

اسم المقال: الحرب السiberانية بين التحديات واستراتيجيات المواجهة : العراق إنموذجاً  
اسم الكاتب: د. مهند جبار عباس، أ.د. هيثم كريم صيوان  
رابط ثابت: <https://political-encyclopedia.org/index.php/library/1386>  
تاريخ الاسترداد: 2025/05/18 02:32 +03

الموسوعة السياسية هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترنت. لمزيد من المعلومات حول الموسوعة السياسية – Encyclopedia Political، يرجى التواصل على [info@political-encyclopedia.org](mailto:info@political-encyclopedia.org)

استخدامكم لأرشيف مكتبة الموسوعة السياسية – Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام المنشورة على الموقع <https://political-encyclopedia.org/terms-of-use>

تم الحصول على هذا المقال من موقع مجلة قضايا سياسية الصادرة عن كلية العلوم السياسية في جامعة النهرين ورفده في مكتبة الموسوعة السياسية مستوفياً شروط حقوق الملكية الفكرية ومتطلبات رخصة المشاع الإبداعي التي ينضوي المقال تحتها.



الحرب السيبرانية بين التحديات واستراتيجيات المواجهة : العراق إنموذجا<sup>٧</sup>

Cyber war between challenges and confrontation strategies:

Iraq as a model

أ.د هيثم كريم صيوان\*\*

د.مهند جبار عباس \*

Prof.Dr. Haithm Karim

Dr. Muhand Jabar

ملخص البحث :

طرق البحث الى موضوع الحرب السيبرانية التي باتت احد سمات الحروب الحديثة في الوقت المعاصر والتي تفرض مهددات وتحديات لعموم الدول المتقدمة او النامية وكل الدول تهتم في تامين امنها الوطني بالدرجة الأولى ، و لا يمكن لها ان تتحقق امنها الوطني بدون تامين وحماية فضائلها السيبراني فالحروب والهجمات أصبحت تدار بشكل الكتروني وتستهدف البنى التحتية للدول و التي باتت هي أيضا تدار بشكل الكتروني ، وتلك الحروب تمتاز بالسهولة وقلة التكاليف وتسبب اضرار بالغة للدولة المستهدفة وعليه أصبحت كل الدول تضع استراتيجيات لمواجهة تلك الحروب وتامين البنى التحتية الحيوية لها و العراق احد الدول النامية التي تعاني من الانكشاف السيبراني لذا على صناع القرار داخل الدولة العراقية ان يهنووا البيئة الأمنية السيبرانية التي تضمن صد أي هجوم قد تتعرض له بناء التحتية الحيوية مستقبلا ، وهذا يتطلب تبني اليات ووسائل فاعلة تجعل من العراق دولة قادرة على الدخول الى فضاءات القوة السيبرانية.

الكلمات المفتاحية سبرانية ، حرب ، استراتيجية ، العراق

Abstract

The research deals with the subject of cyber war, which has become one of the features of modern wars in the contemporary time, which poses threats and challenges to all developed or developing countries. Electronically, it targets the infrastructure of countries, which are now also managed electronically, and these wars are characterized by ease and low costs and cause severe damage to the targeted country. Therefore, all countries have developed strategies to

<sup>٧</sup> تاريخ الاستلام : 2022/7/22 ، تاريخ القبول: 29/8/2022 ، تاريخ النشر : 30/9/2022

\* وزارة الدفاع  
\*\* كلية العلوم السياسية جامعة النهرين

confront these wars and secure their vital infrastructure, and Iraq is one of the developing countries that suffer from cyber exposure. Therefore, decision makers within the Iraqi state must prepare the cyber security environment that guarantees the repelling of any attack on its vital infrastructure in the future, and this requires adopting effective mechanisms and means that make Iraq a state capable of entering the spaces of cyber power.

**Key word : Cyber, war, strategy, Iraq**

### المقدمة :

شهد العالم ونتيجة للتطور التكنولوجي نوع جديد من الحروب تسمى (السيبرانية) وباتت تمثل سمة مميزة للنظام الدولي لعالم ما بعد الحرب الباردة ، والمتغير الحاسم في هذه الحروب هي المعرفة ، فأصبحت كل الدول تتنافس فيما بينها من أجل امتلاك أدوات القوة الجديدة المتمثلة بالمعرفة ومن يمتلك المعرفة يمتلك القوة والسلطة كما عبر عنها (الفن توفر) في كتابه تحول السلطة .

التطور في تكنولوجيا المعلومات أدى إلى ظهور فضاءات الكترونية افتراضية تدار من خلف الشاشات ، وعلى اثر ذلك انتقل الصراع والتتنافس وال الحرب من الحالة الواقعية إلى العالم الافتراضي وباتت الدول تتنافس فيما بينها لامتلاك مقومات القوة السيبرانية ، من أجل ان تبقى فاعلة ومؤثرة في هرم السلطة العالمية .

ويعد الفضاء السيبراني المجال الخامس في الحروب بعد البر والبحر والجو والفضاء ، أدى بالنتيجة إلى ظهور مفهوم الأمن السيبراني (cyber security) كموضوع جديد في حقل الدراسات الأمنية اخذ يكتسب اهتمام الكثير من المختصين في هذا المجال .

وكون القوة السيبرانية تميزت بانخفاض التكلفة وسهولة الدخول إلى الفضاء السيبراني وامكانية اخفاء الهوية وغيرها ، جعل من الجهات الفاعلة الاصغر اي الشركات والمنظمات او الافراد قادرة على ممارسة القوة في الفضاء السيبراني على حساب الدول مقارنة بالعديد من المجالات التقليدية للقوة سابقا .

**أهمية البحث :** للبحث اهمية في انه يمثل محاولة لاعطاء رؤية لما هي السيبرانية وما تفرضه من تحديات ومخاطر مستقبلية ومعرفة مكانة وموقع العراق في منظومة الفضاء السيبراني ومن ثم معرفة اهم

التحديات والتهديدات التي يفرضها الفضاء السيبراني على العراق وامنه مستقبلا ، وأيضا تأتي أهمية البحث في انه يعطي صورة لصانع القرار العراقي بضرورة العمل على اعداد بيئة امنية سiberانية مستقبلا وتوفير كل الإمكانيات والتمويل سبيلا للارتفاع بقدرات العراق السيبرانية .

**هدف البحث :** يحاول البحث تحقيق جملة من الأهداف أهمها :

1. التعريف بمفهوم الحرب السيبرانية وبيان أهميتها وخصائصها وادواتها ومعرفة أطرافها و مجالات توظيفها .

2. بيان موقع العراق وقدراته في مجال المعرفة السيبرانية وبيان فيما اذا كان العراق يعاني انكشاف سيبيرياني .

3. توضيح استراتيجية مواجهة التحديات والتهديدات السيبرانية .

**إشكالية البحث :** بما ان الثورة التكنولوجية اسهمت بشكل كبير في انتاج وسائل وأدوات يمكن توظيفها لتصبح النمط المرجح لحروب القرن الحادي والعشرين ، فان إشكالية البحث تتمحور حول السؤال الاتي .. هل يمتلك العراق مقومات القوة التكنولوجية بحيث يكون قادر على مواجهة هذا النوع من الحروب المستقبلية . لذا نطرح تساؤلات فرعية تتمثل بالاتي :

1. ما هي الحرب السيبرانية وأهدافها والأطراف الفاعلة بها ؟.

2. ما هي الأدوات والخصائص و مجالات التوظيف للقوة السيبرانية ؟.

3. هل يمكن للعراق ان يبقى معزلا عن التطورات العالمية ومنها تطورات القوة السيبرانية و مجالات توظيفها ؟.

**فرضية البحث :** يطرح الباحث فرضية مفادها " العراق في ظل معطياته الحالية نجده من الضعف وعدم القدرة في مواجهة التحديات والتهديدات التي تفرضها القوة السيبرانية وبالتالي نحن امام علاقة دالية طردية تتمثل بأنه كلما تمكن العراق من تطوير امكاناته وقدراته الدفاعية في مجال القوة السيبرانية كلما كان اكثر قوة في مواجهة التحديات والتهديدات التي يفرضها الفضاء السيبراني وبالتالي تعزيز امنه السيبراني " .

**منهجية البحث :** ولتحقيق اهداف البحث فقد تم توظيف المنهج الاستقرائي لتحقيق اهداف البحث وتضمن استخدام الاسلوب الوصفي التحليلي لتحليل الظاهرة السيبرانية ووصفها ومعرفة خصائصها والوقوف على اهم التحديات التي تفرضها الحروب السيبرانية .

## اولاً : الحرب السيبرانية : اطار نظري عام

### 1. مفهوم الحرب السيبرانية .

جاءت كلمة السيبرانية من الكلمة الاغريقية **kybernetes** وتعني ( الطيار او قائد الدفة ) وهي مشقة من الكلمة ساير وتعني اي شئ له علاقة بالحوسبة الالكترونية والعالم الافتراضية المرئية ويكثر استخدام الكلمة في مجال تكنولوجيا المعلومات والانفوميديا ويشير قاموس (المورد) الى انها علم السيطرة وضبط الاشياء والتحكم فيها عن بعد في حين ان (قاموس المصطلحات الامريكية العسكري) عرف السيبرانية بدلالة الهجوم عبر الفضاءات الالكترونية من اجل اختراق بنى تحتية محمية الكترونيا بقصد تعطيلها او تدميرها والحق الاضرار بها <sup>(1)</sup> .

وعلى الصعيد العربي تم استخدام مصطلح القوة الالكترونية كمرادف للسيبرانية وبعد نوربرت وينر اول من استخدم مصطلح السيبرانية في العام 1948 ، وتعد الحرب السيبرانية غامضة الأهداف مجهولة المصدر تتحرك عبر شبكات المعلومات والاتصالات عالميا وتستخدم أسلحة إلكترونية تستهدف تقنية المعلومات، بالإضافة لكونها لاتميز بين استهداف المنشآت المدنية أو العسكرية وصعوبة فرض حماية دولية ضدها <sup>(2)</sup> .

اسلوبها الترويع وبث الخوف ، ولا يمكن معرفه حجم الاضرار التي توقعها، ولا كيف تم الهجوم وتعد من الحروب غير المتكافئة **(asymmetric war)** كون الطرف الذي يتمتع بقوة هجومية ويباغت باستخدامها يعد الطرف الاقوى ، بعض النظر عن حجم امكاناته العسكرية التقليدية وهذا ما يدحض نظريات الردع الاستراتيجي ويمكن استخدامها في وقت السلم او الحرب أو الازمة و لا يحتاج تنفيذها وقت طويق و يؤدي المهارات البشرية دورا اساسيا في تطويرها <sup>(3)</sup> .

والحرب السيبرانية باتت مصطلح يشير الى ، اي نزاع يحصل في الفضاء السيبراني ويأخذ طابع دولي ، ولكن مثل هذا التعريف غير دقيق ولا يعبر عن الحروب في الفضاء السيبراني وفحواها بدقة ، لذلك يقترح

(1) د. لبنى خميس و تغريد صفاء ، اثر السيبرانية في تطور القوة ، مجلة حمورابي ، مركز حمورابي للدراسات الاستراتيجية ، العدد 33 و 34 ، ربيع 2020 ، ص 148 .

(2) عبد الله محمد العصيمي ، السيبرانية .. وشكل الحرب في المستقبل ، مقالة ، صحيفة الجزيرة ، السعودية 2017 ، متاح على

الرابط : <https://www.al-jazirah.com>

(3) عادل عبد الصادق ، مصدر سابق ، ص 10 .

اخرون التركيز على اشكال وانواع النزاع التي تحدث في الفضاء السيبراني مثل القرصنة الالكترونية والتي تعد المستوى الاول من النزاع في الفضاء السيبراني ، والجريمة والتتجسس الالكتروني وهما في المستوى الثاني والثالث من النزاع في الفضاء السيبراني بالإضافة الى الارهاب الالكتروني الذي يقع في المستوى الرابع من النزاع في الفضاء السيبراني ، اما الحرب السيبرانية فهي الاخطر من بين كل المستويات السابقة للنزاع السيبراني ، وتعد جزءا من حرب المعلوماتية بمعناها الاوسع لكونها تؤثر على الارادة السياسية للطرف المستهدف وعلى امكانياته في صنع القرار بالإضافة الى تأثيرها على القيادة العسكرية واهتمامات المدنيين ومصالحهم في الفضاء السيبراني<sup>(1)</sup> .

ومن زاوية نظر اخرى أن مصطلح "الحرب الإلكترونية" او السيبرانية ، لا يمكن ان يطلق على أي أعمال إلكترونية هجومية على أنها "حرب" ، الى ان تسبب ضرراً مادياً للأشخاص والأشياء في العالم الحقيقي ، لذا الحرب السيبرانية هي امتداد للسياسة من خلال الإجراءات المتخذة في الفضاء السيبراني من قبل جهات فاعلة تابعة للدولة أو من قبل جهات فاعلة غير حكومية لديها توجيه أو دعم مهم من الدولة والتي تشكل تهديداً خطيراً لأمن دولة أخرى<sup>(2)</sup>.

لذا يمكن القول ان الحرب السيبرانية ، هي حالة التوظيف لتقنولوجيا المعلومات ضمن استراتيجية عسكرية (قد تكون داعية وقد تكون هجومية ) يكون هدفها تعطيل البنى التحية الحيوية لدولة الخصم ، وعرفت ايضا على أنها ( إجراءات من قبل دولة قومية لاختراق أجهزة الكمبيوتر أو الشبكات الخاصة بدولة أخرى بغرض إحداث ضرر بها أو تعطيلها) <sup>(3)</sup> .

ومن كل ما تقدم يمكن فهم الحرب السيبرانية على انها استخدام تكنولوجيا المعلومات لمهاجمة أجهزة الحاسوب وشبكات المعلومات لدولة ما ، والتي يمكن أن تسبب ضرراً مشابهاً للحرب الفعلية على ارض الواقع لكن بدون سفك الدماء .

## 2. هدف الحرب السيبرانية .

(1) فيصل محمد عبد الغفار ، الحرب الإلكترونية ، ط1، الجنادرية للنشر والتوزيع ، الطبعه الاولى ، الاردن، 2015 ، ص 10-11 .

(2)(<https://en.wikipedia.org/wiki/Cyberwarfare>

) 3 (Ibid.

تستهدف الحرب السيبرانية البنى التحتية الحيوية للدول وتشمل المجالات العسكرية والحكومية والاقتصادية كما يع تغيير البيئة الثقافية والفكرية للخصوم احد اهدافها أيضاً<sup>(1)</sup>.

ومصطلح البنية التحتية الحيوية كما حدتها السياسة الرئاسية للولايات المتحدة الامريكية وتشمل 16 قطاع مهم ادخلته الرئاسة الامريكية ضمن مجالات الامن القومي<sup>(2)</sup>. وكما جاء بجدول(1).

### جدول(1) القطاعات الستة عشر للبنية التحتية الحيوية

الكيماوية الأساسية والمتخصصة والزراعية. الأدوية. و منتجات المستهلك	الكيماويات
التجمعات العامة (الساحات ، وحدائق الحيوان ، والمتحف ، ومرارك المؤتمرات ، وما إلى ذلك) البطولات الرياضية الألعاب. إقامة، أحداث في الهواء الطلق الترفيه والإعلام، العقارات، بيع بالتجزئة	المرافق التجارية
خدمات الصوت والبيانات ؛ أنظمة الإرسال عبر الأقمار الصناعية والسلكية واللاسلكية ؛ مزودي خدمات الاتصالات والمبادرات .	الاتصالات
تصنيع المعادن والآلات والمعدات الكهربائية والأجهزة والمكونات ومعدات النقل	التصنيع الحرج
مرافق توليد الطاقة الكهرومائية؛ أقفال الملاحة السدود والسدود وحواجز الأعاصير ومخلفات المناجم ؛ مستودعات النفايات الصناعية؛ مرفق أخرى لاحتباس المياه والتحكم في المياه .	مشاريع السدود
المجمعات الصناعية العالمية التي تتيح البحث والتطوير والتصميم والإنتاج والتسليم والصيانة لأنظمة الأسلحة العسكرية والأنظمة الفرعية والمكونات أو الأجزاء المطلوبة .	قاعدة الدفاع الصناعية
خدمات الإطفاء والطوارئ. إدارة الطوارئ؛ الخدمات الطبية الطارئة؛ الأشغال العامة؛ المواد الخطرة ، البحث وإنقاذ ؛ التخلص من الذخائر المتفجرة ؛	إنفاذ قانون خدمات الطوارئ

(1) هبة عبدالفتاح ، الحروب السيبرانية الأكثر دماراً.. والأقل دموية ، اخبار اليوم ، 14 سبتمبر 2019 ، متاح على الرابط :

<https://m.akhbarelyom.com>

( 2 ) Jason Rivera , A Theory of Cyberwarfare: Political and Military Objectives, Lines of Communication, and Targets Georgetown Security Studies Review, June 10, 2014 .

أسلحة خاصة وتكتيكات وعمليات تكتيكية ؛ وحدات الطيران نقاط الإجابة على السلامة العامة .	
البترول والفحم والغاز الطبيعي. الكهرباء المولدة من مصادر الطاقة النووية ، والطاقة المائية ، والطاقة الشمسية ، وطاقة الرياح ، والطاقة الحرارية الأرضية ؛ منتجي الطاقة الكهربائية والمرافق الكهربائية ؛ محطات الطاقة الكهربائية الفرعية وأنظمة النقل .	الطاقة
البنوك والاتحادات الائتمانية والوسطاء والمؤسسات المالية الأخرى التي تودع الأموال وتسدد المدفوعات لأطراف أخرى ، وتتوفر الائتمان والسيولة للعملاء ، وتستثمر الأموال لفترات طويلة وقصيرة ، وتحول المخاطر المالية بين العملاء	الخدمات المالية
مطاعم، مرافق تصنيع الأغذية وتجهيزها وتخزينها	مزارع الغذاء والزراعة
التي تملكها أو تستأجرها الحكومات الفيدرالية وحكومات الولايات والحكومات المحلية والتي تُستخدم في أنشطة الأعمال العامة أو المعاملات التجارية أو الأنشطة الترفيهية أو غير المفتوحة للجمهور المستخدمة للحصول على معلومات ومواد وعمليات ومعدات شديدة الحساسية ، المنشآت العسكرية ذات الاستخدام الخاص والسفارات والمحاكم والمختبرات الوطنية ، مرافق التعليم، المعالم والأيقونات الوطنية	المبني الحكومية
والصحة العامة البنية التحتية الحيوية التي تحمي جميع قطاعات الاقتصاد من الأخطار مثل الإرهاب وتقضي الأمراض المعدية والكوارث الطبيعية ، المستشفيات والمرافق الطبية الأخرى	الرعاية الصحية
الوظائف الافتراضية والموزعة التي تنتج وتتوفر الأجهزة والبرامج وأنظمة تكنولوجيا المعلومات والخدمات ، يساعد في توفير وصيانة الإنترن特 بالتعاون مع قطاع الاتصالات	تقنية المعلومات
والمواد والنفايات محطات الطاقة النووية. المفاعلات النووية غير العاملة بالطاقة المستخدمة في البحث والاختبار والتدريب ، مصنعي المفاعلات أو المكونات النووية ، المواد المشعة المستخدمة في المقام الأول في الأوساط	المفاعلات النووية

الطبية والصناعية والأكاديمية ، مراقب دورة الوقود النووي ، نقل وتخزين والتخلص من النفايات النووية والمشعة	
طيران ، البنية التحتية للطرق السريعة وحاملة السيارات ، أنظمة النقل البحري، السكك الحديدية للنقل الجماعي والركاب. أنظمة خطوط الأنابيب سكة الشحن البريدية والشحن	أنظمة النقل
والصرف الصحي شبكات مياه الشرب العامة، أنظمة معالجة مياه الصرف الصحي المملوكة للقطاع العام ، مياه صالحة للشرب، أنظمة الصرف الصحي	أنظمة المياه

A Theory of Cyberwarfare: Political and Military ,Source:Jason Rivera

Objectives, Lines of Communication, and Targets Georgetown Security Studies

<https://georgetownsecuritystudiesreview.org>. June 10, 2014 ,Review

### 3. الاطراف والقوى في الحرب السيبرانية

ونتيجة لاتجاه الصراع الدولي نحو الاعتماد المتزايد على التكنولوجيا والاتصالات ، اصبح الفضاء السيبراني ساحة جديدة للصراع ولكن بطابع الكتروني لا يعترف بالحدود القومية للدول يسعى فيه كل طرف الى تحقيق اكبر المكاسب والحقاقضرر بالطرف الاخر ولكن من غير دماء ، ادواته التجسس وسرقة المعلومات ولا تترك اي مخلفات مادية كما في الحروب التقليدية وهذا النوع من الصراع يتميز بعدم وضوح اطرافه وذو تداعيات خطيرة جدا مثل تدمير الواقع على الانترنت او تعطيلها بالفيروسات وهي اسلحة من السهل استخدامها والحصول عليها من شبكة الانترنت ، هذه الحروب الجديدة تجري وسط الشعوب وليس في الساحات التقليدية للصراع الدولي .

ومن كل ما تقدم نرى ان التطور السريع لเทคโนโลยيا الحاسوب و الشبكات غيرت من مفهوم القوة مما ترتب عليه دخول المجتمع الدولي الى مرحلة جديدة مارست فيها هجمات الفضاء السيبراني دورا أساسيا في تعظيم القوة أو السيطرة على عناصرها الأساسية ، وأصبح التفوق في مجال الفضاء السيبراني عنصرا أساسيا في تنفيذ عمليات فعالة على ارض الواقع .

واضحى امن الفضاء السيبراني من استراتيجيات الأمن القومي للكثير من الدول ، للاستحواذ على مصادر القوة داخل الفضاء السيبراني ، وللدفاع عن بنيتها التحتية الحيوية ضد اي هجوم سبيراني مثل

قطع خدمة الإنترن特 أو ضرب موقعه أو توقيف رسائل البث التلفزيوني أو الإذاعي أو إيقاف موجات الراديو أو تعطيل شبكات المحمول أو البث الفضائي ، ليصل تأثيرها على المجتمع والاقتصاد الدولي . لقد حدد (جوزيف ناي ) ثلاثة اطراف من الفاعلين الذين يمتلكون القوة السيبرانية وهم :<sup>(1)</sup>

- أ. الدول تعد الدول الفاعل الأكبر في الفضاء السيبراني لكن ليس هي الفاعل الوحيد .
- ب. الفاعلون من غير الدول واهمها الشركات متعددة الجنسية : أصبحت بعض الشركات متعددة الجنسية تمتلك موارد للقوة تفوق قدرة بعض الدول، فمثلا خوادم شركات جوجل Google وميكروسوفت Microsoft وأبل Apple المنتشرة في مختلف دول العالم تسمح لها بامتلاك قواعد من البيانات العملاقة ، والتأثير في اقتصadiات كثير من الدول، وإن أرادت فيمكنها التأثير في قوة الدولة الاقتصادية وقتها الناعمة أيضا من خلال تلاعبها بالبيانات والتصنيفات الدولية للاقتصadiات والأسوق .

ومن أبرز الأمثلة على قيام الشركات العاملة في مجال الفضاء السيبراني بالتأثير في العلاقات الدولية، الصراع بين شركة جوجل والحكومة الصينية؛ حيث قامت الأخيرة باختراق حسابات البريد الإلكتروني Gmail الخاصة بالناشطين السياسيين في الصين. وهو ما دفع الشركة إلى التهديد بالخروج من السوق الصينية إن لم تتوقف الحكومة الصينية عن أفعالها، وقامت بتطوير محرك بحث Baidu الصيني حتى تستطيع الصين الاستغناء عن جوجل .

ج. الأفراد (الهاكر) <sup>(\*)</sup> : وهم الفواعل الذين يمتلكون معرفة تكنولوجية متقدمة ولديهم القدرة على استخدامها، ولا يمكن الكشف عن هوياتهم بسهولة، وذلك لصعوبة ملاحقتهم<sup>(2)</sup>.

أصبح الفرد عنصراً فاعلاً في التفاعلات الدولية، و أصبح يمارس من الأنشطة عبر الفضاء السيبراني ما يؤثر به في العلاقات الدولية. ولنا في ظاهرة ويكيликس "phenomena WikiLeaks" ( ) مثل

(1) ايهام خليفة ، مصدر سابق ، ص 33 .

(\*) كلمة هاكر (Hacker) بمعناها الشمولي تفيد الشخص الذي يقوم بتعديل سلوك نظام معين ليؤدي وظائف غير التي انشأها من أجلها ، ويساعد كذلك على ايجاد الحلول للعديد من المشاكل في جميع المجالات، اما في مجال تقنية المعلومات فمصطلح هاكر يرجع الى السنتين من القرن الماضي ، وكان يطلق على الاشخاص اللذين لديهم دراية واسعة بجهاز الكمبيوتر والمتخصصين من البرمجة بصفة مت米زة .

(2) سليم دحماني ، أثر التهديدات "السيبرانية" على الأمن القومي الولايات المتحدة الأمريكية - نموذجا(2001-2017) ، رسالة ماجستير غير منشورة ، جامعة محمد بوضياف - المسيلة ، الجزائر ، 2017 ، ص 25 .

على ذلك حيث نجح (جولييان أسانج) في نشر الملايين من الوثائق الخاصة بوزارة الخارجية الأمريكية؛ حيث تم استغلال شبكة الإنترنت العالمية في تسريب وثائق تحوي معلومات سرية للغاية متداولةٌ بين الإدارة الأمريكية وقنصلياتها الخارجية بدول العالم، الأمر الذي جعل علاقة الولايات المتحدة مع بعض الدول عرضة للتأثير والتهديد. وقد حكمت المحكمة العسكرية بالولايات المتحدة الأمريكية على الجندي (برادلي مانينغ) الذي قام بتهريب الوثائق (لوليانم أسانج)، بالسجن على خلفية تسريب معلومات لموقع ويكيبيديا لمنطقة 35 عام .

ومن أبرز مجموعات القرصنة على الفضاء السيبراني (مجموعة أنونيموس Anonymous)\* وهي مجموعة غير مرئية من القرصنة المنتشرة في العالم، ذات تأثير كبير فيما يسمى بالحرب الإلكترونية، مثلاً مسؤوليتها عن تسريب الآف رسائل البريد الإلكتروني الخاصة بالرئيس السوري (بشار الأسد)، وكما هاجمت موقع حكومة أمريكية وبريطانية وأخرى للناتو قبل أن تعلن مؤخراً هاجمتها لموقع حكومة (إسرائيلية) تعاطفاً مع أهالي قطاع غزة الذين يتعرضون لحملة عسكرية جديدة .

#### د. المنظمات الإجرامية والجريمة الإلكترونية :

تعتبر المنظمات الإجرامية العابرة للجنسية ، أحد الفواعل الدولية ذات التأثير في التفاعلات الدولية، والتي تحظى بحماية من بعض الحكومات الفاسدة . هذه المنظمات الإجرامية دخلت الفضاء السيبراني، وأصبحت تقوم بعمليات قرصنة إلكترونية بهدف سرقة المعلومات، أو اختراق الحسابات المصرفية وتحويل الأرصدة منها، أو من خلال وجود سوق سوداء على الإنترنت لبيع المعلومات المالية المتعلقة بكلمات مرور شخصية وحسابات مصرفية وبطاقات ائتمان حيث تكلف الجرائم الإلكترونية الشركات أكثر من تريليون دولار سنوياً ، وانتهاك شخصيات وهمية، أو حقيقة، و الهجوم على موقع الإنترنـت، والتعديل فيها و التلاعب في التجارة الإلكترونية، واستخدام الفيروسات التي تعطل الأنظمة العاملة، وتضرر الأعمال، بالإضافة إلى جرائم الجنس والإعلان عن الرذائل والابتزاز<sup>(1)</sup> .

#### هـ - الجماعات الإرهابية العابرة للحدود :

(1) سليم دحماني، مصدر سابق ، ص 35 - 36 - 37 .

ومن أبرز الفواعل الدولية بعد أحداث 11 ايلول هي الجماعات الإرهابية ، حيث استخدمت الإنترنط في عمليات التعبئة والتجنيد ، واستغلت الفضاء السيبراني كبوابة لنشر أفكارها وجذب من يؤيدها والمتطوعين لصفوفها ، اضافة الى نشر بياناتها وتعليماتها لافرادها واصبح بإمكانها اختراق شبكات الكهرباء والطاقة والمواصلات، وحتى المفاعلات النووية الموجهة إلكترونياً أو عبر الأقمار الصناعية والسيطرة عليها أو تدميرها، الأمر الذي قد يسبب كارثة بشرية .  
وتعت ممارسة القوة عبر الإنترنط إرهاب اذا صاحبها دوافع سياسية ، مثل التأثير في القرارات الحكومية أو الرأي العام<sup>(1)</sup>.

#### 4. أدوات الحرب السيبرانية

تمتاز الحرب السيبرانية بكونها حرب هلامية الشكل وغير مرئية ، فهي متعددة بميادينها، و مختلفة ، ومتطورة بالياتها و وسائلها التي ترتبط بأكثر المجالات التكنولوجية تطورا وتبدلا في الحياة الإنسانية المعاصرة للدول وهذه الاليات والوسائل هي ببرامج حاسوب وفيروسات الكترونية<sup>(2)</sup> .

ادى هذا النوع الجديد لاليات ووسائل الصراع ان تكون الدول على قدم المساواة فليس هناك دول عظمى واخرى صغرى او متوسطة في تطوير مثل تلك الأسلحة السيبرانية ، والتي استخدمتها الدول او الفواعل من غير الدول في خلق أزمات داخلية للنظام الحاكم أو الهجوم على شبكات البنية التحتية المدنية للعدو، مثل شبكات الماء والسدود ومحطات الكهرباء والطاقة النووية و خطوط سكك الحديد والبنوك والأسواق المالية والقطاعات الإنتاجية المختلفة<sup>(3)</sup>.

ولهذه الحرب السيبرانية الجديدة وسائل مختلفة ، منها اختراق الشبكات و شن الحروب النفسية والتجسس وشن حرب الأفكار ، وسرقة المعلومات ، والتنافس بين أجهزة الاستخبارات الدولية<sup>(4)</sup> ومن الاليات ووسائل

(1) ايها خليفة ، مصدر سابق ، ص 37 – 38 .

(2) بشلاق ليلى ، تأثير الحروب الإلكترونية على العلاقات الأمريكية الروسية ، رسالة ماجستير غير منشورة ، ، جامعة محمد بوضياف المسيلة ، الجزائر ، 2018 ، ص 14 .

(3) عادل عبد الصادق ، اسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني ، وحدة الدراسات المستقبلية ، مكتبة الاسكندرية ، العدد 23 ، مصر ، 2016 ، ص 137 .

(4) شاكر محمود ، الحرب السيبرانية وتداعياتها على الامن العالمي ، الموسوعه الجزائرية للدراسات السياسية والاستراتيجية دراسات امنية ، 2019 . متاح على الرابط : <https://www.politics-dz.com>

الحرب السيبرانية البرامج الخبيثة وتشمل الفيروسات<sup>(\*)</sup> ، والدیدان<sup>(\*)</sup> ، وحيل تصيد المعلومات التي تستغل العيوب والثغرات الموجودة في البرامج الأخرى واخفاء مستخدمو الحواسيب قبل دخولهم إلى المواقع المصابة بالفيروسات أو فتح روابط الالكترونية و مرفقات الرسائل البريدية . وقد يقوم من يشن الهجوم السيبراني بخلق ثغرة تسلل على غرار فكرة (حصان طروادة) وهي عبارة عن برنامج حاسوب غير مرخص يضاف إلى البرنامج المستهدف و يسمح لرجال الفضاء السيبراني باختراق الشبكات ، وانظمة حواسيب العدو وغالبا بعد أن يقومون باختراق الشبكة لأول مرة فإنهم يتذكرون وراءهم ثغرة تسلل تسمح لهم بالدخول في المستقبل بطريقة سهلة وسريعة ؛ وأحيانا لا يكتفون بسرقة نسخة من البرنامج فحسب بل قد يضيفون إليه شيئا ما لاستخدامه مستقبلا ، وأحيانا أخرى تسمح لهم ثغرة التسلل بالوصول إلى جذر البرنامج فتصبح لديهم القدرة و الصالحيات التي يتمتع بها مصمم البرنامج وبالتالي يمكنهم إضافة ما يشاؤون من برمجيات خبيثة ويمدون أي اثر على وجودهم<sup>(1)</sup> .

ومن ناحية أخرى تعد شبكة الانترنت بشكل عام ، ومواقع التواصل الاجتماعي بشكل خاص احدى الادوات الفعالة في الحرب السيبرانية التي تشنها المنظمات الارهابية ، ففي الشرق الاوسط استخدمت هذه المجموعات وسائل التواصل الاجتماعي كوسيلة ناجحة في صراعها ، حيث استخدمتها في تجنيد مقاتليها وتحويلها الى منصة لشن الحرب النفسية ضد الخصوم تصوير مشاهد العنف على نطاق واسع من اجل بث الذعر والخوف<sup>(2)</sup>.

## 5. خصائص الحرب السيبرانية

ويمكن اجمال ابرز الخصائص والسمات للحروب السيبرانية بما يلي :<sup>(3)</sup>

(\*) الفيروسات هي برامج يتم تمريرها من مستخدم إلى آخر عبر الإنترنيت أو الوسائل المحمولة مثل وحدات التخزين الصغيرة

(\*) الدیدان هي برامج لانتطلب تمريرها الى مستخدم اخر لانها قادرة على نسخ نفسها ذاتيا باستغلال عيوب معروفة ثم تزحف كالدیدان عبر الانترنيت .

(1) بشارق ليلي ، مصدر سابق ، ص41.

(2) رولا حطيط ، السيبرانية : الحرب الخفية في المنطقة المظلمة ، مركز باحث للدراسات الفلسطينية والاستراتيجية ، 2020 متاح على الرابط الالكتروني : <https://www.bahethcenter.net/>

(3) حسن مظفر الرزو ، مصدر سابق ، ص231-232 .

- أ - تقسم بالشمولية نتيجة لتنوع اشكال الموارد السيبرانية واختلاف اماكن توطنها ، وتبين قيمتها الاقتصادية وتنوع الفواعل التي تملكها ، وتتنوع الحقول المعرفية التي تمثلها ، مما يؤدي الى تعقيد المجال الذي تمتد على مساحته اضرارها .
- ب - لا يمكن معرفة شخصية و معالم بصمة الحضور لفاعلين في الساحة السيبرانية ، مثل المنظمات او الجماعات او الافراد او الدول ، وذلك لتخفيف خلف كواليس الفضاء السيبراني .
- ج - انعدام البعد المكاني لفضاء السيبراني مما ادى الى صعوبة التحكم بمسارات التهديدات او الهجمات السيبرانية، وسير تفاعلاته في شبكات المعلومات المتراوطة والمعقدة ، الامر الذي يجعل من الصعوبة بمكان ايقاف التهديدات او الهجمات السيبرانية وتکاثر فرص انطلاقها تجاه اي هدف ومن اي عقدة في نسيج شبكاتها العالمي .
- د - تميزت الحروب السيبرانية ايضا ، بتراجع الحصانة الامنية فيها وذلك بسبب تعدد الفضاء السيبراني وتتنوع البيئات البرمجية ، وكثرة انواع معدات المعلومات والاتصالات والية تواصلها فيما بينها وكثرة التغيرات السيبرانية وتتنوعها وحصول تطورات مستمرة لكل هذه الامور ادى الى تفاقم التغيرات وظهور فجوات جديدة يمكن التسلل من خلالها .
- ه - ان امكانية القيام بالحروب السيبرانية عبر حواسيب منفردة او مجموعة من الحواسيب المرتبطة بشبكة الانترنت وتتوفر التطبيقات المجانية المنتشرة على موقع الشبكة ادى الى خفض الكلف المالية لهذه الحروب قياسا بالتحضيرات والدعم اللوجستي والمبالغ الباهضة التي تتطلبها العمليات الحربية التقليدية. توفر الحروب السيبرانية فرص تحقيق برامج سياسية واهداف استراتيجية من دون الدخول في حرب معلن او مواجهة مسلحة مع العدو .
- و - تسمح الحروب السيبرانية بالدخول الى النظم المتحكمة بتشغيل وادارة البنى التحتية للطاقة والاتصالات وشبكات الطاقة الكهربائية وقواعد بيانات المنظومات العسكرية في ساحة المواجهة والدفاع التقليدية .
- س - سرعة تنفيذ الهجوم السيبراني عبر شبكات المعلومات وبدون انذار مسبق يحدث خلخلة واسعة وتسارع للمخاطر لا يستطيع صانع القرار اتخاذ قرارات تتناسب مع حجم المخاطر الناجمة من الهجوم السيبراني.

## 6. مجالات توظيف القوة السيبرانية

نظراً لتحول الفضاء الإلكتروني إلى ساحة للتفاولات الدولية ، بُرِزَ العديد من الاشكال التوظيفية للقوة السيبرانية في الفضاء السيبراني ، وذلك على صعيد الاستعمالات المدنية أو العسكرية و على حد سواء ، مما أدى إلى جعل هذا الفضاء مجالاً للصراعات المتعددة ، بين الفاعلين من الدول أو غير الدول و التسابق في امتلاك أكبر قدر من القدرات والتأثير في هذا المجال الجديد للصراع في الساحة الدولية<sup>(1)</sup> .

### أ. المجالات السياسية

يمكن توظيف القوة السيبرانية سياسياً عبر استخدام موقع اليوتيوب لرفع حاجز التعنت الذي تفرضه الحكومات الديكتاتورية في إخفاء انتهاكها لحقوق شعبها ، وأيضاً تستخدم لإدارة العمليات النفسية والتأثير في الرأي العام ، ومن جانب آخر ساهمت القوة السيبرانية في توضيح أهمية دور الصورة في تأجيج الأحداث الدولية مثل ما حصل في حالة نشر الرسوم الكاريكاتورية المسيئة للرسول الأعظم وهو ما أنتج احتجاجات دولية واسعة وتوترات في طبيعة العلاقات الدولية<sup>(2)</sup> .

بالإضافة إلى أنها غيرت في مفهوم ومصادر الثقافة السياسية والتشريع السياسية ، كما أدت إلى تغيير أدوات العمل السياسي الوطني من خلال استخدام نموذج الحكومة الإلكترونية واستثمار دور وسائل التواصل الاجتماعي في نشر الوعي السياسي و التأثير في العملية الانتخابية<sup>(3)</sup> .

### ب. المجالات الاقتصادية

ان الحرب الاقتصادية التي تشن من خلال استخدام الإنترنت هي استراتيجية عدائية، تتضمن شن هجمات ضد دولة من الدول، بواسطة التكنولوجيا السيبرانية، والهدف إضعاف اقتصادها وبالتالي اضعاف قوتها السياسية والعسكرية. ان تاريخ الحرب الاقتصادية تمتد جذوره إلىآلاف السنين، لكن خصوم اليوم أصبح لديهم أدوات سيبرانية فعالة و غير متماثلة

### ج. المجالات العسكرية

(1) عبد الله زارب ، النظرية السيبرانية .. توظيف الفضاء الإلكتروني في تعظيم قوة الدول ، بحث منشور في موقع افاق الالكترونية ، 2017 . متاح على الرابط : <https://aaafaq.kku.edu.sa>

(2) شيماء عويس أبو عيد ، القوة في العلاقات الدولية: دراسة تأصيلية ، دراسة منشورة على موقع الالكتروني للمعهد المصري للدراسات ، تركيا ، 5 تشرين الأول 2018 ، ص 1 - 17 .

(3) ابراهيم ابراش ، السيبرانية السياسية : السياسة في زمن الثورة المعلوماتية ، دراسة منشورة على موقع دنيا الوطن ، 2019 متاح على الرابط : <https://www.alwatanvoice.com/arabic/news/2019/10/31/1287877.html>

القدرات السيبرانية العسكرية لدى الجيوش على مستوى العالم تعد مقياساً هاماً في تقييم القوة الوطنية لأي دولة، وهذا ما اشار اليه تقرير "التوازن العسكري لعام 2020" الذي يصدر عن المعهد الدولي للدراسات الاستراتيجية في كل عام ، إذ تبين أن عدداً قليلاً من الدول قد تحول بشكل كامل نحو دمج عمليات الفضاء السيبراني في هيكل القوة المتنوعة<sup>(1)</sup>.

نحن على عتبات تحول عظيم في التكنولوجيا العسكرية، ستعكس تأثيراته على كيفية خوض الحروب، وتنعدى ذلك لتأثر على السياسة والاقتصاد والقوانين والأخلاقيات التي ترتبط بالحرب نفسها .

وفي السياق ذاته اشار (بيتر سنجر) في كتابة (الحرب عن بعد : دور التكنولوجيا في الحرب ) الى ان هناك أكثر من 12 ألف منظومة روبوتية مستخدمة في العراق الان، والطيارون الجالسون في نيفادا يقتلون عن بعد "الإرهابيين" في أفغانستان، ويسعى العلماء لمناقشة درجة الذكاء والدموية التي ستترافق بها اختراعاتهم الروبوتية وان الكثير من مؤلفي قصص الخيال العلمي، يقدمون افكاراً خالية ربما تترجم على ارض الواقع من قبل البناة ب شأن الجيل القادم من الأسلحة الروبوتية .

### ثانياً \_ العراق والظاهرة السيبرانية الجديدة :

خرج العراق من عزلة دولية خانقة استمرت لفترة طويلة جداً لا يعرف شي عن التكنولوجيا الحديثة في عام 2003 ثم دخل في مرحلة اضطراب امني استمرت وما زالت مستمرة جعلت الحكومات العراقية تصب جل اهتمامها نحو تأمين متطلبات تحقيق الامن وكل شي يأتي فيما بعد لذا يمكن القول بان العراق منكشف تكنولوجيا امام العالم الخارجي وعليه سنتناول في هذا المحور الاتي :

#### 1. العراق وضرورات انهاء العزلة عن متغيرات التطور التقني العالمي :

مع التقدم التكنولوجي وزيادة اعتماديه الدول كافه على تكنولوجيا المعلومات والذكاء الصناعي وشبكات الانترنت في اداره كل البنى الحيوية داخل الدولة بما فيها القطاع العسكري والمدني وتلك الاعتمادية والتشابك الالكتروني في ما بين الدول اصبح سمة مميزة لعالم اليوم فلا يمكن ان تبقى دولة معزز عن

(1) إبراهيم سيف منشاوي ، تحولات القوة: دمج القدرات السيبرانية في تقرير التوازن العسكري 2020 ، المعهد الدولي للدراسات الاستراتيجية IISS ، بحث منشور على موقع المستقبل للأبحاث والدراسات المتقدمة ، 2021 . متاح على الرابط :

<https://futureuae.com>

العالم ومتغيراته الأساسية واهمها الفضاء السيبراني وما يجري به فظهر لنا الاقتصاد الرقمي والتجارة الإلكترونية والمعاملات المالية التي تتم عبر أنظمة السويفت العالمية والعملات الرقمية والحكومة الإلكترونية ، وهذه كلها متغيرات وتطورات حصلت في البيئة الدولية مؤخراً وتعاظمت بدخول الالفية الجديدة .

والعراق بسبب سياسات النظام السابق والحصار والحروب كان بعيد كل البعد عن تلك المتغيرات لكن بعد عام 2003 ، نجد انتقال العراق وافتتاحه على العالم الخارجي وبمتغيراته كافة بما فيها السيبرانية وما يدور فيها ، فعليها ان ندرك بان السياسة والاقتصاد وال الحرب باتت تتم في الفضاء السيبراني حتى الحروب باتت سيرانية والتي أصبحت المظهر الجديد للحروب في القرن الحادي والعشرين فهناك تحول من الحروب التقليدية التي تعتمد على الجيوش والمقاتلين الى نوع جديد من الحروب الافتراضية الرقمية حتى الأسلحة تغيرت وباتت تعتمد على تكنولوجيا المعلومات وهذه الحروب ترك اثار كبيرة على البنية التحتية الحيوية للدولة ومؤسساتها وتعمل على شلها وتدميرها مما يتربّ عليه اضرار بمؤسساتها بمختلف الميادين الاقتصادية والثقافية والسياسية والعسكرية وهذا يتطلب استراتيجيات لتأمين الامن السيبراني العراقي<sup>(1)</sup> .

## 2. العراق والمهدّدات السيبرانية الجديدة :

دخلنا عالم الفضاءات السيبرانية وبدا كل شيء يدار الكترونياً وعبر شاشات رقمية في الميادين كافة السياسية والاقتصادية والاجتماعية والعسكرية والأمنية وهذا الفضاء ينطوي على مهدّدات جديدة يجب على صانع القرار الأمني العراقي التحوط منها مستقبلاً ، وتلك المهدّدات المستقبلية تتمثل بسهولة توظيف الأطراف والفواعل الدولية كافة للفضاء الإلكتروني العراقي من أجل ضرب البنية الحيوية للدولة فالمهدّدات القادمة لم تعد تقليدية عن طريق استخدام القوة العسكرية بشكل مباشر وإنما من خلال استهداف الفضاء الإلكتروني للدولة وهكذا لابد من توافر ادراك لدى الجميع وخاصة النخب الأمنية والعسكرية العراقية بأن هناك مهدّدات وحروب تتم في الفضاء الإلكتروني (السيبراني) تستهدف شبكات الحوسبة التي توجه وتدير مؤسسات الدولة وبنائها التحتية الحيوية المدنية والعسكرية .

(1) ريمون بو رجيلي ، التكنولوجيا الحديثة في المجالات العسكرية ، مجلة الجيش ، العدد 236 - شباط 2005 ، متاح على الرابط: <https://www.lebarmy.gov.lb/ar/content>

العراق بعد عام 2003 ، بدا يدخل وبشكل متزايد في العالم الرقمي فزاد عدد مستخدمين شبكة الانترنت والهواتف النقالة واستخدم معظم الشعب العراقي للانترنت في مجال الاعمال والتجارة والخدمات الحكومية والتعليم والصحة وغيرها من الأنشطة الاقتصادية والاجتماعية بل وحتى السياسية اي هناك حاله من التزايد في التعاملات والخدمات الالكترونية داخل العراق<sup>(1)</sup> ، اذ امام هذا التزايد في استخدام شبكة الانترنت تبرز تحديات وتهديدات تستهدف البنى التحتية للاتصالات والمعلومات داخل العراق وتهدد تلك التعاملات والخدمات في العراق فقد تتعرض تلك البنى التحتية الى خطر الاختراق والتخرير المتعمد من قبل هجمات سبانية تستهدف اعاقه تقديم الخدمات الحيوية او نشر برامج وفايروسات لتخرير كل البنى التحتية الحيوية للاتصالات وتكنولوجيا المعلومات فضلا عن تدمير نظم التحكم الصناعي الحيوية وخاصة في مرافق الطاقة والغاز الطبيعي والكهرباء والطيران والنقل والقواعد المعلومات والبيانات القومية فضلا عن اختراق البريد الالكتروني ومواقع الانترنت مما يؤثر بشكل كبير على عمل المنشآت الحيوية داخل العراق والتي باتت منكشفة انكشفا كبيرا امام الهجمات السيبرانية .

بعبة أخرى ان العراق يعاني من ضعف الامن الالكتروني مما جعل العراق في حاله من الانكشاف الاستراتيجي تجاه الاطراف الأخرى فهناك سهولة كبيرة لاختراقه والتجسس على بياناته والمعلومات الخاصة بمنظماته الأمنية والعسكرية والمالية والشخصية ... الخ .

### 3. العراق ومخاطر الانكشاف السيبراني بعد عام 2003

العراق بعد عام 2003 نلاحظ بدا يدخل الى مجال المعلوماتية والاتصالات بعد ان فرضت الديكتاتورية عزله دولية على العراق طيلة عقود طويلة امتدت من عام 1979 لغاية 2003 ، الا ان العراق ما يزال يعاني من مشكلة تمثل في ضعف الامن الرقمي وافتقاره للبني التحتية الرقمية سواء كانت مصرافية او امنية او شخصية هذا الضعف يجعله منكشف امام التهديدات الأمنية المتمثلة بالقرصنة المعلوماتية والمصرفية وعمليات التجسس على مؤسساته وأجهزته الأمنية من قبل اطراف داخلية وخارجية اقليمية ودولية ولنا في الانتخابات التي جرت عام 2018 ، مثال على ذلك فعملية التصويت تمت بالاعتماد على نظام الاقمار الصناعية والتي لا يمكن التحكم بها لأنها تدار من خارج العراق لذا زادت احتمالية اختراقها والتلاعب بنتائجها من قبل جهات خارجية ، اضافه الى ذلك العراق تبني مشروع توطين الرواتب الذي

(1) للمزيد ينظر : موقع nas ، إحصائية بأعداد العراقيين على شبكة الانترنت وموقع التواصل ، 2020.03.28 – 17:35 ، على الرابط : <https://www.nasnews.com/view.php?cat=27718>

تدبره الكثير من الشركات المالية والتي باتت تحتفظ بالمعلومات الشخصية للموظفين داخل اجهزة الكترونية خارج البلاد وكذلك ايضا اختراق موقع الكترونيه مهمه تابعه للحكومة العراقيه واهمها موقع جهاز الامن الوطني وكذلك ايضا استخدام التكنولوجيا و منصات التواصل الاجتماعي في التحشيد لتظاهرات تشرين عام 2019.

والعراق احتل مكانة متذبذبة في مؤشرات الامن السيبراني العالمي وهذه المكانة تضعه امام اشكاليه خطيره تتمثل بانكشافه وسهولة اختراق امنه السيبراني وعليه يمكن ان نحدد ملامح البيئة السيبرانية للعراق وكالاتي<sup>(1)</sup>:

- أ. دولة مكشوفه امام القوى السيبرانية والتنظيمات الإرهابية .
- ب. تدني البنية التحتية الرقمية فيه .
- ت. يعني التخلف والامية الرقمية خاصه في الميدان الاقتصادي والاقتصاد الرقمي والحوسبة المالية والمصرفية .
- ث. زيادة احتمالية تعرضه لشن هجمات سبيرانية عليه قد تستهدف المراسلات الحكومية او سرقة الاسرار الأمنية والاقتصادية والاجتماعية للبلد .
- ج. تعاظم تعرضه للإرهاب الإلكتروني والتجسس والقرصنة الإلكترونية وعمليات غسيل الاموال واستخدام شبكات الانترنت لممارسة النصب والاحتيال والجريمة الإلكترونية والاتجار بالبشر والمخدرات .
- ح. ينطوي العراق على الاستخدام السلبي لموقع التواصل الاجتماعي والتي قد توظف للقيام بأثارة الاضطرابات الداخلية فلاحظنا خلال الفترة الماضية كيف ان تنظيمات الإرهابية قامت بتوظيف موقع التواصل الاجتماعي في عمليه التجنيد واصبح لتلك التنظيمات موقع الكترونية واستخدامها للفيسبروك واليوتيوب والتغرام مما اثر تأثيرا كبير على الحالة السيكولوجية للمواطن العراقي ، كذلك ايضا انتشرت فيه الجريمة الإلكترونية مما ولد تداعيات سلبية على النسيج الاجتماعي والامن الداخلي فوجدنا مظاهر التهديد بالقتل والقرصنة المالية وجرائم النصب والاحتيال والابتزاز الإلكتروني والتشهير بالأفراد عبر اختراق الحسابات الشخصية والابتزاز المالي والجنسي والسب والقذف والاتجار بالبشر والمخدرات وهذه

(1) مروان سالم العلي ، التحديات الاستراتيجية للأمن الوطني العراقي في ظل المتغيرات الدولية ، مجلة تكريت للعلوم السياسية ، العدد 20 ، 2020 ، ص 70 .

مظاهر باتت تشكل تهديدات كثيرة على الامن الوطني العراقي وكذلك تزايد احتمالية اخترق المواقع الحكومية لاحظ في الانتخابات العراقية لعام 2018 ،جرى نشر الكثير من التسجيلات الصوتية لعملية شراء مقاعد في مجلس النواب كذلك في عام 2019 ، تعرض نحو 30 موقع الكتروني للحكومة العراقية لحالة من الاختراق منها جهاز الامن الوطني ووزارة الداخلية والصحة وقد قام بعملية الاختراق مجموعة تدعى (ماكس برو)<sup>(1)</sup> وتسريب معلومات وبيعها تتعلق بالأمن الوطني العراقي ، وهذا الاختراق ودليل كافي على انكشاف العراق إلكترونيا وتزايد استخدام التنظيمات الإرهابية لما يسمى بالحرب السيبرانية ، وقد تقوم تلك التنظيمات بعمليات ارهابية وبجرائم منظمة تستهدف تهديد وتعطيل البنية التحتية الحيوية داخل العراق وهذا ما شهدناه في الحرب مع داعش وكيف تم توظيف موقع التواصل الاجتماعي في عملية الدعاية وال الحرب النفسية والتجنيد والتخييب الى اخره<sup>(1)</sup> .

لذا لابد من حماية الامن السيبراني العراقي وخاصة تلك المواقع المرتبطة بأمن البنية التحتية الحيوية التي يجب ان تكون بعيدة عن الاختراق والهجمات السيبرانية مستقبلا فهذا الاختراق هو اختراق للسيادة العراقية والقيم السياسية والاجتماعية السائدة في المجتمع العراقي فهناك قطاعات حيوية مستهدفة تمثل قطاع الاتصالات وتكنولوجيا المعلومات قطاع الخدمات المالية قطاع الطاقة قطاع الخدمات الحكومية قطاع النقل والمواصلات وقطاع الصحة فضلا عن قطاع الاعلام والثقافة فضلا عن هناك مخاطر لسرقة الهوية الرقمية والبيانات الخاصة وكل تلك القطاعات تعد مهمة للأمن الوطني العراقي .

وعليه نقول ان العراق يعد احدى الدول المنكشفة سيرانيا وهذا الانكشاف ينطوي على تحديات ومهددات كثيرة وفي مختلف المجالات وخاصة المجال الامني والاقتصادي المالي فضلا عن السياسي والاجتماعي ، فالعراق يعاني من الضعف الكبير في المجال التكنولوجي والحوسبة وتكنولوجيا المعلومات ولا يمتلك القدرات التي تمكنه من التكيف بشكل ايجابي مع تلك التحديات التي يفرضها الفضاء السيبراني فكل الدول اخذت تسابق للانتقال الناجح من الفضاء الواقعي الى الفضاء الافتراضي الالكتروني الا ان العراق لم يمر بمرحلة تحضيريه او انتقاليه حيث وجد نفسه امام تحديات الفضاء السيبراني وهو ما يزال بحاجه الى امكانيات كبيرة في المجال الامني الالكتروني و ما تفرضه المتغيرات الجديدة في البيئة الدولية.

\* هو فييق هكر متخصص في اختراق مواقع الدول ومنها العراق .

(1) مصطفى ابراهيم سلمان ، الامن السيبراني واثره في الامن الوطني العراقي ، مجلة العلوم القانونية والسياسية ، كلية القانون والعلوم السياسية جامعة ديالى ، العدد 1 ، 2021، ص 171.

### ثالثاً \_ العراق ومتطلبات مواجهة التحديات السيبرانية

#### 1. حتمية تبني استراتيجية وطنية عراقية للأمن السيبراني :

يعد الامن الوطني لأي دولة قضية مهمة ومن الاولويات الإستراتيجية وكل الدول لديها اهتمام كبير بوضع استراتيجيات للأمن تتضح فيها المصالح الحيوية التي في ضوءها يتم وضع الاهداف الإستراتيجية وتحديد الوسائل لتحقيق تلك الاهداف وال العراق يمر بمرحلة مضطربة سياسيا وامنيا واقتصاديا تتطلب معها وضع استراتيجيات جديدة غير تقليدية للأمن والتحديات باتت كثيرة ومتعددة التي تواجه الامن الوطني في العراق ، ومن تلك التحديات التحدي السيبراني الذي بات من ضمن التحديات غير المنظورة والمؤثرة على الامن العراقي مستقبلا ووسط للتقافس المحموم في ما بين الدول من اجل الحصول على القوة السيبرانية كي توظف تلك القوة في ما يخص علاقاتها بالدول الاخرى ونزاعاتها وصراعاتها معها ، نتسأل هل ان صانع القرار العراقي يعمل من اجل تطوير إستراتيجيات تبني وتوظيف اساليب القوة السيبرانية والأسلحة الإلكترونية من اجل التصدي لأي هجمات متوقعة من هذا النوع في المستقبل ، بعبارة أخرى هل العراق قادر على الدفاع عن / او شنه هجوم عبر فضاء السيبراني او شل قدره الاعداء على القيام بهجمات سiberانية على الرغم من ان العراق لم يدخل بعد عالم الفضاء السيبراني فما يزال في مرحلة (الابو ) مقارنة بالدول الاخرى ، فالعراق مؤسساته وبنية التحتية لم تدار بشكل الكتروني بعد ، اذا هو الان بعيد عن مخاطر الهجمات السيبرانية لكن العراق لا يمكن ان يبقى على هذه الوضعية من التخلف التكنولوجي اذ يجب ان نخطط للمستقبل ونشير الى ان العراق في طريقه الى الدخول وبكثافة كبيرة الى عالم المؤسسات الإلكترونية والبنى التحتية الإلكترونية التي تدار من خلال شبكات الحاسوب الالي يضاف الى ذلك حتمية زيادة توجهه نحو التجارة الإلكترونية والاقتصاد الرقمي والمعاملات المالية والمصرفية التي تتم عبر شبكة السويفت العالمية والدخول الى عالم العملات الافتراضية الرقمية ، وهذه كلها لا يمكن ان يبقى العراق بمعزل عنها لذا لابد من تبني استراتيجيات دفاعية على الأقل فضلا عن الهجومية مستقبلا من اجل الارقاء بقدرات العراق على صد اي هجمات سiberانية تصدر من قبل اي طرف خارجي ، وكذلك تطوير قوة ردع سiberانية أيضا كي يدخل العراق الى عالم الفضاء السيبراني فاعل ومؤثر وبالفعل

تم وضع استراتيجية للأمن السيبراني في العراق الا انها بحاجة الى تطوير مستمر وتوفير الأدوات التي تسهل تنفيذ ما جاء في تلك الاستراتيجية<sup>(1)</sup>.

## 2. العراق وضرورة توفير مركبات الامن السيبراني مستقبلاً :

احتل العراق المرتبة (107) عالمياً و(13) عربياً عام 2018 ، الا انه تراجع بمقدار (22) نقطة في عام 2020 ليكون بالمرتبة (129) عالمياً من اصل (184) دولة (17) عربياً<sup>(2)</sup> .

ولكي يحتل العراق مكانة جيدة في مقاييس الامن السيبراني العالمي ويكون دولة فاعله ومؤثرة في الفضاء السيبراني لابد له من تطوير الاستراتيجية القائمة حالياً والاهتمام بتوفير ركائز أساسية مهمة العراق يفتقر اليها في الوقت الحاضر ، لذا على صناع السياسات الأمنية في العراق العمل على إقامة تلك المركبات والتي أهمها :-

أ. المركز التشريعي القانوني ، فلا بد من وجود مؤسسات وتشريعات قانونية تتعامل مع الامن السيبراني والجريمة الإلكترونية والإرهاب السيبراني .

ب. الركيزة التقنية نجد بأن العراق يفتقر الى مؤسسات فنية متخصصه وذات كفاء عاليه تستطيع التعامل مع التحديات السيبرانية لذا لابد من توفير ذلك المركز .

ت. المركز التنظيمي حيث نجد ان العراق يفتقر الى المؤسسات واستراتيجيات الخاصة برسم وصناعة السياسات لتطوير الامن السيبراني على المستوى المحلي.

ث. ركيزة بناء القدرات العراق ما زال يعاني من قلة التخصيص للبحث والتطوير والتعليم والتدريب التي تعمل على بناء تلك القدرات كي تستطيع ان تتعامل مع متغيرات الفضاء السيبراني .

---

(1) للمزيد ينظر : مستشارية الأمن الوطني العراقي امانة سر اللجنة العليا لأمن الاتصالات والمعلومات ، = استراتيجية الأمن السيبراني العراقي ، ص 2-10 . متاح على الرابط :

[https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National\\_Strategies\\_Repository/00056\\_06\\_iraqi-cybersecurity-strategy.pdf](https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf)

(2) باسل علي خريسان ، الامن السيبراني في العراق قراءة في مؤشرات الامن السيبراني لعام 2022 ، مركز البيان للدراسات والتخطيط ، بغداد 2022 ، ص 9 .

ج. ضرورة بناء تعاونات وشراكات وتحالفات في مجال السيبرانية حيث ان العراق ما يزال بعيداً عن وجود شراكات تعاونية وشبكات لتبادل المعلومات فما زال العراق يعاني من عزله اقليميًّا ودولياً واغتراب في مجال الفضاء السيبراني .

#### الخاتمة والاستنتاجات :

تعد الحروب السيبرانية اهم متغير معاصر في العلاقات الدولية فقد انتقل العالم من الحروب التقليدية الى الحروب السيبرانية وذلك بفضل التقدم والتطور التكنولوجي والتي احدثت ثورة في كافة مجالات الحياة البشرية بما فيها الحروب وادواتها والتي اخذت تدار عبر فضاءات افتراضية وشاشات الكترونية .

وبالتالي تلك الحروب تفرض التحديات ومخاطر على الامن الوطني للدول فهي تستهدف البنى التحتية الحيوية للدول ونظرًا لسهولة القيام بها وقلة تكليفها فضلاً عن حجم الاضرار التي من الممكن ان تلحق بها الدولة المستهدفة اصبحت اطرافها لانتقصر على الدول فقط بل على اطراف اخرى من غير الدول مثل الشركات والتنظيمات والجماعات الارهابية بل وحتى الافراد .

ويعد العراق احد دول عالم الجنوب التي لا تمتلك مقومات الدخول الايجابي الى الفضاء السيبراني فانه سيعاني من انكشاف سيراني خارجي وتهديدات ومخاطر مستقبلية في حالة عدم قيام صناع القرار العراقي بتبني استراتيجيات للمواجهة وعلى كافة الانشطة والتصعيد سواء كانت سياسية او اقتصادية او الاجتماعية .

توصلت الدراسة الى مجموعة من الاستنتاجات اهمها :-

1. ان القوة باتت سيرانية اكثر مما هي قوة تقليدية .
2. الحروب الحديثة في القرن الحادي والعشرين اصبحت في جزء كبير منها يتم عبر فضاءات افتراضية وتدار بشكل الكتروني .
3. الحروب السيبرانية اصبحت تستهدف البنى التحتية الحيوية للدول وبما يسبب لها اضرار كبيرة جداً .
4. تعدد الاطراف والفاعل التي لديها امكانيات القيام بهجمات سيرانية الى جانب الدول بل ان الدولة ليست الطرف والفاعل الوحيد في تلك الهجمات .

5. القوة السيبرانية هي قوة شاملة لا تقتصر على الجوانب العسكرية فحسب بل على كل البنية الحيوية للدولة وخاصة قطاعات المالية والمصرفية وقطاع تكنولوجيا المعلومات والنقل والطيران والكهرباء والطاقة الخ .

6. الحروب السيبرانية أصبحت متغير مهم في معادلة الامن الوطني للدولة وقوتها .

7. العراق غير قادر بامكانياته الحالية وخاصة التكنولوجية للولوج فاعلاً ومؤثراً في ما يسمى بالفضاء السيبراني مما يرتب عليه اثار وتداعيات خطيرة على امنة الوطنى بابعاده كافة السياسية والاقتصادية والامنية والعسكرية بل وحتى الاجتماعية.

8. لابد من وضع استراتيجيات لمواجهة الاثار المترتبة التي قد يتعرض لها العراق مستقبلاً نتيجة دخوله الى الفضاء السيبراني العالمي فضلاً التطوير المستمر للاستراتيجيات المعمول بها حالياً وتكييفها وفقاً لمستجدات البيئة الدولية .