعض التشريعات والقوانيين التي تجرم بعض الممارسات ذات الصلة بإساءة استخدام الحاسوب وقررت لها عقوبات محددة كما حدث في السويد والتي اعتبرت بذلك أول دولة يصدر فيها قانون يجرم بعض الأفعال والممارسات المرتبطة بالحواسيب.

٢. المرحلة الثانية

في الثمانينات طفا على السطح مفهوم جديد للجرائم الإلكترونية ارتبط بعمليات اقتحام نظام الحاسب عن بعد وأنشطة نشر وزراعة الفيروسات الإلكترونية التي تقوم بعملية تدميرية للملفات أو البرامج وأنتشر مصطلح المخترق Hacker المعبر عن مُقتحمي النُظم كما ظهر ما يُعرف باسمً المجرم المعلوماتي أو الإلكتروني, فقد حدث تغيراً ملحوظاً في التعامل مع ظاهرة الجريمة الإلكترونية وذلك من جانب الباحثين والعامة على السواء بسبب ارتفاع مؤشر عدد القضايا ذات الصلة بإساءة استخدام الحاسوب و لاسيما بعد اهتمام الصحافة وإبرازها لتلك القضايا حيث أصبح بعضها يؤرق المجتمع الدولي كقضايا الاختراق وقرصنة البرمجيات والتلاعب في أنظمة النقد الإلكتروني و أنتشار العديد من الفيروسات، كما شهد ذلك العهد الانطلاقة الأولى للقوانيين والتشريعات الخاصة بحماية البرامج الحاسوبية والتي أطلق عليها قوانيين حماية الملكية الفكرية واعتبرت من القوانيين الأكثر وضوحاً ونضجاً.

وكذلك في تلك الفترة الزمنية ظهر الاهتمام العربي بظاهرة الجريمة الإلكترونية وتمثل ذلك في صدور العديد من الدراسات العلمية والمؤلفات العربية ذات الشأن بالجريمة الإلكترونية وعقد الندوات المختلفة ذات الصلة بذلك حيث عقدت في ١٩٨٦ م ندوة أمن المعلومات في الحاسبات الآلية والتي تبناها مركز المعلومات الوطني التابع لوزارة الداخلية السعودية.

٣. المرحلة الثالثة

تتمثل في فترة التسعينيات حيث شهدت تزايد هائل في مجال الجرائم الإلكترونية وتغييراً في نطاقها ومفهومها وكأن ذلك بفعل ما أحدثته شبكة الإنترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكة المعلومات.

شهدت التسعينيات والسنوات الأولى من القرن الحادي والعشرين تحولات في مجال الجريمة الإلكترونية حيث ارتبط بتحول شبكة الإنترنت في ذلك الوقت من شبكة أكاديمية إلى شبكة تعني بخدمة المجالات التجارية والفردية حيث بلغ مستخدميها في عام ١٩٩٦ م ما يقارب من ٤٠ مليون مستخدم الأمر الذي أدى إلى نشأة عبء كبير على المختصين بمكافحة الجريمة الإلكترونية ولذلك وُجد مفهوم جديد عرفها "بالجرائم العابرة" حيث يستطيع المجرمون تنفيذ مخططاتهم الإجرامية في دول أخرى.

- **أشهر الجرائم الإلكترونية في التاريخ**

منذ انتشار الحواسيب وشبكة الإنترنت، حدثت العديد من الهجمات الإلكترونية ضد الأفراد والشركات والحكومات، أبرز وأشهر هذه الهجمات:

هجمة فايروس ميليسا

يعتبر فايروس ميليسا أحد أكبر وأقدم التهديدات الإلكترونية، ففي عام ١٩٩٩ م، قام ديفيد لي سميث باختراع فايروس ميليسا وهو فايروس بسيط يصيب مستندات مايكروسوفت ورد، وينشر نفسه تلقائياً كمرفق عبر البريد الإلكتروني، تسبب هذا الفيروس في دمار شديد في أنظمة شركة مايكروسفت والعديد من الشركات الأخرى، وقدر أن إصلاح هذا الأنظمة المتدمرة كلف ما يقارب ٨٠ مليون دولار.

الهجوم الإلكتروني على ناسا

في عام ١٩٩٩ م قام جيمس جوناثأن وهو شاب يبلغ من العمر ١٥ عاماً فقط، باختراق أجهزة الحاسب التابعة لوكالة ناسا، وتسبب هذا الاختراق بإغلاق أجهزة حاسب ناسا لمدة ٢١ يوماً، مما كلف الوكالة حوالي ٤١٠٠٠ دولار في الإصلاحات.

الهجوم الإلكتروني على إستونيا

في أبريل من عام ٢٠٠٧ م، شهدت دولة إستونيا أول هجوم إلكتروني على البلد بأكمله، بحيث سبب هذا الهجوم توقف حوالي ٥٨ موقعاً إستونياً عن الاتصال بالإنترنت، بما في ذلك مواقع الحكومات والبنوك ووسائل الإعلام.

الهجوم الإلكتروني على شركة PlayStation سوني

في أبريل من عام ٢٠١١ م، أدى هجوم إلكتروني على شبكة PlayStation Network التابعة لشركة Sony، إلى المطالبة بالمعلومات الشخصية لحوالي ٧٧ مليون مستخدم.

الهجوم الإلكتروني على موقع Yahoo

في عام ٢٠١٤ م، شهد موقع Yahoo هجوماً إلكترونياً كبيراً تمثل في سرقة المعلومات الأساسية وكلمات المرور لحوالي ٥٠٠ مليون حساب مستخدم على الموقع.

الهجوم الإلكتروني على شبكة كهرباء أوكرانيا

في عام ٢٠١٥ م، تم القيام بهجوم إلكتروني على شبكة الكهرباء في أوكرانيا بحيث أدى هذا الهجوم إلى انقطاع التيار الكهربائي عن نصف المنازل في منطقة إيفانو فرانكيفسك.

الهجوم على خط أنابيب توزيع الوقود الخاص بشركة كولونيال

في عام ٢٠٢١ م، أجبر هجوم إلكتروني شركة كولونيال بايبلاين، وهي شركة طاقة أمريكية على إغلاق خط أنابيب توزيع الوقود للساحل الشرقي للولايات المتحدة، ودفعت شركة كولونيال بايبلاين ما يقرب من ٥ ملايين دولار للقراصنة من أوروبا الشرقية للمساعدة في استعادة أكبر خط أنابيب للوقود في البلاد.

- **تعريف الجرائم الإلكترونية**

الجرائم الإلكترونية أو ما يسمى أيضا الهجمات الإلكترونية، هو استخدام الكمبيوتر كأداة لتحقيق غايات غير قانونية، مثل ارتكاب الاحتيال أو سرقة الملكيات الفكرية أو سرقة الهويات أو اختراق الخصوصيات، وتعتبر الجرائم الإلكترونية امتداداً للسلوك الإجرامي العادي إلا أن الجرائم الإلكترونية تمتاز بأنها نمط جرائم مستحدث غير تقليدي، ويمكن تعريف الجرائم الإلكترونية أيضا بأنه "**عبارة عن هجوم على المعلومات المتعلقة بالأفراد أو الشركات أو الحكومات**" وتتميز الجرائم الإلكترونية بإمكانية حدوثها في منطقة بعيدة جدا عن منطقة المهاجم، ومثال على ذلك يستطيع شخص القيام بمهاجمة دولة تقع في قارة أخرى بعيدة عنه، كمهاجمة شخص في كندا لشخص في أستراليا إلكترونياً .

- **مفهوم الجرائم الإلكترونية**

- هي كل نشاط إجرامي يتم ضد أو باستخدام الحواسيب الآلية والبرامج والتطبيقات المختلفة وشبكات المعلومات، خاصةً شبكة الإنترنت.
- هي كل نشاط إجرامي تُستخدم فيه التقنية الإلكترونية الرقمية (الحاسب الآلي وشبكة الإنترنت) بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المُستهدف.
- وهي أيضا ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومُقاضاة فاعليها.
- هي كل سلوك غير قانوني يتم باستخدام الأجهزة الإلكترونية، ينتج عنها حصول المجرم على فوائد مادية أو معنوية.
- هي فعل أو نشاط إجرامي يرتكب متضمناً استخدام الحاسب الآلي، أو شبكة المعلومات العالمية أو أي وسيلة من وسائل الاتصالات وتقنية المعلومات الأخرى كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود بطريقة مباشرة أو غير مباشرة.
- هي نشاط إجرامي يستهدف جهاز كمبيوتر أو شبكة كمبيوتر أو جهازاً متصلاً بالشبكة وتحاول استخدامهم، تقع معظم الجرائم الإلكترونية على أيدي لصوص أو مخترقين يودون كسب الأموال، وأحيانا نادرة أخرى يكون الهدف من وراء الجرائم الإلكترونية هو إلحاق الضرر بأجهزة الكمبيوتر لأسباب غير الربح، وقد تكون هذه الأسباب سياسية أو شخصية.
- يمكن أن تقع الجرائم الإلكترونية على يد أفراد أو منظمات؛ بعض هؤلاء المجرمين الإلكترونيين منظمين ويستخدمون التقنيات المتقدمة وهم ذوي مهارات فنية عالية، وبعضهم مجرد مخترقين مبتدئين.

- **الجريمة التقليدية والجريمة الإلكترونية**

تطور مفهوم الجريمة من الشكل التقليدي إلى الشكل الإلكتروني نتيجة تغير الدوافع والظروف الاجتماعية التي مر بها الأنسان والتقدم العلمي الكبير في مجال التكنولوجيات والاتصال فقد أصبحت الإنترنت شبكة اتصال دولية ألغت الحواجز والفواصل بين الدول وأصبح النشاط الأنساني مرتكزاً بشكل أكثر على شبكة الإنترنت مما جعلها وسيلة مثالية لتنفيذ العديد من الأفعال غير المشروعة وامتداد شكل الجريمة من الواقع المادي إلى الجريمة في العالم الافتراضي.

ولكن تتشابه أطراف الجريمة الإلكترونية والجريمة التقليدية من حيث وجود مجرم له دافع لارتكاب الجريمة سواء كأن شخصاً طبيعياً أو اعتبارياً، ولكن الاختلاف في الأداة المستخدمة في ارتكاب الجريمة والمتمثلة في شبكة الإنترنت، وهي أداة عالية التقنية كما لا يتطلب مكان الجريمة انتقالا ماديا للجاني، فقد انتشرت الجرائم الإلكترونية على شبكة الإنترنت وتعددت صورها وأشكالها.

- تطور الجريمة من الشكل التقليدي إلى الشكل الإلكتروني

الجريمة التقليدية	الجريمة الإلكترونية
الاحتيال	الاحتيال على الشبكة – المزاد الإلكتروني
السطو	القرصنة – الحرمان من الخدمة – نشر الفيروسات
غسيل الأموال	أنظمة الدفع على الشبكة
السرقة	جرائم الهوية – سرقة الملكية

- تشتمل طرق الجريمة الإلكترونية على :

- سرقة وتخريب وتزوير المعلومات وإساءة استخدامها ويشمل ذلك قواعد المعلومات في المكتبات وتمزيق الكتب وتحريف المعلومات والدراسات الهامة الخاصة بالتطوير التقني والصناعي والعسكري.
- اختراق الخصوصية من خلال سرقة حسابات الأفراد ونشر معلومات سرية عنهم بهدف إفشاء أسرارهم.
- التصنت وتشمل الدخول لقواعد المعلومات تسجيل المحادثات عبر الهاتف.
- التجسس ويشمل اعتراض المعلومات ومحاولة معرفة ما يقوم به الأفراد.
- التشهير ويشمل المعلومات الخاصة أو ذات الصلة بالانحراف ونشرها بشكل القصد منه الإساءة إلى شخصية الأفراد.
- السرقة العلمية الكتب والبحوث العلمية الأكاديمية وخاصة ذات الطبيعة التجريبية والتطبيقية.
- سرقة الاختراعات وخاصة في المجالات العلمية لاستخدامها أو بيعها.
- قرصنة البرمجيات ويشمل النسخ غير القانوني للبرمجيات واستخدامها أو بيعها مرة أخرى.
- قرصنة البيانات والمعلومات ويشمل اعتراض البيانات والاستيلاء عليها بقصد الاستفادة منها وبخاصة أرقام البطاقة الائتمانية وأرقام الحسابات وكلمات الدخول وكلمات السر.
- إرسال الفيروسات على شكل رسائل إلكترونية بهدف تدمير البيانات.
- الاحتيال المالي بالبطاقات وهذا ناتج عن استخدام غير شرعي لبطاقات التسوق أو المالية أو الهاتف.
- سرقة الأرقام والمتاجرة بها وخاصة أرقام الهواتف السرية واستخدامها في الاتصالات الدولية أو أرقام بطاقات الائتمان.
- المطاردة والملاحقة من خلال استخدام البريد الإلكتروني أو إرسال الرسائل.

- **الجريمة المعلوماتية**

الجرائم المعلوماتية هو سلوك غير قانوني يحدث عند اختراق الأجهزة الإلكترونية والذكية والحواسيب، التي تعتمد على الإنترنت في عملها، فيستغل المجرم شبكة الإنترنت للوصول إلى المعلومات الشخصية للأفراد، حيث إن هذه الوسائل تعتبر من أضخم بنوك المعلومات لدى جميع الناس في هذا الزمن، كما أن العديد من الأعمال والصفقات التجارية، أصبحت تنفذ عن طريق الشبكة العنكبوتية وعن بُعد؛ لذلك يجب زيادة الوعي في كل ما يخص البيانات والمعلومات المرفقة على المواقع الإلكترونية.

الجرائم الإلكترونية جرائم ترتكب ضد أفراد أو جماعات أو مؤسسات كاملة؛ باستخدام وسائل الاتصال الحديثة واستخدام الحاسوب، والهدف الأساسي منها يكون ابتزاز الشخص أو تشويه سمعته، وإلحاق الضرر به؛ للحصول على مقابل مادي مثل النقود أو لتحقيق أهداف سياسية، أو إفشاء أسرار أمنية تكون خاصة بالمؤسسة.

الجريمة المعلوماتية

أي فعل يُرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لنظام مكافحة الجرائم المعلوماتية

يمكن تقسيم تلك الجرائم إلى نوعين:

١. جرائم تضر المستخدم بصورة مباشرة، تضر بذات المستخدم وشخصه مثل السب والقذف والتشهير
٢. جرائم تضر المستخدم بصورة غير مباشرة عن طريق إلحاق الضرر بالحواسيب والأنظمة والشبكات التي يتعامل معها.

- **مفهوم الجريمة الإلكترونية**

الجريمة الإلكترونية

هي فعل غير مشروع يعتمد على الدراية والمعرفة الفنية بتقنية المعلومات ويتم بأي أداة من أدوات الاتصال الذكي والبرمجي ويكون فيه الفضاء الإلكتروني هو مكانها.

- **شرح التعريف**

١. فعل غير مشروع

يشمل كل فعل أو امتناع تجرمها الشريعة الإسلامية أو نصوص القانون وتقرر له عقوبة تُطال مرتكب ذلك الفعل.

٢. يعتمد الدراية والمعرفة الفنية بتقنية المعلومات

هو جوهر الجريمة الإلكترونية حيث يستحيل على الذي يجهل بشؤون هذه التقنية ارتكاب هذا النوع من الجرائم فلابد من دراية ومعرفة ولو يسيرة لإتمام هذه الجريمة وهذا الفعل الغير مشروع قد يقوم به شخص أو مجموعة أشخاص ويمكن أن تقوم بها دولة أو عدة دول.

٣. أدوات الاتصال الذكي والبرمجي

لم يعد يقتصر في هذا النوع من الجرائم استخدام الحاسبات الآلية التقليدية لإتمام هذا النوع من الجرائم حيث أصبح هنالك البطائق الممغنطة والأجهزة الرقمية الحديثة كالتليفونات والشرائح الإلكترونية القارئة والناسخة للمعلومات والبرامج والمخترقة للثغرات الأمنية والتجسسية والفيروسية والتي لولاها لما وجدت جرائم إلكترونية من الأساس.

٤. يكون فيه الفضاء الإلكتروني محلا ومسرحاً لها

نقلت هذه الجرائم مسرح الجريمة من أبعادها المحدودة إلى بعد جديد غير مقيد بزمان أو مكان يكون فيها الجاني بعيد عن الضحية بحيث تذوب فيه الحدود الجغرافية وقد تستمر محاولات ارتكاب هذا النوع من الجرائم لأسابيع وشهور بخلاف الجرائم التقليدية.

- **المجرم في الجريمة الإلكترونية**

هو شخص طبيعي يعمل لحسابه ويهدف إلى تحقيق مصلحة خاصة به من وراء الجريمة التي يرتكبها، حيث يتم تصنيف معظم من يرتكب جرائم الحاسب الآلي إلى الجيل الحديث من الشباب وهم قد يكونوا محترفين أو عاملين بمجال الحاسب الآلي أو قد يكونون هواة.

إلى جانب الشخص الطبيعي قد يوجد مشتركون يمدونه بما يحتاجه من أدوات وبرامج ومعدات أو على الأقل يبيعون له تلك المنتجات والبرامج التي بدونها فأنه لن يكون هناك جريمة من الأساس كما من الممكن أن يكون المجرم مجموعة من الأشخاص أو مؤسسات أو أشخاص معنوية وقد يصل الأمر في الجرائم الإلكترونية يكون فيها المجرم أنظمة ودول.

- **الضحية في الجريمة الإلكترونية**

قد يكون شخص طبيعي، أو مجموعة أشخاص، أو أشخاص معنوية، أو أنظمة ودول.

معظم الجرائم الإلكترونية تستهدف المؤسسات المالية والتجارية والصناعية للمجتمع كما أنها أيضا تستهدف الأنظمة السياسية والمصالح الخدمية المدنية والعسكرية والأمنية وذلك عن طريق تدمير أو إتلاف ثرواتهم المعلوماتية الخاصة بها.

فالجريمة الإلكترونية نوعان:

1. الجرائم الموجهة ضد الحاسب الآلي أو أنظمة تقنية المعلومات والاتصالات الأخرى بقصد إتلافها أو تدميرها أو تعطيلها.
2. الجرائم التي يكون فيها الحاسب الآلي وسيلة للارتكاب جرائم الاحتيال وسرقة الهويات وبطاقات الائتمان والأرصدة المالية والتزوير والاختلاس وسرقة حقوق الملكية الفكرية وغيرها.

- **أركان الجريمة الإلكترونية**

١. الركن المادي

السلوك الإجرامي

هو السلوك المادي الصادر عن إرادة الفرد الذي يتعارض مع القانون لأن الجريمة هي في المقام الأول فعل أدمي أي سلوك صدر عن أنسأن فالفعل هو جوهر الجريمة ، قيل لا جريمة دون فعل ، السلوك الإجرامي عند الشروع في ارتكاب الجريمة الإلكترونية يختلف عن السلوك الإجرامي عند الشروع في ارتكاب الجريمة التقليدية ، ذلك أن ارتكاب الجريمة عبر الإنترنت تحتاج بالضرورة إلى منطق تقني بمعنى أنها تتم عبر الإنترنت أو باستخدام المعالجة الآلية للبيانات وتحتاج إلى ممارسة بنشاط تقني أي توافر القدر اللازم من العلم و الإدراك لاستخدام الإنترنت والحاسوب .

النتيجة الإجرامية

يراد بها التغير الذي يحدث في العالم الخارجي كأثر للسلوك الإجرامي فيحقق عدواناً ينال مصلحة أو حقاً ، قدر الشرع جدارته بالحماية الجزائية وهو ما يعني أن للنتيجة الإجرامية مدلولين أحدهما مادي وهو التغير الناتج عن السلوك الإجرامي في العالم الخارجي والأخر قانوني وهو العدوان الذي ينال مصلحة أو حقاً يحميه القانون وتثير مسألة النتيجة الإجرامية في جرائم الإنترنت مشاكل عدة منها تحديد هل جريمة الإنترنت هي جريمة مرتكبة سلوكياً ونتيجة في العالم الافتراضي أم أن هناك امتدادا للنتيجة ليتحقق منتهاها في العالم المادي .

الرابطة السببية

هي العلاقة التي تربط بين السلوك الإجرامي والنتيجة الإجرامية وبانتفاء أو انقطاع هذه الرابطة بين السلوك الإجرامي والنتيجة فأن الركن المادي للجريمة لا يتحقق وبالتالي لا يعود ممكناً إسناد هذه النتيجة إلى مرتكب الفعل.

عند تطبيق هذا التعريف ليشمل الجرائم الإلكترونية فأن الإشكالية هنا تتجسد في أن إثنين من العناصر المكونة للركن المادي وهما السلوك الإجرامي والرابطة السببية يحدثان في العالم الافتراضي بينما العنصر الثالث المكون للركن المادي للجريمة الإلكترونية أي النتيجة الإجرامية فتحدث في العالم المادي الواقعي أي أن لها كيان منفصل عن بقية العناصر المكونة للركن المادي للجريمة الإلكترونية كما أن جرائم الإنترنت تنتشر فيها فكرة النتيجة المحتملة وذلك راجع إلى طبيعة النشاط التقني الذي يترتب عليه نتائج فمن يقصد القرصنة ويتحقق معها أنتشار الفيروسات فأن ذلك يعتبر نتيجة محتملة لذلك العمل وهو ما أدى إلى توسع بعض المشرعين في فكرة النتيجة المحتملة لتشمل الجريمة التي ليس فيها ضحية على الإطلاق .

٢. الركن المعنوي

يعرف بأنه العلم بعناصر الجريمة وإرادة ارتكابها بالتالي يتكون هذا الركن من عنصرين هما العلم والإرادة.

العلم

هو إدراك الأمور على نحو مطابق للواقع، يسبق الإرادة.

الإرادة

هي اتجاه لتحقيق السلوك الإجرامي.

- **يتخذ القصد الجنائي عدة صور منها القصد العام والقصد الخاص:**

- **القصد الجنائي العام**

هو الهدف الفوري والمباشر للسلوك الإجرامي وينحصر في حدود تحقيق الغرض من الجريمة أي لا يمتد لما بعدها.

- **القصد الجنائي الخاص**

هو ما يتطلب توافره في بعض الجرائم فلا يكفي بمجرد تحقيق الغرض من الجريمة، بل هو أبعد من ذلك أي أنه يبحث في نوايا المجرم بطرح لسؤال: ما هو الهدف الذي يريد الجاني تحقيقه من الجريمة؟

٣. الركن القانوني

هو الذي يضع النص لتجريم هذا الفعل.

- **أوجه التطابق بين الجريمة الإلكترونية والتقليدية**

الركن الأول	أن يكون هناك نص يحظر الجريمة ويعاقب عليها وهو ما يسمى في الاصطلاح القانوني بالركن الشرعي للجريمة.
الركن الثاني	إتيان العمل المكون للجريمة سواء كأن فعلا أو امتناعاً وهو ما يسمى في القانون بالركن المادي للجريمة.
الركن الثالث	أن يكون الجاني مكلفاً أي مسؤولا عن الجريمة وهو ما يسمى في الاصطلاح القانوني بالركن الأدبي، وهذه الأركان جميعها متوافرة في الجريمة التقليدية والجريمة المعلوماتية على حد سواء.

❖ أنواع الجرائم الإلكترونية

يمكن تقسيم أنواع الجريمة الإلكترونية إلى أربع مجموعات:

المجموعة الأولى

تشمل الجرائم التي تتمثل في استغلال البيانات المخزنة على الحاسب بشكل غير قانوني.

المجموعة الثانية

تشمل الجرائم التي يتم من خلالها اختراق الحاسب لتدمير البرامج والبيانات الموجودة في الملفات المخزنة عليه وتدخل ضمن الفيروسات الإلكترونية.

المجموعة الثالثة

تشمل الجرائم التي يتم فيها استخدام الحاسب بشكل غير قانوني من قبل الأفراد المرخص لهم باستعماله أي الموظفين المستغلين لمنصبهم.

المجموعة الرابعة

تشمل الجرائم التي يتم فيها استخدام الحاسب بشكل غير قانوني من قبل الأفراد غير المرخص لهم باستعماله أي غير مسموح لهم.

❖ أدوات الجرائم الإلكترونية

١. برامج نسخ المعلومات المخزنة في أجهزة الحاسب الآلي.

٢. الإنترنت كوسيط لتنفيذ الجريمة.

٣. خطوط الاتصال الهاتفي التي تستخدم لربط الكاميرات ووسائل التجسس.

٤. أدوات مسح الترميز الرقمي (الباركود)

٥. الطابعات.

٦. أجهزة الهاتف النقال والهواتف الرقمية الثابتة.

٧. الهندسة الاجتماعية

٨. برامج مدمرة مثل:

- برنامج حصان طروادة trojan horse : بحيث يقوم بخداع المستخدم لتشغيله، حيث يظهر على شكل برنامج مفيد وأمن ويؤدي تشغيله إلى تعطيل الحاسب المصاب.
- برنامج الدودة: الذي يشبه الفيروس، ولكنه يصيب أجهزة الحاسب دون الحاجة إلى أي فعل وغالباً يحدث عندما ترسل بريد إلكتروني إلى كل الأسماء الموجودة في سجل الأسماء.
- القنبلة الإلكترونية , **يوجد نوعين:**

١. **القنبلة المنطقية:** عبارة عن برنامج صغير يتم إدخالها بطرق غير مشروعة ومخفية مع برامج أخرى وتهدف إلى تدمير وتغيير برامج ومعلومات النظام في لحظة محددة أو فترة زمنية منظمة بحيث تعمل على مبدأ التوقيت فتحدث تدميراً في المعلومات والبرامج عند أنجاز أمر معين في الحاسب أو برنامج معين.

٢. **القنبلة الزمنية:** سميت كذلك لقيامها بالعمل التخريبي في وقت يحدد سلفاً.

٩. الباركود وهو عبارة عن أدوات تستخدم لمسح الترميز الرقمي وفك شيفرة الرموز.

❖ خصائص الجرائم الإلكترونية

تتميز الجريمة الإلكترونية بعدة خصائص تميزها عن الجريمة التقليدية فلها طبيعة خاصة لا وجود لها في عالم الجرائم التقليدية، **ساعد ذلك في انتشار تقنية المعلومات والتطور التكنولوجي ما أضفى عليها مجموعة من الخصائص من أهمها:**

١. الجريمة الإلكترونية جريمة عابرة للحدود

تتسم غالباً بالطابع الدولي لأن الطابع العالمي لشبكة الإنترنت وما يترتب من جعل معظم دول العالم في حالة اتصال دائم على الخط يُسهل الجريمة من دولة إلى دولة أخرى فالجريمة الإلكترونية لا تعترف بالحدود بين الدول فهي تعتبر شكلاً جديداً من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم، إذ يُمكن من خلال النظام المعلوماتي ارتكاب العديد من الجرائم مثل تزوير وإتلاف المستندات الإلكترونية والاحتيال المعلوماتي وسرقة بطاقات الائتمان وغيرها، فهي جرائم لا يتم ارتكابها عبر المسافات حيث لا يتواجد المجرم على مسرح الجريمة، بل يرتكب جريمته عن بُعد، وهو ما يعني عدم التواجد المادي للمجرم الإلكتروني في مكان الجريمة ومن ثم تتباعد المسافات مما يزيد من صعوبة اكتشافها .

أي أن الجرائم الإلكترونية تتسم بأنها ذات طابع دولي ولذلك تعتبر من الجرائم الدولية، التي اتفق المجتمع الدولي بمُقتضى عهد دولي على أنها تُشكل عدوانا في كل دولة.

٢. صعوبة إثبات الجريمة الإلكترونية

لا تحتاج الجرائم الإلكترونية إلى أي عنف أو اقتحام لسرقة الأموال وإنما هي أرقام وبيانات تتغير أو تُمحى من السجلات المخزنة في الحاسبات الآلية ولأن هذه الجرائم لا تترك أي أثر خارجي مرئي لها وتكون في الخفاء فيصعب إثباتها وكذلك نتيجة إحجام مجتمع الأعمال عن الإبلاغ عنها تجنباً للإساءة إلى السمعة وهز الثقة في المنظمات والمؤسسات.

ويرجع صعوبة إثبات هذه الجرائم إلى العديد من الأسباب منها:

- ارتكابها من قبل شخص ذي دراية فائقة بها وينتج عن ذلك سهولة إخفاء معالم الجريمة والتخلص من أثارها.
- صعوبة الاحتفاظ الفني بأثارها أن وجدت.
- الحرفية المهنية العالية التي تتطلبها من أجل الكشف عنها.
- تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها.
- تعتمد على قمة الذكاء والمهارة في ارتكابها.
- يؤدي البُعد الزمني والبُعد المكاني والبُعد القانوني دوراً مهما في تشتيت جهود التحري لتعقب مثل هذه الجرائم.

٣. الجريمة الإلكترونية جريمة مُستحدثة

تُعد الجرائم الإلكترونية من أنواع الجرائم الجديدة التي يُمكن أن تُشكل أخطاراً جسيمة في ظل العولمة حيث إن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة بحيث يتجاوز هذا التقدم بقدراته وإمكانياته أجهزة الدولة الرقابية أضعف من قدراتها في تطبيق قوانينها بالشكل الذي أصبح يهدد أمنها وأمن مواطنيها.

٤. من حيث موضوع الجريمة

يختلف موضوع الجريمة الإلكترونية وفقا لحالتين:

الحالة الأولى

يجتمع فيها الجرائم التقليدية وجرائم المعلوماتية بمعناها الفني وحيث يكون موضوع الجريمة هو النظام المعلوماتي أي أن أحد المكونات المادية للنظام المعلوماتي كالأجهزة والمعدات والكابلات وإذا لم يكن ثمة أهمية للتقنية في ارتكاب الجريمة فتكون جريمة تقليدية كما هو الحال في سرقة أو إتلاف الحاسب أو شاشته إما إذا كأن موضوع الجريمة هو أحد المكونات غير المادية للنظام المعلوماتي كالبيانات والبرامج فتكون جريمة معلوماتية.

الحالة الثانية

يكون النظام المعلوماتي والحاسب هو وسيلة تنفيذ الجريمة وأدائها.

٥. عدم وجود مفهوم مشترك للجريمة الإلكترونية

تتميز الجريمة الإلكترونية بعدم وجود مفهوم مشترك لماهية الجريمة الإلكترونية وكذلك عدم وجود تعريف قانوني موحد لها بسبب عدم وجود تنسيق دولي في مجال الجريمة الإلكترونية ويرجع ذلك إلى عدم وجود معاهدات دولية ثنائية أو جماعية لمواجهة الجريمة الإلكترونية أو لاختلاف مفهوم الجريمة تبعاً لاختلاف النظم القانونية وهذا يتطلب إيجاد الوسائل المناسبة لتشجيع المجتمع الدولي لمواجهة الجرائم الإلكترونية والعمل على سن التشريعات الخاصة التي تواجه هذا النوع من الجرائم وإبرام المعاهدات التي تحث على تبادل المعلومات والخبرات وتسليم وتبادل المجرمين.

٦. قلة الإبلاغ عن الجريمة الإلكترونية

في الغالب لا يتم الإبلاغ عن جرائم الإنترنت إما لعدم اكتشاف الضحية لها وإما الخوف من التشهير، معظم جرائم الإنترنت تم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابها.

٧. جرائم متجددة دائمة التطور

الجرائم الإلكترونية تدور في فلك تقنية المعلومات والتكنولوجيا الحديثة ووجودها وتطورها مرتبط بوجود وتطور تكنولوجيا المعلومات ويترافق مع التطور الدائم والمتجدد لتقنية المعلومات والتكنولوجيا الرقمية تطور أساليب وطرق ارتكاب الجرائم الإلكترونية حيث يستغل المجرمون شبكة الإنترنت لتبادل المعلومات والأفكار والخبرات الإجرامية.

٨. جرائم غير عنيفة الأداء

فهي محصورة فقط في استهداف المعلومات والبيانات التي يتم بواسطتها الوصول للأموال والأشخاص فهي ليست ذات طبيعة مادية ملموسة.

❖ خصائص المجرم الإلكترونية

يتسم بخصائص معينة تميزه عن المجرم الذي يرتكب الجرائم التقليدية فإذا كأنت الجرائم التقليدية لا أثر فيها للمستوى العلمي والمعرفي للمجرم في عملية ارتكابها باعتبارها قاعدة عامة، فأن الأمر يختلف بالنسبة للجرائم الإلكترونية فهي جرائم فنية تقنية ومن يرتكبها يكون ذوي الاختصاص في مجال تقنية المعلومات أو على الأقل شخص لديه أدنى حد من المعرفة والقدرة على استخدام جهاز الحاسب والتعامل مع شبكة الإنترنت.

تختلف شخصية المجرم الذي يقوم بارتكاب الجرائم الإلكترونية عن شخصية المجرم الذي يرتكب الجرائم التقليدية فالجرائم الإلكترونية تحتاج إلى شخص على درجة عالية من العلم والثقافة على عكس الجرائم التقليدية، **مثل:**

١. الذكاء والمعرفة التقنية

يعتبر من أهم صفات مرتكب الجرائم الإلكترونية لأن ذلك يتطلب منه المعرفة التقنية لكيفية الدخول إلى أنظمة الحاسب الآلي والقدرة على التعديل والتغيير في البرامج وارتكاب جرائم السرقة والنصب وغيرها من الجرائم التي تتطلب أن يكون مرتكب الجريمة على درجة كبيرة من المعرفة والذكاء لكي يتمكن من ارتكاب تلك الجرائم.

٢. الاحتراف

هو مجرم محترف له من القدرات والمهارات التقنية ما يؤهله لأن يُوظف مهاراته في الاختراق والسرقة والنصب على حقوق الملكية الفكرية وغيرها من الجرائم مقابل المال.

فالأمر يقتضي كثيراً من الدقة والتخصص في هذا المجال للتوصل إلى التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الحاسب.

٣. الخبرة والمهارة

يتميز مرتكب الجريمة الإلكترونية بدرجة عالية من الخبرة و المهارة في استخدام التقنية المعلوماتية وذلك لأن مستوى الخبرة التي يكون عليها هي التي تحدد الأسلوب الذي يرتكب به تلك الجرائم بحيث إذا كأن الشخص مرتكب الجريمة على قدر قليل من مستوى الخبرة فجرائمه محدودة مثل جرائم إتلاف المعلومات أو محوها و نسخ البيانات أو البرامج ، إما الذي على مستوى مهارة عالي فأن أسلوبه للجرائم يختلف حيث يقوم عن طريق استخدام الشبكات بالدخول إلى أنظمة الحاسب الآلي وسرقة الأموال وارتكاب النصب وارتكاب جرائم التجسس وزرع الفيروسات وغيرها من الجرائم التي تتطلب مستوى مهاري وخبرة عالية في ارتكابها.

٤. غير عنيف

فهو ينتمي إلى إجرام الحيلة.

٥. لديه نزعة إجرامية

هذه النزعة الإجرامية تتكون نتيجة لتأثره بعوامل نفسية صاحبت نشأته وتظل طاقة كامنة إلى أن تظهر في شكل عمل إجرامي.

٦. لديه الدافع

وهو الرغبة في تحقيق الربح المادي بطريقة غير مشروعة ويظل هو الدافع الأول وراء ارتكاب الجريمة المعلوماتية أو الانتقام من صاحب العمل.

٧. يمتلك حب المخاطرة.

٨. يمتلك خيال نشط وحب انتحال الشخصيات.

٩. يمتلك الوسيلة

يراد بها الإمكانيات التي يحتاجها المجرم المعلوماتي لإتمام جريمته هذه الوسائل قد تكون في أغلب الأحيان، وسائل بسيطة وسهلة الحصول عليها خصوصاً إذا كأن النظام الذي يعمل به الحاسب من الأنظمة الشائعة، أما إذا كأن النظام من الأنظمة غير المألوفة، فتكون هذه الوسائل معقدة وعلى قدر من الصعوبة.

١٠. يمتلك المجرم المعلوماتي السلطة

يقصد بالسلطة الحقوق والمزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته، فكثير من مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة في اختراق المعلومات، وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات وأيضا قد تكون السلطة عبارة عن حق الجاني في الدخول إلى الحاسب الآلي وإجراء المعاملات، كما أن السلطة قد تكون شرعية وقد تكون غير شرعية كما في حالة سرقة شفرة الدخول الخاصة بشخص آخر.

❖ أنماط المجرم الإلكتروني

القراصنة الهواة

يقصد بهم الأشخاص الذي يستهدفون المعلومات والحسابات الآلية ويكونون من فئة الشباب البالغين ومعظمهم يكون من الطلبة، وبالتالي يقومون هؤلاء الأشخاص بالدخول إلى أنظمة الحاسب الآلي بطرق غير مصرّح لهم الدخول إليها، فَهُم بذلك يكسرون الحواجز الأمنية لأغراض عدّة منها الخبرة أو حتى الفضول.

- **مثل:** الأطفال أو المراهقون المستهترون: (Script Kiddies) : هم أشخاص غير مهرة ويقومون باختراق أجهزة الحاسب باستخدام برامج اختراق يحملونها من الإنترنت ويعتبرون من أخطر أنماط المجرمين لعدم درايته بما يفعل فهو لا يملك الإلمام الكافي بالتقنية.

القراصنة المحترفين

يقصد بهم الأشخاص التي تكون أعمارهم محصورة ما بين ٢٥-٤٥ سنة بحيث يحتلّون مكانة في المجتمع الجرائمي بالإضافة إلى اختصاصهم في مجال التقنية الإلكترونية؛ بحيث يتسمون بالخطورة وتكرارهم للجرائم مرة أخرى.

- **مثل:** القراصنة (Crackers) : هم الأشخاص الذين يخترقون أمن النظام ولديهم نوايا خبيثة، كذلك لديهم مهارة متقدمة بأجهزة الحاسب والشبكات والمهارات اللازمة لتدمير البيانات، وحرمان المستخدمين الشرعيين من الخدمة أو التسبب بمشاكل خطيرة على الأجهزة.

طائفة الحاقدين

يقصد بهم الأشخاص المنتقمون فمعظمهم يكونون ضد أصحاب العمل والمنشآت التي عملوا بها فهم يسعون إلى الانتقام من المدراء في العمل، بالإضافة إلى أن هذه الطائفة تكون أقل خطورة مقارنة بغيرها من الطوائف، يكمن الهدف وراء هذه الطائفة هو التعمد في إخفاء وأنكار الأفعال والأنشطة، التي يقومون بها مستخدمين تقنيات متخصصة في زراعة الفيروسات والبرامج المضرّة؛بهدف تخريب الأنظمة المعلوماتية، حيث إن هذه الطائفة لا تهدف إلى إثبات قدراتهم ومهاراتهم الفنية ولا أيضا يهدفون إلى تحقيق مكاسب مادية، أو حتى سياسية.

- **مثل:** الموظفون: (Employees) : من أكبر التهديدات الأمنية التي تهدد الشركات، فهم يقتحمون أجهزة شركاتهم **لعدة أسباب:** إما عرض الضعف الموجود في نظام الشركة أو لأهداف مادية أو لسخطهم من الشركة وتهديدهم عندما ينوي العودة للعمل في شركتهم.

طائفة الفكريين

فهم عبارة عن أشخاص يستعملون شبكة الإنترنت في نشر، بث، استقبال، أنشاء المواقع التي من شأنها تسهّل عملية الانتقال والترويج لكافة المواد الفكرية التي تساهم في تغذية الطرف الفكري , وقد يقوم المفكرين باستعمال الشبكات الإعلامية الإخبارية وكافة المواقع الإلكترونية بهدف تحقيق أغراض دعائية تحقق مصالحهم.

- **مثل:** الإرهابيون:(Cyber terrorists) : هم أشخاص متخصصون ولديهم مهارات عالية غالبا ما يهددون البنية التحتية لأجهزة الكمبيوتر والشبكات ليسببوا الذعر والمهاجمة من أجل نشر أفكارهم ومبادئهم، وقد يقوموا بنشر معلومات خاطئة وإشاعات كاذبة عن جهات معادية لهم، ويعتبر الإنترنت بحد ذاته من أهم أهدافهم.

طائفة المتجسسين

يقصد بهم الأشخاص الذي يسعون إلى التخريب أو إتلاف المحتويات الشبكية، التي تشكّل خطراً كبيراً، مثل إرسال أسرار العمل في إحدى الشركات عبر الإنترنت ومواقع التواصل الاجتماعي إلى الشركات المنافسة، فهي تهدف في المقام الأول على الحصول على قاعدة بيانات معلوماتية عن الأعداء والأصدقاء.

- **مثل** : المتجسسون:(Spies) : هم أشخاص يستهدفون أجهزة معينة ليس بشكل عشوائي ولذلك لسرقة معلومات معينة أو تدمير أجهزة معينة وغالباً ما تكون أهدافهم لأسباب مالية.

طائفة مخترقي الأنظمة

هؤلاء الأشخاص يقومون بتبادل المعلومات فيما بينهم؛ بهدف معرفة نقاط الضعف في الأنظمة المعلوماتية مستعملين بذلك النشرات الإعلامية الإلكترونية؛ من مثل مجموعات الأخبار وبالتالي يقومون هؤلاء الأشخاص بعقد وتولي المؤتمرات لجميع مخترقي الأنظمة المعلوماتية، مع أهمية وجود خبراء وذلك بهدف المشاركة والتشاور حول وسائل الاختراق وآلياتها.

السمات المشتركة للمجرم الإلكتروني

مجرم متخصص

يستغل مهاراته التقنية في اختراق الشبكات وكسر كلمات المرور والشفرات والحصول على البيانات والمعلومات المخزنة في الأجهزة من خلال الشبكات.

مجرم يعود الى الإجرام

لا يحقق جريمة الاختراق لهدف تحقيق مكاسب معينة، ولكن نتيجة شعوره بقدرته ومهارته في الاختراق.

مجرم محترف

له من القدرات والتقنيات ما يؤهله، لان يوظف مهاراته في الاختراق، والسرقة، والنصب، وغيرها.

مجرم ذكي

يمتلك من المهارات ما يؤهله للقيام بتعديل وتطوير في الأنظمة الأمنية حتى لا تستطيع أن تلاحقه وتتبع أعماله الإجرامية من خلال الشبكات أو داخل الأجهزة الحاسوبية.

❖ أهداف الجرائم الإلكترونية

- التمكن من الوصول إلى المعلومات بشكل غير قانوني كسرقة المعلومات أو حذفها والاطلاع عليها.
- التمكن من الوصول بواسطة الشبكة العنكبوتية إلى أجهزة الخوادم الموفرة للمعلومات وتعطيلها أو التلاعب ببياناتها.
- الحصول على المعلومات السرية للجهات المستخدمة للتكنولوجيا كالبنوك والمؤسسات والحكومات والأفراد والقيام بتهديدهم إما لتحقيق هدف مادي أو سياسي.
- الكسب المادي أو المعنوي أو السياسي غير المشروع مثل تزوير بطاقات الائتمان وسرقة الحسابات المصرفية.

- **أسباب الجريمة الإلكترونية**

مرتكبو الجريمة الإلكترونية يختلفون عن مرتكبي الجريمة التقليدية ويرجع ذلك لاختلاف الأشخاص من حيث السن و المستوى التعليمي وغير ذلك من المؤثرات الخارجية، كما أن الأسباب أو الدوافع التي تدفعهم لارتكاب الجريمة هي أيضا تختلف حيث أنها العوامل المحركة للإرادة التي توجه السلوك الإجرامي كالانتقام وكسب المال فهي القوة النفسية التي تدفع الإرادة لارتكاب الجريمة بهدف تحقيق غاية معينة ولذلك فأن الجريمة الإلكترونية تختلف عن الجريمة التقليدية فالأسباب والدوافع التي تدفع المجرمين للارتكاب الفعل غير المشروع لها تختلف عن الأسباب والعوامل التي تدفع المجرمين لارتكاب الفعل غير المشروع للجريمة التقليدية ويأتي في مقدمة أسباب ودوافع الجريمة الإلكترونية أسباب ودوافع تتمثل في الرغبة بجمع المعلومات التي قد تكون محفوظة في أجهزة الحاسب الآلي أو منقولة عبر الشبكة العالمية للمعلومات كما قد تكون الأسباب و الدوافع الرغبة في الإضرار بالغير من جهات معينة و أشخاص وكذلك الرغبة في الربح والكسب الذي قد يدفعه لاختراق الحواسيب ونظم المعلومات إضافة إلى الدوافع الشخصية لإبراز الذات التي قد تكون سببا في ارتكاب الجريمة الإلكترونية .

- **بعض تلك الأسباب**

١. الرغبة في جمع المعلومات وتعلمها

أولئك الذين يقدمون عليها بهدف الحصول على المعلومات الجديدة **مرتكز على مبدأين**:

- **الأول:** أن الدخول إلى الأنظمة يمكن أن يعلم كيف يسير العالم.
- **الثاني:** أن جمع المعلومات يجب أن يكون غير خاضع للقيود.

ومن وجهة نظرهم أن جمع المعلومات المفيدة بوجه عام يجب أن تكون غير خاضعة للقيود أي أن تتاح حرية نسخها وجعلها تتناسب مع استخدامات الأشخاص وهم يعلنون أن هدفهم من الوصول للمعلومات ودخولهم للشبكات والحواسيب هو التعلم فقط فهم يتعاونون في البحث على شكل جماعات ويتقاسمون المعلومات والخبرات التي يحصلون عليها ويستفيدون منها في أنشطة هادفة ولو بطرق غير مشروعة.

٢. الاستيلاء على المعلومات

الإقدام على ارتكاب هذا الجرم بواسطة تقنية المعلومات بهدف الحصول على المعلومة ذاتها والاستيلاء عليها والتصرف فيها يتمثل في الحصول على المعلومة المحفوظة في الحاسب الآلي، أو المنقولة، أو تغييرها، أو حذفها، أو إلغائها نهائياً من النظام ويختلف الدافع لهذا التصرف فقد يكون الدافع تنافسي أو سببه الابتزاز أو الحصول على مزايا ومكاسب اقتصادية وغالباً ما يكون هدف هذه الجرائم ذو طابع سياسي أو اقتصادي.

٣. قهر النظام وإثبات التفوق على تطور وسائل التقنية

في بعض الأحيان يكون الدافع وراء ارتكاب هذه الجرائم هو قهر النظام وإثبات قدرة الجاني وتفوقه على تعقيدات وتطور وسائل التقنية الحديثة حيث يمضي كل وقته أمام شاشات أجهزته لكسر الحواجز الأمنية للأنظمة الإلكترونية واختراقها ليثبت براعته في القدرة على تحدي دول متعددة دون الاهتمام بأية حدود دولية.

٤. إلحاق الأذى بأشخاص أو جهات

بعض المجرمين الذين يقدمون على ارتكاب الجريمة عبر شبكات المعلومات العالمية وتقنية المعلومات بصورة عامة يتركز الدافع من ورائها على إلحاق الأذى بأشخاص محددين أو جهات معينة وغالباً ما تكون تلك الجرائم مباشرة تتمثل في صورة ابتزاز أو تهديد أو تشهير.

كما يمكن أن تكون هذه الجرائم غير مباشرة وتتمثل في الحصول على البيانات والمعلومات الخاصة بتلك الجهات أو الأشخاص لاستخدامها فيما بعد في ارتكاب جرائم مباشرة.

٥. تحقيق أرباح ومكاسب مادية

هناك بعض الجرائم الإلكترونية يكون الدافع منها تحقيق أرباح ومكاسب مادية كاستخدام شبكة الإنترنت للإعلان عن صفقات تجارية غير مشروعة.

٦. تهديد الأمن القومي والعسكري

بعض الجرائم الإلكترونية الهدف منها أسباب ودوافع سياسية كتهديد الأمن القومي والعسكري ومن ذلك ظهر ما يعرف بالتجسس الإلكتروني والإرهاب الإلكتروني والحرب المعلوماتية كما هو حادث بين الدول المتقدمة الكترونياً.

❖ دوافع الجرائم الإلكترونية

دوافع مادية

تحقيق الكسب المادي تعد الرغبة في تحقيق الثراء من العوامل الرئيسية لارتكاب الجريمة عبر الأنترنت.

دوافع شخصية

الرغبة في التعلم يكرس مرتكبو هذه الجريمة وقتهم في تعلم كيفية اختراق المواقع الممنوعة والتقنيات الأمنية للأنظمة الحاسوبية.

دوافع ذهنية أو نمطية

غالبا ما يكون الدافع لدى مرتكب الجرائم عبر الإنترنت هو الرغبة في إثبات الذات وتحقيق الانتصار على تقنية الأنظمة المعلوماتية دون أن يكون لهم نوايا تخريبية.

دوافع انتقامية

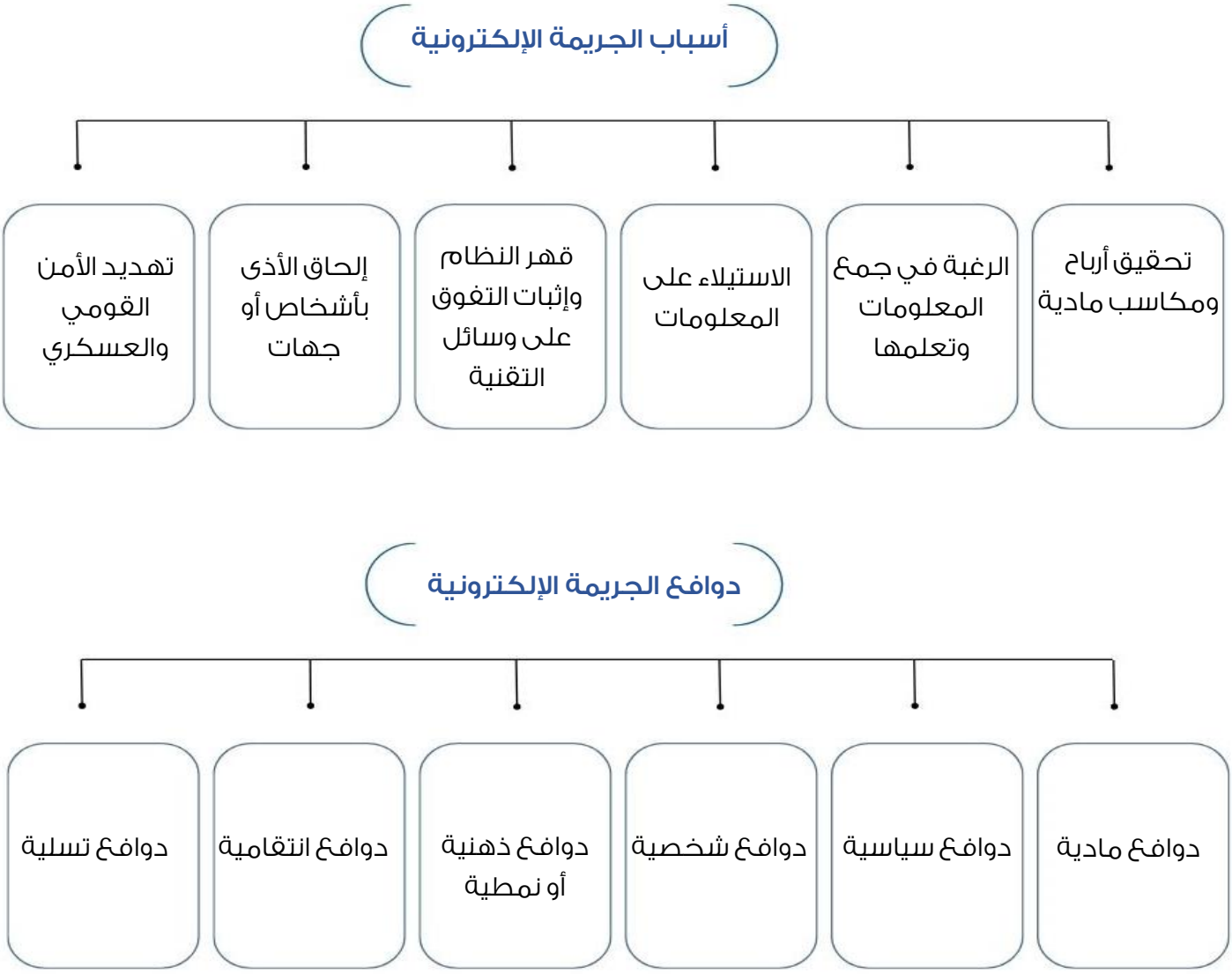
تعد من أخطر الدوافع التي يمكن أن تُفيد شخص يملك معلومات كبيرة عن المؤسسة أو شركة يعمل بها تجعله يقدم على ارتكاب جريمته.

دافع التسلية

هي جريمة ترتكب من أجل التسلية لا يقصد من ورائها إحداث جرائم.

دافع سياسي

يتم غالبا في المواقع السياسية المعادية للحكومة، ويتمثل في تغليق الأخبار والمعلومات، تعد الدوافع السياسية من أبرز المحاولات الدولية لاختراق شبكات حكومية في مختلف دول العالم.



شكل (١) خريطة مفاهيم لأسباب الجريمة الإلكترونية و دوافعها

١. **اختار الإجابة الصحيحة فيما يلي:**

١- **الأشخاص الذي يسعون إلى التخريب أو إتلاف المحتويات الشبكية، التي تشكّل خطراً كبيراً :**

- ● طائفة المتجسسين
- ○ طائفة الحاقدين
- ○ طائفة الفكريين
- ○ طائفة الهواة

٢- **من خصائص المجرم الالكتروني :**

- ○ عنيف
- ○ لبق
- ○ مسالم
- ● الخبرة والمهارة

٣- **من السمات المشتركة للمجرم الالكتروني :**

- ○ ذو سلطة
- ● محترف
- ○ كبير بالسن
- ○ اجتماعي

٢. **ضع علامة (✓) أمام العبارات الصحيحة وعلامة (✗) أمام العبارات الخاطئة:**

١.	الجريمة الإلكترونية هي : مجرم محترف له من القدرات والمهارات التقنية ما يؤهله لأن يُوظف مهاراته في الاختراق والسرقة والنصب على حقوق الملكية الفكرية وغيرها من الجرائم مقابل المال.	✗
٢.	مرت الجريمة الإلكترونية في خمس مراحل تاريخية.	✗
٣.	تهديد الأمن القومي والعسكري من أسباب الجريمة الإلكترونية.	✓
٤.	الدافع العائلي من دوافع الجريمة الإلكترونية.	✗
٥.	الكسب المادي أو المعنوي أو السياسي من اهداف الجرائم الإلكترونية.	✓
٦.	الهندسة الاجتماعية من أدوات الجرائم الإلكترونية.	✓
٧.	من خصائص الجريمة الإلكترونية أنها قديمة.	✗

الفصل الثاني

جرائم الإنترنت

في هذا الفصل سوف نتعرف على المواضيع التالية:

- مفهوم جرائم الإنترنت
- بروتوكولات الإنترنت
- مسميات جرائم الإلكترونية وتصنيفها
- مزايا الإنترنت وعلاقتها بالجرائم الإلكترونية
- دور الحاسب في الجرائم الإلكترونية

❖ مفهوم جرائم الإنترنت

جرائم الإنترنت هي امتداد لما عرف بجرائم الحاسوب ، والمقصود بجرائم الحاسوب: كل عمل إجرامي ـ غير قانوني يرتكب باستخدام الحاسوب كأداة أساسية، ودور الحاسوب في تلك الجرائم قد يكون هدفاً للجريمة أو أداة لها ، وعندما ظهرت شبكة الإنترنت ودخلت جميع المجالات كالحاسوب، بدء من الاستعمال الحكومي ثم المؤسساتي والفردي، كوسيلة مساعدة في تسهيل حياة الناس اليومية ، انتقلت جرائم الحاسوب لتدخل فضاء الإنترنت كأداة أساسية ، وكما هو الحال في جرائم الحاسوب، كذلك جرائم الإنترنت قد تكون الإنترنت هدفاً للجريمة أو أداة لها.

والمقصود بجرائم الإنترنت ، المسماة أيضا الجرائم السيبرانية ، هو أي نشاط غير مشروع ناشئ في مُكوّن أو أكثر من مكونات الإنترنت، مثل مواقع الإنترنت، وغرف المحادثة، أو البريد الإلكتروني، ويمكن أن تشمل أيضا أي أمر غير مشروع، بدء من عدم تسليم البضائع أو الخدمات، مروراً باقتحام الحاسب (التسلل إلى ملفات الحاسب)، وصولاً إلى انتهاك حقوق الملكية الفكرية، والتجسس الاقتصادي (سرقة الأسرار التجارية)، والابتزاز على الإنترنت، وتبييض الأموال الدولي، وسرقة الهوية، وقائمة متنامية من الجرائم الأخرى التي يُسهلها الإنترنت.

أن جرائم الإنترنت هي جزء من الجرائم المرتكبة بواسطة الحاسب أو التي يكون الحاسب محلاً لها ، فكل جرائم الإنترنت تستلزم وجود جهاز الحاسب للاتصال بالشبكة ، في حين لا تعد كل جرائم الحاسب هي جرائم الإنترنت ، فقد ترتكب جرائم على جهاز الحاسب دون استعمال الشبكة و دون أن يكون موصولا بها ، ولقد ذهب الكثير من الفقهاء لاعتبار جرائم الحاسب أو الجرائم المرتبطة مختلفة عن الجرائم التقليدية ، من بينهم الفقيه الألماني الريش زيبر والأمريكي باركي وهما أول من بحث و كتب حول الظاهرة ، ويريان أن الإنترنت ما هو إلا جزء من النظام المعلوماتي ، المتمثل في الحاسب و أصبح مصطلح جرائم الكمبيوتر و الإنترنت هو الأكثر استعمالا ، للدلالة على هذه الجرائم ، كما استعمل مصطلح جرائم الإنترنت – Internet crimes – في مؤتمر جرائم الإنترنت المنعقد في أستراليا ١٩٩٨ ، كاصطلاح يصلح للجرائم التي يكون الإنترنت عنصر من عنصرها ، لتمييزها عن الجرائم التي يعرفها عالم المعلوماتية.

جرائم الإنترنت هيً أفعال تتم باستخدام أو عبر شبكة الإنترنت، مخالفة للكانون والتنظيمات المعمول بها وتلحق أضرار بنظام المعلومات، أو بالأموال، أو الأشخاص، أو النظام العامً وبذلك يمكن إخضاعها للنصوص التقليدية أمام قصر القوانيين التي تحمي المعلوماتية وتجرم كل ما يمكن أن يعد فعل غير مشروع يرتكب من خلال شبكة الإنترنت ويلحق أضرار للغير سواء في شخصه أو ماله، تتناسب مع طبيعة وخصوصية هذه الجرائم .

- **خصائص جرائم الإنترنت**

تعتبر الجرائم التي ترتكب من خلال شبكة الإنترنت، جرائم ذات خصائص منفردة، لا تتوافر في الجرائم التقليدية، سواء من حيث أسلوب وطرق ارتكابها أو الشخص مرتكبها، **وتعددت هذه الخصائص والمميزات، فيرى الدكتور مراد عبد الفتاح، أنها جرائم تتسم بكونها:**

- **أولا :** عالمية لا تعترف بالحدود الجغرافية كونها تقع عبر حدود دولية كثيرة.
- **ثانيا:** صعبة المتابعة والاكتشاف لأنها لا تترك أثر كونها مجرد أرقام كما تفوق معلومات المحقق التقليدية، **ويرى الأستاذان منير محمد الجنبيهي وممدوح محمد الجنبيهي أن لجرائم الإنترنت أربع خصائص:**

١. الحاسب الآلي هو أداة ارتكابها، فلا يمكن ارتكاب أي جريمة على شبكة الإنترنت الا وكأن جهاز الحاسب وسيلة ارتكابها، وهذا ما يميزها عن باقي الجرائم.

٢. ترتكب عبر شبكة الإنترنت، فتعتبر شبكة الإنترنت أنها حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم، كالبنوك، الشركات وغيرها.

٣. مرتكب جرائم الإنترنت هو شخص ذو خبرة فائقة في مجال الحاسب الآلي، فحتى تقع جريمة الإنترنت يجب أن يكون الفاعل متمكن من التقنية ومتمتع بالدراية العالية لاستخدام الحاسب الآلي، فالكثير من الجرائم، اكتشف أن فاعليها من خبراء الحاسب الآلي.

٤. هي جريمة لا حدود جغرافية لها، تقع جرائم الإنترنت متخطية حدود الدولة التي ارتكبت فيها ويمكن أن ترتب أثارها عبر كافة دول العالم.

أن جرائم الإنترنت تعتبر تهديد مباشراً أو غير مباشر لتقدم البشرية بواسطة أعمال إجرامية يقوم بها أشخاص يسيئون استخدام التكنولوجيا الحديثة ، وهذه الجرائم تتسم بالصعوبة والتعقيد ، كما أن ملاحقة مرتكبيها لا تكاد تخلو من الصعوبات كونهم يتصفون ،بصفات تميزهم عن مرتكبي الجرائم التقليدية ، وذلك لكونهم عادة من ذوي المكانة في مجتمعهم ويتمتعون بقدر كاف من العلم ، بسبب ما تتطلبه هذه الجرائم من إلمام بمهارات ومعارف في مجال الحاسب الآلي والإنترنت ، وغالبا ما يكونوا من المتخصصين في هذا المجال ومعتادي الأجرام خاصة في هذا النوع من الأجرام وعلى قدر من الذكاء مصحوب باحتراف في مجال المعلوماتية ومتكيف مع المجتمع .

❖ بروتوكولات الإنترنت

١. بروتوكول التحكم في الإرسال (TCP)

Transmission Control Protocol (TCP) أو بروتوكول التحكم في الإرسال هو بروتوكول اتصال شائع يستخدم للتواصل عبر الشبكة، كما يقسّم أي رسالة إلى سلسلة من الحزم التي يتم إرسالها من المصدر إلى الوجهة وهناك يتم إعادة تجميعها في الوجهة موصُوف بالوثيقة، أي يُؤمن نقلاً موثوقاً خالياً من الأخطاء لدفق من البايتات بين مُضيفين يتصلان مع بعضهما البعض عبر شبكة تدعم بروتوكول الإنترنت.

٢. بروتوكول الإنترنت (IP)

بروتوكول الإنترنت هو بروتوكول الاتصال الأساسي في حزمة بروتوكولات الإنترنت ويُشكّل الأساس الذي تعتمد عليه عمليّة توجيه الرزم ضمن الشبكة، ويسمح ذلك بالاتصال بين الشبكات المُختلفة، وهذا هو جوهر شبكة الإنترنت.

تم تصميم بروتوكول الإنترنت Internet Protocol (IP) بشكل صريح كبروتوكول عنونة، كما أنه يتم استخدامه في الغالب مع بروتوكول TCP تساعد عناوين IP في الحزم على توجيهها عبر عقد Nodes مختلفة في الشبكة حتى تصل إلى النظام الوجهة TCP / IP هو البروتوكول الأكثر شيوعاً الذي يربط بين الشبكات.

٣. بروتوكول مخطط بيانات المستخدم (UDP)

User Datagram Protocol (UDP) هو بروتوكول اتصال بديل لبروتوكول التحكم في الإرسال، كما يتم تنفيذه بشكل أساسي لأنشاء ارتباط يتسامح مع زمن الانتقال المنخفض بين التطبيقات المختلفة.

تناقل البيانات باستعمال UDP أسرع لأنه لا يتحقق من صحة المعلومة لأنه إذا أراد التحقق من صحة المعلومة يحتاج إلى إرسال المزيد من المعلومات للتحقق من صحة النقل وهذا يزيد من حجم البيانات المرسلة ويؤدي إلى زيادة الوقت المستغرق في التراسل ولهذا جعلت مسؤولية التحقق من الإرسال من مسؤولية البرنامج نفسه.

٤. بروتوكول مكتب البريد(POP)

تم تصميم بروتوكول Post office Protocol (POP) لتلقي رسائل البريد الإلكتروني الواردة.

٥. بروتوكول نقل البريد البسيط (SMTP)

تم تصميم بروتوكول Simple mail transport Protocol (SMTP) لإرسال البريد الإلكتروني الصادر وتوزيعه.

٦. بروتوكول نقل الملفات(FTP)

يتيح File Transfer Protocol (FTP) للمستخدمين نقل الملفات من جهاز إلى آخر، كما قد تتضمن أنواع الملفات ملفات البرامج وملفات الوسائط المتعددة والملفات النصية والمستندات وما إلى ذلك.

٧. بروتوكول نقل النص التشعبي (HTTP)

تم تصميم بروتوكول نقل النص التشعبي Hyper Text Transfer Protocol (HTTP) لنقل نص تشعبي بين نظامين أو أكثر، تستخدم علامات HTML لأنشاء الروابط، قد تكون هذه الروابط بأي شكل مثل النص أو الصور، تم تصميم HTTP وفقاً لمبادئ خادم العميل والتي تسمح لنظام العميل بأنشاء اتصال بجهاز الخادم لتقديم طلب يقر الخادم بالطلب الذي بدأه العميل ويستجيب وفقاً لذلك.

٨. بروتوكول نقل النص التشعبي الآمن (HTTPS)

بروتوكول Hyper Text Transfer Protocol Secure (HTTPS) هو بروتوكول قياسي لتأمين الاتصال بين جهازي حاسوب، أحدهما يستخدم المتصفح والآخر لجلب البيانات من خادم الويب، يتم استخدام HTTP لنقل البيانات بين متصفح الويب لدى العميل (الطلب) وخادم الويب (الاستجابة) بتنسيق النص التشعبي، كما هو الحال في حالة HTTPS فيما عدا أن نقل البيانات يتم بتنسيق مشفر، لذلك يمكن القول أن https تمنع المتسللين من مشاهدة أو تعديل البيانات طوال عملية نقل الحزم.

٩. بروتوكول Telnet

بروتوكول Telnet عبارة عن مجموعة من القواعد المصممة لربط نظام بآخر، عملية الاتصال هنا تسمى تسجيل الدخول عن بعد، النظام الذي يطلب الاتصال هو الحاسوب المحلي، والنظام الذي يقبل الاتصال هو الحاسوب البعيد.

١٠. بروتوكول غوفرGopher

هو عبارة عن مجموعة من القواعد المطبقة للبحث والاسترجاع، وكذلك عرض المستندات من المواقع المعزولة كما يعمل Gopher أيضا على مبدأ العميل / الخادم.

- **أنواع بروتوكولات الإنترنت الأخرى**

تعمل بعض البروتوكولات الشائعة الأخرى كبروتوكولات مشتركة مرتبطة بهذه البروتوكولات الأساسية للأداء الأساسي وهي:

- بروتوكول تحليل العنوان ARP (Address Resolution Protocol)
- بروتوكول التكوين الديناميكي للمضيف DHCP (Dynamic Host Configuration Protocol)
- بروتوكول الوصول إلى الرسائل عبر الإنترنت IMAP4 (Internet Message Access Protocol)
- بروتوكول بدء الجلسة SIP (Session Initiation Protocol)
- بروتوكول النقل في الوقت الفعلي RTP (Real-Time Transport Protocol)
- بروتوكول موقع الموارد RLP (Resource Location Protocol)
- بروتوكول الوصول إلى الطريق RAP (Route Access Protocol)
- بروتوكول نفق الطبقة الثانية L2TP (Layer Two Tunnelling Protocol)
- بروتوكول الاتصال النفقي من نقطة إلى نقطة PPTP (Point To Point Tunnelling Protocol)
- بروتوكول إدارة الشبكة البسيط SNMP (Simple Network Management Protocol)
- بروتوكول نقل الملفات البسيط TFTP (Trivial File Transfer Protocol)

❖ مسميات الجرائم الإلكترونية وتصنيفها

- **أولا: مسميات الجرائم الإلكترونية**

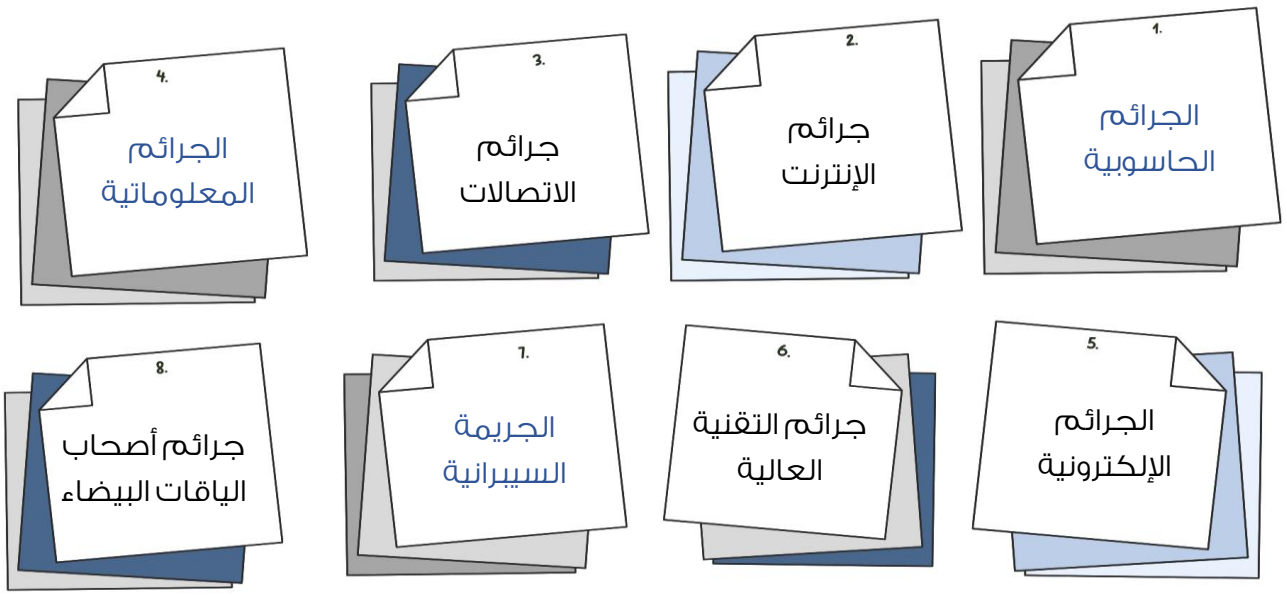
لقد مرت الجريمة الإلكترونية نتيجة للتدرج في الظاهرة الإجرامية الناشئة عن بيئة الحاسب الآلي بعدة مصطلحات ابتداء من إساءة استعمال الحاسوب مروراً باصطلاح احتيال الحاسوب ثم اصطلاح الجريمة المعلوماتية فاصطلاح جرائم الحاسب والجريمة المرتبطة بالحاسب ثم جرائم التقنية العالية وجرائم المخترقين وأخيراً جرائم الإنترنت.

الجرائم الناشئة عن الاستخدام الغير مشروع لشبكة الإنترنت على المعلومة بشكل رئيسي وهذا الذي أدى إلى إطلاق مصطلح الجريمة المعلوماتية على هذا النوع من الجرائم.

وعرف نظام الجريمة الإلكترونية السعودي في المادة الأولى منه بأنها أي فعل يرتكب متضمناً استخدام الشبكة المعلوماتية بالمخالفة لأحكام نظام الجرائم المعلوماتية.

مُعظم الجرائم الإلكترونية تُرتكب ضمن نطاق المُعالجة الإلكترونية للبيانات أو النصوص، لذلك فطابع الأدلة في الجريمة المعلوماتية ذو طبيعة رقمية لا طبيعة مادية، ويصعب إثباتها بالطرق التقليدية.

ونظراً لتعدد وتنوع أنماط وصور الجرائم الإلكترونية فقد أسهم ذلك في ظهور مسميات لها تتناسب مع طبيعتها وشكلها والأدوات المستخدمة فيها مثل:



- **تسمية الجريمة الإلكترونية في الفقه**

لم يتفق الفقه الجنائي على تسمية موحدة للجريمة الإلكترونية إذ يطلق عليها البعض منهم الجريمة الإلكترونية وهناك من يسميها الجريمة المعلوماتية ويذهب أخرون إلى تسميتها بجرائم إساءة استخدام تكنولوجيا المعلومات والاتصال ويطلق عليها أخرون مسمى جرائم الكمبيوتر والإنترنت.

إيجاد تعريف للجريمة الإلكترونية كأن محلاً لاجتهادات الفقهاء فقد ذهبوا في ذلك مذاهب مختلفة ووضعوا تعريفات شتى وبالتالي لا يوجد تعريفاً محدداً للجريمة الإلكترونية ويوجد اختلاف بين الباحثين في تعريف الجريمة الإلكترونية فمنهم من يتناول التعريف من الجانب التقني أي فنياً ومنهم من يتناوله من الزاوية القانونية.

من الناحية الفنية: هو نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود.

أما أنصار الاتجاه القانوني فيذهبون إلى أن تعريف الجرائم الإلكترونية يتطلب تعريف المفردات الضرورية المتعلقة بارتكاب جرائم الحاسب الآلي **وهي:** الحاسب الآلي – برنامج الحاسب الآلي – البيانات – الممتلكات – الدخول – الخدمات– الخدمات الحيوية.

وفريق أخر من الفقهاء يعرف جريمة الحاسب الآلي أو الجريمة الإلكترونية بأنها الجريمة التي تقع بواسطة الحاسب الآلي أو عليه أو بواسطة شبكة الإنترنت.

ويرى أنصار الجانب الفقهي بأن هذه الجريمة تتسم بالسرعة وتطور وسائل ارتكابها وينعدم فيها العنف ضد الأنسان بالمقارنة مع الجرائم التقليدية أثناء تنفيذها وهي عابرة للحدود ومن سماتها أيضا أن أدلتها سهلة الإتلاف كما أن الجهات التي تتولى تعقبها والتحقيق فيها تواجه صعوبات وتعقيدات كثيرة وتنقصها أحيانا الخبرة وعدم كفاية القوانيين الخاصة بمعالجتها.

وهناك من يأخذ على هذا التعريف قصوره في عدم الإشارة إلى بيئة وقوع الجريمة الإلكترونية وهي الشبكة العالمية للمعلومات الإنترنت كما هو الحال عند تعطيل الشبكة عن العمل أو العمل على إبطاء سرعتها أو إتلاف المواقع عليها.

واتجاه أخر من الفقه يتخذ وسيلة ارتكاب الجريمة كأساس لوضع التعريف للجريمة الإلكترونية كما هو الحال عند الفقيه الألماني تاديمان الذي عرفها بأنها هي كل أشكال السلوك غير المشروع أو الضار بالمجتمع والذي يرتكب باستخدام الحاسب الآلي.

وفي نفس الاتجاه عرفت بأنهاً الجرائم التي يكون قد وقع في مراحل ارتكابها بعض عمليات فعلية داخل نظام الحاسوب وبعبارة أخرى هي تلك الجرائم التي يكون دور الحاسوب فيها إيجابياً أكثر منه سلبياً، كذلك تعرف بأنها ً كل نشاط إجرامي يؤدي نظام الحاسب الآلي فيه دوراً لإتمامه على أن يكون هذا الدور على قدر من الأهمية.

وهناك اتجاه أخر من الفقه يركز على الجانب الموضوعي في تعريفه للجريمة الإلكترونية فيرى أن الجريمة الإلكترونية لا يكفي لإطلاق هذا الوصف عليها بمجرد استخدام الحاسب الآلي فيها، ولكن يشترط أن يقع الفعل داخل نظام الحاسب الآلي لاحتسابها جريمة إلكترونية ولذلك عرفوا الجريمة الإلكترونية بأنها نشاط غير مشروع لنسخ أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي ترسل عن طريقه كما عرفوها بأنها غش معلوماتي ينصرف إلى كل سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها.

وفريق أخر من الفقه يركز على الجانب المعرفي لا على الوسيلة أو الموضوع – للجريمة الإلكترونية وذلك لكونها مرتبطة بالجوانب المعرفية الفنية أو المعرفة باستخدام الحاسب الآلي.

ولذلك عرف أنصار هذا الاتجاه الجريمة الإلكترونية بأنها جريمة يكون متطلباً لاقترافها أن تتوفر لدى فاعلها معرفة بتقنية الحاسب الآلي كما عرفها الدكتور هشام فريد رستم بأنها أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه.

كما عرفت في نفس الاتجاه بأنها كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها، وقد أنتقد هذا التعريف حيث يرى منتقدوه بأنه يوسع من نطاق الجريمة الإلكترونية لأنه ساوى بين السلوك غير المشروع قانوناً والمعاقب عليه والسلوك الذي يستحق اللوم أخلاقياً فقط.

يرى جانب من الفقه أن الجرائم التي لها ارتباط بالمعلومات هي ذاتها التي تسمى الغش المعلوماتي وهذه يقصد بها كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع للتقنية المعلوماتية.

وقد عرفها الفقيه الفرنسي Masse بأنها هي كل سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها بغرض تحقيق ربح.

- **ثانيا: تصنيف الجرائم الإلكترونية**

قسم الفقهاء ودارسو الجرائم الإلكترونية إلى فئات متعددة تختلف حسب الأساس والمعيار الذي يستند إليه تقسيم المعنى.

- **تصنيف الجرائم الإلكترونية حسب نوع المعلومات ومحل الجريمة**

تنقسم إلى:

١. **الجرائم الماسة بقيمة معلومات الحاسب وتنقسم إلى فئتين:**

- الفئة الأولى: الجرائم الواقعة على ذات المعلومات

كإتلاف البيانات والمعلومات وإتلاف برامج الحاسب ذاتها بما في ذلك استخدام الفيروسات.

- الفئة الثانية: الجرائم الواقعة على ما تمثله هذه المعلومات

جرائم واقعة على الأموال والأصول كجرائم غش الحاسب التي تستهدف الحصول على المال أو جرائم الإتجار بالمعلومات وجرائم التلاعب بالمعلومات المخزنة داخل الحاسب واستخدامها دون وجه حق كتزوير المعالجة الآلية واستخدامها.

٢. **الجرائم الماسة بالمعلومات الشخصية والبيانات المتصلة بالحياة الخاصة**

تشمل هذه الفئة الهجوم على المعلومات والبيانات المتعلقة بالحياة الخاصة وتُعد هذه الجرائم من أخطر الصور لأنها تحتوي على استغلال المعلومات المخزنة في الحاسب في أمور غير مشروعة، وقد تأخذ هذه الجرائم صورة أو تسجل المحادثات الخاصة في وسائط الاتصال وتتنصت عليها واستغلالها في التشهير لأن معظم الأفراد تكون بياناتهم مُخزنة في المؤسسات وسرقتها تُعد من الجرائم التي تمس الحياة الخاصة ولا يشترط القانون في بعض الدول أن تكون هذه البيانات حقيقية.

٣. **الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسب ونظمه**

تشمل نسخ وتقليد البرامج وإعادة إنتاجها دون ترخيص وتتميز عن باقي الفئات بأنها محلها هو البرامج فقط والاستخدام غير المشروع لها.

- **تصنيف الجرائم الإلكترونية حسب مساسها بالأفراد والأموال**

وتنقسم إلى:

١. جرائم تستهدف الأفراد مثل الملاحقة عبر الوسائل الإلكترونية، نشر المعلومات المزيفة / التسبب بالوفاة وأنشطة البريد الإلكتروني غير المرغوب فيه.

٢. جرائم تستهدف الأموال أي الاقتحام أو الدخول غير المصرح به خلال شبكة المعلومات.

٣. جرائم الاحتيال والسرقة مثل استخدام البطاقات الائتمانية بعد سرقة أرقامها.

٤. جرائم التزوير مثل تزوير البريد الإلكتروني الخاص بالفرد أو مؤسسة معينة أو تزوير للوثائق والسجلات وتزوير الهوية.

- **التصنيف حسب التنفيذ**

فردي – جماعي

يكون المجرم فرداً وبدوافعه الشخصية ايضاً يقوم بمهاجمة أو التعرض لمجموعة أفراد في نفس الوقت كأن يهاجم منظمة أو مؤسسة أو شركة وذلك بهدف الانتقام أو التشهير أو لأي سبب كأن.

جماعي – فردي

يكون المهاجمون جماعة تتكون من أكثر من فرد يقومون بأعمال تخريبية أو تجسسية أو أي نوع من أنواع الجرائم المعلوماتية ويكون الهدف بالنسبة لها فرداً واحداً كأن يقوموا جميعاً بإرسال رسائل متكررة إلى بريد شخص بذاته أو التآمر للدخول على موقعه في نفس الوقت مما يسبب له الدمار والخراب.

جماعي – جماعي

يقوم عدة أشخاص بمهاجمة موقع جهات ذات شخصيات اعتبارية كالمنظمات والهيئات والشركات وغيرهم بهدف القيام بأي عمل تخريبي أو التجسس على معلومات تلك المنظمات والهيئات.

- **خامساً: التصنيف حسب النوع**

التسلل والتجسس

يوجد فئة من الأفراد يحبون التجسس على الآخرين بطرق مختلفة من استرقاق السمع إلى تركيب أجهزة التصنت صوتية ومرئية إلى ابتكار طرق بأساليب حديثة للدخول بها إلى أجهزة الحاسب الآلي الخاصة بالشخص المستهدف للحصول على أكبر معلومات ممكنة.

الإتلاف والتدمير

استطاعة شخص ما الدخول إلى جهاز شخص أخر وإتلاف محتوياته وتدميرها وحذفها أو نقلها إلى مكان أخر داخل هذا الجهاز أو خارجه، حسب نوع تلك الوثائق وأهميتها التي ممكن أن يحصل عليها فهو يسعى إلى معلومات مالية أو أسرار حربية للاستفادة منها أو تخريبها.

التغيير والتزوير

يقوم بها شخص له أهداف مريبة، أتاحت له الفرصة لتغيير الحقائق والوثائق وتواريخ المستندات الموجودة على ذلك الجهاز وتغيير البيانات والصور والأشخاص الموجودين في هذه الصور لاستخدامها لأهداف التشهير وتشويه السمعة وبالمثل ملفات الفيديو.

الخداع والتغرير

بسبب تطور التقنية والبرامج الحاسوبية التي أسيء استخدامها من قبل ضعاف النفوس حيث إنه باستخدام البرامج الاحترافية يستطيع الشخص الحصول على صور محسنة غير الصور الحقيقية وإخفاء العيوب منها ومن مظاهر الخداع هو تقمص شخصية غير الشخصية الأساسية وخاصةً بعض البرامج تغير الصوت.

❖ مزايا الإنترنت وعلاقتها بالجرائم الإلكترونية

العصر الحال هو عصر تقنية المعلومات والاتصالات والتي تعتبر أهم دعائم وأسس تقدم الدول وتطورها وتحقيق الاستقرار الاقتصادي ولذلك سارعت المنظمات التقليدية إلى التحول إلى منظمات إلكترونية تستخدم الإنترنت في أنجاز كل معاملاتها وأعمالها الإدارية بواسطة التبادل غير المادي للبيانات الرقمية وفيما وبين المؤسسات الأخرى والمؤسسات الحكومية وذلك لتسهيل الحصول على البيانات والمعلومات لاتخاذ القرارات المناسبة وتقديم الخدمات للمستفيدين بكفاءة وفاعلية وبأقل تكلفة وبأسرع وقت ممكن.

ولقد وفرت السهولة النسبية لاستخدام التقنية الجديدة والحصول على الإنترنت على نحو متزايد أكثر عن طريق الاشتراك بأسعار معقولة والحصول على أجهزة الحاسب مع أجهزة المودم فائقة السرعة كل ذلك يمكن الأفراد من التواصل وتكوين الصداقات الجديدة والتجارة والترفيه والتعليم والقيام بأعمال تجارية ودفع الفواتير عبر الإنترنت وكونت شبكة ويب عالمية ما يسمى العالم الافتراضي أو الفضاء الإلكتروني والذي يعرف بأنه ً مكان لأجل غير مسمى حيث يتفاعل الأفراد والمجتمعات مما أتاح الكثير من الأفراد الانتقال من العالم الواقعي إلى العالم الافتراضي مما أدى إلى ظهور الجريمة فهي ظاهرة اجتماعية يحاول المجرمون اليوم الاستفادة من تكنولوجيا المعلومات والاتصالات في ارتكاب الجريمة ولهذا ظهرت أنماط جديدة من الجرائم لم تكن موجودة من قبل تتسم بصعوبة اكتشافها وملاحقتها , حيث أنه رغم الفوائد المتعددة للحكومة و الإدارة الإلكترونية إلا في نفس الوقت تزايدت أساليب إساءة الاستخدام لمكوناتها وأصبح الحاسب الآلي بشكل عام وشبكة الإنترنت بشكل خاص أدوات أو محل ارتكاب الجريمة بمفهومها الحديث ومكنت مجرمي الفضاء الإلكتروني تصفح الإنترنت و ارتكاب جرائم القرصنة والاحتيال والتخريب وغسيل الأموال وما هو يتسبب في مشاكل قانونية و اجتماعية واقتصادية وأمنيهما يستدعى بالضرورة إصدار قوانيين خاصة بالجريمة الإلكترونية ويتوافق مع خصوصياتها وتضمن أمن المعلومات الإلكترونية داخل المنظمات وخارجها وللأفراد وحماية خصوصيتهم .

❖ دور الحاسب في الجرائم الإلكترونية

لكي تعتبر جريمة ما جريمة سيبرانية أو الكترونية يجب أن يكون للكمبيوتر أو الشبكة أو الجهاز الرقمي دور مركزي في الجريمة، أي كهدف أو كأداة، وهذا يستبعد الجرائم التي يكون للكمبيوتر فيها دور عرضي فقط مثل كونة مستودعاً للأدلة، **لذلك الجرائم الإلكترونية تعتمد على نظام كمبيوتر أو شبكة أو جهاز رقمي في احد الدورين التاليين:**

١. الكمبيوتر هدف لنشاط إجرامي.
٢. الكمبيوتر أداة لارتكاب نشاط إجرامي.

تشمل جرائم النوع الأول التي يكون فيها الكمبيوتر أو الشبكة أو الجهاز الرقمي هدفا للنشاط الإلكتروني اربع فئات فرعية :

١. جرائم الوصول غير المصرح به **مثل:** الاختراق.
٢. جرائم البرمجيات الخبيثة **مثل:** نشر الفيروسات والديدان.
٣. جرائم تعطيل الخدمات **مثل:** تعطيل أو رفض خدمات وتطبيقات الحاسوب مثل هجمات حجب الخدمة Dos وشبكات الروبوت.
٤. سرقة الخدمات أو إساءة استخدامها **مثل:** سرقة أو إساءة استخدام حساب الإنترنت أو اسم المجال الخاص بشخص ما.

تشمل جرائم النوع الثاني التي يكون فيها الكمبيوتر أو الشبكة أو الجهاز الرقمي هي الأداة المستخدمة لارتكاب الجريمة أو تسهيلها ثلاث فئات فرعية

١. جرائم انتهاك المحتوى **مثل:** حيازة الأسرار العسكرية غير المصرح بها أو جرائم الملكية الفكرية.
٢. التلاعب الغير مصرح به للبيانات أو البرامج لأغراض شخصية أو تنظيمية **مثل:** الاحتيال عبر الإنترنت.
٣. الاستخدام غير السليم للاتصالات **مثل:** المطاردة الإلكترونية أو الرسائل غير المرغوب فيها.

١. اختار الإجابة الصحيحة فيما يلي:

١- الأشخاص الذي يسعون إلى التخريب أو إتلاف المحتويات الشبكية، التي تشكّل خطراً كبيراً

- ○ طائفة الحاقدين
- ○ طائفة الفكريين
- • طائفة المتجسسين
- ○ طائفة الهواة

٢- من خصائص المجرم الالكتروني :

- ○ عنيف
- ○ لبق
- ○ مسالم
- • الخبرة والمهارة

٣- من أدوار الحاسب في الجرائم الإلكترونية:

- • أداة لارتكاب نشاط اجرامي
- ○ البرمجيات الخبيثة
- ○ وسيلة للتفوق
- ○ أداة للعنف

٤- SMTP هو بروتوكول

- • بروتوكول نقل البريد البسيط
- ○ بروتوكول التكوين الديناميكي للمضيف
- ○ بروتوكول الوصول إلى الطريق
- ○ بروتوكول نقل الملفات

٥- من تصنيف الجريمة الإلكترونية حسب التنفيذ:

- ○ شخصي
- • فردي – جماعي
- ○ ميداني
- ○ زمني

٦- إتلاف والتدمير من التصنيف حسب:

- ○ التنفيذ
- ○ نوع المعلومات
- ○ مساسها بالأفراد
- • النوع

٢. **ضع علامة (✓) أمام العبارات الصحيحة وعلامة (✗) أمام العبارات الخاطئة:**

١.	HTTP هو بروتوكول قياسي لتأمين الاتصال بين جهازي حاسوب، أحدهما يستخدم المتصفح والآخر لجلب البيانات من خادم الويب	✗
٢.	من تصنيفات الجرائم الإلكترونية جرائم التسلية	✗
٣.	الجريمة السيبرانية من مسميات الجرائم الإلكترونية	✓
٤.	الدافع العائلي من دوافع الجريمة الإلكترونية	✗

الفصل الثالث

مخاطر الجرائم الإلكترونية

في هذا الفصل سوف نتعرف على المواضيع التالية:

- العوامل التي ساعدت على انتشار الجرائم الإلكترونية
- أشكال الجرائم الإلكترونية ومخاطرها
- جرائم الهواتف الذكية
- جرائم الفضاء الإلكترونية

❖ العوامل التي ساعدت على انتشار الجرائم الإلكترونية

المجرم الإلكتروني هو شخص يختلف عن المجرم العادي فهو مُلم للتقنيات الحديثة الإلكترونية وساعد على انتشار الجرائم ما يلي:

١. انفتاح شبكة المعلوماتية فهي فضاء مفتوح على مصراعيه لا يخضع للرقابة والملكية الأمر الذي سهل عمليات التسلل إليه واختراقه.

٢. انعدام الحواجز الجغرافية.

٣. صعوبة الكشف عن هوية المستخدم إذ يمكن لأي شخص انتحال شخصية أو التخفي وراء أنسأن وهمي.

٤. سهولة التعامل مع الوسائل التكنولوجية وزهد أثمانها.

٥. صعوبة التحقق وإثبات الجرائم.

٦. الثغرات القانونية بين مختلف الدول فما هو صارم في نظام ما مخفف في نظام أخر مما يتيح الفرصة للمجرمين سرعة التكيف وانتقال من نقطة جغرافية لأخرى أكثر أمأناً

٧. إشكالية الاختصاص القضائي والقوانيين الواجب تطبيقها.

هذه الأسباب تساعد الجماعات الإجرامية على المضي قدماً في أنشطتها دون خوف وبكل أمأن وتعتمد في ذلك على شن هجوم على المواقع الشخصية والعامة، الرسمية وغير الحكومية باختراقها والتسلل إليها، للسيطرة عليها وتدميرها أو سرقة بياناتها وحقن جرعات من الفيروسات مما يسبب لأصحابها أضراراً جسيمة مادية ومعنوية فهي جريمة تتخطى الحدود الجغرافية لاتصالها بعالم الإنترنت وتقنية المعلومات حيث قد تتأثر دول كثيرة بهذه الجريمة في أن واحد وبسبب السرعة الهائلة في تنفيذها وحجم الأموال.

❖ أشكال الجرائم الإلكترونية ومخاطرها

في العصر الرقمي الذي نعيشه اليوم، أصبحت الجرائم الإلكترونية منتشرة ومتطورة بشكل متزايد مما يشكل تهديداً للأفراد والمنظمات على حد سواء.

١. أحد أكثر أشكال الجرائم الإلكترونية انتشارا هو **التصيد الاحتيالي**، حيث يستخدم مجرمو الإنترنت رسائل البريد الإلكتروني أو مواقع ويب وهمية لخداع الأفراد لتقديم معلومات حساسة مثل كلمة المرور أو أرقام بطاقات الائتمان أو المعلومات الشخصية، حيث غالباً ما تبدو هذه المواقع أو الرسائل البريدية أنها قادمة من مصادر مشروعة.

٢. الشكل الأخر من أشكال الجرائم الإلكترونية المعروفة هي **برامج الفدية**، وهي نوع من البرامج الضارة (malware) المصممة لتشفير الملفات أو قفل النظام بأكمله، مما يجعل المالك أو المستخدم غير قادر على الوصول إليه، ثم يقوم المجرم بطلب الفدية من الضحية لإعادة الوصول للملفات أو النظام المتأثر.

٣. **سرقة الهوية** هي جريمة لها عواقب وخيمة على الضحايا، حيث يقوم مجرمو الإنترنت بسرقة المعلومات الشخصية مثل أرقام الضمان الاجتماعي وأرقام بطاقات الائتمان ومعلومات الحساب المصرفي من اجل ارتكاب عمليات احتيال أو الوصول الى الحسابات المالية.

٤. **التسلط عبر الإنترنت (التنمر)** هو شكل من أشكال الجرائم الإلكترونية التي تنطوي على استخدام التكنولوجيا لمضايقة الأفراد أو تهديدهم أو تخويفهم، يمكن أن يتخذ أشكالا عديدة، بما في ذلك نشر الشائعات أو مشاركة المعلومات الشخصية دون موافقة صاحبها أو إرسال رسائل تهديد.

- **ماذا تستهدف الجريمة الإلكترونية؟ وماهي أضرارها على كل هدف**

أبرز استهدافات الجرائم الإلكترونية التي تتسبب في ضرر تلحقه على المجتمعات والأفراد والأنظمة المالية والمصرفية والعسكرية هي:

١-الجرائم الإلكترونية التي تستهدف الأموال:

أضرارها: جرائم تستهدف المراكز المالية لتحقيق مكاسب مادية وللاستيلاء على الأموال بشقيها المادي النقدي أو المعلوماتي عن طريق بسرقة معلومات للوصول للمال أو تزوير بطاقات الائتمان والشيكات الإلكترونية أو عن طريق قرصنة الحوالات المالية أو استهداف وسرقة صرافات السحب الآلي التابعة للمؤسسات المالية والمصرفية أو عن طريق مهاجمة البيانات المعلوماتية للبنوك والأنظمة المصرفية بقصد سرقة الأموال والاستيلاء عليها أو عن طريق النصب والاختلاس والاحتيال الإلكتروني.

٢- الجرائم الإلكترونية التي تستهدف المجتمعات:

أضرارها (أنتشار الجرائم الإلكترونية التي استهدفت إفساد المجتمعات في أخلاقياتها ودينها وسلوكياتها وعاداتها وتقاليدها وترتب عليها آثار اجتماعية سيئة مثل تضليل الرأي العام وبث سموم الكراهية في المجتمعات كازدراء العقائد، والأديان، والتفرقة، والعنصرية)

٣-الجرائم الإلكترونية التي تستهدف الأفراد:

تعاني المجتمعات الإلكترونية في الفترة الأخيرة من اختراق الخصوصية الإلكترونية الذي دفع الدول إلى العمل للحد من هذه الجرائم التي تلحق الضرر بالأفراد مثل جرائم السب والتحقير التي تُطال الأشخاص عبر شبكة الإنترنت واختراق البيانات الشخصية للأفراد والابتزاز وانتحال الشخصيات في مواقع التواصل الاجتماعي، والمواقع الإلكترونية، والتشهير، والتهديد.

٤-الجرائم الإلكترونية التي تستهدف الملكية الفكرية

أضرارها (يتم ذلك بقيام الجاني بالاستحواذ على تلك الملكية والاستيلاء عليها والاستفادة منها والتصرف فيها وحرمان المالك من الفائدة المالية والمنفعة التي تأتي من وراء تلك الملكية)

٥- الجرائم الإلكترونية التي تستهدف الأمن القومي للدول

أضرارها (هجوم رقمي إلكتروني أصبح يهدد أمن واستقرار الدول من خلال استهداف النظام المعلوماتي ومهاجمة المصالح الحيوية للدول مثل اختراق الأنظمة العسكرية والتجسس الإلكتروني عليها وتخريبها بنشر الفيروسات وتشويه الصورة الذهنية للمواطنين تجاه بلدهم ليصل الأمر لنشوب حرب إلكترونية).

❖ جرائم الهواتف الذكية

اكتسبت أجهزة الهواتف المحمولة الذكية أهمية خاصة لدى كافة الأفراد على مستوى العالم عموماً والعالم العربي خصوصاً، حيث أصبحت مسألة الاستغناء عنها مشكلة كبيرة لدى معظم مستخدميها، لشعورهم بفقدان آلية التواصل والتقارب مع الآخرين، حيث تمتاز تلك الأجهزة على وجه التحديد بمميزات عديدة سهلت لمستخدميها فضلاً عن عملية التواصل مع الآخرين، القدرة ايضاً على أنجاز الكثير من المهام اليومية في كافة الأنشطة المتعلقة بحياة الفرد.

فالهواتف الذكية تمثل المفهوم الحقيقي للتطور الحادث في ثورة الاتصالات والمعلومات، فتزايد استخدامها ينبأ عن تفضيلها عن باقي أجهزة التقنية الأخرى كالحاسبات الآلية والكاميرا الرقمية والراديو وإلى غير ذلك من أجهزة تقنية أخرى، ومع ذلك رافق ازدياد الإقبال على هذه الأجهزة، ازدياد مطرد في سوء استخدامها، حيث استغل البعض ما لدى الهاتف المحمول من قدرات وإمكانيات يمكن تطويعها في خدمة الجريمة، كالكاميرا الرقمية المدمجة وتقنية البلوتوث وخدمة الرسائل النصية والمصورة، هذا فضلاً عن إمكانية ارتباطها بشبكة الإنترنت التي أعطت فعالية أكبر لارتكاب الجريمة عبر هذه الهواتف الذكية وما تتضمنه من تقنيات عالية تتيح التصوير والتسجيل والبث والنشر والتواصل وغيرها، إلى أداة جريمة يمثل بعد ثبوتها الأفراد أمام القانون ليواجهوا عقوبات رادعة، نتيجة الاستخدام السيئ غير المسؤول أو المقبول اجتماعياً ودينياً، فالتقنيات سهلة الاستخدام الموجودة في الهواتف الذكية، سهلت عملية اختراق الخصوصية ، حيث أنه خلال ثوان معدودة تتم عملية التصوير والبث والنشر دون علم الشخص أو بعلمه، كما أدى الأمر نفسه إلى اندفاع الأفراد نحو تصوير الوقائع والأحداث والتسابق في نشرها دون شعور بالمسؤولية أو إدراك بمدى تأثير ذلك الفعل في المجتمع، ليجد الشخص نفسه أحيانا وقد اخترق خصوصية الآخرين، ويواجه العقوبات المترتبة على ذلك الجرم الذي سنت له الدولة قوانين صارمة ورادعة، تتمثل في القانون الخاص بالجرائم الإلكترونية الذي يتضمن عقوبات مغلظة وذلك للحد من استخدام الهواتف الذكية بشكل يسيء للأخرين و للمجتمع ، وأيضا للحفاظ على خصوصيات الآخرين.

- **الفضاء الإلكتروني**

هو ما يوصف بتدفق البيانات الرقمية من خلال شبكة من أجهزة الحاسب المتصلة لأن الفرد لا يمكنه تحديد موقعه مكانياً ككائن ملموس ولا تظهر آثاره بشكل واضح مثلما تظهر في العالم الحقيقي ويمكن اعتبار الفضاء الإلكتروني واجهة جديدة للمجتمعات نظراً لاحتوائه على خلفيات جديدة تعمل على إعادة تشكيل المجتمع و الثقافة من خلال الهويات الخفية لمستخدميه، أي يمكن وصفه بأنه عالم افتراضي يتشابك مع العالم المادي يتأثر به ويؤثر فيه بشكل مُعقد حيث تقوم العلاقة بين العالمين على نظرة تكاملية تحمل بين طياتها مزايا ومخاطر لا تتوقف.

❖ جرائم الفضاء الإلكترونية

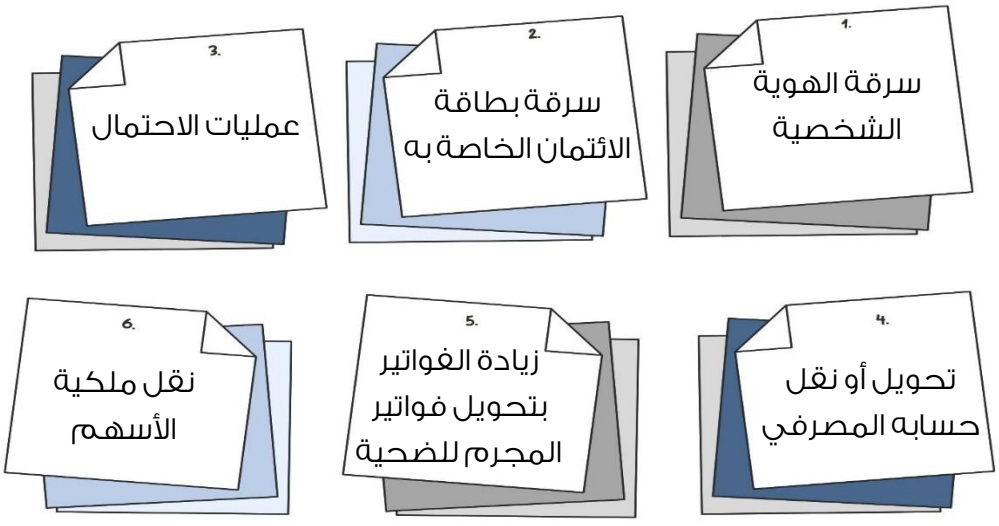
هي شكل متطور من أشكال الجريمة تحدث في مجال الفضاء الإلكتروني الذي لا حدود له، ويمكن لمرتكبي الجرائم الإلكترونية وضحاياهم أن يتواجدوا في مناطق مختلفة، ويمكن أن تتمدد آثار الجريمة عبر المجتمعات في جميع أنحاء العالم، مما يبرز الحاجة الي وضع استجابة عاجلة وديناميكية ودولية.

أكدت الدراسات الحديثة أن جرائم الفضاء الإلكتروني تنطوي عل مخاطر عديدة سياسية واقتصادية واجتماعية وتلحق بالمؤسسات والأفراد خسائر فادحة باعتبارها تستهدف اختراق المعلومات الحيوية وبرمجيات التشغيل الحديثة والبيانات الرقمية والحياة الخاصة للأفراد، وحيث يتعرض الكثير من المستخدمين للمخاطر أثناء التسوق الإلكتروني واستخدام وسائل التواصل الاجتماعي واستخدام الخدمات المصرفية عبر الإنترنت ومن الممكن أن تصاب الحواسيب أو الأجهزة النقالة بالفيروسات وكذلك يمكن سرقة الهوية أو الحسابات المصرفية عبر الإنترنت.

فقد تستهدف جرائم الفضاء الإلكتروني إحداث الدمار من خلال التسبب في الاضطراب والارتباك في شبكات الاتصال وأنظمة المعلومات المستهدفة.

- جرائم الفضاء الإلكتروني التي يتعرض لها الفرد

لقد سمحت الإنترنت للأفراد بالتواصل مع العالم الخارجي بحيث أصبح بإمكانه إجراء معاملات الشراء أو البيع وإدارة أعماله إلكترونياً



- **الجرائم الإلكترونية التي تتعرض لها البنوك**

1	2	3	4	5
السطو الإلكتروني	تعطيل النظام	التلاعب بمخازن المعلومات الخاصة بالبنك بحذفها أو تعديلها أو تعطيل الوصول اليها	نقل ملكية الأسهم	اختراق الموقع الخاص بالبنك

- **جرائم الفضاء الإلكتروني التي قد تتعرض لها المنظمات والمؤسسات**

١. الاطلاع على معلومات سرية والاستفادة منها.

٢. التلاعب بمخازن المعلومات الخاصة بالمنظمة، أو المؤسسة بحذفها، أو تعديلها، أو تعطيل الوصول اليها.

٣. الابتزاز والتهديد.

٤. اختراق الموقع الإلكتروني الخاص بالمنظمة أو المؤسسة.

- **جرائم الفضاء الإلكتروني التي قد تتعرض لها الجهات والأجهزة الحكومية**

1	2	3	4
الوصول الى معلومات سرية والاطلاع عليها أو حذفها أو تعديلها بما يحقق هدف المجرم	دعم الإرهاب والأفكار المتطرفة ونشر الشائعات	تعطيل الإنترنت بالكامل	تعطيل وتخريب الخوادم الموفرة للمعلومات

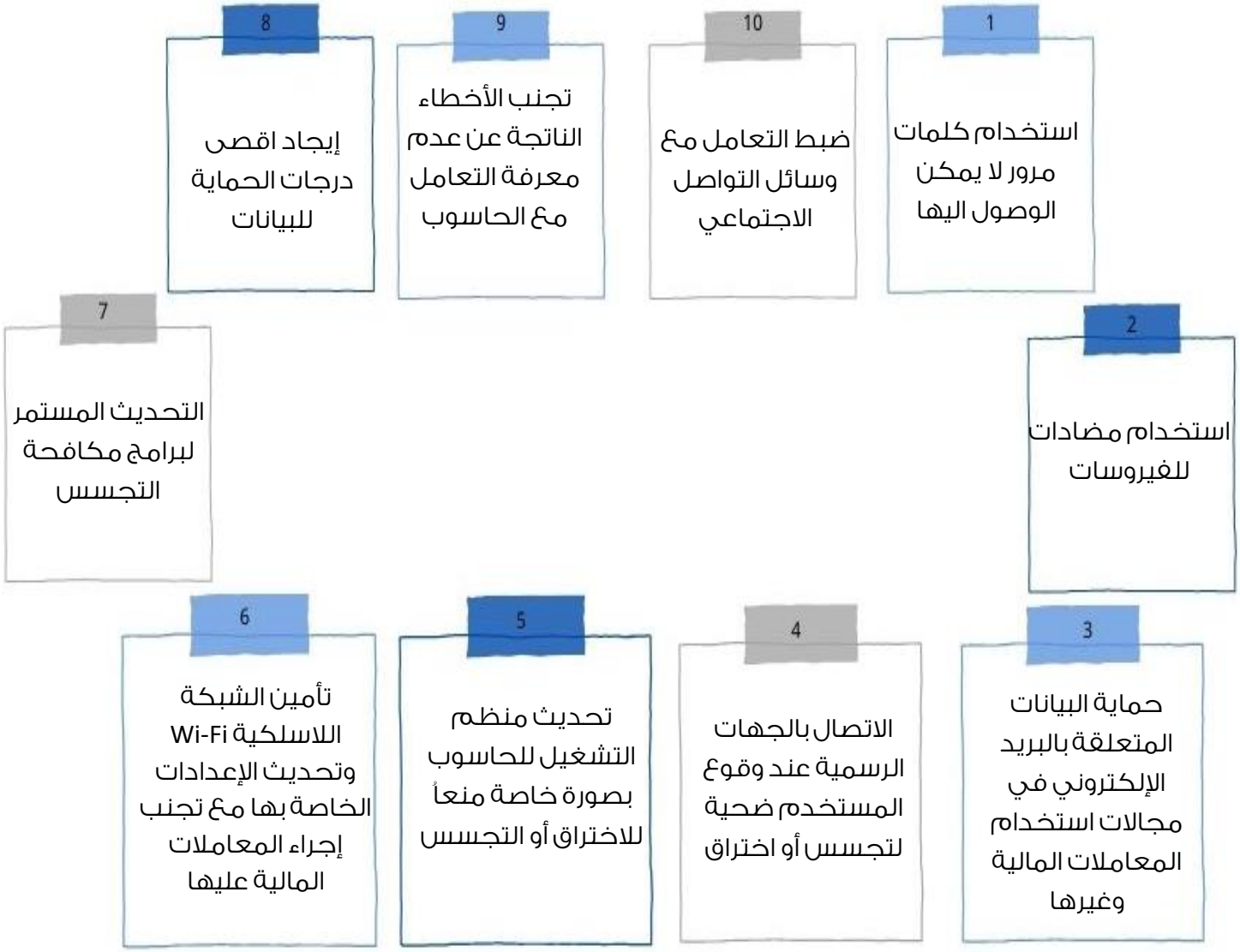
- **الجريمة الفضائية الاقتصادية**

لقد نتج عن الثورة التكنولوجية ظهور نوع جديد من المعاملات الإلكترونية يسمى المعاملات الإلكترونية تختلف عن المعاملات التقليدية من حيث البيئة التي تتم فيها هذه المعاملات فقد سمحت المعلوماتية والإنترنت في تداول الأنشطة التجارية عبر الشبكة مما أتاح للأنشطة الإجرامية تحقيق عوائد مالية عن طريق وسائل غير مشروعة ناتجة عن عمليات التزوير والاحتيال، أهم الجرائم التي تقع على الأموال عبر الإنترنت التحويل الإلكتروني غير المشروع للأموال والسطو على بطاقات الائتمان.

تتم عملية التحويل الإلكتروني للأموال بشكل غير مشروع من خلال التحايل وذلك بالحصول على رقم كلمة السر من جهاز حاسب محتال عليه أو عن طريق انتحال شخصية وهمية و إيهام المحتال عليه بوجود مشروع مربح وبالتالي يتم تحويل إلكتروني للأموال لصالح المحتال كما يمكن أن يتم الاحتيال باستعمال بطاقات الائتمان وهي بطاقة بنكية للدفع أو السحب الإلكتروني تصدرها هيئات عالمية كالماستر كارد أو فيزا كارد تسمح هذه البطاقات بعمليات البيع والشراء عبر الإنترنت تحمل أرقاماً خاصة بكل عميل ومع التطور التقني وتطور البرمجيات أصبح بالإمكان الاستيلاء على هذه الأرقام والحصول على الأموال منها.

- الوقاية من الجريمة الإلكترونية

يتطلب الآتي:



تمارين الفصل الثالث

١. **اختار الإجابة الصحيحة فيما يلي:**

١- **شكل من أشكال الجرائم الإلكترونية التي تنطوي على استخدام التكنولوجيا لمضايقة الأفراد أو تهديدهم أو تخويفهم :**

- ○ برامج الفدية
- ○ السطو الالكتروني
- ○ سرقة الهوية الشخصية
- • التسلط عبر الإنترنت

٢- **المفهوم الحقيقي للتطور الحادث في ثورة الاتصالات والمعلومات :**

- ○ الفيروسات الضارة
- ○ الجريمة الإلكترونية
- • الهواتف الذكية
- ○ الإنترنت

٣- **هي شكل متطور من أشكال الجريمة تحدث في مجال الفضاء الإلكتروني الذي لا حدود له :**

- ○ الجريمة الإلكترونية
- ○ البرمجيات الخبيثة
- ○ الياقات البيضاء
- • جرائم الفضاء الالكتروني

٢. **ضع علامة (✓) أمام العبارات الصحيحة وعلامة (✗) أمام العبارات الخاطئة:**

١.	وجود حواجز جغرافية من العوامل التي ساعدت في أنتشار الجريمة الإلكترونية.	✗
٢.	قد تستهدف الجريمة الإلكترونية التعليم.	✗
٣.	من متطلبات الوقاية من الجريمة الإلكترونية تأمين الشبكة اللاسلكية Wi-Fi.	✓
٤.	الجرائم التي تستهدف الامن القومي تسعى لتحقيق مكاسب مادية وللاستيلاء على الأموال.	✗

الفصل الرابع

أبعاد وأثار الجرائم الإلكترونية

في هذا الفصل سوف نتعرف على المواضيع التالية:

- أبعاد وأثار الجرائم الإلكترونية عربياً وعالمياً
- متطلبات الأمن السيبراني ودوافع اهتمام الدول به
- جهود الدول في مجال الأمن السيبراني وطرق مكافحة الجرائم الإلكترونية
- التعاون الدولي في مواجهة جرائم الإنترنت
- جهود المملكة العربية السعودية في مجال الأمن السيبراني وطرق مكافحتها
- قوانين مكافحة الجرائم الإلكترونية وتشريعاتها عربيا
- قوانين مكافحة الجرائم الإلكترونية في المملكة العربية السعودية
- الهيئة الوطنية للأمن السيبراني
- المعوقات التي تواجه أمن الفضاء الإلكتروني
- رؤية استراتيجية لمواجهة مخاطر الفضاء السيبراني وحروبه
- قوانين دولية للأمن السيبراني

❖ أبعاد وأثار الجرائم الإلكترونية عربياً وعالمياً

- **أولاً: الأبعاد الاقتصادية للجريمة الإلكترونية وأثارها**

أن تحول الاقتصادي العالمي من مرحلة الاقتصاد التقليدي إلى مرحلة الاقتصاد الرقمي وتحول التعاملات التجارية والمالية إلى الشكل الإلكتروني زاد من خطورة الجريمة الإلكترونية والتي أصبحت في تصاعد مستمر ومن المتوقع أن يتزايد حجم الخسائر التي يتكبدها العالم بسبب الجريمة الإلكترونية في العقود القليلة القادمة نتيجة تزايد عدد الشركات التي تعتمد على الإنترنت في ممارسة نشاطها.

فحسب أخر إحصائيات فأن الاقتصاد العالمي يتضرر جراء الجريمة الإلكترونية تريليون دولار سنويا غير أن الخطورة الحقيقية ليس من ضخامة حجم الخسائر فقط، ولكن في تزايدها المستمر.

ونطاق الجريمة الإلكترونية نسبة تتراوح ما بين ١٥ و٢٠ من حجم الاقتصاد العالمي المستند إلى الإنترنت سجلت التكلفة الإجمالية للتهديدات والجرائم الإلكترونية على مستوى العالم أكثر من ٦ تريليونات عام ٢٠٢١م.

وبحسب تقدير Grant Thornton يعتبر القطاع المالي الأكثر عرضة للهجمات بنسبة ٤٦ يليه قطاع الرعاية الصحية بنسبة ٢٤ ثم قطاع الطاقة بنسبة ٢٣ .

وتُعد منطقة الشرق الأوسط من بين الأكثر تضررا في العالم من الهجمات الإلكترونية بحسب تقرير أصدرته PWC وأظهر أن ٥٦ من شركات المنطقة تعرضت لهجوم إلكتروني خسرت ٥٠٠ ألف دولار.

مع تزايد نسبة الجرائم الإلكترونية وتنوع طرقها لا شك أنها تلحق خسائر مادية كبيرة وفادحة أكثر مما تسببه الجرائم التقليدية ليس فقط على مستوى الفرد، بل تتعداه إلى مستوى المنظمات والجهات والمؤسسات وهذا بالطبع يؤثر بشكل سلبي على الاقتصاد.

وتتضح خطورة الجريمة الإلكترونية على الاقتصاد العالمي عبر مقارنة الخسائر التي يتكبدها الاقتصاد العالمي من مصادر التهديد الأخرى.

- **الأبعاد المادية**
- **الخسائر المالية للجريمة الإلكترونية**

ففي الوقت الذي يخسر فيه الاقتصاد العالمي ٠,٨ من إجمالي الناتج المحلي العالمي نتيجة الجريمة الإلكترونية فأن النسبة تقل عن ٠,٢ في الجرائم الأخرى مثل القرصنة البحرية أي أن الجريمة الإلكترونية تكبد الاقتصاد العالمي أربعة أمثال الخسائر التي تكبدها الاقتصاد العالمي نتيجة القرصنة البحرية، وتتساوى الخسائر التي يتكبدها الاقتصاد العالمي نتيجة الجريمة الإلكترونية مع حجم الخسائر التي يتكبدها الاقتصاد العالمي من السلع المغشوشة.

وبحسب تقرير أعدته شركة مكافي المتخصصة في حماية أمن المعلومات فأن الجريمة الإلكترونية تجارة مربحة منخفضة التكلفة قليلة المخاطر تدر أرباحاً طائلة تزيد على إجمالي الدخل القومي للكثير من الدول ولا تقتصر خسائر الجريمة الإلكترونية فقط على الخسائر المباشرة وإنما تشمل أيضا الخسائر غير المباشرة مثل حقوق الملكية الفكرية وسرقة الأصول المالية والمعلومات التجارية المهمة وتكلفة استعادة البيانات وتكلفة الفرص البديلة و لا يمكن تجاهل تأثير الجريمة الإلكترونية على الاقتصاد الوطني وعلى أداء الشركات وعلى حركة التجارة العالمية وعلى القدرة التنافسية و الابتكار.

- **خسائر مالية**

الهجوم الإلكتروني له تأثيرات، ولكن بعيدة المدي ومنها سرقة الملكية الفكرية والخسائر المالية، وفقدان ثقة المستخدم وعند تحديد الأثر المادي الإجمالي للجريمة الإلكترونية على الحكومة والمجتمع يقدر بعدة مليارات الدولارات كل سنة وبعض المجرمون يستفيدوا من التكنولوجيا بطرق عديدة ومختلفة وخصوصاً الإنترنت، لأنها وسيلة يستخدمها المحتالين لكي يمارسوا التجارة الخاصة بهم عندما يقوموا بالتخفي وراء درع لإخفاء الهوية الرقمية لهم , وتقوم الجريمة الإلكترونية بالتأثير على المجتمع بطرق عديدة ومنها ما يكون خلال الإنترنت أو خارج الإنترنت.

عندما يقع شخص ضحية الجريمة الإلكترونية يكون لها آثار على مدى طويل على الحياة والتصيد الاحتيالي من الأساليب المنتشر استخدامها من قبل المحتالون، ومنها ومن الأساليب أيضا إرسال رسالة مزيفة عبر البريد الإلكتروني على أنها واردة من مؤسسة مالية أو بنك تريد منه معلومات شخصية.

وعندما يقوم الشخص بإرسال تلك المعلومات يقوم المجرم بالوصول لحسابات الائتمانية والمصرفية، وتقوم بتدمير التصنيف الائتماني وفتح حسابات جديدة.

- تكاليف الأمن

مجرمون الإنترنت يقوموا بالتركيز في هجماتهم على كلا من الشركات الصغيرة والكبيرة فيقومون بالاستيلاء على الخوادم لهذه الشركات والقيام بسرقة المعلومات الخاصة بها أو يقومون باستخدام أجهزة لتساعدهم في أغراضهم الخاصة.

ولهذا تقوم بعض الشركات تعيين موظفين واستخدام تحديث للبرامج التي تقوم بحمايتهم من الاختراقات تم إيجاد دراسة استقصائية للشركات الكبيرة توضح متوسط الأنفاق على الأمن السيبراني وهو حوالي ٨,٩ مليون دولار سنويا.

للجريمة الإلكترونية آثار كبيرة أيضا على صناعات الموسيقى والترفيه والبرمجيات والتي يصعب القيام بتقديرها عن طريق التعويضات ومن الصعب تحقيقها، ويعاني أصحاب حقوق النشر والطبع من قوانيين الصارمة التي تكون ضد سرقة الملكية الفكرية وهذا جعل إصدار قوانيين كقانون المؤلف للألفية الرقمية.

- **ثانيا: الأبعاد الاجتماعية للجريمة الإلكترونية أثارها**

يقوم مجرمون الإنترنت بالاستفادة من الترابط الذي يقوم بتوفير الإنترنت واختفاء السرية والهوية، ولهذا يقومون بالهجوم على المجتمع الخاص بالمعلومات الحديثة.

وتحتوي الجرائم الإلكترونية على فيروسات الكمبيوتر وشبكات الروبوتات والتسلط من خلال الإنترنت والإرهاب السيبراني والمطاردة عبر الإنترنت وهجمات رفض الخدمة والبرامج الضارة والقرصنة والبريد العشوائي وسرقة الهوية، لذلك يتعرض مستخدمو مواقع التواصل الاجتماعي للجرائم بشكل متزايد وأصبحت تهدد سلامة الأجهزة والحسابات الشخصية وأصبحت خطر يؤثر على الروابط الأسرية.

وأهم التأثيرات السلبية للجرائم الإلكترونية تدمير الحاسب الخاص بالضحية ثم إلحاق آثار نفسية وعقلية بالضحية يليها إلحاق خسائر مادية له.

وأشكال جرائم وسائل التواصل الاجتماعي تتمثل في التنمر والمطاردة وسرقة الهوية ونشر مقاطع الفيديو، والحيل، والسرقات، والاحتيال.

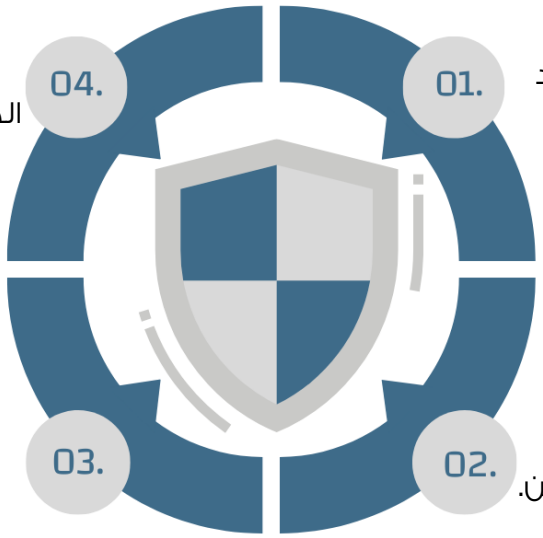
❖ متطلبات الأمن السيبراني ودوافع اهتمام الدول به

- **متطلبات الأمن السيبراني**

1. تعريف الإطار القانوني المناسب لتعزيز الصمود السيبراني ومرونته ضد الهجمات وتطوير اليات فعاله للتشفير، ورفع مستوى وعي المجتمع العالمي بالأمن السيبراني وتعزيز التواصل معه.
2. تعزيز الثقافة الأمنية الوطنية واعتبار أمن الخدمات جزء لا يتجزأ من الخدمات التي تقدمها الدولة للمواطن.
3. الاعتماد على أساليب وتقنيات متطورة للتمكن من الكشف على هوية مُرتكبي الجريمة والاستدلال عليه بأقل وقت ممكن.
4. رسم سياسات دولية تفرض عقوبات صارمة على مرتكبي جرائم الأنترنت ويستلزم التدخل الحكومي والدولي نظرا للخطورة الجسيمة للأمر.
5. توعية الأفراد ونصحهم لماهية الجرائم الإلكترونية وكل ما يترتب عليها من مخاطر.
6. مواكبة التطورات المرتبطة بالجريمة الإلكترونية والحرص على تطوير وسائل مكافحتها.

- **دوافع اهتمام الدول به**

حماية العالم السيبراني هي حماية للعالم الفعلي، فليس العالم السيبراني سوى وسيلة من وسائل العالم الفعلي غايتها جعله أكثر فاعلية في أداء الأعمال والنشاطات المختلفة، سواء ما يرتبط منها بشؤون الخدمات الحكومية، أو الأعمال المهنية، أو النشاطات الاجتماعية، وليس ذلك في إطار محدود الأبعاد، بل على مستوى العالم بأسره، وعلى هذا الأساس، فأن أمن العالم السيبراني جزء مهم لا يتجزأ عن أمن العالم الفعلي، **وهو بذلك يرتبط بأربع دوائر رئيسة، هي:**



01. الدائرة الشخصية أي دائرة الفرد وسلوكه والتزاماته.

02. دائرة المؤسسات وسعيها الى حماية ذاتها وتعاملاتها مع الأخرين.

03. دائرة الدولة المهتمة بخدمة الأمة وحمايتها.

04. دائرة العالم بأسره المنية بالتعاون الدولي والعمل المشترك لحماية العالم بأسره.

الأنسان هو العنصر الحي في جميع هذه الدوائر، وهو المحرك لها، تبعا لموقعه فيها وليست هذه الدوائر منفصلة عن بعضها بعضاً، بل هي متداخلة، وأي خلل أو مشكلات أمنية تقع في إطار أي منها، أثرها واقعاً بدرجات مختلفة على الجميع، وعلى ذلك، فأن حماية الأمن السيبراني مسؤولية تقع على عاتق الجميع .

❖ جهود الدول في مجال الأمن السيبراني وطرق مكافحة الجرائم الإلكترونية

أثبت الواقع العملي أن كل دولة لا تستطيع بجهودها المنفردة القضاء على الجرائم الإلكترونية مع هذا التطور الملموس في كافة المجالات الذي أدى إلى الانتشار الواسع والمتزايد لها ونظراً لخطورتها وزيادة أنتشارها على الصعيد الدولي ووجود قصور في التشريعات الوطنية في مكافحتها الأمر الذي تطلب جهود موحدة لمكافحتها ولذلك أصبحت هناك احتياج لوجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة وتتعاون من خلاله الأجهزة المختلفة في الدول خاصةً فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين بأقصى سرعة ممكنة بالإضافة إلى تعقب المجرمين الهاربين من وجه العدالة ولتخطي الحدود والسيادة التي قد تعترض الجهود الوطنية لملاحقة المجرمين وتعقب مصادر التهديد سواء كانت مساعدة متبادلة قانونيا أو قضائية أو شرطية وسواء اقتصرت على دولتين فقط أو امتدت إقليمياً أو عالمياً .

كما سعت كثير من التشريعات الدولية والعربية إلى وضع قوانيين وقواعد لتأمين التبادل الأمني للمعلومات بين الأطراف عبر شبكة الإنترنت، وأن أهم طرق حماية المعلومات والتوقيع الإلكتروني هي التشفير الإلكتروني والتوثيق الإلكتروني، كما اتجهت معظم التشريعات العربية والدولية إلى تجريم الهجوم على بيانات الرسائل فاهتمت التشريعات بوضع النصوص القانونية للحد من هذه الجرائم وردع المهاجمين.

ويعمل مكتب الأمم المتحدة المعني بالجريمة على تعزيز بناء القدرات على المدى الطويل وعلى نحو مستدام في مكافحة الجريمة الإلكترونية من خلال دعم الهياكل والإجراءات الوطنية، ويستند المكتب تحديداً إلى خبرته المتخصصة في مجال استجابة نظام العدالة الجنائية من أجل تقديم المساعدة التقنية في مجال بناء القدرات، والوقاية والتوعية، والتعاون الدولي، وجمع البيانات، والبحث والتحليل بشأن الجريمة السيبرانية.

في إطار الجهود المبذولة قام المجلس الأوربي بالشراكة مع الولايات المتحدة واليابان، وغيرهم من الدول بالتصديق على اتفاقية مكافحة الجرائم السيبرانية عام ٢٠٠٤، والتي لا تزال التشريع الدولي الوحيد الملزم الذي يتناول مسألة الجرائم السيبرانية.

وترجع أصول هذه الاتفاقية إلى نوفمبر ١٩٩٦، عندما أوصت اللجنة الأوربية المعنية بمشكلات الجرائم، بأن يشكل المجلس الأوربي لجنة من المختصين بالجرائم السيبرانية، ومنذ البداية، أقرت اللجنة الأوربية المعنية بمشكلات الجرائم بطبيعة جرائم الفضاء السيبراني، في أنها حينما ترتكب خلال الإنترنت الاختصاص الإقليمي للسلطات الوطنية لأنفاذ القانون، ومن ثم كأن هناك جهد دولي منسق للتعامل مع مثل هذه الجرائم، ولا يمكن ذلك إلا من خلال أداة دولية ملزمة تضمن الفعالية اللازمة لمكافحة هذه الظواهر الجديدة.

قام مجلس أوروبا والسوق الأوربية المشتركة في مواجهة الجرائم الإلكترونية، ١٧ سبتمبر ١٩٨٠ بتوقيع معاهدة مجلس أوروبا والخاصة بحماية الأشخاص من مخاطر المعالجة الآلية للبيانات ذات الطبيعة الشخصية وقد وضعت الاتفاقية للتوقيع في يناير ١٩٨١ وقد بدأ السريان الفعلي لهذه الاتفاقية في أكتوبر ١٩٨٥.

وتُعرف اتفاقية المجلس الأوربي الخاصة بمكافحة الجرائم السيبرانية باسم اتفاقية بودابست وقد شارك في وضع هذه الاتفاقية والتصديق عليها كندا، واليابان، وجنوب أفريقيا، والولايات المتحدة الأمريكية، وصدقت عليها الولايات المتحدة عام ٢٠٠٦ ، وتتناول تلك الاتفاقية تحديد مفهوم الجرائم السيبرانية، بالإضافة إلى المخالفات التي ترتكب ضد الأنظمة الحاسوبية، وعن طريقها ، وقد تم أنشاء تلك الاتفاقية رداً على التهديد العالمي للجرائم السيبرانية، فهي تعتبر الأداة الدولية القانونية الوحيدة الملزمة للتعامل مع الجرائم السيبرانية، والناتجة عن عدة سنوات من العمل.

- **تحتوي اتفاقية بودابست على أربعة فصول:**

الفصل الأول

يشتمل على استخدام المصطلحات.

الفصل الثاني

على الإجراءات التي يتم اتخاذها على المستوى الدولي.

الفصل الثاني

على التعاون الدولي.

الفصل الرابع

فيشمل الأحكام النهائية للاتفاقية.

شكل (٢) خريطة مفاهيم لجهود الدول في الأمن السيبراني

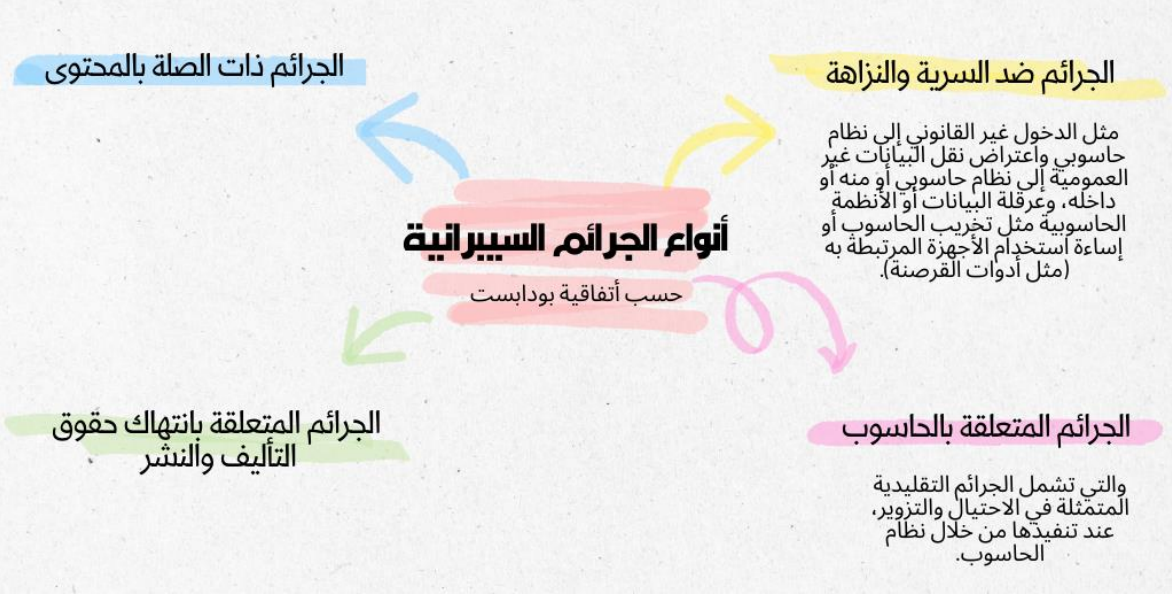
- وفيما يتعلق بالقوانيين الموضوعية قسمت الاتفاقية الجرائم السيبرانية إلى أربع أنواع:

١. الجرائم ضد السرية ونزاهة وتوافر البيانات والأنظمة الحاسوبية، مثل الدخول غير القانوني إلى نظام حاسوبي واعتراض نقل البيانات غير العمومية إلى نظام حاسوبي أو منه أو داخله، وعرقلة البيانات أو الأنظمة الحاسوبية مثل تخريب الحاسوب أو إساءة استخدام الأجهزة المرتبطة به (مثل أدوات القرصنة).

٢. الجرائم المتعلقة بالحاسوب، والتي تشمل الجرائم التقليدية المتمثلة في الاحتيال والتزوير، عند تنفيذها من خلال نظام الحاسوب.

٣. الجرائم ذات الصلة بالمحتوى.

٤. الجرائم المتعلقة بانتهاك حقوق التأليف والنشر وحقوق.



شكل (٣) خريطة مفاهيم لأنواع الجرائم السيبرانية حسب اتفاقية بودابست

وتسعى هذه الاتفاقية من بين أهداف أخرى إلى التصدي للجرائم السيبرانية عن طريق تنسيق القوانين الوطنية، يهدف واضعي الاتفاقية إلى ردع العمل الموجه ضد سرية وسلامة وتوافر أنظمة الحاسوب والشبكات وبيانات الحاسوب بالإضافة إلى إساءة استخدام هذه الشبكات والأنظمة والبيانات، كما تهدف هذه الاتفاقية إلى إتباع سياسة جنائية مشتركة لمكافحة وردع الجرائم السيبرانية، وتجريم أي سلوك يشتمل على جريمة سيبرانية، وتسهيل الكشف والتحقيق والملاحقة القضائية على الصعيدين المحلي والدولي .

ويؤدي المركز الأوربي للجرائم السيبرانية المعروف باسم (EC3) دوراً مهماً في مكافحة الجرائم السيبرانية من خلال التعاون بشكل وثيق مع المجتمع الأوربي، وشركات الإنترنت مثل ميكروسوفت وجوجل وسيمأنتك، حيث يتكون فريق هذا المركز من ٤٣ خبيراً أمنياً يتخذون إجراءات فعالة باستمرار لحماية مصالح المستخدمين الخاصة أو العامة بالشبكات الرقمية، وتدمير المنظمات الإجرامية التي تقف وراء التشفير حتى يمكن التواصل على الإنترنت بحرية دون التعرض لمخاطر التتبع أو الكشف.

كما اهتمت مجموعة الدول الثمانية الكبرى التي تضم كلا من الولايات المتحدة الأمريكية، اليابان فرنسا، بريطانيا، إيطاليا كندا، روسيا، بمكافحة الجريمة الإلكترونية من خلال أنشاء هيئة العمل المعنية بالإجراءات المالية منذ قمة باريس الاقتصادية ١٩٨٩، فضلاً عنة أنشاء مجموعة أخرى بعد اجتماع الحكومات السبع في كندا في سنة ١٩٩٥ التي هدفت إلى مكافحة الجريمة المنظمة عبر الدول، ثم عقدت قمة الحكومات السبع في مدينة ليون الفرنسية في شهر جون،١٩٩٦، والتي تبنت عدة توصيات أهمها تشجيع دوائر الهجرة على مكافحة الجريمة الإلكترونية.

وقد أطلق الاتحاد الأوربي أيضا مبادرة بارزة خاصة بالجرائم السيبرانية، فهو المجلس الدولي الوحيد الذي وضع المبادئ التوجيهية للأخلاقيات الإلكترونية أي حماية حرية الإنترنت والأمن، وحقوق الأنسان والمساعدة في حماية المجتمعات في جميع أنحاء العالم من خطر الجرائم السيبرانية، حيث تنص المسودة الثانية لمبادئ الاتحاد الأوربي لحقوق الأنسان بشأن حرية الرأي والتعبير عبر الإنترنت، وخارجه على أن أي دولة من الدول الأعضاء بالاتحاد الأوربي ملتزمة بضمان وحماية حرية الرأي ضمن حدودها وفي جميع أنحاء العالم.

أما الوضع في التشريع الأميركي فقد اعتبر المشرع الأمريكي برامج الحاسب الآلي ضمن الأعمال المشمولة بالقانون وفقا لقانون النسخ لسنة ١٩٧٦ بعد تعديله عام ١٩٨١ سواء أكانت هذه البرامج بلغة المصدر أو بلغة الآلة وفي عام ١٩٩٧ وبعد مطالبة ملحة القضاء الأمريكي، أصدر القانون الأمريكي قانون الاستنساخ عبر الإنترنت الذي يتعامل مباشرة مع ظاهرة الاستنساخ عبر الإنترنت مدعماً بذلك بقوانين النسخ والعلامات التجارية المنصوص عليها في البابين ١٧ – ١٨ من التقنين الأمريكي حيث تم تعديل هذين البابين حتى يتناسب مع حقوق الملكية الفكرية.

أما بالنسبة للمشرع الفرنسي فأن تجربته في السياسة العقابية ضد الإجرام الإلكتروني أو الجريمة الإلكترونية ظهر منذ السبعينيات حيث كأن أهم هذه المحاولات في سنة ١٩٧٥ ما يعرف بمشروع النائب حول قانون غش المعلومات والذي طرح للمناقشة بعد سنة ونصف من المناقشات أقره المشرع بعد تعديلاته وشكل الباب الثالث من الكتاب الثالث من القسم الثاني من قانون العقوبات الفرنسي وهو متعلق بالجنايات والجنح، أما الباب الثالث فهو متعلق بجرائم المعلوماتية ضمن المواد من ٤٦٢٢ إلى ٤٦٢٩ ومضمون المواد تجريم الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات.

وعلى جانب أخر وضعت المملكة المتحدة (بريطانيا) تشريعات لضبط إساءة استخدام الحاسوب، تتضمن قانوناً تم إصداره عام ١٩٩٠، وكأن هذا القانون استجابة للتعامل مع تزايد جرائم قراصنة الإنترنت في المملكة.

كما تجري المنظمات الدولية أيضا تدريبات دورية لفحص وسائل الدفاع السيبرانية الخاصة بها، وفي المجال الأمني يشارك حلف الناتو في عدة تدريبات مختلفة، تمتد من تدريبات التحالف السيبراني التي عُقدت في عامي ٢٠١٠، ٢٠١١ لفحص التدابير التي يتخذها حلف الناتو للرد على الهجمات السيبرانية واسعة النطاق التي تستهدف بني المعلومات الخاصة به إلى التدريبات المتخصصة التي ينظمها مركز الامتياز المعني بالدفاع الحاسوبي التعاوني التابع لمنظمة حلف شمال الأطلسي (الناتو) في تالين بإستونيا.

وعلى مستوى قارة أفريقيا، تم إطلاق عدد من المبادرات الدولية والإفريقية للتصدي للجرائم السيبرانية ومن أمثلة المبادرات، مبادرة فريق الخبراء رفيع المستوى التابع للاتحاد الدولي للاتصالات السلكية واللاسلكية والتي تهدف إلى وضع استراتيجيات وتوجيهات للبلدان للتعامل مع الجريمة السيبرانية.

ومن الجهود التي قامت بها دولة غانا لمكافحة الجرائم السيبرانية، تطوير القانون الخاص بالإلكترونيات عام ٢٠٠٨، لتعزيز الاتصالات الآمنة، والتخلص من العوائق أمام الاتصالات الإلكترونية، وتعزيز بيئة آمنة لجميع المعاملات الإلكترونية في غانا، حيث تنص المادة ١١٩ من القانون على أن أي شخص يقدم بيانات زائفة لأي وسيلة دفع إلكترونية له أو للأخريين، يعتبر مجرماً ويعاقب بالغرامة أو السجن لمدة لا تزيد عن عشر سنوات، وبالتالي، فأن جميع الأشخاص الذين يتلقوا الأموال عن طريق بيانات مزيفة عبر الإنترنت يتعرضوا للمحاكمة كمتهمين.

- وإدراكاً للتحديات العالمية للجريمة السيبرانية، وخاصة إمكانية تأثيرها على العالم النامي، يعتمد مكتب الأمم المتحدة المعني بالجريمة منهجا قائم على ما يلي:

- زيادة التشريعات ووضع برامج تدريبية لموظفي أنفاذ القانون، ووكلاء النيابة، والسلطات القضائية بشأن تقنيات مكافحة الجرائم السيبرانية، ونهج العدالة الجنائية.
- الأنشطة الوقائية ورفع الوعي، بما في ذلك التعاون المشترك بين مؤسسات أنفاذ القانون، والقطاع الخاص، من خلال زيادة الوعي العام بالجريمة السيبرانية.
- زيادة التعاون الإقليمي والدولي من خلال زيادة التواصل والتنسيق خارج الحدود الوطنية.
- جمع البيانات والبحث والتحليل بشأن الروابط بين الجريمة المنظمة والجريمة السيبرانية.

- **طرق مكافحة الجريمة الإلكترونية**

١. إصدار التشريعات المواكبة لتطورات الجريمة الإلكترونية وتوافق التشريعات الوطنية مع الاتفاقيات والقواعد الدولية والقوانيين المقارنة ذات الصلة لتمكين أجهزة العدالة الجنائية من أداء دورها على النطاق الوطني والإقليمي والدولي بالصورة التي تُسهم بالمكافحة الفعلية للجريمة الإلكترونية.
٢. رفع كفاءة الأجهزة التقنية المختصة برصد التهديدات والمخاطر والتبليغ بالأنذار المبكر وتزويدها بأحدث المعدات.
٣. تدريب وتأهيل الفنيين والمهندسين العاملين في مجال الأدلة الرقمية وترشيد وتطوير أدائهم.
٤. تدريب وتأهيل المختصين بأجهزة العدالة الجنائية على كيفية التعامل مع الأدلة الرقمية.
٥. إتباع كافة وسائل التوعية الأمنية للحد من مخاطر الجريمة الإلكترونية.

يقصد بالدور الفني إتباع أساليب المكافحة الإلكترونية للجرائم من خلال الاستخدام الأمثل للوسائل التكنولوجية والإلكترونية المتمثلة في نظم الحاسبات الآلية والاتصالات متلازمتين.

- **أثر التشريعات والقوانيين في الحد من الجرائم السيبرانية**

تعتبر مكافحة الجرائم السيبرانية تحدياً، خاصةً فيما يتعلق بمشكلات السلطة القضائية التي تنشأ على المستويين الدولي والوطني، حيث تستند الأشكال التقليدية للولاية القضائية على مفهوم الحدود، كما تستند القوانين على السيادة الإقليمية، بينما الفضاء الإلكتروني ليس له حدود مادية، وأنما يمكن للمجرمين تغيير مواقعهم من بلد إلى آخر في غضون ثوان في عالم الإنترنت، وذلك بغض النظر عن موقعهم الفعلي. ويعد الأمن السيبراني هدفاً عاماً لطبيعة الجريمة السيبرانية، المادة الرابعة من نظام الجرائم المعلوماتية السعودية تنص على أنه (يهدف هذا النظام إلى الحد من وقوع الجرائم المعلوماتية، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها مما يؤدي إلى المساعدة على تحقيق الأمن السيبراني، وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية حماية المصلحة العامة والأخلاق والآداب العامة حماية الاقتصاد الوطني).

لكن تزداد الجرائم السيبرانية يومياً بسبب زيادة عدد شبكات الإنترنت، لذا من الضروري حماية بيانات مستخدمي هذه الشبكات من تلك الجرائم التي تتخذ أشكالاً مختلفة من التسلط والمضايقات الإلكترونية وغيرها من أشكال جرائم الإنترنت، ولمكافحة خطر تلك الجرائم من الضروري، فهم هذه الجرائم تقنياً لتمكين المسئولين القانونيين من تحليل أطراف هذه الجرائم، والتقنيات المستخدمة فيها، وتلك الجرائم نفسها.

لذا من الضروري أن يكون لدى الدول أدوات قانونية خاصة بها لمكافحة الجرائم السيبرانية، كما يجب أيضا أن يتم توحيد هذه القوانين.

ومن الآثار المترتبة على التشريعات القانونية أن الحماية المدنية لبرامج الحاسب الآلي تتم بتقرير التعويضات المناسبة عن طريق تعويضات لجبر الضرر بأن يدفع لصاحب الحق تعويضات عن الضرر الذي لحق به.

كما ساهمت التشريعات في الحد من الإرهاب الإلكتروني الذي يتمثل في اتخاذ الجماعات الإرهابية مواقع لها على الإنترنت لتمارس أعمالها كالتحريض على القتل وتعليم صنع القنابل والمتفجرات ونشر الأفكار الإرهابية، بالإضافة إلى حماية اقتصاديات المؤسسات التجارية ومؤسسات الدول والمجتمعات ومحاولة التصدي إلى الجرائم الدولية المنظمة وحماية المواطنين من سرقة أرقام البطاقات الائتمانية وبث الفساد في التجارة الإلكترونية كما ساهمت التشريعات في حماية حقوق المؤلفين ومن نسخ البرامج من الإنترنت وبيعها في السوق السوداء.

كما تعمل التشريعات والقوانين على الحد من الجرائم السيبرانية والحد من وقوع جرائم المعلومات وذلك بتحديد الجرائم والعقوبات المقررة لكل منها مما يؤدي إلى المساعدة على تحقيق الأمن المعلوماتي، وحفظ الحقوق المترتبة على الاستخدام المشروع لبرامج الحاسبات الآلية والشبكات المعلوماتية حماية المصلحة العامة والأخلاق والآداب العامية، بالإضافة إلى حماية الاقتصاد الوطني.

وتعمل التشريعات القانونية على حماية الحقوق القانونية للملكية الفكرية في البيئة الرقمية بالإضافة إلى تحديد وحفظ حقوق المؤلف والحقوق المجاورة ومعايير الحماية اللازمة لمواجهة ما تتعرض لها هذه الحقوق وتحديد المصنفات محل الحماية وذلك عن طريق إعادة النظر في مدى صلاحية التشريعات الحالية بشأن حماية حقوق الملكية الفكرية في البيئة الرقمية لمواجهة الانتهاكات المتطورة التي تدعمها الخبرات والبراعة الفنية لمرتكبي هذه الجرائم وفرض العقوبات الرادعة على مرتكبيها.

وللقوانين دوراً مهم في السعي نحو حماية برامج الحاسوب ومواقع الويب، وخاصةً المواقع الإلكترونية الحكومية بالإضافة إلى الحماية من جميع أنواع الهجمات بشكل عام وذلك لأن أنظمة المعلومات والأنظمة الأخرى تحتاج إلى حماية قانونية وتدابير أخرى، لمقاومة ذكاء مجرمي شبكات المعلومات والمتسللين المهرة فلا بد من سن قوانين تقيد قدرات هؤلاء المجرمين.

بالإضافة إلى حرص التشريعات القانونية على التخلص من الآثار الاجتماعية للجرائم السيبرانية ومنها استخدام التكنولوجيا الحديثة في عمليات غسيل الأموال مما يسبب حدوث خلل هيكلي في المجتمع بسبب صعود المجرمين إلى أعلي الهرم الاجتماعي في الوقت الذي يتراجع فيه مركز المجدين كما تعمل التشريعات على الحد من انتشار الجريمة في المجتمع بسبب انخفاض القيم الأخلاقية والأدبية لأي مجتمع أو حكومة تستمد إيراداتها من أنشطة إجرامية.

كما أن تفعيل قانون حماية الملكية الفكرية يشكل التربة الصالحة لدعم وتشجيع الإبداع والمبدعين في شتى مجالات المعرفة البشرية، حتى لا تكون هذه القوانين حبراً على ورق مما يتسبب لهذه الكفاءات في الهجرة من بلدانهم النامية إلى الدول المتقدمة التي تتمتع بمستوى معيشة مرتفع وتتسم بإطلاق الحريات والحقوق الفكرية ومن ثم إفراغ هذه البلدان من قادة مسيرة نهضتها العلمية والتكنولوجية.

بالإضافة إلى الحد من أثار الجرائم الإلكترونية التي قد تستهدف أمن الأشخاص وممتلكاتهم، حيث تعددت الأساليب الإرهابية في التهديد بالقتل لشخصيات سياسية إلى التهديد بتفجيرات في مراكز سياسية أو تجمعات رياضية والتهديد بإطلاق الفيروسات لإتلاف الأنظمة المعلوماتية في العالم.

يعتبر الإنترنت من أهم التطورات التي توصلت إليها البشرية، وتعد السلوكيات الإجرامية من أقدم الظواهر والآفات التي ظهرت منذ وجود الإنسانية، حيث إن الجريمة من الممكن أن تتجسد في العديد من الصفات والتي من بينها الجرائم الإلكترونية لذا كأن من الضروري إيجاد التشريعات وقوانين تعمل على الحد من انتشار هذا النوع من الجرائم كي يتمكن الأفراد على مستوى العالم من الاستفادة منه دون خوف أو قلق حيث يعتبر الإنترنت من أهم الوسائل التي نتجت عن التطورات المتتالية لتكنولوجيا المعلومات والاتصال.

كما تعمل التشريعات على حماية التجارة الإلكترونية التي تعد إحدى أهم الظواهر التكنولوجية الحديثة في اقتصاد المعرفة والمحرك الأساسي له وفي ظل ما يشهده العالم من تغيرات كبيرة شملت مختلف القطاعات مما يساهم في دفع عجلة التنمية الاقتصادية وتعزيز التنافسية الوطنية، ونظراً للتطور المتزايد لشبكة الإنترنت والاعتماد شبه الكامل على الفضاء الإلكتروني، زادت معدلات انتشار الجريمة الإلكترونية مما استدعى إلى سن التشريعات والقوانين ووضع استراتيجيات فعالة للتأمين على مخاطر الجريمة الإلكترونية.

كذلك تعمل على الحد من تطور الجريمة من الجانبي الاجتماعي والقانوني الاجتماعي نظراً لأن الجريمة ظاهرة من الظواهر الاجتماعية المسلم بها ويعد ارتكابها مخلاً بالنظام الاجتماعي وهذا ما يقتضى الرجوع إلى القوانين من أجل مواجهتها بكل الوسائل التي تؤدى إلى الحد من ارتكابها، بالإضافة إلى الجانب القانوني الذي يعمل علي سياسة التجريم والعقاب أولا عن طريق تحديد المصالح المحمية والأفعال التي يمكن أن تهددها وثانيا عبر تجريمها وتحديد العقوبة المناسبة لها ويتم التعامل مع وقوعها وفق هذه السياسة عن طريق إثباتها ثم معاقبة مرتكبيها.

وتعمل على حماية المعلومات حيث إن فيض المعلومات الذي يوجه الشعوب أصبح العصب لجهود التنمية والتحديث حيث يغطي كل مجالات الحياة المعاصرة، العملية والاقتصادية والاجتماعية والتعليمية والدينية، حيث أضحى للمعلومة دور مهم جداً وحيوي في نتاج البشر وتدبير الأمور أصبح يقاس بمدى التقدم في أي مهنة أو دولة أو مؤسسة أو فرد بما يتوافر لدى كل منها من مستودع لا يتناقص من المعلومات، كما تعمل القوانين على حماية تكنولوجيا المعلومات التي تعمل على تحسين كفاءة المنظمات وفاعليتها.

ولما كأنت الجرائم السيبرانية جرائم حديثة فرضت نفسها محلياً ودولياً كأن على الجهات التشريعية المحلية والدولية أن تواجهها بتشريعات حاسمة لمكافحتها وتقديم مرتكبيها للعدالة، حيث تعمل القوانين والتشريعات واللوائح على الحد من انتشار تلك الجرائم على الصعيدين الدولي والمحلى ومنع الاستخدام غير المشروع للتكنولوجيا الحديثة عن طريق فرض العقوبات والغرامات لكي تكون رادع لمن يتجرأ على ارتكاب مثل هذه الجرائم المخربة التي تستهدف أمن المواطنين وأموالهم ومملكاتهم المادية أو الفكرية.

وتعمل على الحد من استخدام الآليات الحديثة في ارتكاب الجرائم صاحبة التداعيات الخطيرة في المجتمع نظراً لأنه بقدر استخدام التطور والتقدم في ارتكاب الجرائم بقدر ما تحدثه من آثار خطيرة على كافة الجوانب والمستويات في المجتمع وذلك نظراً للميزات التي تختلف بها الجرائم المستحدثة عن الجرائم التقليدية، كما تعمل التشريعات على حماية الأمن الاجتماعي من التهديد، نظراً لأن تهديد الأمني الاجتماعي على رأس التهديدات التي تحدثها هذه النوعية من الجرائم نظراً لكونها تمس كافة الأطراف في المجتمع من دول ومؤسسات وأفرد .

وعلى الرغم من الرقابة القوية لأمن المعلومات والتي وفرت ضمانات جوهرية لحماية أمن المعلومات والحد من الوصول غير المرخص لها وكذلك التحريف والسرقة إلا أن التطورات الحديثة التي حصلت في نظم المعلومات وشبكات الاتصالات قللت من فاعلية الرقابة التقليدية لذا كأن لزاماً علينا وضع التشريعات والقوانين التي تمنع وتعاقب كل مرتكبي هذه الجرائم المتمثلة في اختراق أمن المعلومات وسرقتها وتحريفها وتشويهها وإساءة استخدامها أو تسريبها خارج القنوات المخصصة لها أو الرخصة بتداولها والاستفادة منها.

كما أن كثيراً من الأفراد الذين يقومون بعمليات البيع والشراء عبر الإنترنت أو الذين يقومون بالمضاربات وبيع وشراء الأسهم أو الذين يقومون بالتعاون مع المصارف الإلكترونية يقومون بتزويد الشركات البائعة بمعلومات غاية في الأهمية والسرية مثل أرقام بطاقات الاعتماد والبطاقات الوطنية وأرقام الهاتف والعناوين وغيرها من المعلومات الغاية في السرية والحساسية والأهمية وكل هذه المعلومات يتم تزويدها عبر المواقع الإلكترونية حيث تكون مهددة بالكشف أو الاعتراض لذا كأن لزاماً فرض القوانين والتشريعات التي تحمى تلك المعلومات وتحول دون المخترقين وبينها حفاظا على أمن وخصوصية الأفراد.

وقد أحدثت التقنية العالية منذ نهاية الستينيات آثاراً واسعة على العلاقات والتصرفات القانونية واستوجبت واستلزمت من موجات متلاحقة من التشريعات من أجل حماية أمن المعلومات والحماية من جرائم الكمبيوتر والإنترنت وفرض الحماية على مسائل الخصوصية وحماية الحياة الخاصة بالإضافة إلى حماية المسائل الفكرية للمصنفات الرقمية كالبرمجيات والدوائر المتكاملة وقواعد البيانات، وأسماء نطاقات وعناوين الإنترنت وحماية محتوى المواقع المعلوماتية وكذلك في حقول المعايير والمقاييس التقنية وفي حقل قواعد الإثبات والإجراءات الجنائية وما تبعها من مسائل الاختصاص والقانون.

بالإضافة إلى أن المعلومات والقوانين تعمل على حماية الحياة الخاصة للأفراد، كما تعمل على حماية حقوق الملكية الفكرية وتعمل على الحد من المواقع والخدمات التي تساعد على إفساد الأخلاق وتهدد أمن البلاد، وذلك بالإضافة إلى الحماية من سرقة الأموال وتزوير البيانات والتصدي لعمليات الاحتيال الإلكتروني لذا كأن لزاماً على الدول إقرار حماية جنائية للحاسب بإيجاز بأن المشرع نجح في إقرار الحماية الجنائية لجهاز الحاسب وبرامجه وللأنترنت سينجح في تحقيق إيجابياته وتفادي سلبياته.

❖ التعاون الدولي في مواجهة جرائم الإنترنت

كانت مجرد شبكة صغيرة أصبحت الأن تضم ملايين المستخدمين حول العالم، وتحولت من مجرد شبكة بحث أكاديمي إلى بيئة متكاملة للاستثمار والعمل والإنتاج والإعلام والحصول على المعلومات، وفي بداية تأسيس الشبكة لم يكن ثمة اهتمام بمسائل الأمن بقدر ما كأن الاهتمام ببنائها وتوسيع نشاطها إلا أنه بعد إتاحة الشبكة للعموم بدأ يظهر على الوجود ما يسمى بالجرائم المعلوماتية على الشبكة أو بواسطتها، وهي جرائم تتميز بحداثة الأسلوب وسرعة التنفيذ وسهولة الإخفاء والقدرة على محو آثارها وتعدد صورها وأشكالها، إضافة إلى اتصافها بالعالمية وعبورها للحدود، وقد صاحب تطور شبكة الإنترنت وانتشارها الواسع والسريع ظهور العديد من المشاكل القانونية ، فظهر على الساحة القانونية مصطلح جديد عرف باسمً الفراغ القانوني لشبكة الإنترنت ، تجاه ذلك كأن لابد من تكاتف جهود الدول من أجل مكافحة هذا النوع المستحدث من الجرائم التي لم تعد تتمركز في دولة معينة ولا توجه إلى مجتمع بعينه بل أصبحت تعبر الحدود لتلحق الضرر بعدة دول ومجتمعات مستغلة التطور الكبير للوسائل التقنية الحديثة في الاتصالات وتعزيز التعاون بين هذه الدول واتخاذ تدابير فعالة للحد منها والقضاء عليها ومعاقبة مرتكبيها .

ولمواجهة الصعوبات التي تواجه التعاون الدولي في مكافحة جرائم الإنترنت كأن لا بد من اتخاذ إجراءات سريعة تتمثل في تحديث التشريعات الوطنية المتعلقة بالجرائم المعلوماتية وجرائم الإنترنت وإبرام اتفاقيات (دولية، إقليمية، ثنائية) لمواجهة القصور في التشريعات والقوانين الحالية ، ومعالجة حالات تنازع القوانين والاختصاص القضائي وتحديث الإجراءات التحقيقية الجنائية بما يتناسب مع التطور الكبير الذي تشهده تكنولوجيا المعلومات والاتصالات ، وتأهيل القائمين على أجهزة تنفيذ القانون لتطوير معلوماتهم حول هذا النوع المستحدث من الجرائم وهو ما نبهت إليه الأمم المتحدة وغيرها من التنظيمات الدولية ذات العلاقة على المستويات العالمية والإقليمية ونظراً لتميز جرائم الإنترنت بالعالمية، تم صدور قوانين دولية وبذل الجهود لاتخاذ تدابير فعالة يوجد بعض الاتفاقيات المقررة لمكافحة الجريمة بصورة عامة خاصة المنظمة و العابرة للحدود و التي تنطبق تماماً مواصفات جرائم الإنترنت ،فقد وجدت معاهدات سُنت خصيصاً لمكافحة جرائم الكمبيوتر و الإنترنت.

○ أولا: معاهدات لمكافحة الجريمة عموما

حددت جملة من تدابير مكافحة الجرائم المتصلة بالحواسيب في اطار مؤتمر الأمم الحادي عشر لمنع الجريمة والعدالة الجنائية المنعقد في بانكوك في الفترة ١٨– ٢٥ / ٢٠٠٥/٤ ،و الذي جاء من بين صفحاته ضرورة التعاون الدولي على المستوى القضائي لتخطي حدود الدولة الواحدة للتحقيق في الجريمة ، و يمكن الاعتماد في مجال جرائم الإنترنت على اختصاصات المنظمة الدولية للشرطة الجزائية (Interpol) ، المنشأة بموجب المؤتمر الدولي المنعقد في بروكسل في الفترة من ٦–١٩٤٦/٦/٩ والذي يقوم على مبادئ التعاون الأمني الدولي، بالنسبة للدول الأعضاء، لتقفي أثر المجرمين ومتابعتهم.

وبانعقاد المجلس الأوروبي في لكسمبورج عام ١٩٩١، أنشأت الشرطة الأوروبية لملاحقة جناة الجرائم العابرة للحدود وفي نفس السياق أقام مجلس الوزراء العرب مكتب عربي للشرطة الجنائية يهدف لتنمية التعاون بين الشرطة العربية، والاتفاقية الأوروبية لتسليم المجرمين ١٩٥٧.

يعد إجراء تسليم المجرمين من أهم الإجراءات يدخل من جهة ضمن التعاون الدولي ومن جهة ساهم كثيراً في متابعة جناة الجرائم الإلكترونية، والذي كأن موضوع اتفاقيات دولية وإقليمية مثل اتفاقية الرياض لتعاون دول الخليج ١٩٩٤، اتفاقية التعاون الأممي وتسليم المجرمين للمملكة العربية السعودية ١٩٨٢، اتفاقية بين الجزائر وبلجيكا سنة ١٩٧٠.

- **ثانيا: الاتفاقيات الخاصة بمكافحة جرائم الإنترنت**

جاء في اتفاقية الأوروبية للجرائم المعلوماتية الموقعة بتكليف من المجلس الأوروبي، و التي أبرمت لمساعدة الدول في مكافحة جرائم الإنترنت، في مادتها ٢٤ جملة من الأفعال التي يمكن أن يطبق بشأنها أسـلوب تسليم المجرمين منها : الدخول غير المشروع، الاعتراض غير المشروع ، كما تضمنت الاتفاقية جانب أخر من التعاون هو تدريب مسؤولي الأمن، لإكسابهم خبرات عملية مثل ما ورد في التوصية الصادرة عن اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجرائم المعلوماتية بدول مجلس التعاون الخليجي وهي عملية شملت الكثير من الأجهزة الأمنية عبر العالم مثل كندا ، والجزائر التي أعدت برنامج لمدارس الأمن وأرسلت قضاة للتدريب في الولايات المتحدة الأمريكية ،تم تنظيم الكثير من التظاهرات لتدريب رجال العدالة ،منها المؤتمر الدولي الأول لقانون الإنترنت الذي عقد بالغردقة جمهورية مصر العربية في الفترة من ٢١ الى ٢٠٠٥/٠٨/٢٥ بتنظيم من المنظمة العربية للتنمية الإدارية ، والمؤتمر الدولي لأمن المعلومات الإلكترونية والذي عقد بمسقط – سلطنة عمان– في ١٨/ ١٢ /٢٠٠٥ و غيرها من الندوات المشتركة و أهمها ما عقد في شهر ديسمبر بالجزائر والذي جمع بين مجموعة خبراء أجانب وجزائريين ، لشرح معنى جريمة الكمبيوتر والإنترنت وسبل مكافحتها وتقنيات ارتكابها.

وتعد الولايات المتحدة الأمريكية، من الدول المتطورة تقنيا في مجال مكافحة الجرائم المعلوماتية والشبكات، وهي تساعد على تدريب أجهزة الشرطة وقضاة الدول الأخرى، بتمكينها من تعزيز قدراتها على ضبط مشاكل الجرائم الإلكترونية فقد أوجدت وزارة العدل الأمريكية مكتب للمساعدة والتدريب لتطوير أجهزة الادعاء العام في الدول الأخرى، ويعمل إلى جانبه البرنامج الدولي للمساعدة والتدريب (ICITAP) لتوفير المساعدات لأجهزة الشرطة بالدول النامية.

يوجد بعض العقبات التي تعرقل التعاون الدولي، مثل عدم وجود نموذج موحد للنشاط الإجرامي، فيجب إيجاد تشريعات داخلية تقرب وجهات النظر، حتى يأخذ التعاون مجراه مثل قانون حماية الملكية الفكريـــــة، والإجراءات الجزائية، التشفير.... ، وتساهم الاتفاقيات والصكوك الصادرة عن منظمة الأمم المتحدة كثيراً في استخدام تقنيات خاصة للتخفيف من شدة اختلاف النظر القانونية مثل التسليم المراقب، المراقبة الإلكترونية وغيرها من أشكال المراقبة وهو ما أخذت به الجزائر في تعديلها لقانون الإجراءات الجزائية .

وقد تناولت الاتفاقية الأوروبية للإجرام المعلوماتي في مادتها ٢٩ على سرية حفظ البيانات المعلوماتية المخزنة، وحق كل طرف أن يطلب من الأخر الحفظ السريع للمعلومات المخزنة، عن طريق إحدى الوسائل الإلكترونية الموجودة داخل النطاق المكاني للطرف الأخر، والتي ستكون محلا لطلب المساعدة من الطرف الأول بغرض التفتيش أو الدخول ، ضبط أو الكشف على البيانات المشار اليها، وهو الطلب الذي يجب الاستجابة إليه طبقا للمادة ٣٠ من الاتفاقية ، وعلى المعني تقديم المساعدة للطالب على وجه السرعة للكشف عن هوية مؤدي الخدمة ومصدر الاتصال وقد أجازت اتفاقية المساعدة للدخول للبيانات المحفوظة طبقاً للمادة ٣١ منها ،وسمحت المادة ٣٢ من الاتفاقية بالدخول للبيانات المخزنة خارج نطاق الحدود بشرط وجود اتفاقيات أو أنها بيانات متاحة للجمهور.

وأقرت المادة ٣٣ وجوب تعاون الدول الأطراف في حالة التجارة غير المشروعة، وركزت الاتفاقية في المادة ٣٤ على البيانات المتداولة بالاتصالات عبر الشبكة وقد دعت الاتفاقية الدول الأعضاء لأنشاء نقطة اتصال تعمل لمدة ٢٤ ساعة لتامين المساعدة المباشرة للتحقيقات واستقبال الأدلة ذات الشكل الإلكتروني.

جرائم الإنترنت تبقى دائماً بحاجة لعقد اتفاقيات توحد نظريات الاختصاص وتتبنى نفس الإجراءات لحل هذا المشكلة، ومواكبة الجريمة التي تتسارع، ولقد سمحت الاتفاقية للطرف في الحالات الطارئة طلب المساعدة القضائية الدولية عملا بالمادة ٢٥ منها، عن طريق وسائل الاتصال السريعة ً فاكس، بريد الكتروني والذي يتلقى الرد بنفس الطريقة.

- **ثالثا: اتفاقية بودابست لمكافحة جرائم الإنترنت ٢٠٠١**

أبرم المجلس الأوروبي اتفاقية بودابست في ٢٠٠١/١١/٨ ووضعت للمصادقة في ٢٠٠١/١١/٢٣، والتي تضمنت التعريف بأهدافها ووضعت قائمة للجرائم التي يجب على الدول المصادقة عليها أن تجرمها في قوانينها الداخلية، والتي وقعت عليها ٣٠ دولة.

تعد الأولى في مجال مكافحة جرائم الإنترنت وشملت العديد من جرائم الإنترنت منها: الإرهاب، تزوير بطاقات الائتمان، وغيرها وتعمد الاتفاقية الى تنسيق القوانين الجديدة في دول عديدة، وجاءت نتيجة مشاورات طويلة بين الحكومات وأجهزة الشرطة وقطاع الحاسب، وصاغ نصها عدد من الخبراء في مجلس أوروبا بمساعدة عدة دول منها الولايات المتحدة.

وتحدد الاتفاقية أفضل الطرق الواجب اتباعها للتحقيق في جرائم الإنترنت، التي تعهدت الدول الموقعة بالتعاون الوثيق من أجل محاربتها تحاول الاتفاقية الموازنة بين جهات المتابعة وصلاحياتها وبين احترام حقوق الأنسان ومصلحة مستخدمي ومزودي الخدمة، وخشيت البنوك من تطبيق الاتفاقية الذي ستؤدي لنشر عيوبها الأمنية على، بينما خاف مزودي الخدمة على أن يحملهم ذلك تكاليف باهظة في سبيل تخزين البيانات لاستعمالها مستقبلا في جمع الإثباتات في حالة المتابعة.

كما أبرمت الكثير من المعاهدات في مجال حماية حقوق المؤلف والحقوق المجاورة والمصنفات من القرصنة **مثل:** معاهدة برن ١٩٨١ المنعقدة في سويسرا التي، معاهدة تريبس عام ١٩٩٤ ، معاهدة الويبو.

اتفاقية برن

لحماية المصنفات الأدبية والفنية وتعرف باتفاقية برن وهي اتفاقية عالمية تعنى بحماية الحقوق الفكرية للمؤلفين وغيرهم، تم عقدها لأول مرة في برن، سويسرا عام ١٨٨٦م ووقعت عليها ١٢٠ دولة وقد تم التعديل عليها في مؤتمرات ومناقشات مختلفة وآخر نسخة تم اعتمادها كانت في باريس.

الاتفاقية حول الجوانب التجارية لحقوق الملكية الفكرية أو اتفاق تريبس

اختصارا لـTrade Related Aspects of Intellectual Property Rights هي اتفاق دولي تديره منظمة التجارة العالمية الذي يحدد المعايير الدنيا للقوانيين المتعلقة بالعديد من أشكال الملكية الفكرية كما تنطبق على أعضاء منظمة التجارة العالمية.

معاهدة الويبو

بشأن حق المؤلف هي اتفاق خاص في إطار اتفاقية برن وتتناول حماية المصنفات وحقوق مؤلفيها في البيئة الرقمية، وفضلاً عن الحقوق المنصوص عليها في اتفاقية برن، تمنح هذه المعاهدة بعض الحقوق الاقتصادية للمؤلفين، وتتناول المعاهدة أيضا موضوعين يتعين حمايتهما بموجب حق المؤلف **وهما:**

١. برامج الحاسوب، أيا كانت طريقة التعبير عنها أو شكلها.

٢. مجموعات البيانات أو المواد الأخرى (قواعد البيانات).

❖ جهود المملكة العربية السعودية في مجال الأمن السيبراني وطرق مكافحتها

خدمة ترشيح محتوى الإنترنت

بهدف حماية المجتمع السعودي من أخطار الإنترنت الضارة وضمان تقديم المحتوى الجيد تقوم هيئة الاتصالات وتقنية المعلومات بتقديم خدمة ترشيح محتوى الإنترنت في المملكة وذلك من خلال وضع الضوابط والمتطلبات الخاصة بترشيح خدمات الإنترنت بالتنسيق مع اللجنة الأمنية الدائمة للأنترنت كما توفر قوائم خاصة بالمواقع المحجوبة يومياً لمزودي خدمة المعطيات ويتم حجب المواقع والمواد التي تتنافي مع الدين الحنيف والأنظمة الوطنية.

سياسة الخصوصية وسرية المعلومات للتعاملات البنكية الإلكترونية

يقوم كل قطاع بنكي بنشر سياسات الخصوصية والسرية على الموقع الرسمي للبنك ويقر البنك بحقوق العميل المتعلقة بسرية البيانات الشخصية التي يقدمها للبنك خلال أدائه المعاملات المصرفية عبر الإنترنت والبنك ملتزم بتوفير مستوى عالي من الأمن والسرية لأي معلومات تتعلق بخدماته البنكية التي يقدمها للأفراد عبر الإنترنت ويضمن معالجة أي عملية مصرفية تتم عبر الإنترنت وأي معلومات شخصية أو مالية يتم تبادلها بمثل هذه الوسائل بطريقة مأمونة ومشفرة تلتزم بالمعايير الأمنية الخاصة بالصناعة.

جهود هيئة الاتصالات السعودية

تولي هيئة الاتصالات وتقنية المعلومات اهتماماً بالتثقيف بسلامة أمن المعلومات ونشر الوعي في المجتمع السعودي وخدمتهم في تقديم أحدث المستجدات في مجال تأمين المعلومات بجانب توفير معلومات شاملة وموسعة عن كل ما من له صلة بأمن المعلومات والتقنيات المرتبطة فيها وأسست الهيئة مركزاً وطنياً يكون مقصداً لكل من يحتاج إلى إرشادات أو معلومات أمنية عن أي نوع من التقنيات ذات الصلة بمهام هيئة الاتصالات وتقنية المعلومات وأطلق عليه المركز الوطني الإرشادي لأمن المعلومات.

هذا المركز الوطني هو مركز غير ربحي يهدف إلى رفع مستوى الوعي والمعرفة بأخطار أمن المعلومات ويعمل بالتعاون مع أعضائه وشركائه على تنسيق جهود الوقاية والتصدي للأخطار والحوادث المتعلقة بالأمن الإلكتروني في المملكة العربية السعودية.

- **أهداف المركز**

١. رفع مستوى الوعي بأمن المعلومات في المملكة العربية السعودية.

٢. تنسيق الجهود على المستوى الوطني لتفأدي الاختراقات الأمنية والعمل على احتواء أضرارها في حال وقوعها.

٣. رفع مستوى الثقة في التعاملات الإلكترونية.

٤. التعاون والتنسيق مع المؤسسات والأطراف المؤثرة في تقديم خدمات الاتصالات وتقنية المعلومات في المملكة العربية السعودية في سبيل وقاية البنى التحتية والخدمات الإلكترونية من أخطار وتهديدات أمن المعلومات.

٥. تقديم المشورة والنصح للأفراد والمؤسسات فيما يتعلق بأمن المعلومات.

٦. التوعية توفير الوعي الأمني لدى المستفيدين من خلال برنامج يسهل الفهم في المواضيع المتعلقة بالقضايا الأمنية.

٧. التدريب والتعليم من خلال الدورات التدريبية والمؤتمرات وورش العمل والدروس التعليمية.

- **جهود المركز في خدمات المبادرة**

- **الإعلانات:** التركيز على القضايا الطويلة والمتوسطة الأجل مثل الثغرات المكتشفة حديثا أو أدوات المخترقين.

- **نشر المعلومات الأمنية:** يشمل نشر معلومات أمنية شاملة توفر سهولة العثور على مجموعة من المعلومات المفيدة التي تسعى لتحسين الوضع الأمني.

- **التحذير والتنبيه:** نشر المعلومات المتعلقة بالقضايا الأمنية.

- **التعامل مع الاختراقات الأمنية:** استقبالها وفرزها وتصنيفها وترتيبها حسب الأولوية وتحليلها ومعالجة الحدث.

- **التعامل مع الثغرات الأمنية:** استقبال معلومات حول الثغرات الأمنية وتحليلها واقتراح استراتيجيات لحلها لضمان عدم وقوعها.

❖ قوانين مكافحة الجرائم الإلكترونية وتشريعاتها عربياً

نظراً لتزايد مشكلة الجريمة الإلكترونية تعددت محاولات مكافحتها من الناحية القانونية والناحية الفنية، من الجهود التي بذلتها الدول العربية بشأن مكافحة الجرائم السيبرانية:

– اتفاقية الجرائم السيبرانية العربية: تم التوقيع عليها في المملكة العربية السعودية، وتتصدى هذه الاتفاقية بشكل أساسي لزيادة الجرائم السيبرانية التي تشمل جرائم تزوير بطاقات الائتمان وجرائم الإنترنت والإرهاب السيبراني، وإنتاج الفيروسات أو نشرها، والقرصنة، واختراق الأنظمة، والوصول غير المصرح به، والتنصت، كما تهدف أيضا إلى تشجيع الدول العربية في مجال مكافحة الجرائم، وتنص الاتفاقية أيضا على أهمية تنفيذ قانون حقوق التأليف والنشر، وفرض عقوبات على منتهكي بنود الاتفاقية وقوانينها.

– الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: وتنص المادة السادسة من هذه الاتفاقية على تجريم الوصول غير المشروع أو الإحضار أو التوصل إلى جزء من تقنيات المعلومات أو إلى جميعها، وفي نفس الوقت تضاعف هذه الاتفاقية العقوبات إذا أدى السلوك الوصول أو الإحضار أو التوصل إلى إلغاء، أو تعديل، أو تشويه، أو تكرار، أو إزالة، أو إتلاف البيانات المحفوظة والأدوات والأنظمة الإلكترونية وشبكات الاتصالات، وكذلك إلحاق الضرر بالمستخدمين والمستفيدين أو الحصول على معلومات حكومية سرية.

– وقد سارعت العديد من الدول العربية من أجل سن قوانين خاصة بها بالجرائم الإلكترونية: وعلى سبيل المثال المملكة العربية السعودية والإمارات العربية المتحدة والمغرب.

دولة الإمارات العربية المتحدة تم إصدار القانون الاتحادي رقم (٢) لعام ٢٠٠٦ الخاص بمنع جرائم تكنولوجيا المعلومات، في وقت تم الاعتراف فيه بقضايا الأمن السيبراني، كقضايا عالمية تتطلب من كل دولة وضع مثل هذه القوانين، وفي عام ٢٠١٢ تم تحديث هذا القانون مرة أخرى،

وأيضا المملكة الأردنية الهاشمية، فعلى الرغم من عدم وجود أحكام بالمحاكم الأردنية خاصة بالجرائم السيبرانية، إلا أنه يتم إدراجها تحت الأحكام السارية على الجرائم الجنائية.

كما **في الجمهورية المصرية** تم إصدار قانون الملكية الفكرية رقم ٨٢ عام ٢٠٠٢م الخاص ببرامج الحاسب الآلي، اعتبر المشرع برامج الحاسب الآلي من قبيل المصنفات الأدبية والفنية المشمولة بحماية هذا القانون سواء كانت بلغة المصدر أو بلغة الآلة ومهما كانت قيمتها أو نوعها، فالبند الثاني من ١٤٠ منه نص على أن تتمتع بحماية هذا القانون حقوق المؤلفين على مصنفاتهم الأدبية والفنية وبوجه خاص مصنفات الحاسب الآلي. وقد **نص المشرع الجزائري** على عقوبة جريمة الدخول إلى النظام أو البقاء غير المشروعين في صورتها المشددة في المادة ٣٩٤ بقوله (تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب لنظام اشتغال المنظومة تكون العقوبة الحبس مدة لا تقل عن ٦ أشهر ولا تزيد عن سنتين وغرامة لا تقل عن خمسين ألف دينار (٥٠٠٠٠) ولا تزيد عن مائة وخمسين ألف دينار (١٥٠٠٠٠).

ويعد القانون التونسي المتعلق بالتجارة الإلكترونية رقم ٨٣ لسنة ٢٠٠٠ الخاص بالمبادلات الإلكترونية أول تشريع يتعرض للجرائم الإلكترونية الذي بين أحكاماً خاصة بالمبادلات التجارية الإلكترونية، كما نصت المادة ٤٨ من القانون التونسي أن معرفة أي أسرار تتعلق بالشفرة الخاصة بالتوقيع الإلكتروني ويتم ذلك عن طريق اختراق منظومة معلوماتية وفك رموز الشفرة أو كلمة السر ونشرها واستعمالها بدون وجهي حق عوقب بالحبس مدة لا تتراوح بين ستة أشهر إلى سنتين وغرامة مالية لا تقل عن ألف ولا تزيد عن عشرة ألاف دينار تونسي.

– **سعي الدول العربية لإيجاد اتفاق عام بينها على مفهوم الجرائم الإلكترونية:** مع محاولة وجود اتفاق بين القوانين والإجراءات الجنائية للدول بشأن التحقيق في تلك الجرائم ومعالجة النقص في مجال الخبرة لدى الشرطة وجهات الادعاء والقضاء على الصعيد العربي، مثل اجتماعات تم عقدها في إطار التنسيق بين القضائية العربية التي تسمي اتفاقية عمان للتعاون العلمي بين المعاهد القضائية العربية التي وقعت في ٩ أبريل ١٩٩٧ .

– أمن المعلومات في الحاسبات الآلية والاتصالات ١٩٨٦: ونظمها مركز المعلومات الوطني السعودي في الرياض، ندوة حول الجرائم الناجمة عن التطور التكنولوجي (الأردن١٩٩٨)، ندوة المواجهة الأمنية للجرائم المعلوماتية دبي (١٩٩٩) ندوة دراسة الجرائم المستحدثة بأكاديمية نايف العربية للعلوم الأمنية الرياض ٢٠٠٠، المؤتمر الخليجي لأمن الإنترنت في مسقط ٢٠٠١، ندوة الجرائم الإلكترونية في مسقط،٢٠٠٢، مؤتمر أمن المعلومات العربية في القاهرة،٢٠٠٢، ندوة الإنترنت وأمن المعلومات في ليبيا ٢٠٠٢ .

– أصدر مجلس وزراء الداخلية العرب: وقد بادرت الدول العربية على المستوى التشريعي في إصدار قانون نموذجي حول الجرائم السيبرانية حيث أصدر مجلس وزراء الداخلية العرب مشروع قانون أطلق عليه القانون العربي الموحد للأنترنت وتمت المصادقة عليه في عام ٢٠٠٤.

– الاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات: لسنة ٢٠١٢ فقد نصت في المادة الخامسة من هذه الاتفاقية بأن تلتزم كل دولة طرف بتجريم الأفعال المبنية في الفصل الثاني في الاتفاقية وذلك وفقاً لتشريعاتها وأنظمتها الداخلية.

فمن النادر وجود خلو تشريع هذه الدولة من القوانين تنظم الأمن الإلكتروني حيث صدرت القوانين العربية التي تخص الجريمة المعلوماتية مثل القانون السوداني سنة (٢٠٠٠).

❖ قوانين مكافحة الجرائم الإلكترونية في المملكة العربية السعودية

صدر قانون مكافحة جرائم المعلوماتية بقرار مجلس الوزراء رقم ٧٩ و تاريخ ١٤٢٨/٣/٧ هـ وتمت المصادقة عليه بموجب المرسوم الملكي رقم م/١٧ وتاريخ ١٤٢٨/٣/٨هـ و قد أقر مجلس الوزراء في جلسته في السابع من ربيع الأول ١٤٢٨هـ قانون مكافحة جرائم المعلوماتية الذي يهدف إلى الحد من نشوء جرائم المعلوماتية و ذلك بتحديد تلك الجرائم و العقوبات المقررة لها ، حيث فرض النظام عقوبة بالسجن لا تزيد على سنة و بغرامة لا تزيد على ٥٠٠ ألف ريال أو بإحداهما على كل شخص يرتكب أيا من الجرائم المنصوص عليها في النظام ومنها الدخول غير المشروع إلى المواقع الإلكترونية أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع أو إلغائه أو إتلافه أو تعديله أو المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف المحمولة المزودة بكاميرا أو ما في حكمها بقصد التشهير بالآخرين و إلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة و كذلك فرض النظام عقوبة السجن مدة لا تزيد عن عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال أو بإحداهما على كل شخص ينشئ موقعاً لمنظمات إرهابية على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات تلك المنظمات أو ترويج أفكارها أو نشر كيفية تصنيع المتفجرات.

هذا القانون يسعى إلى تحقيق توازن ضروري بين مصلحة المجتمع في الاستعانة بالتقنية الحديثة ومصلحة الأنسان في حماية حياته الخاصة والحفاظ على أسراره والمساعدة على تحقيق النظام المعلوماتي وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكة المعلوماتية كما يهدف إلى حماية المصلحة العامة والأخلاق والآداب العامة وكذلك حماية الاقتصاد الوطني **ونص قانون مكافحة الجرائم المعلوماتية كالتالي:**

- **قانون مكافحة جرائم المعلوماتية**

  - المادة الأولى

يقصد بالألفاظ والعبارات الآتية – أينما وردت في هذا النظام – **المعاني المبينة أمامها ما لم يقتض السياق خلاف ذلك:**

- **الشخص**

أي شخص ذي صفة طبيعية أو اعتبارية، عامة أو خاصة.

- **النظام المعلوماتي**

مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها، وتشمل الحاسبات الآلية.

- **الشبكة المعلوماتية**

ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها، مثل الشبكات الخاصة والعامة والشبكة العالمية (الإنترنت).

- **البيانات**

المعلومات، أو الأوامر، أو الرسائل، أو الأصوات، أو الصور التي تعد، أو التي سبق إعدادها، لاستخدامها في الحاسب الآلي، وكل ما يمكن تخزينه، ومعالجته، ونقله، وأنشاؤه بوساطة الحاسب الآلي، كالأرقام، والحروف، والرموز، وغيرها.

- **برامج الحاسب الآلي**

مجموعة من الأوامر، والبيانات التي تتضمن توجيهات أو تطبيقات حين تشغيلها في الحاسب الآلي، أو شبكات الحاسب الآلي، وتقوم بأداء الوظيفة المطلوبة.

- **الحاسب الآلي**

أي جهاز إلكتروني ثابت أو منقول سلكي أو لا سلكي يحتوي على نظام معالجة البيانات، أو تخزينها، أو إرسالها، أو استقبالها، أو تصفحها، يؤدي وظائف محددة بحسب البرامج، والأوامر المعطاة له.

- **الدخول غير المشروع**

دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إلكتروني، أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها.

- **الجريمة المعلوماتية**

أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام.

- **الموقع الإلكتروني**

مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد.

- **الالتقاط**

مشاهدة البيانات، أو الحصول عليها دون مسوغ نظامي صحيح.

- المادة الثانية

يهدف هذا النظام إلى الحد من وقوع جرائم المعلوماتية، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها، **وبما يؤدي إلى ما يأتي:**

1. المساعدة على تحقيق الأمن المعلوماتي
2. حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية
3. حماية المصلحة العامة، والأخلاق والآداب العامة
4. حماية الاقتصاد الوطني

- المادة الثالثة

يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، **كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:**

- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي – دون مسوغ نظامي صحيح – أو التقاطه أو اعتراضه.
- الدخول غير المشروع لتهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً.
- الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع الكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.
- المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها.
- التشهير بالآخرين، وإلحاق الضرر بهم، عبر وسائل تقنيات المعلومات المختلفة.

- المادة الرابعة

يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين، **كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:**

- الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة.
- الوصول – دون مسوغ نظامي صحيح – إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات.

- المادة الخامسة

يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين، **كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:**

- الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها، أو تغييرها، أو إعادة نشرها.
- إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها.
- إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت.

- المادة السادسة

يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين، **كل شخص يرتكب أيّاً من الجرائم المعلوماتية الآتية:**

- أنتاج ما من شأنه المساس بالنظام العام، أو القيم الدينية، أو الآداب العامة، أو حرمة الحياة الخاصة، أو إعداده، أو إرساله، أو تخزينه عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي.
- أنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للاتجار في الجنس البشري، أو تسهيل التعامل به.
- أنشاء المواد والبيانات المتعلقة بالشبكات الإباحية، أو أنشطة الميسر المخلة بالآداب العامة أو نشرها أو ترويجها.
- أنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للاتجار بالمخدرات، أو المؤثرات العقلية، أو ترويجها، أو طرق تعاطيها، أو تسهيل التعامل بها.

تم تعديل هذه المادة بموجب المرسوم الملكي رقم (م/٥٤) بتاريخ ٢٢/ ٧/ ١٤٣٦ هـ، **وذلك بإضافة النص الآتي إلى نهايتها:**

"ويجوز تضمين الحكم الصادر بتحديد العقوبة النص على نشر ملخصه على نفقة المحكوم عليه في صحيفة أو أكثر من الصحف المحلية أو في أي وسيلة أخرى مناسبة، وذلك بحسب نوع الجريمة المرتكبة، وجسامتها، وتأثيرها، على أن يكون النشر بعد اكتساب الحكم الصفة النهائية".

- المادة السابعة

يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين، **كل شخص يرتكب أيّاً من الجرائم المعلوماتية الآتية:**

- أنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أي أداة تستخدم في الأعمال الإرهابية.
- الدخول غير المشروع إلى موقع إلكتروني، 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.

- المادة الثامنة

لا تقل عقوبة السجن أو الغرامة عن نصف حدها الأعلى، **إذا اقترنت الجريمة بأي من الحالات الآتية:**

1. ارتكاب الجاني الجريمة من خلال عصابة منظمة
2. شغل الجاني وظيفة عامة واتصال الجريمة بهذه الوظيفة أو ارتكابه الجريمة مستغلاً سلطاته أو نفوذه
3. التغرير بالقصر ومن في حكمهم واستغلالهم
4. صدور أحكام محلية أو اجنبيه سابقة بالإدانة بحق الجاني في جرائم مماثلة

- المادة التاسعة

- يعاقب كل من حرض غيره، أو ساعده، أو اتفق معه على ارتكاب أي من الجرائم المنصوص عليها في هذا النظام؛ إذا وقعت الجريمة بناء على هذا التحريض، أو المساعدة، أو الاتفاق، بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها، ويعاقب بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة لها إذا لم تقع الجريمة الأصلية.

- يعاقب كل من شرع في القيام بأي من الجرائم المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة.

- المادة الحادية عشرة

للمحكمة المختصة أن تعفي من هذه العقوبات كل من يبادر من الجناة بإبلاغ السلطة المختصة بالجريمة قبل العلم بها وقبل وقوع الضرر، وأن كان الإبلاغ بعد العلم بالجريمة تعين للإعفاء أن يكون من شأن الإبلاغ ضبط باقي الجناة في حال تعددهم، أو الأدوات المستخدمة في الجريمة.

- المادة الثانية عشرة

لا يخل تطبيق هذا النظام بالأحكام الواردة في الأنظمة ذات العلاقة وخاصة ما يتعلق بحقوق الملكية الفكرية، والاتفاقيات الدولية ذات الصلة التي تكون المملكة طرفاً فيها.

- المادة الثالثة عشرة

مع عدم الإخلال بحقوق حسني النية، يجوز الحكم بمصادرة الأجهزة، أو البرامج، أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام، أو الأموال المحصلة منها، كما يجوز الحكم بإغلاق الموقع الإلكتروني، أو مكان تقديم الخدمة إغلاقاً نهائياً أو مؤقتاً متى كان مصدراً لارتكاب أي من هذه الجرائم، وكانت الجريمة قد ارتكبت بعلم مالكه.

- **المادة الرابعة عشرة**

تتولى هيئة الاتصالات وتقنية المعلومات وفقاً لاختصاصها تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة.

- **المادة الخامسة عشرة**

تتولى هيئة التحقيق والادعاء العام التحقيق والادعاء في الجرائم الواردة في هذا النظام.

- **المادة السادسة عشرة**

ينشر هذا النظام في الجريدة الرسمية ويعمل به بعد (مائة وعشرين) يوماً من تاريخ نشره.

❖ الهيئة الوطنية للأمن السيبراني

ترجمةً لنهج خادم الحرمين الشريفين الملك سلمان بن عبد العزيز وسمو ولي العهد حفظهم الله في قيادة بلادنا لتكون نموذجًا ناجحًا ورائدًا في العالم على كافة الأصعدة، ولرؤية المملكة ٢٠٣٠ التي جعلت التحول نحو العالم الرقمي وتنمية البنية التحتية الرقمية ضمن مستهدفاتها، واستشعارا لأهمية البيانات والأنظمة التقنية والبنى التحتية الحساسة وارتباطها بالمصالح الوطنية، وأهمية حمايتها من أي تهديدات أو مخاطر يشهدها الفضاء السيبراني يأتي تأسيس الهيئة الوطنية للأمن السيبراني وارتباطها بالملك –حفظه الله– وذلك وفق الأمر الملكي الكريم بالموافقة على تنظيمها بتاريخ ١١/٢/١٤٣٩ هـ لتكون الهيئة هي الجهة المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه، وتهدف إلى تعزيزه؛ حمايةً للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية , ولا يخلي ذلك أي جهة عامة أو خاصة أو غيرها من مسؤوليتها تجاه أمنها السيبراني بما لا يتعارض مع اختصاصات ومهمات الهيئة الواردة في تنظيمها.

ولقد عرف تنظيم الهيئة الأمن السيبراني على أنه: "حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، من أي اختراق، أو تعطيل، أو تعديل، أو دخول، أو استخدام، أو استغلال غير مشروع، كما يشمل هذا المفهوم أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحوها."

- **اختصاصات ومهام الهيئة**

١. وضع السياسات والمعايير وآليات الحوكمة والضوابط المتعلقة بالأمن السيبراني وتعميمها على الجهات ذات العلاقة ومتابعة الالتزام بها وتحديثها.

٢. تطوير مؤشرات الأداء الخاصة بالأمن السيبراني وإعداد التقارير الدورية حول الأمن السيبراني في المملكة على المستويين الوطني والقطاعي.

٣. إعداد الإستراتيجية الوطنية للأمن السيبراني والإشراف على تنفيذها واقتراح تحديثها.

٤. إشعار الجهات المعنية بالمخاطر والتهديدات ذات العلاقة بالأمن السيبراني.

٥. بناء القدرات الوطنية المتخصصة في مجال الأمن السيبراني والمشاركة في إعداد البرامج التعليمية والتدريبية الخاصة بها وإعداد المعايير المهنية والأطر وبناء وتنفيذ المقاييس والاختبارات القياسية والمهنية ذات العلاقة.

٦. وضع أطر الاستجابة للحوادث المتعلقة بالأمن السيبراني ومتابعة الالتزام بها وتحديثها.

٧. تنظيم آلية مشاركة المعلومات والبيانات المرتبطة بالأمن السيبراني بين الجهات والقطاعات المختلفة في المملكة والإشراف على ذلك.

٨. رفع مستوى الوعي بالأمن السيبراني.

٩. تمثيل المملكة في المنظمات والهيئات واللجان والمجموعات الثنائية والإقليمية والدولية ذات الصلة ومتابعة تنفيذ التزامات المملكة الدولية الخاصة بالأمن السيبراني.

قد أصدرت الهيئة الوطنية للأمن السيبراني وثيقة الضوابط الأساسية للأمن السيبراني التي تم إعدادها بهدف وضع حد أدنى من المعايير الواجب الالتزام بتطبيقها في مختلف الجهات الوطنية وذلك لتقليل مخاطر التهديدات السيبرانية على بنيتها التحتية وشبكاتها وأنظمتها مما يسهم في تعزيز أمن المملكة السيبراني وأمن مصالحها الحيوية والاقتصادية ومقدراتها الوطنية.

- **أخر أعمال الهيئة الوطنية للأمن السيبراني**

إطلاق معسكرات الأمن السيبراني ٢٩ ذو القعدة ١٤٤٥ هـ

بالشراكة مع وزارة الداخلية تقيم " المعرض التوعوي بالأمن السيبراني" لموسم حج ١٤٤٥ هـ

بالشراكة مع وزارة الحج والعمرة «تُصدر دليل التوعية السيبرانية» لضيوف الرحمن

إطلاق «البرنامج الوطني للبحث والتطوير والابتكار في الأمن السيبراني»

مشاركة المملكة ممثلة بالهيئة الوطنية للأمن السيبراني في الاجتماع الدولي رفيع المستوى في الأمم المتحدة حول «بناء القدرات في مجال امن تكنولوجيا المعلومات والاتصالات»

اختيار قادة الدول العربية الرياض مقراً لمجلس وزراء الأمن السيبراني العرب ٢٠٢٤ م

استفادة أكثر من ٩٠٠ جهة وطنية من «الحقيبة التوعوية للجهات الوطنية» منذ إطلاقها بداية العام الماضي ٢٠٢٣ م

❖ المعوقات التي تواجه أمن الفضاء الإلكتروني

- **المعوقات على المستوى الوطني**

١. عدم كفاية القوانين الحالية

هذا التلاحق في مجال تقنية المعلومات والاتصالات يقابله استغلال الجناة لهذه التقنية المتطورة بابتكار أساليب جديدة لارتكاب الجرائم الإلكترونية ولذلك يتطلب الأمر مواكبة القوانين لهذه التطورات واستيعابها.

٢. إحجام الكثير من الجهات عن التبليغ عن تلك الجرائم

يهدف هذا الإحجام من قبل هذه الجهات إلى عدم الإساءة لطبيعة عمل المنشأة وعدم بيان عجزها عن تحقيق الأمان الكافي للمعلومات وبالتالي لأصول الأموال التي تتعامل معها وقد يكون لذلك مردود سيء لدى العملاء الذين قد يلجون لسحب أموالهم أو إيقاف تعاملاتهم مع هذه المنشأة.

٣. سهولة إخفاء معالم الجريمة

يتمثل ذلك في عدم معرفة مصدر مرتكب الفعل بحيث إذا تم ارتكاب الفعل وظهرت نتيجته بعد فترة زمنية مثل نشر فيروس ثم اكتشاف آثاره التدميرية.

٤. عدم وجود دليل مادي واضح

الدليل المادي الذي يتوافر قد يكون في الغالب أوراق متحصلة من طابعة من خلال الجهاز والدليل هنا يكون الأوراق المتحصلة وليس ما يحويه الجهاز في حد ذاته.

٥. صعوبة الوصول إلى الدليل في بعض الأحيان

الدليل في الجريمة الإلكترونية عبارة عن معلومات قد تحاط بوسائل فنية لحمايتها وتلك الوسائل قد تكون عائقاً أمام عملية البحث والتحري والاطلاع.

٦. وجود كم كبير من المعلومات يتعين فحصها

يتطلب البحث عن معلومات تفيد في كشف أدلة جريمة معينة البحث في كم كبير من الملفات والبرامج المخزنة والتي قد يكون لها ارتباط بمعلومات خاصة بارتكاب الجريمة.

- **المعوقات على المستوى الدولي**

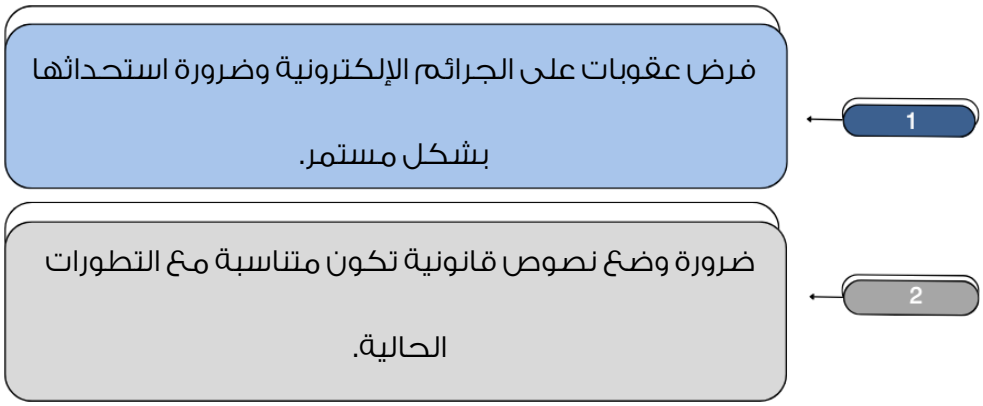
١. اختلاف مفاهيم الجريمة لاختلاف التقاليد القانونية وفلسفة النظم القانونية.

٢. عدم التناسق في القوانين الإجرائية فيما يتعلق بالتحري والتحقيق في الجرائم الإلكترونية.

٣. عدم وجود الخبرة الكافية لدي الأجهزة الأمنية والعدلية لفحص عناصر الجريمة.

٤. عدم كفاية الاتفاقات الدولية والثنائية في مجال تسليم المجرمين.

- الحلول



- الحلول التشريعية

١. إصدار السلطة المختصة ببعض المراسيم التنظيمية.

٢. إصدار مراسيم من أجل تنظيم تكوين محققين ورجال شرطة وقضاة على التقنية المعلوماتية وعلى معرفة كافية بجرائم الإنترنت.

٣. التوعية القانونية والتعريف بمدى خطورة الجرائم الإلكترونية.

٤. وضع برامج للحماية من الفيروسات هذا كله بمراسيم تنظيمية ويمكن للدولة أن تُنظم هذه العملية بتخفيض أسعار هذه البرامج.

٥. وضع البرامج اللازمة لمنع الدخول إلى المواقع المخلة بالحياء والمواقع الإرهابية ومواقع العنف.

❖ رؤية استراتيجية لمواجهة مخاطر الفضاء السيبراني وحروبه

الفضاء السيبراني بيئة مليئة بالمخاطر والتهديدات حيث شكلت تهديداً خطيراً للأمن القومي للدول حيث تغيرت مفاهيم القوة والصراع والحرب، وارتبطت طبيعتها بالفضاء السيبراني، ومع بروز الأمن السيبراني كركيزة أساسية في بناء الأمن القومي، سارعت الدول، لتشكيل الهيئات والمؤسسات المدنية والعسكرية، وسن التشريعات القانونية ووضع استراتيجية خاصة لمواجهة التهديدات السيبرانية الحالية والمستقبلية والدفاع عن أمنها، إضافة إلى العمل على المستويين الإقليمي والدولي من أجل إعداد رؤية عالمية لفضاء سيبرأني آمن وسلمي وتشتمل على إدارة للمخاطر السيبرانية وفهم الترابط بين الأنظمة الرقمية والتشغيلية والخدمات، ودراسة اعتمادها على أصول أخرى، والتعامل الأمثل معها .

- الحرب الإلكترونية

الفضاء أصبح محط الأنظار للدول في الحرب الإلكترونية والتي من خلالها تقوم الدول بالحروب المنطقية دون أسلحة وهذا يجعل الدول الصغيرة في بعض الأحيان في نفس قوة الدول العظمى ذات العتاد الحربي القوي.

الحرب الإلكترونية تعني محاولة الوصول إلى شبكات دولة أخرى بالوصول غير المصرح به واختراق الحواجز الأمنية الخاصة بالنظام الأمني للدولة الضحية، تسخر الدول مجموعة من: المخترقون الدوليون على قدر عالي من التدريب والتعقيد للوصول لموارد الدول الأخرى عن طريق الهجمات المعقدة والمكثفة والتي من شأنها التخريب أو قطع الخدمة أو حتى تعطيل شبكة الكهرباء للدولة الضحية.

الهدف من الحرب الإلكترونية هو كسب موقف أقوى مقارنة بالدول الضحية فالدولة المحاربة تحاول الوصول إلى البنية التحتية للدولة الضحية أو سرقة أسرار الدفاع بالإضافة إلى التجسس على الصناعات والعتاد الحربي، تقوم الدول المحاربة بالتخريب والتلاعب بالبيئة التحتية وتحقيق الخسائر في الموارد والأرواح.

- **الاستراتيجية الوطنية للأمن السيبراني ورؤيتها في المملكة العربية السعودية**

https://nca.gov.sa/strategic

هي وجود بنية فضاء سيبراني وطنية متكاملة وآمنة لأنها أحد أهم العوامل الممكنة للنمو والازدهار؛ لأن التوسع في استخدام التقنية يفتح آفاقاً جديدة للمخاطر والتهديدات السيبرانية؛ مما يستوجب تعزيز الأمن السيبراني لحماية الشبكات، وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات وحماية ما تقدمه من خدمات وما تحويه من بيانات من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال وكذلك لتعزيز الربط التقني الآمن بين الخدمات الحكومية ودعم الاقتصاد الرقمي، وتسعى الهيئة الوطنية للأمن السيبراني إلى قيادة وتنسيق الجهود الوطنية كجهة تشريعية من خلال تفاعل ومشاركة الجهات الوطنية وتكاملها لتحقيق طموحها ومستهدفاتها.

- رؤية الاستراتيجية الوطنية للأمن السيبراني

تم وضع رؤية للاستراتيجية الوطنية للأمن السيبراني تعكس الطموح الاستراتيجي للمملكة وبأسلوب متوازن بين الأمان والثقة والنمو، **وتتضمن الرؤية التي تسعى الهيئة إلى الوصول لها:**

فضاء سيبرأني سعودي آمن وموثوق يمكّن النمو

بحيث تكون هذه الرؤية شاملة للفضاء السيبراني بأكمله؛ تلبي أولويات المملكة وتطلعاتها، وتؤكد على تعزيز حماية الأنظمة التقنية والتشغيلية والبنى التحتية الحساسة والقدرة على الصمود والتصدي للحوادث السيبرانية وامتصاص الأضرار والتعافي منها في الوقت المناسب، بالإضافة إلى تعزيز ثقة الجهات الوطنية والمستثمرين والأفراد في الفضاء السيبراني السعودي، وكذلك المساهمة في النمو الاقتصادي والاجتماعي للمملكة.

- الرؤية تتضمن مصطلحات تم دراستها بعناية

فضاء سيبراني

يشمل الفضاء السيبراني السعودي بأكمله.

سعودي

لتلبية أولويات المملكة وتطلعاتها.

امن

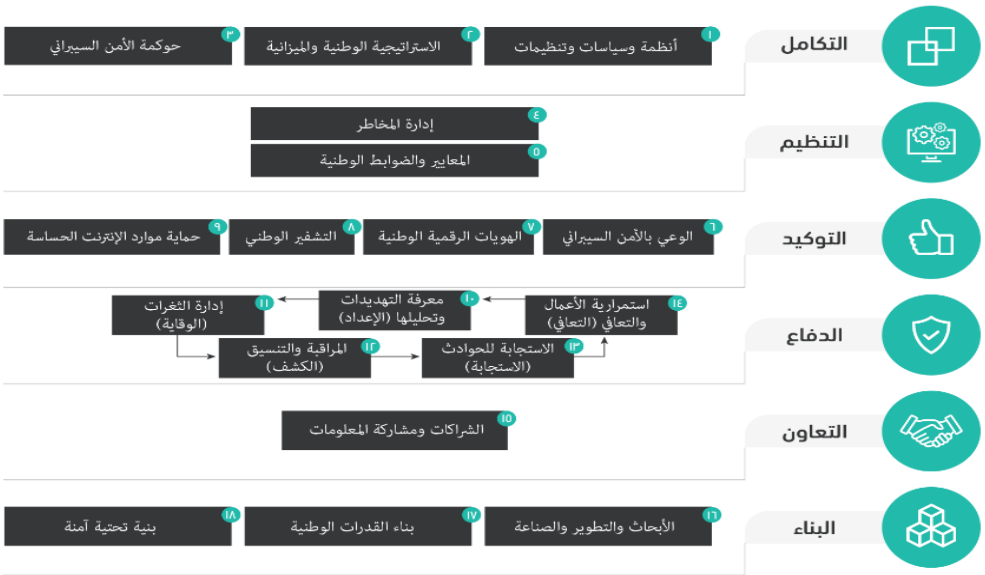
التأكيد على حماية وصمود الأنظمة التقنية والتشغيلية والبنى التحتية الحساسة.

موثوق

يعزز ثقة الجهات الوطنية والمستثمرين والأفراد في الفضاء السيبراني السعودي.

يمكّن النمو والازدهار

إسهام حماية الفضاء السيبراني في النمو الاقتصادي والاجتماعي للمملكة من أجل وضع مرجع عملي للجوانب المختلفة في الأمن السيبراني على المستوى الوطني، حرصت الهيئة على تصميم إطار مرجعي للأمن السيبراني خاص بالمملكة مبني على أفضل الممارسات المحلية والعالمية وأهم المستجدات والتحديات التي تواجه الأمن السيبراني،بحيث يعد نموذجاً متقدماً يشمل الجوانب المختلفة للأمن السيبراني على مستوى الدول , ويحتوي هذا الإطار على ستة محاور تتضمن ثمانية عشر عنصراً رئيسياً من عناصر الأمن السيبراني، ويساعد هذا الإطار على تعميق الفهم لفضاء المملكة السيبراني، وتم استخدام هذا الإطار لتصميم الاستراتيجية على المستوى الوطني , **ويوضح الشكل أدناه الإطار المرجعي:**



- **للوصول إلى فضاء سيبرأني سعودي آمن وموثوق يمكّن النمو والازدهار، سوف تحقق الاستراتيجية الوطنية للأمن السيبراني ستة أهداف رئيسية كما يلي:**

١. حوكمة متكاملة للأمن السيبراني على المستوى الوطني

من أجل ضمان تحقيق درجات عالية من التنسيق والمواءمة، من المهم تبني توجه وطني شامل للأمن السيبراني، وذلك من خلال تكامل وتحديد أدوار ومسؤوليات الجهات ذات العلاقة بالأمن السيبراني على المستوى الوطني لأجل تطوير التنظيمات والسياسات وتنفيذها، ومتابعة الالتزام بالمعايير الوطنية في جميع جوانب الأمن السيبراني، بالإضافة إلى وجود آليات موحدة للتخطيط والميزانية، وترتيب الأولويات في مجال الأمن السيبراني بفعالية مما يعزز رفع كفاءة الأنفاق.

٢. إدارة فعّالة للمخاطر السيبرانية على المستوى الوطني

إدارة المخاطر السيبرانية على مستوى الجهات والقطاعات وعلى المستوى الوطني، وتحديد العناصر المتضررة في الفضاء السيبراني ومدى حدّة الضرر، واختيار أفضل الطرق لمعالجتها أو الحد من آثارها، بالإضافة إلى تحديد إجراءات الحماية والدفاع حسب درجة المخاطر.

٣. حماية الفضاء السيبراني

أن وجود ضوابط شاملة ومعايير وطنية ونظام لمتابعة الالتزام يحقق حماية منظومة الأمن السيبراني، بالإضافة إلى رفع مستوى وعي المجتمع بالأمن السيبراني واستمرار وتعزيز التواصل معه من خلال حملات توعوية إعلامية عامة للأفراد والجهات، مما يحقق النضج والتطبيق لضوابط الأمن السيبراني على مستوى الأفراد والقطاعات والجهات الوطنية.

٤. تعزيز القدرات الفنية الوطنية في الدفاع ضد التهديدات السيبرانية

التعزيز والتطوير المستمر للقدرات الوطنية في الدفاع ضد التهديدات السيبرانية، وذلك لكشف الهجمات والتهديدات السيبرانية، والتعامل معها، والاستجابة والتعافي منها في حال الإصابة بها – لا قدر الله–.

٥. تعزيز الشراكات والتعاون في الأمن السيبراني

يتطلب الأمن السيبراني وجود شراكات محلية ودولية فعالة، ومعززة بآليات متطورة لمشاركة المعلومات؛ إذ تمكّن من التطوير والتحسين المستمر ومشاركة أفضل الممارسات والمعلومات الاستقصائية والتدابير اللازمة، بالإضافة إلى أهميتها العالية لمواكبة التهديدات، والحد من المخاطر، وللوصول للدرجة المرجوة من التعاون، ويساهم تعزيز الشراكات وبناء قنوات لمشاركة المعلومات داخل المملكة وخارجها، في مشاركة المعلومات المتعلقة بالأمن السيبراني.

٦. بناء القدرات البشرية الوطنية وتطوير صناعة الأمن السيبراني في المملكة

حماية الفضاء السيبراني للمملكة تتطلب وجود قاعدة قوية من الكوادر الوطنية المؤهلة في هذا المجال بالإضافة لصناعة أمن سيبرأني وطنية مزدهرة، ومن التوجهات الرئيسية بناء القدرات الوطنية في الأمن السيبراني من خلال برامج تعليم وتدريب عالية الجودة، بالإضافة لبرامج تحفز وتدعم الصناعة والبحث والتطوير والابتكار والاستثمار في الأمن السيبراني لتمكين النمو والازدهار.

- الخطة التنفيذية

تهدف إلى تحقيق أثر وطني ملموس على المدى البعيد ومكاسب سريعة على المدى القصير من خلال العمل على ثلاث مسارات متوازية، وقد تم تحديد ثلاث مسارات رئيسية، تشمل عدداً من المبادرات والمشاريع الوطنية.

مسارات تنفيذ الاستراتيجية

المسار الأول	المسار الثاني	المسار الثالث
مشاريع العائدات المرتفعة	برنامج دعم الجهات الوطنية	المـبادرات الوطنـية

❖ قوانين دولية للأمن السيبراني

تسهم الجهود الدولية والإقليمية في مكافحة الجريمة الإلكترونية بالوسائل المختلفة:

- أولا

قدمت روسيا مشروع قرار للنظر فيه خلال الدورة الـ ٧٣ للجمعية العامة للأمم المتحدة بشأن أمن المعلومات، ينص على أنشاء مجموعة عمل مناسبة وكذلك معايير لسلوك الدول في مجال أمن المعلومات.

قال الممثل الخاص للرئيس الروسي للتعاون في مجال أمن المعلومات أندريه كروتسكي متحدثاً في جلسة اللجنة الأولى للأمم المتحدة ً نقدم مشروع قرار إلى الدورة الثالثة والسبعين للجمعية العامة للأمم المتحدة والتي تتضمن قيمة مضافة حقيقية تتعلق بأنشاء مجموعة عمل متخصصة مفتوحة العضوية تابعة للأمم المتحدة، **وكأولوية تشمل ولايتها النظر في ثلاث مواضيع رئيسية:**

- معايير السلوك المسؤول للدول.
- تطبيق القانون الدولي على مجال المعلومات.
- المساعدة في بناء قدرات البلدان النامية لضمان الأمن السيبراني.

وأوضح أن ذلك يعتبر نوعاً من Traffic rules (قواعد السير) مؤكداً أنه من دون ذلك فسيكون من المستحيل ضمان النظام في بيئة رقمية.

وثيقة مسربة تكشف خطة جوجل السرية للرقابة على الإنترنت وقد قدمت روسيا منتصف شهر أكتوبر مشروع قرار إلى الجمعية العامة للأمم المتحدة بشأن المعلومات يهدف إلى اعتماد المجتمع الدولي قواعد السلوك المسؤول للدول في مجال المعلومات ويركز على الاستخدام السلعي الحصري لتكنولوجيا المعلومات والاتصالات وعدم استخدامها كقوة أو للتدخل في الشؤون الداخلية للدول الأخرى واحترام سيادة الدول ومنع النزاعات في هذا المجال , وتشير وزارة الخارجية الروسية إلى أن القرار أعد لحماية البيئة الرقمية من أفعال الأفراد والدول في إملاء إرادة الأفراد والدول الأخرى , إلا أن هذه المبادرة تم رفضها من قبل الولايات المتحدة وحلفائها.

- **ثانيا: قانون مشاركة وحماية المعلومات الرقمية في الولايات المتحدة الأمريكية**

سيسبا هو قانون اقترح في الولايات المتحدة يسمح بمشاركة معلومات حركة الإنترنت بين الحكومة الأمريكية وشركات التقنية والتصنيع وهدف المعلن من هذه الوثيقة أن يساعد الحكومة الأمريكية على تحري تهديدات الإنترنت وضمان أمن الشبكات ضد الهجمات على الإنترنت، قدم التشريع في ٣٠ نوفمبر ٢٠١١ من قبل النائب الأمريكي مايكل روجرز الجمهوري عن ولاية ميتشغأن و١٢٣ مشارك في الدعم.

تم تمرير الوثيقة في مجلس النواب في ٢٦ إبريل ٢٠١٢ لكن لم يصادق عليها مجلس الشيوخ الأمريكي، جادل مستشارو الرئيس أوباما بأن الوثيقة تفتقر إلى السرية وحماية الحريات المدنية ونصحوه بنقضها، في فبراير ٢٠١٣ أعاد البيت الأبيض تقديم الوثيقة ومررها في ١٨ إبريل ٢٠١٣م.

أنتقدت سيسبا من قبل دعاة خصوصية الإنترنت والحريات المدنية مثل مؤسسة الجبهة الإلكترونية ، اتحاد المدافعين عن الحريات المدنية الأمريكي ، الكفاح من أجل المستقبل وأفاز دوت أورغ بالإضافة إلى مختلف المجموعات المحافظة والتحررية منها ، معهد المشروع التنافسي ، تيك فريدوم ، فريدوم وركس ، أمريكيون من أجل الحكومة المحدودة ، تحالف حرية ، والاتحاد المحافظ الأمريكي ، تجادل تلك المجموعات أن سيسبا تحتوي قيوداً قليلة حول كيفية وفترة مراقبة الحكومة لتصفح أي فرد للمعلومات على الإنترنت ، إضافة إلى ذلك يخشون بأن مثل هذه السلطات الجديدة يمكن أن تستعمل للتجسس على الناس بدلاً من متابعة المخترقين الأشرار.

لقيت سيسبا الاستحسأن من الشركات مثل مايكروسوفت وفيسبوك وغرفة التجارة الأمريكية التي تنظر إليها كوسيلة بسيطة وفعالة لمشاركة المعلومات المهمة حول تهديد الإنترنت مع الحكومة.

رأى بعض النقاد سيسبأ كمحاولة لتقوية قوانين القرصنة الرقمية بعد أن قابل قانون سوياً معارضة هائلة، أدرجت سرقة الملكية الفكرية أولها في الوثيقة كسبب محتمل لمشاركة معلومات حركة الإنترنت مع الحكومة مع أنها أزيلت في المسودات اللاحقة.

يوجد بعض القوانين و اللوائح المعمول بها على نطاق واسع حيث سنت الولايات المتحدة الأمريكية في عام ٢٠٠١ م قانون ساربينز – أوكسلي SOX Sarbanes- Oxley وهو إلزامي ويجب على الشركات الأمريكية المتداولة علناً أن تمتثل لهذا القانون ، وقد أدخل على القانون تغيرات كثيرة على تنظيم الممارسات المالية وحوكمة الشركات وقد سُميت على اسم السناتور بول ساربينز والنائب مايكل أوكسلي اللذين كأنا مهندسيها الرئيسيين وقد تم ترتيب هذا القانون فيما يتعلق بالامتثال وغالباً ما تعتبر اللوائح الأكثر أهمية ضمن هذه البنود هي التي تخص السيبرانية ، وهو مصمم لحماية المستثمرين والجمهور من خلال زيادة دقة وموثوقية الإفصاحات عن الشركات لاسيما المالية منها وهذا يعني أن برامج أمن المعلومات تحتاج إلى التأكد من أن البيانات المالية لمؤسستهم يتم الحفاظ عليها سواء تم تداولها بشكل عام أم لا، معيار أمأن بيانات صناعة بطاقات الدفع عبارة عن مجموعة من متطلبات تأمين بيانات عملاء بطاقة الدفع ، تم تطويره من قبل مؤسسي مجلس معايير الأمن PCI ، **والذي يتضمن:**

- American Expess
- Mastercard
- Visa

يتحقق نظام PCI DSS على أي شخص يتعامل مع بيانات بطاقة الائتمان بما في ذلك تجار التجزئة والبنوك وشركات بطاقات الائتمان، تم سن قوانين إشعار خرق البيانات في معظم الولايات الأمريكية منذ عام ٢٠٠١ كأنت كاليفورنيا واحدة من أولى القوانين في الولايات المتحدة وسن الإتحاد الأوربي قانوناً من هذا القبيل في عام ٢٠٠٩ وتطلب جميعها من المؤسسات إخطار عملائها المتأثرين بخرق البيانات، تتطلب هذه القوانين أيضا من المنظمات اتخاذ خطوات أخرى لحماية المستهلكين المشاركين في الإخلال.

يوجد أيضا بعض اللوائح والمبادئ التوجيهية الخاصة بهذه الصناعة صدر في عام ٢٠٠٢م قانون إدارة أمن المعلومات الفيدرالي الذي يطلب من الوكالات الفيدرالية الأمريكية تنفيذ برنامج لتوفير الأمان لأنظمة المعلومات والمعلومات الخاصة بها، أصدرت مؤسسة الموثوقية الكهربائية لأمريكا الشمالية معايير لنظام الطاقة السائبة في أمريكا الشمالية.

فهو يحمي البنية التحتية الحيوية للصناعة من التهديدات المادية والسيبرانية يتطلب قانون قابلية نقل التأمين الصحي والمساءلة اعتماد معايير وطنية لحماية معاملات الرعاية الصحية الإلكترونية، كما يتطلب القانون حماية أمن وخصوصية المعلومات الصحية الشخصية وهو ينطبق على مقدمي الرعاية الصحية والخطط الصحية وبيوت المقاصة الصحية المعروفة أيضا باسم الكيانات المشمولة، ينطبق HIPPA أيضا على شركاء الأعمال وهم شركات الرعاية غير التابعة للخدمات التي تخدم الكيانات المتحولة.

تعد الشركة الخارجية التي تقوم بطباعة وإرسال رسائل تفصح عن بيانات الفوائد مثالا على شريك تجاري.

قام قانون تكنولوجيا المعلومات الصحية والقانون الصحي الأمريكي بتعديل HIPPA بشكل كبير في عام ٢٠٠٩ م وأضاف متطلبات جديدة تتعلق بالخصوصية والأمان لمعلومات صحة المريض وينطبق على كل من الكيانات المشمولة وشركائها التجاريين على الصعيد الدولي أحد أهم القوانين هو توجيه الإتحاد الأوربي لحماية البيانات.

اعتمد في عام ١٩٩٥م وينظم معالجة البيانات الشخصية داخل الإتحاد الأوربي، الأفراد في الإتحاد الأوربي لديهم توقعات أعلى عندما يتعلق الأمر بالخصوصية الشخصية مقارنة بالولايات المتحدة، وبالتالي فأن التوجيه يحظر على الشركات الأوربية نقل البيانات الشخصية إلى الولايات القضائية الخارجية مع قوانين الخصوصية الضعيفة مالم يكن هناك اتفاق منفصل لحماية البيانات، وحل التنظيم العام لحماية البيانات محل توجيه حماية البيانات في ٢٥مايو ٢٠١٨م.

على المستوى النقدي بالنسبة للتجارة الدولية، اتفقت المفوضية الأوربية والولايات المتحدة على وضع إطار عمل جديد للوفاء بمتطلبات تدفقات البيانات عبر الأطلسي في فبراير ٢٠١٦م، ويسمى درع الخصوصية بين الإتحاد الأوربي والولايات المتحدة معرفة القوانين واللوائح التي يجب تطبيقها على مؤسسة ما تستغرق وقتاً طويلا وتتطلب الاستعانة بمستشار قانوني لتوفير الوقت والمال.

يوجد العديد من القوانين واللوائح التي قننت بشكل صارم وتُطبق في أنحاء العالم ومن المتوقع المزيد من ظهور القوانين في السنوات القادمة، كلما ازداد هذا العلم من تقدم وازدهار وستكون القوانين واللوائح المعمول بها على العديد من مستويات التطبيق في كل شيء وفي كل المجالات بدءا من المنظمات التعليمية أو الطبية ووصولا إلى المستويات الإدارية التي تقرب من صنع القرار.

- **القضايا القانونية والأخلاقية في الأمن السيبراني**

منذ أواخر الثمانينات تطورت الهجمات الإلكترونية عدة مرات بسبب استخدام الابتكارات في تكنولوجيا المعلومات وظهور جرائم الإنترنت في السنوات الأخيرة، ازداد حجم وخطورة الهجمات الإلكترونية بسرعة وتقرير المنتدى الاقتصادي العالمي لعام ٢٠١٨م تتطور قدرات الإنترنت السيئة بسرعة أكبر من القدرة على التعامل مع الحوادث العدائية.

في مايو ٢٠٠٠ حددت فرقة عمل هندسة الإنترنت الهجوم في rfc2828 هجوم على أمن النظام مستمد من تهديد ذكي، فعل ذكي هو محاولة متعمدة للتهرب من الخدمات الأمنية وكسر السياسة الأمنية للنظام.

- القضايا القانونية

يجب أن يكون مهنيو الأمن السيبراني على درجة التدريب والذكاء التي يكون عليها مخترقين القبعة السوداء، الفرق الوحيد بين المهنيون والمخترقون أن المهنيون يعملون بإطار قانوني.

- القضايا الأخلاقية

بالإضافة إلى إتباع القانون يجب أن يُظهر مهنيو الأمن السيبراني بعض الأخلاقيات:

١. على المستوى الشخصي

من الممكن أن يتصرف الشخص بشكل غير أخلاقي وليس غير قانوني مثل الاحتفاظ بنسخة من بيانات الشركة في منزله، أو تتبع شخص لمعرفة إذا كأن قد حصل على نسخة من معلوماته الشخصية أثناء صيانته لجهازه، فالتصرف غير الأخلاقي لا يوجد رادع حقيقي له حيث لا يمكن حصر كل التصرفات غير الأخلاقية ووضعها في صورة قوانين أو حتى إرشادات.

٢. على المستوى المؤسسي

قواعد السلوك الوظيفي في بعض الأحيان يمكن تغطيتها بالقانون، حيث يوجد كثير من النقاط في الأمن السيبراني لم يتم تغطيتها بشكل قانوني، فليس معنى أن التصرف لم يغطيه القانون أن يكون أخلاقياً.

تمارين الفصل الرابع

١. **اختار الإجابة الصحيحة فيما يلي:**

١- **من جهود المملكة في مجال الأمن السيبراني**

- التعامل مع الاختراقات
- جهود هيئة الاتصالات السعودية
- وضع الفدية على المجرمين
- رفع مستوى الوعي

٢- **حسب المادة الأولى مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها، وتشمل الحاسبات الآلية هو تعريف**

- الشخص
- النظام المعلوماتي
- برامج الحاسب الآلي
- الموقع الإلكتروني

٣- **من المعوقات التي تواجة امن الفضاء الالكتروني على المستوى الوطني**

- عدم كفاية القوانين الحالية
- عدم كفاية الاتفاقات الدولية
- عدم وجود الخبرة الكافية لدى الأجهزة الأمنية
- وجود دليل مادي واضح

٤- **من الأبعاد الاجتماعية للجريمة الإلكترونية**

- يخسر الاقتصاد العالمي ٠,٨%
- تعرض مستخدمو مواقع التواصل الاجتماعي للجرائم بشكل متزايد
- متوسط الأنفاق على الأمن السيبراني وهو حوالي ٨,٩ مليون دولار

٥- **ماهي عقوبة التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي – دون مسوغ نظامي صحيح – أو التقاطه أو اعتراضه.**

- سجن مدة لا تزيد عن ثلاث سنوات وغرامة لا تزيد عن مليوني ريال
- سجن مدة لا تزيد عن سنة وغرامة لا تزيد عن خمسمائة ألف ريال
- سجن مدة لا تزيد عن أربع سنوات وغرامة لا تزيد عن ثلاثة ملايين ريال
- سجن مدة لا تزيد عن خمس سنوات وغرامة لا تزيد عن ثلاثة ملايين ريال

٢. **ضع علامة (✓) أمام العبارات الصحيحة وعلامة (✗) أمام العبارات الخاطئة:**

١.	استخدام المصطلحات من متطلبات الأمن السيبراني	✗
٢.	من فصول اتفاقية بودابست الاتفاق على التعليم العام	✗
٣.	من الدوائر الرئيسية التي يربط بها امن العالم السيبراني دائرة الدولة	✓
٤.	حسب المادة الأولى تعريف الشبكة المعلوماتية هو أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام	✗
٥.	من اختصاصات ومهام الهيئة الوطنية للأمن السيبراني إعداد الاستراتيجية الوطنية للأمن السيبراني والأشراف عليها	✓
٦.	من أهداف الاستراتيجية الوطنية للأمن السيبراني تعزيز الشراكات والتعاون في الأمن السيبراني	✓
٧.	تكاليف الأمن من الخسائر المالية للجريمة الإلكترونية	✓

❖ المراجع

١.	د. عبير الرحبأني ،٢٠٢٠م ، الجرائم الإلكترونية و مخاطرها ، دار الثقافة.
٢.	د. عدنأن مصطفى البار، د. عيسى رفاعي السميري، ١٤٤٠هـ، أساسيات الأمن السيبراني، مكتبة الملك فهد الوطنية.
٣.	د. خالد بن سليمأن الغثبر، د. محمد القحطأني، ١٤٤٩ه، أمن المعلومات بلغة ميسرة، مكتبة الملك فهد الوطنية.
٤.	غأنم مرضي الشمري، ٢٠١٦، الجرائم المعلوماتية ماهيتها–خصائصها–كيفية التصدي لها، دار الثقافة.
٥.	مريم عطيف، م. أيمن القاسم ،٢٠١٩م ، كيف تحمي معلوماتك الأمن السيبراني، مكتبة الملك فهد الوطنية .
٦.	.Hack Attack Protecting Yourself in the Age of Cybercrime ،2024 ، Axel Frost
٧.	.Digital Forensics and Cyber Crime ،2011 ، Ibrahim Baggili
٨.	موقع الهيئة الوطنية للأمن السيبراني https://www.nca.gov.sa/news

أكاديمية التعلم
Academy Of Learning

تحت إشراف

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

9 2 0 0 0 3 1 3 7

a o l . e d u . s a

a o l k s a