الأمن السيبراني ..المفهوم والأبعاد والمخاطر

عبدالمنعم علي ابوعائشة صوان
كلية الاقتصاد / صرمان / جامعة صبراتة
Abdulmonm1972@gmail.com

الملخص

نتيجة النمو المتسارع لحجم المعلومات والتي ادت بدورها الى تشابك العلاقات والنشاطات المختلفة على مستوى العالم اصبح العصر الحالي هو عصر الثورة الرقمية الالكترونية التي تمارس نشاطها في الفضاء السيبراني وبالتالي اصبح هذا الفضاء الجديد متغير اساسي وعنصر مؤثر في النظام الدولي نظرا لما يحمله من ادوات تكنولوجية متطورة جعلت منه اداة مهمة في التأثير على انماط القوة والامن القومي واساليب الحرب الغير تقليدية.

وهذا ما عجّل بظهور مفهوم جديد هو مفهوم الأمن السيبراني بأبعاده وخصائصه المختلفة, الأمر الذي جعله على رأس أولويات الدول حيث عملت على صياغة جديدة لأمنها القومي بما يتماشى مع التهديدات والمخاطر المتزايدة والمتطورة لهذا المفهوم على امنها القومي.

Summary

As a result of the exciting growth in the volume of information, which has extended to the intertwining of various relationships and activities at the global level, the current era has become the era of the electronic digital revolution that is active in cyberspace. Consequently, this new space has become the basic diversity and an influential element in the international system due to its era of advanced technology tools, an important tool in Power, national security, and unconventional methods of warfare.

This is what hastened the emergence of a new concept, the concept of cyber, with its various dimensions and characteristics, which placed it at the forefront of innovations, as it designed a new formulation for its national security in proportion to the innovation and the increasing and evolving risks of this construction to its national security.

منهجية الدراسة

الإشكالية :

يعيش العالم اليوم عصر المعلوماتية ومن يمتلك المعلومة يمتلك القوة , وإنطلاقاً من هذا أصبح إمتلاك المعلومة وحمايتها مدخلا إستراتيجيا للأمن القومي للدول وهذا راجع الى بروز حروب جديدة عابرة للحدود الجغرافية تخترق البنى التحتية للاتصالات وقواعد البيانات في شتى المجالات . وانطلاقا بما سبق تسعى هذه الورقة البحثية للإجابة عن الإشكالية التالية :- كيف يمثل الفضاء السيبراني فضاءاً للصراع وإمتلاك القوة وماهي التهديدات التي يشكلها الفضاء على الأمن المجتمعي وعلى الامن القومي للدول ؟

الفرضية

تزداد مخاطر الفضاء السيبراني كلما زاد الاعتماد عليه وبهذا فهو يشكل منطلقاً جديداً لاختراق الدول نتيجة ما يحدثه من تهديدات أمنية بالغة التأثير والخطورة سواء على المؤسسات او على الدولة ,وعليه .. فإن دراسة ومعرفة الاستراتيجية التي يقوم عليها الفضاء السيبراني هي جزء من آليات مواجهة التهديدات التي يحدثها هذا الفضاء على الأمن المجتمعي والدولة بشكل عام.

أهمية الدراسة : تنبع أهمية الدراسة من التهديدات والمخاطر التي تحدثها البيئة *الجديدة(الفضاء السيبراني)* على الأمن القومي بالنظر الى حالة تزايد الإعتماد عليه محلياً ودولياً.

منهج الدراسة:

نظرا لطبيعة الدراسة ,فإن المنهج المستخدم هو منهج دراسة الحالة والذي بدوره يشكل المنهج المناسب لدراستها في مثل هكذا قضايا , كما يهدف هذا المنهج للتعرف على وضعية واحدة بطريقة تفصيلية ودقيقة .

تقسيمات الدراسة:

ان الدراسة في ضوء اشكاليتها الاساسية وفرضيتها العلمية تقترن بتقسيمات علمية تتمثل في التالي:-

- التعريفات الاجرائية للدراسة
- المفاهيم النظرية للدراسة وتتمثل في دراسة مفهوم الامن السيبراني والفضاء السيبراني ومستوياته المعلوماتية

- ابعاد الامن السيبراني
- المخاطر والتهديدات
- الخلاصة
- المصادر العلمية

أهداف الدراسة:

تسعى هذه الدراسة الى تبيان مفهوم الأمن السيبراني بدايةً والأبعاد المختلفة التي يشكلها هذا المفهوم والمخاطر المتزايدة التي يشكلها على الأمن الوطني ومدى حالة الإختراق المحتمل اذا أخذنا بعين الأعتبار المتغيرات المستجدة على حالة الأمن الوطني والإقليمي في المنطقة العربية كما تهدف الدراسة للتعرف على خطورة الإعتماد على هذا الفضاء دون التمكن من التقنيات الدفاعية المعلوماتية من الإختراق وتعرض المصالح الحيوية للخطر سواء داخلياً او خارجياً.

الدوافع الذاتية:

– الإهتمام الشخصي بهذا الموضوع وإدراك مخاطره على الأمن القومي.

– محاولة إثراء النقاش بمثل هذه المواضيع وتبيان مخاطرها المحتملة على الامن القومي .

الدوافع الموضوعية:

معرفة طبيعة الآثار التي يحدثها هذا الفضاء على الأمن القومي وتبيان المخاطر التي تنشأ عنه بالنظر الى حالة الإعتماد المتزايد عليه في تقديم الخدمات المجتمعية دون وجود تقنيات لمواجهة الإختراق الذي ينشأ عنه ترافقاً مع تشابك مصالح العالم *والتهديدات التي يشكلها الفضاء على الأمن المجتمعي وعلى الدولة ..*

مفاهيم الدراسة:

الفضاء السبراني : هو منظومة من العناصر المتفاعلة فيما بينها والمتكونة من أجهزة الكمبيوتر , أنظمة الشبكات ,البرمجات , نقل وتخزين البيانات ومستخدمي هذه العناصر المادية والفضاء الرقمي لتشكل منظومة معلوماتية في إطار برمجيات التواصل الإلكتروني [1].

الأمن السبراني: هو الجهد المستمر لحماية الشبكات المتصلة معاً وكافة البيانات من الاستخدام غير المصرح به او الذي يسبب الضرر على المستوى الشخصي او المؤسساتي وعلو مستوى الدولة.

الحرب الألكترونية : يعد تعريف **ريتشارد كلارك** مستشار البيت الأبيض السابق من أبسط التعريفات وأشملها حيث عرَف الحرب الإلكترونية بأنها الإجراءات المتخذة من قبل الدولة لإختراق أجهزة الكمبيوتر والشبكات التابعة له من دولة لدولة أخرى لغرض تحقيق أضرار بالغة او تعطيلها[2].

اذا فهي حرب إفتراضية تجري معاركها في فضاء مفتوح وتعتمد بالأساس على تكنولوجيا المعلومات والإتصالات والبرامج والشبكات والإنترنت مستهدفةً دولاً ومنظمات وأفراد.

الهجمات السيبرانية: هو إستخدام طرق غير مشروعة لإختراق خصوصية الأفراد او المؤسسات او الشركات والمنظمات اوحتى الحكومات وذلك بهدف الإستيلاء على المعلومات بهدف الإبتزاز المالي او إلحاق الأذى بالجهة المستهدفة كالفضائح واثارة البلبلة وغيرها,او عمليات التجسس او سرقة الإبتكارات.

المقدمة

شكلت الثورة المعلوماتية وانتشار الإنترنت على مستوى العالم ظهور كيان إفتراضي آخر هو الفضاء السيبراني .إنتشر هذا الكيان بشكل واسع على المستوى المحلي والدولي واصبح الإعتماد عليه يتزايد بشكل رهيب ما جعله يشكل مجالا جديداً وبيئة جديدة للصراع بين الدول ,فلم تعد المجالات الأربعة التي عرفت في المواجهة المسلحة التقليدية بين الدول (البر ,البحر ,الجو, والفضاء) وحدها أدوات الصراع بل دخل عنصر آخر وخامس وهو الفضاء السيبراني حيث من المتوقع ان تكون الحرب الإلكترونية هي السمة الغالبة ان لم تكن الرئيسية للحروب المستقبلية في القرن الواحد والعشرين وان لم تكن حربا فسيكون الفضاء السيبرانيي أحد اهم أدوات الصراع في هذا القرن.

ولما كانت الدول اليوم تعتمد بنسبة عالية على هذا الفضاء في تسيير شؤونها العامة فإن اى اختراق أو تعطيل للمنظومة التقنية المعتمدة يشكل تهديداً مباشراً لأمنها القومي سواء كان التهديد من قبل دولة او مجموعة من الدول او حتى من غير الدول الأمر الذي يدفع بالدول الى تحصين دفاعاتها المعلوماتية ضد أي سلوك يستهدف أمنها السيبراني.

تحاول هذه الورقة البحثية تبيان ومعرفة ماهية الأمن السيبراني وأبعاده المختلفة والتهديدات والمخاطر التي يشكلها على الأمن القومي للدول .

المطلب الأول : مفهوم الأمن السيبراني :

الأمن لغة : تعنى الأمان وهو ضد الخوف وتعني أيضا تحقيق الطمأنينة والحماية والصدق وكلها ضد الخوف , اما اصطلاحا : تعني القدرة على مواجهة الأخطار والتحديات وتأمين الحاجات الأساسية للإنسان [3] ولعل المفهوم الشامل للأمن هو ما ورد في القرآن الكريم في قوله سبحانه وتعالى (فليعبدوا رب هذا البيت الذي أطعمهم من جوع وآمنهم من خوف) فالأمن في هذا المستوى يعني السلامة والإستقرار [4] .

على مستوى الدولة فالأمن يعرَف بالقدرة , أي قدرة الدول والمجتمعات للحفاظ على كيانها المستقل وقد عرَف علماء الإجتماع الأمن بأنه قدرة الأمة على حماية قيمها الذاتية من الأخطار الخارجية بغض النظر عن الشكل الذي تتخذه تلك التهديدات الخارجية وان الأمن لا يعني فقط رغبة الدول في البقاء بل رغبتها ايضا في العيش بدون تهديدات خارجية [5].

في هذا السياق وفي إطار البحث في قضايا التهديدات الخاصة فإن الثورة المعلوماتية والإتصالية ثورة شاملة في جميع نواحي الحياة حيث إستطاع العقل البشري (بقدرة الله) ان يطور تقنية الإتصالات بما يتناسب وحاجاته واستطاع الوصول الى طرق لتوصيل المعلومات من مكان لآخر بشكل سريع جدا .على الرغم من الحواجز الطبيعية والسياسية التي تفصل بينه , حيث اصبح الانسان قادرا على الوصول الى أي معلومة يريدها باستخدام جهاز صغير يحمله في جيبه .

لابد من الإشارة هنا الى أن عقد الثمانينات والتسعينات من القرن العشرين شهد تركيزا ملحوظا على موضوع المعرفة وعلاقتها بثورة الإتصالات من ناحية وعلاقتها بتنامي المجتمع المعلوماتي من ناحية اخرى , وتشكل العولمة هنا احد ركائز هذا المجتمع المعلوماتي فهي في هذا الجانب تجسيدا للتطورات الحياتية والفكرية والتكنولوجية المتلاحقة والمتشابكة التي تؤدي في النهاية الى إنكماش العالم من حيث الزمان والمكان وتحول العالم بطابعه المادي الى عالم رقمي إفتراضي حيث انتقلت كافة مجالات الحياة لتأخذ طابعا رقميا يدور في فلك الفضاء الإلكتروني. (*)

وعلى هذا الأساس تشكل هذا الفضاء، الذي هو من صنع العقل البشري الذي يعتمد على نظم الكمبيوتر وشبكات الإنترنت وكم هائل من المعلومات والبيانات والأجهزة.

تاريخيا : ان الإهتمامات الأولى بهذا الأمر كانت في عام 1967 عندما قام المهندسwillis ware بإعداد ورقة بحثية بعنوان "الأمن والخصوصية في نظم الكمبيوتر" والتي أشار فيها الى خطورة مشاركة البيانات والملفات وشبكات الكمبيوتر المتصلة بالانترنت .

- يدور مصطلح المعلوماتية في فضاء واسع من الحقول والتخصصات المتنوعة ويرتبط بابعاد وعلاقات ومداخل متباينة منها ماهو واضح ومرئي ومنها ما هو مؤثر وحيوي وغير مرئي . وتعتمد على التدفق اللامتناهي واللامحدود للمعرفة والافكار

وقبل الخوض في عنصر الأمن في هذا السياق , لابد ان لنا بداية من التعرف على مفهوم الامن السيبراني حيث هناك من عرفه بأنه "الذراع الرابعة للجيوش الحديثة"[6] وهناك من يرى انه "البعد الخامس للحرب" . الا انه يمكن الإعتماد على تعريف الإتحاد الدولي للإتصالات الذي يصف الفضاء السيبراني بانه "المجال المادي وغير المادي الذي يتكون وينتج عنه عناصر هي : اجهزة الكمبيوتر ,الشبكات, البرمجيات , موسوعة المعلومات , المحتوى , معطيات النقل والتحكم ومستخدموا هذه العناصر[7].

وعليه يمكن القول بأن الفضاء السبراني هو بيئة تفاعلية حديثة تشمل عناصر مادية وغير مادية مكونة من أجهزة رقمية وأنظمة الشبكات والبرمجيات والمستخدمين سواء مشغلين او مستعملين. وتجدر الإشارة الى مسألة تحديد مفهوم الفضاء السيبراني فهى مسألة نسبية تتوقف على طبيعة إدراك وفهم كل من الدول والهيئات والافراد كلا حسب رؤيته واستراتيجيته وقدرته على استغلال المزايا المتاحة ومواجهة المخاطر الكامنة في هذا الفضاء [8] .

لقد اصبحت شبكة المعلومات الإلكترونية المتصلة جزءاً لا يتجزأ من الحياة اليومية حيث تستخدم المؤسسات التعليمية والطبية والمالية هذه الشبكة للعمل وتستخدم الشبكة المعلوماتية وتشاركها لذلك اصبحت حماية هذه المعلومات اكثر حيوية لأمننا القومي واستقرارنا الإقتصادي .

ان الامن السيبراني هو الجهد المستمر لحماية هذه الشبكات المتصلة معا وكافة البيانات من الاستخدام غير المصرح به او الذي يسبب الضرر على المستوى الشخصي والمؤسساتي او على مستوى الدولة [9].

ولهذا فإن سلامة المعلومات سواء كانت شخصية او على مستوى الدولة في خطر مالم تتخذ كافة

التدابير الكفيلة بحماية هذا الكم الهائل من المعلومات ولهذا أصبح الفضاء السيبراني بعدا هاما اخر للحرب حيث يمكن للدول ان تنفذ صراعات دون مواجهات تقليدية , وتعتبر الحرب الالكترونية صراعا قائما على الانترنت ينطوي على اختراق انظمة الحاسوب وشبكات الدول الاخرى يمتلك المهاجمون خبرات وقدرات لشن هجمات على الانترنت ضد دول اخرى لإحداث ضرر او تعطيل خدمات ويعد الغرض الأساسي من حروب الانترنت هو التفوق على الخصوم سواء كانوا دولا او مؤسسات اوافراد. لقد اصبح الفضاء السيبراني احد العناصر الاساسية التي تؤثر في النظام الدولي بما يتيحه من ادوات تكنولوجية مهمة لعمليات الحشد والتعبئة في العالم , فضلا عن التأثير في القيم السياسية , فسهولة الاستخدام ورخص التكلفة زاد من قدرته على التأثير في مختلف مجالات الحياة سواء سياسية او اقتصادية او عسكرية او ايدلوجية . وبات جليا من يمتلك آليات توظيف البيئة السيبرانية يصبح اكثر قدرة على تحقيق اهدافه والتأثير في سلوك المستخدمين لهذه البيئة [10].

المطلب الثاني : خصائص وابعاد الأمن السبراني .

اختصر الفضاء السيبراني حاجز الزمان والمكان وخلق مساحات للتفاعلات الداخلية والدولية . ومن ثم برزت فضاءات جديدة للصراع بادوات مختلفة وانماط جديدة تختلف عن الصراعات التقليدية بعد أحداث 11من سبتمبر 2001 التي تعد مفصلية في تاريخ العلاقات الدولية لبداية إستعمال الجماعات الإرهابية للإنترنت بشكل بارز في الترويج للفكر المتطرف [11] . ولا شك ان إزدياد الهجمات الإلكترونية والتي نشهد جزءاً بسيطاً منها اليوم يرتبط ايضا بإزدباد هذا الإعتماد على شبكات الإنترنت في البنية التحتية الوطنية الأساسية وهو ما يعني إمكانية تطور الهجمات الإلكترونية اليوم لتصبح سلاحاً حاسماً في النزاعات بين الدول في المستقبل.

والجدير ذكره أن أبعاد مفهوم الحرب الإلكترونية لا تزال غير مفهومة لدى شريحة واسعة من المراقبين وليس هناك من إجماع على تعريف محدد ودقيق للحرب الإلكترونية حيث تعرفها وزارة الدفاع الإلكترونية بأنها " إستخدام أجهزة الكمبيوتر والإنترنت لإجراء الحرب في الفضاء الإلكتروني " [12] او الرسائل الرقمية من قبل حكومة او بمعرفتها او موافقة صريحة منها ضد دولة اخرى او ملكية خاصة داخل داخل الدولة بما في ذلك الوصول المعتمد او اعتراض البيانات او تدمير البنية التحتية الرقمية وإنتاج وتوزيع الأدوات التي يمكن إستخدامها لتخريب النشاط المحلي " [13].

ومن هذا التعريف نستدل ان حروب الفضاء الإلكتروني لها أدوات جديدة ومسرح جديد هو الفضاء الإلكتروني تضاف الى المجالات التقليدية في الحروب. كما ان هذه الحروب يمكن ان تشن من قبل فاعلين من غير الدول وهي بهذا تتميز بصعوبة وتعذر امكانية تحديد العدو والجهة المهاجمة.

ان التطبيق الأول المباشر لهذا النوع من الهجمات في حرب فعلية جاء مع حرب الخليج الثانية عام 1991 حيث قامت الولايات المتحدة بإختراق وتعطيل منظومة الدفاع الجوي العراقية كما قامت بتدمير كابلات الألياف الضوئية وشبكة الاتصالات العسكرية الممتدة من بغداد حتى البصرة، ثم تطور إستخدام مثل هكذا وسائل في الصراعات بين الدول فكانت الهجمات المتبادلة بين الهند وباكستان وذلك على خلفية النزاع الطويل الأمد بين البلدين بشأن كشمير عام 1999م. وفي عام 2009 نفذت (اسرائيل) بالتعاون مع الولايات المتحدة هجوماً على المنشأة النووية الإيرانية حيث تمكنت وحدة مشتركة من نشر فيروس حاسوبي يطلق عليه ستوكس نت " stux net" داخل المرفق وإستهدف الفيروس نظام التشغيل لأجهزة الطرد المركزي المستخدمة في تخصيب اليورانيوم مما أدى الى جعلها تتحرك بوتيرة خارجة عن السيطرة فتسبب ذلك بتكسُرها وكانت هذه الأجهزة من طراز [cl000] وهي أجهزة متطورة وإتجهت الإتهامات آنذاك مباشرة الى الولايات المتحدة و(إسرائيل)إلَا أنهما نفتا الإتهامات[14].

ويشكل بث الفيروسات والبرامج التخريبية المدمرة للأنظمة والشبكات الحاسوبية وإختراق الحسابات والوصول الى المعلومات السرية وتسريبها او الإستفادة منها لأغراض عسكرية وأمنية وعدائية بعداً آخر للحرب السيبرانية اذ يمكن ان تستهدف ايضا الهجمات السيبرانية أهدافاً مدنية وقطاعات خدمية وإنتاجية وما يحدث أثناء هذه اعداد الدراسة من هجمات على محطات تزويد بالوقود في إيران مثالاً آخر لهذه الهجمات .

وبشكل عام فإن الهجمات السيبرانية مكَنت دولا متفاوتة القوه من استخدامها وكذلك تنظيمات من غير الدول من شن هجمات ضد الدول ذات القوه العسكريه والاقتصاديه الاكبر وهو ما يعرف بالحروب اللامتماثله .

ولا يقتصر الامر في الهجمات السيبرانيه علي الحاق الضرر المادي بالخصم وانما احيانا سرقه

المعلومات والتوصل الي معلومات ذات طبيعة سريه يستخدمها المهاجم سواء اكان من الدول او من غير الدول اثناء الحاجه اليها .

تمثل خاصيه عدم امكانيه تحديد مصدر الهجوم التي يتميز بيها هذا النوع من الحروب ويجعله مختلفا عن الحروب التقليدية، الامر الذي يؤدي الي زعزعه قواعد الاشتباك التقليدية واضعاف سياسة الردع[15]. كما تشكل التكلفة المتدنية نسبيا للأدوات اللازمة لشن هكذا حروب بمعني انه ليس هناك حاجه لقدرات ضخمه لتشكيل تهديد خطير وحقيقي لدوله ما تشكل نوع اخر من الحروب اللا تناضريه كما ان المخاطر التي يشكلها هذا النوع من الحروب تتعدي استهداف المواقع العسكريه كاستهداف شبكات الكهرباء وشبكات النقل والنظام المالي والمنشئات الحساسة بواسطه فيروس يمكنه احداث اضرار ماديه حقيقيه تؤدي الي دمار هائل، كما ان هذا النوع من الحروب يتمتع فيها المهاجم بأفضلية واضحه وسرعه ومرونة وهو ما يجعل مهمة الدفاع عملية صعبه ومعقده.

المطلب الثالث : المخاطر والتهديدات .

من المتعارف عليه في العلاقات الدولية ان مصادر قوة الدولة تتغير فإلى جانب القوة الصلبة ممثلة في القدرات العسكرية والاقتصادية تزايد الإهتمام بالأبعاد الغبر مادية للقوة ومن ثم برز مفهوم القوة الناعمة التي تعتمد على جاذبية النموذج والأقناع , ومع ثورة المعلومات ظهر بشكل جديد شكل من أشكال القوة متمثلة في القوة السيبرانية cyberpower التي لها تأثير كبير على المستوى المحلي والدولي , فمن ناحية أدت الى توزيع وإنتشار القوة بين عدد أكبر من الفاعلين مما جعل قدرة الدولة على السيطرة موضع شك ومن ناحية أخرى منحت الفاعلين الأصغر قدرة أكبر على الممارسة كل من القوى الصلبة والناعمة عبر الفضاء السيبراني وهو مايعني تغييراً في علاقات القوى في السياسة الدولية .

ولعل أبرز ما يعزز إنتشار الأنشطة غير السلمية في الفضاء السيبراني إرتباط العالم المتزايد به وزيادة خطر تعرض المعلومات لهجمات سيبرانية بالإضافة الى إستخدام الفاعلين من غير الدول للفضاء السيبراني لتحقيق أهدافهم والتأثير على سيادة الدولة كما كان لأنسحاب الدولة من قطاعات إستراتيجية لصالح القطاع الخاص دوراً مهماً في تنامي الأنشطة غي السلمية في هذا الفضاء وهكذا كشف إستخدام الفضاء السيبراني عن إمتداد حالة الصراع داخل شبكات الإتصال والمعلومات متجاوزاً

الحدود التقليدية وسيادة الدولة كما كشف عن حالة صراع جديدة بعيداً عن الصراعات التقليدية التي تخوضها الدولة أو الفاعلين من غير الدول على خلفيات دينية أو عرقية او ايدلوجية [16], ومن الملاحظ ان هذا النوع من الصراعات له عدة أنواع او أشكال فهناك صراع تحركه دوافع سياسية ويأخذ شكلاً عسكرياً ويتم فيه استخدام قدرات هجومية ودفاعية عبر الفضاء السيبراني ويوجد صراع آخر ذو طبيعة ناعمة يرتكز حول الحصول على المعلومات والتأثير على المشاعر والأفكار وشن حروب نفسية وإعلامية كما يأخذ الصراع السيبراني شكلاً آخر متمثل في التنافس حول الإستحواذ على سبق التقدم التكنولوجي وسرقة الأسرار الإقتصادية والعلمية والتحكم بالمعلومات والعمل على إختراق الأمن القومي للدولة كهجمات قراصنة الإنترنت والتجسس بما يكون له تأثير على تدمير الإقتصاد والبنى التحتية بنفس القوة التي يحدثها تفجير تقليدي .

كما يمكن ايضا ان يستخدم الفضاء السيبراني كوسيلة من وسائل تحشيد الصراع داخل الدولة بين مكوناتها على أساس طائفي او طبقي او عرقي والشواهد على ذلك كثيرة في الوقت الحالي وخاصة في محيطنا الإقليمي وما شكله ما يسمى بالربيع العربي لخير مثال على ذلك .

لقد دفعت الهجمات الإلكترونية الكثيرمن الدول لإتخاد إجراءات وقائية للحد من الأضرار الناجمة من تلك الهجمات التي تستهدف الدولة ومؤسساتها وقامت بتطوير قدراتها الدفاعية والهجومية في مجال الحرب الإلكترونية وعلى رأس هذه الدول الولايات المتحدة الأمريكية والصبن وروسيا .

على الرغم من إمتلاك الولايات المتحدة للقدرات والتقنيات الهجومية العالية إلا انه من الواضح ان اهتماماتها إنصبت مؤخرا على تعزيز القدرات الدفاعية في هذا المجال ونظرا لأنها الدولة الأكثر اعتمادا في العالم على الإنترنت وعلى الشبكات في مختلف القطاعات المدنية والعسكرية تبدو أنها الأكثر إهتماما بالجانب الدفاعي فيمل يتعلق بالحروب الإلكترونية فقد تضاعفت الميزانية المقررة لوزارة الدفاع الأمريكية ثلاثة أضعاف في عهد الرئيس الأسبق باراك أوباما لتصبح 7 مليارات دولار واستخدمت وزارة الدفاع الأمريكية وحدة متخصصة مكرسة لقيادة الحرب الالكترونية اما العاملون من قبل الجيش الأمريكي في هذا المجال فقد تضاعف ايضا من 1900 الى أربعة آلاف شخص ومن المتوقع ان يصل عددهم الى ستة عشر ألف شخص في السنوات القادمة ولا يقتصر هذا التوسع على أمريكا فقط فقد وصل عدد الدول التي أخذت حذوها الى عشرين دولة[17]

وتنقسم التهديدات السبرانية التي تواجهها الدول والأفراد الى أربعة أنماط رئيسية هي [18]:

1. هجمات الحرمان من الخدمة :

حيث يتم إطلاق حزمة كبيرة من الطلبات والمهمات على خوادم الضحية بصورة تفوق قدرة الخادم او الجهاز على معالجتها والاستجابة لها مما يؤدي الى توقفه بصورة جزئية او كلية او إبطاء عمله وهذا ما يسبب ضررا للمستخدم النهائي وهي تستعمل كثيرا ضد مواقع الإنترنت او البنوك او المؤسسات من اجل التأثير عليها او دفع فدية مالية .

2. إتلاف المعلومات او تعديلها :

ويقصد به الوصول الى معلومات الضحية عبر شبكة الإنترنت او الشبكات الخاصة والقيام بتعديل البيانات الهامة دون ان يكتشف الضحية ذلك فالبيانات تبقى موجودة لكنها مضللة وقد تؤدي الى نتائج كارثية خاصة اذا كانت خطط عسكرية او مواعيد او خرائط سرية.

3. التجسس على الشبكات :

ويقصد به الدخول غير المصرح والتجسس على الشبكات الخصم دون تدمير او تغيير البيانات والهدف منه الحصول على معلومات قد تكون عبارة عن خطط عسكرية او اسرار حربية او إقتصادية , مالية , او سياسية مما يؤثر سلبا على مهام الخصم .

4- تدمير المعلومات :

ويتم فيه مسح وتدمير كامل للأصول والمعلومات والبيانات الموجودة على الشبكة يصطلح عليه " تهديد لسلامة المحتوى " ويعني بها احداث تغيير في البيانات سواء بالحذف او التدمير من قبل اشخاص غير مخولين .

وهناك من يميز بين عدة انواع لمخاطر التهديدات السيبرانية منها: [19]

. النعرض لسرية الإتصالات التي تطال البريد الإلكتروني والدخول الى الأنظمة والملفات دون إذن وهذا إعتداء على الحريات والحقوق الشخصية .

. الجرائم العادية التي تستخدم الإنترنت للسرقة والغش وسرقة الهويات والإعتداء على الملكية الفكرية وغيرها .

. الجرائم التي تتدرج في اطار الجريمة المنظمة والتي تهدد أمن الأفراد والدول كتبييض الأموال , وتمويل الإرهاب .

وأخيراً.. فإنه يمكن القول ان الفضاء السيبراني أصبح تهديدا جديدا لأمن الدول والأفراد واذا كان الأمن القومي يهتم بالحماية من التهديدات وانتفاء حالة الخوف من التعرض لهجمات فان الفضاء السيبراني قد فرض إعادة التفكير في مفهوم الأمن القومي للدول والذي يتعلق بدرجة تمكن الدولة من ان تصبح في مأمن من خطر التعرض للهجوم وإجراءات الحماية ضد تعرض المنشآت الحيوية فيها للتهديد من خلال الإستخدام السيئ لتكنولوجيا الاتصال والمعلومات.

قائمة المراجع

1- د.إسماعيل زروقة ,الفضاء السيبراني والتحول في مفاهيم القوة والصراع ,مجلة العلوم القانونية والسياسية ,المجلدة /العدد/ ابريل 2019 ,ناصر 106 .

2_ karsten friis_Jens Ringsmose _concflect in cyper Space : Theoretical _strategic and legal Perspectives Routledge _2016_P:87

3. أرض الظلام :التاريخ السري للحرب السيبرانية , فريد كابلن (المركز الإقليمي للدراسات الإستراتيجية 2016,) ،ص352

*للمزيد حول كلمة الأمن : ابن المنظور ، لسان العرب ، دار إحياء التراث ، بيروت 1999 ، ص222.

4. القرآن الكريم ، سورة قريش ، الآية 2،3 .

5. رفعت سيد احمد، الامن القومي العربي بعد حرب لبنان، مجلة الشؤون العربية، العدد 35، 1983, ص8.

6. عباس بدران ،الحروب الإلكترونية : الاشتباك في عالم متغير ،مركز دراسات الحكومة الالكترونية , بيروت ,2010,ص4

7. المرجع السابق

8. المرجع نفسه

9الفضاء السيبراني والتحول في مفاهيم القوة والصراع , د. اسماعيل زروقة, مجلة العلوم القانونية والسياسية ,المجلدة ,العدد , ص118

10- مقدمة في الامن السيبراني ,ترجمة اسامة حسام الدين, اكاديمية cisco, ينبع ,المملكة العربية السعودية,2017,ص8

11- الفضاء السيبراني والتحول في مفاهيم القوة والصراع, مرجع سابق ,ص119

12-عادل عبدالصادق, اسلحة الفضاء الالكتروني في ضوء القانون الدولي سلسلةاوراق,العدد23,مكتبة الاسكندرية, مصر, 2016,ص17
13- علي حسين باكير, المجال الخامس الحرب الالكترونية في القرن الواحد والعشرين, مركز الجزيرة للدراسات, 12يناير 2011
14- للمزيد: انظر كتاب فريد كابلان حول التاريخ السري للحرب الالكترونية في نشوء وتطور البنية التحتية لهذا النوع من الحروب
15-فاطمة عيتاني, الوحدة الاسرائيلية8200 ودورها في خدمة التكنولوجيا التجسسية الاسرائيلية, ط1(بيروت: مركز الزيتونة للدراسات, 2019), ص120
16- فريد كابلان, المنطقة المعتمة, التاريخ السري للحرب السيبرانية, ترجمة لؤى عبدالمجيد,ط1(الكويت: المجلس الوطني للثقافة والفنون والاداب,2019),ص126
17- عادل عبدالصادق, اسلحة الفضاء الالكتروني في ضوء القانون الدولي, مرجع سابق, ص18
18-عمر حامد شكر, المجال الخامس- الفضاء الالكتروني, المعهد المصري للدراسات, ص125
19- المرجع السابق,ص127

الخلاصة

تكمن خطورة الفضاء السيبراني في كون العالم اليوم اصبح يعتمد عليه اكثر فأكثر لاسيما في البنى التحتية المعلوماتية والعسكرية والحكومية والمصرفية والخدمية إضافة الى المؤسسات والشركات وهو مايدل على ان مفهوم الأمن مفهوما شاملاً قابل للتأثير باي معطى أولي او ظاهرة دولية ويشكل عصر المعلوماتية فرصا وتحديات يفرضها هذا التغيير على أمن وسلامة الدول فإذا كان هذا التغيير قد ساعد الدول والشعوب في سهولة استخدام ادواته التقنية في شتى المجالات فان تحديات وتهديدات يفرضها وبقوة على تراجع سيادة الدول في ظل هذه التقنيات التي أثرت بشكل كبير على منظومتها الأمنية فالعلاقة بين الأمن السيبراني والأمن القومي تزداد كلما زاد نقل المحتوى المعلوماتي والعسكري والأمني والفكري والسياسي والإقتصادي والخدمي والعلمي البحثي الى الفضاء السيبراني خاصة مع تسارع الدول في تبني الحكومات الإلكترونية والمدن الذكية في العديد من دول العالم واتساع نطاق وعدد مستخدمي الإنترنت في العالم وسهولة ورخص تكلفة الخدمة وهو ما يستوجب على الدولة تبنى تغييرات في العقيدة الأمنية وذلك بإدراج القوة السيبرانية كمحدد رئيس لمدى قوة الدولة وقدرتها على حسم الصراعات والنزاعات لصالحها .