

الأمن السيبراني: المدلول و الماهية Cybersecurity: Meaning and essence

¹ علي بن طراز، مديرية الخدمات الجامعية قالمة.

تاريخ الاستلام: 2024/10/09 تاريخ القبول: 2024/10/27 تاريخ النشر: 2024/11/22

ملخص:

بعد أن أصبح الأمن السيبراني في الوقت الحالي من أهم مقومات الأمن في الدول المتحضرة، خاصة مع ما يعيشه العالم اليوم من تحول كامل نحو السيبرانية في كافة جوانب الحياة، تأتي هذه الورقة البحثية بغرض إلقاء الضوء على مفهوم الأمن السيبراني مُحاولَةً الكشف عن أهم مُحَدِّداته و أهم أبعاده في ظل التغيرات التي أحدثها التَّحول الرِّقَقي في العالم، حيث تناولت الورقة تحديد مفهوم الأمن السيبراني مع التعرُّض إلى بعض المفاهيم المُرتبطة به كمدخل مفاهيمي للبحث، لتُعرِّج إلى التعرُّف على السِّياق العام لظهوره وكذا تحديد أهميته و خصائصه و أهم تقنياته و أبعاده، كما تناولت أيضًا التعرُّض إلى مدلول السيبرانية بين مفهومي الأمن و القوة، حيث تم تناول ما يُعرف بالتهديد السيبراني و كذا الحروب السيبرانية.

الكلمات المفتاحية: الأمن، السيبرانية، الأمن السيبراني.

Abstract:

After Cybersecurity has become at the present time one of the most important elements of security in civilized countries, especially with what the world is experiencing today of a complete transformation towards Cybersecurity in all aspects of life, this research paper comes with the aim of shedding light on the concept of Cybersecurity in an attempt to reveal its most important determinants and most important dimensions in light of the changes brought about by digital transformation in the world, where the paper dealt with defining the concept of Cybersecurity with exposure to some of the concepts associated with it as a conceptual approach to

research, To identify the general context of its emergence as well as determine its importance, characteristics, most important techniques and dimensions, and also dealt with exposure to the meaning of cyber between the concepts of security and force, where what is known as cyber threat and cyber wars were addressed.

Keywords: Security, Cyber, Cybersecurity.

مقدمة:

يلعب الأمن السيبراني دورًا مهمًا في مجال تكنولوجيا المعلومات، حيث أصبح تأمين المعلومات أحد أكبر التحديات في العصر الحديث، فعندما نفكر فيما تعلق بالأمن السيبراني فإن أول ما يتبادر إلى أذهاننا هو الجرائم الإلكترونية التي تتزايد بشكل كبير يومًا بعد يوم، وهو الأمر الذي جعل العديد من حكومات الدول والشركات تتخذ تدابير وإجراءات عدة لمنع ولحد من هذه التهديدات والجرائم التي أصبحت تُشكل مصدر قلق كبير للكثيرين.

و من هنا، توجب طرح التساؤلات التالية: ما المقصود بالأمن السيبراني ؟ و ما هي محدّداته وماهي أبعاده ؟

1. تحديد المفاهيم

تُساعد عملية تحديد المفاهيم على ضبط التصور الخاص بالبحث، حيث تُعتبر كأحد أهم الخطوات الضرورية التي يجب اتباعها في أي بحث علمي، وقد تناولت هذه الورقة لمجموعة من المفاهيم التي نستعرضها فيما يلي:

1.1 - مفهوم الأمن:

الأمن في اللغة: يذكر لسان العرب الأمن من الأمان والأمانة بمعنى: وقد أمنتُ فأنا آمن، وأمنتُ غيري من الأمن والأمان، والإيمان: بمعنى التصديق و ضده التّكذيب. يُقال: أَمَنَ به قومٌ وكذّب به قوم، فأما أَمَنْتُهُ المتعدي فهو ضد أَحَقَّتُهُ. وفي التنزيل العزيز: وَأَمَّهْمُ من خوف. (منظور، صفحة 64)

و يُعدّ مفهوم الأمن من المفاهيم اللغوية ذات الثراء في المعنى، و فيما يلي بيانٌ موجزٌ لذلك، الأمن هو التصديق، فأصل الإيمان التصديق وهو مصدر آمن يؤمن إيمانًا، فهو مؤمن.

و الأمن هو الحفظ، فقد قيل إنّ الأمانة، و هي جمع أمين و هم الحفظة، و المفرد الحافظ، و أصل الحفظ الخوف من الضياع، و المأمون هو من يتولى رقابة الشيء والحفاظ عليه.

و الأمن هو الطمأنينة، فالرجل الأمّنة هو من يطمئن إلى كل واحد و يثق بكل أحد. (منجود، 1996، صفحة 30)

و قد ورد في الاصطلاح، أن الأمن حالة شعورية، إذ لا قيمة له إن لم يُوجد الإحساس به، ويتولّد الشعور بأن ثمة فارقاً بينه وبين الشعور بالخوف. (منجود، 1996، صفحة 45)

2.1 - مفهوم السيبرانية:

كلمة "cyber" هي كلمة من أصل يوناني، وهي اشتقاق من لفظ "kybernetes" بمعنى الشخص الذي يُدير دفة السفينة، و هي تعبير مجازي عن الشخص المُتحكّم "governo"، و يُعد مصطلح السيبرانية أحد أكثر المصطلحات تردّدًا في مُعجم الأمن الدولي. (قره، الأمن السيبراني Cyber Security - ، 2019)

و نعي بالفضاء السيبراني أنه وسيط إلكتروني يُستخدم بغرض تسهيل العملية الاتصالية من خلال شبكة الأنترنت، حيث يتضمن شبكة كبيرة من الحواسيب تتكون بدورها من شبكات فرعية أخرى من الحواسيب في العديد من أقطار العالم، و التي تعمل على استخدام البروتوكول المعروف ب TCP / IP بغرض المساهمة و الزيادة في الأنشطة الاتصالية و تبادل المعلومات، حيث أن ما يُميز الفضاء السيبراني كونه بيئة افتراضية و تفاعلية للعديد من المشاركين.

و في قاموس تكنولوجيا المعلومات، يُمكن اعتبار أي نظام يحتوي على قاعدة مُستخدمين كبيرة أو حتى واجهة جيّدة التصميم بمثابة "فضاء سيبراني" (Rouse, 2023).

1.3 - مفهوم الأمن السيبراني:

و هو مجموعة الآليات و الإجراءات و الوسائل و الأطر التي تهدف إلى حماية البرمجيات و أجهزة الكمبيوتر (الفضاء الإلكتروني "السيبراني" بصفة عامة) من مُختلف الهجمات و الاختراقات (التهديدات الإلكترونية) التي قد تُهدد الأمن القومي للدول. (المعجم الإلكتروني للمعاني)

و تُعرّفه الوكالة الوطنية لأمن نظم المعلومات (الفرنسية ANSSI) بأنه حالة نظام المعلومات الذي يُقاوم الهجمات الإلكترونية و الخوض العرّضي الذي يحدث في الفضاء الإلكتروني، و يتم ضمان الأمن السيبراني من خلال الحماية الإلكترونية، و في حالة الدولة عن طريق الدفاع الإلكتروني.

(Glossaire, 2022).

و من التعاريف الاصطلاحية لمفهوم الأمن السيبراني، ماعرّفه به إدوارد أمورسو Amoroso Edward بأنه : " وسائل من شأنها الحدّ من خطر الهُجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، و تشمل تلك الوسائل الأدوات المستخدمة في مُواجهة القرصنة و كشف الفيروسات و وقفها، و توفير الاتصالات المُشفّرة ". (قره، 2019)

2. الأمن السيبراني ما بين المصطلح و الماهية

يواجه عالم اليوم العدد الكبير من التهديدات الأمنية التي تتميز بتغيُّرها و سرعة تطورها، وكذا اتساع نطاق تأثيرها بحيث لا يقتصر على الإضرار بأمن فواعل بعينها، وإنما يمتد ليؤثر في الأمن العالمي بشكل عام، ولعل أبرز هذه التهديدات و أكثرها حداثة و أوسعها انتشارًا هي ما عُرف بالتهديدات الإلكترونية Cyber threats، حيث بات من الصعب حصرها في نطاق مُعَيَّن أو تطوير استراتيجيات مُحكمة لمواجهتها بشكل كامل، خاصة مع تعدُّد أشكالها و مصادرها، و تطورها المتسارع والمستمر.

فكما كان للأنترنت و وسائل التكنولوجيا الحديثة دورٌ كبيرٌ في تحقيق تقدم الدول و التواصل ما بين الشعوب و تطور عدد هائل من المجالات، فقد أصبح الفضاء الإلكتروني مساحة جديدة تُمارس فيها الأنشطة الإنسانية المختلفة، سواء على مستوى الأفراد أم الدول، و نجد أن هذه التطورات على صعيد آخر قد أدت إلى ظهور تهديدات أمنية جديدة لا تقل خطورة عن التهديدات الأمنية التقليدية، ولذا باتت مُواجهة هذه التهديدات على قمة أولويات السياسات الأمنية للدول و المنظمات الدولية، و خاصة مع توقع إمكانية حدوث طفرة في التطورات التكنولوجية في السنوات القادمة، لتتعاظم معها خطورة هذه التهديدات. (شفيق، 2020)

1.2 - المفاهيم المرتبطة بالأمن السيبراني

إن مصطلح الأمن السيبراني حسب مُسرد اليونسكو UNESCO لمُصطلحات إدارة الأنترنت، مُصطلح واسع المجال في العديد من القضايا، وهذا بدءًا من أمن تكنولوجيا المعلومات و مُرورًا بأمن المعلومات أو المحتويات، و وُصولًا إلى التدابير الأمنية التي ترمي إلى الحد من سوء الاستخدام الأمثل للأنترنت و ما تبعها من جرائم إلكترونية. (مُسرد مصطلحات إدارة الإنترنت، 2024)

و جاء في تعريف آخر، أن الأمن السيبراني هو أمن الشبكات و الأنظمة المعلوماتية و البيانات و المعلومات و الأجهزة المتصلة بشبكة الأنترنت، و بالتالي، فهو المجال الذي يتعلق باتخاذ تدابير و إجراءات و معايير للحماية الواجب اتخاذها أو الالتزام بها لمُجابهة التهديدات و الحد من التعديّات و من أثارها في أسوأ الأحوال.

وجدير بالذكر، أن الحديث عن الأمن يستدعي التعريف بالخطر، أي التهديد الذي يتعرض له النظام، إضافة إلى نقاط الضعف أو الثغرات التي من الممكن أن تعتره، و من ثَم وجب الحرص على تفعيل الإجراءات المفروض اتخاذها لدفع الخطر، فالخطر يتناول أمن الشبكات و أمن الأنترنت من ناحيتين، أولاهما، البنية التحتية و ما عليها من نقاط دخول و خُروج و تخزين و اعتراض للمعلومات، وثانيهما، عمليات التخريب و التدمير و التعطيل التي تطلُّها و تَطالُ الأموال و الأشخاص من خلالها.

وقد عرّف الاتحاد الدولي للاتصالات* في تقرير له (تقرير حول اتجاهات الإصلاح في الاتصالات للعام 2010-2011) أن الأمن السيبراني هو " مجموعة من المهّمات و التقنيات التي من الممكن العمل عليها بغرض حماية البيئة السيبرانية وكذا المؤسسات والمستخدمين".

و الهدف هنا من الحماية هو جعل المعتدين يُحجمون عن خُطّطهم، أو إلى منعهم من تحقيقها و إلى ضمان حدٍ مقبول من الخسائر والأضرار، وذلك عبر وضع خارطة أمن تتلاءم مع المحيط العام، التقني، البشري، التنظيمي والقانوني. (جبور، الصفحات 25-26)

و حتى تتّضح الرؤية أكثر، هناك العديد من المفاهيم المرتبطة بالأمن السيبراني، والتي يُمكن أن نذكر منها:

- الفضاء السيبراني: وقد عرّفته الوكالة الفرنسية لأمن أنظمة الإعلام ANSSI ، و هي وكالة حكومية مُكلّفة بالدّفاع السيبراني الفرنسي، بأنه: "فضاء للاتصال و التواصل عن طريق الربط العالمي لأجهزة المعالجة الأوتوماتيكية للمُعطيات الإلكترونية (الرقمية)"، كما أن هناك مَنْ عرّف الفضاء السيبراني بوصفه الدّرع الرابعة للجيش الحديثة.
 - الرّدع السيبراني: و يُعرّف بأنه " العمل على منع كل ما من شأنه إلحاق الضّرر بالأصول الوطنية في الفضاء و الأصول التي تدعم العمليات الفضائية "، حيث يتم الاعتماد في ذلك أساسًا على مصداقية الدفاع Credible Defense، و القُدرة على الانتقام An Ability to Retaliate، و الرّغبة في الانتقام A Will to Retaliate.
 - الهجمات السيبرانية: يُمكن تعريفها بكونها " فعل يُضعف من قُدرة ووظيفة شبكة الكمبيوتر لغرض سياسي أو قومي، من خلال العمل على استهداف نقاط ضعف مُعيّنة تُمكن المهاجم من الوصول للتلاعب بالنظام".
 - الجريمة السيبرانية: " و هي الفعل المُرتكّب باستعمال جهاز إلكتروني مُرتبط بشبكة الأنترنت من خلال اعتماد تقنيات برمجية خاصة.
 - القُوة السيبرانية: يعرفها جوزيف. س ناي Nye.S Joseph و هو من أبرز المُهتمين بالقوة السيبرانية بأنها استخدام مصادر المعلومات المُتعلقة بالفضاء السيبراني بغرض الوصول إلى النتائج المُستهدفة، أي بمعنى آخر، هي تحويل استخدام الفضاء السيبراني لإضافة مزايا للدولة، و ذلك باستغلال الأدوات و الأجهزة الإلكترونية المُتاحة للاستعمال في الفضاء السيبراني بغرض التأثير على الوقائع التي تتعلق ببيئات التشغيل ". (قرّه، 2019)
- 2.2 - السّياق العام لظهور الأمن السيبراني

تكمُن أهمية الأمن السيبراني كقضية ناشئة في حقل العلاقات الدولية من خلال حداثة هذا المجال، فهناك تاريخ طويل من التخمينات حول دور التكنولوجيا الرقمية في الدراسات الأمنية و التي يعود منشأها إلى حدٍ ما مع Arquilla و Ronfeldt's عام 1993، من خلال مفهوم حرب الأنترنت Netwar و الحرب السيبرانية Cyber war، وقد كان هناك تاريخ واسع من الاختبارات النظرية و الأخلاقية بشأن المخاوف المتعلقة بالأمن السيبراني، حيث أنه و مع نهاية الحرب الباردة حدثت عدة تحولات، ظهر أبرزها على مُستوى التفكير في إعداد دراسات أمنية، لأن النظرة الضيقة المُتمركزة حول الدولة the narrow state centric way of viewing كانت ستاتيكية ثابتة و دائماً ما تُؤدّي إلى الانتقاد الرأمي إلى النظرة التقليدية لمفهوم الأمن.

و ضمن المجال الدراسي الأمني النقدي، يُمكن فهم الدور الذي يلعبه الأمن السيبراني، و هو ما تجلّى في أعمال و مُخرجات مدرسة كونهانغن و روادها أمثال: باري بوزان Barry Buzan و أولي ويفر Ole Waever، حيث اكتسبت أعمالهم أهمية كبرى خاصةً عند التفكير في الأمن السيبراني، لأن تركيزهم لم يقم على مُحاولة موضوعية لتصنيف ما هو التهديد أو ما هي الثغرة الأمنية، بل ما هي الشُروط أو الحالة الرّاهنة التي يجب أن تُباشرها جهات فاعلة مُحدّدة من أجل إظهار فعل ما بأنه تهديد، و هو ما يُعرف بعملية الأمننة the process of securitization، و من خلاله يُمكن للمُنظّرين تحديد ما ينبغي و ما لا ينبغي أن يُعرّف على أساس أنه مُشكلة أمنية.

من هذا المنطلق، أصبح باحثو مجال العلاقات الدولية و بقية المجالات الفرعية الأخرى في الدراسات الاستراتيجية و الدراسات الأمنية يُركّزون بشكلٍ كبير و مُتزايد حول تأثير التكنولوجيا على الأمن المحلي و الدولي، حيث يشمل ذلك، التأثير على المفاهيم ذات الصلة كمفهوم القوة power و مفهوم السيادة sovereignty، و الحوكمة العالمية global governance و الأمننة securitization و قد وصف " سيجال " كيف يعمل توسّع الأنترنت على إعادة بلورة الأشكال التقليدية و قواعد القوة الدولية التي تعمل على نطاق واسع للدخول في عصر جديد للجيو - بوليتيك، و تاريخ هذا التطور هو محور ملف استراتيجي قام بتجميعه المعهد الدولي للدراسات الاستراتيجية بلندن و الذي يعرض بالتفصيل التطور التكنولوجي و آثاره السّياسية بدءاً من الخمسينات.

و وفق تلك الرؤية، فقد كان لظهور الأمن السيبراني علاقة مُباشرة بظهور الهجمات السيبرانية، و التي كان من أسباب حدوثها عاملين هامين:

كان الأول منها، العمل على استحداث حواسيب في مُنتصف الخمسينيات من القرن الماضي كأداة للمُعالجة و للحِفظ الرقمي للمعلومات، و قد رافقه تكاثف جهود عدد من الشّركات العامة و الخاصة، حيث توجّ بتطوير وحدة المُعالجة المركزية (CPU)، و ذلك بغرض العمل على تسهيل المهام المُوكلة له،

و قد تطور ذلك بصورة جذرية في العقود اللاحقة، حتى أصبح الحاسوب أساساً في عمل الكثير من المؤسسات، فضلاً عن الحياة العامة اليومية للأفراد.

أما الثاني، فكان ظهور الشبكة العنكبوتية (الأنترنت)، و الذي أحدث انقلاباً مثيراً في حياة البشرية من خلال التواصل و نقل المعلومات بسرعة و دقة فائقة، و قد سارعت الدول في وتيرة استخدام الحاسوب (الكمبيوتر) لغرض تحقيق استراتيجية عمل جديدة و فعّالة في المجال الأمني و العسكري مع بداية فترة التسعينيات من القرن المنصرم، و ذلك حتى أطلق البعض عليها مُصطلح الحرب السيبرانية الباردة Cyber Cold War

و قد بدأ مفهوم الأمن السيبراني يحظى بالاهتمام الواسع منذ استخدامه من طرف الرئيس الأمريكي باراك أوباما عام 2009، حيث اعتبره سبباً في تعزيز الأمن القومي لبلاده. (باي، 2023، صفحة 190)

3.2 - أهمية الأمن السيبراني

تعمل العديد من المؤسسات و الشركات من قطاعات شتى على استخدام النظم الرقمية والاتصال فائق السرعة بغية توفير أحسن و أجود خدمات لعملائها، مع ضمان خفض من تكلفة إجراءات العمليات التجارية، كما تعمل أيضاً على تأمين ما تتمتع به من أصول مادية، فضلاً على ضمان تأمين أصولها الإلكترونية (الرقمية) مع التأكيد على الحماية المثلى للأنظمة من أي وصول إليها غير مقصود على اعتبار أنّ أي اختراق للحصول على وصول غير مصرّح به إلى نظم الحاسوب أو الشبكة أو أي أجهزة تتصل بها يُعتبر بمثابة هُجوم سيبراني إن كان مقصوداً، حيث مفاد الهجوم السيبراني الناجح هو محاولة سرقة أو حذف أو تغيير البيانات السرية أو محاولة الكشف عنها، حيث أن الأمر لم يقتصر على الشركات و المؤسسات فحسب، بل تخطّت الهجمات إلى مستوى الأفراد، حيث يسعى مجرمو الأنترنت على خداع الضحايا بغية سرقة بياناتهم الشخصية و كذا المالية، فضلاً عن التعرف على نقاط ضعف البنية التحتية لشبكة الأنترنت لديهم، حيث تؤدي إلى تلك الهجمات الاحتيالية تهديد الأمن الفكري للأفراد، فإنه و عليه، توجب تعزيز أمن أنظمة الأمانة المعلوماتية دون إجراء خفض في الأداء (لطفي، 2021، صفحة 585)، حيث تعمل تدابير الأمن السيبراني على الدفاع ضد الهجمات السيبرانية بغية تحقيق الآتي:

• منع الانتهاكات أو تقليل تكلفة عواقبها

تقلّل المؤسسات التي تُطبق استراتيجيات الأمن السيبراني من العواقب غير المرغوب فيها للهجمات السيبرانية التي قد تؤثر في سمعة الشركات، و وضعها المالي، و العمليات التجارية، و ثقة العملاء. على سبيل المثال، تُفعل الشركات خطط التعافي من الكوارث لاحتواء التدخّلات المحتملة و تقليل مدة تعطيل العمليات التجارية.

• ضمان الامتثال للوائح التنظيمية

يهدف الوصول إلى الحماية المثلى للبيانات الحساسة من الأخطار السيبرانية المحتملة توجب على المؤسسات والشركات في بعض المناطق والمجالات المحددة ضرورة الامتثال للمتطلبات التنظيمية.

• الحد من التهديدات السيبرانية المتطورة

مع تغير التقنيات، تنشأ أشكال جديدة من الهجمات السيبرانية، حيث يستخدم المجرمون أدوات جديدة وابتكرون استراتيجيات حديثة للوصول إلى النظام بدون إذن، وتتبنى المؤسسات تدابير الأمن السيبراني وتحثها لمواكبة تقنيات وأدوات الهجوم الرقمي الجديدة والمتطورة. (ما المقصود بالأمن السيبراني؟)

4.2 - خصائص الأمن السيبراني

يختص الأمن السيبراني بجملة من الخصائص، أهمها:

(1) **الثقة و عدم الثقة:** يمتلك جدار الحماية الخاص بنظام الأمن السيبراني بما يشبه مُرشح إلكتروني لنوع وطبيعة البرامج والتقنيات المسموح بتفعيلها، بحيث يسمح بمرور البرامج التي بالفعل تمتلك الثقة من المُستخدم ليتم التأكد من ضمان أمان استخدامها، ومنع البرامج الضارة من التغلغل والاختراق، ويمكن ترجمة فلسفة أمن المعلومات في هذه النقطة كون الأمن السيبراني يتعامل مع كافة البرامج كونها برامج غير جديرة بالثقة، حتى يتم السماح لها من قبل المستخدم والتأكد من أمانها من خلال مصداقيتها في المتاجر الإلكترونية، فيسمح بمرور ما تم التأكد من سلامته، ويمنع المصادر المجهولة من اختراق النظام.

(2) **الحماية من التهديدات الداخلية:** هي واحدة من أهم خصائص الأمن السيبراني، وهو حماية الجهاز من التهديدات الداخلية والتي قد تتم بناءً على قلة ثقافة المستخدم أو جهله بمجال أمن المعلومات، وفيه قد يقوم بالسماح ببرامج مجهولة المصدر ليتم تفعيلها أو أن يقوم باستخدام أدوات تمس أمنه الشخصي أو حساسية مشاركة ما يملكه من معلومات، أو تحتوي إحدى الأدوات التي يقوم باستخدامها بفيروس خبيث لا يجب أن يحتوي نظامه عليه، حينها يقوم الأمن السيبراني بسرعة تنبيه الفرد أو المؤسسة بالخطر الذي تواجهه، ويقوم بمنع حدوث هذا الإجراء في أسرع وقت.

(3) **الحماية من التهديدات الخارجية:** من خلال هذه الخاصية يتم العمل على تعزيز الجدار الخاص بالحماية لتمكينه من القدرة على فلترة المخاطر الخارجية والتي من الممكن أن تحدث نتيجة التواصل مع العالم الرقمي، بدءاً من المخاطر التي تتضمنها الرسائل الإلكترونية الخطرة أو الروابط الخبيثة أو الفيروسات أو معالجة الضعف في النظام أو الثغرات التي قد يستغلها طرف ثالث في السيطرة والتحكم.

(4) الرؤية الشاملة: تقوم الأدوات الخاصة بالأمن السيبراني على منح مُستخدميها - أفرادًا كانوا أو شركات - رؤية شاملة على ما تحتويه أنظمتهم من نقاط قوة و ضعف، بحيث يُمكنهم معرفة الثغرات التكنولوجية و العمل على حلها بأسرع وقت، مع منحهم اقتراحات تخص الطريقة المثالية لمنع تكراره مرة أخرى.

(5) المراقبة المُستمرة: و أساس هذه الخاصية هو الدوام والاستمرارية في عملية المراقبة، و هذا بأن يقوم الجدار الخاص بالحماية بالعمل بشكل دائم بغرض الكشف عن أي تهديد و العمل على تدارك سرعة منعه من خطر إحداث أي تخريب أو إلحاق أي ضرر مع الحفاظ على أمن البيانات لأطول مدة قدر الإمكان.

(6) الامتثال للسياسات و القوانين: بُغية تحقيق هدف الحفاظ على السرية و الخصوصية للبيانات و المعلومات، و ردع كل ما تعلق بخطر ما يُمكن أن تُسببه الهجمات السيبرانية، و جب العمل على التقيد بالسياسات و القوانين الخاصة بالشركات و المؤسسات ضمن تحديد و منح صلاحيات الوصول إلى قاعدة البيانات، لذلك، فإن هذه الخاصية تُعد من أهم خصائص الأمن السيبراني، كون عملية الاطلاع عما يتم العمل عليه من معلومات و بيانات حساسة غير مُتاح لأي مصدر غريب عن المؤسسة أو الشركة.

(7) التَّنوع: و نعني بالتنوع، تعدُّد الخُلول التي بإمكانها التعامل مع مُختلف الأخطار أو التهديدات الإلكترونية و التي يجب أن تختص بها النُظم الخاصة بالأمن السيبراني، بحيث لا تكون نُظم الحماية مُفعَّلة لنوع مُحدَّد من التهديدات و السماح لآخر، بل عليه يجب العمل على التحليل و الاكتشاف و التعامل و المنع لجميع أنواع و أشكال الهجمات المُحتملة. (كل ما ترغب في معرفته عن الأمن السيبراني، 2023)

5.2 - أنواع الأمن السيبراني

للأمن السيبراني أنواع عديدة، يُمكن ذكرها في الآتي:

(1) أمن الشبكات: في الغالب، تحدث الهجمات المُفتعلة على مُستوى الشبكات الإلكترونية، لذلك تم العمل على إدراج أنظمة أمنية تعمل كفلتر أو صمام أمان للشبكة، بحيث تعمل هذه الأنظمة على التحكم الكامل في عناصر البيانات و الوصول للشبكة كحلول آنية، حتى تمنع أي هجمات قد تُحاول سرقة أو إتلاف تلك البيانات المخزَّنة على الخوادم الخاصة بها .

(2) الأمن السحابي: نظرًا لكون التوجُّهات الغالبة الآن لمعظم المؤسسات حول العالم هي استخدامها لتكنولوجيا الذكاء الاصطناعي و السحابة التخزينية، أصبح من اللازم تأمين السحابة الرقمية

بسبب احتوائها على كمية بيانات هائلة لهذه المؤسسات، و تُقدم مجموعة من الشركات المتخصصة في هذا المجال خدمات لحل تلك الأزمة، مثل Google Cloud و Microsoft Azure. (3) أمن التطبيقات: وهي تلك التطبيقات الخاصة بالويب، و التي تكون على اتصال مباشر بشبكة الأنترنت، و عليه، فمن المنطقي أنها تكون تحت وطأة التهديد الإلكتروني، و يعمل هذا النوع من الأمن السيبراني على تقديم المساعدة للمؤسسات و الشركات باكتشاف البيانات الحساسة التي يجب العمل على حمايتها من أي هجمات مُتوقعة من خلال برامج مُضادات الفيروسات، و جدران الحماية، و عمليات تشفير المعلومات.

(4) أمن أنترنت الأشياء: رغم أن استخدام أجهزة أنترنت الأشياء (مثل الأجهزة الذكية و أدوات الذكاء الاصطناعي و المستشعرات الحساسة عبر شبكة عالمية واحدة) يُوفر العديد من الفوائد الإنتاجية، إلا أنه يُعرض المؤسسات للتهديدات الإلكترونية، حيث يقوم أمن أنترنت الأشياء بالعمل على حمايتها من خلال اكتشاف الأجهزة المتصلة و تصنيفها حسب دورها التشغيلي بالإضافة لمدى الصلاحية الممنوحة للوصول إلى قاعدة البيانات، و عند استشعار أي حركة غير مألوفة، يقوم بالتحكم في أنشطة الشبكة و مراقبة أي عملية استغلال لهذه الأجهزة وقت التشغيل و التعامل معها.

(5) أمن المُستخدم النهائي: و هو عبارة عن مجموعة من المعاملات التقنية التي تُستخدم في حماية أجهزة المستخدمين النهائيين من أي هجوم إلكتروني مُتوقع و الذي يكون مصدره الأساسي تلك البرامج الخبيثة و الضارة، و مثال على ذلك، الحواسيب المكتبية و المحمولة، الهواتف الذكية التي يستخدمها موظفو المؤسسات و الشركات في التّواصل بشبكات الشركة بغرض الوصول إلى الموارد المتعدّدة، لذلك تسعى المؤسسات إلى حماية هذه الأجهزة بهدف وقف أي محاولة خارجية هدفها الوصول إلى نُظم الشبكات و قواعد البيانات.

(6) أمن البنية التّحتية: نعي بأمان البنية التّحتية للمؤسسات على أنه إجراء أمني يقوم على أساس حماية البنية التّحتية الحيوية للنظام و الحد من نقاط الضعف في هذه الأنظمة من فساد و تخريب و إرهاب، مثل اتصالات الشبكة أو مركز البيانات أو الخادم أو مركز تكنولوجيا المعلومات، حيث يتم العمل على وضع تدابير احترازية للطوارئ في حالة ما تم استهداف الأنظمة و البيانات، و تشمل البنية التّحتية جميع الأنظمة الحيوية كالطاقة، المياه، نُظم التدفئة و التبريد و غيرها.

(7) أسلوب التّعافي: و نعي به التّعافي من حالات الكوارث أو استمرارية العمل في ظروف التّعافي من الهجمات الإلكترونية، و هو أسلوب يعتمد على عملية استئناف العمل بعد حدوث أي تخريب في قواعد البيانات، و يتم ذلك اعتمادًا على حجم و نطاق و أعمال المؤسسة أو الشركة، حيث يتم

تفعيل العمل على أهداف مُحدّدة و مُختلفة بغرض مُساعدة المُستخدمين على الاستمرارية والتّواصل في أداء مهامهم في حالة حُدوث أي طارئ.

(8) أمن المعلومات و البيانات: وهو عملية تصميم و نشر الأدوات الخاصة بحماية معلومات عملك الهامة من التدمير أو التعطيل أو التغير، فهو العامل الحاسم في تأمين الأمن السيبراني، تم تصميمه خصيصًا بهدف الحفاظ على سرية و سلامة و توافر بيانات العمل، و ضمان أن التطبيقات والأنظمة المصرّح لها فقط هي من يُمكنها الوصول إلى معلومات مُعينة، كما أن له دور محوري حيث يُراقب و يُحقق في السُّلوك الضّار المحتمل، محاولةً منه لاحتواء التّهديدات والاستجابة الفورية للحوادث مع الحفاظ على الأدلّة للمُقاضاة المُحتملة.

(9) الأمان المالي: تم العمل على إنشاء هذا النظام مع تزويده بحلول مُبتكّرة في حال ما تم الهجوم على قواعد البيانات من قِبَل مُجرمي الأنترنت، و حماية البيانات من التّهديدات والانتهاكات المالية التي تُهدد سُبل العيش و نمو الأعمال و العلاقات مع العملاء و غير ذلك، كون أن التّهديدات المُتعلقة بالقرصنة المالية على البيانات الخاصة بالشّركات أو المؤسّسات المالية يُمكن أن تحتوي على أخطاء أو خرق غير مقصود للبيانات. (كل ما ترغب في معرفته عن الأمن السيبراني، 2023)

6.2 - تقنيات الأمن السيبراني

(1) التّحكّم في الوصول و أمن كلمة المرور: إن مفهوم اسم المُستخدم و كلمة المرور طريقة أساسية لحماية معلوماتنا حيث يُعد كأحد الإجراءات الأولى المتعلقة بالأمن السيبراني.

(2) توثيق البيانات: يجب دائماً توثيق المستندات التي نتلقاها قبل التنزيل، و يجب التّحقّق مما إذا كانت قد نشأت من مصدر موثوق و موثوق به، و لم يتم تغييرها، و عادةً ما تتم مُصادقة هذه المستندات بواسطة برنامج مُكافحة الفيروسات الموجود في الأجهزة، و بالتالي فإن برنامج مُكافحة الفيروسات الجيد ضروري أيضاً لحماية الأجهزة من الفيروسات.

(3) ماسحات البرامج الضّارة: هذه البرامج تقوم عادةً بمسح جميع الملفات و المُستندات الموجودة في النظام بحثاً عن تعليمات برمجية ضارة أو فيروسات ضارة، و الفيروسات و الدّيدان و أحصنة طروادة هي أمثلة على البرامج الضّارة التي غالباً ما يتم تجميعها معاً، و يُشار إليها باسم البرامج الضّارة.

(4) جدران الحماية: جدار الحماية هو برنامج أو قطعة من الأجهزة التي تُساعد على حجب المُتسلّلين و الفيروسات و الدّيدان التي تُحاول الوصول إلى جهاز الكمبيوتر الخاص بك عبر الأنترنت، تُمر جميع الرسائل التي تدخل الأنترنت أو تغادرها عبر جدار الحماية و من ثم تلعب جدران الحماية دوراً مُهماً في اكتشاف البرامج الضّارة.

(5) برامج مكافحة الفيروسات: برامج مكافحة الفيروسات هي برامج كمبيوتر تكتشف و تمنع و تتخذ إجراءات وقف البرامج الضارة أو إزالتها، مثل الفيروسات و الديدان، تتضمن معظم برامج مكافحة الفيروسات ميزة التحديث التلقائي التي تُمكنها من تنزيل ملفات تعريف الفيروسات الجديدة حتى يُتمكّن من التّحقق من الفيروسات الجديدة بمُجرد اكتشافها، و برامج مكافحة الفيروسات أمرٌ لا بد منه و ضرورة أساسية لكل نظام الحالي، و الذي يفحص كل رسالة و يحطّر تلك التي لا تفي بمعايير الأمان المحدّدة. (Chin, 2023)

7.2 - أبعاد الأمن السيبراني

يُطاول الأمن السيبراني جميع المسائل الاقتصادية و الاجتماعية و السياسية و الإنسانية، و ذلك انطلاقاً من المعطى له على أنه قُدرة الدولة على حماية مصالحها و شعبيها من جهة، و من كونه مُرتبط بسلامة مصادر الثروة في العصر الحالي، و نعني بها البيانات و المعلومات و القُدرة على الاتصال و التواصل، لذا لا بد من التوقّف عند أبعاده، و التي نستعرضها كالآتي:

(1) الأبعاد الاجتماعية: و تتّضح من خلال إتاحة التعبير عن الطّموحات و التطلّعات الاجتماعية من خلال تطبيقات الشبكة العنكبوتية، حيث تتم و تتشكّل عملية مُشاركة جميع شرائح المجتمع و مُكوناته بما يُتيح فرصة للاطّلاع على الأفكار و المعلومات المختلفة، إضافةً إلى تُقدمه الأنترنت من إمكانيات و خدمات تسمح بالوصول إلى فئات خاصة ككبار السّن و المرضى و ذوي الاحتياجات الخاصة .

(2) الأبعاد الاقتصادية: تُتيح تقنيات المعلومات و الاتّصالات تعزيز التنمية الاقتصادية لبلدان كثيرة عبر إفادتها بفرص الاستخدام التي تُقدّمها الشّركات الدولية، يُضاف إلى ذلك دخول عالم اليوم عصر المال الإلكتروني و العملة الإلكترونية و المحفظة الإلكترونية و استخدامها كرصيد افتراضي.

(3) الأبعاد السياسية: و تتمثّل في حق الدولة في حماية كيائها و نظامها السياسي و مصالحها الاقتصادية، حيث أصبح بإمكان المواطن الاطّلاع على خلفيات و مُبررات القرارات السياسية التي تتّخذها الحكومات، و ذلك من خلال الكم الهائل من المعلومات التي يُمكنه الوصول إليها عبر نشرها على الأنترنت.

(4) الأبعاد القانونية: بحيث يترتب النشاط الفردي و المؤسّساتي و الحكومي في الفضاء السيبراني بنتائج قانونية و مُوجبات تستدعي الاهتمام، و نُشير هنا إلى استحداث بعض المفاهيم القانونية كحق النّفاذ إلى الشبكة العالمية للمعلومات، و توسّع البعض الآخر لتشمل أساليب الممارسة الجديدة باستخدام تقنيات المعلومات و الاتصالات كالحقّ في إنشاء المدونات الإلكترونية و الحقّ في إنشاء التّجمعات على الأنترنت.

(5) الأبعاد العسكريّة: و تتجلىّ الأبعاد العسكريّة في حُطورة الهجمات أو الحروب السيبرانية التي يُمكن أن تُلحق الضرر بالأمن القومي، و عليه، صار من الضرورة التصديّ لها بالعمل على تفعيل تدابير احترازية من شأنها القُدرة و التّحكّم و السيّطرة في وقت الأزمات. (جبّور، صفحة 28 و ما بعدها)

3. السيبرانية بين مفهوميّ الأمن و القوة

تغيّرت طبيعة التهديدات السيّبرية تغيّراً جذريّاً خلال السنوات الخمس و العشرين المنصرمة، ففي الأيام الأولى للحاسب الشخصي، كان أكثر ما يُحَقِّزُ المُهاجمين هو التّهليل و الضّحك، فكانوا يخترقون نظاماً حاسوبياً لمجرد أن باستطاعتهم فهل ذلك أو ليُثبتوا وجهة نظرٍ ما، و قد كان أحد أول الفيروسات الحاسوبية التي أصابت حواسيب آي بي إم الشخصية هو " فيروس برين (الدماغ) "، الذي صنعه الأخوان " أمجد فاروق ألفي و باسط فاروق ألفي "، اللذان كانا في الرابعة و العشرين و السّابعة عشرة، من لاهور في الباكستان، و كان الغرض من فيروسهما حميداً، إذ كانت مُهمته منع الآخرين من قرصنة البرمجيات التي كان الأخوان قد أمضيا سنوات في تطويرها. فقد قام الأخوان - و قد أزعجتهم قرصنة الآخرين لبرمجياتهما من دون دفع ثمنها - بتضمين هذه البرمجيات تحذيراً شديد اللّهجة يقول: أهلاً بك في دُونجِيُون برين و أمجد (العنوان و الهاتف) احذر هذا الفيروس و اتّصل بنا لمعالجته، و في نهاية المطاف، تنقّل فيروس برين عبر المعمورة معروفاً باسم باسط و أمجد. (دوغمان، 2016، الصفحات 20-21)

1.3 - القُوّة السيبرانية cyber power

أبرزت الثورة المعلوماتية شكلاً جديداً من أشكال القوة، و هي القوة السيبرانية، و ذلك نتيجة للتقدم التكنولوجي السّريع في أجهزة الكمبيوتر و الاتّصالات و البرمجيات بحلول القرن الحادي و العشرين (صفاء و مهدي، 2020، صفحة 152) و يتضمن مفهوم القوة السيبرانية تغطية جميع القضايا التي تتعلق بالتفاعلات الدولية، و التي تشمل القضايا العسكريّة و الاقتصادية و السياسيّة و الثقافية و الإعلاميّة و غيرها، و هي تختلف عن مُسمى " الحرب السيبرانية " التي تقتصر على التّطبيقات العسكريّة للفضاء الإلكترونيّ.

و يعتقد جوزيف ناي أيضاً أن هذه الفترة ليست الأولى التي يتأثر مفهوم القوة فيها بالتطور التكنولوجي، فقد تأثر العالم في القرن الخامس عشر باختراع الطباعة و ما أحدثه من تطور في الإصلاح داخل أوروبا من خلال سهولة وُصولها إلى الناس و استخدامها، و يُضيف أن الثّورة التكنولوجية الحالية في بعض الأحيان تتم تسميتها بالثّورة الصّناعيّة الثالثة التي تعتمد على سرعة و تطور أجهزة

الكمبيوتر و أجهزة الاتصالات و أنظمة المعلومات و البرامج، و التي أثّرت بصورة دراماتيكية على صناعة و خلق و نقل المعلومات.

و يُردف " ناي " أن الدولة سوف تظل هي الفاعل المهيمن على الفضاء الإلكتروني، ولكن هناك فواعل أخرى سوف تُشاركها في هذا الفضاء الإلكتروني، و سوف تجد الدُول صُعوبة في السيطرة عليه، فالحكومات قلقة من حالة تسرب المعلومات و تدفقها و صُعوبة السيطرة عليها، و يرى أيضاً أن القوى الكبرى ليست لها المساحة نفسها التي يُمكن من خلالها السيطرة على الفضاء الإلكتروني مُقارنةً بقدرتها على السيطرة على الإقليم البحري أو البري، و أن الكيانات الافتراضية التي تنشأ عبر الأنترنت تستطيع أن تلتقي في إقليم افتراضي جديد خاص بها عبر الأنترنت و تُؤسّس لذاتها كيانات تنظيمية، و من ثَم يتراجع دور الدولة المركزية في حياة البشر، و يُضيف أن الدول الكبرى التي تمتلك القوة الصّلبة أو الناعمة، حتى الولايات المتحدة الأمريكية، وجدت نفسها تُواجه مشاكل في السيطرة على حُدودها على الأنترنت. (خليفة، 2019، الصّفحات 142- 143)

و من خلال تقييم مُقاربات الجيو - بوليتيك، ثَمّ التوصل إلى نظرية القوة السيبرانية التي رأت أن القوة السيبرانية يجب أن ترتكز على أربعة عوامل رئيسية و هي، التقدّم التكنولوجي، سرعة نطاق العمليات، السيطرة على السمات الرئيسية و التعبئة الوطنية، و تماشياً مع هذه الميزات تبيّن أن الاعتماد على الفضاء الإلكتروني أدى إلى نقاط ضعف كونه عُرضة لمجموعة من التهديدات، كهجمات رفض الخدمة و الفساد المحتمل للبيانات الحساسة، لكن نظراً لانتشار التكنولوجيا المتطورة للفضاء الإلكتروني فقد تعزّزت سرعة و نطاق العمليات مثل القدرة على إشراك أهداف حساسة بنجاح في أي مكان من العالم، مما حسّن في القدرة على التحكم و القيادة و قلّل من تركيز عمليات مُراقبة الأزمنة الكلاسيكية. (باي، 2023، الصفحات 195- 196)

2.3 - أثر السيبرانية في تطور القوة

مما هو مُتعارف عليه فإن المصادر و الأشكال الخاصة بقوة الدولة تتغير من حين لآخر، خاصة ما تعلّق منها بالجانب الخاص بالقوة الصّلبة و التي تتمثل في القدرة العسكرية و الاقتصادية للدولة، و في ظل تلك الظروف، تزايد الاهتمام بالأبعاد غير المادية للقوة، و من ثَم برز ما يُعرف بالقوة الناعمة التي تعتمد على جاذبية النموذج و الإقناع، و مع ثورة المعلومات ظهر شكل جديد من أشكال القوة هو القوة السيبرانية (Cyber power) التي لها تأثير كبير على المستوى الدولي و المحلي، فمن ناحية أدّت إلى توزيع و انتشار القوة بين عدد أكبر من الفاعلين ما جعل قُدرة الدولة على السيطرة موضع شك، و من ناحية أخرى فقد تم العمل على منح عدداً أصغر من الفاعلين قُدرةً أكبر فيما تعلّق بمُزاوجة الممارسة ما بين القوة الصّلبة و القوة الناعمة عبر الفضاء السيبراني، و هو لدليل واضح على التغيّر المشهود في موازين و علاقات القوى الدولية. (قُره، 2019)

3.3 - القوة الناعمة

تحول مفهوم الأمن القومي من النمط التقليدي، المتعلق بمدى قدرة القوة العسكرية - التي تتمتع بها الدول - على حمايتها من التهديدات الأمنية، ولم يعد مناسباً اقتصار الأمن القومي على القوة الصلبة، فقد تغيرت مصادر قوة الدولة، و شملت التكنولوجيا و الاتصالات و المعلومات، إلى جانب القوة الدبلوماسية و الاقتصادية للدولة، و هذه المصادر الجديدة للقوة أقل تكلفة و ذات تأثير عالٍ في النظام الدولي. (صابر، 2022)

و قد أشار إلى ذلك " جوزيف ناي " حيث يرى أن القوة ارتبطت بالسياق و النمو السريع للفضاء السيبراني الذي أصبح مجالاً مهماً في السياسة الدولية، حيث أن انخفاض تكلفة الدخول و عدم الكشف عن الهوية و عدم التماثلية في الانكشافية أعطى فرصة للفواعل الصغيرة لأن تكون لها قدرة أكبر على ممارسة القوة الصلبة و الناعمة في هذا الفضاء مقارنةً بالعديد من المجالات التقليدية في السياسة الدولية. (شرايطية، 2020، صفحة 398)

و جدير بالذكر، أن القوة العسكرية تبقى بطبيعة الحال كأحد عناصر القوة ثقلًا و أهمية، إلا أنها لم تعد تُعتبر كما في السابق المصدر الوحيد، فقد انضمت إليها مصادر " القوة الناعمة " Soft power، و مع ما شهده العالم من تحول نحو الرقمية بالاعتماد على الشبكة الإلكترونية في شتى مجالات التعاون الدولي فضلاً عما تعلق بالصراعات الدولية تعاضل تحول طبيعة القوة، لتزداد حدة التهديدات المتعلقة بالأمن السيبراني و استغلال الفضاء الإلكتروني لتحقيق مزايا و دور فعال و مؤثر من خلال أدوات إلكترونية. (صابر، 2022)، فالأمن السيبراني اليوم هو جزء من الصراع الدولي، لأنه يمثل القوة الناعمة التي تتغلغل بسرعة خارقة دون مقدمات لتصل إلى الاقتصاد و التكنولوجيا و الثقافة و جميع مناحي الحياة، و ذلك عبر ما يُسعى بالفضاء السيبراني و الردع السيبراني و الهجوم السيبراني و الجريمة السيبرانية، و هي أسلحة الحرب الجديدة. (شعبان، 2024)

و تأسيساً لما سبق، يتضح أن الثورة المعلوماتية و التكنولوجية، قد نتج عنها استبدال عناصر القوة التقليدية بأدوات جديدة، و أصبحت القدرات العسكرية المتميزة، و أيضاً الأموال، و الثروات التي تمتلكها الدول، عناصر غير كافية لحماية أمنها، أو تعزيز دور فعال لها إقليمياً، و دولياً، فقد بات من الضروري امتلاك الدولة أدوات القوة السيبرانية، بل توظيفها كأدوات داعمة للقوة الناعمة و الصلبة.

فما جاء به التطور التكنولوجي، و ما صاحبه من عمليات العمل عليه بواسطة الفواعل من الدول و من غير الدول لتحقيق أهداف مؤدّاها تهديد الأمن القومي حفّز على ضرورة استيعاب الفضاء

السيبراني على اعتباره كأحد عناصر و مقومات الأمن القومي، حيث تؤدي الهجمات الإلكترونية إلى تداعيات سلبية على التنمية الشاملة (الاقتصادية، الاجتماعية، و السياسية.. و غيرها)، حيث تنتشر الجرائم الإلكترونية كالايتزاز الإلكتروني، و القرصنة، و المسامات لأجل مقابل مادي، و قد يستغل الفاعلون وسائل التواصل الاجتماعي في تهديد الأمن القومي، عبر إثارة القلق في المجتمع، و تهديد السلم الاجتماعي، مما يستوجب العمل باستمرار على بناء استراتيجية فعّالة، مع تحديثها بشكل مستمر للتعامل مع التهديدات السيبرانية، و إدارة هذه المواقف بكفاءة، و التنسيق الدولي لمواجهة هذه الهجمات الإلكترونية، فتأثير الفضاء الإلكتروني على المجال الأمني لا يقتصر على الدولة داخلياً فقط، بل إنه يمتد و يصل للمحيط الدولي، فيرسم مضموناً جديداً للأمن و السلم الدوليين، و يضع أطراً جديدة لواقع العلاقات الدولية، و قد بات مؤشر "الأمن السيبراني" GCI ضمن أهم الآليات لقياس أمن كل دولة حول العالم. (صابر، 2022)

و من هنا، جاءت فكرة المزاوجة بين القوة الناعمة و القوة الصلبة بغرض خلق ما يُعرف بالقوة الذكية، كون أن تحقيق الأهداف لا يمكن أن يتحقق دائماً باستخدام القوة الناعمة، لذلك تَعَمَد القوى الاستكبارية إلى عملية المزاوجة هذه من أجل كسب السلام، غير أن هذا المزج لا يُعطي حاصلاً حسابياً دقيقاً، لأن هناك علاقة جدلية بين القوتين، خاصة و أن القوة الصلبة لها جانب جَذَاب أو ناعم، و لأن عامة الناس تميل إلى الطرف القوي حتى و إن كانت تُشفق على الطرف الضعيف. (طي و ياغي، تموز 2011، الصّفحات 17-18)

4.3 - التهديدات السيبرانية

تهديدات الأمن السيبراني هي أفعال يقوم بها أفراد لديهم نوايا ضارة، و هدفهم هو سرقة البيانات أو إلحاق الضرر بأنظمة الحوسبة أو تعطيلها، و تشمل الفئات الشائعة للتهديدات السيبرانية البرامج الضارة و الهندسة الاجتماعية و في تعطيل الخدمة و هجمات الحقن، و يمكن أن تنشأ التهديدات السيبرانية من مجموعة مُتنوعة من المصادر كالدول المعادية و الجماعات الإرهابية أو الأفراد المتسللين أو الأفراد الموثوق بهم مثل الموظفين أو المقاولين الذين يُسيئون استخدام امتيازاتهم للقيام بأعمال خبيثة. (Cybersecurity Threats)

و تُعد جرائم الأنترنت من الجرائم المستحدثة التي تُستخدم فيها شبكة الأنترنت كأداة لارتكاب الجريمة أو لتسهيل ارتكابها، و قد أُطلق مُصطلح جرائم الأنترنت في مؤتمر جرائم الأنترنت المُنعقد في استراليا عام 1998، و تُعرّف جرائم الأنترنت بأنها جميع الأفعال الإجرامية المُرتكبة بواسطة الحاسب الآلي من خلال شبكة الأنترنت، و يشمل ذلك الجرائم الجنسية و الممارسات غير الأخلاقية، جرائم الاختراقات، الجرائم المالية، جرائم إنشاء أو ارتياد المواقع المُعادية و جرائم القرصنة. و هي مسألة ذات أبعاد خاصة سيما إذا أدركنا أن العالم الافتراضي هو نتاج اجتماع الاتصالات و التكنولوجيا

و المعلومات التي تتجاوز منطق الحدود الدولية هو بيئة مناسبة لارتكاب أفعال يَغْدُها المجرى العادي للأُمور في عالمنا المادي أفعال غير مشروعة تصل إلى التجريم في النُظم الجنائية المعاصرة. (الحسيناوي، 2011، صفحة 34)

و تُعدُّ الهجمات السيبرانية أخطر مصادر تهديد الأمن القومي في ظل مُجتمع ما بعد المعلومات، وهي تلك الهجمات التي تتم عبر شبكة الأنترنت بهدف التدمير أو التجسس أو التزييف، سواءً كانت عبر أجهزة كمبيوتر، أو هواتف ذكية، أو أجهزة أنترنت الأشياء، بل يتعدى الأمر ذلك ليشمل أيضًا الأجهزة غير المتصلة بالأنترنت مثل المولِّدات و المُحرِّكات، و التي يُمكن تدميرها عبر فيروسات الكمبيوتر، و تكون الخسائر في هذه الحالة فادحة، خاصةً إذا استهدفت البنية التحتية للدولة، من نُظم اتصالات، و مُواصلات، و مُستشفيات، و سُدود، و خزانات مياه، و محطات طاقة، أو استهدفت سيارات ذاتية القيادة، أو درونز، أو رُبُوتات، تُكوِّن منها جيوشًا يُمكن استخدامها في إلحاق خسائر بشرية أو مادية. (خليفة، 2019، صفحة 104)

1.4.3 - معايير تصنيف الهجمات السيبرانية

يُشير مُصطلح الجريمة السيبرانية إلى أي نشاط غير قانوني يستخدم الكمبيوتر كوسيلة أساسية للعمولة و السرقة، و تُوسّع وزارة العدل الأمريكية تعريف الجريمة السيبرانية (الإلكترونية) " ليشمل أي نشاط غير قانوني يستخدم جهاز كمبيوتر لتخزين الأدلة ". و تشمل القائمة المتزايدة للجرائم الإلكترونية الجرائم التي أصبحت مُمكنة بواسطة أجهزة الكمبيوتر، مثل اقتحام الشبكة ونشر فيروسات الكمبيوتر، بالإضافة إلى الاختلافات القائمة على الكمبيوتر للجرائم الحالية، مثل سرقة الهوية و المطاردة و البلطجة و الإرهاب التي أصبحت مُشكلة رئيسية للناس و الأمم، و عادةً ما يتم تعريف الجريمة السيبرانية بلغة الرجل العادي على أنها جريمة تُرتكب باستخدام الكمبيوتر و الإنترنت لسلب هوية شخصٍ ما أو لبيع الممنوعات أو لملاحقة الضحايا أو تعطيل العمليات ببرامج خبيثة. (Reddy & Reddy, 2014) و بينما يستخدم ما يقرب من 4.8 مليار شخص في جميع أنحاء العالم منصة وسائط اجتماعية واحدة أو أكثر، أو ما يزيد قليلاً عن 59 % من سكان العالم، و بينما تُساعد منصات الوسائط الاجتماعية المستخدمين على البقاء على اتصال مع الأصدقاء و التواصل مع العملاء و الترويج للشركات، فإنها تزيد أيضًا من تعرُّض الأشخاص و الشركات للتهديدات السيبرانية بالطرق التالية (Chin, 2023) .

1.1.4.3 - حسب الأسلوب المُستخدَم

- هجمات التَّصَيِّد phishing

يعتمد هذا الأسلوب على الهندسة الاجتماعية Social Engineering من خلال تحفيز الضحية لفتح رابط يحتوي على برمجية خبيثة تُصيب الجهاز، وذلك من خلال إرسال رسائل تحتوي على موضوعات قد تكون من اهتمام الضحية، أو استخدام أسماء قد تكون مألوفة بالنسبة لها، مع إرفاق إحدى البرمجيات الخبيثة بهذه الرسائل، وبمجرد قيام الضحية بفتح الرسالة تبدأ عملية القرصنة، ويُعتبر البريد الإلكتروني و الرسائل الشخصية و التطبيقات التي يتم تنصيبها على مواقع التواصل الاجتماعي من أكثر الأشكال شيوعاً. (خليفة، 2019، الصفحات 104 - 105)

و الأمر نفسه ينطبق على حسابات وسائل التواصل الاجتماعي الشخصية للموظفين، حيث يُمكن أن تُساهم كل مشاركة في كل ملف تعريف على وسائل التواصل الاجتماعي مُرتبط بنشاط تجاري في قدرة مُجرمي الأنترنت على استخدام تقنيات الهندسة الاجتماعية أو طرق أخرى لتقديم تنازلات لأنظمة و بيانات الأعمال بمجرد إنشاء ملف تعريف رقمي، و عادةً ما تكون المعلومات مرئية للجُمهور، فكلما زاد عدد المعلومات التي يقوم المستخدم بتحميلها زاد خطر الجريمة الإلكترونية.

مثال على ذلك، هو عندما يستهدف مُجرمو الأنترنت مُستخدمي وسائل التواصل الاجتماعي باستخدام حسابات مزيفة لخداع المستخدمين المطمئنين لتقديم معلومات شخصية أو الوصول إلى بيانات الاعتماد أو النقر فوق الروابط التي تقوم بتنزيل البرامج الضارة. (Chin, 2023)

• هجمات وقف الخدمة DDOS

هي أحد أخطر أشكال الهجمات السيبرانية، حيث يتم استخدام برامج كمبيوتر مُخصّصة لهذا الغرض، أو السيطرة على عدد كبير من أجهزة الكمبيوتر و تكوين شبكة زُبوتية بينها تُسمى Botnet، يستخدمها الهاكرز في إطلاق هجمة إلكترونية ضخمة على الضحية، و إغراقها بالآلاف من الرسائل و الطلبات التي تُؤدي في النهاية إلى انقطاع الخدمة و وقفها، سواء كان ذلك موقع أنترنت، أو خدمة إلكترونية خاصة أو حكومية.

• الثغرات الصّفرية Zero-Day

هي الثغرات الحديثة نسبياً، و التي لم يتم اكتشافها بعد من قِبل المطورين و الباحثين الأمنيين، و عادةً ما تكون موجودة في برامج التّشغيل و تطبيقات الكمبيوتر و الهواتف الذّكيّة، و إذا اكتشفها أحد قراصنة المعلومات قبل الفنينين، فإنه قد يستغلها في السيطرة على أجهزة الضحايا بصورة مباشرة أو حقنها بعدد من التّطبيقات و البرمجيات الخبيثة التي تقوم بوظائف مُعينة.

• الأبواب الخلفية Backdoors

تلجأ بعض الشّركات إلى هذه الآلية بهدف الدخول على جهاز المُستخدم بصورة مُباشرة لإصلاح مُشكلة فنيّة مثلاً أو جمع معلومات عن آلية عمل الجهاز، أو يقوم بعض المنظمات والمُؤسّسات الأمنية

بوضعها على أجهزة الضحايا بهدف التجسس و المراقبة، و من ثم فهي ليست ثغرات مجهولة، بل ثغرات مقصودة.

• الثغرات التقنية

هي الأخطاء التقنية التي تؤدي إلى ثغرات، مثل سوء هندسة الشبكة الداخلية الخاصة بالشركة أو المؤسسة، أو ضعف إجراءات التأمين الخاصة بها، أو الثغرات الموجودة في التطبيقات سيئة السُّمعة، و التي يستغلها القراصنة لإصابة الأجهزة و الخوادم، و من الأنماط التي تستخدم في ذلك نمط SQL Injection Attack

2.1.4.3 - حسب القطاع المُستهدف: يُمكن تصنيف الهجمات السيبرانية أيضًا وفق طبيعة الجمهور المُستهدف منها، فقد يكونون أفرادًا عاديين يتم اختراقهم بهدف الابتزاز أو استغلال أجهزتهم مرة أخرى في إطلاق هجمة أعنف و أشدّ، أو شركات خاصة لسرقة حقوق الملكية الفكرية و براءات الاختراع و خطط التسويق، أو القطاع المالي و المصرفي بهدف الإضرار باقتصاد الدولة أو سرقة الأموال، أو خدمات حكومية للتعبير عن الاعتراض على موقف معين، أو أجهزة أمنية بهدف سرقة معلومات استخباراتية و خطط عسكريّة و تصميمات أسلحة، أو مؤسسات إعلامية بسبب موقفها من إحدى القضايا التي تشغل الرأي العام.

3.1.4.3 - حسب الهدف من الهجمة: يُمكن تصنيف الهجمات السيبرانية وفقًا لطبيعة الهدف منها، فقد يكون الهدف "مالي" من خال اختراق الحسابات البنكية و بطاقات الائتمان أو اختطاف أجهزة الأفراد و طلب فدية منهم، أو هدف "عسكري"، مثل اختراق النظم العسكريّة و الطائرات من دون طيارو سرقة المعلومات الاستخباراتية، أو هدف "سياسي" للتعبير عن الغضب من قرارات أو تصرّفات سياسية، أو هدف " إنساني " للتعبير عن التعاطف مع قضية إنسانية مثلًا، كاختراق المواقع الإسرائيلية تعاطفًا مع القضية الفلسطينية، أو حتى لهدف "دِعائي" مثل اختراق مواقع الشركات الكبرى بهدف إظهار القُدرات والاستعراض.

4.1.4.3 - حسب الفواعل المُشاركة: قد يقوم بهذه الهجمات " قوات مُسلحة " و جيوش إلكترونية في إطار الصّراعات العسكريّة و السّياسيّة بين الدول و بعضها البعض، أو "مجموعات إجرامية " و عصابات مُنظمة من أجل السّرقَة و غسيل الأموال، أو "جماعات إرهابية " كأحد أنواع مُمارسة الإرهاب الإلكتروني، أو مجموعات قرصنة عادية لأسباب مختلفة، قد تكون بهدف سرقة أموال أو التعبير عن غضب أو إرسال رسالة مُحدّدة ... إلخ. (خليفة، 2019، الصّفحات 104-105-106)

2.4.3 - أنواع قرصنة المعلومات

يرتبط ارتكاب جرائم المعلومات في أي زمان ومكان بما يعرف بالمجرم المعلوماتي، وهناك من يتوسع في تحديد فئات المجرم المعلوماتي تبعاً للخطورة الإجرامية الكامنة فيه، حيث يرى كثير من الباحثين بأن التركيز يجب أن ينصبَّ على فئتين هما: (تمام، 2019، صفحة 22)

• الفئة الأولى Hacker

و يُطلق عليهم اسم الهاكر ذو القُبعة البيضاء White Hat Hacker أو الهاكر الأخلاقي Ethical، وهم الأشخاص الذين يستخدمون قدراتهم في مجال الكمبيوتر بصورة شرعية لا يترتب عليها الإضرار بمصالح الغير، و يُحاولون أن يجدوا الثغرات في أنظمة الكمبيوتر بهدف تأمينها من محاولة الاختراق الخارجية (خليفة، 2019، صفحة 107) وهم فئة المجرمين الأقل خطورة و الذين تتوافر لديهم خبرة مُعتبرة في مجال الحاسب الآلي و وظائفه و مكوناته، و نُظم المعلوماتية، و معرفة البرامج التي يجري العمل بها كالبرامج المحاسبية، و بما أن هؤلاء يُمارسون مواهبهم لغرض الوُلوج الى نُظم المعلومات بدافع الفضول أو اللهو، فهم لا يُدركون ولا يُقدِّرون النتائج المحتملة التي يُمكن أن تُؤدي إليها أفعالهم غير المشروعة، لذلك فإن هذه الفئة تُعد أقل خطورة، و لكن مع ذلك يُلاحظ أن ازدياد الأعداد المستخدمة لتكنولوجيا الإعلام و الاتصال، و ما يتبعه من ازدياد نسبة الجرائم في هذا المجال، فلا يستبعد معه احتمال انزلاق هذه الفئة من مُجرد هُوة للأفعال غير المشروعة إلى مُحترفين.

• الفئة الثانية Crackers

و يُطلق عليهم اسم الهاكر ذو القُبعة السوداء Black Hat Hacker، وهم الأشخاص الذين يستغلّون قدراتهم للإضرار بمصالح الآخرين، أو لتحقيق أهداف غير شرعية، كسرقة البنوك و البطاقات الائتمانية، و اختراق الهواتف المحمولة و مواقع الأنترنت و الشبكات. (خليفة، 2019، صفحة 107) أصحاب هذه الفئة يتمتعون بمُستوى مهاري عالي يسمح لهم بالدخول و اقتحام الأنظمة الحاسوبية بكل سهولة و اقتدار رغم احتياطات الأمن المتعددة، و رغم قلة العناصر القادرة على اكتشافها، مما تبدو معه خطورة هذه الفئة من المجرمين واضحة بصورة كبيرة، إذ غالبًا ما تكون جرائم التحويل و النسخ و الإضافة للمعلومات على البرامج و تغيير محتواها من جانب هذه الفئة ضخمة.

و تبعًا لذلك، يُميز بين مُصطلحي Le cracker و Crasher من حيث نتيجة الفعل الإجرامي، فالأول يلج داخل النظام و يُحطِّم المعطيات بدافع الرغبة، أما الثاني فيدخل إلى النظام للتحريف في هذه المعطيات أو مُحوها أو إدخال معلومات أخرى، كما يُطلق على فئة Cracker ب Spiders لأنهم يعملون في الخفاء، ولا يتركون آثارًا مادية لأفعالهم، و قد يُصبحوا أشد خطورة إذا ما تم تبادل تقنياتهم فيما بينهم، و شكّلوا ما يُعرف بالجماعات أو الفرق المتخصصة أو العمل عن طريق الوساطة. (تمام، 2019، الصفحات 22-23)

و يُعتبر الأمريكي " كيفن ميتنيك " من أشهر القراصنة في العالم، بل يُعد أشهر هكرز في التاريخ، حيث أطلق على نفسه اسم The menetor ، ليقوم بعدها بنشر دراسة الشهيرة التي عُرفت باسم "بيان الهاكر"، وهو بيان لأهداف وجهات نظر القُراصان، نُشرت الدراسة في المجلة الإلكترونية Phrack، و من ثَم تم اعتقاله، و تُعد الدراسة أشهر ما كُتب عن قرصنة الحاسوب. (ليتيم و ليتيم، 2015، صفحة 242)

5.3 - الحُروب السيبرانية

راجت في القرن العشرين مفاهيم تنطوي على دلالات ترتبط بفلسفة مُطلقها، هذه المفاهيم شكّلت مادة للاستعمال في إطار العلاقات الدولية كمفهوم الحرب الباردة و الحرب الدبلوماسية و حرب النجوم و غيرها، و مع مطلع القرن الواحد و العشرين سيتم الترويج لمفهوم جديد هو الحرب الناعمة المُوازي للحرب الصلبة التي تقوم على القتل و التدمير و الإخضاع. (طي و ياغي، تموز 2011، صفحة 07)

و تُعرّف وزارة الدفاع الأمريكية الحرب الإلكترونية بأنها نوع من أنواع القتال الذي يستهدف النَّصر من خلال إخضاع الخصم و النيل من إرادته و هزيمته دون أن يَنْجِزَ عن ذلك سفكٌ للدماء. (درسي، 2022، صفحة 916)

فيما يُعرّف آخرون الحرب الإلكترونية بأنها مُصطلح يُشير إلى أي تتنازع تدور أحداثه في الفضاء الإلكتروني و على أن يكون ما بين أطراف دولية. (الغفار، 2016، صفحة 10)

و في الحقيقة، يُقسّم خبراء الأمن السيبراني (الإلكتروني) الحُروب الرقمية إلى قسمين:

الأولى، و تُدعى الحرب الشبكية (Netwar)، و يتعلق هذا النوع من الحروب بالصِّراعات ذات الطابع المعلوماتي على مُستوى الأمم و المجتمعات، و تهدف إلى تخريب أو تدمير ما يمتلكه الهدف من معرفة عن نفسه أو ما يعتقد أنه يعرفه عن نفسه أو عن العالم من حوله.

و يدخل استهداف الرأي العام أو النُخب الحاكمة في نطاق أهداف هذه الحرب، و ذلك من خلال المُراوحة بين الأساليب الدبلوماسية و " البروباغندا " أو الحروب النفسية.

أما النوع الثاني، فيُعرّف بالحرب الإلكترونية (syberwar)، و هي عبارة عن شَنّ عمليات عسّكرية، مُستندة على مبادئ تكنولوجيا المعلومات، و تهدف إلى تخريب أو تدمير الأنظمة المعلوماتية للخصم، و كذا التطلُّع للحصول على كل بياناته و معلوماته، و السَّعي في الوقت ذاته لجعله يعيش حالة استنفار و قلق و ارتباك مُؤداها في الأخير حُدوث انقلاب في موازين القوى المعلوماتية لفائدة العنصر المهاجم الذي لا يتمتّع في الغالب بتفوق مادي على الخصم، و ربما يكون من المبكر الحديث عن طبيعة هذا النوع من الحروب الرقمية، و لكن الأكيد أن هذا النوع من الحروب يفرض نفسه كأمر واقع،

و تُعبّر عن مدى الخطر الحقيقي الذي بات يُهدد الأمن القومي للدول و الجماعات و الأفراد على حدٍ سواء. (الحروب الرقمية و القصف الإلكتروني، 2017)

و لحرب المعلومات أبعادًا هُجومية و دفاعية تتمثل في:

• **عمليات هُجومية: Offensive Operations**

و الهدف منها مهاجمة نُظم معلومات الطرف العدو سواء لأسباب عسكريّة أو سياسية أو اقتصادية أو لمجرد الإثارة و إظهار القُدرات و شن حرب نفسية على الخصم.

• **عمليات دفاعية: Defensive operations**

و تشمل جميع الوسائل المعلوماتية الوقائية المتوفرة للحدّ و التّقليل من أعمال التّخريب التي قد تستهدف أنظمة المعلومات، وهي كالآتي:

(1) أسلوب المنع و الوقاية: و نعني به التزام كافة تدابير حماية الأنظمة الخاصة بالمعلومات قبل التعرّض لأيّ هُجوم مُحتمل.

(2) التحذير و التنبيه: أي التنبؤ بحدوث الهُجوم قبل وقوعه من خلال تفعيل أنظمة الإنذار المُبكر.

(3) كشف الاختراقات و التعامل معها قبل وقوعها: و تستمد حُرُوب المعلومات تأثيرها و فعاليتها من العديد من الخصائص، فهي حُرُوب ذات طابع أكثر شُمولاً و تستهدف جميع نُظم المعلومات المتّصلة بتكنولوجيا الحاسوب و الرقمنة و البرمجيات عبر العالم، إضافة إلى الفجوات و المخاطر المرافقة لها، بحيث تحمل هذه الحروب أشكالاً جديدة من التّهديدات أهمها إمكانية التعرّض للاختراق و إصابة البنى التّحتية و مؤسّسات الدولة المرتبطة بتكنولوجيات الحاسوب و الشبكات، و هو ما ينجر عنه قابلية شديدة للعطب، و تهديدًا حقيقيًا للأمن القومي للدول، بالإضافة إلى البُعد النفسي و السيكولوجي من خلال إرباك العدو و جعله في حالة من التوتّر و الشّلل و غير قادر على المواجهة من جزاء الأعطاب التي تمس مراكز ثقله الاستراتيجي. (درسي، 2022، الصّفحات 912-913)

و من أشهر نماذج الحُرُوب السيبرانية في العالم، تلك الهجمات التي شنتها الصين على الولايات المتحدة الأمريكية في عام 2001، حيث تعرّض ما يقرب من 1200 موقع أمريكي لهجمات من قراصنة صينيين في الفترة من 30 أبريل حتى 7 مايو عام 2001، و شملت تلك الهجمات مواقع البيت الأبيض و القُوّات الجوية الأمريكية و وزارة الطاقة الأمريكية، و ذلك على خلفية اصطدام مُقاتلة صينية من طراز " J-8 land " مع طائرة تجسّس أمريكية من طراز " EP-3E " فوق جزيرة " هاينان " الصّينية في الأول من أبريل عام 2001.

كما قام قراصنة صينيون بشن هجمات على شركة " لوكهيد مارتين" الأمريكية، حيث تمكّنوا من سرقة معلومات عن تكنولوجيا تصنيع مُقاتلة " إف 35 " التي استخدمتها الصين فيما بعد عند تصميم و تصنيع مُقاتلة " تي 20 " الصينية، و شملت الهجمات السيبرانية أيضًا مُقاولين لدى وزارة الدفاع الأمريكية يعملون على صناعة و تطوير الطائرات من دون طيار الأمريكية، بهدف سرقة معلومات حول هذه الطائرات و كيفية صنعها و تطويرها. (خليفة، 2019، صفحة 114)

خاتمة:

إن الوعي بالدور الذي يُمكن للأمن السيبراني أن يؤديه في ظل ما يعيشه عالم اليوم من تسارع نحو الرقمية التي صحبتها الصور المستحدثة للجريمة هو لزامٌ بعد أن أصبحت كُبرى الدول و كُبرى الشركات في العالم تُقر بأنها ليست في مأمن أمام مخاطر الاختراق و تهديدات الجرائم الإلكترونية في ظل ما يعرفه العالم من صراعات دولية، لذا فقد أصبح الوعي بضرورة هذا المفهوم حتمية لا بُدّ منها، و هو الأمر الذي يستدعي إعادة التفكير بجدية بغرض إيجاد ميكانيزمات و حلول فعّالة لمواجهة المخاطر و التهديدات السيبرانية التي تتميز بالدقة و السرعة و الغموض كونها تُمثّل تلك القوة الناعمة التي تتغلغل من دون إعطاء أية مُقدمات لتصل إلى جميع مناحي الحياة، و هذا من أجل الحفاظ على مكاسب الدول و العمل على تعزيز و إرساء أمنها القومي.

و في خاتمة هذه الورقة البحثية التي تم التعرّض من خلالها إلى جوانب عدّة لمفهوم الأمن السيبراني و إلى أهم مُحدّداته و أبعاده، نأمل أن تكون هذه الورقة محطّ تحفيز للباحثين في المجال بغرض استمرار التفكير في تناول الموضوع بشكل و فكر جديد و ذلك ما نأمله و نرجّوه.