العراق والأمن السيبراني ..الفرص والتحديات

Ministry of Higher Education and Scientific Research

أ.م.د. زهير خضير عباس الزبيدي
جامعة واسط – كلية القانون

أ.م.د. ظفر عبد مطر التميمي
الجامعة المستنصرية

الملخص :-

تعتمد المجتمعات الحديثة بشكل متنامي على تكنولوجيات الاتصالات والمعلومات المتصلة بالشبكة العالمية ، وفي ظل الثورة الرقمية المعاصرة والتي شكلت ثورة حقيقية في كل مناحي الحياة ، ومع التطور الهائل في وسائل وأجهزة الاتصالات ، وهو ما حول العالم إلى نقطة الصفر وتحولت الكرة الأرضية إلى اصغر من كرة صغيرة بيد مستخدم هذه الوسائل . لقد بات الأمن السيبراني يشكل جزءاً أساسياً من أي سياسة أمنية وطنية ، وصار معلوماً أن صناع القرار في الدول المتقدمة مثل : الولايات المتحدة الأمريكية، الاتحاد الأوروبي، روسيا، الصين، الهند وغيرها من الدول، أصبحوا يصنفون مسائل الدفاع السيبراني/الأمن السيبراني كأولوية في سياساتهم الدفاعية الوطنية ، فضلا عن أن أكثر من 130 دولة حول العالم قامت تخصيص أقساماً وسيناريوهات خاصة بالحرب السيبرانية ضمن فرق الأمن الوطني . وتضاف جميع هذه الجهود إلى الجهود الأمنية التقليدية لمحاربة الجرائم الالكترونية، الاحتيال الالكتروني والأوجه الأخرى للمخاطر السيبرانية . إن سوء الاستغلال المتنامي للشبكات الالكترونية لأهداف إجرامية يؤثر سلباً على سلامة البنى التحتية للمعلومات الوطنية الحساسة .

الكلمات المفتاحية : الأمن السيبراني – المعلومات – النهضة المعلوماتية .

Ministry of Higher Education and Scientific Research

Wasit University / College of Law

Al- Mustansiriyah University

Al Mustansiriyah Centre for Arabic and International Studies

Abstract :-

Modern societies are increasingly dependent on communication and information technologies connected to the global network, in light of the contemporary digital revolution, which has constituted a real revolution in all aspects of life, with the tremendous development in the means and devices of communication, which transformed the world to zero point and turned the globe into smaller than a small ball in the user of these means . Cyber security has become an essential part of any national security policy, it has become known that decision-makers in developed countries such as: the United States of America, the European Union, Russia, China, India and other countries have come to classify cyber defense / cyber security issues as a priority in their policies national defense . In addition , more than 130 countries around the world have allocated sections and scenarios for cyber warfare within the national security teams. All of these efforts are in addition to traditional security efforts to combat cybercrime, fraud and other aspects of cyber risks . The growing misuse of electronic networks for criminal purposes negatively affects the integrity of sensitive national information infrastructures .

Key words:- Cyber security - Information - Information Renaissance .

المقدمة :-

قدمت المعلومات إنجازات مهمة للإنسانية على مر العصور، تمثلت في المساعدة على بناء المجتمعات وتأسيس وتطوير المنظمات الإدارية والسياسية والإقتصادية والعسكرية، وساعدت الإنسان على اكتشاف الزراعة والتحول من المجتمع الرعوي إلى المجتمع (الزراعي، والصناعي، المعلوماتي)، من خلال ثوراتها المتوالية (اللغة، والكتابة، والطباعة، والثورة الصناعية، وثورة المعلومات). توجهت العديد من الدول لوضع إستراتيجية وطنية شاملة من أجل ضمان أمن

المعلومات في الفضاء السيبراني، فأمن المعلومات مهمة تعتبر ضمن مفهوم الأمن الوطني العام والشامل للدول مؤسسات وأفراد، وبدأت الكثير من الدول تدرك أن التغيرات المتسارعة في التكنولوجيا تؤدي إلى تهديدات ليست بالسهلة لأمن الوطن والمواطن ، ولذا لا بد من ضرورة العمل على ضمان أمن المعلومات من خلال خطوات مهمة للأمن السيبراني لحماية الأمن الوطني بمفهومه الشامل، من أجل حماية نظم المعلومات ووسائل الاتصالات لحماية الوطن والمواطن والمؤسسات من أخطار الفضاء السيبراني. أن الدول أصبحت ترتب أمورها لمواجهة حروب المستقبل التي تعتمد على التخريب والتدمير من خلال الفضاء السيبراني، وهذا أصبح جزءً من تكتيك واستراتيجيات الدول المتقدمة، لمواجهة هذه الحروب أو القيام بها . أن التطور الهائل في الجانب المعلوماتي لم يكن ليصل بالضرورة إلى كافة أصقاع المعمورة، كما أن تباينا في الاستخدام والتوظيف والاستفادة يكاد يكون واضحا بين دولة وأخرى ، طبقا للمنهج الفكري والإستراتيجية التي تتبعها الدول والتي تعبر فيها عن رؤيتها لمقدار المصالح المتحققة من إدخال مفهوم المعلومات إلى منظومة بناء الدولة . ومن هنا توجهت العديد من الدول لوضع إستراتيجية وطنية شاملة من أجل ضمان أمن المعلومات في الفضاء السيبراني، فأمن المعلومات مهمة تعتبر ضمن مفهوم الأمن الوطني العام والشامل للدول مؤسسات وأفراد، وبدأت الكثير من الدول تدرك أن التغيرات المتسارعة في التكنولوجيا تؤدي إلى تهديدات ليست بالسهلة لأمن الوطن والمواطن، ولذا لا بد من ضرورة العمل على ضمان أمن المعلومات من خلال خطوات مهمة للأمن السيبراني لحماية الأمن الوطني بمفهومه الشامل، فالأمن السيبراني يعتمد على مجموعة كبيرة من وسائل قانونية وتقنية لمقاومة الاستخدام الغير قانوني للشبكة العنكبوتية ومن أجل حماية نظم المعلومات ووسائل الاتصالات لحماية الوطن والمواطن والمؤسسات من أخطار الفضاء السيبراني .

الأهمية :-

يسعى البحث إلى التأكيد على مفهوم الأمن السيبراني باعتباره احد المواضيع الحديثة التي أخذت اهتماما واسعا من لدن الباحثين بالشأن الأمني والسياسي ، ويعد الأمن السيبراني حاجة ملحة للواقع العراقي بعد عام 2003 ، فالعراق يفتقد للمعلومات والمختصين في مجال الأمن السيبراني مقارنة بالدول الأخرى ، وهذا يعني أهمية العمل على إيجاد قاعدة موسعة من المعلومات لجميع المؤسسات الحكومية واعتمادها لمواجهة المخاطر السيبرانية التي تنتهك الاستقرار في العراق الجديد.

الهدف :-

يعد العراق من الدول التي حاربت مجموعات مسلحة ومتطرفة على أراضيها ، وقد استطاعت تلك المجموعات الإرهابية اختراق الأمن العراقي في فترة وجيزة ، مما تطلب من الحكومة العراقية العمل وبالسرعة القصوى لإبعاد الخطر الكبير لتلك المجموعات على امن واستقرار العراق ، وذلك يعني أن المؤسسات الأمنية العراقية كان يقع على عاتقها الثقل الأكبر في محاربة الإرهاب ، وإحدى الوسائل التي تم اعتمادها في تلك الحرب هي قوة المعلومة الأمنية ودقتها وطريقة استخدامها في القضاء على العدو ، وهنا يبرز هدف البحث في محاولة التعرف على دور الأمن السيبراني في إدارة ملف النظام الأمني في العراق خلال الحرب على الإرهاب وما بعده ، وتقديم حلول ممكنة لتعزيز مفهوم الأمن السيبراني ، وتعميق المفهوم العلمي في الميادين الأمنية والسياسية والعسكرية والاقتصادية والثقافية ، والاعتماد عليها لجمع المعلومات والمشاركة والتخطيط في صناعة القرارات الإستراتيجية .

الإشكالية :-

إن المشكلات الأمنية التي يصدرها العالم السيبراني إلى جميع أنحاء العالم قد أضحت وسيلة فعالة وآمنة لعدة جهات خارجية للتدخل في الشأن العراقي الأمني والسياسي والاقتصادي ، وهي إحدى الميادين التي يتخذها العدو للوصول إلى أهدافه من دون الحاجة إلى سلوك السبل التقليدية ، مما يشكل ثغرة أمنية لا يستهان بها . الفرضية :-

لقد بني البحث على افتراض مفاده:- (أن الدور الذي يؤديه الأمن السيبراني في تطوير السياسة الأمنية في العراق سوف يؤدي بالضرورة إلى تحسين الوضع العام في العراق واستقراره) ، وبالتالي فإننا كباحثين نجد أن في حال قيام الحكومة العراقية بتأسيس قاعدة قوية من أنظمة الأمن السيبراني في جميع مؤسسات الدولة ، فان ذلك يعني إنشاء جدار صد أولي ضد الإرهاب العالمي والقدرة على ربط تلك المعلومات مع الأنظمة الأمنية العالمية .

المنهجية :-

تم الاعتماد على منهجية تجمع بين منهج التحليل والمنهج الوصفي والذي نحاول من خلاله الوصول إلى قوانين وافتراضات يتم العمل بها لاحقا ضمن المؤسسة الأمنية العراقية ، ولأجل توضيح مفردات البحث فقد تم تقسيمه إلى ثلاثة محاور رئيسة :-

المبحث الأول :- تعريف الأمن السيبراني .. الأهمية والمرتكزات .

المبحث الثاني :- تحديات الأمن السيبراني في العراق .

المبحث الثالث:- الأمن السيبراني وفرص الاستقرار السياسي.

الخاتمة .

المبحث الأول :- تعريف الأمن السيبراني .. الأهمية والمرتكزات .

أدت نهاية الحرب الباردة إلى ظهور العديد من التحديات والتهديدات التي لم يشهدها المجتمع الدولي من قبل، والتي تُعرف بالتهديدات اللا تماثلية أو اللا تناظرية العابرة للحدود والتي لا تعترف لا بالحدود أو السيادة الوطنية أو فكرة الدولة القومية، الأمر الذي أدى إلى حدوث تحولات في حقل الدراسات الأمنية والإستراتيجية وكذلك على مستوى الممارسة السياسية ، وترافق ذلك مع التطور التكنولوجي في وسائل الاتصالات ، مما نتج عنه تداعيات عدة بسبب ظهور تهديدات وجرائم سيبرانية أصبحت تشكّل تحدياً كبيراً للأمن الوطني وكذلك العالمي ، ووفقا لتلك التهديدات فقد عد الفضاء السيبراني بمثابة المجال الخامس من الحروب بعد البر والبحر والجو والفضاء، وهو ما استدعى ضرورة وجود ضمانات أمنية ضمن هذه البيئة الرقمية ، وتبلورت بشكل أساس في ظهور الأمن السيبراني (cyber security) كبُعد جديد ضمن أجندة حقل الدراسات الأمنية ، وكمتغير جديد في العلاقات الدولية. [1]

إن الأمن السيبراني يتكون من شقين وجب علينا كباحثين إلقاء الضوء عليهما كمدخل للتعرف على أهمية الأمن السيبراني في العراق الجديد .

فالأمن هو نقيض الخوف أي بمعنى السلامة ، والأمن مصدر الفعل أَمِنَ أَمْناً وأَمَاناً وأَمَنَةً ، أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال: أَمِنَ من الشر، أي سَلِمَ منه ونقول: أمن منه أي سلم منه، وأمن على ماله عند فلان أي جعله في ضمانته ، والأمان والأمانة بمعنى واحد، فالأمن ضد الخوف، والأمانة ضد الخيانة، والمأمن الموضع الأمن . [2] واستنادا إلى تعريف سياسة الأمن ، يمكن القول أن الأمن : هو مجموع القواعد التي يضعها مسؤولوا الأمن في أي مكان والتي يجب أن يتقيد بها جميع الأشخاص الذين يمكنهم الوصول إليه ، وهو مفهوم واسع يطال جميع عمليات الدخول، والخروج ، والبقاء ، أو التصرف في مكان ما ، ويشمل الأمن في الفضاء السيبراني قواعد وأصول ضبط الاتصال، وانتقال المعلومات، وتخزينها وحفظها ، وأمن المواقع، والأنظمة الالكترونية وعمليات استثمارها، فضلا عن أمن الاتصالات . [3] وقد عرّفه قاموس بنغوين للعلاقات الدولية بأنه مصطلح يشير إلى غياب ما يُهدد القيم النادرة .[4] أما مصطلح السيبرانية فهو واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي، وتشير المقاربة الإيتيمولوجية* لكلمة cyber إلى أنها لفظة يونانية الأصل مشتقة من كلمة kybernetes بمعنى الشخص الذي يدير دفة السفينة ، إذ تستخدم مجازاً للمتحكم((governor ، وتجدر الإشارة إلى أن العديد من المؤرخين يرجعون أصلها إلى عالم الرياضيات الأمريكي norbert wieners **،

وذلك للتعبير عن التحكم الآلي، فهو الأب الروحي المؤسس للسبرنيتيقية من خلال مؤلفه الشهير : Cybernetics or control and communication in the Animal and the machine ، وأشار في كتابه إلى أن السبرنتيقية هي: التحكم والتواصل عند الحيوان والآلة والإنسان والآلة ليستبدل مصطلح الآلة بعد الحرب العالمية الثانية بالحاسوب .[5])واصطلاحياً هناك العديد من التعاريف التي قُدمت لمفهوم الأمن السيبراني، إذ يُعرّف بأنه : مجموعة من الإجراءات المتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة ، وهذا ما ذهب إليه الكاتبان Neittaanmäki Pekka,Lehto Martti في كتابهما :Cyber Security: Analytics, Technology and Automation ، إذ اعتبرا أن الأمن السيبراني أنه : عبارة عن مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة .[6]

ومصطلح الأمن السيبراني جاء من لفظ سايبر المعرب من كلمة (Cyber) اللاتينية، والذي ظهر حديثا في قواميس اللغة الإنكليزية، والتي تعني باللغة العربية إلكتروني، والتي تهتم بخصائص وثقافة أجهزة الحاسوب وتكنولوجيا المعلومات والواقع الافتراضي، أما مفهوم الأمن السيبراني والذي يُعرف أيضًا باسم أمن تكنولوجيا المعلومات أو أمن المعلومات الإلكتروني حسب تعريف شركة كاسبرسكي Kaspar sky)) هو ممارسة الدفاع عن أجهزة الكمبيوتر والخوادم والأجهزة المحمولة والأنظمة الإلكترونية والشبكات والبيانات من الهجمات الضارة ، فالأمن السيبراني يعد المضلة لكل من أمن الشبكات، وأمن المعلومات، وأمن التطبيقات، وأمن العمليات التي تتم في الحواسيب المرتبطة بالشبكة وقدرتها على استرجاع المعلومات في حال حدوث كوارث طبيعية أو إختراق ، إن تطور وسائل الاتصالات وتكنولوجيا المعلومات، والانتقال إلى الجيل الثالث من الثورة المعلوماتية والمعروفة باسم انترنت الأشياء (IOT)، وزيادة عدد الهجمات الالكترونية في الفضاء المعلوماتيّ واستخدامها للأسلحة الالكترونية مثل التجسس والفيروسات وتحليل البيانات المرسلة أو حجب الخدمة جعل هنالك ضرورة ملحة وحاجة متزايدة لسن قانون الأمن السيبراني . [7]

فالأمن السيبراني هو ممارسة حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية التي تهدف عادةً إلى الوصول إلى المعلومات الحساسة أو تغييرها أو إتلافها أو ابتزاز المال من المستخدمين أو مقاطعة العمليات التجارية ، وينتهج الأمن السيبراني الناجح نهجاً معيناً يتكون عادة من طبقات متعددة للحماية تنتشر في أجهزة الكمبيوتر أو الشبكات أو البرامج أو البيانات التي ينوي المرء الحفاظ على سلامتها وفي أي منظمة يجب على المستخدمين والعمليات والتكنولوجيا أن يكملوا بعضهم بعضاً ويتكاتفوا لإنشاء دفاع فعال من الهجمات السيبرانية .[8] وقدمت وزارة الدفاع

الأمريكية (البنتاغون) تعريفاً دقيقاً لمصطلح الأمن السيبراني، فعدته : جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية، من مختلف الجرائم كالهجمات، التخريب، التجسس والحوادث ، وفي حين اعتبر الإعلانُ الأوروبي الأمنَ السيبراني أنه يعني : قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات ، وهنا تجدر الإشارة إلى أن الأمن السيبراني مفهوم أوسع من أمن المعلومات، فالأمن السيبراني يهتم بأمن كل ما هو موجود على السايبر من غير أمن المعلومات، بينما أمن المعلومات لا يهتم بذلك، كما أن أمن المعلومات يهتم بأمن المعلومات الفيزيائية الورقية ، وإجرائياً : يمكن القول إن الأمن السيبراني هو مجموعة الآليات والإجراءات والوسائل والأطر التي تهدف إلى حماية البرمجيات وأجهزة الكمبيوتر في الفضاء السيبراني بصفة عامة من مختلف الهجمات والاختراقات والتهديدات السيبرانية التي قد تهدد الأمن القومي للدول.[9]

إذن برأينا كباحثين ، يعرف الأمن السيبراني: باتخاذ جميع التدابير والاحتياطات اللازمة، التي تضمن حماية النظام المستخدم، بحيث تتأمن سلامة المعلومات والبيانات، التي تنتقل بواسطته، وعبره، أو تحفظ عليه ، وإذا كان العالم التقني، متفقا على تحديد معنى أمن المعلومات، وأمن الشبكات، والأمن المادي، للأموال والأشخاص، فان الأنظمة القانونية والسياسية، تختلف حول مضمون ومعنى الحماية، ومدى الحفاظ على الحقوق والحريات، كما تختلف حول حق الدولة في التدخل، وحدود هذا التدخل وأصوله، في إطار الحفاظ على الأمن، سواء منه المعلوماتي، والقانوني، كما يبرز الاختلاف، على مستوى تحديد الجهات المعنية بالتنظيم والحماية، في الفضاء السيبيري ، ويتسم النظام العالمي بحركته السريعة التي تتلاحق فيها التحولات ، وتزداد فيها العوامل الداخلية والخارجية التي تؤثر على استقرار النظم الإدارية والأمنية للدول ، مما يفرض عليها بالتالي تحسين قدراتها لتحمل المسؤولية ومواجهة تلك التحولات والتحديات ، من اجل الارتقاء بفاعلية التنظيمات والأجهزة الأمنية المختلفة .

مرتكزات الأمن:

للأمن في مجتمع المعلومات وجهان: الأول تقني ، والآخر قانوني – تنظيمي ، والارتباط بين الاثنين، حتمي وضروري ، فإذا كان لا يمكن للقانون أن يعمل بعيدا عن التقنيات وخصائصها، وعن طبيعة النشاط التقني سواء لتقرير الحقوق، أو لوضع قواعد المسؤوليات، فان الاتكال على الهندسة المعلوماتية، والمقاييس والمعايير الدولية العلمية فقط، لا يمكنه أن يوفر الحل للمسائل القانونية ، ولعل ما يؤكد على تكامل دوري التكنولوجيا والقانون، في تحقيق الأمن، في الفضاء السيبيري، هو ما أشارت إليه قرارات الجمعية العمومية للأمم المتحدة، التي تحدثت عن هندسة

تكنولوجيا المعلومات والاتصالات، بما يضمن مساعدة، وردع، وكشف الاستعمالات الجرمية، وجمع الأدلة ، كما تحدثت في المقابل، عن ضرورة وضع القواعد التشريعية الملائمة، للحماية، والوقاية من الجريمة . [10]

أهمية الأمن السيبراني :

تبرز الأهمية الأسمى للأمن السيبراني بالقدرة على مقاومة التهديدات المتعمدة وغير المتعمدة والاستجابة والتعافي ، وبالتالي التحرر من الخطر أو الأضرار الناجمة عن تعطيل أو إتلاف تكنولوجيا المعلومات والاتصالات أو بسبب إساءة استخدام تكنولوجيا المعلومات والاتصالات ويتطلب حماية الشبكات وأجهزة الكمبيوتر، والبرامج والبيانات من الهجوم أو الضرر أو الوصول غير المصرح به، ونتيجة لأهمية الأمن السيبراني في واقع مجتمعات اليوم فقد جعلته العديد من الدول على رأس أولوياتها، خاصة بعد الحروب الإلكترونية التي بدأت تظهر تجلياتها بين بعض الدول الكبرى، في إشارة صريحة إلى نهاية الحروب التقليدية التي كانت تستخدم فيها الأسلحة الثقيلة، والإعلان عن بداية حروب جديدة هي الحروب الإلكترونية ، ويتميز الأمن السيبراني بمجموعة من الخصائص منها :- [11])

1. طابع متعدد التخصصات الاجتماعية والتقنية.
2. كونه شبكة خالية من الحجم والتي قدرات الفاعلين يمكن أن تكون مماثلة على نطاق واسع.
3. درجة عالية من التغيير والترابط وسرعة التفاعل.

لقد أصبحت للمعلوماتية حضور في تأسيس سمة هذا العصر المتغير وسط تسيُّد تقنية المعلومات والاتصالات، وتستهدف تحقيق متغيرات سريعة على صعيد بناء المستقبل، وتتأثر قيادات الدولة ومفاصلها المختلفة، وبضمنها المؤسسات الأمنية بهذه الآلية الجديدة ومتغيراتها اللاحقة، مما يتطلب الأمر في هذه الحالة التدقيق في ماهية هذه المعلومات ، ومدى دقتها وشموليتها وعلاقتها بالمواقف التي تستدعي اتخاذ القرار بشأنها .

المبحث الثاني :- تحديات الأمن السيبراني في العراق .

إن ثورة المعلومات، والتكنولوجيا في العالم ، تفرض علينا أن نتحرك بسرعة وفاعلية ، لنلحق بركب هذه الثورة، لأن من يفقد في هذا السباق العلمي والمعلوماتي مكانته ، لن يفقد فحسب صدارته ، ولكنه يفقد قبل ذلك إرادته . [12]

وتساعد المعلومات الأمنية المختلفة على تهيئة القيادة السياسية العليا في أي دولة لاتخاذ القرارات السليمة لإدارة نظامها السياسي ، وحماية مصالحها الوطنية والقومية ، وهذا يعني بالضرورة العمل على إيجاد مؤسسات تعتمد على المعلومات وتقنياتها المتطورة في رفد المؤسسة الحاكمة بالخطط والقرارات الأكثر حكمة .

إن وجود تقنية متقدمة لدى الدولة تتطلب فريقا متخصصا لاستغلالها ، إن تقنية الأمن السيبراني تشكل وبقدر كبير جدا مفاتيح الحل للنجاح والتصدي لجميع مشاكل الدولة ولان الأجهزة الأمنية تعتمد وبشكل كبير على المعلومات الواردة لها وعلى دقتها فان ذلك يقتضي تفعيل دور نظم المعلومات واستغلال التكنولوجيا بشكل كامل يتجاوب مع المتغيرات التي أفرزتها أشكال متنوعة من الأزمات والتي أصبحت تمثل تحديا لزعزعة الاستقرار في منطقة الشرق الأوسط .[13] ويحاجج الكثيرون من المحللين بأن الحروب في العقد الثالث من القرن الحادي والعشرين، لن تكون حروبا بالمفهوم الكلاسيكي، إذ تتقاتل الجيوش على الأرض وفي البحر أو الجو، وإن كانت هذه واردة وبقوة، إلا أن أحد أوجه الحروب المعاصرة الشديدة الوقع، هي الحروب الاقتصادية، ومن هنا تتأتى قضية الاختراقات السيبرانية من أجل الحصول على المعلومات الاقتصادية، سواء تلك التي تتعلق بالشركات أو الأفراد، وحتى المؤسسات الاقتصادية الكبرى في الدول ، وفي هذا الصدد يشير (مايكل سيكريست) ، التقني الرئيس في شركة (بوز ألن هاملتون) الأميركية الشهيرة إلى : أن العالم يشهد زيادة في أنواع المنصات التي قد تستخدم للاعتداء الإلكتروني ومنها السيارات، وطائرات الدرون، والأقمار الصناعية ، ومكونات الأجهزة الإلكترونية، وإننا أمام تشويش متزايد يعتمده لاعبون محنكون من خلال إعادة استخدام رموز البرامج الخبيثة .[14]

ويمكن القول إن منظومة الأمن الوطني (الاستراتيجي) للعراق، تواجه جملة من التحديات التي يمكن تصنيفها بالتحديات المرئية وغير المرئية ، وتتجلى أخطرها بتلك التي تتمظهر بالصورة غير المرئية ، فلا يمكن التماسها بصورة مباشرة إلا من خلال البحث والاستقراء التحليلي ، وتشكل هذه التحديات تهديداً استراتيجياً من شأنها أن تؤثر على الأمن الاستراتيجي (للفرد والدولة) ، بمعنى: أن هذه التحديات تشمل معظم القطاعات والمؤسسات الحكومية وغير الحكومية ، التي تتمحور حول البنية التحتية الارتكازية للدولة لتصل إلى الأمن الإدراكي للمواطن، وتتراوح هذه التحديات ما بين التهديدات السيبراني لمنظومة الرقمي للدولة ، وزيادة عدد السكان من دون أن يصيب هذه الزيادة تخطيطٌ استراتيجيٌ يواكب التطورات والتحديات المحدقة بمؤسسات الدولة الرسمية وغير الرسمية، فتشكل تحدياً كبيراً لمنظومة الأمن الاستراتيجي للعراق، وبالتالي باتت الضرورة الملحة تركز الجهود البحثية والاستشرافية في هذا المجال ، ولاسيما في ظل زيادة الملحوظة للتحديات المحدقة بمنظومة

الأمن الاستراتيجي للعراق . [15])

أن التهديدات الإلكترونية (السيبرانية) تنتشر عبر تحديات غير مرئية تؤثر على منظومة الأمن الوطني العراقي ومن المظاهر التي أشرتها الأجهزة الأمنية أن أكثر المؤسسات العراقية تتعاقد لتجهيز معلوماتها من أقمار صناعية ذات مورد خدمة واقع خارج الحدود العراقية الذي يؤدي إلى مرور تلك المعلومات في خوادم تلك الدول، ورجوعها إلى العراق ، إذ يشكل هذا الإجراء خرقاً لأمن المعلومات العراقي، ولتلافي مثل هذه الخروقات الكبيرة التي تتعرض لها حركة المعلومات في العراق يتوجب بناء منظومة متكاملة لأمن المعلومات؛ مع التركيز على ضمان توافر أنظمة المعلومات وتمتين الخصوصية، وحماية سرية المعلومات الشخصية، واتخاذ جميع الإجراءات الضرورية لحماية المواطنين من مخاطر الفضاء السيبراني .[16])

تمثل التحديات غير المنظمة للأمن الوطني عموماً مجمل العوامل التي تشكل تهديداً مباشراً على الثوابت القيمية والتحتية لأي مجتمع، فالأمن الوطني العراقي يوجه جملة من التحديات المرئية التي تشكل خطراً مباشراً على منظومة الأمن الاستراتيجي، وهذه التحديات يمكن التماس حيثياتها وتأثيراتها بنحو عيني مباشر، لكن التحديات التي تشكل تهديداً أكبر على المنظومة الإستراتيجية للأمن الوطني هي التي لا يمكن التماس تأثيراتها مباشرةً على وحدات الأمن الوطني ، لذا فإن التحديات غير المرئية للأمن الوطني العراقي تتجلّى بجملة من العوامل والمؤثرات التي تخصُّ قطاعات إستراتيجية مهمة في الدولة، كقطاع البنى التحتية، التي تمسُّ تأثيراتها حياة المواطنين، فضلاً عن تحديات أخرى محدقة بالمنظومة الرقمية للعراق والمتمثلة بالتهديدات السيبرانية الإلكترونية، فضلاً عن تحديات زيادة السكان وضعف التخطيط الاستراتيجي ، ويمكن التطرق إلى هذه التحديات بنحو أوسع كالآتي :- [17]

1- ضعف البنى التحتية .

يعرف مفهوم البنية التحتية لأي دولة بأنها كلّ المؤسسات والهياكل الفنية التي تدعم المجتمع، وتمسّ الأمن الوطني الاقتصادي، والعلمي، والصحي، والخدمي، مثل: المدارس، والمستشفيات، والطرق، والجسور، والسدود، والمحطات، والمطارات، والمصانع، والإنتاج الزراعي، والكهرباء، أما مفهوم البنية الفوقية، فيقصد بها كل التشريعات والأنظمة والقوانين والإطار الأكبر لها وغيرها من مؤسسات الدولة التي كانت تحكم عمل تلك البنى التحتية، ويمكننا أن نضيف إلى مفهوم البنية التحتية منظومة القيم التي أقامها المجتمع منذ آلاف السنين وآمن بها، فالبنى التحتية ضرورة لا غنى عنها لعملية النمو والتنمية الاقتصادية في العراق، إذ إن وجودها يُعَدُّ من أهم عناصر جذب الاستثمار وتنمية الاقتصاد الوطني وتطوره ، وبالتالي أن عملية التنمية الشاملة في العراق يجب أنه

ترافقها خدمات للبنى التحتية موازية لها، تهدف إلى تحسين الظروف المعيشية للأفراد من خلال تزويدهم بالخدمات المادية والاجتماعية، ولكن دخول البلد بحروب طويلة عقوبات اقتصادية دولية على العراق ، وكل ذلك أدّى إلى دمار تلك البنى التحتية وخرابها .

2- ضعف التخطيط التنموي .

يعدُّ التخطيط من المهام الرئيسة للقيادة الإستراتيجية، وعنصراً مهماً لثبات منظومة الأمن الوطني، إذ إن التخطيط يرتبط بالمستقبل واستخدام علم المستقبل والنظريات والأساليب العلمية الحديثة التي تساعد على ذلك، فهو عملية تقوم بها المؤسسات الإستراتيجية من أجل تحديد الأهداف المستقبلية، ومواجهة التحديات ، واتخاذ القرارات بشأن تخصيص مواردها لردع هذه التحديات وتحقيق الأهداف المنشودة، ونتيجة التداعيات والانعكاسات السلبية التي تمسُّ مسار عمل المؤسسات الدولة العراقية الإستراتيجية، ويعاني العراق اليوم من حالة ضعف في منظومة التخطيط الاستراتيجي، وهو ما انعكس سلباً على عمل معظم مؤسسات الدولة العراقية ونتاجها التي باتت تعاني من ضعف في التخطيط الاستراتيجي الذي يمثّل أحد السمات الرئيسة للعصر الحديث، وأساس عمل المؤسسات الحكومية لأجل تحقيق الأهداف الوطنية المنشودة ، لذلك فإنه يتطلب قدرات خاصة على التوقع والتنبؤ فيما يخص المستقبل . أن العراق في هذه المدة الحساسة يحتاج إلى رؤية تخطيطية يقع على عتقها حلّ المعضلات المالية والأمنية التي باتت تعصف بالمنظومة المؤسساتي للعراق، من خلال وضع برنامج حكومي ثابت الأركان مع أساليب تخطيطية واجب إتباعها لمواجهة التحديات المرحلة القادمة، بمعنى التفكير والتخطيط قبل الأداء بوضع حلول لمشكلات الدولة العراقية لتحسين أداء المنظومة الإستراتيجية الشاملة في ضوء الإمكانات المتاحة.

3- ضعف الأمن الالكتروني .

تتمثل التهديدات الإلكترونية (السيبرانية) بتحديات غير مرئية توثر على منظومة الأمن الوطني العراقي، ففي عصر التكنولوجيا أصبح لأمن المعلومات الدور الأكبر صدّ أي هجوم إلكتروني ومنعه، وقد تتعرض له أنظمة الدولة المختلفة، وأيضاً حماية الأنظمة التشغيلية من أي محاولات للولوج بنحو غير مسموح به لأهداف غير سليمة، ومن الملاحظ أن أكثر المؤسسات العراقية تتعاقد لتجهيز معلوماتها من أقمار صناعية ذات مورد خدمة واقع خارج الحدود العراقية الذي يؤدي إلى مرور تلك المعلومات في خوادم تلك الدول، ورجوعها إلى العراق إذ يشكل هذا الإجراء خرقاً لأمن المعلومات العراقي، ولتلافي مثل هذه الخروقات الكبيرة التي تتعرض لها حركة المعلومات في العراق يتوجب بناء منظومة متكاملة لأمن المعلومات، لذا يتوجب على الأمن الإلكتروني العراقي أن يشكّل مجموع الأطر القانونية والتنظيمية، والهياكل التنظيمية، فضلاً عن الوسائل التقنية

والتكنولوجية والتي تمثل الجهود المشتركة للقطاعين الخاص والعام، المحلية والدولية و تهدف إلى حماية الفضاء السيبراني الوطني، مع التركيز على ضمان توافر أنظمة المعلومات وتمتين الخصوصية، وحماية سرية المعلومات الشخصية، واتخاذ جميع الإجراءات الضرورية لحماية المواطنين من مخاطر الفضاء السيبراني .

نستنتج مما ذكر أعلاه ، بان التحديات التي تواجه مفهوم الأمن السيبراني في العراق تشكل سببا لعدم الاستقرار السياسي وكثرة الاضطرابات واختلاف التوجهات بين من يصنع القرار ومن ينفذه ، وهذا يعني أن العراق بحاجة إلى دراسة مستفيضة لأسباب تراجع الأمن بشكل عام ، والأمن السيبراني بشكل خاص ، علما أن المدة الزمنية التي قضاها العراق في ظل الحصار الاقتصادي في فترة التسعينيات من القرن الماضي قد شكلت عقبة كبيرة لتطور المستوى الأمني التقني ، وذلك لعدم وصول التقنيات الالكترونية الحديثة إلى يد المواطن العراقي ، وعدم القدرة على مواكبة ما يحدث من تغييرات متسارعة في عالم التقنيات الأمنية .

المبحث الثالث:- الأمن السيبراني وفرص الاستقرار السياسي .

ساعدت ثورة المعلومات على إفراز ثلاثة عناصر أساسية هي: المعلومة(Information) والطابع الإلكتروني((Digital والفضاء الإلكتروني (cyber space)، ولقد أضحى الفضاء الإلكتروني بفضل ثورة المعلومات والإنترنت أحد العناصر الأساسية التي تؤثر على النظام الدولي بما يحمله من أدوات تكنولوجية قادرة على القيام بعمليات حشد وتعبئة في العالم، بجانب تأثيره في القيم السياسية وأشكال القوة المختلفة سواء كانت القوة الصلبة أو الناعمة . [18]كما تحول العنصر الرئيس في بناء القوة من الملكية إلى المعرفة والمعلومات ، وهو ما نتج عنه زيادة الوعي بأهمية الابتكار والتقدم التكنولوجي كأساس للاستحواذ على القوة، وبالتالي أهمية تطوير مفاهيم إستراتيجية، والتقدم الاستخباراتي في المجال التقني والاقتصادي ونظم الاتصالات، ومن هنا فقد أثر الفضاء الإلكتروني في التحول من مفهوم القوة على أساس الكم إلى القوة على أساس النتيجة المترتبة عليها ، والتحول بمفهوم توازن القوى على أساس " الثقل المعادل إلى مفهوم الترابط . [19]

هناك قلق متزايد بشأن إساءة استخدام تقنية المعلومات والاتصالات على أيدي الإرهابيين، وخاصة الإنترنت والتقنيات الرقمية الجديدة، لارتكاب أعمال إرهابية أو التحريض عليها أو التجنيد لها أو تمويلها أو التخطيط لها، وقد شددت الدول الأعضاء على أهمية التعاون بين الجهات المتعددة ذات العلاقة في مواجهة هذا التهديد ، بما في ذلك بين الدول الأعضاء والمنظمات الدولية

والإقليمية ودون الإقليمية والقطاع الخاص والمجتمع المدني ، وفي القرار **2341** لعام 2017 أشار مجلس الأمن بالدول الأعضاء إلى ضرورة : إنشاء أو تعزيز الشراكات الوطنية والإقليمية والدولية مع الجهات صاحبة المصلحة من القطاعين العام والخاص، حسب الاقتضاء، لتبادل المعلومات والخبرات من أجل منع الهجمات الإرهابية على الهياكل الأساسية الحيوية والحماية منها والتخفيف من آثارها والتحقيق فيها ومواجهتها والتعافي من أضرارها، وذلك بوسائل منها التدريب المشترك واستخدام أو إنشاء شبكات ملائمة للاتصال والإنذار في حالات الطوارئ . [20]

لقد أصبح الفضاء السيبراني جزءاً من التفاعلات الدولية التي تبذل الأمم المتحدة والمجتمع الدولي الجهود لضبط مجالات المسئوليات فيه، لأن معدلات التهديدات وفرص الحروب السيبرانية تتوسع بشكل كبير ، وبزيادة عدد الأطراف في هذا المجال، صار الصراع ذا طبيعة سياسية، لكنه يتخذ شكلاً عسكرياً من حيث طبيعة الأضرار وتدمير الثروة المعلوماتية في البنية التحتية للدولة لأهداف سياسية ، فخط التقسيم الجديد للعالم لن يكون بين عالم الشمال والجنوب، والعالم المتقدم والمتخلف، بل على أسس جديدة أولها من يملكون القوة السيبرانية والقدرة على صناعتها وإدارتها، وعلى الجانب الآخر المحرومين منها وإن كان يُسمح لهم باستخدامها ، أن المعرفة والمعلوماتية أصبحت عنصراً رئيسياً من عناصر قوة الدولة، وعلى قمة هرمها القوة السيبرانية، وهو ما يؤثر على مصفوفة الأمن القومي لأي دولة . [21]

وفي العراق تعمل إستراتيجية الأمن السيبراني على تكوين إستراتيجية منسقة وتستجيب بشكل ديناميكي نحو التهديدات التي تواجه الأمن القومي ، وتهدف الإستراتيجية الوطنية للأمن السيبراني في العراق إلى إدارة التهديدات الأمنية في الفضاء الإلكتروني بما يتماشى مع أهدف الأمن القومي العام والمصلحة العامة ، إذ أن الرؤية الوطنية للأمن السيبراني تتجه نحو مجتمع آمن ومضمون ونابض بالحياة ومرن وموثوق به يوفر فرصا لمواطنيه ويحمي المصالح الوطنية ويعزز التفاعلات السلمية والمشاركة الاستباقية في الفضاء السيبراني من أجل الرخاء الوطني ، كذلك تهدف الرؤية إلى تعزيز القدرات الوطنية في مجال الأمن السيبراني في العراق على نحو متناسق ومستدام ومتكامل من أجل التصدي والتخفيف من المخاطر السيبرانية في الفضاء السيبراني والتقليل من حدته ، وحماية للبنى التحتية المعلوماتية الوطنية في مختلف الميادين للارتقاء بمستوى العراق السيبراني نحو بيئة سيبرانية آمنة ، كما أنها تسلط الضوء على الطرق التي سيتم به تقييم وتطوير وتنفيذ الإنذار المبكر والكشف والتفاعل وإدارة الأزمات لتوفير الاستعداد ألاستباقي للرد على التهديدات الموجهة إلى البنى التحتية المعلوماتية الحرجة في العراق والتعامل معها . [22]

إن التقرير الصادر عن الاتحاد الدولي للاتصالات التابع للأمم المتحدة قد منح العراق المركز 107 عالميا في الأمن السيبراني، والترتيب 13 عربيا، وقد تفوقت عليه في المستوى عدة دول عربية لا يمكن، تحت أي ظرف، مقارنة موازناتها المالية بالعراق، مثل السودان وفلسطين والأردن ، كما حصدت أربع دول من الوطن العربي، هي السعودية وعُمان وقطر ومصر، مراكز متقدمة في الربع الأول من المؤشر العالمي للأمن السيبراني جي سي اي (GCI) ومع أن مرتبة العراق تعد متقدمة عن السنة التي سبقتها، إذ كان يحتل المرتبة 158 عالميا و19 عربيا ، لكن ما سبب حصول العراق على هذه المرتبة خصوصا انه كان يخوض معركة مصيرية ضد تنظيم إرهابي استخدم الفضاء السيبراني في حربه الإعلامية والنفسية ضد العراق، وكان العراق يواجه تحديا كبيرا على هذا المستوى، إذ استخدم شبابه هذه المنصات الرقمية بطريقة محترفة وواجهوا التنظيم ببطولة وشجاعة ومهنية ووطنية قلّ نظيرها، ولذا كان من المفترض، بعد هذه التجارب الحقيقية، أن يمتلك العراق خبرة واسعة في هذا المجال من خلال سيطرته على كل الأدوات التي تطور خطط وبرامج الأمن السيبراني وتعزز بيئته لمواجهة العدو الإرهابي الذي أجاد العمل في هذا المجال[23] .

ومن الممكن القول بان الأمن السيبراني يعد فرصة حقيقية رغم مخاطره ، في إعادة النظر في البنى التحتية للمؤسسات الأمنية في العراق ، وخاصة بعد خروج العراق من العديد من الحروب والأزمات السياسية والتي استمرت أكثر من 35 عاما ، ورغم تواضع الإمكانيات الحكومية قياسا بالدول الأخرى ، إلا أن العمل على بناء إستراتجية أمنية رفيعة المستوى قد ينقل العراق إلى مرحلة متقدمة من الأمن السيبراني تمكنه من مواجهة التحديات المستقبلية والآخذة في التطور .

الخاتمة .

إن الدراسات البحثية المستمرة في المجال الأمني لأي دولة تهدف إلى أن يكون لدى هذه الدولة أو تلك حصنا أمينا تلجأ إليه في أوقات الأزمات ، وان يكون هذا الحصن أو الملجأ عبارة عن حزمة من المعلومات الدقيقة والواضحة والتي تشكل اللبنة الأولى التي يتم من خلالها بناء المنظومة الحكومية التي يتفرع عنها الميدان الأمني، والعسكري ، والسياسي ، والاقتصادي ، والثقافي . ولأن العراق والشرق الأوسط الموسع كان ولا يزال جزءا من منظومة أمنية اقل تطورا من مثيلاتها في بقية بلدان العالم المتقدمة ، فهي ستكون بالتأكيد الأكثر حاجة لإيجاد أسس جديدة في إدارة الدولة وتعزيز أمنها ، المتسم بالقلق والاضطراب نظرا لكثرة الأزمات والصراعات التي تتميز بها منطقة الشرق الأوسط . إن افتقار العراق ودول المنطقة إلى أسس واضحة في كيفية التعامل مع التقنيات

الحديثة ، وكيفية استثمار المعلومات والتقنيات المتطورة في محاربة الإرهاب العالمي ، يجعلها دول ضعيفة غير مستقرة وذلك لان آلية التواصل التقني والمعلوماتي لاستلام المعلومة الأمنية ضعيف جدا ولا يتلائم مع الحاجة الملحة لهذه الدول وشعوبها في البحث عن الأمن والاستقرار . ولذا تظهر تقنية المعلومات في واجهة المطالب الأولى والضرورية لبناء دول آمنة في منطقة لطالما كانت مفتقدة للأمن والأمان .

الهوامش:

1 . الموسوعة السياسية :- https://political-encyclopedia.org/dictionary

2 . ابن منظور محمد بن مكرم (711هـ) : لسان العرب، ط1، دار صادر، بيروت، لبنان ، 2000 ، ج1، ص163.

3 . Security handbook, RFC 2196, A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide .

4 . ينظر في : إيفانز غراهام و نوينهام جيفري : قاموس بنغوين للعلاقات الدولية ، ترجمة : مركز الخليج للأبحاث ، الإمارات العربية المتحدة ، مركز الخليج للأبحاث ، 2004 .

*5المقاربة الإيتيمولوجية : الإيتيمولوجيا تعني البحث في أصل المفهوم.

** Norbert Wiener (1894 1964)-: عالم رياضيات أمريكي ولد في أمريكا من أبوين يهوديين وكان والده أستاذا للغات في جامعة هارفرد في عمر لا يتجاوز 11 سنة بدء فينر دراساته الجامعية للرياضيات في سنة 1909 انتقل إلى هارفرد حيث درس علم الأنواع zoology لكنه انتقل ثانية لكورنل ليدرس الفلسفة وعاد في نهاية المطاف لجامعة هارفارد حتى يكمل دراسته ببحث حول المنطق الرياضي ثم تحول ليدرس في إنجلترا وألمانيا اشتغل فينر كمحاضر في جامعة هارفارد وفي شركة جنرال إلكتريك في الحرب العالمية اشتغل لحساب الجيش وطور الآليات المضادة للطيران أو ما يسمى الدفاع الجوي.

.باره سمير: الأمن السيبراني cyber security في الجزائر السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني ، 2017

. 6جبور منى الأشقر: السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية ، بيروت ، لبنان ، ب ص ، 2016. وللمزيد ينظر في :- Lehto Martti , Neittaanmäk Pekka .Cyber Security: Analytics, Technology and Automation. Switzerland : Springer International Publishing, 2015.

7. محمد سالم العتوم : الأمن السيبراني في سطور ، مقالة منشورة ، صحيفة الرأي ، 2019/8/8 .

8. علي شهاب : ماذا يعني الأمن السيبراني ، مقال منشور ، صحيفة مكة ، 2017/11/1 ، المكتبة الالكترونية :- https://makkahnewspaper.com/article/617135

9 . ينظر في : أحمد عبيس نعمة الفتلاوي : الهجمات السيبرانية .... مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية ، المجلد 8 ، العدد 4 ، كلية القانون ، جامعة بابل ، العراق ، 2016 .

10 . The UN adopted General Assembly Resolutions 55/63 and 56/121 on Combating the Criminal Misuse of Information Technologies– December 2000 and January 2002 .

11. مرزوق عنترة و حرشاوي بن محيي الدين : الأمن السيبراني كبُعد جديد في السياسة الدفاعية الجزائرية ، ورقة بحث قدمت في الملتقى الدولي حول: سياسات الدفاع الوطني بين الالتزامات السيادية والتحديات الإقليمية، ورقلة، الجزائر، 31 /1/ 2017.

12 . إبراهيم عبد الله الهجري : التعليم في الوطن العربي أمام التحديات التكنولوجية، كلية العلوم (قسم الفيزياء)،جامعة صنعاء، الجمهورية اليمنية ، ص1 .

13 . محمود محمد غنام: دور تكنولوجيا المعلومات في إدارة الأزمات لدى العاملين في غرف عمليات الأجهزة الأمنية التابعة لوزارة الداخلية الفلسطينية ، جامعة الخليل ، فلسطين ، 2011، ص2 .

14. إميل أمين: الأمن السيبراني العالمي... حروب خلفية ومساحات إرهابية ، مقال منشور ، 12 /2/ 2020 ، المكتبة الالكترونية :- https://www.independentarabia.com/node/93586

15. علي زياد العلي : التحديات غير المرئية للأمن الوطني العراقي ، **26/6/2018** ، المكتبة الالكترونية :-
https://www.bayancenter.org/2018/06/4565/

16 . حامد شهاب : مخاطر المواقع الالكترونية على الأمن الوطني، مقال منشور ، صحيفة ميدل ايست أون لاين،2020/10/20 ، المكتبة الالكترونية https://middle-east-online.com/ :-

17 . علي زياد العلي : المصدر السابق .

. 18إيهاب خليفة : استخدام القوة في إدارة التفاعلات الدولية: الولايات المتحدة الأمريكية أنموذجا خلال الفترة من 2001 إلى 2012 ، رسالة ماجستير ،جامعة القاهرة: كلية الاقتصاد والعلوم السياسية، مصر ، 2015 ، ص ص 46-48 .

. 19صباح عبد الصبور عبد الحي : استخدام القوة الإلكترونية في التفاعلات الدولية ، جزء 2، بحث منشور ، 2016/11/5 ، المعهد المصري للدراسات ، المكتبة الالكترونية :- https://eipss-eg.org

20 . أمن الفضاء الإلكتروني : مكتب مكافحة الإرهاب ، الأمم المتحدة ، المكتبة الالكترونية :- https://www.un.org/counterterrorism/ar/cybersecurity

21 . ينظر في : عبد الغفار عفيفي الدويك : إعادة تقسيم العالم على أسس سيبرانية .... قراءة في تقرير التوازن العسكري لعام 2018 ، مركز الأهرام للدراسات السياسية والإستراتيجية ، مصر ، 2019/1/6 .

22 . إستراتيجية الأمن السيبراني العراقي : مستشارية الأمن الوطني ، أمانة سر اللجنة الفنية العليا ، أمن الاتصالات والمعلومات ، ص8 .

. 23مهند حبيب السماوي : الأمن الرقمي العراقي ... خريطته تحدياته ومستقبله ، مقال منشور ، قناة ناس ، 2020/4/21 .

المصادر :-

1. إبراهيم عبد الله الهجري : التعليم في الوطن العربي أمام التحديات التكنولوجية، كلية العلوم (قسم الفيزياء)،جامعة صنعاء، الجمهورية اليمنية ، ص1 .
2. ابن منظور محمد بن مكرم (711ه) : لسان العرب، ط1، دار صادر، بيروت، لبنان ، 2000 ، ج1، ص163.
3. أحمد عبيس نعمة الفتلاوي : الهجمات السيبرانية .... مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية ، المجلد 8 ، العدد 4 ، كلية القانون ، جامعة بابل ، العراق ، 2016 .
4. إستراتيجية الأمن السيبراني العراقي : مستشارية الأمن الوطني ، أمانة سر اللجنة الفنية العليا ، أمن الاتصالات والمعلومات ، ص8 .
5. الموسوعة السياسية :- https://political-encyclopedia.org/dictionary
6. أمن الفضاء الإلكتروني : مكتب مكافحة الإرهاب ، الأمم المتحدة ، المكتبة الالكترونية :- https://www.un.org/counterterrorism/ar/cybersecurity
7. إميل أمين: الأمن السيبراني العالمي... حروب خلفية ومساحات إرهابية ، مقال منشور ، 12 /2/ 2020 ، المكتبة الالكترونية :- https://www.independentarabia.com/node/93586
8. إيفانز غراهام و نوينهام جيفري : قاموس بنغوين للعلاقات الدولية ، ترجمة : مركز الخليج للأبحاث ، الإمارات العربية المتحدة ، مركز الخليج للأبحاث ، 2004 .
9. إيهاب خليفة : استخدام القوة في إدارة التفاعلات الدولية: الولايات المتحدة الأمريكية أنموذجا خلال الفترة من 2001 إلى 2012 ، رسالة ماجستير ،جامعة القاهرة: كلية الاقتصاد والعلوم السياسية، مصر ، 2015 ، ص ص 46-48 .
10. باره سمير: الأمن السيبراني cyber security في الجزائر السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني ، 2017.
11. جبور منى الأشقر: السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية ، بيروت ، لبنان ، ب ص ، 2016.
12. حامد شهاب : مخاطر المواقع الالكترونية على الأمن الوطني، مقال منشور ، صحيفة ميدل ايست أون لاين،2020/10/20 ، المكتبة الالكترونية :- https://middle-east-online.com/

13. صباح عبد الصبور عبد الحي : استخدام القوة الإلكترونية في التفاعلات الدولية ، جزء 2، بحث منشور ، 2016/11/5 ، المعهد المصري للدراسات ، المكتبة الالكترونية :- https://eipss-eg.org

14. عبد الغفار عفيفي الدويك : إعادة تقسيم العالم على أسس سيبرانية .... قراءة في تقرير التوازن العسكري لعام 2018 ، مركز الأهرام للدراسات السياسية والإستراتيجية ، مصر ، 2019/1/6 .

15. علي زياد العلي : التحديات غير المرئية للأمن الوطني العراقي ، **26/6/2018** ، المكتبة الالكترونية https://www.bayancenter.org/2018/06/4565 -:

16. علي شهاب : ماذا يعني الأمن السيبراني ، مقال منشور ، صحيفة مكة ، 2017/11/1 ، المكتبة الالكترونية :- https://makkahnewspaper.com/article/617135

17. محمد سالم العتوم : الأمن السيبراني في سطور ، مقالة منشورة ، صحيفة الرأي ، 2019/8/8 .

18. محمود محمد غنام: دور تكنولوجيا المعلومات في إدارة الأزمات لدى العاملين في غرف عمليات الأجهزة الأمنية التابعة لوزارة الداخلية الفلسطينية ، جامعة الخليل ، فلسطين ، 2011، ص2 .

19. مرزوق عنترة و حرشاوي بن محيي الدين : الأمن السيبراني كبُعد جديد في السياسة الدفاعية الجزائرية ، ورقة بحث قدمت في الملتقى الدولي حول: سياسات الدفاع الوطني بين الالتزامات السيادية والتحديات الإقليمية، ورقلة، الجزائر، 31 /1/ 2017.

20. مهند حبيب السماوي : الأمن الرقمي العراقي ... خريطته تحدياته ومستقبله ، مقال منشور ، قناة ناس ، 2020/4/21 .

21. Security handbook, RFC 2196, A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide .

22. Lehto Martti , Neittaanmäk Pekka .Cyber Security: Analytics, Technology and Automation. Switzerland : Springer International Publishing, 2015.

23. The UN adopted General Assembly Resolutions 55/63 and 56/121 on Combating the Criminal Misuse of Information Technologies- December 2000 and January 2002 .