مجلة العلوم السياسيّة

اسم المقال: استراتيجية التحكم بالفضاء السيبراني لتعزيز الأبعاد غير الملموسة للأمن القومي العراقي
اسم الكاتب: محمد كاظم عباس المعيني
رابط ثابت: https://political-encyclopedia.org/index.php/library/9524
تاريخ الاسترداد: 2026/11/01 14:34 +03

الموسوعة السياسيّة 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 السياسيّة - Encyclopedia Political، يرجى التواصل على info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسيّة - Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام المتاحة على الموقع https://political-encyclopedia.org/terms-of-use

تم الحصول على هذا المقال من موقع مجلة العلوم السياسيّة جامعة بغداد ورفده في مكتبة الموسوعة السياسيّة مستوفياً شروط حقوق الملكية الفكريّة ومتطلبات رخصة المشاع الإبداعي التي ينضوي المقال تحتها.

Political Sciences Journal
Issue (69) June (2025) **ISSN**: 1815-5561 **E-ISSN**: 2521-912X

Cyberspace Control Strategy to Strengthen the Intangible Aspects of Iraq's National Security

Mohammed Kadhim Abbas Al-Maeeni*

Receipt date: 28/1/2025 Accepted date:17/4/2025 Publication date:1/6/2025

https://doi.org/10.30907/jcopolicy.vi69.806

Copyrights: © 2025 by the author.
The article is an open access article distributed under the terms and condition of the (CC By) license Creative Commons Attribution 4.0 International License

Abstract:

This study explores a strategic approach to controlling cyberspace in order to enhance the intangible dimensions of Iraq's national security. In the evolving global security landscape, cyberspace has emerged as a pivotal domain that reshapes deterrence concepts, warfare tactics, and the balance of power. Unlike conventional warfare, cyber conflicts are characterized by their non-physical nature, requiring advanced technological capabilities and skilled human resources. For Iraq, like many other states, the challenges in cyberspace are both horizontal and vertical, particularly in the security and capacity-building sectors. These challenges reflect the state's struggle to manage and secure its digital infrastructure effectively. The study investigates whether Iraq possesses the necessary capabilities to control its cyberspace and proposes strategies for addressing non-traditional threats within national defense frameworks.

Utilizing a descriptive and analytical methodology, the research analyzes key concepts, strategies, and policies related to cyberspace governance and connects them to Iraq's broader national security framework. The findings reveal that cyberspace is increasingly becoming a contested domain, central to geopolitical competition, symbolic power projection, and state sovereignty. The study concludes that addressing Iraq's cyber vulnerabilities requires high-level governmental coordination, integration of artificial intelligence in defense systems, strategic resource allocation, and inclusive policymaking that involves all stakeholders. Furthermore, a national cyberspace strategy must ensure respect for fundamental human rights while building a trusted, adaptive, and secure digital environment aligned with Iraq's socio-political priorities.

Keywords: Strategy, cyberspace, national security, cyber security, Cyber warfare.

*Asst.Prof.Dr./ University of Baghdad/ Center for Strategic and International Studies.
Mohammed.k@cis.uobaghdad.edu.iq

مجلّة العلوم السياسية
العدد (69) حزيران (2025) **E-ISSN**: 2521-912X **ISSN:** 1815-5561

إستراتيجية التحكم بالفضاء السيبراني لتعزيز الأبعاد غير الملموسة للأمن القومي العراقي

محمد كاظم عباس المعيني*

الملخص:

تستكشف هذه الدراسة نهجًا استراتيجيًا للسيطرة على الفضاء الإلكتروني بهدف تعزيز الأبعاد غير الملموسة للأمن القومي العراقي. في ظل المشهد الأمني العالمي المتطور، برز الفضاء الإلكتروني كمجال محوري يُعيد صياغة مفاهيم الردع وتكتيكات الحرب وتوازن القوى. وعلى عكس الحروب التقليدية، تتميز الصراعات الإلكترونية بطبيعتها غير المادية، مما يتطلب قدرات تكنولوجية متطورة وموارد بشرية ماهرة. بالنسبة للعراق، كغيره من الدول، فإن تحديات الفضاء الإلكتروني أفقية ورأسية، لا سيما في قطاعي الأمن وبناء القدرات. تعكس هذه التحديات كفاح الدولة لإدارة وتأمين بنيتها التحتية الرقمية بفعالية. تبحث الدراسة فيما إذا كان العراق يمتلك القدرات اللازمة للسيطرة على فضاءه الإلكتروني، وتقترح استراتيجيات لمواجهة التهديدات غير التقليدية ضمن أطر الدفاع الوطني.

باستخدام منهجية وصفية وتحليلية، يُحلل البحث المفاهيم والاستراتيجيات والسياسات الرئيسية المتعلقة بحوكمة الفضاء الإلكتروني، ويربطها بإطار الأمن القومي الأوسع للعراق. تكشف النتائج أن الفضاء الإلكتروني أصبح مجالًا متنازعًا عليه بشكل متزايد، ومحوريًا للتنافس الجيوسياسي، واستعراض القوة الرمزية، وسيادة الدولة. وتخلص الدراسة إلى أن معالجة نقاط الضعف السيبرانية في العراق تتطلب تنسيقًا حكوميًا رفيع المستوى، ودمجًا للذكاء الاصطناعي في أنظمة الدفاع، وتخصيصًا استراتيجيًا للموارد، وصنع سياسات شاملة تُشرك جميع الجهات المعنية. علاوة على ذلك، يجب أن تضمن الاستراتيجية الوطنية للفضاء الإلكتروني احترام حقوق الإنسان الأساسية، مع بناء بيئة رقمية موثوقة ومتكيّفة وآمنة تتماشى مع الأولويات الاجتماعية والسياسية للعراق.

كلمات مفتاحية: استراتيجية، الفضاء السيبراني، الأمن القومي، الأمن السيبراني، الحرب السيبرانية.

* أستاذ مساعد دكتور/ جامعة بغداد/ مركز الدراسات الاستراتيجية والدولية.

المقدمة:

أسهمت ثورة المعلومات وتكنولوجيا الاتصالات في تطوير بنية الفضاء السيبراني، والتي احدثت تفاعلات مستجدة للعلاقات الدولية وعلى المستويات كافة، ارتبطت فيها الدول وبعض الفواعل من غير الدول كأطراف لتلك المعادلة في رسم نتائج تلك التفاعلات وعكسها على البيئة الرقمية، فسيادة الدول لم تعد قائمة على السيطرة على المجال الأرضي والجوي والبحري؛ فهناك مجال الفضاء السيبراني الذي يُعّد البعد الرابع للسيطرة والتحكم بسيادة وأمن الدولة والمواطن، واصبح هو العامل المؤثر في إدارة المصالح الوطنية العليا المختلفة للدولة. ولغرض بناء استراتيجية فاعلة للتحكم بالفضاء السيبراني يتوجب الحفاظ على البنية التحتية الحيوية للمعلومات، من طريق التعرف على الثغرات والعيوب التقنية ومحاولة معالجتها وايجاد التدابير اللازمة لتقوية هيكل النظم المعلوماتية، وبناء القدرات الوطنية ضد التهديدات السيبرانية المحتملة؛ فالاستعمال الواسع والكبير من المؤسسات الرسمية وغير الرسمية والافراد جعل الاستغناء عنه امراً صعباً ومستحيلاً ومن ثم سيكونون عرضة للهجمات السيبرانية. وتكمن أهمية الموضوع في صعوبة التكيف مع حالة الضعف التي يعيشها العراق وعلى اكثر المستويات لاسيما الأمني منها، والتي تشكل تحدياً كبيراً امام الحكومة، اذ اصبح العراق اكثر عرضة للهجمات السيبرانية بعد عام 2003، بسبب انفتاحه الواسع والسريع على العالم، كما أسهم التطور التقني والمعلوماتي والانتقال السريع للمجتمعات إلى الفضاء الافتراضي في إدخال العراق إلى هذا الفضاء ربما عنوةً من دون أن يمر بمرحلة انتقالية تمهيدية لهذا الواقع الجديد والمجهول، الأمر الذي يحتم على الحكومة العمل بمثابرة واجتهاد على تقليص الهوة المعرفية والتقنية في هذا الحقل الجديد الذي اصبح ساحة عالمية مفتوحة ومباحة للجميع، والمنتصر والمتحكم فيها من يملك مفاتيح هذا العالم الإفتراضي الجديد، وإن سياسات الدفاع الحديثة تعطي الأولوية الآن لتطوير تدابير الأمن السيبراني بشكل كبير لحماية البنية التحتية الحيوية والمعلومات الحساسة. ويمكننا التساؤل هنا؛ هل يملك العراق القدرة على السيطرة والتحكم بفضاءه السيبراني؟، وماهي الاستراتيجيات الفعالة لمعالجة التهديدات الأمنية غير التقليدية في إدارة الدفاع عن الأمن القومي؟، وعليه تفترض الدراسة؛ بان العراق مازال أمامه وقت لكي يصل إلى حد التحكم بفضائه السيبراني وحماية أمنه السيبراني، وهذا الوقت يرتبط بمدى استجابة صانع القرار للتكيف مع التحديات، وامتلاكه للقدرات اللازمة للتأثير في هذا الفضاء.

المنهجية:

لاستكمال إعداد هذه الدراسة اعتمدنا على المنهج الوصفي والتحليلي لوصف الظاهرة أصل الموضوع والتعرف على مجموعة المفاهيم والاستراتيجيات والسياسات التي تناولها البحث، وتحليلها وفق المعطيات والأحداث بشكل علمي، وربطها بالأمن القومي العراقي.

المحور الاول: الفضاء السيبراني ومعضلة الأمن القومي

اتسع مدى تأثير الفضاء السيبراني ليشمل مجالات الحياة كافة الاجتماعية والاقتصادية والسياسية والأمنية والثقافية والتعليمية والصحية الخ...، اذ أنشأ تصورات وتفاعلات جديدة لم تكن مسبوقة، تحول فيها العالم الواقعي المرتبط بالفضاء العمومي* إلى عالم افتراضي، ومع تفجر ثورة المعلومات والاتصالات ودخولنا العصر الرقمي، عدّ قسم من الباحثين بالشأن الاستراتيجي إن الفضاء السيبراني هو المجال الخامس في الحروب بعد البر والبحر والجو والفضاء، وسنتناول في هذا المحور بعض التعاريف لمفهوم وماهية الفضاء السيبراني وعلاقته بالأمن السيبراني، ومدى ارتباطهما بالأمن القومي.

اولاً: الفضاء السيبراني وعلاقته بالأمن السيبراني

هناك ارتباط عضوي بين المفهومين لايصح الفصل بينها، كما انه لايوجد تعريف واحد متفق عليه لكلا المفهومين؛ بسبب حداثة الموضوع وتوسع مجالاته، ويعكس اهتمامات ومصالح الجهات الفاعلة، فالروس مثلاً نادراً ما يستعملون مصطلح "الفضاء الالكتروني" ويفضلون التحدث عن "الانترنت" أو "أمن المعلومات" كبديل عنها، ولكننا سنحاول اعتماد تعريف واحد أو اكثر لزيادة الإستيضاح والإحاطة من دون الولوج عميقاً بالتعاريف الكثيرة التي سبق وأن تناولها كثير من الباحثين لتجنب التكرار (Douzet 2014).

1- يعود مصطلح الفضاء السيبراني وأصل كلمة Cyberspace إلى المعنى اليوناني للحكم (Cyber)، وتعني حكم أو التحكم بالفضاء، وببساطة يمكننا تعريف الفضاء السيبراني على انه "تلك الشبكة المرتبطة من البنى التحتية لتكنولوجيا المعلومات، والتي تشمل الانترنت وشبكات الاتصالات السلكية واللاسلكية ونظم الحواسيب والمعالجات المدمجة وأجهزة التحكم" (Costigan and Henness 2016, 17)، والفضاء السيبراني اكبر وأشمل من الانترنت؛ فهو يشير إلى بيئة الانترنت التي تشمل التفاعلات الاجتماعية من طريق استعمال الوسائط الرقمية ومن طريق مواقع الشبكات الاجتماعية مثل "Facebook و X و

Instagram"، اذ يعمل الفضـــاء الســـيبراني في ظل الأوضـــاع المادية غير التقليدية ليكون وســـيطاً بين ماهو ملموس Tangible، من حواســـيب وشـــبكات اتصـــال، وغير الملموس Intangible، من بيانات ومعلومات رقمية (Qi 2005,4)، ويمكن تعريف الفضـاء السـيبراني على انه ذلك المجال المجازي (غير المادي) لإنظمة الحاســـوب والشـــبكات الإلكترونية، اذ تُخزن المعلومات الكترونياً وتتم الاتصـالات مباشـرةً على الشـبكة؛ فهو من جانب يوصـف بأنه غير محســـوس (غير ملموس وغير مرئي) من طريق تدفق المعلومات والبيانات الرقمية عبر شـــبكة الحواســـيب والأجهزة الاخرى المرتبطة مع بعضـــها، وفي الوقت ذاته هو محســـوس وحقيقي؛ بسبب الآثار الناتجة عنه، إذ منح هذا الفضـاء فرصـاً جديدة لإعادة تشـكيل المجتمع والهوية الثقافية عبر الهويات الخفية وتطوير وربط العلاقات البشـرية، وبذلك اصـبح مصـطلح الفضـــاء الســـيبراني وســـيلة لوصـــف كل شـــيء مرتبط بالانترنت وثقافتة المتنوعة والشـــبكة العنكبوتية العالمية، واثار ايضـاً قضـايا ومواضـيع لم تكن بالحسـبان، كالملكية الفكرية وانتهاك حقوق النشـر، والذي تطلب ايجاد نماذج جديدة للتجارة وأرضـية مشـتركة للاتصـال السـريع للأفكار والقيم (خريسان 2021، 21-22). يوصف العالم الافتراضي الذي نعيشه اليوم بأنه عالم بحدود هلامية لم تتشـكل ملامحه بعد، ولذا يصـعب تحديد الإمكانيات المعرفية والمادية اللازمة لتحقيق الاستقرار النسبي والعيش للانسان والمجتمع، لاسيما للطرف الضعيف معرفياً ومادياً، ويمكننا هنا ان نحدد بعض العناصـر الرئيسـة التي يتكون منها الفضـاء السـيبراني، وهي: (قاسيمي 2016، 68-69):

أ. الاتصـال والتفاعل البشـري بأشـكاله الرسـمية وغير الرسـمية جميعها، ومسـتوياته المختلفة (السياسية، التجارية، القانونية، الاجتماعية، الخ..)، ونتائج ذلك على الانترنت.

ب. المجتمع الرقمي الجديد (مجتمع الانترنت)، بخصـــائصـــه اللامحدودة كلها، وانفتاحه اللامتناهي، واتجاهاته المختلفة، وطبيعته الافتراضية.

ت. الفرد الرقمي (الفرد الانترنيتي)، وتشـكله كشـخصـية سـيبرانية انسـانية، ذات الخصـائص الجماعية الافتراضية القائمة على التواصل والحوار.

ث. العقل الجمعي الرقمي الناتج من تفاعل العقول الفردية الافتراضـية داخل العالم الافتراضـي، الموجه الشمولي لحركة وتدفق المعلومات داخل مجتمع الانترنت، الذي يخدم التجسيد المتكامل للقرية السيبرانية.

2- الأمن السيبراني (Sybersecurity): ظهر هذا المصطلح مع ظهور حرب الانترنت في نهاية الحرب الباردة، والذي تزامن مع بداية الاعتماد على الحواسيب التي دخلت العمل في مؤسسات الدولة الرسمية والشركات الكبرى، واقتصر دوره في البداية على الحماية من البرامج الضارة والفيروسات، اذ ظهر اول فيروس في سبعينيات القرن العشرين وكان على شكل رسالة نصية مختصرة ولم تسبب اضراراً كبيرة، ولكنها كانت العامل الذي دفع الى اتخاذ التدابير الوقائية وتأسيس الأمن السيبراني، ولكي نعرف هذا المصطلح وجدنا هناك عشرات التعاريف له، وسنتناول اكثرها إحاطة وشمولية حتى نقرب الصورة للقارئ، ويمكننا وصفه على انه تلك الأساليب الدفاعية من عمليات وتقنيات وممارسات التي تكشف المتسللين المحتملين وتحبط عملهم، وتحمي الشبكات وأجهزة الحاسوب والبرامج والمعلومات المخزونه فيه من الهجمات السيبرانية المتمثلة بالاختراق والتخريب، وذلك من طريق استعمال الأدوات المناسبة لايقاف عمل البرامج الضارة (الفايروسات، وغيرها)، والكشف عن الأضرار والاختراقات، وتمكين الاتصالات المشفرة وتشغيلها، وضمان أمن المعلومات والأصول والبنية التحتية الحيوية (Craigen et al. 2014, 14-17).

ينقسم الأمن السيبراني على مستويين، هما (Jain and Pal 2017 ،791):

أ. الأمن المادي لأجهزة الحاسوب والتطبيقات والبرامج والشبكات، وحمايته من أي هجوم وأضرار محتملة، أو فقدان التحكم والسيطرة على تلك الاجزاء.

ب. الأمن غير المادي المرتبط بالمعلومات والبيانات وحمايتها من الاختراق والسرقة أو الفقدان أو عدم القدرة للوصول إليها.

تكمن أهمية الأمن السيبراني في حماية الهوية والمعلومات بانواعها جميعها(العسكرية، المالية، استخبارية، فكرية، طبية، تقنية، الخ...)، من الاحتيال والسرقة والدخول غير المصرح، ليس على مستوى الحكومة والمؤسسة أو المنظمة فقط، بل حتى على مستوى الفرد والأسرة والمجتمع، واتساقاً مع ذلك يمكننا تحديد أهم أهداف الأمن السيبراني التي وضعت قسم منها أمانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات التابعة لمستشارية الأمن القومي العراقية والمتمثلة بما يأتي (استراتيجية الأمن السيبراني العراقي د.ت، 6-7):

أ. السرية في إدارة أو تلقي أو تغيير المعلومات من الاشخاص المخولين أو المصرح لهم.

ب. النزاهة التي تضمن قيام الاشخاص المصرح لهم فقط بالتغييرات في النظام.

ت. وضع تشريعات شاملة لمكافحة الجريمة السيبرانية والتدابير المضادة للتهديد السيبراني التي يمكن اعتمادها على الصعيد الوطني والإقليمي والعالمي، ذات الصلة في سياق تأمين الفضاء السيبراني للبلاد.

ث. بناء القدرات الذاتية ونشر الوعي العام وتمكين المهارات الضرورية، وتوفير التدابير التي تحمي البنية التحتية الحيوية للمعلومات، فضلاً عن تقليل مواطن الضعف ومعالجة الثغرات على المستوى المحلي، ووضع آليات فعالة للاستجابة لحالة الطوارئ التي قد يتعرض لها الحاسوب، من طريق تطوير وتحسين قدرة فريق الاستجابة الوطني لمعالجة الهجمات السيبرانية (Uganda's Ministry of ICT and National Guidance 2024)

ج. وضع آلية مناسبة وموثوقة للتصدي للتهديدات السيبرانية عبر التعاون والتنسيق والشراكة بين اصحاب المصلحة الوطنيين (الحكومي، والخاص)، فضلاً عن الشركاء الدوليين.

ح. تنسيق مبادرة الأمن السيبراني على المستويات جميعها، لحماية الحكومة من أشكال الهجمات السيبرانية جميعها.

خ. العمل على تعزيز الرؤية الوطنية للأمن السيبراني، من طريق التوعية والشراكة وتقاسم المسؤوليات، وكذلك العمل على ايجاد مجتمع موثوق به من أصحاب المصلحة.

ثانياً: تأثير الفضاء السيبراني في الأمن القومي:

تبين لنا فيما سبق العلاقة التفاعلية بين الفضاء السيبراني والأمن السيبراني اللذان لايمكن الفصل بينهما؛ لانه ليس هناك معنى في استعمالنا الواسع ودخولنا غير المحدود في الفضاء السيبراني والعالم الافتراضي من دون تأمين معلوماتنا وبياناتنا وأجهزة الحواسيب وبرامج التشغيل من الهجوم والاختراق السيبراني، فكلما زاد استعمالنا للفضاء السيبراني زادت مخاطر الاختراق وتطلب ذلك زيادة الحماية وتعزيز الأمن السيبراني، وتوضح تلك العلاقة الجدلية أهمية الأمن السيبراني في الحفاظ على الفضاء السيبراني، استناداً لذلك اصبح الأمن السيبراني أحد أهم ركائز ومقومات الأمن القومي، بعد أن باتت المعرفة والمعلومة أهم ركن من أركان قوة الدولة، اذ يجسد الأمن القومي أولوية تتصدر مجمل الاستراتيجيات التي تضعها الدولة من أجل تحقيق مصالحها الحيوية؛ وبسبب التطور والحداثة التي يعيشها العالم اليوم، تطورت مفاهيمه واتسع نطاق ادراكه نحو مديات تجاوزت المجال العسكري وحتى الاقتصادي والسياسي والاجتماعي، الخ..، وبات مفهوم الأمن القومي شاملاً متعدد الأوجه يحاول

الاســـتجابة لنمط التحديات المختلفة والمتعددة مع بروز نمط جديد من التحديات الكامنة التي تشكل تهديداً حقيقاً لأمن الدولة، ولعل الفضـاء السيبراني وحمايته من أهم هذه التحديات التي يجب وضع تصورات ادراكية فاعلة لمواجهتها والتعامل معها والحد من تأثيراتها.

1- مستويات الأمن القومي

إن التغيرات والأحداث العالمية الكبرى والحروب العالمية جعلت من الأمن القومي للدول لايقف عند حدودها، بل يمتد حيث مصـالحها الاسـتراتيجية وتهديداتها المحتملة، فهو يختلف عن مفهوم الأمن الوطني، اذ إن دائرة الأحداث الداخلية التي عاشـــها العراق أو الأحداث الخارجية في محيطه الاقليمي وضـــحت بشـكل لايقبل الشـك بان الأمن القومي العراقي يمتد مسافات ابعد من حدوده الدولية المرسومة، وعليه فان الأمن القومي ببساطة هو ماتملكه من فاعلية الآداء والتأثير في محيطك، وتحد من تأثير الآخرين على مصـــالحك، والذي يتحدد بالحتمية والقدر الجيوبوليتيكي ودروس التأريخ، كما ويجسد الأمن القومي للدولة قضية رئيسة تقع على قمة الأولويات الاسـتراتيجية التي تحشـد الدولة مواردها وإمكاناتها من اجل تحقيقها، وبالمحصـلة هو تعبير عن حماية الدولة لمواطنيها ومواردها وحدودها وحضـارتها وقيمها (عبد القادر 2024، 107).

هناك الكثير من الآراء حول تصنيف مستويات وانماط الأمن القومي، بل وحتى هناك اختلاف في المسـميات بين مصـطلحي الأمن الوطني والأمن القومي، ونحن في كتاباتنا نعتمد تسـمية الأمن القومي اذا كان نطاق البحث يشـــمل التهديدات الخارجية والداخلية التي قد يتعرض لها أمن الدولة وأمن المواطن المقيم داخل البلد أو خارجه، ولا يخفى على الجميع بأن الأمن هو أحد الحاجات الاســاســية للانســان والتي لايمكن العيش بدونها، فهو كالهواء والماء والغذاء، يمكن أن يشير مصطلح الأمن القومي إلى أحد المستويات الأنطولوجية الأربعة (ظاهرة العلوم الاجتماعية، جزء من استراتيجية، سياسة حكومية، أو حقيقة قائمة بذاتها، وبالمثل، يعبر هذا المصـــطلح عن اربعـة أهـداف امنيـة (أمن الفرد، أمن النظـام، أمن الأمـة، أمن النظـام الاجتماعي)، ويترتب على ذلك بطبيعة الحال صـعوبة تحقيق هذه الأهداف مجتمعة، اذ حوّل التفاعل المعقد بين تصـورات التهديد والأهداف والوسـائل الأمنية في العالم الحديث مجموعة واسعة من القيم والمبادئ والمؤسسات والقوى، إلى نوع من "الوحدة الضخمة"، اذ يبدو إن هناك

نوع من الاندماج بين المصلحة الوطنية ومصلحة الأمن القومي (Valdes 1982, 10) . وفي بحثنا قسمنا الأمن القومي على مستويين هما: –

أ– **المستوى الأول:** يشمل هذا المستوى مجالات الأمن المادية (المرئي والملموس) كلها، والتي تضم الأمن السياسي الذي يمثل الحفاظ على السيادة ووحدة وسلامة اراضي الدولة من أي تهديد خارجي أو داخلي، والأمن الاقتصادي المتمثل بالإستثمار الأمثل للموارد الطبيعية وتحقيق التنمية المستدامة وكل مايرتبط بالأمور المالية والسياسة النقدية (Holmes 2015, 23)، والأمن العسكري المتمثل بتطوير القدرات العسكرية للدولة، وأمن الطاقة المسؤول عن انتاج وتوفير الطاقة واسعار السوق وأمن الممرات، والأمن الصحي المتمثل بتحصين المجتمع من الأوبئة وتوفير اللقاحات والعلاجات والرعاية الصحية، والأمن البيئي المسؤول عن حماية البيئة والطبيعة من الملوثات والانبعاثات الحرارية لغازات الدفيئة، والأمن الغذائي المتمثل بتوفير الطعام المناسب ودعم المحاصيل الاستراتيجية، والأمن المائي المرتبط بادارة وتوفير المياه اللازمة للسقي والشرب وادامة الحياة، وغيره (Holmes 2015, 18).

ب– المستوى الثاني: يشمل هذا المستوى المجالات الأخرى من الأمن القومي خارج عن نطاق الأمن المادي والتي نطلق عليها الأمن غير المادي (Intangible)، ومن الممكن ادراجها ضمن مكونات القوة الرمزية، اذ ظهرت الحاجة دولياً إلى وجود قوة غير مادية إلى جانب القدرات المادية التي ذكرت آنفاً، ومنها الأمن الاجتماعي المتمثل بقدرة الدولة على حماية قيمها الايدولوجية وثقافتها الخاصة من الثقافات والأفكار الدخيلة (Blanchette 2020 , 4)، ثم يأتي الأمن السيبراني الذي بدأت الدول تولي اهتماماً واسعاً به لتأثيره الكبير والمباشر في المستويين المحلي والدولي، وهو مثار وتخصص بحثنا هذا، اذ يشير هذا المجال من الأمن إلى حماية البنية التحتية للحواسيب ومعالجة البيانات وأنظمة التشغيل الخاصة بالحكومة والأفراد من التداخل الضار، سواء من خارج الدولة أم داخلها، وهي لا تنطوي على الدفاع الوطني والأمن الداخلي فقط؛ ولكن على إنفاذ القانون (Holmes2015,19).

2– استراتيجية الفضاء السيبراني في تعزيز الأمن القومي:

تلامس التقنيات الرقمية اليوم اغلب جوانب الحياة في اغلب مجتمعات العالم، واصبح الانترنت هو مفتاح الوصول والاتصال والإنفتاح على المجتمعات والأفراد في كل مكان، بدّل ذلك من قواعد اللعبة القديمة بشكل كبير، فباتت الأجهزة الذكية في متناول الجميع تقريباً لاسيما الهاتف

النقال، واستعمالاتها تجاوزت التواصل مع الآخرين ومشاركة الأفكار إلى ادارة الأعمال التجارية وانجاز الأعمال الأخرى، ومن ثم اصبح من الضروري أن يتوفر نظام بيئي رقمي آمن وموثوق وسريع يلبي تلك الحاجات على مدار الوقت، وهنا لابد لنا أن نضع استراتيجية وطنية للأمن السيبراني تحقق لنا الاستعمال الأمثل والآمن للفضاء السيبراني، والتأكد من إمكانية كسب الفوائد وضمان مستقبلنا الرقمي، اذ اصبح الأمن السيبراني ضرورياً لتحريك الاقتصاد وتشغيل البنية التحتية الحيوية، والحفاظ على خصوصية البيانات والاتصالات، والدفاع عن الدولة وسيادتها (National Cybersecurity Strategy 2023).

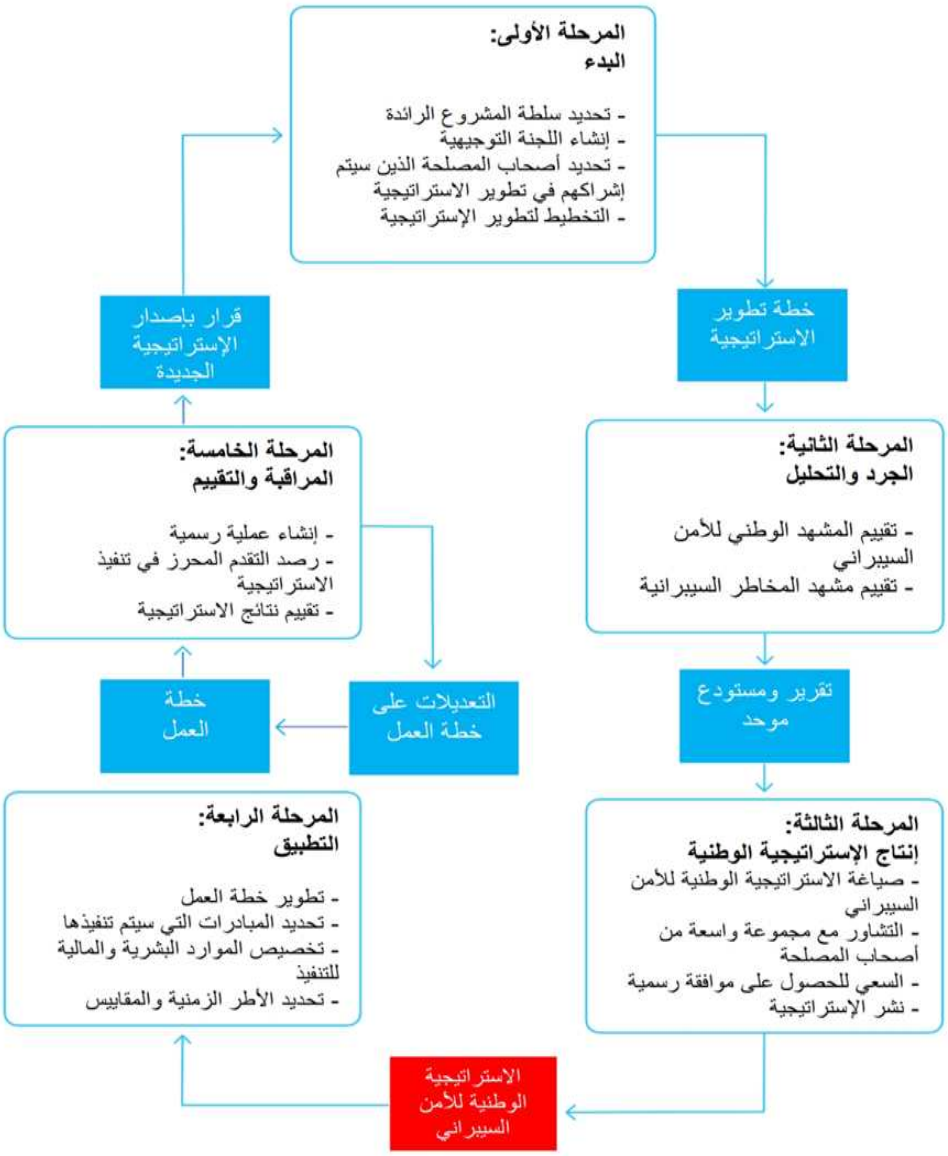
يمكن أن تتخذ استراتيجيات الأمن السيبراني الوطنية اشكالاً عديدة، وتدخل في مستويات متفاوتة من التفاصيل، اعتماداً على أهداف ومستويات الاستعداد السيبراني لكل بلد، وهنا لابد لأصحاب المصلحة التفكير والعمل على انتاج استراتيجية وطنية للأمن السيبراني على النحو الآتي (International Telecommunication Union 2021):

أ- تعبير عن الرؤية والأهداف والمبادئ والأولويات الرفيعة المستوى التي توجه الدولة في معالجة الأمن السيبراني، وتقدم نظرة عامة لأدوار ومسؤوليات اصحاب المصلحة المكلفين بتحسين الأمن السيبراني للدولة.

ب- تصف الخطوات والبرامج والمبادرات التي ستتخذها الدولة لتعزيز أمنها القومي وقدرتها على الصمود، وحماية بنيتها التحتية السيبرانية.

ت- تعتمد خوارزميات الذكاء الصناعي في تحليل كميات هائلة من البيانات والمعلومات من مصادر متنوعة، كصور الاقمار الصناعية ووسائل التواصل الاجتماعي وشبكات الاستشعار، لاكتشاف التهديدات المحتملة أو الانشطة المشبوهة بالوقت المناسب(60، Sarjito 2024).

فيما يأتي مخطط يوضح مراحل دورة حياة الاستراتيجية الوطنية للأمن السيبراني التي من المفترض أن يضعها صانع القرار واصحاب المصلحة في حساباتهم إذا ارادوا بناء مثل تلك الاستراتيجية:



الشكل رقم (1) – مراحل دورة حياة الاستراتيجية الوطنية للأمن السيبراني

(International Telecommunication Union 2021, 17)

المحور الثاني: بناء استراتيجية سيبرانية وطنية

تفتقر كثير من دول العالم وحتى المتقدمة منها، إلى استراتيجية فعالة لمنع الهجمات السيبرانية بالتزامن مع ازدياد اعداد تلك الأنشطة الضارة وتصاعد حدتها وانعكاسات نتائجها الكارثية على سائر مجالات الحياة؛ فهناك فجوة اخذت بالإتساع والتنامي بين الدراسات الاكاديمية والممارسات الدولية، فلو نأخذ الولايات المتحدة الأمريكية كمثال للدول المتقدمة في مجال توظيف القدرات السيبرانية لتحقيق الأهداف الاستراتيجية، نرى انها لم تترجم تلك القدرات إلى استراتيجية واضحة لمواجهة الهجمات السيبرانية التي تتعرض لها (Hoffman 2019, 135)، وظهر ذلك جلياً في اكثر من مناسبة تعرضت فيها الولايات المتحدة الأمريكية لهجمات وقرصنة سيبرانية ضربت مؤسسات الدفاع (Pentagon) ووكالة الفضاء الأمريكية (NASA) ووكالة المخابرات المركزية (CIA) وغيرها من المنشآت والمؤسسات الحكومية وغير الحكومية.

إن اساس بناء استراتيجية الأمن السيبراني العراقي هو لضمان أمن العراق وحماية وجوده ومصالحه في الفضاء السيبراني وحماية المعلومات الحيوية، وتأسيس مجتمع انترنيتي فعال يحظى بالرعاية والموثوقية، على أن تتعامل هذه الاستراتيجية مع أشكال وأنماط التحديات السيبرانية جميعها التي قد يتعرض لها البلد من طريق مجموعة من الإجراءات والفعاليات التي تحمي الفضاء السيبراني العراقي، وسنستعرض في هذا المحور آليات ومعوقات بناء تلك الاستراتيجية.

اولاً: آليات بناء استراتيجية سيبرانية

تقوم تلك الاستراتيجية على حماية الأمن القومي والاستقرار السياسي والاجتماعي والرخاء الاقتصادي من التهديدات المتوقعة داخل الفضاء السيبراني وعبره، فهناك علاقة طردية بين نوع وكمية الهجمات السيبرانية وبين سعة استعمال الفضاء السيبراني سواء على مستوى الفرد ام مستوى الشركات والمصارف والمؤسسات، فالدول التي خضع نظامها الإداري إلى الأتمته (حكومة الكترونية) يكون بيئة خصبة وساحة للاختراق السيبراني اكثر من الدول الأخرى التي تعتمد الآليات القديمة بالإدارة (الأوراق)، وتكون الهجمات السيبرانية على العموم من افراد Hackers يقومون بالاختراق إما لمصلحة شخصية، أو لمصلحة دولة تحاول الإضرار بدولة اخرى، عبر سرقة معلومات مهمة جداً، أو التجسس على الاسرار العليا للدولة، أو الحاق

ضـرر مادي واقتصـادي للدولة من طريق تعطيل منشـآت أو معامل أو مفاعلات أو شـبكات نقل أو محطات كهرباء الخ..، وهناك امثلة كثيرة على تلك الحالات لامجال لتكرار ذكرها بالتفصيل، بدءاً من الهجمات السيبرانية التي تعرضت لها البرازيل في عامي 2005 و 2007 على شـبكات ومحطات الكهرباء، مما جعل اقسـام كبيرة من البلاد تعيش في ظلام لمدة من الوقت، مروراً بأهمها وأبرزها القيام باختراق سيبراني اتهمت به (اسرائيل) على مواقع عسكرية ومنشـآت نووية ايرانية عامي 2010 و 2020، مما اخرج أجهزة الطرد المركزي لتخصـيب اليورانيوم عن السيطرة، فضلاً عن الهجوم السيبراني الذي اتهمت به روسيا على أجهزة التحكم بالنظام الالكتروني لفرز الأصـوات في انتخابات الرئاسـة الأمريكية عام 2017 التي فاز فيها الرئيس (ترامب)، والهجوم السيبراني على اللجنة الدولية للصليب الأحمر عام 2022، واخيرها وليس آخرها الهجوم السيبراني على بعض المراكز الطبية والمستشفيات في لندن عام 2024 مما أدى إلى الغاء عدد كبير من العمليات الجراحية وتعطيل جناح الطوارئ والعناية المركزة (اللجنة الدولية للصليب الأحمر 2022 ؛ بي بي سي 2020).

هناك عدة آليات وخطوات ينبغي اتباعها لبناء اسـتراتيجية فاعلة للتحكم قدر الإمكان بالفضـاء السيبراني؛ فاذا تمكنا من تحقيق الأمن السيبراني كمستوى ثاني للأمن القومي، حينذاك نستطيع تحقيق الأمن القومي الشامل، فبعد أن تناولنا آنفاً مجموعة التحديات المرئية وغير المرئية التي قد تواجه أمننا القومي، وتجلى أخطرها بالنوع الثاني غير المرئي، الذي يعد تهديداً مباشراً على منظومة الأمن الاسـتراتيجي للعراق، والذي لايمكن تحسـسـه الا من طريق البحث العميق والتحليل المسـتمر، وسـنتناول هنا كيفية بناء تلك الاسـتراتيجية اسـتناداً على تأثير الفضـاء السـيبراني في مجالات الأمن القومي بعد دراسـة اسـتراتيجيات بعض الدول في مجال الأمن السـيبراني، ولغرض بناء تلك الاسـتراتيجية السـيبرانية لمواجهة الهجمات السـيبرانية ينبغي أن نعي جيداً بأنه لاتوجد اسـتراتيجية محددة قادرة على منع الفعاليات الضـارة كافة في الفضـاء السيبراني، في ظل تشابك مصالح الدول وارتباطه بشكل متزايد بالأصول الرقمية، وهنا سنحدد بعض الآليات المتاحة لتعزيز بناء استراتيجية سيبرانية خاصة بالعراق، ومنها:

أ- يجب أن لاتركز الاستراتيجية السيبرانية على الردع والدفاع فقط، وإنما على التأثير في الاتجاهات السلوكية والتكنولوجية، والموائمة بين القدرات والوسائل والأهداف، والتركيز على

العمليات السيبرانية الهجومية والدفاعية على حد سواء، وتقسيم مسؤوليات الأمن السيبراني بين الحكومة والقطاع الخاص(Hoffman 2019, 140).

ب- تعزيز أمن البيانات من طريق تخزينها على جهاز وسيط خارجي غير موصول بنظام الحاسوب وتخزينها بمكان آمن، مع وضع تقنيات تشفير عالية المستوى لحمايتها من الاختراق غير المصرح به في اثناء نقلها عبر الشبكة (الجزيرة نت 2024).

ت- تعزيز أمن التطبيقات من طريق رفع مستوى الحماية عبر وضع برامج آمنة لمنع الأخطاء والاختراق، وتحدد الثغرات الأمنية بعمل اختبارات للاختراق وتحديث تلك البرامج باستمرار.

ث- تعزيز أمن الشبكات من طريق جدران الحماية التي تراقب حركة انتقال ومرور البيانات بين الشبكة الداخلية والخارجية، وكذلك تحليل سلوك المستعملين والنظام عبر أنظمة الكشف.

ج- تعزيز حماية الحواسيب والأجهزة المتصلة بالشبكة من طريق وضع برامج تساعد في كشف وازالة الفيروسات والبرامج الضارة من النظام، فضلاً عن تحديث البرامج والأنظمة بانتظام لضمان سد الثغرات الأمنية، وتعزيز أمن الولوج وادارة هويات المستعملين المصرح لهم بالدخول.

ح- تدريب الأفراد العاملين في هذا المجال على أعلى مستوى، للقيام بتلك المهام التي ذكرت آنفاً وتوعيتهم حول استراتيجيات الأمن السيبراني، من طريق هندسة الأمن السيبراني عبر تصميم الأنظمة والشبكات لكي تجعلها مقاومة للاختراق، والقيام برصد الأنشطة السيبرانية الغريبة وتحليلها لكي تكون الاستجابة سريعة، وتطوير ثقافة الإبلاغ عن النشاط المشبوه، مع الحرص على سرعة التعافي بعد الهجوم أو الاختراق لضمان الاستمرارية بالعمل، ووضع خطة طوارئ تسمح للمؤسسات بالاستجابة السريعة لحوادث الهجوم السيبراني (Cyber Security Center for the Isle of Man 2022 – 2027 2022).

خ- ترجمة رؤية الحكومة إلى سياسات متماسكة وقابلة للتنفيذ تساعدها على تحقيق أهدافها، وهذا لا يشمل فقط الخطوات والبرامج والمبادرات التي ينبغي وضعها، بل يشمل ايضاً الموارد المخصصة لتلك الجهود، وكيفية استعمال تلك الموارد، وبالمثل، يجب أن تحدد العملية المقاييس التي سيتم استعمالها للمساعدة في ضمان تحقيق النتائج المرجوة ضمن الميزانيات والجداول الزمنية المحددة(International Telecommunication Union 2021, 13).

ثانياً: معوقات بناء استراتيجية سيبرانية:

يظل الأمن القومي مصدر قلق بالغ للدول في أنحاء العالم جميعاً، مما يقود إلى التطور المستمر لاستراتيجيات إدارة الدفاع، وهذا يتطلب مواكبة التطورات التكنولوجية الحديثة والتحولات الجيوسياسية والتهديدات الناشئة، وإعادة تقييم استراتيجيات الدفاع التقليدية (Sarjito 2024، 57)، وهذا قد يشكل صعوبة في التوصل إلى رؤية مشتركة للاستراتيجية السيبرانية في ظل عدم الإتفاق على أهداف ووسائل وأهمية تلك الاستراتيجية؛ فهناك تباين حتى في توصيف الفضاء السيبراني، هل يمثل شكلاً جديداً من الاقليم؟ ولو كان نحو ذلك، ماهي حدود السيادة على هذا الاقليم؟، بين قسم يراه تغيير جوهري في طبيعة التنافس الاستراتيجي، وقسم آخر يعتقد بانه امتداد لانماط التنافس الراهن من طريق وسائط تكنولوجية جديدة، وهناك من يركز على استغلال أنظمة الحواسيب للتجسس أو ادخال برامج ضارة لتعطيل عمل الحواسيب، وهناك من يدعم الشركات الوطنية وحصصها التجارية من تكنولوجيا المعلومات، وقدرات الأفراد التقنية الكامنة، اذ تكمن عملية بناء استراتيجية سيبرانية على مواجهة وتحدي الحرب السيبرانية على مستوى الأسلحة السيبرانية ومن يستعملها من الدول أو الفواعل من غير الدول، وتكمن معوقات بناء تلك الاستراتيجية على عدة أمور منها:

أ- صعوبة تحديد هوية الفاعل مع صعوبة تحديد جهة الاسناد لكي نحدد من هو العدو الحقيقي والذي على اساسه نضع وسائل الاحتواء والمنع والتقييد.

ب- صعوبة الفصل بين القدرات السيبرانية والأدوات السياسية، ومعوق دمج القدرات السيبرانية مع القدرات والقوة التقليدية، من طريق ربط مشغلي الانترنت والقادة السياسيين، فضلاً عن تحقيق المرونة الاستراتيجية المتمثلة بتنوع الخيارات(Hoffman 2019, 136).

ت- يفتقر العراق إلى التشريعات القانونية اللازمة لإدارة وتنظيم استعمال الفضاء السيبراني وحمايته من أي اختراق غير مصرح به أو هجوم أو تخريب يطال البنية التحتية الاستراتيجية للدولة؛ اذ قطعت اغلب دول العالم اشواطاً كبيرة في مجال وضع الأطر القانونية وتشريع القواعد القانونية التي تنظم العمل في الفضاء السيبراني وتحاسب من يخرق تلك القوانين (Al-Jibouri 2016) ، أما في العراق هناك تشريع واحد فقط يخص الجريمة الالكترونية، لم يصل بعد إلى مستوى الطموح، واغلب جزائاته وعقوباته يطبق فيها قانون العقوبات العراقي لعام 1969.

ث- عدم وجود منظومة انترنت خاصة بالعراق، كحال كثير من دول العالم، اذ يرتبط العراق بمنظومات انترنت خارجية مملوكة لشركات ودول اجنبية تتجهز أو تمر معلوماتها عبر كابلات بحرية أو اقمار صناعية ذات مورد خدمة يمر من خوادم تلك الدول لترجع تلك المعلومات مرة ثانية إلى العراق، مما يجعله منكشفاً استراتيجياً ومصيره مرتبط بهذا الخارج الذي يملك حق التشغيل والخصوصية، ولذا فان هذه الحالة ستؤثر بشكل كبير في أمننا السيبراني(العلي 2018).

ج- الفوضى التي تعم سوق الانترنت في العراق؛ بسبب حالة عدم الاستقرار التي يعاني منها البلد لاسيما في الجانب الأمني، مما أدى إلى تضرر البنية التحتية للانترنت، والذي يدفع المشتركين إلى تنويع مصادر تجهيز الانترنت، لإنعدام المسؤولية المشتركة وعدم فاعلية العلاقة بين القطاعين العام والخاص في ان يكونا جزءاً من الاستراتيجية الوطنية للأمن السيبراني(Kovacs 2018 , 115).,العراق في بدايات مراحله لمواجهة الجريمة السيبرانية، وهذا ناتج من كون المجتمع لايضع هذه المواضيع في أولوية اهتماماته، فضلاً عن قلة الملاك الفنية المتخصصة، وضعف الخبرات والقدرات التكنولوجية والعلمية، مع شحة التخصيصات المالية الواجب توفرها لرفع وترقية مستوى تلك الإمكانيات، الأمر الذي يؤدي إلى زيادة التحديات المفروضة على الأمن السيبراني(Aboud 2014, 422-424).

الخاتمة:

لقد احدث الاستعمال الواسع للفضاء السيبراني والنمو المتسارع للانترنت، ثورة في أسلوب حياتنا، وتغيير في نمط اقتصادنا، ووسع بشكل كبير وسائل الاتصال لدينا، ومن جانب آخر أدى ذلك إلى انتشار الصراعات حول كثير من القضايا المهمة كمراقبة وتنظيم الانترنت، واستعمال الشبكات في النزاعات السياسية ، والحرب العسكرية والاقتصادية، والعمل الاستخباري، وممارسة القوة الرمزية، واحترام الخصوصية والحريات المدنية الأخرى، لذلك اصبح الفضاء السيبراني هدفاً للتنافس على السلطة بين أصحاب المصلحة، ومسرحاً للمواجهة المفتوحة، واداة قوية في النزاعات الجيوسياسية، ووسيلة للهيمنة والسيطرة في النظام الدولي. ولمدة طويلة ظلت هذه القضايا ضمن اختصاص مجتمع صغير من الخبراء ذوي المهارة والخلفية العلمية والتكنولوجية، واليوم مع التطور الهائل للانترنت ووجوده الفاعل والمستمر في مفاصل حياتنا اليومية جميعاً، تحتاج الحكومات بمؤسساتها المدنية والعسكرية والأمنية، والشركات والمجتمع المدني كلها، إلى فهم هذه التحديات وتحليلها، والتعامل معها بشكل

افضـــل. وتواجه منظومة الأمن القومي العراقي جملة من التحديات الخطيرة لاســيما التحديات غير المادية وغير الملموسـة والتي من الصـعب كشـفها بالوقت المناسـب، والتي تشـكل تهديداً اســـتراتيجياً لأمن الدولة والفرد، فاصـــبحت التهديدات الســـيبرانية من أهم تلك التحديات في عصرنا الراهن، والحفاظ على أمن المعلومات وحماية أنظمة التشغيل والحواسيب من الاختراق والتعطيل، الشغل الشاغل للدول والحكومات، إذ شهد العراق هو الآخر تطوراً تكنولوجياً واسعاً في مجال الاتصـــالات والمعلومات؛ لكنه تزامن مع ضـــعف البنية التحتية الســـيبرانية، والذي انعكس سلباً على أمنه السيبراني، وبات الفضاء السيبراني العراقي منكشفاً على كثير من الدول والتنظيمات والأفراد لاختراقه والتجســس على بياناته ومعلوماته، أو اســتعماله كســاحة لشــن هجمات ارهابية منه أو ضده.

الاستنتاجات:

1-بما إن الأمن هو صناعة وتمكين واقتدار، فعلى صانع القرار الأمني أن يكون على مستوى عالٍ من الثقافة الأمنية، ويملك المهارة والقدرة على تشخيص التحديات ويميزها عن التهديدات، ومسـتعد أمنياً لمواجهة المخاطر وتداعيات التحديات الكامنة والظاهرة، ووضـع الاسـتراتيجيات المناسبة لها وفق اساليب الإدراك والاستجابة.

2- توظيف التطورات التكنولوجيـة، لا ســـيما في الذكاء الاصـــطناعي والتعلم الآلي في اســتراتيجيات إدارة الدفاع وعمليات صــنع القرار، من طريق تعزيز التقنيات والقدرات الدفاعية الشاملة واكتشاف التهديدات المحتملة لأمننه المعلومات، وتخصيص موارد بشرية ومالية كفوءه وكافية.

3-وسـط عدم اليقين العالمي، ومع اسـتمرار تطور مشـهد التهديدات السـيبرانية، يظل التكيف المســتمر والابتكار في اســتراتيجيات الدفاع ضـــروريين لحماية المصـــالح الوطنية وتعزيز الاســتقرار العالمي، وينبغي أن تتيح الاســتراتيجية إدارة فعالة لمخاطر الأمن الســيبراني؛ وأن تعزز الرخاء الاقتصـــادي والاجتماعي وتزيد إلى اقصـــى حد إســـهام تكنولوجيا المعلومات والاتصالات في التنمية المستدامة.

4-وضـع الاسـتراتيجية من قبل أعلى مسـتوى في الحكومة، وبمشـاركة نشـطة من اصـحاب المصلحة المعنيين جميعاً، وان تلبي احتياجاتهم ومسؤولياتهم، والتي ستكون مسؤولة بعد ذلك عن اسناد الأدوار والمسؤوليات ذات الصلة، وأن تضع رؤية واضحة للحكومة والمجتمع ككل.

5-يجب أن تساعد الاستراتيجية في بناء بيئة رقمية ينتج عنها فهم وتحليل شاملين لتلك البيئة، يمكن للمواطنين والمنظمات الوثوق بها، مع تكيفها مع أوضـــاع البلد وأولوياته، وأن تحترم حقوق الانسان الاساسية وتكون متسقة معها.

ملاحظات ختامية:

* يعد العالم "يورغن هابرماس" صـاحب نظرية الفضـاء العمومي؛ إن هذا الفضـاء يعد مجالاً للنقاشات والممارسات الفكرية المبنية على العقل والمنطق من النخب غير المنتمية بالمؤسسات الرسمية والحاكم. والتي تجمعهم قضـايا المجتمع الذي يتشكل من طريقها الآراء والمواقف التي تجســد اهتمامات وطموح وهموم الناس. من اجل اتخاذ القرارات التي تحقق المصـــلحة العامة (المحمداوي 2004، 65).

قائمة المصادر:

المحمداوي، علي محمود. 2004. *الاشكالية السياسية للحداثة من فلسفة الذات الى فلسفة التواصل: هابرماس انموذجاً*. الرباط: دار الامان.

استراتيجية الامن السيبراني العراقي. د ت. مستشارية الامن الوطني. امانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات.

https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf

الجزيرة نت. 2024."الأمن السيبراني مفهومه وتاريخه". 19 أيلول، 2024.

https://www.aljazeera.net/encyclopedia/2024/9/19/.

العلي، علي زياد. 2018. التحديات غير المرئية للأمن الوطني العراقي. بغداد: مركز البيان للدارسات والتخطيط.

https://www.bayancenter.org/2018/06/4565.

اللجنة الدولية للصليب الاحمر. 2022. "هجوم سيبراني على اللجنة الدولية: المعلومات التي نعرفها". 16 فبراير، 2022.

https://www.icrc.org/ar/document/%D9%87%.

بي بي سي. 2020. "الهجوم الالكتروني على الولايات المتحدة: بومبيو يتهم روسيا ويصف رئيسها بأنه خطر حقيقي". 19 كانون الأول، 2020.

https://www.bbc.com/arabic/world-55377723

خريسان، باسم علي. 2021. *الفضاء السيبراني: مدخل ابستيمولوجي*. بغداد: دار قناديل للنشر والتوزيع.

عبد القادر، ايمان. 2024. "اثر الفضاء السيبراني على الأمن القومي العربي خلال الفترة من 2011 حتى نوفمبر 2023." *مجلة الاكاديمية العسكرية للدراسات العليا والاستراتيجية*، عدد.3 (يناير): 106- 120.

https://doi.org/10.21608/nsas.2024.337116

قاسيمي، صافية. 2016. "الفضاء السيبراني والاغورا الالكترونية – اشكالية خلق فضاء عمومي افتراضي حسب المنظور الهابرماسي." *مجلة الحكمة للدراسات الفلسفية*، عدد.7 (ديسمبر): 75–60.

https://asjp.cerist.dz/en/downArticle/338/4/7/10740

List of References:

Abdel Qader, Iman. 2024. "The impact of cyberspace on Arab national security during the period from 2011 until November 2023." *Journal of the Military Academy for Postgraduate and Strategic Studies,* No.3 (January):120 -106 . https://doi.org/10.21608/nsas.2024.337116 (in Arabic)

Aboud, Sattar J. 2014. "Cybercrime in Iraq", *International Journal of Scientific & Engineering Research* 3, No.2 (March): 63-68. https://www.researchgate.net/publication/261722490_Cybercrime_in_Iraq/citations.

Al-Ali, Ali Ziyad. 2018. Invisible Challenges of Iraqi National Security. Baghdad: Al Bayan Center for Studies and Planning. Research Department. https://www.bayancenter.org/2018/06/4565. (in Arabic)

Al Jazeera Net. 2024. "Cybersecurity: Its Concept and History." September 19, 2024. https://www.aljazeera.net/encyclopedia/2024/9/19/. (in Arabic)

Al Muhammadawi, Ali Mahmoud. 2004. *The political problem of modernity from the philosophy of self to the philosophy of communication: Habermas as a model*. Rabat: Al-Aman. (in Arabic)

Al-Jibouri, Farook. 2016. "Iraq Cyber Security Overview and announcing our Cyber Security Framework." Cyber Code Technologies FZE. December, 2016. https://www.linkedin.com/pulse/iraq-cyber-security-overview-announcing-our-framework-al-jibouri

BBC News. 2020. "Electronic attack on the United States: Pompeo accuses Russia and describes its president as a real danger." December 19, 2020. https://www.bbc.com/arabic/world-55377723 (in Arabic)

Blanchette, Jude. 2020. Ideological Security as National Security. Washington: Center for Strategic and International Studies.https://www.csis.org/analysis/ideological-security-national-security

Craigen, Dan Nadia, Diakun-Thibault, and Randy Purse. 2014. "Defining Cybersecurity, Technology Innovation Management Review." October, 2014.https://timreview.ca/sites/default/files/article_PDF/Craigen_et_al_TIMReview_October2014.pdf

Costigan, Sean S, and Michael A. Hennessy. 2016. Cyber security A Generic Reference curriculum. North Atlantic Treaty Organization.https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/20161025_1610-cybersecurity-curriculum.pdf

Cyber Security Center for the Isle of Man. 2022. "National Cybersecurity Strategy 2022 – 2027." July, 2022.https://csc.gov.im/media/qd2p4o2z/approved-national-cyber-security-strategy-1.pdf.

Douzet, Frederick. 2014. "Understanding Cyberspace with Geopolitics." *Herodote1*, No.1 (January): 152-153. understanding-cyberspace-with-geopolitics.pdf.

Hoffman, Wyatt. 2019. "Is Cyber Strategy Possible?." *The Washington Quarterly 42*, No. 1(Spring):131-152. Doi.org/10.1080/0163660X.2019.1593665.

Holmes, Kim R. 2015. "What is national Security?." The Heritage Foundation. 2015.https://www.heritage.org/sites/default/files/201910/2015_IndexOfUSMilitarySt rength_What%20Is%20National%20Security.pdf

International Committee of the Red Cross. 2022. "Cyber attack on the ICRC: what we know." February 16, 2022.https://www.icrc.org/ar/document/%D9%87%.(in Arabic)

Iraqi Cyber Security Strategy. n.d. National Security Advisory. Secretariat of the Higher Technical Committee for Communications and Information Security.https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf (in Arabic)

International Telecommunication Union. 2021. "Strategic Engagement in Cybersecurity: Guide to Developing a National Cybersecurity Strategy." 2021. https://ncsguide.org/wp-content/uploads/2024/05/508938E.pdf

Jain, Jitendra, and Parashu Ram Pal. 2017. "A Recent Study over Cyber Security and its Elements." *International Journal of Advanced Research in Computer Science8*, No.3(March – April):791-793. https://www.researchgate.net/profile/ParashuPal/publication/321528686_A_Recent_ Study_over_Cyber_Security_and_its_Elements/links/5a2a7134aca2728e05db41bf/A -Recent-Study-over-Cyber-Security-and-its-Elements.pdf .

Khreisan, Basem Ali. 2021. *Cyber space. Epiphrology entrance*. Baghdad: Dar Qanadeel for Publishing and Distribution. (in Arabic)

Kovacs, Lszlo. 2018. National Cyber Security as the cornerstone of national security. *Land Forces Academy Review*, No.2 (June): 113-120. DOI: 10.2478/raft-2018-0013.

National Cybersecurity Strategy. 2023. The White House Washington, (March). 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf .

Qasimi, Safia. 2016. "Cyberspace and the Electronic Agora – The Problem of Creating a Virtual Public Space According to the Habermasian Perspective." *Al-Hikma Journal of Philosophical Studies*, No.7 (December): 60-75. https://asjp.cerist.dz/en/downArticle/338/4/7/10740. (in Arabic)

Qi, Wei. 2005. "Cyberspace and Political Participation in Contemporary China A Preliminary Assessment Based on Two Case Studies." Master's thesis., Lund University/Center for East and South-East Asian Studies.

Sarjito, Aris. 2024. "Enhancing National Security: Strategic Policy Development in Defense Management. *Journal Pelita Nusantara*2, No.1 (May): 56 – 68. DOI: 10.59996/jurnal pelitanusantara. v2i1.524.

Uganda's Ministry of ICT and National Guidance. 2024. "National Cybersecurity Strategy 2022 – 2026." 2024.https://dig.watch/resource/ugandan-national-cybersecurity-strategy-2022-2026 .

Valdes, J.A. Tapia. 1982. "A Typology of National Security Policies." *The Yale Journal of World Public Order*, No.9 (January): 10 -39. https://core.ac.uk/download/pdf/72839271.pdf