أفـــــاق التعـاون العربـــي
لحمايـــة الفضـاء السيبرانـــي

د. سوهام بادي
كلية العلوم الإنسانية و الاجتماعية
جامعة العربي التبسي-تبسة
souhem.badi@univ-tebessa.dz

الباحثة. اسماء قرزيز
كلية العلوم الإنسانية و الاجتماعية
جامعة العربي التبسي-تبسة
Guerzize.cne@gmail.com

ملخص:

تعتمد المجتمعات الحديثة بشكل متنامي ومتزايد على تكنولوجيات المعلومات والاتصالات المتصلة بالشبكة العالمية، غير أن هذا الاعتماد المطرد صاحبه مجموعة من التهديدات و المخاطر الناشئة والمحتملة التي تهدد وبشكل أساسي الشبكة وأمن المعلومات والمجتمع المعلوماتي وأطرافه حيث اتسع نطاق انتشار الفيروسات والبرمجيات الخبيثة، والهجوم على الشبكات، وتخريب المعلومات والاستخدام غير المشروع للبيانات الشخصية ونشر المحتوى غير اللائق ، وقد اهتمت كل دول العالم تقريبا باتخاذ كافة الإجراءات والتدابير للتصدي لهذه الظاهرة، حيث أصدرت معظمها قوانين لمكافحة الجرائم المعلوماتية وسوء استخدام تكنولوجيا المعلومات والاتصالات من أجل ضمان أمن المعلومات في الفضاء السيبراني ، وتهدف هذه القوانين إلى حماية تبادل ونقل البيانات وتجريم الاعتداء على البيئة الرقمية ووضع نظام للعقوبات يساهم في ردع المخالفين او المعتدين وتعزيز الثقة في خدمات التكنولوجيا وتطبيقاتها،

وكما هو معروف ان مخاطر هذه الظاهرة بأبعادها المختلفة عابرة للحدود، فلا بد لمكافحتها ومواجهتها، ولما كانت اجهزة وسلطات الامن في اي بلد كان، مرتبطة بحدود صلاحياتها الاقليمية والوطنية، فانه لا يمكن لها تجاوز هذه الحدود والصلاحيات، في سعيها لمكافحة هذه الظاهرة وتطبيق القانون ، لذا لجأت الدول عامة، الى استنباط آليات تعاون، تضمن ملاحقة المجرمين عبر الحدود، عبر التعاون مع الدول الاخرى، على المستويات التشريعية، والقضائية، والتنفيذية،

إن الدول العربية تواجه تحديات كبيرة في الفضاء السيبراني و بإمكانها ان تخلق فرص كبيرة للتعاون البيني على مستوى السياسات والاستراتيجيات في الجانب التقني والتنفيذي والذي يمكن ان يعزز الثقة والأمن بالخدمات الإلكترونية وتنظيم الأعمال والتعاملات الإلكترونية، ويتيح الاستفادة من التطبيقات المتعددة التي تشمل الحكومة الإلكترونية والتجارة الإلكترونية وغيرها والاقتناع بعدم وجود مخاطر تهدد الحقوق والأموال من خلال الرفع من وتيرة التعاون لتحقيق الحماية المطلوبة لمواجهة الأخطار والتهديدات التي تخترق البيئة الرقمية ولا تعرف حدودا بين الدول العربية، خاصة وانه تبدو الحاجة واضحة و ملحة الى اتفاقية عربية للأمن السيبراني، تساهم في دفع الدول العربية، نحو اعتبار الامن السيبراني جزءا لا يتجزأ من مهمات الدفاع المشترك، والاقرار بمسؤولية كل دولة، عن ضمان أمن

شبكة اتصالاتها وبنيتها التحتية، وبالتزامها التعاون مع الدول الاخرى، لاعتماد المعايير والمقاييس الدولية الخاصة، بالحماية والأمن السيبراني .

سنحاول من خلال هذه الورقة البحثية الى القاء الضوء على عدد من المفاهيم والمسائل، التي ترتبط بالأمن والفضاء السيبراني، ورصد أبعادها على المستوى العربي ،والتعرف على مخاطر الامن السيبراني في العالم العربي ،ومحاولة تقديم عرضاً لوسائل تعزيز وتنسيق الجهود والتعاون لمكافحة جرائم الفضاء السيبراني وضمان سلامته.

مقدمة:

مع الاعتماد المتزايد، في حياتنا اليومية، على الأنظمة المعلوماتية، والاجهزة المتصلة بالشبكة العالمية للمعلومات، وتشعب طبيعة هذه الاجهزة، من هواتف محمولة، وأجهزة حواسيب شخصية، يزداد عدد المتصلين بالفضاء السيبراني، حيث يوجد في العالم اليوم حوالي 23 بليون جهاز متصل بالإنترنت، أي أكثر منا كبشر بثلاثة أضعاف! ويتوقَّع أن يصل الرقم إلى أكثر من 30 بليوناً عام 2020م، وأكثر من 75 بليون جهاز في عام 2025م ، وتزداد احتمالات الاعتداءات والجريمة والهجمات الإلكترونية والقراصنة والبرمجيات الخبيثة ،وبات من الضروري توفير أمناً خاصاً، لأننا بدأنا نفقد السيطرة شيئاً فشيئاً.

ان الفضاء السيبراني أصبح جزءاً حيوياً من الحياة المعاصرة، فله دور محوري في ازدهار الاقتصاد، وتطوير التعليم، وتسهيل كثير من الأمور المتعلقة بالحياة اليومية، ولا يزال يَعِدُ بالكثير من الفوائد والفرص. وفي المقابل نجد أن هناك كثيراً من المخاطر التي تهدِّد قدرتنا على الاستخدام الآمن لهذا الفضاء الرحب، فبسبب إمكانات الوصول لشبكة الإنترنت غير المحدودة، أتيحت للجهات التخريبية من منظمات وأفراد، ثغرات ونقاط ضعف تمكنهم من الوصول إلى بيانات الأفراد والشركات والجهات الحكومية وتشويهها أو تدميرها أو سرقتها والمساومة عليها، ولهذا تأتي حماية النظم والبنية الأساسية لتكنولوجيا المعلومات والاتصالات على رأس أولويات الدولة. فالفوائد العظيمة التي يقدمها لنا الفضاء الإلكتروني محفوفة بعدد من التحديات التي قد تهدد البنية التحتية التي تعزز من قدرتنا على الاستخدام الآمن للإنترنت، ولهذا أصبح لزاماً حماية المقدرات المختلفة من الهجمات السيبرانية من خلال ابتكار أساليب حديثة وناجعة للتعامل معها بمنعها واكتشافها والتحقيق فيها.

إن الدول العربية الموقّعة سعياً منها لحماية بيانات ومعلومات شبكتها الإلكترونية من أي اختراقات من جهات أو أفراد أو منظمات ورغبة في تعزيز التعاون كون غالبية الدول العربية اعتمدت في تعاملاتها برامج وأنظمة إلكترونية لتأمين وسلامة وحماية الأمن السيبراني للعمليات الإلكترونية وقدرات الدول للتصدّي على الهجمات الإلكترونية ومنعها، ورغبة منها في تعزيز الأمور المشتركة بين أمن المعلومات والأمن السيبراني المتمثّل في مراقبة في التهديدات الإلكترونية وتحليلها وتبادل المعلومات وإدارة الأزمات وحرصاً لانسجام التنسيق في هذا المجال مع المراكز الوطنية والعربية الإسترشادية لأمن المعلومات.

أهداف البحث:

نهدف من خلال هذا البحث الى :

- التعريف بمفهوم الفضاء السيبراني ودلالاته وبنيته.

- التعرف على الأمن السيبراني وأبعاده ،أهدافه ومؤشراته على المستوى العربي.
- التعرف على وسائل تعزيز وتنسيق الجهود والتعاون العربي لمكافحة جرائم الفضاء السيبراني.

أهمية البحث:

يتناول البحث موضوع يطرح بشدة على الساعة العالمية خاصة مع تزايد الترابط الإلكتروني ،حيث أننا نعيش اليوم مرحلة فريدة من تاريخ البشرية من المنطقي أن تسمى مرحلة "إنترنت الأشياء"، تترابط فيها الأجهزة الحياتية الشخصية إلكترونياً، وتتواصل مع بعضها بعضاً، مرحلة تتوزع فيها معلوماتنا الشخصية وتُخزَّن في أكثر من قاعدة بيانات وأكثر من جهاز، يتحكم بحياتنا بشكل إيجابي من دون شك، لكنه لا يخلو من المخاطر لأنه بات من الممكن الوصول إلى كل معلوماتنا بطرق لا تخطر لنا ببال أثرت سلبا على الحياة في شكلها العام.

أولا: الفضاء السيبراني

ان الثورة التكنولوجية المتقدمة أحدثت تغييرات نوعية في شتى نواحي الحياة المختلفة بحيث زادت الاعتمادية على التقنية بمختلف انواعها والاتصال عبر الانترنت لإنجاز المعاملات اليومية، بل اصبحت متطلبا أساسيا في القطاعين الحكومي والخاص لتقديم الخدمات وانجاز المعاملات، كما أدى هذا التقدم والانفتاح التكنولوجي المتسارع والنمو المطّرد بأعداد المستخدمين الى ايجاد فجوات بين سرعة الانفتاح والحفاظ على أمن المعلومات والذي نتج منه العديد من الآثار السلبية في جوانب مختلفة والمتمثلة بظهور أنماط غير تقليدية من الجرائم وهي ما تسمى بـ «الجرائم الإلكترونية» والتي تُرتكب وتدار من أشخاص أو جماعات يتمتعون بقدر كاف من المهارات للتعامل مع التقنية عبر **الفضاء السيبراني**.

مفهوم الفضاء السيبراني:

تختلف التعريفات حول الفضاء السيبراني على حسب طبيعة كل دولة أو كيان وعلى مدى قدرته على تحديد رؤيته واستراتيجيته للتعامل مع مجال الفضاء السيبراني بشقيه المدني والعسكري وكذلك مدى قدرته على استغلال المزايا ومواجهة المخاطر الكامنة في هذا المجال.

فهناك من عرفه: بأنه عالم افتراضي يتشابك مع عالمنا المادي ، يتأثر به ويؤثر فيه بشكل معقد، حيث تقوم العلاقة بين العالمين على نظرة تكاملية تحمل بين طياتها مزايا ومخاطر لا تتوقف وهناك من وصفه بالأذرع الأربعة للجيوش الحديثة إلى جوار القوات الجوية والبحرية والبرية وخاصة أن الانترنت شهد بداية الحديث عن معارك حقيقية تدور في هذا العالم الافتراضي[1].

كما يعرف على أنه: المجال المادي وغير المادي الذي يتكون من عناصر هي اجهزة الكومبيوتر، والشبكات والبرمجيات وحوسبة المعلومات والمحتوى ومعطيات النقل والتحكم ومستخدمو كل هذه العناصر، حيث تعد كل هذه العناصر العامل المشترك في جميع محاور استخدام الفضاء السيبراني، سواء أكانت الجهات

المستخدمة قادرة على تعظيم قيمتها وقدراتها بما في ذلك رفع كفاءة العنصر البشري أم كانت في مرحلة متأخرة[2]،

حيث عرّفته الوكالة الفرنسية لأمن أنظمة الإعلام (ANSSI)، وهي وكالة حكومية مُكلفة بالدفاع السيبراني الفرنسي على أنّه: "فضاء التواصل المشكّل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية"[3].

نُلاحظ أن هذا التعريف يركز على الجانب التقني للفضاء السيبراني من خلال إدراج مفهوم الربط التقني، مما يجعله يقتصر على أصحاب الاختصاص من التقنيين فقط، دون عامة الجمهور أو حتى الباحثين من تخصصات أخرى، كما أن هذا التعريف يُغفل العامل البشري، والذي يُعد جزءا أساسيا في فهم الفضاء السيبراني.

ويمكن توزيع الاخطار في الفضاء السيبراني انطلاقا من أهدافها على ما يطال الدول، وما يطال الأشخاص، ويندرج في اطار **الفئة الاولى**، كل ما يعرض الأمن القومي، والعسكري، والاقتصادي، والاجتماعي، ويهدد البيئة التحتية والحرجة للدول، وأسواق المال والقطاعات المصرفية، والسلم الدولي، والمنشآت النووية، والمؤسسات الصحية، وقطاعات النقل بكل انواعه: البري والبحري والجوي، ورفاه الشعوب، بينما يندرج في **الفئة الثانية**: سرقة البيانات الشخصية، وتسريبها، واستخدامها دون اذن، ودون وجه حق، وسرقة الأموال، واختراق أنظمة المعلومات، والاعتداء على الملكية الفكرية، والصناعية، والعلامات التجارية، كما تشمل هذه الفئة أيضا: الاحتيال، والبريد غير المرغوب فيه، والجرائم ضد الاطفال، والمحتوى غير المشروع، وغيرها الكثير مما يعتبر جرائم سيبرانية، ضد الاشخاص وضد الاموال.

كما أن عملية تعزيز الجانب الدلالي لهذا الفضاء تستدعي تحليل البنية التركيبية له، إذ يُمكن اعتبارها بنية ذي ثلاث طبقات هي[4]:

شكل رقم01: البنية التركيبية للفضاء السيبراني

1. الطبقة المادية: تشمل معدات الحواسيب، والبرمجيات، والمعدات الضرورية لعملية الربط البيني.
2. الطبقة المنطقية: تشمل مجموع البرامج المترجمة للمعلومة على شكل معطيات رقمية، حيث يتم الانتقال من لغة الإنسان إلى لغة الآلة في شكل خوارزمية، ومنها إلى برامج مطوّرة بلغة البرمجة.

3. الطبقة الإعلامية: وتتمثل هذه الطبقة في البُعد الاجتماعي الذي يُضاف إلى الطبقتين السابقتين، حيث أنه في الفضاء الرقمي يُمكن أن يكون لكل إنسان عدة هويات رقمية (عنوان بريده الالكتروني، رقم هاتفة النقال، صور رمزية على مواقع التواصل الاجتماعي...).

إن موضوع الفضاء السيبراني يبقى واسعاً جداً ويشمل جميع النشاطات السياسية، الاقتصادية، الاجتماعية والأمنية ونظم الاتصالات المتطورة والتعاملات المادية والتحويلات المصرفية الداخلية والعالمية والمعاملات التجارية التي تشمل التوقيع والإثبات الإلكترونيين وتعاملات البورصة.....وغيرها، وهي تمثل المواضيع ذات الصلة بشكل رئيسي في:

- المعاملات الإلكترونية في كافة المؤسسات التجارية وشركات البورصة المحلية والعالمية في مختلف الدول التجارية الكبرى.
- حماية البيانات والمعلومات في المؤسسات العامة والخاصة والفردية من الجرائم السيبرانية التي قد تقع عليها من جراء استعمال الحواسيب والشبكة العنكبوتية.
- الإتصالات الإلكترونية كافة وبالأخص المتعلقة بالأمن الداخلي للدولة، حرية التعبير بوسائل إلكترونية وخاصة وسائل الإعلام ومواقع التواصل الإجتماعي (فيسبوك، تويتر وغيرها من الوسائل).
- حماية حقوق الملكية الفكرية وخاصة للكتاب والشعراء والفنانين الذين يطرحون اعمالهم على الشبكة العنكبوتية وقواعد الإثبات وأصول المحاكمات.
- مكافحة الإرهاب على الشبكة وخاصة نشر الافكار الجهادية والتشجيع على أعمال العنف والقتل أو التهديد، حيادية شبكة الإنترنت، التحقيق الجنائي على الحاسوب.
- المعاملات والتواقيع الالكترونية والاثبات الإلكتروني والتي يستعملها كبار رجال الأعمال (عبر العالم) لتتماشى مع عصر التكنولوجيا والاتصالات ومع العولمة الاقتصادية.

ثانيا: الأمن السيبراني

1.مفهوم الأمن السيبراني:

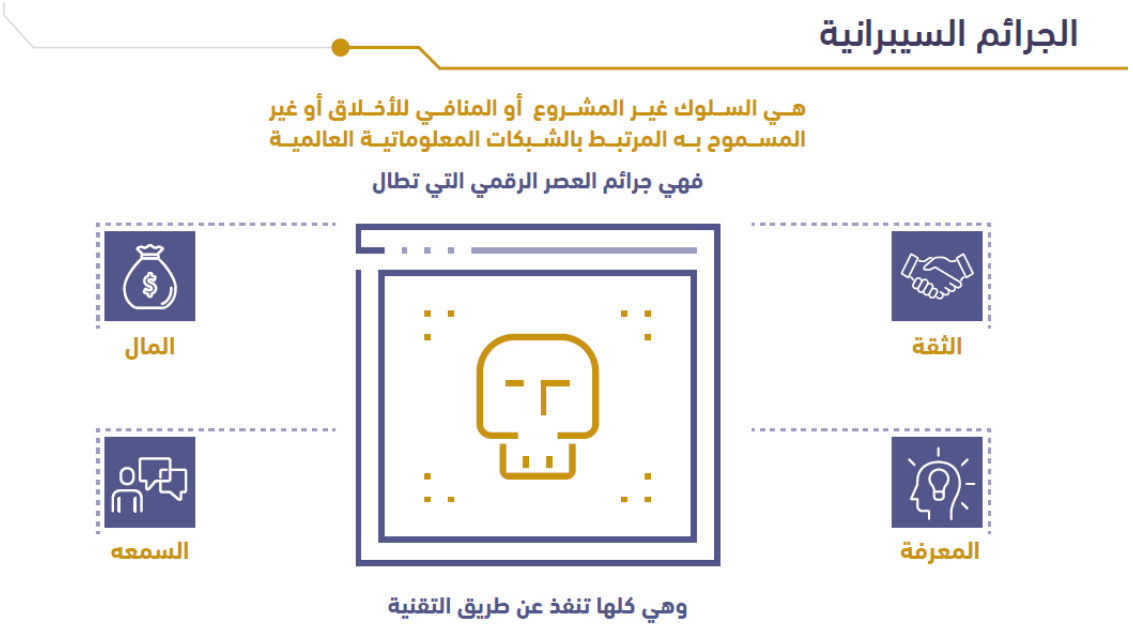
الأمن السيبراني، بحسب التعريف المعطى له، في التقرير الصادر عن الاتحاد الدولي للاتصالات،حول "اتجاهات الاصلاح في الاتصالات للعام 2010-2011" ، هو مجموعة من المهمات، مثل تجميع وسائل، وسياسات، واجراءات امنية، ومبادىء توجيهية، ومقاربات لإدارة المخاطر، وتدريبات، وممارسات فضلى، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين[5] .

الأمن السبراني: هو أمن المعلومات على أجهزة وشبكات الحاسب الآلي، والعمليات والآليات التي يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرّح به أو تغيير أو اختلاف قد يحدث، حيث يتم استخدام مجموعة من الوسائل التقنية والتنظيمية والإدارية لمنع الاستخدام غير المصرّح به، ومنع سوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها[6].

الأمن السيبراني أتى من كلمتي(Cyber security) ، وكلمة **سيبر** لاتينية الأصل ومعناها الفضاء المعلوماتي فيصبح المقصود بالأمن السيبراني أمن الفضاء المعلوماتي وهو تعبير أشمل وأعم من أمن المعلومات لذا يمكن القول أن الأمن السيبراني هو عبارة عن مجموع الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام غير مصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات الشخصية ولحماية المواطنين .[7]

كما يمكن تعريف **الأمن السيبراني**، بانه أمن الشبكات، والأنظمة المعلوماتية، والبيانات، والمعلومات، والأجهزة المتصلة بالأنترنت. وعليه فهو المجال الذي يتعلق بإجراءات، ومقاييس، ومعايير الحماية، المفرو ض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات للحد من آثارها في أقسى و أسوأ الاحوال ويرتبط هذا الأمن، ارتباطا وثيقا، بأمن المعلومات. فالوصول إلى هذه الأخيرة، أو بثها، الاطلاع عليها والمتاجرة بها، أو تشويهها واستغلالها، هو ما يقف، غالب الاحيان، وراء عمليات الاعتداء على الشبكات وعلى الانترنت.

وهذا المصطلح يدل على وجود ما نسمية بالجرائم السيبرانية التي تمثل:



شكل رقم02:الجرائم الالكترونية[8]

صلاحية الأمن السيبراني تعتمد على الركائز الخمسة التالية[9] :

- تطوير إستراتجية وطنية للأمن السيبراني وحماية البنية التحتية للمعلومات الحساسة.
- إنشاء تعاون وطني بين الحكومة ومجتمع صناعة الاتصالات والمعلومات.
- ردع الجريمة السيبرانية.
- خلق قدرات وطنية لإدارة حوادث الحاسب الآلي.
- تحفيز ثقافة وطنية للأمن السيبراني.

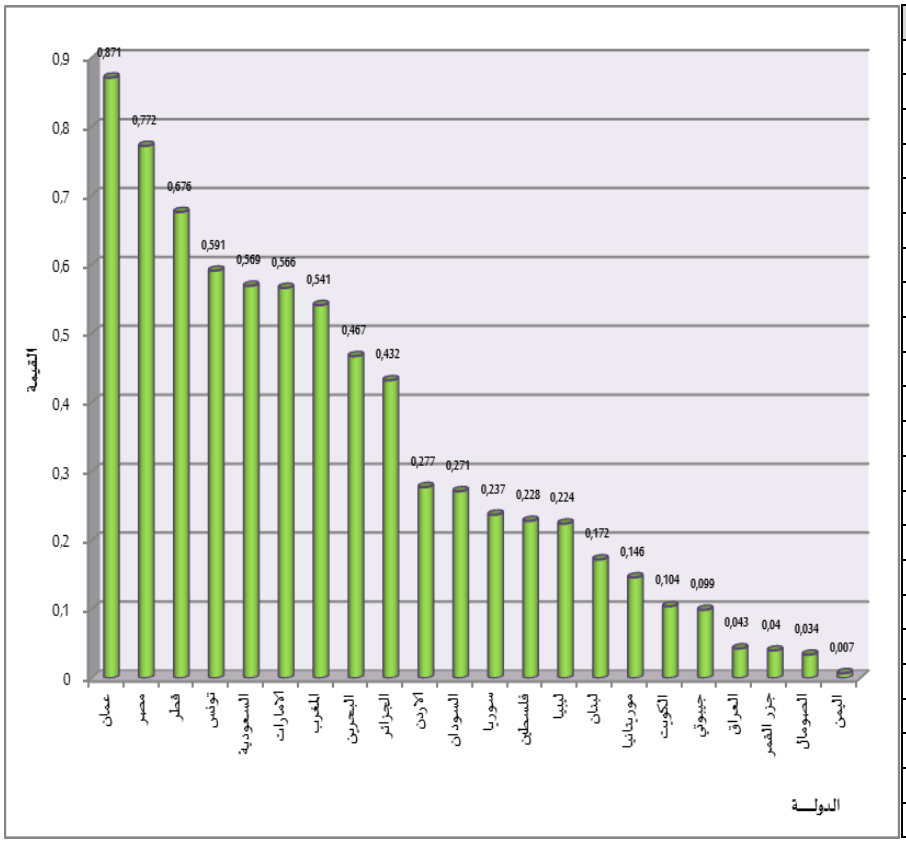
2.الهدف من الأمن السيبراني:

شكل رقم 03 :اهداف الامن السيبراني

الأمن السيبراني له درجات ومكونات مهمة حسب الاستخدام وهي كالتالي[10]:

- **المستوى الأول (إتاحة الوصول إلى المعلومات)** ويعني ذلك من منظور أمن المعلومات منع أو فلترة وعرض المعلومات الملوثة والضارة على الشبكة من المنبع أي قبل نشرها من البداية وهذا يستحيل تطبيقه عملياً نظراً لأن الإنترنت عالم ليس له حواجز أو قانون يحكمه، فكل شيء مباح وجائز نشره وعرضه على الشبكة.
- **المستوى الثاني (الحفاظ على المعلومات)** ويتم ذلك بواسطة أمن المعلومات من خلال عمل الاحتياطات الضرورية لحماية المعلومات المهمة والقيمة والخدمات الأساسية من الهجمات الإلكترونية.
- **المستوى الثالث (السرية)** ويكون ذلك في مجال أمن المعلومات بالنسبة للمعلومات الهامة جداً كالحسابات البنكية والمستندات الخاصة بالجهات السيادية يقصد بها اتخاذ إجراءات وتدابير لمحاولة السيطرة عليها وفق أنظمة مشددة وقوية وهذا ما تنشده العديد من الدول وتسعى إلى تحقيقه في الوقت الحالي.

3: مؤشر الأمن السيبراني في الوطن العربي:



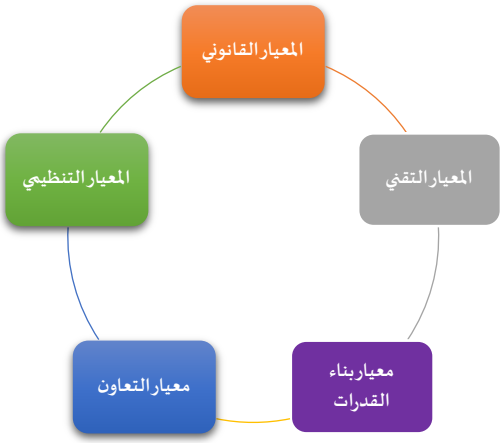
الدولة	Score	الترتيب العالمي	الترتيب العربي
عمان	0.871	4	1
مصر	0.772	14	2
قطر	0.676	25	3
تونس	0.591	40	4
السعودية	0.569	46	5
الامارات	0.566	47	6
المغرب	0.541	49	7
البحرين	0.467	65	8
الجزائر	0.432	68	9
الاردن	0.277	93	10
السودان	0.271	96	11
سوريا	0.237	102	12
فلسطين	0.228	104	13
ليبيا	0.224	105	14
لبنان	0.172	119	15
موريتانيا	0.146	125	16
الكويت	0.104	139	17
جيبوتي	0.099	140	18
العراق	0.043	159	19
جزر القمر	0.040	161	20
الصومال	0.034	162	21
اليمن	0.007	164	22

https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-

جدول رقم 01: ترتيب الدول العربية في مجال الأمن السيبراني

شكل رقم 04: ترتيب الدول العربية في مجال الأمن السيبراني

ويركز مؤشر الأمن السيبراني Global Cybersecurity Index 2017 على أمن المعلومات على أجهزة وشبكات الحاسب الآلي، وضمان تمتين الخصوصية، وحماية سرية المعلومات الشخصية، واتخاذ جميع الإجراءات الضرورية لحماية المواطنين والمستهلكين من مخاطر الفضاء السيبراني. ويعد الاتحاد الدولي للاتصالات هذا المؤشر استنادًا إلى خمسة معايير هي:



شكل رقم 05:معايير الأمن السيبراني

ما نسجله من خلال الجدول رقم 01 أن سلطنة عمان حصلت على المركز الرابع عالميًا، والأول عربيًا، في مؤشر الأمن السيبراني العالمي لعام 2017، الذي أصدره الاتحاد الدولي للاتصالات ، وحازت السلطنة على

0.871 حيث أقرت الحكومة مؤخرا الاستراتيجية الوطنية للأمن السيبراني (أمن المعلومات)؛ وذلك للمضي بتنفيذها خلال السنوات المقبلة في وقت تتزايد فيه التهديدات الأمنية يوما بعد يوم مع التطور الهائل والمتسارع في الاتصالات وتقنية المعلومات. إن هذه الاستراتيجية الجديدة ستغطي الفترة من 2018 الى 2023 وبشكل ينسجم مع التطورات التكنولوجية والمخاطر والتهديدات المتنامية التي يواجهها الفضاء السيبراني العماني؛ حيث انتهت الفترة التي تغطيها الاستراتيجية السابقة والتي كانت تمتد من 2012 الى 2017.

كما احتلت مصر المرتبة الرابعة عشر دوليا و المرتبة الثانية على مستوى الدول العربية ب 0.772 نقطة، حيث تشارك بمجموعة كاملة من مبادرات التعاون، وهي عضو في فريق الخبراء الحكوميين التابع للأمم المتحدة المعني بالأمن السيبراني، وترأست الفريق العامل المعني بحماية الطفل على الإنترنت التابع للاتحاد الدولي للاتصالات، كما تُعد عضو مؤسس في فريق الاستجابة للطوارئ الحاسوبية لمنطقة إفريقيا AfricaCERT، ولديها عدد من الاتفاقات الثنائية والمتعددة الأطراف بشأن التعاون في مجال الأمن السيبراني. كما أطلق المجلس الأعلى للأمن السيبراني، التابع لرئاسة مجلس الوزراء، برئاسة وزير الاتصالات وتكنولوجيا المعلومات، الاستراتيجية الوطنية للأمن السيبراني 2017-2021.

دولة قطر حلت بالمركز الثالث عربيا واحتلت المرتبة 25 عالمياً ب 0.676 نقطة، بفضل الجهود لمواجهة هذه التحديات ومجابهة المخاطر والتهديدات الحالية والناشئة، وانطلاقًا من أهداف الاستراتيجية القطرية للاتصالات وتكنولوجيا المعلومات 2015 الرامية إلى حماية البنية التحتية للمعلومات الحيوية الوطنية وتوفير بيئة آمنة لمختلف القطاعات لتقديم خدمات إلكترونية متكاملة وآمنة؛ تم وضع "الاستراتيجية الوطنية للأمن السيبراني" من قبل "اللجنة الوطنية لأمن المعلومات" التي أنشئت بموجب قرار رئيس مجلس الوزراء رقم (18) لسنة 2013 برئاسة الوزارة لتوفير هيكل حوكمة للتعامل مع قضايا الأمن السيبراني بشكل جماعي على أعلى المستويات الحكومية.

واحتلت تونس المرتبة الرابعة عربيا والاربعين دوليا بمجموع 0.591، حيث قامت ببعث لجنة الأمن السيبراني تتألف من ممثلين عن رئاسة الجمهورية ووزارة تكنولوجيا الاتصالات والاقتصاد الرقمي و وزارة الدفاع الوطني ووزارة الداخلية. ومن ناحية أخرى، أصبحت تونس الآن عضوا في اللجنة الدولية للأمن السيبراني اضافة الى الوكالة التونسية للسلامة المعلوماتية وتعمل اليوم على وضع استراتيجية وطنية للأمن السيبراني تساهم في انشاء وتعزيز فضاء الكتروني آمن .

بينما احتلت السعودية المرتبة 5 عربيا و46 عالميا بمجموع 0.569، حيث تم إنشاء الهيئة الوطنية للأمن السيبراني تجمع أهم قطاعات الدولة الأمنية في مكان واحد (وزارة الدفاع، وزارة الداخلية، الاستخبارات العامة، ورئاسة أمن الدولة) ، وكذلك إنشاء الاتحاد السعودي للأمن السيبراني.

بينما احتلت الامارات المرتبة 6 عربيا و47 عالميا بقيمة 0.566،حيث تقدمت دولة الإمارات بلدان منطقة الشرق الأوسط في إصدار والقوانين والتشريعات اللازمة لضمان الأمن السيبراني، بعدما صدر قانون مكافحة الجرائم السيبرانية في عام 2012، وتعديلاته في عام 2016،كما أنشأت الفريق الوطني للاستجابة لطوارئ الحاسب الآلي عام 2008، وذلك تماشياً مع أفضل الممارسات الدولية، ليكون بمثابة

مركز وطني لتطوير برامج التوعية الأمنية للجمهور، وتطوير برامج التدريب وبناء القدرات للمختصين بأمن المعلومات، بالإضافة إلى تجهيز الفريق ليكون بمثابة خط المواجهة للدفاع، والكشف، وتقديم المشورة، والتصدي للتهديدات الأمنية السيبرانية في الدولة.

اما الجزائر فقد احتلت المرتبة 9 عربيا و68 عالميا بقيمة 0.432.جهود الجزائر في مجال تحقيق الأمن السيبراني تبقى ضئيلة، حيث تركزت أساسا في مجال اتخاذ التدابير القانونية دون غيرها من التدابير الأخرى، ويتضح ذلك من خلال صدور القانون رقم 39-31 المؤرخ في 35 أوت 2009 ،الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والتي تم فيه تحديد الحالات التي تسمح باللجوء إلى مراقبة الاتصالات الإلكترونية، ونجد أيضا انشاء:

-مركز الوقاية من جرائم الاعلام الالي و جرائم المعلوماتية للدرك الوطني.

-المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة للمديرية العامة للأمن الوطني.

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها.

مصلحة الدفاع السيبراني و مراقبة أمن الأنظمة التابعة للجيش الوطني الشعبي.

ويأتي اهتمام الجزائر بإنشاء مثل هذه المؤسسات او الهياكل إلى تزايد معدلات الجرائم الإلكترونية التي أصبحت تشكل تهديدا كبيرا على الأمن الوطني، فقد ارتفع معدل الجرائم الإلكترونية في الجزائر بشكل كبير خلال السنوات الأخيرة.

4.التهديدات التي تتعلق بأمن المعلومات في الوطن العربي:

سيواجه الوطن العربي تهديدات تخص امن المعلومات في السنوات القليلة القادمة وأهمها كما يلي[11]

شكل رقم 05:التهديدات المتعلقة بأمن المعلومات

5.الهجمات الإلكترونية في الوطن العربي:

من خلال تتبع بيانات خريطة كاسبرسكي العالمية للأمن الإلكتروني التي تحدد الدول الأكثر تعرضاً للهجمات الإلكترونية، وتستمد البيانات عبر أدوات متعددة تشمل On-Access Scan و On-Demand Scan وWeb Mail Anti-Viruses، وكذا Vulnerability Scan ، و Intrusion Detection System.

(/https://cybermap.kaspersky.com)

حيث سجلت على سبيل المثال لا الحصر يوم الخميس 22 ديسمبر 2018 أكثر الدول العربية تعرضاً للهجمات الإلكترونية، وجاءت الامارات العربية في صدارة الدول العربية، محتلة المركز 27 عالمياً حيث أعلنت هيئة تنظيم الاتصالات في الإمارات عن إحباط 615 هجمة إلكترونية خلال أول عشرة أشهر من 2017، تتبعها المملكة العربية السعودية في المركز 28 حيث كشف مركز الأمن الإلكتروني السعودي في اخر إحصائية له عن زيادة عدد التهديدات الإلكترونية بالمملكة العربية السعودية في الربع الأخير من 2017 بنحو 7% مقارنة بالربع الثالث من العام نفسه، استهدفت أغلب التهديدات جهات حكومية وقطاعي الطاقة والاتصالات، ثم الجزائر في المركز الثالث عربياً و36عالمياً من حيث التعرض للهجمات الإلكترونية. حيث أن 44% من المستخدمين الجزائريين واجهوا هجمات عبر الانترنت وهي النسبة الأعلى عالمياً.

وجاءت مصر في المركز 43 عالمياً وفقاً لما أظهرته خارطة كاسبرسكي اللحظية، لتصبح رابع أكثر دولة عربية تتعرض لهجمات إلكترونية، وأحرزت مصر تقدماً على صعيد مواجهة جرائم الإنترنت، وهو ما دفعها للمركز 14 عالمياً في مؤشر قياس استعدادات الدول في مجال الأمن السيبراني، وفقاً للاتحاد الدولي للاتصالات، والثاني على مستوى الدول العربية والأفريقية.

تأتي المغرب كخامس أكثر دولة عربية تتعرض لهجمات إلكترونية، وتحتل المرتبة 50 عالمياً، وأشار كاسبرسكي لاب في تقرير إلى أن 53.5% من المستخدمين المغاربة قد واجهوا مخاطر مرتفعة جراء التعرض لهجمات إلكترونية محلياً في 2017.

شكل رقم 06:الدول العربية الاكثر عرضة للهجمات الالكترونية

https://arabic.rt.com/photolines/935147-%D8%A3%D9%83%D8%AB%D8%B1-%D8%A7%D9%84%D8%AF%D9%88%D9%84-%D8%AA%D8%B9%D8%B1%D8%B6%D8%A7-%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9/

ثالثا: اتفاقيات التعاون العربي في مجال الأمن السيبراني

ان التعاون بين الشعوب والدول، ظاهرة تضرب في التاريخ البعيد للاجتماع الانساني. وقد اتخذ هذا التعاون أشكالا مختلفة، وشهد اطرا متنوعة منها: الرسائل، والمواثيق، والبروتوكولات، والشرع، واتفاقات التفاهم، والمعاهدات، والاتفاقات الثنائية، و الاقليمية، و الدولية.

1.أسباب التعاون العربي في مجال الأمن السيبراني[12]:

- أجهزة وسلطات الأمن في أي بلد كان، مرتبطة بحدود صلاحياتها الاقليمية والوطنية، فانه لا يمكن لها تجاوز هذه الحدود والصلاحيات، في سعيها لمكافحة الجريمة وتطبيق القانون. لذا لجأت الدول ، الى استنباط آليات تعاون، تضمن ملاحقة المجرمين عبر الحدود، عبر التعاون مع الدول الأخرى، على المستويات التشريعية، والقضائية، والتنفيذية.
- تشكل التحقيقات وعمليات جمع الادلة، و الملاحقات في مجال الجرائم والاعتداءات السيبرانية، اهم التحديات، في مجال تحقيق الأمن السيبراني، واحد اهم مجالات التعاون، التي تضمن حفظ الادلة وتتبع آثار الاعتداءات، ورصد حركة مرتكبيها. وغالبا ما تفرض طبيعة الجرائم والاعتداءات تعاونا متعدد الاطراف، نظرا للخط الذي تتخذه، والذي يتجاوز حدود اكثر من بلد.
- ان التحقيق في مسائل الامن السيبراني يستدعي تقصي اثر النشاط الجرمي او الاعتداء، عبر مجموعة من المعنيين بإدارة البنية التحتية، مثل مقدمي الخدمات، والشركات التي تدير البنية التحتية، وموقع

الجهاز الخاص بالضحية، كما وجهاز او الاجهزة الخاصة بمصدر أو مصادر الاعتداء، والتي يمكن ان تعمل مع مقدمي خدمات مختلفين، وفي بلدان متعددة، اضافة الى ضرورة الاطلاع على وثائق وسجلات خاصة بالتوصيلات، وبمنفذها.

- انطلاقا من مبدأ سيادة الدولة على اقليمها، لا يمكن الحديث عن تنظيم الفضاء السيبراني، وضمان سلامة الافراد فيه، بعيدا عن دورها الاساسي، في وضع السياسات الخاصة بهذا الموضوع، والسهر على تطبيقها، على المستوى الوطني، اولا، وفي ايجاد الاطر القانونية المناسبة للتعاون مع بقية الدول، في كل مرة تدعو الحاجة الى ذلك
- تتعاظم الاخطار السيبرانية التي تهدد البشرية، وتعجز الارادات والمعالجات المنفردة على التصدي لها، تبدو الحاجة اكثر من ملحة، الى تعاون وعمل جماعي واع وهادف، مؤطر ومقنن، يضمن دورا فاعلا للمجتمع العربي في مواجهة تحديات مجتمع المعرفة ومواكبة تطوراته والافادة منها، باقل قدر ممكن من المخاطر.

2.**أهداف التعاون العربي في مجال الامن السيبراني**:

يمكن تفصيل بعض الاهداف على الشكل الآتي:

- التماشي مع التوجهات والتوصيات الدولية الداعية الى نشر ثقافة الأمن السيبراني، والحفاظ على سلامة البيانات، وحماية البنية التحتية لتكنلوجيا المعلومات والاتصالات.
- تنسيق الجهود العربية، لوضع الاطر التشريعية الملائمة لحماية الفضاء السيبراني، وتشجيع التجارة الالكترونية، وحماية الملكية الفكرية والادبية والصناعية، ما يعزز الانخراط السليم في مجتمع المعرفة.
- المساهمة في دعم السلام والامن الدوليين .
- حماية حق الشعوب العربية في النفاذ الآمن الى المعلومات والمعرفة، والافادة من الامكانات الهائلة لتكنولوجيا المعلومات والاتصالات، حسب ما جاء في المواثيق الدولية.
- تعزيز الجهود العربية في الحفاظ على السلامة والامن، والملاحقة الفاعلة، وتطبيق القوانين، ومنع تحول الفضاء السيبراني، الى ساحة وأرضية للجريمة.
- تعزيز الامن القومي العربي، عبر تفعيل مواجهة الارهاب الالكتروني، والجريمة المنظمة، اللذين يستفيدان من تقنيات المعلومات والاتصالات، واستخدامات الانترنت، بشكل خاص.
- وضع استراتيجية عربية مشتركة للدفاع والامن السيبراني.
- خلق مبادرة عربية، لتطوير قدرات الدفاع السيبراني، وبناء القدرات والتدريب.
- تعزيز الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات، وحماية الأطفال على الإنترنت، ومكافحة جميع أشكال التهديد السيبراني، بما في ذلك إساءة استخدام تكنولوجيات المعلومات والاتصالات.

3.نماذج من التعاون العربي في مجال الامن السيبراني:

أ.المركز العربي الإقليمي للأمن السيبراني (ITU-ARCC)

المركز العربي الإقليمي للأمن السيبراني
ITU - ARAB REGIONAL CYBERSECURITY CENTER

تأسيس المركز

تأسس المركزالعربي الإقليمي للأمن السيبراني (ITU-ARCCمن قبل الاتحاد الدولي للاتصالات (ITU)وسلطنة عمان في ديسمبر2012 ممثلة في هيئة تقنية المعلومات مع رؤية لإنشاء بيئة أكثر أمناً وتعاوناً في مجال الأمن السيبراني في المنطقة العربية وتعزيز دور الاتحاد الدولي للإتصالات في بناء الثقة والأمن في إستخدام تكنولوجيا المعلومات والاتصالات في المنطقة. تماشياً مع أهداف الأجندة العالمية الأمن السيبراني للإتحاد الدولي للأتصالات ولإضفاء الطابع المحلي وتنسيق مبادرات الأمن السيبراني في المنطقه العربيه حيث يتم استضافته وإدارته وتشغيله من قبل المركز الوطني للسلامة المعلوماتيه (OCERT)

اهداف المركز

*الاشراف على تنفيذ البرنامج العام للأمن السيبراني للاتحاد الدولي للاتصالات في جميع أنحاء المنطقة العربية.

*الاستجابة لمتطلبات الأمن السيبراني لأحدث التطورات

*يكون مركزا للإدارة ومنصة لتنفيذ أهداف الأمن السيبراني

*توفير مركز موحد للدول الأعضاء لإدارة برامج مبادرات الأمن السيبراني للدول الأعضاء

*العمل على وضع الأطر والخطط في مجال الامن السيبراني من خلال إجراء الدراسات الإقليمية وعقد ورش العمل. رفع مستوى الوعي والخبرات في الأمن السيبراني في قطاع البنى التحتية للمعلومات.

خدمات المركز

*استراتيجية وحوكمة الأمن السيبراني

*الاستجابة للطوارئ والحوادث السيبرانية

*الضمان والإلتزام بالأمن السيبراني

*الخدمات التقنية وتبادل المعلومات

*بناء القدرات لتعزيز الأمن السيبراني

ب. مشروع الإسكوا لتنسيق التشريعات السيبرانية في المنطقة العربية:

ج. اتفاقيات في اطار جامعة الدول العربية:

4.مجالات التعاون لحماية الفضاء السيبراني العربي[13]:

1. التعاون في مجال رصد وتغطية كل ما يستجد عن الامن والسلامة في الفضاء السيبراني على المستوى التجاري، والاقتصادي، والاكاديمي، والاجتماعي، والقانوني، والتنظيمي.
2. التعاون في مجال بناء قاعدة بيانات للأطر التشريعية والتنظيمية السائدة في الدول العربية الخاصة بإدارة الانترنت، والاتصالات، والتي تمس الامن السيبراني لإرساء بنية تحتية في مجال البرمجيات توفر وسائل وأدوات تقنية من شأنها التصدي للمخاطر السيبرانية المتجددة.

3. التعاون على الأصعدة كافة بين المؤسسات العسكرية والمؤسسات التكنولوجية في مجال البرمجيات لتطوير القدرات العسكرية والحفاظ على سرية المعلومات والبيانات العسكرية ومنع مهاجمتها، بالاضافة للتعاون في مجال تقييم الأطر التشريعية والتنظيمية العربية ومدى كفاءتها لمكافحة جرائم أمن المعلومات.
4. التعاون في مجال عقد ورش عمل، ولقاءات علمية، ومؤتمرات، وندوات، ووضع برامج تدريبية حول مكافحة الجرائم المعلوماتية وعن الاستخدام غير الآمن للأنترنت وأمن المعلومات ونشر الوعي به.
5. التعاون في مجال التدريب حول موضوعات الحكومة الالكترونية، الملكية الفكرية، التجارة الالكترونية، والخدمات الالكترونية.
6. التعاون في مجال نشر الوعي بالأمن السيبراني لفئات مختلفة من المجتمع سواء الطلاب والعاملين بالقانون وصناع القرار في القطاعين العام والخاص والتنسيق مع الجهات الحكومية -العربية لتسويق امن المعلومات .
7. التعاون في مجال التوعية والتثقيف بجرائم الانترنت ووضع خطط توعية شاملة بالأمن السيبراني .
8. التعاون في مجال انشاء قواعد المعلومات الخاصة بالمعايير، والمقاييس المعتمدة في مجال امن المعلومات، والانظمة، وامن الاشخاص الطبيعيين والمعنويين.
9. تبادل الخبرات والاساتذة والمتخصصين بين الدول لتهيئة الفرصة للاستفادة من الخبرات البحثية والقانونية والتقنية بالإضافة لتحفيز الاستثمار في مجال الامن السيبراني للإسهام في تحقيق نهضة تقنية تخدم مستقبل الاقتصاد في المنطقة العربية.

النتائج:

- معظم الدول العربية تفتقر لوجود تشريعات متكاملة للفضاء السيبراني. يوجد تباين بين دول المنطقة في وضع التشريعات السيبرانية.
- تعاني معظم دول المنطقة من بطء إجراءات إصدار القوانين الخاصة بالفضاء السيبراني، وقد يعود السبب إلى تعدد الجهات المعنية بذلك : وزارات العدل والاتصالات والتجارة والداخلية
- تفتقر دول المنطقة العربية الى التعاون القضائي الفعال في مجال تحقيقات الجرائم السيبرانية وعلى الرغم من وجود الاتفاقية العربية المتعلقة بمكافحة جرائم تقنية المعلومات خاصة في فصلها الرابع التي تضمن التعاون القانوني والقضائي ولكن لا زال التعاون غير فعال بينها.
- بعض الاتفاقيات العربية على غرار القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات لم تتضمن نصوصا ذات طابع اجرائي او نصوص حول التنسيق والتعاون بل تضمن فقط قواعد موضوعية تفصل جرائم تقنية المعلومات.
- بالنسبة للإجرام المعلوماتي و السيبراني، يحجم العديد من الدول العربية حتى اليوم، عن وضع قوانين خاصة بالجرائم المعلوماتية و السيبرانية. وكانت تونس اول من بادر الى تعديل قانون الجزاء، في العام 1999 بحيث بات يطاول الجرائم المعلوماتية. ثم اصدر عدد من الدول العربية، قوانين خاصة او

متصلة، هي: قانون جرائم المعلوماتية الصادر عام 2007 في السودان، والذي سبقه القانون الاتحادي رقم 2 للعام 2006 الصادر في دبي، ونظام مكافحة الجرائم المعلوماتية الصادر عن مجلس الوزراء السعودي في 7 مارس 2007 ، و قانون جرائم أنظمة المعلومات المؤقت الصادر عام 2010 في الاردن، والمرسوم السلطاني العماني، الذي عدل القانون الجزائي بحيث يشمل جرائم الحاسوب، وتعميم رقم 4 عام 2006 حول حماية برامج المعلوماتية ومكافحة القرصنة في لبنان.

- يشهد العالم العربي، صعوبات وعراقيل عديدة، على مستوى البيئة التنفيذية، للتشريعات الخاصة بالفضاء السيبراني، ناتجة عن تقاعس الجهات المعنية، عن اصدار المراسيم التنفيذية، والآليات الضرورية، لتطبيق التشريعات. وتعود أسباب ذلك، بشكل أساسي، الى بنية الادارة، وطبيعة عملها، والتي تتجلى غالبا في بطء العمل، أو اللجوء الى اصول اجرائية وادارية، لم ينص عليها القانون.
- تأخر التشريعات المتعلقة بالجريمة السيبرانية وذلك لعدم وجود استقرار سياسي و اعطاء الاولوية لملفات اخرى.

الاقتراحات:

- وضع استراتيجية عربية شاملة للأمن السيبراني بمختلف نواحيها التشريعي والتنفيذي والتنظيمي(تحديد الأهداف، انشطتها، متطلباتها ،آليات تنفيذها)
- تنسيق وتحديث التشريعات بين الدول في مجال الامن السيبراني.
- تبني سياسة تعميم ثقافة عربية تعنى بموضوع حماية الفضاء السيبراني.
- تفعيل الاتفاقيات العربية وتطبيقها و تسريع اجراءات التعاون بين اجهزة التحقيق في الدول عن طريق الربط الإلكتروني بينها
- وضع خطة إعلامية عربية تهدف إلى القيام بحملات تثقيفية واسعة النطاق تشمل جميع فئات المواطنين والمؤسسات التجارية، ودعوة القطاع الخاص للمساهمة الفعالة.
- التعاون في مجال نشر الوعي بالأمن السيبراني لفئات مختلفة من المجتمع سواء الطلاب والعاملين بالقانون وصناع القرار في القطاعين العام والخاص والتنسيق مع الجهات الحكومية -العربية لتسويق امن المعلومات للإدارات والدوائر الحكومية و تدريس مناهج عن "الفضاء الإلكتروني" في المستويات التعليمية المختلفة، وعمل تدريبات للموظفين في المؤسسات المختلفة حول استخدام البيانات بطرق تقلل من احتمالية تعرضها للمخاطر.
- العمل على ايجاد نظام إلكتروني واحد تتعاون فيه كافة الدول العربية لصد الاختراقات الإلكترونية .

خاتمة:

ما يمكن قوله في الأخير إن الدول العربية تواجه تحديات كبيرة في الفضاء السيبراني و هناك فرص كبيرة للتعاون البيني على مستوى السياسات والاستراتيجيات في الجانب التقني والتنفيذي ما بين مراكز الاستجابة لطواري المعلومات والشبكات على المستوى العربي .وهذا ما جعل حاجة الدول العربية لاتفاقية

للأمن السيبراني واضحة، والتي ممكن ان تساهم في دفع الدول العربية، نحو اعتبار الامن السيبراني جزءا لا يتجزأ من مهمات الدفاع المشترك، والاقرار بمسؤولية كل دولة لضمان أمن شبكة اتصالاتها وبنيتها التحتية، وبالتزامها التعاون مع الدول الاخرى، لاعتماد المعايير والمقاييس الدولية الخاصة بالحماية والامن السيبراني. كذلك، يمكن لهذه الاتفاقية ان تؤطر تبادل المعلومات بين الدول الاعضاء، وتبادل المساعدة لمواجهة الهجمات والاحداث السيبرانية. ويبقى أن نرفع من وتيرة هذا التعاون لتحقيق الحماية المطلوبة.

المراجع:

1.بدران،عباس. الحرب الالكترونية: الاشتباك في عالم المعلومات. بيروت: مركز دراسات الحكومة الالكترونية، 2010.

2.شلوش، نورة . القرصنة الالكترونية في الفضاء السيبراني "التهديد المتصاعد لأمن الدول". مجلة مركز بابل للدراسات الانسانية،2018 ،مج:8، ع: 2.

http://bcchj.com/papers/uobj_paper_2018_71850522.pdf

3.يعود استعمال هذا المصطلح إلى "نوبير فينير" (Norbert Wiener) أستاذ بمعهد مساشوسيت التكنولوجي، في كتاب نشره عام 1948 تحت عنوان: " Cybernetic"، وذلك للدلالة على المجال الشامل لنظرية التحكّم والاتصالات لذا الكائنات والآلة.

4.بلفرد، لطفي .الفضاء السيبراني: هندسة وفواعل"، المجلة الجزائرية للدراسات السياسية، ENSSP، ع.5، الجزائر،2016.

5.الأشقر جبور، منى. الأمن السيبراني: التحديات ومستلزمات المواجهة. اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني ،بيروت 27 – 28 أغسطس (آب) 2012.

https://carjj.org/sites/default/files/wrq_ml_lmrkz_-_d._mn_lshqr.docx

6. الربيعة،صالح بن علي بن عبدالرحمن. الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت.

https://edu.moe.gov.sa/jeddah/DocumentCentre/Docs

7. البار ،عدنان مصطفى ، المرحبي، خالد علي . أمن المعلومات و الأمن السيبراني.

https://www.kau.edu.sa/GetFile.aspx?id=287270&fn=Article-of-this-week-DrAdnan-ALBAR-and-MrKhalid-Al-Marhabi-Jan-2018.pdf

8. الربيعة، صالح بن علي بن عبدالرحمن. الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت.

https://edu.moe.gov.sa/jeddah/DocumentCentre/Docs

9.العلي،علي زياد. المرتكزات النظرية في السياسة الدولية.دار الفجر للنشر والتوزيع.

https://books.google.dz/books?id=0Ft9DwAAQBAJ&pg=PA226&lpg=PA226&dq

10. ريان ،محمد سيد . الأمن السيبراني .. رفاهية أم ضرورة ؟!2018

http://asbar.com/ar_lang/?p=30280

11. 5 تهديدات تتعلق بأمن المعلومات يواجهها العالم خلال 2018.

https://www.emaratalyoum.com/technology/electronic-equipment/2017-12-04-1.1049514

12. الاشقر جبور، منى . أهمية الاتفاقية العربية للأمن السيبراني. اللقاء السنوي الرابع للمختصين في أمن وسلامة الفضاء السيبراني،2015.

https://carjj.org/sites/default/files/events

13.الهيئة العربية للبث الفضائي. الأمن السيبيراني.

http://arabcb.org/initiative/733/