مجلة الباحث
موقع المجلة: https://journals.uokerbala.edu.iq/index.php/bjh/

الهجمات السيبرانية على المؤسسات العراقية وانعكاساتها على قوة الدولة واستقرارها الامني و المؤسسي

م.م.حيدر عبدالله عباس
haiderabdullahalnasah@ec.edu.iqoman
وزارة التربية / مديرية تربية محافظة المثنى

التخصص العام للبحث :الجغرافية	التخصص الدقيق للبحث :الجغرافية السياسية

معلومات الورقة البحثية

الكلمات الرئيسية:

الهجمات السيبرانية ،الامن السيبراني ، الفضاء السيبراني ،الامن القومي ،الجريمة الالكترونية .

المستخلص باللغة العربية:

المستخلص :

بعد ما اصبح العالم قرية واحدة كما يعبر عنه ،و القرية هذه ترتبط بدورها بشبكة معلوماتية تحتوي على كم هائل من المعلومات ،سواء ما يخص معلومات المواطنين الشخصية ،او قاعدة بيانات الدولة بمختلف مؤسساتها ،وان هذه المعلومات قابلة للمشاركة ،او للأختراق ،وهي مرتبطة معاً ضمن شبكة الأنترنت نفسها ،فبالتالي لابد من وضع سبل حماية رقمية مواكبة للتقدم التكنلوجي ضمن الفضاء السيبراني للدول ،ليكون خط الصد والمدافع عن اختراق هذه المعلومات او العبث بها ، فالاهتمام بالأمن السيبراني ،اصبح ضرورة ملحة ،لحماية الانظمة والشبكات الخاصة بهذا الشأن ،وهو السبيل الوحيد لصد الهجمات الالكترونية والتهديدات التي تطال الامن القومي للدولة ،حتى لا يتم اختراقها ،و تسريبها ،والتلاعب بها من قبل المجرمين الالكترونيين (الهاكرز) ،خاصة بعدما تدخل الذكاء الاصطناعي كسلاح خارق ذو حدين ، ووسيلة سريعة ،يستعملها المجرمون الالكترونيون ،للوصل للمعلومات المستهدفة ،تحت اي ظرف ،وفي اي زمان ومكان ،مهددة بذلك امن الدول المستهدفة ،فالامن السيبراني ،اصبح جزءاً اساسياً ضمن سياسة الامن الوطني والقومي للدول ،حتى انه اصبح رمزاً لاستعراض امكانيات الدولة ،وسيادتها ضمن هذا الصعيد ،فلابد من اخذ الحيطة والحذر ،والعمل الجاد للدول ،التي لم تلتحق بالتقدم التكنلوجي وبشكل خاص الامن السيبراني ،بأن تولي اهمية كبيرة فيما يخص هذا المجال ،لكي لا تكون عرضة لأي خرق او هجوم ،او اي حرب الكترونية متوقعة ،مع المعرفة الكافية للتعامل مع هكذا ازمات ،والعراق من ضمن الدول التي بدأت تلتحق بمضمار التطور الالكتروني ،فيما يخص امن المعلوماتية للدولة والمواطنين ،لكن بخطى خجولة ومحدودة.

doi: https://doi.org/10.63797/bjh.

المقدمة :

لقد اصبحت قوة وسيادة الدول ،في الوقت الراهن، ليس بما تمتلكه من ترسانة عسكرية (جنود ، طائرات ، غواصات ، دبابات) ،او مصانع اسلحة وغيرها ،فأن هذه التجهيزات العسكرية ،وان كان لابد منها ، الا ان الحرب الهجينة ،والحرب الذكية ،قد قللت من قيمة الحرب التقليدية ،كما كانت في الحربين العالميتين على سبيل المثال ،اذ دخلت الدول ،في سباق محتدم بتطبيقها للتكنلوجيا الحديثة في مؤسساتها ،العسكرية منها ،والمدنية واصبح الفضاء

السيبراني، ساحة تتبارى فيها الدول ،وتستعرض قوتها ،ضمن مجال الامن السيبراني ، وكيفية حماية هذه الدول امنها القومي، وقاعدة البيانات الخاصة بها ،امام القوة السيبرانية المقابلة ،التي قد تحاول ان تعبث بأمنها ،وكيف لهذه الدول ،من ان تحمي ،او تواجه مرتكبي الجرائم الرقمية ،التي تستهدفها ،اذ اصبحت الحرب الآن ،اقل كلفة ،واسرع تنفيذاً ،وبأقل الخسائر ،حتى ان الآليات العسكرية المتطورة ، والصواريخ الحديثة ،هي بحد ذاتها ،معرضة للعطب والاتلاف ،من خلال هجوم سيبراني بسيط ،باعتبارها موجهة ،وتمتلك تكنلوجيا حاسوبية ذكية في اجهزة التشغيل الخاصة بها ،وقد يشل اي هجوم رقمي حركتها ،ويعطل (خوارزميات) التوجيه فيها ،كونها موجهة وعاملة بشكل الكتروني ،مما يجعلها من دون فائدة ،لتبرز بذلك اهمية ،وضرورة قصوى ،من ان تعمل الدولة على ،تحصين بناها التحتية الرقمية ،من هذه الهجمات ،مع اعطاء الاولوية في ذلك ،لقاعدة البيانات و المعلومات الحكومية المدنية ،منها والعسكرية ،فضلاً عن معلومات مواطنيها من الاختراق ،خاصة وان الجريمة الالكترونية العابرة للحدود وغير المقيدة ، اصبحت اكثر انتشاراً واسرع تنفيذاً ،وبالتالي كلها تنعكس على الامن القومي للدولة وسياداتها .

المبحث الاول

مفهوم الفضاء السيبراني والامن السيبراني

مع تزايد انتشار استخدام الحواسيب ،وانتشار شبكة الانترنت حول العالم ،ظهرت الحاجة الملحة ،الى حماية المعلومات في مؤسسات الدولة كافة من التهديدات السيبرانية ، وكانت البداية عندما ظهرت الفايروسات والبرامج الضارة بالاجهزة الحاسوبية ، ومنذ ذلك الحين اصبحت تهديدات الامن السيبراني ،اكثر تعقيداً ،وهنا بدت الحاجة الى ظهور استراتيجيات متطورة ،تتعلق بأمن المعلوماتية ، كما في دمج الامن السيبراني في التخطيط الاستراتيجي للدولة ، مع تدريب متخصصين لمراقبة التهديدات ،اذ ان الانتشار الواسع للجريمة السيبرانية ،ادى بالنتيجة الى ،رفع الوعي من اهمية وجود اطر قانونية ،تحمي المواطنين ومعلوماتهم الحساسة ،فضلاً عن معلومات وبيانات الدولة التي تخص امنها القومي وسيادتها ،لا سيما وان المهاجمون ،يستفادون من وجود ثغرات في الانظمة الالكترونية ،فهنا لابد للدولة من ان تعزز استراتيجية التخفيف من الاخطار المحدقة في فضاءها السيبراني ، والحرص على انشاء هياكل وانظمة امنية جديدة تتوافق مع التحديات والجرائم والهجمات الالكترونية المتطورة باضطراد (علاء عبد الخالق حسين وآخرون ، 2024 ،ص13).

اولاً : الفضاء السيبراني

مصطلح يشير الى البيئة الافتراضية ،التي تنشا من ،تفاعل شبكات الحواسيب والانظمة الرقمية ،اذ يتم تبادل المعلومات ، والبيانات بين المستخدمين والاجهزة بشكل غير محدود ،وهو لا يتطلب وجوداً مادياً حقيقياً ،بل يعتمد على البنية التحتية ،العاملة على شبكة الانترنت حول العالم ،ومن مميزاته ، قابليته على تجاوز الحدود الجغرافية والزمنية كذلك ، ما يجعله وسيلة من الوسائل الاساسية، للتعامل فيما بين المستخدمين ، لينفذون من خلاله الكثير من الانشطة منها ، التجارية ، والتعليمية ، والترفيهية ، وهو يشكل منصة لظهور تقنيات حديثة ،مثل برامج الذكاء الاصطناعي ، وانترنيت الاشياء ،التي تعزز من تداخل الحياة اليومية للمستخدمين مع عالمهم الرقمي ،وهو في الوقت ذاته ،يشكل تحديات كبيرة فيما يتعلق بأمن المعلومات ،وخصوصية الافراد والمؤسسات ،حيث ان التوسع الكبير ،في استخدامات المنصات الرقمية ،والاجهزة الالكترونية المرتبطة بشبكة الانترنت ،ادى الى ازدياد مثل هكذا هجمات ،والتهديدات التي تطال الامن السيبراني ،الذي يعد جزءاً رئيس من الفضاء السيبراني للدول(سيناء علي محمود ،2025 ،ص 315).

ثانياً : العناصر الرئيسة التي يتكون منها الفضاء السيبراني

هنالك عدة عناصر تمثل بمجمعها الفضاء السيبراني (محمد كاظم عباس المعيني،2025 ،ص83) :

1- الاتصال والتفاعل البشري بأشكاله ،الرسمية وغير الرسمية جميعها ، ومستوياته المختلفة (السياسية ، التجارية ، القانونية وغيرها) ،ونتاج ذلك على شبكة الانترنت .
2- المجتمع الرقمي ،بجميع خصائصه ،وابعاده اللامتناهية ،واتجاهاته ،وطبيعته الافتراضية .
3- الفرد الرقمي (العاملين على شبكة الانترنت)، كشخص عامل على الفضاء السيبراني ،ذات الخصائص الجماعية الافتراضية القائمة على التواصل والحوار .
4- العقل الجمعي الرقمي ،الناتج من تفاعل العقول الفردية الافتراضية ،داخل العالم الافتراضي الموجه الشمولي، لحركة وتدفق المعلومات داخل مجتمع الانترنت .

بما معناه ،ان اي عمل جاد وخطط تطوير ،ترسمها الدولة لرفع مستوى اداء امنها السيبراني ، عليها الاخذ بالحسبان ،هذه العناصر ،وان الحكومة العراقية ،بدأت بالفعل بالعناية بهذا الجانب ،من خلال ،تطوير الافراد العاملين على الاجهزة الالكترونية في المؤسسات العراقية ،وكذلك فتح اقسام علمية من معاهد وكليات تعنى بهذا الشأن ،في خطوات صحيحة نحو حماية وتحصين امن الدولة .

ثالثاً: مفهوم الامن السيبراني

ان كلمة (cyber) اي سيبراني ،تطلق على كل متعلقات الشبكة الحاسوبية الالكترونية ،وشبكة الانترنت، اما كلمة (Cyberspace)،فتعني الفضاء الالكتروني ،وهو يعنى بكل ما يتعلق بشبكات الحاسوب والانترنت ،كذلك التطبيقات الالكترونية المختلفة مثل (facebook، WhatsApp) على سبيل المثال ،وهناك غيرها من التطبيقات التي لا تعد ولا تحصى ،فضلا عن شمول هذا المصطلح ما يتعلق بـ (تحويل الاموال الكترونياً ،والبيع والشراء الكترونياً) وغيرها، الكثير من الخدمات التي يعمل عليها المستخدمون حول العالم (علي عبد الخضر محمد ، 2024 ،ص335 - 336).

ومن الممكن تعريف الامن السيبراني بأنه : النشاط او العمل و القدرة على التحكم في نظم المعلومات واتصالات الدولة ،حيث تكون المعلومات الواردة فيه محمية من التلف ،والاستعمال غير المصرح به للتعديل او الاستغلال ،او يعرف كذلك بانه : مجموع الوسائل التقنية ،والتنظيمية ،والادارية ،التي يمكن استعمالها لمنع الاستخدام غير المصرح به ،وسوء الاستغلال ،واستعادة المعلومات التي يحتويها ، وذلك بهدف ضمان استمرار عمل نظم المعلومات ،وتعزيز سرية البيانات الشخصية ،وخصوصيتها ،واتخاذ التدابير اللازمة لحماية المواطنين من الجرائم الالكترونية ،وكذلك يمكن تعريفه من الناحية الالكترونية بأنه : ادارة وحماية شبكات الكومبيوتر ،والمعلومات التي يحتويها من الاختراق او التدمير او التوقف (تامر سعيد عبد اللطيف ، 2025 ،ص268).

ويعرف ادوارد امورسو صاحب كتاب الامن (السيبراني) ،الذي اصدره عام 2007 بانه " مجموعة من الوسائل والاجراءات ،التي بإمكانها الحد من مخاطر الهجوم والتهديد على الشبكات وانظمة الحاسوب " ،فهو بالتالي عملية للدفاع عن اجهزة الحاسوب ،وما تحويه من بيانات ،من الهجمات المنظمة (الهجمات السيبرانية) ،كونه يعد من التحديات التي تواجه الامن القومي للدول ،وتأثيره بالتالي على الامن والسلم الدوليين ،اذ انه وبحسب الاحصائيات التي قدمها المعهد الدولي للدراسات الاستراتيجية في لندن ،انه توقع وصول حجم تكلفة الخروقات السيبرانية ،الى حوالي (10.5) ،ترليون دولار في العام الحالي (2025) ،لذا فان الهدف الرئيس للأمن السيبراني ،هو تعزيز قدرة الدولة على مواجهة التهديدات التي يتعرض لها الفضاء السيبراني بشكل عام ،والامن القومي للدولة بشكل خاص ،وفي هذا الصدد ،تجد بان الدول العظمى كالولايات المتحدة الامريكية ،وروسيا ،والصين ،قد خصصت ميزانيات ضخمة ،ووضعت منظومات حديثة من شانها العمل على مواجهة التهديدات والجرائم السيبرانية (زينب ضياء محمد ،2025 ،ص968)، فلابد لكل دولة من دول العالم ، بما فيها العراق من ان تلتحق بركب المتنافسين في التطور والتسلح الالكتروني والسيبراني ،لكي لا تصبح ضحية الهجمات والاختراقات الالكترونية تارة ، ومن اجل التقدم في التصنيفات الدولية التي تخص امن الدول السيبراني تارة اخرى .

رابعاً : اهمية الامن السيبراني

لابد لكل دولة ان تولي اهتماماً كبيراً بمجال امنها السيبراني ،لا سيما وان البيانات الخاصة بمواطني دولة ما ،وبيانات مؤسسات هذه الدولة ،اصبحت بشكل تلقائي موجودة على اجهزة الحاسوب المختلفة ، وان غالبية هذه الاجهزة متصلة بشبكة الانترنت ،اي انها مهددة بأن تخترق في اي لحظة ، من قبل المغرضين ،او خبراء الهجمات الالكترونية في حال النزاع بين دولتين ، او حتى التجسس على بيانات ،ومعلومات امنية عسكرية وسياسية تخص الامن القومي لدولة ما ،وان هذا بجملته اعطى اهمية للأمن السيبراني ، التي من الممكن ايجازها بالنقاط التالية (منى عبدالله السمحان ،2020، ،ص12- 13):

1- الحفاظ على المعلومات وسلامتها من العبث بها ،فضلاً عن جعل هذه البيانات ،جاهزة في حالة الحاجة لها .
2- حماية الشبكات والاجهزة ، من الاختراقات والجرائم الالكترونية ،حتى تكون سداً منيعاً للبيانات التي تحويها هذه الاجهزة .
3- العمل على كشف نقاط الضعف والثغرات في الانظمة ومعالجتها .
4- توفير بيئة آمنة ومحصنة ، خلال العمل عبر الانترنت .

خامساً: ضوابط الامن السيبراني

لتحسين الامن السيبراني هنالك عدة ضوابط تتمثل بالتالي (رأفت عاصي حسين ورغد خير الدين صبري ، 2025،ص143) :

1- استخدام جدار حماية لتأمين الانتماء الخاص بالافراد .
2- اختيار الاعدادات الاكثر اماناً للأجهزة والبرامج الشخصية .
3- التحكم في من يمكنه الوصول الى البيانات (الشخصية) ذات العلاقة بالفرد نفسه .
4- توعية المستخدمين بحماية اجهزتهم الالكترونية، من الفايروسات والبرامج الضارة الاخرى .
5- الحفاظ على تحديث الاجهزة وبرامجها بشكل مستمر .

سادساً : خصائص الامن السيبراني :

يمكن تحديد خصائص الامن السيبراني بالنقاط التالية (زينب ضياء محمد ، 2025 ،ص968) :

1- مفهوم شامل وواسع وهو قابل للتغيير ،وفق المستحدثات التي تطرأ عليه .

2- فيه العديد من الفاعلين ، كالدول او الشركات المتعددة الجنسية ،او المنظمات باختلاف اختصاصاتها او التنظيمات الارهابية .
3- يتمتع بخاصية مواكبة التطورات والتغيرات التي تطرأ على النظام الدولي بشكل عام .
4- هو فضاء واسع وغير محدد وهو يضم خصوم متعددة .
5- يضم (الجرائم السيبرانية) و هنالك امكانية فيه لخلق حروب سيبرانية معقدة .
6- ممكن عده من اخطر المفاهيم الحديثة التي تواجه الدول ،لما له من امكانية التسبب بالاضرار ،بما فيها خرق النظام الامني والمؤسسي للدولة .

سابعاً : اهداف الامن السيبراني

حتى تكون بيانات ومعلومات الافراد والحكومات بمأمن عن الهجمات السيبرانية ،والجرائم الالكترونية ،يجب ان تحقق في امنها السيبراني هذه الاهداف (منى عبدالله السمحان ،2020 ،ص12):

1- تعزيز حماية انظمة التقنيات التشغيلية على كافة الاصعدة ،ومكوناتها من اجهزة وبرمجيات ، وما تقدمه من خدمات ، وما تحويه من بيانات .
2- التصدي لهجمات وحوادث امن المعلومات التي تستهدف الاجهزة الحكومية ،ومؤسسات القطاع العام والخاص .
3- توفير بيئة آمنة وموثوقة ،للتعاملات في مجتمع المعلومات .
4- صمود البنى التحتية الحساسة للهجمات الالكترونية .
5- توفير المتطلبات اللازمة للحد من المخاطر ،والجرائم الالكترونية التي تستهدف المستخدمين .
6- التخلص من نقاط الضعف ،في انظمة الحواسيب الآلية على اختلافها .
7- سد الثغرات في انظمة امن المعلومات .
8- مقاومة البرمجيات الخبيثة ،لكي لا تلحق اضرار بالغة .
9- الحد من التجسس ،والتخريب الالكتروني ،على مستوى الافراد والحكومات .
10- اتخاذ التدابير اللازمة لحماية المستخدمين ،حتى لا تخترق اجهزتهم والاضرار بالبيانات الخاصة بها ،او محاولة اتلافها او تسريبها .
11- تدريب الافراد على مواجهة التحديات الخاصة بالهجمات ،والجرائم السيبرانية المحدقة .

المبحث الثاني

الهجمات السيبرانية و الجرائم الالكترونية تعريفها خصائصها

تلك الهجمات التي يتم من خلالها استخدام الاسلحة الالكترونية ،من اجل التهديد ،او احداث اضرار منها مادية ،او الكترونية ،وهي تختلف من حيث قوتها وتعقيدها ،حيث تتراوح ما بين اسلحة بسيطة ،قادرة فقط على احداث ضرر خارجي بالنظام الالكتروني ،من دون ان تخترقه ،اما الاخرى فهي معقدة ،اذ يمكن من خلالها اختراق النظام المستهدف ،والحاق ضرراً بالغاً فيه ،تصل في بعض الاحيان الى ان يدمر كلياً ،وقد يتوقف عن العمل ،وان الهجمات الالكترونية ،تتم بأستخدام آليات وشبكات الحاسب الآلي ،المرتبط بالانترنت ،وهي تلحق الضرر بهذه الاجهزة ،من خلال اختراق قاعدة بياناتها وسرقة المعلومات فيها ،و قد تتعرض اهداف الكترونية الى هجمات غير الكترونية ،كما في الهجمات الحركية ،او المادية ،او الهجمات الكهرومغناطيسية ،وهي تؤدي بطبيعة الحال الى احداث الضرر بها ،وربما توقفها عن العمل وبشكل نهائي (علي عبد الخضر محمد ، 2024، ص337) ، كما في جدول (1) الذي يبن انواع التهديدات السيبرانية ودوافع واهداف منفذيها .

جدول (1) انواع التهديدات السيبرانية ودوافع واهداف ومنفذيها

ت	التهديدات السيبرانية	اصناف منفذي التهديدات	الدوافع	الاهداف
1	القرصنة	الافراد المتسللون (الهاكرز)	السمعة والانانية السياسية	احداث الاضطرابات ولفت الانتباه
2	الجريمة السيبرانية	الجواسيس وصناع الجريمة المنظمة	المعلومات الاقتصادية	البيانات التنظيمية للأصول الرقمية
3	التجسس الالكتروني	الجواسيس وصناع الجريمة الحكومية المنظمة	الايديولوجية الاعلامية والسياسية	البيانات التنظيمية المعرفية للأصول الرقمية

4	الارهاب الالكتروني	الحكومات الارهابية	الايديولوجية السياسية والدينية والاجتماعية	اضطرابات المنظمات الوطنية والبنى التحتية الحرجة
5	الحرب الالكترونية	الحكومات الارهابية	الانانية السياسية والدينية والاجتماعية	اهداف عسكرية وطنية نافذة

المصدر : من عمل الباحث ،بالاعتماد على رأفت عاصي حسين ورغد خير الدين صبري ،مدى جاهزية المنظمات لإقامة ابعاد الامن السيبراني دراسة تحليلية لآراء عينة من العاملين في البنك المركزي العراقي فرع الموصل ،مجلة العلوم الادارية والانسانية ، الجامعة التقنية الشمالية ،المجلد (5) ، العدد (2)،ص143 .

بعد تغيير النظام السياسي في العراق بعد عام 2003 ،حدثت تغييرات جذرية ،طالت غالبية مؤسسات الدولة مثل اتمتة وحوكمة البيانات والمعلومات في غالبية مؤسسات الدولة ، حيث ان دول العالم قد سبقت العراق بمراحل في هذا المجال ،فبدأ التحول واصبح انجاز المعاملات وبيانات المواطنين في غالبيتها الكترونياً ،انطلاقاً من البطاقة الوطنية ،فالبطاقة التموينية وبيانات السيارة ،من اجازة القيادة او السنوية و متعلقاتها، او اصدار الجواز ،وصولاً الى المعاملات الصغيرة ، كما في التقديم على الكليات بالنسبة لخريجي الدراسة الاعدادية ،او فيمن يروم التقديم على الوظيفة الحكومية ،او حتى غير الحكومية ، وهذه بمجملها تتطلب البيانات الشخصية للمواطن العراقي ،وتفاصيل ومعلومات الشخص وعائلته ووظيفته ومكان سكنة ورقم الهاتف الخاص به ،وبما ان كل هذه المعلومات تكون محملة على اجهزة الكومبيوتر ،او الهاتف الشخصي ،وان هذا الجهاز الالكتروني من الطبيعي يكون متصلاً بشبكة الانترنت العالمية ، فأنه من الممكن الوصول اليها في اي زمان ومن اي مكان ،سواء بالوصول الرسمي الاصولي ،او من خلال اختراق الكتروني ،متمثلاً بالهجمات المذكورة في جدول (1) ، هذا فيما يخص امن المعلوماتية للفرد ،وان هذه الآلية المذكورة هي بذاتها الآلية التي تتبعها مؤسسات الدولة كافة ،كما في المؤسسات الامنية كوزارة الداخلية او الخارجية او المؤسسات الامنية الاخرى ،التي هي بدورها تدرج بياناتها ومعلوماتها ،على اجهزتها الالكترونية ،وبالتالي فهي ايضاً معرضة الى الاختراق والهجوم الالكتروني وعلى مستوى الدولة وامنها القومي ،فعند الوصول الى بيانات وزارة الدفاع على سبيل المثال اعداد (الآليات العسكرية – الصواريخ – الجنود – التحركات الامنية – الخطط العسكرية – ساعة الصفر لبعض التحركات والعمليات الامنية داخل وخارج العراق) ،كلها بيانات ومعلومات من المفترض ان تكون سرية ،حتى تؤتي نتائجها كاملة ،من دون ان يتم تسريبها وافشالها قبل التنفيذ ،وبالتالي تكون بيانات الدولة وامنها السيبراني متهيئاً ،لأي سيناريو متوقع ،وان ما حدث ان العراق على مر السنين المنصرمة ،قد تعرض لجميع انواع التهديدات المذكورة في الجدول (1) ،كونه لم يكن فضاءه السيبراني ، وامنه السيبراني على القدر من الحصانة والقوة .

اولاً : خصائص الهجمات والجرائم السيبرانية

الجريمة الالكترونية وان كانت تحمل عنوان (جريمة) ،الا انها تحدث عبر الاجهزة الالكترونية المختلفة ،وعلى يد مستخدمين غير معروفين ،ولها خصائص تميزها عن الجرائم التقليدية ، تتمثل بالآتي (زينب ضياء ،2025 ،ص970) :

1- انها هجوم رقمي غير تقليدي بعيد المدى ، يستهدف الاجهزة التقنية والتكنلوجية الحديثة وبرامجها وبياناتها .
2- هجمات غير محددة الاهداف ،فهي تتعدى مخاطرها ساحات القتال التقليدية ،فهي تمس مؤسسات الدولة الحساسة وتهدد امنها القومي وسيادتها .
3- تتصف بالسرعة ، ولها امكانية المناورة ،حيث تعطي بذلك المهاجم افضلية واضحة .
4- تشكل خطراً على البنى التحتية ،فهي تستهدف الافراد ،والحكومات على حد سواء .
5- تتطلب استراتيجية خاصة لمكافحتها ،كما وتتطلب تكنلوجيا متقدمة ،ومؤسسات محصنة .

ثانياً : تصنيف الهجمات السيبرانية

تختلف الهجمات السيبرانية من حيث درجة الخطورة ،والاضرار التي تسببها ،فمن الممكن تصنيف الهجمات السيبرانية الى (احمد عبد الكريم عبد الوهاب ومحمود عبد الرحمن خلف ،2020 ،ص6) :

1- الهجمات السيبرانية الدولية : حيث تشمل كل تهديد يستهدف الامن القومي ،العسكري ، الاقتصادي ، الاجتماعي ،او يهدد بنى الدولة التحتية اجمالاً ،وسوق المال ، والقطاعات المصرفية ،والمؤسسات الصحية ، والمنشآت النووية ،وقطاع النقل بكل صنوفه سواء كان النقل برياً ام بحرياً ام جوياً ، وكذلك تهدد هذه الهجمات الامن والسلم الدوليين بشكل عام .
2- الهجمات السيبرانية الشخصية :وهنا تستهدف هذه الهجمات الافراد ،من قبيل ،البيانات الشخصية حيث العبث بها وتسريبها واستخدامها دون اذن ،وكذلك سرقة الاموال ،واختراق انظمة المعلومات ،والاعتداء على الملكية الفكرية ، والصناعية ، والعلامات التجارية ،وتشمل كذلك عمليات الاحتيال ، وارسال البريد الغير مرغوب فيه ،والجرائم ضد الاطفال ،والمحتوى غير الاخلاقي ،وهي بجميعها تتجه صوب الافراد .

ثالثاً : الاسباب والعوامل التي تؤدي الى تزايد الهجمات السيبرانية

كلما يتقدم الزمن ،تتقدم معه التكنلوجيا بمختلف اصنافها ،بما فيها تكنلوجيا الحاسوب والانترنت (الفضاء السيبراني) ،مما جعل المستخدمين كذلك تزداد اعدادهم ،ومع تطور ادوات الذكاء الاصطناعي تتطور عمليات دخول المستخدمين ،الى فضاءات الشبكة العنكبوتية ،وبهذا ازدادت عمليات الاختراق والعبث الالكتروني ،ممن يستخدم الشبكة بغير هدف ،او من خلال العبث ببيانات الآخرين والاضرار بهم ،او قد يكون العابث (الهاكرز) يعمل بأجر ،او يتبع الى حكومات بعض الدول بشكل خفي ،وان هذه الزيادة في اعداد الهجمات والمهاجمين تعزى الى الاسباب الآتية (سيناء علي محمود ، 2025 ،ص317 – 318):

1- تزايد ارتباط العالم بالفضاء السيبراني ،اذ اصبح الفضاء السيبراني العمود الفقري للتواصل العالمي ،وكذلك ادارة البنى التحتية كافة ،مما جعلها اكثر عرضة وسهولة للمهاجمين ،لتحقيق اهداف عدائية وتخريبية .
2- تراجع دور الدولة ،اذ ان انسحاب دور الدولة من بعض القطاعات الاستراتيجية ،وتصاعد دور الشركات ،وخاصة العاملة في مجال التكنلوجيا ،جعلها فاعلاً رئيس في الفضاء السيبراني ،واحياناً تتحكم به الشركات بقدراتها التي تفوق ما تمتلكه الدول احياناً ،مما قلل من سيطرة بعض الحكومات على فضائها السيبراني .
3- الاعتماد المتزايد على الانظمة الالكترونية ،فالدول اصبحت تعتمد بشكل كبير على الانظمة الالكترونية في جميع مؤسساتها ، بما فيها القطاعات الخدمية ،والبنوك والقطاع العسكري ،مما جعلها عرضة للهجمات السيبرانية التي من الممكن ان تلحق اضرار جسيمة في الدولة ، بالخصوص في اوقات النزاعات .
4- التكلفة المنخفضة للهجمات الالكترونية ،فيما لو قورنت بالحرب او الهجمات التقليدية ،التي تتطلب موارد مادية وبشرية ، بطبيعة الحال ،بينما الهجوم الالكتروني لا يحتاج الى ذلك القدر ولا تلك المدة الزمنية ،التي تحتاجها الحروب التقليدية .
5- الحروب السيبرانية كأداة للتأثير على المعلومات ،فهي تؤثر على المعلومات المستخدمة في مختلف مراحل الصراع ، على المستوى التكتيكي والاستراتيجي ،حتى تؤثر سلباً على دقة المعلومات ،او تعطيل انظمة التشغيل فيها ،مما يضعف قدرات الدولة المستهدفة بالهجوم .
6- تعظيم القوة الوطنية من خلال الفضاء السيبراني ،وذلك من خلال تحقيق تفوق استراتيجي او تأثير مباشر على البيانات المختلفة ،والعسكرية منها او الاقتصادية ،مما اظهر بما يسمى (الاستراتيجية السيبرانية) ،باعتبارها عنصراً اساسياً في امن الدولة وقوتها .
7- اتساع نطاق الانشطة العدائية في الحروب والهجمات السيبرانية ،فأنها لم تعد تقتصر على الدول فقط ،بل اصبح الفضاء السيبراني بيئة متاحة للفاعلين غير الحكوميين ،كما في القراصنة الالكترونيين ،او ما يسمى (الهاكرز) ،حتى انه احياناً تستخدم الدول هؤلاء ،كأداة لشن هجمات ضد الخصوم ،ومن دون ارتباط رسمي ،وهذا بدورة يخلق صعوبة في تحديد من المسؤول عن الهجمات .

رابعاً : الهجمات السيبرانية و الارهاب الالكتروني

لقد عرفت وزارة الدفاع الامريكية الارهاب الالكتروني بأنه " عمل اجرامي يتم الاعداد له باستخدام الحاسبات ،ووسائل الاتصالات ، ينتج عنها عنف، او تدمير، او بث الخوف تجاه تلقي الخدمات بما يسبب الارتباك وعدم اليقين ، وذلك بهدف التأثير على الحكومة او السكان ، لكي تمتثل لأجندة سياسية او اجتماعية او فكرية معينة " ،وفيما يخص الارهاب الالكتروني في العراق ،فهو لا ينحصر بشاكلة واحدة فقط ، فهو يبدأ من الجرائم الالكترونية باستخدام الانترنت ،كنوافذ للتخطيط والتنفيذ ،وصولاً الى جرائم تخص الاتجار بالبشر ،ثم تجارة المخدرات ،حتى ارتكاب الجريمة المنظمة ،والقرصنة الالكترونية ،وجرائم انتحال الشخصيات ،وجرائم الاحتيال المالية ،وتزوير البيانات ،حيث تعد هذه الجرائم منتشرة في العراق بشكل واسع ،ان جميع هذه الجرائم والهجمات الالكترونية ،لها آثار وخيمة تكون كفيلة بتدمير مؤسسات الدولة وانهيارها(رعد خضير صليبي ، 2024، ،ص514 - 515) .

حيث ان هذه الهجمات تعد من ابرز المخاطر التي تواجه البنى التحتية للحكومات ،وهنا تحتاج هذه الحكومات الى تطوير طرائق حديثة للمراقبة والرد على هذه الهجمات والتهديدات ،فينبغي ان تتضمن ادوات حديثة ،تساعد في مواجهة كل السيناريوهات المحتملة ، ففقدان البيانات او خرق الانظمة ، يمكن ان يؤدي الى نتائج سلبية ،مثل فقدان ثقة المواطن بحكومته ، او يتم من خلالها تعطيل الخدمات الاساسية في الدولة ،وهذا كله يستدعي انشاء طرائق لتقييم ومراجعة دورية ،لحماية تلك الانظمة من التهديدات المتزايدة ،اذ ان الابحاث تظهر ان مركزية الانظمة ،وضعف حماية الشبكات يزيدان من التعرض لمخاطر الهجمات السيبرانية ،فمن المهم جداً اتباع تقنيات جديدة لتعزيز الدفاعات ، والاستثمار الجدي في الابحاث المتعلقة بأمن المؤسسات الالكتروني ،فضلاً عن تطوير مهارات الموظفين الرقمية لمواجهة هذه التهديدات ،اذ ان هذا التحدي يعد من التحديات الاساسية لبناء بيئة تحتية رقمية آمنة ومستدامة ،تستطيع حماية الدولة وامنها القومي (علاء عبد الخالق حسين وآخرون ،2024 ،ص 39 – 40) ،وهنا يحتاج العراق الى تعزيز الجهود التي ترمي الى تطوير فضاء الدولة وامنها السيبرانيين ،وتخصيص الميزانيات التي تستوعب ادخال التحديثات اللازمة للبنى التحتية والافراد العاملين في المؤسسات التي تعنى بأمن الدولة السيبراني ،والحفاظ على قاعدة البيانات الحكومية وغير الحكومية وحفظها من السرقة او الاختراق او اي هجوم .

خامسا : تأثير الامن السيبراني على قوة الدولة واستقرارها الامني و المؤسسي

ان من اهم ابعاد الامن السيبراني ،انه يمثل العامل الاساس في الحفاظ على المرافق الامنية المهمة في اركان الدولة ،وذلك عبر تأمين الاتصال بين هذه المؤسسات ، بما يسهل من تبادل المعلومات وتبادل الاوامر فيما بينها لتسهيل العمل ،وانجاز المهام بأسرع وقت ،ومن اجل هذا فأن تطوير شبكات الانترنت ،في جميع اركان الدولة ، بات امراً ضرورياً ،فهي تعد نقطة ضعف اذا كانت غير مؤمنة ومحصنة ، لمنع اختراقها او تدميرها او الاعتداء من خلالها على مختلف المؤسسات ، ما يؤدي الى تدمير البيانات الخاصة بالدولة وامنها القومي ككل ، او كما يحدث في قطع الاتصال فيما بين هذه المؤسسات ، خاصة العسكرية منها ،وما يتعلق بالتحكم اللاسلكي بالاسلحة الحديثة و المتطورة ،في حال خروجها عن السيطرة ، كما في الصواريخ الموجهة ، او الطائرات بدون طيار ، وغيرها من الاجهزة الحديثة ، حيث انها غالباً ما تكون متصلة بوسائل الاتصال الحديثة ، وشبكات الانترنت ، وقاعدة البيانات العسكرية ،وحتى المدنية ،وفيما يخص معلومات الافراد مواطني الدولة كذلك ،وهذه تمكن مستخدمها من التحكم بها عن بعد ،وان قاعدة البيانات هذه ،تعد من اخطر الابعاد تأثيراً على الامن القومي لأي دولة في العالم ، بالنظر لما تحويه من معلومات حساسة رقمية والكترونية تخص جوانب مهمة ، مثل الجانب العسكري والنظام المصرفي والتجاري ،وبيانات المواطنين ، فن هذا المنطلق بدأت العديد من الدول بادخال الفضاء السيبراني ضمن استراتيجيات الاهتمام بأمنها القومي ،حيث دفعت الهجمات السيبرانية ، العديد من الدول على بذل المجهود الحقيقي ،للعمل على حفظ امن الدولة وفضائها السيبراني ،من خلال انشاء هيئات متخصصة لمواجهة الهجمات السيبرانية ،وكذلك استحداث قوانين حديثة في سبيل مكافحة الجريمة السيبرانية ،وانشاء قيادة عسكرية لحماية هذا الفضاء ،وكذلك استحداث وحدات خاصة لتحسين القدرات الامنية بالضد من الهجمات السيبرانية التي تتعرض لها (ياور عمر محمد ،2025، ص224).

المبحث الثالث

مركز العراق في مؤشر الامن السيبراني العالمي ،ومدى كفاءة مؤسساته امام الهجمات السيبرانية

ان غالبية الدول بدأت العمل منذ زمن ليس بقريب ،على الدخول في عمليات تطوير بناها التحتية والمؤسسية سيبرانياً ، حتى تلحق بركب الدول الرائدة في هذا المجال ،اذ اصبحت قوة وهيبة الدولة في المحافل الدولية تقاس بمدى سعيها في تحصين امنها الالكتروني ، فضلاً عن حماية قاعدة بياناتها ،وبيانات مواطنيها ،من الاختراق الالكتروني ،لا سيما المؤسسات العسكرية والامنية التي تخص امن الدولة القومي وكيانها واستقلالها .

اولاً : مركز العراق وفق تصنيف المؤشر العالمي للأمن السيبراني (Global Cybersecurity Index – GCI)

يقيس هذا المؤشر مدى التزام الدول بحماية الفضاء السيبراني من الهجمات والاختراقات، وهو يصدر عن الاتحاد الدولي للاتصالات (ITU) ، فهو يعكس مدى حماية بيانات المواطنين والبنية التحتية المعلوماتية اومن الدول السيبرباني، و يساعد في وضع سياسات وطنية فعّالة للأمن الرقمي ،و يقيس أداء الدولة وفق خمسة مجالات او ركائز رئيسة تتمثل بـالتدابير الآتيــة (Global Cybersecurity Index ,2024 ،p74) :

- التدابير والاجراءات القانونية
- التدابير والاجراءات التقنية او الفنية
- التدابير والاجراءات التنظيمية او المؤسساتية
- بناء القدرات (التعليم والتدريب)
- التعاون ،الاتفاقيات مع الدول والمنظمات

وقد جاء تصنيف العراق في مؤشر الامن السيبراني في المرتبة (159) ،وفق تصنيف المؤشر لعام 2017 ،ومن ثم احتل التصنيف (107) عالمياً ،في عام 2018 ،اما في عام 2019 ،فجاء في المرتبة (147) عالمياً، ليحصل بعدها على المركز (107) عالميا وفق مؤشر عام 2020 ، اما في العام 2021 فقد اصبح في المرتبة (129) عالميا ،من مجموع (194) دولة ،محققاً نتيجة اجمالية بلغت (20.71) ، جدول (2) .

جدول (2) يبين المركز الذي حققه العراق في مؤشر (GCI) لعام 2021

الاجراءات القانونية	الاجراءات التقنية	الاجراءات التنظيمية	بناء القدرات	اجراءات التعاون	النتيجة الاجمالية
صفر	6.56	7.75	2.14	4.26	20.71

المصدر : , international Telecommunication Union , Global Cybersecurity Index ,2024 Geneva :ITU ,Retrieved from ,https://www.itu.int,p74

اما في عام 2023 فقد حقق المركز (107)، وفي آخر نسخة من تقرير (GCI) ،الصادر عام 2024 ، فجاء العراق في المرتبة (127) عالمياً ،من أصل (193) دولة ،اذ تحصل في النتيجة الاجمالية على درجة 53,07% ،وهي نتيجة لا بئس بها فيما لو قورنت بنتائج الاعوام (2017 - 2019)، اما في الترتيب الخاص بالفئات ، فقد جاء العراق ضمن المستوى الرابع من أصل خمسة فئات ، جدول (3)، ويعتمد هذا المؤشر في تقييمه لـ (193) دولة ،عضواً في الاتحاد الدولي للأتصالات والامن السيبراني ،وهذا يدل على ان العراق يسير في الطريق الصحيح نحو بناء امنه السيبراني ،لمنه بحاجة الى تعزيز الاجراءات الخمس التي يعتمد عليها المؤشر ، وهنا يبين الجدول ،بأن العراق حصل في خانة الاجراءات القانونية على درجة (11.21) ،في اشارة الى ان العراق يخطو خطوات جيدة فيما

جدول (3) يبين المركز الذي حققه العراق في مؤشر (GCI) لعام 2024

الاجراءات القانونية	الاجراءات التقنية	الاجراءات التنظيمية	بناء القدرات	اجراءات التعاون	النتيجة الاجمالية
11.21	9.6	15.77	8.38	8.11	53.7

المصدر : international Telecommunication Union , Global Cybersecurity Index ,2024 , Geneva :ITU ,Retrieved from ,https://www.itu.int,p72

، الامور التشريعية والتنظيمية ، ضمن فضاءه السيبراني ،اما الاجراءات الاضعف ، فهي التي تخص بناء القدرات ،وهي دلالة على ان العراق بحاجة لتعزيز القوى البشرية ،(كالبحث العلمي ، التعاون الدولي ،المشاركة في الاتفاقيات الدولية ، المتعلقة بالأمن السيبراني) ،وقد اشار التقرير في مجمله ، ان العراق في مرحلة انتقالية ، فهو يمتلك بينة مؤسسية تشريعية ، الا انه لم يحقق التكامل فيما بين الجوانب التقنية ،والتنظيمية ،والتعاون العالمي ،بحسب مؤشرات التقرير ، اما بالنسبة لنسخة عام 2022 فلم يدرج العراق في هذه النسخة .

ومن الجدير بالذكر ان العراق انشأ عام 2017 ،فريق استجابة الحوادث السيبرانية ،وكذلك تم اعداد سياسات عامة للأمن السيبراني ،عام 2020 ، كما اصدر استراتيجية للأمن السيبراني ،من قبل مستشارية الامن الوطني ،متمثلة بفريق الاستجابة للحوادث السيبرانية (Cert) ،للتعامل مع الامن العراقي السيبراني ،وفحص الثغرات ،وتقييم المواقع الحكومية من الناحية الامنية ،الى جانب حماية البنية التحتية للانترنت ،والمواقع الرسمية ونشر الوعي الالكتروني ، وحماية ودعم الفضاء السيبراني العراقي ،ليعزز بذلك ثقة المواطن بمؤسسات الدولة ،وهو كذلك يعمل على الاستجابة للحوادث الامنية ،وتلقي البلاغات من الحوادث السيبرانية (عباس فاضل علوان ، 2025،ص38 – 39)، وكذلك تم تأسيس مديرية الامن السيبراني في العراق تابع لوزارة الداخلية العراقية ، بتاريخ 2022/12/4 ، تعنى بمجالات الامن السيبراني ،وترتبط بمكتب الوزير ،وتعمل على تعزيز جهود وزارة الداخلية، في بناء منظومة فعالة للأمن السيبراني ،ويهدف الى تطويرها وتنظيمها لحماية الوزارة من تهديدات الفضاء السيبراني ، ومواجهتها بكفاءة ،بما يضمن استدامة العمل ،والحفاظ على الامن الوطني ،وسلامة بيانات ومعلومات المؤسسات والافراد (Cybersecurity@moi.gov.iq ،2024) ،وكذلك تم استحداث العديد من المعاهد والاكاديميات والجامعات بمختلف محافظات الدولة ،تدرس تخصص الامن السيبراني ،والتي بدورها ستعمل على رفد القطاعات والمؤسسات الخاصة بأمن الدولة وفضاءها السيبراني ،بطاقات شبابية متعلمة ،ومحدثة معلوماتياً ،لكي يتم الاعتماد عليها في العمل على قطاعات الامن السيبراني في المؤسسات المختلفة .

ثانياً : امثلة عن الهجمات السيبرانية التي تعرضت لها بعض الدول

وفيها تتعرض مؤسسات الدولة العسكرية منها، و المدنية ،او حتى الافراد (مواطني هذه الدولة) ، الى هجمات سيبرانية بمختلف صنوفها ،وهي تشكل خطراً كبيراً هدفه تعطيل انظمة هذه المؤسسات ،وبرامج التشغيل فيها ، وحواسيبها التي تحوي بياناتِ مهمة او سرية ،مما يؤدي الى شلل كامل في الانشطة المختلفة في الدولة ،وتمنع بالتالي تدفق وسير البيانات بشكلها الطبيعي ،وتؤدي كذلك الى ارباك العمل اليومي مما يعطل مرافق الحياة الاساسية ،فهي تشمل استهداف محطات الطاقة ، وشبكات الوقود ، اضف الى ذلك الخدمات المصرفية ،ونظم الاتصالات المختلفة ،ووسائل النقل ،مما يجعل الدول بمواجهة مخاطر غير تقليدية ،نتيجة تصاعد وتيرة هذه الهجمات ،التي تستهدف عادة الامن القومي للدولة ،وتهدد استقرارها ،مثال على ذلك ما حصل في الولايات المتحدة التي يعد الامن السيبراني فيها حصين ، وهي تتربع عادة على المراكز الاولى في التصنيف العالمي للأمن السيبراني (GCI) ،حيث طالت شبكات الكهرباء فيها في عام (2009) هجمات سيبرانية ،تسببت في انقطاعات واسعة في التيار الكهربائي في مناطق متفرقة ،او كما حدث في الجمهورية الاسلامية الايرانية عام (2010) ،عندما تسبب فايروس (Stuxnet) ،الذي استهدف منشاة (نطنز) الخاصة بتخصيب اليورانيوم ، والذي ادى الى تعطيل حوالي (1000) جهاز طرد مركزي فيها ، وفي كوريا الجنوبية تعرضت شركة الطاقة المائية والنووية لهجوم الكتروني ،عام (2014) مما تسبب في تلكؤ العمل وتوقفه في هذه المنشاة ،اما في اوكرانيا ،فقد تعرضت لهجوم سيبراني واسع

النطاق عام (2017)،استهدف محطات الطاقة ، ومؤسسات مالية ،حتى تسبب بتعطيل انظمتها الحيوية، ،اما السعودية فتعرضت الى هجوم سيبراني في عام (2017) ،بأستخدام فايروس (Stone Drill) ،او ما يسمى بالصخرة الدوارة ،مستهدفاً قطاعات الطيران ،والبتروكيمياويات ،مسبباً بلك خسائر كبيرة للشركات العاملة في هذه القطاعات (سيناء علي محمود، 2025 ،ص319 – 320) .

في رسالة واضحة للعالم اجمع ، بأن الفضاء السيبراني لأي دولة، ليس في مأمن من الهجمات او الخروقات الالكترونية بمختلف اصنافها ،حتى وان كانت هذه الدولة او تلك ،قد حصلت على تصنيف عالٍ في مؤشرات الامن السيبراني ،اذ ان المخترقون في العادة او المهاجمون ،هم عبارة عن عباقرة الكترونيون ،او هم انفسهم مطورون لفايروسات ،او راسمو خرائط اختراق ،للأنظمة الامنية عالية الحراسة ،او الحسابات الحكومية الامنية ،فخلاصة الموضوع ان دول العالم بأجمعها تكون معرضة للهجمات الالكترونية والسيبرانية دون استثناء ،وهي بالتالي بحاجة الى العمل على رفع جاهزية امنها السيبراني ،بمختلف اشكال الدعم لهذه المؤسسات ،وما مدى نجاح اسلوب التعامل مع هذه الهجمات ،والخروج منها بأقل الخسائر .

ثالثاً : التهديدات والهجمات السيبرانية التي تعرض لها العراق

لم يكن العراق في منأى عن اجواء الخروقات والهجمات السيبرانية ، التي استطاعت ان تطال اعتى واقوى اجهزة الامن رصانة وحماية حول العالم ،كما في الدول المتقدمة في تصنيفات الامن السيبراني ،كالولايات المتحدة الامريكية ،او سنغافورة ،السعودية ،او اليابان ،على سبيل المثال ، فيما لو قورن وضع الامن السيبراني العراقي مع هذه الدول ، فأمن العراق السيبراني في حال نمو وتطور ،ولم يصل بعد ،الى حالة الكمال ،وهنا سنورد بعض الامثلة ،لهجمات الكترونية مختلفة تعرض لها العراق منها :

- بتاريخ 2013/2/2 تعرض الموقع الرسمي لرئيس الوزراء العراقي نوري المالكي ،الى اختراق من قبل قراصنة نشروا على صفحته ،رسالة تنتقده ،متزامنة مع فترة مظاهرات تملأ الشارع ،تطالب بإقالته ،وتطلق هذه الجماعة المهاجمة على نفسها (فريق قراصنة الكويت) ،وقد وصفت النظام العراقي " بنظام الطغاة " في رسالة قصيرة موجهة الى شخص الرئيس ،وقد حذرت هذه الرسالة رئيس الوزراء ، بقرب اسقاطه ،وقد ذكر ،بأن هذه المرة الثانية التي يتم اختراق موقع الرئيس نوري المالكي ،حيث توقف الموقع لعدة ايام ،جراء هذه الهجمات (www. Youm7.com، 2013) .
- بتاريخ 28 / 9/ 2016 ،تعرض موقع مستشارية الامن الوطني ،للأختراق الالكتروني ،اذ عمل المخترقون على نشر صورة كاريكاتورية ،لشخص مستشار الامن الوطني العراقي ،تليها عبارة "ان موقعكم لم تقوموا بحمايته فكيف تحافظون على امن شعبكم" (صلاح مهدي هاوي وزيد محمد علي ،2020 ،ص 279 – 280) .
- وفي عام 2017 واعلنت وزارة الخارجية العراقية ،على لسان متحدثها ،ان الوزارة تعرضت خلال يوم واحد الى (23) الف محاولة اختراق لموقع الوزارة ،حيث جاء هذا الاعلان بعد يومين من اعلان تعرض الموقع الالكتروني الرسمي لجهاز الامن الوطني العراقي للاختراق ،اذ كتب المخترق على صفحة الموقع ما نصه "كفاكم استهتاراً بأرواح العراقيين ،والذي هو اهم اسباب دمار هذا البلد " ،ثم قال المخترق انه :حصل على ستة الاف رسالة من مخاطبات ادارية رسمية سرية ،و معنونة الى دوائر الدولة الاخرى ،واضاف "ماذا لو وقعت كل هذه المخاطبات وما تتضمنه من اسماء بيد الاعداء ؟ " (www.aljazeera.net/news، 2017) .
- وفي عام 2021 ،ذكر جهاز الامن الوطني العراقي ،انه وفق معلومات استخبارية دقيقة ،تمكنت قوات من الامن الوطني ،لمحافظتي صلاح الدين ،وكربلاء ، من تفكيك اخطر شبكة تجسس وقرصنة معلومات في البلاد ،واكد ان هذه الشبكة تضم (5 اشخاص) ،تم القبض عليهم في محافظة كربلاء ،وقد اعترفوا بتلقيهم تدريبات خارج العراق ،لغرض تمكينهم من اختراق قواعد بيانات مؤسسات الدولة الامنية ،وتسريب المعلومات الخاصة بجهاز الامن الوطني لغرض التصرف بها (www.yenisafak. Com، 2020) .
- في نهاية عام 2019 ،نجحت مجموعة من القراصنة ،من تنفيذ اختراقات واسعة ،شملت ،مجموعة من المواقع الرسمية الحكومية ،على رأسها موقع رئيس الوزراء ،وفيها ادعى المتسللون انهم كذلك قد استولوا على (8 كيكا بايت) ،من الرسائل السرية الخاصة بوزارة النفط (www.baghdadtoday. news، 2023).
- ومن ضمن الاختراقات الاخرى ،تأتي قضية (التنصت) التي جرت احداثها عام 2023،وهي شبكة تنصت وتزوير ،يديرها موظفين وضباط ،ينتمون لمكتب رئيس الوزراء ،محمد شياع السوداني ،وكانت هذه الشبكة تنفذ اعمالاً غير قانونية ،كالتنصت على هواتف سياسيين ،وكذلك توجيه جيوش الكترونية ،ونشر اخبار مزيفة ،قد اعترفت الشبكة خلال التحقيقات ،انها نفذت عمليات تزوير وانتحال شخصية (www.infoplusnetwork. Com ، 2024).
- ومن الهجمات السيبرانية الخطيرة ،اعلن الكيان الصهيوني في الثاني من ايلول عام 2025 ،عن اطلاقه القمر الصناعي التجسسي ،الجديد الذي اطلق عليه اسم (افق 19) ،وهو مزود بتقنيات رادارية متقدمة ،تسمح بالرصد على مدار الساعة ،وبمختلف الظروف الجوية ،وقد خصص هذا القمر بمراقبة دول الشرق الاوسط ،وخاصة ايران والعراق وسوريا واليمن ، وهي بداية لنشر حوالي (20) قمرا صغيرا تباعاً ، لزيادة جغرافية المكان الذي تغطيه هذه الاقمار ،كالأنشطة النووية ،والتحرك العسكري ،وعمليات اطلاق الصواريخ ،وغيرها من الامور التي تهدد امن اسرائيل ،على حد وصفها ،وقد

كشف البروفيسور (يتسحاق بن يسرائيل) ،رئيس مركز الامن السيبراني في (جامعة تل ابيب) ،مصرحاً عن مشروع الاطلاق هذا ،بأن القمر الجديد ،يهدف لتصوير مناطق الشرق الاوسط التي يمر فوقها ،ومن ثم نقل المعلومات الاستخبارية ،التي يجمعها لمراكز فك التشفير(www.infoplusnetwork. Com،2025) ،ويعد اطلاق هذا القمر تهديد كبير ،وخطر محدق ووشيك ،في ضل وضع الدولة العراقية الحالي ،الذي يخلو من التحصين الكافي والحماية الحقيقية والردع السريع ،لمختلف التهديدات والهجمات ،على كل الاصعدة ،فضلاً عن امن الفضاء السيبراني .

- كشف نائب مدير الامن السيبراني في جهاز الامن الوطني ،عن تسجيل اكثر من ثلاثة الاف حالة احتيال الكتروني ،خلال الاشهر الستة الاولى من عام 2025 ،والتي بلغت خسائرها نحو ثلاثة مليار دينار عراقي ،وقد حذر من ان ما يتم الابلاغ عنه ،لا يمثل سوى 30% فقط من حجم الاحتيال والابتزاز الرقمي ،الموجود على ارض الواقع (www. Kurdistan24 .net ،2025) .

ان ما ذكر في اعلاه من تهديدات وهجمات ،انما هو فيض من غيض ،فيما لو كشف عن الارقام الحقيقية التي يتعرض لها فضاء العراق السيبراني ،سواء ما كان منه متعلقاً ببيانات ومعلومات الافراد ،او المؤسسات الحكومية ،لأن الاعلان عن كل او معظم الحالات ،يكشف عن مدى هشاشة البنى التحتية الخاصة بأمن العراق السيبراني ،والواقع يشير الى ان اعلى سلطات الدولة المتمثلة بـ (رئيس الوزراء) ،لم تسلم من هذه الهجمات ،و الوزارات و المؤسسات الامنية ، كذلك هي الاخرى تعرضت وبشكل واسع الى هجمات متكررة ،يهدف من خلالها المهاجمون الى كشف ضعف هذه المؤسسات ،او ابراز قوة المهاجمون ،من بعد ان تمكنوا من الوصول الى قاعدة بيانات اهم المؤسسات الامنية في الدولة ، وربما قد يكونوا هؤلاء المهاجمون مستأجرون او يعملون لصالح دولة ما ،بغية تحقيق اغراض عدائية ،او انتحال شخصية ،ضد الجهة المقابلة او الدولة التي يرام استهدافها ،وهي فلسفة الحروب الحديثة بطبيعة الحال .

النتائج :

1- تعرض العراق ويتعرض الى الهجمات السيبرانية باستمرار ،تتوزع ما بين المؤسسات الامنية في الدولة ،او على مستوى الافراد والمواطنين، دون تحديد صنف او جهة خاصة ، ما يظهر ضعف البنية التحتية ،(افراد وتكنلوجيا)، التي من الممكن ان تؤهل العراق، ليكون ضمن مصاف الدول المتقدمة في هذا المضمار ،او يبقى متذيلاً التصنيف .

2- حصل العراق في تقرير (GCI) ،الصادر عام 2023 على المرتبة (107) عالمياً ،من مجموع اكثر من 190 دولة خضعت للتصنيف ،وهو افضل تصنيف حصل عليه العراق ،اما اضعف تصنيف فكان عام 2017 ،اذ جاء بالمرتبة (159) ،وهو الترتيب الاضعف في التصنيفات التي دخل العراق من ضمنها .

3- قلة عقد الندوات ،او اقامة الورش التي تخص الامن السيبراني ، سواء داخل الدولة ،او في المشاركات والدورات الخارجية ،في الدول الرائدة في هذا المجال .

4- الاعتماد الكلي على توريد والاجهزة الالكترونية والحواسيب ،والهواتف النقالة بمختلف انواعها ، من خارج الدولة ، يجعل منها موضع شك ،من ان تكون مراقبة ،او احتوائها على برامج تجسس ،او تتبع ،وغيرها ،كما حصل في بعض الحالات في العالم .

5- بدأ العراق وان كانت بداياته متأخرة ،من العمل على رفع مستوى الامن السيبراني للدولة ،واستحدثت مديريات ،واقسام علمية واكاديمية في اكثر من محافظة تخص الامن السيبراني ،في خطوة مهمة ،تعمل على رفع امكانيات وقدرات مؤسسات الدولة الامنية .

المقترحات :

1- ان تعزيز قواعد المؤسسات السيبرانية ،وتحديث بنيتها (المادية والبشرية) باستمرار ووضع استراتيجية وطنية للأمن السيبراني في الدولة ،يجعله مهيأ ومستعد للتصدي ،لأي تهديد سيبراني ،في اي وقت ،ومهما كان حجم هذه الهجمات .

2- العمل الجاد لرفع مستوى الركائز الخمسة التي وضعها مؤشر الامن السيبراني العالمي الـ (GCI) ،وبالخصوص الركائز الخاصة بـ (بناء القدرات – تطوير الركائز التقنية) ،او اي ركيزة لا تحقق نتيجة مرضية و التركيز عليها ،للحصول على نتائج افضل .

3- العمل على تشريع القوانين التي تخص الامن السيبراني ،والتركيز على المشاركة في المحافل والندوات في المجال نفسه ،سواء الداخلية منها او الخارجية ،لكي تتم الاستفادة من التجارب التي خاضتها هذه الدول .

4- العمل على تأسيس شبكات اتصالات وطنية ،فضلاً عن انشاء مصانع حتى لو على مستوى تجميع الاجهزة الالكترونية المختلفة ،وبالاخص اجهزة الاتصال ،كونها من الركائز الاساسية في المؤسسات التي تعنى

بالامن السيبراني ،حتى تكون هذه الاجهزة في مأمن من شبكات التنصت او التتبع ،او حتى ان تكون قابلة لأحداث اضرار ،كما حصل في اجهزة (البيجر) في لبنان على سبيل المثال .

5- التوسع في استحداث اقسام اكاديمية علمية ،على مستوى المدارس او الجامعات ،الذي من شأنه رفد مؤسسات الدولة كافة ،الامنية منها وغير الامنية ،بالطاقات الشابة المتعلمة والمتدربة .

المصادر :

- القرآن الكريم

اولاً – الكتب :

1- حسين علاء عبد الخالق وآخرون ، الامن السيبراني المبادئ والممارسات لضمان سلامة المعلومات ،دار السرد للطباعة والنشر والتوزيع – العراق - بغداد، ط1 2024.

ثانياً – المجلات العلمية :

1- احمد عبد الكريم عبد الوهاب ومحمود عبد الرحمن خلف ،اشكالية الامن السيبراني العراقي بين التهديدات السيبرانية والتقنين المقيد للحريات ،مجلة العلوم السياسية ،كلية العلوم السياسية ،جامعة النهرين ، العدد (60) السنة الثانية عشر ،2020.

2- السمحان منى عبدالله ،متطلبات تحقيق الامن السيبراني لأنظمة المعلومات الادارية بجامعة الملك سعود ،مجلة كلية التربية – جامعة المنصورة ،العدد (11) ،2020.

3- المعيني محمد كاظم عباس ، استراتيجية التحكم بالفضاء السيبراني لتعزيز الابعاد غير الملموسة للأمن القومي العراقي ، مجلة العلوم السياسية ، العدد (69) ،2025 .

4- رأفت عاصي حسين ورغد خير الدين صبري ،مدى جاهزية المنظمات لإقامة ابعاد الامن السيبراني دراسة تحليلية لآراء عينة من العاملين في البنك المركزي العراقي فرع الموصل ،مجلة العلوم الادارية والانسانية ، الجامعة التقنية الشمالية ،المجلد (5) ، العدد (2)،2025 .

5- صليبي رعد خضير ، تعزيز الامن السيبراني في العراق : التحديات والفرص ، مجلة دراسات دولية ،جامعة بغداد / مركز الدراسات الاستراتيجية ، العدد (99) ، 2024.

6- عبد اللطيف تامر سعيد ،الاستمرارية والتغير في استراتيجية الامن السيبراني للولايات المتحدة الامريكية في المدة من 2009 الى 2014 ،مجلة العلوم السياسية ، العدد (69) ، 2025 .

7- علوان عباس فاضل ، سياسات الامن الوطني العراقي في ظل التحديات العالمية للأمن السيبراني ، المجلة العلمية لجهاز مكافحة الارهاب ، المجلد (5) العدد (9) ،2025.

8- محمد زينب ضياء ، استراتيجية الامن السيبراني الروسي ، مجلة القادسية للقانون والعلوم السياسية ، الجزء (2) ، المجلد (16) ،2025.

9- محمد علي عبد الخضر ، آليات الامن السيبراني ودورها في الحد من الهجمات الالكترونية على المستوى الدولي ،مجلة ضياء الفكر للبحوث والدراسات العدد (29 – 30) ، 2024 .

10- محمد ياور عمر، تأثير الامن السيبراني على الامن القومي العراقي – الفرص والتحديات ،مجلة كلية القانون للعلوم القانونية والسياسية ، المجلد (14) ، العدد (53) ،2025.

11- محمود سيناء علي، التحديات الامنية للدول في الفضاء السيبراني ،مجلة قضايا سياسية ، العدد (80) ،2025 .

12- هاوي صلاح مهدي وزيد محمد علي ، الامن السيبراني كمرتكز جديد في الاستراتيجية العراقية ،مجلة قضايا سياسية ،جامعة النهرين ،كلية العلوم السياسية ،العدد (22) ،2020 .

ثالثاً – الشبكة الدولية للمعلومات الانترنت :

1- رؤية مديرية الامن السيبراني – وزارة الداخلية ، مقال منشور بتاريخ 2024/12/22 ،على الرابط Cybersecurity@moi.gov.iq ، تم الدخول الى الموقع بتاريخ 2025/10/9 .

2- قراصنة يخترقون الموقع الرسمي لرئيس وزراء العراق نوري المالكي ،مقال منشور بتاريخ 2013/2/2 على موقع اليوم السابع ،على الرابط . www. Youm7.com ، تم الدخول الى الموقع بتاريخ 2025/11/5

3- هجمات الكترونية ضد مواقع وزارات عراقية ، مقال منشور بتاريخ 2017/6/2 على موقع الجزيرة ،على الرابط . www.aljazeera.net/news، تم الدخول الى الموقع بتاريخ 2025/11/12

4- العراق يعلن عن تفكيك شبكة تجسس وقرصنة معلومات امنية ،مقال منشور بتاريخ 2021/11/24، على الرابط ، www.yenisafak. Com ، ، تم الدخول الى الموقع بتاريخ 2025/11/5.

5- استعراض حالات اختراق عالمية نفذها هكرز عراقيون ..لماذا تنشط القرصنة في العراق ، مقال منشور على صفحة وكالة بغداد اليوم الاخبارية ، بتاريخ ،2023/8/29 ،على الرابط ، www.baghdadtoday. news ، تم الدخول الى الموقع بتاريخ 2025/11/12.
6- السجن 4 سنوات بحق محمد جوحي ..تعرف على آخر ما آلت اليه قضية التنصت وتفاصيل الحكم واحتمالية تورط السوداني ،مقال منشور بتاريخ ،2024/12/9 ،على الرابط ، www.infoplusnetwork. Com، تم الدخول الى الموقع بتاريخ 2025/11/12.
7- "افق 19" فوق العراق :قمر تجسسي للكيان الصهيوني يهدد سيادة العراق ودول المنطقة ،مقال منشور بتاريخ 10/ 9 /2025 ،على موقع انفوبلس ،على الرابط ، www.infoplusnetwork. Com، تم الدخول الى الموقع بتاريخ 2025/11/5 .
8- الامن الوطني : اكثر من 3 الاف حالة احتيال الكتروني في العراق خلال ستة اشهر ، مقال منشور بتاريخ ،2025/8/30 ،على الرابط ، www. Kurdistan24 .net، تم الدخول الى الموقع بتاريخ 2025/11/12.

رابعاً – المصادر باللغة الانكليزية :

1- international Telecommunication Union , Global Cybersecurity Index ,2024 , Geneva :ITU ,Retrieved from ,https://www.itu.int,p74

Abstract

Now that the world has become a global village, as it is often described, and this village is linked by an information network containing a vast amount of information—whether it pertains to citizens' personal data or the databases of various state institutions—and given that this information is susceptible to sharing or hacking by other parties connected to the same internet network, it is imperative to establish digital protection measures that keep pace with technological advancements within the cyberspace of nations. These measures serve as a line of defense and a protector of this information. Cybersecurity has become an urgent necessity for protecting national systems and networks, and it is the only way to repel cyberattacks and threats to national security. This is crucial to prevent the breaching, leaking, and manipulation of information by cybercriminals (hackers), especially after the advent of artificial intelligence as a powerful weapon and a rapid means used by cybercriminals to access targeted information under any circumstances, at any time, and in any place, thus threatening the security of the targeted state. Cybersecurity has become an essential component of national security policies, to the point that it has become As a symbol of showcasing the state’s capabilities in the field of smart power and its sovereignty in this regard, it is necessary for countries that have not joined the technological progress to take precautions and work hard to give great importance to their cybersecurity, so that they do not remain vulnerable to any breach or any electronic war, with sufficient knowledge to deal with such crises. Iraq is among the countries that have begun to join the field of electronic development with regard to the information security of the state and citizens.

Keywords: Cyberattacks, Cybersecurity, Space, Digital Security, Cybercrime