الامن في الفضاء السيبراني: دراسة في التهديدات واستراتجية المواجهة

د.باسم علي خريسان

جامعة بغداد-مركز الدراسات الاستراتجية والدولية

المقدمة:

يحمل الفضاء السيبراني تاثيره في مختلف مجالات الحياة حيث يساهم الفضاء السيبراني ومن خلال ادواته المختلفة في اعادة رسم مختلف ابعاد الحياة ، فيعمل على اعادة تشكيل الوعي والادراك الثقافي والاجتماعي والسياسي والامني للافراد والمجتمعات والدول بصورة مغايرة عما كانت عليه ،حيث نجد تصورات وبنى جديدة يتم تأسيسها في المجال السياسي والامني والاقتصادي والاجتماعي والثقافي والنفسي .الخ ، فالانسان والمجتمعات والدول لم تعد تعيش في العالم الواقعي – المحدود فقط، وانما اصبح للاواقعية واللامحدودية التي يشكلها الفضاء السيراني حضورها المؤثر في ذلك ،واصبح الحديث عن الحرب السيبرانية والامن السيبراني والردع السيبراني والجيوش السيبرانية والاسلحة السيبرانية والارهاب السيبراني والعنف السيبراني والسلام السيبراني والسياسية السيبرانية والجريمة السيبرانية والقانون السيبراني والقضاء السيبراني والجهاد السيبراني والتجسس السيبراني والدين السيبراني والاخلاق السيبرانية والطب السيبراني والهوية السيبرانية واللغة السيبرانية..الخ، واتجهت الدول نحو تأسيس مؤسسات بحثية وامنية تهتم بدراسة الفضاء السيبراني وكيفية توظيفه بالشكل الذي يساهم في تحقيق مصالحها السياسية والامنية والاقتصادية .الخ، ليكون التحدي المستقبلي الذي يفرضه الفضاء السيبراني يتمثل في قدرة الدول على التكيف مع التغيير السريع والتحديات التي يفرضها الفضاء السيبراني في المجالات العامة عموماً والمجال الامني خصوصاً، الى جانب امتلاك القدرات والبنى المادية والبشرية التي تمكنها من ان تكون مؤثرة وفاعلة فيه. وهذا التاثير الذي يحمله الفضاء السيبراني لا يقتصر على الواقع الداخلي للدول وانما يمتد الى المحيط الدولي الواسع ليؤثر في اعادة رسم شكل ومضمون النظام الدولي ويحدد اطر جديدة لطبيعة العلاقات الدولية والصراع والاستقرار والامن الدولي.

اولاً:مفهوم الفضاء السيبراني.

تحديد او تعريف المفاهيم من ضروريات العمل البحثي لدورها في تقديم فهم اوسع لموضوع الدراسة، ودراسة الفضاء السيبراني تحتوي لحداثتها العديد من المفاهيم التي لابد من دراستها،ولعل من اهم تلك المفاهيم مفهوم الفضاء السيبراني(cyberspace) جيث يعود أصل كلمة cyber إلى المعنى اليوناني القديم للحكم. بدأ استخدام Cyber في عصرنا من خلال كتاب (نوربرت فينز) * (Cybernetics)* الصادر عام ١٩٤٨، الذي يتعامل مع الحوكمة التي تعتمد على المعلومات [١] .و امام مفهوم الفضاء السيبراني فقد ظهر لأول مرة في ١٩٨٤ [٢] في إحدى روايات الخيال العلمي للكاتب

---

* - نوربرت فينز أو نوربرت وينر: (٢٦ شباط ١٨٩٤ - ١٨ اذار ١٩٦٤)، عالم رياضيات أمريكي، ولد في أمريكا من أبوين يهوديين وكان والده أستاذاً للغات في جامعة هارفرد. في عمر لا يتجاوز ١١ سنة بدء فينر دراساته الجامعية للرياضيات في سنة ١٩٠٩ ومن ثم انتقل إلى هارفرد حيث درس علم الأنواع zoology لكنه انتقل ثانية لجامعة كورنل ليدرس الفلسفة وعاد في نهاية المطاف لجامعة هارفارد حتى يكمل دراسته ببحث حول المنطق الرياضي ثم تحول ليدرس في إنجلترا وألمانيا. اشتغل فينر كمحاضر في جامعة هارفارد وفي شركة جنرال إلكتريك. في الحرب العالمية اشتغل لحساب الجيش وطور الآليات المضادة للطيران أو ما يسمى الدفاع الجوي.https://ar.wikipedia.org/wiki/ /

* - علم التحكم الآلي: أو التحكم والاتصال في الحيوان والآلة هو كتاب كتبه نوربرت وينر ونشر في عام ١٩٤٨إنه أول استخدام عام لمصطلح "علم التحكم الآلي" للإشارة إلى آليات التنظيم الذاتي. وضع الكتاب الأساس النظري للآليات المؤازرة (سواء الكهربائية أو الميكانيكية أو الهيدروليكية) ، والملاحة التلقائية ، والحوسبة التناظرية ، والذكاء الاصطناعي ، وعلم الأعصاب ، والاتصالات الموثوقة. https://en.wikipedia.org/wiki/Cybernetics:_Or_Control_and_Communication_in_the_Animal_and_the_Machie

[1] - Jovan Kurbalija , Different prefixes, same meaning: cyber, digital, net, online, virtual, e-, 17 Apr 2015, https://www.diplomacy.edu/blog/different-prefixes-same-meaning-cyber-digital-net-online-virtual-e.

[٢] -Jason Whittaker, The cyberspace, handbook, *Routledge, Taylor & Francis Group*, 2OO4. Book Description, https://www.routledge.com/The-Cyberspace-Handbook-1st-Edition/Whittaker-Curran/p/book/9780415168366.

الامريكي الكندي(ويليام فورد جيبسون) [*] والتي تحمل اسم (نيورومانسر) Neuromancer [٣]،وهي رواية خيالية علمية ، وصف جيبسون الفضاء السيبراني بأنه إنشاء لشبكة كمبيوتر في عالم مليء بالكائنات الذكية المصطنعة[٤]، وكذلك يصف جيبسون الفضاء السيبراني بانه هلوسة توافقية يمر بها المليارات من الناس يومياً ، وبالتالي يشير إلى مساحة غير حقيقية مشتركة بين الجميع. وبشكل أكثر تحديداً ، يتحدث عن تمثيل رسومي للبيانات الذي يظهر بالتجريد من كل كمبيوتر، يأتي المرء ليكون في الفضاء السيبراني عن طريق تشغيل وبالتالي إنتاج انتقال فوري إليه. بمجرد الوصول إلى هناك ، يمكن للناس الاستمتاع بالبهجة الجسدية للفضاء السيبراني، على الرغم من أنها مربكة إلى حد ما ، إلا أنها وصفات قوية[٥].والفضاء السيبراني مساحة ثلاثية الأبعاد من "التعقيد اللامتناهي" ، يتم إنشاؤها إلكترونياً ، حيث يتصل المشاركون ببعضهم البعض من خلال أجهزة الكمبيوتر، وبالتالي فإنه يقدم تمثيلاً عقلياً للبيانات والمعلومات المخزنة في أعماق أنظمة المعلومات للبشرية جمعاء ، والتي تناسب أجيال مستخدمي الإنترنت[٦].وياتي الفضاء السيبراني نفسه من علم التحكم الآلي،الذي وضعه (نوربرت فينز) ،والذي يُشتق بدوره من الكلمة اليونانية القديمة (kybernētēs) ،والتي تعني موجه الدفة (steersman) أو الحاكم أو الطيار.[٧]، لدراسة التغذية المرتدة والاتصالات والتحكم، والتي تشير إلى حقيقة أن المحركات التوجيهية للسفينة هي بالفعل واحدة من أقدم وأشهر أشكال آلية التغذية المرتدة[٨].وبالاضافة الى ذلك يعد الفضاء السيبراني مجال عالمي ضمن بيئة المعلومات يتكون من شبكة مترابطة من البنى التحتية لتكنولوجيا المعلومات بما في ذلك الإنترنت وشبكات الاتصالات وأنظمة الكمبيوتر والمعالجات المدمجة ووحدات التحكم. نشأ المصطلح في الخيال العلمي ، حيث يتضمن أيضاً أنواعاً مختلفة من الواقع الافتراضي وهي تجربة "الوجود" في الواقع البديل ، أو "الوجود" المحاكي في مثل هذا الواقع[٩]. من جهة اخر يُعد الفضاء السيبراني امتداد لفكرة الواقع الافتراضي، ويتألف الفضاء السيبراني من أجهزة كمبيوتر واتصالات وبرامج وبيانات في شكل أكثر تجريدي. في صميم الفضاء السيبراني توجد المصفوفة أو الشبكة التي تنضم جميع أجهزة الكمبيوتر والهواتف على الأرض، وتتكون عن طريق الاتصالات اللاسلكية والهاتفية والخلوية مع مرسلات الموجات الدقيقة التي تنقل المعلومات إلى المدار وما بعده. في القرن العشرين ، كان الوصول إلى الشبكة متاحاً فقط عبر جهاز كمبيوتر ، باستخدام جهاز يسمى مودم لإرسال المعلومات وتلقيها، ولكن في العام ٢٠١٣ ، اصبح بالامكان الدخول الى الشبكة مباشرة باستخدام دماغك والمقابس العصبية وبرامج الواجهة المعقدة التي تحول بيانات الكمبيوتر. في العديد من الأماكن ، تتم الإشارة إلى الأصل العسكري لواجهات الفضاء السيبراني[١٠].

و الفضاء السيبراني هو أكثر من مجرد إنترنت. يشير إلى بيئة الإنترنت حيث يشارك العديد من المشاركين في التفاعلات الاجتماعية ولديهم القدرة على التأثير على بعضهم البعض. يتفاعل الناس في الفضاء السيبراني من خلال استخدام الوسائط الرقمية. أمثلة على تفاعلات الفضاء السيبراني هي من خلال مواقع الشبكات الاجتماعية القائمة على الإنترنت مثل

---

* -ويليام فورد جيبسون: (ولد في ١٧ اذار عام ١٩٤٨) هو روائي أمريكي كندي له طابع خيالي تأملي، ويُدعى "بالرسول الأسود. أدخل جيبسون مصطلح الفضاء السيبراني في قصته القصيرة "الكروم المحترق" التي صدرت عام ١٩٨٢ ثم أشاع هذا المفهوم في روايته الأولى نيورومانسر التي صدرت عام ١٩٨٤. في تخيل الفضاء السيبراني، قام جيبسون بأول وصف لعصر المعلومات وذلك قبل ظهور الإنترنت في تسعينيات القرن العشرين. وكان له الفضل أيضاً في التنبؤ بازدهار تلفزيون الواقع وإرساء المفاهيم الأساسية المرتبطة بالنمو السريع للبيئات الافتراضية مثل ألعاب الفيديو والشبكة العنكبوتية العالمية،https://ar.wikipedia.org/wiki/

[3] -Christian Ponti, Cyberspace
A Feasibility Study, https://www.inf.usi.ch/faculty/lanza/Downloads/Pont07a.pdf,
Wei Qi, Cyberspace and Political Participation in Contemporary China A Preliminary Assessment Based on Two Case Studies, lund university: Centre for East and South-East Asian Studies, 2005, p4.

[4] - Jennifer Bussell, Cyberspace Communction ,https://www.britannica.com/topic/cyberspace.

[5] -Cyberspace, https://www.encyclopedia.com/science-and-technology/computers-and-electrical-engineering/computers-and-computing/cyberspace.

[6] - Frédérick Douzet, Understanding Cyberspace with Geopolitics, https://www.cairn-int.info/article-E_HER_152_0003--understanding-cyberspace-with-geopolitic.htm.

[7] - The Difference Between Cyberspace & The Internet, https://www.cybersecurityintelligence.com/blog/the-difference-between-cyberspace-and-the-internet-2412.html.

[8] - Jason Healey, From Cybernetics to Cyberspace, Jan. 21, 2019, https://www.airforcemag.com/article/from-cybernetics-to-cyberspace.

[9] - https://www.newworldencyclopedia.org/entry/Cyberspace.

[10] - David G.W. Birch & S. Peter Buck, Hyperion, What Is Cyberspace?, http://project.cyberpunk.ru/idb/what_is_cyberspace.html

Facebook و Twitter و Instagram ، يمكن للأشخاص البقاء على اتصال بأحبائهم (مثل العائلة والأصدقاء) ومجتمعهم الأكبر (مثل الأقارب البعيدين وزملاء سابقين) ، وحتى تكوين صداقات جديدة عبر الإنترنت ، عندما يكون الأشخاص متصلين بالإنترنت ، ينخرط معظمهم في أنشطة تترك بصمة رقمية. تشير البصمة الرقمية إلى جميع المعلومات الموجودة على الإنترنت عن الشخص ؛ يتم نشره بواسطة هذا الشخص أو غيره ، عن قصد أو عن غير قصد. تترك هذه المعلومات علامة دائمة حيث يمكن للآخرين استردادها واسترجاعها ونقلها بسهولة. يمكن استخدام البصمة الرقمية من قبل أرباب العمل والجامعات المحتملين الباحثين عن معلومات حول الموظفين والطلاب المحتملين [١١].

في الثقافة الشعبية في التسعينيات ، تم استخدام الفضاء السيبراني كمصطلح لوصف "الموقع" الذي يتفاعل فيه الأشخاص بعضهم مع البعض الاخر أثناء استخدام الإنترنت. وهو المكان الذي تحدث فيه الألعاب عبر الإنترنت ، وأرض غرف الدردشة ، وموطن محادثات الرسائل الفورية. بهذا المعنى ، يمكن القول أن موقع الألعاب أو غرفة الدردشة نفسها "موجود" في الفضاء السيبراني. وايضاً أصبح الفضاء السيبراني موقعاً مهماً للمناقشات الاجتماعية والسياسية ، في أواخر القرن العشرين وأوائل القرن الحادي والعشرين مع الظهور الشعبي للوحات المناقشة والمدونات المستندة إلى الويب، حيث عادةً ما يتم إنتاج المدونات بواسطة الأفراد الذين يدونون كتاباتهم الشخصية وكثيراً ما يقدمون تعليقات تشغيل وروابط لمواقع أخرى على الويب يرون أنها ذات أهمية. مع ظهور برمجيات التدوين ، حتى الأشخاص الذين ليسوا على دراية ببرمجيات الويب يمكنهم إنشاء مدونة خاصة بهم. وبالتالي ، يمكن النظر إلى المدونات على أنها تقدم فرصة للمناقشة العامة في الفضاء السيبراني غير متاحة في العالم خارج الإنترنت. وفي وقت مبكر من تطور الإنترنت ، في منتصف التسعينيات ، اعتقد العديد من المستخدمين أن عالم الفضاء السيبراني يجب أن يكون خالياً من وجود الحكومات الوطنية. اقترح (جون بيري بارلو)* إعلان استقلال الفضاء السيبراني الذي اكد فيه يجب على الحكومات الوطنية ان لا تلعب أي دور في إدارة الفضاء السيبراني. وجادل بأن المجتمع الموجود في الفضاء السيبراني سيضع قواعده الخاصة ويدير النزاعات بصرف النظر عن القوانين والقضاء في أي بلد. كانت حماية حرية التعبير في الفضاء السيبراني ذات أهمية خاصة كونه سوف تمكن من إخفاء الموقع الفعلي والهوية لاي شخص مشارك في اي نشاط في الفضاء السيبراني [١٢]. ليتخذ مفهوم الفضاء السيبراني مع الآنترنت معنى الفضاء الجديد للاتصال، حيث ينشئ الناس عالماً وهو ليس مكاناً واقعياً كما أنه ليس فضاءً حقيقياً ، بل هو مكان خيالي أو وهمي ينشأ من خلال النقر على لوحة مفاتيح الحاسوب التي تسمح بتبادل المعلومات و نقلها بطريقة رقمية، لتشير إلى أشهر تعبير في عصر المعلومات، ليصبح (Cyber) مقترن بكلمة (Space) المفهوم ألاشمل والاوسع من الآنترنت ليضُم كل الاتصالات والشبكات وقواعد البيانات، ويُشير كذلك إلى مجموعة المعلومات المتوفرة الكترونياً ووالتي يتم تبادُلها وتشكيلها في مجموعات بناءً على استخدامها، ويعمل الفضاء السيبراني تحت ظروف مادية غير تقليدية حيث يكون وسيطاً للعمل من خلال أجهزة الكمبيوتر وشبكات الاتصال [١٣].يعرفه فريدريك مايور (بأنه بيئة انسانية وتكنولوجية جديدة للتعبير والمعلومات والتبادل، وهو يتكون أساساً من الآشخاص الذين ينتمون لكل الاقطار والثقافات واللغات والاعمار والمهن المرتبطة ببعضها البعض عن طريق البنية التحتية الاتصالية)، ويعرف الفضاء السيبراني ايضاً بانه (مجال مجازي لانظمة الحاسوب والشبكات الالكتروني حيث تخزن المعلومات الكترونياً وتتم الاتصالات المباشر على الشبكة ،لذا فهوم عالم غير مادي يشمل مواضيع مثل المعلومات والمعاملات الالكترونية والملكية الفكرية وغيرها من المواضيع ذات الصلة)[١٤].

---

[11] - About the Cyber World, https://ictconnection.moe.edu.sg/cyber-wellness/cyber-wellness-101/about-the-cyber-world.

* - جون بيري بارلو: (٣ تشرين الاول ١٩٤٧ - ٧ شباط ٢٠١٨) شاعراً وكاتباً أمريكياً ، ومربياً للماشية ، وناشطًا إلكترونياً و ناشطاً سياسياً كان مرتبطاً بالحزبين الديمقراطي والجمهوري. كما كان عضو مؤسس لمؤسسة Electronic Frontier Foundation ومؤسسة Freedom of the Press. كان زميلاً فخرياً في مركز بيركمان كلاين لجامعة الإنترنت في جامعة هارفارد ،نشر اعلان الاستقلال الفضاء السيبراني على الإنترنت في ٨ شباط في العام ١٩٩٦ من دافوس، سويسرا. وتم كتابته في الأساس رداً على تمرير قانون الاتصالات لعام ١٩٩٦ في الولايات المتحدة. https://en.wikipedia.org/wiki/John_Perry_Barlow ،

[12] -Jennifer Bussell, Cyberspace COMMUNICATIONS, Op, Cit.

[١٣] - صافية قاسيمي، الفضاء السيبراني و الأغورا الاكترونية_ اشكالية خلق فضاء عمومي افتراضي حسب المنظور الهابرماسي،ص٧-٨، www.google.com

Wei Qi, Cyberspace and Political Participation in Contemporary China
A Preliminary Assessment Based on Two Case Studies, Lund university, Centre for East and South-East Asian Studies, 2005, p4.

[١٤] -بحث الفضاء السيبراني ،مؤتمر حروب الفضاء السبراني ،Seconf.wordpress.com

أولا، يصف الفضاء السيبراني تدفق البيانات الرقمية من خلال شبكة الحواسيب المترابطة: فهو ليس حقيقياً في آن واحد، حيث لا يمكن للمرء أن يحدده مكانياً كجسم ملموس، ومن الواضح أنه حقيقي في آثاره. ثانياً، الفضاء السيبراني هو موقع الاتصالات بوساطة الحاسوب ، التي تم فيها إقامة العلاقات عبر الإنترنت والأشكال البديلة للهوية عبر الإنترنت، مما يثير أسئلة هامة حول علم النفس الاجتماعي لاستخدام الإنترنت، والعلاقة بين الأشكال على الإنترنت و خارج الانترنت من الحياة والتفاعل، والعلاقة بين الحقيقي والظاهري. وكذلك يلفت الفضاء السيبراني الانتباه إلى معالجة الثقافة من خلال تقنيات وسائل الإعلام الجديدة: فهي ليست مجرد أداة اتصال ولكنها وجهة اجتماعية، وهي ذات أهمية ثقافية في حد ذاتها. وأخيراً، يمكن النظر إلى الفضاء السيبراني على أنه يوفر فرصاً جديدة لإعادة تشكيل المجتمع والثقافة من خلال الهويات الخفية، أو يمكن اعتباره تواصل وثقافة بلاحدود وبذلك أصبح مصطلح الفضاء السيبراني وسيلة تقليدية لوصف أي شيء مرتبط بالإنترنت وثقافة الإنترنت المتنوعة) [١٥].

ومن جهة اخرى يثير الفضاء السيبراني قضايا فريدة ، لا سيما فيما يتعلق بالملكية الفكرية وانتهاك حقوق النشر ، وقد يتطلب نماذج جديدة للتجارة. علاوة على ذلك ، أصبح الفضاء السيبراني منطقة فريدة لتطوير العلاقات والمجتمعات البشرية. في حين يجادل البعض بأن هذه الأرضية العالمية للتواصل تساعد على تقريب العالم معاً ، ويشير آخرون إلى أن الناس سوف يستمرون في الارتباط الضيق مع أولئك الذين لديهم اهتمامات ووضع اقتصادي واجتماعي مماثل. ومع ذلك ، أصبح الفضاء السيبراني ، إلى حد كبير عبر الإنترنت ، أرضية مشتركة للاتصال السريع للأفكار والقيم، و هو مساحة محايدة تسمح بالاتصال السريع بالأفكار ، فإن استخدام هذه المساحة سيحدد قيمته وفائدته للبشرية. ، خاصة وأنه يربط البشرية جمعاء في علاقات مترابطة لا تنفصم ، فإن الاستخدام الحر لهذه المساحة يتطلب أيضاً الاستخدام المسؤول من أجل ضمان قيمته في سعي البشرية الشامل للحرية و السعادة،ويكشف عن الحاجة إلى منظور قائم على القيمة لاستخدام هذه التكنولوجيا[١٦].ومن خلال ماذكر اعلاه يمكن تحديد الفضاء السيبراني بالتالي [١٧]:

١- المساحة غير المادية التي أنشأتها شبكات الكمبيوتر ، حيث يمكن للأشخاص التواصل بطرق مختلفة..

٢- تتكون هذه المساحة غير المادية من أجهزة الكمبيوتر وأنظمتها وبرامجها والمستخدمين مثل المبرمجين ومحللي البيانات وفنيي الكمبيوتر ، على سبيل المثال لا الحصر.

٣- يستخدم مصطلح الفضاء السيبراني بالاقتران مع الواقع الافتراضي ، يحدد المكان الخيالي حيث توجد الأشياء الافتراضية.

٤- يعد شبكة الترابط بين البنى التحتية لتكنولوجيا المعلومات ، والتي تشمل الإنترنت وشبكات الاتصالات وأنظمة الكمبيوتر والمعالجات وأجهزة التحكم المضمنة.

٥- يشير المصطلح إلى البيئة التي يحدث فيها التنمر عبر الإنترنت .

٦- يعد الفضاء السيبراني المساحة التفاعلية التي تم إنشاؤها للتفاعل والتبادل على الإنترنت.

٧- الفضاء السيبراني هو البيئة النظرية التي يحدث فيها الاتصال عبر شبكات الكمبيوتر.

٨- الفضاء السيبراني هو البيئة الافتراضية حيث يحدث الاتصال الرقمي عبر شبكات الكمبيوتر .

٩- يستخدم مصطلح الفضاء السيبراني لوصف الشبكة الافتراضية العالمية للأجهزة الرقمية المتصلة.

١٠- أصبح مصطلح الفضاء السيبراني مرادفًا للإنترنت و / أو شبكة الويب العالمية.

١١- يتميز الفضاء السيبراني باستخدام الإلكترونيات والطيف الكهرومغناطيسي لتخزين البيانات وتعديلها وتبادلها عبر أنظمة الشبكات والبنى التحتية المادية المرتبطة بها.

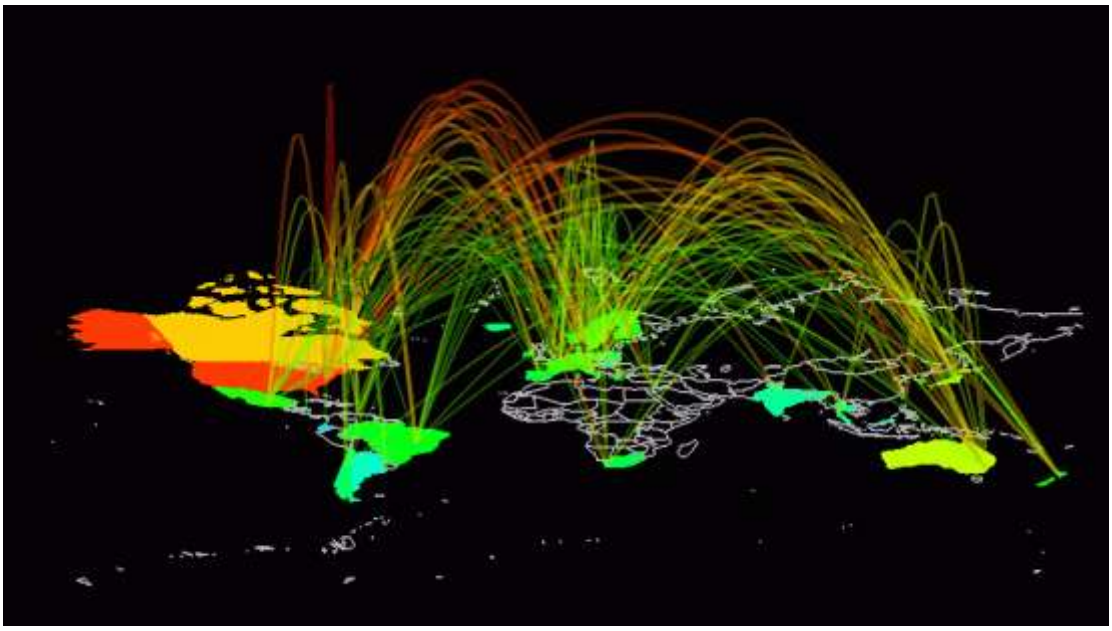
١٢- يمثل الفضاء السيبراني البيئة التي تم إنشاؤها بواسطة الروابط الملموسة مثل الكمبيوتر ، وغير الملموس مثل التطبيقات والخدمات ، والشبكات مثل الإنترنت والاتصالات.

---

[15] -Cyberspace,https://en.wikipedia.org/wiki/Cyberspace

[16] - https://www.newworldencyclopedia.org/entry/Cyberspace

[17] - https://www.igi-global.com/dictionary/cybersecurity-new-challenge-information-society/6619



صورة للفضاء السيبراني

Atlas cyber space , https://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/geographic.html

ثانياً: مفهوم الامن السيبراني.

ما الأمن السيبراني؟ ما يبدو وكأنه سؤال بسيط في قلب التحدي السياسي الذي أصبحت عليه هذه القضية. يتجلى في الصعوبات التي يعترف بها العديد من الجهات الحكومية عندما يتعلق الأمر بالموافقة على التعاريف الرسمية ، الأمن السيبراني من الصعب تحديده وهو محل نزاع سياسي في الساحات الوطنية والدولية[١٨].

يوجد اكثر من (٤٠٠)مفهوم للامن السيبراني تم تصنيفها بواسطة مجموعة متنوعة من الجهات الفاعلة ، بما في ذلك الحكومات والشركات والمنظمات الدولية والمجتمع التقني والمجتمع المدني. تؤثر تهديدات الأمن السيبراني على النظام البيئي للإنترنت بأكمله ، بما في ذلك البنية التحتية المادية والبرامج / الأجهزة والتطبيقات. يتعلق الأمر بحماية المعلومات التي نشاركها ونحتفظ بها عبر الإنترنت وفي الفضاء السيبراني ، بما في ذلك الاتصالات والمعلومات المالية والسجلات الطبية وبيانات الملكية الى الخ. بعض هذه التهديدات لها تأثيرات أكثر بكثير من إغلاق موقع أو الوصول إلى البيانات. يمكن أن يكون لها آثار خطيرة على حياة الناس - من المحامين والصحفيين والمستهلكين[١٩].

وفقًا للاتحاد الدولي للاتصالات ، يشير الأمن السيبراني إلى مجموعة الأدوات والسياسات ومفاهيم الأمن ،و الضمانات الأمنية و المبادئ التوجيهية و نهج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات والضمان والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية والمنظمة وأصول المستخدم. تشمل المنظمة و أصول المستخدم أجهزة الحوسبة المتصلة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات ومجموع المرسل و / أو المعلومات المخزنة في البيئة السيبرانية. يسعى الأمن السيبراني إلى ضمان تحقيق وصيانة الخصائص الأمنية لأصول المنظمة والمستخدم ضد المخاطر الأمنية ذات الصلة في البيئة السيبرانية- الإنترنت. يمكن أيضاً وصف الأمن السيبراني بأنه مجموعة التقنيات والعمليات والممارسات المصممة لحماية الشبكات وأجهزة الكمبيوتر والبرامج والبيانات من الهجوم أو الضرر أو الوصول غير المصرح به. يلاحظ الاتحاد الدولي للاتصالات أيضاً أن الأهداف العامة للأمن السيبراني هي: التوفر ؛ النزاهة (والتي قد

[18] - Myriam Dunn Cavelty and Florian J. Egloff, The Politics of Cybersecurity: 37 Balancing Different Roles of the State, Center for Security Studies, ETH Zürich, St Antony's International Review 15 no.1 (2019),P27.

[19] -Cybersecurity and Human Rights, https://www.publicknowledge.org/cybersecurity-and-human-rights/

تشمل المصداقية وعدم التنصل) والسرية. من أجل فهم مفهوم الأمن السيبراني بشكل كامل ، سنقوم بفحص مختلف مكونات الأمن السيبراني والتدابير الواجب اتخاذها لضمان لتأمين الفضاء السيبراني [٢٠].

ينظر للامن السيبراني بانه ممارسة تأمين الشبكات والأنظمة وأي بنية تحتية رقمية أخرى من الهجمات الخبيثة. من المتوقع أن تتجاوز الأضرار الناجمة عن الجرائم السيبرانية مبلغاً مذهلاً يبلغ اكثر(٦) تريليون دولار بحلول عام ٢٠٢٣ ، فلاعجب أن تستثمر البنوك وشركات التكنولوجيا والمستشفيات والوكالات الحكومية وكل قطاع آخر تقريباً في البنية التحتية للأمن السيبراني لحماية ممارسات أعمالهم والملايين من العملاء الذين يثقون بهم. ما هي أفضل استراتيجية للأمن السيبراني؟ تتضمن البنية التحتية الأمنية القوية طبقات متعددة من الحماية موزعة عبر أجهزة الكمبيوتر والبرامج والشبكات الخاصة بالشركات. مع وقوع هجمات سيبرانية في كل (١٤)ثانية ، يجب أن تعمل جدران الحماية وبرامج مكافحة الفيروسات وبرامج مكافحة برامج التجسس وأدوات إدارة كلمات المرور في وئام لتتفوق على المجرمين السيبرانيين المبدعين بشكل مدهش. مع وجود الكثير من المخاطر ، ليس من المبالغة الاعتقاد بأن الادوات وخبراء الأمن السيبراني بمثابة خط الدفاع الأخير بين المعلومات الأكثر أهمية لدينا والفوضى الرقمية [٢١].لذلك يعرف الامن السيبراني بانه ممارسة الدفاع عن أجهزة الكمبيوتر والخوادم والأجهزة المحمولة والأنظمة الإلكترونية والشبكات والبيانات من الهجمات الخبيثة. يُعرف أيضاً باسم أمن تكنولوجيا المعلومات أو أمن المعلومات الإلكتروني. ، ويشمل مجالات واسعة من النشاطات المختلفة ويمكن تقسيمها خمسة مجالات[٢٢].

١-أمن الشبكة هو ممارسة تأمين شبكة الكمبيوتر من المتسللين ، سواء كانوا مهاجمين مستهدفين أو برامج ضارة انتهازية.

٢- أمن البيانات يركز على إبقاء البرامج والأجهزة خالية من التهديدات.. يبدأ الأمان الناجح في مرحلة التصميم ، قبل نشر البرنامج أو الجهاز بوقت طويل.

٣- أمن المعلومات يحمي سلامة وخصوصية البيانات ، سواء في التخزين أو في النقل.

٤-٠ أمن التشغيلي يشمل العمليات والقرارات للتعامل مع أصول البيانات وحمايتها. الأذونات التي يمتلكها المستخدمون عند الوصول إلى الشبكة والإجراءات التي تحدد كيفية ومكان تخزين البيانات أو مشاركتها تقع جميعها تحت هذه المظلة.

٥- يحدد التعافي من الكوارث واستمرارية الأعمال كيفية استجابة المنظمة لحادث الأمن السيبراني أو أي حدث آخر يتسبب في فقدان العمليات أو البيانات. تملي سياسات التعافي من الكوارث كيفية استعادة المنظمة لعملياتها ومعلوماتها للعودة إلى نفس القدرة التشغيلية التي كانت عليها قبل الحدث. استمرارية الأعمال هي الخطة التي ترجع إليها المنظمة أثناء محاولتها العمل بدون موارد معينة.

٦- عالج تعليم المستخدم النهائي أكثر عوامل الأمن السيبراني التي لا يمكن التنبؤ بها: الأشخاص. يمكن لأي شخص إدخال فيروس إلى نظام آمن عن طريق الفشل في اتباع ممارسات الأمان الجيدة. يعد تعليم المستخدمين حذف مرفقات البريد الإلكتروني المشبوهة ، وعدم توصيل محركات أقراص USB غير المعروفة ، والعديد من الدروس المهمة الأخرى أمراً حيوياً لأمان أي مؤسسة.اما ابرز الاتجاهات في الامن السيبراني ،فيمكن ان نسلط الضوء على ثلاثة اتجاهات تشير إلى الطبيعة المتغيرة للجناة. اولاً اقتصاد الجريمة الاقتصادية السيبرانية الجديد المتزايد. الثانية ، تتلاقى القدرات الجهات الحكومية والمنظمة والجماعات الإجرامية: الجهات الحكومية توظف بشكل متزايد مثل هذا المجموعات باسم "المرتزقة السيبرانيين". ثالثاً ، لأن الدول تطور بسرعة القدرات الهجومية ، التهديد بأن تصبح الأسلحة السيبرانية مكوناً رئيساً في الحرب هو في ازدياد [٢٣].

ثالثا: خصائص الأمن السيبراني.

للأمن السيبراني مجموعة من الخصائص التي تميزه عن غيره من المجالات، أهمها هم:

---

[20] - UNDERSTANDING THE
CONCEPT OF CYBER SECURITY
Policy Competition & Economic Analysis Department,P7.

[21] - https://builtin.com/cybersecurity.

[22] - What is Cyber Security?, https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security.

[23] - Maarten Gehem, Artur Usanov, Erik Frinking, Michel Rademaker, ASSESSING CYBER SECURITY A META-ANALYSIS OF THREATS, TRENDS, AND RESPONSES TO CYBER ATTACKS, The Hague Centre for Strategic Studies,2015,p10.

١- الثقة وعدم الثقة: يمتلك جدار الحماية الخاص بالنظام شبه مرشح إلكتروني لنوع وطبيعة البرامج والتقنيات المسموح بتفعيلها، بحيث يسمح بمرور البرامج التي بالفعل تمتلك الثقة من المستخدم وكذلك المتجر الإلكتروني وتم التأكد من أمان استخدامها، ومنع البرامج الخبيثة من التطفل أو استغلال الثغرات، وهنا يمكن ترجمة فلسفة خاصية الأمن السيبراني، بأنه يتعامل مع كافة البرامج كونها برامج غير جديرة بالثقة، حتى يتم السماح لها بواسطة المستخدم والتأكد من أمانها من خلال مصداقيتها في المتاجر الإلكتروني، فيسمح بمرور ما تم التأكد من سلامته، ويمنع المصادر المجهولة من اختراق النظام.

٢-الحماية من التهديدات الداخلية: أهم خصائص الأمن السيبراني حماية الجهاز من التهديدات الداخلية والتي قد تتم بناء على قلة ثقافة المستخدم أو جهله بسياسات الأمان التكنولوجي، وفيه قد يقوم بالسماح لبرامج مجهولة المصدر أن يتم تفعيلها أو أن يقوم باستخدام أدوات تمس أمن معلوماته أو حساسية مشاركة ما يملكه من معلومات، أو تحتوى إحدى الأدوات التي يقوم باستخدامها على بفيروس خبيث لا يجب أن يحتوى نظامه عليه، حينها يقوم الأمن السيبراني بسرعة تنبيه الفرد أو المؤسسة بالخطر الذي يواجهه ويقوم بمنع حدوث هذا الإجراء في اسرع وقت.

٣-الحماية من التهديدات الخارجية: وفيها يقوم جدار الحماية التابع لنظام الأمن السيبراني بتصفية المخاطر الخارجية التي يسفر عنها التعامل مع الفضاء السيبراني، بداية من مخاطر الرسائل الإلكترونية الخطرة أو الروابط الخبيثة أو الفيروسات أو معالجة الضعف في النظام أو الثغرات التي قد يستغلها طرف ثالث في السيطرة على النظام والتحكم فيه.

٤-رؤية شاملة: تقوم الادوات الخاصة بالأمن السيبراني على منح مستخدمها-أفراد كان أو شركات-رؤية شاملة على ما يحتويه أنظمتهم من نقاط قوة وضعف، بحيث يمكنهم معرفة الثغرات والعمل على حلها بأسرع وقت، مع منحهم اقتراحات تخص الطريقة المثالية لمنع تكرارها مرة أخرى.

٥-مراقبة مستمرة: يقوم الأمن السبيرانية على خاصية المراقبة المستمرة، حيث لا يقوم جدار الحماية الخاص به بالعمل لمرة واحدة أو في ساعات معينة، بل النظام يعمل طوال الوقت بهدف اكتشاف أي خلل بمجرد وجوده والعمل على سرعة إصلاحه ومنعه من إحداث أي ضرر.

٦-الامتثال للسياسات والقوانين: الهدف من الأمن السيبراني في المقام الأول الحفاظ على سرية وخصوصية البيانات والمعلومات، لذلك ليس من الطبيعي أن يتم استغلال الصلاحيات التي تمنح له في سبيل اختراق القاعدة التي من أساسها تم إنشائه، لذلك تعد خاصية الامتثال للقوانين والسياسات التشريعية الخاصة بأمن المعلومات واحدة من أهم خصائص الأمن السيبراني، حيث لا يتاح لمصادر خارجية الاطلاع عما يتم مشاركته من معلومات وبيانات حساسة، أو إساءة استغلالها بأي صورة ممكنة، وتتنوع هذه القوانين طبقاً لنوع وطبيعة المجال الذي يتم فيه تطبيق الحماية السيبرانية.

٧-التنوع: يجب أن يمتلك النظام الخاص بالأمن السيبراني حلول شاملة تتعلق بالتعامل مع الهجمات السيبرانية المختلفة، بحيث لا يكون النظام مفعل للحماية من نوع معين من التهديدات والسماح بأخر، بل عليه أن يحلل ويكتشف ويتعامل ويمنع كل أنواع الهجمات الممكنة والتي تشكل تهديداً على سلامة وأمن المعلومات[٢٤].

رابعاً:اهمية الامن السيبراني.

على الرغم من أن تعزيز الأمن السيبراني يعد مرحلة حاسمة ، إلا أنه من المقترح أن تضع الحكومات خطط عمل وطنية متماسكة للتغلب على التحديات الناشئة في القرن الحادي والعشرين. ويجب أن تكون التطورات الحالية نحو الأتمتة والإنترنت والرقمنة وقابلية التشغيل البيني مقصورة على الأمن بشكل متبادل. هذا هو السبب في أنه لا يمكن فحص التحديات الناشئة للأمن السيبراني إلا بكفاءة من خلال فهم جميع مجالات المخاطر والتهديدات. لا يمكن حل التهديدات بشكل فعال إلا بواسطة صانعي السياسات والاستراتيجيين وأولئك الذين يتحكمون في الواجهة الأمامية للأمن السيبراني لتقليل فرص التهديدات. بحث وبناء القدرات بواسطة الحكومات حول صياغة السياسات وفعاليتها يعد امر مطلوب أيضاً. يجب عليهم صياغة خطط واستراتيجيات متماسكة بطريقة مثمرة للمساءلة والتنفيذ. يجب على الشركات تنفيذ عمليات مصادقة قوية وتجاهل الصحة السيبرانية الأساسية يجعلها مصدراً شائعاً جداً لمخاطر الأمن السيبراني. يجب أن يكون هنالك تحقق مناسب ويجب التحريض عليه لحماية جميع الأجهزة من التهديدات السيبرانية وتقليل التحديات الناشئة للأمن السيبراني. يحتاج قادة التكنولوجيا وخبراء الأمن السيبراني وصناع السياسات والباحثون السيبرانيون أيضاً إلى هيكلة رسائلهم ليس فقط في مجال الأمن السيبراني ، ولكن أيضاً في قطاع تكنولوجيا المعلومات لتجنب الغموض وسوء الفهم[٢٥].

---

[24] - https://www.e3melbusiness.com/blog/cyber-security.

[25] - Iram Zahid, Cybersecurity and its Emerging Challenges in the 21st Century, December 18, 2021, https://www.cyber-insights.org/cybersecurity-and-its-emerging-challenges-in-the-21st-century/.

اما اهم فوائد تطبيق ممارسات الأمن السيبراني والحفاظ عليها ما يلي:
١-حماية الأعمال ضد الهجمات السيبرانية وخروقات البيانات.
٢-حماية البيانات والشبكات.
٣-منع وصول المستخدم غير المصرح به.
٤-تحسين وقت الاسترداد بعد الخرق.
٥-حماية للمستخدمين النهائيين وأجهزة نقطة النهاية.
٦-التدقيق المطلوب.
٧-استمرارية الأعمال.
٨-تحسين الثقة في سمعة الشركة والثقة للمطورين والشركاء والعملاء وأصحاب المصلحة والموظفين [٢٦].

خامساً:أبعاد الأمن السيبراني.

١- الأبعاد العسكرية:

تنشا 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 عالمية.

٢- الأبعاد السياسية:

تقوم الأبعاد السياسية للأمن السيبراني على أساس حماية نظام الدولة السياسي 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.

٣- الأبعاد الاقتصادية:

يرتبط الأمن السيبراني ارتباطا وثيقا 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.

٤- الأبعاد القانونية:

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

٥-الأبعاد الاجتماعية:

تسمح طبيعة الإنترنت المفتوحة عبر شبكات التواصل الاجتماعي لكل مواطن بان 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، والمعتقدات 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 امنه واستقراره على هدم القيم وضياع الهوية الثقافية[٢٧].

سادساً:التهديدات الامنية في الفضاء السيبراني.

على مدى العقدين الماضيين ، تم شن هجمات سيبرانية ضد البنية التحتية الحيوية في جميع الدول المتقدمة ، وتكبد عدد لا يحصى من الشركات خسائر فادحة. هنالك أكثر من(٢٠٠٠) انتهاك مؤكد للبيانات على مستوى العالم كل عام ، مع كل خرق يكلف أكثر من (٣,٩) مليون دولار في المتوسط (٨,١ مليون دولار في الولايات المتحدة الامريكية). منذ عام ٢٠٠٠ ، سرق مجرمو الإنترنت معلومات خاصة لاكثر من ٣,٥ مليار شخص ، أي نصف سكان العالم، يمكن أن تؤثر الانتهاكات والتهديدات الأمنية على أي نظام تقريبا بما في ذلك:

[26] - Sharon Shea, Alexander S. Gillis, Casey Clark, What is cybersecurity?, https://www.techtarget.com/searchsecurity/definition/cybersecurity .
[27] - https://ab7as.net/cybersecurity/.

١-الاتصالات - يمكن استخدام المكالمات الهاتفية ورسائل البريد الإلكتروني والرسائل النصية وتطبيقات المراسلة في الهجمات السيبرانية.
٢-التمويل - بطبيعة الحال ، تعد المؤسسات المالية هدفاً أساسياً للمهاجمين ، وتتعرض أي مؤسسة تعالج معلومات البنوك أو بطاقة الائتمان أو تتعامل معها للخطر
٤-الحكومات - عادة ما يتم استهداف المؤسسات الحكومية بواسطة مجرمي الإنترنت ، للحصول على معلومات المواطنين الخاصة أو البيانات العامة السرية.
٥-النقل - السيارات المتصلة وأنظمة التحكم في حركة المرور والبنية التحتية للطرق الذكية كلها معرضة لخطر التهديدات السيبرانية.
٦-الرعاية الصحية - السجلات الطبية في اي عيادة محلية إلى أنظمة الرعاية الحرجة في المستشفى العام تكون عرضة للهجوم.
٧-التعليم - تتعرض المؤسسات التعليمية وبياناتها البحثية السرية والمعلومات التي بحوزتها عن الطلاب أو الموظفين لخطر الهجوم السيبراني.
إن التحضير والدفاع ضد تهديدات الأمن السيبراني يجب أن يكون أحد أهم المجالات،الهدف الأساس للأمن السيبراني هو حماية البيانات. يشير مجتمع الأمان عموماً إلى مثلث من ثلاثة مبادئ ذات صلة تضمن أمان البيانات ، والمعروف باسم ثالوث وكالة المخابرات المركزية:
١-السرية - ضمان عدم إمكانية الوصول إلى البيانات الحساسة إلا لأولئك الأشخاص الذين يحتاجونها بالفعل ، ويُسمح لهم بالوصول إليها وفقاً للسياسات التنظيمية ، مع حظر الوصول إلى الآخرين.
٢-النزاهة - التأكد من عدم تعديل البيانات والأنظمة بسبب الإجراءات التي تتخذها الجهات المهددة ، أو التعديل العرضي. ينبغي اتخاذ تدابير لمنع الفساد أو فقدان البيانات الحساسة ، والتعافي السريع من مثل هذا الحدث في حالة حدوثه.
٣-التوفر - ضمان بقاء البيانات متاحة ومفيدة لمستخدميها النهائيين ، وعدم إعاقة هذا الوصول بسبب عطل في النظام أو الهجمات السيبرانية أو حتى الإجراءات الأمنية نفسها. ([٢٨]).
اما الجهات الفاعلة في مجال التهديد السيبراني فانها ليست متساوية من حيث القدرة و التطور ، ولديها مجموعة من الموارد ، والتدريب ، ودعم أنشطتهم. يجوز للجهات الفاعلة في التهديد السيبراني تعمل بمفردها أو كجزء من منظمة أكبر (أي برنامج استخبارات الدولة القومية أو الجريمة المنظمة). في بعض الأحيان ، حتى الجهات الفاعلة المتطورة تستخدم أدوات وتقنيات أقل تطورة ومتاحة بسهولة لأن هذه يمكن أن تظل فعالة لمهمة معينة و / أو تجعل من الصعب على المدافعين. اما اهم الادوات التي تستخدم في احداث تهديد للامن في الفضاء السيبراني فهي كالتالي:
١-البرمجيات الخبيثة
وهي البرامج التي تؤدي مهمة ضارة على جهاز أو شبكة مستهدفة ، على سبيل المثال إفساد البيانات أو الاستيلاء على نظام.
٢-التصيد
هجوم عبر البريد الإلكتروني يتضمن خداع مستلم البريد الإلكتروني للكشف عن معلومات سرية أو تنزيل برامج ضارة بالنقر فوق ارتباط تشعبي في الرسالة.
٣-التصيد بالرمح
شكل أكثر تعقيداً من التصيد الاحتيالي حيث يتعرف المهاجم على الضحية وينتحل شخصية شخص يعرفه الضحية ويثق به.
٤-هجوم "رجل في الوسط" (MitM)
حيث ينشئ المهاجم موقعاً بين مرسل الرسائل الإلكترونية ومتلقيها ويعترضها ، وربما يغيرها أثناء النقل. يعتقد المرسل والمتلقي أنهما يتواصلان مباشرة مع بعضهما البعض. يمكن استخدام هجوم MitM في الجيش لإرباك العدو.
٥-حصان طروادة
تم تسميته على اسم حصان طروادة في التاريخ اليوناني القديم ، وهو نوع من البرامج الضارة التي تدخل نظاماً مستهدفاً يشبه شيئاً واحداً ، على سبيل المثال قطعة قياسية من البرامج ، ولكنها تسمح بعد ذلك بإخراج الشفرة الضارة مرة واحدة

[28] -CYBERSECURITY, https://www.imperva.com/learn/application-security/cyber-security/.

داخل النظام المضيف.(هي شفرة صغيرة يتم تحميلها مع برنامج رئيسي من البرامج ذات الشعبية العالية، ويقوم ببعض المهام الخفية، غالباً ما تتركز على إضعاف قوى الدفاع لدى الضحية أو اختراق جهازه وسرقة بياناته)

٦-برامج الفدية

هجوم يتضمن تشفير البيانات على النظام المستهدف والمطالبة بفدية مقابل السماح للمستخدم بالوصول إلى البيانات مرة أخرى. تتراوح هذه الهجمات من الإزعاج منخفض المستوى إلى الحوادث الخطيرة مثل إغلاق مدينة أتلانتا بالكامل لبيانات الحكومة البلدية في عام ٢٠١٨.

٧-هجوم رفض الخدمة أو هجوم رفض الخدمة الموزع (DDoS)

حيث يستولي المهاجم على العديد (ربما الآلاف) من الأجهزة ويستخدمها لاستدعاء وظائف النظام المستهدف ، على سبيل المثال موقع ويب ، مما تسبب في تعطله بسبب زيادة الطلب.

٨-الهجمات على أجهزة إنترنت الأشياء

أجهزة إنترنت الأشياء مثل المستشعرات الصناعية عرضة لأنواع متعددة من التهديدات السيبرانية. يتضمن ذلك المتسللين الذين يستولون على الجهاز لجعله جزءاً من هجوم DDoS والوصول غير المصرح به إلى البيانات التي يتم جمعها بواسطة الجهاز. نظرًا لأعدادها وتوزيعها الجغرافي وأنظمة التشغيل القديمة في كثير من الأحيان ، تعد أجهزة إنترنت الأشياء هدفاً رئيسياً للجهات الفاعلة الخبيثة.

٩-خروقات البيانات

خرق البيانات هو سرقة البيانات من قبل جهة فاعلة ضارة. تشمل دوافع انتهاكات البيانات الجريمة (أي سرقة الهوية) ، والرغبة في إحراج مؤسسة (مثل إدوارد سنودن أو اختراق DNC) ، والتجسس.

١٠-البرامج الضارة على تطبيقات الجوال

الأجهزة المحمولة عرضة لهجمات البرامج الضارة تماماً مثل أجهزة الحوسبة الأخرى. قد يقوم المهاجمون بتضمين البرامج الضارة في تنزيلات التطبيقات أو مواقع الويب للجوال أو رسائل البريد الإلكتروني المخادعة والرسائل النصية. بمجرد اختراق الجهاز المحمول ، يمكن أن يمنح الفاعل الضار إمكانية الوصول إلى المعلومات الشخصية وبيانات الموقع والحسابات المالية والمزيد .

اما مصادر تهديدات الأمن السيبراني فهي تاتي من مجموعة متنوعة من الأماكن والأشخاص والسياقات. تشمل الجهات الخبيثة: الأفراد الذين يقومون بإنشاء ناقلات هجوم باستخدام أدوات البرامج الخاصة بهم.المنظمات الإجرامية التي تدار مثل الشركات ، حيث يقوم عدد كبير من الموظفين بتطوير ناقلات هجوم وتنفيذ هجمات.الدول.إرهابيون.جواسيس المجال الصناعي، جماعات الجريمة المنظمة.المطلعين غير سعداء، القراصنة والمنافسون في العمل [٢٩].

سابعاً-المناهج الدولي للامن السيبراني.

تحتاج الأمم إلى العمل بشكل جماعي للحد من إمكانية التهديد السيبراني. أولا ، يجب أن يتفقوا على قائمة موسعة من قواعد السلوك الدولية. ثانياً ، يجب عليهم المشاركة في معرفة التهديدات والحالة الصحية للانترنت مع الدول الأخرى ذات التفكير المماثل. يجب أن يؤسسوا أيضاً خطوط ساخنة للاستخدام في أوقات الأزمات والتعاون بشأنها والبحث لجعل شبكاتهم أكثر قوة وأجهزة الكمبيوتر لديهم أكثر أماناً. ومن اجل الوصول لذلك لابد من اعتمادة الاليات الاتية:

١- وضع معايير دولية للسلوك. يجب ان تتعاون الامم لمكافحة سوء الاستخدام الإنترنت ، للمساعدة في تطوير ثقافة عالمية للأمن السيبراني ، واتخاذ خطوات أخرى مصممة للحد من المخاطر بما في ذلك تدابير مثل تبادل بيانات الحوادث والانخراط في أفضل الممارسات. ستساعد هذه الخطوات على إنشاء أساس الثقة التي ستقلل من خطر الصراع خلال أوقات التوتر.

٢-ا نشاء أنظمة الإنذار المبكر الدولية.

مثل هذا الانذار سيحذر النظام الدول من المشاكل الناشئة ، مثل الأخطاء في إعلانات (BGP) والاتصالات وانقطاع التيار وتفشي الهجمات الخطيرة. تيار متواصل من المعلومات المشتركة حول وضع الفضاء السيبراني سوف يساعد في طمأنة الدول في أوقات الأزمات. كل دولة مصلحة في السيطرة على الجريمة على أراضيها.إن الجرائم السيبرانية دولية تتطلب تعاون دولي للتعامل معها. المصلحة جماعية للدول الحفاظ على فضاء سيبراني صحي. لذلك يجب على الأمم أن تشارك

29 - CYBER SECURITYINTRODUCTION TO CYBERSECURITY, JUN 16 2021, https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/.

في المناقشات لمعالجة عدم الاستقرار هذا. يمكن للدول أيضا التشارك بنهجا الوطني في التشريعات المتعلقة بأمان الكمبيوتر والاتفاق على مشترك المصطلحات المشتركة لتحسين الاتصالات حول شبكات الحاسوب .

٣- مساعدة العالم النامي. مع صول العالم النامي إلى الإنترنت ،سوف يحتاجون إلى تعلم أهمية إبقاء برامجهم محدثة و توظيف جميع الضمانات التي يتم نشرها بشكل عام في العالم المتقدم. إذا وصلوا إلى الإنترنت بعداد كبيرة دون اتباع على الفور الأمن المعمول به في ذلك ، سوف توفر عدد كبير من الآلات التي يمكن اختراقها بسهولة. هذا هو الوضع الناشئة على طول الساحل الغربي لأفريقيا. تحت سطح البحر يتم تثبيت الكابلات التي توفر وصول بسرعة عالية إلى العديد من البلدان التي من المرجح أن تكون غير مستعد لعواقب ذلك .

٤- تطوير صناعة برامج وأجهزة (هارد وسوف وير) عالية الضمان.، نعتقد أن هنالك قوة الطلب الكامن على الصعيد العالمي للأجهزة البرمجيات عالية الضمان. و. تتطلب المصالح الوطنية تطبيقات عالية لضمان. تقترن بالطبيعة الغرائز التنافسية للدول القومية ، يجب أن ينتج عن ذلك تطوير صناعات محلية جديد عالية الضمان. هذه الصناعات لديها القدرة على الحد من البطالة وزيادة الإيرادات الضريبية وتكون محرك إيجابية للنمو الاقتصادي العالمي.

٥-الدور الدبلوماسي: يمكن ان تلعب الدبلوماسية دوراً مهم في تحقيق ما ذكر اعلاه ، وبالفعل تم اتخاذ الاجراءات المطلوبة حيث اتخذت بالفعل خطوات هامة لتطوير الأطر القانونية للتعامل مع الجرائم السيبرانية الدولية و شجيع ثقافة الأمن السيبراني وبدء مناقشات حول المعايير لحد من الخطر على البنى التحتية الوطنية الحرجة ، استخدام الإنترنت خلال الحرب ، ومشاركة نهج الأمن السيبراني الوطني ، ومساعدة البلدان العالم النامية ، من بين أمور أخرى. يجب على جميع الدول التشجع على زيادة التزاماتهم بهذه الجهود في هذه المناطق. يمكن أن تكون الدبلوماسية مفيدة للغاية في تجنب الصراع السيبراني ، وإذا حدث ، تقلل تأثيره على الدول في الصراع. يمكن أن يساعد على حماية البنى التحتية للمدنيين والحد من نطاق الهجوم السيبراني[٣٠].

تاسعاً:اجراءات الامن في الفضاء السيبراني.

للوصول الى امن سيبراني مهم ومؤثر لابد من اتبع مجموع من الاجراءات .

١-الحد من المعلومات الشخصية التي يتم مشاركتها عبر الإنترنت.

٢- تغيير إعدادات الخصوصية ولا تستخدم ميزات الموقع.

٣-المحافظة على تطبيقات البرامج وأنظمة التشغيل محدثة.

٤- إنشاء كلمات مرور قوية باستخدام الأحرف الكبيرة والصغيرة والأرقام والأحرف الخاصة. استخدم مدير كلمات المرور وطريقتين للتحقق.

٤-مراقبة النشاط المشبوه الذي يطلب القيام بشيء على الفور ، أو يقدم شيئاً يبدو جيداً بدرجة يصعب تصديقها ، أو يحتاج إلى معلوماتك الشخصية. فكر قبل النقر فوق. عندما تكون في شك ، لا تنقر فوق.

٥- حماية منزلك و / أو عملك باستخدام اتصال آمن بالإنترنت وشبكة Wi-Fi ، وقم بتغيير كلمات المرور بانتظام.

٦-لا تشارك أرقام التعريف الشخصية أو كلمات المرور. استخدم الأجهزة التي تستخدم المسح البيومتري عندما يكون ذلك ممكناً (مثل ماسح بصمات الأصابع أو التعرف على الوجه).

٧-تحقق من كشوف الحساب والتقارير الائتمانية بانتظام.

٨- الحذر بشأن مشاركة المعلومات المالية الشخصية ، مثل رقم حسابك المصرفي أو رقم الضمان الاجتماعي أو رقم بطاقة الائتمان. لا تشارك المعلومات الشخصية إلا على المواقع الآمنة التي تبدأ بـ https: //. لا تستخدم المواقع ذات الشهادات غير الصالحة. استخدم شبكة افتراضية خاصة (VPN) تنشئ اتصالاً أكثر أماناً.

٩-استخدم حلول مكافحة الفيروسات والبرامج الضارة وجدران الحماية لمنع التهديدات.

١٠-نسخ ملفات احتياطي بانتظام في ملف مشفر أو جهاز تخزين ملفات مشفر.

١١-لا تنقر على روابط في نصوص أو رسائل بريد إلكتروني واردة من أشخاص لا تعرفهم. يمكن للمحتالين إنشاء روابط وهمية لمواقع الويب.

١٢-تذكر أن الحكومة لن تتصل بك أو ترسل لك رسالة نصية أو تتصل بك عبر وسائل التواصل الاجتماعي بشأن المدينين بها.

[30] - Les Bloom and John E. Savage, On Cyber Peace, Atlantic council, August 2011, p7.

١٣-ضع في اعتبارك أن المحتالين قد يحاولون الاستفادة من المخاوف المالية من خلال الاتصال بفرص العمل من المنزل وعروض توحيد الديون وخطط سداد قروض الطلاب

اما اثناء التعرض لهجوم سيبراني لابد من عمل التالي:

١-تحقق من بطاقتك الائتمانية وكشوف الحسابات المصرفية بحثًا عن الرسوم التي لا يمكن التعرف عليها.

٢-تحقق من تقارير الائتمان الخاصة بك لأي حسابات أو قروض جديدة لم تفتحها.

٣-كن متيقظًا لرسائل البريد الإلكتروني ومستخدمي الوسائط الاجتماعية الذين يطلبون معلومات خاصة.

٤-إذا لاحظت نشاطاً غريباً ، فحد من الضرر عن طريق تغيير جميع كلمات مرور حساب الإنترنت الخاص بك على الفور.

٥-ضع في اعتبارك إيقاف تشغيل الجهاز المتأثر. اصطحبها إلى أحد المحترفين للبحث عن فيروسات محتملة وإزالة أي فيروسات يعثرون عليها. تذكر: لن تتصل بك الشركة وتطلب التحكم في جهاز الكمبيوتر الخاص بك لإصلاحه. هذه عملية احتيال شائعة.

٦-دع أصحاب العمل أو المدرسة أو النظام الآخرين يعرفون ما حدث.

٧-قم بإجراء فحص أمني على جهازك للتأكد من أن نظامك غير مصاب أو يتصرف بشكل أبطأ أو غير فعال.

٨-إذا وجدت مشكلة ، فافصل جهازك عن الإنترنت وقم بإجراء استعادة كاملة للنظام [٣١].

ثامناً:الفرص الوظيفية في مجال الامن السيبراني.

مع استمرار نمو مشهد التهديدات السيبرانية وظهور تهديدات جديدة - مثل تهديدات إنترنت الأشياء - هنالك حاجة إلى أفراد لديهم وعي بالأمن السيبراني ومهارات في الأجهزة والبرمجيات. وتشمل :

١- كبير مسؤولي أمن المعلومات (CISO) هو الشخص الذي ينفذ برنامج الأمان في جميع أنحاء المنظمة ويشرف على عمليات قسم أمن تكنولوجيا المعلومات.

٢-رئيس مكتب الأمن (CSO) هو المسؤول التنفيذي عن الأمن المادي و / أو الأمن السيبراني للشركة.

٣-مهندسو الأمن مسؤولون عن تخطيط وتحليل وتصميم واختبار وصيانة ودعم البنية التحتية الحيوية للمؤسسة، يحمي مهندسو الأمن أصول الشركة من التهديدات مع التركيز على مراقبة الجودة داخل البنية التحتية لتكنولوجيا المعلومات.

٤-يتحمل محللو الأمن العديد من المسؤوليات التي تشمل التخطيط للتدابير الأمنية والضوابط ، وحماية الملفات الرقمية ، وإجراء عمليات تدقيق الأمن الداخلية والخارجية.

٥-مختبرو الاختراق هم قراصنة أخلاقيون يختبرون أمان الأنظمة والشبكات والتطبيقات ، ويبحثون عن نقاط الضعف التي يمكن استغلالها من قبل الجهات الخبيثة.

٦-صائدو التهديدات هم محللو تهديدات يهدفون إلى الكشف عن نقاط الضعف والهجمات والتخفيف منها قبل أن يعرضوا الأعمال للخطر.

٧-تشمل وظائف الأمن السيبراني الأخرى مستشاري الأمن ، وموظف حماية البيانات ، ومهندسي الأمن السحابي ، ومديري ومحللي عمليات الأمان (SOC) ، والمحققين الأمنيين ، وخبراء التشفير ومسؤولي الأمن [٣٢].

تاسعاً:بناء استراتيجية للامن السيبراني.

يمكن تعريف استراتيجية الأمن السيبراني على أنها خطة تتضمن اختيار وتنفيذ أفضل الممارسات للحماية من التهديدات الداخلية والخارجية.تضع استراتيجية الأمن السيبراني أيضاً أساساً لبرنامج أمان الذي يسمح بالتكيف باستمرار مع التهديدات والمخاطر الناشئة. يعد إنشاء وتنفيذ استراتيجية الأمن السيبراني أكثر أهمية من أي وقت مضى حيث زاد عدد الانتهاكات المتعلقة بالأمن أثناء وباء كورنا بنسبة ٦٠٠٪.علاوة على ذلك ، قفز متوسط مدفوعات برامج الفدية بنسبة ٨٢٪ في عام ٢٠٢١ إلى ٥٧٢ ألف دولار عن العام السابق.ليس هنالك ما يشير إلى تباطؤ هذه الهجمات والأدلة التي تدعم أن الجهات الفاعلة في التهديد ستستمر فقط في مهاجمة الأنظمة الضعيفة. تعد سياسة أمن المعلومات عنصراً هاماً في استراتيجية أمنية فعالة [٣٣].

تتكون إستراتيجية الأمن السيبراني من خطط عالية المستوى لكيفية قيام المؤسسة بتأمين أصولها وتقليل المخاطر السيبرانية. مثل سياسة الأمن السيبراني ، يجب أن تكون استراتيجية الأمن السيبراني وثيقة حية ومتنقلة قابلة للتكيف مع مشهد التهديدات

31 -https://www.ready.gov/cybersecurity.

32 - Sharon Shea, Alexander S. Gillis, Casey Clark,op,CIT.

33 - https://purplesec.us/learn/cyber-security-strategy/.

الحالي ومناخ الأعمال المتطور باستمرار. عادة ، يتم تطوير استراتيجيات الأمن السيبراني برؤية تمتد من ثلاث إلى خمس سنوات ولكن يجب تحديثها وإعادة النظر فيها بشكل متكرر قدر الإمكان.

في حين أن سياسات الأمن السيبراني أكثر تفصيلاً وتحديداً ، فإن استراتيجيات الأمن السيبراني هي مخطط لتوجيه أصحاب المصلحة الرئيسيين. أحد أهم الأهداف لأي استراتيجية للأمن السيبراني تحقيق المرونة الإلكترونية. لكي تكون مرناً ، يجب على المسؤولين أن يتذكروا أن كل مؤسسة فريدة وتتطلب نهجاً مخصصاً للاستراتيجية. يشبه إلى حد كبير الاعتماد على منتج أمني أو بائع واحد للقضاء على جميع التهديدات تماماً ، لا توجد استراتيجية واحدة للأمن السيبراني تلبي احتياجات كل مؤسسة بشكل مناسب.

لتحقيق الهدف النهائي المتمثل في المرونة ، ستتطلب استراتيجية الأمن السيبراني الخاصة تحولاً في العقلية من رد الفعل إلى الاستباقي. بدلاً من التركيز على الرد على الحوادث ، تؤكد الاستراتيجيات الأكثر فاعلية على أهمية منع الهجمات السيبرانية. ومع ذلك ، فإن أي استراتيجية قوية للأمن السيبراني تساهم أيضاً في وضع أفضل للرد على أي هجوم. في حالة تعرض المؤسسة للهجوم، يمكن للاستراتيجية الناجحة أن تحدث فرقاً بين حادثة بسيطة وحادثة كبيرة. عندما يتعلق الأمر بإدارة المخاطر ، فإن النهج الاستباقي دائماً ما يكون متفوقاً على النهج التفاعلي. لكن ان تكون استباقياً ، خاصةً عند اكتشاف تهديدات جديدة واكتشافها بمثل هذا المعدل المثير للقلق ، فإن قول ذلك أسهل من فعله.لسوء الحظ بالنسبة لمعظم المؤسسات وإدارات الأمن السيبراني ، فإن اتباع نهج رد الفعل هو القاعدة.توفر دراسة حديثة أجراها معهد بونيمون ، والتي استطلعت آراء (٥٧٧)من ممارسي أمن تكنولوجيا المعلومات وتكنولوجيا المعلومات في الولايات المتحدة الامريكية، الأرقام للتأكيد على النضال نحو الاستباقية:

اعترف ٦٩٪ من المجيبين بأن نهج شركتهم للأمن هو رد الفعل ومدفوع بالحوادث وأعرب ٥٦٪ من المشاركين عن قلقهم من احتواء البنية التحتية لأمن تكنولوجيا المعلومات للفجوات في التغطية ، ما يسمح للمهاجمين بالالتفاف على دفاعات الشبكة ٤٠٪ من المشاركين لا يتتبعون أو يقيسون وضع أمن تكنولوجيا المعلومات في الشركة.نهج الأمن السيبراني الاستباقي لا يضعك في مقدمة المهاجمين فحسب ، بل يمكن أن يساعدك في الحفاظ على المتطلبات التنظيمية بل وتجاوزها. تقدم الاستراتيجيات الاستباقية الهيكل والتوجيه الذي يساعدك على البقاء مستعداً وتجنب الارتباك الذي قد ينشأ. مع تقليل عدم اليقين والارتباك إلى الحد الأدنى ، تم تحسين تدابير منع الحوادث واكتشافها والاستجابة لها بشكل كبير[٣٤].

عاشراً:موقع العراق في مؤشر الامن السيبراني العالمي.

١-مؤشر الامن السيبراني:

عمل الاتحاد الدولي للاتصالات(ITU) على انشاء مؤشر للامن السيبراني على المستوى العالمي. حيث تم إطلاق مؤشر الأمن السيبراني العالمي (GCI) لأول مرة في العام ٢٠١٥ لقياس مدى التزام ١٩٣ دولة عضواً في الاتحاد الدولي للاتصالات بالاضافة الى دولة فلسطين بمرتكزات الامن السيبراني ، فضلاً عن مساعدة الدول من خلال زيادة الوعي بحالة الأمن السيبراني في جميع أنحاء العالم من خلال تحديد مخاطر الأمن السيبراني والأولويات والموارد ، وقد تكيفت(GCI) أيضاً لتقديم المزيد من تدابير الأمن السيبراني، كذلك يهدف المؤشر إلى فهم التزامات البلدان تجاه الأمن السيبراني بشكل أفضل وتحديد الثغرات و تشجيع دمج الممارسات الجيدة ، وتقديم رؤى مفيدة للدول لتحسين مواقف الأمن السيبراني الخاصة بهم. ورفع مستوى الوعي بين مختلف أصحاب المصلحة بشأن احتياجات التنسيق على المستوى الوطني [٣٥].

طريقة -الإصدار الرابع لمؤشر الامن السيبراني العالمي الصادر في ٢٩-٦-٢٠٢١): لكل من الركائز - (١) القانونية ، (٢) التقنية (٣) التنظيمية (٤) تنمية القدرات و (٥) التعاون - تم تقييم التزام الدولة من خلال سؤال- المسح القائم على الإنترنت ، والذي سمح كذلك بجمع الأدلة الداعمة. من خلال التشاور مع مجموعة من الخبراء ، تم ترجيح هذه الأسئلة من أجل الوصول إلى مجموع نقاط مؤشر [٣٦].

٢-ترتيب الدول في المؤشر

---

34 - Mark Stone, What is a cybersecurity strategy and how can your business develop one?, April 9, 2021, https://cybersecurity.att.com/blogs/security-essentials/cybersecurity-strategy-explained.

35 - Global Cybersecurity Index 2020, International Telecommunication Union Development Sector, ITUPublications,2021,P6.

36 - https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx, تم الاطلاع في ٢٩-٦-٢٠٢١

يختلف ترتيب الدول في مؤشر الامن السيبراني العالمي وفقا لمدى تحقيقها للركائز المطلوبة لبناء امن سيبراني ، حيث تُظهر نتائج المؤشر تحسناً عاماً وتعزيزاً لجميع الركائز الخمس لجدول أعمال الأمن السيبراني ، لكن الفجوات الإقليمية في القدرات السيبرانية لا تزال قائمة . يستند هذا الإصدار من مؤشر الأمن السيبراني العالمي إلى البيانات المبلغ عنها بمستوى قياسي لمشاركة الدول الأعضاء ، من ١٠٥ رد في نسخة ٢٠١٣-٢٠١٤ ، إلى ١٥٠ استبياناً تم إرجاعها في عام ٢٠٢٠[٣٧]، وعند معاينة المؤشر سوف نجد الولايات المتحدة الامريكية قد جاءت بالمركز الاول وقد حصلت على درجة (١٠٠) وجاءت بعدها المملكة المتحدة البريطانية والمملكة العربية السعودية بالمركز الثاني بدرجة (٩٩,٥٤)، جاءت دولة الامارات بالمركز الخامس بدرجة (٩٨,٠٦) وسلطنة عمان بالمركز ٢١ بدرجة (٩٦,٠٤) ومصر بالمركز ٢٣ بدرجة (٩٥,٤٨).

٣- مكانة العراق في المؤشر.

يعد العراق من الدول العديد التي تواجه تحدي الفضاء السيبراني في مختلف مجالاته ومنها المجال الامني ،فحالة الضعف التي يعيشها تعقد المسالة اكبر فهو لايزال يعاني عدم الاستقرار العام ولايمتلك القدرات المطلوبة للتكيف مع تلك التحديات التي يفرضها الفضاء السيبراني ، فمع الانتقال السريع للمجتمعات من الفضاء الحقيقي الى الفضاء الافتراضي وجد العراق نفسه يدخل الى هذا الفضاء الواسع وسريع الحركة دون ان يمر بمرحلة انتقالية ، فالبنى المادية والبشرية في العراق لاتزال غير قادرة على التفاعل الايجابي مع تلك التحديات العديدة للفضاء السيبراني ،وعند البحث في الامكانيات العراقية في مجال الامني السيبراني سوف نجد بان العراق لايزال يحتاج الكثير من الجهد المعرفي والاداري والقانوني والتقني لكي يكون قادر على التاثير في المجال الامني السيبراني من جهة ومن جهة اخرى قادر على حماية أمنه السيبراني من التهديدات السيبرانية ، وعند النظر في المؤشر الامن السيبراني العالمي الذي يعتمد خمسة ركائز للامن السيبراني من خلال تحليل ٨٠ مؤشر فرعي لقياس مستوى الامن السيبراني لكل دولة ،وهذه الركائز هي :

١ . القانونية: التدابير القائمة على وجود المؤسسات والأطر القانونية التي تتعامل مع الأمن السيبراني والجريمة الإلكترونية.

٢-التقنية: التدابير القائمة على وجود المؤسسات الفنية والتعامل مع الأمن السيبراني.

٣-التنظيمية: التدابير القائمة على وجود مؤسسات واستراتيجيات تنسيق السياسات لتطوير الأمن السيبراني على المستوى الوطني.

٤-بناء القدرات: التدابير القائمة على وجود البحث والتطوير والتعليم وبرامج التدريب والمهنيين المعتمدين ووكالات القطاع العام التي تعزز بناء القدرات.

٥-التعاون: التدابير القائمة على وجود شراكات وأطر تعاونية وشبكات تبادل المعلومات.

نجد بان العراق وبالرغم من التحسن الذي حدث في موقعه في مؤشر عام ٢٠١٨ حيث شغل (١٠٧) عالمياً و(١٣) عربيا، فانه تراجع (٢٢) نقطة في مؤشر العام ٢٠٢٠ ليكون (١٢٩)عالمياً من اصل(١٨٤) دولة و(١٧) عربياً بدرجة (٢٠,٧١) ، فضلاً عن تقاعس المؤسسات المعنية بالرد على اجاجات الاسئلة التي وجهت لها من فريق مؤشر الامن السيبراني.

النتيجة الكلية	الاجراءات القانونية	الاجراءات التقنية	الاجراءات التنظيمية	بناء القدرات	جراءات التعاون
20,71	0,00	6,56	7,75	2,14	4,6

Global Cybersecurity Index 2020, International Telecommunication Union Development Sector, ITUPublications,2021,P74.

وعند البحث عن اسباب هذا التراجع سوف نجد بان الجهود الحكومية التي اتخذها العراق في مجال الامن السيبراني لم تستمر وشهدت تراجع والتي شملت الاتي :

١- تراجع دور فريق الإستجابة للأحداث السيبرانية. وهو فريق وطني مشترك مختص بمجال الأمن السبراني والاستجابة للحوادث السبرانية وحماية البنية التحتية للانترنت ونشر الوعي في مجال حماية الخصوصية والحماية الذاتية للافراد والمؤسسات على الانترنت يعمل تحت إشراف مستشارية الأمن الوطني العراقي. يحمل الفريق على عاتقه مسؤولية تأمين

37 - Global Cybersecurity Index 2020, Op.Cit,P8.

و حماية الشبكات ومراكز البيانات الوطنية والمواقع الرسمية التي تعمل في مجال الفضاء السبراني العراقي ويقوم بتنسيق الجهود الوطنية ودعم المؤسسات في القطاعين العام والخاص في حماية نفسها وخدماتها في الفضاء السيبراني،
٢-لايزال قانون جرائم المعلوماتية لم يصوت عليه بالرغم من القراءة الاولى له.
٣- عدد المؤتمرات وورش العمل والندوات عن الامن السيبراني لاتزال محدودة جداً بالمقارنة مع دول الجوار مثل السعودية.
٤- لاتزال الاموال المخصصة للامن السيبرانية قليلة بالمقارنة مع دول الجوار ومنها ايران التي خصصت مليار دولار سنوياً
٤- لاتوجد بنية تحتية مادية وبشرية متكاملة في مجال الامن السيبراني ولاتوجد هيئة وطنية مسؤولة عن الامن السيبراني في العراق.
٥-لانجد للعراق دور في المنتديات الدولية المعنية بالامن السيبراني.

التوصيات

العراق بحاجة للتكيف مع تحديات الفضاء السيبراني في مختلف المجالات ومنها المجال الامني. وذلك من خلال العمل على اجراء الاتي:
١-تأسيس البنية المادية والبشرية المطلوبة للتعامل مع الفضاء السيبراني .
٢- تأسيس هيئة وطنية للامن السيبراني .
٢- تأسيس كليات واقسام علمية في الجامعات العراقية المدنية والعسكرية تختص بالامن السيبراني تمنح درجات علمية في تخصص الامن السيبراني.
٣- بناء مؤسسات امنية سيبرانية مثل (الشرطة السيبرانية ،والمخابرات والاستخبارات السيبرانية، والجيش سيبراني، الخ) من اجل مواجهات التهديدات السيبرانية الداخلية والخارجية.
٤- بناء وعي اعلامي وثقافي حول خطورة التهديدات السيبرانية .
٥- بناء منظومة قانونية وقضائية تتعلق بالجرائم السيبرانية.
٧- المشاركة في الجهود الدولية المتعلقة بالامن السيبراني ، مثل الاتفاقيات الدولية والمؤتمرات التي تعقد حول خطر التهديدات السيبراني وكيفية التعامل معها دولياً.