دور الامن السيبراني في تحقيق الامن الوطني العراقي
(زيارة الاربعين أنموذجا)

ا.م.د.علي جاسم محمد التميمي
كلية العلوم السياسية-الجامعة المستنصرية
Dr.alitop8085@gmail.com

ا.م.د.سعد علي حسين
كلية العلوم السياسية-الجامعة المستنصرية
Saadali76@yahoo.com

الملخص

يمثل الامن الهدف المنشود للإنسان ، ومع تطور المجتمعات والثورة المعلوماتية والاتصال والتوجه الى عالم المعرفة والمعلومات تشكل فضاء جديد هو الفضاء السيبراني الذي تستعمله الدولة، واوجدت هذه التطورات التقنية والمعلوماتية العديد من التهديدات الامنية وخاصة على المستوى الوطني الذي اصبح اكثر عرضة لخطر الانكشاف بسبب سهولة الحصول على المعلومات الذي وفرته وسائل الاتصال والتواصل الحديثة مع وجود العديد من وسائل الاقتناص الامني والمعلوماتي التي تهدف للاستحواذ على المعلومات المنتشرة عبر الفضاء الالكتروني بمختلف الطرق والاساليب، اضافة الى الدعاية وبث الشائعات الارهابية عبر وسائل التواصل الاجتماعي والتي تعد جزء مهم من الارهاب الالكتروني ولا سيما في التجمعات البشرية الكبيرة كالزيارات المليونية لا سيما زيارة اربعينية الامام الحسين عليه السلام ذلك الحدث السنوي العظيم والمهم والذي يستقطب الملايين من الزائرين من مختلف انحاء العالم وهو ما قد يستغله الارهابيون لإشاعة الفوضى ما استدعى تطوير مفهوم جديد للأمن من اجل مواجهة تلك التهديدات والتحديات الالكترونية وجاء مفهوم الامن السيبراني كرد فعل على تلك التهديدات من اجل الحفاظ على الامن الوطني وسلامة الدول وسيادتها لان الامن السيبراني المعلوماتي يمارس دورا مهما في حماية الامن الوطني للدولة، فهو قد يهدد امن الدولة كليا اذا ما تعرض للانكشاف او الاختراق الامر الذي قد يكلف الدولة الكثير من الخسائر على المستوى الامني والسياسي والاجتماعي والاقتصادي.

الكلمات المفتاحية: امن سيبراني – امن وطني – ارهاب الكتروني– مكافحة – زيارة الاربعين.

The role of cyber security in achieving Iraqi national security (zyarat al-arbaeen as a model)

Asst.Prof.Dr. Ali Jassim Mohammed
College of Political Science - Al-Mustansiriyah University
Asst.Prof.Dr. saad ali hussein .
College of Political Science - Al-Mustansiriyah University

Abstract:

Security is the desired goal of humanity. With the development of societies, the information revolution, communication, and the move towards the world of knowledge and information, a new space has been formed, namely cyberspace, which is used by the state. These technical and information developments have created many security threats, especially at the national level, which has become more vulnerable to the risk of exposure due to the ease of access to information provided by modern means of communication and contact, with the presence of many means of security and information espionage that aim to seize information spread across cyberspace in various ways and methods, in addition to propaganda and the dissemination of terrorist rumors via social media, which is an important part of electronic terrorism, especially in large human gatherings such as million-person visits, especially the zyarat al-arbaeen of Imam Hussein (peace be upon him), that great and important annual event that attracts millions of visitors from all over the world, and what terrorists may exploit to spread chaos, is what necessitated the development of a new concept of security in order to confront these electronic threats and challenges. The concept of cyber security came as a response to these threats in order to preserve national security and the safety and sovereignty of states, because cyber security information plays an important role in protecting the national security of the state. It could completely threaten the security of the state if it is exposed or breached, which could cost the state a lot of losses on the security, political, social and economic levels.

Keywords:Cyber security - National Security - Cyber Terrorism - Combating - Arbaeen Pilgrimage.

المقدمة

احدثت تكنولوجيا المعلومات والاتصالات ثورة هائلة في كل جوانب الحياة فكان للمستوى الاجتماعي تأثير كبير في سلوك وهوية المجتمع وانتشار آليات التشبيك بين الجماعات الانسانية التي تمثلها وسائل التواصل الاجتماعي وعبر الاجهزة الالكترونية مما ترتب عليه تغيرات كبيرة في المرتكزات الاجتماعية كالتعارف وبناء العلاقات الاجتماعية والخصوصية والتبادل الثقافي والاتصال الحضاري بين الجماعات المختلفة ثقافيا . عندما تصبح تكنلوجيا المعلومات هي المهيمنة على انماط الحياة بالمقابل تزداد المخاطر الالكترونية لذلك يواجه المجتمع جرائم الكترونية حقيقية ومتكاملة الاركان تتم عبر الفضاء الالكتروني متمثلة بالإرهاب السيبراني والالكتروني واشاعة الاخبار المظللة والدعاية المؤثرة ولاسيما في التجمعات البشرية الضخمة كالزيارات المليونية في العراق (زيارة اربعينية الامام الحسين عليه السلام وغيرها) ولا ننسى ما حصل في زيارة الامام الكاظم ع في ٢٠٠٥ عندما اشاع الارهاب بوجود عناصر ارهابية بين الزائرين مما تسبب باستشهاد عشرات الزائرين بعد ان القوا بأنفسهم من فوق جسر الائمة صوب نهر دجلة خوفا وهربا من الارهاب الذي كانت عبارة عن دعاية واشاعة لا اكثر وسرقة الاموال والابتزاز الالكتروني والنصب والاحتيال والتلاعب والتزوير وهذه الجرائم هي الاكثر شيوعا في الفضاء الالكتروني.

ان هذا التطور الذي يعيشه العالم ولاسيما في الالفية الثالثة والذي يرمي بظلاله على جميع المتغيرات في المنظومة المحلية والدولية جعل من الادوات التكنلوجية المستخدمة في المنافسة والسباق والتدافع نحو المصالح سلاحا يمكن من خلاله تحقيق اهداف تتراوح ما بين الامنية والاقتصادية وصناعة الرأي وتغيير نمط

الثقافة الاجتماعية عبر غزو فكري وثقافي لشبكات التواصل الاجتماعي ونشر ثقافة الاقصاء والعنف والتحريض الطائفي والديني او القبلي ومن جانب اخر الاهتمام بالمحتوى الالكتروني القائم على انتشار العلم والمعرفة وتقارب الثقافات بين الشعوب والحضارات عبر ما يسمى بالفضاء السيبراني والذي يعد من اهم مقومات عملية الاستحواذ والهيمنة المعاصرة امنيا وعسكريا لذلك اصبحت الدول تهتم كثيرا بهذا النوع من التسلح الالكتروني السيبراني للحفاظ على امنها سيبرانيا وصد كل الضربات الموجهة ضدها وحماية امنها ومكافحة التطرف الموجة من خلالها اي الارهاب الالكتروني لان تحدي الامن السيبراني هو التهديد الاكبر للأمن الوطني في عصرنا الراهن وان مفاهيم الامن الحديثة لا تقتصر على الجوانب العسكرية وانما تتشعب الى تحديات تحقق الامن لاسيما بعد ثورة المعلومات الهائلة وما انتجته من ارهاب الكتروني لا يصد الا عن طريق الامن السيبراني والالكتروني .

اهمية البحث :

ان اهمية البحث تنبع من ان صياغة منظومة الامن السيبراني تؤدي دورا مهما للتأثير في نجاح اداء الدولة داخليا وخارجيا وهذا ما دلت عليه التجارب من دول عدة سواء في المحيط الاقليمي او الدولي فكلما كانت الدولة اكثر اهتماما في الامن السيبراني وتطورا كانت الاقدر على مواجهة التحديات وتهديدات الامن السيبراني والارهاب الالكتروني ولاسيما ان العراق يشهد تجمعات بشرية كبيرة جدا بصورة مستمرة وسنوية كالزيارة الاربعينية وغيرها من زيارات الائمة الاطهار عليهم السلام والتي تحتاج الى امن الكتروني للحفاظ على امن الزائرين ومكافحة الدعاية والشائعات الارهابية.

اهداف البحث:

يهدف البحث الى بيان دور الامن السيبراني في حفظ الامن الوطني العراقي من خلال حفظ التجمعات البشرية وحمايتها في مختلف المناسبات وخصوصا الدينية منها ومن ابرزها زيارة اربعين الامام الحسين عليه السلام وتفكيك الخلايا الارهابية التي استفادت من التطور التكنلوجي واخذت تسخر المجال السيبراني لبث افكارها وخلق الفوضى وعدم الاستقرار من خلال زعزعة امن التجمعات البشرية الكبيرة لاسيما الزيارات المليونية وبث الشائعات السموم الفكرية والانحرافات العقائدية وغيرها.

اشكالية البحث:

تنبع اشكالية البحث من تساؤل مركزي واسئلة فرعية مرتبطة به، ويتمثل السؤال المركزي في الاتي: الى اي مدى يعد الامن السيبراني المرتكز الاهم في عملية مكافحة الارهاب الالكتروني وصياغة استراتيجية الامن الوطني ؟

اما الاسئلة الفرعية فتتجسد في الاتي :-

١. ماهي انماط الامن السيبراني؟
٢. ماهي اليات حماية الامن الوطني؟
٣. ماهي تحديات وتهديدات الامن السيبراني؟
٤. ماهي ادوات حفظ امن الزائرين في الزيارات المليونية ومكافحة الشائعات والدعاية الارهابية؟

فرضية البحث :

ينطلق البحث من فرضية مفادها: ان الامن السيبراني يعد واحدا من اهم انماط الامن الوطني للدول في القرن الواحد والعشرين ويعد مرتكزا اساسيا في حماية امن الدولة ومكافحة كل صور الارهاب الالكتروني وينطبق هذا الامر على العراق الذي يشهد حدثا سنويا مهما يتمثل في الزيارة المليونية لأربعين الامام الحسين عليه السلام وما يمكنه ان يشهده هذا الحدث من تهديدات ارهابية الكترونية وسيبرانية تهدد الامن الوطني العراقي وهو ما يستدعي تكثيف الجهود لتحقيق الامن السيبراني العراقي.

منهجية البحث :

تقتضي ضرورة البحث العلمي عند معالجة اي ظاهرة او اشكالية علمية تحديد المنهج كي يكون الوسيلة المعنية للوصول الى النتائج السليمة لذلك اعتمدنا في هذا البحث على المنهج الوصفي الذي يقوم على تفسير الظاهرة (ظاهرة الارهاب والتهديد الالكتروني) وتحديد خصائصها فضلا عن وصف طبيعة ونوعية العلاقة بين الامن السيبراني والامن الوطني عن طريق جمع البيانات الوطنية حول واقع التهديدات السيبرانية .

هيكلية البحث:

تم تقسيم البحث الى ثلاثة محاور تضمن المحور الاول استعراض ماهية الامن السيبراني والارهاب الالكتروني اما المحور الثاني فقد استعرض دور الامن السيبراني في مكافحة الارهاب الالكتروني في حين استعرض المحور الثالث دور الامن السيبراني في تحقيق الامن الوطني العراقي خلال زيارة اربعين الامام الحسين عليه السلام.

المحور الاول

ماهية الامن السيبراني والارهاب الالكتروني

من خلال تطور تكنلوجيا المعلومات ظهر فضاء جديد يسمى الفضاء السيبراني والفضاء الالكتروني الرقمي الذي بدأ من الانترنيت وما احدثته من انقلاب وتحول كبير في العالم المعاصر في جميع المجالات سلبا وايجابا من خلال ما اتاح هذا الفضاء من قوة جديدة بيد الدول الاكثر قدرة على توظيف السيبرانية وانعكاسها بشكل ايجابي غير مسبوق في تقديم الخدمات للدول والمؤسسات والافراد وفي الوقت نفسه اصبحت هناك مخاطر غير مسبوقة في حماية الامن القومي للدول ومهددات وتحديات للأمن الوطني لان الدول لم تكن هي الفاعل الوحيد في هذا الفضاء بل ان هناك فواعل اخرى من غير الدولة كالمؤسسات والافراد تؤثر في هذا الفضاء السيبراني .

لذا سنبين في هذا المحور ماهية الامن السيبراني وماهي اهم المهددات والتحديات المتمثلة بالإرهاب الالكتروني.

اولا: ماهية الامن السيبراني:

يؤثر الفضاء الالكتروني في مختلف مجالات الحياة اذ يسهم عن طريق ادواته المختلفة في اعادة رسم ابعادها المتعددة فيعمل على اعادة تشكيل الوعي والادراك الثقافي والاجتماعي والسياسي والامني للأفراد والمجتمعات والدول بصورة مغايرة عما كانت عليه اذ نجد تصورات وبنى جديدة يتم تأسيسها في المجال السياسي والامني والاقتصادي والاجتماعي والثقافي وغير ذلك وابرز تحدي يواجه الدولة في المستقبل الذي يفرضه الفضاء السيبراني يتمثل في قدرة الدولة على التكيف مع التغيير السريع والتحديات التي يفرضها الفضاء السيبراني في المجالات كافة ولاسيما المجال الامني وكيفية مواجهة التهديدات السيبرانية والارهاب من هذا النوع مع ضرورة مسايرة هذا التطور.

مجلة علمية محكمة نصف سنوية
www.arbnj.com
المجلد الرابع - السنة الرابعة - العدد الاول

أ- مفهوم الفضاء السيبراني:

يعود اصل كلمة (cyber) الى المعنى اليوناني القديم للحكم وبدأ استعمال كلمة (cyber) في عصرنا اول مرة من قبل عالم الرياضيات الامريكي (نوربرت فينز)(نوربرت فينز :- عالم رياضيات امريكي ولد في ٢٦ شباط ١٨٩٤ وتوفى ١٨ اذار ١٩٦٤ درس في جامعة هارفارد الامريكية ثم في انكلترا والمانيا وعمل في شركة جنرال الكتريك . ينظر https//www.ar.m.wikipedia.org) في كتابه (علم التحكيم الالي) الصادر عام ١٩٤٨ الذي يتعامل مع الحوكمة التي تعتمد على المعلومات ، وهو اول استعمال عام لمصطلح علم التحكيم الالي في الاشارة الى آليات التنظيم الذاتي، ووضع الكتاب الاساس النظري للحوسبة التناظرية والذكاء الاصطناعي وعلم الاعصاب والاتصالات الموثوقة.(فينز)

اما مفهوم الفضاء السيبراني فقد ظهر لأول مرة في عام ١٩٨٤ في احد روايات الخيال العلمي للكاتب الامريكي الكندي (ويليام فورد جيبسون) التي تحمل اسم (نيور مانسر) وهي رواية خيال علمي وصف فيها الكاتب الفضاء السيبراني بأنه انشاء لشبكة كمبيوتر في عالم مليء بالكائنات الذكية المصطنعة ، وكذلك يصف جيبسون الفضاء السيبراني بأنه هلوسة توافقية يمر بها المليارات من الناس يوميا. (خريسان ,٢٠٢١, ص١٤).

ويعرف الفضاء السيبراني كذلك على انه عالم الحاسوب الافتراضي او هو الوسيلة الالكترونية المستخدمة او الاكثر استخداما لتسهيل التواصل عبر شبكات حاسوبية فرعية منتشرة في جميع انحاء العالم المختلفة ويعتمد هذا الفضاء على بروتوكولات وذلك لتسهيل تبادل البيانات والملفات المهمة بشكل عام والتواصل بفاعلية بين مجموعة كبيرة من المستخدمين على هذه الشبكة اذ تصنع هذه الشبكة الفرصة لتبادل المعلومات والافكار والآراء والمشاركة في مختلف المناقشات في

المجالات كافة او المنتديات الاجتماعية وممارسة الالعاب الالكترونية وذلك من خلال وسائط سهلة الاستخدام بالنسبة لمستعملي هذه الشبكات وغير ذلك الكثير من خلال الخدمات المتنوعة.(العضيني , ٢٠١٧ , ص٢)

ان الفضاء السيبراني اكثر بكثير من مجرد بيئة للإنترنيت او انه بيئة تشغيل واسعة النطاق وشاملة بل ان الفضاء السيبراني هو مجال اصبح مؤثر بكافة تفاصيل حياة البشر دولا ومؤسسات وافراد وفي النظام الامني العالمي وامتد تأثيره في المجالات كافة الاقتصادية والسياسية والاجتماعية والعسكرية والبنى التحتية والفوقية للدول واصبح مجال للتحكم والمنافسة والصراع والحرب والردع وغير موازين القوة اذ يمكن لدولة صغيرة لا تمتلك قوة عسكرية كبيرة ان تؤثر في دول كبرى وتهدد امنها من خلال امتلاك قوة في الفضاء السيبراني بل انه يمكن لفرد ان يؤثر في الامن القومي لدول كبرى والاضرار فيها، لذا يعرف الفضاء السيبراني بأنه «مجال تشغيلي مؤطر باستخدام الالكترونيات تستعمل المعلومات عبر انظمة مترابطة وبنية تحتية مرتبطة بها تعتمد القوة على السياق وتعتمد القوة السيبرانية على الموارد التي تميز مجال الفضاء السيبراني (الشمري ,٢٠٢٢ ,ص٤٠-٤١).

ويتألف مجال الفضاء السيبراني من ثلاث طبقات:(خريسان ؛٢٠٢١؛ص ٥٦)

١. الطبقة المادية والتي تشمل الاجهزة والكابلات والاقمار الصناعية والمعدات والاخرى ومن دون هذه الطبقة المادية لا يمكن ان تعمل الطبقات الاخرى.
٢. الطبقة النحوية والتي تتضمن البرنامج الذي يوفر تعليمات التشغيل للمعدات المادية.
٣. الطبقة الدلالية وتشمل التفاعل البشري مع المعلومات التي تم انشاؤها بواسطة

اجهزة الكمبيوتر والطريقة التي يتم بها فهم المعلومات وتفسيرها بواسطة مستخدميها.

وهذه الطبقات الثلاث عرضة للهجوم ويمكن شن هجمات سيبرانية ضد البنية التحتية المادية للفضاء السيبراني باستعمال الاسلحة التقليدية على سبيل المثال تلف اجهزة الكمبيوتر وممكن عن طريق هجمات سيبرانية وتتداخل شبكاتها وتتلف وغير ذلك. وهذه الهجمات على الفضاء السيبراني تكون على قسمين: الاولى تسمى الهجمات النشطة فيكون الهدف منها هو تعطيل نظام التحكم والتأثير على تشغيل المرفق المستهدف او الجهة .الثانية: الهجمات غير النشطة:- هدفها الحصول على المعلومات والاستفادة منها دون التأثير على موارد النظام الاساسي.

وتنقسم وفقا لجهة التنفيذ الى: (كلارك؛٢٠١٢،ص٩٣):

أ. هجمات داخلية:-من خلال اطراف داخل الدولة مصرح لها بالوصول الى نظم التحكم وموارد النظام.

ب. هجمات خارجية : من كيانات او اطراف غير مصرح لها ويمكن ان تكون من قبل حكومات معادية.

تعريف الامن السيبراني:

من الصعب تحديد الامن السيبراني فهو يحتوي على اكثر من (٤٠٠) مفهوم تم تصنيفها بواسطة مجموعة متنوعة من الجهات الفاعلة بما في ذلك الحكومات والشركات والمنظمات الدولية والمجتمع التقني والمجتمع المدني(خريسان؛ص ٩٣)، وشاع استعمال مصطلح امن المعلومات في عصرنا الحالي ليحدث ثورة امنية في عالم الاتصالات الحديثة واختلافا ملحوظا في الادبيات التي تناولت تفسير هذا المفهوم اذ عرفه البعض بالقول: الامن السيبراني هو مجموعة الادوات والسياسات ومفاهيم الامن وضوابط الامن والمبادئ التوجيهية ونهج ادارة المخاطر والاجراءات والتدريب

وافضل الممارسات وأليات الضمان والتكنلوجيا التي يمكن استخدامها في حماية البيئة السيبرانية , واصول المؤسسات والمستعملين وتشمل اصول المؤسسات ومستعملي اجهزة الحوسبة الموصولة بالشبكة والموظفين والبنية التحتية والتطبيقات والخدمات وانظمة الاتصالات ومجموعة المعلومات المنقولة والمحفوظة في البيئة السيبرانية ويسعى الامن السيبراني الى تحقيق خصائص امن اصول المؤسسات والمستعملين والحفاظ عليها وحمايتها من المخاطر الامنية ذات الصلة في البيئة السيبرانية .(الموسوي , ٢٠٢١ ص٢٠)

كما يعرف الامن السيبراني بانه (العمليات التي تؤمن حماية كافة الموارد والاليات المستخدمة والمتبعة في معالجة المعلومات امنيا اذ يتم تأمين كافة الموارد البشرية وغير البشرية المختصة بجهة معينة بوسائل واجراءات وعمليات امنية وتقنية توفر لها سلامة محتواها المعلوماتي من اي مخاطر)، فالمعلومات هي الكنز الثمين الذي يتوجب على اية دولة في العالم حمايته من اي مخاطر داخلية او خارجية لذلك على الاجهزة الامنية او الجهات المختصة اتخاذ سلسلة من الاجراءات للحفاظ على سرية المعلومات الالكترونية وتفادي الخروقات الفيروسية لضمان وصول المعلومات الالكترونية الى السلطات المختصة في الوقت المناسب وعدم وقوعها في ايدي الاعداء او الاصدقاء لذا اصبح هذا النوع من الامن شاغلا استراتيجيا للقوة الدولية ، وعليه يمكن القول ان الامن السيبراني هو عبارة عن «محاولة تكثيف الجهود السياسية والاقتصادية والاجتماعية للتكنلوجيا الرامية لحماية المحتوى المعلوماتي للأدوات وافراد والمؤسسات والحكومات والدول من اي ثغرات داخلية وخارجية»، وهذا يتناسب مع التعريف الذي اورده (ادوارد امورسو) عن الامن السيبراني الذي عرفه على انه : «مجموعة وسائل للحد من مخاطر مهاجمة البرامج واجهزة الكمبيوتر او الشبكات المتصلة وتشمل وسائل وادوات لمكافحة القرصنة واكتشاف الفيروسات

ومنعها» ، اي انه عبارة عن وسائل دفاعية من شأنها كشف واحباط المحاولات التي يقوم بها القراصنة.(الموسوي،٢٠٢١؛ ص٢٢)

وقدمت وزارة الدفاع الامريكية (البنتاغون) تعريفا دقيقا لمصطلح الامن السيبراني فوصفته باعتباره «جميع الاجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع اشكالها المادية والالكترونية من مختلف الجرائم من الهجمات التخريب والتجسس والحوادث».(الموسوي؛٢٠٢١؛ص٢١)

وهذا يبين ان الامن السيبراني مفهوم اوسع من امن المعلومات ، فالأمن السيبراني يهتم بأمن كل ما هو موجود على السايبر من غير امن المعلومات، بينما امن المعلومات لا يهتم بذلك وان امن المعلومات يهتم بأمن المعلومات الورقية بينما لا يهتم الامن السيبراني بذلك.(مبادرة الباحثون السوريون؛٢٠٢٣)

ج. الفرق بين الامن السيبراني والفضاء السيبراني:

يتألف الفضاء السيبراني من نظم حاسوبية مختلفة متصلة بالشبكة ونظم اتصالات سلكية ولاسلكية متكاملة واصبح الفضاء السيبراني احد سمات المجتمع الحديث وهو ما يعمل على تعزيز وتمكين الاتصال السريع وانظمة القيادة والتحكم الموزعة وتخزين ونقل البيانات وكميات هائلة ومجموعة من الانظمة الموزعة بشكل كبير ، اما الامن السيبراني فهو حماية جميع ما تقدم سواء كانت الانظمة والشبكات او البيانات في الفضاء السيبراني ضد التهديدات مثل الجريمة السيبرانية او الحرب السيبرانية.(الشمري,٢٠٢٢ ,ص٢٤٥)

ومن اهم صور الامن السيبراني هي: (شلوش, ٢٠١٨ , ص١٩٣)

١. الدفاع الالكتروني ، الذي يعني بالدفاع عن انظمة واجهزة ومعلومات الدولة والجيش والمجتمع.

٢. الهجوم الالكتروني ، وهو المجال المختص بالعمليات الالكترونية والتي تهدف الى التشويش على مصادر المعلومات وتدميرها وحرمان العدو من استخدامها لمصلحتهم .

٣. التجسس الرقمي على امكانيات وقدرات الفاعلين الاخرين.

ثانيا : ماهية الارهاب الالكتروني:

ان الثورة التكنلوجية والتطور التقني في عصرنا الحاضر وظهور الحواسيب الالية وغيرها من الادوات التكنلوجية قد ادى الى تغيير شكل الحياة في العالم واصبحت الوسائل الالكترونية اهم مقومات المؤسسات العامة والخاصة سواء في المؤسسات الامنية او المدنية ، ولا يمكن انكار ما للوسائل الالكترونية من فوائد يصعب حصرها فأن الوجه الاخر والمتمثل في الاستخدامات السلبية لهذه التقنيات الحديثة ومنها الارهاب الالكتروني اصبح خطرا يهدد العالم بأسره، واخذت اساليب الارهاب الالكتروني والسيبراني ابعادا واشكالا مختلفة تهدد امن المجتمع والمؤسسات والدولة تحت مبررات وشعارات تتباين من منظمة ارهابية الى اخرى.

أ- معنى الارهاب الالكتروني:

ان الارهاب الالكتروني هو نوع خاص من الارهاب اذ يكون المكان او الوسط الذي يمارس فيه الارهاب هو الفضاء الالكتروني ، ويشير مفهوم الارهاب الالكتروني عادة الى مجموعة من الاجراءات المتنوعة جدا بدءا من الانتشار البسيط للدعاية عبر الانترنيت الى تغيير المعلومات او تدميرها وحتى التخطيط للعمليات الارهابية وتنفيذها عبر استعمال شبكات الكمبيوتر واشراك الاطفال والنساء والترويج لهجمات الالكترونية واستعمال وسائل التواصل الاجتماعي والتهديدات المستقبلية ، كما يشمل الارهاب الالكتروني الهجمات ضد البنى التحتية المالية

والهندسية الحكومية ، ويجب ان يرتكب السلوك الارهابي في الفضاء الالكتروني حتى نكون امام ارهاب الكتروني.(باسم علي خريسان؛٢٠٢١, ص٧٤)

ويعرف بعض الفقهاء الارهاب الالكتروني بأنه : العدوان او التخويف او التهديد ماديا او معنويا باستخدام الوسائل الالكترونية الصادرة من الدول او الجماعات او الافراد على الانسان نفسه ، عرضه او عقله او ماله بغير حق بشتى صنوفه وصور الافساد في الارض.(محمد ؛٢٠١٨ ؛ص٤٨٩)

ويستخلص من تعريف الارهاب الالكتروني هنا بأنه يكون باستخدام الوسائل الالكترونية الحديثة بكل انواعها وقد يصدر من الفرد او جماعة او دولة لذلك فأن خطره يكمن في سهولة استخدامه مع شدة اثره وضرره، فيقوم مستخدم الارهاب الالكتروني بعمله الارهابي وهو في منزله او مكتبه او في مقهى او اي مكان اخر مع ان الارهاب في تهديده لا يعرف الحدود ولا يميز بين الاشخاص والمؤسسات او الانظمة,هي حرب مفتوحة بلا حدود وحدود المواجهة لم تقتصر على فرد او مؤسسة معينة الا ان اكثر الجهات استهدافا من الارهاب هي المنظمات والمؤسسات الامنية.(محمد ؛٢٠١٨؛ ٤٩٠)

وقد اصبح الارهاب الالكتروني هاجسا يخيف العالم الذي اصبح عرضة لهجمات الارهابيين عبر الانترنيت الذين يمارسون نشاطهم التخريبي من اي مكان في العالم وهذه المخاطر تتفاقم بمرور الوقت لان التقنية الحديثة وحدها غير قادرة على حماية الناس من العمليات الارهابية الالكترونية التي تسبب اضرارا جسيمة على الافراد والمؤسسات الدولة لاتقف خطورة الارهاب الالكتروني عند ذلك لان الخطورة الامنية والاجتماعية تأخذ بعدا اخطر اذا ادركنا ان التنظيمات الارهابية هي من اوائل الجماعات التي دخلت عالم التكنلوجيا والفضاء الالكتروني للاستفادة منه في نشر ارهابهم وتحقيق اهدافهم الاجرامية.(عبد العزيز،٢٠١٩ ،ص٣).

ب- خصائص الارهاب الالكتروني:

يتميز الارهاب الالكتروني بعدد من الخصائص والسمات التي يختلف فيها عن بقية الجرائم وتحول دون اختلاطه بالإرهاب العادي ومن الممكن ايجازها فيما يلي : (ايسر؛٢٠١٤ ؛ص ١١).

١. ان الارهاب الالكتروني لا يحتاج في ارتكابه الى العنف والقوة بل يحتاج حاسوب متصل بشبكة الانترنت ومزود ببعض البرامج اللازمة.
٢. يتميز الارهاب الالكتروني بكونه جريمة ارهابية متعدية الحدود وعابرة للدول والقارات وغير خاضعة لنطاق اقليمي محدود .
٣. صعوبة اكتشاف جرائم الارهاب الالكتروني ونقص الخبرة لدى بعض الاجهزة الامنية والقضائية في التعامل مع مثل هذا النوع من الجرائم.
٤. صعوبة الاثبات في الارهاب الالكتروني نظرا لسرعة غياب الدليل الرقمي وسهولة اتلافه وتدميره.
٥. يتميز الارهاب الالكتروني بأنه يجري عادةً بتعاون اكثر من شخص على ارتكابه .
٦. ان الارهاب الالكتروني لا يترك اي دليل مادي بعد ارتكابه جرائم وهذا يصعب عملية التعقب واكتشاف الجريمة اساسا.
٧. سهولة اتلاف الادلة في حال العثور على اي دليل يمكن ادانة الجاني وغيرها من الخصائص والسمات التي تتنوع وتكثر مع حداثة الوسائل الالكترونية المستخدمة في الارهاب.
٨. ان مرتكب الارهاب الالكتروني يكون في العادة من ذوي الاختصاص في مجال تقنية المعلومات او على الاقل شخص لديه قدرة من المعرفة والخبرة في التعامل مع الحاسوب والشبكة المعلوماتية.

المحور الثاني

دور الامن السيبراني في مكافحة الارهاب الالكتروني

في ظل وجود الخطر الارهابي ووجود الجرائم الارهابية في مناطق العالم المختلفة يمكن القول ان هناك جهود حثيثة ومستمرة لمكافحة هذه المخاطر ، وهو ما اتضح في جميع مراحل التاريخ وعلى كافة المستويات الدولية والوطنية وفي كافة المجالات والاجراءات والتدابير للازمة بالنسبة لجميع صور الارهاب، ومن هذا المنطلق لا بد من التقرير بان مكافحة الارهاب في حد ذاتها تواجه مصاعب كثيرة فيما يتعلق بالإرهاب التقليدي فكيف يكون الامر عندما يتعلق بالفضاء السيبراني حيث الانتشار الواسع على الشبكة وسهولة التخفي وسهولة ارتكاب الجرائم وتدمير اثارها وما الى ذلك من خصائص تدور حول الجريمة السيبرانية، وهو ما يستدعي بذل المزيد من الجهود لمكافحة الارهاب الالكتروني مع عدم اغفال وانكار دور الوسائل التقليدية في مواجهة تلك التهديدات، والتأكيد على تحقيق الامن السيبراني من خلال مكافحة الارهاب الالكتروني.

ويعد الفضاء الالكتروني عنصر جذب مهم للتنظيمات الارهابية على اختلاف انواعها وتباين فكرها نظرا لما يتيحه من وسيلة اعلام عالمية هي في الوقت ذاته سلاح خطير، وتقوم هذه التنظيمات باستخدام الفضاء الالكتروني في الدعاية والتجنيد والتمويل وجمع المعلومات وتنسيق الهجمات الارهابية وحشد المتعاطفين من مختلف دول العالم، بالإضافة الى سهولة استخدام الارهاب الالكتروني وتنفيذه من اي مكان في العالم ولا يلزم ان يكون الفاعل في موقع العمل الارهابي بل يكفي ان تتوافر على نطاق واسع وصلات الانترنت اللازمة لتنفيذ الهجوم باستخدام اي هاتف محمول حديث، ولا تعتمد سرعة الهجمات الالكترونية على سرعة وصلة الانترنت

التي يستخدمها المهاجم بل يمكن استغلال السرعة العالية لوصلة الانترنت التي تستخدمها الحواسيب التي تتعرض للهجوم وذلك لان (الفايروسات) وغيرها من البرمجيات المؤذية يمكن ان تنتشر بأعلى سرعة ممكنة دون الحاجة الى المزيد من التدخل من المهاجم، ويمكن ابقاء الاعمال المرتكبة عبر الشبكة مجهولة المصدر وغير قابلة لاقتفاء اثرها وتتبعها عن طريق خدمات تجهيل المصدر وما شابهها من تقنيات التمويه مثل استخدام حواسيب مسيطر عليها عن طريق القرصنة، ويزيد من الاغراء بالإرهاب الالكتروني انخفاض تكلفة الانترنت وكثرة الاهداف التي يمكن قصدها واختيار مهاجمتها وكثير من تلك الاهداف قد لا يتمتع بحماية كافية، وفي ظل هذه المغريات سارعت مختلف التنظيمات والجماعات الارهابية الى امتلاك مواقع على الانترنت وبخاصة شبكات التواصل الاجتماعي من اجل التعريف بأهدافهم الفكرية والسياسية ومهاجمة خصومهم من العلماء والمفكرين ومن الحكومات والاجهزة الامنية.(محمد،٢٠٢١، ص١٨٩)

وهناك العديد من المخاطر المترتبة على الارهاب الالكتروني ومن ذلك على سبيل المثال : تعطيل الاتصالات والتشويش عليها، والتنصت على المكالمات وبث معلومات مضللة وتقليد الاصوات وخاصة اصوات القادة العسكريين لإصدار اوامر خطيرة، واستهداف شبكات الحاسوب بالتخريب عن طريق نشر (الفايروسات) ، مسح الذاكرة الخاصة بالأجهزة المعادية، منع تدفق الاموال وتغيير مسار الودائع، وايقاف محطات الكهرباء عن العمل عبر اعداد قنبلة الكترونية خاصة يطلق عليها اسم (Cbu49) تنطلق منها عدة قنابل في الجو تستهدف محطات الكهرباء وتؤدي الى احتراقها وتدميرها بالكامل، ويقدم الباحث (باري كولين) قائمة بأعمال الارهاب الالكتروني التي يمكن ان تهدد مستقبل البشرية وكالآتي(محمد،ص١٩١).

١. الوصول عن بعد الى انظمة التحكم بمصانع الحبوب وتغيير مستويات مكملات الحديد للأضرار بصحة المستهلكين.

٢. اجراء تعديلات عن بعد في معالج حليب الاطفال للإضرار بصحة الاطفال الرضع.

٣. تعطيل المصارف والمعاملات المالية الدولية والبورصات لإفقاد النظام الاقتصادي الثقة فيه.

٤. تغيير مكونات صناعة الادوية عن بعد لدى شركات الادوية.

٥. تغيير الضغط في خطوط الغاز وزيادة حمل شبكات الكهرباء مما يوقع انفجارات وحرائق مروعة.

٦. مهاجمة انظمة التحكم في الحركة الجوية وجعل طائرات مدنية تصطدم مع بعضها عن طريق الولوج الى اجهزة الاستشعار في قمرة القيادة بالطائرة وكذلك الخطوط السكك الحديد.

ومع ان هذه التصورات يمكن اعتبارها تصورات نظرية لكنها ممكنة وقابلة للتطبيق في ظل عدم الاستهانة بعقلية الارهابيين والاستعداد للتصدي لأي افكار قد يلجأ اليها الارهابيون.

ومن اجل مواجهة خطر الارهاب الالكتروني فان هناك سبلا وتدابير عدة يمكن اتباعها واعتمادها كالاتي:

اولا: التدابير السياسية والتنظيمية

١. السياسات السيبرانية: ان سياسة الدولة على المستويين المحلي والدولي تحدد توجهاتها في الفضاء السيبراني، ويبدو ان بعض الدول الكبرى الناشطة في الفضاء الالكتروني مثل الصين وروسيا لديها تحفظات تتعلق بهذا الفضاء اذ رأت في العولمة السيبرانية تعديا على سيادة الدولة القومية، ولا يمكن لأي دولة في ظلها ان تسيطر على المضمون المتداول بين مواطنيها عبر شبكة الانترنت، لذلك اقامت كل منهما الحواجز اللازمة وانشأت شبكاتها القومية الخاصة ضمن اطار شبكة الانترنت العالمية وبحسب ضوابطها الخاصة، ونجحت كلا الدولتين في تحقيق ذلك، اضافة الى تبني معظم الدول الكبرى جماعات سيبرانية وسيطة تعمل لصالحها مثل الجيوش او ما يطلق عليه الذباب الالكتروني.

٢. الجوانب التنظيمية والتشريعية: ان التشريعات القانونية التي تراعي الجوانب الموضوعية والشكلية مهمة في مواجهة الارهاب الالكتروني على صعيد الدول، اذ يجب ان تنظم التشريعات العمل في المجال الرقمي بإنشاء مؤسسات متخصصة بموجب قوانين خاصة، وتحديد طبيعة الجرائم والعقوبات الملائمة والرادعة لها، وشمول جميع الجوانب المتعلقة بالتجريم والعقوبات والاجراءات الشكلية كالضبط والتحقيق والتوقيف وما شاكلها.

٣. الاستراتيجيات السيبرانية: الاستراتيجية السيبرانية للدولة تحدد توجهها في هذا المجال، وتشمل السياسات والجوانب الاخرى ذات الصلة كافة مثل المؤسسات

المخولة بتنظيم النشاطات الرقمية وضبطها، ومواكبة التشريعات للتطور الحاصل في هذا المجال، والاهتمام بتوعية المستخدمين بالمخاطر المحتملة.

٤. الاتفاقيات الاقليمية والتعاون الدولي: تشمل الاتفاقيات الثنائية بين الدول الجوانب القانونية اللازمة للتعاون في مجال التحقيق في حوادث الفضاء الالكتروني، اما التحالفات السيبرانية بين الدول او مع القطاع الخاص، فهي مهمة في عمليات التتبع والتحقيق في الحوادث وتبادل المعلومات عن ابرز الطرق الاجرامية المتبعة، واهم الاختام الرقمية والبصمات الالكترونية الخاصة بالتنظيمات الارهابية، واحدث البرمجيات والاسلحة السيبرانية المستخدمة، ما يساعد على تحديد هوية الجهة التي تنفذ الهجمات الارهابية السيبرانية ويسهل استهدافها. (الحمدان، ٢٠٢١).

ثانيا: التدابير الامنية والاستخبارية السيبرانية:

يبرز اثر الجهات الامنية السيبرانية في مجال التوعية والقيام بإجراءات الاستخبارات لكشف ثغرات الانظمة المحلية ومعالجتها، ووضع التدابير لمواجهة الهجمات، والقيام بالتحقيقات الفنية اللازمة، والتنسيق مع مؤسسات تنفيذ القانون والجهات الاخرى ذات العلاقة، فضلا عن متابعة النشاطات السيبرانية الحديثة والاسلحة السيبرانية المستحدثة ومراقبة الفضاء الرقمي، ومدى التزام المستخدمين بالمعايير المرعية محليا ودوليا، والتعاون مع الجهات المناظرة لها اقليميا ودوليا، ويمكنها توظيف القراصنة المحليين واستقطابهم ليكونوا جيوشا الكترونية لصالحها.

ثالثا: التدابيرالفنية:

تتضمن تطوير البرمجيات والتطبيقات والادوات والبنية التحتية الالكترونية اللازمة للمواجهة وتتمثل في: (الحمدان ؛٢٠٠٦؛ ٢٠٢٢).

١. انشاء جدران الحماية (firewalls) لتكون خط الدفاع الاول للأنظمة والمعلومات، وهي برمجيات لحماية الانظمة والبيانات وكشف الهجمات.

٢. اجراءات امن حسابات المستخدمين وطرق التحقق من الهوية وتتضمن حماية الحسابات الرسمية والمصنفة، ويعد الفرد هو العنصر الاهم في هذا المجال اذ على مديري الانظمة وضع الوسائل الالية واليدوية اللازمة للتحقق من هوية المستخدم.

٣. تعمية البيانات وهي من وسائل حماية البيانات عند ارسالها في الانترنت او عند تخزينها بوصف ذلك عنصر اعاقة في حال حصلت جهة غير مخولة على البيانات ما قد يمنع او يؤخر استفادة هذه الجهة من البيانات.

٤. تقنية المفتاح العام وهي تعتمد تشفير البيانات وتقسيمها الى اجزاء وتوزيعها الى عدة خوادم في مناطق مختلفة من العالم من قبل المرسل ولا يتمكن المستقبل من جمعها الا باستعمال مفتاح التشفير.

٥. تقنية القفز المشفر وهي تقنية تعتمد انتقال البيانات المشفرة من المرسل عبر عدة عقد متتالية في الشبكة بأن تضيف كل عقدة تشفيرا حتى تصل الى المستقبل.

٦. الشبكة الافتراضية الخاصة وهي شبكة افتراضية فرعية عن شبكة الانترنت مصنفة لتكون شبكة سرية خاصة تربط الاجهزة الامنية والاستخبارية والحكومية ذات العلاقة بمواجهة الارهاب الالكتروني، وتستخدم المنظمات والدول بعض الشبكات الخاصة والمعدة للاستخدام الخاص بين موظفيها ومديريها وتكون معزولة جزئيا عن الانترنت وتخضع لرقابة المختصين الدائمة لحمايتها.

٧. تقنية الفجوة الهوائية وهي تقنية تستخدمها انظمة التحكم والاشراف والحوسبة للبنى التحتية الحساسة وادارة البيانات فيها بأن تجعل الانظمة معزولة كليا عن شبكة الانترنت عبر اعداد فجوات فنية تُزال فقط وفق اجراءات سرية محددة وبأوقات سرية كذلك.

٨. مسجل لوحة المفاتيح وهي تقنية تستخدمها الاستخبارات السيبرانية وتستخدم للتجسس على اجهزة الجهات الاجرامية والمتطرفة باستخدام البرمجيات اللازمة لاختراق انظمة هذه المنظمات وارسال برمجية التجسس للجهة المستهدفة في الفضاء الرقمي.

٩. تقنية خلية العسل او الطعم وهي تقنية تستخدمها الاستخبارات السيبرانية بوضع معلومات غير حقيقية على احد الخوادم لتكون طعما للإرهابيين وفق خطة محكمة بهدف معرفة نشاطات الارهابيين وامكاناتهم وتحديد مواقعهم.

١٠. تقنية استمرار الاعمال اي ان يستمر استعمال البيانات باستخدام النسخ الاحتياطية (backup) وفقا لبرمجة محددة تديرها ادارة النظام او الجهة الامنية المسؤولة.

المحور الثالث

دور الامن السيبراني في تحقيق الامن الوطني العراقي خلال الزيارة الاربعينية

اشرنا سابقا الى ان الفضاء الالكتروني اصبح عنصر جذب مهم للتنظيمات الارهابية على اختلاف انواعها وتباين فكرها نظرا لما يتيحه من وسيلة اعلام عالمية هي في الوقت ذاته سلاح خطير، اذ تقوم هذه التنظيمات باستخدام الفضاء الالكتروني في الدعاية والتجنيد والتمويل وجمع المعلومات وتنسيق الهجمات الارهابية وحشد المتعاطفين من مختلف دول العالم، بالإضافة الى سهولة استخدام الارهاب الالكتروني وتنفيذه من اي مكان في العالم ولا يلزم ان يكون الفاعل في موقع العمل الارهابي بل يكفي ان تتوافر على نطاق واسع وصلات الانترنت اللازمة لتنفيذ الهجوم باستخدام اي هاتف محمول حديث، ولا تعتمد سرعة الهجمات الالكترونية على سرعة وصلة الانترنت التي يستخدمها المهاجم بل يمكن استغلال السرعة العالية لوصلة الانترنت التي تستخدمها الحواسيب التي تتعرض للهجوم وذلك لان (الفايروسات) وغيرها من البرمجيات المؤذية يمكن ان تنتشر بأعلى سرعة ممكنة دون الحاجة الى المزيد من التدخل من المهاجم، ويمكن ابقاء الاعمال المرتكبة عبر الشبكة مجهولة المصدر وغير قابلة لاقتفاء اثرها وتتبعها عن طريق خدمات تجهيل المصدر وما شابهها من تقنيات التمويه مثل استخدام حواسيب مسيطر عليها عن طريق القرصنة، ويزيد من الاغراء بالإرهاب الالكتروني انخفاض تكلفة الانترنت وكثرة الاهداف التي يمكن قصدها واختيار مهاجمتها وكثير من تلك الاهداف قد لا يتمتع بحماية كافية، وفي ظل هذه المغريات سارعت مختلف التنظيمات والجماعات الارهابية الى امتلاك مواقع على الانترنت وبخاصة شبكات التواصل الاجتماعي من اجل التعريف بأهدافهم الفكرية والسياسية ومهاجمة خصومهم من العلماء والمفكرين ومن الحكومات والاجهزة الامنية.

وهناك العديد من المخاطر المترتبة على الارهاب الالكتروني ومن ذلك على سبيل المثال : تعطيل الاتصالات والتشويش عليها، والتنصت على المكالمات وبث معلومات مضللة وتقليد الاصوات وخاصة اصوات القادة العسكريين لإصدار اوامر خطيرة ، واستهداف شبكات الحاسوب بالتخريب عن طريق نشر (الفايروسات) ، مسح الذاكرة الخاصة بالأجهزة المعادية، منع تدفق الاموال وتغيير مسار الودائع، وايقاف محطات الكهرباء عن العمل عبر اعداد قنبلة الكترونية خاصة يطلق عليها اسم (Cbu49) تنطلق منها عدة قنابل في الجو تستهدف محطات الكهرباء وتؤدي الى احتراقها وتدميرها بالكامل.

وبالنسبة للعراق يمكن اعتبار تهديدات الامن السيبراني (تحديات غير مرئية) تؤثر على منظومة الامن الوطني العراقي، فالتطور التكنولوجي الذي شهده العراق في مجال الاتصالات والمعلومات بعد عام ٢٠١٣ والذي تزامن مع ضعف الأمننة الالكترونية في البنية التحتية الوطنية (سواء كانت امنية ام شخصية ام مصرفية) ادى الى ان يصبح العراق منكشفا استراتيجيا لكثير من دول العالم لاختراقه والتجسس على المعلومات الخاصة بالمؤسسات كافة واستخدامه لشن الهجمات الالكترونية لضرب امن معلومات اي دولة كانت واختراقه وتنفيذ عمليات ارهابية، ومن ابرز تلك الاخطار والتهديدات (الاختراق الالكتروني، الارهاب الالكتروني)، ويكفي ان نشير في هذا الصدد الى تنظيم داعش الارهابي وتوظيفه للتطورات التكنولوجية الحاصلة في وسائل الاتصال والتواصل وخصوصا عبر شبكة الانترنت في بث عمليات الاعدام التي يقوم بها ضد الاسرى من اجل بث الرعب والخوف في نفوس اهالي المدن التي كان يرغب في السيطرة عليها بهدف دفعها الى الاستسلام خوفا من تعرضها لمصير من سبقها، كما سمح التطور التقني لتلك الجماعات الارهابية بإخفاء عملياتها بطرق جديدة فضلا عن

تجنيد العديد من الشباب عبر المواقع الالكترونية، وقامت الجماعات الارهابية باستغلال التطورات الحاصلة في المجال التكنولوجي في تطوير اهدافها وعملياتها وادواتها وهو ما مثل ويمثل تهديدا للأمن الوطني العراقي.(صلاح،٢٠٢٠، ص٢٨٣.)

ولعل من الاحداث المهمة والمناسبات السنوية التي تمثل حدثا عالميا يشهد حضور الملايين زيارة اربعين الامام الحسين ﷺ ، تلك الزيارة التي تعد واحدة من اكبر التجمعات الدينية في العالم، ففي كل عام يستنفر العراق جهوده لاستقبال الزائرين من كل مكان لأداء مراسم الزيارة الاربعينية (اربعينية الامام الحسين ﷺ) في كربلاء، ومع اهمية ذلك الحدث العظيم قد تكون هناك محاولات من قبل التنظيمات الارهابية للتأثير في هذه المناسبة وهذا الحدث ، والتأثير في جموع وحشود الزائرين عبر اللجوء الى الارهاب الالكتروني وذلك من خلال بث الدعايات والشائعات المغرضة التي يمكن ان تنعكس على حركة ونشاط الزائرين بهدف تخريب تلك المناسبة فضلا عن استخدام الجانب التقني عبر الاستفادة من خدمة البريد الالكتروني لنشر افكارهم والترويج لها او عبر اختراق وتخريب المواقع او التهديد والترويع الالكتروني عن طريق ارسال رسائل تهديد من اجل نشر الرعب والخوف بين صفوف الاشخاص سواء كان التهديد بقتل شخصيات معينة او التهديد بتفجير منشآت وطنية، وكل ذلك الغاية منه التأثير في الاشخاص والجموع من اجل ثنيها عن القيام بما تعتقده صحيحا وصائبا ومن ذلك اداء الطقوس الدينية الصحيحة وزيارة الائمة الاطهار ﷺ ومن ابرز تلك المراسم زيارة اربعين الامام الحسين ﷺ.(مباركة،٢٠١٧، ص٣٤٧ ؛ عبد الحميد , ٢٠٢٤، ص٧)

ومن ابرز اشكال التهديدات الالكترونية التي يمكن ان تقع خلال زيارة الاربعين الآتي:

- الهجمات السيبرانية من خلال استهداف شبكات الاتصال ، قطع الانترنت، تعطيل نظم الاتصالات في وقت الذروة.
- حملات التضليل الاعلامي من خلال نشر اخبار كاذبة حول تفجيرات مزعومة او بث مقاطع مفبركة تهدف الى اثارة الذعر.
- التحريض الطائفي عبر الفضاء الرقمي من خلال بث محتوى يثير النعرات بين مكونات واطياف الشعب العراقي.
- استهداف انظمة النقل والامداد من خلال اختراق تطبيقات الملاحة او منصات الدعم اللوجستي.
- جمع بيانات المستخدمين من خلال عمليات تجسس رقمية على المتطوعين او المنظمين او الزائرين.

ومن اجل مواجهة خطر تهديد الارهاب الالكتروني للتنظيمات الارهابية وتأثيره في الامن السيبراني العراقي والحفاظ على الامن الوطني العراقي خصوصا خلال زيارة اربعين الامام الحسين عليه السلام ، فإن ذلك يستدعي اليات يمكن تحديدها كما يأتي:

١. وجود اجهزة مختصة بمواجهة التهديدات السيبرانية تمتلك منهجية لحفظ امن البلد وسلامته والعمل على تحقيق الامن الوطني عبر منع الاعداء من النيل من سيادة وامن البلد، بالاعتماد على وسائل عدة في تلك المواجهة اهمها الرقابة والتدقيق الالكتروني من اجل تعزيز الامن السيبراني والمحافظة على الامن الوطني. (المعموري،٢٠٠٣، ص١٤٢)

٢. ايجاد فريق وطني مشترك مختص بمجال الامن السيبراني والاستجابة للحوادث السيبرانية وحماية البنية التحتية للأنترنت، ونشر الوعي في مجال حماية الخصوصية والحماية الذاتية للأفراد والمؤسسات ، وان يحمل على عاتقه مسؤولية تأمين وحماية الشبكات ومراكز البيانات الوطنية والمواقع الرسمية التي تعمل في مجال الفضاء السيبراني، وتنسيق الجهود الوطنية ودعم المؤسسات في القطاعين العام والخاص في حماية نفسها وخدماتها في الفضاء السيبراني.

٣. تطوير الوسائل التقنية الالكترونية لتحقيق الامن السيبراني، اذ يعتمد ضمان سرية المعلومات ومحتواها وتوافرها عند الحاجة اليها على مجموعة من الادوات والوسائل التقنية التي تستخدم للوقاية من خطر التهديدات الالكترونية، او التخفيف من حجم الخسائر والاضرار الناجمة في حال حدوثها ، وتتعدد وسائل الحماية بحسب طبيعتها والغرض من استعمالها ، ويتم ذلك عبر مجموعة من الوسائل الاجرائية التي يقصد بها تقوية اجهزة التحريات والمعلومات من قبل الاجهزة المعنية والتي تؤدي الى ضبط مرتكبي الجرائم والمساهمة في ردعهم والاجهاض المبكر للعمليات الارهابية وكشف المخططات الاجرامية للإرهابيين والهجوم عليهم وضربهم بالطريقة الاستباقية بعد جمع المعلومات الضرورية والدقيقة عنهم وعن مخططاتهم، وبذلك تعتبر الوسائل التقنية الجانب الاهم في مجال تحقيق الامن السيبراني ومواجهة التهديدات الالكترونية، ومن الوسائل التي تؤدي الى مقاومة التهديدات السيبرانية التي يجب على الاجهزة الامنية اتباعها لغرض حماية المنظومة المعلوماتية من الانكشاف الاتي:

١. تشفير البيانات المهمة المنقولة عبر الانترنت.

٢. ايجاد نظام امني متكامل يقوم بحماية المعلومات والبيانات.

٣. العمل على توفير برامج الكشف عن الفيروسات والمقاومة لحماية الحاسوب.

٤. عدم استخدام شبكات الحاسب الالي المفتوح لتداول المعلومات الامنية مع عمل وسائل تحكم في الدخول الى المعلومات والمحافظة عليها.

٥. تطبيق التوقيع الالكتروني وتكمن اهميته في زيادة مستوى الامن والخصوصية في التعاملات لقدرتها على حفظ سرية المعلومات والرسائل المرسلة كما يمكن تحديد هوية وشخصية المرسل والمستقبل الكترونيا مما يمنع التحايل والتلاعب بالمعلومات.

٦. تقنية الدخول على الانترنت والقيام بحجب المواقع الضارة للجماعات والتنظيمات الارهابية التي تدعو للفساد والشر والارهاب والعدوان وتحرض عليها وتساهم في تعلمها.

٧. استخدام تقنية جدران النار التي تعمل كمصفاة تمنع وصول الطلبات المشبوهة الى الاجهزة المزودة اعتمادا على السياسات التي يحدد بموجبها مدراء الشبكة طبيعة المعلومات التي يسمح للعاملين بالمؤسسة الولوج اليها.

٨. تأمين حسابات المستخدمين ونظم التحقق من الهوية.

٩. اعتماد تقنية التشفير الالكتروني للوقاية من التنصت على حزم المعلومات الخاصة والمنشآت الحيوية.

١٠. التركيز على وسائل التواصل الاجتماعي واتقان العمليات المتعلقة بها عن طريق التكنولوجيا الحديثة لدحض وتفنيد ومحاربة الافكار الارهابية المتطرفة.

وينبغي على الاجهزة المعنية بتحقيق الامن السيبراني استخدام تلك الوسائل استخداما فعالا عبر توافق الوسيلة المستعملة مع درجة السرية المعلومة وحجم الضرر الناجم عن تعرضها لاعتداءات الكترونية من اجل ضمان تحقيق الامن السيبراني بالشكل المطلوب.

الخاتمة

يمثل الامن الهدف المنشود للإنسان ، ومع تطور المجتمعات والثورة المعلوماتية والاتصال والتوجه الى عالم المعرفة والمعلومات تشكل فضاء جديد هو الفضاء السيبراني الذي تستعمله الدولة، واوجدت هذه التطورات التقنية والمعلوماتية العديد من التهديدات الامنية وخاصة على المستوى الوطني الذي اصبح اكثر عرضة لخطر الانكشاف بسبب سهولة الحصول على المعلومات الذي وفرته وسائل الاتصال والتواصل الحديثة مع وجود العديد من وسائل الاقتناص الامني والمعلوماتي التي تهدف للاستحواذ على المعلومات المنتشرة عبر الفضاء الالكتروني بمختلف الطرق والاساليب، وهو ما استدعى تطوير مفهوم جديد للأمن من اجل مواجهة تلك التهديدات والتحديات الالكترونية وجاء مفهوم الامن السيبراني كرد فعل على تلك التهديدات من اجل الحفاظ على الامن الوطني وسلامة الدول وسيادتها لان الامن السيبراني المعلوماتي يمارس دورا مهما في حماية الامن الوطني للدولة، فهو قد يهدد امن الدولة كليا اذا ما تعرض للانكشاف او الاختراق الامر الذي قد يكلف الدولة الكثير من الخسائر على المستوى الامني والسياسي والاجتماعي والاقتصادي.

وفيما يخص العراق يمثل الارهاب الالكتروني تحديا امنيا متعاظما في سياق زيارة الاربعين ، اذ تنتقل التهديدات من الميدان الى الفضاء السيبراني ، ومع ذلك فان التجربة العراقية في ادارة الزيارة اثبتت مرونة في التصدي للهجمات الرقمية ومع ذلك فان الامر يستدعي استراتيجية وطنية للأمن السيبراني تربط بين الابعاد الامنية والدينية والسياسية لهذا الحدث الفريد.

التوصيات

توصل البحث الى التوصيات الاتية:

أ. انشاء استراتيجية وطنية للأمن المعلوماتي تهدف الى:

- اقامة نظام وطني منسق للاستجابة لأمن الفضاء السيبراني.
- انشاء جهة تنسيق لإدارة الحوادث السيبرانية وتضم العناصر المهمة والاساسية في الحكومة والعناصر الاساسية من مشغلي البنية التحتية بغية الح من المخاطر.
- المشاركة في اليات مراقبة الحوادث والانذار بوجودها والاستجابة لها وتقاسم المعلومات.
- وضع الخطط والاجراءات بشأن الاستجابة لحالات الطوارئ واختبارها والتدريب عليها والتعاون بين الجهات الحكومية وغير الحكومية وقت الازمات.

ب. الترويج لثقافة وطنية خاصة بتنمية الوعي بالأمن السيبراني وبذل كافة الجهود في هذا المجال.

ج. سن القوانين والتشريعات الخاصة بمواجهة الجرائم السيبرانية.

د. حجب المواقع الالكترونية المشبوهة التي تسعى الى نشر الارهاب والافكار المتطرفة.

هـ. تفعيل الدور الوقائي الذي يسبق وقوع الجريمة السيبرانية وذلك من خلال تفعيل دور المؤسسات التوعوية مثل: (المساجد ، الاسرة ، مؤسسات التعليم ، اجهزة الاعلام) وذلك من اجل التوعية بخطورة تلك الجرائم على الاسرة والمجتمع.

و. التركيز على توافر انظمة المعلومات وتمتين الخصوصية وحماية سرية المعلومات الشخصية واتخاذ الاجراءات الضرورية لحماية المواطنين من مخاطر الفضاء السيبراني.

ز. دراسة مقارنة بين التهديدات الالكترونية خلال زيارة الاربعين وسائر الفعاليات الدينية الكبرى عالميا والاستفادة من الاجراءات والاليات المتخذة.

ح. تحليل بيئي سيبراني للجهات المروجة للتحريض الرقمي الطائفي.

ط. بناء انظمة ذكاء اصطناعي للتنبؤ بالهجمات السيبرانية خلال الزيارات المليونية وخصوصا زيارة اربعين الامام الحسين عليه السلام.

المصادر

١. احمد فاروق مطني و د. خالد عبدالاله، سبل مواجهة الارهاب التكنو-معلوماتي في العراق بعد العام ٢٠٠٦، المجلة السياسية والدولية، كلية العلوم السياسية، الجامعة المستنصرية، العدد ٥٣، كانون الاول ٢٠٢٢.

٢. احمد فاروق العزاوي، الارهاب التكنو معلوماتي وتأثيره في النظام السياسي العراقي ما بعد ٢٠٠٦ دراسة في اليات التوظيف ، كلية العلوم السياسية الجامعة المستنصرية، بغداد، ٢٠٢٢.

٣. ايسر محمد عطية ، دور الاليات الحديثة للحد من الجرائم : الارهاب الالكتروني وطرق المواجهة ، دراسة مقدمة الى الملتقى العالمي ، كلية العلوم الاستراتيجية الاردن ، ٢٠١٤.

٤. ايناس ممدوح محمد، دور الامن السيبراني في مواجهة الارهاب الالكتروني ، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، العدد ١، يناير ٢٠٢١.

٥. باسم علي خريسان ، الفضاء السيبراني مدخل ايستيمولوجي ، دار قناديل للنشر والتوزيع ، بغداد ، ٢٠٢١ .

٦. حازم الشمري ، توظيف القوة السيبرانية في استراتيجيات الدول الكبرى ، دار انكي للنشر والتوزيع ، بغداد ، ٢٠٢٢ .

٧. ريتشارد كلارك ، روبروت نيك ، حرب الفضاء الالكتروني التهديد الثاني للامن القومي وكيفية التعامل معه ، مركز الامارات للدراسات والبحوث الاستراتيجية، ابو ظبي ، ٢٠١٢.

٨. سامر مؤيد عبداللطيف، الارهاب الالكتروني وسبل مجابهته، مجلة جامعة كربلاء العلمية، مركز الدراسات القانونية والدستورية، جامعة كربلاء، العدد ٣، ٢٠١٦.

٩. عادل عبيد صحن الموسوي ، نحو مرتكز جديد في استراتجية الامن الوطني العراقي : الامن السيبراني إنموذجا ، رسالة ماجستير ، علوم سياسية ، معهد العلمين للدراسات العليا ، النجف الاشرف ، ٢٠٢١.

١٠. عبد الله محمد العضيني ، السيبرانية واشكال الحروب في المستقبل ، صحيفة الجزيرة السعودية العدد (١٦٥١٩) ، ٢٠١٧.

١١. علي ابراهيم المعموري، الامن السيبراني العراقي واثره في الامن الوطني العراقي بعد العام ٢٠٠٣، رسالة ماجستير غير منشورة، كلية العلوم السياسية ، جامعة بغداد.

١٢. علي جاسم محمد ، الارهاب الالكتروني واثره على المجتمع ، المجلة السياسية والدولية – الجامعة المستنصرية ، كلية العلوم السياسية، العدد (٣٣-٣٤) ، ٢٠١٨.

١٣. مبادرة الباحثون السوريون ، الفرق بين امن المعلومات والامن السيبراني ، على الرابط الالكتروني التالي : www.syres.comlarticle.

١٤. محمود الحمدان، الارهاب الالكتروني وسبل المواجهة، موقع التحالف الاسلامي العسكري لمحاربة الارهاب، ٢٠٢١/١/٢١ على الرابط الالكتروني:https://www.imctc.org

١٥. نورة شلوش ، القرصنة الالكترونية في الفضاء السيبراني ، مجلة بابل للدراسات الانسانية ، عدد (٢) ، ٢٠١٨.