المحور الثالث: الأمن ألمعلوماتي و السيبراني

تقديم: تعتمد المجتمعات الحديثة بشكل متنامي على تكنولوجيات الاتصالات والمعلومات المتصلة بالشبكة العالمية. غير أن هذا الاعتماد المطرد ترافقه مجموعة من المخاطر الناشئة والمحتملة التي تهدد وبشكل أساسي الشبكة وأمن المعلومات والمجتمع ألمعلوماتي وأعضائه. إن سوء الاستغلال المتنامي للشبكات الالكترونية لأهداف إجرامية يؤثر سلباً على سلامة البنى التحتية للمعلومات الوطنية الحساسة. لقد بات الأمن السيبراني يشكل جزءاً أساسياً من أي سياسة أمنية وطنية، حيث بات معلوماً أن صناع القرار في الولايات المتحدة الأمريكية، الاتحاد الأوروبي، روسيا، الصين، الهند وغيرها من الدول، أصبحوا يصنفون مسائل الدفاع السيبراني/الأمن السيبراني كأولوية في سياساتهم الدفاعية الوطنية. بالإضافة إلى ما تقدم، فقد أعلنت معظم الدول حول العالم عن تخصيص أقساماً وسيناريوهات خاصة بالحرب السيبرانية ضمن فرق الأمن الوطني. تضاف جميع هذه الجهود إلى الجهود الأمنية التقليدية لمحاربة الجرائم الالكترونية، الاحتيال الالكتروني والأوجه الأخرى للمخاطر السيبرانية.

السيبرانية:

تطلق كلمة سيبر Cyber على أي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي فالسيبرانية تعني فضاء الإنترنت.

مفهوم الأمن السيبراني

يقصد بالأمن السيبراني " Security Cyber " حماية الأشياء من خلال تكنولوجيا المعلومات مثل الأجهزة والبرمجيات ويشار إليها " ICT " وذلك اختصار and Information Communication Technologies .

والقول بالأمن السيبراني يعني اتخاذ التدابير اللازمة لحماية الفضاء السيبراني من الهجمات السيبرانية، وذلك من خلال مجموعة من الوسائل المستخدمة تقنياً وتنظيمياً وإداريًا في منع الوصول غي ر المشروع للمعلومات الإلكترونية ومنع استغلالها بطريقة غير قانونية ونظامية، وبذلك فإنه يهدف إلى الحفاظ على استمرارية الأنظمة والمعلومات المتوفرة بها، وحمايتها بكل خصوصية وسرية من خلال إتباع التدابير والإجراءات اللازمة لحماية البيانات.

الأمن السيبرانى لغوياً: الأمن السيبراني مكون من لفظتين: "الأمن" و "السيبراني" الأمن: هو نقيض الخوف، أي بمعنى السلامة، والأمن مصدر الفعل أَمِن أَمناً وأَماناً و أَمنَةً ، أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال أَمِن من الشر، أي سلِم منه . السيبراني: مصطلح السيبرانية الآن هو واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي، وكلمة" cyber" لفظة يونانية الأصل مشتقة من كلمة" kybernetes" بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازاً للمتحكم " gouverner".، و أشار بعض المؤرخين إلي أن أصلها يرجع إلى عالم الرياضيات الأمريكي (1964-1894) Wieners Norbert وذلك للتعبير عن التحكم الآلي.

الأمن السيبراني اصطلاحاً: هناك العديد من التعاريف التي قُدمت لمفهوم الأمن السيبراني، حيث يعرف بأنه عبارة عن مجموع من الإجراءات التقنية والإدارية تشمل العمليات والآليات التي يتم اتخاذها لمنع أي تدخل غير مقصود أو غير مصرح به بالتجسس أو الاختراق لاستخدام أو سوء الاستغلال للمعلومات والبيانات الإلكترونية الموجودة على نظم الاتصالات والمعلومات، كما تضمن تامين وحماية وسرية وخصوصية البيانات الشخصية للمواطنين، كما تشمل استمرارية عمل حماية معدات الحاسب الآلي ونظم المعلومات والاتصالات والخدمات من أي تغيير أو تلف.

وعليه فإن الأمن السيبراني يشكل مجموع الأطر القانونية و الهياكل التنظيمية ، بالإضافة إلى الوسائل التقنية والتكنولوجية والتي تمثل الجهود المشتركة للقطاعين الخاص والعام، المحلية والدولية والتي تهدف إلى حماية الفضاء السيبراني الوطني، مع التركيز على ضمان توافر أنظمة المعلومات وتتميز بالخصوصية وحماية سرية المعلومات الشخصية واتخاذ جميع الإجراءات الضرورية لحماية المواطنين من مخاطر الفضاء السيبراني.

أهداف الأمن السيبراني

1- تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحويه من بيانات.

2- التصدي لهجمات وحوادث امن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص.

3- توفير بيئة أمنة موثوقة للتعاملات في مجتمع المعلومات.

4- صمود البني التحتية الحساسة للهجمات الإلكترونية.

5- توفير المتطلبات الأزمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين.

6- التخلص من نقاط الضعف في أنظمة الحاسب الآلي والأجهزة المحمولة باختلاف أنواعها.

7- سد الثغرات في أنظمة امن المعلومات.

8- مقاومة البرمجيات الخبيثة، وما تستهدفه من أحداث أضرار بالغة بالمستخدمين.

9- الحد من التجسس والتخريب الإلكتروني على مستوى الحكومة والأفراد.

10- اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة.

11- تدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزتهم التقنية بقصد الضرر بمعلوماتهم الشخصية سواء بالإتلاف أو بقصد السرقة.

أهمية الأمن السيبراني:

في عالم اليوم المترابط بواسطة الشبكات ، يستفيد الجميع من برامج الدفاع السيبراني . وتتمثل أهمية الأمن السيبراني فيما يلي :

1- الحفاظ على المعلومات وسلامتها وتجانسها، وذلك بكف الأيادي من العبث بها.

2- تحقيق وفرة البيانات وجاهزيتها عند الحاجةِ إليها.

3- حماية الأجهزة والشبكات ككّل من الاختراقات لتكون درع واقٍ للبيانات والمعلومات.

4- استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها .

5- استخدام الأدوات الخاصة بالمصادر المفتوحة وتطويرها لتحقيِق مبادئ الأمن السيبراني.

6- توفير بيئة عمل آمنة جدا خلال العمل عبر الشبكة العنكبوتية.

أنواع الأمن السيبراني:

للأمن السيبراني أنواع مختلفة هي:

أمن الشبكات: (Network Security) وفيه يجري حماية أجهزة الحاسوب من الهجمات التي قد يتعرّض لها داخل الشبكة وخارجها، ومن أبرز التقنيات المُستخدمة لتطبيق أمن الشبكات جدار الحماية الذي يعمل واقيًا بين الجهاز الشخصي والأجهزة الأخرى في الشبكة، بالإضافة إلى أمن البريد الإلكتروني. أمن التطبيقات: (Application Security) وفيه يجري حماية المعلومات المتعلقة بتطبيق على جهاز الحاسوب، كإجراءات وضع كلمات المرور وعمليات المصادقة، وأسئلة الأمان التي تضمن هوية مستخدم التطبيق.

الأمن السحابي: (Cloud Security) تُعرف البرامج السحابية بأنّها برامج تخزين البيانات وحفظها عبر الإنترنت، ويلجأ الكثير إلى حفظ بياناتهم عبر البرامج الإلكترونية عوضًا عن برامج التخزين المحلية ممّا أدى إلى ظهور الحاجة إلى حماية تلك البيانات، فتعنى البرامج السحابية بتوفير الحماية اللازمة لمستخدميها.

الأمن التشغيلي: (Operational Security) وهو إدارة مخاطر عمليات الأمن السيبراني الداخلي، وفيه يوَظّف خبراء إدارة المخاطر لإيجاد خطة بديلة في حال تعرض بيانات المستخدمين لهجوم إلكتروني، ويشمل كذلك توعية الموظفين وتدريبهم على أفضل الممارسات لتجنب المخاطر.

عناصر الأمن السيبراني: حتى يتحقق الهدف من الأمن السيبراني، لا بد من توفر مجموعة من ا لعناصر مع بعضها البعض لتكمل الدور في ذلك، ومن أهم أبعاد وعناصر الأمن السيبراني:

1- التقنية technologie : تشكل التكنولوجيا والتقنية دوراً في غاية الأهمية في حياة الأفراد والمنظمات، حيث توفر الحماية الفائقة لهم أمام الهجمات السيبرانية، وتشتمل حماية الأجهزة بمختلف

أشكالها الذكية والحاسوبية والشبكات بالاعتماد على جدران الحماية واستخدام البرامج الضارة ومكافحة الفيروسات وغيرها.

2- الأشخاص People : يستوجب الأمر لزوماً على الأشخاص من مستخدمي البيانات والأنظمة في منشأة ما استخدام مبادئ حماية البيانات الرئيسية كتحديد كلمة مرور قوية، وتفادي فتح الروابط الخارجية والمرفقات عبر البريد الإلكتروني، إلى جانبِ القيام بعمل نسخ احتياطية للبيانات.

3- الأنشطة والعمليات Process : يتم توظيف الأشخاص والتقنيات للقيام بالعديد من العمليات والأنشطة وتسييرها بما يتماشى مع تطبيق أسس الأمن السيبراني والتصدي لهجماته بكل كفاءة.

أبعاد الأمن السيبراني

أولا: الأبعاد العسكرية:

تنشأ أهمية الأمن السيبراني في هذا البعد من خطورة الهجمات السيبرانية والاختراقات التي تؤدي إلى نشأة الحروب والصراعات المسلحة، واختراقات أنظمة المنشاة النووية، وما قد يحدث عنها من تهديدات لأمن الدول والحكومات ويؤدي إلى كوارث.

ثانيا: الأبعاد السياسية:

تقوم الأبعاد السياسية للأمن السيبراني على أساس حماية نظام الدولة السياسية وكيانها، حيث يمكن أن تستخدم التقنيات في بث معلومات وبيانات قد يحدث من خلالها زعزعة لاستقرار امن الدول والحكومات حيث تصل بسرعة فائقة إلى أكبر شرائح من المواطنين بغض النظر عن صحة البيانات والمعلومات التي يتم نشرها.

ثالثا: الأبعاد الاقتصادية:

يرتبط الأمن السيبراني ارتباطاً وثيقاً بالحفاظ على المصالح الاقتصادية لكل الدول، فالترابط وثيق بين الاقتصاد والمعرفة فاغلب الدول تعتمد في تعزيز اقتصادها وازدهاره على إنتاج وتداول المعرفة

والمعلومات على المستويات، مما يبرر الدور الخطير للأمن السيبراني في حماية الاقتصاد من السرقة والملكية الفكرية.

رابعا: الأبعاد القانونية:

ترتبط الأنشطة المختلفة التي يقوم بها الأفراد والمؤسسات بالقوانين، ومن ظهور المجتمع ألمعلوماتي ظهرت القوانين الجديدة التي تعد البيئة التنظيمية التشريعية المنظمة لحماية هذا المجتمع وحفظ الحقوق فيه بكافة ما يتضمن من أبعاد ويقوم الأمن السيبراني في هذا البعد على حماية المجتمع ألمعلوماتي ويساعده في تطبيق وتنفيذ هذه القوانين والتشريعات.

خامسا: الأبعاد الاجتماعية:

تسمح طبيعة الإنترنت المفتوحة عبر شبكات التواصل الاجتماعي لكل مواطن بأن يعبر عن أفكاره والاطلاع على مختلف المعلومات والانفتاح عبر جميع الثقافات المختلفة، وهنا يكمن أهمية الأمن السيبراني في حماية وصيانة القيم الجوهرية في المجتمع كالانتماء، المعتقدات الدينية، والعادات والتقاليد.

وفي هذا السياق تعمل المنظمات والهيئات على نشر ثقافة الأمن السيبراني وتطالب بضرورة تعاون كل أفراد المجتمع في تحقيقه للحد من مخاطر الهجمات والجرائم السيبرانية التي مما لا شك فيه تطول المجتمع ككل وتهدد أمنه واستقراره على هدم القيم وضياع الهوية الثقافية.

أنواع الجرائم السيبرانية

أولا: جرائم التعدي على البيانات المعلوماتية:

تشمل الجرائم التي يكون موضوعها البيانات المعلوماتية، أي التي تقع على بيانات معلوماتية، وهي جرائم التعرض للبيانات المعلوماتية، وجرائم اعتراض بيانات معلوماتية، والبيانات هي كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة الحاسب الآلي كالأرقام والحروف والرموز وما إليها.

ثانيا: جرائم التعدي على الأنظمة المعلوماتية:

تشمل جرائم الولوج غير المشرع إلى نظام معلوماتي أو المكوث فيه، مع التعرض للبيانات المعلوماتية وجرائم إعاقة عمل معلوماتي، ويتمثل النظام ألمعلوماتي في مجموعة البرامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات.

ثالثا: إساءة استعمال الأجهزة أو البرامج المعلوماتية:

تتضمن هذه الجرائم كل من قدم أو أنتج أو وزع أو حاز بغرض الاستخدام جهازا أو برنامجاً معلوماتي أو أي بيانات معلوماتية معدة أو كلمات سر أو كودات دخول، وذلك بغرض اقتراف أي من الجرائم المنصوص عليها سابقا.

ويتضمن البرنامج ألمعلوماتي مجموعة من التعليمات والأوامر القابلة للتنفيذ باستخدام الحاسب الآلي ومعدة لإنجاز مهمة ما، إما البرامج المعلوماتية هي الكيان المعنوي غير المادي من برامج ومعلومات وما إليها ليكون قادرا على القيام بوظيفة.

رابعا: الجرائم الواقعة على الأموال:

1- جرم الاحتيال أو الغش بوسيلة معلوماتية

2- جرم التزوير ألمعلوماتي

3- جرم الاختلاس أو سرقة أموال بوسيلة معلوماتية.

4- جرم أعمال التسويق والترويج غير المرغوب فيها.

5- جرم الاستيلاء على أدوات التعريف والهوية المستخدمة في نظام معلوماتي والاستخدام غير المشرع لها.

6- جرم الاطلاع على معلومات سرية أو حساسة أو إفشائها.

خامسا: جرائم الاستغلال الجنسي للقاصرين:

تظهرها الأفعال التي تتعلق باستغلال القاصرين في أعمال جنسية، وتشمل:

1- الرسومات أو الصور أو الكتابات أو الأفلام.

2- أعمال إباحية يشارك فيها القاصرون.

3- تتعلق باستغلال القاصرين في المواد الإباحية.

4- إنتاج مواد إباحية للقاصرين بقصد بثها بواسطة نظام معلوماتي.

سادسا: جرائم التعدي على الملكية الفكرية للأعمال الرقمية:

تشمل جرام 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.

سابعا: جرائم البطاقات المصرفية والنقود الإلكترونية:

تشمل أعمال تقليد بطاقات مصرفية بصورة غير مشروعة واستعمالها عن قصد، وتزوير إلكترونية بصورة غير مشروعة عن قصد، لما لذلك من إخلال بالاقتصاد الوطني وتأثير سلبي على العمليات المصرفية.

ثامنا: الجرائم التي تمس المعلومات الشخصية:

تتضمن الأفعال الجرمية التي تتعلق بمعالجة البيانات ذات الطابع الشخصي دون حيازة تصريح أو ترخيص مسبق يتيح القيام بالمعالجة، وإنشاء معلومات ذات طابع شخصي لأشخاص لا يحق لهم الاطلاع عليها.

تاسعا: جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية:

1- جرم نشر وتوزيع المعلومات العنصرية بوسائل معلوماتية.

2- جرم تهديد أشخاص أو التعدي عليهم بسبب انتهائهم العرقي أو المذهبي أو لونهم وذلك بوسائل معلوماتية.

3- جرم توزيع معلومات بوسيلة إلكترونية من شانها إنكار أو تشويه أو تبرير أعمال إبادة جماعية أو جرائم ضد الإنسانية.

4- جرم المساعدة أو التحريض بوسيلة إلكترونية على ارتكاب جرائم ضد الإنسانية.

عاشرا: جرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية عبر الإنترنت:

تشمل جرم تملك وإدارة مشروع مقامرة، وجرم تسهيل وتشجيع مشروع مقامرة، وجرم ترويج الكحول للقاصرين، وجرم ترويج المواد المخدرة.

الحادي عشر: الجرائم المعلوماتية ضد الدولة والسلامة العامة:

تتضمن الأفعال الجرمية الناشئة عن المعلوماتية التي تطال الدولة وسلامتها وأمنها واستقرارها ونظامها القانوني، وهي:

1- جرائم تعطيل الأعمال الحكومية أو أعمال السلطة العامة باستعمال وسيلة معلوماتية.

2- جرائم الإخفاق في الإبلاغ أو الإبلاغ عن قصد بشكل خاطئ عن جرائم المعلوماتية، والاطلاع أو الحصول على معلومات سرية تخص الدولة.

وذلك من خلال شبكة الإنترنت أو باستعمال وسيلة معلوماتية، بالإضافة إلى فعل العبث بالأدلة القضائية المعلوماتية أو إتلافها أو إخفائها، والأعمال الإرهابية التي ترتكب باستخدام شبكة الإنترنت أو أي وسيلة معلوماتية، وجرائم التحريض على القتل عبر الإنترنت أو أيه وسيلة معلوماتية.

الثاني عشر: جرائم تشفير المعلومات:

تشمل أفعال تسويق أو توزيع أو تصدير أو استيراد وسائل تشفير، بالإضافة إلى أفعال تقديم وسائل تشفير تؤمن السرية دون حيازة تصريح أو ترخيص من قبل المراجع الرسمية المختصة في الدولة، وأيضاً بيع أو تسويق أو تأجير وسائل تشفير ممنوعة.

أسباب الجرائم السيبرانية:

1- الرغبة في جمع المعلومات وتعلمها.

2- الاستيلاء على المعلومات والاتجار فيها.

3- قهر النظام وإثبات التفوق على تطور وسائل التقنية.

4- إلحاق الأذى بأشخاص أو جهات.

5- تحقيق أرباح ومكاسب مادية.

6- تهديد الأمن القومي والعسكري.

آليات (متطلبات) تحقيق الأمن السيبراني:

قد تساعدك الخطوات البسيطة أدناه في الحفاظ على مستوى جيد من الأمان والسلامة السيبرانية :

1- الموثوقية: وتعني استخدام المواقع الموثوق بها عند تقديم معلومات شخصية، والقاعدة الأساسية هي التحقق من عنوان URL.، وإذا كان الموقع يتضمن https في بدايته، فهذا يعني أنه موقع آمن، أما إذا كان عنوان URL يحتوي على http بدون s؛ فيجنّب الحذر من إدخال أي معلومات حساسة مثل بيانات بطاقة الائتمان، أو رقم التأمين الاجتماعي.....الخ.

2- البريد الاحتيالي : ويعني عدم مرفقات البريد الإلكتروني أو النقر فوق روابط الرسائل من المصادر غير المعروفة، إذ إن إحدى الطرق الأكثر شيوعاً التي يتعرض فيها الأشخاص للسرقة أو الاختراق هي عبر رسائل البريد الإلكتروني المتخفية على أنها مرسلة من شخص موثوق به.

3- التحديثات Always up-to-date وتعني الحرص دائما على تحديث الأجهزة ، فغالباً ما تحتوي تحديثات البرامج على تصحيحات مهمة لإصلاح مشكلات الأمان، وإن هجمات المخترقين الناجحة تتركز على الأجهزة القديمة بنسبة كبرى، والتي لا تملك أحدث برامج الأمان.

4- النسخ الاحتياطي: ويتطلب هذا عمل نسخ احتياطية من الملفات بانتظام لمنع هجمات الأمان على الإنترنت.

نصائح وإرشادات لمكافحة الجرائم السيبرانية:

قد تساعدك الخطوات البسيطة أدناه في الحفاظ على مستوى جيد من الأمان والسلامة السيبرانية:

1- توعية الأفراد بأهمية الأمن السيبراني وتزويدهم بالإرشادات والنصائح اللازمة لإتباعها.

2- تدريب أفرادها على التعامل مع المخاطر الإلكترونية قدر الإمكان.

3- التدريب على تفادي الأخطاء ومساعدة أفرادها في الحد من المخاطر الناجمة من اختراق أجهزة وشبكات الحاسب، والتي ترجع لعدم وعيهم بطرق وأساليب الوقاية والحماية.

4- إعطاء النصائح التي تساهم في تنمية الوعي بالأمن السيبراني لتحقيق درجة عالية من الأمان والحماية في عالم رقمي سهل الاختراق.

5- العمل على تحقيق الأمن السيبراني وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية.

6- حماية المصلحة العامة والآداب والأخلاق العامة، والاقتصاد الوطني أيضاً.

7- تقتضي الضرورة سن تشريعات تغطي كافة الثغرات القانونية في مجال وجود فضاء سيبراني آمن، بالاستعانة بالإرشادات الخاصة بالمنظمات المختصة قصد تطوير البنية التشريعية الجنائية الوطنية بذكاء تشريعي مماثل تعكس فيه الدقة الواجبة على المستوى القانوني وسائر جوانب وأبعاد تلك التقنيات الجديدة.

8- ينبغي تعديل قواعد الإجراءات الجزائية لتتلاءم مع تلك الجرائم السيبرانية، وأيضاً ضرورة التنسيق والتعاون الدولي أمنياً وإجرائياً وقضائياً في مجال مكافحتها ببيان الأحكام اللازم إتباعها حال التفتيش على الحاسبات وعند ضبط المعلومات التي تحتويها وضبط البريد الإلكتروني حتى يستمد الدليل مشروعيته.

9- ضرورة تخصيص شرطة متمكنة علميا وعمليا وفنيا لمواجهة تحديات مكافحتها، وذلك من رجال الشرطة المدربين على كيفية التعامل مع أجهزة الحاسوب والإنترنت وكذلك النيابة العامة والقضاة يتعين تدريبهم وتحديثهم في هذا المجال السيبراني.

10- إعطاء الوقت الكافي للتحقيق والملاحقة القضائية من قبل شرطة متخصصة مزودة بآليات تقنية وتنظيمية.

11- ينبغي أن يسمح للسلطات القائمة بالضبط والتحقيق، بضبط البريد الإلكتروني، وأي تقنية أخرى قد تفيد في إثبات الجريمة والحصول على دليل، والكشف عن الحقيقة.