مجلة جامعة الانبار للعلوم القانونية والسياسية

Journal of Anbar University for Law and Political Sciences
مجلة جامعة الانبار للعلوم القانونية والسياسية
P. ISSN: 2706-5804 E.ISSN: 2075-2024
Volume 14- Issue 1- March 2024 المجلد ١٤- العدد ١ – اذار ٢٠٢٤

Cyber war and its impact on national security (Iraq as an example)

[1] Assist. Lecturer. Mahmood Yaseen Ahmed [2] Assist. Lecturer. Mohammed Jubair abbas

[1]College of Law and Political Science, Anbar University [2] College of Administration and Economics/University of Fallujah

Abstract:

The focus of the study is to clarify what is the concept of cyberwar and what its dimensions are, and through our acquaintance with the concept of cyberwar as well as its definitions, a comprehensive and specific definition of war has not been identified. Thus, the impact of cyberwar on the People's Armed Forces, by highlighting the importance of the repercussions that pose a threat to the security state, also continues to demonstrate international perseverance to address war. It also explains how the cyber war occurred to Iraqi national security, and what is the Iraqi strategy for confronting the war.

1: Email: mahmood.yaseen@uoanbar.edu.iq

2: Email: mohammed.j.abbas@uofallujah.edu.iq

DOI
10.37651/aujlps.2024.145683.1153

Submitted: 24/1/2024
Accepted: 10/2/2024
Published: 15/03/2024

Keywords:
Cyber
Security
Iraq.

الحرب السيبرانية وتأثيرها على الامن القومي (العراق انموذجاً)

[١] م.م.محمود ياسين احمد[٢] م.م محمد جبير عباس

[١] كلية القانون والعلوم السياسية /جامعة الانبار [٢] كلية الإدارة والاقتصاد/ جامعة الفلوجة

الملخص:

تهدف الدراسة الى تبيان ما هو مفهوم الحرب السيبرانية وماهي ابعادها، والذي من خلال تعرفنا على مفهوم الحرب السيبرانية وكذلك تعريفاتها، والذي لم يتم ايجاد تعرف جامع ومحدد للحرب. كذلك اثر الحرب السيبرانية على الامن القومي للدول من خلال ابراز اهم الانعكاسات التي شكلت خطر يهدد من خلالها امن دولة، وتهدف ايضا الى تبيان الجهود الدولية لمعالجة الحرب السيبرانية. وكذلك تبيان كيف اثرت الحرب السيبرانية الى الامن القومي العراقي، وما هي الاستراتيجية العراقية لمواجهة الحرب.

الكلمات المفتاحية:

الحرب السيبرانية ، الامن ، العراق

المقدمة

شهد العقد الاخير من القرن الماضي تطورات كبيرة على مستوى التقدم التكنولوجي المعلومات والاتصالات وشبكات الانترنت على مختلف استعمالاتها، صاحب ذلك التطور الملحوظ في تنامي ما يسمى بالحرب السيبرانية والتهديدات الامنية التي انتج عنها تهديدات الامنية للدول ضمن الفضاء السيبراني، الذي ساهم من خلال ادواته المختلفة في أعادة رسم البعد الامني والعالمي والمحلي، ويعمل على تشكيل الوعي والادراك السياسي والامني للأفراد والمجتمعات بصورة مغايرة مما كانت عليه. وفي ضل الحرب السيبرانية انتفت مفهوم السيادة واصبحت حرب عابرة للحدود، ولهذا اصبحت الحرب السيبرانية تهدد وبشكل مستمر الدول والمؤسسات البنكية والمصرفية. ما يجعل الدول تعمل على ايجاد قوانين تحد من التهديدات السيبرانية. يعد الامن القومي العراقي الركيزة الاساسية في قوة الدولة ولا يمكن ان نتصور بأي شكل من الاشكال تقدم الدولة دون تحقيق استقرار في أمنها القومي، لذلك يعاني الامن القومي العراقي من تحديات كبيرة بعد عام ٢٠٠٣ وعلى جميع المستويات، واحده من اكثر من هذه التحديات هي الحرب السيبرانية التي باتت تشكلت تهديدا كبيراً على المنظومة الاستراتيجية للأمن القومي العراقي.

أولاً: اهمية الدراسة: ينبع اهمية هذا الموضوع كون الحرب السيبرانية تشكل اليوم واحد من هم المواضيع الحيوية في مجال الاكاديمية والتي تمس الحياة الاجتماعية والسياسية والاقتصادية، كما تعطي رؤية لماهية الحرب السبرانية وما تفرضه من تحديات ومخاطر مستقبلية ومعرفية على مكانة العراق في المنظومة السيبرانية ، ومن ثم معرفة اهم التحديات التي يفرضها الفضاء السيبراني على الامن القومي العراقي، كما تنبع اهمية الدراسة التي تعطي تصور لصانع القرار العراقي بضرورة العمل على اعداد بيئة امنية سليمة في المستقبل.

ثانياً: اشكالية الدراسة: تتمحور اشكالية الدراسة حول سؤال مركزي هي "ما مدى طبيعة التهديدات الحرب السيبرانية على الامن القومي للدول، وكيف اثرت على طبيعة الامن القومي العراقي"؟

وهذا السؤال ترتبط معه اسئلة فرعية هي:

١- ما الحرب السيبرانية وما ابعادها؟
٢- كيف اثرت الحرب السيبرانية على الامن القومي للدول وما هو سبل معالجتها؟
٣- ما تداعيات الذي يواجها العراق في اطار الحرب السيبرانية وما الاستراتيجية لمعالجتها؟

ثالثاً: فرضية الدراسة: تنطلق فرضية الدراسة مفادها ان الحرب السيبرانية اصبحت تشكل تهديدا كبيرا وبارزاً في القرن الواحد والعشرين على سياسات الامن القومي للدول والعراق واحده منها. **مناهج الدراسة:** تعتمد الدراسة على المنهج التحليلي والوصفي لتحليل ووصف الحرب السيبرانية ومدى تأثيرها على الامن القومي للدول وذلك تحليل رؤية صانع القرار العراق في مجال الحرب السيبرانية.

I. المبحث الاول

الحرب السيبرانية مفهومها وأبعادها

انتج التطور التكنولوجي خلال السنوات الاخيرة من ظهور التقنيات والمعلومات في مجالات الحاسوب وظهور متخصصين في هذه المجالات الحديثة، ما ادى هذه التطور الى انتشار واسع في استخدام شبكات الانترنت، وظهور مفاهيم جديدة في اطار السياسة الدولية ومن هذه المفاهيم ما يسمى بالحرب السيبرانية، والذي من خلال هذا المبحث سوف نبين ما هي الحرب السيبرانية وما هي ابعادها.

I.أ. المطلب الاول

مفهوم الحرب السيبرانية

شهد مطلع القرن الحادي والعشرون التقدم الهائل في التكنولوجيا المعلومات الذي كان له دور كبير في كافة مجالات الحياة، ولقد انتج هذا التطور في تقنيات الالكترونية الجديدة واعتمادها الكبير في البنى التحتية وفي المؤسسات الحكومية وغير الحكومية، ما ادى الى اتساع دائرة المخاطر والتهديدات العسكرية التي تم اعتمادها على انظمة الحاسوب والنظم الالكترونية الحديثة [١].والحرب السيبرانية واحده من المفاهيم التي انتجها هذا التطور في التكنولوجيا الحديثة، الا ان هذا المفهوم اخذ يشكل حالة من عدم الوضوح، بل وجود جدل بين الاكاديميين أيضا حول مفهوم الحرب السيبرانية ، والسبب في ذلك الى تطور الكبير في المعلومات الالكترونية، ما ادى الى ضيق الفجوة الحرب السيبرانية تشكل ويعاد تشكيلها بصورة مستمرة، وهو ما انتج الى عدم اتضاح مفهوم بكافة ابعاده[٢].

تعد الحرب السيبرانية مفهوماً جديداً على صعيد النزاعات المسلحة، وتشمل هذه الحرب على اساليب ووسائل قتالية تتألف من عمليات الكترونية ترقى الى مستوى النزاع المسلح، وتستخدم في سياقة وتعمل هذه الحرب على تدمير الكلي لأنظمة والمعلومات وشبكات الاتصال لعدو[٣].

وتتميز الحرب السيبرانية عن الحروب التقليدية، إذ ان الحرب التقليدية تستخدم فيها الجيوش والاسلحة التقليدية النظامية ويسبقها اعلان واضح كحاله الحرب وميدان قتال محدد، بينما هجمات الحرب الالكتروني تبدو غير محدده الاهداف كونها تتحرك عبر شبكات المعلومات الاتصالات عابرة للحدود الدولية، بالضافة الى اعتماده ما يمكن وصفة بالأسلحة الالكترونية وطبيعة الجديدة للسباق الالكتروني لعصر المعلومات، إذ يتم استخدامها ضد الاجهزة الاستخبارات والمنشآت الحيوية او عملاء ، وعليه فأن احد المعايير التميز بين الحرب السيبرانية والحرب التقليدية يمكن ان يكون بالاستناد الى طبيعة السلاح المستخدم، وبالتالي يمكن القول ان الحرب السيبرانية، هي الحرب التي تستخدم فيها الاسلحة غير

---

(١) قيس خلف المحمداوي، *الحروب الجديدة والتحول في مفاهيم القوة بعد الحرب الباردة*، (عمان: دار امجد، ٢٠٢٢)، ص٣٥.

(٢) ايهاب خليفة، *الحرب السيبرانية(الاستعداد لقيادة المعارك العسكرية في الميدان الخامس)*، (ابو ظبي: دار العربي، ٢٠٢١)، ص٧٢.

(٣) باي سمير، "التهديدات الامنية السيبرانية: دراسة في انعكاسات الحرب الالكترونية على الامن القومي للدول واستراتيجيات المقاومة"، *مجلة الرسالة للدراسات والبحوث الانسانية، الجزائر*، العدد (٢)، المجلد(٨)، (٢٠٢٣): ص١٩٦.

التقليدية وفقاً للأثار المترتبة على استخدام هكذا نوع من الاسلحة والمتمثلة بالتدمير واسع النطاق[١].

ونظراً لما تقدم اتضح ان الحرب السيبرانية لها خمسة جوانب تحدد عملها وهي[٢]:

١- ان هذه الحرب رقمية تستهدف فئات معينة، قد تكون افراداً او مؤسسات او منظمات او دول.
٢- ان بيئة المعلومات الرقمية هي المستهدفة في هذه الحرب.
٣- ان سلاح هذه الحرب هي النظم والوسائل الالكترونية والاتصالية بشتى انواعها.
٤- لهذه الحرب تكاليف سياسية واقتصادية اجتماعية وامنية باهظة الثمن.
٥- الجانب الايديولوجي والذي قد يعتلى ممارسات هذه الحرب في الفضاء الالكتروني.

ويمكن ان تكون الحرب السيبرانية صراعاً بين الدول، ولكنها قد تشمل جهات فاعلة اخرى غير الدول بطرق مختلفة، وفي الحرب السيبرانية من الصعب توجيه قوة دقيقة ومتتالية ويمكن الهدف عسكرياً وصناعياً ومدنياً او يكون هناك مجموعة متنوعة من العملاء يحكمهم هدف واحد بينهم[٣]. ولهذا تتميز الحرب السيبرانية بسمات وهي[٤]:

١- نشوئها في الفضاء السيبراني بشكل غير متوقع للجهة المهاجمة، ذلك لكون الفضاء السيبراني يرتبط بالحاسبات وشبكات الاتصال وان هذا الهجوم يخلف الاضطراب وتعطل الانظمة والاجهزة.
٢- هذه الحرب تتجاوز الحدود الوطنية في كثير من الاحيان، وتؤثر على عمليات نقل البيانات على كثير من بلد في نفس الوقت، وقد تتسبب للجهات المعرضة للهجوم اضراراً مالية ضخمة لشركات اعمال التجارة الالكترونية، وشبكات الاتصالات المدنية والمواقع الاخرى.
٣- المهاجمون السيبرانيون لا يحتاجون للتواجد في المكان الذي يحدث فيه الهجوم او حتى في المكان الذي يظهر فيه، ويستطيع المهاجمون اثناء القيام بالمهجوم استعمال تكنولوجيا، تصال مجهول الهوية التشفير لإخفاء هويتهم.

---

(١) فارس محمد العمارات وابراهيم الحماصة، *الامن السيبراني: المفهوم وتحديات العصر*، (عمان: دار الخليج، ٢٠٢٢)، ص١٢٥.

(٢) غريب حكيم، شرقي صبرينة، "تداعيات الحرب الالكترونية على العلاقات الدولية: دراسة في الهجوم الالكترون على ايران"، *مجلة دفاتر السياسية وقانونية، الجزائر*، العدد (٢)، المجلد (١٢)، ص٩٦.

(1)-Paul Cornish, David livingstone and otler, on cyber war fare the royal institute of international affairs, London, 2010, p.8.

(٤) علاء عبد الرزاق محمد، *المدخل الى الامن السيبراني(الفضاء السيبراني -تهديدات الفضاء السيبراني- الاسلحة السيبرانية ووسائل مواجهة التهديدات-استراتيجيات الامن السيبراني)*، (بغداد: دار الكتب والوثائق، ٢٠٢١)، ص٤٣-٤٤.

وعلى الرغم من عدم وجود تعريف جامع للحرب السيبرانية الا ان قد عرفها بعض المختصين، بأنها: تلك الحرب التي تتم ادارتها في مجال الفضاء الرقمي، تمثل الدول فيها كفواعل رئيسية، إذ تستخدم الاليات والاسلحة الالكترونية في الهجوم الذي يكون موجة اساسياً الى اجهزة الحاسب الآلي او شبكات الالكترونية الخاصة بالعدد او الانظمة الالكترونية وما تحتويه من معلومات وخاصة بالدول مما يحول دون استخدام هذه الانظمة والاجهزة والشبكات او تدميرها بالكامل(١).

ويعرف كل من "جون أركيلا" و"دافيد رونفيلت" الحرب السيبرانية بأنها: تنفيذ، والاستعداد لتنفيذ العمليات العسكرية وفقاً للمبادئ المعلوماتية، من خلال تعطيل- ان لم يكن تدمير- نظم المعلومات والاتصالات على واسع نطاق"(٢).

I.ب. المطلب الثاني

انواع الحرب السيبرانية

تتنوع اشكال الحرب السيبرانية مع انماط متعددة تعود لطبيعة الصراع وللضرورة التي تفرض أي شكل من هذه الاشكال، وقدرة العدو على التصدي لها(٣).وللحرب السيبرانية عدة أشكال، يمكن توضيحها وفق الآتي:

اولاً: الحرب السيبرانية منخفضة الشدة:

يعد الفضاء السيبراني ساحة للصراع المستمر بين الفاعلين، وقد يكون ذات طبيعة غير سلمية وتتميز بالعدائية، ويوصف انه جذوره عميقة ومتداخلة، له نواح متعددة اقتصادية، اجتماعية وثقافية. وفي ضل هذه الصراعات الغالب يتم استخدام القوة الناعمة للحرب السيبرانية فيها، على الرغم من انها لأتطور لتصل الى الحرب التقليدية في الغالب، او قيام بحرب سيبرانية شاملة(٤).

وتشكل هذه الحرب في حالات الصراع الطويل بين الدول والقوى والمنظمات كالصراع الامريكي الروسي، والصراع الصيني الامريكي، والصراع بين كوريا الجنوبية والشمالية.

---

(٣) ينظر الى:ا لعوفي دليلة، "الحرب السيبرانية في عصر الذكاء الاصطناعي ورهاناتها على الامن الدولي"، *مجلة الحكمة للدراسات الفلسفية، الجزائر*، العدد(٢)، المجلد(٩)، (٢٠٢١): ص٧٨٣.

(٢) ينظر الى شريفة كلاع، *الامن السيبراني واشكال التهديد: تحديات عالمية*، (الجزائر: ألفا للوثائق، ٢٠٢٣)، ص١٣٠.

(٣) بن تغري موسى، "الحرب السيبرانية والقانون الدولي الانساني"، *مجلة الاجتهاد القضائي، الجزائر*، العدد(٢٢)، المجلد(١٢)، (٢٠٢٠): ص٢٠٤.

(٤) فراس جمال شاكر، *السيبرانية وتحولات القوة في النظام ادولي*، (عمان: دار امجد، ٢٠٢٢)، ص٢٥٣.

كما تنشط كذلك بين الانظمة الحاكمة والمعارضات السياسية والعسكرية، وبين المنظمات التي تتبنى وتدافع عن الحقوق والحريات كالانونموس وجماعات حماية البيئة وغيرها، وبهذا الشكل من اشكال الحرب السيبرانية الناعمة وسائل كثيرة منها، التجسس وسرقة المعلومات الالكترونية والحرب النفسية والهندسة الاجتماعية والتأثير على اراء الناخبين والتضليل الالكتروني، وحروب العقول والافكار الاختراعات والتصنيع الحربي، والتنافس على الريادة الالكترونية العالمية في عصر الرقمية والاتصالات[١].

وتتجلى هذا النمط في حالات الحروب الهجمات السياسية ذات البعد الديني والاجتماعي الممتد، مثل الصراع الهندي الباكستاني، والصراع العربي الاسرائيلي، او صراع الكوريتين. وفي الانتخابات الامريكية تعرضت روسيا للاتهام بالقرصنة الالكترونية لدعم المرشح الامريكي دونالد ترامب في مواجهة منافسة الديمقراطي كلينتون. وفي النرويج، والتشيك وبريطانيا تم اتهام روسيا بشن هجمات الالكترونية عليها، مما دفع الدول الاخيرة لإعلان انها قادرة على الرد بالمثل. وايضا استطاعت ايران شن هجمات الالكترونية في منطقة الخليج العربي على منشآتها النفطية[٢].

ثانياً: الحرب السيبرانية متوسطة الشدة:

في هذا النمط من الحرب يكون فيه الفضاء السيبراني ساحة موازية لحرب التقليدية التي تحدث على الارض. وذلك يكون تعبيراً عن طبيعة الصراع القائم بين الاطراف، كما انه يكون مهدد لقيام لعمل عسكري، وتدور حرب السيبرانية عن طريق اختراق الانظمة المعلوماتية وتدميرها وشن حرباً نفسية ضد الخصوم، وتستمد هذه الحروب شدتها من قوة اطرافها، وارتباطها ايضا بإعمال عسكرية وتقليدية، وتشير بعض التقديرات الى قلت تكلفة الحرب السيبرانية مقارنة بالحروب التقليدية، وقد تمول حملة سيبرانية كاملة بتكلفة دبابة[٣].

يعود استخدام هذا النمط من الحروب في هجمات حلف شمال الاطلسي في عام ١٩٩٩ على يوغسلافيا، إذ عملت هذه الهجمات السيبرانية على تعطيل شبكات الاتصالات للخصوم، كما حدثت ايضا خلال الحرب لبنان "واسرائيل" عام ٢٠٠٦، وكذلك الامر بين وجورجيا روسيا عام ٢٠٠٨، والهجمات بين حركة حماس الفلسطينية " واسرائيل" في عامي ٢٠٠٨ و ٢٠١٢[٤].

(١) شريفة كلاع، مصدر سبق ذكره، ص١٣٦.
(٢) عادل عبد الصادق، "الحرب السيبرانية وتداعياتها على الامن العالمي"، *مجلة السياسة الدولية*، مركز *الاهرام للدراسات السياسية والاستراتيجية، القاهرة*، العدد(٢٠٨)، المجلد(٥٢)، (٢٠١٧): ص٣٤.
(٣) فراس جمال شاكر، مصدر سبق ذكره، ص٢٥٤.
(٤) شريفة كلاع، مصدر سبق ذكره، ص١٣٨-١٣٩.

ثالثاً: الحرب السيبرانية الصلبة مرتفعة الشدة:

وهي حرب سيبرانية لا تصاحبها أي اعمال عسكرية تقليدية، هذا النوع من الحروب ولم يشهد العالم، وان كان احتمال وقوعه وارد في المستقبل مع تطور التكنولوجي للمعلومات، وهذا الشكل من الحروب يسيطر عليه البعد التكنولوجي، فتستخدم الاسلحة السيبرانية فقط ضد منشآت الخصوم، مع اللجوء الى الروبوتات الالية في الحروب والطائرات بدون طيار، وادارتها عن بعد، مع توفر القدرات التقنية في الدفاع والهجوم الالكتروني والاستمرار على القوة الالكترونية(١).

وفي هذا السياق، يتم استخدام الفضاء الالكتروني للاستعداد لحرب المستقبل، عبر قيام الدول بتدريبات على توجيه ضربة اولى لحواسب العدو، واختراق العمليات العسكرية عالية التقنية، او حتى باستهداف الحياة المدنية، والبنية التحتية المعلوماتية، والهدف من وراء ذلك، تحقيق الهيمنة الالكترونية الواسعة، بشكل اسرع في حال حدوث صراع(٢).

II. المبحث الثاني

الحروب السيبرانية وتحديات الامن القومي

ادى الانفتاح في مجال المعلومات والانترنت في الفضاء السيبراني عموماً، جعلها عرضة للتعديات والانشطة غير السليمة، فمستخدمو الفضاء السيبراني من الدول وغير الدول عرضة للتهديدات لمنظومتها الالكترونية، ما يؤدي تنامي هذه التهديدات على الامن القومي للدول، ولهذا تسعى الدول الى ايجاد طرق سلمية من خلالها تحد من الحروب السيبرانية التي باتت تهدد الامن القومي لها. ومن خلال هذا المبحث سوف نبين ما تداعيات هذه الحرب على الامن القومي ومن ثم ماهي الجهود الدولية لمعالجتها.

II.أ. المطلب الاول

انعكاسات الحروب السيبرانية على الامن القومي

لقد شكل الفضاء السيبراني ميدان المعركة الخامس بين القوى الدولية، وذلك بعد الارض، البحر، الجو والفضاء، فاستهداف الهجوم للبنية التحتية المعلوماتية، يمكن أن يشكل ضربة قاضية لاقتصاد بلد من البلدان، او يمكنه إلحاق الضرر الفادح في كل القطاعات التي

(١) احمد عمرو، *ما بعد الانسانية العوالم الافتراضية واثرها على الانسان*، (مصر: افاق المعرفة، ٢٠٢٢)، ص٢٣٨.
(٢) فراس جمال شاكر، مصدر سبق ذكره، ص٢٥٥.

يمكن التسلل لها إلكترونيا سواء كانت عسكرية او مدنية، فالتالي فان الدول فلا تستطيع ان تعبر عن سيادتها في الفضاء السيبراني، لأن اعتماد الناس على هذا البعد التكنولوجي يجعله عرضة بشكل خاص للأعمال العدائية، فلا يزال المهاجمون السيبرانيون يتمتعون بميزات تفوق امكانيات المدافعين بسبب التأثير المفاجئ الذي يمتلكون القدرة على إخفاء آثارهم، ولا تسمح الحالة المعرفية بوضع توصيف دقيق للعمليات الهجومية التي تحدث في الفضاء السيبراني، الامر الذي يجعلها في مواجهة جميع الاحتمالات[١]. ولهذا خلفت هذه الحروب جملة من المخاطر والتداعيات على الامن القومي والتي يمكن ان نجزها فيما يلي[٢]:

اولاً- تصاعد المخاطر السيبرانية: إذ زادت وتيرة المخاطر السيبرانية لاسيما مع تزايد المنشأت الحيوية (المدنية والعسكرية) في الدول التي تتعرض لهجوم الالكتروني عليها عبر استخدام ناقل للخدمات، او تعطيل حركة الانظمة المعلومات الامر الذي يسبب تأثير على القيام بوظائف المنشآت، ولاسيما فإن التحكم في تنفيذ هذا الهجوم يعد اداة سيطرة استراتيجية بالغة الاهمية سواء كان في زمن السلم او الحرب.

ثانياً- تعزيز القوة وانتشارها: لقد عزز الفضاء الالكتروني ما يسمى "القوة المؤسسية" في العلاقات الدولية، والتي يمكن ان يكون لها دور بارز في قوة فاعليها وتحقيق اهدافها وقيمها في ظل التنافس مع الاخرين، ومن ثم فإن سهولة الحصول على تلك القوة السيبرانية قد أدت الى ما يسمى "انتشار القوة" من خلال انتقال القوة من تركيزها في أيدي الدول الكبرى لتتوزع بين أكبر عدد من الفاعلين من الدول المتوسطة والصغيرة وكذا الفاعلين من غير الدول، وهو ما يعني ضعف سيطرة الدولة وارتفاع حجم التهديدات التي تواجه النظام الدولي، عبر ازدياد قدرات الفاعلين في العلاقات الدولية على ممارسة كل من القوة الخشنة والقوة المرنة من خلال استغلال الفضاء الالكتروني.

ثالثاً- عسكرة الفضاء السيبراني: وذلك سعياً لدرء التهديدات الامنية الواقعة عبر الفضاء السيبراني، وقد برز في هذا الاطار مؤشرات وسياسات تدعو لذلك كمثل تطورت في مجال السياسات الدفاعية والامن السيبراني، والقدرات المتصاعدة في سباق التسليح السيبراني، وتبنى السياسات الدفاعية السيبرانية لدى الاجهزة المكلفة بالدفاع والامن في الدول، والعمل على تزايد الاستثمار من اجل السعي على تطوير مقومات الحرب السيبرانية داخل الجيوش الحديثة، وزيادة الاتفاق على الامن السيبراني في العديد من الدول ومنها الولايات المتحدة الامريكية، التي خصصت وزارة دفاعها خلال الفترة ٢٠١٠-٢٠١٥ حوالي من ٢٢% الى

(١) شريفة كلاع، "الامن السيبراني وتحديات الجوسسة والاختراقات الالكترونية للدول عبر الفضاء السيبراني"، *مجلة الحقوق والعلوم الانسانية، جامعة الجزائر، الجزائر*، العدد(١)، المجلد(١٥)، (٢٠٢٢): ص٢٩٩.

(٢) شريفة كلاع، *الامن السيبراني واشكال التهديد: تحديات عالمية*، مصدر سبق ذكره، ص١٤١.

٣٠%، كما تخصصت ايضا خلال سنة ٢٠١٧ ميزانية تبلغ حوالي ١٩ مليار دولار امريكي للأمن السيبراني.

رابعاً- إدماج الفضاء السيبراني ضمن الامن الوطني للدول: وذلك من خلال العمل تجديد الجيوش وتدشين وحدات متخصصة في الحروب السيبرانية، وإقامة هيئات وطنية للأمن والدفاع السيبراني، والقيام بالتدريبات واجراء المناورات من خلال تعزيز القدرة الدفاعية السيبرانية، والعمل على تعزيز التعاون الدولي في مجالات تأمين الفضاء السيبرانية، والقيام بمشروعات وطنية للأمن السيبراني(١).

خامساً- تحديث القدرات الدفاعية والهجوم: إذ عملت الدول الى السعي على تحديث النشاط الدفاع والعمل على مواجهة التهديدات الحرب السيبرانية والقيام بالاستثمار في مجال البنية التحتية المعلوماتية، ورفع القدرات العسكرية والجاهزية وكفاءتها لمثل هذه الحرب عن طريق تكثيف التدريبات والمشاركات الدولية في حماية امن المعلومات، والاستثمار في رفع القدرات البشرية داخل الاجهزة الوطنية المعنية، وهنا يتعلق التوجه الاخطر ينقل تلك القدرات من الدفاع الهجوم عن طريق استخدام الهجمات السيبرانية في اطار الصراع والتوتر مع الدول اخرى.

سادساً- توتر واحتقان العلاقات الدبلوماسية بين الدول: فغالباً ما تسفر الهجمات السيبرانية عن احداث نوع من التوتر والاحتقان في العلاقات الدبلوماسية بين الدول، على اغرار حالة التوتر التي حدثت بين روسيا والولايات المتحدة الامريكية خلال الانتخابات الرئاسة الامريكية سنة ٢٠١٦.

ان تحدي الحرب السيبرانية يعد اعلى تحديات الامن القومي في القرن الواحد والعشرين، لان العالم اليوم يواكب كل التغيرات في مفهوم أمن إذ لا يقتصر فقط على الجوانب العسكرية بل يتسع على كل التهديدات التي يمكن ان تشكل عائق امام الاقتصاد الرقمي وتدفق المعرفة، إذ ان التطور تكنولوجي في المعلومات والاتصالات قد نفت الحدود الجغرافية والسياسية والاقتصادية والاجتماعية بين الدول وهو ما يضع مفهوم السيادة الوطنية والامن القومي على المحك لاسيما مع الاختراق المتكرر والمتزايد للمواقع الرسمية للدولة والتجسس المعلوماتي على الدول(٢).

(١) اسماعيل زروقة، "الفضاء السيبراني والتحول في مفاهيم القوة الصراع"، *مجلة العلوم القانونية والسياسية، الجامعة محمد بوضياف المسيلة، الجزائر*، العدد(١)، المجلد(١٠)، (٢٠١٩): ص١٠٢٨.
(٢) عبدالله جعفري، "التهديدات السيبرانية وتأثيرها على الامن القومي الجزائري"، *مجلة الافريقية للدراسات القانونية والسياسية، جامعة احمد دراية، الجزائر*، العدد(٢)، المجلد(٦)، (٢٠٢٢): ص٢٥٠.

II.ب. المطلب الثاني

الجهود الدولية لمواجهة الحروب السيبرانية

اصبحت الحرب السيبرانية واحده من التكتيكات الحديثة للحروب والهجمات بين الدول، وتعتبر الحماية الامنية لتناقل البيانات على شبكات الاتصالات تحولاً جذرياً في عملية مساعدة الدول لإيجاد الاستراتيجية واضحة بهدف تعزيز الامن السيبراني وحماية مصالحها الحيوية وأمنها الوطني والبنى التحتية الحساسة فيها، ومنع القرصنة وتعد هذه الحماية سداً منيعاً ضد التحديات والقرصنة الالكترونية التي يواجها دول العالم(١).

وتسعى الدول على تكريس امنها السيبراني تبادل للخبرات من الجانب الاجرائي والموضوعي ومن خلال عقد اتفاقيات حماية أي ان تكون القوانين موحدة او على الاقل متقاربة، وان تكون الاجراءات القضائية والامنية متعاونة في ما بينها من اجل الاستفادة من التقنيات الحديثة والتي تمتلكها الدول المتطورة تكنولوجياً وتحتاجها باقي الدول، ويعد التعاون الدولي ضرورة حتمية في العالم اليوم لا منأى لأي دولة عنه حفاظاً على سلمها وامنها من خلال الحفاظ على السلم والامن الدولي(٢)، ومن هذه الاتفاقيات اتفاقية بودانست وتعد اول اتفاقية دولية تضمن مواجهة الحروب السيبراني، ووقعت هذه الاتفاقية في عام ٢٠٠١ بين ٢٦ دولة بهدف التعاون بين الدول من اجل محاربة الجرائم السيبرانية(٣). كما اتفقت الدول في القمة العالمية لمجمع ٢٠٠٥ لضرورة وضع آليات فعالة على مستوى الدولي والوطني للنهوض بالتعاون الدولي في مجال الامن السيبراني(٤).

كما قام مجموعة من الخبراء في القانون الدولي الانساني في ابرام قانون عام ٢٠١٣ يدعى دليل تالين، هذا الدليل يظم نقاط حساسة ذات الصلة بالحروب والهجمات السيبرانية التي تنفذها الدول او تلك التي تقوم بها جهات فاعلة دون الدول كمفهوم النزاع المسلح في اطار الحرب السيبرانية، كذلك مفهوم الجيوش السيبرانية، وكيفية ادارة الحرب السيبرانية من خلال قواعد الاشتباك السيبراني، وصفه المقاتل السيبراني إضافة بالمكانية مراعاة القانون الدول

(١) علاء عبد الرزاق محمد السالمي، مصدر سبق ذكره، ص٢١٨.
(٢) شويرب جيلالي، دمراد فائزه، "مفهوم الحرب السيبراني ولامن السيبراني"، *مجلة الحقوق والحريات*، *الجزائر*، العدد (١)، المجلد (١١)، (٢٠٢٣): ص١٦٨.
(٣) وفاء لطفي، " الجهود الدولية في مجال مكافحة جريمة الارهاب السيبراني التجربة الماليزية نموذجاً"، *المجلة* ، *مصر*، العدد (١)، المجلد(٢٣)، (٢٠٢٢)، ص١٦٣.
(٤) شويرب جيلالي، دمراد فائزه، المصدر السابق، ص١٦٧.

المعروفة كمبدأ التمييز، ومدى شرعية استهداف المقاتل السيبراني بالوسائل العسكرية المادية كالطائرات العسكرية بدون طيار[١].

ومما لا شك فيه تسعى الدول للتفاوض في ما بينها وهذا في اطار الدبلوماسية السيبرانية، عن طريق التبادل المعلومات حول الجرائم المعلومات وتحديتها المختلفة من اجل بناء الثقة، فقد اتفقت كل من امريكا وروسيا بعد المفاوضات على تحديد طرق التعاون في الازمات السيبرانية وذلك عبر خط ساخن ومركز الرد على الطوارئ التي تحدث بسبب الانترنت، وكذلك الاتصال بين المراكز النووية لمواجهة مخاطر الجريمة المعلوماتية[٢].

ومن الضروري بمكان ان تعمل الدول على التنسيق من اجل مواجهة الحروب السيبرانية وذلك من خلال عدة اساليب وهي[٣]:

١- وضع إطار قانوني وتنظيمي مشترك مع اقامة نظام لتحديث هذه القوانين لمعالجة الطبيعة المتغيرة للتهديدات.
٢- إصدار معايير دولية وقواعد سيبرانية كوسيلة لتحسين الامن السيبراني على الصعيد الدولي بإصدار اهداف توجيهية لتحقيق هذا النوع من الامن.
٣- ضرورة النظر في الخصائص المميزة للفضاء السيبراني وابراز التحديات التي تطرحها هذه السمات، وذلك بالعمل على تطوير نموذج للتشريعات المتعلقة بالجرائم السيبرانية يكون قابلاً للتطبيق على الصعيد العالمي.
٤- إجراءات التشغيل المعيارية لحوادث الانترنت والتهديدات تشمل الانشطة التي وضعها الخبراء والمختصون السيبرانيون خلال فترت الاستقرار النسبي، بالرجوع الى معرفة طبيعة الهجمات التي تستهدف تعطيل الانشطة التجارية للدول.

III. المبحث الثالث

الحرب السيبرانية وتأثيرها على الامن القومي العراقي

يعد الامن القومي العراقي الركيزة الاساسية في قوة الدولة ولا يمكن ان نتصور بأي شكل من الاشكال تقدم الدولة دون تحقيق استقرار في أمنها القومي، لذلك يعاني الامن القومي العراقي من تحديات كبيرة بعد عام ٢٠٠٣ وعلى جميع المستويات، بالإضافة الى التهديدات

(١) لامية طالة، مصدر سبق ذكره، ص٦٧.
(٢) دليلة العوفي، مصدر سبق ذكره، ص٧٩٨.
(٣) سمير بلي، "التهديدات الامنية السيبرانية: دراسة في انعكاسات الحرب الالكترونية على الامن القومي للدول واستراتيجيات المقاومة"، *مجلة الرسالة للدراسات والبحوث الانسانية*، *جامعة الجزائر، الجزائر*، العدد (٢)، المجلد(٨)، (٢٠٢٣): ص١٩٨.

السيبرانية التي شكلت تهديداً جديداً على المنظومة الاستراتيجية للأمن القومي العراقي، وان اخطر ما في التهديدات السيبرانية بأنها تهديدات غير مرئية.

وعليه ان هذه الدراسة سنحاول توضيح في المطلب الاول انعكاسات الحرب السيبرانية على الامن القومي العراقي وفي المطلب الثاني نوضح فيها ماهي الاستراتيجية العراقية في مواجهة هذه الحرب.

III.أ. المطلب الاول

انعكاسات الحرب السيبرانية على الامن القومي العراقي

التطور التكنولوجي الذي شهده العراق في مجال المعلومات والاتصالات بعد عام ٢٠٠٣ والذي تزامن مع ضعف الأمنة الإلكترونية لدى البنية التحتية الوطنية (أمنية أو مصرفية أو شخصية) مما جعل العراق منكشفاً سيبرانياً لكثير من دول العالم، لاختراقه والتجسس على المعلومات الخاصة بالمؤسسات الأمنية، واستخدام العراق كساحة لشن الهجمات الإلكترونية لضرب أمن معلومات اي دولة كانت واختراقه، فضلاً عن اختراق اي معلومة واستخدامها لأغراض المساومة أي: لتنفيذ عمليات ارهابية وغيرها، وهذا نتيجة عدم اهتمام المؤسسات الحكومية العراقية لمسألة الامن السيبراني، إذ يشير التقرير الصادر عن الاتحاد الدولي للاتصالات (GCI) التابع للأمم المتحدة لعام ٢٠١٨، ان العراق يحتل مكانة متأخرة في تحقيق الامن السيبراني، إذ جاء بتسلسل ١٠٧ من اصل ١٧٥ دولة، وال١٣ عربياً[١].

لذلك استغل تنظيم داعش الارهابي في حربه بالعراق في السنوات الماضية الحرب السيبرانية خلال الهجمات الارهابية في العراق من حيث استخدام مواقع التواصل الاجتماعي (فيس بوك) لتجنيد الشباب، وايضاً استغل الارهاب في بث عمليات الاعدام التي كان يقوم بتنفيذها في الاسرى، من اجل بث الرعب في الاهالي خوفاً من تعرضهم لمصير من قبلهم، وهذا ما تحقق جزئياً هو هروب واستلام مدن وقرى لتنظيم داعش الارهابي، وبالتالي استطاعت تلك الجماعات الارهابية من التواصل مع بعضها البعض بعد ان كانت تستغرق شهوراً في الماضي، وفي ذات السياق عام ٢٠١٤ رصدت شركات امنية مختصة بالأمن السيبراني ان هناك حرباً سيبرانية في العراق يتم فيها استخدام وسائل التواصل الاجتماعي

(١) - نور علي صكب، "الامن الوطني العراقي في ظل الاختراق السيبراني (أمن المعلومات)"، *مجلة كلية القانون والعلوم السياسية*، العدد ١١، (٢٠٢١): ص١٣.

لحشد المؤيدين ونشر الدعاية ولجمع المعلومات الامنية عن طريق مجموعة من قراصنة الانترنت[١].

وعند البحث عن اسباب تراجع العراق في مجال الامن السيبراني سوف نجد ان الجهود الحكومية التي اتخذها العراق في مجال الامن السيبراني لم تستمر وشهدت تراجع كبير انعكس بشكل سلبي على أمنها القومي والتي شملت الاتي:

١- تراجع دور فريق الاستجابة للأحداث السيبرانية، وهو فريق وطني مشترك مختص بمجال الامن يعمل تحت اشراف مستشارية الامن القومي العراقي، وايضاً لا تزال الاموال المخصصة للامن السيبراني قليلة بالمقارنة مع دول الجوار ومنها ايران والتي خصصت مليار دولار سنويا لهذا القطاع[٢].
٢- ضعف الجهد الاستخباراتي وتراجع القدرات العملياتية المتنوعة[٣].
٣- لا توجد بنية تحتية مادية وبشرية متكاملة في مجال الامن السيبراني، وكذلك لا نجد للعراق دور في المنتديات الدولية المعنية بالامن السيبراني، وقلة المؤتمرات والندوات والورش التي تخص الامن السيبراني بالمقارنة مع دول الجوار مثل السعودية وغيرها من الدول المحيطة بالعراق التي تسعى دائماً في المحافظة على امنها القومي[٤].
٤- ان احد الازمات التي يعاني منها الامن الوطني العراقي في ظل الاختراق السيبراني هو العجز الحكومي عن اتخاذ التدابير والاجراءات اللازمة، فضلا من المؤسسات العراقية ليس لديها القدرة على مواجهة الجريمة الالكترونية او السيبرانية، إذ انتشرت مؤخرا نوعية خطيرة من الهجمات والجرائم السيبرانية التي تعتمد على تقنيات متقدمة (كالجاسوسة الحسابية والذكاء الاصطناعي واختراق المواقع الرسمية والاحتيال المصرفي والصيد الاحتيالي للمعلومات)، وكان من ابرز هذه البرامج التي تهدد الامن السيبراني العراقي (الفدية الخبيثة) والتي حذرت منها هيئة الاعلام والاتصالات العراقية، هو يعمل على حجب جميع المعلومات في اجهزة الحواسيب الحكومية والشخصية واستخدامها كأوراق ضغط وابتزاز مقابل مبالغ مالية كبيرة[٥].

---

(١) - صلاح مهدي هاوي الشمري، زيد محمد علي اسماعيل، "الامن السيبراني كمرتكز جديد في الاستراتيجية العراقية"، *مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين*، العدد ٦٢، (٢٠٢٠): ص٢٨٣.
(٢) - باسم علي خريسان، *الامن السيبراني في العراق قراءة في مؤشر الامن السيبراني العالمي ٢٠٢٠*، (سلسلة اصدارات مركز البيان للدراسات والتخطيط : ٢٠٢١)، ص١٠.
(٣) - سليم كاطع علي، "تحديات واليات تعزيز الامن الوطني العراق بعد عام ٢٠١٤"، *مجلة حمورابي، مركز الدراسات الاستراتيجية والدولية، جامعة بغداد*، العدد ٣٩، (٢٠٢١): ص١١٢.
(٤)المصدر نفسه، ص١٠.
(٥) - نور علي صكب، مصدر سبق ذكره، ص١٤-ص١٥.

٥- ضعف التخطيط الاستراتيجي والذي يعد من المهام الرئيسة للقيادة الاستراتيجية، وعنصرا مهما لثبات منظومة الامن الوطني، وبالتالي يعاني العراق اليوم من حالة ضعف في منظومة التخطيط الاستراتيجي، وهو ما انعكس سلبا على عمل معظم مؤسسات الدولة العراقية ونتاجها التي باتت تعاني من ضعف في التخطيط الاستراتيجي التي يمثل احد السمات الرئيسة للعصر الحديث، لذا ومن خلال تحليل وفحص عمل معظم المؤسسات الاستراتيجية للدولة نجد ان هناك ترهلاً وضعفاً واضحاً في عملية الخطط الاستراتيجية بسبب ضعف القيادة الادارية(١).

وفي سياق التحديات السيبرانية تعرض العراق في ٢٦ و٢٧ /ايلول/٢٠١٩ الى هجوم سيبراني من قبل قراصنة طالت قرابة (٣٠) موقعاً حكومياً، ابرزها مواقع وزارة الدفاع والداخلية والخارجية والامن الوطني والصحة، وقد استغل المهاجمون بعض الثغرات فعملوا على تطبيق التغيرات في بيانات موقع البحث التي من شأنها توجيه المستخدمين الى صفحة بحث مختلفة، وعلى الرغم ان الجهات الحكومية نجحت في استعادة سريعة لبعض المواقع الا ان بعضها استغرق وقتاً اطول، علما ان المهاجمون تمكنوا من الدخول الى أجهزت الحواسيب الحكومية واختراق قاعدة البيانات التي من المفروض ان تكون محمية بشكل جيد مما سمح لهم بأخذ معلومات كثيرة، وقد حذرت لجنة الامن البرلمانية من خطورة مثل هذا الاختراق مستقبلاً كونه سيؤدي الى تسريب معلومات أمنية مهمة وحساسة(٢). وبالتالي لا يمتلك العراق القدرات المطلوبة للتكيف مع تلك التحديات التي يفرضها الفضاء السيبراني، ومع الانتقال السريع للمجتمعات من الفضاء الحقيقي الى الفضاء الافتراضي وجد العراق نفسه يدخل الى فضاء واسع وسريع الحركة، دون ان يمر بمرحلة انتقالية فالبنى المادية والبشرية لا تزال غير قادرة على التفاعل الايجابي مع تلك التحديات العديدة للأمن السيبراني، وعند البحث في الامكانات العراقية في مجال الامن السيبراني نجد انه يحتاج الى الكثير من الجهد المعرفي والاداري والقانوني والتقني لكي يكون قادر على التأثير في مجالات الامن السيبراني من جهة ومن جهة اخرى ان يكون قادر على حماية امنه من التهديدات السيبرانية(٣).

---

(١) - علي زايد العلي، "التحديات غير المرئية للأمن الوطني العراقي"، مركز البيان للدراسات والتخطيط، ٢٠١٨/٦/٢٦، ينظر الى الرابط: https://www.bayancenter.org/2018/06/4565

(٢) - مصطفى ابراهيم سلمان الشمري، "الامن السيبراني وأثره في الامن الوطني العراقي"، *مجلة جامعة ديالى، جامعة ديالى، كلية القانون والعلوم السياسية*، المجلد العاشر، العدد الاول، (٢٠٢١): ص١٧٤-ص١٧٥.

(٣) - ماجد صدام سالم، "الامن السيبراني العراقي واثره في قوة الدولة"، *مجلة العلوم التربوية والانسانية، كلية التربية الاساسية، جامعة ميسان*، العدد ١٨، (٢٠٢٢): ص٧٧.

III. ب. المطلب الثاني

الاستراتيجية العراقية لمواجهة الحروب السيبرانية

يعد الامن الوطني لأي دولة قضية مهمه ومن الاولويات الاستراتيجية وكل الدول لديها اهتمام كبير بوضع استراتيجيات للأمن تتضح فيها المصالح الحيوية التي في ضوئها يتم وضع الاهداف الاستراتيجية والعراق يمر بمرحلة مضطربة سياسيا وامنيا واقتصاديا تتطلب معها وضع استراتيجيات جديدة غير تقليدية للأمن والتحديات باتت كثيره ومتعددة التي تواجه الامن الوطني العراقي، فالعراق مؤسساته وبناه التحتية لم تدار بشكل الكتروني بعد، 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 الالكترونية والبنى التحتية الالكترونية التي تدار من خلال شبكات الحاسب(١).

وفي العراق تعمل استراتيجية الامن السيبراني على تكوين استراتيجية منسقة وتستجيب بشكل ديناميكي نحو التهديدات التي تواجه الأمن القومي، وتهدف الاستراتيجية الوطنية للأمن السيبراني في العراق الى ادارة التهديدات الامنية في الفضاء الالكتروني بما يتماشى مع اهداف الأمن القومي العام والمصلحة العامة، إذ ان الرؤية الوطنية للأمن السيبراني تهدف الى تعزيز القدرات الوطنية في مجال الامن السيبراني في العراق على نحو متناسق ومستدام ومتكامل من أجل التصدي والتخفيف من المخاطر السيبراني، وحماية البنى التحتية المعلوماتية الوطنية في مختلف الميادين للارتقاء بمستوى العراق السيبراني نحو بيئة سيبرانية امنة، كما انها تسلط الضوء على الطرق التي سيتم به تقييم وتطوير وتنفيذ الانذار المبكر والكشف وادارة الازمات لتوفير الاستعداد الاستباقي للرد على التهديدات الموجهة الى البنى التحتية المعلوماتية الحرجة في العراق والتعامل معها(٢).

ولكي يحتل العراق مكانة جيدة في مقياس الامن السيبراني العالمي ويكون دولة فاعلة ومؤثره في الفضاء السيبراني لابد له من تطوير الاستراتيجيات القائمة حاليا والاهتمام بتوفير ركائز اساسية مهمه العراق يفتقر اليها في الوقت الحاضر، لذا على صناع السياسات الامنية في العراق العمل على اقامة تلك المرتكزات والتي اهمها:-

(١) - مهند جبار عباس، هيثم كريم صيوان، "الحرب السيبرانية بين التحديات واستراتيجية المواجهة : العراق إنموذجا"، *قضايا سياسية*، *كلية العلوم السياسية*، *جامعة النهرين*، العدد ٧٠، (٢٠٢٢): ص١٦١.
(٢) - زهير خضير عباس الزبيدي، ظفر عبد مطر التميمي، "العراق والامن السيبراني: الفرص والتحديات"، *مجلة واسط للعلوم الانسانية والاجتماعية*، مجلد ١٨، العدد ٥١، (٢٠٢٢): ص١٣.

١- الاهتمام بوضع آليات وسن تشريعات لمجابهة التدهور الاخلاقي والقيمي المستفحل في الفضاء السيبراني (كالتنمر الالكتروني والتطرف الفكري والديني)، وضرورة اصدار قانون بشأن حماية الخصوصية يتيح آليات المراقبة من خلال استحداث تقنية لإنذار المسؤولين بسوء الاستخدام فيما يعطيها الحق في التدخل والرقابة[١].

٢- ان تحقيق الامن الوطني العراقي يتطلب قبل كل شيء بناء مقومات قوة العراق الداخلية، وبناء قوته العسكرية، وبما يحقق استقراره السياسي والاقتصادي والامني، وهو ما يتطلب توفير المستلزمات الاساسية التي يحتاجها العراق في هذا الجانب، لعل في مقدمتها توفير الجهد الاستخباراتي، كونه الوسيلة الرئيسة التي تعتمد عليها القيادة السياسية في صناعة واعداد القرارات المتعلقة بالأمن الوطني، الى جانب العمل على تطوير المنظومة الامنية بصورة عامة والعسكرية بصورة خاصة ودعم قدراتها التسليحية والتدريبية للعمل على تجاوز العقبات التي تحول دون تطور في صفوف الجيش العراقي وباقي المؤسسات الامنية[٢].

٣- النهوض بثقافة وطنية للأمن السيبراني عبر زيادة وعي أفراد المجتمع بأهمية الامن السيبراني والمخاطر المتعلقة بالإنترنت، وتشجيع اتباع الممارسات الآمنة في التعامل مع التقنية، وتشجيع المؤسسات على نشر الوعي السيبراني بفاعلية، والعمل على مبدأ الثواب والعقاب، وتخصيص مكافأة التميز في مجال الامن السيبراني عبر برامج الجوائز الوطنية، وتشجيع المؤسسات على اطلاق برامج حول الامن السيبراني، وايضاً وضع اليات وطنية فعالة للاستجابة للحوادث السيبرانية لتمكين الاستجابة السريعة والمنسقة في الدولة عبر تنظيم الية الكشف عن حوادث الامن السيبراني وفق معايير منهجية موحدة لتقييم درجة خطورة الحوادث[٣].

٤- بناء مؤسسات امنية سيبرانية مثل (الشرطة السيبرانية، والمخابرات السيبرانية والاستخبارات السيبرانية، والجيش السيبراني، الخ) من اجل مواجهات التهديدات السيبرانية الداخلية والخارجية، وايضاً العمل على تأسيس كليات واقسام علمية في الجامعات العراقية المدنية والعسكرية المختصة بالامن السيبراني تمنح درجات علمية في تخصص الامن السيبراني[٤].

٥- بناء بنية تحتية حيوية آمنة تمنع المهاجمين من استهداف هذه الانظمة الحيوية، وان افضل طريقة معروفة لحماية البنية التحتية حاليا هي ضمان وجود اجراءات الاستبدال والمرونة

---

(١) - إسلام فوزى، "الامن السيبراني الابعاد الاجتماعية والقانونية تحليل سوسيولوجي"، *المجلة الاجتماعية القومية، جامعة دمنهور، كلية الاداب*، المجلد السادس والخمسون، العدد الثاني، (٢٠١٩): ص١٣٣.

(٢) - سليم كاطع علي، مصدر سبق ذكره، ص١١٦-ص١١٧.

(٣) - نور علي صكب، مصدر سبق ذكره، ص١٧.

(٤) - باسم علي خريسان، مصدر سبق ذكره، ص١١.

واختبارها ومراجعتها باستمرار، ومراقبة الشبكة لتسجيل الاشخاص الذين يسجلون الدخول الى النظام والموقع، وكذلك استخدام تطبيقات منع التسلل للمواقع المهمة[١].

٦- تنسيق مبادرة الامن السيبراني على جميع مستويات الحكومة في البلاد، مع وضع الية موثوقة لإشراك اصحاب المصالح المتعددين والوطنيين والدوليين من اجل التصدي بشكل جماعي للتهديدات السيبرانية، والعمل على تحسين قدرة وتطوير فريق الاستجابة لحالات الطوارئ في الحاسوب العراقي، وايضاً العمل على بناء استراتيجية وطنية تعمل على التنسيق العالي في المجال العالمي للعمل والتعاون في حماية الهياكل الوطنية الحيوية من الهجمات السيبرانية[٢].

يتضح مما سبق ان الانفتاح الذي شهده العراق ولا سيما في مجال التقنية والمعلومات، وتزايد الاعتماد الية فرض عليه تحديات عدة، ونظراً لكون العراق مستهدف بالدرجة الاساس من قبل التنظيمات الارهابية، فقد شهدت المؤسسات الرسمية وغير الرسمية خروقات وهجمات سيبرانية عدة، ومن هنا ظهرت تحديات أمنية معاصرة فرضت نفسها على العراق منها الارهاب السيبراني والقرنصة السيبرانية والجريمة الالكترونية وغيرها، وهذا يتطلب بناء كوادر وطنية والاستفادة من المنظمات الدولية المختصة من اجل مواجهة هذه المخاطر[٣].

الخاتمة

شكلت الحرب السيبرانية واحدة من التحديات التي تفرضها على الامن القومي، وتعد نتيجة السلبية التي خلفها التقدم التكنولوجي الهائل الذي شهده العالم، حيث ان الفضاء السيبراني ساحة هامة للتفاعلات الدولية المختلفة، في ظل تزايد الحرب السيبرانية بين الدول، بما يؤثر على امنها القومي، مما سعت الدول الى بذل الجهود من اجل تطوير قدراتها واتخاذ الاجراءات الوقائية من اجل حمايتها من اخطار هذه الحرب.

وفيما يتعلق بالعراق فأنه شهد انفتاح لا سيما في مجال المعلومات والتطور التكنولوجي والتقني، وتزايد الاعتماد عليه فرض تحديات كبيرة، ونظرا لكون العراق مستهدف بالدرجة الأساس من قبل الجماعات الإرهابية وهذا ما شهدة العراق خلال السنوات السابقة، وبالتالي شهدت مؤسسات الدولة العراقية الرسمية وغير الرسمية هجمات وخروقات سيبرانية مختلفة، ومن هنا شهد العراق تحديات على جميع الأصعدة واهمها على الصعيد الأمني الذي فرض

(١) - حسين باسم عبد الامير، "تحديات الامن السيبراني، مركز الدراسات الاستراتيجية"، جامعة كربلاء، ٢٠١٨، ينظر الى الرابط التالي https://kerbalacss.uokerbala.edu

(٢) مستشارية الامن الوطني، "امانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات، استراتيجية الامن السيبراني العراقي"، ص٦-ص٧.

(٣) - مصطفى ابراهيم سلمان الشمري، مصدر سبق ذكره، ص١٧٦.

نفسه على العراق ومنها الإرهاب السيبراني والقرصنة والجريمة الالكترونية وهذا يتطلب بناء فريق وطني متكامل لمعالجة هذه الهجمات وايضاً الاستفادة من الجهود الدولية الخاصة في معالجة الظواهر السيبرانية، وبالتالي لا بد من اهتمام حكومي بالمؤشرات الدولية والاجابة الدقيقة بشفافية على الاستبيانات المعنية وفق المعطيات الأمنية الممكنة، وكذلك بناء منظومة قانونية وقضائية تتعلق بالجرائم السيبرانية، اذن ان نجاح أي استراتيجية للامن القومي العراقي لا يمكن ان يتم الا اذا وقفت على حقيقة مصادر التهديد داخلياً وخارجياً، ولا يمكن الاكتفاء او الإشارة اليها فقط، انما العمل على إيجاد معادل موضوعي للحد من خطورة التهديدات والمخاطر والتحديات في بلد يعاني من ضعف القانون، اذن لا بد من إيجاد استراتيجية تبحث عن مواطن القوة لتعزيزها وعن نقاط الضعف من اجل تجاوزها ومعالجتها، فالأمن في مجمله مفهوم وقائي يشمل جميع مرافق الحياة.

المصادر

أولاً: - الكتب:

١- احمد عمرو، *ما بعد الانسانية العوالم الافتراضية واثرها على الانسان*، مصر: افاق المعرفة، ٢٠٢٢.

٢- ايهاب خليفة، *الحرب السيبرانية(الاستعداد لقيادة المعارك العسكرية في الميدان الخامس)*، ابو ظبي: دار العربي، ٢٠٢١.

٣- شريفة كلاع، *الامن السيبراني واشكال التهديد: تحديات عالمية*، الجزائر: ألفا للوثائق، ٢٠٢٣.

٤- علاء عبد الرزاق محمد، *المدخل الى الامن السيبراني(الفضاء السيبراني –تهديدات الفضاء السيبراني- الاسلحة السيبرانية ووسائل مواجهة التهديدات-استراتيجيات الامن السيبراني)*، بغداد: دار الكتب والوثائق، ٢٠٢١.

٥- فارس محمد العمارات وابراهيم الحماصة، *الامن السيبراني: المفهوم وتحديات العصر*، عمان: دار الخليج، ٢٠٢٢.

٦- فراس جمال شاكر، *السيبرانية وتحولات القوة في النظام الدولي*، عمان: دار امجد، ٢٠٢٢.

٧- قيس خلف المحمداوي، *الحروب الجديدة والتحول في مفاهيم القوة بعد الحرب الباردة*، عمان: دار امجد، ٢٠٢٢.

ثانياً: - الدوريات:

١. إسلام فوزى، "الامن السيبراني الابعاد الاجتماعية والقانونية تحليل سوسيولوجي"، *المجلة الاجتماعية القومية*، جامعة دمنهور، كلية الاداب، المجلد السادس والخمسون، العدد الثاني، (٢٠١٩).

٢. اسماعيل زروقة، "الفضاء السيبراني والتحول في مفاهيم القوة الصراع"، *مجلة العلوم القانونية والسياسية، الجامعة محمد بوضياف المسيلة، الجزائر*، العدد(١)، المجلد(١٠)، (٢٠١٩).

٣. باي سمير، "التهديدات الامنية السيبرانية: دراسة في انعكاسات الحرب الالكترونية على الامن القومي للدول واستراتيجيات المقاومة"، *مجلة الرسالة للدراسات والبحوث الانسانية، الجزائر*، العدد (٢)، المجلد(٨)، (٢٠٢٣).

٤. بن تغري موسى، "الحرب السيبرانية والقانون الدولي الانساني"، *مجلة الاجتهاد القضائي، الجزائر*، العدد(٢٢)، المجلد(١٢)، (٢٠٢٠).

٥. زهير خضير عباس الزبيدي، ظفر عبد مطر التميمي، "العراق والامن السيبراني: الفرص والتحديات"، *مجلة واسط للعلوم الانسانية والاجتماعية*، مجلد ١٨، العدد ٥١، (٢٠٢٢).

٦. سمير بلي، "التهديدات الامنية السيبرانية: دراسة في انعكاسات الحرب الالكترونية على الامن القومي للدول واستراتيجيات المقاومة"، *مجلة الرسالة للدراسات والبحوث الانسانية، جامعة الجزائر، الجزائر*، العدد (٢)، المجلد(٨)، (٢٠٢٣).

٧. شريفة كلاع، "الامن السيبراني وتحديات الجوسسة والاختراقات الالكترونية للدول عبر الفضاء السيبراني"، *مجلة الحقوق والعلوم الانسانية، جامعة الجزائر، الجزائر*، العدد(١)، المجلد(١٥)، (٢٠٢٢).

٨. شويرب جيلالي، دمراد فائزه، "مفهوم الحرب السيبراني ولامن السيبراني"، *مجلة الحقوق والحريات، الجزائر*، العدد (١)، المجلد (١١)، (٢٠٢٣).

٩. صلاح مهدي هاوي الشمري، زيد محمد علي اسماعيل، "الامن السيبراني كمرتكز جديد في الاستراتيجية العراقية"، *مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين*، العدد ٦٢، (٢٠٢٠).

١٠. عادل عبد الصادق، "الحرب السيبرانية وتداعياتها على الامن العالمي"، *مجلة السياسة الدولية، مركز الاهرام للدراسات السياسية والاستراتيجية، القاهرة*، العدد(٢٠٨)، المجلد(٥٢)، (٢٠١٧).

١١. عبدالله جعفري، "التهديدات السيبرانية وتأثيرها على الامن القومي الجزائري"، *مجلة الافريقية للدراسات القانونية والسياسية، جامعة احمد دراية، الجزائر*، العدد(٢)، المجلد(٦)، (٢٠٢٠).

١٢. العوفي دليلة، "الحرب السيبرانية في عصر الذكاء الاصطناعي ورهاناتها على الامن الدولي"، *مجلة الحكمة للدراسات الفلسفية، الجزائر*، العدد(٢)، المجلد(٩)، (٢٠٢١).

١٣. غريب حكيم، شرقي صبرينه، "تداعيات الحرب الالكترونية على العلاقات الدولية: دراسة في الهجوم الالكتروني على ايران"، *مجلة دفاتر السياسية وقانونية، الجزائر*، العدد (٢)، المجلد (١٢).

١٤. ماجد صدام سالم، "الامن السيبراني العراقي واثره في قوة الدولة"، *مجلة العلوم التربوية والانسانية، كلية التربية الاساسية، جامعة ميسان*، العدد ١٨، (٢٠٢٢).

١٥. مصطفى ابراهيم سلمان الشمري، "الامن السيبراني وأثره في الامن الوطني العراقي"، *مجلة جامعة ديالى، جامعة ديالى، كلية القانون والعلوم السياسية*، المجلد العاشر، العدد الاول، (٢٠٢١).

١٦. مهند جبار عباس، هيثم كريم صيوان، "الحرب السيبرانية بين التحديات واستراتيجية المواجهة : العراق إنموذجا"، *قضايا سياسية، ، كلية العلوم السياسية، جامعة النهرين*، العدد٧٠، (٢٠٢٢).

١٧. نور علي صكب، "الامن الوطني العراقي في ظل الاختراق السيبراني (أمن المعلومات)"، *مجلة كلية القانون والعلوم السياسية*، العدد ١١، (٢٠٢١).

١٨. وفاء لطفي، " الجهود الدولية في مجال مكافحة جريمة الارهاب السيبراني التجربة الماليزية نموذجاً"، *المجلة* ، مصر، العدد (١)، المجلد(٢٣)، (٢٠٢٢).

ثالثاً- الانترنيت:

١- حسين باسم عبد الامير، تحديات الامن السيبراني، مركز الدراسات الاستراتيجية، جامعة كربلاء، ٢٠١٨، ينظر الى الرابط التالي https://kerbalacss.uokerbala.edu

٢-سليم كاطع علي، "تحديات واليات تعزيز الامن الوطني العراق بعد عام ٢٠١٤"، مجلة حمورابي، العدد ٣٩، مركز الدراسات الاستراتيجية والدولية، جامعة بغداد، ٢٠٢١.

٣-علي زايد العلي، التحديات غير المرئية للأمن الوطني العراقي، مركز البيان للدراسات والتخطيط، ٢٠١٨/٦/٢٦، ينظر الى الرابط: https://www.bayancenter.org/2018/06/4565

٤-باسم علي خريسان، الامن السيبراني في العراق قراءة في مؤشر الامن السيبراني العالمي ٢٠٢٠، سلسلة اصدارات مركز البيان للدراسات والتخطيط ، ٢٠٢١.

رابعاً:-الوثائق:

١-مستشارية الامن الوطني، امانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات، استراتيجية الامن السيبراني العراقي.

خامساً- المصادر الاجنبية:

(1)-Paul Cornish, David livingstone and otler, on cyber war fare the royal institute of international affairs, London, 2010, p.8.

Sources

First - documents:

-National Security Advisory, Secretariat of the Supreme Technical Committee for Communications and Information Security, Iraqi Cybersecurity Strategy.

Second - Books:

-١Ahmed Amr, Transhumanism, Virtual Worlds and Their Impact on Humans, Knowledge Horizons, Egypt, 2022.

-٢Ihab Khalifa, Cyber War (Preparing to Lead Military Battles in the Fifth Field), Dar Al-Arabi, Abu Dhabi, 2021.

-٣Sherifa Klaa, Cybersecurity and Threat Forms: Global Challenges, Alpha Documents, Algeria, 2023.

-٤Alaa Abdul Razzaq Muhammad, Introduction to Cybersecurity (Cyberspace - Cyberspace Threats - Cyberweapons and Means of Countering Threats - Cybersecurity Strategies), Dar Al-Kutub and Documentation, Baghdad, 2021.

-٥Fares Muhammad Al-Amarat and Ibrahim Al-Hamasa, Cybersecurity: The Concept and Challenges of the Age, Dar Al-Khaleej, Amman, 2022.

-٦Firas Jamal Shaker, Cyber and Power Shifts in the International System, Dar Amjad, Amman, 2022.

-٧Qais Khalaf al-Muhammadawi, New Wars and the Transformation in Concepts of Power after the Cold War, Amjad House, Amman, 2022.

Third - Periodicals:

.١Islam Fawzi, "Cybersecurity, Social and Legal Dimensions, Sociological Analysis," National Social Journal, Volume Fifty-Six, Issue Two, Damanhour University, Faculty of Arts, 2019.

.٢Ismail Zarrouka, "Cyberspace and the Transformation in Concepts of Power and Conflict," Journal of Legal and Political Sciences, Issue (1), Volume (10), University Mohamed Boudiaf M'sila, Algeria, 2019.

.٣Bay Samir, "Cybersecurity Threats: A Study of the Implications of Electronic Warfare on States' National Security and Resistance Strategies," Al-Resala Journal for Humanitarian Studies and Research, Issue (2), Volume (8), Algeria, 2023.

.٤Ben Taghri Moussa, "Cyberwarfare and International Humanitarian Law," Journal of Judicial Jurisprudence, Issue (22), Volume (12), Algeria, 2020.

.٥Zuhair Khudair Abbas Al-Zubaidi, Zafar Abdul Matar Al-Tamimi, "Iraq and Cybersecurity: Opportunities and Challenges," Wasit Journal for Humanities and Social Sciences, Volume 18, Issue 51, 2022.

.٦Samir Belli, "Cybersecurity Threats: A Study of the Implications of Electronic Warfare on States' National Security and Resistance Strategies," Al-Resala Journal for Humanitarian Studies and Research, Issue (2), Volume (8), University of Algiers, Algeria, 2023.

.٧Sharifa Klaa, "Cybersecurity and the challenges of espionage and electronic intrusions of countries through cyberspace," Journal of Law and Human Sciences, Issue (1), Volume (15), University of Algiers, Algeria, 2022.

.٨Shawirb Djilali, Damrad Faiza, "The Concept of Cyber War and Cyber Security," Journal of Rights and Liberties, Issue (1), Volume (11), Algeria, 2023.

.٩Salah Mahdi Hawi Al-Shammari, Zaid Muhammad Ali Ismail, "Cybersecurity as a new foundation in the Iraqi strategy," Political Issues Magazine, No. 62, College of Political Science, Al-Nahrain University, 2020.

.١٠Adel Abdel-Sadiq, "Cyberwar and its repercussions on global security," International Politics Journal, Issue (208), Volume (52), Al-Ahram Center for Political and Strategic Studies, Cairo, 2017.

.١١Abdullah Jaafari, "Cyber Threats and their Impact on Algerian National Security," African Journal of Legal and Political Studies, Issue (2), Volume (6), Ahmed Draya University, Algeria, 2020.

.١٢Al-Awfi Dalila, "Cyberwar in the era of artificial intelligence and its stakes on international security," Al-Hikma Journal for Philosophical Studies, Issue (2), Volume (9), Algeria, 2021.

١٣. Gharib Hakim, Sharqi Sabrina, “The Repercussions of Electronic Warfare on International Relations: A Study of the Electronic Attack on Iran,” Journal of Political and Legal Notebooks, Issue (2), Volume (12), Algeria.

١٤. Majid Saddam Salem, “Iraqi cybersecurity and its impact on state power,” Journal of Educational and Human Sciences, No. 18, College of Basic Education, University of Maysan, 2022.

١٥. Mustafa Ibrahim Salman Al-Shammari, “Cybersecurity and its impact on Iraqi national security,” Diyala University Journal, Volume Ten, Issue One, University of Diyala, College of Law and Political Science 2021.

١٦. Introduction to Cybersecurity, course offered by Kosk, p. 29.

١٧. Muhannad Jabbar Abbas, Haitham Karim Siwan, “Cyber War between Challenges and Confrontation Strategy: Iraq as a Model,” Political Issues, No. 70, College of Political Science, Al-Nahrain University, 2022.

١٨. Nour Ali Sakab, “Iraqi National Security in Light of Cyber Hacking (Information Security),” Journal of the College of Law and Political Science, No. 11, 2021.

١٩. Wafaa Lotfy, “International Efforts in the Field of Combating the Crime of Cyber Terrorism: The Malaysian Experience as a Model,” Magazine, Issue (1), Volume (23), Egypt, 2022.

Fourth - Research centers:

-١ Hussein Basem Abdel Amir, Cybersecurity Challenges, Center for Strategic Studies, University of Karbala, 2018, see the following link https://kerbalacss.uokerbala.edu

-٢Salim Kate Ali, “Challenges and Mechanisms for Strengthening Iraq’s National Security after 2014,” Hammurabi Magazine, No. 39, Center for Strategic and International Studies, University of Baghdad, 2021.

-٣Ali Zayed Al-Ali, The Invisible Challenges to Iraqi National Security, Al-Bayan Center for Studies and Planning, 6/26/2018, see the link: https://www.bayancenter.org/2018/06/4565

-٤Bassem Ali Khresan, Cybersecurity in Iraq, a reading of the Global Cybersecurity Index 2020, Al Bayan Center for Studies and Planning publication series, 2021.

Fifth - Foreign sources:

(1)-Paul Cornish, David livingstone and otler, on cyber war fare the royal institute of international affairs, London, 2010, p.8.