Ashur Journal of Legal and political Sciences (AJLSP) is published by the Iraqi Association for Legal Sciences
ISSN: 3005-3269, Vol 3(No.2), pages: 298-318 (2026)
https://ashurjournal.com/index.php/AJLPS/about

Iraq and the Challenges of Cybersecurity

Assistant Lecturer Harir Essam Mohammed

Center for Strategic and International Studies / University of Baghdad, harir.e@cis.uobaghdad.edu.iq

ARTICLE INFORMATION

Received:1 Mar 2026
Accepted:18 Mar 2026
Published:1 Jun 2026

Keywords:

-cyber security
-information security
- cyber warfare
- cyberspace

ABSTRACT

The national (strategic) security system of Iraq faces a number of challenges that can be classified into visible and invisible challenges. The most dangerous of these challenges are the invisible ones, which cannot be directly perceived except through research and analytical induction. These cyber challenges are a strategic threat that will affect strategic security (for individuals, institutions and the state), meaning that these challenges include most governmental and non-governmental sectors and institutions These cyber challenges pose a strategic threat that can affect strategic security (of individuals, institutions, and the state), meaning that these challenges encompass most governmental and non-governmental sectors and institutions

مجلة آشور للعلوم القانونية والسياسية تصدر عن الجمعية العراقية للعلوم القانونية
المجلد الثالث (العدد الثاني)، الصفحات:298 - 318، (2026) ISSN: 3005-3269
https://ashurjournal.com/index.php/AJLPS/about

العراق و تحديات الأمن السيبراني

م . م حرير عصام محمد

مركز الدراسات الاستراتيجية و الدولية / جامعة بغداد ، harir.e@cis.uobaghdad.edu.iq

معلومات المقالة

تاريخ الاستلام : ١ اذار ٢٠٢٦
تاريخ القبول :١٨ اذار ٢٠٢٦
تاريخ النشر : ١ حزيران ٢٠٢٦

الملخص

إن منظومة الأمن الوطني (الاستراتيجي) للعراق تواجه جملة من التحديات و التي يمكن تصنيفها الى تحديات مرئية و غير مرئية و تتجلى أخطر هذه التحديات هي غير المرئية ، فلا يمكن التماسها بصورة مباشرة الا من خلال البحث و الاستقراء التحليلي ، و هذه التحديات السيبرانية تعد تهديداً استراتيجيا من شأنها ان تؤثر على الامن الاستراتيجي (للأفراد و المؤسسات و الدولة) بمعنى ان هذه التحديات تشمل معظم القطاعات و المؤسسات الحكومية و غير الحكومية .

الكلمات المفتاحية:

- الأمن السيبراني
- أمن المعلومات
- الحرب السيبرانية
- الفضاء السيراني

المـقدمة

شهد القرن الحادي و العشرين تطورا هائلً في مجال تكنولوجيا المعلومات و الاتصالات ولقد نجم عن التطور التكنولوجي السريع لتكنولوجيا المعلومات و الاتصالات تحولاً كبيراً في مفهوم الامن ، اذ برز مفهوم الامن السيبراني و بات من الضروري تحقيقه و تقوم فكرة الامن السيبراني على تأمين البنية التحتية للمعلوماتية و البيانات الضرورية سواء للدولة أو المؤسسات الحكومية و غير الحكومية و الافراد من الجرائم الالكترونية ، اذ اصبحت قضية أمن و حماية المعلومات من أهم قضايا العصر، و دور الامن السيبراني هنا هو منع وقوع مثل هذه الافعال التي تضر بمصلحة الافراد و المجتمع و تلحق الضرر بهم و من الجدير بالذكر بعد الحرب الباردة أصبح العالم يواجه تحديات و تهديدات لم يشهدها من قبل المجتمع الدولي و التي تعرف بالتحديات و التهديدات العابرة للحدود التي لا تعترف بالحدود الجغرافية و تشمل هذه التهديدات اي هجوم ضار محتمل يسعى الى الوصول الغير مصرح به (غير قانوني) الى معلومات و بيانات مهمه و الحصول عليها او تسريبها او اتلافها وغيرها و هذه التهديدات السيبرانية تؤثر على منظومة الامن الوطني حيث تشكل تهديداً مباشراً على الثوابت القيمية و البنى التحتية لأي مجتمع و في (العراق) تعمل استراتيجية الامن السيبراني على تكوين استراتيجية منسقة لأداره هذه التهديدات في الفضاء السيبراني بما يتماشى مع المصلحة العامة و تحقيق الامن السيبراني.

اولاً / أهمية البحث : و تنبع أهمية هذا البحث من خلال تسليط الضوء على التحديات الجديدة التي بدأت تواجهه العالم ، و هي التحديات السيبرانية و ضرورة الحد منها ، ففي عالم اليوم الرقمي الذي تتزايد فيه التحديات و التهديدات السيبرانية أصبحت الحاجة الى الامن السيبراني أمراً بالغ الاهمية ، فالامن السيبراني هو عبارة عن المجال الذي يهدف الى الى حماية الانظمة و البيانات و المعلومات و الشبكات من الهجمات او الاختراقات الالكترونية و ضمان الحفاظ على المعلومات و البيانات من الاختراقات او التلاعب و ضمان سلامتها .

ثانياً/ الإشكالية : و يقوم البحث على إشكالية مفادها الاتي :

1. ماهية الامن السيبراني و خصائصه ؟
2. علاقة الامن السيبراني بالمفاهيم المقاربة له ؟
3. ماهي علاقة الفضاء السيبراني بالجغرافية السياسية ؟
4. ماهي ابرز التحديات التي تواجهه الامن السيبراني العراقي
5. ماهي ابرز آليات او سبل معالجة هذه التحديات ؟

ثالثاً/ فرضية البحث : تنطلق الدراسة من فرضية مفادها ان في ظل التطورات التكنولوجيا الحديثة و المتسارعة التي يشهدها العالم و التوجه نحو الاعتماد على التحول الرقمي ، بات من الضروري تحقيق السيطرة على حماية امن

المعلومات و السيطرة و تحقيق الامن السيبراني في ظل التحديات العديدة التي يواجها و المتمثلة بالهجمات و الاختراقات و غيرها .

رابعاً /هيكلية البحث : تقسمت الدراسة الى مبحثين بالإضافة الى المقدمة و الخاتمة و الاستنتاجات ، و قد تناول المبحث الاول مفهوم الامن السيبراني ، أما المبحث الثاني فقد تناول تحديات و أبعاد الامن السيبراني في العراق .

المبحث الاول

مفهوم الأمن السيبراني

أن ظهور الثورة التكنولوجية الرقمية الجديدة و التي كانت نتيجتها زيادة المعلومات بصورة كبيرة و ذلك بسبب التعداد الهائل في وسائل الاتصالات و نظم الحاسوب و غيرها من نظم المعلومات حيث برز المفهوم الخاص بالأمن السيبراني حتى يكون المحور للجانب الأمني الذي يختص بحماية قاعدة البيانات و المعلومات .

أولا / التعريف بماهية الامن السيبراني و خصائصه

التعريف اللغوي / أن كلمة سيبراني أو سايبر تعتبر ترجمة حرفية لكلمة (Cyber) و المشتقة من كلمة (Cybernetics) و قد أستخدم هذا المصطلح أكاديميا من قبل عالم الرياضيات الأمريكي (نوربت وينير) عام 1948م في كتابه الشهير (علم التحكم الآلي) أو التحكم و الاتصال في الآلة و ذلك للإشارة الى آليات التنظيم الذاتي .[1]

التعريف الاصطلاحي / يقول المختصون في هذا المجال أن مصطلح الأمن السيبراني أتى من لفظ (Cyber) اللاتينية و معناها الفضاء المعلوماتي و يعني مصطلح الأمن السيبراني بأنه أمن الفضاء المعلوماتي و هو عبارة عن تعبير شامل عن العالم الافتراضي الذي يحوي كل ما يتعلق باستعمالات و آليات و تطبيقات و تجهيزات تقنية المعلومات و الحاسوب الآلي و الاتصالات و الانترنيت .[2]

ولكن من الجدير بالذكر ان من أهم التحديات التي تواجهه مصطلح الامن السيبراني هو الاستعمال غير المدروس للمصطلح فلا يوجد تعريف واحد متفق عليه للأمن السيبراني ، اذ هماك من يعده متداخلاً مع أمن المعلومات مدعياً ان الامن السيبراني فرع من أمن المعلومات و هناك من يربط بين الامن السيبراني و الخاصية العالمية للأنترنيت على أعتبار انه أوسع من أمن المعلومات الذي يهتم أساساً بالسرية . [3]

و من أبرز تعريفات الامن السيبراني : [4]

هناك من عرف الامن السيبراني على انه الاسلوب و الاجراءات المرتبطة بعملية إدارة المخاطر الامنية التي تتبعها المنظمات و الدول لحماية سلامة و سَرية و توافر البيانات و الاصول المستعملة في الفضاء السيبراني و يتضمن المفهوم

ارشادات و سياسات و مجموعات من الضمانات و التقنيات و الادوات و التدريب و ذلك لتوفير أفضل حماية لحالة البيئة السيبرانية و مستخدميها .

تعريف الاتحاد الدولي للاتصالات للأمن السيبراني : انه مجموعة من الادوات و السياسات و المفاهيم الامنية و المبادئ التوجيهية و نهج إدارة المخاطر و الاجراءات و الممارسات الفضلى و الضمانات التكنولوجية التي يمكن استعمالها لحماية البيئة السيبرانية و المنظمة و أصـول المستعمل و يقصد بالأصول هنا أجهزة الحاسوب و مستعمليه و أنظمة الاتصالات و الخدمات و التطبيقات و جميع المعلومات الموجودة في الفضاء السيبراني بما يضمن سلامة الـخدمة و سَريتها و استمرارها و حمايتها من المـخاطر الأمنية المنتشرة في البيئة السيبرانية .

أ) خـصائص الأمـن السيبراني

ان للأمن السيبراني خصائص متعددة يمكن توضيحها بما يلي : [5]

1. الحماية من التهديدات الداخلية / و التي تعد واحدة من أهم مميزات الأمن السيبراني فقد تتعرض المعلومات الى هجوم الكتروني و ذلك بسبب ضعف معرفة المستخدمين في هذا المجال و فيه يتم السماح ببرامج مجهولة المصدر بالتفعيل أو القيام باستخدام أدوات تمـس الأمن الشخصي للمستخدم و هنا يبرز دول الأمن السيبراني من خلال سرعة تنبيه الفرد أو المؤسسة بالخطر و منع وقوعه في أسرع وقت ممكن.
2. الرؤية الشـاملة / أذ تمنح وسائل الأمن السيبراني لمستخدميها سواء كانوا افراد أم شركات رؤية شاملة على نقاط القوة و الضعف في انظمتهم و من خلال ذلك يكون بإمكانهم معرفـة الثغرات التكنولوجية و حلها بأسرع وقت و كذلك أبداء المقترحات الخاصة بالطرق المثلى لمنع تكرار هذه الثغرات.
3. المـراقبة المستمرة / حيث تعمل جدران الـحماية في وقت محدد و تتوقف بالعمل باستمرار لغرض الكشف عن أي ثغرة أو خلل و العمل على التعامل معه و معالجته بالسرعة الممكنة .
4. الامتثال للقوانين و السياسات / اذ لا يتيح لمصادر خارجـية الاطلاع على ما يتم مشاركته من معلومات و بيانات او اساءة استغلالها بأي صورة كانت .
5. التنـوع / أي انه يمتلك حلولاً متنوعة و متعددة فيما يخص معالجة مشاكل الامن السيبراني كما و يتعامل مع كافة أنواع التهديدات المهددة لسلامة و أمن المعلومات.

ب) خصـائص الفضاء السيبراني

و تعود أسباب اهتمام الفاعلين سواء أكانوا من الدول ام من غيرها بهذا الفضاء كمجال لتحقيق الهيمنة و النفوذ و أدارة الصرعات الى امتلاكه عدة سمات أساسية و أهمها الآتي :[6]

1) ان الفضاء السيبراني عبارة عن ساحة صراع افتراضية : فالفضاء السيبراني مساحة افتراضية و ليست جغرافية لذلك يتخطى الفضاء السيبراني العديد من الثنائيات التي تظهر في الصراعات التقليدية ، وخسائر الصراعات في الفضاء السيبراني اقل كلفة على الصعيد المادي و أكثر تحديداً للهدف مقارنة بالصراعات التقليدية

2) زيادة الاعتماد التكنولوجي : إذ باتت الدول الحديثة تربط بنيتها التحتية بالفضاء السيبراني ، مثل شبكات الكهرباء و البنوك و البورصة و الاتصالات و غيرها فضلاً عن أنظمة السيطرة و التحكم العسكرية و جمع المعلومات مثل الاقمار الصناعية و الطائرات دون طيار ، و من ثم أصبح استهداف تلك البنى التحتية للدولة ذات الطابع الالكتروني أحد عوامل الصراع السيبراني .

3) تماهي حدود الداخل والخارج : اي بمعنى وجود حالة من التأثير الشبكي المتزايد داخل الشبكة و خارجها ، إذ اتسع استعمال الافراد و الدول و المنظمات و الشركات للتكنولوجيا الحديثة المرتبطة بالفضاء السيبراني .

4) غياب الشفافية الالكترونية : فمع عدم القدرة على معرفة هويات القائمين على الهجمات الالكترونية مثل عمليات القرصنة الالكترونية ، نشبت معضلة غياب الشفافية و القوانين المقيدة للصراعات في المجال السيبراني .

5) ان الفضاء السيبراني لا يقتصر على شبكة الانترنيت فحسب و أنما شبكات عالمية و خاصة أخرى مثل (GPS , ACARS, PSTN,SWIFT) .

6) القدرة على التشبيك و بناء روابط افتراضية ، إذ تتيح الادوات السيبرانية للأفرادة قدرة أكبر على التواصل و التشبيك و بناء مجتمعات افتراضية بأشكال مختلفة للتأثير في القضايا على عبر وسائل التواصل الاجتماعي .

ثانيا : الأمن السيبراني و المفاهيم المقاربة له

هناك العديد من المفاهيم المرتبطة بالأمن السيبراني و من أهمها ما يأتي

1. الإرهاب السيبراني / ان مفهوم الارهاب السيبراني (Cyber Terrorism) ظهر في ثمانينيات القرن العشرين فقد عرفه باري كولين (Barry colin) آنذاك بتعريف عام بأنه هجمة إلكترونية الغرض منها تهديد الحكومات او العدوان عليها سعياً لتحقيق أهداف سياسية أو أيديولوجية وتكون ذات أثر تخريبي مكافئ للأفعال المادية للإرهاب ،

كما عرف دورثي دينيغ (Dorothy Denningg) الارهاب السيبراني بأنه الهجوم القائم على مهاجمة الحاسوب و ان التهديد به يهدف الى الترويع أو أجبار الافراد أو المؤسسات أو الحكومات بهدف تحقيق غايات و أهداف سياسية أو عقائدية و يكون هذا الهجوم مدمراً و تخريبياً لتوليد الخوف و الذعر بحيث يكون مشابهاً للأفعال المادية للإرهاب . [7]

و من الجدير بالذكر ان بعد أحداث 11 أيلول 2001 أصبح هناك ارتباط واضح بين الانترنيت و الارهاب ، اضحت المواجهة الالكترونية ضد الارهابيين بعد ان كانت قد اقتصرت على مواجهة مادية فحسب و تحولت الحروب الى حروب رقمية و ذلك بعد ان اصبح الانترنيت أكثر الاسلحة تدميراً و تأثيراً و من الممكن القول ان الاختلاف الوحيد

بين الارهاب العام و الارهاب السيبراني هو نوعية الاداة المستعملة لتحقيق الهدف اذ يوظف الارهاب السيبراني التكنولوجيا كوسيلة لتحقيق اهدافه بدلا من الاسلحة التقليدية.[8]

2. أمن المعلومات / و هو من المفاهيم المقاربة للأمن السيبراني و يعرف أمن المعلمات بشكل مختصر بأنه حماية المعلومات من الوصول غير المصرح به كما يعرف أيضاً بأنه المفاهيم و التدابير و التقنيات الادارية و التقنية المستعملة لحماية أصول المعلومات من الوصول غير المأذون به عمداً أو سهواً أو حيازتها أو الاضرار بها أو التلاعب بها أو إساءة استخدامها و يعد أمن المعلومات من المفاهيم الحديثة المشابهة للأمن السيبراني[9].

3. الحرب السيبرانية / و تعد الحرب السيبرانية مفهوماً جديداً على صعيد النزاعات المسلحة و تشمل هذه الحرب على أساليب و وسائل قتالية تتألف من عمليات الكترونية ترقى الى مستوى النزاع المسلح و تستعمل في سياقة و تعمل هذه الحرب على التدمير الكلي لأنظمة المعلومات و شبكات الاتصال [10].

4. الاستراتيجية السيبرانية / و هي عبارة عن خطط و طريقة لأداره جميع العمليات السيبرانية بطريقة حكيمة في جميع مؤسسات و قطاعات الدولة تفادياً للتهديدات السيبرانية الداخلية و الخارجية لتحقيق أمن الدولة و الوصول الى هدفها المبتغى و تتغير هذه الاستراتيجية بتغير المعطيات المتحكمة بالبيئة الدولية ، و يعد المفكر الامريكي (جوزيف ناي) أبرز المهتمين بالاستراتيجية السيبرانية و يعرفها (بأنها القدرة على الحصول على النتائج المرجوة عن طريق استعمال مصادر المعلومات المرتبطة بالفضاء السيبراني) اي انها القدرة على استعمال الفضاء السيبراني لخلق مزايا للدولة[11].

5. الهجمات السيبرانية / و هي اجراءات عديدة تتخذها الدولة لغرض الهجوم على نظم المعلومات المعادية بهدف الاضرار بها و التأثير عليها و تحقيق عدد من الاهداف و في الوقت ذاته لغرض الدفاع عن النظم و المعلومات الخاصة بالدولة المهاجمة [12] .

6. الصراع السيبراني / و يعد الصراع السيبراني أحد أوجهه الصراع الدولي ، إذ يستطيع أحد أطراف الصراع أن يوقع خسائر فادحة بالطرف الاخر ، و انه قد يتسبب في فشل البنية المعلوماتية و الاتصال الخاص به و هو مايسبب خسائر عسكرية و اقتصادية فادحة من خلال قطع أنظمة الاتصالات بين الوحدات العسكرية ببعضها البعض أو تضليل معلوماتها أو سرقة معلومات مهمه و سرية عنها [13].

ثالثا : الجغرافية السياسية و الأمن السيبراني

أ) القوة السيبرانية و المجال الحيوي الخامس

اصبحت مساحة المعلومات مجالاً جديداً للجغرافية السياسية و غيرت توازن القوى بين الجغرافية السياسية للدول ، إذ وجد الانترنيت فضاءاً جديداً بالكامل و يتجاوز فضاء المعلومات المساحة الجغرافية المكانية التقليدية ففضاء المعلومات يجعل الجغرافية السياسية لها ميزات و خصائص مكانية جديدة حيث كان التحدي السابق يتمثل في الدفاع عن حدود

الدولة في حين ساهمت تقنيات المعلومات و الشبكات في إضعاف الحدود الجغرافية التقليدية بين الدول و أصبح من السهل للغاية اختراقها [14] .

كما توسعت أيضاً السيـادة الـوطنية من المناطق و المجال الحيوي الى (حدود المعلومات) و تغيير الفكر الجيوسياسي التقليدي و القائم على العوامل الطبيعية للجغرافية و مما يجعل من أمن المعلومات جزءاً جديداً مهماً من السيادة الوطنية كما أصبح أمن حدود المعلومات جزءاً مهماً من ألامن الـقومي[15] .

و من الممكن القول ان الفضاء السيبراني يعد الميدان الجديد المؤثر للحروب الحديثة و على الرغم من انه ميدان صناعي تحكمه بروتوكولات تدفق البيانات عبر الاسلاك و بين الاجهزة في موجات هوائية الا انه أصبح عصب الحياة البشرية و ذلك من خلال ادارة مؤسسات الحياة اليومية جميعها ، إذ أحدث التطور في مجال الفضاء السيبراني تحولاً كبيراً في مفهوم القوة نتج عنه دخول المجتمع الدولي في مرحلة جديدة تؤدي فيها الهجمات السيبرانية دوراً أساسياً في التأثير على طبيعة الحروب الحديثة و أصبح النفوذ في مجال تسليح الفضاء السيبراني عنصراً حيوياً في تنفيذ عمليات عسكرية فاعلة الأرض و الجو و البحر و ذلك من خلال الاعتماد على نظام التحكم و السيطرة على الفضاء السيبراني [16] .

ومن الجدير بالذكر ان الفضاء السيبراني عد المجال الحيوي الخامس الذي يلي كل المجالات البرية و البحرية و الجوية و الفضاء الخارجي ، و ان كان وجود هذه المجال افتراضياً الا ان كل ما يدور في هذا المجال او الحيز من منافسة و صراع و حروب حديثة و هجمات جميعها حقيقية و ذات تأثير و أبعاد سياسية ، إذ لا تنحصر أبعاد و تداعيات هذه الحروب الحديثة لا يقتصر على الفضاء السيبراني فحسب ، إذ من المتوقع ان من يتحكم في الحيز الافتراضي سيكون له الصدارة في قيادة العالم [17].

ب) الجغرافية الـخامسة

ان من الملائم عد الفضاء السيبراني نطاقاً جغرافياً خامساً للحرب و السلام و الدفاع و الاستراتيجية ، بعد (البر و البحر و الجو و الفضاء الـخارجي) ، فأنه يختلف اختلافاً جذرياً عن الجغرافية الاخرى ، ذلك يعزى لما يتمتع من مستعملين و الآلات متخصصة فضلاً عن التفاعلات الالكترونية و بهذا لا يمكن ان نعده مجرد جغرافية أخرى في المجال (السياسة، الصراع ، الاستراتيجية) بل انها وحدة فريدة من نوعها ، حيث قد تعمل الاتجاهات الجيوسياسية العالمية على ان تكون حاضرة في البيئة السيبرانية و بشكل مكثف فالابتكار الرقمي يتيح للخصوم السياسيين فرصة متزايدة لإيجاد نقاط الضعف التي يمكنها تدمير قدرات القوة الاقتصادية و العسكرية للدولة المعادية [18].

وتقف الجغرافية السياسية في مفترق طرق شديد الخطورة عندما يصبح مجال الفضاء الالكتروني هو خط المواجهة الرئيس و على مدى السنوات الماضية بذلت الحكومات و الشركات و المجموعات غير الحكومية في منطقة الشرق

الاوسط جهوداً كبيرة لبناء قدراتها الالكترونية لمواجهة التهديدات السيبرانية و من الجدير بالذكر ان انتشار الاسلحة الالكترونية و استعمالها بوصفها أدوات جيوسياسية قد يؤدي الى تصاعد الازمات الاقليمية و تفاقمها[19].

المبحث الثاني

تحديات و أبعـاد الأمن السيـبراني في العراق

هناك العديد من التحديات و التهديدات التي تواجهه الامن السيبراني والتي تعتبر أكبر آفـة يتعامل معها العالم الرقمي و التي في الغالب ما تتسبب في خسائر فادحة يصعب التعامل معها و هنا يبرز دور الامن السيبراني حيث ان الامن السيبراني لا يقوم بالدفـاع ضد الهجمات السيبرانية فحسب و أنما يمنع حدوثها من الاساس[20].

ولابد لنا من الاشارة الى الفرق بين التحديات و الهجمات التي يتعرض لها الامن السيبراني

أ) الهجمات التي يتعرض لها من خلال الاسلحة التقليدية حيث يتكون الفضاء السيبراني من ثلاث طبقات رئيسة تكون عرضة للهجوم التقليدي اي استعمال الاسلحة التقليدية لتدمير البنية التحتية للفضاء السيبراني و هذه الطبقات تتضمن
1) الطبقة المادية / و التي تكون الاساس في عمـل الطبقات الاخرى و تكون هذه الطبقة من الاقمار الصناعية و الاجهزة و الكابلات و المعدات الاخرى.
2) الطبقة النحوية / و هي عبارة عن برامج توافر تعليمات التشغيل للطبقة الاولى المادية
3) الطبقة الدلالية / و تشمل هذه الطبقة التواصل و التأثير المتبادل بين المعلومات و البشر بواسطة أجهزة الحاسوب وهذه الطبقات تتعرض الى هجمات مادية وذلك من خلال استعمال الاسلحة التقليدية بهدف ضرب و تدمير البنى التحتية للأمن السيبراني لدولة أو مؤسسة أو شركة .

ب) أما بالنسبة للتحديات التي تتمثل بالهجمات السيبرانية و التي تهدد الامن السيبراني و ذلك من خلال عمليات الاختراق او التشويش او التجسس او سرقة المعلومات المهمة من أجهزة الحاسوب أو أتلاف بيانات مهمة و غيرها وتتمثل هذه التهديدات بالآتي. أ)البـرامج الخبيثة / و هي نوع من البرامج المصممة خصيصاً للوصول غير المصرح به الى جهاز الكمبيوتر أو إلحاق الضرر به بمعنى انها تتضمن مجموعة من البرامج التي يتم انشاؤها من أجل منع أطراف ثالثة أمكانية الوصول غير المصرح به الى المعلومات المهمة أو القدرة على تعطيل سير العمل العادي للبنية الاساسية ومن ابرز الامثلة على هذه البرامج (حصان طروادة ، برامج التجسس ، الفيروسات) و هي برامج مصممة بالأساس بهدف اتلاف انظمة الحماية المثبتة على النظام.
ب) تصيد البيانات و المعلومات / وهـي عملية أرسال رسائل بريد الكتروني احتيالية تشبه رسائل البريد الالكتروني من المصادر الموثوقة و الهدف منها هو سرقة البيانات و المعلومات المهمة مثل سرقة ارقام بطاقة الائتمان و تعد عملية تصيد المعلومات و سرقتها الاكثر شيوعاً [21] .

و سنتناول هنا أبرز التحـديات التي تواجهه الامن السيبراني [22] .

1) صعوبة معرفة مصدر الهجمات / فعلى الرغـم مما وصلت اليه التكنولوجيا من تقدم في عملية التتبع الا انها في الوقت نفسه تتقدم في عمليات التمويه و الاخفاء بصورة تجعل معرفة مصدر الهجمة صعب جدا ، الا في حالة الهجمات الصغيرة البسيطة التي يرتكب أصحابها أخطاء و ليس في حالة الهجمات المعقدة التي تقوم بها الدول ومن

ابرز الامثلة على ذلك الهجمات الروسية على إستونيا في عام 2007 و كذلك هجمات كوريا الشمالية علي شركة (سونـي) عام 2015 و الرد الامريكي بقطع الانترنيت على كوريا الشمالية لمدة 10 ساعات و كذلك الهجمات الصينية المستمرة على الولايات المتحدة الامريكية و جميع هذه الهجمات لم يتم تبنيها صراحة من قبل الدول المعتدية فهذه الاتهامات مبنية على الظروف السياسية المرتبطة على الصراعات القائمة بينهما .

2) صعوبة منـع الهجمات الصفرية / و يتميز الفضاء السيبراني بالتحديث التكنولوجي المستمر فبشكل مستمر يتم تطوير الفيروسات لم يتم الكشف عنها و لم ترصدها شركات الامن السيبراني ، فبعضها يصيب المكون المادي مثل (ستـاكنت) و بعضها و هو كثير يصيب الجانب البرامـجي و بعضها و هو ايضاً غير محدود يركـز على المعلومات بهدف السرقة أو التضليل او التشويش او التدمير ، كما ان هذه الفيـروسات تستغل الثغرات الحديثة التي تظهر في الانظمة قبل ان يتم تحديثها و معالجتها فيما يعرف بـ (الهجمات الصفرية) اذ قد تظهر هذه الثغرة و تستغلها بعض الفواعل بشكل مباشر لشن هجمة الكترونية قبل ان يتم اكتشافها او معالجتها من قبل الجهات المختصة .

3) فشل نماذج (الـردع) المعروفة / و يعد مفهوم الردع الذي تم تطبيقه بشكل اساسي في الحرب الباردة ، غـير مُـجدٍ في الحروب السيبرانية ، فالردع بالانتقام او العقاب لا ينطبق على هذه الحروب بخلاف الحروب التقليدية ففي كثير من الاحيان من الصعوبة تحديد الهجمات الالكترونية ذات الزخم العالي ، اذ هناك بعض الهجمات السيبرانيه تتطلب أشهر لـرصدها ، ما يلغي مفهوم الردع بالانتقام

4) المـخاطر السيبرانية تتعدى استهداف المواقع العسكرية / لا ينحصر اطـار الحرب السيبرانية في استهداف المواقع العسكرية فحسب، اذ هناك جهود متزايدة لاستهداف البنى التحتية الحساسة للبلدان المستهدفة ، و هو أمر أصبح واقعيـاً في ظل القدرة على استهداف شبكات الطاقة و الكهرباء و شبكات النقل و المنشآت النفطية أو الصناعية بواسطة فيروسات تتسبب بأضرار هائلة مادية او الحاق الضرر بمعلومات هامة

أولاً: التدابير التقنية و الفنية لتحقيق الامن السيبراني العراقـي

إن الوقاية من مختلف الهجمات السيبرانية و الحماية من البرامج الخبيثة التي تهدف الى سرقة البيانات و المعلومات المهمة أو الترويج لأخبار كاذبة و إشاعات او الاحتيال على الافراد كل ذلك يتطلب معرفة متخصصة بأحدث تقنيات الحماية و الامن السيبراني و ذلك بهدف حماية المعلومات المهمة من عمليات القرصنة الالكترونية و الهجمات و الحروب السيبرانية و سرقة و اتلاف المعلومات و سنتناول هنا أهم التدابير الآزمة لتفادي الجرائم الإلكترونية [23].

1. استـعمال البرمجيات المضادة للاعتداءات الالكترونية ،اذ تعمل هذه البرمجيات على تحطيم البرامج الخبيثة كما تعمل على ايقاف أغلب الاعتداءات الاخرى مثل برامج التجسس.
2. تطوير وسائل الدفع المالي كالبطاقة الائتمانية و التي تعتبر من أكثر الوسائل أمناً
3. أنشاء نسخ احتياطية من المعلومات العامة و الخاصـة بحيث يمكن استرجاعها في حال فقدانها

4. التحكم بدخول استعمال جدار الحماية (fire wall) و هذه لمقاومة اخطار المتطفلين و جدار الحماية هو عبارة عن مكونات مادية و برمجيات خاصة توضع بين الشبكة الداخلية و بين الشبكات الخارجية و يعمل على منع اي من المستخدمين الخارجيين من التوغل في الشبكات الخاصة او الدخول غير المصرح به .
5. تشفير الملفات (File encryption) و يقصد به تحويل محتوى الرسائل بشكل يصعب على الغير معرفة المحتوى الاساس أو أعادته الى وضعه الاصلي و لا يقوم بذلك الامر الا من يعرف كيف يتم تحويره فالتشفير (هو عبارة عن تغيير صيغة الكتابة من صيغة مفهومة الى صيغة غير مفهومة من قبل عامة الناس)
6. حماية البرمجيات و هناك بعض العناصر الآليات المستخدمة في أمن البرمجيات منها أ) تحديث البرامج المضادة للفيروسات باستمرار

ب) وضع كلمة مرور تكون قوية بحيث لا تكون مكونة من كلمة واحدة أو تتضمن معلومات شخصية كالاسم و تاريخ الميلاد بحيث تكون مكونة من أحرف و أرقام و رموز مما يصعب اختراقها

ج) التحديث المستمر للبرمجيات كبرنامج windows فبسبب التحسين المستمر لهذه البرامج قد تظهر عليها ثغرات أمنية تعرض الجهاز للاختراق و لتلافي ذلك فلا بد من تحديث هذه البرامج باستمرار

ثانياً / الاستراتيجية الوطنية للأمن السيبراني العراقي :

و أشارت الاستراتيجية الوطنية للامن السيبراني العراقي لعام 2017 في الفقرة (3 ، 3) الى الاهداف التالية : [24]

1) تشريعات شاملة لمكافحة التهديدات السيبرانية و التدابير المضادة للتهديد السيبراني و تأمين الفضاء السيبراني للبلاد .

2) توفير التدابير التي تحمي البنية التحتية الحيوية للمعلومات ، فضلاً عن الحد من الثغرات و ذلك من خلال اطار ضمان الامن السيبراني .

3) وضع آلية فعالة للاستجابة لحالات الطوارئ في الحاسوب .

4) العمل على تطوير فريق الاستجابة لحالات الطوارئ في الحاسوب .

و أضافة الى ما تقدم هنالك آليات أخرى لتحقيق الامن السيبراني و تتمثل في : [25]

1) اقرار وثيقة سياسات و معايير امن المعلومات و البيانات و التي تهدف الى وضع أطر العمل و السياسات و المعايير و تحديد الادوار و المسؤوليات داخل المؤسسة .

2) تشكيل الفريق الوطني للاستجابة للتهديدات السيبرانية ، و الذي يعد فريقاً وطنياً مشتركاً و متخصصاً في مجال الامن السيبراني ، و يختص هذا الفريق بالاستجابة للحوادث السيبرانية و حماية البنية التحتية للانترنيت ، و لا يقتصر الامر على ذلك فحسب ، بل يعمل على نشر الوعي في مجال حماية الخصوصية و الحماية الذاتية للأفراد و المؤسسات على الانترنيت و يتولى كذلك حماية تأمين و حماية الشبكات و مراكز البيانات الوطنية و المواقع الرسمية التي تعمل في الفضاء السيبراني العراقي .

3) تأسيس مـركز الامن السيبراني بتاريخ 4 ديسمبر 2022 و يعد هذا المركز جهة أمنية متخصصة في مجال الامن السيبراني و يهدف هذا المركز الى تعزيز جهود وزارة الداخلية في بناء منظومة متكاملة و فعالة لحماية الفضاء السيبراني ، كما يسعى هذا المركز الى تنظيم و تطوير آليات الحماية لمواجهة التهديدات السيبرانية بكفاءة و فاعلية .

و من الجدير بالذكر ان مجال الامن السيبراني في العراق يشهد تطورات عديدة .[26]

فعلى المستوى الحكومي

1. أنشأت الجهات المختصة (المركز الوطني للاستجابة للطوارئ السيبرانية) (IQ_CERT) لرصد و مكافحة الهجمات الالكترونية ، فضلاً عن تشكيل فرق الاستجابة للطوارئ السيبرانية (CSIRT) في بعض الوزارات .

2.التشريعات و القوانين : اصدار قانون الجرائم الالكترونية العراقي (رقم 5 لسنة 2022) و الذي يجرم الاختراق و التجسس الالكتروني .

3. التعاون الدولي : تعاون العراق مع منظمات مثل الاتحاد الدولي للاتصالات و الانتربول لتحسين القدرات الدفاعية ، فضلاً عن اتفاقيات مع دول مثل الاردن و الامارات العربية المتحدة.

ثالثاً: أبـعاد الأمن السيبراني و تـداعياته الـمستقبلية

و يعد متغير الامن السيبراني ذات أبعاد نسبية أهمها ما يأتي : [27]

1. البعد العـسكري / لقد تجلت البدايات الاولى للأنترنيت في بيئة عسكرية بشكل مضاعف و ذلك لكي تنتقل في سياق لاحق الى الاوساط العلمية و الاكاديمية و أبحاث تخدم القدرات العسكرية و مما تجدر اليه الاشارة الى ان الميزة النسبية للأمن السيبراني تتمثل في بعده العسكري عن طريق قدرة القوة السيبرانية على ربط الوحدات العسكرية ببعضها البعض عبـر العالم الافتراضي و هذا ما يسهل عملية تبادل المعلومات و الذي ينعكس ايجاباً على تحقيق الاهداف العليا للمؤسسة العسكرية .
2. البعد السياسي / إن لكل دولة الـحق في حمـاية نظامها السياسي و مصالحها و أهدافها التي تسعى الى تحقيقها و قد تغيرت موازين القوى حتى أصبح بإمكان الافراد ان يتحولوا الى لاعبين سياسيين و ذلك من خلال الاطلاع على القرارات السياسية عبر الكم الهائل من المعلومات كذلك ايضا دور شبكات التواصل الاجتماعي في تنظيم الدعايات السياسية و كذلك افتعال الاحتجاجات الالكترونية .
3. البعد القانوني / و يترتب عن النشاطات الفردية و المؤسساتية والحكومية في الفضاء السيبراني نتائج قانونية تتمثل في إيجاد القواعد القانونية التي تنظم التعاملات في الفضاء الالكتروني و حـل النزاعات التي تنشأ عنها و قد نشأت أساليب ممارستيه عديده في استعمال تقنية المعلومات ، كأنشاء المدونات و التجمعات عبر الانترنيت و الحـق في حماية ملكية البرامج المعلوماتية و الابلاغ عن المخالفات و الجرائم السيبرانية و هذا ما أكد على ضرورة وجـود تـرسانة قانونية تتوافق مع تلك التغيرات الحاصلة.

4. البعد الاقتصادي / يرتبط الامن السيبراني ارتباطاً وثيقاً بالاقتصاد فقد توسع استعمال تقنيات المعلومات و الاتصالات كما بالقيمة التي تمثلها البيانات و المعلومات المتداولة و تتيح تقنيات المعلومات تعزيز التنمية الاقتصادية للعديد من البلدان من فرص الاستعمال التي تقدمها الشركات الدولية الكبرى اضافة الى ما تقدم حلول عصر المال الالكتروني ضمن بيئة الكترونية متحركة كوجود المحفظة الالكترونية و اصدار التطبيقات التي تسمح بالدفع الالكتروني.
5. البعد المجتمعي / يوجد أكثر من 4 مليار مستخدم للأنترنيت حول العالم ، حي يستخدم 2,6 مليار شخص مواقع التواصل الاجتماعي ، حيث تتمتع مواقع التواصل الاحتماعي بأعلى معدلات التفاعل البشري مما يتيح فرصاً واسعة لمشاركة الافكار و التجارب الناجحة ، لكنها في المقابل تكشف أيضاً عن أخلاقيات الافراد و صعوبة الرقابة على محتوى الانترنيت ليست مجرد خطر على المجتمعات فحسب بل تعرض أيضاً المعلومات الشخصية لاستخدامات غير مشروعة من جهات خارجية مما يهدد السلم المجتمعي للبلدان [28].

الخاتمة

على الرغم من الميزات العديدة التي يحظى بها الفضاء السيبراني و الدور المهم للأمن السيبراني في عالمنا اليوم الذي يمتاز بالتطور التقني و الرقمي و يتمثل ذلك من خلال سهولة و سلاسة الحصول على المعلومات و المرونة في التعاملات على كافة الاصعدة و النواحي الاجتماعية و الاقتصادية و التجارية و غيرها الا انه ذلك لا يمكن التغاضي عن الجوانب السلبية للفضاء السيبراني ، إذ ان ما يميز شبكة الانترنيت و الفضاء السيبراني بأنه لا يعترف بالحدود الجغرافية للدول و هذ بحد ذاته يشكل تحدياً و تهديداً حيث كان التحدي في السابق يتمثل في الدفاع عن الحدود التقليدية للدول اما في الوقت الحالي بدأ نمط الحروب الحديثة يشكل تهديداً على أمن الدول و ذلك من خلال التهديدات السيبرانية و المتمثلة بتدمير أنظمة الكترونية لمنشآت حيوية عسكرية او مدنية او التعرض لهجمات سيبرانية بهدف الاختراق او التعطيل او التدمير لشبكات القطاع الخاص او من خلال محاولات ارباك او تشويش المعاملات الشخصية او المالية للافراد ، فالفضاء الالكتروني الجديد غير مادي و افتراضي لكنه موجود في كل مكان من العالم المادي و لم يعد الفضاء الالكتروني منطقة مثالية يتم تبادل المعلومات فيه بكل سلاسة لكنه اصبح يعد مجالاً جديداً للجغرافية السياسية فالتنافس في الفضاء الالكتروني لا يمكن فصله عن الجغرافية السياسية كونه يعد مجالاً عالمياً لا تؤثر الخصائص السيبرانية السياسية للفضاء السيبراني على الوصول الى الشبكة و سرعة الشبكة بل تؤثر ايضاً على الحوكمة العالمية ومن الجدير بالذكر ان هذه التهديدات تصل الى الامن الوطني للدول و من ابرز هذه الدول (العراق) حيث أصبحت موضوع الامن السيبراني على رأس اولويات الامن الوطني العراقي في محاولة لمواجهة تصاعد التهديدات السيبرانية إذ باتت العلاقة بين الامن و التكنولوجيا علاقة متزايدة مع امكانية تعرض المصالح الاستراتيجية ذات الطبيعة الالكترونية الى هجمات الكترونية و مما تجدر اليه الاشارة ان في العام 2018 احتل العراق وفق مؤشر الامن السيبراني العالمي للعام 2018 المرتبة (107)على الصعيد العالمي من أصل (175) دولة شملها التقرير و كذلك احتل العراق المرتبة (13)على صعيد الدول العربية و هذا يعني ان الامن السيبراني في تطور مستمر و ايجابي لمجابهة التحديات التي يتعرض لها وهذه دلالة على نجاح القائمين عليه.

اولاً/ الاستنتاجات :

تـوصلت الدراسة الى مجموعة من الاستنتاجات أهمها الآتي :

1. ان من ابرز خـصائص الفضاء السيبراني هو تلاشي الـحدود التقليدية للدول، إذ تجاوز الفضاء السيبراني مفهوم الحدود الجغرافية التقليدية وأصبحت مساحة المعلومات مجالاً جديداً للجغرافية السياسية و غيرت توازن القوى بين الجغرافية السياسية للدول ، إذ وجد الانترنيت فضاءاً جديداً بالكامل و يتجاوز فضاء المعلومات المساحة الجغرافية المكانية التقليدية ففضاء المعلومات يجعل الجغرافية السياسية لها ميزات و خصائص مكانية جديدة حيث كان التحدي السابق يتمثل في الدفاع عن حدود الدولة في حين ساهمت تقنيات المعلومات و الشبكات في إضعاف الحدود الجغرافية التقليدية بين الدول و أصبح من السهل للغاية اختراقها .
2. أن من أهم التحديات التي تواجهه الامن السيبراني هو سهولة تمكن اي شخص من القيام بهجمات سيبرانية و ذلك لتوافر ادوات الهجوم التي تتمثل في جـهاز الحاسوب و الذي من خلاله يتم الاختراق .
3. نـجد أن معظم الدول قد استشعرت مخاطر الامن السيبراني لذلك أخذت عديد من الدول خـطوات عـاجلة و ذلك من خلال تبني استراتيجية تقنية شـاملة و ذلك بهدف تطوير قدرات الامن السيبراني و ذلك باستعمال الوسائل و الادوات التكنولوجيا المتعلقة بالتحكم و السيطرة للتصدي للهجمات و التهديدات السيبرانية .

ثانياً / المقترحات :

1. العمل على اجراء حملات توعوية لتعريف الافراد بالمخاطر و التهديدات السيبرانية و أساليب الوقاية منها .

2. حث الافراد على الاستخدام الصحيح لأجهزة الحاسوب و الهواتف و التطبيقات و عدم مشاركة المعلومات الشخصية المتعلقة بهم بشكل عشوائي .

3. حث الافراد على استخدام أدوات الحماية الرقمية و على سبيل المثال استخدام كلمات مرور قوية .

4. اقامة ورش تدريبية و حلقات نقاشية في مؤسسات القطاع العام و كذلك القطاع الخاص من قبل مختصين في مجال الامن السيبراني لتعريفهم بمخاطر هذه التهديدات و كيفية التصدي لها.

5. الترويج الاعلاني بهدف توعية المجتمع بمخاطر التهديدات السيبرانية و ذلك من خلال استخدام وسائل التواصل الاجتماعي و التلفاز لتوعية اكبر قدر من الافراد و عدم تعرضهم لمث هذه التهديديات .

- الهوامش :

[1]) محمد كمال ، الارهاب السيبراني عندما يستخدم الارهابي الكيبورد بدلاً من القنبلة ،ط 1 ، دار كليم للطباعة و النشر ، القاهرة ، 2022 ، ص 12 .

[2]) علي منيف الرفيعي ، تحديات الأمن في الفضاء السيبراني الامريكي، مجلة دراسات دولية ، العدد (85) ، مركز الدراسات الاستراتيجية و الدولية ، جامعة بغداد ، 2021 ، ص 294.

[3]) مصطفى ابراهيم سلمان ، الامن السيبراني و أثره في الامن الوطني العراقي، مجلة العلوم القانونية و السياسية ،العدد(1)،كلية القانون و العلوم السياسية، جامعة ديالى،2021،ص155.

[4]) المصدر نفسه ، ص 155 .

[5]) يسرى ستار بيركة ، الأمن السيبراني و أثره على الامن الوطني العراقي ، مجلة المستنصرية للدراسات العربية و الدولية ، العدد (1) ، مركز المستنصرية للدراسات العربية و الدولية ، الجامعة المستنصرية ، 2024 ، ص 207.

[6]) جاسم محمد طه ، التهديدات السيبرانية و انعكاسها على الامن القومي الامريكي ، مجلة تكريت للعلوم السياسية ، العدد 32 ، كلية العلوم السياسية ، جامعة تكريت، 2023 ، ص 189.

[7]) أحمد حسين الربيعي ، استراتيجيات مواجهة التهديدات غير النمطية الارهاب السيبراني إنموذجاً ، المجلة العلمية لجهاز مكافحة الارهاب ، العدد (7) ، جهاز مكافحة الارهاب ، ص 171 .

[8]) محمد زهير عبد الكريم ، الإرهاب السيبراني أزمة عالمية جديدة ، مجلة قضايا سياسية ، العدد (64) ، كلية العلوم السياسية ، جامعة النهرين ، 2021 ، ص282 .

[9]) آيات فاخر محمد ، الامن السيبراني العراقي الواقع و آفاق المستقبل ، المجلة السياسية و الدولية ، العدد (58) ، كلية العلوم السياسية ، الجامعة المستنصرية ، 2024 ،

[10]) محمود ياسين أحمد ، محمد جبر عباس ، الحرب السيبرانية و تأثيرها على الامن القومي (العراق إنموذجاً) ، مجلة جامعة الانبار للعلوم القانونية و السياسية ، العدد (1) ، كلية القانون و العلوم السياسية ، جامعة الانبار ، 2024 ، ص 902.

[11]) محمد أكرم محسن ، مروان سالم العلي ، السيبرانية الماهية ـ الخصائص ـ الفواعل ـ الابعاد الاستراتيجية ، مجلة حمورابي للدراسات ، العدد 43 ، مركز حمورابي للبحوث و الدراسات الاستراتيجية ، 2022، ص 387.

[12]) المصدر نفسة ، ص 389.

[13])المصدر نفسه ، ص 389.

[14]) تغريد معين حسن ، الأثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة ، مجلة البحوث الجغرافية ، العدد (30) ، كلية التربية للبنات ، جامعة الكوفة ، 2019، ص 242 .

[15]) تغريد معين حسن ، الأثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة ، مصدر سبق ذكره ، ص 243 .

[16]) اسراء شريف جيجان ، صفا عباس فاضل ، تأثير الفضاء السيبراني على الحروب الحديثة ، مجلة دراسات تربوية ، العدد (65) ، وزارة التربية ، ص11.

[17]) فراس جمال شاكر الربيعي ، مرتكز تأثير الأمن السيبراني على منظومة الامن القومي (المجال الحيوي الخامس) ، مجلة جامعة الامام جعفر الصادق (ع) للعلوم الانسانية و الاجتماعية ، العدد 4 ، جامعة الامام جعفر الصادق ، 2024 ، ص 90.

[18]) فراس جمال شاكر الربيعي ،مصدر سبق ذكره ، ص 90، 91.

[19]) فراس جمال شاكر الربيعي ،مصدر سبق ذكره ، ص 91.

[20]) بدر عدنان احمد تحديات و تهديدات الامن السيبراني و كيفية التغلب عليها ، حوليات آداب عين شمس ، العدد (7)، كلية الآداب، جامعة عين شمس ، القاهرة ، 2023، ص 241

[21]) المصدر نفسه، 242.

[22]) حـازم محمـد خليل ، استغلال الفضاء السيبراني في الحروب غير التقليدية : دراسة في الوكالة السيبرانية و الارهاب السيبراني ، المجلة العلمية لكلية الدراسات الاقتصادية و العلوم السياسية ، العدد 15 ، جامعة القاهرة ، القاهرة ، 2023، ص 277-278 .

[23]) حسام عبـد الامير خلف ، وهـج علي حمزة ، مفهوم الامن السيبراني و علاقته بالذكاء الاصطناعي (دراسة تحليلية قانونية) ، مجلة جامعة الانبار للعلوم القانونية و السياسية ، العدد (2) ، كلية القانون و العلوم السياسية ، جامعة الانبار ، 2023، ص 515-516.

[24]) حميـدة علي جابـر ، آليات الامم المتـحدة لتحقيق الامن السيبراني و أثرها على التشريعات العراقية ، مجـلة الباحث للعلوم القانونية ، العدد 1 ، كلية القانون ، جامعة الفلوجـة ، 2025 ، ص 59 .

[25]) المصدر نفســة ، ص 60 .

[26]) سيماء علي مهدي ، دور الامن السيبراني في استقرار الدولة ، المجلة السياسية الدولية ، العدد 64، كلية العلوم السياسية ، الجامعة المستنصرية ، 2025، ص 392.

[27]) يوسف بوغرارة ، الامن السيبراني : الاستراتيجية الجزائرية للأمن و الدفاع في الفضاء السيبراني ، مجلة الدراسات الافريقية و حوض النيل ، العدد (3) ، المركز الديمقراطي العربي للدراسات الاستراتجية و السياسية و الاقتصادية ، برلين ، 2018، ص108_109.

[28]) حسن نايف مبارك ، دور الذكاء الاصطناعي في تعزيز الامن السيبراني : رؤى نظرية ، مجلة الدراسات الجامعية للبحوث الشاملة ، العدد 32 ، 2024 ، ص 14083.

قـائـمة الـمـصـادر

اولاً/ الكتب :

1. محمـد كمال ، الارهاب السيبـراني عندما يستخدم الارهابي الكيبورد بدلاً من القنبلة ،ط1 ، دار كليـم للطباعة و النشر ، القاهرة ، 2022 .

ثانياً / المجلات :

1. أحـمد حسين الربيعي ، استراتيجيات مواجهة التهديدات غير النمطية الارهاب السيبراني إنموذجاً ، المجلة العلمية لجهاز مكافحة الارهاب ، العدد (7) ، جهاز مكافحة الارهاب .
2. اسراء شريف جيجان ، صفا عباس فاضل ، تأثير الفضاء السيبراني على الحروب الحديثة ، مجلة دراسات تربوية ، العدد (65) ، وزارة التربية.
3. آيـات فاخر محمـد ، الامن السيبراني العراقي الواقع و آفاق المستقبل ، المجلة السياسية و الدولية ، العدد (58)، كلية العلوم السياسية ، الجامعة المستنصرية ، 2024.
4. بدر عدنان احمد تحديات و تهديدات الامن السيبراني و كيفية التغلب عليها ، حوليات آداب عين شمس ، العدد (7)، كلية الآداب، جامعة عين شمس ، القاهرة ، 2023.

5. تغريد معين حسن ، الأثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة ، مجلة البحوث الجغرافية ، العدد (30) ، كلية التربية للبنات ، جامعة الكوفة ، 2019 .
6. جاسم محمد طـه ، التهديدات السيبرانية و انعكاسها على الامن القومي الامريكي ، مجلة تكريت للعلوم السياسية ، العدد 32 ، كلية العلوم السياسية ، جامعة تكريت، 2023.
7. حـازم محمـد خليل ، استغلال الفضاء السيبراني في الحروب غير التقليدية : دراسة في الوكالة السيبرانية و الارهاب السيبراني ، المجلة العلمية لكلية الدراسات الاقتصادية و العلوم السياسية ، العدد 15 ، جامعة القاهرة ، القاهرة ، 2023.
8. حميدة علي جابر ، آليات الامم المتحدة لتحقيق الامن السيبراني و اثرها على التشريعات العراقية ، مجلة الباحث للعلوم القانونية ، العدد 1 ، كلية القانون ، جامعة الفلوجة ، 2025.
9. حـسام عبـد الامير خلف ، وهـج علي حمزة ، مفهوم الامن السيبراني و علاقته بالذكاء الاصطناعي (دراسة تحليلية قانونية) ، مجلة جامعة الانبار للعلوم القانونية و السياسية ، العدد (2) ، كلية القانون و العلوم السياسية ، جامعة الانبار ، 2023.
10. حسن نايف مبارك ، دور الذكاء الاصطناعي في تعزيز الامن السيبراني : رؤى نظرية ، مجلة الدراسات الجامعية للبحوث الشاملة ، العدد 32 ، 2024
11. سـالم صـابر ، انعكاسات البعد العسكري للفضاء السيبراني على الجغرافيا السياسية للدولة، مجلة دارسات الدفاع و الاستشراف ، العدد 17 ، الجزائر ، 2022.
12. سفيان يوسفي ، الامن الفكري و تحديات الامن السيبراني : دراسة نظرية ، مجلة الباحث ، العدد 2 ، المدرسة العليا للأساتذة ببوزيعة ، الجزائر ، 2024.
13. عـلي منيف الرفيعي ، تحديات الأمن في الفضاء السيبراني الامريكي، مجلة دراسات دولية ، العدد (85) ، مركز الدراسات الاستراتيجية و الدولية ، جامعة بغداد ، 2021 .
14. فراس جمال شاكر الربيعي ، مرتكز تأثير الأمن السيبراني على منظومة الامن القومي (المجال الحيوي الخامس) ، مجلة جامعة الامام جعفر الصادق (ع) للعلوم الانسانية و الاجتماعية ، العدد 4 ، جامعة الامام جعفر الصادق ، 2024 .
15. محمـد أكرم محسن ، مروان سالم العلي ، السيبرانية الماهية ـ الخصائص ـ الفواعل ـ الابعاد الاستراتيجية ، مجلة حمورابي للدراسات ، العدد 43 ، مركز حمورابي للبحوث و الدراسات الاستراتيجية ، 2022.
16. محمـد زهير عبد الكريم ، الإرهاب السيبراني أزمة عالمية جديدة ، مجلة قضايـا سياسيـة ، العدد (64) ، كلية العلوم السياسية ، جـامعة النهرين ، 2021.
17. محمود ياسين أحمد ، محمـد جبر عباس ، الحرب السيبرانية و تأثيرها على الامن القومي (العراق إنموذجاً) ، مجلة جامعة الانبار للعلوم القانونية و السياسية ، العدد (1) ، كلية القانون و العلوم السياسية ، جامعة الانبار ، 2024 .

18. مصطفى ابراهيم سلمان ، الامن السيبراني و أثره في الامن الوطني العراقي، مجلة العلوم القانونية و السياسية ،العدد(1)،كلية القانون و العلوم السياسية، جامعة ديالى،2021.
19. يسرى ستـار بيركة ، الأمن السيبراني و أثره على الامن الوطني العراقي ، مجلة المستنصرية للدراسات العربية و الدولية ، العدد (1) ، مركز المستنصرية للدراسات العربية و الدولية ، الجامعة المستنصرية ، 2024.
20. يوسف بوغرارة ، الامن السيبراني : الاستراتيجية الجزائرية للأمن و الدفاع في الفضاء السيبراني ، مجلة الدراسات الافريقية و حوض النيل ، العدد (3) ، المركز الديمقراطي العربي للدراسات الاستراتجية و السياسية و الاقتصادية ، برلين ، 2018.
21. سيماء علي مهدي ، دور الامن السيبراني في استقرار الدولة ، المجلة السياسية الدولية ، العدد 64، كلية العلوم السياسية ، الجامعة المستنصرية ، 2025.

List of Sources

First / Books:

1 .Muhammad Kamal, The Cyber User's Ability When He Uses the Keyboard, 1st Edition, Kalim Printing and Publishing House, Cairo, 2022.

Second / Journals:

1. Ahmed Hussein Al-Rubaie, "Confronting the Undefined Confrontation: The Internet User as a Model," Scientific Journal for Counterterrorism, Issue (7), Counterterrorism Department.

2. Israa Sharif Jagan and Safaa Abbas Fadel, "The Impact of Cyberspace on Wars," Journal of Modern Educational Studies, Issue (65), Ministry of Education.

3 .Ayat Fakhra Mahmoud, "The Iraqi Cyber Police: Reality and Future Prospects," *Al-Riyadiya Wal-Dawliya* Journal, Issue (58), College of Political Science, Al-Mustansiriya University, 2024.

4. Bader Adnan Ahmed, "Cybersecurity Challenges, Its Most Prominent Features, and How to Overcome Them," *Annals of Arts, Ain Shams University*, Issue (7), Faculty of Arts, Ain Shams University, Cairo, 2023.

5. Taghreed Moein Hassan, "The Impact of Cybersecurity on Modern Geography," *Global Marketing Journal*, Issue (30), College of Education for Girls, University of Kufa, 2019.

6 .Jassim Mohammed Taha, "Electronic New York and its Impact on Americans," *Tikrit Journal of Political Science*, Issue 32, College of Political Science, Tikrit University.

7. Hazem Mohammed Khalil, "Cyber Anger in Unconventional Warfare: In Cyberspace and its Management," Scientific Journal of the College of Economics and Political Science, Issue 15, Cairo University, Cairo, 2023.

8 . Hamida Ali Jaber, "Unifying the Cybersecurity Unit and Issuing its Licenses in Iraq," Journal of Research in Legal Sciences, Issue 1, College of Law, University of Fallujah, 2025.

9. Hussam Abdul-Amir Khalaf and Wahaj Ali Hamza, "The Concept of Cybersecurity and Communications with Artificial Intelligence (An Analytical Study)," University of Anbar Journal of Legal and Political Sciences, Issue 2, College of Law and Political Philosophy, University of Anbar, 2023.

10 . Hassan Nayef Mubarak, "The Role of Artificial Intelligence in the Cybersecurity Enhancement System: A Perspective," Journal of Comprehensive University Research, Issue 32, 2024.

11. Salem Saber, Reflections on the Dimensions of Cyberspace on Military-Political Geography, Journal of Defense and Supervision Schools, Issue 17, Algeria, 2022.

12 .Sofiane Yousfi, Security Forces and Cybersecurity Challenges: A Study, Exploration Journal, Issue 2, Higher Teacher Training School, Bouzaia, Algeria, 2024.

13.Ali Munif Al-Namdhiji, Challenges of American Cyberspace, International Studies Journal, Security Issue (85), Center for Strategic and International Studies, University of Baghdad, 2021

14 .Firas Jamal Shaker Al-Rubaie, Focusing on the Cyber Impact on National Security (The Fifth Communism), Imam Jaafar Al-Sadiq University Journal of Humanities and Social Sciences, Issue 4, Imam Jaafar Al-Sadiq University, 2024.

15. Mahmoud Akram Mohsen and Marwan Salem Al-Ali, "Cybersecurity: Its Essence, Returns, Actors, and Cultural Dimensions," Hammurabi Journal of Studies, Issue 43, Hammurabi Center for Research and Tourism, 2022.

16. Mohammed Zuhair Abdul Karim, "Combating Cyberterrorism: A New Global Crisis," Political Issues Journal, Issue 64, College of Political Science, Al-Nahrain University, 2021.

17 .Mahmoud Yassin Ahmed and Mohammed Jabr Abbas, "Cyber Warfare and Its Impact on National Security (Iraq as a Case Study)," Anbar University Journal of Legal and Political Sciences, Issue 1, College of Law and Political Science, Anbar University, 2024.

18. Mustafa Ibrahim Salman, "Cyber Police and Its Contribution to the Iraqi National Police," Legal and Political Science Materials, Issue 1, College of Law and Political Science, Diyala University, 2021.

19. Yusra Stratka, "Internet Law: Its Efforts in Iraqi National Leaders," Al-Mustansiriya Journal of Arab and International Studies, Issue (1) Al-Mustansiriya Center for Arab and International Studies, Al-Mustansiriya University, 2024.

20. Youssef Boughrara, Cybersecurity: The Algerian Strategy for Security and Defense in Cyberspace, Austrian and Nile Studies Journal, Issue (3), Center for Strategic, Liberal and Economic Democracy, Berlin, 2018.