المحاضرة الأولى–الإطار المفاهيمي للأمن السيبراني:

الأمن السيبراني –ويسمى أيضا أمن الكمبيوتر–وسيلة لحماية البرمجيات وأجهزة الحاسوب والشبكات، وهو مجموعة من الإجراءات المتخذة لمواجهة الهجمات والاختراقات السيبرانية وما ينتج عنها من أخطار. ظهر مع بداية الحرب الباردة وتطور مع ثورة الإنترنت وأنظمة الحاسوب، وصار وسيلة أمنية وحربية دولية أساسية.

ويشكل الهجوم السيبراني خطرا أمنيا على الأفراد والمؤسسات والدول، فقد يستعمل لسرقة البيانات والاحتيال والوصول غير القانوني إلى بيانات مالية أو طبية أو عسكرية أو أمنية سرية، أو حتى التلاعب في أنظمة أجهزة إلكترونية عن بعد وتوجيهها بأهداف سياسية بقصد التسبب بضرر مادي، كتفجير أجهزة عن بعد أو تعطيل أنظمة.

ويهدف الأمن السيبراني إلى حماية 5 أنواع من المعدات والأنظمة الأساسية، هي أمن البنية التحتية (الاتصالات والنقل والطاقة وغيرها) وأمن الشبكات وأمن السحابة وأمن إنترنت الأشياء (الأجهزة الذكية المرتبطة بالإنترنت) وأمن التطبيقات.

أولا–تعريف الأمن السيبراني:

الأمن السيبراني مفهوم معقد يحمل الكثير من المعاني والتعريفات، ورغم اختلافها فإنها تتفق على وظيفته العامة تقريبا.

وحسب الاتحاد الدولي للاتصالات فالأمن السيبراني هو "مجموعة من الأدوات والسياسات والمفاهيم الأمنية والتحفظات الأمنية والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب، وغيرها من الممارسات وآليات الضمان والتكنولوجيات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المؤسسات والمستعملين من المخاطر الأمنية ذات الصلة في البيئة السيبرانية."

وتعرفه وكالة الأمن السيبراني وأمن البنية التحتية الأميركية (سي آي إس إيه) بأنه "فن حماية الشبكات والأجهزة والبيانات من الوصول غير المصرح به أو الاستخدام الإجرامي، ويمثل ممارسة ضمان سرية المعلومات وسلامتها وتوافرها."

وتعرفه الموسوعة البريطانية بأنه "حماية نظم الحوسبة والمعلومات من الأضرار والسرقة والاستخدام غير المصرح به."

وتعرفه شركة "كاسبر سكاي" الدولية الخاصة للأمن السيبراني بأنه "أشكال الدفاع عن الحواسيب والخوادم والأجهزة المحمولة والأنظمة الإلكترونية والشبكات والبيانات من الهجمات الخبيثة، ويعرف أيضا بأمن تكنولوجيا المعلومات أو الأمن الإلكتروني للمعلومات."

يعرف الأمن السيبراني حسب الهيئة الوطنية للأمن السيبراني (الهيئة الوطنية للأمن السيبراني، 2022) بأنه "تأمين كل الفضاء السيبراني الموجود والمترابط شبكيا من البنية التحتية لتقنية المعلومات، التي تشمل الانترنت وشبكات الاتصالات، وأنظمة الحاسب الآلي والأجهزة المتصلة بالانترنت، إلى جانب المعالجات وأجهزة التحكم المرتبطة بها"، كما أنه يعني(هيئة الاتصالات وتقنية المعلومات، (2020) بأنه "حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة، عتاد وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع، ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي".

أما المعهد الوطني للمعايير والتكنولوجيا فعرفه بأنه: "حماية أنظمة الحاسب وأنظمة الاتصالات الإلكترونية وخدمات الاتصالات الإلكترونية والاتصالات السلكية والاتصالات الإلكترونية، بما في ذلك المعلومات الواردة فيها؛ واستعادتها لضمان توافرها وسلامتها والمصادقة والسرية وعدم الانتهاك"، في حين أكد إدوارد أمورسو بأن: الأمن السيبراني يضم مجموع الوسائل التي من شأنها الحد من أخطر الهجومات على البرمجيات أو أجهزة الحاسوب أو الشبكات،" فهو يبدأ بـ "الاحساس الفعلي والتخيلي بعدم وجود و/أو تأثير التهديدات الفيزيقية والتخيلية لبنى المجتمع المعلوماتي(خاصة الحساسة منها) في جوانبها العسكرية، والاجتماعية، والثقافية، والاقتصادية...إلخ، المختلفة أيا كان مصدرها داخلي، أو خارجي، وتستدعي التأهب و/أو الفعل الاجتماعي و/أو التأهب والفعل الرسمي لمواجهتها."

بالنسبة للمشرع الجزائري :الامن السيبراني يمثل مجموع الوسائل التقنية والتنظيمية والادارية التي يتم استخدامها لمنع الاستخدام الغير مصرح به و سوء الاستغلال واستعادة المعلومات الالكترونية ونظم

الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني.

مما سبق يتضح أن الأمن السيبراني، يتعلق في الأساس بحماية وتأمين مختلف الممارسات السيبرانية من مختلف التهديدات والمخاطر الممكنة والمحتملة والتي تمس فضاء صناعة وتداول المحتوى الرقمي بما يضمه وتداول المحتوى الرقمي بما يضمه هذا الفضاء الرحب من اليات ووسائل فاعلة ومتفاعلة في عملية نقل وحفظ وتخزين ومعالجة المعلومات والبيانات الرقمية، وتقع الأنظمة الحاسوبية وبرامج المعالجة ضمن أهم الحلقات المتصلة بتأمين المعلومة الرقمية.

ويتعلق الأمن السيبراني بالحفاظ على حقوق وواجبات الاستخدام للمعلومة إذ يحفظها لأصحابها مع منع ومحاربة أي استخدام غير مصرح به، وغير مشروع، غير قانوني وعليه، فالأمن السيبراني عملية دفاعية وقائية تستهدف الاحاطة الأمنية التامة والشاملة للمعلومات والبيانات منكل استخدام غير به بما يقتضيه ذلك من صد للهجمات والجرائم الإلكترونية .

ثانيا–بداية ظهوره:

ظهر الأمن السيراني مع نهاية الحرب الباردة، وظهور مصطلح حرب الإنترنت أو الحرب السيبرانية، التي جاءت مع بداية اعتماد الدول على أجهزة الكمبيوتر في مؤسساتها وتطوير وحدة المعالجة المركزية في هذه الأجهزة، التي دخلت في عمل المؤسسات والحكومات وحتى في الحياة اليومية، واقتصر دور الأمن السيبراني في الفترة الأولى على الحماية من الفيروسات والبرمجيات الخبيثة.

وظهر أول فيروس رقمي في سبعينيات القرن العشرين على شبكة "أربانت"، إحدى أوائل الشبكات في العالم لنقل البيانات باستخدام تقنية تبديل الرزم، وكان على شكل رسالة نصية بسيطة لم تتسبب بأضرار تقنية لكنها دفعت إلى اتخاذ تدابير وقائية.

وفي عام 1983، طوّر معهد ماساتشوستس للتقنية نظام اتصالات يعتمد على التشفير، أصبح أساسا لتطوير تقنيات الأمن السيبراني الحديثة.

وشكل ظهور الإنترنت ثورة نوعية في حياة البشرية، إذ بدأ استخدامه في المجالين الأمني والعسكري وتسابقت الدول في تطويره مع مطلع تسعينيات القرن العشرين، حتى سميت تلك الفترة بـ"الحرب

السيبرانية الباردة" أو "سباق التسلح السيبراني"، وظهرت حينئذ هجمات التصيد الاحتيالية "فيشينغ" والتجسس الإلكتروني و"الهجوم الموزع لحجب الخدمة" (دي دي أو إس).

وظهرت الحاجة دوليا إلى وجود قوة غير مادية إلى جانب القدرات العسكرية والاقتصادية، فبدأت الدول تولي اهتمامها بالقوة السيبرانية لتأثيرها على المستويين المحلي والدولي. ومع انفجار الثورة المعلوماتية ودخول العصر الرقمي، واعتبار عدد من الباحثين الفضاء السيبراني بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء، ظهرت الحاجة لتوفير ضمانات أمنية، خاصة مع بداية ظهور التهديدات والجرائم السيبرانية مع دخول القرن الـ21.

ودخل الأمن السيبراني ضمن حقل الدراسات الأمنية، وظهرت تقنيات متطورة مثل التشفير والأمان السحابي والكشف عن التهديدات بالذكاء الاصطناعي، ومع ذلك فإن الهجمات السيبرانية مجال معقد وسريع التطور، مما يستلزم استجابات أمنية سريعة تضاهي وتيرة نموه السريع.

ثالثا–مكونات الأمن السيبراني وعناصره التركيبية:

يشترط لتحقيق الأمن السيبراني وجود ثلاثة مركبات أساسية وهي:

1. **الأدوات التقنية المستخدمة:**

تسمى أيضا بالبنية التحتية لأنظمة المعلومات ويتضمن ذلك الإنترنت وشبكات الاتصالات وانظمة الحاسب والمعالجات المدمجة.

2. **الإجراءات:**

يندرج فيها كل الاجراءات التقنية والمادية والقانونية لتوفير هذه الحماية والأمن.

3. **العامل البشري من مبرمجين ومستخدمين:**

يضم كل الكفاءات والكوادر المكونة والمختصة في مجال الاعلام الآلي والذكاء الصناعي والتقني والالكتروني، من مهندسين وتقنيين سامين...الخ.

وهناك من يقول أن مكوناته تتمثل فيما يلي:

1– **أمن الشبكات:** حماية البيئة التحتية للشبكة من التسلسل والهجمات.

2– **أمن المعلومات:** ضمان سرية وسلامة وتوافر المعلومات.

3- **أمن التطبيقات:** تامين البرامج والتطبيقات من الثغرات البرمجية.

4- **أمن الأجهزة الطرفية:** حماية أجهزة المستخدمين مثل الحواسيب والهواتف.

5- **الأمن السحابي:** حماية البيانات المخزنة في بيئات الحوسبة السحابية.

6- **التوعية والتدريب:** تثقيف المستخدمين حول المخاطر وأساليب الحماية.

ثالثا-كيف يعمل الأمن السيبراني:

تعتمد المؤسسات على متخصصي الأمن السيبراني لتنفيذ إستراتيجيات الحماية. ويقيم هؤلاء الخبراء المخاطر الأمنية التي قد تواجه أنظمة الحوسبة والشبكات ومخازن البيانات والتطبيقات والأجهزة المتصلة. ثم يضعون إطارا شاملا للأمن السيبراني ويطبقون تدابير الحماية اللازمة داخل المؤسسة.

وتحرص المؤسسات على توعية الموظفين بأفضل الممارسات الأمنية، وتفعيل تقنيات الدفاع الآلي في البنية التحتية لتكنولوجيا المعلومات. بهدف تشكيل طبقات من الحماية ضد التهديدات المحتملة، مما يساعدها في تحديد المخاطر المتوقعة، وحماية الهويات والبيانات والبنية التحتية، ومراقبة الأعطال ورصدها، والاستجابة السريعة وتحليل أسبابها، والأهم التعافي بعد وقوع الهجمات.

وتعتمد مؤسسات الأمن السيبراني عدة مبادئ أساسية في عملها، الأول مبدأ "انعدام الثقة"، الذي يتطلب مصادقة صارمة ومراقبة مستمرة لجميع المستخدمين والتطبيقات. الثاني تحليلات السلوك لمراقبة الأنشطة غير المعتادة في نقل البيانات والتنبيه بشأنها.

كما تعتمد المؤسسات على أنظمة كشف التسلل لتحديد الهجمات بسرعة باستخدام تعلم الآلة. إضافة إلى التشفير السحابي لحماية البيانات المخزنة عبر تشفيرها، باستخدام خدمات للتحكم في مفاتيح التشفير.