استراتيجية الامن السيبراني العراقي لعام ٢٠١٧

أ. م. د. بدرية صالح عبد الله

جامعة بغداد / مركز الدراسات الإستراتيجية والدولية

badrea.salh@gmail.com

المقدمة

يعد الأمن ركيزة أساسية للدول وأساس أي تقدم على المستوى الداخلي والخارجي وهي تمثل قدرة الدولة على حماية أراضيها ومواردها ومصالحها من التهديد الداخلي والخارجي فضلاً عن ذلك هو تعبير عن مجموعة سياسات تتخذ لضمان سلامة الدولة والدفاع عن مكتسباتها في مواجهة الأعداء في الداخل والخارج وفي العقود الأخيرة اتسع مفهوم الأمن ليشمل مجموعة من الاجراءات الاقتصادية والثقافية والاجتماعية وفيما يتعلق الامر بالأمن السيبراني الذي هو ركيزة من ركائز التنمية المستدامة وهو بذلك يشكل قيمة مضافة الى الأمن الوطني لكل دولة .

اما مفهوم الامن السيبراني (امن المعلومات) هو حزمة من عمليات و اجراءات تتوخى تامين وحماية الشبكات وأجهزة الكمبيوتر والبرامج والبيانات من الهجوم والتلف او السرقة والتعطيل والعرقلة كمتغير جديد على الدولة الوطنية وأمنها.

كما و ينظر الى الأمن السيبراني بأنه مجموعة من الوسائل التقنية والتنظيمات الإدارية والتشريعات القانونية التي يجري توظيفها لمنع الأستخدام غير المصرح به للإنترنت فهو مصدر حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية وتهدف للوصول إلى المعلومات الحساسة، ويتجه الأمن السيبراني في العموم نحو ثلاث مجالات لحمايتها تتمحور في جهاز الحاسوب والهواتف واللوائح الذكية وأجهزة بث الإنترنت لحمايتها وهناك خمس تهديدات سيبرانية رئيسية (الدول الأجنبية ، النقابات الجنائية المنظمة ، الإرهابيين ، الجماعات المتطرفة ، الهاكرز ، الشركات) . ومن أجل تقديم الأطر والآليات الاستراتيجية لمعالجة التهديدات السيبرانية وتأمين العراق لمجابهة الهجمات السيبرانية ، أطلق العراق وثيقة مهمة في عام ٢٠١٧ سميت (إستراتيجية الأمن السيبراني العراقي) وهي بمثابة إستراتيجية الإستعداد الوطني لتوفير تدابير متماسكة وإجراءات إستراتيجية لضمان أمن وحماية الوجود العراقي في الفضاء السيبراني وحماية البنية التحتية الحيوية للمعلومات وبناء ورعاية مجتمع إنترنت موثوقا به ، وتتألف الأستراتيجية الوطنية من عدة استراتيجيات قصيرة و متوسطة وطويلة الأمد تغطي جميع أنحاء العالم التي

تضر بالمصلحة الوطنية مثل (الجريمة الإلكترونية ، الأرهاب الإلكتروني ، الصراع السيبراني ، التجسس السيبراني ، إساءة معاملة الأطفال واستغلالهم عبر الإنترنت) .

هدف البحث : يهدف البحث الى الاطلاع على استراتيجية الامن السيبراني في العراق بعد العام ٢٠١٧ وتوفير خارطة الطريق متماسكة وآليات التنفيذ والاستعداد للتهديدات الامنية والمساعدة في معالجة ضعف البلاد في المجال الرقمي ، فضلا عن تعزيز قدرات العراق لمكافحة الهجمات السيبرانية .

أهمية البحث : تكمن أهمية البحث في دراسة الأمن السيبراني الذي ظهر مع قيام الثورة المعلوماتية وتطورها وهو يستهدف أنظمة المعلومات وعلاقتها بالامن الوطني العراقي التي تتطلب الحل على المستوى الوطني وضرورة التنسيق والتعاون الدولي .

إشكالية البحث : تتضمن إشكالية البحث اثر ومخاطر الفضاء السيبراني وتهديد الارهاب السيبراني على الامن الوطني خاصة مع ظهور تنظيم داعش الارهابي إضافة الى ذلك يحاول البحث الاجابة على التساؤلات الآتية :

١. ما هي الامن الوطني والمقصود بالفضاء السيبراني والإرهاب السيبراني .

٢. ما هي طبيعة الهجمات السيبرانية وما هي خطورتها .

٣. ما هي جهود الوطنية والدولية لمكافحة الارهاب السيبراني.

فرضيه البحث : الرؤيا الوطنية العراقية للامن السيبراني هي بناء مجتمع آمن ومضمون وموثوق فيه يوفر فرص للمواطنين ويحمي الاصول والمصالح الوطنية ويعزز التفاعلات والمشاركة الاستباقية في الفضاء السيبراني من اجل الرخاء الوطني .

منهجية البحث : لمتابعة الاحداث التاريخية لدخول تنظيم داعش الارهابي ثم الاعتماد على المنهج التاريخي و لدراسة ظاهرة الامن السيبراني وتأثيرها على الامن الوطني العراقي تم الاعتماد على المنهج الوصفي التحليلي.

هيكلية البحث : تم تقسيم البحث الى ثلاث : المحور الاول : اهمية الامن السيبراني ، المحور الثاني : الابعاد السياسية للامن السيبراني ، المحور الثالث : العراق في مواجهة تحديات الامن السيبراني، مع المقدمة والخاتمة .

المحور الاول : اهمية الامن السيبراني

يعد الامن ركيزة أساسية للدول وأساس اي تقدم على المستوى الداخلي والخارجي للدولة لانه يعد قدرة الدولة على حماية أراضيها ومواردها ومصالحها من التهديد الخارجي والداخلي فضلا عن ذلك هو تعبير عن مجموعة سياسات تتخذ لضمان سلامة الدولة والدفاع عن مكتسباتها في مواجهة الاعداء من الداخل والخارج وفي العقود الأخيرة اتسع مفهوم الامن ليشمل مجموعة من الاجراءات الاقتصادية والثقافية والاجتماعية .

اما مفهوم السيبرانية هي كلمة تطلق (سيبر cyber) على اي شيء مرتبط بثقافة الحواسيب او تقنية الواقع الافتراضي فالسبرانية تعني (فضاء الانترنت) ويعد الفضاء الالكتروني هو السمة التي تتميز بها الحياة العصرية والمكون الاساس للبنية التحتية لمؤسسات الدولة المختلفة او القطاعين العام والخاص ، واصبح وسيلة للتعبير عن الحرية والتجمع والخصوصية الفردية والتدفق الحر للمعلومات والاتصالات الالكترونية ومعالجة البيانات ذات الطابع الشخصي والجرائم والمعاملات والتواقيع والاثبات والتجارة الإلكترونية وحماية المستهلك وحقوق الملكية الفردية في المجال المعلوماتي السيبراني وفيما يتعلق الامر بالأمن السيبراني هو ركيزة من ركائز التنمية المستدامة وهو بذلك يشكل قيمة مضافة الى الامن الوطني لكل دولة ، ومع بروز ثورة المعلومات (الامن السيبراني ، وامن المعلومات) والذي يمكن تعريفه (حزمة من عمليات واجراءات تتوخى تامين وحماية الشبكات وأجهزة الكمبيوتر والبرامج والبيانات من الهجوم او التلف او السرقة او التعطيل و العرقلة) كمتغير جديد على الدولة الوطنية وامنها اصبحت العديد من الدول تتصارع في سبيل الحصول على مستويات اعلى من تعزيز القدرات في مجال الدفاع والهجوم وذلك من خلال تبني استراتيجيات وطنية للامن السيبراني ولم يرتبط ذلك بالعمل على تحقيق الاهداف الامنية والسياسية فقط بل العمل على حفظ فرص النمو الاقتصادي في ظل ترابط العلاقات بين الامن الاقتصادي في العصر الرقمي وانعكس ذلك على الثقة في الاجراءات السياسية المتبعة ، اما مفهوم الأمن الوطني هو قدرة الدولة على رد اي عدو وان قد تتعرض له من قبل دولة اخرى سواء باستعمال الدفاع العسكري او اي اسلوب اخر يساهم في المحافظة على توفير الامن الخارجي والداخلي للدولة دون وجود سيطرة او سلطة من دولة او اي جهة اخرى بمعنى اخر يشير الامن الوطني الى قدرة الدولة على حماية اراضيها وشعبها ومصالحها وعقائدها وثقافتها واقتصادها من اي عدوان خارجي فضلا عن قدرتها للتصدي لكل

المشاكل الداخلية وتعمل على حلها واتباع سياسة متوازنة تمنع الاستقطاب وتزيد من وحدة الكلمة والتجذير الولاء والانتماء للوطن والقيادة (الاميري و العموش ٢٠٢٠ ، ٥٣٢) ، ويذكر الباحث السياسي(باري لوزان) مفهوم الأمن هو العمل على التحرر من التهديد وفي سياق النظام الدولي فهو قدرة الدول والمجتمعات على الحفاظ على كيانها المستقل وتماسكها الوظيفي ضد قوى التغيير التي تعدها معادية في سعيها للأمن (عنتر٢٠٠٥ ، ٥٩) ، اما الأمن السيبراني هو مجموعة من الإجراءات التقنية والإدارية تشمل العمليات والآليات التي يتم اتخاذها لمنع أي تدخل غير مقصود أو غير مصرح به بالتجسس أو الاختراق للاستخدام أو سوء الاستغلال للمعلومات والبيانات الإلكترونية الموجودة على نظم الاتصالات والمعلومات كما تضمن تأمين وحماية و سرية وخصوصية البيانات الشخصية للمواطنين كما تشمل استمرارية عمل حماية معدات الحاسب الآلي ونظم المعلومات والاتصالات والخدمات من أي تغير أو تلف ، وتأتي أهمية الأمن السيبراني في انه يقوم بتأمين المعلومات الحساسة البالغة الأهمية للدول والأفراد على حد سواء و المعرضة للخطر والاختراق والاستيلاء كي تحافظ على الأمن الوطني وحفظ وحماية السرية والخصوصية للبيانات الشخصية للمواطنين ، وقد وصف الاتحاد الدولي للاتصالات الفضاء السيبراني بالمجال المادي والغير المادي والذي يتكون وينتج عن عناصر هي(أجهزة الكمبيوتر، الشبكات، البرمجيات،حوسبة المعلومات، المحتوى معطيات النقل والتحكم) إذا الفضاء بيئة تفاعلية حديثة تشمل عناصر مادية وغير مادية كما عرف الفضاء السيبراني بأنه(المدى المفتوح المشترك لجميع الأفراد في المجتمعات الذين لهم القدرة على الدخول لشبكة الإنترنت والتي تتيح لهم الحصول على المعلومات وإجراء مناقشات مع الآخرين وحرية التعبير عن الرأي دون التقيد بإلقاء المباشر أو الزمان أو المكان ، ويتشكل الفضاء السيبراني من ثلاث طبقات هي: (عبد الصبور ٢٠١٧، ٦) .

١ – الطبقة المادية وهي أجهزة الحاسوب.

٢ – الطبقة المنطقية وهي مجموعة البرمجيات.

٣ – الطبقة الدلالية والإعلامية والبعد الاجتماعي للمستخدمين.

كما يضم الفضاء السيبراني من الفواعل الدولاتية والفواعل الغير دولاتية وتضم الأفراد والمنظمات الغير الحكومية (رزوقة ٢٠١٩، ١٩) ، أو المجموعات الافتراضية ، أسهم الفضاء الإلكتروني في وجود أشكال حديثة من العدوان غير التقليدي على مواطنين الدولة ومؤسساتتها

أصاب الدولة بالعجز عن توفير الأمن على المستوى الداخلي المتمثل بحفظ وسلامة الأفراد وممتلكاتهم وأموالهم ومهمة الدفاع وقدرتها على تحديد مصدر الهجمات أو الأخطاء وعدم القدرة على اتخاذ رد فعل سريع بسبب عجز الأطر القانونية التي تتبناها المتمثلة في الإجراءات القانونية يتضمنها القانون الدولي والقانون الجنائي ويوظف الفضاء الإلكتروني أيضا في حروب الجيل الرابع ويهدف إلى زعزعة استقرار الشعوب وإنهاك إرادة الدول المستهدفة بنشر الفوضى فيها و ذلك من خلال عدة طرق منها العمل على ضرب أجهزة القوى لدى الدولة وأجهزتها الشرطة والجيش وضرب المؤسسات الداخلية فلا يتم الفصل في هذه الطريقة بين السلطة والنظام السياسي وبين الدولة ، والعمل على تأجيج الصراع واستخدام العنف ضد المجتمع بمختلف فئاته وطبقاته وطوائفه وتأجيج مشاعر التمرد والعصيان ورفض الواقع وتتم مواجهة حروب المعلومات من خلال استراتيجية تتضمن شقين الأول دفاعي يحمي أنظمة الدولة والآخر هجومي يوجه ضد أنظمة الدولة المعادية ويعتمد على العمليات النفسية والاستخبارات ومهاجمة الوسائط والهاكرز وأعمال التجسس وزرع العملاء وهو ما ينتهي إلى خلق مناخ عدائي بين الأطراف المتصارعة يؤثر في المؤسسات الداخلية وتماسك النسيج الوطني للشعوب (صادق٢٠١٧ ، ٢٦-٢٨) ، كما يحدد جوزيف ناي ثلاث أنواع من الفاعلين الذين يمتلكون القوة السيبرانية هي :

١- الدول والتي لديها القدرة الكبيرة على تنفيذ هجمات سيبرانية وتطوير البنية التحتية وممارسة السلطات داخل حدودها.

٢- الفاعلون من غير الدول يستخدم هؤلاء الفاعلون القوة السيبرانية لأغراض هجومية بالأساس إلا أن قدرتهم على تنفيذ أي هجوم سيبراني مؤثر يتطلب مشاركة ومساعدة أجهزة استخباراتية متطورة ولكن يمنعهم اختراق المواقع الإلكترونية و استهداف الأنظمة الدفاعية.

٣- الأفراد الذين يمتلكون معرفة تكنولوجية عالية القدرة على توظيفها وعادة ما تكون هناك صعوبة بالكشف على هوياتهم ومن الصعب ملاحقتهم .

اما الفاعلين من غير الدول وهي: (جيجان٢٠٠١ ، ٣٨) و (عثمان ٢٠١٧، ١٩)

١ -الشركات المتعددة الجنسيات

٢ . المنظمات الإجرامية التي تقوم بها لعمليات القرصنة السيبرانية

٣-الجماعات الإرهابية

٤-الأفراد.

المحور ألثاني : أبعاد الأمن السيبراني

للأمن السيبراني اهداف تسعى إلى تحقيقها منها تعزيز حماية انظمة التقنيات التشغيلية على كافة الأصعدة و مكوناتها من أجهزة وبرمجيات، التصدي لهجمات أمن المعلومات التي تستهدف الأجهزة الحكومية ، توفير بيئة أمنة وموثوقة للتعاملات في مجتمع المعلومات، صمود البنى التحتية الحساسة للهجمات الإلكترونية، التخلص من نقاط الضعف في أنظمة الحاسب الآلي والأجهزة المحمولة باختلاف أنواعها، سد الثغرات في أنظمة أمن المعلومات ، مقاومة البرمجيات الخبيثة وما تستهدفه من أحداث أضرار بالغة للمستخدمين، الحد من التجسس والتخريب الإلكتروني على مستوى الحكومة والأفراد.

وللأمن السيبراني أبعاد عديدة منها: (اللجنة الاقتصادية لغربي آسيا الاسكوا ٢٠١٥،٧٢)

البعد العسكري : تنشأ أهمية الأمن السيبراني في هذا البعد من خطورة الهجمات السيبرانية والاختراقات التي تؤدي إلى نشات الحروب والصراع المسلح واختراقات أنظمة المنشآت النووية وما قد يحدث عنها من تهديدات لامن الدول والحكومات ويؤدي إلى كوارث.

البعد السياسي : يقوم البعد السياسي للأمن السيبراني على أساس حماية نظام الدولة السياسية وكيانها حيث يمكن ان تستخدم التقنيات في بث المعلومات والبيانات قد يحدث من خلالها زعزعة الاستقرار أمن الدول والحكومات حيث تصل بسرعة فائقة إلى أكبر شرائح من المواطنين بغض النظر عن صحة معلومات وبيانات التي يتم نشرها.

البعد الاقتصادي : يرتبط بالأمن السيبراني ارتباط وثيقاً بالحفاظ على المصالح الاقتصادية لكل الدول والترابط الوثيق بين الاقتصاد والمعرفة فأغلب الدول تعتمد في تعزيز اقتصادها وازدهارها على إنتاج وتداول المعرفة والمعلومات على المستويات وما يبرر الدور الخطير للأمن السيبراني في حماية الاقتصاد من السرقة والملكية الفردية.

البعد القانوني : ترتبط بالأنشطة المختلفة التي تقوم بها الأفراد والمؤسسات والقوانين ومن ظهور المجتمع لمعلومات ظهرت القوانين الجديدة التي تعد البيئة التنظيمية التشريعية المنظمة لحماية هذا المجتمع.

البعد الاجتماعي : إن أهمية الأمن السيبراني لحماية وصيانة القيم الجوهرية في المجتمع كالانتماء والمعتقدات الدينية والتقاليد بضرورة تعاون أفراد المجتمع التحفظية للحد من المخاطر والهجمات والجرائم السيبرانية التي مما لا شك فيه تشمل المجتمع ككل وتهدد أمنه واستقراره على

هدم القيم والضياع الهوية الثقافية. وللأمن مستويات منها الأمن القومي ويعرف بأنه مفهوم شامل يتعلق بالدولة كافة بالابعاد السياسية والاقتصادية والاجتماعية ويذهب إلى أن مجموعة التهديدات الموجهة ضد الدولة لاتنشئ من مصادر خارجية فحسب وإنما من مصادر داخلية عابرة لحدود الدولة ويقع مجموعة بدائل غير العسكرية ذات التأثير الشامل مثل(الشرعية، السياسية، التعايش الديني و القومي ، القدرات الاقتصادية، توفير الموارد الأولية).

الإرهاب السيبراني: هو الهجوم ذي الدوافع السياسية والتهديد بالهجوم على أجهزة الكمبيوتر والشبكات أو أنظمة المعلومات من أجل تدمير البنية التحتية وترهيب الحكومة أو المواطنين وإجبارهم على تحقيق أهداف سياسية واجتماعية بعيدة المدى بمعنى أوسع بأن الإرهاب السيبراني يعني استخدام الإنترنت للتواصل والدعاية والتضليل من قبل المنظمات الإرهابية، والإرهاب السيبراني هو جزء من جهد منظم الإرهابيين سيبرانيين أو وكالات ومخابرات أجنبية أو أي جماعات تسعى لاستغلال ثغرات أمنية محتملة في الأنظمة المعلوماتية الحيوية و الإرهاب السيبراني هو الشخص الذي يدفع حكومة أو منظمة أو جهة لتلبية أهداف سياسية من خلال إطلاق هجوم إلكتروني على أنظمة الحواسيب ونظام تشغيلها مما يؤدي إلى انهيار النظام. (الرشيدي ٢٠١٦، ١١٠)

الصراع السيبراني: انه مصطلح أكثر ملائمة لأنه يؤكد على وجود تكنولوجيا إلكترونية في كل مجال من مجالات النشاط بما في ذلك النزاع ويعد الصراع الإلكتروني أحد أوجه الصراع الدولي اذ يستطيع أحد أطراف الصراع أن يوقع خسائر فادحة للطرف الآخر وأن يتسبب في فشل البنية التحتية المعلوماتية والاتصالاتية الخاصة به وهو ما يسبب خسائر عسكرية واقتصادية فادحة من خلال قطع أنظمة الاتصال بين الوحدات العسكرية بعضها بعض أو تضليل معلوماتها أو سرقة معلومات سرية عنها. (سلمان ٢٠٢٢، ٢٣٩)

الجريمة السيبرانية : وهي نشاط غير مشروع موجه إلى نسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزونة داخل الحاسوب او التي تنقل عن طريقه كما تعرف بأنها سلوك غير مشروع بما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات.

ومن أنواع الجرائم السيبرانية :

١- جرائم التعدي على البيانات المعلوماتية وتشمل جرائم الولوج التي يكون موضوعها البيانات المعلوماتية هي كل ما يمكن تخزينه معالجته ونقله بواسطة الحاسب الآلي كالأرقام والحروف والرموز وما إليها.

٢- جرائم التعدي على الأنظمة المعلوماتية وتشمل جرائم الولوج غير المشروع إلى النظام المعلوماتي في مجموعة برامج وأدوات متعددة لمعالجة وإدارة البيانات والمعلومات.

٣- إساءة استعمال الأجهزة والبرامج المعلوماتية وتتضمن هذه الجرائم لكل من قدم أو انتج او وزرع أو حاز لغرض استخدام الجهاز أو برنامج المعلوماتية أو أي بيانات معلوماتية معدة أو كلمات سرا اوكودات دخول و ذلك لغرض اختراق من الجرائم المنصوص عليها مسبقا وتتضمن البرنامج المعلوماتي مجموعة من الأوامر والتعليمات والأوامر القابلة للتنفيذ باستخدام الحاسب الآلي ومعدل إنجاز مهمة ما. (لطفي٢٠٢١، ٥٦٥)

٤- الجرائم الواقعة على الأموال منها جرائم الاحتيال والغش بوسيلة معلوماتية.

٥- جرائم الاستغلال الجنسي للقاصرات ويشمل الرسومات والصور والأفلام والكتابات. (عبد الفتاح ، ٢٦)

٦- جرائم التعدي على الملكية الفردية للاعمال الرقمية وتشمل جرائم وضع اسم مختلس على عمل وجرم تقليد وامضاء المؤلف او ختمه وجرم تقليد عمل رقم او قرصنه البرمجيات وجرم بيع او عرض عمل مقلد أو وضعه في التداول.

٧- جرائم البطاقات المصرفية والنقود إلكترونية وتشمل اعمال تقليد بطاقات بصورة غير مشروعة عن قصد لما لذلك من اخلال بالاقتصاد الوطني وتأثير سلبي على العمليات المصرفية.

٨- الجرائم التي تمس المعلومات الشخصية تتضمن الأفعال الجرمية التي تتعلق بمعالجة البيانات ذات الطابع الشخصي دون حيازه تصريح أو ترخيص مسبق ينتج القيام بالمعالجة.

٩- جرائم العنصرية وجرائم ضد الإنسانية: بوسائل معلوماتية نشر وتوزيع المعلومات العنصرية برسائل معلوماتية وتهديد أشخاص وتعدي عليهم بسبب انتماءاتهم العرقية او المذهبية والتحريض على ارتكاب جرائم ضد الإنسانية.

١٠- جرائم المغامرة وترويج المواد المخدرة بوسائل معلوماتية عبر الإنترنت وجرائم تسهيل وتشجيع شروع مغامرة وترويج الحكول للقاصرين.

١١- الجرائم المعلوماتية ضد الدولة والسلامة العامة تتضمن الأفعال الإجرامية الناشئة عن المعلوماتية التي تطال الدولة وسلامتها وأمنها واستقرارها ونظامها القانوني وهي جرائم تعطل الأعمال الحكومية أو أعمال السلطة العامة باستعمال وسيلة معلوماتية والعبث بالادلة القضائية المعلوماتية أو اتلافها أو إخفائها أو الأعمال الإرهابية التي ترتكب باستخدام شبكة الإنترنت.

١٢- جرائم تشفير المعلومات وتشمل افعاله تسويق أو توزيع أو تصدير أو استيراد وسائل تشفير بالإضافة إلى أفعال تقديم وسائل تشفير تؤمن بالسرية دون حيازة تصريح أو ترخيص من قبل المراجع الرسمية المختصة في الدولة .(شلوش ٢٠١٨،١٩١-١٩٢)

ومن مخاطر الجرائم السيبرانية التي فيها المساس بالاقتصاد والأمن الوطني وتهديده والمساس بالعلاقات الأسرية وتشكيل الخلافات بين أفراد الأسرة مما يؤدي للتفكك الأسري ، أما أسباب الجرائم السيبرانية هي:

أ . الرغبة في جمع المعلومات وتعلمها .

ب . الاستيلاء على المعلومات والإتجار فيها.

ت . قهر النظام وإثبات التفوق على تطوير وسائل التقنية.

ث . الحاق الآذى بالأشخاص أو الجهات .

ج . تحقيق أرباح و مكاسب مادية.

ح . تهديد الأمن القومي العسكري.

ولمكافحة الجرائم ينبغي توعية الأفراد بأهمية الأمن السيبرانية وتزويدهم بالإرشادات والنصائح الضرورية لاتباعها :

١-تدريب أفرادها على التعامل مع المخاطر الإلكترونية قدر الإمكان.

٢-تدريب على تفادي الأخطاء ومساعدة أفرادها في الحد من المخاطر الناتجة من اختراق أجهزة وشبكات الحاسوب وترجع لعدم وعيهم بالطرق وأساليب الوقاية والحماية.

٣- إعطاء النصائح التي تساهم في تنمية الوعي بالأمن السيبراني لتحقيق درجة عالية من الأمان والحماية.

٤-العمل على تحقيق الأمن السيبراني وحفظ الحقوق المترتبة في الاستخدام المشروع للحاسبات الآلية.

٥-حماية المصلحة العامة والآداب والأخلاق العامة والاقتصاد الوطني.

٦-تقتضي الضرورة سن تشريعات تغطي كافة الثغرات القانونية من مجال وجود فضاء سيبراني أمن بالاستعانة بالإرشادات الخاصة بمنظمة (الأوسكوا) أي تطوير البنية التشريعية الجنائية الوطنية بذكاء تشريعي مماثل تعكس فيه الدقة الواجبة على المستوى القانوني.

٧- ينبغي تعديل قواعد الإجراءات الجزائية لتتلائم مع تلك الجرائم السيبرانية وضرورة تنسيق والتعاون الدولي أمنيا وإجرائيا وقضائيا في مجال مكافحتها بيان الأحكام اللازم اتباعها حال التفتيش على الحسابات وعند ضبط المعلومات التي تحتويها وضبط البريد الإلكتروني حتى يستمد الدليل مشروعيته.

٨- ضرورة تخصيص شرطة متمكنة علميا وعمليا وفنيا لمواجهة التحديات مكافحتها وذلك من رجال الشرطة المدربين على كيفية التعامل مع أجهزة الحاسوب والإنترنت كذلك نيابية العامة والقضاء بتعيين وتدريبهم وتحديثهم في المجال السيبراني.

٩-إعطاء الوقت الكافي للتحقيق والملاحقة القضائية من قبل شرطة متخصصة مزودة بآليات تقنية تنظيمية و ضبط البريد الإلكتروني من قبل السلطات القائمة بالضبط.

الهجمات السيبرانية : تعرف الهجمات السيبرانية على أنها فعل يقوض من قدرات وظائف شبكة الكمبيوتر لغرض قومي أو سياسي من خلال استغلال نقطة ضعف ما تمكن المهاجم من التلاعب بالنظام ومن بين الهجمات السيبرانية :

١- سرقة كلمات المرور للمستخدمين للتسلل في النظام مثل التخمين والخداع والبرمجيات الخبيثة والنفاذ إلى ملف تخزين كلمات المرور والسطو على كلمات المرور السرية والتجسس على المستخدمين.

٢-هجمات رفض أداء الخدمة وأنكار الخدمة هجمات(ddos) تستخدم لزيادة التحميل على الإنترنت والبنية التحتية لشبكات والخدمات وهو يزعج الشركات والمنظمات وهو على العكس من التقنيات التي تستخدمها مجرموا الإنترنت فيها تمنع المستخدمين الشرعيين من الوصول إلى المنتجات والخدمات ويمكن أن يرتكبها فردا أو جماعة .(عبد الكريم٢٠٢١)

ويأخذ الصراع الإلكتروني طابعاً تنافسيا حول الاستحواذ على سبق التقدم التكنولوجي وسرقة الأسرار الاقتصادية والعلمية إلى أن يمتد ذلك إلى محاولة السيطرة على إلانترنت من خلال السعي للسيطرة على أسماء البطاقات وعناوين المواقع والتحكم بالمعلومات والعمل على اختراق الأمن القومي للدول دون استخدام طائرات أو متفجرات أو حتى انتهاك للحدود السيادية

كهجمات قراصنة الكمبيوتر وتدمير المواقع والتجسس بما يكون له تاثير على تدمير الاقتصاد والبنية التحتية بنفس القوة التي قد يسببها تفجير تقليدي مدمر بعمنى آخر إن الحرب السيبرانية تأخذ ثلاث صور رئيسية:

الاولى/هجمات شبكات الحاسوب.

الثانية/ الدفاع عن شبكات الحاسوب الآلي من أي اختراق خارجي عبر تأمينها من خلال إجراءات يقوم بها حراس الشبكات.

الثالثة/استطلاع لشبكات الحاسب الآلي وتعني القدرة على الدخول الغير المشروع والتجسس على شبكات الخصم بهدف الحصول على البيانات دون تدميرها.

وإذا كان الأمن القومي يهتم بحماية وغياب التهديد للقيم المجتمع الأساسية وغياب الخوف من تعرض هذه القيم للهجوم فإن الفضاء الإلكتروني قد فرض إعادة التفكير في مفهوم الأمن الذي يتعلق بتلك الدرجة التي يمكن أن تصبح في مأمن من خطر التعرض للهجوم العسكري والإرهابي وأصبح أمن الفضاء السيبراني يدخل في استراتيجيات الأمن القومي للعديد من الدول من أجل الاستحواذ على مصادر القوة داخل الفضاء الإلكتروني (الشهدي ، ٢٤٤-٢٤٧) ، كما أن عناصر القوة الإلكترونية ترتكز على وجود نظام متماسك يعظم من قوته المتحصلة في التناغم بين القدرات التكنولوجية والسكان والاقتصاد والصناعة والقوة العسكرية وإدارة الدولة وغيرها من العوامل التي تسهم في دعم إمكانات الدولة على ممارسة الإكراه أو الإقناع أو ممارسة التأثير السياسي على أعمال الدول الأخرى أو على الحكام في العالم لغرض الوصول لاهداف الوطنية من خلال قدرات التحكم والسيطرة على الفضاء الإلكتروني ومن مقاومات الردع السيبراني تتمثل فيه مصداقية الدفاع القدرة على الانتقام وأن الردع السيبراني صعب التنفيذ .

كما أن هناك العديد من العوامل التي يجب أن تحدث لضمان تحقيق النتائج المرجوة منها يتطلب الردع السيبراني تطبيق طرق وأساليب جديدة وأعادة تكييف مفاهيم الردع التقليدية تتناسب مع هذا المجال فلا يمكن معرفة الهدف من الهجمات دون معرفة من شنها دون معرفة الخصم وهدفه لا يمكن للردع أن ينجح وسرقة المعلومات قد تتكرر مستقبلا ومن هذه المتطلبات الردع السلبي الاحتجاجات الدبلوماسية والتدابير القانونية والعقوبات الاقتصادية والانتقام وفي الفضاء الافتراضي وانتقام العسكري واستراتيجيات الردع السيبراني والأنظمة البديلة وإعادة التأسيس (شلوش ٢٠١٨،٢٠١) . ويشمل الأمن السيبراني جميع المسائل العسكرية الاقتصادية

والاجتماعية والسياسية والإنسانية بهدف تحقيق منظومة أمن متكاملة تعمل على الحفاظ على الأمن القومي للدولة من كل التهديدات السيبرانية وتنقسم التهديدات السيبرانية التي تواجهها الدول والأفراد إلى أربعة أنماط (هجمات الحرمان من الخدمة) وهي تستخدم ضد مواقع الإنترنت أو البنوك أو المؤسسات من أجل التأثير عليها أو لدفع فدية مالية لاتلاف المعلومات أو تعديلها والتجسس على الشبكات وتدمير المعلومات اضافة للجرائم العادية التي تستخدم الإنترنت للسرقة والغش وسرقة الهوية و الاعتداء على الملكية الفكرية وغيرها من الجرائم التي تندرج في إطار الجريمة المنظمة وهي أداة إجرامية انتشرت عبر الإنترنت . (الهرمزي ٢٠١٩، ٤٢٧)

وأصبحت البرامج الخبيثة (ارانسوم) احدى التهديدات السيبرانية المنتشرة بشكل متزايد خلال السنوات الأخيرة ويستهدف مرتكبوا الجرائم السيبرانية المؤسسات الكبيرة التي تمتلك ملفات وانظمة كمبيوتر ذات أهمية بالغة لعملياتهم اليومية مما يمكنهم من طلب مبالغ فدية أكبر .

إن العلاقة بين الأمن السيبراني والأمن القومي تزداد كلما زادت ثقل المحتوى المعلوماتي والعسكري والأمني والفكري السياسي والاجتماعي والاقتصادي والخدمي والعلمي والبحثي إلى الفضاء السيبراني خاصة مع التسارع في تبني الحكومات الإلكترونية المدن الذكية في العديد من الدول ولم يقتصر اهتمام الدول بالأمن السيبراني على البعد التقني وحسب الأبعاد الأخرى ثقافية اجتماعية واقتصادية وعسكرية وهو ما عمل على دعم حقيقة إن الاستخدام غير السلمي للقضاء الإلكتروني يؤثر على الرخاء الاقتصادي والاستقرار الاجتماعي لجميع الدول التي أصبحت تعتمد على البنية التحتية الكونية للمعلومات.

إضافة إلى ذلك تصاعد دور الفاعلين من غير الدول في العلاقات الدولية قد أثر بدوره على سيادة الدول وخاصة مع بروز دور الشركات التكنولوجية عابرة للحدود الدولية وبروز اخطار القرصنة والجريمة السيبرانية والجماعات الإرهابية بمعنى آخر قد يتسبب توافر الإمكانات والموارد والتقنيات التكنولوجية اللازمة لغزو الفضاء الخارجي. وقد أدى الإفراط في التركيز على التهديدات الأمنية الناجمة عن تنافس القوى الكبرى في الفضاء الخارجي والسباق لتسليح الفضاء فيما بينهم إلى اقفال التركيز عن التهديدات الإرهابية التي تمثلها الفواعل من غير الدول خاصة القراصنة والعصابات وطالبي الفدية والجماعات الإرهابية وهو أمر يستلزم العديد من الجهود الجماعية لردعه ومجابهته . (بدر ٢٠٢١ ، ٢٢)

المحور الثالث: العراق في مواجهة الأمن السيبراني

أصبحت قضية الأمن السيبراني والفضاء الإلكتروني تدخل ضمن استراتيجيات الأمن القومي للعديد من الدول للحيلولة دون تعرض بنيتها التحتية الحيوية للخطر الذي ينجم جراء قطع شبكة المعلومات الدولية أو توقف وسائل البث الإذاعي أو تزويد الانتخابات أو التجسس الإلكتروني أو سرقة الملكية الفردية للاختراعات أو اختراع أنظمة صواريخ العسكرية وأدوات مهددة للأمن القومي للدول ، وأعطت القوة السيبرانية دفعا رئيسيا في اتجاهين :

الاول : تدعيم القوة الناعمة للدول لأن الفضاء الإلكتروني السيبراني أصبح مسرحا لشن هجمات تخريبية ونشر المعلومات المظللة والحرب النفسية والتأثير في الرأي العام والنشاط السري والاستخباراتي .

الثاني : تبني الدول زيادة الإنفاق في سياسات الدفاع الإلكتروني وحماية شبكاتها الوطنية من خطر التهديدات.

وتم توظيف الفضاء السيبراني من قبل الجماعات الإرهابية حيث أصبح هناك ارتباط كبير بين مواقع شبكة الإنترنت وبين انتشار المخاطر الأمنية التي تعرض لتهديد الاستقرار والأمن مثل التطرف والإرهاب إذا يوفر الإنترنت منبراً مهماً يظهر الإرهاب بواسطته في ترويع المجتمع ، ويتم استخدام الإنترنت من قبل المجاميع الإرهابية وإنصارها لتحقيق عدة أهداف منها: (الاتصال ، التدريب ، الجانب العملياتي ، الدعاية ، التجنيد ، نشر الأفكار) .

إضافة إلى ذلك ازدادت أهمية الفاعل الرقمي بعد استخدامه من قبل التنظيمات الإرهابية أو الجماعات السياسية التي تدعوا إلى العنف حتى أصبحت هذه الجماعات تتمتع بقوة كبيرة وقادرة على التأثير في العلاقات الدولية بين الدول ومن سمات الفاعل الرقمي في ظل العصر الرقمي الجديد وتطور عمليات (التنصت ، انتشار الطائرات بدون طيار المزودة بالكاميرات ، انتشار ظاهرة الإرهاب الإلكتروني). (الغازي ٢٠١٧ ، ٥٧)

ولقد كان للإنترنت دور كبير في تنفيذ الإرهابيين لعملياتهم الإرهابية والوصول للشباب والنشئ والسيطرة عليهم وتجنيدهم . (عفيفي ٢٠١٧، ٢٠) . خاصة وإن الإرهاب الرقمي من خصائصه لا يترك دليل مادي بعد ارتكاب جرائمه وبالتالي صعوبة عملية التعقب واكتشاف الجريمة إلى جانب ذلك سهولة اتلاف الأدلة ، كما يمتازون بخبرات في استخدام هذه التقنيات يحدث في بيئة لا تحتاج إلى القوة والعنف وإنما جهاز حاسوب آلي وبرامج شبكة الإنترنت (حمزة

٢٠٠٧، ٨٨) . وأن سياسة الانفتاح الكلي على الفضاء السيبراني دخلت مع دخول القوات الأمريكية للعراق بعد العام ٢٠٠٣ وشهد انفتاح واسع وهي متأثرة بسياسة الفضاء المفتوح التي تتبناها الولايات المحددة ذاتها واتخذت السياسة محورين:

الاول : حرية وسائل الإعلام وفتح الفضاء السيبراني ومنح الأفراد الحرية الكاملة في الوصول إلى محتوياته أو نشر من خلال معاملته معاملة مساوية لوسائل الإعلام الأخرى وأخذت بعدا تشريعيا من خلال إلغاء وزارة الاعلام وإنشاء المفوضية العليا للاتصالات والإعلام آذار ٢٠٠٤ .

والثاني : تقليل الرقابة الأمنية على وسائل الإعلام بما فيها الإنترنت عن طريق إلغاء الأجهزة والمؤسسات الأمنية التي كان يستعملها النظام السابق وأن إنشاء جهاز امني موحد هو اللجنة الوزارية للأمن القومي في نيسان ٢٠٠٤ . (الحمزة ، ٥٣٢)

وبدأت الجرائم السيبرانية في العراق منذ عام ٢٠٠٦ بشكل كبير والتي تمثلت بالغش عبر الإنترنت، غسيل الأموال، تزايد مواقع القرصنة، التجارة السيبرانية غير المشروعة، التطفل على الشبكات ، الاختطاف،التجسس ، التهديد، الاختراق ، المعلومات الشخصية، تجارة المخدرات، الإرهاب الإلكتروني.(ناظم ٢٠٢١ ، ١٧٩-١٨٠) . ولقد أثر الفضاء السيبراني بشكل كبير على الأمن الوطني العراقي من خلال ما تملكه الجماعات الإرهابية من وسائل تكنولوجية متطورة يصعب تتبع أثرها والسيطرة عليها حيث استخدمت المواقع الإلكترونية تقوم الجماعات الإرهابية من خلالها ممارسة نشاطاتها المختلفة في العراق ، ومن مظاهر الإرهاب السيبراني في العراق:

١ . **الابتزاز الإلكتروني:** يتم من خلال الحصول على معلومات سرية أو صور شخصية أو مواد فيديوية لاستغلالها لأغراض مالية أو القيام بأعمال غير مشروعة حيث شهد عام ٢٠٢١ بغداد و إحصائية الابتزاز من النساء وفق إحصائية الشرطة المجتمعية في وزارة الداخلية(١٩٥) حالة ابتزاز . (البدري و علي و محمد ٢٠٢٠ ، ٥٨).

٢. **التجسس الإلكتروني** : وهي الدخول غير المشروع والاطلاع على الشبكات الخصم دون تخريب أو تدمير للبيانات والمعلومات وتشمل خطط عسكرية دفاعية أو هجومية أو مخططات سرية حربية كانت أم سليمة . (وكالة يقين للأنباء ٢٠٢٢)

٣. **الاختراق الإلكتروني** : الذي يقوم به الإرهابيون المبرمجون الذي يطلق عليه الهاكرز أو قراصنة الحاسوب يقوم باستعمال البرامج التجسس على الشبكات والأنظمة الإلكترونية والاعتداء على البنية المعلوماتية للمؤسسات الحكومية وفي انتخابات عام ٢٠١٨ جرت عملية التصويت

بالاعتماد على نظام الأقمار الصناعية والتي لا يمكن التحكم بها لأنها تدار من خارج العراق لذا زادت احتمالية اختراقها والتلاعب بنتائجها من قبل جهات خارجية ولعل اخطرها في ٢٥/ تشرين الثاني/ ٢٠١٩ عندما اختراق الموقع الرسمي لجهاز مكافحة الإرهاب والإعلان عن انقلاب ضد الحكومة استجابة لدعوة المتظاهرين إلا أن جهاز مكافحة الإرهاب أعلن من موقعه الرسمي لاحقا عن تعرض الموقع الرسمي للاختراق وإن ما نشر فيه ليس صحيحا . (الحمزة ، ٥٣٣)

ويشير تعقب السلطات الأمنية العراقية لتنظيم داعش إلى تلك العلاقة بين التأثيرات السلبية لمواقع الإنترنت على الأمن الوطني اذ تنوعت أساليب التعامل هذه الوسائل من قبل الجماعات الإرهابية بين التخطيط والتنفيذ التنفيذ لأعمالهم الإجرامية ونشر أفكار التطرف والعنف الترويج لها واستقطاب ، ومن أدوات الإرهاب السيبراني :

١- **الفيروسات (virus)** : وتعد من أخطر استخدامات الشبكة المعلوماتية وتعمل على تعطيل الخدمة مؤقتاً لأعلى تدمير قاعدة البيانات والمعلومات ولها قدرة على ربط نفسها بالبرامج الأخرى وسرعة التضاعف والانتشار بإطلاق حزمة كبيرة من البيانات والمهام server على جهاز الطرف المتضرر مما يؤدي إلى توقف وشل مصالحه بصورة كلية أو جزئية وتعطيل نظم المعلومات الإلكترونية لديه.

٢. **برنامج الدودة (womsperogram)** : وهي التي تقوم باستغلال أية فجوة في أنظمة التشغيل من نظام إلكتروني لأخر أو شبكة لأخرى عبر الوصولات التي ترتبط بها.

٣. **هجمات أنكار الخدمة (Denial ofservice.Dos)** : وهي عبارة عن هجمات إلكترونية تتم بإغراق الموقع بسيل من البيانات غير اللازمة يجري ارسالها ببرامج متخصصة تعمل على نشرها مما يؤدي البطء في الخدمات وازدحام مروري على هذه المواقع و يصعب بالتالي وصول المستخدمين لها.

٤. **أحصنة طروادة (Trojans)** : وهو عبارة عن فايروس ذا مقدرة على الاختفاء داخل برامج أخرى اصلية للنظام الإلكتروني وينشط هذا الفايروس عندما تبدأ برامج التشغيل بالعمل ليبدأ أعماله التخريبية ويختلف هذا الفايروس عن الفايروس العادي لكونه لا يتكاثر في الملفات وإنما هو برنامج مستقل بذاته و تصل أعمالها تخريبية إلى تدمير النظام برمته ويستطيع فتح أحد المنافذ في جهاز المجني عليه دون أن يشعر وفتح القرص الصلب بجهاز المجني عليه والعبث به بحذف أو إضافة ملفات جديدة أيضا يمكن للمخترق معرفة كلمة السر المخزنة في الجهاز

ورقم بطاقة الائتمان وأيضا(ميكروفون أو كاميرا) المجني عليه ويستمع ويرى كل ما يفعل في المساحة التي يغطيها المايكرفون أو الكاميرا. (الزيدي ، ١٤١)

٥. **القنابل المنطقية (Logie Bombs)** : هي برمجيات يتم زرعها داخل النظام أو البرنامج أي أن يكون البرنامج أو النظام مصابا منذ البدء بالبرنامج الضار أي بالسلاح السيبراني .

٦. **الفيروسات الإلكترونية (Electronic viruses)** : كفايروس (ستاكس – نت stuxnet) الذي يعد أخطر أنواع الأسلحة السيبرانية ثم اكتشافه ٢٠٠٩ ونظام فايروس دوكو (Dayo) في ٢٠١١ بواسطة معامل التشفير والأمن الإلكتروني (crysysLab) التابع لجامعة بودابست وفايروس (فليم flamp) في٢٠١٢ بواسطة فريق الاستجابة و الطوارئ الإيراني فضلا عن شركة (كاسير سكي) ومعمل التشفير والأمن الإلكتروني التابع بجامعة وايست .

٧. **البرمجيات الخبيثة مثل (اريد البكاء wanna cry)** : إذا تتميز هذه البرمجيات لكونها تستهدف الكيانات الاقتصادية وليست الأفراد لأن هذه المؤسسات الاقدر على دفع الفدية وهذه الهجمة تم نشرها من وكالة الأمن القومي الأمريكي حيث قام مجموعة من القراصنة المجهولين ٢٠١٧ بالهجوم على أكثر من(١٥٠) دولة وإصابة(٢٠٠)الف شخص ، (فرج٢٠٢١ ، ٢٠٥) اعضاء جدد وإمكانية نشر توترات بين مكونات المجتمع إلى جانب إجبار الدولة على اتخاذ إجراءات للضبط قد تؤثر في صورتها على المستوى الدولي .

كما قام تنظيم (داعش الإرهابي) باستخدام الإنترنت في بث عمليات إعدام التي كان يقوم بتنفيذها على الأسرى وذلك لبث الرعب والفزع في نفوس الأهالي المدن التي كان يرغب في السيطرة عليها هذا ما ادى الى هروب واستسلام قرى و مدن للتنظيم داعش خوفاً من تعرضها للمصير نفسه من قبلهم وتجنيد الشباب . كما استخدم تنظيم داعش الإرهابي وسائل التواصل الاجتماعي لجمع المعلومات الأمنية عن طريق مجموعة من قراصنة الإنترنت الذين يخدعون الناس بإرسال رسائل تحتوي شفرات وبرامج ضارة عبر وسائل التواصل الاجتماعي وما أن يتم فتحها حتى يبدأ المهاجمون على الفور بالتحكم الكامل بالجهاز وسرقة الملفات واستخدام كاميرا الكمبيوتر والميكروفون لمراقبة ما يجري للشخص المستهدف وذكرت شركة (أنتل كراولر) الأمريكية في مجال مكافحة التهديدات السيبرانية عام ٢٠١٤ أن هناك جهات فاعلة تتخذ من العراق مقرا لها وتشارك في أنشطة غير مشروعة مختلفة في الفضاء السيبراني ويستخدم الإرهاب الإلكتروني إلانترنت الشبكات الاجتماعية تطبيقات الهواتف الذكية والألعاب الإلكترونية كوسيط

تجنيدي تنظيمي معلوماتي من ناحية وكوسيط لوجستي مالي ودعائي من ناحية أخرى كما يشمل أيضا استخدام التقنيات الذكية مثل الطائرات بدون طيار والطابعات الثلاثية الأبعاد والتقنيات والمواقع الافتراضية في التخطيط والتنفيذ للعمليات الإرهابية (خليفة٢٠١٧ ، ٧٨) ، وتعمل كمرتزقة وقد زادت بشكل كبير ولديها علاقات بجماعات أخرى في كل من (مصر، لبنان، ليبيا، إيران، سوريا،) ودور الجماعات الإسلامية المنتشرة في العديد من الدول.

وتأثرت منظومة الأمن الوطني العراقي بالتهديدات السيبرانية خاصة وأن العراق يعاني من ضعف في البنية التحتية الخاصة بالحماية الإلكترونية من الهجمات السيبرانية وأصبح العراق مخترق ومكشوف لكثير من الدول العالم بسبب التجسس عليه للمؤسسات الأمنية ومن دون قيود رقابية خاصة وانه لا يوجد قانون خاص في العراق لمكافحة الجرائم الإلكترونية فقط تضمن دستور العراق الدائم لعام ٢٠٠٥ وفق المادة (٧) تجريم الإرهاب ، كما نصت المادة(٢١) الفقرة الثالثة على ان (لا يمنح حق اللجوء السياسي إلى المتهم بارتكاب جرائم دولية وإرهابية أو كل من الحق ضرر بالعراق) (سلمان ٢٠٢١، ١٧٤) . وفي المادة (٧٣) من الدستور العراقي لعام ٢٠٠٥ التي تنص على (أن يتولى رئيس الجمهورية صلاحيات إصدار العفو بتوجيه من رئيس مجلس الوزراء باستثناء ما يتعلق بالعقود الخاصة والمحكومين بارتكاب جرائم دولية والإرهاب والفساد المالي والإداري) . (المادة (٧٣) وفقا لدستور العراق الدائم لعام ٢٠٠٥)

كما نص قانون مكافحة الإرهاب رقم (١٣) لسنة ٢٠٠٥ وتضمن هذا القانون تعريف للإرهاب في مادته الأولى (ان لكل فعل إجرامي يقوم به فرد أو جماعة او منظمة و تستهدف فرد أو مجموعة أفراد أو جماعة أو مؤسسات رسمية أو غير رسمية أوقع الأضرار للممتلكات العامة أو الخاصة بغية الإخلال بالوضع الأمني والاستقرار والوحدة الوطنية أو إدخال الرعب والخوف والفزع بين الناس وإثارة الفوضى تحقيقا لغايات ارهابية). (عبد الرضا والمعموري ٢٠٢٠، ١٧٧)

واصبح الفضاء السيبراني إلى حد كبير عبر الإنترنت أرضية مشتركة للاتصال السريع للأفكار والقيم وهو مساحة محايدة إلا أن استخدام هذه المساحة هو الذي سيحدد قيمة الفضاء السيبراني وفائدته للبشرية أم العكس(خرسان ٢٠٢٠،٢-٣) ،كما أن الفضاء الإلكتروني يوظف في حروب الجيل الرابع لزعزعة واستقرار الشعوب و نشر الفوضى وذلك من خلال عدة طرق :

١. العمل على ضرب أجهزة القوة لدى الدولة وأجهزة الشرطة و الجيش.
٢. ضرب المؤسسات الداخلية فلا يتم الفصل بين السلطة والنظام السياسي وبين الدولة.

٣.العمل على تأجيج الصراع واستخدام العنف ضد المجتمع بمختلف فئاته وطوائفه وتأجيج مشاعر التمرد والعصيان ورفض الواقع وتتم مواجهة حروب المعلومات من خلال استراتيجية تتضمن شقين الأول دفاعي يحمي أنظمة الدولة والآخر هجومي يوجه ضد أنظمة الدولة المعادية ويعتمد على العمليات التقنية و الاستخباراتية و مواجهة الوسائط والهكرز وزرع العملاء وهو ما ينتهي إلى خلق مناخ عدائي بين الأطراف المتصارعة يؤثر في المؤسسات الداخلية وتماسك النسيج الوطني للشعوب . (الصادق ٢٠١٧، ٢٨)

وقامت الحكومة العراقية بالتعاون مع شركائها الدوليين في مجال تطوير الأمن السيبراني للافادة من خبراتهم بالتنسيق مع حلف شامل الأطلس الناتو على تدريب موظفين من فريق استجابة للأحداث السيبرانية على أساسيات الدفاع السيبراني من التسريب والتحليل في عام ٢٠١٦ / تشرين الثاني وقد احتل العراق المرتبة (١٥٨) على الصعيد العالمي استنادا إلى مؤشر الأمن السيبراني العالمي لعام٢٠١٧ (Global cybersec urityindex–Gci) الصادر من الاتحاد الدولي للاتصالات في عام ٢٠١٨ احتل العراق المرتبة(١٠٧) على الصعيد العالمي من أصل(١٧٥) دولة وفق مؤشر الأمن السيبراني وهذا يعني إن العراق في تطور إيجابي و عقد في بغداد ٢٠١٩ /اذار/٥ مؤتمر لتطوير الاستراتيجيات العراق للأمن السيبراني بالتعاون مع المجلس الدولي للاستشارة الإلكترونية(EG–council) التابع لمفوضية الاتحاد الأوروبي ، لا يمكن لأي دولة في العالم سواء كانت متقدمة أم نامية أن تهمل أو تتجاهل الأمن السيبراني و اذا كان وجود استراتيجية للأمن السيبراني بهذه الأهمية للدول فإن العراق بأمس الحاجة لمثل هذه الاستراتيجية لاسيما وأنه يعد من أكثر الدول تعرض للإرهاب السيبراني ، يقتضي الأمر وضع تنفيذ خطة وطنية للأمن السيبراني من خلال استراتيجية شاملة تشمل استعراضا عاماً أوليا لمدى كفاية الممارسات الوطنية الحالية والنظر في دور أصحاب المصلحة (الهيئات الحكومية ، القطاع الخاص، المواطنين) في هذه العملية والأسباب تتعلق بالأمن القومي والرفاه الاقتصادي تحتاج الحكومة إلى المساعدة في عملية حماية البنية التحتية لمعلوماتها الحيوية وتعزيز هذه الحماية وضمانها لا يمكن الوصول إليه الأ من خلال وجود إستراتيجية وطنية تعتني بالأمن السيبراني في المجالات الآتية:

١. حماية خصوصية المواطن والبيانات من الضياع والاستعمال غير المصرح به.

٢ . مرونة الخدمات الحكومية والنظم والبنية التحتية للتهديدات الإلكترونية.

٣ . استمرارية الحكومة أثناء وبعد الحوادث السيبرانية الخطيرة.

٤ . حماية أمن الخدمات الرقمية للمواطنين.

٥ . تنسيق الاستجابة للتهديدات ضد البنية التحتية.

٦ . أمن وسلامة البنية التحتية الأساسية للحكومة (Ics) .

ولقد أطلق العراق المؤتمر الوطني الثاني لتطوير وبناء القدرات الأمنية في الفضاء السيبراني في بغداد ايلول/٢٠٢١ فضلا عن ذلك تواصل العمل على تعزيز الشراكات الأكاديمية والأمنية بين وزارة الداخلية العراقية وجامعة نايف العربية للعلوم الأمنية و وزارة الداخلية السعودية وبالتنسيق مع سفارة الجمهورية العراقية في الرياض وتهدف إلى التعاون وتبادل الخبرات والمعارف وتقديم برامج تدريبية متخصصة تساهم في رفع مستوى الكفاءات الأمنية لمواكبة التطورات العالمية وتعد جامعة نايف للعلوم الأمنية من أبرز المؤسسات الأكاديمية في المنطقة متخصصة في أعداد الكوادر الأمنية عبر برامج متطورة وتشمل الأمن السيبراني ، الأمن الوطني ، العمل الشرطي ، كما توفر الجامعة بيئة تعليمية حديثة تجمع بين التعليم النظري والتطبيق العملي . وهنا نشير إلى أن تبادل الخبرات التقنية التي تكتسبها الدول الصديقة عند صد هجوم سيبراني او أعادة تأهيل الشبكات بعد اختراق المنظومة الأمنية يعتبر العمود الفقري لبسط الأمن السيبراني ، والعراق يستفيد من تجارب الدول الصديقة في المجال التكنولوجي وتعمل على تطوير وبناء القدرات الأمنية في الفضاء السيبراني ، كذلك يجب اتباع الإرشاد الدولي حول الأمن السيبراني ، والعمل مع شركاء دولتين في القطاعين العام والخاص لإطلاق قمر صناعي عراقي للاتصالات لتأسيس البنية التحتية الأساسية اللازمة لنظام الأمن ، المعلومات المتكاملة والتخطيط لنظام بيئي تشريعي وقانوني و فضائي حول الفضاء السيبراني يوفر معايير وأنظمة وطنية لأمن الفضاء الإلكتروني في كل من القطاعين الخاص والعام ويخلق بيئة قانونية مؤاتية المؤسسات وتفعيل بيئة ملائمة لملاحقة الجريمة السيبرانية مع ضمان الحريات المدنية وتأسيس وكالة سيبرانية وطنية تخصص لتنفيذ السياسة السيبرانية وتكون مسؤولة عن التثقيف والتوعية السيبرانية وأمن المعلومات والدفاع عن الفضاء السيبراني الوطني العراقي ، والدخول في معاهدات و اتفاقات متعددة الجنسيات تتعلق بأمن الفضاء السيبراني بوصفها آليات اساسية لتدوين القواعد والسلوك أثناء إبرام المعاهدات و اتفاقيات ثنائية تنص على تبادل المعلومات وتنمية القدرات وسد الفجوة الحالية في الخبرة الفنية وتهيئة قاعدة يمكن عن طريقها رعاية رأس

المال البشري العراقي وتطويره وتشجيعه على المدى الطويل . وأطلق جهاز الأمن الوطني أول منصة لأمن السيبراني في العراق وتقوم هذه المنصة بعملية تأمين الروابط التي يستخدمها المواطنون خوفا من أن تحمل هذه الروابط بعض الملفات الخبيثة وأيضا معرفة بيانات المواطنين مسربة أم لا يمكن للمواطنين استخدام الدخول إلى هذه المنصة التي تحمل أسم أمان وهي سهلة الاستخدام مع كل ما تقدم وهنا نشير إلى ملاحظة مهمة ، إن وثيقة استراتيجية الأمن السيبراني العراقي لعام ٢٠١٧ فيها بعض نقاط الضعف وفشلت في تحفيز وتطبيق الإطار الذي يقترحه حيث كانت الإستراتيجية نظرية في الأساس وتذكر التهديدات العامة التي تواجه الجهات الفاعلة الخاصة والعامة في الفضاء السيبراني بدلا من التركيز على طبيعة التهديدات الإلكترونية التي يواجهها العراق ولم تحاول الإستراتيجية توفير ما يمكن اعتباره تحليل ومخطط ملموس لتصنيف البنية التحتية الحيوية التي يمكن ان تكون موضع استهداف متكرر ، و أخفقت الوثيقة في تحديد الجهة والمؤسسة الحكومية التي ستكون مسؤولة عن تنفيذ توصياتها أو خططها أو أهدافها ، كما أنها لم تقدم برامج استراتيجية مفصلة على مدة تنفيذ للسياسات المذكورة ولهذا لم يشهد أي من الأهداف أو السياسات أو الاصلاحات المقترحة اي تقدم حقيقي فيما يتعلق بتحقيقها. ولا بد أن تنطلق استراتيجية الأمن السيبراني العراقي(Ics) من مبدأ ضمان أمن العراق وحماية وجوده في الفضاء السيبراني وحماية بنية معلوماته الحيوية وبناء مجتمع إنترنت موثوق به والتعامل مع التحديات السيبرانية من خلال مجموعة من الإجراءات:

١- المرتكز التشريعي القانوني والقضائي حول الأمن السيبراني من خلال توفير معايير وانظمة وطنية لامن الفضاء للإلكتروني في كل من القطاعين العام والخاص.

٢-المرتكز التقني من خلال توفير مؤسسات فنية بكفاءة عالية للتعامل مع التحديات السيبرانية .

٣- المرتكز النظمي من خلال إيجاد مؤسسات واستراتيجيات خاصة برسم وصناعة السياسات للتطوير الأمن السيبراني على المستوى المحلي.

٤- تأسيس الهيئة الوطنية للأمن السيبراني العراقي.

٥- ركيزة بناء قدرات العراق إذا انه ما زال يعاني من قلة التخصيص للبحث والتطوير والتعليم والتدريب التي تعمل على بناء تلك القدرات ليستطيع أن يتعامل مع متغيرات الفضاء السيبراني.

٦-المرتكز الاجتماعي إن الفضاء الإلكتروني يحمل الايجابيات والأخطار لذا يجب زيادة وعي المجتمع والفرد بالاخطار (هادي وإسماعيل٢٠٢٠،٢٨٢)(صقر http://fuTurcuae.com)

٧- ضرورة بناء تعاونات وشراكات وتحالفات في مجال السيبرانية اذا مازال العراق يعاني من عزلة إقليمية واغتراب في مجال الفضاء السيبراني ولا يملك اتفاقيات ثنائية مع الأطراف الإقليمية والدولية والعقود الاستراتيجية مع القطاع الخاص الدولي لتفعيل عمل حماية الأمن السيبراني . (مستشارية الأمن الوطني العراقي أمانة سر اللجنة العليا لأمن الاتصالات والمعلومات ،٢-١٠)

٨- العمل مع شركاء دوليين من القطاعين الخاص والعام لإطلاق قمر صناعي عراقي للاتصالات لتأسيس البنية التحتية الأساسية اللازمة لنظام أمن المعلومات المتكامل وأن مخاطر أمن المعلومات قد تهدد الأمن الوطني وأن وسائل المواجهة والحماية لابد أن تطلقها من منظومة أمن وطني لأنه من غير المعقول أن تكون الأخطار والتهديدات شاملة وربما مشتقة ومخططة أحيانا ينبغي البدء بتنفيذ برنامج شامل على مستوى مؤسسات هيئات الدولة والشركات الخاصة يستهدف التدريب على صد الهجمات الإلكترونية الشاملة بتنوعاتها المختلفة سواء الفيروسات أو التجسس الاقتصادي أو التخريب الإلكتروني أو هجمات تعطيل شبكات الاتصالات والمعلومات.

٩- تحفيز قدرات القطاع الخاص في دول العالم الثالث بتوظيفهم في العراق وذلك لسد الفجوات الحالية في الخبرة الفنية والمهنية وتهيئة قاعدة يمكن عن طريقها رعاية رأس المال البشري العراقي وتطويره وتشجيعه على المدى الطويل.(موسى ٢٠٢٠) (عباس و صوان https://political_encyclopedia.org/library/1386)

مما تقدم ولضمان نجاح وفاعلية الاستراتيجية الوطنية للأمن السيبراني لابد من توفير مجموعة من العناصر الأساسية لها أهمية ضمان أعلى مستوى في التأييد والدعم الرسمي لها مادياً ومعنوياً من قبل الحكومة وتشكيل هيئات متخصصة بالأمن السيبراني واشراك الهيئات الحكومية المعنية وضمان التعاون والتنسيق فيها بينها واشراك أصحاب المصلحة الآخرين ولاسيما القطاع الخاص الموثوق بهم لضمان عمل البنى التحتية الأساسية للأمن السيبراني وتخصيص موارد لها في ميزانية الدولة الوطنية وضرورة أن تضمن الاستراتيجية خططاً قابلة للتنفيذ وأهداف قصيرة ومتوسطة وبعيدة المدى تسعى لتحقيقها ، إضافة إلى ذلك استحداث اختصاص جامعي يختص بالأمن السيبراني (incybersec aritybachcl ordegree) إضافة إلى تخصص يعني بالجنائيات الرقمية (digital forensic) وطرق التحقيق الإثبات في القضايا المتعلقة بالجرائم المعلوماتية وإضافة المناهج المتخصصة التي تعني بالجرائم المعلوماتية لطلاب كلية الحقوق والقضاء.

الخاتمة

الأمن السيبراني له صلة وثيقة بالأمن الوطني لأي دولة وتزداد خطورته كلما زاد الاعتماد من قبل الدولة على تقنية المعلومات وارتباطها بالفضاء السيبراني وتنطلق الاستراتيجية الأمنية العراقية من مبدأ أساسه ضمان أمن العراق وحمايته من الجرائم السيبرانية وحماية البنية التحتية المعلوماتية الحيوية وبناء مجتمع ناجح في مواجهة التحديات السيبرانية التي تهدد امن العراق الوطني وسلامته .

اذن يتطلب الامن اذا يتطلب واقع الأمن السيبراني العراقي والمخاطر والتهديدات المستمرة التي تعترضه أحداث هيئة وطنية موحدة لجميع التشكيلات والفرق الإلكترونية للأجهزة العراقية التي يمكن أن تشكل البنية التحتية الأساسية له ضمن مسار الاستراتيجية الوطنية للأمن السيبراني وصلاحيات واسعة تعمل على تأمين حال البلاد في البعد الخامس للحروب المعاصرة إلى جانب تعديل النصوص التشريعية المرتبطة بمواجهة الجرائم السيبرانية على وفق المعطيات المعاصرة و إرساء ثقافة عامة للأمن السيبراني على صعيدي المؤسسات والأفراد وتشجيع البحث العلمي المتعلق بهذا المجال عن طريق افتتاح أقسام أو فروع علمية في الجامعات العراقية الى جانب تحفيز بتخصصاتهم العلمية وتدريب وتنمية الباحثين لإجراء دراسات الامن السيبراني وبحسب ارتباطه المهارات الرقمية بشكل مستمر لمواكبة المستجدات الإلكترونية على مستوى المنطقة و العالم والنقطة المهمة هي إجراء تقسيم على مستوى الدولة كاملا من أجل تحديد نقاط الضعف في نظم المعلومات الحكومية والمواقع الشبكية وعمليات معالجة البيانات وكذلك مواطن الضعف الموجودة في البنية الأساسية للمعلومات الحيوية للبلاد ويساعد تقييم الضعف الوطني الحكومي لمعالجة وحماية البنى التحتية المعلوماتية و العمل على دعم وبناء مجتمع سيبراني موثوق به .

ويتم الامن السيبراني بتدريب كوادر مختصة وتنمية مهاراتهم وتشجيع البحث والتطوير والابتكار فضلا عن ذلك تعاون العراق مع المحيط الاقليمي والدولي لتحقيق الامن السيبراني والسيطرة على الجرائم السيبرانية ومن أهم التوصيات التي يجب العمل بها لتحقيق الأمن السيبراني هي :

- تفعيل نظام الحكومة الإلكترونية .

- تبني النظام الإلكتروني لتأسيس قاعدة بيانات في جميع مؤسسات الدولة يضمن سرعة ودقة إنجاز المعاملات وبناء منظومة متكاملة لأمن المعلومات .
- إنشاء المدن الذكية التي تحفز المواطن على التعامل والتطوير مع التطور التقني العالمي.
- تبني أنظمة التعليم الإلكتروني والتدريب على الأمن السيبراني لتوظيف الفاعل الرقمي لبناء استراتيجيات معلوماتية تخدم المواطن وتزيد من كفاءة المؤسسات كافة.
- تحويل مؤسسات الدولة لمؤسسات إلكترونية لبناء منظومة أمنية شاملة تضمن حماية المعلومات وترسيم الخصوصية وحماية سرية المعلومات الشخصية.
- تبني نظم قانونية تنظم أليات التعامل الإلكتروني وتجريم المنتهكين والهاكرز .

المصادر

عنتر ، عبد النور بن ، تطور مفهوم الأمن في العلاقات الدولية، مجلة السياسة الدولية ، المجلد(٤٠) ، العدد(٦٠)، القاهرة ، مركز الدراسات السياسية والاستراتيجية، أبريل٢٠٠٥.

عبد الصبور، سماح ، الصراع السيبراني طبيعة المفهوم وملامح الفاعلين، مجلة السياسة الدولية ،العدد(٢٠٨) ،أبريل ٢٠١٧.

صادق ، عادل ، استخدامات الفضاء الإلكتروني في منظور التداخل الخارجي، مجلة السياسة الدولية ، القاهرة، العدد(٢١٠)، أكتوبر ٢٠١٧ .

جيجان، إسراء شريف ، الأمن السيبراني الصيني : دراسة في الدوافع والتحديات، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، العدد(٥٦)، نيسان/٢٠٠١.

عثمان ، أحمد زكي ، تأكيدات القدرات السيبرانية في الصراعات الإقليمية، مجلة السياسة الدولية، العدد(٢٠٨) ، أبريل/٢٠١٧.

اللجنة الاقتصادية لغربي آسيا الاسكوا ، الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة الغربية، توصيات سياسية ، ٩/شباط/٢٠١٥.

الرشيدي ، أحمد ، إشكاليات التطور الجدل الدولي على مفهوم الإرهاب، مجلة السياسية الدولية ، العدد(٢٤٠)، أبريل٢٠١٦.

سلمان ، عبير ، التكنولوجيا في عالم الإرهاب :سلاح ذات أوجه متعددة، مجلة السياسة الدولية، العدد(٢٢٧)، يناير ٢٠٢٢.

لطفي ، رشا عادل ، جرائم الاتصال عبر الإنترنت وضبط أخلاقياته في ضوء الاتجاهات البحثية الحديثة رؤية تحليلية، مجلة البحوث الإعلامية، جامعة الأزهر، كلية الإعلام، العدد الثامن والخمسون الجزء ٢، يوليو ٢٠٢١.

عبد الفتاح ، فاطمة الزهراء ، تطور توظيف جماعات العنف ل(الارهاب السيبراني)، مجلة السياسة الدولية، العدد(٢٠٨).

شلوش ، ثورة ، القرصنة الإلكترونية في الفضاء السيبراني التهديد المتصاعد لامن الدول، مجلة مركز بابل للدراسات الإنسانية،٢٠١٨، المجلد(٨)، العدد(٢) .

عبد الكريم ، محمد زهير ، الإرهاب السيبراني أزمة عالمية جديدة، مجلة قضايا سياسية، العدد(٦٤) ،العلوم السياسية ،جامعة النهرين،٢٠٢١.

الشهدي ، تغريد معين حسن ، الأثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة، مجلة البحوث الجغرافية، العدد(٣٠) ،جامعة الكوفة .

الهرمزي ، سيف نصره ، وصف المقاربات المنظورات الفاعل الرقمي والانكشاف الاستراتيجي في ظل الفضاء السيبراني ، مجلة آداب الفراهيدي، العدد(٣٧)،اذار ،٢٠١٩.

بدر ، اية ، الفاعلين دون الدول في الفضاء الخارجي، مجلة السياسة الدولية، العدد(٢٢٦) ، اكتوبر ٢٠٢١، المجلد ٥٦.

الغازي ، عبد القادر ، دور الأمم المتحدة في مكافحة الإرهاب الدولي، السياسة الدولية ، العدد(٢١٠) ، اكتوبر ٢٠١٧ .

عفيفي ، عبد الغفار ، معظلة تعريف الإرهاب في الفكر وألممارسة ، السياسة الدولية ، العدد(٢١٠)،٢٠١٧.

حمزة ، مجيد كامل ، الإعلام الرقمي الإلكتروني للإرهاب وسبل المواجهة، مجلة السياسة الدولية، جامعة المستنصرية، العدد(٣٥-٣٦)،٢٠٠٧.

ناظم ، أحمد عدنان ، العنف والتطرف في العراق مقاربات في الدوافع وسبل المواجهة ، مجلة العلوم السياسية ، جامعة بغداد ،العدد (٦١) ، ٢٠٢١ .

البدري و علي و محمد ، مروة حامد و وردة هاشم و آية احمد ، نشأت وتطور الجماعات الجهادية في افغانستان حركة طالبان وتنظيم القاعدة الدولة الاسلامية في العراق والشام نموذجا ، المجلة العلمية للبحوث والدراسات التجارية ، المجلد (٣٤)، العدد الاول ، ٢٠٢٠ .

الزيدي ، عبد الهادي محمود ، التجسس الإسرائيلي الإلكترونية على الدول العربية، مجلة ودراسات دولية ، العدد(٥٨) ، مركز دراسات الاستراتيجية و الدولية .

خليفة ، إيهاب ، الإرهاب الذكي كيف توظف الحركات المتطرفة للتطورات التكنولوجية، مجلة السياسة الدولية، العدد(٢١٠) ، أكتوبر ،٢٠١٧.

سلمان ، مصطفى إبراهيم ، الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة كلية القانون والعلوم السياسية، جامعة ديالى ، العدد الأول، المجلد العاشر، ٢٠٢١.

المادة (٧٣) وفقا لدستور العراق الدائم لعام ٢٠٠٥ .

عبد الرضا و المعموري ، سعد طارش وعلي إبراهيم مشجل ، الأمن السيبراني ودوره في انتشار ظاهرة الإرهاب في العراق بعد عام ٢٠٠٣، مجلة دراسات دولية، جامعة بغداد، العدد(٨٠) ،كانون الثاني،٢٠٢٠.

خرسان ، باسم علي ، الفضاء السيبراني ، حتمية الاتصال وتحدي التواصل مع الآخر ، مجلة تكريت للعلوم السياسية ، العدد(٢٢) ،٢٠٢٠ .

الصادق ، عادل عبد ، استخدامات الفضاء الإلكتروني في منظور التدخل الخارجي، مجلة السياسة الدولية ، العدد(٢١٠)، أكتوبر ٢٠١٧.

هادي و إسماعيل ، فلاح مهدي وزيد محمد علي ، الأمن السيبراني كمركز جديد في الإستراتيجية العراقية ، مجلة قضايا سياسية ، العدد(٦٢) ، تموز/٢٠٢٠ .

الحمزة ، سامر محي عبد ، السياسة التشريعية العراقية لحماية الأمن الوطني السيبراني دراسة في ضوء أحكام القانون الدولي العام ، على الموقع الالكتروني: lark.uowasit.edu.iq

وكالة يقين للأنباء، ضحايا الابتزاز الإلكتروني، ٥/تموز/٢٠٢٢، على الموقع الإلكتروني: aqinnews.net

فرج ، كرار عباس متعب ، الحرب السيبرانية دراسة في استراتيجية الهجمات السيبرانية بين الولايات المتحدة وإيران، مجلة حمورابي، العدد(٤٠) ،شتاء ٢٠٢١ ، على الموقع الإلكتروني : https://wwwlasj.net

صقر ، امل ، محاضرة واقعية كيف يهدد التواصل الاجتماعي الأمن الوطني على الموقع: http://fuTurcuae.com

مستشارية الأمن الوطني العراقي أمانة سر اللجنة العليا لأمن الاتصالات والمعلومات، استراتيجية الأمن السيبراني العراقي، ص٢ – ١٠ ، وعلى الرابط :https://www.itu.int/enlltuD/cybersecurity/Documents/National_strategies Repository/00056-06-iraqi-cybersecurity-strategy.pdf .

موسى ، حازم حامد ، الرؤية الاستراتيجية للأمن الوطن العراقي في الفضاء السيبراني ، المجلة الجزائرية للعلوم القانونية والسياسية ،المجلد(٥٧) ، العدد(٥) ، ٢٠٢٠ ، على الموقع: www.asip.cerist.dzpdf .

عباس و صوان ، مهند جبار و هيثم كريم ، الحرب السيبرانية بين التحديات والاستراتيجيات المواجهة العراق نموذجاً ، على الموقع: https://political_encyclopedia.org/library/1386

الاميري و العموش ، خالد علي محمد واحمد فلاح ، الامن الوطني المفهوم والابعاد والنظريات ، مجلة الاداب ، ملحق العدد (١٣٣) ، حزيران ٢٠٢٠ . على الموقع الالكتروني : https://www.researchgate.netpdf