المجلة السياسية والدولية

دور الامن السيبراني في استقرار الدولة

م.م سيماء علي مهدي
الجامعة المستنصرية/ كلية العلوم السياسية
simea@uomustansiriyah.edu.iq

الملخص:

الأمن السيبراني ليس مجرد قضية تقنية، بل هو ركيزة أساسية للاستقرار السياسي والاجتماعي. ففي العراق، يعد تعزيز القدرات السيبرانية خطوة حيوية لحماية الديمقراطية، ومكافحة الإرهاب، وجذب الاستثمارات، وبناء ثقة المواطنين في مؤسسات الدولة، لأن الأنترنيت اليوم قادر على ارسال واستقبال أي شكل من اشكال البيانات ، و بدون استراتيجية فعالة للأمن السيبراني، تظل البلاد عرضة لتهديدات قد تؤدي إلى انعدام الأمن وعدم الاستقرار على المدى الطويل.

كلمات مفتاحية: الأمن السيبراني، الاستقرار ، الجرائم الإلكترونية، الحرب السيبرانية، الحماية الرقمية.

The role of cybersecurity in state stability

TA. Saima Ali Mahdi
Al-Mustansiriya University/College of Political Sciences
simea@uomustansiriyah.edu.iq

Abstract:

Cybersecurity is not just a technical issue but a fundamental pillar of political and social stability. In Iraq, enhancing cyber capabilities is a vital step to protect democracy, combat terrorism, attract investments, and build citizens' trust in state institutions. Today, the internet is capable of sending and receiving any form of data, and without an effective cybersecurity strategy, the country remains vulnerable to threats that could lead to insecurity and long-term instability.

Keywords: Cybersecurity, stability, cybercrimes, cyber warfare, digital protection.

المقدمة:

تلعب السيبرانية (الأمن السيبراني والفضاء السيبراني) دوراً متزايداً في الاستقرار السياسي للدول، سواء من خلال تعزيز الأمن الوطني أو عبر التهديدات التي تشكلها الهجمات الإلكترونية على البنية التحتية الحيوية والمؤسسات الحكومية. إذ تعتمد الدول الحديثة على أنظمة إلكترونية في إدارة قطاعات حيوية مثل الطاقة، النقل، الاتصالات، والخدمات المالية، وأي اختراق لهذه الأنظمة قد يؤدي إلى شلل كامل، مما يؤثر على الاستقرار السياسي والاقتصادي. فضلاً عن الاختراقات الإلكترونية التي تستهدف الحكومات والأحزاب السياسية يمكن أن تؤدي إلى تسريب معلومات حساسة تستخدم للتأثير على الرأي

العام أو زعزعة الثقة في النظام السياسي، ويكمن أن تستخدم لنشر الأخبار المزيفة عبر منصات التواصل الاجتماعي لبث الفرقة وتأجيج الصراعات الداخلية.

أهمية البحث:

في عصر التحول الرقمي والاعتماد المتزايد على التكنولوجيا، أصبح البحث في الأمن السيبراني ضرورة حيوية لضمان استقرار الدول وحماية الأفراد والمؤسسات. فضلاً عن المؤسسات الحكومية العراقية تعاني من ضعف أنظمة الحماية، مما يجعلها عرضة لاختراق البيانات الحساسة (مثل السجلات الأمنية، المعلومات الشخصية للمواطنين)، والاختراقات قد تستغل للتجسس، التلاعب السياسي، أو الاحتيال المالي.

إشكالية البحث:

تواجه الدول تحديات في تحقيق التوازن بين الأمن وحقوق الأفراد، مما قد يؤدي إلى انتهاكات للخصوصية، فضلاً عن تزايد الهجمات السيبرانية التي تستهدف البنية التحتية الحيوية، مما يهدد استقرار الدول وأمان مواطنيها. كما أن انتشار المعلومات المضللة والتلاعب بالرأي العام عبر وسائل التواصل الاجتماعي يزيد من تعقيد الوضع، إذ تؤثر هذه الممارسات على الانتخابات والعمليات الديمقراطية. وإن غياب الوعي الأمني لدى المواطنين والمؤسسات يجعلهم فريسة سهلة لعمليات الاحتيال الإلكتروني، أو البرمجيات الخبيثة.

فرضية البحث:

الأمن السيبراني في العراق ليس رفاهية، بل ضرورة أمنية واقتصادية وسياسية لضمان استقرار البلاد في العصر الرقمي. بدون استراتيجية سيبرانية فاعلة، سيبقى العراق عرضة لتهديدات قد تؤثر على أمنه الوطني ومستقبله التنموي.

منهجية البحث:

استخدمت المنهج التحليلي الوصفي ليتضح من ذلك؛ بأن الأمن السيبراني في العراق يعاني من تحديات هيكلية وقانونية وبشرية، ولكن هناك فرص لتحسينه عبر تحديث البنية التحتية، تعزيز التشريعات، كما أنه يساعد صانعي القرار على فهم الواقع واتخاذ إجراءات فعالة لتعزيز الأمن الرقمي.

الفرع الأول: مفهوم السيبرانية والمفاهيم المقاربة لها

السيبرانية لم تعد مجرد مفهوم تقني، بل أصبحت مكوناً أساسياً للأمن الوطني والاستقرار الاجتماعي في العصر الرقمي ، ولذلك ترجع كلمة "سيبرانية" إلى المصطلح الإنجليزي "Cyber" الذي اشتق بدوره من الكلمة اليونانية(kybernētēs) والتي تعني "ربان السفينة" أو "القيادة والسيطرة (wienier 1948 , 19) . وبهذا تعرف بأنها: "كل ما يتعلق بالعالم الافتراضي الرقمي وشبكات الحاسوب (المعجم الموحد ٢٠٠٥) .

أولاً/ الامن السيبراني

يعرف الامن السيبراني على أنه: "العلم الذي يهتم بحماية البنى التحتية الرقمية والبيانات من التهديدات الداخلية والخارجية عبر أدوات تقنية وتشريعات قانونية (حمدي ٢٠١٩ ، ٢٤) أو تعرف بانها: "حماية الشبكات والأنظمة والبرامج من الهجمات الرقمية التي تهدف إلى اختراق أو تعطيل أو تسريب المعلومات الحساسة (الهيئة الوطنية للامن السيبراني ٢٠١٨ ، ٨) .

وبذلك يشمل الأمن السيبراني أنظمة الأمن العسكري والاقتصادي والاجتماعي والسياسي والإنساني المتصل بشبكة للإنترنت التي تهدف إلى الحفاظ على الأمن من جميع التهديدات السيبرانية.

ثانياً/ الاستخبارات السيبرانية

تعرف الاستخبارات السيبرانية بأنها: "عملية منهجية لجمع وتحليل المعلومات عن التهديدات السيبرانية، القدرات، النوايا، وأنشطة الجهات المعادية في الفضاء الرقمي لدعم القرارات الأمنية. (white 2018 , 23). أو تعرف بأنها: "نشاط استخباري متخصص في رصد وتحليل الهجمات الإلكترونية المحتملة، وتحديد الجهات الفاعلة خلفها، وتوفير الإنذار المبكر للجهات المعنية (الوهيبي ٢٠٢٠ ، ٨٧) أو أنها : "فرع من الاستخبارات الأمنية يهتم بتتبع النشاط العدائي في الفضاء الإلكتروني وتقديم التقديرات الاستراتيجية للقيادات (الوهيبي ، ٨٧) .

ثالثاً: الحرب السيبرانية

تعرف الحرب السيبرانية بأنها: "نزاع بين دول أو فواعل منظمة يستهدف إلحاق الضرر بأنظمة الحاسوب أو الشبكات الحيوية للخصم، سواء عبر تعطيل الخدمات، سرقة البيانات، أو التلاعب بالبنى التحتية الرقمية (Clarke 2010, 12) أو تعرف بأنها: "استخدام القدرات الرقمية لشن هجمات تهدف إلى إضعاف الخصم في زمن السلم أو الحرب، مع إمكانية تحقيق نتائج مماثلة للأسلحة التقليدية (alilled 2020,5) وتعرف أيضاً بأن: "الحرب السيبرانية تمثل البعد الخامس للحرب الحديثة بعد البر والبحر والجو والفضاء (الوهيبي ، ٣٣) . وكذلك تعرف بأنها: "أي نشاط عدائي في الفضاء السيبراني ينتهك سيادة دولة ما، ويخضع لمبادئ القانون الدولي الإنساني (schimitt 2017) .

رابعاً/ الجريمة السيبرانية

تعرف الجريمة السيبرانية بأنها، أي نشاط إجرامي يرتكب باستخدام الشبكات الرقمية أو الأجهزة الإلكترونية مثل الحواسيب والهواتف الذكية، سواء كان الهدف هو الاختراق، السرقة، التهديد، أو الاعتداء على البيانات والخصوصية، ولذلك تشمل (الغامدي ، ٣٣) :

١- الجرائم ضد الأفراد: مثل التهديد الإلكتروني، التنمر السيبراني، وانتحال الهوية.

٢- الجرائم ضد الممتلكات: مثل سرقة البيانات المالية، الاحتيال المصرفي، وبرامج الفدية.

٣- الجرائم ضد الحكومات: مثل القرصنة على الأنظمة الحكومية أو البنية التحتية الحيوية.

أما الانتربول فيعرف الجريمة السيبرانية على أنها : " أي نشاط إجرامي يستهدف أو يستخدم الحواسيب أو الشبكات الرقمية، بما في ذلك جرائم مثل الاختراق، التصيد الاحتيالي، البرمجيات الخبيثة، والاحتيال المالي (تقرير الانتربول ٢٠٢٣ ، ١٢) .

خامساً/ الردع السيبراني

يشير الردع السيبراني إلى استراتيجيات تستخدم لثني الخصوم أو المهاجمين عن تنفيذ هجمات إلكترونية ضارة، من خلال إقناعهم بأن تكاليف الهجوم أو عواقبه تفوق أي فوائد محتملة. يعتمد هذا المفهوم على نظريات الردع التقليدية في الأمن القومي، لكنه يطبق في الفضاء السيبراني، إذ تشمل أدواته على (MARTIAN 2009):

١- الردع بالعقاب: القدرة على الرد على الهجمات الإلكترونية بعقوبات سياسية أو اقتصادية أو عسكرية.

٢- الردع بالإنكار: جعل الهجمات السيبرانية غير فعّالة عبر تعزيز الدفاعات الإلكترونية (مثل التشفير، جدران الحماية).

٣- الردع عبر التشويه: تقليل ثقة المهاجم في نجاح هجومه (مثل نشر معلومات مضللة عن القدرات الدفاعية).

الفرع الثاني: الاستقرار السياسي والمفاهيم المقاربة لها

إن كلمة استقرار في اللغة العربية مشتقة من استقر، يستقر، استقراراً، فيعني المكان أو القرار أو الثبات (محمد ٢٠٢٤) . أما اصطلاحاً فيعني الاستقرار السياسي ، قدرة النظام السياسي على الحفاظ على استمراريته دون اضطرابات كبيرة، مع تحقيق درجة من التوافق بين مكونات المجتمع وقدرته على مواجهة التحديات الداخلية والخارجية (عارف ٢٠٠٣ ، ١٤٧) .

أولاً/ الشرعية السياسية

تعني الشرعية السياسية ، قبول الشعب للنظام السياسي والحكومة، واعتبارهما يتمتعان بالحق في ممارسة السلطة، سواء كان ذلك بناءً على القوانين، التقاليد، أو الرضا العام، وهي عنصر أساسي لاستقرار الأنظمة السياسية (احمد ٢٠١٠ ، ٨٩) ويحدد ماكس فيبر ثلاثة أنواع أساسية للشرعية، وهي (فيبر ٢٠٠٥ ، ٢١٥) :

١- الشرعية التقليدية: تستند إلى العرف والتقاليد (مثل الملكيات الوراثية).

٢- الشرعية الكاريزمية: تعتمد على شخصية الزعيم وجاذبيته.

٣- الشرعية العقلانية-القانونية: تقوم على القوانين والمؤسسات الرسمية.

أما مصادر الشرعية السياسية، فهي (سليم ٢٠١٥) :

أ- الإنجاز الاقتصادي والاجتماعي: عندما يحقق النظام رفاهية المواطنين.

ب–المشاركة السياسية: الانتخابات والمؤسسات التمثيلية.

ت–العوامل الثقافية والدينية: كالشرعية المستمدة من الدين أو العرف.

أما ازمة الشرعية السياسية، ، فتحدث عندما يفقد النظام السياسي قبول الشعب، مما يؤدي إلى الاحتجاجات أو الانقلابات، ومن أسبابها (عوض ٢٠١٢ ، ٨٠) :

- الفساد.
- التزوير الانتخابي.
- فشل السياسات الاقتصادية.

ثانياً/الامن السياسي

يشير الأمن السياسي إلى قدرة الدولة على حماية نظامها السياسي من التهديدات الداخلية والخارجية التي قد تعرض استقرارها للخطر، و يشمل الحفاظ على سيادة الدولة ووحدة أراضيها واستقرار نظامها السياسي (النفيسي ٢٠٠٧ ، ٥٦) . فضلاً عن قدرة النظام السياسي على حفاظه بشرعية ، وتوفير الحماية لمؤسساته من الانهيار أو التغيير القسري (الجابري ٢٠١٠ ، ١٢٣) . وهناك أبعاد الأمن السياسي، وهي (امين ٢٠٠٨) :

١– البعد الداخلي: يتعلق بحماية النظام من التهديدات الداخلية مثل الانقلابات، الاحتجاجات العنيفة، أو التمرد.

٢– البعد الخارجي: يركز على حماية الدولة من التهديدات الخارجية مثل العدوان العسكري أو التدخل الأجنبي.

٣– البعد المؤسسي: يشمل قدرة المؤسسات السياسية على الصمود أمام الأزمات وإدارة الصراعات.

أما مصادر التهديد للأمن السياسي، فتشمل (السويدي ٢٠١٥ ، ٤٥) :

أ– الانقسامات الداخلية: مثل الصراعات الطائفية أو العرقية.

ب– الفساد السياسي: الذي يقوض ثقة المواطنين بالنظام.

ت– التدخل الخارجي: من خلال دعم جماعات معارضة أو فرض عقوبات.

أما استراتيجيات تعزيز الأمن السياسي، فتشمل (عارف ٢٠٠٣ ، ١٦٠) :

- تعزيز الشرعية السياسية عبر الانتخابات النزيهة والمشاركة الشعبية.
- بناء مؤسسات قوية قادرة على إدارة الأزمات.
- تحقيق التنمية الاقتصادية، لتقليل أسباب السخط الداخلي.

الفرع الثالث: علاقة الامن السيبراني بالاستقرار السياسي

أصبح الأمن السيبراني عنصرا حاسما في الحفاظ على الاستقرار السياسي في العصر الرقمي، إذ تشكل الهجمات الإلكترونية تهديدا مباشرا لأمن الدول وسيادتها، ويهدد انعدام الأمن السيبراني الاستقرار السياسي من خلال:

اولاً/ اختراق المؤسسات الحكومية

هي عملية اقتحام غير مصرّح به لأنظمة المعلومات التابعة للجهات الحكومية، بغرض سرقة بيانات حساسة، تعطيل الخدمات، أو التلاعب بالعمليات الإدارية (تقرير الامن السيبراني ٢٠٢٣) ، والاختراقات الحكومية تمثل أعلى مستوى من التهديدات السيبرانية بسبب حساسية البيانات المستهدفة (ميتنيك ٢٠١٩) .وهناك عدة أنواع اختراقات المؤسسات الحكومية، وهي:

١- هجمات التجسس: سرقة أسرار دولة أو معلومات استخباراتية، مثل اختراق البنتاغون ٢٠١٥ (CLARKE 2020).

٢- هجمات التعطيل: تعطيل خدمات حكومية أساسية (كهرباء، صحة)، مثل هجوم كولونيال بايبلاين ٢٠٢١ .

٣- التلاعب بالبيانات: تغيير السجلات الرسمية أو نتائج الانتخابات، مثل تدخل روسيا في انتخابات الولايات المتحدة ٢٠١٦ (muller 2019 , 92) .

أما تقنيات الاختراق الشائعة، فهي:

أ- التصيد الاحتيالي: ويكون عن طريق إرسال رسائل مزيفة لسرقة بيانات الدخول (simon 2021 , 45) .

ب- الثغرات الصفرية: استغلال ثغرات غير معروفة في الأنظمة. مثل استغلال ثغرة في برنامج البريد الإلكتروني للبنتاغون لعام ٢٠١٥م، والتي تسببت بسرقة ٣٠ ألف وثيقة سرية (us government 2016) .

ت- الهجمات : تعني إغراق الخوادم بطلبات وهمية لتعطيلها مثل هجوم سولار ويندز لعام ٢٠٢٠م، والجهات المتأثرة ٩ وكالات حكومية أمريكية عن طريق تزويد برمجيات ضارة عبر تحديثات شرعية، ونتجت بذلك اختراق شبكات وزارة الخزانة والتجارة (report 2021) .

ثانياً/ التأثيرات السياسية والأمنية

يشكل الأمن السيبراني تحدياً رئيسياً للدول في العصر الرقمي، ويكون ذلك في عدة نقاط منها:

١- تهديد السيادة الوطنية: يمكن للهجمات السيبرانية استهداف البنية التحتية الحيوية (مثل أنظمة الطاقة والاتصالات)، مما يضعف سيطرة الدولة على مواردها. مثال، هجوم Stuxnet- ستوكسنت (هو أول فيروس إلكتروني مصمم خصيصاً لتخريب الأنظمة الصناعية، وخصوصاً

أجهزة الطرد المركزي المستخدمة في تخصيب اليورانيوم؛ استهدف به المنشآت النووية الإيرانية عام ٢٠١٠، مما تسبب في تعطيلها وتأخير البرنامج النووي الإيراني لعدة سنوات) (Clarke 2010) .

٢- التلاعب بالانتخابات والديمقراطية: يمثل الانتخاب الوسيلة الوحيدة من وسائل اسناد السلطة في النظام الديمقراطي (علي ٢٠٢٤) ، وحدث محاولة في التلاعب والتأثير على نتائج الانتخابات الامريكية عبر اختراق البريد الإلكتروني للجنة الوطنية الديمقراطية (DNC) من قبل مجموعة "Fancy Bear" الروسية عام ٢٠١٦، ونشر محتويات عبر ويكيليكس ، فضلاً عن نشر المعلومات المضللة لبث دعاية سياسية مزيفة (muller 2019) .

٣- الأسلحة السيبرانية كأداة للصراع الدولي(الهجمات على البنية التحتية الحيوية) مثال على ذلك، الهجوم الروسي في ٢٧حزيران٢٠١٧ الذي استهدف أوكرانيا عبر برنامج خبيث تسبب في شل البنية التحتية الأوكرانية (البنوك، الطاقة، الحكومة) نتج عنها خسائر مادية تقدر بـ ١٠ مليار دولار، وكان الهدف الرئيسي منها معاقبة أوكرانيا بعد الثورة الأوكرانية ٢٠١٤؛ التي اندلعت بعد رفض الرئيس" فيكتور يانوكوفيتش" توقيع اتفاقية الشراكة مع الاتحاد الأوروبي في تشرين الثاني ٢٠١٣، مفضلاً التقارب مع روسيا (report 2018 , 4). أما في السعودية فقد شهدت أرامكو ، التي تضخ ١٠٪ من إمدادات النفط العالمية، أكبر هجوم إلكتروني لها حتى الآن في أب ٢٠١٢، عندما تسبب هجوم فيروس شمعون في إتلاف حوالي ٣٠٠٠٠ جهاز كمبيوتر ومسحت بيانات ٧٥% من أجهزتها بالكامل ، وتسببت في تعطيل العمليات الانتاجية لمدة أسبوعين . استهداف شركة سابك (أكبر شركة بتروكيماويات في الشرق الأوسط) ٢٠١٧، عبر الاصدار الجديد من فايروس "Shamoon" اكثر تطور من نسخة ٢٠١٢ ، وتسبب في تعطيل ٢٠,٠٠٠ جهاز في سابك (شمعون ٢٠١٩) .

أما في العراق، فلا يزال يعاني من ضعف البنية التحتية السيبرانية ونقص التشريعات الفاعلة والكفاءات المتخصصة، ولذلك شهد العراق في السنوات الأخيرة تصاعداً كبيراً في الهجمات الإلكترونية، خاصة ضد المؤسسات الحكومية والبنوك والبنية التحتية الحيوية. تعكس هذه الهجمات ضعف البنية التحتية الأمنية وعدم كفاية الإجراءات الوقائية، مما يجعل العراق هدفاً سهلاً للمجموعات الإلكترونية الخبيثة. وجدول رقم (١) يوضح ذلك:

جدول رقم(١) أبرز الهجمات السيبرانية على العراق (٢٠٢٠-٢٠٢٤)

السنة	الهدف	نوع الهجوم	الجهة المنفذة (المشتبه بها)	المصدر
٢٠٢٠	شبكات حكومية	برنامج "Shamoon" المدمر	مجموعات مرتبطة بإيران (APT34)	Kaspersky Report 2021
٢٠٢١	مواقع وزارات عراقية	هجوم DDoS	جماعات قرصنة مجهولة	Rudaw News 2021
٢٠٢٢	البنك المركزي العراقي	محاولة اختراق أنظمة الدفع	عصابات إلكترونية دولية	Al-Sumaria TV 2022
٢٠٢٣	مستشفيات بغداد	هجوم ببرنامج الفدية "LockBit"	مجموعة "LockBit" الإجرامية	Symantec Threat Report 2023
٢٠٢٤	منصة التداول الحكومية	تسريب بيانات المواطنين	قراصنة محليون	Iraqi Cybersecurity Directorate Statement

ففي جدول رقم(١) يوضح إن في عام ٢٠٢٠م، تعرضت شبكات حكومية عراقية لهجوم ببرنامج "Shamoon" المدمر، الذي يحذف البيانات بشكل كامل. أما في عام ٢٠٢١ م، تعرضت مواقع حكومية عراقية (بما في ذلك وزارات وهيئات رسمية) لهجمات DDoS تسببت في تعطيل الخدمات لساعات، وفي عام ٢٠٢٢م، تعرضت المستشفيات العراقية الى هجمات فدية ، مما عطل أنظمة التشخيص الطبي. وفي ٢٠٢٣م، أعلنت بعض البنوك العراقية عن تعرضها لهجمات مماثلة، مما أثر على الخدمات المصرفية الإلكترونية.

الفرع الرابع/ طرق تحسين الأمن السيبراني

إن تحسين الأمن السيبراني أصبح من الأولويات الأساسية في العصر الرقمي، نظراً للتزايد المستمر للهجمات الإلكترونية التي تهدد المؤسسات والأفراد على حد سواء. إذ إن هناك أهم الممارسات الأمنية التي يمكن تبنيها من قبل الأفراد والمؤسسات لتعزيز الحماية الإلكترونية وتقليل المخاطر، وهي كالتالي:

أولاً/ التوعية والتدريب المستمر للمستخدمين: أحد أهم جوانب تحسين الأمن السيبراني هو التأكد من أن الأفراد على دراية بكيفية حماية أنفسهم وأجهزتهم من الهجمات الإلكترونية. إذ يمكن أن يساعد التدريب على حماية البيانات والتعامل مع التهديدات السيبرانية بحذر مثل التصيد الاحتيالي والهجمات الإلكترونية مما يقليل الأخطاء البشرية التي تشكل أحد أكثر الثغرات شيوعاً في النظام الأمني، وذلك عبر إجراء اختبارات محاكاة للتصيد الاحتيالي لقياس استعداد الموظفين وقدرتهم على التعامل مع الهجمات. فضلاً عن استخدام دراسات الحالة عن أمثلة حقيقية من الهجمات الإلكترونية لكي تساعد الموظفين في فهم التهديدات بشكل أفضل (version 2023) .

ثانياً/ تحديث البرمجيات بانتظام: من الضروري تحديث البرمجيات والتطبيقات بشكل دوري لضمان حماية الأجهزة من الثغرات الأمنية التي تعد من الأسباب الرئيسية لنجاح الهجمات السيبرانية. إذ تشير الدراسات إلى أن ٦٠% من الاختراقات يمكن منعها من خلال التحديثات المنتظمة (27 , 2023 ibm)

ثالثاً/ استخدام كلمات مرور قوية : كلمات المرور الضعيفة تشكل نقطة ضعف رئيسية في الأنظمة الإلكترونية. لذا يجب أن تكون كلمات المرور طويلة ومعقدة، وتحتوي على مزيج من الأحرف الكبيرة

والصغيرة، الأرقام، والرموز. فضلاً عن تفعيل المصادقة الثنائية (المعهد الوطني للمعايير التقنية ٢٠٢٣) .

رابعاً/ استخدام الذكاء الاصطناعي في مكافحة الجريمة السيبرانية: في ظل التطور التكنولوجي المتسارع، أصبحت الجرائم السيبرانية تشكل تهديداً كبيراً للأفراد والشركات وحتى الحكومات، فالحقيقة أن معظم الهجمات الالكترونية تتمحور حول الشبكة التي تتم بواسطة عملاء اذكياء، مثل الفيروسات، وبالتالي لابد من محاربتها بعوامل ذكية شبه مستقلة يمكنها اثبات الهجمات السيبرانية وتقييمها والرد عليه ، ومع تزايد تعقيد هذه الجرائم، ظهر الذكاء الاصطناعي (AI) كأداة فعالة لمكافحتها، إذ يوفر حلولاً ذكية وسريعة للكشف عن التهديدات الأمنية والتصدي لها (حسين ٢٠٢٤) . إذ يمكن للذكاء الاصطناعي تحليل كميات هائلة من البيانات لاكتشاف أنماط غير طبيعية، مثل الهجمات الإلكترونية أو محاولات الاختراق، كما يمكنه تعزيز أنظمة الحماية عبر التعلم الآلي لاكتشاف التهديدات الجديدة (karmi 2023)

خامساً/ تشفير البيانات الحساسة: تعد تقنيات التشفير من أهم الأدوات لحماية البيانات الحساسة سواءً أثناء تخزينها (Data at Rest) أو نقلها عبر الشبكات (Data in Transit). إذ يعتمد التشفير على تحويل البيانات إلى صيغة غير قابلة للقراءة إلا باستخدام مفتاح فك التشفير المناسب. ومن أهم طرق تشفير البيانات هي كالتالي (walliam 2023) :

١- تشفير الملفات والمجلدات عبر استخدام خوارزميات قوية مثل AES-256 (معيار التشفير المتقدم)، وأدواته مثل BitLocker (لنظام Windows) و FileVault (لنظام macOS).

٢- تشفير قواعد البيانات عبر تشفير الحقول الحساسة مثل كلمات المرور والمعلومات المالية باستخدام Transparent Data Encryption (TDE) في أنظمة مثل SQL Server و Oracle.

٣- تشفير الاتصالات الشبكية عبر استخدام بروتوكولات آمنة مثل:TLS/SSL لحماية اتصالات الويب (HTTPS)، و VPN لتشفير البيانات المتبادلة عبر الشبكات العامة.

٤- تشفير الأجهزة المحمولة والأقراص الصلبة عبر تفعيل ميزة التشفير الكامل (Full Disk Encryption – FDE) على الهواتف والأجهزة المحمولة.

سادساً/ النسخ الاحتياطي المنتظم للبيانات: يعد النسخ الاحتياطي أحد الركائز الأساسية للأمن السيبراني واستمرارية الأعمال، إذ يحمي البيانات من الفقدان بسبب الهجمات الإلكترونية (مثل برامج الفدية)، الأعطال التقنية، أو الكوارث الطبيعية (person 2007 , 45)

سابعاً/ مراقبة الشبكة باستخدام أنظمة كشف التسلل (IDS/IPS): تعد من الأدوات الأساسية في تأمين البنية التحتية للشبكات. إذ إن IDS (نظام كشف التسلل) يراقب حركة الشبكة ويبلغ عن الهجمات (مثل Snort). أما IPS (نظام منع التسلل) يمنع الهجمات تلقائياً (مثل Suricata) (Richard)

أما في العراق، تواجه العراق العديد من التحديات في مجال الأمن السيبراني، والتي تؤثر على أمنه القومي واستقراره الاقتصادي والسياسي. من أبرزها ، ضعف البنية التحتية الرقمية، و نقص الكوادر المؤهلة، فضلاً عن غياب التشريعات والقوانين الفعالة (سعيد ٢٠١٥ ، ٦٠)، ولذلك يتطلب تعزيز الأمن السيبراني في العراق استثمارات كبيرة في البنية التحتية، وتدريب الكوادر، وتطوير التشريعات، وتعزيز التعاون الإقليمي والدولي.

ويشهد الأمن السيبراني في العراق تطوراً تدريجياً في السنوات الأخيرة، رغم التحديات الكبيرة التي تواجهها البلاد في هذا المجال فمنها (الشمري ٢٠١٥) :

١- على المستوى الحكومي

أ- إنشاء الجهات المختصة: تأسيس المركز الوطني للاستجابة للطوارئ السيبرانية (IQ-CERT) لرصد ومكافحة الهجمات الإلكترونية. فضلاً عن تشكيل فرق الاستجابة للطوارئ السيبرانية (CSIRT) في بعض الوزارات. إذ إن في عام ٢٠٢١، أقر مجلس الوزراء العراقي قانون الهيئة الوطنية للأمن السيبراني بموجب القانون رقم (٩) لسنة ٢٠٢١، والتي تهدف إلى حماية البنية التحتية الرقمية للدولة ، وتطوير استراتيجيات وسياسات الأمن السيبراني. فضلاً عن التنسيق بين المؤسسات الحكومية لتعزيز الحماية من الهجمات الإلكترونية (قانون الهيئة الوطنية للامن السيبراني ٢٠٢٥) .

ب-التشريعات والقوانين: إصدار قانون الجرائم الإلكترونية العراقي (رقم ٥ لسنة ٢٠٢٢) الذي يجرم الاختراق والتجسس الإلكتروني، والعمل على تحديث القوانين لمواكبة التهديدات الحديثة مثل التصيد الإلكتروني وبرامج الفدية.

ت-التعاون الدولي: تعاون العراق مع منظمات مثل الاتحاد الدولي للاتصالات (ITU) والإنتربول لتحسين القدرات الدفاعية. فضلاً عن توقيع اتفاقيات مع دول مثل الأردن والإمارات لتبادل الخبرات في الأمن السيبراني.

٢- على مستوى القطاع الخاص والبنوك: بدأت بعض البنوك العراقية تطبيق أنظمة تشفير متقدمة لحماية المعاملات المالية. فضلاً عن زيادة استخدام جدران الحماية (Firewalls) وأنظمة كشف التسلل (IDS/IPS).

٣- التدريب وبناء الكوادر: عقدت دورات تدريبية بالتعاون مع منظمات دولية لرفع كفاءة المختصين. فضلاً عن إطلاق برامج جامعية وتخصصية في الأمن السيبراني في بعض الجامعات العراقية.

الخاتمة:

يعد الأمن السيبراني في العراق تحديا كبيرا، إذ يحتاج إلى تضافر الجهود بين الحكومة والقطاع الخاص والمجتمع المدني. ورغم ذلك ، فإن الوعي المتزايد بأهمية هذا المجال يبشر بتحسينات مستقبلية مما يساهم في تحقيق التنمية المستدامة في العراق. إذ بدأت الحكومة العراقية والقطاع الخاص باتخاذ خطوات لتعزيز الأمن السيبراني، منها، إنشاء المركز الوطني للأمن السيبراني ، فضلاً عن التعاون مع المنظمات الدولية: مثل الاتحاد الدولي للاتصالات (ITU) لتحسين القدرات الدفاعية في مواجهة التهديدات الإلكترونية. ومحاولة زيادة الوعي المجتمعي من خلال حملات توعوية تستهدف المؤسسات والأفراد لتعريفهم بأهمية الحماية الإلكترونية. فضلا عن تطوير التشريعات الوطنية ، إذ تسعى الحكومة العراقية إلى تحديث القوانين الخاصة بالجرائم الإلكترونية لتكون أكثر فاعلية في مواجهة التحديات الحديثة.

المصادر باللغة العربية :

١- المعجم الموحد لمصطلحات الحاسوب ، ٢٠٠٥ . المنظمة العربية للتربية والثقافة والعلوم .
٢- حمدي ، جاسم . ٢٠١٩ . *الامن السيبراني : المفاهيم والتطبيقات* . عمان : دار المناهج.
٣- الهيئة الوطنية للامن السيبراني ، ٢٠١٨ . إستراتيجية الامن السيبراني لدولة الامارات .
٤- الوهيبي ، خالد عبد الله . ٢٠٢٠ . *الحرب السيبرانية : المفاهيم والتهديدات والاستراتيجيات* . الرياض : دار جامعة الملك سعود للنشر .
٥- الغامدي ، خالد . *الجريمة الالكترونية والامن السيبراني* .
٦- تقرير الانتربول عن الجرائم السيبرانية . ٢٠٢٣ .
٧- محمد ، هديل ناصر جاسم . ٢٠٢٤ . " دور الاحزاب السياسية في الاستقرار السياسي : تونس انموذجا" . *المجلة السياسية والدولية* . الجامعة المستنصرية – كلية العلوم السياسية . العدد (٦٠) .
٨- عارف ، نصر محمد . ٢٠٠٣ . *النظم السياسية : الدولة والحكومة* . مصر : المكتبة الاكاديمية .
٩- احمد ، سمير نعيم . ٢٠١٠ . *التحول الديمقراطي والاستقرار السياسي* . بيروت : مركز دراسات الوحدة العربية.
١٠-فيبر ، ماكس . ٢٠٠٥ . *الاقتصاد والمجتمع : مقدمة في علم الاجتماع التفهمي* . ترجمة : محمد ناصر الجوهري . القاهرة : الهيئة العامة المصرية للكتاب .
١١-سليم ، محمد السيد . ٢٠١٥ . *تحليل السياسات العامة* . الاسكندرية : دار الجامعة الجديدة .
١٢- عوض ، جابر سعيد . ٢٠١٢ . *الاستقرار السياسي في العالم العربي* . القاهرة : دار الشروق .
١٣- النفيسي ، عبد الله . ٢٠٠٧ . *الدولة والاستقرار في الخليج* . الكويت : دار قرطاس .
١٤- الجابري ، محمد عابد . ٢٠١٠ . *المسألة السياسية في الوطن العربي* . بيروت : مركز دراسات الوحدة العربية.
١٥- أمين ، سمير . ٢٠٠٨ . *الامن القومي العربي* . القاهرة : دار المستقبل العربي .
١٦- السويدي ، جمال سند . ٢٠١٥ . *الامن الوطني الاماراتي في عالم متغير* . ابو ظبي : مركز الامارات للدراسات والبحوث الاستراتيجية .
١٧- تقرير الامن السيبراني العالمي ، ٢٠٢٣ . جنيف : المنظمة الدولية للامن السيبراني .
١٨- ميتينك ، كيفن . ٢٠١٩ . *فن الاختراق : القصص الحقيقية وراء إستغلال القراصنة والمتسللين والمخادعين*.ترجمة : فريق الترجمة بجامعة الملك سعود .

المصادر باللغة الانكليزية :

1. The Unified Dictionary of Computer Terms, 2005. Arab League Educational, Cultural and Scientific Organization.
2. Hamdi, Jassim. 2019. Cybersecurity: Concepts and Applications. Amman: Dar Al-Manahij.
3. The National Cybersecurity Authority, 2018. Cybersecurity Strategy for the United Arab Emirates.

4. Al-Wahaibi, Khaled Abdullah. 2020. Cyberwarfare: Concepts, Threats, and Strategies. Riyadh: King Saud University Press.
5. Al-Ghamdi, Khaled. Electronic Crime and Cybersecurity.
6. Interpol Report on Cybercrime. 2023.
7. Muhammad, Hadeel Nasser Jassim. 2024. "The Role of Political Parties in Political Stability: Tunisia as a Model." Political and International Journal. Al-Mustansiriya University - College of Political Science. Issue (60).
8. Aref, Nasr Muhammad. 2003. Political Systems: State and Government. Egypt: Academic Library.
9. Ahmed, Samir Naeem. 2010. Democratic Transition and Political Stability. Beirut: Center for Arab Unity Studies.
10. Weber, Max. 2005. Economy and Society: An Introduction to Comprehensive Sociology. Translated by: Muhammad Nasser Al-Jawhari. Cairo: General Egyptian Book Organization.
11. Salim, Muhammad Al-Sayyid. 2015. Public Policy Analysis. Alexandria: Dar Al-Jami'a Al-Jadida.
12. Awad, Jaber Saeed. 2012. Political Stability in the Arab World. Cairo: Dar Al-Shorouk.
13. Al-Nafisi, Abdullah. 2007. State and Stability in the Gulf. Kuwait: Dar Qurtas.
14. Al-Jabri, Muhammad Abed. 2010. The Political Question in the Arab World. Beirut: Center for Arab Unity Studies.
15. Amin, Samir. 2008. Arab National Security. Cairo: Dar Al-Mustaqbal Al-Arabi.
16. Al-Suwaidi, Jamal Sanad. 2015. UAE National Security in a Changing World. Abu Dhabi: Emirates Center for Strategic Studies and Research.
17. Global Cybersecurity Report, 2023. Geneva: International Cybersecurity Organization.
18. Mitink, Kevin. 2019. The Art of Hacking: The Real Stories Behind the Exploitation of Hackers, Intruders, and Phishers. Translated by: King Saud University Translation Team.
19. Wiener, N,1948. Cybernetics: Or Control and Communication in the Animal and the Machine, Paris: Hermann & Cie.
20. Scott J. White,2018 . Cyber Intelligence Handbook, Taylor & Francis Group .
21. Richard A. Clarke, 2010 . Cyber War: The Next Threat to National Security and What to Do About It, HarperCollins .
22. Allied Joint Doctrine for Cyberspace Operations, 2020 .
23. Michael Schmitt, 2017 . International Law and Cyber Warfare. Oxford University Press .
24. Martin C. Libicki, 2009 . Cyberdeterrence and Cyberwar. RAND Corporation .