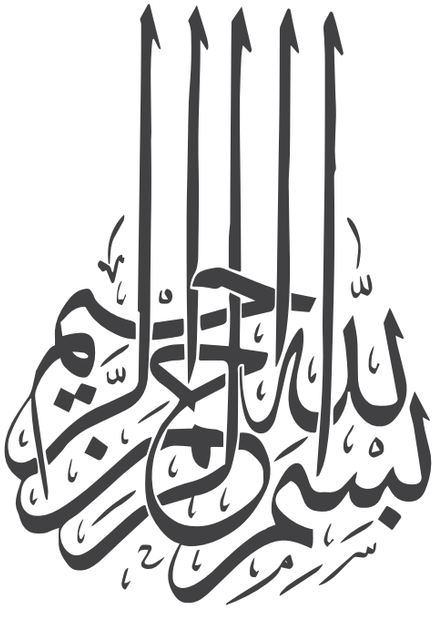
الأمـــن السيـــبراني والمواطَنة الرقمية

د. حليمة المنتشري

م. محمد المنتشري



الأمـــن السيبـــراني
والمواطَنة الرقميـــة

د . حليمة المنتشري م. محمد المنتشري

رقم الإيداع : ١٤٤٠/٢٩٠٦
ردمك : ٩٧٨-٦٠٣-٠٢-٨٤٩٧-٩

المقدمة

أحدثت التطورات التكنولوجية الحديثة في القرن العشرين، نقلة نوعية وثورة حقيقية في عالم الإتصال، حيث انتشرت شبكة الإنترنت في كافة أرجاء المعمورة، وربطت أجزاء هذا العالم المترامية بفضائها الواسع، ومهدت الطريق لكافة المجتمعات للتقارب والتعارف وتبادل الآراء والأفكار والمعلومات، واستفاد كل متصفح لهذه الشبكة من الوسائط المتعددة المتاحة فيها، وأصبحت أفضل وسيلة لتحقيق التواصل بين الأفراد والجماعات، وغيرت مضمون وشكل الإعلام الحديث، وعلى الرغم من أن هذا التقدم في تكنولوجيا المعلومات والاتصالات ساهم في تقديم العديد من المنافع والايجابيات للاقتصاد والمجتمع، إلا أنه طرح بعض الآثار السلبية من أبرزها ظهور الجرائم السيبرانية والتي تعد نوعاً من أخطر الحروب الخفية التي تهدد الأمن الشخصي والدولي بكافة أنواعه،مما يتطلب توعية شاملة لجميع الفئات وتزويدهم بوسائل الحماية اللازمة للتعامل مع الفضاء السيبراني بانفتاح واعي يساهم بحفظ الأمن

وتعزيزه مع إبراز الإجراءات والوسائل المتخذة لتضييق الجرائم والاعتداءات الإلكترونية، والأفعال غير الأخلاقية والتي تشكل أكبر تحدي في ظل تطور استخدامات تكنولوجيا الانترنت، وبما أن التربية في الفضاء السيبراني أصبحت أمراً معقداً في عصر العولمة والتي صارت البيئة فيها هي العالم كله بما فيه من اختلاف الثقافات والديانات يزداد حيناً ليكون تضاداً ويقل حيناً لتكون تنوعاً ،مما جعل المعلوماتية تدخل البيوت دون إذن أصحابها ولا رقابة لتؤثر في تكوين شخصيات أبنائنا والتأثير عليهم سلباً وإيجاباً، فكان لزاماً توعية الطلاب وتحذيرهم من الغزو الفضائي الضار الموجه المنظم الذي يستهدف العقيدة والوطن ووحدته والأخلاق والقيم فكان هذا الكتاب ليسلط الضوء على الفضاء السيبراني وما يتعلق به وآلية التعامل معه لتحقيق مواطنة رقمية آمنة سائلين المولى عز وجل التوفيق والسداد لما فيه خدمة ديننا ووطننا.

الفصل الأول

الأمن في الفضاء السيبراني

ما هو الأمن السيبراني؟

أهمية الامن السيبراني

الفرق بين الأمن السيبراني و أمن المعلومات

الأمن السيبراني من منظور إسلامي

التطور التاريخي للأمن السيبراني

تجارب دولية في الأمن السيبراني

الأمن في الفضاء السيبراني

"الفضاء السيبراني" بات تعبيراً مُتداولاً في العالم يُشير إلى بيئة إلكترونية متكاملة تحيط بنا وتتحكم في مناشط حياتنا السياسية والاقتصادية والاجتماعية والتعليمية وكل ما يتعلق بهذا الفضاء من الشبكات الحاسوبية والإنترنت والتطبيقات المعلوماتية والفاكس وجميع الاتصالات المعتمدة على الأقمار الصناعية . فالبيئة السيبرانية تتطلب حماية تامة من المخاطر المختلفة التي تواجهها، كالهجمات الإلكترونية (الفيروسات) التي تزداد شراسة وتعقيداً يوماً بعد يوم، والتي تعدُّ نوعاً من الحروب المفتوحة قد تقف خلفها منظمات أو دول لأهداف سياسية وعسكرية واقتصادية فالحرب السيبرانية (حرب الفضاء الإلكتروني) هي حروب ميدانها الفضاء الإلكتروني لا تنطبق عليها قوانين وأعراف الحروب التقليدية، ولا تقيدها الحدود السياسية للدول، فهي عابرة للقارات(الشراري ،٢٠١٧)مما قد يكلف الدول مبالغ باهظة وقد يعطل أجهزتها ويعرضها للاختراق وفي ذلك أورد (عشقي،٢٠١٦) أن اليوم نعيش حرباً سيبرانية تتمثل في اختراق أجهزة الحاسب الآلي أو تعطيله، ما يكلف الدول مبالغ باهظة فيتعرف المخترق على قدراتها ويكتشف أسرارها، وقد أصبحت الحرب السيبرانية لها القدرةعلى تدمير بعض الأسلحة وإسقاط بعض الطائرات وإحداث الشلل في الاتصالات فتحول المجتمعات إلى مجتمعات معلوماتية حدث بفضل اندماج التكنولوجيا الجديدة في كل مجال من مجالات النشاط وفي كل نوع من أنواع البنية

التحتية ليزيد اعتماد الأفراد والبلدان والمنظمات على نظم المعلومات والشبكات مما يشكل مصدراً رئيساً من مصادر الخطر يجب معاملته كخطر أمني.

السيبرانية مأخوذة من كلمة سيبر(Cyber) وهي وصف يتعلق بثقافة الحاسب وتكنولوجيا المعلومات والاتصالات والواقع الافتراضي. فالسيبرانية تعني القيادة والتحكم والسيطرة على سلوك الفرد مما يجعله مدمناً يتأثر بسلوكيات التقنية وتسيطر على تحركاته فتجعله يتصرف دون شعور ولا أدنى مسؤولية مما يجعله عرضةً للاستغلال من قبل مجرمي السيبرانية وهذا يؤيد ماذكره المحمادي (٢٠١٨) بأن البشر تتغير سلوكياتهم ومشاعرهم وقيمهم حين يكونون في الفضاء السيبراني ويستغل المجرمون تلك التغيرات لنفرض مثلاً في السناب يخبر الشخص الجميع سواءً معرفات حقيقية أو وهمية بأموره الحياتية ،ولكن هل سيخبر شخص مجهول بكل هذه الأمور لو كان بجانبه على مقعد الطائرة هنا يكون عدم الإحساس بالمؤثرات الخارجية ومن هذه الزاوية يتم الاستغلال فالفضاء السيبراني مجال عالمي يتضمن شبكات عالمية وخاصة وتمثل ميداناً خامساً للحرب والأمن هنا ليس لكسب المال ولكن لحماية المقدرات من هجمات العدو.

إن السيبرانية مجال عالمي يتضمن شبكات عالمية وخاصة وتمثل ميداناً خامساً للحرب والأمن هنا ليس لكسب المال ولكن لحماية المقدرات من هجمات العدو ، وقد أوضح الفضالة (٢٠١٧) أن المملكة العربية السعودية بلغت خسائرها الناجمة عن الهجمات السيبرانية على الأفراد السعوديين ٥٢٧مليون دولار في عام ٢٠١٣ وفي قراءة متعمقة للدراسة التي كشفت عنها شركة كاسبر سكاي لاب أن المملكة العربية السعودية تحتل المرتبة الأولى عربياً والمرتبة العشرين عالمياً من حيث التهديدات السيبرانية، وقد أشار المقصودي (٢٠١٧) أن الجرائم السيبرانية جرائم مبتكرة ومستحدثة وتمثل ضرباً من ضروب الذكاء الإجرامي استعصى إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية فإن متوسط تكلفة الاختراقات الإلكترونية حوالي ٤ملايين دولار وفي دراسة حديثة أجرتها ميكروسوفت لما يقرب من ١٠٠٠مؤسسة في دول الخليج العربي لا يزال أكثر من ٨٠٪ من الأفراد يستخدمون اسم المستخدم وكلمة المرور للدخول في شبكاتهم ويؤكد ذلك مايك جانكوفسكي أن أكثر من ٢٥٪ من الاختراقات سببها أخطاء في الاستخدام من قبل الأفراد وتحميلهم لبرمجيات مجهولة المصدر وأوصى بضرورة تمكين الأفراد من الابتكار من أجل تحقيق أفضل حماية ودفاع للبيئة التي يعيشونها وتبني تقنيات إدارة الهوية كالتعرف على الوجه و تحديد الهوية البيولوجية والمصادقة المتعددة.

ما هو الأمن السيبراني؟

يُعد مفهوم الأمن السيبراني أو أمن الفضاء الإلكتروني من المفاهيم الحديثة، والتي ظهرت في سياق ثورة تكنولوجيا المعلومات والإتصالات المعاصرة، وتشير كلمة الأمن في هذا المجال إلى إجراءات الحماية ضد التعرض للأعمال العدائية والاستخدام السيئ لتكنولوجيا الإتصال والمعلومات (عبد الصادق، ٢٠١٧).

وعرف الاتحاد الدولي للإتصالات في تقريره الصادر بعنوان حول "اتجاهات الإصلاح في الإتصالات للعام ٢٠١٠-٢٠١١" الأمن السيبراني باعتباره مجموع الأدوات والسياسات ومفاهيم الأمن وضوابط الأمن والمبادئ التوجيهية ونهج إدارة المخاطر، والإجراءات والتدريب وأفضل الممارسات، وآليات الضمان والتقنيات التي يُمكن استخدامها في حماية البيئة السيبرانية، وتشمل أصول المؤسسات ومستخدمي أجهزة الحوسبة الموصولة بشبكة الإنترنت، والبنية التحتية والتطبيقات والخدمات وأنظمة الإتصالات ومجموع المعلومات المنقولة أو المحفوظة في البيئة السيبرانية.

ويعرفه "فون سولمس" Von Solms، ٢٠١٥)) بأنه اتخاذ جميع التدابير اللازمة لحماية الأفراد من أخطار الفضاء الإلكتروني.

ويرى "كانونجيا وماندارينو" Canongia and Mandarino

(٢٠١٤) أن الأمن السيبراني هو "فن ضمان ووجود واستمرارية مجتمع المعلومات، وضمان وحماية الفضاء الإلكتروني، بما يشمل المعلومات والأصول والبنية التحتية الحيوية"

كما يُعرف الأمن السيبراني بأنه النشاط الذي يؤمن حماية الموارد البشرية، والمالية، المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن امكانات الحد من الخسائر والأضرار، التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه، بأسرع وقت ممكن، بحيث لا تتوقف عجلة الانتاج، وبحيث، لا تتحول الأضرار الى خسائر دائمة (جبور، ٢٠١٢).

ويشمل الأمن السيبراني الحد من مخاطر الهجمات والبرمجيات الخبيثة والفيروسات والتي تستهدف البرامج وأجهزة الحاسوب وشبكات المعلومات والإتصالات، واستخدام الأدوات الخاصة بالكشف عن عمليات اختراق الشبكات وإيقاف الفيروسات، وفرض نظم المصادقة وتمكين الاتصالات المشفرة، وعلى هذا يُعرف الأمن السيبراني بأنه "عملية تنظيم وتجميع الموارد والعمليات والهياكل التي تُمكن الفضاء السيبراني من إيقاف عمليات الاختراق بصورها المختلفة، والتي تتم بصورة غير صحيحة قانونية" (Craig، Daikun & Purse، ٢٠١٤)

كما ذكر(الربيعة،٢٠١٨) الأمن السيبراني بأنه أمن المعلومات على

أجهزة وشبكات الحاسب الآلي، والعمليات والآليات التي يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرح به أو تغيير أو اختلاف قد يحدث، حيث يتم استخدام مجموعة من الوسائل التقنية والتنظيمية والإدارية لمنع الاستخدام غير المصرح به، ومنع سوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها "

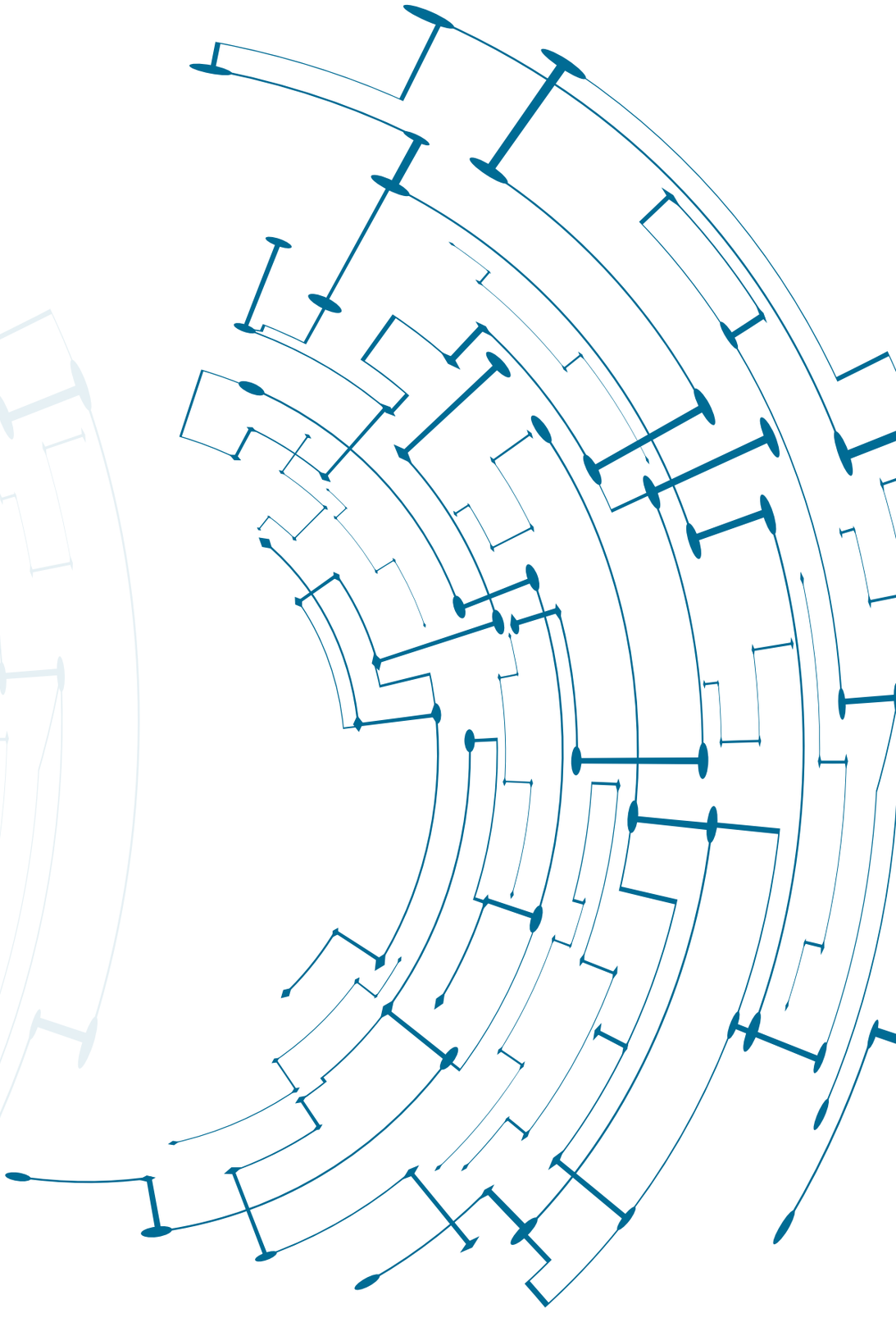
وأشار (عشقي ،٢٠١٦) بإبقاء معلوماتك تحت سيطرتك المباشرة بشكل كامل والحيلولة دون الوصول إليها من قبل الآخرين دون السماح من قبلك، مع علمك بمخاطر السماح للآخرين الذين سمحت لهم.

وعرفه Muller، L. P. (٢٠١٥). في التقرير الصادر من جمعية شؤون الدولة بالنرويج بأنه تمكين الأفراد والمجتمعات والحكومات من عدم الاستجابة للتهديدات التي يتعرض لها الفضاء السيبراني وذلك لتحقيق الأهداف الإنمائية للدولة، وتقليل مخاطر الأمن الرقمي الناجمة عن الوصول واستخدام الفضاء الإلكتروني لأهداف غير مشروعة. ويتضح من استعراض التعريفات السابقة أن الأمن السيبراني :يحتاج بناء قدرات أمنية عالية الجودة تستهدف البنى التحتية لأنظمة الاتصالات وتقنية المعلومات والتي تعد أساساً جزءاً هاماً من الفضاء السيبراني تدريب الأفراد والمنظمات لصد أي هجوم أو اعتداء يستهدف الفضاء السيبراني .

أهمية الامن السيبراني

تأتي أهمية الأمن السيبراني في عالم اليوم بصورة لا تقل عن أهمية الأمن القومي لأي دولة، حيث ظهرت الجرائم الإلكترونية، واستخدام الفضاء الإلكتروني في القيام بحروب غير تقليدية عبر هجمات الإرهاب الإلكتروني وإطلاق فيروسات الحاسب والتجسس الإلكتروني والاختراق المباشر لشبكات المعلومات، ولم تعد أشكال الخطر التي تهدد المحتوى المعلوماتي والمجتمعي المشترك مقصورة على الأشكال التقليدية، بل أصبح لها أوجه رقمية إلكترونية غير مسبوقة في شمولها وعمقها واتساع نطاق تغطيتها، وفداحة أضرارها وتعقد آلياتها وتواصل هجماتها وتتضمن إفساد وتعطيل إتاحة المعلومات مثل المعلومات العسكرية والأمنية والاقتصادية والمحتوى الفكري والسياسي والاجتماعي والعلمي (عبد الصادق، ٢٠١٧).

وللأمن السيبراني بعد اجتماعي كبير في عالم اليوم، الذي يشهد استخداماً متزايداً لمواقع التواصل الاجتماعي من قبل شرائح كبيرة من فئات عمرية مختلفة، حيث تُستخدم تلك المواقع للتعبير عن التطلعات والطموحات الشخصية لمستخدمتها، كما تتم مشاركة الأفكار والمعلومات بين ملايين المشتركين حول العالم، وعلى هذا تشير (جبور، ٢٠١٢) إلى أهمية



تحقيق الامن السيبراني وضمانه، ومكافحة المحتويات غير المشروعة وغير المرغوب لما لها من تأثير سلبي أكيد، على اخلاقيات المجتمع معين، وعلى ارتفاع نسبة الممارسات الجرمية، ومن الامثلة على ذلك: الاباحية، والترويج للإتجار بالممنوعات، والدعارة، والارهاب، والتجنيد لقضايا تمس الامن والسلام الدوليين. وعليه، لا بد من بناء مجتمع مسؤول، ومدرك لمخاطر الفضاء السيبيراني، قادر على التعامل بحد ادنى من قواعد السلامة، مع ادراك للعواقب القانونية، التي يمكن ان تترتب على التصرفات، والتي تعرض سلامة الغير، وسلامة رؤوس الاموال وحركتها، للخطر.

الفرق بين الأمن السيبراني و أمن المعلومات

لا شك أن تساؤلا مثل هذا قد جال في فكر القارئ و كما نعلم أن في الآونة الأخيرة وجدنا كثيرا من أهل الاختصاص يخوضون في هذا الفرق و الذي يعده البعض منهم تساؤلا مهما و جوهريا عند الحديث عن الأمن المعلوماتي أو الأمن السيبراني .

و من خلال تتبعنا لأبرز ما قيل في هذا الشأن و جدنا أن هناك آراء متباينة بعضها يصل لغاية القطع ان هناك فرق و عليه يضع قناعاته و تصوراته من هذا المنطلق ، و البعض يرى أن الأمر خلاف ذلك ..

وعليه سوف نستعرض معك أيها القارئ أبرز الآراء في الفرق بين أمن المعلومات و الأمن السيبراني :

فريق من المختصين ذكر أن أمن المعلومات هو أعم و أشمل و أنه هو المظلة التي ينضوي تحتها الأمن السيبراني و أنه يهتم بالمعلومات أي كان مصدرها سواء كانت في الحاسب أو الورق بينما يرى أن الأمن السيبراني يهتم بكل ما هو داخل الحاسب و أتصل به فقط .

و الفريق الثاني على النقيض من الفريق الأول حيث ذكر أن الأمن السيبراني هو أعم و أشمل لقناعته أن الأمن السيبراني يهتم بالفضاء التقني و بالتالي يرى أن أمن المعلومات هو من ذلك الفضاء.

و فريق ثالث يرى أن أمن المعلومات هو الأمن السيبراني و أنها كلمتين مترادفتين و لا يوجد في نظر هذا الفريق ما يستوجب التفريق بينهما بحكم أن كلاهما يهتم بأمن المعلومات أياً كان شكل المعلومة و مصدرها .

و خلاصة القول في هذا الشأن أن الأمر يبقى وجهات نظر و مدار عمل و بحث و أن قناعتك ليس بالضرورة أن تكون هي الحقيقة المحضة فكلا له ما يدعمه و يؤيده.

قال تعالى:

(لَوْ خَرَجُوا فِيكُم مَّا زَادُوكُمْ إِلَّا خَبَالًا وَلَأَوْضَعُوا خِلَالَكُمْ يَبْغُونَكُمُ الْفِتْنَةَ وَفِيكُمْ سَمَّاعُونَ لَهُمْ وَاللَّهُ عَلِيمٌ بِالظَّالِمِينَ)

(التوبة ٤٧)

الأمن السيبراني من منظور إسلامي

قبل الحديث عن الجرائم السيبرانية والهجمات الإلكترونية وموقف المنظمات العالمية منها فإن ديننا الإسلامي الحنيف له السبق في حماية جميع أنواع الأمن بتشريعات ربانية كفلت حقوق الأفراد والدول على حدٍ سواء ويمكن استعراض بعضاً منها كما وردت في القرآن الكريم والسنة المطهرة :

جريمة التشهير

قوله تعالى: (وَالَّذِينَ يُؤْذُونَ الْمُؤْمِنِينَ وَالْمُؤْمِنَاتِ بِغَيْرِ مَا اكْتَسَبُوا فَقَدِ احْتَمَلُوا بُهْتَانًا وَإِثْمًا مُبِينًا) (الأحزاب ٥٨)

قوله تعالى: (لَوْلَا إِذْ سَمِعْتُمُوهُ ظَنَّ الْمُؤْمِنُونَ وَالْمُؤْمِنَاتُ بِأَنفُسِهِمْ خَيْرًا وَقَالُوا هَذَا إِفْكٌ مُّبِينٌ) (سورة النور ١٢)

جريمة الإساءة الإلكترونية لولي الأمر ورموز الدولة

قوله تعالى: (يَا أَيُّهَا الَّذِينَ آمَنُوا أَطِيعُوا اللَّهَ وَأَطِيعُوا الرَّسُولَ وَأُولِي الْأَمْرِ مِنْكُمْ فَإِنْ تَنَازَعْتُمْ فِي شَيْءٍ فَرُدُّوهُ إِلَى اللَّهِ وَالرَّسُولِ إِنْ كُنْتُمْ تُؤْمِنُونَ بِاللَّهِ وَالْيَوْمِ الْآخِرِ ذَلِكَ خَيْرٌ وَأَحْسَنُ تَأْوِيلًا)

فهذه الآية نص في وجوب طاعة أولي الأمر، وهم: الأمراء والعلماء وقد جاءت السنة الصحيحة عن رسول الله صلى الله عليه وسلم تبين أن هذه الطاعة لازمة، وهي فريضة في المعروف وقوله صلى الله عليه وسلم «من خرج من الطاعة وفارق الجماعة فمات مات ميتة جاهلية».

جريمة التعرض للأديان والأعيان بالسب والشتم

قوله تعالى: (وَلَا تَسُبُّوا الَّذِينَ يَدْعُونَ مِن دُونِ اللَّهِ فَيَسُبُّوا اللَّهَ عَدْوًا بِغَيْرِ عِلْمٍ كَذَلِكَ زَيَّنَّا لِكُلِّ أُمَّةٍ عَمَلَهُمْ ثُمَّ إِلَى رَبِّهِم مَّرْجِعُهُمْ فَيُنَبِّئُهُم بِمَا كَانُوا يَعْمَلُونَ) (الأنعام١٠٨)

قوله تعالى: (لَّا يَنْهَاكُمُ اللَّهُ عَنِ الَّذِينَ لَمْ يُقَاتِلُوكُمْ فِي الدِّينِ وَلَمْ يُخْرِجُوكُم مِّن دِيَارِكُمْ أَن تَبَرُّوهُمْ وَتُقْسِطُوا إِلَيْهِمْ إِنَّ اللَّهَ يُحِبُّ الْمُقْسِطِينَ) (الممتحنة١٨)

قوله صلى الله عليه وسلم :

«المسلم من سلم المسلمون من لسانه ويده» (رواه البخاري ومسلم).

جريمة الإرجاف الإلكتروني

ويقصد به بث الأخبار المحبطة والسيئة ونشر الشائعات بغرض إحداث الخوف والاضطرابات وزعزعة الأمن والإيمان في نفوس الناس وقد حذر الله منه بقوله تعالى: (لَئِن لَّمْ يَنتَهِ الْمُنَافِقُونَ وَالَّذِينَ فِي قُلُوبِهِم مَّرَضٌ وَالْمُرْجِفُونَ فِي الْمَدِينَةِ لَنُغْرِيَنَّكَ بِهِمْ ثُمَّ لَا يُجَاوِرُونَكَ فِيهَا إِلَّا قَلِيلًا) (الأحزاب: ٦٠)

وحذر الله من الاستماع لهم فقال تعالى : (لَوْ خَرَجُوا فِيكُم مَّا زَادُوكُمْ إِلَّا خَبَالًا وَلَأَوْضَعُوا خِلَالَكُمْ يَبْغُونَكُمُ الْفِتْنَةَ وَفِيكُمْ سَمَّاعُونَ لَهُمْ وَاللَّهُ عَلِيمٌ بِالظَّالِمِينَ) (التوبة ٤٧)

جريمة الاحتيال الإلكتروني

قوله تعالى: (يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَأْكُلُوا أَمْوَالَكُمْ بَيْنَكُمْ بِالْبَاطِلِ إِلَّا أَنْ تَكُونَ تِجَارَةً عَنْ تَرَاضٍ مِنْكُمْ وَلَا تَقْتُلُوا أَنْفُسَكُمْ إِنَّ اللَّهَ كَانَ بِكُمْ رَحِيمًا)(وَمَنْ يَفْعَلْ ذَلِكَ عُدْوَانًا وَظُلْمًا فَسَوْفَ نُصْلِيهِ نَارًا وَكَانَ ذَلِكَ عَلَى اللَّهِ يَسِيرًا) (سورة النساء: ٢٩-٣٠)

قوله صلى الله عليه وسلم: «من غشنا فليس مني » رواه مسلم.

وقوله صلى الله عليه وسلم: « أتدرون من المفلس؟ قالوا : المفلس فينا من لا درهم له ولا متاع، قال: إن المفلس من أمتي من يأتي يوم القيامة بصلاة وصيام وزكاة، ويأتي وقد شتم هذا، وضرب هذا، وأكل مال هذا، وسفك دم هذا، فيأخذ هذا من حسناته، وهذا من حسناته فإن فنيت حسناته قبل أن يوفى الذي عليه، أخذ من سيئات صاحبه ثم طرحت عليه، ثم طرح في النار» (رواه مسلم).

وفي صحيح البخاري عن أبي هريرة رضي الله عنه قال: قال رسول الله صلى الله عليه وسلم: «من أخذ أموال الناس يريد أداءها أدى الله عنه، ومن أخذ أموال الناس يريد إتلافها أتلفه الله »

نهى رسول الله صلى الله عليه وسلم عن بيع المضطر ، وعن بيع الغرر ، وبيع الثمر قبل أن يطعم . (سنن أبي داوود)

جريمة التجسس

قوله تعالى: (يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ وَلَا تَجَسَّسُوا وَلَا يَغْتَبْ بَعْضُكُمْ بَعْضًا أَيُحِبُّ أَحَدُكُمْ أَنْ يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ وَاتَّقُوا اللَّهَ إِنَّ اللَّهَ تَوَّابٌ رَحِيمٌ) (الحجرات ١٢)

عن أبي هريرة رضي الله عنه قال: قال رسول الله -صلى الله عليه وسلم:

«إياكم و الظن، فإن الظن أكذب الحديث، ولا تحسسوا ولا تجسسوا ولا تنافسوا ولا تحاسدوا ولا تباغضوا، ولا تدابروا وكونوا عباد الله إخواناً »

(رواه البخاري (٦٠٦٤)، ومسلم(٢٥٦٣)

وعن أبي برزة الأسلمي رضي الله عنه-: قال رسول الله -صلى الله عليه وسلم :

«يا معشر من آمن بلسانه ولم يدخل الإيمان قلبه، لا تغتابوا المسلمين، ولا تتبعوا عوراتهم، فإنه من اتبع عوراتهم يتَبّع الله عورته، ومن يتبع الله عورته يفضحه في بيته»

رواه أبو داود (٤٨٨٠)، وأحمد (٤/ ٤٢٠) (١٩٧٩١)، وأبو يعلى (١٣/ ٤١٩) (٧٤٢٣)، والبيهقي (١٠/ ٢٤٧) (٢٠٩٥٣). وقال الألباني في (٤٨٨٠): حسن صحيح.

نشر الشائعات

قوله تعالى: (يَا أَيُّهَا الَّذِينَ آمَنُوا إِن جَاءكُمْ فَاسِقٌ بِنَبَأٍ فَتَبَيَّنُوا أَن تُصِيبُوا قَوْمًا بِجَهَالَةٍ فَتُصْبِحُوا عَلَى مَا فَعَلْتُمْ نَادِمِينَ)

(سورة الحجرات٦)

وقوله تعالى: (وَإِذَا جَاءهُمْ أَمْرٌ مِّنَ الأَمْنِ أَوِ الْخَوْفِ أَذَاعُواْ بِهِ وَلَوْ رَدُّوهُ إِلَى الرَّسُولِ وَإِلَى أُوْلِي الأَمْرِ مِنْهُمْ لَعَلِمَهُ الَّذِينَ يَسْتَنبِطُونَهُ مِنْهُمْ)

(سورة النساء٨٣)

حديث النبي صلى الله عليه وسلم : (فأتينا على رجل مستلق لقفاه ، وإذا آخر قائم عليه بكلوب من حديد ، وإذا هو يأتي أحد شقي وجهه ويشرشر شدقه إلى قفاه ، ومنخره إلى قفاه ، وعينه إلى قفاه ، ثم يتحول إلى الجانب الآخر ، فيفعل به مثل ما فعل بالجانب الأول ، فما يفرغ من ذلك الجانب حتى يصبح ذلك الجانب كما كان ، ثم يعود عليه فيفعل مثل ما فعل في المرة الأولى ،)وأما الرجل الذي أتيت عليه يشرشر شدقه إلى قفاه ، ومنخره إلى قفاه ، وعينه إلى قفاه ، فإنه الرجل يغدو إلى بيته فيكذب الكذبة تبلغ الآفاق .

(صحيح البخاري)

جريمة الاعتداء

قال تعالى: (إِنَّ اللَّهَ يَأْمُرُ بِالْعَدْلِ وَالْإِحْسَانِ وَإِيتَاءِ ذِي الْقُرْبَى وَيَنْهَى عَنِ الْفَحْشَاءِ وَالْمُنْكَرِ وَالْبَغْيِ يَعِظُكُمْ لَعَلَّكُمْ تَذَكَّرُونَ) (النحل ٩٠)

قال الله تعالى:(عَاوَنُوا عَلَى الْبِرِّ وَالتَّقْوَى وَلَا تَعَاوَنُوا عَلَى الْإِثْمِ وَالْعُدْوَانِ) (المائدة ٢)

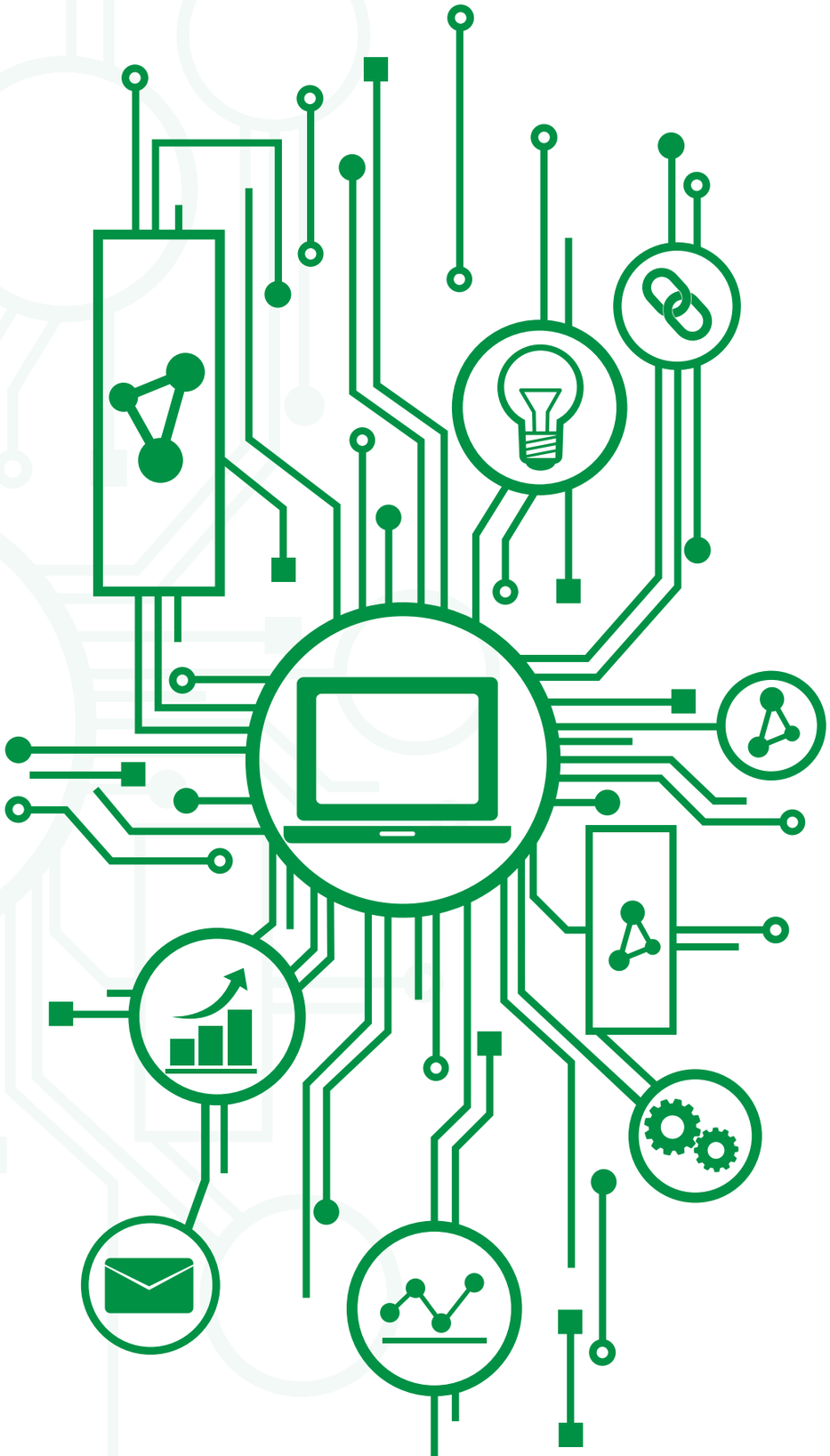
قال تعالى : (وَلَا تَعْتَدُوا إِنَّ اللَّهَ لَا يُحِبُّ الْمُعْتَدِينَ) (البقرة ١٩٠)

قوله صلى الله وسلم عليه - : « كل المُسلم على المسلم حرام؛ دمُه ومالُه وعِرضُه »

(رواه مسلم)

التطور التاريخي للأمن السيبراني

مع بداية الألفية الثالثة لاحظنا اعتماد مجالات الحياة بشكل رئيس على الإنترنت وتكنولوجيا الاتصالات والمعلومات مما جعل العالم قرية صغيرة في التعاملات الإلكترونية التجارية والصحية والتعليمية والأخبار المتنوعة الاقتصادية والسياسية والاجتماعية كل ذلك يتم في ثواني معدودة متخطياً عوامل البعد الزماني والمكاني بل أصبح الإدمان الإلكتروني أشد فتكاً من إدمان المخدرات والكحول والقمار وشعبيته شملت جميع الجنسيات والفئات والأعمار، وبدأت تطبيقات التكنولوجيا في الإنفجار بواجهات سهلة الاستخدام تتيح للجميع الانتقال والتجول عبر الإنترنت فأنشئت مجموعة من الطبقات المعقدة استنادا إلى رزمة بروتوكول TCP-IP الشهيرة كالطبقة الاجتماعيةالتقنية لتمكين العديد من الأنشطة السيبرانية اليوم. وتشمل هذه الأنشطة العديد من أنواع البيانات وتبادل المعلومات و البحث عن المعلومات واسترجاعها ، والمشاهدة الإلكترونية والاستماع ، و تمكين تكنولوجيا المعلومات والمعاملات ، والتحكم عن بعد ، ونظم التخزين ومعالجة البيانات ، يحدث بين (حوالي ٣ مليارات) من الناس النشطين في الفضاء السيبراني مما أوجد الجريمة السيبرانية ، وحرب الإنترنت واختراق البيانات وفي دراسة قدمها (the Ponemon) Institute أن التكلفة السنوية للجريمة السيبرانية زادت بنسبة ٣٠ في المائة من عام ٢٠١٢ إلى عام ٢٠١٣ ، وقدرت الخسائر المادية للجرائم السيبرانية عام٢٠١٥ بمبلغ ١١,٦ مليون دولار سنويا للشركات.



وأشار Van den Berg، (٢٠١٤). أنه خلال السنوات ١٥-٢٠ الماضية أصبحت المجتمعات تعتمد بشدة على أنظمة تكنولوجيا المعلومات من خلال إنشاء الفضاء الإلكتروني. الذي لم يولد فرصاً ومزايا جيدة فحسب بل إنه يولد أيضًا مخاطر إنترنت فظهر مصطلح الأمن السيبراني وأصبح شائعا كمتابعة لما كان يسمى بأمن المعلومات لإدراك أنه يجب علينا موازنة الفرص والمخاطر السيبرانية لتكوين تصور واضح حول ما هو الفضاء الإلكتروني وكيف يتم تنظيمه؟ ومن هم مبدعوالهجوم ،وماهي دوافعهم،وماهي المخاطر السيبرانية الحالية التي نواجهها؟ وماهي الحوادث السيبرانية المحتملة؟ ما هي مستويات المخاطر السيبرانية المقبولة؟ ما هي الحرب السيبرانية ومن ينفذ عمليات الحرب؟ وكيف يمكن تأمين الفضاء السيبراني؟

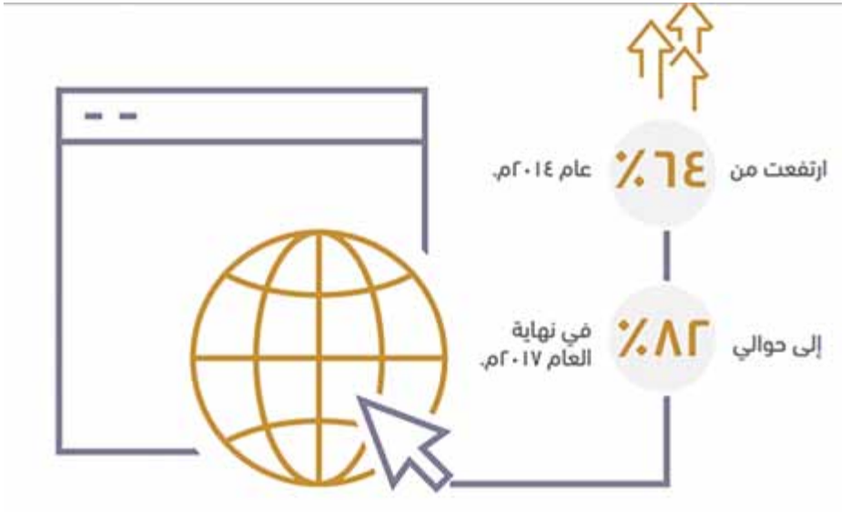
أهداف الأمن السيبراني

بما أن الجريمة السيبرانية جريمة لايحدها مكان أو زمان معين فهي عابرة للقارات ولاتقتصر على دولة بعينها فكل العالم يعتبر مسرحاً لها وذلك بحد ذاته يثيرتحديات ومعوقات مما يتوجب نشر الوعي بأهداف الأمن السيبراني واستعراض أبعاده الدينية والاجتماعية والاقتصادية والسياسية كالتالي:

- الحماية الدينية والأخلاقية: حيث أصبح من الممكن تجاوز القيم والمعايير والضوابط الاجتماعية فهناك مواقع إباحية تعمل على تدمير القيم والأخلاق وتبعد الإنسان عن دينه وعاداته وتقاليده وتدفعه لارتكاب الجرائم وفعل المحرمات فالأمن السيبراني يقدم الحلول التكنولوجية والحماية التامة من مثل هذه المواقع المدمرة.
- الحماية الوطنية :بما أن الفضاء السيبراني أصبح مجالاً للحروب الإلكترونية الخفية والتي بسببها تدمر مقدرات الوطن وإمكانياته وقد تستخدم أفراد هذا الوطن ضمن جيوشها المعادية دون معرفتهم فالأمن السيبراني يجعل لهذا المواطن حزام أمان يستطيع من خلاله الحذر والتنبه لمثل هذه الحرب الخطيرة.
- الحماية المالية: فعن طريق الأمن السيبراني سيتم معرفة جميع أنواع وطرق الإحتيال الإلكترونية التي تستهدف معلومات البنك والبطاقات الإئتمانية وبطاقات الصرف الآلي الشخصية والإعلانات والدعايات التجارية المضللة.
- الحماية الشخصية: يتعلم من خلال الأمن السيبراني عدم الإدلاء بأي معلومات شخصية مثل كلمات المرور الخاصة ومكان العمل والسكن وغيرذلك من المعلومات التي لايمكن لأي شخص غريب الإطلاع عليها.

أرقام وإحصائيات مهمة

زادت نسبة انتشار خدمات الإنترنت بمعدلات عالية خلال السنوات الماضية حيث ارتفعت من ٦٤٪عام ٢٠١٤م إلى حوالي ٨٢٪في نهاية العام ٢٠١٧م،ويقدر عدد مستخدمي الإنترنت في المملكةحالياً بأكثر من ٢٦مليون مستخدم،ويلحظ زيادة الطلب على خدمات الإنترنت والنطاق العريض مؤخراً مع زيادةالاستخدام والارتباط الكبير بقنوات التواصل الاجتماعي، واستخدام قنوات المحتوى بحسب الطلب (مثل يوتيوب، سناب شات،) إضافة الى الألعاب عبرالإنترنت؛ إذ أصبح المشترك يبحث عن سرعات أعلى وسعات تحميل أكبر؛ ولذلك زادت كمية البيانات المستخدمة بشكل كبيرفي السنوات القليلة الماضية.



عدد مستخدمي الانترنت

إحصائيات استخدام الخدمات الإلكترونية

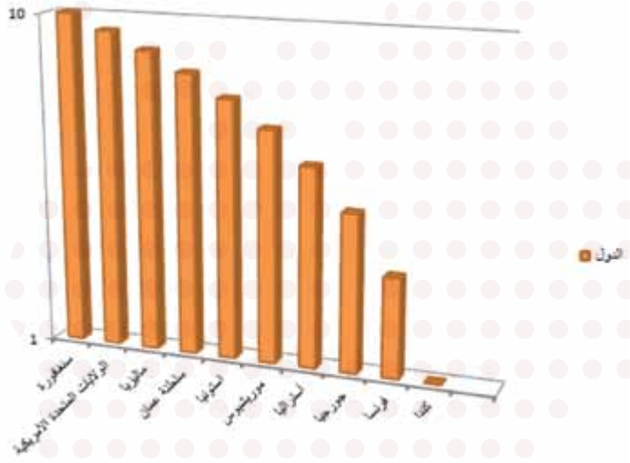
عدد بلاغات ٢٠١٧العناوين مصابة ببرمجيات خبيثة أو ثغرات أمنية ١٠,٤٣٠ بلاغاً

تجارب دولية في الأمن السيبراني

وبناءً على التقرير الصادر من الاتحاد الدولي للاتصالات IUT في ٢٠١٧ حيث صنفت الدول حسب قوتها في الأمن السيبراني

قائمة بالدول الـ ١٠ التي تصدرت التصنيف

سنغافورة	الولايات المتحدة الأمريكية	ماليزيا	سلطنة عمان	استونيا
موريشيوس	أستراليا	جورجيا	فرنسا	كندا



وقد تناول هذا الكتاب تجربة الدول الأوائل في مجال الأمن السيبراني كالتالي:

تجربة سنغافورة في الأمن السيبراني:

أنشأت وكالة CSA وهي وكالة وطنية تشرف على استراتيجيات الأمن السيبراني والعمليات والتعليم والتوعية والتطوير في مجال الأمن

السيبراني في سنغافورة أصدرت قانون الأمن السيبراني في ٥ فبراير ٢٠١٨ وحصل على موافقة الرئيس في ٢ مارس ٢٠١٨ ليصبح قانون الأمن السيبراني ويضع القانون إطارًا عاماً للإشراف على الأمن السيبراني الوطني وصيانته في سنغافورة. وتتمثل أهدافه الرئيسية الأربعة في:

١.تعزيز حماية البنية التحتية للمعلومات ضد الهجمات السيبرانية و أنظمة الكمبيوتر لتوفير الخدمات الأساسية للتصدي للهجمات السيبرانية التي لها تأثير مدمر على الاقتصاد والمجتمع ويوفر القانون إطارًا لتزويد المختصين بوضوح حول التزاماتهم بحماية البنية التحتية بشكل استباقي من الهجمات السيبرانية بما يحقق مرونة في ، حماية CII لاقتصاد سنغافورة وتتمثل قطاعات CII في: الطاقة ، والمياه ، والخدمات المصرفية والمالية ، والرعاية الصحية ، والنقل (التي تشمل الأراضي والبحرية والطيران المعلومات الاتصالية، وسائل الإعلام ، الأمن وخدمات الطوارئ ، والحكومة.

٢.تفويض الوكالة لمنع التهديدات والحوادث المتعلقة بالأمن السيبراني والاستجابة لها. ويخول القانون مفوض الأمن السيبراني بالتحقيق في التهديدات والحوادث المتعلقة بالأمن السيبراني لتحديد أثرها ومنع وقوع المزيد من الضرر أو حوادث الأمن السيبراني وهذا يؤكد للسنغافوريين أن الحكومة يمكن أن تستجيب بفعالية للتهديدات الأمنية السيبرانية والحفاظ على سنغافورة آمنة.

٣.إنشاء إطار لتبادل معلومات الأمن السيبراني، ويسهل القانون أيضًا تبادل المعلومات ، وهو أمر بالغ الأهمية ، حيث تساعد المعلومات في الوقت المناسب الحكومة ومالكي أنظمة الكمبيوتر على تحديد نقاط الضعف ومنع الحوادث السيبرانية على نحو أكثر فعالية.

٤.إنشاء إطار ترخيص يعمل باللمس الخفيف لمقدمي خدمات الأمن السيبراني يتبنى نوعين من الخدمات، وهما اختبار الاختراق ومركز مراقبة العمليات الأمنية المدارة وبالتالي للوكالة تأثير كبير على المشهد الأمني العام يسعى إلى تحقيق توازن بين الاحتياجات الأمنية وتطوير نظام بيئي آمن للأمن السيبراني.

تجربة الولايات المتحدة الامريكية

-أنشأت شبكة NSAمشتركة بين قطاعات الولايات المتحدة لتعزيز الأمن السيبراني على كافة الأصعدة تشمل معلومات سرية ، أو التي تعتبر ضرورية للبعثات العسكرية والاستخباراتية.

-تواجه هذه الأنظمة تهديدات إلكترونية سريعة التطور وابتكار الحلول ووضع معايير لأنظمة الأمن القومي.

-تنشر الاستشارات والتوجيهات وأفضل الممارسات للعاملين في مجال الأمن السيبراني.

- تعززالمعرفة بالأمن السيبراني من خلال مبادرة علوم الأمان والخصوصية.

- تقوم بتدريب الجيل القادم من المتخصصين على الإنترنت على برامج مثل NSA Cyber Exercise منحة MIT إلى برامج غيردرجة المحترفين للمحترفين من معهد ماساشيتوش.

-يوفر التعليم الاحترافي في معهد ماساتشوستس للتكنولوجيا ، الذي تم تنظيمه في إطار كلية الهندسة في عام ٢٠٠٢ ، دورات تعليمية مستمرة في الأمن السيبراني ، بمشاركة المتخصصين من جميع أنحاء العالم الذين يدرسون دورات دراسية منتظمة في معهد ماساتشوستس للتكنولوجيا لمدة فصل دراسي واحد أو أكثر.

-وتستقطب "البرامج القصيرة" ، التي كانت تعرف سابقا باسم "المعهد المهني" ، أكثر من ١٢٠٠ مشاركًا عالميًا في الحرم الجامعي كل عام وبحضور حوالي ٥٠ دورة قصيرة ، مدتها ١-٥ أيام ، يتم تقديمها بشكل أساسي في فصل الصيف يتم تقديم بعض الدورات القصيرة من خلال البرامج الدولية.

- تشارك الشركات والمؤسسات معهد MIT للتعليم المهني في مجال الأمن السيبراني لإرشادهم لحماية منشآتهم على أفضل وجه من خلال هذه الدورات .

تجربة ماليزيا

لماليزيا تجربة رائدة في مجال الأمن السيبراني حيث بدأت بتوظيفه في التعليم و أنشأت مركز CyberSecurity Malaysia ، وتأتي هذه المبادرة للتوعية الأمنية عبر الإنترنت للجميع ، و تثقيف وتعزيز وعي الجمهور العام بشأن المشكلات التكنولوجية والاجتماعية التي تواجه مستخدمي الإنترنت ، وخاصة المخاطر التي يواجهونها على الإنترنت واستهدفت هذه المبادرة توعية الشباب والأباء والمنظمات والأطفال والمواقع الاجتماعية وخصصت لكل منهم موقعاً على الانترنت يصف المخاطر السيبرانية وكيفية الوقاية منها مزوداً بمقاطع فيديو شارحة وقد فازت هذه المبادرة بلقب البطل عام ٢٠١٨ في الملتقى الذي عقد في (Asia Pacific University APU) كوالالمبور.

الشكل(١) يوضح موقع الآباء في مركز الأمن السيبراني ماليزيا

تجربة سلطنة عمان

يعد المركز الوطني للسلامة المعلوماتية أحد مبادرات عمان الرقمية والنقطة المحورية للحوادث الأمنية في سلطنة عُمان، إذ تم تدشينه في شهر أبريل عام ٢٠١٠م بهدف توفير بيئة معلوماتية آمنة لأي مستخدم لمواقع جهات حكومية أو خاصة على حد سواء. وتعمل على بناء الثقة في استخدام الخدمات الحكومية، وتطوير استراتيجيات وسياسات أمن المعلومات لتستفيد منها الجهات الحكومية والخاصة، كما أنها تقدم نصائح فنية مبدئية وتقارير تقنية تساعد إداريي الشبكات والأنظمة والتطبيقات في كل من القطاع العام أو الخاص على تجنب تعريض مواقعهم لأية مخاطر أمنية.

والجدير بالذكر أن الخدمات التي يوفرها المركز مقدمة للأفراد وللقطاع العام والخاص والهياكل الوطنية الحساسة في الدولة.

ويسعى المركز الى تحقيق الأهداف التالية:

١. توفير بيئة معلوماتية آمنة عند استخدام الخدمات الالكترونية الحكومية لكل مواطن عماني ومقيم.

٢. تشجيع الأفراد الذين يتلقون التدريب في المركز على العمل في قطاع أمن المعلومات في أي جهة أو مؤسسة في السلطنة.

٣. الإستجابة لأية حوادث أمنية ومحاولة الحد من أثارها.

٤. نشر الوعي حول أهمية أمن المعلومات بين أفراد المجتمع العماني.

كما يوفر المركز العديد من الخدمات مثل:

١. تأهيل كوادر عمانية متخصصة في هذا المجال.

٢. مراقبة مواقع حية من أجل اكتشاف أية أخطار قد تهدد هذه المواقع.

٣. تقديم دورات وورش وحلقات تدريبية لكافة المستهدفين.

٤. الإستجابة الاستباقية والتفاعلية لأية مشكلة مباشرةً.

٥. حماية أي نظام ومعالجته في حالة تعرضه لأية مشكلة عن طريق تقديم التوجيه.

إحصائيات حول المركز الوطني للسلامة المعلوماتية وفقا للتقرير السنوي لهيئة تقنية المعلومات (٢٠١٤):

- الكشف عن أكثر من ٨،٧١٣ هجمة خطيرة ومرتبطة بالأمن المعلوماتي موجهة للفضاء المعلوماتي العماني ناتجة عن تحليل ملايين من محاولات الاتصال وتصنيفها.
- الكشف عن ٥٣٧ حالة ألحقت أضرارا وانتشارًا لبرمجياتٍ خبيثة تستهدف الفضاء المعلوماتي في الدولة.
- إجراء ١٣ تقييم لنقاط الضعف الأمنية واختبارات اختراق وتحقق للمؤسسات الحكومية وللهياكل الوطنية الحساسة عام ٢٠١٤.
- علاج ١١٨ حالة للأدلة الرقمية ناتجة عن تحليل ٢٨٨ جهاز بما فيها أجهزة الكمبيوتر والهواتف والأقراص الصلبة الخارجية ووحدات التخزين المتنقل.
- اكتشاف ٢٨٨ دليلَ إدانة رقمي خلال عام ٢٠١٤م.
- تم تدشين المركز الإقليمي للأمن السيبراني التابع للاتحاد الدولي

للاتصالات رسميا عام ٢٠١٣م ، والانتهاء من إنشاء خارطة طريق لدراسة الأمن السيبراني في المنطقة العربية ويقوم هذا المركز بتلبية متطلبات الوطن العربي فيما يتعلق بأمن المعلومات ويشكل عاملا أساسيا في دعم شبكات الشراكة الدولية متعددة الأطراف ضد التهديدات السيبرانية (IMPACT) على مستوى العالم في مختلف المناطق من خلال اضفاء الطابع العربي على خدمات أمن المعلومات وذلك بناء على حاجة الوطن العربي وقام المركز بعقد وتنظيم المؤتمراالاقليمي الثالث للأمن السيبراني عام ٢٠١٤ وشارك المركز في اجتماع الفريق العامل التابع لمجلس الاتحاد الدولي للاتصالات حول حماية الأطفال من مخاطر الانترنت الذي عقد في جنيف.

إنجازات المركز:

- حصل المركز على جائزة القمة العالمية لمجتمع المعلومات في سويسرا في فئة بناء الثقة والحماية في استخدام تقنية المعلومات والاتصالات.

- حصلت السلطنة على المركز الأول في قائمة أمن المعلومات العالمي على مستوى الوطن العربي التي نظمها الاتحاد الدولي للاتصالات.

تجربة المملكة العربية السعودية في الأمن السيبراني

أنشأت المملكة العربية السعودية الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز Saudi Federation for Cybersecurity، Programming and Drones وهو مؤسسة وطنية تحت مظلة اللجنة الأولمبية السعودية يسعى لبناء قدرات محلية واحترافية في مجال الأمن السيبراني وتطوير البرمجيات بناءً على أفضل الممارسات والمعايير العالمية، للوصول بالمملكة العربية السعودية إلى مصاف الدول المتقدمة في صناعة المعرفة التقنية الحديثة قدمت العديد من الفعاليات النوعية منها على سبيل المثال:

- **"كايزن العربية" مسابقة التقط العلم**

وهوالحدث التفاعلي المهم، مصمم لإبراز مهارات هواة "الأمن السيبراني"، عبر منافسات في مجالات عدة مثل التحليل الجنائي، اختراق المواقع والهواتف الذكية، تطوير وبرمجة الثغرات، التشفير والهندسة العكسية وقد شارك فيه ٣٧٠ متسابق في ٧ أبريل ٢٠١٨.

- **هاكاثون الحج**

لاستغلال التكنولوجيا والإبداع لتيسير العملية وتحسين التجربة العامة للحجيج في ٢٠١٨/٣/١وقدمت جوائز تفوق قيمتها ٢،٠٠٠،٠٠٠ ريال سعودي للمتسابقين وبعض المزايا ك:

-التذاكر المجانية لمؤتمر المطورين في Google IO ٢٠١٩ بامريكا في

أبريل-يونيو.

-جهاز Google Home Mini مدمج بـ Google Assistant

-رصيد Google Cloud

-تذاكر مجانية لمؤتمر RiseUp Summit ٢٠١٨

مسابقة التقط العلم (Capture The Flag) الأحد ٣ يونيو ٢٠١٨ م وهي مسابقة في مجال الأمن السيبراني، تحاكي بيئة تقنية حقيقية ويتنافس فيها الأفراد ضد بعضهم البعض. المسابقة تقام خلال المساء وتحتوي على تحديات بمستويات مختلفة تحت مواضيع مختلفة مثل التشفير، الهندسة العكسية، اختراق الويب والشبكات، والبرمجة، بمستويات مختلفة، ويقوم المشاركون بحل تحديات تتمثل في استغلال الثغرات الأمنية، أو تعدي أنظمة الحماية، أو صد هجمات سيبرانية ، أو فك معلومات مشفرة ، الحل الصحيح لأحد التحديات يؤدي إلى الحصول على "علم"، وكل علم يحمل عدداً من النقاط حسب نوعية التحدي وصعوبته. الشخص الذي يجمع أكبر عدد من النقاط يفوز في المسابقة!

•إنشاء كلية الأمن السيبراني والبرمجة والذكاء الاصطناعي.

صدر قرار رئيس مجلس إدارة الاتحاد السعودي للأمن السيبراني والبرمجة سعود بن عبدالله القحطاني، بإنشاء كلية تختص بالأمن السيبراني والبرمجة والذكاء الاصطناعي، مقرها الرياض.

ويأتي ذلك بناء على رؤية المملكة ٢٠٣٠ في التحول إلى مجتمع معرفي وتقني ينافس الدول العالمية المتقدمة في الإبداع التقني المعلوماتي والرياضات الذهنية وبالأخص في مجال السايبر والبرمجة.

وتسعى الكلية إلى بناء وتأهيل قدرات وطنية شابة محترفة بأحدث الوسائل التقنية التي يمكن من خلالها المساعدة في تحقيق أهداف رؤية المملكة ٢٠٣٠ .

وتأتي مبادرة إنشاء الكلية متزامنة مع التطورات والتحديات التي تواجهها الدول العالمية في هذه المجالات الحيوية.

•استحداث كلية الأمن السيبراني في عدد من الجامعات كجامعة الملك سعود وجامعة جدة.

تجربة المملكة المتحدة في الأمن السيبراني:

أنشأت المملكة المتحدة مركز ابتكار إلكتروني رائد على مستوى العالم يتم تطويره في East Here مما يوفر ٢٠٠٠ وظيفة في المملكة المتحدة في مجال الأمن السيبراني.

انطلاقاً من مركز الابتكار في Plexal في Here East ، فقدعزز نشاط المؤسسات الرقمية في شرق لندن ويحفز تطوير التكنولوجيا المتطورة لمنع الجريمة السيبرانية في المملكة المتحدة.

ويتم تمويل المركز من قبل وزارة الثقافة الرقمية والإعلام والرياضة ، كجزء من استثمار الحكومة البالغ ١,٩ مليار جنيه استرليني في الأمن عبر الإنترنت.

وأضافت مارغوت جيمس ، وزيرة الصناعات الرقمية والإبداعية : إن لندن هي القائد بلا منازع للتكنولوجيا الأوروبية ، حيث تتدفق مليارات الاستثمارات في كل عام ، وتقوم الشركات الرائدة في العالم بتطوير الابتكارات الرائدة.

تجربة استراليا في الأمن السيبراني

تم إنشاء مركز الأمن السيبراني في أستراليا The Australian Cyber Security Centre وهو مركز لدعم الأمن وتعزيزه في العصر الرقمي والتصدي للحوادث الرقمية والتبليغ عنها (ACSC) ويعد المعهد الأسترالي لبحوث الأمن السيبراني (ACSRI) أول مركز أسترالي استراتيجي منسق في مجال البحوث والتعليم بين الوكالات الحكومية والقطاع الخاص والباحثين. ويسعى إلى تركيز الحكومة على الأمن السيبراني من خلال الجمع بين شبكة تعاونية للتصدي للتهديدات السيبرانية وتحسين فرص تطوير مهنيين متخصصين في مجال الأمن السيبراني.

مثل العديد من الدول الأخرى ، تعاني أستراليا من نقص في مهارات الأمن السيبراني هذه المهارات الخاصة ضرورية في العالم المتصل بالتكنولوجيا ، الإستراتيجية. إلا أن هذه المهارات نفسها تعاني من نقص في المعروض ، وتوقع المعهد أن يشهد مجال أمن المعلومات عجزًا عالميًا يبلغ ١,٥ مليون متخصص بحلول عام ٢٠٢٠.

ويلتزم المعهد بتزويد الأستراليين بمهارات الأمن السيبراني الصحيحة ورفع مستويات الوعي الأمني الإلكتروني حتى يتمكن الجميع من الاستفادة من الفرص المتاحة في الفضاء السيبراني.

وسيقدم المعهد تعليمًا أمنيًا في المرحلة الجامعية والدراسات العليا من خلال منهج دراسي متسق وتعليم متميز و ستعمل الحكومة مع القطاع الخاص ، ومؤسسات خدمة الولايات والأقاليم والمهارات لدعم التوسع في التدريب على الأمن السيبراني في منظمات التدريب ليشمل ذلك تطوير التدريب المهني على الأمن السيبراني و التركيز على طلاب الجامعات إلى برنامج أوسع من المسابقات وفرص تطوير المهارات لمجموعة أوسع من المشاركين ، وسيتيح الفرصة للناس على جميع المستويات في القوى العاملة ، بما في ذلك في المناصب التنفيذية ، لتحسين معرفتهم ومهاراتهم الأمنية عن طريق المشاركة في الدورات القصيرة والتدريب التنفيذي وغيرها من البرامج و زيادة عدد الأشخاص الذين يتمتعون بمهارات الأمن السيبراني.

الفصل الثاني

الجرائم السيبرانية (cyber crime)

التطور التاريخي للجريمة السيبرانية

أنواع الجرائم السيبرانية

الجرائم السيبرانية (cyber crime)

تعتبر الجرائم السيبرانية من الجرائم التي تباينت مسمياتها عبر المراحل الزمنية لتطورها التي ارتبطت بتقنية المعلومات وقد عرفتها أبونعارة" أنها كل أشكال السلوك غير المشروع، والمتعمد الذي يرتكب باستخدام الحاسب الآلي المرتبط بالانترنت، وكل ما يمس به أو بمحتوياته أو بالعمليات التي تتم بواسطته،بغرض إلحاق الضرر بالضحية أو الكسب المادي أو غير ذلك من الأغراض، من طرف أفراد على درايةكاملة بتقنيات التكنولوجيا المعلوماتية وأسرارها"

وتعرف الجرائم السيبرانية إجرائياً "هي كل سلوك مخالف يرتكب ضد أفراد أوجماعات باستخدام وسائل الاتصالات الحديثة بهدف الإساءة الإلكترونية للضحية مادياً أومعنوياً بطريقة مباشرة أو غير مباشرة" الجريمة السيبرانية تتم بدون مسرح للجريمة ولايشترط تواجد المجرم والضحية في نفس المكان.

التطور التاريخي للجريمة السيبرانية:

ذكرت أبونعاره (٢٠١٦) أن مفهوم جريمة الكمبيوتر مر بتطور تاريخي تبعا لتطور التقنية واستخداماتها ويمكن تقسيمها إلى ثلاثة مراحل:

المرحلة الأولى:

مبدأت المرحلة الأولى بظهور استخدام الكمبيوتر وربطه بالشبكة في الستينات إلى السبعينات حيث ظهرت أول معالجة لجرائم الكمبيوتر في شكل مقالات صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والتجسس المعلومات ، وشكلت موضوع التساؤل إذا ما كانت هذه الجرائم مجرد حالة عابرة أم ظاهرة إجرامية مستجدة ؟ وهل هي جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في مجال المعلوماتية؟

فبقيت محصورة في إطار السلوك اللاأخلاقي دون النطاق القانوني ومع توسع الدراسات تدريجيا و خلال السبعينات بدأ الحديث عنها كظاهرة إجرامية جديدة .

المرحلة الثانية :

وفي الثمانينات ظهر نوع جديد من الجرائم ارتبط بعمليات اقتحام نظم الحاسوب عن بعد ونشر الفيروسات عبر شبكات الكمبيوتر ،الذي سبب تدمير الملفات و البرامج أين شاع اصطلاح "الهاكرز"، المعبر عن مقتحمي النظم، وبقي دائما الحديث عن دوافع هذه الجرائم محصور في اختراق أمن المعلومات وإظهار التفوق التقني من قبل مرتكبي هذه الأفعال الذين لم يتعدوا فئة صغار السن العباقرة في هذا المجال، لكن بتزايد خطورة هذه الممارسات أصبح من الضروري إعادة تصنيف

الفاعلين وتحديد طوائفهم خاصة بعد تحول الجريمة من مجرد مغامرة و إبداء التفوق إلى أفعال تستهدف التجسس والاستيلاء على البيانات الاقتصادية والاجتماعية والسياسية والعسكرية.

المرحلة الثالثة:

شهدت التسعينات تناميا هائلا في حقل الجرائم التقنية وتغيرا في نطاقها ومفهومها، وكان ذلك بفعل ما أحدثته شبكة الإنترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكات المعلومات، فظهرت أنماط جديدة كأنشطة إنكار الخدمة، التي تقوم على فكرة تعطيل نظام تقني ومنعه من القيام بعمله المعتاد، وأكثر ما مورست ضد مواقع الإنترنت التسويقية الناشطة والهامة التي يعني انقطاعها عن الخدمة لساعات خسائر مالية بالملايين، ونشطت جرائم نشر الفيروسات عبر مواقع الإنترنت لما تسهله من انتقالها إلى ملايين المستخدمين في ذات الوقت، وظهرت أنشطة الرسائل والمواد الكتابية المنشورة على الإنترنت أو المرسلة عبر البريد الإلكتروني، المنطوية على إثارة الأحقاد أو المساس بكرامة واعتبار الأشخاص أو المستهدفة الترويج لمواد أو أفعال غير قانونية وغير مشروعة (جرائم المحتوى الضار) .

أنواع الجرائم السيبرانية

في ظل تحديات العصر الرقمي الذي يتجسد في بنية تحتية رقمية عالية تساعد الجماعات الإجرامية على ارتكاب أعمال غير مشروعة باستغلال التسهيلات التي تمنحها شبكة الإنترنت كوسيلة لتنفيذ الجرائم السيبرانية مع تزايد التوسع في استخدام بيئة الإتصالات والمعلومات التي تتسم بالسرعة والعالمية والتنافسية وقد صاغ كلاً من ابن تاج(٢٠١٨)، الهزاني(٢٠١٨)،العتيبي(٢٠١٧) ،المقصودي (٢٠١٧)الردفاني(٢٠١٤)، ،أبو نعارة(٢٠١٤) أنواع الجرائم السيبرانية :

•انتهاك الخصوصية:

حيث تعتبر من الحقوق الفردية التي نصت عليها التشريعات الداخلية والاتفاقات الدولية ،والحياة الخاصة تشمل الحياة العاطفية والزوجية والعائلية والحالة الصحية والأحاديث الخاصة والمحادثات الهاتفية والمراسلات والحقوق المالية والمعتقدات الدينية والمسكن والاسم والمهنة والعمل وللفرد كامل الحق في الحفاظ على خصوصية معلوماته ومعالجتها آلياً وترشيد استخدامها ومن صور انتهاكها في الفضاء السيبراني مايلي :

-إدخال معلومات وهمية وانتحال الشخصية بهدف حصول المعتدي على مبالغ مالية.

-التجسس الإلكتروني بتتبع العيوب واصطياد الأخطاء.

-الاعتداء على الحياة الخاصة والتصنت ومحاولة الوصول للسجلات والمعلومات الإلكترونية.

-القذف والسب والشتم سواء بلفظ صريح أو تعريض مما ينشأ عنه ارتكاب الجرائم.

-التشهير ويعتبر من الانتهاكات السيبرانية المحرمة شرعاً وقانوناً.

-سرقة البيانات الشخصية وبيعها كمعلومات لمروجي السلع والإعلانات التجارية عبر الإنترنت.

•انتهاك أمن المعلومات :

وتعرف المعلوماتية إجرائياً بمجموعة البيانات التي تخضع للمعالجة والتشغيل والتحليل والتفسير والاستخدام المنظم لأغراض معينة لتحقيق زيادة المعرفة وتشمل جرائم الولوج إلى نظام معلوماتي أوالمكوث فيه، مع التعرض للبيانات المعلوماتية وجرائم إعاقة عمل معلوماتي .

جرائم الاستغلال الجنسي للقاصرين: تظهرها الأفعال التي تتعلق باستغلال القاصرين في أعمال جنسية، وتشمل الرسومات أو الصور أو الكتابات أو الأفلام أو الإشارات، أو أي أعمال إباحية يشارك فيها قاصرون، أو تتعلق باستغلال القاصرين في المواد الإباحية، وتشمل أيضاً إنتاج مواد إباحية للقاصرين بقصد بثها بواسطة نظام معلوماتي.


السعودية.. المتحرش بالأطفال "طمبق" في قبضة العدالة

تاريخ النشر: 06.07.2018 | GMT 07:15 | أخبار العالم العربي

•جرائم التعدي على الملكية الفكرية للأعمال الرقمية:

تشمل الجرائم الآتية : جرم وضع اسم مختلس على عمل، وجرم تقليد إمضاء المؤلف أو ختمه، وجرم تقليد عمل رقمي أو قرصنة البرمجيات،

وجرم بيع أو عرض عمل مقلد أو وضعه في التداول، وجرم الاعتداء على أي حق من حقوق المؤلف أو الحقوق المجاورة.

•جرائم الاختراق:

هي عملية اقتحام الأنظمة أو الشبكات الخاصة بأفراد أو منظمات خاصة أو حكومية بمساعدة بعض البرامج المتخصصة في فك وسرقة كلمات السر، وتصريحات الدخول بهدف الاطلاع على المعلومات أو تخريبها أو سرقتها حيث يتسبب الاختراق في مشاكل مزعجة مثل تبطئ حركة التصفح وانقطاعه على فترات منتظمة، ويمكن أن يتعذر الدخول إلى البيانات، وفي أسوأ الأحوال يمكن اختراق المعلومات الشخصية للمستخدم.

•الاقتحام أو التسلل:

يشمل الاختراقات سواء للمواقع الرسمية أو الشخصية، أو اختراق الأجهزة الشخصية واختراق البريد الإلكتروني، أو وسائل الاتصال الاجتماعي ،أو الاستيلاء عليه، والاستيلاء على اشتراكات الآخرين وأرقامهم السرية، وهي أفعال أصبحت تنشر يوميا في الصحف والأخبار.

•الانتهاك عبر المواقع :

ومن ابرزها المواقع الدينية التي تنشر الإرهاب وتدعو إليه والعقائد الباطلة والخرافات الدينية المضللة واستغلال الأحاديث الموضوعة وتفسيرالآيات القرآنية بلوي أعناق النصوص واستدلالات في غير محلها.

١.الجرائم المعلوماتية ضد الدولة والسلامة العامة:

تتضمن الأفعال الجرمية الناشئة عن المعلوماتية التي تطال الدولة

وسلامتها وأمنها واستقرارها ونظامها القانوني، وهي جرائم تعطيل الأعمال الحكومية أو أعمال السلطة العامة باستعمال وسيلة معلوماتية، والإطلاع أو الحصول على معلومات سرية تخص الدولة، وذلك من خلال شبكة الإنترنت أو باستعمال وسيلة معلوماتية،والأعمال الإرهابية التي ترتكب باستخدام شبكة الإنترنت أو أي وسيلة معلوماتية.

أعلنت حكومة سنغافورة سرقة البيانات الشخصية لمليون ونصف المليون شخص بينهم رئيس الوزراء لي هسين لونج، في هجوم إلكتروني كبير على قاعدة البيانات الصحية التابعة لها.

تنبأت شركة الأبحاث الأميركية «سايبرسيكيوريتي فينتشرز» في عام ٢٠١٦، بأن الجرائم الإلكترونية ستكلف العالم ٦ تريليونات دولار أميركي سنوياً بحلول عام ٢٠٢١، أي بزيادة الضعف عن كلفتها التي بلغت ٣ تريليونات دولار أميركي عام ٢٠١٥.

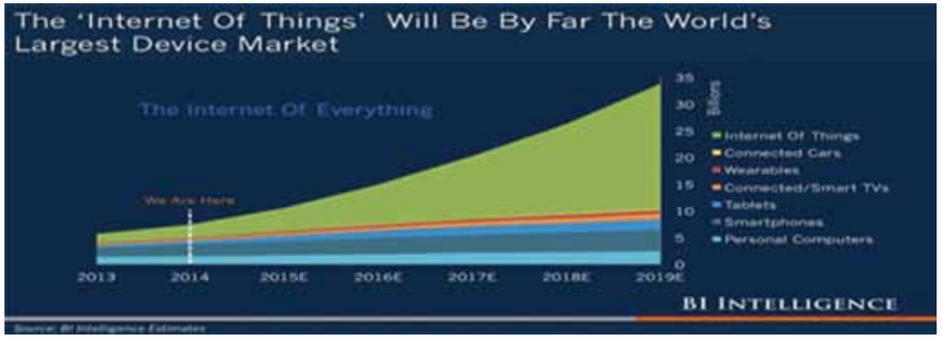
وبلغ متوسط تكاليف اختراق البيانات التي تتحملها أي منظمة ٣,٦ ملايين دولار أميركي، وفقاً لدراسة أجريت في عام ٢٠١٦ على ٤١٩ شركة في ١٣ بلداً من قبل معهد بونيمون وهو شركة أبحاث أميركية.

انفوجرافيك مجلة البيان

٢.التنمر الإلكتروني باستخدام الألعاب الإلكترونية

بالتهديد بالأذى البدني والابتزاز والتهديد بالضرب والقتل وإعطاء أوامر ظاهرها الرحمة وباطنها العذاب.

بحلول٢٠٢٠، سيكون حجم سوق إنترنت الأشياء أكبر من سوق الهواتف المحمولة و أجهزة الحاسب و الأجهزة اللوحية مجتمعين بمقدار الضعفين! حيث ستصل عدد أجهزة إنترنت الأشياء إلى ٣٥ مليار جهاز متصل بالإنترنت.



الفصل الثالث

تقنيات الاستخدام المعلوماتي

التوعية المستمرة بمبادئ المواطنة الرقمية

التخطيط المستقبلي لريادة الأمن

السيبراني لدى طلابنا

تقنيات الاستخدام المعلوماتي

حرصك ووعيك في استخدام تقنيات الفضاء السيبراني يمثل حزام أمان لحياتك المادية والمعنوية ودولتك ومجتمعك وكيانك الذي تعيش فيه .

ذكر الربيعة (٢٠١٨) خطوات مهمة للحفاظ على الأمن السيبراني تناول هذا الكتاب أهمها :

١.الجهاز الشخصي:

- للمحافظة على أمن جهازك وملفاتك الشخصية قم بالتالي:
- تركيب برامج مكافحة الفيروسات والحرص على تحديثها وفحص الجهاز بشكل دوري.
- الحذر عند الإتصال بالشبكات اللاسلكية العامة.
- المداومة على تحديث نظام التشغيل والتطبيقات.
- الاحتفاظ بنسخة احتياطية.

٢.كلمة المرور:

- اختيار كلمة مرور قوية تحتوي على مجموعة من الاحرف والأرقام و الرموز.
- استخدام كلمة مرور مستقلة لكل حساب.
- عدم اختيار كلمة مرور مبنية على معلومات شخصية.
- عدم مشاركتها.
- تغييرها بشكل دوري.

٣.حماية بريدك الإلكتروني:

- وضع كلمات مرور قوية و تفعيل التحقق الثنائي.
- عدم فتح المرفقات من مصدر مجهول.
- تفادي الوقوع ضحية للرسائل الاحتيالية.
- تخصيص بريد خاص للاستخدامات الرسمية والهامة.
- استخدام تطبيقات لإدارة كلمة المرور.
- Dashlane free password manager
- LastPass
- 1U Password Manager

٤.استعادة السيطرة بعد الاختراق:

- فصل جهازك من الإنترنت حتى يفصل الرابط بينك وبين المخترق.
- إعادة تهيئة الجهاز.

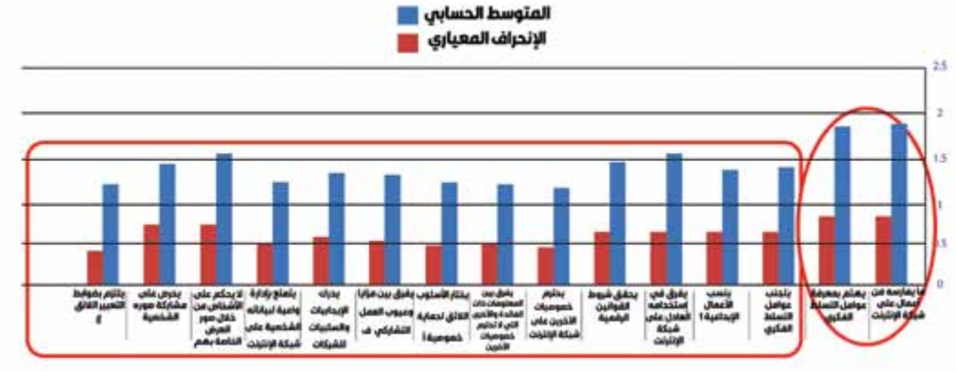
- تثبيت برامج حماية الفايروسات و إجراء فحص شامل للجهاز.
- استعادة البيانات والمعلومات من النسخ الاحتياطية.

٥.استعادة السيطرة بعد الاختراق في مواقع التواصل الاجتماعي:

- استعمال جهاز آخر للدخول إلى حساباتك الشخصية وتغيير كلمات المرور.
- في حال عدم تمكنك من الدخول للبريد الإلكتروني الخاص بجهازك ؛ يمكن استعادته باستخدام خاصية نسيان كلمة المرور، ويمكنك في هذه الحالة الاستفادة من عنوان البريد الثانوي(الاحتياطي).
- في حال عدم تمكنك من استعادة حساب التواصل الاجتماعي أو البريد الإلكتروني يجب التواصل مع الدعم الفني الخاص بالجهة الموفرة للحساب.

التوعية المستمرة بمبادئ المواطنة الرقمية

في دراسة استهدفت طلاب وطالبات الثانوية لدول الخليج العربي (٢٠١٨) أوضحت النتائج أن هناك تدنياً في مستوى الوعي بقيم المواطنة الرقمية حيث جاءت النتائج على النحو التالي:



المتوسط الحسابي والانحراف المعياري لعبارات الاستبيان لمدى الوعي بقيم المواطنة الرقمية

لو تأملنا مفهوم الأمن السيبراني ومفهوم المواطنة الرقمية لأدركنا أن هناك تداخلاً في المفهومين ولكن الحقيقة التي تظهر للمتمعن أن كلاهما مكمل للآخر فالمواطنة الرقمية التي تعني الحماية والتوجيه تتعلق بالشخص وتأهيله وإعداده وإمداده بالمباديء والقيم والأعراف والقوانين ليعرف حقوقه وواجباته حينما يتواجد في الفضاء الإلكتروني

فيكون مسؤولاً عن استخداماته الرقمية والأمن السيبراني هو مجموعة من التدابيروالاحتياطات يستدعي الشخص فيها مهارات المواطنة الرقمية ليحافظ على أمنه واستقراره ومقدرات بيئته ومجتمعه فالعلاقة بين المفهومين قوية ولاغنى لهما عن بعضهما وسنستعرض بعضاً من قيم المواطنة الرقمية لتتضح أمام القارئ من أهمها التالي:

١.الوصول الرقمي (Access Digital) : تكافؤ الفرص أمام جميع الألفراد فيما يتعلق بالوصول إلى التكنولوجيا واستخدامها.

٢.التجارة الرقمية (Commerce Digital) : بيع البضائع وشراؤها إلكترونيا والمواطنة الرقمية تثقف الفرد بالقضايا المتعلقة بهذه العملية من حيث القوانين واللوائح المتعلقة باستخدام التكنولوجيا، وبقوانين الدولة.

٣.الإتصالات الرقمية (Communication Digital) : التبادل الإلكتروني للمعلومات: و تهتم المواطنة الرقمية بأن يمتلك الفرد القدرة على اتخاذ القرار السليم أمام العديد من خيارات الاتصالات الرقمية المتاحة وأن يكون على وعي بكيفية استخدامه.

٤.محو الأمية الرقمية (Literacy Digital): عملية تعليم وتعلم

التكنولوجيا واستخدام أدواتها وهذا ماتسعى إليه رؤية ٢٠٣٠ والمواطنة الرقمية تقوم على تعليم وتثقيف الأفراد بأسلوب جديد – أخذاً في الاعتبار حاجة هؤلاء الأفراد إلى مستوى عالي جدا من مهارات محو الأمية المعلوماتية.

٥.اللياقة الرقمية (Etiquette Digital): و تهتم المواطنة الرقمية بنشر "ثقافة الإتيكيت" الرقمي بين الأفراد وتدريبهم ليكونوا مسؤولين في ظل مجتمع رقمي جديد، ليتصرفوا بتحضر، مراعين القيم والمبادئ ومعايير السلوك الحسن.

٦.القوانين الرقمية (Law Digital): المسؤولية الإجتماعية على الأعمال والأفعال: هي تلك القوانين في المجتمع الرقمي التي تعالج مسألة الأخلاقيات الرقمية، ومعاقبة الاستخدام غير الأخلاقي للتكنولوجيا أو ما يسمى الجرائم الرقمية.

٧.الحقوق والمسؤوليات الرقمية (Responsibilities & Rights Digital): الحريات التي يتمتع بها الجميع في العالم الرقمي: يتمتع

المواطن الرقمي بحزمة من الحقوق مثل الخصوصية ومشاركة الأعمال وإبداء الرأي والحرية تكون منضبطة حسب قوانين دينه ودولته.

٨.الصحة والسلامة الرقمية (Wellness & Health Digital): الصحة النفسية والبدنية في عالم التكنولوجيا الرقمية: فقد ظهر مايسمى بالهندسة الاجتماعية (فن اختراق البشر) والتي تعتمد على استغلال الحالة النفسية للإنسان والسيطرة عليه بمحفزات أساسية كالخوف والفضول والإثارة بالإضافة لصحة الجسم كمتاعب البصر والرقبة وغيره وهنا تلعب المواطنة الرقمية دوراً كبيراً في الحماية والنصح والتوجيه.

٩ - Security Digital self protection): إجراءات ضمان الوقاية والحماية الرقمية: وقد تناولنا في هذا الكتاب كيف يمكن تحقيقه لنوضح بذلك الترابط والتكامل بين المواطنة الرقمية والأمن السيبراني.

كلما كان مواطناً رقمياً كان آمناً سيبرانياً

التخطيط المستقبلي لريادة الأمن السيبراني لدى طلابنا

-استحداث قسم في وزارة التعليم مختصاً بالأمن السيبراني ويكون تحت إدارة مركز التوعية الفكرية وأمن الدولة يكون مشرفاً على التعليم العام والتعليم العالي.

-استقطاب المتميزين والخبراء والمختصين بالمجال لشغل وظائفه.

-استحداث دروس في الأمن السيبراني والمواطنة الرقمية لدى طلاب التعليم العام ملحقة بدروس الحاسب الآلي والتربية الوطنية والمهارات الحيوية والسنة التحضيرية لطلاب التعليم العالي.

-استهداف الأسر وأولياء الأمور والمعلمين والمعلمات وأعضاء هيئة التدريس بالجامعات من خلال التدريب عن بعد والتدريب المباشر والتدريب المدمج

-عقد الشراكات مع الدول المتقدمة في مجال الأمن السيبراني للاستفادة من تجاربهم.

-تحقيق التكامل بين القطاعات الحكومية والخاصة فيما يتعلق بالأمن السيبراني.

-عقد مسابقات لاكتشاف الثغرات الأمنية والوقاية منها.

-توعية الطلاب بسلوكيات المواطنة الرقمية في الفضاء السيبراني والتي تشمل :

أولاً: العناية التامة بالمعرف الشخصي وأن يكون حقيقياً

-عدم إبداء أي معلومات شخصية سرية هامة .

-حماية المعرف بكلمات مرور قوية

-التفكير جيداً قبل نشر الصور الشخصية أو إرسال نصوص أو ملفات صوت أو فيديو عبر الإنترنت.

-الاستئذان من صاحب الشأن قبل نشر صور الأخرين أو إرسال بريدهم الإلكتروني وأرقام جوالاتهم لشخص أخر على الإنترنت.

-عدم قبول أي رسائل مجهولة المصدر.

-عدم إضافة أخرين لقائمة الأصدقاء ما لم يكونوا معروفين شخصياً.

-عدم الإرسال في حالة الغضب.

-الإدراك أن عدم اتخاذ موقف حيال عمليات التعدي تعد نوعاً من التستر على المتعدي، لذا يجب المبادرة بإتخاذ إجراء مناسب أو إخبار من تثق بهم من الكبار

-الوعي بكيفية حظر وصول بعض الأشخاص إلى غرف الدردشة والإبلاغ عنهم، وكيفية حفظ أو طباعة نسخة من أي حوار، فقد يحتاج الوالدين الإبلاغ عنها.

-الوعي بحظر الرسائل العدائية أو استلام أي رسائل إلكترونية مزعجة من أشخاص آخرين.

- إدارك أن الحوارت عبر الإنترنت ليس ذات خصوصية، فقد يقوم أخرون

بنسخ هذه الحوارات وطباعتها واطلاع الأخرين على أي تعليقات، أو صور تقوم بنشرها

-تجنب الدخول إلى المواقع الإباحية.

-تجنب دخول مواقع التفحيط والمواقع الدينية المشبوهة والمواقع السياسية العدائية ومجهولة الهوية.

مواقع التواصل الاجتماعي

-عدم متابعة أي شخص حتى تعرف من هو وماهي توجهاته.

-الحذر من المعرفات المسيئة للدولة والدين قد تبدأ بأدعية ونصائح ثم إذا زاد عدد المتابعين تحولت لحسابات إرهابية أو تجسس.

-الحذر من المشاركة في هاشتقات وأوسمة مثيرة للجدل والإرجاف الديني والوطني.

-الحذر من تتبع الوصلات والروابط الدعائية فقد تكون محملة ببرامج ضارة.

-لا تحمل أي برنامج إلا من مصدر موثوق مثل أبل ستورأومتجر إندرويد.

-في حالة تعرضك للإساءة الاستعانة بأدوات الإبلاغ الموثوقة.

المراجع

- ابن تاج، لحمر. عباس. (2018). أخلاقيات الأعمال الإلكترونية وتحديات الأمن المعلوماتي في ظل الاقتصاد الرقمي. المجلة المصرية للدراسات القانونية والاقتصادية - مصر، ع10 ، 299 - 329.
- أبو نعارة، ياسمينة.(2016). الجريمة الإلكترونية متوفر على شبكة الإنترنت.
- أطروحة (ماجستير)-جامعة نايف العربية للعلوم الأمنية، كلية العدالة الجنائية، قسم الشريعة والقانون،
- أطروحة ماجستير، جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية، قسم الأمن الإنساني.
- جبور، منى الأشقر (2012). الأمن السيبراني: التحديات ومستلزمات المواجهة. اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، جامعة الدول العربية: المركز العربي للبحوث القضائية والقانونية، بيروت، أغسطس 27 – 28.
- الربيعة، صالح علي.(2018).الأمن القومي وحماية المستخدم من مخاطر الإنترنت ورقة عمل مقدمة في ملتقى تقنية المعلومات الأول بجدة يوم 10/8/1439هـ.
- الردفاني ، محمد قاسم. (2014). تحقيقات الشرطة في مواجهة تحديات الجرائم السيبرانية. المجلة العربية للدراسات الامنية والتدريب (السعودية)، مج30، ع61 ، 157 - 192.
- الشراري، حامد الوردة .(2017)."الفضاء السيبراني ساحة فضاء المستقبل"

متوفر على الانترنت تم استرجاعه بتاريخ 1439/11/1 .

•الصادق، حنان بيزان (2017). دراسات ورؤى معلوماتية في إدارة المعلومات والمعرفة. القاهرة: دار حميثرا للنشر والترجمة.

•العتيبي ،عبد الرحمن بجاد.(2017). دور الأمن السيبراني في تعزيز الأمن الإنساني.

•عشقي، أنور ماجد. (2016). الأمن السيبراني والقمة الخليجية الأمريكية. الأمن والحياة (جامعة نايف العربية للعلوم الأمنية) - السعودية، مج35، ع409، 146.

•الفضالة،أحمد الشيخ عبدالله.(2017). قراءة في كتاب الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، مجلة العلوم الأمنية-السعودية مج26،ع66، 252.

•المحمادي،عبدالله.(2018) .الأمن السيبراني متوفر على https://www.ghrannews.com/?p=111795

•المقصودي،محمد أحمد.(2017).الأمن السيبراني والجهود الدولية لمكافحة الجرائم عابرة القارات(جامعة نايف العربية للعلوم الأمنية) - السعودية، مج37، ع427، 107.

•المقصودي، محمد أحمد. (2017). الأمن السيبراني والجهود الدولية لمكافحة الجرائم عابرة القارات. الأمن والحياة - جامعة نايف العربية للعلوم الأمنية - السعودية، مج37، ع427، 102 - 107.

•الملاح،تامر المغاوري (2017). المواطنة الرقمية آمال وتحديات .دار السحاب

•الهزاني، محمد ناصر.(2018) المسؤولية الجنائية عن انتهاك قواعد الفضاء السيبراني : دراسة تأصيلية مقارنة بالقانون الإماراتي.

• https://www.itu.int/ar/about/Pages/default.aspx

• Canongia, C., & Mandarino, R. (2014). Cyber security the new challenge of the information society. In Crisis Management: Concepts, Methodologies, tools and applications: 60-80. Hershey, PA: IGI Global.

• Craigen, D., Diakun, N. & Purse, R. (2014). Defining Cyber security.Technology Innovation Management Review, Carleton University, October, pp. 13-22.

• http://professional.mit.edu/programs/short-programs/applied-cybersecurity

• http://www.al-jazirah.com/2017/20171116/ar8.htm

• http://www.citc.gov.sa/ar/Pages/default.aspx/

• http://www.cybersafe.my/en/

• http://www.univ-emir.dz/download/madjala-oussoul/39bounarayasmina.pdf 20/10/2018

• https://cert.gov.om/contact_oir_arabic.aspx

• https://safcsp.org.sa

• https://www.acsri.org.au

• https://www.albayan.ae/across-the-uae/accidents/2018-03-02-1.3200109

• https://www.csa.gov.sg/

• https://www.nsa.gov/about/central-security-service

• https://www.tech-wd.com/wd/2015/03/04/internet-of-things/

• Van den Berg, J., Van Zoggel, J., Snels, M., Van Leeu-

الفهرس

wen, M., Boeke, S.,van de Koppen, L., ... & De Bos, T. (2014). On (the Emergence of)Cyber Security Science and its Challenges for Cyber Security Education. In The NATO IST-122 Cyber Security Science and Engineering Symposium.

• Von Solms, R., & Von Solms, S. (2015). Cyber safety education in developing countries Muller, L. P. (2015). Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities.

• www.itu.int/ar/pages/default.asp http://www.lborolondon.ac.uk/news-events/news/2018

رقم الإيداع : ١٤٤٠/٢٩٠٦

ردمك : ٩٧٨-٦٠٣-٠٠٢-٨٤٩٧-٩