الفضاء السيبراني و تحديات الأمن العالمي

Cyberspace And Global Security Chalenges

أ.م.د/حميد صغير سعد الريمي،
أستاذ مشارك بقسم علوم الحاسوب
كلية علوم و هندسة الحاسوب، جامعة الحديدة،
Email:halraimi@gmail.com

ملخص البحث

خلال العقود الثلاثة الأخيرة تغير عالمنا تغيراً كبيراً، مع التطور السريع و الهائل لتكنولوجيا المعلومات و الاتصالات، و انتقلت الكثير من الأعمال في مختلف المجالات إلى ما نسميه اليوم بالفضاء السيبراني. و قد برزت أهمية الفضاء السيبراني في العامين الأخيرين مع ظهور فيروس كوفيد ١٩ المستجد، فجائحة كورونا تسببت في فرض القيود على السفر، والحجر المنزلي، وتخفيض القوى العاملة في جميع القطاعات الاقتصادية، مما أدى إلى فقدان العديد من الناس لوظائفهم، كما أغلقت المدارس والجامعات. كان لجائحة كورونا دور كبير في تسريع التحول الرقمي لمختلف الأنشطة الاقتصادية بمختلف قطاعاتها. فأهمية الفضاء السيبراني تكمن في أنه أصبح اليوم البيئة الحاضنة لمختلف الأنشطة في مختلف القطاعات.فلم يكن العمل في الفضاء السيبراني آمناً؛ بسبب الكثير من التحديات و التهديدات الموجودة اليوم في هذا الفضاء، فالتحديات و التهديدات خطيرة جدا، تمثلت في ظهور جرائم عدة، منها الاقتصادية، والسياسية، والأخلاقية. فالجريمة السيبرانية المعاصرة أصبحت تمثل خطرا على الفرد والمجتمع وعلى أمن الدولة؛ لأنها تتقدم بوتيرة سريعة إذ يستخدم المجرمون أحدث التقنيات في تنفيذ هجماتهم السيبرانية، لذا لابد من مواكبة الفضاء السيبراني والتعرف على كل التحديات التي باتت تهدد الدول و المؤسسات و الأفراد، وكذا التعرف على طرق التصدي لهذه الجرائم المستحدثة باستخدام التقنيات الحديثة التي تحد منها، هذه الجرائم و بضرورة سن قوانين وأنظمة تختص بمكافحة الجرائم السيبرانية، وفرض العقوبات على المجرمين.

Abstract

During the last three decades our world has greatly changed with the rapid and huge developments of information and communication technology. Hence, too many works in different fields have been transferred to what we call today "the cyber space". The importance of cyber space has raised in the last two years with the appearance of newly covid19, the cataclysm that has caused imposing restrictions for travelling, home quarantine and lowering human capital (workers) in all economic fields which has resulted in many people losing their jobs and closing schools and universities. Coronavirus cataclysm has a great role in quickening the digital converting of various economical activities in all their diverse sectors. The importance of cyber space lies in the fact that it has become the incubating environment of different activities in several fields. Nevertheless, working in cyber space is insecure due to plenty of challenges and threats that exist today in this space. These challenges and threats are very dangerous, exemplified in the appearance of several crimes: economic, political, and moral crimes. Modern cyber-crimes have become a danger to the individual, the community and the state security, as they are speedily developing and the criminals use the newest and most modern techniques in achieving their cyber-attacks. Therefore, it is necessary to keep up with cyber space and to know all the challenges that are threatening the countries, the institutions and the individuals. In addition, we should learn the ways of confronting these new crimes by using modern techniques that refrain them, in addition to legislating laws and regulations related to fighting cyber-crimes and imposing retributions on criminals.

الكلمات المفتاحية : الفضاء السيبراني (Cyber Space)، الجريمة السيبرانية (Cyber crime)، إنترنت الأشياء (Internet of Things)، الحكومة الإلكترونية (E-Government)، التعليم الإلكتروني (E-learning)، الجيوش السيبرانية (Cyber Armies)، التجارة الإلكترونية (E-Trade)، الحرب السيبرانية (Cyber War)، القوة السيبرانية (Cyber Power).

المحور الأول: الإطار المنهجي للدراسة

أولا: المقدمــة

شهدت البشرية منذ سنوات تقدما تقنيا وتكنولوجيا، قلما عرفه عصر من العصور السابقة من قبل، حتى بات هذا التقدم ثورة قائمة بذاتها في عالم الاتصالات والعلاقات الدولية، وأصبح العالم بفضل هذه التكنولوجيا بمثابة قرية كونية. إذ يُعَدُّ الإنترنت من أسرع وسائل الاتصالات التي عرفها الإنسان حيث أصبحت خدماته اليوم تغطي العالم بأسره، بحسب الإحصائيات[1]. كان عدد مستخدمي الإنترنت في العالم في العام ٢٠١٠م فقط ٢,٠٢٩,٤٦٨,٧٨٢، أي ما يقارب ثلث سكان العالم أو ما يعادل ٢٩,٦٪ من إجمالي السكان في العالم والذين قدرهم التقرير ب ٦,٨٤٥,٦٠٩,٩٦٠ نسمة، في حين كان عدد مستخدمي الإنترنت في العام ٢٠٠٠م قرابة ٣٦١ مليون مستخدم[2]، وفي مارس من العام ٢٠٢١ وصل عدد مستخدمي الإنترنت إلى نحو ٥,١٦٩٠٠٠٠٠٠[3]، هذا النمو السريع جعل من الإنترنت وسيلة الاتصال الأسرع نموا في تاريخ البشرية. فالتطور السريع في تقنية المعلومات والاتصالات، وكذا دخولها مختلف مجالات الحياة فرض على الجميع ممارسة جميع الأعمال و الأنشطة في بيئة افتراضية تسمى بالفضاء السيبراني، فأصبح اليوم لهذا الفضاء السيبراني دور كبير، تمثل في فتح مجال جديد للعلاقات الدولية،و أحدث تغييراً كبيراً في حركة التفاعلات والتحولات البنيوية، وبدأ ينتقل تأثيره من تغييرات هيكلية وتحتية إلى إحداث تغييرات كيفية في النظام الدولي، و بسبب ظهور وباء كوفيد١٩ المستجد في نهاية العام ٢٠١٩ انتقلت الكثير من الأعمال في مختلف المجالات للفضاء السيبراني، صاحب ذلك بروز العديد من التحديات و المخاطر، مخاطر باتت تهدد الأفراد و المؤسسات و الحكومات في جميع أنحاء العالم. مخاطر حاولت و تحاول التأثير على مجريات العالم السياسية والاقتصادية من جهة، والمعطيات الأمنية والعسكرية من جهة ثانية، و هذا يعود إلى أن جزءاً كبيراً من الصراعات بين القوى العظمى في العالم انتقلت إلى الفضاء السيبراني، لذا يشهد العالم اليوم سباق تسلح

سيبراني يرافقه توتر كبير في العلاقات الدولية، هذا التوتر من شأنه أن يتسبب في نشوب صراعات و حروب مستقبلية، سيكون الفضاء السيبراني هو المسرح الذي ستدور فيه تلك الصراعات و الحروب. في ظل هذه التكنولوجيا المتطورة يشهد العالم تغيرات سريعة جدا، تغيرات ايجابية وسلبية، كانت التغيرات السلبية لها درجة أقوى من التأثير على عالمنا خاصة في مجال المساس بأمن الدول؛ نتيجة انتشار الهجمات في الفضاء السيبراني، الأمر الذي فرض على كثير من الدول رسم خطط، و وضع إستراتيجيات، و سن قوانين جديدة للحد من الهجمات السيبرانية.

ثانيا: مشكلة الدراسة:

يحاول البحث إثبات أهمية الفضاء السيبراني في عالم اليوم، هذا الفضاء الذي أصبح مسرحا تقام فيه جميع الأعمال في مختلف المجالات، خصوصا في العامين الأخيرين؛ بسبب جائحة كوفيد ١٩ المستجد (كورونا)، هذه الجائحة تطلبت من دولٍ كثيرة فرض قوانين جديدة، تهدف لحماية شعوبها من هذا الوباء، قوانين أجبرت الأفراد على الإقامة الجبرية في المنازل، و فرضت على الأفراد مزاولة أعمالهم من منازلهم، و دفعت بهم إلى العمل في الفضاء السيبراني، لأغراض عديدة كالتسوق، والمقابلات الطبية، والتعليم، وإقامة المؤتمرات العلمية و الندوات، كل هذه العوامل ساعدت في انتقال جميع الأعمال للفضاء السيبراني، و زادت من أهمية هذا الفضاء. لكن العمل في الفضاء السيبراني فرض تحديات كثيرة، تحديات تمثلت في الهجمات السيبرانية التي أصبحت اليوم تهدد كيان الكثير من الدول إما بالدمار أو بالانهيار أو بتهديد الأمن الداخلي للدول، تحديات تسببت في توتر العلاقات الدولية؛ بسبب الأضرار و المشاكل الكثيرة التي تلحقه بالدول و المؤسسات و الأفراد. تحديات تسببت في توتر للعلاقات الدولية، و بظهور مؤشرات لسباق تسلح سيبراني.

ثالثا: أهداف الدراسة:

- توضيح مفهوم الفضاء السيبراني و تحدياته.
- التعرف على طبيعة الصراعات الدولية التي تدور في الفضاء السيبراني.
- التعرف على طبيعة الأسلحة المستخدمة للسيطرة على الفضاء السيبراني.
- التعرف على الدور المتنامي للشركات التكنولوجية في التحكم بالفضاء السيبراني.
- التعرف على تأثير الهجمات السيبرانية في تأجيج الصراع الدولي.
- التعرف على الأضرار الاقتصادية التي تسببت بها الهجمات السيبرانية.
- التعرف على التحديات المستقبلية للفضاء السيبراني.
- التعرف على إمكانية الحد من الهجمات السيبرانية لتعزيز الأمن السيبراني.

رابعاَ: أسئلة الدراسة:

كيف أثرت الهجمات السيبرانية في بروز أنماط جديدة للصراع الدولي؟

هل يشهد العالم اليوم سباق تسلح سيبراني؟ وما هي أغلب الأسلحة الإلكترونية الجديدة؟

هل الفضاء السيبراني يهدد الأمن القومي للدول ؟

هل الفضاء السيبراني يشجع على ارتكاب العديد من الجرائم السيبرانية؟

هل يمكن الحد من هذه الهجمات السيبرانية في الفضاء السيبراني ؟

ما الدور الذي يمكن أن تلعبه المؤسسات التعليمية في تعزيز الأمن السيبراني ؟

ما التقنيات المتاحة اليوم لتعزيز الأمن السيبراني؟

هل أغلب الهجمات السيبرانية سببها البريد الإلكتروني؟

خامسا: فرضيات البحث

- الفضاء السيبراني يساعد على انتشار الجريمة و تفشي الرذيلة.
- توتر العلاقات الدولية بسبب الصراع السيبراني.
- في الفضاء السيبراني تنامى دور الشركات التكنولوجية على حساب الدول.

- الهجمات السيبرانية قد تطال أماكن حساسة جدا كمخازن السلاح النووي.
- تزايد الطلب العالمي لمختصي الأمن السيبراني.
- استعداد الكثير من الدول لمواجهة نشوب حرب سيبرانية.
- تؤثر الهجمات السيبرانية في بروز أنماط جديدة من الصراع الدولي.
- معظم الهجمات السيبرانية لها دوافع مادية.
- تلعب وسائل التواصل الاجتماعي دورا كبيرا في نشر الفوضى و تضليل الرأي العام
- الكثير من الدول غيرت نظمها و خططها العسكرية لمواجهة أي حرب سيبرانية مستقبلية.

سادساً: منهجية الدراسة:

اعتمدت الدراسة على المنهج الوصفي التحليلي، المتمثل في جمع البيانات، وتحليلها؛ لتحقيق أهداف البحث، و التأكد من صحة الفرضيات و الاجابة عن أسئلة البحث.

سابعا: أهمية الدراسة:

تستمد الدراسة أهميتها من حداثة الموضوع وحيويته الذي تطرحه، وكذا أهميته، ففي ظل تغلغل التكنولوجيا واستخدامات الإنترنت في الحياة اليومية، وزيادة انتشار الهواتف الذكية، وشبكات التواصل الاجتماعي، وظهور وانتشار مفاهيم جديدة، مثل: الرقمنة، وإنترنت الأشياء، و تزايد اتصال الناس مع بعضهم، ومع الأشياء من حولهم في فضاء افتراضي يسمى بالفضاء السيبراني، الذي تدار فيه اليوم جميع الأعمال و الأنشطة حتى أصبح منجماً و مخزناً عالميا للمعلومات. فالعمل في هذا الفضاء محفوف بتحديات و مخاطر كثيرة، سببها الكثير من الجرائم السيبرانية التي ترتكب. لذا لابد من تأمين مكونات هذا الفضاء من أجهزة كمبيوتر، و شبكات، وأجهزة اتصالات، و أجهزة ذكية؛ الأمر الذي يتطلب تطبيق أعلى معايير الأمان؛ بهدف حماية أنفسنا كجهات حكومية، مؤسسات، شركات أو أفراد من تبعات هذه الجرائم.

المحور الثاني: الفضاء السيبراني، مفهومه، خصائصه، أهميته، تحدياته، القوى الفاعلة فيه

مفهوم الفضاء السيبراني:

هو الفضاء الذي تتواجد فيه شبكات الكمبيوتر، ويحصل من خلالها التواصل الإلكتروني. وبمفهوم أشمل يعرف بأنه المجال المادي وغير المادي الذي يتكون من عناصر، هي: أجهزة الكمبيوتر، والشبكات، والبرمجيات، وحوسبة المعلومات، والمحتوى، ومعطيات النقل، والتحكم، ومستخدمو كل هذه العناصر. التي تعد العامل المشترك في جميع محاور استخدام الفضاء السيبراني [٤].

هناك 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 و مخاطر لا تتوقف ، وهناك من يرى أنه يمثل البعد الخامس للحرب.

تعريف السيبرانية في اللغة (cyber) : هي كلمة إنجليزية، ولقد عرَّف قاموس أكسفورد كلمة سيبراني أو (Cyber) ، بأنها صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي.

السيبراني:جاء من لفظ سايبر المعرّب من كلمة (Cyber) اللاتينية، والذي ظهر حديثا في قواميس اللغة الإنجليزية، والتي تعني باللغة العربية إلكتروني، و تهتم بخصائص وثقافة أجهزة الكمبيوتر، وتكنولوجيا المعلومات، والواقع الافتراضي[٥].

خصائص الفضاء السيبراني

الفضاء السيبراني بصفته مجالاً افتراضياً يعتمد على نظم الكمبيوتر، التي تتكون من ملايين من شبكات الحواسيب، و شبكات الهواتف المنتشرة في جميع أنحاء العالم، و أشياء أخرى، مثل: السيارة، والتلفاز، ونظارات جوجل (Google Glasses)، والأدوات المنزلية المختلفة. كالثلاجات، والغسالات، والمراوح، وغيرها، كل هذه الأشياء تكون شبكات تمتلك مخزونا هائلا من البيانات و المعلومات، وترتبط هذه الشبكات ببعضها عبر

خطوط اتصالات هائلة و سريعة، و أقمار صناعية تمكنها من تبادل المعلومات دون تقيد بالحدود الجغرافية. لذا يطلق على عصرنا الحالي بالعصر الرقمي؛ لكونه يتضمن تطورات تكنولوجية هائلةK تخدم جميع مناحي الحياة العامة والخاصة،و تنعكس على خدمة المجتمع الدولي بأكمله(٦).عصر بات يتحرك من خلال تكنولوجيا المعلومات والاتصالات، لذا واكبته حركة إجرامية كبيرة، و انتشرت الجرائم السيبرانية بشكل خطير في جميع دول العالم، و أصبحت الدول اليوم عرضه للوقوع تحت تهديد هذه الجرائم التي تستخدم الفيروسات، وبرامج التجسس؛ لإلحاق أضرار كبيرة بالدول، و بأمنها، و كذا بالمؤسسات و الأفراد. تكمن مخاطر هذه الجرائم أنه في الكثير من الحالات من الصعب جدا تحديد هوية مرتكب الجريمة ، و كذا غياب التشريعات الدولية التي تضع الدول أو المؤسسات التي تقوم بمثل هذه الأنشطة تحت طائلة القانون الدولي، ما يعني عدم القدرة على ملاحقتها قانونيا.

إنترنت الأشياء:

إنترنت الأشياء (بالإنجليزية: Internet of Things - IoT) يعرف إنترنت الأشياء الموضح في الشكل(١) بأنه مجموعة من الأجهزة الرقمية الذكية المتصلة فيما بينها عبر أحد البروتوكولات المعروفة، مثل: الواي فاي، والبلوتوث... تُرسِل وتستقبل المعلومات فيما بينها، دون اعتماد على البشر في إمدادها بهذه المعلومات بل الحصول عليها من الوسط الخارجي عبر الحواس الاصطناعية أو ما يعرف بـ المستشعرات الرقمية، هذه الأجهزة تشمل الأدوات، والمستشعرات، والحساسات، وأدوات الذكاء الاصطناعي المختلفة، وغيرها(7). هذه الأشياء يمكن تجهيزها و ربطها بالإنترنت بعنوان إنترنت IPv6 ، يوفر بروتوكول الإصدار السادس IPv6 حوالي 340 تريليون تريليون تريليون عنواناً، مما يعني بأن جميع الأشياء المتصلة بالشبكة حالياً وتلك التي ستتصل بشبكة الإنترنت لاحقاً يمكنها الحصول على عناوين فريدة لا يشاركها فيها أحد(8).

إن ما يميز إنترنت الأشياء أنها تتيح للإنسان التحرر من المكان ،أي إن الشخص يستطيع التحكم في الأدوات من دون الحاجة إلى المكزث في مكان محدّد للتعامل مع جهاز معين.

ووفقاً لدراسة حديثة صادرة عن مجموعة حلول أعمال الإنترنت من سيسكو من المتوقع أن تتجاوز أعداد الأجهزة المتصلة بالإنترنت ٥٠ مليار جهاز بحلول العام ٢٠٢٠.

الشكل (١) إنترنت الأشياء، Internet of Things

أهمية الفضاء السيبراني

خلال العقود الثلاثة الأخيرة تغير العالم تغيراً كبيراً، فمع التطور الهائل لتكنولوجيا المعلومات و الاتصالات انتقلت الكثير من الأعمال في مختلف المجالات إلى الفضاء السيبراني. برزت أهمية الفضاء السيبراني في العامين الإخيرين مع ظهور فيروس كوفيد ١٩ المستجد. إذ تسببت جائحة كورونا في فرض القيود على السفر، والحجر المنزلي، وتخفيض القوى العاملة في جميع القطاعات الاقتصادية مما أدى إلى فقدان العديد من الناس لوظائفهم، كما أغلقت المدارس والجامعات. فجائحة كورونا كان لها دور كبير في تسريع التحول الرقمي لمختلف الأنشطة الاقتصادية بمختلف قطاعاتها. أهمية الفضاء السيبراني تكمن بأنه أصبح اليوم البيئة الحاضنة لمختلف الأنشطة في مختلف القطاعات، من هذه القطاعات مثلا:

مجال المواصلات: أصبحت التكنولوجيا مسؤولة عن تسيير جميع وسائل المواصلات، وصارت الكمبيوترات هي التي تتحكم في حركة وتوجيه الطائرات والقطارات السريعة وغيرها من وسائل المواصلات الحديثة. كذلك الحجز وإصدار التذاكر، صار المواطن يستصدرها من بيته عبر الإنترنت.

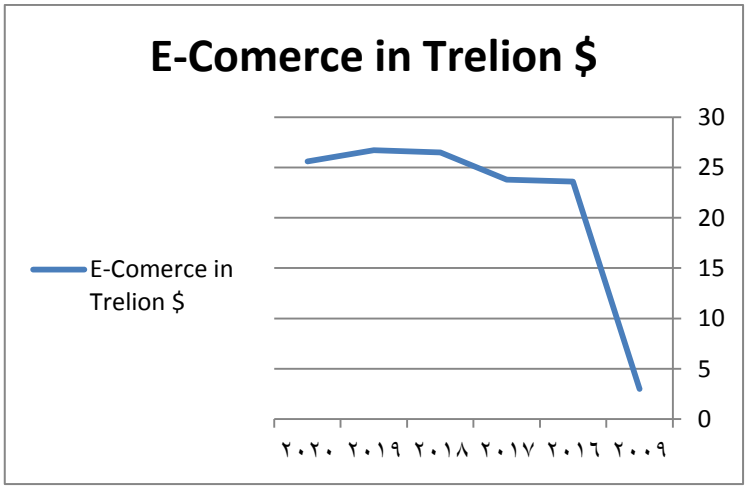
مجال الزراعة: لدى الغرب مجسات كبيرة غائصة في أعماق التربة، تتحسس نسبة الرطوبة فيها، وبمجرد أن ينخفض مستوى الرطوبة عن الحد المطلوب، تصدر هذه المجسات إشارات إلكترونية لرشاشات ضخمة؛ لتقوم بري آلاف الفدانات على الفور، فلا يحدث أي ضرر للمحصول. وتقوم هذه المجسات بقياس نسبة السماد في التربة، والتحكم في كميته، واختيار النوعية الملائمة للتربة أو المحصول المزروع عن طريق الكمبيوتر.

مجال التعليم: التعليم الإلكتروني (E-learning) أصبح الطالب عن طريق الإنترنت قادراً على الالتحاق بالجامعة التي يريدها، ويحضر المحاضرات، ويناقش الدكاترة، ويتقدم للامتحانات ويحصل على الشهادة، كل هذا وهو جالس في بيته. وأوجد الإنترنت مكاتب إلكترونية، بحيث تمكن أي أستاذ في أي صف دراسي أن يشرح للتلاميذ عن أمر ما.

الحكومة الإلكترونية: تتزايد يوما بعد يوم متطلبات العمل مع تزايد أعداد السكان، و حجم الخدمات المتنوعة و دخول المعلوماتية، و ثورة تقنية الاتصالات إلى حياتنا اليومية؛ الأمر الذي دعا إلى ضرورة مواكبة هذه الثورة مما دفع الحكومات لتحويل أعمالها للفضاء السيبراني فيما يعرف بالحكومة الإلكترونية، وتعرف الحكومة الإلكترونية بأنها تشمل الاستخدام الشامل و الفعال لجميع تقنيات المعلومات والاتصالات؛ وذلك لتسهيل العمليات الإدارية اليومية في القطاعات الحكومية، وتلك التي تتم فيما بينها (حكومة – حكومي) و تلك التي تربطها بالمواطنين (حكومة – مواطن) أو قطاعات الأعمال (حكومية – أعمال)[١٠].

المجال الصحي: الفضاء السيبراني يمكن لجراح في لندن أن يقوم بعملية عن طريق المنظار، يتصل عن طريق النت بطبيب آخر في أستراليا؛ ليراقب العملية معه، ويبدي رأيه واستشارته، لترتفع نسبة نجاح وكفاءة العمليات إلى أعلى مستوى. عندما تفشى فيروس كورونا في مدينة ووهان الصينية استخدمت الصين تتبع درجة حرارة المواطنين عبر تطبيق للهاتف المحمول، والذي يظهر المواطن ودرجة حرارته اللحظية، ومكانه على الخريطة، وبالمثل اتجهت المؤسسات والشركات التجارية إلى الاعتماد على ريادة الأعمال الرقمية.

المجال التجاري: بفضل تكنولوجيا المعلومات تغير مفهوم التجارة التقليدي، وأصبح بيع وشراء السلع، و بيع الخدمات متداولة في الفضاء السيبراني[١١]، هذا النشاط نسميه اليوم بالتجارة الإلكترونية (E-Commercial). أصبح اليوم لمعظم الشركات العالمية مواقعها الخاصة على الشبكة العنكبوتية، بحيث يتصل بها الزبون أو العميل، فيختار ما يريد من السلع أو الخدمات، ويجري عليها التعديلات التي يريدها، ثم يشتريها، ويدفع الثمن ببطاقة الائتمان. شهدت التجارة الإلكترونية زيادة هائلة فيما يتعلق بالمبيعات، فقد تنامى حجم التجارة الإلكترونية، ففي العام ٢٠٠٩م كان الحجم العالمي للتجارة الإلكترونية فقط ٣ تريليون دولار، بينما في العام ٢٠٢٠م وصل حجمها ٢٥ , ٦ تريليون دولار. الشكل(٢) يوضح نمو التجارة الإلكترونية من العام ٢٠٠٩م و حتى العام ٢٠٢٠م، في العام ٢٠٢٠ و وصل عدد المتسوقين عبر الإنترنت ١ , ٢ مليار، الشكل (٣) يوضح جنسيات المتسوقين. و تشير التقديرات إلى أنه بحلول ٢٠٤٠م ستكون ٩٥ في المئة من جميع المشتريات تتم عبر التجارة الإلكترونية[١٢].



الشكل (٢) نمو التجارة الإلكترونية من العام ٢٠٠٩ و حتى العام ٢٠٢٠م[١٣]. الشكل (٣) عدد المتسوقين و جنسياتهم في العام ٢٠٢٠م[١٤].المصدر إحصاءات التجارة الإلكترونية وحقائق التسوق عبر الإنترنت Source: http://www.nasdaq.com

الشكل (٣) عدد المتسوقين و جنسياتهم في العام ٢٠٢٠م. المصدر إحصاءات التجارة الإلكترونية وحقائق التسوق عبر الإنترنت Source: http://www.nasdaq.com

مجال الثقافة والفنون: كافة الخدع السينمائية والأفلام الكرتونية، والمونتاج، وكذا الإخراج، صارت اليوم تتم بتقنيات عالية جداً باستخدام وسائل التكنولوجيا الحديثة.

مجال البحث العلمي: بسبب جائحة كورونا تغيرت المؤتمرات العلمية، و تحولت للفضاء السيبراني، أصبحت جميع المؤتمرات العلمية في جميع أنحاء العالم تقام في بيئة افتراضية باستخدام العديد من التطبيقات (برنامج الزووم) مثلا.

مجال الأمن الداخلي: جميع البطاقات الشخصية، وجوازات السفر، ووثائق أخرى صارت الآن ممغنطة، بحيث يعرف رجل الأمن بمجرد أن يمررها على جهاز الكمبيوتر كل شيء عن مالك الوثيقة.

مجال الدفاع والأمن: صارت الأسلحة الآن والصواريخ كلها توجه و يتحكم بها عن بعد، وطائرات التجسس والطائرات المقاتلة دون طيار، وكذا الطائرات المسيرة التي يتم التحكم بها من بعد.

مجال الإعلام: أصبح الإنترنت من أهم وسائل الإعلام في الكثير من الدول، وهذا يعود لعدم وجود أية رقابة على محتواه، يستخدم الإنترنت اليوم كأداة لتسويق المنتجات والخدمات، توقّع تقرير حديثٌ أصدرته مؤسسة (E Marketer) للأبحاث التسويقية وصول حجم الإنفاق العالمي على الإعلانات الرقمية على شبكة الإنترنت خلال العام ٢٠٢٢، إلى ٤٥٧,٩ مليار

دولار، مقارنة بـ٤ ,٣٨٠ مليار دولار في العام ٢٠٢٠، بزيادة ٥ ,٧٧ مليار دولار، و حسب التقرير أنفق كلٌّ من الصين وأمريكا أكثر من ١٠ مليارات دولار، خلال العام الماضي على الإعلانات الرقمية(١٤).

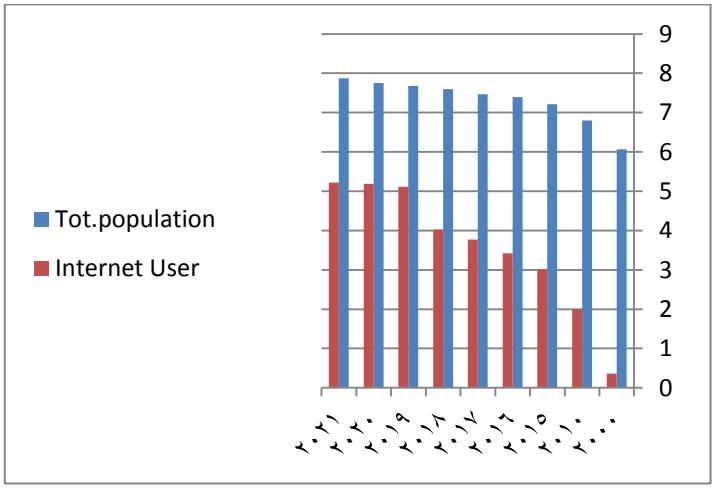
القطاع المصرفي: مع التطور الهائل والانتشار الكبير في استخدام انظمة التواصل الإلكتروني والوسائل التكنولوجية الحديثة أصبح الاقتصاد العالمي يعتمد على هذه التكنولوجيا في تنفيذ معاملاته المحلية أو مع العالم الخارجي بشكل شبه كلي وخاصة في مؤسساته المالية والمصرفية.

تحديات الفضاء السيبراني

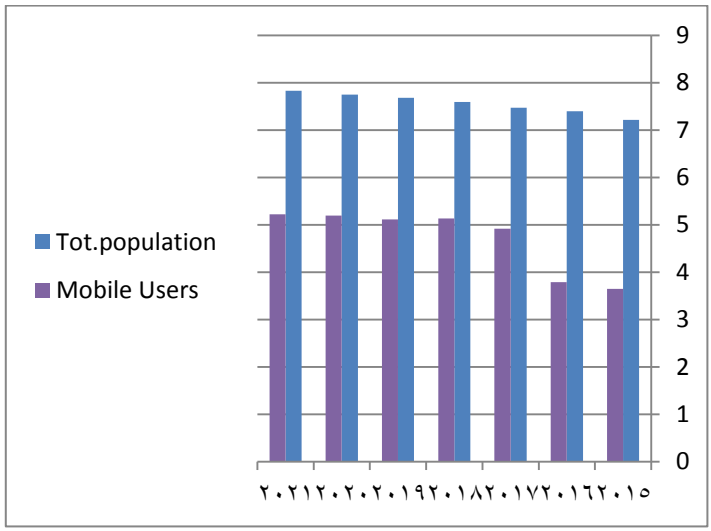
في ظل تغلغل التكنولوجيا و دخولها معظم القطاعات، و بسبب الانتشار الواسع لشبكة الإنترنت في الحياة اليومية تحول العالم إلى ما يشبه القرية الكونية، حيث بلغ عدد مستخدمي الإنترنت في مارس من العام ٢٠٢١م 5ٍ168ٍ780ٍ607، الشكل(٤) يوضح نمو مستخدمي الإنترنت منذ العام ٢٠١٥م.و ارتفع عدد مستخدمي الهواتف الذكية حول العالم، في مارس من العام ٢٠٢١، حيث وصل العدد إلى نحو ٥ ,٢٢ مليار، الشكل (٥) يوضح نمو عدد مستخدمي الهواتف المحمولة منذ العام ٢٠١٥م. كذلك ارتفع عدد مستخدمي وسائل التواصل الاجتماعي ، في يناير من العام ٢٠٢١ وصل عدد المستخدمين إلى أكثر من ٤ ,٢٠ مليار مستخدم(١٥)، الشكل (٦) يوضح نمو عدد مستخدمي وسائل التواصل الاجتماعي من العام ٢٠١٥ . إنترنت الأشياء هي الأخرى ستسمح بتزايد اتصال الناس مع بعضهم ومع الأشياء من حولهم، وتشير الدراسات بأنه في العام ٢٠٢٠م سيصل عدد الأجهزة المتصلة بالإنترنت إلى نحو ٥٠ مليار جهازٍ(١٦).

على الرغم من المزايا الهائلة التي تحققت بفضل تقنية المعلومات في شتى ميادين الحياة ،إلا أن هذه الثورة التكنولوجية المتنامية صاحَبَتها في المقابل انعكاسات سلبية خطيرة جراء سوء الاستخدام لهذه التقنية المتطورة . من بين تلك الانعكاسات السلبية الجرائم الكثيرة التي تنفذ في هذا الفضاء و التي تسمى الجريمة السيبرانية (cyber-crime) [17]. إذ تصاعدت مخاطرها في ظل البيئة الافتراضية التي تمثلها شبكة المعلومات الدولية(الإنترنت) واسعة الانتشار، ما أفرز نوعاً جديداً

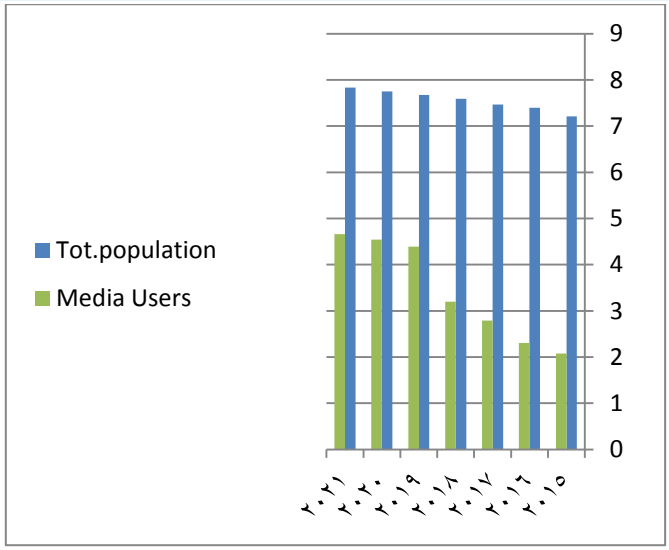
من الجرائم العابرة للقارات، التي لم تعد مخاطرها و آثارها محصورة في النطاق الإقليمي لدولة بعينها؛ بسبب وجود العديد من التحديات الأمنية في الفضاء السيبراني. أصبحت حماية المعلومات و الأجهزة تشكل أولوية قصوى، و تحدياً كبيراً يهدد مصالح الدول و المؤسسات و الشركات و الأفراد، الأمر الذي يتطلب تعزيز الأمن السيبراني باتخاذ التدابير الضرورية لحماية الفضاء السيبراني، و الحد من ارتكاب مثل تلك الجرائم.



الشكل (٤) نمو عدد مستخدمي الإنترنت منذ العام ٢٠٠٠م حتى العام ٢٠٢١م، المصدر https://wearesocial.com



الشكل(٥) نمو عدد مستخدمي الهواتف المحمولة منذ العام ٢٠١٥م. المصدر https://wearesocial.com



الشكل (٦) نمو عدد مستخدمي وسائل التواصل الاجتماعي من العام ٢٠١٥. المصدر https://wearesocial.com

مفهوم الأمن السيبراني

عرّف الاتحاد الدولي للاتصالات الأمن السيبراني بأنه «مجموعة من الأدوات والسياسات والمفاهيم الأمنية وضمانات الأمان والمبادئ التوجيهية، وأساليب إدارة المخاطر، والإجراءات والتدريب، وأفضل الممارسات والضمان والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المنظمة والمستخدم». وتتضمن أصول المؤسسة والمستخدم أجهزة الحوسبة المتصلة، والموظفين، والبنية التحتية، والتطبيقات، والخدمات، وأنظمة الاتصالات، ومجموع المعلومات المرسلة و/ أو المخزنة في البيئة الإلكترونية، ويسعى الأمن السيبراني جاهدًا لضمان تحقيق الحفاظ على الخصائص الأمنية للمؤسسة، وأصول المستخدم ضد المخاطر الأمنية ذات الصلة في البيئة الإلكترونية.

إدوارد أمورسو Edward Amorso عرف الأمن السيبراني أنه" مجموعة من الوسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الكمبيوتر أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة، وكشف الفيروسات، ووقفها، وتوفير الاتصالات المشفرة"[١٨].

الفاعلين في الفضاء السيبراني

أشار البروفيسور و المفكر الأميركي (جوزيف. اس. ناي) صاحب رؤية "القوة الناعمة"، بأن هناك قوى عدة في العالم تمثل العناصر المحركة الرئيسة في الفضاء السيبراني، هذه العناصر هي:

- الدول بمختلف أحجامها، كبيرة أو صغيرة، باتت مسألة الشراكة في الفضاء السيبراني ميسرة لأصحاب العقول، غير أن الهجمات السيبرانية هي التي تحتاج إلى دول كبيرة فاعلة تمتلك بنى تحتية سيبرانية لإحداث خسائر في أعدائها على المستوى الدولي.
- قوى غير دولية، أصغر في مقدراتها من الدول، وقد تكون أقرب إلى الكيانات الأممية، وعادة ما يكون لهؤلاء أهدافٌ تخريبية، إلا أن قدرتهم على القيام بعمليات واسعة النطاق تعوزها مساعدة أجهزة استخبارات دولية، وإن كان من اليسير عليها اختراق المواقع الإلكترونية، واستهداف الأنظمة الفاعلة.
- الشركات متعددة الجنسيات، تمتلك بعض شركات التكنولوجيا موارد للقوة تفوق قدرة بعض الدول. الشكل (٧) يوضح القدرات المادية لبعض شركات التقنية، لا تنقص هذه الشركات سوى شرعية لممارسة القوة التي مازالت حكرا على الدول. خوادم شركات مثل :جوجل Google ، فيسبوك Facebook،ميكروسوفت Microsoft، آبل Apple وأمازون Amazon ، تسمح لها بامتلاك قواعد البيانات العملاقة التي من خلالها تستكشف وتستغل الأسواق، وتؤثر في اقتصاديات الدول، وفي ثقافة المجتمعات وتوجهاتها.
- الجماعات الإرهابية، هنا تتضح المخاطر الحقيقية للعالم السيبراني، إذ تستخدم العصابات الإجرامية هذا الفضاء لسرقة المعلومات، وتسهيل كل ما هو غير مشروع، مثل: تجارة البشر والسلاح. تقوم هذه المنظمات الإجرامية بعمليات القرصنة السيبرانية، وسرقة المعلومات واختراق الحسابات البنكية، وغسيل

الأموال، كما توجد سوق سوداء على الإنترنت العميق Deep internet لتجارة المخدرات والأسلحة والبشر، حيث تكلف هذه الجرائم السيبرانية الاقتصاد العالمي مليارات الدولارات سنويا.

- الأشخاص الاعتياديون، إن فردا واحدا يمكنه أن يغيّر ويبدل من حال العالم، والمثال على ذلك ما رأيناه في ظاهرة ويك ليكس، حيث استطاع مخترق للأمن المعلوماتي الأميركي أن يهدد أكبر دولة في العالم، ويكشف أوراقها وتحالفاتها حول الكرة الأرضية.

الشركة	القيمة السوقية(مليار دولار)
أمازون	٧٩٨
مايكروسوفت	٧٨٨
أبل	٧٨٥
ألفابيت	٧٧٨
فيسبوك	٤٧٣

الشكل (٧) القيمة السوقية لبعض الشركات التقنية (فبراير ٢٠١٩) المصدر

(Source: http://www.nasdaq.com)

المحور الثالث : أبعاد الأمن السيبراني، أهميته، الخسائر الناجمة عن الهجمات السيبرانية

أدركت العديد من الدول بأن الفضاء السيبراني أصبح اليوم جزءا لا يتجزأ من الأمن القومي، خصوصا مع ارتفاع منسوب الهجمات السيبرانية التي تستهدف الشركات ، جهات حكومية و أجهزة استخبارات، الأمر الذي سيؤدي مستقبلا لاحتدام المواجهة السيبرانية بين القوى العالمية. فعلى الرغم من الترسانة الرقمية الهائلة لدى بعض الدول، التي أعدت لتكون جزءا من الأمن القومي لهذه الدول، إلا أنها لا تمنع من التهديدات العابرة للحدود، لذا من المتوقع أن تندلع هذه المواجهات مستقبلا أكثر فأكثر بين الدول.

البعد العسكري : فكرة الانترنت جاءت في الأساس لخدمة الأهداف العسكرية، فمنذ الحرب العالمية الثانية وحتى مطلع التسعينيات من القرن الماضي كانت الشبكة حكراً على الاستخدامات والتطبيقات العسكرية وبالتحديد لدى الجيش الأمريكي. ثم كان هناك قرار إستراتيجي بفتح باب الاستخدام للتطبيقات المدنية في أواخر الثمانينيات وأوائل تسعينيات القرن الماضي. كانت الحروب تشن في الماضي جواً أو بحراً أو براً، لكنها باتت اليوم تدور ضمن أبعاد أخرى، أبعاد افتراضية. فمع الاعتماد المتزايد على تكنولوجيا المعلومات فتحت جبهة جديدة لمثل هذا النوع من الحروب غير المرئية. اختصر الفضاء السيبراني حاجز الزمان والمكان، وخلق مساحات للتفاعلات الداخلية والدولية في الواقع الافتراضي، ومن ثم برزت فضاءات جديدة للصراع بأدوات مختلفة، وأنماط جديدة تختلف عن الصراعات التقليدية[١٩]. من الصرعات التي حدثت في الفضاء السيبراني ذات طابع عسكري الحرب على أستونيا في العام ٢٠٠٧م، والحرب على جورجيا في العام ٢٠٠٨م، ألهجوم على برنامج إيران النووي في العام ٢٠١٢م و العام ٢٠٢١، والهجوم على الولايات المتحدة في ديسمبر من العام ٢٠٢٠م.

البعد الاقتصادي

مع تزايد نسبة الجرائم السيبرانية، وتنوع طرقها، أصبحت هذه الجرائم تشكل خطرا كبيرا على الاقتصاد، و تلحق خسائر مادية كبيرة وفادحة ليس فقط على مستوى الفرد بل تتعداه إلى مستوى المنظمات، والحكومات والمؤسسات وهذا بالطبع يؤثر تأثيراً سلبياً على الاقتصاد. و ما نواجهه هو هجوم شرس من أشخاص أو مجموعات أو منظمات محترفة هدفها الرئيسي تحقيق ربح مادي بالإضافة إلى أهداف أخرى.و تشير التوقعات أنه في عام ٢٠٢١ ستكون تكاليف أضرار الجرائم الإلكترونية العالمية ٦ تريليون دولار في السنة[٢٠].

البعد الثقافي و الاجتماعي

باتت اليوم وسائل التواصل الاجتماعي أحد أهم الفاعلين الدوليين، فلم يعد تأثيرها يقتصر على النظام الداخلي في دولة ما، بل أصبح يمتد إلى مجال العلاقات الدولية، وباتت تلعب دوراً في التفاعلات السياسية الدولية .ولهذا يمكن اعتبارها أحد أهم الفاعلين من غير الدول التي تمتلك القدرة على التأثير في تطورات الأحداث الإقليمية والعالمية، ولعل ما أثير عن تدخل روسي في الانتخابات الرئاسية الأمريكية في العام ٢٠١٦ يُعد أحد تجليات التأثير الذي يمكن أن تحدثه وسائل التواصل الاجتماعي في هذا الشأن. وسائل التواصل الاجتماعي تعد اليوم من أهم الأسلحة المستخدمة في ما يسمى بحروب الجيل الرابع، التي تهدف إلى إضعاف الدول، وإنهاكها، وإفشالها من الداخل عن طريق نشر الفتن، والقلاقل، وزعزعة الاستقرار الاقتصادي والاجتماعي، وإثارة الاقتتال الداخلي. من الأدوار الخطيرة لوسائل التواصل الاجتماعي تضليل الرأي العام، ونشر التطرف والترويج لخطاب الكراهية، ونشر الشائعات والتحريض على الفوضى وإثارة الاضطرابات[٢١].و ترى وسائل الإعلام الأمريكية و النخبة السياسية بأن تحريض الرئيس الأمريكي السابق (ترامب) على إثر هزيمته في الانتخابات الرئاسية لأتباعه عبر الفيس بوك كان له دور كبير في أحداث العنف التي رافقت اقتحام مجلسي الشيوخ و النواب، كذلك الدور الذي لعبته هذه الوسائل في أحداث ما يسمى بالربيع العربي.

البعد السياسي

للفضاء السيبراني اليوم دور كبير على الحياة السياسية، حيث تشهد العلاقات بين الدول توترات كبيرة، الشاهد على ذلك توتر العلاقات بين الولايات المتحدة و روسيا خصوصا بعد الهجوم السيبراني الذي ضرب الولايات المتحدة في ديسمبر ٢٠٢٠م، واتهام روسيا بالوقوف وراء هذه الهجمات، فقد كان الأمن السيبراني أحد أهم القضايا التي جرى مناقشتها في أعمال القمة المنعقدة في جنيف يوم ١٦ يونيو ٢٠٢١ بين الرئيس الأمريكي بايدن و الرئيس الروسي بوتين، حيث صرح بايدن بأن الولايات المتحدة وروسيا ستبدآن مشاورات بشأن الأمن السيبراني، مضيفًا أنه يتعين على كلا الجانبين تحمل التزامات معينة حول قضية القرصنة الإلكترونية التي تعد من أبرز القضايا المثيرة للخلافات بين البلدين[٢٢]. وتوازياً مع انعقاد هذه القمة جاء إتهام البيت الأبيض لروسيا بحماية القراصنة الإلكترونيين المتواجدين على أراضيها لقاء حصولها على بعض الدعم منهم في مجالات تصب في مصلحة الحكومة الروسية، وقال جون ديميرس، المسؤول عن الأمن القومي في وزارة العدل الأميركية: إن هناك هجمات إلكترونية كثيرة مصدرها روسيا، مضيفاً أن الحكومة الروسية تعرقل عمل السلطات الأميركية التي تهدف إلى مكافحتهم [٢٣].

البعد الأخلاقي

تؤثر الشبكات الاجتماعية بشكل كبير في تغيير ملامح المجتمعات الثقافية والاجتماعية، خاصة أمام التزايد المتصاعد لعدد المستخدمين المنخرطين في هذا الفضاء السيبراني، الذين يقضون أوقات فراغهم للمشاركة في مختلف الأنشطة والبرامج المتاحة عبر صفحاتهم لفترات طويلة، حيث يتفاعلون ويبنون علاقات جديدة مع غيرهم من المستخدمين، الذين تتعدد و تختلف ثقافاتهم وهوياتهم وانتماءاتهم الدينية، مما قد يجرهم إلى تبني بعض السلوكيات غير الأخلاقية، و مِنْ ثَمَّ ظهور العديد من المشاكل غير الأخلاقية، مثل: الاغتراب

الاجتماعي، وتفكك العلاقات الأسرية والاجتماعية، واهتزاز القيم المجتمعية، وانتشار الشائعات، والعنف، والعلاقات غير الشرعية بين الجنسين، وانتهاك الخصوصية[٢٤].

أهمية الأمن السيبراني

يوما بعد يوم تتزايد التهديدات السيبرانية لتهدد كيانات الدول و المؤسسات و الأفراد، و تلحق بهم خسائر مادية كبيرة، إذ تشير التوقعات أنه في العام ٢٠٢١م ستكلف الجرائم الإلكترونية الاقتصاد العالمي ٦ تريليون دولار، الأمر الذي يتطلب ضرورة تأمين الفضاء السيبراني بجميع مكوناته، حيث تتعرض هذه المكونات لتهديدات كثيرة، سببها الجرائم السيبرانية[٢٥]. ذكر خبراء المعهد الأوروبي لدراسة مكافحة الإرهاب والاستخبارات أن الحرب السيبرانية ستمثل مفاتيح الانتصار في المستقبل القريب، ولذلك أصبح الأمن السيبراني في سلم أولويات الدول لضمان أمن منشآتها الإلكترونية وسلامتها. في العام ٢٠٢١م سيصل الإنفاق على الأمن السيبراني إلى ٦٠ مليار دولار[٢٦].

الجريمة السيبرانية

تسمى أيضا جريمة معلوماتية أو جريمة الفضاء الإلكتروني (بالإنجليزية: Cyber crime)[٢٧] تشير إلى أي جريمة تتضمن الكمبيوتر أو شبكات الكمبيوتر. قد يستخدم الكمبيوتر في ارتكاب الجريمة و قد يكون هو الهدف. و يمكن تعريف الجريمة السيبرانية على أنها أية مخالفة ترتكب ضد أفراد أو جماعات بدافع إجرامي أو بنية الإساءة لسمعة الضحية أو لجسدها أو عقليتها، سواءً كان ذلك بطريقة مباشرة أم غير مباشرة، و أن يتم ذلك باستخدام وسائل الاتصالات الحديثة، مثل: الإنترنت (غرف الدردشة أو البريد الإلكتروني أو المجموعات). وتُرتكب الجريمة السيبرانية لأسباب عديدة اقتصادية، سياسية، عسكرية[٣].

الخسائر المادية الناجمة عن الجرائم السيبرانية

- يخسر الاقتصاد العالمي تريليونات الدولارات سنوياً؛ بسبب القرصنة الإلكترونية، حيث قدرت خسائر العالم من عمليات القرصنة في العام ٢٠٢١ بنحو ٦ تريليونات دولار، مقابل ٣ تريليونات دولار في عام ٢٠١٥[٢٨].
- من المتوقع أن تنمو تكاليف الجرائم الإلكترونية العالمية بنسبة ١٥٪ سنويًا على مدى السنوات الخمس المقبلة ، لتصل إلى ١٠,٥ تريليون دولار أمريكي سنويًا بحلول عام ٢٠٢٥ ، ارتفاعًا من ٣ تريليونات دولار أمريكي في عام ٢٠١٥[٢٣].
- في "منتدى ٢٠١٧" للأمن الاستخباراتي، كشف نائب مدير مركز رصد معلومات تابع لهيئة الأمن الفيدرالي الروسية، نيكولاي موراشوف، أن "خسائر العالم في السنوات الأخيرة، تقدر حسب أساليب تقييم مختلفة، من ٣٠٠ مليار إلى تريليون دولار" وأضاف "هذه المؤشرات تميل إلى طابع النمو المتزايد".
- كشفت تقارير منظمة التعاون الاقتصادي وغرفة التجارة الأميركية أن القرصنة عبر الإنترنت تكلف الاقتصاد الأمريكي وحده نحو ٣٠ مليار دولار سنوياً، لكن شركة فورستر الأميركية للأبحاث رفعت خسائر الشركات الأميركية وحدها من التجسس بنحو ٥٠٠ مليار دولار سنوياً، حيث سرقَتْ القراصنة حقوق الملكية الفكرية، وخطط التطوير والأبحاث، وبيعها لشركات منافسة مقابل ملايين الدولارات. وفي الاتحاد الأوروبي تبدو أزمة القرصنة ملحوظة ومقلقة جداً، إذ تخسر دولة نحو ٦٠ مليار يورو سنوياً في ١٣ قطاعاً اقتصادياً.
- كلفة الهجمات السيبرانية في قطاع الخدمات المالية قد تصل إلى ما يقدر بنحو – 270 إلى 350 مليار دولار سنويا حال اتساع نطاق، انتشارها وفق تقديرات صندوق النقد الدولي[٢٩].
- من المتوقع أن تصل أرباح الجرائم الإلكترونية إلى ٥ مرات أكثر من الجرائم العالمية مجتمعة. المخدرات، والاتجار بالبشر، وسرقة النفط، والتعدين غير المشروع، وصيد

الأسماك، وتهريب الأسلحة ، الذي يقدر ما بين ١,٦ تريليون دولار و ٢,٢ تريليون دولار سنويًا[٣٠].

- زادت الجرائم الإلكترونية المبلغ عنها بنسبة ٣٠٠٪ خلال عام ٢٠٢٠[٣١].
- البريد الإلكتروني العشوائي هو الطريقة الأكثر شيوعًا لمجرمي الإنترنت لنشر البرامج الضارة[٣١].
- تشير الإحصاءات إلى أن ٨٦ في المائة من خروقات البيانات تنطوي على دوافع مالية[٣٣].

المحور الرابع: الصراع الدولي في الفضاء السيبراني، مؤشرات الصراع، تحولات مضامين القوة، الفاعلين فيه، أهداف الصراع، الأدوات المستخدمة،نماذج عن الهجمات السيبرانية، استعدادات الدول للحرب السيبرانية

شهدت البشرية خلال تاريخها الطويل حروبًا كثيرة؛ لأسباب عديدة، راح ضحيتها ملايين البشر، وخلّفت وراءها خسائر هائلة على مختلف الأصعدة. واليوم بات الفضاء السيبراني أحد العناصر الأساسيّة التي تؤثّر في النظام الدولي، بما يتيحه من أدوات تكنولوجيّة مهمّة لعمليّات الحشد والتعبئة في العالم، إضافة إلى تأثيره في القيم السياسيّة و الأخلاقية؛ نتيجة لسهولة الاستخدامK ورخص التكلفة، زادت قدرت هذا الفضاء على التأثير في مختلف مجالات الحياة السياسيّة، والاقتصاديّة، والعسكريّة، والاجتماعيّة وحتى الأيديولوجيّة؛ وبات واضحاً أن من يمتلك آليّات توظيف البيئة السيبرانية يصبح أكثر قدرة على تحقيق أهدافه، والتأثير في سلوك الفاعلين المستخدمين لهذه البيئة. الحرب اليوم تدار في الفضاء السيبراني، فيه تستخدم أسلحة جديد كالقرصنة و التهكير لاختراق الشبكات والأنظمة الإلكترونية، وإحداث أضرارٍ جسيمةٍ بها. الحرب في الفضاء السيبراني تتطلب جيوشًا مُنظمةً ومُدربةً؛ لتكون قادرة على شن الهجمات أو صدها.و نظرا لأهمية هذا الفضاء توقعت العديد من الدول وقوع مواجهات، و أعدت العدة لها، فجهزت جيوشا سيبرانية، و سلحتها بمختلف الأسلحة المناسبة .

الحرب السيبرانية

يقول خبراء بريطانيون إن الهجمات السيبرانية هي اليوم أكثر دمارا من التفجير الذري، حيث إنه باستطاعتها تدمير الأنظمة الإلكترونية، وتعطيل محطات ضخ المياه، والهواتف، ومحطات الإذاعة والتلفزة، وتوقيف الاتصالات، وشل مراكز الطاقة، والتسبب في انهيار الأنظمة المالية، وعمل البورصات، يُسجّل لنا التاريخ المعاصر العديد من الهجمات السيبرانية.

الفضاء السيبراني له اليوم أهمية كبيرة، إذ يعتبر منصة لمختلف الأنشطة في مختلف المجالات، لذا تتسابق الدول على السيطرة و التحكم بهذا الفضاء، ومع هذا التسابق برزت صراعات عديدة رافقها ظهور مصطلح الحرب السيبرانية[٣٤]. التي تزداد، و يتسع مجالها نظراً للانتشار الواسع للمعدات والأجهزة الإلكترونية المستخدمة في المجالات المدنية و العسكرية، والهدف من هذه الحرب محاولة التأثير على مجريات العالم السياسي و الاقتصادي من جهة، وعلى المعطيات الأمنية والعسكرية من جهة ثانية. وتعرف الحرب السيبرانية بأنها هجماتٌ إلكترونيةٌ يشنها أفرادٌ أو مجموعاتٌ منظمةٌ تستهدف أجهزة الكمبيوتر والأنظمة والبيانات الموجودة فيها، والتابعة لإحدى الجهات الحكومية أو الخاصة، وذلك عن طريق شبكة الإنترنت، والهدف من ذلك سرقة البيانات أو تغيير الأنظمة المستخدمة أو إلحاق الضرر بأجهزة الكمبيوتر المستخدمة وتدميرها[٣٥].

ارتكزت البنى التحتية لمختلف دول العالم المتقدم على ذلك الفضاء السيبراني، القائم على تقنية المعلومات و الاتصالات، في كافة المجالات؛ الصناعية، والعسكرية، والطاقة، والمياه، والصحة، ومنظومة النقل، وقطاع البنوك والمؤسسات المالية والحكومية، لذلك فقد تصدر الأمن السيبراني لائحة أولويات سياسات وإستراتيجيات تلك الدول، بصفته جزءًا لا يتجزأ من الأمن القومي، وتغير شكل الحروب وتقنياتها وأساليبها؛ نتيجة لاستخدام الفضاء السيبراني للتهديدات والاعتداءات، وإلحاق الضرر بالمؤسسات والمراكز الحيوية والإستراتيجية للدول، فظهر ما يسمى بالحرب السيبرانية أو الحرب الإلكترونية؛ نتيجة لتلك التهديدات والهجمات الإلكترونية[٣٥].

مؤشرات تنامي الصراع الدولي في الفضاء السيبراني

شهدت العلاقات الامريكية الروسية توترا كبيرا وصل إلى سحب السفراء، هذه التوترات كان سببها الهجمات السيبرانية التي نفذت في ديسمبر ٢٠٢٠ و مايو ٢٠٢١ ضد الولايات المتحدة، أتهمت روسيا بالوقوف وراء هذه الهجمات. في آخر لقاء جمع بين الرئيس

الأمريكي بايدن و الروسي بوتين في جنيف في ١٦/ ٦/ ٢٠٢١م إذ كان جوهر اللقاء يتمحور عن الحرب السيبرانية التي تقوم بها روسيا ضد أمريكا، حيث وجه بايدن تحذيرا لبوتين أنه في حال قامت روسيا بهجوم سيبراني على مؤسسات أمريكية، فإن لدى أمريكا من وسائل الردع ما لا تتوقعه روسيا. أكد بايدن بأن ١٦ مؤسسة أمريكية تعرضت لهجوم سيبراني من بينها وزارة الدفاع., الاتهامات المتبادلة بين الصين والولايات المتحدة الأمريكية من جهة و بين روسيا و الولايات المتحدة تدل على وجود تنافس دولي كبير، و صراع للسيطرة على الفضاء السيبراني[٢٣]. و مما يدل على تنامي هذا الصراع قيام إدارة ترامب بحظر شركة هواوي من شبكات تقنيات الجيل الخامس (٥ جي) اللاسلكية في الولايات المتحدة، وضغطت على حلفائها للقيام بالمثل. حيث أعلنت المملكة المتحدة كذلك حظر أي معدات لشركة هواوي في إطار تطوير شبكة الجيل الخامس على أراضيها.وحظرت أستراليا واليابان "هواوي" على أراضيهما.و استنادًا لما تقدم، فإن الأمن السيبراني يُعَدُّ من أهم المتغيرات الجديدة المؤثرة في العلاقات الدولية؛ بسبب إن إمتلاك القوة التقنية والمعرفية هي قوة إضافية لعناصر قوة الدولة الشاملة في القرن الحادي والعشرين.

التحولات في مضامين القوة وظهور القوة السيبرانية

مع ثورة المعلومات ظهر شكل جديد من أشكال القوة هو القوة السيبرانية Cyber power، التي لها تأثير كبير على المستوى الدولي والمحلي، tثورة المعلومات أدت إلى توزيع وانتشار القوة بين عدد أكبر من الفاعلين مما جعل قدرة الدولة على السيطرة موضع شك، كذلك منحت الفاعلين الأصغر قدرة أكبر على ممارسة كل من القوة الصلبة والقوة الناعمة عبر الفضاء السيبراني، وهو ما يعني تغيرا في علاقات القوى في السياسة الدولية. مفهوم القوة السيبرانية يتناول مجمل القضايا التي تتعلق بالتفاعلات الدولية العسكرية، والاقتصادية، والسياسية، والثقافية، والإعلامية وغيرها. وحتى تتمكن الدولة اليوم من ممارسة النفوذ داخليا أو خارجيا عبر القوة السيبرانية يجب أن تتوافر لها مجموعة عناصر أهمها، وجود بنية

تحتية سيبرانية، تشمل أجهزة الكمبيوتر، وشبكات الاتصالات، والبرمجيات، وقواعد البيانات لمختلف الأنظمة والقطاعات. وجود بنية مؤسسية تتولى مهمة ممارسة القوة السيبرانية ،وتحقيق الأمن السيبراني للدولة.و وجود بنية تشريعية تكون ضامنة ومحددة لاستعمال القوة السيبرانية.وحتى تكتمل عناصر القوة السيبرانية لابد للدولة من القيام بتطوير أسلحة في مجال الحرب السيبرانية لاستعمالها سواء في العمليات الهجومية أو من أجل الردع.

أهداف الصراع السيبراني

للصراع السيبراني جملة من الأهداف، منها:

- صراع سيبراني سياسي، قد يأخذ شكلا عسكريا يتم فيه استخدام قدرات هجومية و دفاعية عبر الفضاء السيبراني بهدف إفساد النظم المعلوماتية، و الشبكات و البنية التحتية.
- صراع سيبراني ناعم: صراع حول الحصول على المعلومات، و التأثير في المشاعر و الأفكار، و شن حرب نفسية و إعلامية، من خلال تسريب معلومات، و استخدامها عبر منصات إعلامية، بما يؤثر على العلاقات الدولية كالدور الذي لعبه موقع ويكيليكس في الديبلوماسية الدولية.
- صراع سيبراني على التقدم التكنولوجي، يأخذ هذا النوع من الصراعات طابعا تنافسيا حول الاستحواذ على سباق التقدم التكنولوجي، وسرقة الأسرار الاقتصادية و العلمية، قد يمتد لمحاولة السيطرة على الإنترت و العمل على اختراقات الأمن القومي للدول، الأمر الذي قد يكون له تأثيرات مدمرة في الاقتصاد و البنية التحتية.

الأدوات المستخدمة في الصراع السيبراني

أولا: الجيوش السيبراني (Cyber Armies): نتيجةً لتطور المجتمعات، وتقدم الوسائل التكنولوجية التي تعتمد عليها في إجراء مختلف التعاملات، وتأمين المستلزمات

الضرورية، أصبح العالم يعتمد بشكل كبير على شبكات الإنترنت والاتصالات للحصول على كافة الخدمات المالية، والاجتماعية وإتمام عمليات البيع والشراء، وإرسال البيانات واستلامها إلكترونيًّا.كل هذا جعل الحكومات تفكر في تشكيل مجموعاتٍ إلكترونيةٍ عرفت باسم الجيوش السيبرانية، وتدريبها لحماية مواقعها، وقواعد البيانات التي تعتمد عليها خاصةً الحساسة منها، والتي قد تكون أهدافًا لدولٍ معاديةٍ، إضافةً لشن الهجمات على الأنظمة الإلكترونية في دولٍ أخرى كنوعٍ من الحروب ذات تكاليفَ أقل، ودون الحاجة للجنود والعتاد؛ لكونها قادرةً على تحقيق ضررٍ كبيرٍ لمختلف القطاعات والمجالات، وشل حركة البلاد. وتعرف الجيوش السيبرانية (Cyber Army) بأنها مجموعةٌ من الأفراد يتمتعون بخبرةٍ عاليةٍ في مجال تكنولوجيا المعلومات و الاتصالات، ويعملون لصالح حكومات أو دول أو جهات ذات توجهاتٍ سياسيةٍ محددةٍ، يعملون في الخفاء دون الظهور للعلن، وتستخدمهم الدول لحفظ أمنها السيبراني الوطني، وشن الهجمات السيبرانية على أهدافٍ معاديةٍ إن لزم الأمر[٢٨].

ثانيا الأسلحة السيبرانية: تصنف الأسلحة السيبرانية المستخدمة وفق التصنيف المستخدم في الحروب التقليدية،الذي يقسم الأسلحة إلى نوعين، أسلحة هجومية وأخرى دفاعية. كذلك الأسلحة المستخدمة في الفضاء السيبراني يمكن تقسيمها إلى:

أسلحه هجوميه:- تركز بشكل أساسي على تدمير البنية التحتية لدى الخصم أو إعطابها وعدم القدرة على الاستفادة منها ،أو تركز على جمع المعلومات بواسطة برامج للتجسس يتم زرعها في أجهزة الكمبيوتر الخاصة بالخصم، بحيث تقوم هذه البرامج بإرسال المعلومات أولاً بأول، ومن أشهر الأسلحة الهجومية(٣٧):

فيروسات الكمبيوتر: يعرف الفيروس بأنه برنامج صغير أو جزء من برنامج، يربط نفسه ببرنامج آخر لكنه يغير عمل ذلك البرنامج لكي يمكن الفيروس من التكاثر عن طريقه.

الديدان Worms: الدودة عبارة عن برنامج مستقل، يتكاثر بنسخ نفسه عن طريق الشبكات، وإذا لم تدمر الدودة البيانات، مثل الديدان التي تنتشر عبر الإنترنت؛ فهي قد تقطع

الاتصالات، كما أنها قادرة على تغيير شكلها، ومن هنا اختير لها لفظ (worm) الذي يعني بالإنجليزية إما دودة أو أفعى، للجمع بين سرعة انتشار الأولى وقدرة الثانية على تغيير جلدها، وهي غالبا تستخدم شبكات البنوك، أو البورصات.

أحصنة طروادة Trojan horses: نوع آخر من أنواع الأسلحة الهجومية، حصان طروادة عبارة عن جزء من الشفرة أو برنامج صغير مختبئ في برنامج أكبر، غالبا ما يكون من النوع ذائع الانتشار والشهرة، ويؤدي حصان طروادة مهمة خفية، هذه المهمة غالبا ما تكون إطلاق فيروس أو دودة.

القنابل المنطقية Logic Bombs: نوع من أحصنة طروادة، يزرعها المبرمج داخل النظام الذي يطوره أو تكون برنامجا مستقلا، والدول التي بسبيل شن حرب سيبرانية على أخرى تستخدم هذا النوع في التلصص والتجسس والوقوف على حالة الدولة المعادية، فمثلا يمكن للانتشار غير المنافس لبرامج التطبيقات والنظم الآلية التي تنتجها الولايات المتحدة الأمريكية وبدون منافس، مثل: مايكروسوفت، ويونكس و غيرها أن تقرر أمريكا عند نشوب حرب إلكترونية بينها وبين أية دولة أخرى معادية أو منافسة، أن يقوم البرنامج بإرسال معلومات هامة من الصعب الحصول عليها بواسطة النظام المخابراتي التقليدي، كما يمكن لهذه البرامج إتلاف كل ما هو موجود من بيانات على هذه الأجهزة.

الأبواب الخلفية backdoors: هي ثغرة تترك عن عمد من مصمم النظام؛ للتسلل إلى النظام عند الحاجة، وتجدر الإشارة إلى أن كل البرامج والنظم التي تنتجها الولايات المتحدة الأمريكية تحتوي على أبواب خلفية تستخدمها عند الحاجة، وهو ما يمكن هيئات وأركان حرب المعلومات من التجوال الحر داخل أي نظام لأية دولة أجنبية، وكشف أسرار هذه الدولة في جوانب عديدة.

الرقائق chipping : تماما مثلما يمكن للبرامج والنظم (software) أن تحتوي على وظائف غير معروفة أو متوقعة، فمن الممكن أن تحتوي بعض الرقائق على مثل تلك الوظائف، والمصانع

الأمريكية تنتج الملايين من تلك الرقائق، وهم سادة العالم في هذه الصناعة الدقيقة؛ حيث يمكن للدوائر المجمعة (Integrated Circuit-IC) التي تُعَدُّ من أهم مكونات الحواسيب أن تحتوي على وظائف إضافية أثناء تصنيعها، لا تعمل في الظروف العادية، إلا أنها قد تعلن العصيان في توقيت معين، أو بالاتصال بها عن بعد.

الماكينات والميكروبات فائقة الصغر: يطلق عليها (Nano machines and Microbes) ، وهي على عكس الفيروسات التي تصيب برامج ونظم المعلومات، يمكنها إصابة عتاد النظام نفسه ..(hardware) فالـ (Nano machines) عبارة عن (robots) فائقة الصغر قد تنتشر في مبنى نظام معلوماتي في دولة معادية أو منافسة؛ حيث تتفشى بداخل هذا المبنى حتى تجد حاسبًا آليا، وتدخل إليه من خلال الفتحات الموجودة به، وتقوم بإتلاف الدوائر الإلكترونية التي تُعَدُّ المكون الأساسي للكمبيوتر. أما الميكروبات؛ فمن المعروف أن بعضًا منها يتغذى على الزيت، فإذا تم تحويرها جينيًّا لتتغذى على عنصر الـ (silizium) المكون الهام في الدوائر الإلكترونية، فهذا يعني تدمير وإتلاف الدوائر الإلكترونية بأي معمل به حاسبات آلية أو حاسب خادم server لموقع على الإنترنت، أو مبنى هام أو حساس يدار بالكمبيوتر، أو حتى مدينة بأسرها عن طريق إتلاف دوائر التحكم الإلكترونية فيها، والتي تقوم على إدارة مرافقها الحيوية.

الاختناق المروري الإلكتروني: سلاح آخر من الأسلحة الإلكترونية يمكن من خلاله سد وخنق قنوات الاتصالات لدى العدو، بحيث لا يمكنهم تبادل المعلومات بشكل صحيح، حيث يتم استبدال المعلومات، وهي في طريقها بين المستقبل والمرسل بمعلومات مضللة.

الأسلحة الدفاعية:- الأسلحة الدفاعية المستخدمة في الفضاء السيبراني، تركز بشكل أساسي على حماية البنية التحتية من هجوم الخصم أو محاولة إعطابها و عدم القدرة على الاستفادة منها، وتتمثل هذه الأسلحة الدفاعية ببرامج مكافحة الفيروسات، وبرامج تمنع الخصم من اختراق نظم المعلومات، إضافة للبرامج التي تعمل على تشفير المعلومات حتى لا يتمكن

الخصم من الاستفادة من المعلومات المسروقة، ومن أشهر الأسلحة المستخدمة في الدفاع وردع هجوم الخصم:

برمجيات كشف ومقاومة الفيروسات: وهي البرمجيات المخصصة في اكتشاف الفيروسات والقضاء عليها قبل أن تتسبب هذه الفيروسات بالقضاء على نظم الكمبيوتر مما يؤدي إلى خسائر مادية لا حصر.

الجدران النارية Firewall: تقوم الجدران النارية بهذه المهمة، وتلعب دور حارس المنشأة الذي يقوم بالتأكد من هويات الداخل والخارج من وإلى المنشأة في السماح أو عدم السماح لشخص ما بالدخول لهذه المنشأة. تقوم الجدران النارية الحديثة بالبحث عن الفيروسات، ومراقبة عناوين الإنترنت، وكذلك مراقبة المحتوى الوارد إلى الشبكة. كما يمكن بواسطة هذه الجدران منع المتطفلين أو ما يسمى بالها كرز المختصين في اختراق شبكات الكمبيوتر، والعبث بالبيانات المخزنة، كذلك يمكن حجب مواقع مشبوهة بعدم السماح في الدخول وتصفح هذه المواقع.

التشفير Encryption: يعد علم التشفير أحد العلوم الهامة الذي يتطرق إلى مسألة أمن البيانات (Information Security)، والحاجة إلى سرية البيانات تعد حاجة قديمة بقدم الحضارة الإنسانية. فعملية تشفير المعلومات لها تأريخ طويل جدا، وقد استخدم المصريون القدماء طرق لتشفير معلوماتهم السرية قبل نحو ٤٠٠٠ سنة.و يُعَدُّ علم التشفير اليوم مهماً جدا خصوصا و أن جميع الأنشطة في جميع المجالات المدنية و العسكرية تمارس في الفضاء السيبراني.و يستخدم التشفير اليوم كأداة من أجل حماية الأسرار الدولية. في الفضاء السيبراني. يحظى علم التشفير في الوقت الحاضر باهتمام استثنائي في ميدان أمن المعلومات ، ومرد ذلك إلى أن الحماية بالتشفير يمثل الوسيلة الأكثر أهمية لتحقيق وظائف الأمن الثلاثة ، السرية والتكاملية، وتوفير المعلومات.

نماذج من الصراع السيبراني

الهجوم السيبراني الذي نفذته الولايات المتحدة الأمريكيّة، وصرّحت به عام 1982 ضدّ منظومة التحكّم العالية في أنبوب نفط (Chelyabinsk) التابع للاتحاد السوفياتي السابق، وهو ما نفاه الاتحاد السوفياتي السابق آنذاك(٤).

- في عام ٢٠٠٧ ، تعرضت دولة أستونيا، إلى وابل من الهجمات ضد مواقعها الإلكترونية، وكانت الأهداف الرئيسة، هي: مواقع الرئاسة الأستونية وبرلمانها، والوزارات والمؤسسات الحكومية، والأحزاب السياسية، ووكالات الأخبار، واثنان من أكبر البنوك ، وشركات متخصصة في مجال الاتصالات .
- في عام ٢٠٠٨م، تعرضت جورجيا إلي هجوم رقمي على شبكة الإنترنت، هذا الهجوم الذي يسمى بحجب الخدمة استهدف البنية التحتية للإنترنت، وموقع الرئاسة في جورجيا، ومواقع حكومية إلكترونية، وشبكات عسكرية[٣٨].
- في نيسان من العام2020م أعلن الكيان الإسرائيلي عن هجوم سيبراني، استهدف شبكات المياه الخاصة بها، واتهم الإسرائيليون إيران بالمسؤوليّة عن الهجوم، في حين أنّ الولايات المتحدة الأمريكيّة و الكيان الإسرائيل أطلقتا أكثر من فيروس؛ لاستهداف المنشأة النوويّة الإيرانيّة، وآخرها ما وقع في شباط وأيار وتموز من العام2020م، بحيث أقرّ وزير الأمن الإيراني "محمود علوي" بأنّ هناك أكثر من مليوني هجوم سيبراني وقع بين عامي 2019 م و2020م.
- يوم الثلاثاء ١٥ ديسمبر ٢٠٢٠ ذكرت وكالة رويترز أن مستشار الأمن القومي الأمريكي روبرت أوبراين قد قطع زيارته إلى أوروبا، وعاد إلى واشنطن من أجل تنسيق الرد على هجوم إلكتروني "سايبر" واسع النطاق وعالي المستوى. كانت وكالة "رويترز" قد أفادت يوم الأحد ١٣ ديسمبر بأن وزارتي الخزانة والتجارة الأمريكيتين تعرضتا لهجوم قراصنة إلكتروني ناجح من قبل مجموعة من هاكرز تدعمهم دولة أخرى. ونقلت صحيفة "واشنطن بوست" عن مصادر لها أن أصابع الاتهام، وجهت إلى قراصنة روس، دون ورود أي أدلة تدعم هذه الفرضية. وطال

الاختراق الإلكتروني عددا من أبرز المؤسسات الحكومية الأمريكية، من بينها وزارات الخارجية، والخزانة، والأمن الداخلي، والتجارة. من جانبها ذكرت صحيفة "نيويورك تايمز"، بأن الهجوم يعد واحدا من أكثر الاختراقات تعقيدا، وربما أكبرها منذ أكثر من خمس سنوات، وأفادت بأن المتسللين "على الأرجح يعملون لصالح روسيا"[٢٠].

- في مايو ٢٠٢١م أعلن البيت الأبيض حالة الطوارئ في ١٧ ولاية أمريكية، إثر تعرض شركة "كولونيال بايبلاين" المشغلة لأنابيب الوقود في الولايات المتحدة لهجوم إلكتروني. وشملت حالة الطوارئ ولايات فرجينيا، وماريلاند، وديلاويرو، وأركنساس، وفلوريدا، وجورجيا، وكنتاكي، ولويزيانا، وميسيسيبي، ونيوجيرسي، ونيويورك، وكارولينا الشمالية، وبنسلفانيا، وكارولينا الجنوبية، وتينيسي، وتكساس، وآلاباما، حيث سيتم نقل الوقود عن طريق البر للعاصمة واشنطن[٢٠].

استعدادت الدول للحرب السيبرانية

أدركت العديد من الدول من وقت مبكر أهمية الفضاء السيبراني، و احتمالات نشوب حرب في هذا الفضاء، لذا عززت من قدراتها حيث أنشأت تشكيلات عسكرية خاصة بالفضاء السيبراني، قامت بتطوير إستراتيجية أساسية في مجال الأمن السيبراني في إطار الإستراتيجية العامة في كل القطاعات. قال فلاديمير أوليانوف مدير دائرة التحليل لدى وكالة الاستشارات الأمنية زيكوريون الاستشارية في تحليل المعلومات، والتي مقرها موسكو: إن الولايات المتحدة تنفق على أمن الفضاء الإلكتروني أكثر من أي بلد آخر، وزارة الدفاع الأمريكية لديها ميزانية سنوية تبلغ ٧ مليارات $ للأمن السيبراني، وعدد الموظفين القراصنة يبلغ أكثر من ٩٠٠٠ موظف، لذا تأتي في المرتبة الأولى، و تأتي الصين في المرتبة الثانية تنفق سنويا ١,٥ مليار دولار، في المرتبة الثالثة، تأتي المملكة المتحدة تنفق سنويا ٤٥٠ مليون دولار، تأتي كوريا الشمالية في المرتبة الرابعة، خصصت نحو ١٪ من الميزانية العسكرية

للأمن السيبراني، روسيا تحتل المرتبة الخامسة في العالم، حسب تقارير كوميرسانت اليومية، نقلا عن دراسة أجرتها وكالة زيركون للتحليلات. تقارير كوميرسانت تظهر أن قوات الأمن السيبراني الروسية وصلت إلى ١٠٠٠ موظف، وتنفق وزارة الدفاع الروسية حوالي ٣٠٠ مليون $ سنويا على مثل هذه الأنشطة[٣٩].

القدرات السيبرانية الأمريكية: تُعَدُ الولايات المتحدة الأمريكية الدولة الأكثر تفوقًا في مجال امتلاك القدرات العسكرية السيبرانية، فقد تم تشكيل قيادة سيبرانية موحدة في وقت مبكر من عام ٢٠١٨م، من أجل التماشي مع التطور الكبير والواسع في القدرات السيبرانية الأمريكية، وقد كان هذا أحد أهداف الإستراتيجية السيبرانية الوطنية لوزارة الدفاع الأمريكية. ويشغل منصب قائد هذه القيادة الموحدة مدير وكالة الأمن القومي، وتشرف السلطات الحكومية الأمريكية على تنظيم قدراتها المختلفة. تعتمد القيادة السيبرانية الأمريكية على خمسة مكونات أساسية: القيادة السيبرانية للجيش، وقيادة الأسطول السيبراني، والقيادة الإلكترونية للقوات الجوية، والقيادة الإلكترونية لقوات مشاة البحرية وخفر السواحل، بالإضافة إلى وحدات الحرس الوطني. ويبلغ عدد الفرق السيبرانية في هذه القيادة نحو ١٣٣ فريقًا يضطلع بمهام مختلفة في مجال حماية الأمن السيبراني الأمريكي.

القدرات السيبرانية الصينية: أنشأت الصين في عام ٢٠١٥م قوة الدعم الإستراتيجي كجزء من الإصلاحات التنظيمية لجيش التحرير الشعبي، وتجمع هذه القوة بين قدرات الحرب الفضائية والسيبرانية والنفسية. وتتبع اللجنة العسكرية المركزية، ولها فرعان: إدارة أنظمة الشبكة التي تسيطر على القوة الإلكترونية المسؤولة عن عمليات المعلومات، وإدارة النظم للعمليات الفضائية. وتتحدد مسؤولية هذه القوة في دعم المعلومات الإستراتيجية من خلال جمع المعلومات الاستخباراتية الفنية، ومد القوات المسلحة بهذه المعلومات؛ لتمكينها من شل وتخريب عمليات العدو وأنظمة قيادة الحرب[١٨].

القدرات السيبرانية البريطانية: تتركز القوة السيبرانية للمملكة المتحدة – بشكل أساسي- في المركز القومي للأمن السيبراني، إلى جانب القدرات التي يمتلكها مكتب الاتصالات

الحكومية (جهاز المخابرات البريطاني) في مجال الاستخبارات السيبرانية. وتقود التشكيلات العسكرية السيبرانية في بريطانيا القيادة الإستراتيجية التي تأسست في عام ٢٠٢٠، لعدم وجود قيادة عسكرية سيبرانية موحدة. فالقوات المسلحة البريطانية تمتلك بعض التشكيلات الخاصة بالفضاء الإلكتروني. كما قامت الدولة بتطوير إستراتيجية أساسية في مجال الأمن السيبراني في إطار الإستراتيجية العامة في كل القطاعات[٢٦]. أعلنت وزارة الدفاع في المملكة المتحدة أن الجيش البريطاني أطلق فوجه السيبراني المتفرغ الأول المخصص لمواجهة الدول المعادية والمجموعات الإرهابية المحلية والخارجية. (ويطلق تعبير "سيبراني" على الوسائل الإلكترونية التي تعمل في الفضاء الافتراضي للإنترنت وغيرها من الشبكات الرقمية[٣١].

القدرات السيبرانية الروسية: اعتبرت الإستراتيجية والعقيدة العسكرية الروسية –تاريخيًا– الأمن السيبراني والعمليات الإلكترونية مكونًا من عمليات المعلومات بمفهومها الواسع، كشفت العقيدة العسكرية الروسية لعام ٢٠١٥ عن أن الفضاء السيبراني جزء من الأراضي الروسية، ومن ثم كلفت القوات المسلحة بحمايته، كما قدمت وثيقة صادرة في عام ٢٠١١ بعنوان "آراء مفاهيمية حول نشاط القوات المسلحة للاتحاد الروسي في فضاء المعلومات".شكلت السلطات الروسية في عام ٢٠١٧ "قوات عمليات المعلومات".

المحور الخامس: تعزيز الأمن السيبراني (تعزيز بيئة العمل في الفضاء السيبراني)،طرق مكافحة الجرائم السيراني، دور مؤسسات التعليم العالي في تعزيز العمل الفضاء السيبراني وتأمينه.

أصبحت قضية أمن الفضاء السيبراني تدخل في إستراتيجيات الأمن القومي للعديد من الدول من أجل الاستحواذ على مصادر القوة داخل الفضاء الإلكتروني ،و للعمل على الحيلولة دون تعرض بنيتها التحتية الحيوية للخطر الذي ينجم جراء قطع خدمة الإنترنت أو ضرب مواقعها أو توقف رسائل البث الإذاعي أو التلفزيوني أو توقف موجات الراديو أو سقوط شبكات المحمول أو البث الفضائي ، وأصبح لها تأثير عميق على المجتمع والاقتصاد على النطاق الدولي[٢٧].

طرق مكافحة الجرائم السيراني

مكافحة الجريمة السيبرانية للحد منها، و التقليل من الخسائر الناجمة عنها تتمثل في تكاتف و تظافر الجهود الدولية و المحلية؛ لكونها جريمة عابرة للحدو، و للحد من هذه الجريمة يجب القيام بمهام عديدة، من هذه المهام[١٢]:

- توعية المجتمع لمفهوم الجريمة السيبرانية و بمخاطرها ، المخاطر التي تهدد السلم المحلي و الدولي، لذا يجب مواجهة هذا الخطر، والحرص على ألا يقعوا ضحية ، هذه التوعية تتمثل في ضرورة التأكد من العناوين الإلكترونية التي تتطلب معلومات سرية خاصة كبطاقة ائتمانية أو حساب بنكي، وعدم الإفصاح عن كلمة السر لأي شخص والحرص على تحديثها بشكل دوري واختيار كلمات سر غير مألوفة يسهل التنبأ بها، وعدم حفظ الصور الشخصية في الكمبيوتر، عدم تنزيل أي ملف أو برنامج من مصادر غير معروفة. والحرص على تحديث أنظمة الحماية باستخدام برامج الحماية، مثل: نورتون(norton) ، كاسبر سكي، ومكافي...(Mcafee)...إلخ.
- ضرورة إنشاء منظمة محلية لمكافحة الجريمة الإلكترونية.
- إبلاغ الجهات المختصة في حال تعرض لجريمة سيبرانية.
- ضرورة تتبع تطورات الجريمة الإلكترونية وتطوير الأجهزة والتشريعات لمكافحتها

- تطوير برمجيات محلية آمنة ونظم تشغيل قوية للحد من الاختراقات الإلكترونية، وكذا برمجيات الفيروسات، وبرامج التجسس، مثل: مضادات التجسس، وهي: برامج تقوم بمسح الحاسب للبحث عن مكونات التجسس وإلغائها مثل (lava soft).

دور مؤسسات التعليم العالي في تعزيز و تأمين العمل الفضاء السيبراني

تعد الجامعات من المؤسسات التربوية الهامة؛ إذ تقع في قمة السلم التعليمي ، وتقع عليها العديد من المسؤوليات المتعلقة بمواجهة مشكلات المجتمع، وتلبية احتياجاته، وتحقيق تقدمه. و الجامعات تضم النخب الفكرية والعلمية في المجتمع، ولم يعد ينظر إليها على أنها مكان للدراسة فحسب، بل أصبح ينظر إليها فضلاً عن ذلك على أنها بيت الخبرة، وعلى عاتق هذه المؤسسات يقع العديد من الأعمال و الأنشطة التي من شأنها تعزيز الأمن السيبراني، فقيام هذه المؤسسات بتوعية المجتمع وتثقيفه بأساسيات أمن المعلومات باستخدام طرق وأساليب متعددة كالدورات، والندوات، والمحاضرات، والورش، والمطويات، ونقل الثقافة والمعرفة داخل المؤسسة. بعض أدوار الجامعات في مواجهة الجرائم المعلوماتية والحفاظ على الأمن المعلوماتي منها[٤٠].

- نشر التوعية و تثقيف المجتمع بما من شأنه تعزيز الأمن السيبراني.
- إقامة دورات متخصصة للعاملين في مختلف القطاعات، و تعريفهم بتحديات الفضاء السيبراني، و كيفية مواجهة تلك التحديات و التهديدات.
- إدخال بعض المقررات الجديدة التي تعني بهذه المشكلة، للطلاب في جميع التخصصات.
- تعاون الجامعة مع بعض مؤسسات المجتمع المدني، والوزارات في مواجهة هذه المشكلة، من خلال دورات وندوات توعية بثقافة أمن المعلومات.
- إنشاء تخصص مستقل في الأمن السيبراني.
- تبادل الخبرات مع الجامعات الأجنبية والعربية في مجال الامن السيبراني.

- توعية الطلاب بهذا النوع من الجرائم من خلال الندوات، و البحوث، و المؤتمرات، والمناقشات الجماعية.
- تحديث مناهج كلية الشريعة و القانون لمواكبة التحديات التي فرضها الفضاء السيبراني، التحديات المتمثلة بالجرائم التي ترتكب في الفضاء السيبراني.

المحور السادس: النتائج و التوصيات

■ أولاً النتائج:

- تشهد التقنية والتكنولوجيا تطورات كثيرة، واستحداث لأمور جديدة، هذا الامر ينذر بتطور أدوات وسبل الجريمة السيبرانية بشكل أكثر تعقيدا أو أشد ضررا من قبل، الأمر الذي يلزم الدول لتطوير آليات مكافحة هذه الجرائم، واستحداث خطوط دفاع، وسن قوانين لردع مرتكبي هذه الجرائم.
- في ظل هذه التكنولوجيا المتطورة يشهد العالم تغيرات سريعة جدا، تغيرات إيجابية وسلبية، كانت التغيرات السلبية لها درجة أقوى من التأثير خاصة في مجال المساس بأمن الدول؛ وذلك نتيجة انتشار الهجمات في الفضاء السيبراني، الأمر الذي فرض على كثير من الدول رسم خطط، و وضع إستراتيجيات، و سن قوانين جديدة للحد من الهجمات السيبرانية.
- في ديسمبر ٢٠٢٠م أفادت مجلة بوليتيكو الأمريكية، نقلا عن مسؤولين مطلعين بشكل مباشر، أن لدى وزارة الطاقة الأمريكية وإدارة الأمن النووي الوطنية، التي تدير مخزون الأسلحة النووية في البلاد، أدلة على أن قراصنة تمكنوا من الوصول إلى أنظمتهم في إطار حملة إلكترونية ضخمة.
- لحماية أنفسنا سواءً جهات حكومية، مؤسسات، شركات أو أفراد من هجمات القرصنة والاختراق لا بد من التعامل مع أمن المعلومات كضرورة؛ وذلك بتطبيق أعلى معايير الأمان لحماية الشبكات، والأجهزة، و الأشياء الموصولة بالإنترنت، خصوصا في ظل تزايد اتصال الناس مع بعضهم ومع الأشياء من حولهم.
- ذكر تقرير منتدى الاقتصاد العالمي أن وظائف الأمن السيبراني تعد من وظائف العصر الجديد التي سيستمر الطلب عليها بشكل كبير خلال الأعوام القادمة، بحلول عام ٢٠٢١ من المتوقع أن تتزايد الوظائف في المجال السيبراني إلى نحو ٣,٥ مليون، و تشير التوقعات المستقبلية أن هذا الرقم سيصل إلى قرابة 6 ملايين وظيفة شاغرة في عام

2022م منها ٪ 25في منطقة الشرق الأوسط، هناك اليوم أكثر من 250 ألف وظيفة شاغرة في الشرق الأوسط لمختصي الأمن السيبراني[٢٨].

- مع تحول الفضاء السيبراني إلي ساحة للتفاعلات الدولية، برز العديد من الأنماط التوظيفية له، سواء على صعيد الاستخدامات ذات الطبيعة المدنية أو العسكرية، الأمر الذي جعل هذا الفضاء مجالا للصراعات المختلفة، سواء للفاعلين من الدول أو غير الدول لحيازة أكبر قدر من النفوذ والتأثير السيبراني.
- الحرب السيبرانية ليست لها تأثيرات نقدية فقط، يمكنها أن تتسبب في حدوث أضرار نفسية واجتماعية، و يمكن لها تدمير أخلاقيات المجتمع لكسب دعمه أو لزعزعة استقراره عبر تشويه الجهود التي يبذلها القادة لحماية مواطنيهم، ويمكنها أيضا تعطيل البنية التحتية الحيوية الإستراتيجية للدولة مما يهدد الجيوش والأمن؛ لعدم وجود وسائل قيادة، وأدوات فعالة أو كافية، الأمن للمرافق التي تعمل في الفضاء السيبراني.
- باتت منصات التواصل الاجتماعي أماكن مثالية للجماعات المتطرفة والإرهابية لنشر أفكارها الهدامة، وتجنيد النشء والشباب، وغسل أدمغتهم. لذا باتت هذه الوسائل تمثل تحديا كبيرا؛ بسبب طبيعة تأثيرها في صناعة الرأي العام وتشكيله، و كذا في كيفية تأثيرها في تشكيل الوعي لدى الشباب، كل هذه التحديات من شأنها تهديد أمن الدول واستقرارها. كما باتت تمثل أهم الأدوات التي يتم توظيفها في إدارة الصراعات والأزمات الدولية، سواء من خلال بث الإشاعات الاقتصادية والسياسية والعسكرية التي يمكن أن تزلزل اقتصادات دول كبيرة[٢١].
- أظهرت أحداث الهجوم على مبنى الكونجرس الأمريكي و مجلس النواب من قبل أنصار الرئيس الأمريكي السابق بايدن على إثر هزيمته في الفوز بولاية ثانية وكذا أحداث الربيع العربي، أن الفيسبوك والتوتير وغيرها من وسائل التواصل الاجتماعي تحتوي على الكثير من المحتوى الذي يهدد الاستقرار الاجتماعي

والسياسي و أنه لا توجد وسيلة فعالة لمواجهة مثل هذه التكنولوجيا حتى لدى الدول المصنعة لهذه التكنولوجيا.

- أثبتت الدراسة وجود صراع دولي كبير في السيطرة على الفضاء السيبراني، وذلك لما لهذا الفضاء من أهمية و تأثير في مختلف المجالات، لذا تنافس الدول اليوم في تطوير الأبحاث في مجال الذكاء الاصطناعي والنانو تكنولوجي لتعزيز قوتها السيبرانية لمواجهة نشوب أي حرب سيبرانية قادم.
- اختراق البريد الإلكتروني للشركات يعد أحد أكثر أنواع الهجمات السيبرانية شيوعاً، يؤكد مكتب التحقيقات الفيدرالي إن هذه الهجمات تتسبب في خسائر بقيمة ما يقرب من ٩ مليارات دولار سنوياً.
- أشار التقرير الصادر في مايو ٢٠٢٠ عن الاتحاد الدولي للاتصالات أن التوسع في اعتماد إنترنت الأشياء مع وجود عشرات إن لم يكن مئات المليارات من الأجهزة الجديدة الموصولة يفتح الباب أمام عدد كبير من نقاط الضعف الجديدة المحتملة في هذا الفضاء[٣٧].
- تشير التوقعات أن تزداد المخاطر الأمنية في الفضاء السيبراني مستقبلا خصوصا مع ظهور تكنولوجيات جديدة من قبيل الجيل الخامس وإنترنت الأشياء. في ٢٠١٧ أكد مكتب التحقيقات الفيدرالي الأمريكي على الفرص المختلفة المتاحة لمرتكبي الجرائم السيبرانية للنفاذ إلى إنترنت الأشياء وأجهزة أخرى إلى جانب المعلومات المخزنة بهذه الشبكات.
- مما لا شك فيه بأن لشبكات التواصل الاجتماعي، من "تويتر" و"فيسبوك" وسواهما، وقع مهم في تاريخ صناعة الرأي العام، إذ تنتشر على نطاق واسع، على صعيد مختلف الشرائح الاجتماعية، وحتى أكثرها فقراً، و تعد ثورة القرن الواحد والعشرين من الناحية الإعلامية، نظراً إلى أهمية الدور الذي باتت تؤديه في مختلف الميادين، السياسية منها والاجتماعية والتسويقية.

- كشف تقرير صادر عن مركز شكاوى جرائم الإنترنت التابع لمكتب التحقيقات الفيدرالي عن زيادة كبيرة في جرائم الإنترنت المبلغ عنها، زادت الجرائم المبلغ عنها بنسبة ٣٠٠٪ خلال عام ٢٠٢٠.
- أفضل التقنيات المتاحة اليوم لتعزيز الأمن السيبراني هي التشفير، وبرامج مكافحة الفيروسات، وجدار الحماية، والتوقيعات الرقمية، والمصادقة الثنائية.

■ **ثانيا الـتوصيات:**

- تأسيس هيئة عليا في الدولة أو فرع في القوات المسلحة له ارتباط مباشر بالقيادة العامة للقوات المسلحة، يتولى مهمة وضع الخطط الإستراتيجية، وتهيئة الكوادر، وإدارة الحرب الإلكترونية في الجوانب الدفاعية والهجومية على حدٍ سواء.
- مضاعفة الاهتمام بالأنشطة والفعاليات والبحوث في المجال الإلكتروني سواء في الجوانب السلمية أو العسكرية، ومن صور ذلك:
  - استحداث قسم لدراسات الحرب الإلكترونية في الجامعات العسكرية أو المدنية.
  - تنظيم المسابقات والمعارض والندوات والمؤتمرات العلمية والدولية في المجالات الإلكترونية؛ لاستقطاب، وتشجيع الموهوبين في مجال الحاسبات الإلكترونية، وتقديم الرعاية لهم؛ لغرض الاستفادة من خبراتهم في سبيل بناء قوة ردع إلكتروني أو ما يسمى ب (الجيش الإلكتروني) .
  - إرسال البعثات الدراسية والزمالات البحثية المتخصصة في مجال حرب الشبكات والوقاية منها .
  - وضع إستراتيجية مستقبلية لتشجيع الاستثمار في مجال صناعة الأجهزة والمنظومات الإلكترونية محليا؛ بغية التقليل من الاعتماد على استيرادها من الخارج، لتعزيز الأمن السيبراني، واستبعاد خطر إرسال أجهزة مصممة في

الدول الاجنبية لاختراق الأنظمة، و كذا لحماية المجتمع من مخاطر الفضاء السيبراني بفلترة المعلومات المنتشرة في هذا الفضاء .

- السعي لإبرام اتفاقيات تعاون مشترك مع الدول التي لها خبرة كبيرة في مجال البرمجيات الإلكترونية؛ للإفادة منها في تطوير كوادرنا الوطنية .يمكن كذلك تبني مبادرة دولية لإبرام اتفاقية دولية متعددة الأطراف في سبيل تطوير قواعد القانون الدولي في مجال مواجهة مخاطر الحرب الإلكترونية، أو تحديد نطاقها وضبط مساراتها على أقل تقدير[٢١].
- ضرورة عزل المنظومات الأمنية والسيادية الحيوية بشبكة داخلية مستقلة ومحمية من الحاسبات لمنع اختراقها أو التأثير عليها تحت أي ظرف، مع عمل نسخ احتياطية، لكل ملفات المعطيات والبرامج العاملة، ومراعاة تجديدها باستمرار.
- وضع إستراتيجية وطنية لضمان الأمن السسيراني و مكافحة الجرائم السيبرانية.
- ضرورة اعتماد وسائل ناجعة للتوعية و التدريب حول الأمن السيبراني.
- تفعيل و تطبيق قوانين و تشريعات تجريم الجرائم السيبرانية لحماية المجتمع.
- متابعة التوصيات الصادرة من المنظمات الدولية المعنية بالأمن السيبراني، خصوصا الصادرة من الاتحاد الدولي للاتصالات،و من البرنامج العالمي للأمن السيبراني الجهود و غيرها من المنظمات و الهيئات الدولية المهتمة بالأمن السيبراني.
- تعزيز الأمن السيبراني يتم من خلال القيام بمجموعة من الأعمال، أهمها يتمثل في:
  - ضرورة توفير الدورات التدريبية العالية المستوى، وتنظيم الندوات، وورش العمل والمؤتمرات بمشاركة الشركات والمؤسسات الدولية المتطورة في مجال تقنيات المعلومات والاتصالات لاطلاع الكوادر الفنية على أحدث التقنيات لمواكبة التطور السريع، والتعرف على التقنيات الحديثة في مجال الخدمات الإلكترونية على المستوى العالم؛ وذلك بهدف خلق كوادر فنية

عالية قادرة على التصدي للتحديات الجديدة المرتبطة بهذه التقنيات وكيفية التغلب عليها.

- ضرورة حصول المؤسسات على أحدث التقنيات الحديثة سواء فيما يتعلق بالأجهزة (Hardware)، و البرامج Software) لمواجهة أحدث التطورات والأساليب المتبعة في مجال الهجمات والقرصنة الإلكترونية الدولية، بهدف اقتناء جدار أمني أكثر فعالية وقادر على التصدي لأحدث الأساليب المتبعة في هذا الشأن.
- ضرورة استحداث تخصص الأمن السيبراني في الجامعات العربية المتخصصة في مجال تقنية المعلومات أسوة بالجامعات العالمية، بهدف خلق الكوادر العربية المتخصصة ذات المستوى العالي في هذا المجال.جب، خصوصا في ظل الاحتياجات المتنامية للمتخصصين في هذا المجال .

المراجع

١. د.حميد الريـــمـــي، تكنولوجيا المعلومات متطلب أساسي للاقتصاد المعرفي، المؤتمر العربي الدولي للتكنولوجيا الإلكترونية– الدورة الثالثة، جامعة الزرقاء، ٢٥-٢٧/ ٤/ ٢٠١٢.

٢. د.حميد الريمي، تكنولوجيا المعلومات وأثرها على الاقتصاد، مجلة الباحث الجامعي، العدد(٢٩) يناير–مارس ٢٠١٣، ٣٨٣-٤٣٠.

٣. almalnews.com

٤. يائير كوهين، الفضاء الإلكتروني والبعد الخامس للحرب، القدس، ٢٠١٢.

٥. إيمان محمد الشورة، الأمن السيبراني في البنوك الإسلامية الأردنية،الجامعة الأردنية، كلية الشريعة، ٢٠٢٠م.

٦. د.نورة شلوش، القرصنة الإلكترونية في الفضاء السيبراني" التهديد المتصاعد لأمن الدول"، مجلة مركز بابل للدراسات الإنسانية، ٢٠١٨م، المجلد :٨ ،العدد :٢.

٧. روان بنت عطية الله الصحفي، الجرائم السيبرانية، المجلة الإلكترونية الشاملة، العدد ٢٤، مايو ٢٠٢٠م.

٨. http://taqana.net/introduction-to-the-internet-of-things

٩. د.حميد الريـــمـــي، أهمية تقنية المعلومات في خدمة المعارف الإسلامية، المجلة الدولية للتطبيقات الإسلامية في علم الحاسب والتقنية، المجلد3 ، العدد 2 يونيو،2015، ٢٤-٤٤.

١٠. د.حميد الريـــمـــي، الفجوة الرقمية مظاهرها،مستوياتها و تداعياتها على الوطن العربي، مؤتمر المحتوى العربي على الإنترنت،التحديات والطموحات، جامعة الإمام محمد بن سعود الإسلامية، ٣-٥ / ١٠ / ٢٠١١.

١١. http://www.nasdaq.com، إحصاءات التجارة الإلكترونية وحقائق التسوق عبر الإنترنت

١٢. ٢٠٢٠ https://entrepreneuralarabiya.com/2017/01/12/8796

١٣. الأمان في الفضاء السيبراني و مكافحة الجرائم السيبرانية في المنطقة العربية،تقرير اللجنة الاقتصادية و الاجتماعية لغربي أسيا (الإسكو)، ٢٠١٥.

١٤. https://www.nasdaq.com/articles/uk-online-shopping-and-e-commerce-statistics

١٥. https://www.researchgate.net/publication/

١٦. https://wearesocial.com

١٧. روان بنت عطية الله الصحفي، الجرائم السيبرانية، المجلة الإلكترونية الشاملة، العدد ٢٤، مايو ٢٠٢٠.

١٨. https://www.itu.int/en/ITU- T/studygroups/com17/Pages/cybersecurity.aspx
١٩. خالد وليد محمود، الهجمات عبر الإنترنت :ساحة الصِّراع الإلكترونيِّ الجديدة،المركز العربي للأبحاث ودراسة السياسات، سبتمبر ٢٠١٣م.
٢٠. https:// hbrarabic.com
٢١. مشتاق طلب فاضل،دور مواقع التواصل الاجتماعي في تكوين الرئي العام المحلي، مجلة تكريت للعلوم الإنسانية،العدد١٢، ١٩٣-٢٣١.
٢٢. https://democraticac.de/wordpress/، الأبعاد العسكرية للقوة السيبرانية على الأمن القومى للدول ''دراسة حالة إسرائيل"
٢٣. www.bbc.com\ Arabic
٢٤. https:// hbrarabic.com
٢٥. www.bbc.com\ Arabic
٢٦. infosecurity-magazine.com
٢٧. دويب حسين صابر، القوانين العربية وتشريعات تجريم الجرائم السيبرانية وحماية المجتمع، الرياض، ٢٠٠٩م.
٢٨. www.jinfowar.com،
٢٩. www.amf.org.ae (صندوق النقد العربي).
٣٠. purplesec.us
٣١. https://www.independentarabia.com/)،وحدة أولى في الجيش البريطاني متفرغة لحروب الإنترنت
٣٢. blog.f-secure.com
٣٣. verizon.com
٣٤. د.محمود محارب إسرائيل والحرب الإلكترونية، قراءة في كتاب :حرب في الفضاء الإلكتروني :اتجاهات وتأثيرات على إسرائيل، حقوق النشر والطبع محفوظة للمركز العربي للأبحاث ودراسة السياسات2022.
٣٥. https://www.alroeya.com/ ،» صراع الكبار».. حرب سيبرانية أمريكية روسية في الأفق.
٣٦. https://www.aliqtisadalislami.net/، إستراتيجية تعزيز الأمن السيبراني للاقتصاد الرقمي.
٣٧. Diego Rafael Canabarro and Thiago Borne," Reflection on the fog of Cyber War", National Center for Digital Government, Policy working Paper No.13:001, March 1, 2013, footnote 11, p.10
٣٨. https://www.sasapost.com
٣٩. https://katehon.com/ar
٤٠. مديحة فخري محمود محمد، دراسة مستقبلية لدور الجامعات المصرية في مواجهة الجرائم الإلكترونية لدي الطلاب، مؤتمر التربية في عالم متغير، الجامعة الهاشمية، الأردن، ٢٠١١، 205-166 .