الحرب السيبرانية بين التحديات واستراتيجيات المواجهة : العراق إنموذجا [▽]

Cyber war between challenges and confrontation strategies: Iraq as a model

د.مهند جبار عباس [*]
Dr. Muhand Jabar

أ.د هيثم كريم صيوان[**]
Prof.Dr. Haithm Karim

ملخص البحث :

تطرق 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 تحقق امنها الوطني بدون تامين وحماية فضائها 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 يهئوا البيئة الأمنية السيبرانية التي تضمن صد أي هجوم قد تتعرض له بناه التحتية الحيوية مستقبلا ، وهذا يتطلب تبنى 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

[▽]تاريخ الاستلام : 2022/7/22 ، تاريخ القبول :2022 /8/29 ، تاريخ النشر : 2022/9/30
[*]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 اجل امتلاك أدوات القوة الجديدة المتمثلة بالمعرفة ومن يمتلك المعرفة يمتلك القوة والسلطة كما عبر عنها (الفن توفلر) في كتابه تحول السلطة .

التطور في تكنولوجيا المعلومات أدى الى ظهور فضاءات الكترونية افتراضية تدار من خلف الشاشات ، وعلى اثر ذلك انتقل الصراع والتنافس والحرب من الحالة الواقعية الى العالم الافتراضي وباتت الدول تتنافس فيما بينها لامتلاك مقومات القوة السيبرانية ، من اجل 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 الى 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 .

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

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

هدف البحث : يحاول البحث تحقيق جملة من الأهداف أهمها :

1. التعريف بمفهوم الحرب السيبرانية وبيان أهميتها وخصائصها وادواتها ومعرفة أطرافها ومجالات توظيفها .
2. بيان موقع العراق وقدراته في مجال المعرفة السيبرانية وبيان فيما اذا كان العراق يعاني انكشاف سيبراني .
3. توضيح استراتيجية مواجهة التحديات والمهددات 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 مواجهه هذا النوع من الحروب المستقبلية . لذا نطرح تساؤلات فرعية تتمثل بالاتي :

1. ما هي الحرب السيبرانية وأهدافها والأطراف الفاعلة بها ؟.
2. ماهي الأدوات والخصائص ومجالات التوظيف للقوة السيبرانية ؟.
3. هل يمكن للعراق ان يبقى بمعزل عن التطورات العالمية ومنها تطورات القوة السيبرانية ومجالات توظيفها ؟.

فرضية البحث : يطرح الباحث فرضية مفادها " العراق في ظل معطياته الحالية نجده من الضعف وعدم القدرة في مواجهة التحديات والمهددات التي تفرضها القوة السيبرانية وبالتالي نحن امام علاقة دالية طردية تتمثل بانه كلما تمكن العراق من تطوير امكانياته وقدراته الدفاعية في مجال القوة السيبرانية كلما كان اكثر قوة في مواجهة التحديات والمهددات 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 .

اولا : الحرب السيبرانية : اطار نظري عام

1. مفهوم الحرب السيبرانية .

جاءت كلمة السيبرانية من الكلمة الاغريقية kybernetes وتعني (الطيار او قائد الدفة) وهي مشتقة من كلمة سايبر وتعني اي شئ له علاقة بالحوسبة الالكترونية والعوالم الافتراضية المرئية ويكثر استخدام الكلمة في مجال تكنولوجيا المعلومات والانفوميديا ويشر 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 والحاق الاضرار بها [1] .

وعلى الصعيد العربي تم استخدام مصطلح القوة الالكترونية كمرادف للسيبرانية ويعد 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، بالاضافة لكونها لاتميز بين استهداف المنشآت المدنية أو العسكرية وصعوبة فرض حماية دولية ضدها [2].

اسلوبها الترويع وبث الخوف ، ولا يمكن معرفه حجم الاضرار التي توقعها، ولا كيف تم الهجوم وتعد من الحروب غير المتكافئة (war asymmetric) كون الطرف الذي يتمتع بقوة هجومية ويباغت باستخدامها يعد الطرف الاقوى ، بغض 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 طويل وتؤدي المهارات البشرية دورا اساسيا في تطويرها [3].

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 و34 ، ربيع 2020، ص 148 .

(2) عبد الله محمد العصيمي ، السيبرانية .. واشكال الحروب 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 والتجسس الالكتروني وهما في المستوى الثاني والثالث من النزاع في الفضاء السيبراني بالاضافة 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 بالاضافة الى تأثيرها على القيادة العسكرية واهتمامات المدنيين ومصالحهم في الفضاء السيبراني[1] .

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 ضررًا ماديًا 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 تهديدًا خطيرًا لأمن دولة أخرى[2].

لذا يمكن القول ان الحرب السيبرانية ، هي حالة التوظيف لتكنولوجيا المعلومات ضمن استراتيجية عسكرية (قد تكون دفاعية 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) [3] .

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

2. هدف الحرب السيبرانية .

(1) فيصل محمد عبد الغفار ، الحرب الالكترونية ،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 يعد تغيير البيئة الثقافية والفكرية للخصوم احد اهدافها أيضا[1].

ومصطلح البنية التحتية الحيوية كما حددتها السياسة الرئاسية للولايات المتحدة الامريكية وتشمل 16 قطاع مهم ادخلته الرئاسة الامريكية ضمن مجالات الامن القومي[2] . وكما جاء بجدول(1).

جدول(1) القطاعات الستة عشر للبنية التحتية الحيوية

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

(1) هبة عبدالفتاح ، الحروب السيبرانية الأكثر دمارًا.. 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 .
الطاقة	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 .
الخدمات المالية	البنوك والاتحادات الائتمانية والوسطاء والمؤسسات المالية الأخرى التي تودع الأموال وتسدد المدفوعات لأطراف أخرى ، وتوفر الائتمان والسيولة للعملاء ، وتستثمر الأموال لفترات طويلة وقصيرة ، وتحول المخاطر المالية بين العملاء
مزارع الغذاء والزراعة	مطاعم، مرافق تصنيع الأغذية وتجهيزها وتخزينها
المباني الحكومية	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
الرعاية الصحية	والصحة العامة البنية التحتية الحيوية التي تحمي جميع قطاعات الاقتصاد من الأخطار مثل الإرهاب وتفشي الأمراض المعدية والكوارث الطبيعية ، المستشفيات والمرافق الطبية الأخرى
تقنية المعلومات	الوظائف الافتراضية والموزعة التي تنتج وتوفر الأجهزة والبرامج وأنظمة تكنولوجيا المعلومات والخدمات ، يساعد في توفير وصيانة الإنترنت بالتعاون مع قطاع الاتصالات
المفاعلات النووية	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

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

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 والفواعل 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 والحاق الضرر بالطرف الاخر ولكن من غير دماء ، ادواته التجسس وسرقة المعلومات ولا تترك اية مخلفات مادية كما في الحروب التقليدية وهذا النوع من الصراع يتميز بعدم وضوح اطرافه وذو تداعيات خطيرة جدا مثل تدمير المواقع على الانترنيت او تعطيلها بالفايروسات وهي اسلحة من السهل استخدامها والحصول عليها من شبكة الانترنيت ، هذه الحروب الجديدة تجري وسط الشعوب وليست في الساحات التقليدية للصراع الدولي .

ومن كل ما تقدم نرى ان التطور السريع لتكنولوجيا 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 اساسيا فى تنفيذ عمليات فعالة على ارض الواقع .

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

قطع خدمة الإنترنت أو ضرب مواقعه أو توقيف رسائل البث التلفزيوني او الإذاعي أو ايقاف 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 : [1]

أ. **الدول** تعد الدول الفاعل الأكبر في الفضاء السبراني 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 و أبل Apple المنتشرة في مختلف دول العالم تسمح لها بامتلاك قواعد من البيانات العملاقة ، والتأثير في اقتصاديات كثير من الدول، وإن أرادت فيمكنها التأثير في قوة الدولة الاقتصادية وقوتها الناعمة أيضا من خلال تلاعبها بالبيانات والتصنيفات الدولية للاقتصاديات والأسواق .

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 Gmailالخاصة 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)**[*] : وهم الفواعل الذين يمتلكون معرفة تكنولوجية متطوره ولديهم القدرة على استخدامها، ولايمكن الكشف عن هوياتهم بسهوله، وذلك لصعوبة ملاحقتهم[2].

أصبح الفرد عنصرا" فاعلاً في التفاعلات الدولية، و أصبح يمارس من الأنشطة عبر الفضاء السيبراني ما يؤثر به في العلاقات الدولية. ولنا في ظاهرة الويكيليكس "phenomena WikiLeaks") مثال

(1) ايهاب خليفة ، مصدر سابق ، ص 33 .

(*) كلمة هاكر(Hacker) بمعناها الشمولي تفيد الشخص الذي يقوم بتغيير سلوك نظام معين ليؤدي وظائف غير التي انشأ من اجلها ، ويساعد كذلك على ايجاد الحلول للعديد من المشاكل في جميع المجالات، اما في مجال تقنية المعلومات فمصطلح هاكر يرجع الى الستينات من القرن الماضي ، وكان يطلق على الاشخاص اللذين لديهم دراية واسعة بجهاز الكمبيوتر والمتمكنين من البرمجة بصفة متميزة .

(2) سليـم دحمـاني ، أثر التهديدات "السيبرانية" على الأمن القومي الولايات المتحدة الأمريكية – أنموذجا(2001-2017) ، رسالة ماجستير غير منشورة ، جامعة محمد بوضياف – المسيلة ، الجزائر ، 2017 ، ص25 .

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

ومن أبرز مجموعات القرصنة على الفضاء السيبراني(مجموعة أنونيموس Anonymous»)* وهي مجموعة غير مركزية من القراصنة المنتشرين في العالم، ذات ثقل كبير فيما يسمى بالحرب الإلكترونية، مثلا مسئوليتها عن تسريب الاف رسائل البريد الإلكتروني الخاصة بالرئيس السوري (بشار الأسد) ، و كما هاجمت مواقع حكومية أمريكية وبريطانية و أخرى للناتو قبل أن تعلن مؤخرا مهاجمتها لمواقع حكومية (إسرائيلية) تعاطفا مع أهالي قطاع غزة الذين يتعرضون لحملة عسكرية جديدة .

د. المنظمات الإجرامية والجريمة الإلكترونية :

تعتبر المنظمات الإجرامية العابره للجنسية ، أحد الفواعل الدولية ذات التأثير في التفاعلات الدولية، والتي تحضى بحماية من بعض الحكومات الفاسدة . هذه المنظمات الإجرامية دخلت الفضاء السيبراني، و أصبحت 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 ترليون دولار سنويا" ، وانتحال شخصيات وهمية، أو حقيقية،و الهجوم على مواقع الإنترنت، والتعديل فيها و التلاعب في التجارة الإلكترونية،واستخدام الفيروسات التى تعطل الأنظمة العاملة، وتضر الأعمال، بالاضافة إلى جرائم الجنس والإعلان عن الرذائل والابتزاز [1] .

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 الإنترنت 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 إلكترونيًا أو عبر الأقمار الصناعية والسيطرة عليها أو تدميرها، الأمر الذي قد يسبب كارثة بشرية .

وتعد ممارسة القوة عبر الإنترنت إرهاب اذا صاحبها دوافع سياسية ، مثل التاثير في القرارات الحكومية أو الرأي العام[1].

4. ادوات 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 الانسانية المعاصرة للدول وهذه الاليات والوسائل هي برامج حاسوب وفيروسات الكترونية[2] .

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 والاسواق المالية والقطاعات الإنتاجية المختلفة[3].

ولهذه الحرب السيبرانية الجديدة وسائل مختلفة ، منها اختراق الشبكات و شن الحروب النفسية والتجسس وشن حرب الأفكار ، وسرقة المعلومات ، والتنافس بين أجهزة الاستخبارات الدولية[4] ومن أليات ووسائل

---

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

(2) بشلالق ليلى ، تاثير الحروب الالكترونية على العلاقات الامريكية الروسية ، رسالة ماجستير غير منشورة ، ، جامعة محمد بوضياف المسيلة ، الجزائر ،2018 ، ص 14 .

(3) عادل عبد الصادق ، اسلحة الفضاء الالكتروني في ضوء القانون الدولي الانساني ، 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(*) ، والديدان(*)، وحيل تصيد المعلومات التي تستغل العيوب والثغرات الموجودة في البرامج الأخرى واخطاء 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 ، وانظة حواسيب العدو وغالبا بعد أن يقومون باختراق الشبكة لأول مرة فإنهم يتركون وراءهم ثغرة تسلل تسمح لهم بالدخول في المستقبل بطريقة سهلة وسريعه ؛ وأحيانا لايكتفون بسرقة نسخة من البرنامج فحسب بل قد يضيفون إليه شيئا ما لاستخدامه مستقبلا ، وأحيانا اخرى تسمح لهم ثغرةالتسلل بالوصول إلى جذر البرنامج فتصبح لديهم القدرة و الصلاحيات التي يتمتع بها مصمم البرنامج وبتالي يمكنهم إضافة ما يشاؤون من برمجيات خبيثة ويمحون أي اثر على وجودهم[1] .

ومن ناحية اخرى تعد شبكة الانترنيت 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 كتصوير مشاهد العنف على نطاق واسع من اجل بث الذعر والخوف[2].

5. خصائص الحرب السيبرانية

ويمكن اجمال ابرز الخصائص والسمات للحروب السيبرانية بما يلي : [3]

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

(*) الديدان هي برامج لاتتطلب تمريرها الى مستخدم اخر لانها قادرة على نسخ نفسها ذاتيا باستغلال عيوب معروفة ثم تزحف كالديدان عبر الانترنيت .

(1) بشلالق ليلى ، 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 – تتسم بالشمولية نتيجة لتعدد اشكال الموارد السيبرانية واختلاف اماكن توطنها ، وتباين قيمتها الاقتصادية وتعدد الفواعل التي تملكها ، وتنوع الحقول المعرفية التي تمثلها ، مما يؤدي الى تعقيد المجال الذي تمتد على مساحته اضرارها .

ب – لا يمكن معرفة شخصية و معالم بصمة الحضور للفاعلين في الساحة السيبرانية ، مثل المنظمات او الجماعات او الافراد او الدول ، وذلك لتخفيهم خلف كواليس الفضاء السيبراني .

ج – أنعدام البعد المكاني للفضاء السيبراني مما ادى الى صعوبة التحكم بمسارات التهديدات او الهجمات السيبرانية، وسير تفاعلاته في شبكات المعلومات المترابطة والمعقدة ، الامر الذي يجعل من الصعوبة بمكان ايقاف التهديدات او الهجمات السيبرانية وتكاثر فرص انطلاقها تجاه اي هدف ومن اي عقدة في نسيج شبكاتها العالمي .

د – تميزت الحروب السيبرانية ايضا ، بتراجع الحصانة الامنية فيها وذلك بسبب تعقد الفضاء السيبراني وتنوع البيئات البرمجية ، وكثرت انواع معدات المعلومات والاتصالات والية تواصلها فيما بينها وكثرت الثغرات السيبرانية وتنوعها وحصول تطورات مستمرة لكل هذه الامور ادى الى تفاقم الثغرات وظهور فجوات جديدة يمكن التسلل من خلالها .

هـ – ان امكانية القيام بالحروب السيبرانية عبر حواسيب منفردة او مجموعه من الحواسيب المرتبطة بشبكة الانترنيت وتوفر التطبيقات المجانية المنتشرة على مواقع 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 معلنه 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 و تسارع للمخاطر لا يستطيع صانع القرار اتخاذ قرارات تتناسب مع حجم المخاطر الناجمة من الهجوم السيبراني.

6. مجالات توظيف القوة السيبرانية

نظرا لتحول الفضاء الإلكتروني إلي ساحة للتفاعلات الدولية ، برز العديد من الاشكال التوظيفية للقوة السيبرانية في الفضاء السيبراني ، وذلك على صعيد الاستعمالات المدنية أو العسكرية و على حد سواء ، مما ادى الى جعل هذا الفضاء مجالا للصراعات المتنوعة ، بين الفاعلين من الدول أو غير الدول و التسابق في امتلاك أكبر قدر من القدرات والتأثير في هذا المجال الجديد للصراع في الساحة الدولية [1] .

أ. المجالات السياسية

يمكن توظيف القوة السيبرانية سياسياً عبر استخدام موقع اليوتيوب لرفع حاجز التعتيم الذي تفرضه الحكومات الديكتاتورية في إخفاء انتهاكها لحقوق شعبها، وايضا" تستخدم لإدارة العمليات النفسية والتأثير في الرأي العام، ومن جانب اخر ساهمت القوة السيبرانية في توضيح أهمية دور الصورة في تأجيج الأحداث الدولية مثل ما حدث في حالة نشر الرسوم الكاريكاتورية المسيئة للرسول الأعظم وهو ما أنتج احتجاجات دولية واسعة وتوترات في طبيعة العلاقات الدولية [2] .

بالإضافة الى انها غيرت في مفهوم ومصادر الثقافة السياسية والتنشئة السياسية ، كما ادت الى تغيير أدوات العمل السياسي الوطني من خلال استخدام نموذج الحكومة الالكترونية واستثمار دور وسائل التواصل الاجتماعي في نشر الوعي السياسي و التأثير في العملية الانتخابية[3].

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 إلى آلاف السنين، لكن خصوم اليوم اصبح 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://aafaq.kku.edu.sa

(2) شيماء عويس ابو عيد ، القوة في العلاقات الدولية: دراسة تأصيلية ، دراسة منشوره على موقع الاليكتروني 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 مقياسا" هامًا في تقييم القوة الوطنية لأي دولة، وهذا ما اشار الية تقرير "التوازن العسكري لعام 2020 الذي يصدر عن المعهد الدولي للدراسات الاستراتيجية في كل عام ، إذ تبين أن عددًا قليلًا من الدول قد تحوّل بشكل كامل نحو دمج عمليات الفضاء السيبراني في هياكل القوة المتنوعة [1].

نحن على عتبات تحول عظيم في التكنولوجيا العسكرية، ستنعكس تأثيراته على كيفية خوض الحروب، وتتعدى 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 الآن، والطيارون الجالسون في نيفادا يقتلون عن بعد "الإرهابيين" في أفغانستان، ويسعى العلماء لمناقشة درجة الذكاء والدموية التي ستبرمَج بها اختراعاتهم الروبوتية وان الكثير من مؤلفي قصص الخيال العلمي، يقدِّمون افكارا خيالية ربما تترجم على ارض الواقع من قبل البنتاجون بشأن الجيل القادم من الأسلحة الروبوتية .

ثانياً _ العراق والظاهرة السيبرانية الجديدة :

خرج العراق من عزلة دولية خانقة استمرت لفترة طويلة جدا 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 تامين متطلبات تحقيق الامن وكل شي ياتي 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 وزياده 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 بمعزل 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 الالكترونية والتعاملات المالية التي تتم عبر أنظمة السويفت العالمية والعملات الرقمية والحكومة الالكترونية ، وهذه كلها متغيرات وتطورات حصلت في البيئة الدولية مؤخرا 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 وانفتاحه على العالم الخارجي وبمتغيراته كافة بما فيها السيبرانية وما يدور فيها ، فعلينا ان ندرك بان السياسة والاقتصاد والحرب باتت تتم في الفضاء السيبراني حتى الحروب باتت سيبرانية 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 تترك اثار كبيره على البنى التحتية الحيوية للدولة ومؤسساتها وتعمل على شلها وتدميرها مما يترتب عليه اضرار بمؤسساتها بمختلف الميادين الاقتصادية والثقافية والسياسية والعسكرية وهذا يتطلب استراتيجيات لتامين الامن السيبراني العراقي[1] .

2. العراق والمهددات السيبرانية الجديدة :

دخلنا عالم الفضاءات السيبرانية وبدا كل شي يدار الكترونيا وعبر شاشات رقمية في الميادين كافة السياسية والاقتصادية والاجتماعية والعسكرية والأمنية وهذا الفضاء ينطوي على مهددات جديدة يجب على صانع القرار الأمني العراقي التحوط منها مستقبلا ، وتلك المهددات المستقبلية تتمثل بسهولة توظيف الأطراف والفواعل الدولية كافة للفضاء الإلكتروني العراقي من اجل ضرب البنى الحيوية للدولة فالمهددات القادمة لم تعد تقليدية عن طريق استخدام القوة العسكرية بشكل مباشر وانما من خلال استهداف الفضاء الإلكترونية للدولة وهكذا لابد من توافر ادراك لدى الجميع وخاصة النخب الأمنية والعسكرية العراقية بان هناك مهددات وحروب تتم في الفضاء الالكتروني (السيبراني) تستهدف شبكات الحوسبة التي توجه وتدير مؤسسات الدولة وبناها 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 متصاعد في العالم الرقمي فزاد عدد مستخدمين شبكة الانترنت والهواتف النقالة واستخدم معظم الشعب العراقي اللأنترنت في مجال الاعمال والتجارة والخدمات الحكومية والتعليم والصحة وغيرها من الأنشطة الاقتصادية والاجتماعية بل وحتى السياسية اي هناك حاله من التزايد في التعاملات والخدمات الإلكترونية داخل العراق[1] ، اذ امام هذا التصاعد في استخدام شبكة الانترنت تبرز تحديات ومهددات تستهدف البنى التحتية للاتصالات والمعلومات داخل العراق وتهدد تلك التعاملات والخدمات في العراق فقد تتعرض تلك البنى التحتية الى خطر الاختراق والتخريب المتعمد من قبل هجمات سبرانيه تستهدف اعاقه تقديم الخدمات الحيوية او نشر برامج وفايروسات لتخريب كل البنى التحتية الحيوية للاتصالات وتكنولوجيا المعلومات فضلا عن تدمير نظم التحكم الصناعي الحيوية وخاصه 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 انكشافا كبيرا امام الهجمات السيبرانية .

بعبارة أخرى ان العراق يعاني من ضعف الامن الالكتروني مما جعل العراق في حاله من الانكشاف الاستراتيجي تجاه الاطراف الاخرى فهناك سهولة كبيرة لاختراقه والتجسس على بياناته والمعلومات الخاصة بمنظوماته 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 تتمثل في ضعف الامن الرقمي وافتقاره للبنى التحتية الرقمية سواء كانت مصرفية 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 تبنى مشروع توطين الرواتب الذي

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

تديره الكثير من الشركات المالية والتي باتت تحتفظ بالمعلومات الشخصية للموظفين داخل اجهزه الكترونية خارج البلاد وكذلك ايضا اختراق مواقع الكترونيه مهمه تابعه للحكومة العراقية واهمها موقع جهاز الامن الوطني وكذلك ايضا استخدام التكنولوجيا ومنصات التواصل الاجتماعي في التحشيد لتظاهرات تشرين عام 2019.

والعراق احتل مكانة متدنية 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 [1]:

أ. دولة مكشوفه امام القوى السيبرانية والتنظيمات الإرهابية .

ب. تدني البنى التحتية الرقمية فيه .

ت. يعاني التخلف والامية الرقمية خاصه في الميدان الاقتصادي والاقتصاد الرقمي والحوسبة المالية والمصرفية .

ث. زيادة احتمالية تعرضه لشن هجمات سيبرانية عليه قد تستهدف المراسلات الحكومية او سرقة الاسرار الأمنية والاقتصادية والاجتماعية للبلد .

ج. تعاظم تعرضه للإرهاب الالكتروني والتجسس والقرصنة الإلكترونية وعمليات غسيل الاموال واستخدام شبكات الانترنت لممارسة النصب والاحتيال والجريمة الإلكترونية والاتجار بالبشر والمخدرات .

ح. ينطوي العراق على الاستخدام السلبي لمواقع التواصل الاجتماعي والتي قد توظف للقيام بأثارة الاضطرابات الداخلية فلاحظنا خلال الفترة الماضية كيف ان تنظيمات الإرهابية قامت بتوظيف مواقع التواصل الاجتماعي في عمليه التجنيد واصبح لتلك التنظيمات مواقع الكترونية واستخدامها للفيسبوك واليوتيوب والتلغرام 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 الالكتروني والتشهير بالأفراد عبر اختراق الحسابات الشخصية والابتزاز المالي والجنسي والسب والقذف والاتجار بالبشر والمخدرات وهذه

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

مظاهر باتت تشكل تهديدات كثيره على الامن الوطني العراقي وكذلك تزايد احتمالية اختراق المواقع الحكومية لاحظ في الانتخابات العراقية لعام 2018 ،جرى نشر الكثير من التسجيلات الصوتية لعمليه 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)• 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 ارهابيه وبجرائم منظمة تستهدف تهديد وتعطيل البنى التحتية الحيوية داخل العراق وهذا ما شهدناه في الحرب مع داعش وكيف تم توظيف مواقع التواصل الاجتماعي في عملية الدعاية والحرب النفسية والتجنيد والتخريب الى اخره[1] .

لذا لابد من حماية الامن السيبراني العراقي وخاصة تلك المواقع المرتبطة بأمن البنى التحتية الحيوية التي يجب ان تكون بعيده عن الاختراق والهجمات السيبرانية مستقبلا فهذا الاختراق هو اختراق للسيادة العراقية والقيم السياسية والاجتماعية السائدة في المجتمع العراقي فهناك قطاعات حيوية مستهدفه تتمثل بقطاع 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 لسرقه الهوية الرقمية والبيانات الخاصة وكل تلك القطاعات تعد مهمة للأمن الوطني العراقي .

وعليه نقول ان العراق يعد احدى الدول المنكشفة سيبرانيا وهذا الانكشاف ينطوي على تحديات ومهددات كثيرة وفي مختلف المجالات وخاصه 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 السبيراني فكل الدول اخذت تسابق للانتقال الناجح من الفضاء الواقعي الى الفضاء الافتراضي الالكتروني الا ان العراق لم يمر بمرحله 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 فريق 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، ص171.

ثالثاً _ العراق ومتطلبات مواجهة التحديات السيبرانية

1. حتمية تبني استراتيجية وطنية عراقية للأمن السيبراني :

يعد الامن الوطني لأي دولة قضية مهمه 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 والعراق يمر بمرحله مضطربة سياسيا وامنيا واقتصاديا تتطلب معها وضع استراتيجيات جديده غير تقليدية للأمن والتحديات باتت كثيره 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 للتنافس 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 تتبنى وتوظف اساليب القوة السيبرانية والأسلحة الإلكترونية من اجل التصدي لأي هجمات متوقعه 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 سيبرانية على الرغم من ان العراق لم يدخل بعد عالم الفضاء السيبراني فما يزال في مرحلة (الحبو) مقارنة بالدول الاخرى ، فالعراق مؤسساته وبناه 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 الالكترونية التي تدار من خلال شبكات الحاسب الالي يضاف الى ذلك حتمية زيادة توجهه نحو التجارة الالكترونية والاقتصاد الرقمي والتعاملات 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 الارتقاء بقدرات العراق على صد اي هجمات سيبرانية تصدر من قبل اي طرف خارجي ، وكذلك تطوير قوة ردع سيبرانية 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 [1].

2. العراق وضرورة توفير مرتكزات الامن السيبراني مستقبلا :

احتل العراق المرتبة (107) عالميا و(13) عربيا عام 2018 ، الا انه تراجع بمقدار (22) نقطة في عام 2020 ليكون بالمرتبة (129) عالميا من اصل(184) دوله (17) عربيا [2] .

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

أ. المرتكز التشريعي القانوني ، فلابد من وجود مؤسسات وتشريعات قانونيه تتعامل مع الامن السيبراني والجريمة الإلكترونية والإرهاب السيبراني .

ب. الركيزة التقنية نجد بان العراق يفتقر الى مؤسسات فنيه متخصصه وذات كفاء عالية تستطيع التعامل مع التحديات السبرانيه لذا لابد من توفير ذلك المرتكز .

ت. المرتكز التنظيمي حيث نجد ان العراق يفتقر الى المؤسسات واستراتيجيات الخاصة برسم وصناعه السياسات لتطوير الامن السبراني على المستوى المحلي.

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

---

(1) للمزيد ينظر : مستشارية الأمن الوطني العراقي امانة سر اللجنة العليا لأمن الأتصالات 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

(2) باسل علي خريسان ، الامن السيبراني في العراق قراءة في مؤشرات الامن السيبراني لعام 2022 ، مركز البيان للدراسات والتخطيط ، بغداد 2022 ، ص9 .

ج. ضرورة بناء تعاونات وشراكات وتحالفات في مجال السيبرانية حيث ان العراق ما يزال بعيدا عن وجود شراكات تعاونيه وشبكات لتبادل المعلومات فما زال العراق يعاني من عزله اقليميه ودوليه 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 .

وباتت تلك الحروب تفرض التحديات ومخاطر على الامن الوطني للدول فهي تستهدف البنى التحتية الحيوية للدول ونظراً لسهولة القيام بها وقلة تكليفها فضلا عن حجم الاضرار التي من الممكن ان تلحق بها الدولة المستهدفة اصبحت اطرافها لاتقتصر 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 سيبراني خارجي وتهديدات ومخاطر مستقبلية في حالة عدم قيام صناع القرار العراقي بتبني استراتيجيات للمواجه وعلى كافة الانشطة والصعد سواء كانت سياسية او الاقتصادية او الاجتماعية .

توصلت الدراسة الى مجموعة من **الاستنتاجات اهمها** :-

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

5. القوة السيبرانية هي قوة شاملة لاتقتصر على الجوانب العسكرية فحسب بل على كل البنى الحيوية للدولة وخاصة قطاعات المالية والمصرفية وقطاع تكلنوجيا المعلومات والنقل والطيران والكهرباء والطاقة الخ .
6. الحروب السيبرانية اصبحت متغير مهم في معادلة الامن الوطني للدولة وقوتها .
7. العراق غير اقدر بامكانياتة الحالية وخاصة التكلنوجية للولوج فاعلا ومؤثراً في ما يسمى بالفضاء السيبراني مما يرتب عليه اثار وتداعيات خطيرة على امنة الوطني بابعادة كافة السياسية والاقتصادية والامنية والعسكرية بل وحتى الاجتماعية.
8. لابد من وضع استراتيجيات لمواجة 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 .