

الفضاء الرقمي تحدي أمني جديد واستراتيجيات الدول في تحقيق الأمن السيبراني العالمي

Digital space, a new security challenge, and countries' strategies in achieving global cybersecurity

حبيب عوفي^{1*}

Habib AOUI^{*1}

¹ جامعة الجزائر 3 (الجزائر) habibaoufi25021993@gmail.com

تاريخ النشر: 2022/06/18

تاريخ القبول: 2022/03/03

تاريخ الإرسال: 2022/01/05

Abstract :

The development in the field of information and technological systems has achieved human ambitions from great facilities in his life, including: the speed of transportation, the development of the effectiveness of electronic commerce and the speed of commercial exchanges, the development of the national and national defense system, and this information and technological revolution with its technological means, programs, the Internet and other concepts included Within the term cyberspace, it has become a security challenge that imposes itself on the arena of the international community, due to many considerations, including the difficulty of protecting information, especially sensitive information from it. Achieving global cyber security.

Keywords: cyberspace, cyber security, global cyber peace.

الملخص:

حقّق التطور الحاصل في مجال المعلومات والنظم التكنولوجية طموحات الإنسان من تسهيلات كبيرة في حياته منها: سرعة المواصلات وتطوير فعالية التجارة الإلكترونية وسرعة المبادلات التجارية، وتطوير منظومة الدفاع الوطني والقومي، كما أنّ هذه الثورة المعلوماتية والتكنولوجية بما تحتويه من وسائل تكنولوجية وبرامج وأنترنت وغيرها من المفاهيم المُدرّجة ضمن مصطلح الفضاء السيبراني أصبحت تحديّ أمني يفرض نفسه على ساحة المجتمع الدولي، وذلك لاعتبارات عديدة منها صعوبة حماية المعلومات لاسيما المعلومات الحساسة منها وبالتالي أصبح من الصعوبة بما كان حماية الأمن القومي للدول، مما جعل الدول تفكر في تفعيل آليات دولية تخلق ثقة سيبرانية عالمية تؤدي إلى تحقيق أمن سيبراني عالمي.

الكلمات المفتاحية: الفضاء السيبراني، الأمن السيبراني، السلام السيبراني العالمي.

* المؤلف المرسل.

1. مقدمة

مرّ التاريخ البشري بثورات عديدة آخرها الثورة التكنولوجية التي مهدت لبروز ثورة جديدة وهي ثورة المعلومات التي أدخلت العالم في بيئة جديدة تماما، وهي ثورة لم يشهد التاريخ البشري مثلها وذلك من ناحية سرعة انتشارها، نطاقها الواسع جدا وكذا درجة تعقيدها.

حيث تجسدت هذه الثورة في تطور تكنولوجي ورقمي كبيرين جدا، مزجت بين التطور في المجالات الصناعية والطاقوية والعسكرية والاتصالات والمواصلات، وكذا التكنولوجيات الحيوية والبيولوجية والذكاء الصناعي وتكنولوجيا الروبوتات، تعمل المجالات الأخيرة ضمن قواعد بيانات ضخمة جدا في مجال افتراضي اصطلح عليه بالفضاء السيبراني.

هذا الأخير الذي أصبح تهديدا مباشرا وأكثر خطورة لأمن الدول والمجتمعات، وهو ما يصطلح عليه في الأدبيات السياسية والأمنية بالتهديدات السيبرانية، مما جعل الدول ترتب ضمن أولوياتها الأمنية الإهتمام بمسائل الأمن السيبراني لما له صلة مباشرة بأمن المجتمعات والأمن الوطني والقومي للدول.

حيث يتم الإهتمام السابق الذكر في إطار الاستراتيجيات التشريعية والتقنية وتأمين الحوسبة وسياسة تأمين المعلومات الوطنية وخاصة الأجهزة الاستراتيجية والحساسة منها.

من خلال التقديم السابق يمكن طرح الإشكالية التالية:

كيف يمكن للدول أن تحقق أمنها السيبراني في ظل التحدي الأمني الذي يفرضه الفضاء السيبراني؟

بناء على الإشكالية السابقة يمكن طرح الأسئلة الفرعية التالية:

- 1- ما المقصود أساسا بالفضاء السيبراني؟
- 2- هل هناك حقيقة استراتيجية ذات بعد دولي فعلية لتحقيق الأمن السيبراني العالمي؟

بناء على الأسئلة الفرعية السابقة يمكن طرح الفرضيات التالية:

- 1- الفضاء السيبراني هو استخدام الفضاء الإلكتروني في تبادل المعلومات.
- 2- لا توجد استراتيجية أمنية ذات بعد عالمي لتحقيق الأمن السيبراني العالمي.

أهمية الموضوع:

لدراسة موضوع الفضاء السيبراني أهمية كبيرة جداً، منها على سبيل المثال لا الحصر:

1- يعتبر موضوع الفضاء السيبراني ميدان لصنع التهديدات التي تمس أمن الدول -أمنها الوطني والقومي-

2- يشهد الفضاء السيبراني تنامي سريع غير مسبوق ومن ثم يجب دراسته من زوايا ورؤى عديدة بما يؤهل الدول للتأشفي معه بما يحقق أمنها السيبراني والقومي.

خطة الدراسة:

مقدمة

المبحث الأول: الفضاء السيبراني

المطلب الأول: مفهوم الفضاء السيبراني

المطلب الثاني: أهم الفواعل على مستوى الفضاء السيبراني

المبحث الثاني: الأمن السيبراني

المطلب الأول: النزاع السيبراني

المطلب الثاني: استراتيجيات الدول في تحقيق أمنها السيبراني -حالة الإتحاد الدولي للإتصالاتالعالمي-

الإستنتاجات والتوصيات

خاتمة

2. المبحث الأول: الفضاء السيبراني

استُخدم مفهوم "الفضاء السيبراني" لأول مرة من قبل كاتب الخيال العلمي ويليام جيبسون في رواية نشرها عام 1984 بعنوان Neuromancer، في هذه الرواية وصف جيبسون الفضاء السيبراني بأنه: "شبكة من الحواسيب، في عالم مليء بكائنات اصطناعية الذكاء"¹.

لاحقاً استخدم هذا المفهوم لوصف شبكات الإتصالات وتقنيات الواقع الافتراضي الناتجة عن ربط مئات الملايين من الحواسيب وغيرها من مكونات البنية التحتية للإنترنت، وحالياً يمثل الفضاء السيبراني شبكة حيوية تمتد عبر العالم، وتشمل بيئة كثيفة من الشبكات التي تتفاعل جميعها معاً، وعلى الرغم من

أنه غالبًا ما يُنظر إلى هذا الفضاء على أنه عالم مستقل عن الواقع المادي، إلا أنه لاحقًا صار الفضاء الحقيقي -الواقعي- والفضاء السيبراني يتبادلان التأثير، ويشكل كل منهما الآخر على نحو مستمر².

يعمل الفضاء السيبراني بأنظمة المعلومات والإنترنت على تحويل بيئة العالم بطرق غير عادية من خلال تمكين النمو في مجالات عديدة وتوفير وسائل جديدة يتواصل بها الأشخاص ويتفاعلون مع بعضهم البعض على المستوى العالمي، التطور المستمر لمكونات تكنولوجيا المعلومات والاتصالات؛ يتجسد أساسًا في المكونات الرقمية الأساسية (الإلكترونيات الأساسية) والانخفاض المقابل في التكاليف الذي أصبح متاحًا بشكل متزايد ويمكن الوصول إليه في جميع أنحاء العالم، والنتيجة هي أن المزيد من الأفراد حول العالم سيعتمدون في نهاية المطاف على الأداء الفعال للإنترنت من أجل البقاء والازدهار، يشير هذا إلى تصاعد مستمر في عدد المواطنين الإلكترونيين على مستوى العالم أي على مستوى إفتراضي عالمي.

1.2 المطلب الأول: مفهوم الفضاء السيبراني

مصطلح "الفضاء السيبراني" لا يزال بحاجة إلى تعريف مقبول عالميًا على الرغم من أنه في بعض الأحيان يرقى إلى مفهوم الإنترنت أو وجهة نظر عالم افتراضي رقمي.

ظهرت العديد من التعريفات من منظمات بارزة مثل:

وكالة الاستخبارات المركزية (CIA)، ووكالة الأمن القومي (NSA)، وقمة الأمن السيبراني الروسية الأمريكية، وما إلى ذلك (معهد الشرق والغرب ومعهد أمن المعلومات بجامعة موسكو الحكومية).

وفقًا لوزارة الدفاع الأمريكية يعد الفضاء الإلكتروني: "مجالًا عالميًا داخل بيئة المعلومات يتكون من شبكة مترابطة من البنى التحتية لتكنولوجيا المعلومات، بما في ذلك الإنترنت وشبكات الاتصالات وأنظمة الكمبيوتر والمعالجات ووحدات التحكم المدمجة"³.

ويعرف الفضاء السيبراني على أنه: "الفضاء الإلكتروني الذي يتميز باستخدام الإلكترونيات والطيف الكهرومغناطيسي لتخزين وتعديل وتبادل المعلومات عبر الشبكات ونظم المعلومات والبنى التحتية المادية"⁴.

و تصف القمة الروسية الأمريكية للأمن السيبراني الفضاء الإلكتروني بأنه: "وسيط إلكتروني يتم من خلاله إنشاء المعلومات ونقلها واستلامها وتخزينها ومعالجتها وحذفها"⁵.

يشير كلا التعريفين إلى أن الفضاء السيبراني:

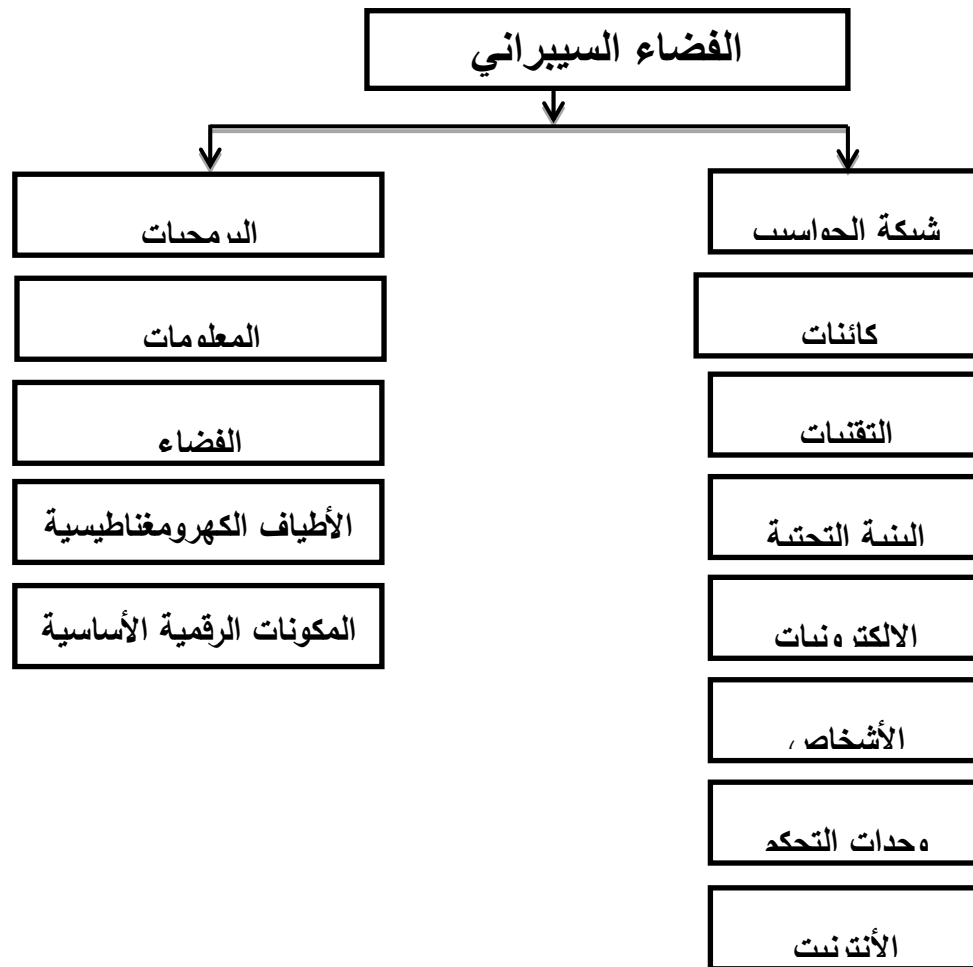
يشمل مزيجاً من تقنيات الإنترنت والاتصالات التي تسمح بتسجيل المعلومات وتخزينها واسترجاعها ونقلها⁶.

وبالتالي يمكن تعريف الفضاء السيبراني على أنه:

مصطلح لوصف الأنظمة والخدمات المتصلة إما بشكل مباشر أو بشكل غير مباشر إلى شبكة الإنترنت والاتصالات السلكية واللاسلكية وشبكات الكمبيوتر⁷.

يتضح من خلال التعاريف السابقة أنّ الفضاء السيبراني يشمل العناصر الرئيسية التالية:

الشكل رقم (01): يوضح العناصر الأساسية للفضاء السيبراني



المصدر: من إعداد الباحث بالإعتماد على التعاريف السابقة

2.2 المطلب الثاني: أهم الفواعل على مستوى الفضاء السيبراني

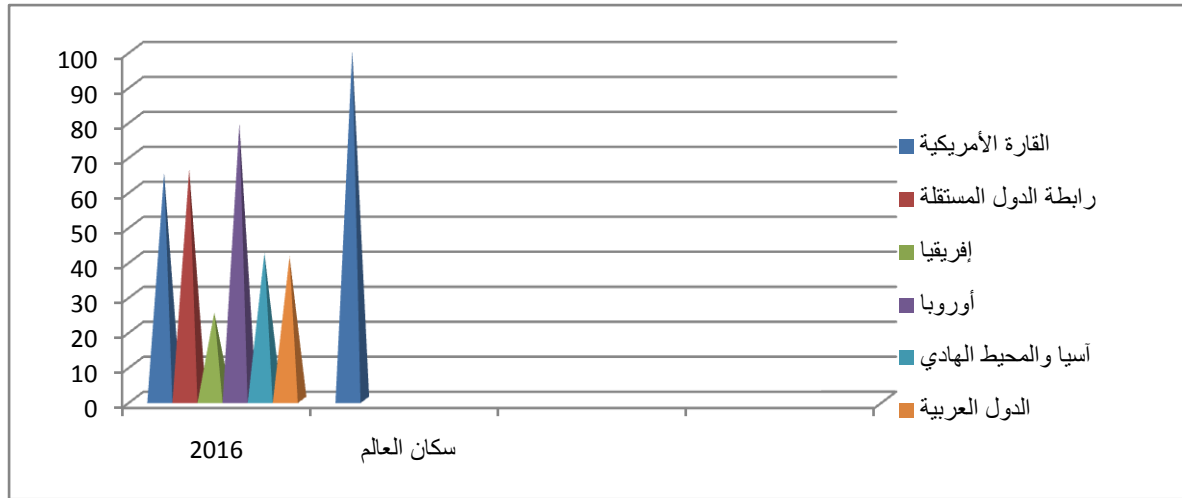
1.2.2 مستخدمي شبكة الأنترنت:

تشير إحصائيات Internet World Stats (الشركة التي تجمع هذه البيانات) في عام 1995 كان هناك ما يقرب من 16 مليون مستخدم للإنترنت في ديسمبر 2011، تجاوز عدد مستخدمي الإنترنت 2.2 مليار ، أي أكثر من 30 بالمائة من سكان العالم⁸.

وأعلن الاتحاد الدولي للاتصالات، أن عدد مستخدمي الإنترنت في العالم يصل إلى 60% من مجموع سكان العالم بحلول وهذا سنة 2020 وبحسب إحصاءات الاتحاد الدولي للاتصالات، فإن "عدم مستخدمي الشبكة العنكبوتية في العالم، لم يتجاوز 1% عام 1995، في حين بلغت هذه النسبة 7% في 2000".

وبحسب معطيات الاتحاد لسنة 2016، بلغ عدد مستخدمي الإنترنت في القارة الأمريكية 65%، وفي رابطة الدول المستقلة 66%، وإفريقيا 25%، وأوروبا 79%، وآسيا والمحيط الهادئ 42%، والدول العربية 41%⁹.

مخطط بياني يوضح النسبة المئوية لاستخدام الأنترنت لقارات العالم¹⁰:



ويتوقع الاتحاد الدولي للاتصالات، أن يصل عدد مستخدمي الإنترنت في العالم إلى 4.1 مليار شخص عام 2020، أي ما يعادل 60% من مجموع سكان العالم (7.753 مليار نسمة).

يبلغ عدد مستخدمي الإنترنت في العالم 4.80 مليار شخص وذلك بحلول شهر جويلية 2021، وهذا الرقم يعادل تقريباً 61% من إجمالي سكان العالم.

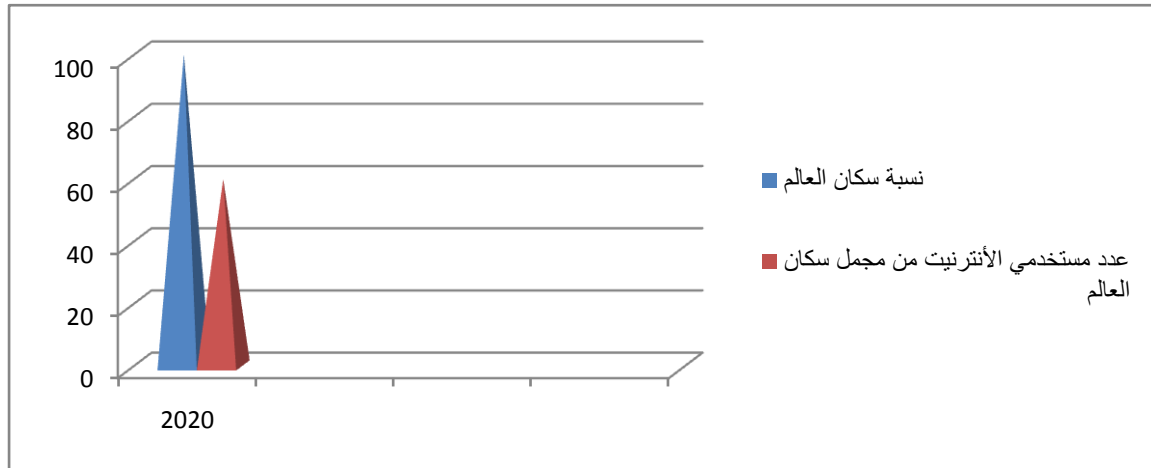
لا يزال هذا الرقم في تزايد مستمر، حيث يوجد حوالي 257 مليون مستخدم جديد للإنترنت خلال العام الواحد تقريباً، ويقدر معدل نمو مستخدمي الإنترنت حالياً بحوالي 5.7%، أي ما يعادل أكثر من 700 ألف مستخدم جديد كل يوم في المتوسط.

ويعتمد معظم مستخدمي الإنترنت (حوالي 92.1%) على الأجهزة المحمولة للاتصال بالإنترنت وتصفح الشبكة العنكبوتية، لكن مع ذلك لا تزال أجهزة الكمبيوتر تمثل حصة مهمة من نشاط الإنترنت العالمي.

يوجد 4.48 مليار مستخدم للشبكات الاجتماعية المختلفة، وهو ما يعني أن 56% من سكان الأرض يستخدمون على الأقل شبكة اجتماعية واحدة مثل فيس بوك أو انستغرام.

في الفترتين بين جويلية 2020 وجويلية 2021 انضم حوالي 520 مليون مستخدم جديد إلى وسائل التواصل الاجتماعي وهو ما يعادل نمو أكثر من 1.4 مليون مستخدم جديد كل يوم، مع العلم أن هناك ستة شبكات اجتماعية على الأقل لديها أكثر من مليار مستخدم نشط شهرياً¹¹.

مخطط بياني يوضح توقعات استخدام الأنترنت لمجمل سكان العالم بحلول عام 2020¹²:



المصدر: من إعداد الباحث بالإعتماد على المعطيات السابقة

- الدول الأكثر استخدامًا للإنترنت¹³:

حلت الصين في مقدمة البلدان المستخدمة للإنترنت بعدد 721.4 مليون، بحسب موقع "internet live stats".

وجاءت الهند في المرتبة الثانية، بـ 462.1 مليون شخص، والولايات المتحدة، 286.9 مليون، والبرازيل 139.1 مليون، واليابان 115.1 مليون، وروسيا 102.2 مليون، ونيجيريا 86.2 مليون، وألمانيا 71 مليونًا، وبريطانيا 60.2 مليون، والمكسيك 58 مليونًا.

- الدول الأكثر استخدامًا للإنترنت وفقًا لعدد السكان¹⁴:

تصدرت جزر برمودا، صدارة عدد مستخدمي الإنترنت في العالم، مقارنة مع عدد سكانها، حيث بلغ عدد المستخدمين لديها 98.3%، بحسب أرقام البنك الدولي.

وجاءت آيسلندا في المرتبة الثانية بواقع 98.2%، ولوكسمبورغ 97.3%، وأندورا 96.9%، والنرويج 96.8%، وليختنشتاين 96.6%، والدنمارك 96.3%، وجزر فارو 94.2%، والبحرين 93.5%، وموناكو 93.4%، ويمكن تفسير ذلك إلى أن معظم هذه الدول منتجة لخدمات النات وأنها دول متقدمة، وذات دخل قومي قومي جيد يسمح لها باستخدام النات بدرجة أعلى، كما أن المعطيات اقتصر فقط على متغير عدد السكان، وأن معظم سكان هذه الدول قليل مقارنة بالدول الأخرى.

كما يتوقع الاتحاد، ارتفاع عدد الأجهزة التي تمتلك خاصية الاتصال بالإنترنت، إلى 25 مليار جهاز في 2020، أي ما يعادل 3.4 جهازًا للفرد.

ومن المنتظر أن تستحوذ مقاطع الفيديو على ثلاث تريليونات دقيقة شهريًا، وسيتم تحميل مليون دقيقة مقطع فيديو في الثانية على الإنترنت، مع قدوم عامي 2020 و 2021، بحسب شركة "سيسكو سيستمز" الأمريكية لاتصالات والتكنولوجيا¹⁵.

2.2.2 النشاطون والمتسللون على مستوى الفضاء السيبراني

يُصنف مستخدمي الفضاء السيبراني إلى صنفين:

1- النشاطون الرقميون الإيجابيون الذين يستخدمون الفضاء السيبراني كمنصة للتعبير عن أفكارهم وطموحاتهم، وهم صناع المحتوى مثل: المؤثرين Influencers واليوتيوبرز YouTubers وغيرهم ممن يستغلون الفضاء بطريقة إيجابية.

2- القرصنة الرقميين ، Hackers والمتسللين Crackers فالعديد من المؤسسات الرسمية

تصنف عبر تقاريرها الاستراتيجية للأمن السيبراني "الناشطين الرقميين" كأعداء محتملين، وتعتبر أنهم يشكلون تهديدا لأركان الدولة ومؤسساتها الأساسية؛ لكونهم يزاحمون الدولة في العديد من مظاهر التأثير، على نحو يخصص من قدراتها أو على الأقل يتحداها، حتى إن تقريراً أمريكياً رسمياً لعام، 2010 اعتبر أن أحد أكبر الأخطار التي تواجه الأمن القومي الأمريكي هي شبكات الاتصال الافتراضية، كما حذرت حكومة الولايات المتحدة من أن التقنيات ذاتها التي تمكننا من القيادة تمكن أيضاً أولئك الذين يبتغون التعطيل¹⁶.

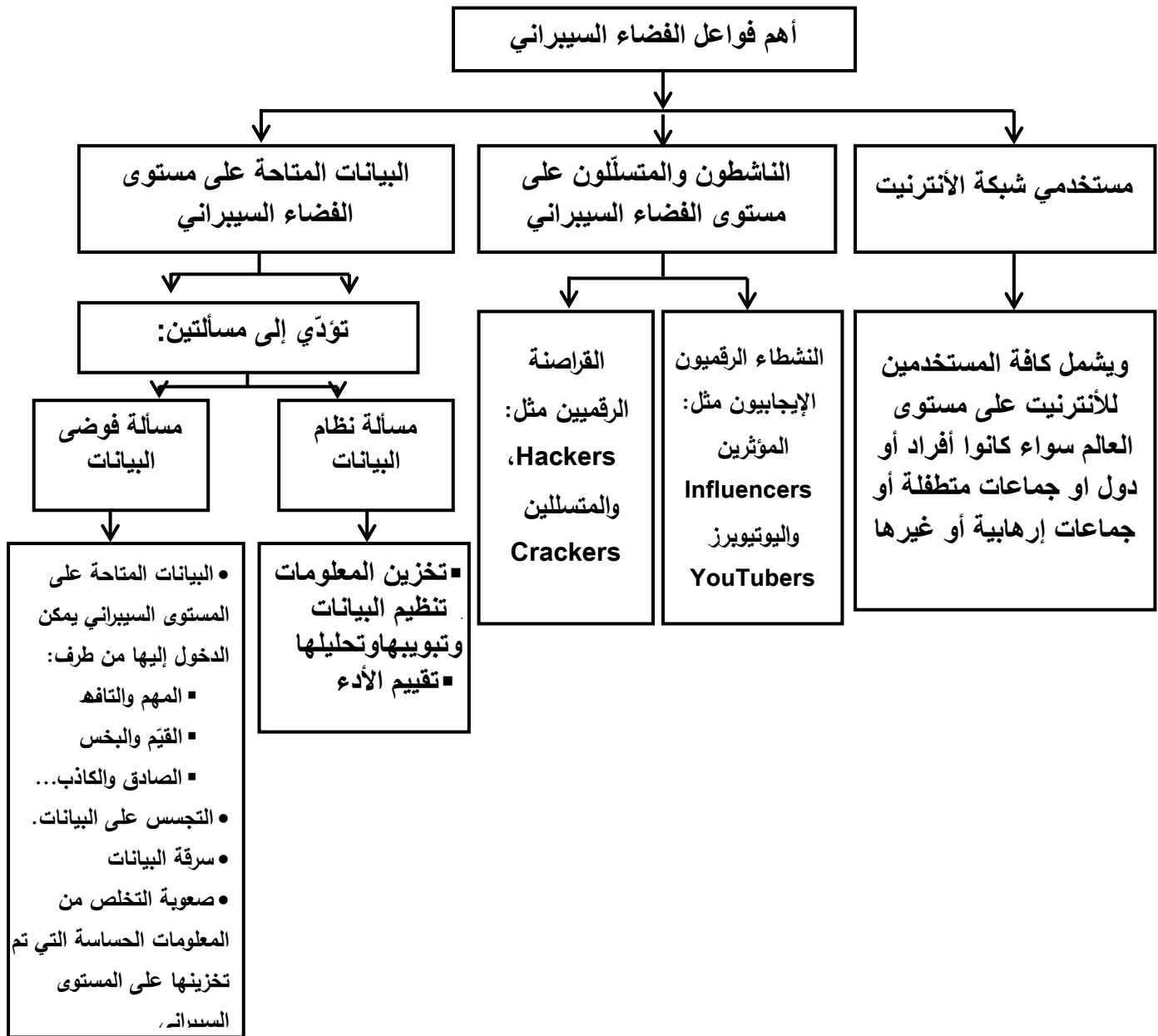
3.2.2 البيانات المتاحة على الفضاء السيبراني وقضية الفوضى والنظام.

يرتبط مفهوم الفضاء الافتراضي بتضخم هائل في القدرة على تخزين المعلومات، حيث أصبح من السهل تسجيل كل كلمة كتبها الإنسان أو نطق بها طوال حياته، بفضل التضخم الهائل في القدرات الاستيعابية للوسائط المعلوماتية، فضلاً عن تنامي سرعة نقل المعلومات ومشاركتها، هذه القدرة المتواترة على الاحتفاظ بكل شيء، ولدت نوعاً جديداً من التسهيلات، سواء بالنسبة للمؤسسات الحكومية أو للمؤسسات الخاصة، فبالنسبة للأولى أصبح لدى الحكومات الرقمية ميل إلى الإبقاء على كميات هائلة من البيانات والمعلومات، حتى يتسنى لها لاحقاً التدقيق فيها؛ للكشف عن الفساد، أو إجراء التحقيقات، أو تقييم الأداء أو ما شابه، أما بالنسبة للثانية فإن الكثير من الشركات تدفعها لرغبة للتمتع بقدرة اقتصادية تنافسية إلى تخزين كل ما تجمعه من بيانات عن ملايين المعاملات، وتفاصيل كل معاملة، من حيث تاريخها، ووقتها والمبيع منها والمتجر والسعر والمشتري، وكيفية السداد، وهل كان عن طريق بطاقة ائتمانية أم عن طريق الخصم من الحساب الشخصي، أم عن طريق الدفع نقداً، لدرجة أن المعادلة الآن أصبحت معكوسة، فبعد أن كانت المطالب قديماً تتوجه إلى ضرورة سن تشريعات لتوثيق وأرشفة المعلومات، أصبحت تتوجه حالياً إلى ضرورة سن قوانين تحدد متى يمكن التخلص من المعلومات، فمن دون سنّ هذه القوانين الردعية يبدو أنه سيكون من الصعب على أي جهة أن تتخلص طواعية من أي بيانات تمتلكها بفعل هذه الخاصية.

من خلال ما سبق يرى بعض ناقدى المجتمع السيبراني على أنه سيؤول إلى حالة من الفوضى، الناتجة عن التراكم الهائل وغير المسبوق للمعلومات، افترض هؤلاء أن تراكم كميات هائلة من المعلومات من مصادر متعددة، لن يترجم إلى مزيد من النظام، بقدر ما سيشير إلى حالة من الفوضى التي تتساوى فيها الأضداد، المهم والتافه، القيم والبخس، الصادق والكاذب، ومن ثم فإن الرغبة في مراكمة المزيد من المعلومات لن يتولد عنها إلا المزيد من العمى المعلوماتي، سيؤدي هذا إلى مجتمع ما بعد الحقيقة، والمتعلق بغياب أي معايير مشتركة للصدق، وانهايار الفواصل بين الحقائق والأخبار والمعلومات والآراء والمعتقدات، ولكن لم يصدق هذا النقد على نحو كامل في الواقع الذي شهد في كثير من الأحيان عكسه، فتنامي القدرة على تخزين ومراكمة المعلومات صاحبته قدرة موازية على تصنيف هذه المعلومات والاستفادة منها؛ إذ ازدادت أجهزة الحاسوب قدرةً على استخلاص المعاني من هذا التراكم المعلوماتي الهائل، بل ونشأت حقول علمية جديدة مهمتها وضع هذه المادة الخام الهائلة موضع الاستفادة، مثل حقول علم البيانات، Data Science، والبيانات الكبيرة Big Data بل إن القدرة على التصنيف والاستفادة لم تعد تقتصر على مصادر البيانات والمعلومات التقليدية، الموجودة في السجلات الحكومية والخاصة فقط، وإنما تخطتها لتشمل البيانات غير المنظمة Unstructured data التي تشمل التعليقات على صفحات التواصل الاجتماعي، وكلمات البحث، والتدوينات والتغريدات، بل وأصبح المحتوى المرئي والمسموع نفسه، ضمن المصادر المحتملة للمعلومات، والتي يمكن تحليلها واستخلاص الاتجاهات من خلال استطلاع مضمونها¹⁷.

من خلال ماسبق يمكن ملاحظة أن فواعل الفضاء السيبراني عديدة لايمكن حصرها وإنما اقتصر هذا البحث على أهم الفواعل:

يمكن توضيحها في المخطط التالي:



المصدر: من إعداد الباحث بالإعتماد على المعطيات السابقة

يتضح من خلال ماسبق أنّ فواعل الفضاء السيبراني عديدة جدا لا يمكن حصرها، وذلك باعتبار أنّه فضاء واسع جدا ومعقد في نفس الوقت وأنّه أصبح من السهل استخدامه سواء من طرف الفواعل الرسميين أو غير الرسميين سواء من طرف القطاعات الخاصة أو العمومية وكذا من طرف الأفراد أو الجماعات وكذا من حيث الهدف سواء كان الهدف إيجابي مثل: البحث والتطوير... أو كان الهدف سلبي مثل: التجسس والإختراقات وسرقة البيانات... إلخ، مما أدى بالدول إلى بلورة مؤسسات ردعية تهدف إلى تحقيق الأمن السيبراني وهذا ما يتم توضيحه في العنصر التالي.

3. المبحث الثاني: الأمن السيبراني

1.3 المطلب الأول: مفهوم الأمن السيبراني

تعددت التعاريف حول الأمن السيبراني منها على سبيل المثال لا الحصر:

يعرف الأمن السيبراني، Cybersecurity حسب وزارة الأمن الداخلي الأمريكي بأنه: "النشاط أو العملية أو القدرة أو الإمكانية أو الحالة التي يتم بموجبها حماية نظم المعلومات والاتصالات والمعلومات الواردة فيها و/أو الدفاع عنها ضد الضرر أو الاستخدام أو التعديل غير المصرح به أو الاستغلال"¹⁸. حيث انتهجت الولايات المتحدة الأمريكية في عهد الرئيس باراك أوباما مجموعة من الإجراءات التي يتم بموجبها تحقيق الأمن السيبراني وهي¹⁹ :

".. تدور نقاشات محتدمة حول أعمال الأمن السيبراني... أصدر الرئيس الأمريكي أوباما أمرًا تنفيذيًا في فبراير 2013 للتقليل من مخاطر الإنترنت إلى درجة قصوى لحماية البنية التحتية وتحسين تبادل معلومات الأمن السيبراني بين القطاعين العام والخاص".

ومنه أطلقت المبادرة الوطنية للأمن السيبراني (CNCI) المبادرات التالية: -لضمان وجود بنية تحتية للمعلومات والاتصالات موثوقة ومرنة عبر الوكالات الحكومية-

1. إدارة شبكة المؤسسة الفيدرالية كمؤسسة شبكة للأنترنت.
2. نشر نظام كشف التسلل لأجهزة الاستشعار عبر المؤسسة الفيدرالية.
3. متابعة نشر أنظمة منع التطفل عبر الحكومة الاتحادية.
4. تنسيق وإعادة توجيه جهود البحث والتطوير.
5. ربط مراكز العمليات السيبرانية الحالية لتعزيز الوعي الظرفي.
6. تطوير وتنفيذ خطة لمكافحة التجسس السيبراني على مستوى الحكومة.
7. زيادة أمن شبكاتنا المصنفة.
8. توسيع نطاق التعليم السيبراني.
9. تحديد وتطوير تقنيات واستراتيجيات وخطوات "قفزة إلى الأمام" دائمة البرامج.
10. تحديد وتطوير استراتيجيات وبرامج الردع الدائمة.
11. تطوير نهج متعدد الجوانب لإدارة مخاطر سلسلة التوريد العالمية.

12. تحديد الدور الفيدرالي لتوسيع نطاق الأمن السيبراني ليشمل البنية التحتية الحيوية المجالات.

2.3 المطلب الثاني: من الفضاء السيبراني إلى النزاع السيبراني

حاليا، ساحة الفضاء السيبراني هي المجال الرئيسي للصراع الدولي حيث أن تطور هذا الفضاء مبني على الخوف من أن يصبح بناء التهديد مهيم، لقد تبدد الخوف المرتبط بالإرهاب بعد 11 سبتمبر 2001، وتم استبداله من نواح كثيرة بالخوف من الصراع السيبراني، القوة، وحتى الحرب الإلكترونية أو السيبرانية²⁰.

مع ظهور مجتمع الإنترنت وتزايد الترابط في عالم يتسم بالعولمة أكثر من أي وقت مضى، يجادل الكثيرون بأنه يجب علينا ذلك أن نخشى أيضاً من الضعف الذي تسببه هذه الروابط المتمثل في إنشاء اتصالات مثل الطائرات بدون طيار والأقمار الصناعية وعناصر التحكم التشغيلية السيبرانية الظروف التي تتفاعل لإنتاج نقاط ضعف في ديناميكيات الأمن الموجودة حاسمة لبقاء الدولة، يجعل التشبيه بأن تصفح الإنترنت الفضاء الإلكتروني مثل السباحة في بركة قذرة²¹.

1.2.3 توازن القوى الدولية على المستوى السيبراني

تحتفظ الدول في الفضاء السيبراني بكثير من ملامح العلاقات بينهم في العالم اللافتراضي، فمن ناحية تتنافس الدول الكبرى بقوة على موقع الصدارة في العالم السيبراني، وعلى سبيل المثال الحرب التجارية التي اندلعت بين الولايات المتحدة والصين تمحورت حول منع شركة Huawei الصينية الكبرى المصنعة للتكنولوجيا من دخول السوق الأمريكية في ظل اتهامات لها بالتلاعب والتجسس لصالح الحكومة الصينية، حذر الكثيرون من أن تنافسا سيبرانياً بين الولايات المتحدة والصين كفيلاً بالإضرار بالاقتصاد العالمي. تطرح الصين استراتيجيتها الدولية للتعاون في الفضاء السيبراني بوصفها استراتيجية بديلة استثناء، وعلى احترام مبدأ السيادة بحيث لا تستخدم الدول الإنترنت للتدخل في شؤون الدول الأخرى، وعلى تجنب سباقات التسلح وسياسات الردع في الفضاء السيبراني لما لها من تأثير سلبي على السلم والأمن الدوليين،

تقوم الاستراتيجية على التنافس الحر والعدل وتروج لأهمية إتاحة فرصة المشاركة المتكافئة للجميع في الفضاء السيبراني من خلال إتاحة التكنولوجيا اللازمة لهذا الأمر، ومن خلال إتاحة فرص متساوية لجميع اللغات وإتاحة فرصة للتبادل الثقافي والحضاري بين الشعوب جميعها خدمة للإنسانية.

ومن ناحية أخرى تؤثر قدرة الدول على الاستفادة من الفضاء السيبراني في موقعها من خرائط توازنات القوى حيث تتفوق إسرائيل في هذا المجال بشكل يستحق التأمل، تنتج إسرائيل تكنولوجيا تقيد في عمليات الزراعة والري الذكية بحيث تتلقى كل نبتة ما تحتاجه من عناية ومياه، كذلك تنتج أجهزة تستعين بالذكاء الاصطناعي لكي تستخرج الماء من الهواء لتحل مشكلة نقص المياه في مناطق كثيرة من العالم .

وتمتلك إسرائيل حصة تصل إلى عشرون بالمائة (20%) من نصيب الاستثمارات في مجال التأمين السيبراني للبنوك والشركات وغيرها، وتجدر الإشارة إلى أن رئيس الوزراء الإسرائيلي الأسبق بنيامين نتنياهو تحدث بثقة على أن التكنولوجيا الإسرائيلية تسيطر على العالم، وأن إسرائيل التي كانت تعيش في حالة عزلة شبه كاملة عند تأسيسها أصبحت اليوم علناً اتصالاً بمعظم دول العالم، فتذهب إليها الصين والهند والدول الإفريقية - وحتى دول مسلمة ككازاخستان وغيرها - طلباً للمشورة والمساعدة، في حين تبقى الدول النامية بعيدة عن هذه المنافسات ولا نصيب لها من هذا التنافس على سلم القوى الدولية الذي يتولد عن استغلال الدول لما يتيحه الفضاء السيبراني لها من فرص، ومن ناحية ثالثة تختلف الدول الفقيرة مقارنة بالدول الغنية من حيث القدرة على الاستفادة من عوائد الإنترنت، وهو واقع يرمز إليه البعض بـ: "الفجوة الرقمية"²² فإذا كان أكثر من خمسين بالمائة (50%) من سكان العالم يستطيعون المشاركة في الفضاء السيبراني²³، فإنّ هناك قرابة نصف سكان العالم لا يستطيعون ذلك وإذا كان بعض هؤلاء المحرومين يعيش في دول غنية، فإن غالبيتهم العظمى تعيش في الدول النامية، وهو أمر له تداعيات عديدة وهامة تؤثر على سبيل المثال حول فرص التنمية المستدامة بشدة بقدرة الدول على الانفتاح على الفضاء السيبراني؛ وهو ما يشير إليه تقرير التنمية الصادر عن اتحاد الاتصالات الدولي في عام 2018؛ حيث اعتبر أن القدرة على دخول الإنترنت هي سبيل أساسي أمام الدول لتحقيق التنمية المستدامة،

فالفضاء السيبراني يتيح فرصة تقديم الخدمات للمواطنين بشكل أسرع وأكثر كفاءة كما هو الحال مع خدمات التعليم والصحة والإغاثة في حالات الأزمات الطارئة والنقل، إلخ، في السياق ذاته يتحدث البعض عن أن الفضاء السيبراني لن يزيد الدول النامية - كذلك الموجودة في إفريقيا - إلا تهميشاً، فما الفائدة التي تعود على دول فقيرة منهوبة الثروات والخيرات، تعتمد بالكلية على الاستيراد والديون، من كل

تلك الطفرات التي تشهدها الصناعة والتكنولوجيا وتلك الثورة الرقمية غير المسبوقة؟ يرى Everisto Benyera أن أفريقيا -في عصر السيبرانية- لا ينتظرها سوى المزيد من النهب والاستغلال، فعمليات سلب الموارد والعمالة التي شهدتها أفريقيا في عصور الاستعمار تمتد اليوم لتصبح عمليات من السلب الرقمي؛ حالة من الاستعمار المعلوماتي²⁴ the coloniality of data تستغل معه الشركات الكبرى تلك البيانات الضخمة التي تتمكن من جمعها من أفريقيا -بلا أي رقابة مؤسسية محلية حقيقية- وذلك لتحقيق المزيد من الثراء والثروة، وليس غريباً أن يهدي Benyera كتابه إلى "كل العبيد، في الماضي والحاضر والمستقبل"، وبالعبيد الذين لا يدركون أنهم عبيد" في إشارة إلى جهل شعوب الدول النامية بما تحمله الثورة السيبرانية من استغلال لثرواتهم في الوقت ذاته تثبت بعض الدراسات أن ثمة علاقة متبادلة بين إساءة استخدام الفضاء السيبراني وبين زيادة معدلات الفقر²⁵. يسهم الفضاء السيبراني في كثير من الدول النامية بالفعل في زيادة حالة التبعية والفقر، فالمقامرات والدعارة والنصب والاحتيال والإتجار في المخدرات والإتجار بالبشر وغسيل الأموال والمعاملات المالية غير المشروعة والعنف السيبراني والجرائم (أو ما يُعرف إجمالاً بإساءة استخدام الفضاء السيبراني cyberspace abuse كلها أمور تحيل دخول الكثيرين في الدول النامية إلى الفضاء السيبراني من النعمة إلى النقمة، قاد الانفتاح على الفضاء السيبراني إلى زيادة نسبة الفقراء في نيجيريا إلى أربعة وخمسون بالمائة (54%) على سبيل المثال، تبدو الدول النامية بوجه عام أقل قدرة على الاستفادة من هذا الفضاء بسبب ضعف سرعة الإنترنت وبسبب الرقابة الحكومية التي تمارسها الدولة على انسياب المعلومات إلى المواطنين.

تتميز المجتمعات النامية بوجود أجيال اتصال مختلفة في داخلها، فبينما تنعزل أجزاء من الشعب خاصة في الريف والمناطق النائية -تماماً عن التطورات الحديثة، يعيش البعض في جيل أكثر تقدماً من أجيال الاتصال والتواصل، تضغط هذه الانقسامات على البنية المجتمعية للدول النامية وتماسكها، بينما تقل هذه الانقسامات بشكل واضح في المجتمعات المتقدمة حيث يشارك معظم أبناء هذه المجتمعات بنسب تزيد عن 80% في الفضاء السيبراني، كما هو الحال بالنسبة للولايات المتحدة²⁶.

2.2.3 خطورة ربط المجالات الحيوية بالفضاء السيبراني

أ- الأمن الوطني والقومي:

يقول المؤلف نسيم طالب، في مؤلفه كتاب "البجعة السوداء"، "الاتصال والنفوذ التشغيلي يجعل الأحداث الثقافية والاقتصادية متتالية أسرع وأعمق"²⁷. هذا التأثير المتسلسل له قوة خاصة في الفضاء

السيبراني لأن الاضطرابات في الأنظمة الإلكترونية تنتشر بسرعة أكبر، والنطاق أوسع، من الاضطرابات التي حدثت في الماضي - على وجه التحديد بسبب الفضاء الإلكتروني الذي يربط العالم بشكل شامل ، حيث أن عولمة الفضاء السيبراني هو العامل الغالب في عولمة الاعتماد الدولي، حيث أصبح عالم ما بعد 11 سبتمبر، يواجه العالم نوعاً جديداً من التهديد لكل من الإقتصاد الوطني والأمن الوطني والقومي، فالهجمات المتعمدة على البنى التحتية الوطنية يمكن أن تحطم شبكات التحكم الرئيسية المعتمدة على الكمبيوتر، مثل: شبكات الطاقة الكهربائية وأنظمة شبكات الاتصالات، أنظمة النقل والمؤسسات المالية؛ هذه الأنظمة والهياكل حيوية لدول للعالم لاسيما الدول الرائدة في المجال السيبراني مثل الولايات المتحدة الأمريكية، سيكون لعجزهم أو تدميرهم تأثير فوري على الأمن القومي والاقتصاد وكذا المجتمع.

ب- أمن وسلامة البيانات المتاحة على مستوى الفضاء الإلكتروني:

لقد أدى انتشار الاتصال عبر الفضاء الإلكتروني إلى جمع المعلومات الاستخباراتية وحتى التجسس الاقتصادي، حيث يمكن سرقة المعلومات الهامة عن بعد وبأكثر سهولة مما كانت عليه في الماضي، كما يؤدي هذا الانتشار إلى انتهاك الملكية الفكرية والمزايا الاقتصادية التنافسية وكذا الأمن القومي، وكذا تدمير السرية والخصوصية والكشف عن هويات الأفراد في حياتهم الخاصة²⁸.

يمكن القول ان الفضاء السيبراني أدى إلى ظاهرة النزاع السيبراني، وذلك يربط إلى عدة أسباب

منها:

الفجوة الرقمية أو مسألة توازن القوى على المستوى السيبراني بين الدول المنتجة والدول المستهلكة، بمعنى أن الدول الرائدة فيا لمجال السيبراني دائما متفوقة على غيرها وبالتالي يؤدي ذلك إلى غياب الثقة بين الدول بسبب احتكار التكنولوجيا.

أن الفواعل على مستوى الفضاء السيبراني، منها الفواعل النظامية التي تسعى إلى تحقيق أهداف إيجابية مثل الدول والشركات الاقتصادية وغيرها، أو الفواعل الغير النظامية مثل الأفراد والجماعات الإرهابية هذا ما يؤدي بشكل أو آخر إلى النزاع السيبراني الذي يهدد امن الأفراد وأمن الدول.

ومن خلال ذلك كان لابد ولزما على الدول ان تنتهج سياسة أمنية سيبرانية فعالة من أجل حماية أمنها المجتمعي والقومي وهو ما يصطلح عليه في الأدبيات الأمنية بالأمن السيبراني.

3.3 المطلب الثالث: استراتيجيات الدول في تحقيق أمنها السيبراني حالة المركز الدولي للاتصالات

تنتهج دول العالم مجموعة من الاستراتيجيات الفعالة من أجل تحقيق الأمن السيبراني العالمي وذلك من خلال تأسيس مجموعة من الآليات ذات الاختصاص الإقليمي والعالمي في سبيل التوصل إلى أمن سيبراني عالمي، على سبيل المثال: المنظمة الدولية للشرطة الجنائية (الأنتربول) *، الإتحاد الدولي للاتصالات) وسيتم اختيار الاتحاد الدولي للاتصالات كحالة من أجل تحقيق أمن سيبراني عالمي.

المركز الدولي للاتصالات كآلية من الآليات الدولية لخلق ثقة سيبرانية عالمية²⁹:

هو وكالة الأمم المتحدة الرائدة في قضايا تكنولوجيا المعلومات والاتصالات ونقطة التنسيق العالمية للحكومات والقطاع الخاص بشأن تطوير الشبكات والخدمات.

ومن الأدوار الأساسية التي اهتم بها الاتحاد الدولي للاتصالات في أعقاب القمة العالمية لمجتمع المعلومات (WSIS) ومؤتمر المندوبين المفوضين لعام 2006 يتمثل في بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات (ICT)، فقد قام رؤساء الدول والحكومات وغيرهم من قادة العالم المشاركين في القمة العالمية لمجتمع المعلومات، وكذلك الدول الأعضاء في الاتحاد، بتكليف الاتحاد باتخاذ خطوات ملموسة للحد من التهديدات وانعدام الأمن فيما يتصل بمجتمع المعلومات، ولتحقيق هذا الهدف أطلق الأمين العام للاتحاد حمدون إ.توريه برنامج الأمن السيبراني العالمي (GCA) ليكون إطارا للتعاون مع أصحاب المصلحة المتعددين على الصعيد الدولي في مجال الأمن السيبراني.

ويركز هذا البرنامج على مجالات العمل الخمسة التالية³⁰:

1. البرنامج الوطني للاستجابة للحوادث الحاسوبية وهو برنامج تجري في إطاره عمليات تقييم وتنفيذ وطني وتدريبات سيبرانية إقليمية لهذه العملية بناء على طلب الدول الأعضاء.
2. إنشاء مراكز إقليمية للأمن السيبراني لتكون بمثابة محفز لتعزيز التعاون والتنسيق والتآزر على الصعيد الإقليمي من أجل التصدي للتهديدات السيبرانية المتصاعدة.
3. مشروع تعزيز الأمن السيبراني في البلدان الأقل نموا وهو مشروع يساعد الإتحاد من خلاله البلدان الأقل نموا في تعزيز إمكاناتها وقدراتها واستعدادها ومهاراتها ومعارفها في مجال الأمن السيبراني.
4. مؤشر الأمن السيبراني العالمي (GCI) وهو مقياس لمستوى كل دولة في مجال تطوير الأمن السيبراني والهدف من هذا المؤشر تزويد البلدان بالزخم المناسب كي تكثف جهودها في مجال الأمن

السيبراني والهدف النهائي هو المساعدة في بناء ثقة عالمية في الأمن السيبراني وإدماجها في صميم تكنولوجيا المعلومات والاتصالات.

4. خاتمة:

يعتبر الفضاء السيبراني من صنع البشر، من أجل تحقيق طموحات الإنسان، إلا أنه ومع تطور هذا المجال أصبح يشكل خطراً على الشعوب والدول سواء على مستوى أمن الفرد أو على مستوى الأمن الوطني والقومي، الأمر الذي جعل دول العالم تعيش تحت هاجس الخوف لاسيما الحديث عن الدول المتنافسة فيما بينها والسعي نحو تحقيق الريادة العالمية في المجال الإقتصادي والعسكري والتكنولوجي. ومن هنا أصبح الفضاء السيبراني مجال تهديد بدل مجال أمن واستقرار وهذا التهديد سواء من طرف الدول فيما بينها من خلال عمليات التجسس والاستخبارات والقرصنة وسرقة المعلومات أو من طرف المنظمات الإجرامية والإرهابية... ومن هنا اتجهت الدول إلى خلق آليات من أجل خلق الثقة السيبرانية بينها، منها مثلاً: الإتحاد الدولي للاتصالات، والإتحاد الدولي للعلماء، لكن يبقى ذلك غير كاف على أرض الواقع، ومن هنا يجب على كل دولة تأسيس وحدات متخصصة وذات كفاءة عالية من أجل التصدي للهجمات السيبرانية بمختلف أنواعها ومن مختلف مصادرها، وقبل التصدي يجب توفير برامج الحماية للمعلومات لاسيما الحديث عن المعلومات السرية والحساسة التي تخص القطاعات الاستراتيجية للدول وكذا المعلومات السرية التي تخص الأفراد والأشخاص وبعبارة أخرى يجب الخروج من مجرد رد الفعل إلى استباق الفعل.

الإستنتاجات والتوصيات:

1 الإستنتاجات:

1. الفضاء السيبراني مجال تهديد لأمن الدول والأمن المجتمعي.
2. دول العالم فكرت ولا زالت تفكر في خلق آليات دولية واستراتيجيات عالمية تعمل على توفير الأمن والثقة السيبرانية.
3. أن الفضاء السيبراني مهّد وشكل مسرح عمليات حربية على المستوى الإلكتروني.

2. التوصيات:

1. يجب على كل دولة وعلى حدة توفير وحدات متخصصة ذات كفاءة وقدرات عالية تعمل على توفير الحماية والأمن في المجال السيبراني.
2. العمل على تعزيز وتفعيل برامج التوعية لمختلف المؤسسات التابعة للدولة لاسيما القطاعات الإستراتيجية والسيادية للدولة، وكذا توعية مختلف شرائح المجتمع بضرورة تفادي كل مايؤدي بالخصوصية إلى الانتهاك على المستوى السيبراني.
3. خلق وتطوير مراكز تكوين في المجال الإلكتروني تهتم باستقطاب الكفاءات ذات الجودة العالية وتوفير لهم سبل العيش الكريم مهمتهم الرئيسية هي: حماية كل المعلومات والبيانات الحساسة للدولة ويتم توظيفهم على مستوى القطاعات الاستراتيجية والحيوية للدولة.
4. تعزيز التبادل المعلوماتي مع الحلفاء الاستراتيجيين في المجال السيبراني مع الأخذ بعين الاعتبار التدابير اللازمة لذلك.

5. الهوامش والمراجع

1. نبيل علي ونادية حجازي (2005)، الفجوة الرقمية، رؤية عربية لمجتمع المعرفة، مطابع السياسة، الكويت.
2. نسيم طالب (2009)، تر: حليم نسيب صبر، البجعة السوداء، تداعيات الأحداث غير المتوقعة، دار العربية للعلوم ناشرون، بيروت، لبنان، ط01.
3. حمدون إ. توريه الأمين العام للإتحاد الدولي للإتصالات، وفريق الرصد العالمي لأمن المعلومات، والإتحاد العالمي للعلماء، نوفمبر 2014.
4. أميرة أبو سمرة (أكتوبر 2021)، الفضاء السيبراني: مساحات جديدة للدفاع والتغيير؟، مجلة قضايا ونظرات، تجديد الوعي بالعالم الإسلامي والتغيير الحضاري، تقرير ربع سنوي، ع 23، مركز الحضارة للدراسات والبحوث.
5. شريف عبد الرحمن سيف النصر (أفريل 2021)، السيبرانية، المفهوم، الخصائص، الفرص والإشكاليات، مجلة قضايا ونظرات، تجديد الوعي بالعالم الإسلامي والتغيير الحضاري، تقرير ربع سنوي، ع 21، مركز الحضارة للدراسات والبحوث.
6. مريم غوكناش، 60 بالمائة من سكان العالم سيستخدمون الأنترنت بحلول سنة 2020، بحسب الإتحاد الدولي للإتصالات، الأناضول، أنقرة، <https://www.aa.com.tr/ar/%D8%A7%D9%84%D8%B9%> تاريخ الإطلاع: 2021/11/13 على الساعة: 09:09.
7. من إعداد الباحث بالإعتماد على المعطيات المقدمة حسب الموقع.
8. عدد مستخدمي الانترنت في العالم على الموقع:

9. اطلع عليه بتاريخ: <https://abuomar.ae/2021/08/05/%D8%B9%D8%AF%D8%AF>

2021/11/28 على الساعة 12:59.

10. William Gibson (1984), neuromancer, Ace Science Fiction Books are published by the Berkley Publishing Group 200 Madison Avenue, New York, The United States Of America.
11. Uche mbanaso, Eman Dandaur (june 2015), the cyber space : redefining a new world, projects : bi-annual, Cyber Abuja Conference_Centre for Cyber Space Studies, Nasarawa State University, Keffi, devoloping cyber warfare capablity and capacity in africa.
12. Daniel T. Kuehl, From Cyberspace to Cyberpower: Defining the Problem CHAPTER 2, p02, le lien : <https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02>.
13. Frederick Wamala, the ITU cybersecurity strategy guide, international telecommunication, union.
14. Newton Lee (2015), Conterterrorism and cybersecurity, total information awareness, usa, second edution, 2012.
15. Julian Richards Co-Director (2014), Cyber-War: TheAnatomy of the GlobalSecurity Threat, Centre for Security and IntelligenceStudies, University of Buckingham, UK, , p28.
16. Brandon Valeriano and Ryan C. Maness (2015), cyber war versus cyber realities, Cyber Conflict in the International System , Published in the United States of America by Oxford University Press 198 Madison Avenue, New York, NY 10016.
17. Paul Rosenzweig (2013), Cyber Warfare How Conflicts in Cyberspace are challenging america andchanging the World, 130 Cremona Drive, P.O. Box 1911 Santa Barbara, California 93116-191.
18. Paola Ricaurte (2019), Data Epistemologies, The Coloniality of Power, and Resistance, tlevision and new média.

¹William Gibson (1984), neuromancer, Ace Science Fiction Books are published by the Berkley Publishing Group 200 Madison Avenue, New York, The United States Of America , , pp 01-11.

² شريف عبد الرحمن سيف النصر، السيبرانية، المفهوم، الخصائص، الفرص والإشكاليات، مجلة قضايا ونظرات، تجديد الوعي بالعالم الإسلامي والتغيير الحضاري، تقرير ربع سنوي، ع 21، أبريل 2021، مركز الحضارة للدراسات والبحوث، ص 05.

³Uche mbanaso, eman dandaur, the cyber space : redefining a new world, projects : bi-annual, Cyber Abuja Conference_Centre for Cyber Space Studies, Nasarawa State University, Keffi, devoloping cyber warfare capablity and capacity in africa, june 2015, p18.

⁴ Daniel T. Kuehl From Cyberspace to Cyberpower: Defining the Problem CHAPTER 2, p02, le lien : <https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02>.

⁵Ipid, p 18.

⁶ Ipid, p 18.

⁷ Frederick Wamala, the ITU cybersecurity strategy guide, international telecommunication, union, p 05.

⁸ Paul Rosenzweig, Cyber Warfare How Conflicts in Cyberspace are challenging america and changing the World, 130 Cremona Drive, P.O. Box 1911Santa Barbara, California 93116-1911, 2013, p03.

- ⁹ مريم غوكتاش، 60 بالمائة من سكان العالم سيستخدمون الإنترنت بحلول سنة 2020، بحسب الإتحاد الدولي للاتصالات، الأناضول، أنقرة، <https://www.aa.com.tr/ar/%D8%A7%D9%84%D8%B9%>، تاريخ الإطلاع: 2021/11/13 الساعة: 09:09.
- ¹⁰ من إعداد الباحث بالإعتماد على المعطيات المقدمة حسب الموقع.
- ¹¹ عدد مستخدمي الانترنت في العالم على الموقع:
- <https://abuomar.ae/2021/08/05/%D8%B9%D8%AF%D8%AF> اطلع عليه بتاريخ: 2021/11/28 على الساعة 12:59.
- ¹² من إعداد الباحث بالإعتماد على المعطيات المقدمة حسب الموقع.
- ¹³ مريم غوكتاش، مرجع سبق ذكره.
- ¹⁴ المرجع نفسه.
- ¹⁵ المرجع نفسه.
- ¹⁶ شريف عبد الرحمن سيف النصر، مرجع سبق ذكره، ص 10.
- ¹⁷ شريف عبد الرحمن سيف النصر، مرجع سبق ذكره، ص 06.
- ¹⁸ شريف عبد الرحمن سيف النصر، مرجع سبق ذكره، ص 10.
- ¹⁹ Newton Lee (2015), Conterterrorism and cybersecurity, total information awareness, usa, second edition, 2012, p 251.
- ²⁰ Julian Richards (2014) Co-Director, Cyber-War: The Anatomy of the Global Security Threat, Centre for Security and Intelligence Studies, University of Buckingham, UK, p28.
- ²¹ Brandon Valeriano and Ryan C. Maness (2015), cyber war versus cyber realities, Cyber Conflict in the International System, Published in the United States of America by Oxford University Press 198 Madison Avenue, New York, NY 10016, p 19.
- ²² أنظر: نبيل علي ونادية حجازي (2005)، الفجوة الرقمية، رؤية عربية لمجتمع المعرفة، مطابع السياسة، الكويت، ص 13-17.
- ²³ أميرة أبو سمرة، الفضاء السيبراني: مساحات جديدة للتدافع والتغيير؟، مجلة قضايا ونظرات، تجديد الوعي بالعالم الإسلامي والتغيير الحضاري، تقرير ربع سنوي، ع 23، أكتوبر 2021، مركز الحضارة للدراسات والبحوث، ص 13-14-15.
- ²⁴ Paola Ricaurte (2019), Data Epistemologies, The Coloniality of Power, and Resistance, television and new média.
- ²⁵ أميرة أبو سمرة، مرجع سبق ذكره، ص 14-15.
- ²⁶ المرجع نفسه.
- ²⁷ أنظر: نسيم طالب، تر: حليم نسيب صبر، البجعة السوداء، تداعيات الأحداث غير المتوقعة، دار العربية للعلوم ناشرون، بيروت، لبنان، ط 01، 2009 ص - ص 75-274.

²⁸ Paul Rosenzweig (2013), Cyber Warfare How Conflicts in Cyberspace are challenging america andchanging the World, 130 Cremona Drive, P.O. Box 1911 Santa Barbara, California 93116-1911, pp 03-04.

* منظمة الشرطة الجنائية الدولية، تضم 186 دولة عضوا فيها، تم تأسيسها سنة 1923، مقرها مدينة ليون الفرنسية،

مهمتها التنسيق والتعاون الشرطي الدولي في مكافحة الجريمة المنظمة عبر الدول، ولهذه المنظمة مكاتب على مستوى الدول الأعضاء (المكتب المركزي الوطني للأنتربول)، ومن مهامها كذلك ملاحقة وتسليم المجرمين الفارين الدوليين).

²⁹ حمدون إيتوريه الأمين العام للإتحاد الدولي للإتصالات، وفريق الرصد العالمي لأمن المعلومات، والإتحاد العالمي

للعلماء، نوفمبر 2014، ص 07.

³⁰ المرجع نفسه، ص 07-08.