دور الأمن السيبراني في مكافحة الإرهاب في العراق

م.م. مينا حاتم محمد

جامعة النهرين / كلية العلوم السياسية

الملخص

مما لا شك فيه ان الامن الركيزة الأساسية للمجتمع، وقد تحول الأمن، مع بروز مجتمع المعلومات، والفضاء السيبراني الى واحد من قطاعات الخدمات التي تشكل دعامة أساسية، الأنشطة الفاعلين الدوليين وغير الدوليين على السواء، كما هو الحال مع التطبيقات الخاصة بالحكومة الالكترونية، والصحة الالكترونية، والتعليم عن بعد، والاستعلام، والتجارة الالكترونية وغيرها فاصبح الأمن السيبراني في عالمنا المعاصر أكثر من كونه مسألة مرتبطة بأمن المعلومات والتقنيات وشبكات الحاسوب بحكم علاقته المباشرة بالمجال السياسي والأمني والاقتصادي والاجتماعي والثقافي، إذ تعتمد معظم إن لم تكن جميع المؤسسات الحيوية لأي دولة على تقنيات المعلومات في عملياتها اليومية التي تعتمد بدورها على أنظمة الاتصالات والمعلومات وهذا يعني بالنتيجة أنها تعتمد على الأمن السيراني وقد أدى التطور السريع للفضاء السيبراني بحكم الاستعمال الواسع جدا للأفراد والمنظمات المحلية والإقليمية والدولية والمؤسسات الحكومية وغير الحكومية إلى تنامي أهميته الحيوية، مما جعل الاستغناء عنه أمرا محالا ، وعليه تأتي أهمية الأمن السيبراني في العراق كونه أصبح يمثل عنصر مهم في الحياة الانسانية على المستويات كافة اذ ان الانفتاح الذي شهده العراق في تكنولوجيا المعلومات والاتصالات في ظل التطور التكنولوجي المتنامي وعلى الرغم من المزايا التي تركتها وسائل الاتصال الحديثة ألا أن ذلك تزامن مع عدم وجود بنية تحتية متكاملة ومؤمنة لأنظمة المعلومات سواء كانت أمنية او مصرفية او شخصية أدى الى ان يكون العراق ساحة مفتوحة للكثير من دول العالم ودول الجوار الإقليمية، للاختراق والتجسس على المعلومات الخاصة بالمؤسسات الأمنية العراقية وان الأمر الأخطر من ذلك استغلال القضاء السيبراني من قبل التنظيمات الإرهابية اذ أصبح القضاء السيبراني حاضنة لبروز نوع وإشكال جديدة من الإرهاب فأصبح لتلك التنظيمات الإرهابية الآلاف من الصفحات والمواقع الالكترونية التي تستخدمها، وبرزت الحاجة إلى الاهتمام والتطور بالأمن السيبراني كمفهوم حديث في العراق من أجل قيام الدولة بوضع استراتيجية أمنية وطنية ومن اجل ضمان الأمن السيبراني لأنه أصبح جزء من الأمن الوطني في العراق.

Abstract

There is no doubt that security is the basic pillar of society, and security has transformed, with the emergence of the information society and cyberspace, into one of the service sectors that constitute a basic pillar of the activities of international and non-international actors alike, as is the case with applications for e-government and e-health. , distance education, inquiry, electronic commerce, and others. Cybersecurity in our contemporary world has become more than an issue related to the security of information, technologies, and computer networks by virtue of its direct relationship to

the political, security, economic, social, and cultural sphere, as most, if not all, of any country's vital institutions depend on information technologies. In its daily operations, which in turn depend on communications and information systems, this means, as a result, that they depend on cyber security. The rapid development of cyberspace, due to the very widespread use of individuals, local, regional and international organizations, and governmental and non-governmental institutions, has led to its growing vital importance, which has made it impossible to dispense with it. Therefore, The importance of cybersecurity in Iraq comes from the fact that it has become an important element in human life at all levels, as the openness that Iraq witnessed in information and communications technology in light of the growing technological development and despite the advantages left by modern means of communication, this coincided with the lack of infrastructure. Integrated and secure information systems, whether security, banking, or personal, have led to Iraq being an open arena for many countries of the world and neighboring regional countries, to hack and spy on information related to Iraqi security institutions. What is more dangerous than that is the exploitation of the cyber judiciary by terrorist organizations, as the cyber judiciary has become An incubator for the emergence of a new type and form of terrorism. These terrorist organizations have thousands of pages and websites that they use, and the need has emerged for attention and development in cybersecurity as a modern concept in Iraq in order for the state to develop a national security strategy and in order to ensure cybersecurity because it has become part of national security in Iraq.

أهمية البحث:

في ظل الأوضاع الأمنية غير المستقرة التي يشهدها العراق خصوصا ومنطقة الشرق الأوسط عموماً، ومع تسارع التطورات التكنولوجية الكبيرة التي يشهدها عالم اليوم ، لم تعد سياسات الدفاع والأمن العراقية مقتصرة على مكافحة الأرهاب وحماية سيادته والمحافظة على استقراره ووحدته من خلال الاعتماد على الطرق التقليدية فقط، بل تجاوزتها لتشمل حماية أمن المجتمع و الدولة من التهديدات التي أفرزتها الثورة التكنولوجية المعلوماتية المعاصرة، وذلك يتطلب تحقيق الأمن السيبراني باعتباره من أولويات السياسة الدفاعية العراقية.

اهداف البحث

يهدف البحث إلى:

- بيان مفهوم الأمن السيبراني وبعض المفاهيم المقاربة وكذلك مفهوم الإرهاب ومكافحة الإرهاب والإرهاب السيبراني.

- التعرف على استراتيجية الأمن السيبراني العراقي و كيفية استغلال التنظيمات الإرهابية للقضاء السيبراني التعرف على الوسائل الأمنية المتخذة لمكافحة الإرهاب في مجال الأمن السيبراني.

- بيان المشكلات والمعوقات التي يعاني منها الأمن السيبراني في مجال مكافحة الإرهاب في العراق.

إشكالية البحث :

ينطلق البحث من اشكالية مفادها ما هو الإرهاب؟ وما هو الإرهاب السيبراني؟ وما هو الأمن السيبراني؟ وما هي إستراتيجية الأمن السيبراني في العراق؟ وكيف تستخدم التنظيمات الإرهابية (داعش) الأمن السيبراني ؟ وهل هناك إجراءات امنية على وفق الأمن السيبراني في مكافحة الإرهاب في العراق ؟ وما هي الاهداف والوسائل والمعوقات الأمن السيبراني في العراق وما هو ودوره في مكافحة الإرهاب ؟

فرضية البحث :

هناك دور مهم وبارز للأمن السيبراني في العراق الذي أصبح كجزء جديد من استراتيجية الأمن الوطني وله دور مهم في مكافحة الإرهاب والتهديدات الالكترونية التي يوجهها العراق من قبل التنظيمات الإرهابية (داعش) وهناك عدة أهداف ووسائل تدعم استراتيجية مكافحة الإرهاب وفق الأمن السيبراني، ولا يخلو الأمن السيبراني من المشاكل والمعوقات التي يواجهها في العراق وفي ظل مكافحة الإرهاب.

حدود البحث

- **حدود الزمان:** يقتصر البحث على الفترة الزمنية من ٢٠٠٣ الى ٢٠١٧.

- **حدود المكان:** يقتصر البحث على العراق.

منهجية البحث :

اعتمدت الباحثة على المنهج الاستقرائي فضلا عن استخدام مقتربات وطرائق للوصول الى التكامل المنهجي ومنها المقترب الوصفى والمقترب التحليلي كونه يعمل على وصف الظاهرة ومن ثم تحليلها وفق مؤشرات علمية.

هيكلية البحث:

لقد قسمنا هيكلية البحث الى مقدمة وخاتمة وثلاثة محاور قسمنا المحور الأول وهو المحور المفاهيمي من ثلاث مطالب جاء المطلب الأول لبيان مفهوم الأمن السيبراني، أما المطلب الثاني فكان لبيان مفهوم الإرهاب والمطلب الثالث ناقشنا مفهوم الإرهاب السيبراني اما المحور الثاني فجاء بمطلبين ناقش المطلب الأول إستراتيجية الأمن السيبراني في العراق وجاء المطلب ثاني لبيان كيفية استخدام الأمن السيبراني من قبل التنظيمات الإرهابية في العراق (داعش أنموذجا) أما المبحث الثالث فجاء بثلاث مطالب ناقش المطلب الأول الإجراءات الأمنية المتحدة في مجال الأمن السيبراني لمكافحة الإرهاب في العراق . اما المطلب ثاني فتحدثنا عن الأهداف والوسائل الداعمة لنجاح إستراتيجية مكافحة الإرهاب في العراق على وفق الأمن السيبراني وفي المطلب ثالث والأخير ناقشنا المعوقات والمشاكل التي يعاني منها الأمن السيبراني لمكافحة الإرهاب في العراق.

المحور الاول

المطلب الأول: مفهوم الأمن السيبراني

الأمن السيبراني لغة لابد لنا ان نتعرف على أصل ومعنى كلمة سيبراني، التي تعتبر ترجمة حرفية لكلمة Cyber والمشتقة من كلمة Cybernetic استخدمت في الماضي للدلالة على كيفية تواصل الآلات والكائنات الحية مع بعض وتحكمها ومن تلك الكلمة نشأت مصطلحات كثيرة استخدمت في قصص وافلام او الفضاء لخيال العلمي Cyberspace مثل مصطلح السيبراني والذي يستخدم عادة للإشارة الى الانترنيت وشبكات الاتصال وكأنها فضاء وهمي او افتراضي الأمن السيبراني اصطلاحا[١]، وكما عرفة الاتحاد الدولي للاتصالات عبارة عن مجموعة الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الالكترونية، ونظم الاتصالات والمعلومات التي تحتويها، وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات، وتعزيز حماية وسرية وخصوصية البيانات الشخصية، واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني[٢]، وعليه قدمت وزارة الدفاع الأمريكية " البنتاغون" تعريفا لمصطلح الأمن السيبراني، إذ اعتبرته على انه جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها الالكترونية والمادية من مختلف الجرائم، والهجمات والتخريب، والتجسس والحوادث[٣]، وكذلك يعرف "اريتشارد تمرر" الأمن السيبراني، بانه عبارة عن وسائل دفاعية من شانها

كشف وإحباط المحاولات التي يقوم بها القراصنة، بينما عرفه "ادوارد مورسو" على أنه، وسائل من شانها الحد من خطر الهجوم على البرمجيات او أجهزة الحاسوب أو الشبكات وتشمل تلك الوسائل المستخدمة في مواجهة القرصنة وكشف الفيروسات. ويعرفه الاتحاد الدولي للاتصالات في تقريره حول اتجاهات الإصلاح في الاتصالات للعام (٢٠١٠-٢٠١١) هو مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات امنية ومبادئ توجيهية لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين[٤]، وبناء على ما تقدم يمكن تعريف الأمن السيبراني، بانه النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات ويضمن إمكانات الحد من الخسائر والأضرار التي تترتب في حال تحقق المخاطر والتهديدات كما يتيح أعادة الوضع الى ما كان علية بأسرع وقت ممكن، بحيث لا تتحول الأضرار الى خسائر دائمة ان الحصول على قدر كاف من أمن المعلومات (لمواجهة مخاطر التكنولوجيا والمعلومات امر ضروري للأداء السليم للحكومات والمنظمات أي انه مجموعة الآليات والإجراءات والوسائل والأطر التي تهدف إلى حماية البرمجيات وأجهزة الكمبيوتر من مختلف الهجمات والاختراقات التي قد تهدد الأمن القومي[٥]، وتوجد بعض المفاهيم المقاربة للأمن السيبراني ومنها القضاء السيبراني هو المكان الذي أوجدته تكنولوجيا المعلومات والاتصالات، وفي مقدمتها الأنترنت، ويرتبط الفضاء السيبراني ارتباطا وثيقا بالعالم المادي، عبر البنى التحتية المختلفة للاتصالات والأنظمة المعلوماتية، وعبر العديد من الخدمات التي لم يكن بالإمكان الحصول عليها من دونه[٦].

المطلب الثاني: مفهوم الإرهاب

الإرهاب لغة تعني الخوف والفزع والرهبة، وهي من رهب رهبة يرهب ورهبا بالضم ورهبا بالتحريك أي إخافة ورهب الشيء رهبة رهبا خاف فيقال رهبوت خير من رحموت باعتبار الترهيب خير من أن ترحم، وأيضا أرهبه واسترهبه وتوعده رهب اي خاف أو منع تحرز التي تشير في اللغة العربية إلى الخوف المشوب والفزع، والرهبة في اللغة العربية تستخدم للدلالة على الخوف المقترن بالاحترام أو الذي يختلف بطبيعته عن الإرهاب الذي يقصد به الفزع والخوف الناتج من تهديد بقوة طبيعية أو مالية[٧]، وأقدم تعريف للإرهاب في القاموس الفرنسي وعرف بمعنى الاستخدام المتعسف للقوة والعمل الموجه ضد الشخص الخصم وإجباره على القيام بالعمل مخالفة لإرادته وباستخدام القوة والتخويف الأخرين للسيطرة عليهم وتدميرهم وإخضاعهم للهزيمة، ووردت كلمة

الإرهاب في اللغة الانكليزية (terrorism) وفي قاموس أكسفورد الانكليزي للتعبير عن العنف والتخويف بغية تحقيق أغراض سياسية[٨]. اما مفهوم الإرهاب اصطلاحا لا يزال يشكل معضلة من بين المصطلحات التي اختلف في وضع تعريف جامع لها، إذ تعددت بشأنه وجهات النظر بسبب تعدد الثقافات والإيديولوجيات وتباينها من مجتمع لآخر، إذ عرفت وكالة التحقيقات العدلية الأمريكية الإرهاب بأنه التهديد والاستعمال غير المشروع للعنف ضد أشخاص أو ممتلكاتهم لإجبار المدنيين او الحكومة لتحقيق أهداف سياسية وجماعية، وورد مفهوم الإرهاب في التقرير الصادر عن وزارة الخارجية الأمريكية في ٢٠٠١ بأنه العنف المتقصد والذي يرتكب ضد اشخاص غير مقاتلين للتأثير في أفراد والجمهور[٩]، وقد وصفت الموسوعة السياسية الإرهاب بالعنف غير القانوني والتهديد بمختلف صوره وأشكاله كالتشويه والاغتيال والتعذيب والتخريب بغية تحقيق أهداف سياسية معينة[١٠].

أما مفهوم الإرهاب في التشريع العراقي اذا تناول المشرع العراقي مفهومة وعدها عنصرا من عناصر الرئيسية لبعض الجرائم المعاقب عليها كجريمة الاعتداء على النظم السياسية أو محلولة الغير مبادئ الدستور الع فعرفه قانون مكافحة الإرهاب العراقي رقم (١٣) لسنة ٢٠٠٥ وفي المادة ١١ على أن كل فعل أجرامي يقوم به فرد أو جماعة منظمة لاستهداف الإفراد والجماعات او المؤسسات الرسمية وغير الرسمية وإيقاع الضرر بالممتلكات العامة والخاصة للإخلال بالوضع الأمني والاستقرار وإدخال الرعب والخوف بين الناس وإثارة الفوضى تحقيقا للغايات الإرهابية[١١].

وعليه مع ظهور الشبكات المعلوماتية ووسائل التقنية الحديثة ومنها الحاسوب وشبكة الانترنيت ونظرا لما تقدمه من مزايا وخدمات كبيرة اتجه الإرهابيون إلى الاستفادة منها كوسيلة إعلامية لنشر أفكارهم وعقائدهم والدعاية لتنسيق عملياتهم وتسهيل الاتصال فيما بينهم وتضيف هذه الشبكات للتجسس وتنفيذ الأنشطة الإرهابية بأساليب وطرق إجرامية متقدمة التدمير وفعاليات المؤسسات والدول لينشا بذلك نمط جديد من الإرهاب سمي بالإرهاب الالكتروني وعلية فان يقوم بالأعمال التخريبية التي تستهدف شبكات الحاسوب والانترنيت سواء كانت عسكرية أو اقتصادية أو أمنية أو غيرها والتي من شأنها تهديد الأمن القومي او العسكري او الاقتصادي لدولة ما أو لعدة دول[١٢].

المطلب الثالث: مفهوم الإرهاب السيبراني :

الإرهاب السيبراني هو عمل اجرامي لكن يستخدم السلاح فيه وسائل اتصال ينتج عنه عنف وتدمير أو بث الخوف تجاه المستهدف سواء كان فردا أو مؤسسة أو دولة، والهدف التأثير على الحكومات أو السكان عادة ما يمثل أجندة سياسية أو اجتماعية او فكرية معينة، لذا عرف بعض الفقهاء الإرهاب الالكتروني بأنه " خرق قانون يقدم عليه فرد من الأفراد أو تنظيم جماعي. بهدف اثارة اضرار خطيرة في النظام العام عن طريق شبكة المعلومات"[١٣]، ويعرف أيضا بأنه استخدام شبكات المعلومات والكمبيوتر من أجل التخويف والإرغام لتحقيق أهداف سياسية حيث تقوم الجماعات الإرهابية بالتهديد عبر وسائل الاتصالات من خلال الشبكة العالمية للمعلومات، ، وذلك من أجل نشر الخوف والرعب وتتعدد أساليب التهديد وتتنوع طرقه بين الأشخاص والدول والشعوب ومحاولة الضغط عليهم للرضوخ لأهداف. وقد ذهب البعض الى تعريف الجريمة الإرهابية السيبرانية بأنها أي نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإرهابي المقصود[١٤].

ذهب رأي آخر في تعريفه للإرهاب السيبراني الدولي بأنه استخدام في مجالات الاتصالات الهاتفية ونظم المعلوماتية ومواردها أو التأثير عليها في مجالات المعلوماتية الدولية بهدف القيام بأعمال إرهابية وعرفه مكتب الأمم المتحدة المعنى بمكافحة الإرهاب (CTITF) : بأنه عمل يرتكب من خلاله هجمات إرهابية عن طريق التغيير عن بعد معلومات بين أنظمة الكمبيوتر او تعطيل تدفق البيانات بين أنظمة الكمبيوتر[١٥]، وعليه يشمل الإرهاب السيبراني أي نشاط إجرامي يتم من خلال شبكة الإنترنت بهدف بث الأفكار المتطرفة، سواء كانت سياسية أو دينية أو عنصرية للسيطرة على وجدان الإفراد وإفساد عقائدهم وإذكاء تمردهم واستغلال معاناتهم في تحقيق مارب خاصة تتعارض مع مصالح المجتمع. فعن طريق شبكة الإنترنت يمكن للإرهابيين الالتقاء بسهولة في أي مكان، إذ يمكن أن يلتقي عدة أشخاص في أماكن متعددة وفي زمن معين، ويتبادلوا، ويمكن أن يجمعوا لهم الحديث والاستماع لبعضهم عبر شبكة الإنترنت، بل يمكن أن يجمعوا لهم اتباعا عبر نشر افكارهم ومبادئهم من خلال المواقع والمنتديات وغرف الحوار الإلكترونية كذلك أيضا يعتبر البريد الإلكتروني من أعظم الوسائل المستخدمة في الإرهاب الإلكتروني وذلك من خلال استخدامه في التواصل بين الإرهابيين وتبادل المعلومات فيما بينهم، ومن إشكال الإرهاب الالكتروني التجنيد السيبراني و التهديد والترويع السيبراني، التجسس السيبراني[١٦].

المحور الثاني

المطلب الأول : استراتيجية الأمن السيبراني في العراق

تنطلق استراتيجية الأمن السيبراني العراقي، من مبدأ أساس هو ضمان أمن العراق وحماية وجوده في الفضاء السيبراني" ، وحماية بنية معلومات الحيوية، وبناء مجتمع انترنت ، موثوق" به ورعايته ، والتعامل مع التحديات السيبرانية ، التي قد أمن العراق الوطني وسلامته ، عن طريق تقي مجموعة من الاجراءات تعمل على حماية ، فضاء العراق السيبراني والدفاع عنه وبدأ تسجيل إحصائيات رسمية عن الجرائم السيبرانية في العراق منذ العام ٢٠٠٦ بسبب الانتشار السريع للخدمات والعمليات عبر الإنترنت، فارتفعت معها نسبة جرائم الإنترنت والانشطة المضرة بالنظام والمجتمع العراقي ، بل ان نسبة القرصنة السيبرانية في العراق هي الأعلى في الشرق الأوسط" ، وتنوعت حالات الجرائم السيبرانية في العراق منها : الغش عبر الإنترنت، وغسيل الأموال، وتزايد مواقع القرصنة ، والتجارة السيبرانية غير المشروعة، والتطفل على الشبكات ، والإرهاب الإلكتروني"[١٧]، وعليه فإن التطور التكنولوجي الذي شهده العراق في مجال المعلومات والاتصالات بعد عام ٢٠٠٣ تزامن معه ضعف الأمننة الإلكترونية وركاكة البنية التحتية أدى إلى أن يصبح العراق منكشفاً استراتيجياً لكثير من دول العالم، يسهل اختراقه والتجسس على المعلومات المؤسساتية لدرجة استخدام العراق كساحة لشن الهجمات الإلكترونية لضرب أمن معلومات دول اخرى واختراق منظومتها الأمنية الإلكترونية، فضلا عن استراق أي معلومة واستخدامها لأغراض المساومة أي لتنفيذ عمليات هكرية وإسنادها، ومن الملاحظ أن أكثر المؤسسات العراقية تتعاقد لتجهيز معلوماتها من أقمار صناعية ذات مورد خدمة واقع خارج الحدود العراقية الذي يؤدي إلى مرور تلك المعلومات في خوادم تلك الدول، ورجوعها إلى العراق إذ يشكل هذا الإجراء خرقا لأمن المعلومات العراقي[١٨]، ولتلافي مثل هذه الخروقات الكبيرة التي تتعرض لها حركة المعلومات في العراق يتوجب بناء منظومة متكاملة لأمن المعلومات لذا يتوجب بناء منظومة للأمن الإلكتروني العراقي بهدف حماية القضاء السيبراني الوطني، مع التركيز على ضمان توافر أنظمة المعلومات وتمتين الخصوصية، وحماية سرية المعلومات الشخصية، واتخاذ جميع الإجراءات الضرورية لحماية امن المواطنين وامن المؤسسات من مخاطر الفضاء السيبراني[١٩]، وعلية فان إن إستراتيجية الأمن الوطني السيبراني بشكل عام هي كافة التدابير المتعلقة بسرية المعلومات والبيانات التي يتم معالجتها وتخزينها وإبلاغها عن طريق وسائل إلكترونية أو مشابهة وحمايتها

والنظم المرتبطة بها من التهديدات الخارجية أو الداخلية وتهدف هذه الإستراتيجية إلى تطوير وتنفيذ قدرات الأمن السيبراني لتحسين والحفاظ على المجالات الآتية[٢٠]:

١- حماية خصوصية المواطن وغير ذلك من البيانات من الضياع، والتغييرات الضارة، والاستخدام غير المصرح به.

٢- مرونة الخدمات الحكومية والنظم والبنية التحتية للتهديدات الإلكترونية .

٣- استمرارية الحكومة أثناء وبعد الحوادث السيبرانية الخطيرة .

٤- حماية أمن الخدمات الرقمية للمواطنين.

٥- تنسيق الاستجابة للتهديدات ضد البنية التحتية ٦ أمن وسلامة البنية التحتية الأساسية للحكومة.

إن قضية الأمن السيبراني تعد من القضايا المهمة والحساسة المرتبطة بالأمن الوطني لكل دولة منفردة أو مجتمعة. لذا لا يمكن لأي دولة في العالم سواء كانت متقدمة أم نامية أن تحمل أو تتجاهل ذلك. وإذا كان وجود استراتيجية للأمن السيبراني بهذه الأهمية للدول ، فإن العراق هو بحاجة ملحة لوجود مثل هذه الاستراتيجية.

المطلب الثاني : استخدام الأمن السيبراني من قبل التنظيمات الإرهابية في العراق (داعش انموذجا) ...

لقد وجدت أغلب التنظيمات الإرهابية ضالتها المنشودة في شبكات التواصل الاجتماعي واعطت الأولوية لها، وجندت عناصرها للتركيز على هذه الساحة الجديدة للصراع الإيديولوجي بين أفكار هذه التنظيمات من جانب ، والدولة ومؤسساتها من جانب أخر ، و قد وفرت شبكات التواصل الاجتماعي أدوات عدة وساعدت هذه التنظيمات على العمل بشكل ميسر، إذ انها من حيث المبدأ تسمح لاي شخص ان ينتحل أي مسمى و أي صفة ، وأتاحت الفرص لإنشاء ما يطلق عليه الصفحات Pages بأنواعها المختلفة ، سواء المجموعات group أكانت المجموعات Public Groups المتاحة للجميع أم المجموعات المغلقة Closed group وقد استفادت المجموعات السرية Secret group التنظيمات الإرهابية من هذه التقنيات للترويج لأفكارها و التواصل مع مؤيديها أو من تسعى اجتذابهم ، فضل عن تقنية المجموعات السرية لخلق بيئة افتراضية أمنة للتواصل مع

أعضائها ، أو نقل المهام لهم وعقد اجتماعات افتراضية لأشخاص ربما يكونوا في مدن او بلاد مختلفة بمعزل عن رقابة ورصد الأجهزة الأمنية وبذلك أصبحت التنظيمات الإرهابية شبكية وليست هرمية كما في السابق، فيما تتخذ القرارات في الفضاء السيبراني، لتنفذ الأوامر على أرض الواقع بعد تلقيها عن بعد عبر شبكات التواصل الاجتماعي والأخطر من ذلك يتمثل في أن الفرد الواحد قد تحول إلى "منظمة إرهابية" او ما يمكن تسميته بال " ذئاب المنفرد "ما يعني أن انتشار الفكرة عبر الفضاء السيبراني لا يشترط لتطبيقها وجود مجموعة تتبنى هذه الفكرة، بل يكفي فرد واحد لتنفيذها(٢١).

وعلية فان قيام التنظيمات الإرهابية بتوظيف الفضاء الالكتروني عبر مواقع التواصل الاجتماعي لتطبيق استراتيجياتها وضمان التواصل بين عناصرها وتجنيدهم عبر تلك المواقع، كتنظيم دولة الإسلام في العراق (داعش) وهذا الجيل الجديد من التنظيمات الإرهابية يجسد خطرا كبيرا على الأمن الوطني العراقي حتى أصبح لتلك التنظيمات مواقع الكترونية فيها الآلاف من المشتركين وذلك بهدف زيادة شعبيته على الانترنيت، فضلا عن قيام تلك التنظيمات باستخدام تلك المواقع في تبادل المعلومات والخطط بصناعة المتفجرات والقنابل واستهداف مواقع معينة، وتقوم بتنجيد أكبر عدد من الأشخاص، وهذا يفسر لنا نجاح تنظيم القاعدة وتنظيم داعش عن تجنيد الآلاف من الأشخاص(٢٢)، واستطاعت ان توسع من شبكة العنكبوتية فان تنظيم الدولة الإسلامية من بين أهم التنظيمات التي واهتمت بشبكة الانترنيت والاتصالات الرقمية إذ يعتبر القضاء السيبراني احد أركانها حيث فتحت المئات من المواقع وإنشاءه العديد من المنابر والمنشورات والمجلات بعضها ذو طابع عسكري للتعرف بعملياته الميدانية وبعضها ذو طابع أيديولوجي لنشر الآراء المتشددة أن تعتمد داعش على استراتيجية الانترنيت واستغلال الجماعات الإرهابية للقضاء السيبراني وذلك من خلال عوامل(٢٣):

. ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق. غياب الحدود الجغرافية وتدني مستوى المخاطر

سهولة الاستخدام التقني وقلة التكلفة . صعوبة تحديد هوية وملاحقة مرتكبي العمليات الإرهابي مما يساعدهم على الحركة بحرية داخل المواقع التي يستهدفها قبل ان ينفذ جريمته ضعف التشريعات والقوانين الرادعة لهذا النوع من الجرائم في بعض الدول.

الأمر الذي يفسر تنامي وتزايد التنظيمات الإرهابية في هذا المجال حيث أصبح نشاط الجماعات الإرهابية على شبكة الانترنيت مكثف ومؤثر بشكل كبير في توجيه نشاطاتها الإرهابية سواء بالتواصل بين فروعها وخلاياها او في تنفيذ جرائم التخريب ضد المواقع الحكومية او التجسس عليها، وعليه فإن التهديدات السيبرانية تمثل تحديات غير مرئية تؤثر في منظومة الأمن الوطني العراقي، فمع الانفتاح على العالم والتطور التكنولوجي الذي شهده العراق لاسيما في مجال الاتصالات والمعلومات لكن بالوقت ذاته يعاني العراق من ضعف في البنية التحتية الخاصة بالحماية الالكترونية من الهجمات السيبرانية مما جعل العراق مكشوفا لدى الكثير من دول العالم لاختراقه والتجسس علية لاسيما المتعلقة منها بالمؤسسات الأمنية، ولأجل ذلك عمل العراق مع شركاته الدوليين في مجال تطوير الأمن السيبراني للإفادة من خبراتهم[٢٤].

المحور الثالث

المطلب الأول : الإجراءات الأمنية المتخذة في مجال الأمن السيبراني لمكافحة الإرهاب في العراق....

في ظل وجود الخطر الإرهابي ووجود الجرائم الإرهابية في الكثير من مناطق العالم لابد من القول بأن هناك آليات وجهود حثيثة ومستمرة لمكافحة هذه المخاطر وهذا ما تضح في جميع مراحل التاريخ وعلى كافة المستويات الدولية والوطنية وفي كافة المجالات والإجراءات والتدابير اللازمة بالنسبة لجميع صور الإرهاب، ومن هذا المنطلق أيضا لابد من التقرير بأن مكافحة الارهاب بحد ذاتها تواجه كثير من الصعوبات وهذا الأمر بالنسبة للإرهاب التقليدي فكيف يكون الأمر عندما يتعلق الأمر بالقضاء السيبراني حيث الانتشار الواسع على الشبكة وسهولة التنافي وسهولة ارتكاب الجرائم وتدمير أدارها وما إلى ذلك من خصائص تدور حول الجريمة السيبرانية وبالتالي فإن مزيد من الجهود يجب أن تبال في هذا المجال، مع عدم اعمال وانكر دور الوسائل التقليدية في مواجهة تلك التهديدات اذ يمكن القول في ان اطار مكافحة التهديدات والارهاب الالكتروني من تطبيق ذات الوسائل والإجراءات المستخدمة في علاج الأرهاب الالكتروني والإرهاب التقليدي في مكافحتهما مع فارق الخصوصية الذي يتمنع القضاء السيبراني وعليه سوف تذكر أهم التدابير والإجراءات اللازمة لمواجهة الإرهاب الالكتروني والتهديدات بما يلي[٢٥]:

١- تعزيز إمكانيات الإلمام والتحديث لوضع الأمن السبراني في العراق.

٢- بناء قدرات الاستجابة للهجمات الالكترونية والارهاب الالكتروني وتحسينها باستمرار من خلال:

* وضع آلية للتنسيق وإدارة التعامل مع الحوادث الالكترونية.

* إنشاء شبكة لتبادل المعلومات بين مراكز عمليات الأمن السيبراني وذلك لتيسير التعامل مع الحوادث وتبادل المعلومات.

* إنشاء مراكز عمليات خاصة بقطاعات او مؤسسات بعينها أو مراكز معلومات للكشف عن التهديدات الإرهابية والجرائم.

٣- الحد من أمكانية تعرض البنية التحتية للمعلومات الحيوية لهجمات الإرهاب الالكترونية.

٤- وضع الآليات والإجراءات التي من شأنها تسهيل اتخاذ الإجراءات اللازمة وتداول المعلومات مع الأطراف المعنية في الوقت المناسب.

٥- ضمان الجاهزية من خلال إجراء تدريبات المحافظة على الأمن السيبراني في العراق.

قانون مكافحة الارهاب في العراق لسنة ٢٠٠٥

نظرا لتزايد العمليات الإرهابية وتهديد حياة المواطنين في العراق فقد أصبحت الحاجة ماسة التشريع قانون خاص ومستقل لمكافحة الإرهاب في العراق لذا وافقت الجمعية الوطنية العراقية على قانون رقم ١٣ لسنة ٢٠٠٥ وتضمن هذا القانون تعريفا للإرهاب في مادته الأولى بأنه " كل فعل أجرامي يقوم به فرد او جماعة منظمة تستهدف فردا او مجموعة أفراد او جماعة أو مؤسسات رسمية أو غير رسمية أو وقع الأضرار بالممتلكات العامة أو الخاصة بغية الإخلال بالوضع الأمني او الاستقرار والوحدة الوطنية او إدخال الرعب والخوف والفزع بين الناس واثارة الفوضى تحقيقا لغايات "إرهابية" بالإضافة إلى الإشارة إلى الجرائم التي تمس امن الدولة المادة ٣،

والعقوبات المادة ٤ والأعذار المخففة المادة ٥ والاحكام الختامية المادة ٦ ولقد حددت الجمعية الوطنية الأسباب الموجهة لهذا القانون في فداحة الأضرار الناتجة عن الهجمات التي باتت تهدد الوحدة الوطنية العراقية والنظام الديمقراطي الاتحادي التعددي فيه ، ولدفع عجلة التنمية إلى الأمام والتي من شأنه القضاء على الهجمات الإرهابية والحد من التفاعل مع القائمين بها بأي شكل من الإشكال الدعم والمساندة[٢٦]، غير ان المشرع العراقي لم يشر في مضمونة ونصوصه إلى الإرهاب الالكتروني وإثارة على المجتمع، ويشير قانون جهاز مكافحة الإرهاب إلى أن أهداف هذا الجهاز والقوات التابعة له تدور حول الاتي[٢٧]:

١- مكافحة الإرهاب بجميع أشكاله والقضاء عليه.

٢ وضع سياسات استراتيجية شاملة لمكافحة الإرهاب وتطويرها.

٣- التعاون مع الجهات الأمنية ذات الصلة بمكافحة الإرهاب.

٤- انقاذ وتحرير الرهائن عن طريق التفاوض السلمي او الاقتحام المباشر لمكان الحدث الإرهابي.

٥- التنسيق مع الأجهزة الاستخباراتية المتخصصة لتنفيذ خطط مكافحة الإرهاب.

٦- تبادل المعلومات وتداولها وتقيمها الخاصة بمكافحة الارهاب داخل العراق وخارجة.

٧- تنفيذ اي مهمات اخرى يطلبها رئيس الجهاز وبمصادقة الهيئة الوزارية للأمن الوطني.

المطلب الثاني: الأهداف والوسائل الداعمة لنجاح استراتيجية مكافحة الإرهاب في العراق على وفق الأمن السيبراني:

١- حماية البنية التحتية للمعلومات الحيوية الوطنية، ولتحقيق هذا ينبغي العمل على[٢٨]:

أ- تقييم المخاطر التي تواجهها البنية التحتية للمعلومات الحيوية وتتضمن ... وضع إطار زمني الإدارة المخاطر على البنية التحتية للمعلومات الحيوية وتقييم التهديدات ونقاط الضعف والعواقب وتطوير ملفات المخاطر.

- إجراء تقييمات منتظمة للمخاطر التي تواجه وزارت الدولة.

- أجراء تقييمات حول مدى الترابط والاعتماد المتبادل بين مؤسسات الدولة لتحديد المخاطر المنهجية التي تواجهها.

ب- تنفيذ ضوابط ومعايير خاصة بالأمن السيبراني للحد من مخاطر على البنية التحتية للمعلومات الحيوية، وتتضمن:

- وضع نموذج ومعايير خاصة بالأمن السيبراني لبنية التحتية للمعلومات يتضمن ضوابط محددة للأمن السيبراني.

- إجراء عمليات تقييم وتدقيق منتظمة لوزارات الدولة والمؤسسات الحيوية.

- وضع استراتيجيات إدارة المخاطر لحماية الخدمات والأنظمة والمؤسسات الأكثر حيوية ومتابعة تنفيذ تلك الاستراتيجيات.

- تبادل المعلومات حول المخاطر واستراتيجيات إدارة المخاطر بين مختلف قطاعات الدولة لتحديد أولويات إجراءات التخفيف من تلك المخاطر واستثمار الموارد المتاحة.

ج- تحليل اتجاهات الأمن السيبراني والمخاطر التي تهدد البنية التحتية للمعلومات.

د- تعزيز استخدام المنتجات والخدمات التكنولوجية الموثوق بها من خلال وضع مبادئ توجيهية لتحديد المتطلبات الأمنية لمزودي خدمات تكنولوجيا المعلومات والاتصالات.

هـ- المراقبة المستمرة لأمن البنية التحتية للمعلومات الحيوية، اي وضع إلية لإجراء عمليات تشخيص ومراقبة مستمرة للشبكات من اجل تشكيل وعي اكبر بالمخاطر وتعزيز الإجراءات الوقائية والكشف عن الأجهزة المتضررة ومعالجتها.

٢- الاستجابة للحوادث والهجمات الالكترونية وحلها والتعافي منها من خلال تداول المعلومات في الوقت المناسب والتعاون واتخاذ الإجراءات اللازمة.

٣- وضع الإطار القانون والتنظيمي لتعزيز سلامة وحيوية الفضاء الالكتروني ولتحقيق هذا ينبغي العمل على[٢٩]:

أ- تعزيز قدرات العراق على مكافحة الجريمة والإرهاب الالكتروني من خلال تطوير قدرات جديدة للتحقيق في الأنشطة الإجرامية من خلال التدريب من قانون مكافحة الإرهاب والجريمة الالكترونية.

ب- وضع وتنفيذ القوانين واللوائح والسياسات الوطنية للتعامل مع القضايا الأمن السيبراني والجريمة الالكترونية.

ج- مراقبة وتعزيز الالتزام بالقوانين واللوائح والسياسات المتعلقة بالأمن السيبراني والجريمة الالكترونية،

د- بناء شراكات دولية متينة والحفاظ عليها لوضع معايير وقواعد الأمن السيبراني من خلال التعاون مع شركاه دوليين بشكل منتظم ومن خلال ابرام اتفاقيات ثنائية ومتعددة الإطراف لتبادل المعلومات حول قضايا الأمن السيبراني.

٤- تعزيز ثقافة الأمن السيبراني التي من شانها دعم الاستخدام الأمن والمناسب للفضاء الالكتروني.

٥- تطوير وصقل الإمكانيات الوطنية للأمن السيبراني.

٦- تنمية الوعي بالمخاطر السيبرانية والحلول المتاحة .

المطلب ثالث: المعوقات والمشاكل التي يعاني منها الأمن السيبراني لمكافحة الإرهاب في العراق[٣٠]:

١- ضعف القوانين والتشريعات الحكومية الخاصة بالأمن المعلوماتي والسيبراني، مما يتطلب تبني تشريعات قانونية فعالة يتم تطبيقها على القطاع الحكومي والخاص، وهنا يأتي دور الحكومة في تنفيذ إجراءات أمنية محددة في وزاراتها ومؤسساتها فضلا عن القطاع الخاص مما يعزز الأمن المعلوماتي والسيبراني على حد سواء في العراق.

٢- ضعف القدرات المهنية المحلية وقلتها في مجال أمن المعلومات المتقدمة والأمن السيبراني وهذا يتطلب العمل الجاد على تدريب وتطوير كوادر مهنية محترفة في القطاع الحكومي والخاص تؤهلها على مواجهة التحديات السيبرانية.

٣- ارتباط منظومات الانترنت في العراق بالخارج مما يعني ان الأمن السيبراني العراقي مرتبط بالنتيجة بدول وشركات خارجية، وهذا يتطلب من الحكومة العراقية إنشاء شراكة فعالة شركات محلية لإقامة علاقات موثوقة بها وفعالة لسد النقص في هذا المجال.

٤- قلة أدراك الشركات المحلية في مجال تكنولوجيا المعلومات بحجم المخاطر الأمنية المعاصرة وهذا يتطلب تنمية الوعي لديهم بأن التحديات الامنية المعاصرة تختلف عن المرحلة السابقة، مما يستلزم البحث عن حلول جديدة مناسبة للتطورات الأمنية المعاصرة، والابتعاد عن وسائل المعالجة التقليدية بهدف انشاء تكنولوجيا معلوماتية متقدمة في العراق تواكب التطور السريع.

الخاتمة :

لقد كان الامن ولا يزال الهدف المنشود للإنسان ومع تطور المجتمعات والثورة المعلوماتية والاتصال والتوجه نحو مجتمع المعلومات تشكل فضاء جديد هو الفضاء السيبراني الذي تستعمله الدولة افراد ومؤسسات الا ان هذه التطورات خلقت العديد من التهديدات الأمنية وخاصة على مستوى الامن الوطني الذي أصبح عرضة للخطر نضرا لانكشاف المعلومات الذي وفرته وسائل الاتصال الحديثة، لذلك ادى الانفتاح الذي شهده العراق لاسيما في المجال التقني والمعلوماتي وتزايد الاعتماد علية فرض تحديات عدة. ونظرا لكون العراق مستهدف بالدرجة الأساسية من قبل التنظيمات الإرهابية. فقد شهدت المؤسسات الرسمية وغير الرسمية خروقات و هجمات سيبرانية عدة ومن هذه التحديات التي فرضت نفسها على العراق هو الارهاب والتهديدات السيبرانية. وهذا يتطلب تعزيز وبذل الجهود من خلال الاهتمام بتطوير استراتيجية الأمن السيبراني وتحسين القدرات لمواجهة ومكافحة الارهاب والتهديدات الالكترونية.

النتائج:

١- ان الأمن السيبراني المعلوماتي يلعب دورا مهما في حماية الامن الوطني للدولة فهو قد يهدد امن الدولة كليا اذا تعرض للانكشاف او الاختراق.

٢- استغلت الجماعات الإرهابية في العراق الفضاء السيبراني ومواقع التواصل الاجتماعي من اجل تحقيق أهدافها في الدعاية والتجنيد ونشر الأفكار المتطرفة.

٣- تتخذ الدولة العديد من الإجراءات من تعزيز الإمكانات وبناء القدرات لمكافحة الجماعات الإرهابية في مجال الأمن السيبراني.

٤- أن المشرع العراقي في قانون مكافحة الإرهاب عام ٢٠٠٥ لم يشر إلى مكافحة الإرهاب الالكتروني وخطره على المجتمع فلا يوجد قانون في العراق خاص بالأمن السيبراني والجرائم السيبرانية .

٥- يواجه الأمن السيبراني في العراق في مجال مكافحة الإرهاب الكثير من المعوقات والمشكلات.

التوصيات

١ – الإقرار بالمسؤولية عن تحقيق الأمن السيبراني كجزء لا يتجزأ من الأمن القومي العراقي الوطني.

٢ – إنشاء مراكز للسلامة والمعلوماتية ولطوارئ والاتصالات تتعاون فيما بينها وفق آلية واضحة وشفافة وفاعلة.

٣- ضرورة تعزيز وتطوير والاهتمام في استراتيجية الأمن السيبراني كبعد حديث في استراتيجية الأمن الوطني العراقي.

٤- ضرورة تعاون العراق مع شركائه الدوليين في مجال تطوير الأمن السيبراني والإفادة من خبراتهم لمواجهة الإرهاب والتهديدات الالكترونية التي يواجهها العراق . ٥- يجب الإشارة الى الارهاب الالكتروني في مضمون ونصوص قانون مكافحة الارهاب.

٦- معالجة المشاكل التي يعاني منها الأمن السيبراني لمكافحة الارهاب في العراق.

المصادر:

١- حازم جري الشمري، توظيف القوة السيبرانية في استراتيجيات الدول الكبرى (الولايات المتحدة وروسيا – انموذجا) أطروحة دكتوراه، كلية العلوم السياسية جامعة النهرين.

٢- آيات ناصر جابر، استراتيجية مكافحة الإرهاب في العراق – دراسة مستقبلية ، رسالة ماجستير، كلية العلوم السياسية جامعة النهرين، ٢٠١٦ .

٣- سليم دحماني، اثر التهديدات السيبرانية على لأمن القومي الولايات المتحدة انموذجا، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، ٢٠١٨ .

٤- منى الأشقر جبور، الأمن السيبراني: التحديات ومستلزمات المواجهة، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، بيروت، ٢٠١٢.

٥- فريدة طاجين، تأثير القوة السيبرانية على الاستراتيجيات الأمنية للدول الكبرى دراسة حالة الصين، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة .

٦- اسعد طارش عبد الرضا، علي إبراهيم مشجل، الأمن السيبراني ودوره في انتشار ظاهرة الإرهاب في العراق بعد العام ٢٠٠٣ ، مجلة دراسات دولية، العدد الثمانون.

٧- بن مرزوق عنترة، حرشاوي محي الدين، الأمن السيبراني- كبعد جديد في السياسة الدفاعية الجزائرية، ص٦٦، متوفر على الرابط

https://dspace.unly ouargla dr/ispui/handle/123456789/14052

٨- عادل عبد المنعم، أمن المعلومات والأمن القومي، مجلة السياسة الدولية، العدد ٢١٣، ٢٠١٨.

٩- محمد عزيز شكري، الإرهاب الدولي والنظام الدولي الراهن، مطبوعات دار النشر، دمشق، ٢٠٠٢،ص٨٧ ص٨٨.

١٠- أحمد نعمة حسن الصحاف، جدل الإرهاب والحداثة كلفة مضاعفة في المجتمعات المأزومة، مجلة كلية التربية الأساسية، مجلد ٢٠، العدد ٨٥، سنة ٢٠١٤.

١١- عبد الوهاب الكيالي، الموسوعة السياسية، الجزء الثالث، الطبعة الثانية، المؤسسة العربية للدراسات والنشر، بيروت، ١٩٩٣.

١٢- حسن سعد عبد المجيد، السياسات العامة لمكافحة الإرهاب في العراق بعد ٢٠٠٣، المركز الديمقراطي- العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين- المانيا، ٢٠١٧، ط١.

١٣- اميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد٣٥، ٢٠٢٠.

١٤- حازم جري الشمري، توظيف القوة السيبرانية في استراتيجيات الدول الكبرى (الولايات المتحدة وروسيا- أنموذجاً)، أطروحة دكتوراه، كلية العلوم السياسية، جامعة النهرين، ٢٠٢٠.

١٥- نور علي صكب، الأمن الوطني العراقي في ظل الاختراق السيبراني (أمن المعلومات)، مجلة كلية العلوم القانونية والسياسية، العدد١، ٢٠٢١.

١٦- أحمد يوسف كيطان، استراتيجية الأمن الوطني السيبراني- الصين: قراءة في قانون الأمن السيبراني الصيني، مركز النهرين للدراسات الاستراتيجية، متوفر على الرابط https://www.alnahrain in/post

١٧- صلاح مهدي هادي الشمري، زيد محمد على إسماعيل، الامن السيبراني كمرتكز جديد في الاستراتيجية العراقية، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين العدد ٢٢، ٢٠٢٠.

١٨- أحمد عبد الكريم عبد الوهاب، محمد عبد الرحمن، إشكالية الأمن السيبراني والتقنين المقيد للحريات، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، ٢٠٢٠.

١٩- مروان سالم العلي، التحديات والاستراتيجية للأمن الوطني العراقي في ظل المتغيرات الدولية، مجلة تكريت للعلوم السياسية، العدد ٢٠٢٠.٢٠.

٢٠- اسعد طارش عبد رضا، علي إبراهيم مشجل المعموري، الأمن السيبراني ودوره في انتشار ظاهرة الإرهاب في العراق بعد عام ٢٠٠٣، بحث مستل من رسالة ماجستير، مجلة دراسات دولية، جامعة بغداد، العدد ٨٠، ٢٠١٩.

٢١- حازم حامد موسى، الرؤية الاستراتيجية للأمن الوطني العراقي في الفضاء السيبراني، المجلة الجزائرية للعلوم القانونية و السياسية، العدد ٥، ٢٠٢٠.

٢٢- المادة رقم ١ من قانون مكافحة العراقي رقم (١٣) لسنة ٢٠٠٥.

٢٣- مستشارية الامن الوطني، استراتيجية الأمن السيبراني العراقي، أمانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات.

الهوامش

(١) اسعد طارش عبد الرضا، علي إبراهيم مشجل، الأمن السيبراني، ودوره في انتشار ظاهرة الإرهاب في العراق بعد العام ٢٠٠٣، مجلة دراسات دولية، العدد الثمانون، ١٥٣.

(٢) سليم دحماني، أثر التهديدات السيبرانية على امن الولايات المتحدة أنموذجا، رسالة ماجستير كلية الحقوق والعلوم السياسية، جامعة محمد. بوضياف ٢٠١٨ ص٣٠.

(٣) بن مرزوق عنترة، حرشاوي محي الدين، الأمن السيبراني- كبعد جديد في السياسة الدفاعية الجزائرية، ص٦٦، متوفر على الرابط

https://dspace.unly ouargla dr/ispui/handle/123456789/14052

(٤) عادل عبد المنعم، أمن المعلومات والأمن القومي، مجلة السياسة الدولية، العدد ٢١٣، ٢٠١٨ ص٢٠٣.

(٥) منى الاشقر جبور، الأمن السيبراني: التحديات ومستلزمات المواجهة، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، بيروت، ٢٠١٢، ص٢-ص٤.

(٦) فريدة طاجين، تأثير القوة السيبرانية على الأستراتيجيات الأمنية للدول الكبرى، دراسة حالة الصين، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، ص١١.

(٧) محمد عزيز شكري، الإرهاب الدولي والنظام الدولي الراهن، مطبوعات دار النشر، دمشق، ٢٠٠٢،ص٨٧ ص٨٨.

(٨) أحمد نعمة حسن الصحاف، جدل الإرهاب والحداثة كلفة مضاعفة في المجتمعات المأزومة، مجلة كلية التربية الأساسية، مجلد ٢٠، العدد ٨٥، سنة ٢٠١٤، ص٧٢٩.

(٩) آيات ناصر جابر، استراتيجية مكافحة الإرهاب في العراق دراسة مستقبلية، رسالة ماجستير، كلية العلوم السياسية، جامعة النهرين، ٢٠١٦، ص١٤، ص١٨.

(١٠) عبد الوهاب الكيالي، الموسوعة السياسية، الجزء الثالث، الطبعة الثانية، المؤسسة العربية للدراسات والنشر، بيروت، ١٩٩٣، ص١٥٣.

(١١) حسن سعد عبد المجيد، السياسات العامة لمكافحة الإرهاب في العراق بعد ٢٠٠٣، المركز الديمقراطي- العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين- المانيا، ٢٠١٧، ط١، ص٢٧.

(١٢) حسن سعد عبد المجيد، مصدر سبق ذكره، ص٢٧.

(١٣) حازم جري الشمري، توظيف القوة السيبرانية في استراتيجيات الدول الكبرى (الولايات المتحدة وروسيا- أنموذجاً)، أطروحة دكتوراه، كلية العلوم السياسية، جامعة النهرين، ٢٠٢٠، ص٥٢، ص٥٣.

(١٤) حازم جري الشمري، مصدر سبق ذكره، ص٢٦.

(١٥) اميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد٣٥، ٢٠٢٠، ص٤٢٠.

(١٦) أميرة عبد العظيم، مصدر سبق ذكره، ص٤٢٢.

(١٧) مصطفى ابراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني- العراقي، مجلة العلوم القانونية والعلوم السياسية، العدد٤، ٢٠١٩، ص٩.

(١٨) نور علي صكب، الأمن الوطني العراقي في ظل الاختراق السيبراني (أمن المعلومات)، مجلة كلية العلوم القانونية والسياسية، العدد١، ٢٠٢١، ص١٧٠.

(١٩) أحمد يوسف كيطان، استراتيجية الأمن الوطني السيبراني- الصين: قراءة في قانون الأمن السيبراني الصيني، مركز النهرين للدراسات الاستراتيجية، متوفر على الرابط https://www.alnahrain in/post

(٢٠) صلاح مهدي هادي الشمري، زيد محمد على إسماعيل، الامن السيبراني كمرتكز جديد في الاستراتيجية العراقية، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين العدد ٢٢، ٢٠٢٠، من ٢٨٥ من ٢٨٦.

(٢١) أحمد عبد الكريم عبد الوهاب، محمد عبد الرحمن، إشكالية الأمن السيبراني والتقنين المقيد للحريات، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، ٢٠٢٠، ص٨.

(٢٢) مروان سالم العلي، التحديات والاستراتيجية للأمن الوطني العراقي في ظل المتغيرات الدولية، مجلة تكريت للعلوم السياسية، العدد ٢٠٢٠.٢٠ ص٥٨.

(٢٣) اسعد طارش عبد رضا، على إبراهيم مشيل المعموري، الأمن السيبراني ودوره في انتشار ظاهرة الإرهاب في العراق بعد عام ٢٠٠٣ بحث مستل من رسالة ماجستير، مجلة دراسات دولية، جامعة بغداد، العدد ٨٠, ٢٠١٩ من ١٦١ ص ١٦٢.

(٢٤) حازم حامد موسى، الرؤية الاستراتيجية للأمن الوطني العراقي في الفضاء السيبراني، المجلة الجزائرية للعلوم القانونية والسياسية، العدد٥، ٢٠٢٠، ص٥٨.

(٢٥) صلاح مهدي هادي، مصدر سبق ذكره، ص٢٨٩.

(٢٦) المادة رقم ١ من قانون مكافحة العراقي رقم (١٣) لسنة ٢٠٠٥.

(٢٧) اسعد طارش عبد الرضا، مصدر سبق ذكره، ص١٧٨.

(٢٨) مستشارية الامن الوطني، استراتيجية الأمن السيبراني العراقي، أمانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات، ص ٦، ص ٧.

(٢٩) صلاح مهدي هادي الشمري، مصدر سبق ذكره، ص٢٩٠.

(٣٠) مصطفى ابراهيم سلمان، مصدر سبق ذكره، ص١٧٥.