الأمن الوطني العراقي في عصر الذكاء الاصطناعي: الإرهاب السيبراني وتحديات السيادة الرقمية

م.م همسة عامر نجم
hamssaamir@gmail.com
الجامعة المستنصرية/ كلية العلوم السياسية

م.م فدك حسين منحوش
Fadakh.manhoosh@uokufa.edu.iq
جامعة الكوفة/ كلية الإدارة والاقتصاد

الملخص:

أحدثت تكنولوجيا المعلومات والاتصالات ثورة هائلة في كل جوانب الحياة، فكان للمستوى الاجتماعي تأثير كبير في سلوك وهوية المجتمع، وانتشار آليات التشابك بين الجماعات الإنسانية، التي تمثلها وسائل التواصل الاجتماعي عبر الأجهزة الإلكترونية، مما ترتب عليه تغييرات كبيرة في مرتكزات اجتماعية كالتعارف وبناء العلاقات الاجتماعية، والخصوصية والثقافة، ووسائل الإعلام، وعندما تصبح تكنولوجيا المعلومات والاتصالات هي المهيمنة على أنماط الحياة، بالمقابل تزداد المخاطر السيبرانية، لذلك نحن نواجه جرائم حقيقية ومتكاملة الأركان، تتم عبر الفضاء الإلكتروني متمثلة ب (التخطيط لعلميات إرهابية، إشاعة الأخبار المضللة، سرقة الأموال الابتزاز الإلكتروني النصب والاحتيال التلاعب والتزوير)، وهذه الجرائم هي الأكثر شيوعاً في العالم الرقمي.

تمثل التحديات الثقافية والفكرية أهم بوابات التهديدات السيبرانية عبر الغزو الفكري لشبكات الاتصالات ونشر ثقافة الإقصاء والعنف والتحريض على الجرائم بأعذار طائفية أو دينية أو قبلية أو عرقية، وظهرت كواحدة من الاهتمام بالمحتوى الإلكتروني القائم على انتشار العلم والمعرفة وتقارب ثقافات الشعوب والحضارات، ويتعرف مستقبل تكنولوجيا المعلومات والاتصالات على التهديدات الإلكترونية الرئيسة، مما يحول الإنترنت إلى منطقة كبيرة تزداد فيها التهديدات، والاختراقات، والهجمات، والمخاوف.

ما لا شك فيه ستكون فرصة كبيرة للاستثمارات والتحالفات، وهذا الأمر يحتم على التعامل مع جوانب الأمن السيبراني بمهنية عالية ومرونة كاملة ونهج استباقي.

يمكن القول: إن تحدي الأمن السيبراني هو التحدي الأكبر للأمن الوطني في عصرنا الراهن، وتجدر الإشارة إلى أن مفاهيم الأمن الحديثة لا تقتصر على الجوانب العسكرية، ولكنها تسير إلى جنب جميع التهديدات والتحديات التي قد تصبح حجر عثرة أمام الأمن الشامل، وأمام تدفق المعرفة والاقتصاد الرقمي، فقد أسقطت تكنولوجيا المعلومات والاتصالات مفاهيم عديدة وعلى سبيل المثال لا الحصر الحدود الجغرافية السياسية، والثقافية بين الدول، مما يضع السيادة الوطنية أمام خطر محدق، ولاسيما التجسس المعلوماتي على الدول، واختراق المواقع الحكومية الرسمية

الكلمات المفتاحية: الذكاء الاصطناعي، الأمن الوطني، التهديدات السيبرانية

Iraqi national security in the age of artificial intelligence: cyber threats and challenges to digital sovereign

Assist. Lect. Fadak Hussein Manhoosh Assist. Lect. Hamsa Amir Najm
Fadakh.manhoosh@uokufa.edu.iq hamssaamir@gmail.com

Abstract:

Information and communication technologies (ICTs) have revolutionized all aspects of life. The social sphere has had a profound impact on societal behavior and identity, and the proliferation of interconnectedness among human groups, facilitated by social media platforms on electronic devices, has led to significant changes in fundamental social norms such as acquaintance, relationship building, privacy, culture, and media. As ICTs become dominant in lifestyles, cyber risks also increase. We now face fully-fledged cybercrimes, including planning terrorist operations, spreading misinformation, theft, extortion,

fraud, manipulation, and forgery. These crimes are among the most prevalent in the digital world.

Information and communication technologies have revolutionized all aspects of life, particularly in the social sphere. Cultural and intellectual challenges represent the most significant gateways for cyber threats, through the intellectual invasion of communication networks and the dissemination of a culture of exclusion, violence, and incitement to crime under the guise of sectarian, religious, tribal, or ethnic pretexts. This has emerged as a consequence of the growing interest in electronic content aimed at spreading science and knowledge and fostering understanding between cultures and civilizations. The future of information and communication technology will identify key cyber threats, transforming the internet into a vast arena where threats, breaches, attacks, and anxieties are escalating.

Undoubtedly, this will present a significant opportunity for investment and alliances, necessitating a highly professional, flexible, and proactive approach to cybersecurity. It can be argued that cybersecurity is the greatest challenge to national security in our time. It is worth noting that modern security concepts are not limited to military aspects, but encompass all threats and challenges that could hinder comprehensive security and the flow of knowledge and the digital economy. Information and communication technologies have overturned many concepts, including, but not limited to, geopolitical and cultural boundaries between countries, thus placing national sovereignty under imminent threat, particularly through cyber espionage and the hacking of official government websites.

Keywords: Artificial Intelligence, National Security, Cyber Threats

المقدمة:

يُعد التقدم التكنولوجي الذي شهده العالم واحد من أهم التحديات التي أثرت على الأمن الداخلي للدولة، إذ أصبحت التكنولوجيا سلاح ذو حدين من الممكن أن تستخدم في خدمة مصالح وإهداف الدول ويمكن أن تكون جزء من التحديات التي تواجه الدول.

شكلت التطورات في مجال الاتصالات وتكنلوجيا المعلومات إيذاناً لظهور العصر السيبراني و بزوغ بيئة جديدة أو مجال آخر فضلاً عن البر والبحر والجو والفضاء هو المجال السيبراني أو الفضاء السيبراني، إذ غيرت هذه التطورات مظاهر التفاعل بين الدول، وجعلتها تبدو على نحو مختلف من حيث الشكل والمضمون، وكذاك طريقة التعامل مع القضايا والتحديات على وفق ما بدأت تحمله من مظاهر جديدة انعكست بشكل مباشر في الأداء الإستراتيجي للدول وان هذا التأثير لا يقتصر على الواقع الداخلي للدول وإنما يمتد إلى المحيط الدولي الواسع ليؤثر في إعادة رسم شكل ومضمون الأمن الدولي، ويحدد أطر جديدة لطبيعة العلاقات الدولية والأمن الدولي، ما جعل الفضاء السيبراني مجالاً جديداً للصراع بين الدول.

أذ أدى الفضاء الإلكتروني دوراً مهماً في تعظيم القوة، أو الاستحواذ على عناصرها الأساسية في العلاقات الدولية، فقد أصبح التفوق في ذلك المجال عنصراً حيوياً في تنفيذ عمليات ذات فاعلية في الأرض، والبحر، والجو، والفضاء، واعتماد القدرة القتالية في الفضاء الإلكتروني على نظم التحكم، والسيطرة التكنولوجية، وأدى ذلك الأمر إلى تغيير في مفهوم القوة الوطنية للدولة، فبات بالإمكان تعريفها بأنها مجموعة الوسائل، والطاقات، والإمكانيات

المادية وغير المادية المنظورة، وغير المنظورة التي بحوزة الدولة، ويستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة، وتؤثر في سلوك الوحدات السياسية الأخرى. وأعطت القوة السيبرانية دافعاً رئيسياً في اتجاهين، الأول: تدعيم القوة الناعمة للدول، فقد بات الفضاء الإلكتروني مسرحاً لشن هجمات تخريبية، ترتبط بالحرب النفسية، وبنشر المعلومات المضللة والتأثير في توجهات الرأي العام، والنشاط السري والاستخباراتي، أما الاتجاه الآخر، فيتعلق بتبني الدول الزيادة الإنفاق في سياسات الدفاع الإلكتروني، وحماية شبكاتها الوطنية من خطر التهديدات، وإنشاء مؤسسات وطنية للحماية الإلكترونية

❖ أهمية الدراسة:

تنبع بيان أهمية الدراسة من صياغة منظومة أمن سيبراني، تؤدي دوراً مهماً للتأثير في نجاح أداء الدولة في البيئتين الداخلية والخارجية، وهذا ما دلت عليه التجارب في دول عدة سواء في المحيط الاقليمي أم الدولي واتساقاً مع تطور عصر التكنولوجيا، وما نتج عنه ومن تطورات شملت كل الميادين، فما كان للأمن

السيبراني إلا أن يكون واحداً من أهم حقول المعرفة والعلوم المعاصرة، إذ يؤدي الأمن السيبراني دوراً مهماً في ظل الصراعات السياسية على مستوى الساحة العالمية.

إذ يهدف البحث إلى تحليل التهديدات التي يفرضها الذكاء الاصطناعي على الأمن الوطني العراقي والتعرف على أهم الفرص والتحديات التي تواجه مؤسسات الدولة، فضلاً عن استكشاف السياسات والاستراتيجيات الممكنة لتعزيز الأمن الوطني وحمادية السيادة.

❖ أهداف الدراسة:

تنقسم أهداف الدراسة على نوعين:

١. الأهداف العلمية:

تظهر الأهداف العلمية للبحث في الكشف عن أنماط الأمن والتحديات الناجمة عنها، ويشتق من هذا الهدف

الرئيس عدد من الأهداف الفرعية الأخرى؛ لعل من أهمها ما يأتي:

- تحديد أنماط الأمن.
- تحديد ماهية الأمن السيبراني.
- إظهار تأثير الأمن السيبراني كمرتكز في استراتيجية الأمن الوطني العراقي.

٢. الأهداف العملية:

تكمن الأهداف العملية للبحث في تقديم عدد من التوصيات والمقترحات التي يؤمل أن تساعد صانعي القرار، فهناك الوزارات السيادية، التي تؤدي دوراً أساسياً في المشاركة، ورسم صناعة، وسيرورة أمن الدولة في البيئتين الداخلية والخارجية، ويقع على عاتقها إدارة الشؤون والمصالح العراقية في الساحة الإقليمية والدولية وهي بحاجة كبيرة للاستفادة كثيراً من تجارب الدول الناجحة، واستثمارها، والحرص على تطوير استراتيجيات التضمن عن طريقها تحقيق الأهداف التي تسعى إليها.

❖ إشكالية الدراسة:

انبثقت هذه الدراسة من تساؤل مركزي أساسي هو: إلى أي مدى يعد الأمن السيبراني المرتكز الأهم في عملية صياغة إستراتيجية الأمن الوطني العراقي على المديين المتوسط والبعيد؟

مما حدي بالباحث أن ذلك مشكلة استوجب البحث والتقصي، وعن طريق ما تم طرحه في أعلاه يمكن تحديد التساؤلات الفرعية الآتية:

١. ما هي أنماط الأمن ومرتكزاته؟

٢. ما المتغيرات الدافعة نحو التركيز على الأمن السيبراني؟

٣. ما هي تحديات ضعف وهشاشة الأمن السيبراني على بنية وتماسك كيان الدولة العراقية؟

٤. كيف تعامل العراق مع التهديدات السيبرانية؟

❖ فرضية الدراسة:

ينطلق البحث من فرضية مفادها:" كلما زاد اعتماد العراق على البنية الرقمية غير المؤمنة، زادت قابلية تعرضه للتهديدات السيبرانية المرتبطة بتقنيات الذكاء الاصطناعي".

❖ منهجية الدراسة:

اعتمدنا في هذه الدراسة على جملة من المناهج العلمية، فقد اعتمدنا **المنهج الوصفي** ويقوم المنهج الوصفي على تفسير ظاهرة التهديدات السيبرانية، وتحديد خصائصها، فضلا عن وصف طبيعة ونوعية العلاقة بين الأمن السيبراني والأمن القومي، ومن ثم الاعتماد على **المنهج التحليلي** وقد استخدم لتحليل الظواهر والأحداث المؤثرة في الأمن السيبراني وكيفية توظيفه في استراتيجيات الدول الكبرى كنموذج، لنوضح من خلاله مدى تأثير التهديدات السيبرانية على الأمن الوطني العراقي، ورصد أهم الحالات، والأضرار الناجمة عن هذه التهديدات، وأخيراً تم الاستعانة **بالمنهج الاستشرافي** لبيان مستقبل توظيف الأمن السيبراني في استراتيجية الأمن الوطني العراقي في المواجهة للتهديدات السيبرانية.

❖ هيكلية الدراسة:

تم تقسيم البحث الى مبحثين فضلاً عن مقدمة وخاتمة ونتائج:

- **المبحث الأول: ماهية الأمن الوطني وتطوره**

المطلب الأول: مفهوم الأمن الوطني

المطلب الثاني: مفهوم الإرهاب السيبراني

المطلب الثالث: علاقة الأمن السيبراني بالأمن الوطني

- **المبحث الثاني: طبيعة الإرهاب السيبراني في العراق**

المطلب الأول: ظهور الإرهاب السيبراني في العراق

المطلب الثاني: مظاهر الإرهاب السيبراني في العراق

المطلب الثالث: التحديات التي تواجه الأمن السيبراني في العراق

المطلب الرابع: سبل معالجة الإرهاب السيبراني في العراق

❖ الدراسات السابقة:

سنركز على أهم الدراسات السابقة التي تطرقت لبعض المفاصل المختلفة لـ عنوان الدراسة:

١. منى الأشقر جبور، السيبرانية هاجس العصر، بيروت: جامعة الدول العربية – المركز العربي للبحوث والدراسات القانونية والقضائية، ٢٠١٦. تندرج هذه الدراسة، في أطار جهود جامعة الدول العربية، التي أخذت على عاتقها، مهمة نشر الوعي بأهمية الأمن السيبراني وذلك عبر تنظيمها ورعايتها عدداً من المؤتمرات واللقاءات والمنشورات، ونوقشت خلال هذه الورش والمؤتمرات العلمية المسائل الخاصة بهذا الجانب، وعليه، فقد انطلقت هذه الدراسة من رؤية حددت معالمها عبر مقاربة لواقع الحال في التحليل والاستنباط والمقارنة، ومتطلبات بناء الثقة، وإرساء قواعد مرنة تواكب تحديات التهديدات السيبرانية، والحد من الخسائر الناجمة، التي تترتب عليها وطرق مواجهتها.

٢. عادل عبد المنعم، أمن المعلومات والأمن القومي، دراسات استراتيجية، مجلة السياسة الدولية، العدد (٢١٣)، مركز الأهرام للدراسات والبحوث الإستراتيجية، القاهرة، يوليو ٢٠١٨
٣. أوس مجيد غالب العوادي، الأمن المعلوماتي السيبراني، مركز البيان للدراسات والتخطيط، بغداد، أغسطس ٢٠١٦.
٤. إيهاب خليفة، القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الأنترنت، القاهرة: العربية المتحدة للنشر والتوزيع ٢٠١٧

المبحث الأول: ماهية الأمن الوطني وتطوره

إن تعرفنا على معنى كلمه الأمن لغة واصطلاحاً وتعرفنا على المعنى اللغوي المصطلح "الأمن الوطني"، يقودنا إلى توضيح معنى مصطلح "الأمن القومي" و "الأمن الوطني"، فكما هو أمن الفرد ضروري لبقائه واستمراره وتطوره وتقدمه فهو كذلك أساس التنمية والتقدم والرقي للدول والمجتمعات.

المطلب الأول: مفهوم الأمن الوطني

إن مصطلح "الأمن الوطني" هو مصطلح سياسي حديث نسبياً إذ ظهر مع بداية ولادة الدولة القومية في أوروبا أي بعد معاهدة وستيفاليا ١٦٤٨ التي بموجبها تغير شكل النظام الدولي وبدأت حقبه جديدة من حياة العالم تمثلت بظهور فكر التنوير وبداية النهضة العلمية والصناعية في أوروبا، ولعل الظروف السياسية والأمنية التي عاشتها أوروبا تفسر لنا سبب ظهور هذا المصطلح وكذلك فان رغبه كل دوله في الحفاظ على جغرافيتها وسكانها ومقدراتها الوطنية وخوفها الكبير من جيرانها هو ما عزز مفهوم الأمن الوطني وزادة تطوراً وانتعاشاً (الدليمي، ٢٠٠٣، ٥٦).

أما الاستخدام الرسمي لمصطلح الأمن الوطني فكان في نهاية الحرب العالمية الثانية عام ١٩٤٧، عندما أنشأ الأمريكيون هيئة رسمية، سُميت "مجلس الأمن الوطني الأمريكي" والذي اسند لهُ بحث كافة الأمور والأحداث، التي تمس كيان الأمة الأمريكية، وتهدد أمنها (الياسري، ٢٠١٠، ٥٦).

أما الأمن الوطني من حيث التعريف فقد تعددت وتنوعت التعريفات التي قُدمت فيه وذلك باختلاف البحث من ناحية الثقافة والبيئة والزاوية التي ينظر منها لهذا المفهوم وكذلك من ناحية الخلفية الأكاديمية والخبرة العملية، فنظرة المدرسة الغربية للأمن الوطني تختلف وبلا شك عن نظرة المدرسة الشرقية التي كان يتبناها الإتحاد السوفيتي السابق والدول التي كانت تسير في المنظومة الشيوعية وكذلك فان التعريفات والدراسات الخاصة بهذا المفهوم في مناطق العالم الثالث لها أسس وقواعد تنطلق منها، ولعل ذلك يرجع إلى القيم العلياء التي يؤمن بها المجتمع والتي يسعى وبكل ما أوتي من طاقة للمحافظة عليها(الدليمي، ٢٠٠٣، ٥٦).

أن تعريفات "الأمن الوطني" تسير وفق اتجاهين وذلك حسب ما يقول الخبراء الإستراتيجيين وهما:

- **الاتجاه التقليدي:**

يرى أن الأمن القومي هو قدرة الدولة على دحر أي هجوم عسكري عليها وبالتالي فانهُ يَعُد الأمن العسكري هو كل شيء بالنسبة لمفهوم الأمن القومي للدولة وهنا يسيطر المفهوم العسكري للأمن عادة على سياسات الدول، وهذا الاتجاه يقدم الأمن الوطني على أساس انه القيمة الأعلى والأسمى في الدولة، والذي تتقدم فيه البندقية على رغيف الخبز، وهو ما أسماه ادم سميث مأزق الاختيار بين الرخاء والدفاع، وبالتالي فإن العلاقات الدولية كانت تسير وفق الأسس التي ترى أنها علاقات مبنية على القوة العسكرية وان النظام الدولي قائم

على هذا الأساس، لذلك فان على كل دوله أن تبني استراتيجيه أمنها الوطني على أساس عسكري، وهذه هي فكرة النظرية الواقعية في العلاقات الدولي (الشقحاء ٢٠٠٤، ١٢).

- **الاتجاه الشمولي المعاصر**

هو الذي فرضته معطيات الواقع الدولي المُعاش إلى جانب التغيرات التي أصابت النظام العالمي وتغير شكلة من ثنائي القطبية إلى أحادي القطبية تهيمن فيه قوة واحدة على كل مجريات الأمور، وقد كان لانهيار الإتحاد السوفيتي أكبر الأثر في تغير مفهوم الأمن القومي أو الوطني لاسيما إذا ما علمنا أن الأسباب الرئيسية التي أدت إلى انهيار الإتحاد السوفيتي لم تكن عسكريه أو سياسية فحسب، بل إن الأسباب الاجتماعية والاقتصادية أدت الدور الأكبر في هذا الانهيار، مما جعل الأفكار والأنظار تتجه في هذا المجال نحو أنواع جديدة من الأمن لا تقل أهمية عن الأمن العسكري الذي يعتمد على الآلة العسكرية فقط، مثل: الأمن الاجتماعي والأمن الاقتصادي والأمن الثقافي، والأمن البيئي (الوندي، ٢٠٠٤، ١٢).

إن هذا الاتجاه متأثر أيضاً بالتغيرات التي حدثت في العالم وظهور مفهوم العولمة، وتوسع مفهوم السوق وبدء الحديث عن الأمن الإنساني العالمي الجماعي والذي يَعُد إن العالم يشترك مع بعضه البعض في بناء مجتمعي واحد مما جعل مهددات الأمن عالميه وتتطلب حلولاً عالميه مشتركة وبالتالي نقل المفهوم من معناه الضيق إلى مفهوم أكثر اتساعاً إذ تم وضع الأمن العسكري ضمن إطار مجتمعي يشمل الجوانب الاجتماعية واقتصادية وسياسية وثقافية وبيئية وغيرها، وهذا ما قدمة (ماكنمارا) الذي عدَّ أن مفهوم الأمن تختص به جميع أجهزة الدولة بدون استثناء وتشترك فيه بكل طاقاتها وإمكاناتها ويشمل ميادين مختلفة(روبنسون، ٢٠٠٩، ٢٦٩)

يرى خبراء الأمن القومي المتخصصون أن الأمن أصبح وفق هذه الاتجاهات يشير إلى بعدين هما (شيبي، ٢٠١٥، ١٤):

أولا: ارتباط الأمن القومي بالتنمية، وهو ما أكد عليه كثير من الباحثين أمثال (ماكنمار) و (جبرائيل الموند) إذ يربط ماكنمار بين الأمن والتنمية بشكل قوي فيقول: "إن الأمن القومي هو التنمية وبدون التنمية لا يمكن أن يوجد امن، وان الدول التي لا تنمو بالفعل لا يمكن أن تظل آمنه وأن الأمن والتنمية وجهان لعملة واحدة"، هذا ما أكد عليه بعض الباحثين المعاصرين أمثال جبرائيل الموند، إذ يقول أن الأمن ليس فقط المعدات العسكرية ولا النشاط العسكري ولا القوة العسكرية وإن كان الأمن يشملها جميعاً أن الأمن هو التنمية وبدون التنمية وخصوصاً في الدول النامية لا يمكن أن يكون هناك أمن واستقرار على الإطلاق.

ثانياً: ارتباط الأمن القومي بإستراتيجية الأمن التي تضعها الدولة لحماية نفسها والتي تتعلق بقدرة الدولة العسكرية والمادية من أجل حماية قيمها الذاتية من التهديدات أياً كان مصدرها، ولعلة من باب التنوع المعرفي أن تذكر هنا جمله من التعريفات التي تناولت الأمن الوطني والتي من خلالها نرى ما هي الزاوية التي ينظر كل باحث من خلالها إلى هذا المفهوم، إذ يعرفه ماكنمار بأنه: ما تقوم به الدولة أو مجموعة الدول التي يضمها نظام جماعي واحد من إجراءات في حدود طاقتها للحفاظ على كيانها ومصالحها في الحاضر والمستقبل مع مراعاة المتغيرات المحلية والدولية، ويضيف إلى ذلك قوله: إن الأمن ليس المعدات العسكرية وان كان يتضمنها وليس القوة العسكرية وان كان يحتويها وهو ليس النشاط العسكري وان كان يشمله (برد،٢٠١٦)

يرى الباحثين إن الأمن الوطني قد يتحقق في الحالات التالية (شيبي، ٢٠١٥،١٤):

١. غياب التهديد.
٢. امتلاك القوة الكفيلة المواجهة التهديد.
٣. الابتعاد بالبلاد عن أثار الخطر حال وقوعه.

بناءً على ما تقدم يعرف الباحث مفهوم الأمن القومي: هو ما تسعى آلية الحكومة للمحافظة على كيان الأمة وحمايتها من تسلط أي قوة خارجية بدفع العدوان عن الدولة وضمان استقلالها، ويهدف الأمن الوطني للدولة إلى تأمينها من الداخل ودفع التهديد الخارجي عنها بما يكفل لشعبها حياة مستقرة توفر لهُ استغلال أقصى طاقاته للنهوض والتقدم والازدهار.

المطلب الثاني: مفهوم الإرهاب السيبراني

تعد السيبرانية Cybernetic مصطلحاً مشتقاً بالأصل من المصطلح الإغريقي (Kubernetes) الذي يعني الطيار أو الحاكم على أن أصل الكلمة مأخوذاً من الكلمة الإنكليزية (سيبر، Cyber) وهي صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي / التخيلي، وبشكل عام فإن كيان السايبر يتشكل من ثلاثة عناصر أساسية هي (الرحمن، ٢٠١٧، ٦):

١. الأجهزة الصلبة (Hardware)
٢. البرمجيات الرقمية (Software)
٣. العامل البشري من مبرمجين ومستخدمين.

في مجال تكنولوجيا المعلومات والاتصالات كثر استعمال مصطلحات معينة كـ (الفضاء السيبراني، Cyber Space)، الذي يُعبر عن مجموعة من الوسائل المستعملة لإنتاج واستغلال وتوزيع المعلومات بكل أشكالها المكتوبة والمسموعة والمرئية، والتي تعد البنية التحتية التي تمكن التواصل الاجتماعي وتؤمن انتقال الرسالة من المرسل إلى المتلقي، وبذلك بعد الفضاء السيبراني

التعبير التكنولوجي الفائق السرعة لانتقال وانتشار المعلومات بين رواد هذا الفضاء، فإن الفضاء السيبراني، يعد بمثابة المستودع الكبير الذي تجرى فيه جميع عمليات التواصل الاجتماعي عبر شبكات الحواسيب أو الهواتف النقالة(يعقوب، ٢٠١٣، ٦)، وبتعبير أكثر اتساعاً، هو منظومة من العناصر المتفاعلة فيما بينها والمتكونة من أجهزة الكومبيوتر وأنظمة الشبكات وبرمجيات حوسبة المعلومات ونقل وتخزين البيانات ومستخدمي كل هذه العناصر، وتتداخل بنية الفضاء السيبراني بأنظمة البرمجيات والعناصر المادية والفضاء الرقمي، لتشكل منظومة معلوماتية في اطار برمجيات التواصل الإلكتروني(الصادق، ٢٠٠٩، ٣٧).

ولعل أهم سمات الفضاء السيبراني ما يلي(Mahmoud,2013,3) :

١. أنه مجال عملياتي إذ يعد ميدان التفاعلات المدنية والعسكرية.
٢. تعد البنى التحتية لأنظمة الاتصالات وتقنية المعلومات جزء أساسياً من الفضاء السيبراني.
٣. الفضاء السيبراني لا يقتصر على شبكة الأنترنت فقط وإنما هي شبكات عالمية وخاصة مثل نظام تحديد المواقع (ACARS، SWIFT، PSTN)

يعد الإرهاب (Terrorism) من المصطلحات التي كثر الخلاف في بيان معناها وتحديد مدلولها. فعلى الرغم من أنه من أكثر الكلمات استعمالاً في مختلف وسائل الإعلام العالمية ولاسيما منذ أحداث ١١ أيلول ٢٠٠١م، إلا أن الباحثين لم يتفقوا على تعريف دقيق ومحدد له، وذلك نظراً لطبيعة الأعمال الإرهابية

واختلاف وجهات النظر لمثل هذه الأعمال، ومن أجل وضع تعريف محدد للإرهاب السيبراني، فقد ارتأينا قبل ذلك بيان تعريف الإرهاب بشكل عام (مباركة، ٢٠٢٣، ٣٤١)

أما الإرهاب السيبراني (Cyber Terrorism)، فهو الإرهاب الذي ارتبط وجوده بوجود الفضاء السيبراني، وذلك نتيجة التوسع في الاعتماد على الاتصالات والمعلومات في تسيير الشؤون الحياتية للأفراد والمؤسسات والدول(الكريم، ٢٨٢)، أي أنه يرتبط بنوع البيئة التي يمارس فيها، وكانت بداية استعمال مصطلح الإرهاب الإلكتروني في ثمانينات القرن العشرين على يد المختص بالشؤون المعلوماتية والوقاية والأمن باري كولن Barry Collin الذي أقر بصعوبة وضع تعريف شامل للإرهاب التكنولوجي(مهني، ٢٠١٨،٢١)، ولكنه عرفهُ بأنه (هجمة الكرتونية تهديد الحكومات أو العدوان عليها سعياً لتحقيق أهداف سياسية أو دينية أو إيديولوجية، وإن الهجمة يجب أن تكون ذات أثر مدمر تخريبي مكافئ للأفعال المادية للإرهاب) (الشمري ٢٠٢٢، ٥١).

كما يُعرف الإرهاب السيبراني على أنه عمل إجرامي يكون السلاح فيه وسائل اتصال ينتج عنه عنف وتدمير أو بث الخوف، تجاه المستهدف سواء كان فرداً أو مؤسسة أو دولة، والهدف منه هو التأثير على الحكومة أو السكان، وعادة ما يمثل أجندة سياسية أو اجتماعية أو فكرية معينة.

تعددت خصائص الإرهاب السيبراني بما يلي (مهدي وصفاء،١٥٨،٢٠٢٠):

١. غياب جهة السيطرة والرقابة على الشبكة المعلوماتية، أي لا توجد جهة مركزية موحدة تتحكم فيما يعرض على الشبكة وتتحكم في مدخلاتها ومن ثم مخرجاتها.
٢. عابر للدول والقارات أي غياب الحدود الجغرافية بين الدول، إذ تربط شبكة المعلومات العالمية أعداد هائلة لا حصر لها من الحواسيب عبر العالم، ويغدو أمر التنقل والاتصال فيما بين المجموعات الإرهابية أمراً سهلاً، بمعنى آخر، فإن الشبكة المعلوماتية تتميز بسهولة الاستعمال والدخول إليها من أي مكان في العالم، فهي تتجاوز الحدود الجغرافية للدول.

٣. تدني مستوى المخاطر، إذ يتميز الاتصال المعلوماتي بعدم وضوح الهوية الرقمية للمستخدم المستوطن في بيئته المفتوحة مما تعد فرصة مناسبة للإرهابيين إذ يستطيع الإرهابي أن يقدم نفسه بالهوية والصفة التي يرغب فيها أو التخفي تحت شخصية وهمية ومن ثم يشن هجومه الإلكتروني من دون مخاطر مباشرة

٤. صعوبة الإثبات، إذ يعد استعمال الوسائل الفنية والتقنية أمراً بالغ الصعوبة في التوصل إلى الدليل المادي للجريمة المرتكبة من قبل المجموعات الإرهابية، فضلاً عن التباعد الجغرافي، وبالتالي صعوبة تحديد هوية المتصل وملاحقة مرتكبي العمليات الإرهابية مما يساعدهم على الحركة بحرية داخل المواقع التي يستهدفها قبل أن ينفذ جريمته.

٥. أنه قوة ناعمة، إذ لا يحتاج إلى المواجهة العسكرية أو استعمال الأسلحة التقليدية، وأنها جريمة لا تحتاج إلى مجهود عضلي كالقتل والسلب.

وفيما يتعلق بأدوات الإرهاب السيبراني، والتي يمكن أن تطلق عليها، بأسلحة الهجوم الإلكتروني، فهي على النحو الآتي (عبد الحي وآخرون، ٢٠١٥، ٤٤٨):

١. **الفايروسات Virus: والتي تعد من أخطر آفات الشبكة المعلوماتية، وتتميز** بقدرتها على ربط نفسها بالبرامج الأخرى وسرعة التضاعف والانتشار وتعمل على تعطيل الخدمة مؤقتاً لا على تدمير قاعدة البيانات والمعلومات، ويتم من خلال هذا النمط إطلاق حزمة كبيرة من البيانات والمهمات خادم (Server) على جهاز الطرف المتضرر وبشكل يفوق قدرته على الاستجابة والمعالجة مما يؤدي إلى توقف وشل مصالحه بصورة كلية أو جزئية، وتعطيل نظم المعلومات الإلكترونية لديه.

٢. برنامج الدودة Worms Program: وهي التي تقوم باستغلال أية فجوة في أنظمة التشغيل من نظام إلكتروني لآخر أو من شبكة لأخرى عبر الوصلات التي ترتبط بها، وتتكاثر هذه البرامج تلقائياً في أثناء عملية انتقالها، وتعمل على تقليل كفاءة الشبكة أو التخريب الفعلي للملفات والبرامج ونظم التشغيل.

٣. أحصنة طروادة Trojans وهو عبارة عن فايروس ذا مقدرة على الاختفاء داخل برامج أخرى أصلية للنظام الإلكتروني، ينشط وينتشر هذا الفايروس عندما تبدأ برامج التشغيل بالعمل ليبدأ أعماله التخريبية، ويختلف هذا الفايروس عن الفايروس العادي بكونه لا يتكاثر في الملفات إنما هو برنامج مستقل بذاته، وقد تصل أعماله التخريبية إلى تدمير النظام برمته، كذلك يمكن للمخترق معرفة كلمة السر المخزنة في الجهاز ورقم بطاقة الائتمان، وكذلك يمكن للمخترق إذا كان لدى المجني عليه ميكرفون أو كاميرا أن يستمع ويرى كل ما يفعل في المساحة التي يغطيها الميكرفون أو الكاميرا.

٤. الفايروسات الإلكترونية (Electronic Viruses): كفايروس ستاكس نت Stuxnet الذي يعد أخطر أنواع الأسلحة السيبرانية، والذي تم اكتشافه في عام ٢٠٠٩م ومثل نقلة نوعية في خطورة الحرب السيبرانية، إذ انتقلت الحرب من تدمير البيانات وسرقتها إلى تدمير المكونات المادية نفسها ونظم التشغيل، وأيضاً فايروس (دوكو Dugo) الذي تم اكتشافه في عام ٢٠١١م بواسطة معامل التشفير والأمن الإلكتروني (Crysis Lab) التابع لجامعة بودابست.

٥. البرمجيات الخبيثة مثل أريد البكاء (Wanna Cry)، إذ تتميز هذه البرمجيات يكونها تستهدف الكيانات الاقتصادية وليست الأفراد، وذلك لأن هذه المؤسسات هي الأقدر على دفع الفدية، ويلاحظ أنه في عام ٢٠١٧م قام مجموعة من القراصنة المجهولين بشن هجوم تمكن من إصابة أكثر من (٢٠٠,٠٠٠) ضحية في أكثر من (١٥٠) دولة خلال أول (٤٨) ساعة من

الهجوم، والشيء المقلق إن هذه الهجمة اعتمدت على أسلحة وثغرات تم تسريبها من وكالة الأمن القومي الأمريكي، إذ أشارت بعض التحليلات إلى ضلوع الوكالة في تطوير هذا البرنامج قبل أن تتم سرقتها منها وتسريبها(فرج،٢٠٥،٢٠٢١).

المطلب الثالث: علاقة الامن السيبراني بالأمن الوطني

قبل الحديث عن علاقة الأمن السيبراني بالأمن الوطني لا بد من التأكيد على مسألة مهمة وهي إن مفهوم الأمن الوطني يتسم بالعمومية لتأثره بحقائق متنوعة ومتغيرة ونسبية نابعة من العوامل الداخلية والخارجية، ويُعد الأمن في قمة الضرورة لأية دولة، لذلك تلجأ الدولة إلى العديد من التشريعات والإجراءات التي تكفل سلامة امنها الوطني بما يعززه داخلياً ويحميها من الأخطار الخارجية، وعليه فإن الأمن الوطني يساوي كيان الدولة وأساس بقائها.

إن التطورات المعاصرة فرضت على دول العالم ضرورة تبني استراتيجية وطنية للأمن السيبراني على إن يراعى فيها التوازن بين متطلبات الأمن الأساسية وبين احترام خصوصية المواطنين وطبيعة الثقافة السائدة في البلد، علماً إن هذهِ الاستراتيجية لا بد إن تكون ذات نهج شمولي أي لا تقتصر على الحكومة فحسب، بل من الضروري أشراك جميع أصحاب المصلحة وهم: الحكومة والقضاء والأجهزة الأمنية والمسؤولين عن البنية التحتية للأمن السيبراني من القطاع العام والخاص، ومجهزي خدمة الأنترنت وتكنولوجيا المعلومات والمؤسسات التعليمية المختصة، والمواطنين، فضلاً عن الهيئات الإقليمية والدولية المعنية بمجال الأمن السيبراني إن الهجمات السيبرانية المعاصرة تستهدف القيادات السياسية والأنظمة العسكرية والمنشآت الحيوية والمواطنين العاديين في أي مكان من العالم في وقت السلم والحرب مستفيدين من إمكانية إخفاء هوية المهاجم(شاكر، ٢٠٢٣، ٢٤-٢٥)، والأمثلة على ذلك

كثيرة منها تعرض البرازيل إلى هجمات سيبرانية في عامي ٢٠٠٥ و ٢٠٠٧ أغرقت مدناً بأكملها في الظلام وأثرت في ملايين المدنيين وما زال مصدر الهجمات مجهولاً، كما تعرضت شبكات الكهرباء في الولايات المتحدة أيضا المثل هذه الهجمات في أيار ٢٠٠٩، ونظراً للأهمية المتزايدة للأمن السيبراني وتأثيره المباشر في الأمن الوطني لأية دولة أنشأت الولايات المتحدة قيادة متخصصة بالأمن السيبراني التي أعلنت أن الفضاء السيبراني هو المجال الجديد للحرب(الشهري، ٢٠٢٣)، كما إن الأولويات الثلاثة الأولى لمكتب التحقيقات الفيدرالي الأمريكي (FBI) هي مكافحة الإرهاب والتجسس والهجمات السيبرانية، ويأتي الهجوم على الكهرباء كونها من اهم البنى التحتية وان قطعها سيؤثر بلا شك على شبكات الكمبيوتر التي تعتمد عليها مما سيؤثر بالنتيجة على الأمن الوطني، فضلاً عن ذلك تعرض منشآت ايران النووية في العام ٢٠١٠ إلى هجوم سيبراني – دودة الكمبيوتر من نوع Stuxnet بحيث نجح نصف ميغابايت من رمز الكمبيوتر من الحاق أضرار تتجاوز فاعلية أي هجوم عسكري تقليدي، ونظرًا لتطور الأمن السيبراني من تخصص تقني إلى مفهوم استراتيجي، ولأن الهجمات السيبرانية يمكن أن تؤثر في الأمن الوطني على المستوى الاستراتيجي، فانه يجب على الدول وقادتها حشد جميع موارد الدولة بما يحمي الأمن السيبراني الاستراتيجي(الشهري، ٢٠٢٣).

من الجدير بالذكر إن الدول المعتمدة على البنية التحتية للمعلومات والاتصالات يمكن لأي هجوم سيبراني إن يؤثر في طبيعة عمل مجتمعاتها، ولهذا يوصف الأمن السيبراني بأنه "حجر الزاوية" للمجتمع والمعلومات، وعليه فانه يتطلب تخطيطاً استراتيجياً متماسكاً ومفصلاً وتنظيماً قانونياً مناسباً، وقد أخذت الدول تتبنى استراتيجيات وطنية للأمن السيبراني خاصة بها اعتباراً من العام ٢٠١١، وتختلف الاستراتيجيات الوطنية للأمن السيبراني في كل دولة

على حدة من حيث المحتوى والشكل والتنفيذ وغيرها، فلا يوجد حالياً إطار وطني موحد لحماية الأمن السيبراني، ومع ذلك فإن وجود مثل هذه الاستراتيجيات وتنفيذها بشكل صحيح يمكن أن يساعد في حماية الأمن الوطني لأية دولة، كما يضمن التطور السليم للمجتمع، ويمكن أن تساعد الاستراتيجية الوطنية الفعالة للأمن السيبراني في حل النزاعات بين الدول وضمان السلام، وفي هذا الخصوص صرّح (ينس ستولتنبرغ) الأمين العام لحلف الناتو بان الأنترنت أصبح الآن جزءاً أساسياً من جميع الأزمات والصراعات تقريباً (المطيري، ٢٠٢٢، ٩٨١).

علماً أن مؤشرات الهجمات السيبرانية وجرائم الإنترنت كثيرة جداً لعل أهمها: انه في العام ٢٠١٧ ارتفعت نسبة الهجمات السيبرانية بنسبة (٦٠٠%)، ويعزى هذا الارتفاع إلى زيادة عدد الأجهزة المرتبطة بالإنترنت، وتكمن المشكلة في أن الأمن لا يواكب وتيرة التهديدات المتزايدة، وركزت (٦٣١) من الهجمات السيبرانية على البنية التحتية، كما تم شن (٩١%) من الهجمات السيبرانية برسائل احتيال عبر البريد الإلكتروني، وان (٨٥%) من جميع المرفقات التي يتم إرسالها بالبريد الإلكتروني يومياً ضارة للمستلمين المقصودين (المطيري، ٢٠٢٢، ٩٨١)، وان (٣٨%) من المرفقات الخبيثة يتم أرسالها على أنها ملفات البرامج مايكروسوفت اوفس أو برامج أخرى، ويمكن أن تشل البرامج الضارة الأنظمة بالكامل أو تجعلها عديمة الفائدة، وان أي هجوم ناجح للبرامج الضارة سيؤدي إلى خرق للأمن السيبراني، ويمكن أن تنهار بسببه شركة بأكملها، ويبلغ متوسط تكلفة هجوم البرامج الضارة (٢) مليون دولار ويطلب من الشركات حتى تتمكن من الكشف عن خرق البيانات قرابة (٦) أشهر، ففي العام ٢٠١٧ شكلت الشركات الصغيرة التي لديها اقل من ألف موظف قرابة (٦١%) من ضحايا خرق البيانات وبناء على المؤشرات السابقة صنف تقرير

المخاطر العالمية للعام ٢٠٢٠ حرب الجيل الخامس بانها أعلى الحروب خطراً، بعد إن أثرت الهجمات السيبرانية على مدن بأكملها وشملت القطاعين العام والخاص على حد سواء، وما زاد من خطورتها صعوبة كشفها وملاحقتها ففي أعلى دولة بالعالم على الصعيد التقني وهي الولايات المتحدة فإن قدرة ما كشف منها وملاحقته وصلت ما نسبته إلى (٥,٣%)، فضلاً عن ذلك هناك أكثر من (٢١) مليار جهاز متصل بالإنترنت في جميع أنحاء العالم وعددها سيضاعف بحلول العام ٢٠٢٥، يرافق ذلك ارتفاع نسبة الهجمات على الأجهزة المرتبطة بالإنترنت إلى أكثر من (٣٠٠ %)، ومن المتوقع إن تصل تكلفة الأضرار الناجمة عن جرائم الأنترنت العالمية إلى (٦) تريليون دولار بحلول العام ٢٠٢١ بعد إن كانت (٣) تريليون دولار في العام ٢٠١٥، مما يعد أكبر تحويل للثروة الاقتصادية في التاريخ(صالح، ٢٠٢٤، ٢٢٣).

مما تقدم يتضح بان الأمن السيبراني أصبح قريب الصلة بالأمن الوطني لأية دولة، وتزداد الخطورة كلما زاد اعتماد الدولة على تقنية المعلومات وارتباطها بالفضاء السيبراني، ذلك إن الهجمات السيبرانية يمكن لها إن تقوض الأمن الوطني، فأية فجوة تقنية ستؤدي إلى خسائر كبيرة للدولة في مؤسساتها الرسمية ولمواطنيها، بل إنهُ يعرض هيبة الدولة وسمعتها الدولية إلى الخطر، إذ لا تقف هذه الخسائر عند الجانب المادي فحسب بل ستؤثر مباشرة أيضا على الجانب المعنوي إذ ستلحق ضرراً في نفسية المواطنين وقادتهم، كونه يولد قناعة عامة بضعف قدرة الدولة على حماية المواطنين ومؤسساتها، وعليه يمكن القول إن الأمن السيبراني يعد قضية أمنية وطنية ضرورية يجب فهمها بعناية وشمولية.

المبحث الثاني: طبيعة الإرهاب السيبراني في العراق

أدى الانتشار الهائل في استعمال شبكات الأنترنت في العراق إلى إحداث ثورة كبرى تركت تأثيراتها على جوانب الحياة كافة، ومن بينها الأمن الوطني للدولة العراقية الذي أصبح يواجه تحديات جديدة، لذا توسع مفهوم الأمن الوطني العراقي ليتجاوز نطاق مواجهة التهديدات العسكرية وضمان حماية المواطن ووحدة وسلامة أراضيه وسيادته إلى مجالات أخرى تشمل الاستقرار السياسي والاقتصادي والانسجام الاجتماعي وسلامة البيئة.

المطلب الأول: ظهور الإرهاب السيبراني في العراق

قدمت وسائل الاتصالات وأنظمة المعلومات الحديثة خدمة غير مقصودة للتنظيمات الإرهابية في العراق، إذ استغلت تلك التنظيمات هذا التطور لخدمة أغراضها غير المشروعة وإتمام عملياتها الإجرامية، أي أن الفضاء السيبراني مثلَّ عنصر جذب مهم للتنظيمات الإرهابية على تعدد أنواعها واختلاف أيديولوجياتها، وذلك لأن تطور وسائل الاتصال وشبكات المعلومات ومختلف الإمكانيات العلمية والتقنية جعل استغلالها في تنفيذ العمليات الإرهابية أكثر سهولة لتميزها بالدقة والسرعة، كما أن استهداف تدمير وتخريب البنية التحتية الشبكة المعلومات الحكومية أو العامة للمؤسسات الاقتصادية والشركات، قد يتم بكلف كبيرة جداً تتجاوز الخسائر التي تكون نتيجة العمليات الإرهابية بشكلها التقليدي، والأخطر من ذلك إن الجماعات الإرهابية قد تنفذ عملياتها التخريبية وهي في أماكن بعيدة وآمنة (المعموري، ٢٠١٩، ١٠١).

منذ عام ٢٠٠٦ بدأ تسجيل إحصائيات رسمية عن الجرائم السيبرانية في العراق، بسبب الانتشار السريع للخدمات والعمليات عبر الأنترنت، فارتفعت معها نسبة جرائم الأنترنت والأنشطة المضرة بالنظام والمجتمع العراقي (الشمري، ٢٠٢١، ١٧١).

بالتزامن مع الحرب على تنظيم (داعش) الإرهابي منذ عام ٢٠١٤، رصدت شركات أمنية مختصة بالأمن السيبراني إن هناك حرباً سيبرانية في العراق يتم فيها استعمال وسائل التواصل الاجتماعي لحشد المؤيدين ونشر الدعاية ولجمع المعلومات الأمنية عن طريق مجموعة من قراصنة الأنترنت الذين يعملون على خداع الناس بإرسال رسائل تحوي شفرات وبرامج ضارة عبر وسائل التواصل الاجتماعي، وما أن يتم فحتها حتى يبدأ المهاجمون على الفور بالتحكم الكامل بالجهاز وسرقة الملفات أو استخدام كاميرا الكومبيوتر أو الميكرفون المراقبة ما يجري للشخص المستهدف. وفي هذا الخصوص قال أندرو كوماروف (Andrew) Komarov وهو الرئيس التنفيذي لشركة انتل كراولر (Intel Crawler)الأمريكية المختصة في مكافحة التهديدات السيبرانية إن هناك بعض الجماعات في العراق تستخدم برامج ضارة، ومن الصعب التأكد من هويتهم، وقد استهدفوا بالفعل مدناً وجماعات معينة وحتى عائلات معينة، أي أن كل الهجمات السيبرانية هي انتقائية للغاية وتتأثر في معظمها بالأطراف المحلية المتصارعة، وأضاف إلى إن المهاجمين يستهدفون ضحاياهم باستخدام وسائل التواصل الاجتماعي ويقومون أيضاً بالبحث عن أجهزة التوجيه في داخل العراق لتخريبها بأدواتهم الخاصة، وقد تركزت غالبية هذه الهجمات في بغداد والبصرة والموصل وأربيل، وكانت الغاية منها جمع المعلومات عن المظاهرات المحلية والأحزاب والاتصالات بين السكان المدنيين أو الحكومة والعكس بالعكس (الشمري، ٢٠٢١، ١٧٢).

تم ملاحظة أنه في الانتخابات العراقية لعام ٢٠١٨م، جرى نشر الكثير من التسجيلات الصوتية العمليات شراء مقاعد في مجلس النواب كذلك في عام ٢٠١٩م تعرض نحو ٣٠ موقع الكتروني للحكومة العراقية لحالة من الاختراق منها جهاز الأمن الوطني العراقي ووزارة الداخلية والصحة، وقد قام بعملية

الاختراق مجموعة تدعى (ماكس برو) وتسريب معلومات وبيعها تتعلق بالأمن الوطني العراقي (صالح، ٢٠٢٣، ٢٣٠).

في ٢٦ و٢٧ أيلول ٢٠١٩م كان العراق قد تعرض إلى هجوم سيبراني من قبل قراصنة طالت قرابة (٣٠) موقعاً حكومياً، أبرزها مواقع وزارة الدفاع والداخلية والخارجية والأمن الوطني والصحة، وقد استغل المهاجمون بعض الثغرات فعملوا على تطبيق التغييرات على بيانات موقع البحث التي من شأنها توجيه المستخدمين إلى صفحة بحث مختلفة، وعلى الرغم من أن الجهات الحكومية نجحت في استعادة سريعة لبعض المواقع إلا أن بعضها استغرق وقتاً أطول علماً إن المهاجمين تمكنوا من الدخول إلى أجهزة الحواسيب الحكومية واختراق قاعدة البيانات التي من المفروض أن تكون محمية بشكل جيد، مما سمح لهم بأخذ معلومات كثيرة (الشمري، ٢٠٢١، ١٧٤).

غالباً ما تم تعطل الصفحات الرسمية الخاصة بالوزارات الأمنية مثل وزارة الداخلية ومستشارية الأمن الوطني وجهاز مكافحة الإرهاب، ولعل أخطرها كان في ٢٥ تشرين الثاني ٢٠١٩ عندما تم اختراق الموقع الرسمي لجهاز مكافحة الإرهاب والإعلان عن انقلاب ضد الحكومة استجابة لدعوة المتظاهرين، إلا أن جهاز مكافحة الإرهاب أعلن في موقعه الرسمي لاحقاً عن تعرض الموقع للاختراق، وإن ما نشره فيهِ ليس صحيحاً (الحمزة، ٥٣٣).

المطلب الثاني: مظاهر الإرهاب السيبراني في العراق

تتمثل أبرز مظاهر الإرهاب السيبراني في العراق بالآتي:

أولاً: الابتزاز الإلكتروني، الذي يتم من خلال الحصول على معلومات سرية أو صور شخصية أو مواد فيدوية لاستغلالها لأغراض مالية أو القيام بأعمال غير مشروعة، وتعد تلك الأعمال من أشد الجرائم خطورة

لأنها تهدد حقوق الإنسان من خلال اختراق خصوصيته وتجعله عرضة للكثير من الآثار النفسية والاجتماعية، لقد راح عدد غير قليل من العراقيين، ولا سيما النساء منهم، كضحايا لعمليات الابتزاز الإلكتروني (السند، ٢٠١٨،١٨)، وذلك نتيجة التفاعل الكبير مع منصات التواصل الاجتماعي، فقد كشفت السلطات القضائية العراقية إن الأشهر الأولى من العام ٢٠٢٢ تم تسجيل نحو (٢٤٠٠) حالة ابتزاز الكتروني، وكان لبغداد النصيب الأكبر منها، بينما سجل العام ٢٠٢١ وفق إحصائية كشفت عنها مديرية الشرطة المجتمعية بوزارة الداخلية (١٩٥٠) حالة ابتزاز الكتروني، كان معظم ضحاياها من النساء بينهن فتيات في سن المراهقة وأطفال دون سن الـ(١٤) سنة (يقين، ٢٠٢٢).

ثانياً: التجسس الإلكتروني، أي القدرة على الدخول غير المشروع والاطلاع على شبكات الخصم من دون أن يصاحب ذلك تدمير أو تخريب للبيانات والمعلومات، بهدف الحصول على المعلومات التي قد تشمل خطط عسكرية دفاعية أو هجومية، أو مخططات سرية حربية كانت أم سلمية، أو دراسات وأبحاث استراتيجية، فضلاً عن استطلاعات سياسية واستخباراتية، كما يمكن من خلال هذه العملية إعداد خرائط لشبكات الحاسب الآلي واستعمالها مستقبلاً لتنفيذ عمليات إرهابية في الفضاء السيبراني، وتعد برامج التجسس نوع خاص من البرمجيات الخبيثة التي تعمل على مراقبة كل ما يكتب، إذ تقوم بتسجيل النقرات على لوحة المفاتيح وترسلها إلى المخترق وغيرها من الأعمال الخبيثة الأخرى، وتقوم هذه البرامج بتنفيذ مهامها عن طريق الاتصال بالشبكات الاجتماعية أو موقع ما على شبكة الأنترنت، وتقوم بجمع المعلومات حول ما يقوم به المستخدم من أنشطة سواء عبر الأنترنت أو في وضع عدم الاتصال بالإنترنت على الجهاز الخاص بالضحية وإرسال هذه المعلومات للمخترق فور اتصال الحاسب الآلي الأنترنت، على إن أهم ما يهدف إليه التجسس

الإلكتروني هو زعزعة الأمن ونشر الخوف والرعب والإخلال بالنظام العام للدولة وتهديد الأشخاص والسلطات العامة والمنظمات الدولية والسطو وجمع الأموال، فضلاً عن جذب الانتباه والدعاية والإعلان (اليوسف، ١٩٩٩، ١٥٥).

لقد كشفت صحيفة أمريكية عن أن هاتف الرئيس العراقي السابق (برهم صالح) كان على قائمة تضم (٥٠) ألف رقم اختيرت من أجل احتمال استهداف أصحابها بالمراقبة ببرنامج (بيغاسوس Pegasus) للتجسس، وذكرت صحيفة واشنطن بوست(Washington Post) إنه لم يتسن التحقق فيما إذا كان برنامج (بيغاسوس) الذي تنتجه شركة (إن إس أو) (NSO) الإسرائيلية قد أصاب هاتف (برهم صالح) أو ما إذا كانت قد نفذت أصلاً أي محاولة لذلك (الجزيرة، ٢٠٢١).

ثالثاً: الاختراق الإلكتروني، الذي يقوم به الإرهابيون المبرمجون، الذين يطلق عليه بـ(الهاكرز أو قراصنة الحاسوب) من خلال اختراق المواقع أو الحواسب الإلكترونية باستعمال برامج التجسس على الشبكات والأنظمة الإلكترونية، والاعتداء على البنية التحتية المعلوماتية للمؤسسات الحكومية والخاصة على حد سواء بما في ذلك البريد الإلكتروني، واشتراكات المستخدمين، والأرقام السرية للبطاقات الائتمانية وما إلى ذلك، وارتكاب جرائم الأتلاف والتشويه للبيانات والمعلومات وبرامج الحاسب الآلي بإطار جرائم الإرهاب الإلكتروني، يتم باستعمال الفايروسات الإلكترونية بقصد الحصول على معلومات متعلقة بالأماكن والمنشآت الحيوية لاستهدافها بالعمليات الإرهابية أو من أجل تدمير أو تعطيل في برامج الحواسيب، ومن الأساليب المستعملة لتدمير المواقع أيضاً ضخ كميات هائلة من الرسائل الإلكترونية إلى الموقع المستهدف بالتدمير

مما قد يؤثر على سعته التخزينية ويؤدي في نهاية المطاف إلى تفجير الموقع وتشتيت بياناته وانتقال معلوماته لجهاز الشخص الذي اخترقه (الصادق، ٢٠٠٩، ١٣٥).

تواريخ اختراق مواقع إلكترونية لوزارات عراقية بين عامي ٢٠١٦- ٢٠١٧

اسم الوزارة	تاريخ الاختراق
موقع رئيس الوزراء العراقي	2016/3/23
موقع مجلس النواب العراقي	2016/6/8
وقع الاستمارة الإلكترونية للتعيين على ملاك وزارة الصحة	2016/7/3
موقع وزارة الداخلية	2016/8/22
موقع وزارة الاتصالات	2016/10/11
الموقع الرسمي للمفوضية العليا المستقلة للانتخابات	2017/2/12
موقع وزارة الشباب والرياضة	2017/6/2

المصدر من إعداد الباحثة بالاعتماد على (التميمي وإسماعيل، ٢٠٢٠، ٢٠٨)

المطلب الثالث: التحديات التي تواجه الامن السيبراني في العراق

الأمن السيبراني في العراق يواجه تحديات هائلة نتيجة للتقدم التكنولوجي السريع والتحولات الكبيرة في مجال الاتصالات والمعلومات، فيعد هدفاً استراتيجياً للهجمات السيبرانية لضعف الأمان الإلكتروني في البنية التحتية الوطنية، تلك التحديات تتفاقم بسبب استخدام المؤسسات العراقية لخدمات خارجية تتيح للمعلومات المهمة تداولها في خوادم خارج الحدود الوطنية، مما

يفتح باباً لاختراقات واستخدامات غير مشروعة، ما ينتج عنها أعمال تجسسية أو حتى للمساس بأمان الدول الأخرى، ويمكن أيجاز عدداً من تلك التحديات:

أولا: ضعف البنية التحتية التكنولوجية

أن تهديدات الأمن السيبراني يمكن اعتبارها تحديات غير مرئية" تؤثر على منظومة الأمن الوطني العراقي ، فالتطور التكنولوجي الذي شهده العراق في مجال الاتصالات والمعلومات والذي تزامن مع ضعف البنية الأمنية الإلكترونية التحتية الوطنية سواء أكانت أمنية أو مصرفية أو شخصية، مما أدى إلى أن يصبح العراق منكشفاً إستراتيجياً لكثير من دول العالم، لاختراقه والتجسس على المعلومات الخاصة بالمؤسسات كافة، واستخدامه كساحة لشن الهجمات الإلكترونية لضرب أمن معلومات أي دولة كانت واختراقه ، فضلاً عن سرقة أي معلومة واستخدامها لأغراض المساومة، وتنفيذ العمليات الإرهابية، وأن أكثر المؤسسات العراقية تتعاقد لتجهيز معلوماتها من أقمار صناعية ذات مورد خدمة واقع خارج الحدود العراقية مما يؤدي إلى مرور تلك المعلومات في خوادم تلك الدول، ورجوعها إلى العراق ، إذ يشكل هذا الإجراء خرقاً لأمن المعلومات، إذ يجب تشكيل مجموع الأطر القانونية والتنظيمية والهياكل التنظيمية والتقنية والتكنلوجية حيث تمثل جهود مشتركة للقطاع العام والخاص محلياً وخارجياً وذلك لحماية الفضاء السيبراني العراقي والتركيز على ضمان توافر أنظمة للمعلومات وحماية سرية للمعلومات الخصوصية واتخاذ جميع الإجراءات اللازمة الحماية المواطن من مخاطر الفضاء السيبراني (التميمي، ٢٠٢٢، ١١-١٢).

ويشهد العراق بين الحين والآخر هجمات سيبرانية من قبل مجموعات متطرفة وهاكرز غير معروفين، تستهدف البنية التحتية الحكومية والقطاع الخاص، مما يؤثر سلبًا على الخدمات الحكومية ويعرض الأفراد والمؤسسات لمخاطر جرائم

الاحتيال وسرقة الهوية، ،إذ شهد العراق في الآونة الأخيرة استحداث ٣ أقسام متخصصة في دراسة الأمن السيبراني في جامعات رئيسية منها جامعة المستنصرية، والجامعة التقنية الشمالية، وجامعة الموصل وكذلك في جامعة المستقبل، وافتتاح فروع الأكاديميات دولية لتدريس الأمن السيبراني والحوسبة السحابية في العراق، وهو تطور إيجابي يسهم في تعزيز الكفاءات في هذا المجال (صليبي، ٢٠٢٤، ٢١٥).

ثانياً: ضعف تشريعات الأمن السيبراني

أن استخدام التقنيات المستحدثة للتحكم في المعلومات وأساليب تجميعها ومعالجتها واختزانها وتحسين الانتفاع منها من خلال الحاسبات وثورة الاتصالات والسرعة والتطور التكنولوجي في العراق والعالم، مع وجود فجوات قانونية في مجال الإنترنت تشكل تحدياً كبيراً، ففي ظل غياب معايير موحدة لقوانين الإنترنت، يصبح صعباً لاسيما عندما تتعلق المسألة بأفراد أو كيانات من دول مختلفة ويظهر الخلل بشكل واضح عندما يتورط الهجوم السيبراني في قضايا تجاوز الحدود أذ قد يقوم المهاجمون بتنفيذ هجمات إرهابية في بلد لا تكون فيه قوانين صارمة، مما يثير تحديات في مجال تنازع القوانين، وتكمن المشكلة الحقيقية في عدم وجود سلطة مركزية على مستوى دولي تعمل على تطبيق قوانين تحمي الخصوصية وتضمن الأمان الرقمي (المعموري، ٢٠١٩، ١٧)، إذا يصبح الحل لهذه التحديات هو التعاون الدولي الفعّال، وفي ظل غياب سلطة دولية مركزية، يزيد نشوء ظاهرة الإرهاب الإلكتروني فهي التحديات التي تواجه الأمان الوطني، ولحماية الخصوصية وضمان الأمان السيبراني، يجب وضع معايير وسياسات تنظيمية دولية تحدد التزامات يجب اتباعها في البيئة السيبرانية، لذلك أن الفجوات القانونية تجعل من الصعب إثبات الدليل المادي للاعتداءات السيبرانية، مما يجعل التحقيق والمساءلة أموراً

معقدة، ولكن يمكن أن تؤثر الهجمات السيبرانية على مستويات مختلفة، مما يبرز أهمية تنسيق الجهود الدولية لمواجهة هذه التحديات، ولتحقيق ذلك، يجب أن تلتزم الدول بالتعاون الدولي وتطوير إطار قانوني دولي ينظم الهجمات السيبرانية ويحدد العقوبات للمتورطين، وإن إقامة هياكل دولية تعمل على توحيد الجهود وتعزيز التعاون ستكون أساسية لتحقيق أمان الإنترنت ومواجهة التهديدات السيبرانية بفعالية (العلي، ٢٠٢٠، ٢٥).

لتحسين الأمان السيبراني في العراق، يلزم إصدار وتعزيز تشريعات فعّالة وشاملة تغطي جوانب متنوعة من الأمان السيبراني، بما في ذلك الوقاية من الهجمات، وتحقيق العدالة في حال وقوع الاختراقات، وتحديد العقوبات المناسبة للمخترقين، وفي جلسته بتاريخ ٢١ نوفمبر / ٢٠٢٣ طرح البرلمان العراقي مشروع قانون جرائم المعلوماتية، بعد فشل دورات المجلس السابقة في إقراره خلال العقد المنصرم، وعلى الرغم من التعديلات المتكررة على مشروع القانون، ومع التأكيد على أهمية تنظيم عملية التواصل الإلكتروني خصوصاً وأن العراق تأخر كثيراً في سن تشريع، ذلك القانون الذي تضمن ٣١ مادة يعود إلى عام ٢٠١١، فقد نصت المادة السادسة من القانون على "يعاقب كل من حاول استخدام شبكة المعلومات لتكدير الأمن والنظام العام بالسجن المؤبد أو بغرامة تتراوح بين (٢٥) و (٥٠) مليون دينار عراقي، أما المادة الثانية والعشرون تنص على الحبس لمدة سنتين ودفع غرامة لا تقل عن مليوني دينار ولا تزيد على خمسة ملايين دينار، لمن نسب إلى الغير عبارات أو أصوات أو صوراً تنطوي على القذف والسب من خلال شبكة المعلومات، وقد تم سحب ذلك المشروع من قبل الحكومة، لغرض إضافة بعض التعديلات عليه (صليبي، ٢٠٢٤، ٢١٥).

ثالثاً: غياب الأمن الإلكتروني

إن أكثر المؤسسات العراقية تتعاقد لتجهيز معلوماتها من الأقمار الصناعية ذات مورد خدمة واقع خارج الحدود العراقية الذي يؤدي إلى مرور تلك المعلومات في خوادم العديد من الدول ، ورجوعها إلى العراق إذ يشكل هذا الإجراء خرقاً لأمن المعلومات العراقي، فضلاً عن عدم قدرة المؤسسات العراقية على مواجهة الجريمة الإلكترونية أو السيبرانية، إذ انتشرت مؤخراً نوعية خطيرة من الهجمات والجرائم السيبرانية التي تعتمد على تقنيات وبرامج متقدمة كالجاسوسية الحسابية والذكاء الاصطناعي واختراق المواقع الرسمية والاحتيال المصرفي والصيد الاحتيالي للمعلومات (صكب، ٣٩٠)، وكان من بين ابرز هذه البرامج التي تهدد الأمن السيبراني العراقي "الفدية الخبيثة" والتي حذرت منها هيئة الأعلام والاتصالات العراقية فهو برنامج يعمل على حجب جميع المعلومات في أجهزة الحواسيب الحكومية والشخصية واستخدامها كأوراق ضغط وابتزاز مقابل مبالغ مالية كبيرة، وكذلك برنامج الهكر الأخلاقي وغيرها من البرامج، فضلا عن ذلك هناك العديد من المواقع الحكومية العراقية التي تتعرض الى الاختراق لاسيما بعد تعاقد وزارة الاتصالات مع شركات مشبوهة مثل سيمفوني وايرثلنك لتنفيذ مشروع الكابل الضوئي مما جعل الباب مفتوح لتهكير المواقع الحكومية وسرقة البيانات والمعلومات الحكومية والمؤسسات الخاصة (صكب، ٣٩١).

استطاعت الجماعات الإرهابية المتطرفة (القاعدة) و (داعش) على تسخير الشبكة الرقمية والفضائيات، للوصول الى الجماهير وتبرير وتسويغ العمليات الإرهابية والترويج للفكر الذي تتبناه وفي معظم المواقع يبدو التوظيف العاطفي اقوى من الحجج العقلية، مما مكن التنظيم من تجنيد الأشخاص على مستوى العالم، ففي مطلع عام ٢٠١٤ جاء تقرير للأمن البريطاني في صحيفة (ديلي ستار صندي) بأن البريطانيين يقاتلون مع تنظيم القاعدة في سوريا والعراق

ويتبادلون المعلومات وتجنيد الشباب للقتال عبر وسائل التواصل الاجتماعي (السبيعي، ٢٠١٥، ٥٥).

وتكمن أسباب جاذبية هذه المواقع للإرهابيين هي (بسيوني، ٢٠١٨، ٣٩-٤٣):

- قدرت الجماعات الإرهابية على تحقيق التواصل مع الآخرين بكل اللغات والثقافات لمختلف شعوب العالم، وبخصوصية عالية مع أمكانية تشكيل المنتديات الحوارية المتطرفة التي تقوم على منهج الأقناع مما يجعل هذه المواقع بيئة خصبة لتجنيد الإرهابيين.
- إقبال الشباب على وسائل التواصل يقابله عجز المؤسسات العراقية من الرقابة على التواصل بين أطراف الاتصال مما سهل عمليتي التثقيف والتجنيد.

أحد الأزمات التي يعانيها الأمن الوطني العراقي في ظل الاختراق السيبراني هو العجز عن حماية الفكر والمعتقدات والحفاظ على العادات والتقاليد والقيم الوطنية فالأمن الوطني يعني تمكين الشعب من ممارسة منظومة القيم الخاصة به على أرضه المستقلة، وهذا العجز أوجد حالة فراغ كبيرة بين العادات والتقاليد العراقية الأصيلة وثقافة الأجيال الشابة الناشئة والعجز الحكومي عن اتخاذ التدابير اللازمة.

رابعاً: عدم وجود هيئة مختصة بالأمن السيبراني

إذ لا توجد حالياً هيئة مستقلة للأمن السيبراني، على الرغم من ذلك نلاحظ إن العراق قد حاول أن يساير بعض الدول في موضوع الأمن السيبراني فأنشأ هيئة وحيدة للأمن السيبراني هي فريق الاستجابة السريعة للأحداث السيبرانية وهي هيئة تابعة لمستشارية الأمن الوطني التي هي ذاتها تفتقر لقانون ينظمها والفريق مازال في بداية تكوينه، كما أن موقعه الإلكتروني يتعرض للاختراق أكثر من مرة. وتتهمه بعض وسائل الإعلام بالفساد الإداري وإن أعضاؤه

يعملون في مكاتب خاصة تتقاطع مع عملهم في هذا الفريق، وعلى الرغم من أن الحكومة العراقية كانت قد حاولت تطوير عمل هذا الفريق حينما طلبت رسمياً من حلف شمال الأطلسي / الناتو تدريب أعضاء الفريق البالغ عددهم (١٦) موظفاً للمدة من ٢١ تشرين الثاني لغاية ٢ كانون الثاني ٢٠١٦، وكان البرنامج التدريبي قد تضمن جلسات نظرية ومختبرية عملية عن أساسيات الدفاع السيبراني وحماية البيانات من التسرب وتحليل الشفرات والأدلة الإلكترونية ورفع مستوى الخبرة التقنية لحماية الشبكة الوطنية وزيادة الوعي بالأمن السيبراني، وستعمل هذه الدورات على تعزيز قدرات الدفاع السيبراني الوطنية العراقية، إلا أن إمكانيات الفريق تبقى متواضعة قياساً بحجم التحديات التي يفترض به مجابهتها (الشمري، ٢٠٢٢، ١٧٥).

في عام ٢٠١٧، أصدر فريق الاستجابة السريعة للأحداث السيبرانية، ما أسماه بـ (استراتيجية الأمن السيبراني العراقي (ICS) في (١١) صفحة، وعلى الرغم من أن نشر هذه الوثيقة يُعد خطوة يجدر الإشادة بها لأنها تعرض للأولويات المتزايدة للمجال السيبراني كما أنها كانت بمنزلة أول جهد كبير وعام تبذله الدولة العراقية، من أجل تحليل مكامن الخلل في السياسة الإلكترونية الوطنية، ولرسم خريطة طريق لتأسيس بنية تحتية الكترونية فوقية للبلاد لوضع العراق على قدم المساواة مع نظرائه الإقليميين والدوليين وحلفائه، إلا أن الاستراتيجية ذاتها يشوبها عيوب واضحة، إذ أنها فشلت بالعموم، في تحفيز تطبيق الإطار الذي يقترحه، فكانت استراتيجية الأمن السيبراني المنشورة استراتيجية نظرية بالأساس، وتوضح تفصيلاً التهديدات العامة التي تواجه الجهات الفاعلة الخاصة والعامة في الفضاء السيبراني، بدلاً من التركيز على طبيعة التهديدات الإلكترونية التي يواجهها العراق خصوصاً، ومن ثم، لم تحاول

الاستراتيجية توفير ما يمكن عده تحليلاً أو مخططاً ملموساً لتصنيف البنية التحتية الحيوية التي يمكن أن تكون موضع استهداف متكرر(شبر، ٢٠٢٢).

من جهة ثانية، فإن استراتيجية الأمن السيبراني كانت قد تضمنت ما يفترض أنه يمثل جوهر سياسة الدولة المتعلقة بحماية الأمن السيبراني، فإنه يلاحظ بأن فريق الاستجابة السريعة للأحداث السيبرانية، لم ينشر ذلك الاستراتيجية في موقعه، وإنما الورقة متاحة فقط على موقع الاتحاد الدولي للاتصالات ضمن قسم تقارير الدولة، وكان الفريق أراد منها فقد إظهار رسالة للعالم مفادها وجود جهاز أمن سيبراني في العراق من غير اهتمام حقيقي بالموضوع، والاستراتيجية جاءت مخيبة للآمال كثيراً إذ لم تتضمن طبيعة المشاكل وتحديد المهام التي يجب إنجازها لتعزيز الأمن السيبراني، إذ ورد فيها عبارات عامة تشير إلى التمني والرغبة وليس سياسة جادة لمواجهة المشكلة، كعبارة ضرورة أنشاء قوانين سيبرانية جديدة مثل قانون أمن الاتصالات وعبارة (ضرورة أنشاء منصة مركزية للعمل السيبراني) و (العمل على سد الفجوة الأمنية السيبرانية) (شبر ٢٠٢٢).

ومن جهة ثالثة، كانت استراتيجية الأمن السيبراني العراقي قد تضمنت مدد زمنية تتراوح بين عام وخمسة أعوام لإنجاز المهام أعلاه، غير أنها لم تبين من هي الهيئة المكلفة بإنجاز كل هذه المهمات الصعبة في ظل عدم وجود قانون للأمن السيبراني أو هيئة مستقلة له أو حتى بنية تحتية لهذا المشروع، وكيف يمكن إنشاء قوانين سيبرانية في وقت لم تتم المصادقة على قانون الجرائم المعلوماتية المطروح على مجلس النواب منذ أكثر من ١٠ سنوات، بالإضافة إلى ذلك فشلت الوثيقة في تحديد الجهة أو المؤسسة الحكومية التي ستكون مسؤولة عن تنفيذ توصياتها أو خططها أو أهدافها، كما أنها لم تقدم برامج استراتيجية مفصلة أو مدد تنفيذ للاستراتيجية المذكورة، لذا نحن مع الرأي القائل

بأن هذه الاستراتيجية هي رؤية غير واقعية ولا يمكن الركون إليها لتحقيق الأمن السيبراني العراقي وهي إن دلت على شيء فتدل على انعدام رؤية واضحة للأمن السيبراني في العراق (صالح، ٢٠٢٣، ٢٤١).

المطلب الرابع: سبل معالجة الإرهاب السيبراني في العراق

لتلافي العديد من الخروقات التي تتعرض لها حركة المعلومات في العراق وما لها من انعكاسات خطيرة على منظومة الأمن الوطني العراقي في جميع المجالات الاقتصادية والأمنية والثقافية لذا يتوجب على المؤسسات العراقية أن تشكل مجموعة من الأطر القانونية والتنظيمية، فضلاً عن الوسائل التقنية والتكنولوجية والتي تمثل الجهود المشتركة للقطاعين الخاص والعام، وخلق تعاون فعال بين الداخل العراقي والمحيط الاقليمي يهدف إلى حماية الفضاء السيبراني الوطني، مع التركيز على ضمان توافر أنظمة المعلومات، وحماية سرية المعلومات الشخصية، واتخاذ جميع الإجراءات الضرورية لحماية المواطنين من مخاطر الفضاء السيبراني، لذا على الحكومة إن تتحرك بثلاث مستويات وهي الاتي :

- **على المستوى الداخلي** : لغرض الحفاظ على الامن الوطني من الهجمات السيبرانية الخطيرة نحتاج الى أفضل الوسائل التكنولوجية من أجل مقاومة الاختراقات والتخريب وضرورة الاطلاع على افضل الطرق لحماية الأمن الوطني بشموليته، وحماية البنية المعلوماتية لكل المؤسسات، إضافة لعمليات التدريب والتثقيف والتوعية، فهذا يعني تكاليف عالية لا يمكن لمؤسسات فردية أن تتحملها، وهنا كانت ضرورة أنشاء الهيئات الوطنية للأمن السيبراني، فمن خلالها يمكن التوجه أيضا لصناعة استراتيجية وطنية للأمن السيبراني تعمل على تعزيز المنظومة المتكاملة للأمن من خلال تنفيذ عدد من المبادرة ضمن

سقف زمني محدد، وتهدف الى خلق بيئة سيبرانية آمنة وصلبة تساعد على تمكين الأفراد من تحقيق طموحاتهم، وتمكن المؤسسات الحكومية والخاصة من التطور والنمو في بيئة امنه مزدهرة (جويسي، ٢٠١٥، ٥)، تعمل الاستراتيجية إلى دعم معايير الأمن الإلكتروني بالدولة عبر آليات ومحاور مختلفة أهمها (صكب، ٣٩٣):

١. تصميم وتنفيذ إطار قانوني وتنظيمي شامل لحماية الأمن السيبراني ومعالجة جميع أنواع الجرائم السيبرانية، وبناء إطار تنظيمي لحماية التقنيات الحالية والناشئة، ووضع أنظمة داعمة لتمكين الشركات الصغيرة والمتوسطة وحمايتها من التهديدات السيبرانية.

٢. النهوض بثقافة وطنية للأمن السيبراني عبر زيادة وعي أفراد المجتمع بأهمية الأمن السيبراني والمخاطر المتعلقة بالإنترنت، وتشجيع اتباع الممارسات الآمنة في التعامل مع التقنية، وتشجيع المؤسسات على نشر الوعي السيبراني بفاعلية والعمل على مبدا الثواب والعقاب، وتخصيص مكافأة التميز في مجال الأمن السيبراني عبر برامج الجوائز الوطنية، وتشجيع المؤسسات على إطلاق برامج حول الأمن السيبراني، والهام رواد الأعمال الابتكار في المجال، ودعم الأبحاث الخلاقة في المؤسسات الأكاديمية، وتنشيط تشجيع الطلبة على الانخراط في مجال الأمن السيبراني.

٣. وضع اليات وطنية فعالة للاستجابة للحوادث السيبرانية لتمكين الاستجابة السريعة والمنسقة في الدولة عبر تنظيم آلية الكشف عن حوادث الأمن السيبراني وفق معايير منهجية موحدة لتقييم درجة خطورة الحوادث

٤. إقامة تعاون على المستوى الوطني بين الحكومة ومجتمع صناعة الاتصالات والمعلومات.

- **على المستوى الاقليمي** في ظل التطورات الكبيرة التي طرأت على الامن الوطني، أصبح من الصعب على أي دولة تحقيق أمنها الوطني دون تعاون إقليمي، لذا على الحكومة العراقي التعاون إقليمياً مع عدد من الدول ذات التجارب الناجحة في تحقيق الأمن السيبراني، وان يكون هذا التعاون ضمن أطر مؤسساتية تابعة لجامعة الدول العربية، وما على العراق سوى التوقيع على اتفاقية عام ٢٠١٨ العربية لحماية الفضاء السيبراني التي اعدها المركز العربي للبحوث القانونية والقضائية في مجلس وزراء العدل العرب والذي ضمن تشكيلات جامعة الدول العربية (صكب، ٣٩٤).
- **على المستوى الدولي** : تنطلق عملية التعاون الدولي لتحقيق الأمن من فكرة الأمن الجماعي التي طرحها وزير الخارجية الأمريكي (جون فوستر دلس) والتي يعني بها مسؤولية جميع الدول عن تحقيق الأمن والالتزام التصدي لأي عدوان تتعرض له دولها منفردة أو مجتمعة، لذا تبذل العديد من الدول والهيئات الدولية جهوداً حثيثة تؤكد على حامية الأمن السيبراني، فعلى العراق إن يعمل متعاونا مع هذه الهيئات لكبح الجرائم السيبرانية التي تحدث داخل مؤسساته من قبل الاختراق الخارجي، وفي مقدمه هذه الهيئات ، الاتحاد الدولي للاتصالات ، إذ يخصص جزءاً أساسيا من برامجه وخطط عمله المختلفة لتحقيق الأمن السيبراني، وكذلك تعاملت الأمم المتحدة مع تقنيات المعلومات والاتصالات(جبور، ٢٠٢١، ٧)، لاسيما فيما يتعلق بالأنترنت من منطلق كونها أداة للتنمية الاجتماعية والاقتصادية ووسيلة ناجحة في السعي الى تحقيق أهداف الألفية، وعليه فقد أوكل المجلس الاقتصادي الاجتماعي لمتابعة قضايا التنمية المتعلقة بالأنترنت، في المقابل تهتم اللجنة الخاصة بالعدالة الجنائية ومنع الجريمة الموكلة بمتابعة الجهود الدولية في مكافحة ومنع الجرائم الوطنية والعابرة للحدود ، بالقضايا المتعلقة بجرائم الأنترنت، وكذلك يمكن للعراق التعاون مع المجلس

الأوروبي، الذي اقر معاهدة مكافحة الجريمة السيبرانية، التي دخلت حيز التنفيذ، سنة ٢٠٠٤، داعياً جميع الدول الى التوقيع عليها، منذ تاريخ إقرارها في العام ٢٠٠١ وتعد أحكام هذه المعاهدة منسجمة مع متطلبات مكافحة الجريمة السيبرانية، لاسيما وانها تطلب من الدول الأعضاء أنشاء مراكز اتصال تعمل بحسب مبدأ استمرارية الخدمة أي تأمين متابعة على امتداد ساعات اليوم، إذ تكون دائمة الاستعداد للتجاوب مع الطلبات القادمة من خارج الحدود الجغرافية، وللتعاون مع القوات المعنية بمكافحة الجريمة بسرعة وفعالية، ويأتي في هذا السياق أيضاً التزام الدولة في حال كونها مصدر الفعل الجرمي الملاحق، الاحتفاظ بالبيانات الخاصة بحركة الاتصالات، والكشف عنها الى الدولة التي تطلب ذلك نتيجة وقوع نتائج الجرم فيها، ويعني ذلك ضرورة وضع عدد من التشريعات الخاصة التي تسمح بتسهيل عمليات البحث والاستقصاء والمتابعة ووضع اليد على معلومات الاتصالات وإدخال التعديلات اللازمة على القوانين الجزائية إذ تأتي منسجمة مع متطلبات تسليم المطلوبين من العدالة وتبادل المعلومات(جبور، ٢٠٢١، ٧-٨).

الخاتمة:

في ظل التطورات السريعة للتكنولوجيا والتحولات الرقمية، يظل الأمن السيبراني في العراق أمراً حاسماً لضمان استدامة التقدم والازدهار، ويتطلب هذا التحدي تبني استراتيجيات شاملة لتعزيز القدرات السيبرانية وحماية المعلومات والبنية التحتية الرقمية، ومن المهم تعزيز التعاون الدولي وتبادل المعلومات لمكافحة التهديدات السيبرانية العابرة للحدود، وتعزيز القدرة على التصدي للهجمات المتقدمة، ويجب تعزيز الوعي والتدريب للمواطنين والكوادر العاملة لتكون قوة فاعلة في حماية الأمان السيبراني، مع استمرار التحديات، يتعين

على العراق أن ينظر إلى مجالات الفرص المتاحة، مثل تطوير صناعة الأمان السيبراني واستثمار الشباب في مجالات الابتكار وتطوير التقنيات السيبرانية المتقدمة، ويكمن مستقبل الأمن السيبراني في تحقيق توازن بين التحديات الحالية واستغلال الفرص المستقبلية، مما يمكن العراق من أن يكون لاعباً فاعلاً ومبتكراً في عالم الأمن السيبراني المتطور.

التوصيات:

هنالك عدة توصيات لتعزيز الأمن السيبراني في العراق:

١. تطوير البنية التحتية السيبرانية: يجب على الحكومة العراقية الاستثمار في تحديث وتعزيز البنية التحتية السيبرانية لتكون قوية ومتقدمة تحسين أمان الشبكات وتعزيز الحماية من هجمات القرصنة والاختراق.

٢. تعزيز التشريعات والسياسات: ينبغي تطوير وتعزيز التشريعات والسياسات ذات الصلة لتكون أكثر فعالية في مكافحة الجرائم السيبرانية، بما في ذلك فرض عقوبات صارمة على المتسللين والمخترقين.

٣. تعزيز التعاون الدولي: دعم التعاون الدولي لمواجهة التهديدات السيبرانية، من خلال مشاركة المعلومات والخبرات مع دول أخرى والانضمام إلى مبادرات دولية لتحسين الأمن السيبراني.

٤. تعزيز الوعي والتثقيف: يجب تعزيز الوعي بأمن الإنترنت ومخاطر الهجمات السيبرانية بين المواطنين والكوادر العاملة من خلال حملات توعية وبرامج تثقيفية.

٥. تطوير قدرات الموارد البشرية: يتعين تعزيز تدريب وتطوير قدرات الكوادر البشرية لفهم التهديدات السيبرانية والاستجابة الفعالة لها.

قائمة المصادر:

١. الدليمي، إبراهيم مصحب. (٢٠٠٣). المخدرات والأمن القومي العربي: دراسة من منظور سوسيولوجي. دراسات استراتيجية، العدد (٨٤)، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي.
٢. الياسري، علي عبد العزيز. (٢٠١٠). الأمن القومي العراقي: الأبعاد الفكرية السياسية لاستراتيجية الأمن القومي في العراق. بغداد، العراق.
٣. الشقها، فهد بن محمد. (٢٠٠٤). مجلس وطني: تصور شامل. الرياض، السعودية: مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية.
٤. الوندي، بشير. (٢٠١٣). مجلس إيران: دور المجلس في استتباب الأمن. بيروت، لبنان: دار الهور.
٥. روبنسون، بول. (٢٠٠٩). قاموس الأمن الدولي. أبو ظبي، الإمارات العربية المتحدة: مركز الإمارات للدراسات والبحوث الاستراتيجية.
٦. شيبي، الخميسي. (٢٠١٠). الأمن الدولي والعلاقة بين منظمة حلف شمال الأطلسي والدول العربية بعد الحرب الباردة (١٩٩١–٢٠٠٨). القاهرة، مصر: المكتبة المصرية للنشر والتوزيع.
٧. عبد الرحمن، صالح بن علي. (٢٠١٧). الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت: رؤية ٢٠٣٠. المملكة العربية السعودية: هيئة الاتصالات وتقنية المعلومات.
٨. يعقوب، توامي. (٢٠١٣). أثر استخدام تكنولوجيا المعلومات والاتصال على الأداء المالي للمؤسسة الاقتصادية: دراسة حالة (رسالة ماجستير غير منشورة). جامعة قاصدي مرباح، الجزائر.
٩. عبد الصادق، عادل. (٢٠٠٩). الإرهاب الإلكتروني: القوة في العلاقات الدولية نمط جديد وتحديات مختلفة. القاهرة، مصر: مركز الدراسات السياسية والاستراتيجية بالأهرام.
١٠. مباركة، سليماني. (٢٠١٧). الاتحاد الإلكتروني للشمس ومحرمته. مجلة حقوق الاتحاد الشمسي، العدد (٨).
١١. الشمري، حازم حمد. (٢٠٢٢). إحياء الثقافة السيبرانية في المؤتمرات الدولية: الولايات المتحدة الأمريكية. بغداد، العراق: المجلس الوطني للعلوم الاجتماعية.
١٢. مهدي، لبنى خميس، & صفاء، تغريد. (٢٠٢٠). أثر السيبرانية في تطور القوة. مجلة حمورابي، العدد (٣٤).

١٣. عبد الصادق، عادل. أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني. الإسكندرية، مصر: المركز العربي لأبحاث الفضاء.
١٤. عبد الحي، وليد، وآخرون. (٢٠١٥). فهم الأمن القومي الجزائري من مدخلي الأمن الوطني والدفاع الوطني. عمان، الأردن: دار الحامد للنشر والتوزيع.
١٥. شاكر، فراس جمال. (٢٠٢٣). الحروب المعلوماتية في المجال الأمني والعسكري: أمريكا والصين. القاهرة، مصر: العربي للنشر والتوزيع.
١٦. الشهري، حنان بنت شعشوع. صحة استخدام شبكات التواصل الإلكتروني على الاتصالات الاجتماعية، جامعة الملك عبد العزيز، السعودية.
١٧. المطيري، خالد ظاهر عبد الله جابر. (٢٠٢٢). دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي. مجلة البحوث الفقهية والقانونية، العدد (٣٨).
١٨. https://jlr.journal.ekb.eg
١٩. المعموري، إبراهيم. (٢٠١٩). الأمن السيبراني وأثره في الأمن الوطني العراقي بعد العام ٢٠٠٣ (رسالة ماجستير غير منشورة). كلية العلوم السياسية، جامعة بغداد، العراق.
٢٠. هادي، صلاح مهدي، إسماعيل، زيد محمد علي. (٢٠٢٠). الأمن السيبراني كمرتكز جديد في الاستراتيجية العراقية. مجلة قضايا سياسية، العدد (٦٢)، كلية العلوم السياسية، جامعة النهرين، بغداد، العراق.
٢١. اليوسف، عبد الله. (١٩٩٩). التقنية والجرائم المستحدثة: الظواهر الإجرامية وسبل معالجتها. الرياض، المملكة العربية السعودية: أكاديمية نايف العربية للعلوم الأمنية.
٢٢. السند، عبد الرحمن بن عبد الله. (٢٠١٠). وسائل الإرهاب الإلكتروني: حكمها في الإسلام وطرق مكافحتها.
٢٣. قناة الجزيرة. (٢٠٢١، ٢١ يوليو). رئيس العراق على قائمة أهداف برنامج التجسس الإسرائيلي. تم الاسترجاع من: www.aljazeera.net
٢٤. التميمي، ظفر عبد مطر. (٢٠٢٢). العراق والأمن السيبراني: الفرص والتحديات. مجلة واسط للعلوم الإنسانية والاجتماعية، المجلد (١٨)، العدد (٥١)، جامعة واسط، العراق.
٢٥. العلي، مروان سالم. (٢٠٢٠). التحديات الاستراتيجية للأمن الوطني العراقي في ظل المتغيرات الدولية. مجلة تكريت للعلوم السياسية، المجلد (٢)، العدد (٢٠).

٢٦. بسيوني، عبد الحميد. (٢٠١٨). الديمقراطية الإلكترونية. القاهرة، مصر: دار الكتب العلمية.
٢٧. السبيعي، سعد بن عبيد. (٢٠١٤). الإعلام الجديد ودوره في تعزيز الأمن في المملكة العربية السعودية: دراسة تطبيقية. جامعة نايف العربية للعلوم الأمنية.
٢٨. شهر، هاشم.. تنظيم الجهد المؤسسي والوزاري المشترك إزاء الأمن السيبراني في العراق. مركز البيان للدراسات والتخطيط.
٢٩. جيوسي، زياد. (٢٠١٥). الهيئة الوطنية للأمن السيبراني الأمثل لحماية الأمن الشخصي. في المؤتمر الخامس لأمن وسلامة المعلومات في الفضاء السيبراني، مؤتمر الأيام العربية للأمن السيبراني، بيروت، لبنان
30. Mahmoud, Khalid Walid. (2013). Cyber Attacks: The Electronic Battlefield. Arab Center for Research and Policy Studies.