دور الأمن السيبراني في مكافحة التطرف

The role of cybersecurity in combating extremism

الباحث : علي قاسم خيرالله *

عضو لجنة مكافحة التطرف العنيف المؤدي للأرهاب /مستشارية الأمن القومي

Researcher: Ali Qasim Khairallah

Member of the Committee to Combat Violent Extremism that Leads to Terrorism/National Security Advisory

aq776881@gmail.com

الملخص:

لقد تسببت الرقمنة العالمية بشكل كبير بالاعتماد على الانترنت، سواء في الحياة الشخصيّة أو المهنيّة، او حتى في الامور المالية و المصرفية ، متداخلة مع باقي البرامج الخاصة بالتواصل الاجتماعي، أو حتّى ممارسة الاعمال عن طريق الانترنت و بصورة مريحة و سريعة و سلسلة سواء ابتداء من الدخول و انتهاءا بالممارسة الطويلة الا انها اظهرت بمرور الوقت عدة معوقات اثرت على عمل الفضاء الالكتروني و من ثم اثرت على الافراد و حياتهم الخاصة ذلك لما بدات تحويه من جرائم افتراضية هددت امن الافراد بل و حتى المؤسسات و الدولة بشكل عام ، فظهرت السرقة الالكترونية و الارهاب الالكتروني و غيرها على المستوى الشخصي فتوسعت رقعة التهديد لتستغلها الجماعات الارهابية في التهديد و نشر الارهاب و نشر الايديلوجية المتطرفة و جذب المتطرفين فقد استخدمت التنظيمات الإرهابية منصات التواصل الاجتماعي لأغراض التجنيد من خلال تحديد الأهداف المحتملة عبر مراقبة ملفات التعريف والمحادثات على تلك المنصات، بهدف اختبار مدى تعاطف مختلف المستخدمين مع الفكر الإرهابي، ثم إضافتهم كأصدقاء للتواصل المباشر معهم .

و وصل الامر الى استثمار هذا العامل من قبل بعض الدول لتسبب الاذى للدول المعادية لها و من هنا جاءت اهمية الامن السيبراني لكي تضع حد لانتهاكات الفضاء الالكتروني . و بهذا يعتبر الأمن السيبراني أحد أبعاد الأمن القومي غير التقليدي، بالنظر إلى تعدد التهديدات السيبرانية المحتملة وما قد ينتج عنها من خسائر سياسية وعسكرية واقتصادية فادحة. ومن هذا

* حائز على المركز الاول في مسابقة افضل بحث تخرج حول موضوع التطرف من وزارة التعليم العالي والبحث العلمي عام 2023

المنطلق، أولت نظريات العلاقات الدولية اهتمامًا بالغًا بالأمن السيبراني لتدفع الواقعية بأن الدول في سعي حثيث لتطوير قدراتها السيبرانية الهجومية بهدف استخدام الإنترنت كسلاح استراتيجي.

الكلمات المفتاحية :الاستراتيجية ،الأمن السيبراني ، الرقمنة ، التطرف ،الارهاب .

Abstract:

Global digitization has caused a great deal of dependence on the Internet, whether in personal or professional life, or even in financial and banking matters, intertwined with the rest of the programs for social networking, or even doing business via the Internet in a comfortable, fast and smooth manner, whether from entry to long practice, but it has shown over time several obstacles that affected the work of cyberspace and then affected individuals and their private lives so that when It began to contain virtual crimes that threatened the security of individuals and even institutions and the state in general, so electronic theft, electronic terrorism and others appeared on the personal level, so the threat expanded to be exploited by terrorist groups in the threat, spreading terrorism, spreading extremist ideology and attracting extremists, terrorist organizations used social media platforms for recruitment purposes by identifying potential targets by monitoring profiles and conversations on those platforms, with the aim of testing the extent to which different users sympathize with terrorist ideology, then add them as friends to communicate directly with them.

The matter reached the exploitation of this factor by some countries to cause harm to countries hostile to them, hence the importance of cybersecurity in order to put an end to violations of cyberspace. Thus, cybersecurity is considered one of the dimensions of non-traditional national security, given the multiplicity of potential cyber threats and the resulting heavy political, military and economic losses. From this standpoint, international relations theories have paid great attention to cybersecurity to push the realism that countries are actively seeking to develop their offensive cyber capabilities with the aim of using the Internet as a strategic weapon.

Keywords: strategy, cybersecurity, digitization, extremism, terrorism.

المقدمة:

يعد الامن واحد من اهم مقومات الحياة الاجتماعية منذ النشأة , و عليه تعمل الدول و بشتى الطرق الى المحافظة عليه و تطويره وفق الحاجة اضافة الى ديموته ذلك من خلال تعزيز مجموعة من المقومات السياسية و الاجتماعية و العسكرية و حتى الاقتصادية و نتيجة للتطور الرقمي الذي حصل في العقود الاخيرة و الطفرة الرقمية على المستوى العالمي ظهرت هناك مشاكل و سلبيات مرافقة لايجابيات التقنية الحديثة و منها ما يستدعي الاستعداد للمواجهة كونها اصبحت تؤثر على الامن القومي للدول و لهذا باشرت دول عديدة الى وضع ملف اخر و هو ملف الامن السيبراني على اجندتها .

و مع تزايد الثورة المعلوماتية في مجال التواصل زادت نسب الخطر السيبراني و تاثيراته ابتداء من المجال الاقتصادي و وصولاً الى المجالات الاخرى كالاتصالات و قطاعات الصحة و التعليم و غيرهاو التي ارتبطت بشكل او باخر بامن المجتمع و الدولة مما دعى اصحاب القرار و الاختصاص انهم يدؤكون بانه لايمكن فصل امن الفضاء السيبراني و السياسة و الاقتصاد و الامن القومي للدولة .

هدف البحث: يهدف هذا البحث الي بيان اهمية التطور التكنلوجي و كذلك اهمية الرقمنة العالمية و دخولها في كافة مجالات الحياة السياسية و الاجتماعية و الاقتصادية و على الاثار و المخاطر الامنية المترتبة عليه , لذلك جاء هذا البحث ليبين اهمية الامن السيبراني و دوره المهم في حماية الامن القومي للدول و كذلك يستعرض المشاكل و الثغرات التي يواجهها العراق في هذا الجانب خاصة في الجانب الفكري العنيف و المتطرف .

مشكلة البحث: يستعرض البحث مشكلة الامن السيبراني والدور الذي يلعبة في مواجهة التطرف العنيف و الافكار المتطرفة و كيفية معالجتها خصوصا ان العراق واحد من اكثر الدول التي تواجه التطرف , و وتعمل على تحديد الجهة المسؤولة عن وضع المعالجات .

فرضية البحث: تنطلق الفرضية من تساؤل مهم و هو ما مدى تاثير هذه التطرف على المجتمع و من ثم ما اهمية حماية الخطر الامني عن طريق الامن السيبراني و ماذا على الدولة و الحكومة ان تعمل و الى أي مدى لها ان تتخل .

هيكلية البحث :قسم البحث الى مقدمة ذكرت فيها اهمية اختيار الموضوع , و من ثم اشكاليته و فرضيته , ثم جاءت بعد ذلك ثلاثة مباحث :**المبحث الاول** يتحدث حول التطرف مفهومه و تاريخه و اشكاله و دوافعه و جواذبه .

المبحث الثاني يتحدث عن مفهوم و تاريخ الامن السيبراني و فواعله و انواع الهجوم السيبراني و كذلك واقع الامن السيبراني عربياً و محلياً . المبحث الثالث و يتحدث عن دور الامن السيبراني في مكافحة التطرف العنيف . و من ثم خاتمة و توصية و استنتاجات .

المبحث الاول :التطرف "نظرة تاريخية" يعد التطرف ظاهرة قديمة عرفتها الامم منذ القدم , وقد واكبت هذه الظاهرة مختلف اشكال الصراع بين الافكار و الارادات و المجموعات العرقية , و هناك مقولة لليهود ان التوراة و السيف قد نزلا معاً من السماء , و قد عرف الارهاب منذ فجر التاريخ الفرعوني في مصر , كما ان الحضارات الهيلينية و الرومانية قد عرفتا صنوفاً من التطرف و الارهاب انعكس بعد زولهما على الحضارات المسيحية و الاسلامية بين الفرق و الاحزاب آنذاك , و قد سجلت القرون الوسطى ابشع صور البطش و العنف متمثلة بالمحاكم التفتيش التي نصبها الباباوات للانتقام من المارقين و كل من الايدين بالولاء لهم [1]

اولا:مفهوم التطرف يعد مفهوم التطرف من المفاهيم المطاطية ذات الصعوبة في التحديد بشأن اعطائها تعريف مطلق , ذلك كون ما يذهب اليه المعنى اللغوي من تجاوز لحدود العدل و ان هذا الحد بذاته غير ثابت بحيث يتغير من بيئة اجتماعية الى بيئة اخرى وفقاً لنسق القيم السائدة في كل بيئة اجتماعية فما يعتبر تطرفاً في مجتمع يعد امر طبيعي في مجتمع اخر و مألوفاً , ان التطرف و الاعتدال يرهن بالوضع البيئي و الحضاري و السياسي و الثقافي و التي يمر بها . [2]و كذلك يختلف مفهوم التطرف باختلاف الفترات الزمنية فما كان معروف سابقاً قد تغيير وفقاً لظروف خاصة الا اننا سنحاول ان نتطرق لاهم ما تناوله الباحثين و من [3] ثم نصل الى تعريف مناف لهذا المفهوم , و من هذه : يقصد بالتطرف : (اتخاذ الفرد موقف متشدداً يستم هذا الموقف بالقطيعة في استجاباته للمواقف الاجتماعية التي تهمه , و الموجودة في بيئته التي

1 تيري إيغلتون. أوهام ما بعد الحداثة. المركز العربي للأبحاث ودراسة السياسات, 2019, ص8

2 عبد الصمد الديالمي ,دار الساقي .المدينة الإسلامية والأصولية والإرهاب: مقاربة جنسية.

3 نايل ممدوح أبو زيد "الوسطية حاجة ذاتية وضرورة إنسانية–دراسة قرآنية" , مجلة 12 العدد 3.

يعيش فيها الان , و قد يكون التطرف ايجابياً في القبول التام , او سلبياً في اتجاه الرفض التام , و يقع الاعتدال في منتصف المسافة بينهما) .[1] و كذلك يعرف التطرف:بانه الغلو في عقيدة او فكرة او مذهب او غيره و يختص به دين او جماعة حزب.

ثانيا:أشكال التطرف :ان اشكال التطرف متعددة بتعدد مجالات الحياة منها ما هو سياسي (اليميني أو اليساري) و منها ما هو تطرف عرقي ومنها ما هو تطرف اجتماعي و ما هو تطرف ديني وكثيراً من الاشكال الاخرى ، وأيا من هذه الاشكال الذي يأخذه التطرف إلا انه يمكننا ان نقسمه إلى ثلاثة أنواع .

أولا : التطرف المعرفة يعني أن ينغلق الشخص على أفكار معينة ، ولا يقبل المناقشة أو إعادة النظر فيها ، ويعتبرها من الثوابت المطلقة ، وهو في هذه الحالة لا يلغي وظيفة عقله فقط في تمحيص هذه الأفكار بل إنه يلغي أي رأي آخر مخالف ، ولا يسمح لهذا الرأي أن يدخل مجال وعيه فضلا عن أن يتفهمه أو يناقشه أو يتقبله.

ثانياً : التطرف الوجداني: (شعور حماسي يطغي على نحو شيء معين يجعل الشخص مندفعا في اتجاه معين دون تبصر وربما يدفعه هذا الانفعال إلى تدمير نفسه أو غيره ، وربما يندم بعد ذلك حين تخف حدة هذا الانفعال) [2]ويعود إلى رشده ، وفي بعض الأحيان لا يحدث هذا وإنما يظل الشخص يشحن نفسه

ثالثاً : (التطرف السلوكي هي المغالاة في سلوكيات ظاهرية معينة بما يخرج عن الحدود المقبولة وكأن هذه السلوكيات هدف في حد ذاتها ولذلك يكرهها الشخص بشكل نمطي وهي خالية من المعنى وفاقدة للهدف . ولا يتوقف الأمر عند الشخص ذاته بل يحاول إرغام الآخرين على التقيد بما يفعله هو قهراً أو قسراً ، وربما يلجأ إلى العدوان على الآخرين لإرغامهم على تنفيذ ما يريد)[3]

ثالثا:دوافع التطرف(يعد غسيل الدماغ من أدوات التطرف الرئيسة اذ يدور محوره حول إلغاء

[1] http://www.moqatel.com/openshare/Behoth/Mnfsia15/Extremity/sec01.doc_cvt.htm

[2] مجلة العلوم الأساسية Basic Science journal ISSN 2306-5249 وظائف العدد الثاني ٢٠٢١م / ١٤٤٢هـ (المؤيد أو الرافض).

[3] أ. د. نايل ممدوح أبو زيد. الوسطية حاجة ذاتية وضرورة إنسانية–دراسة قرآنية. 2015.

شخصية الفرد بمعنى نقل الشخصية المتكاملة أو التي تعد متكاملة إلى حد التمزق العنيف، ويصبح من الممكن التلاعب بها للوصول بها إلى أن تكون أداة طيعة في أيدي مثيري الفتن)[1].

وقد مارست التنظيمات الإرهابية غسيل الدماغ بأساليب التجديد الفكري مستغلة الظروف الاقتصادية والمشاكل الاجتماعية وبعض أخطاء الحكومية فضلاً عن إغرائهم بحور العين في الجنة واستخدام آيات قرآنية وتوظيفها بطريقة تنسجم مع أهداف الإرهاب وبصورة بعيدة جدًا عن المضمون الحقيقي [2].كذلك أدى الفراغ الأمني والقانوني بعد 2003م إلى سيادة الفوضى وأعمال التخريب والإرهاب، ومن ثم بروز الطروحات الطائفية لتستغل من قبل منظمات ظهرت بشكل واضح مدعومة من قبل دول ومخابرات إقليمية ودولية مستغلة التراكمات والسياسات الشوفينية للنظام السابق وقد مر العراق بأزمات متعددة مازال يعاني منها [3] والتي كونت دوافع التطرف وهي:

اولاً: ازمة اسرية ويعد الفشل في الحياة الأسرية من أهم الأسباب المؤدية إلى جنوح الأفراد واكتسابهم بعض الصفات السيئة، وبالنتيجة التطرف والوقوع في متاهات التطرف وامتهان [4]، وأن رفقة السوء من العوامل الكبيرة ولا سيما إذا كان الشخص ضعيف العقيدة متميع الخلق سرعان ما يكتسب من الأشرار أحط العادات وأقبح الصفات حتى يصبح الإجرام جزءًا من طبعه .

ثانياً : أزمة الهوية تتعلق هذه الأزمة بتشكيل روابط مشتركة وشعور واحد بين أفراد المجتمع الواحد المجتمعات الأخرى. الذين توحدهم مميزات تختلف عن غيرهم في إن التنوع في مكونات المجتمع العراقي وتعدد الثقافات العرقية لم يرتق إلى الاندماج في هوية وطنية شاملة، وأن التمسك بهذه الانتماءات الضيقة يؤثر على خطط التنمية السياسية، ويضع الوحدة الوطنية في خطر دائم

ثالثاً : أزمة الشرعية هذه الأزمة ترتبط بأزمة الهوية، وتتعلق بشرعية السلطة وتوزيع المسؤوليات الخاصة بالنظام السياسي، من بينها سياسة المحاصصة , مما أدى إلى تأجيل عدد من

[1] مجموعة مؤلفين .المدينة العربية: تحديات التمدين في مجتمعات متحولة .المركز العربي للأبحاث ودراسة السياسات, 2020.

[2] مصدر سابق

[3] برهان غليون. نظام الطائفية من الدولة إلى القبيلة. المركز العربي للأبحاث ودراسة السياسات, 2017.

[4] صالحي بن شريف; حنيفة. الأسرة و عنف الطفل: علاقة افتراضية أم حتمية؟/ Insaniyat .إنسانيات . Revue algérienne d'anthropologie et de sciences sociales, 2008, 41: 35-50.

المشكلات المتعلقة بالدستور الدائم، مثل طبيعة النظام السياسي, هوية العراق, توزيع الثروات إلى أجل غير معلوم, ومن جانب آخر فإن تردي الوضع الأمني, وقلة الخبرة السياسية لدى النخبة الحاكمة والتكلؤ في تقديم الخدمات وانتشار الفساد في مؤسسات الدولة وتفاقم البطالة أدى إلى فقدان النظام السياسي للثقة مع الجماهير [1]

رابعاً : أزمة التغلغل: (هذه الأزمة يتسبب بها ضعف النظام السياسي ومؤسساته في التعبير عن إرادة المواطنين، ومن ثم التقصير في الأداء على المساحة الجغرافية أو في البنى المجتمعية عاموديا, وعلى النظام السياسي أن يتمكن من الوصول إلى مستوى القرية, ويؤثر في الحياة اليومية، ومن أسباب الأزمة, وانخفاض مستوى أداء القوات الأمنية) [2]

خامساً : أزمة المشاركة السياسية تنتج هذه الأزمة عن عدم إسهام أعداد كبيرة من المواطنين في الحياة العامة واتخاذ القرارات السياسية واختيار أعضاء السلطة التشريعية. و نتيجة لذلك جاءت التنظيمات السرية والجماعات المسلحة لتملأ الفراغ بسبب افتقاد الشباب أي فرصة للممارسات السياسية التي تنمي لديهم القدرة على إبداء الرأي والحوار حول مسائل سياسة أو اجتماعية عامة [3]إن شيوع القهر والقمع من قبل الدولة يلعب دورًا مهما في التطرف , ان الاستبداد مذهب يجعل المواطن خاضعًا إلى النظام القاسي المفروض من قبل السلطة ضد حرية الفرد، فيكون الحكم فرديًا غاشما، ومصدر النظام شخص واحد وصل إلى مركزه بالعنف ، وقد تجلى الحكم الفردي من خلال إلغاء الفصل بين السلطات الثلاث، وحصر السلطات كلها في يد الحاكم الفردي، وترافق الحكم الاستبدادي ظواهر أهمها التخلخل الاجتماعي إكثار التكاليف السياسية، وصعلكة الجماهير وتدجينها، خصوصا في الأزمات والاضطرابات والحروب .

سادساً : أزمة الاندماج: تعني هذه الأزمة التنسيق بين الرأي العام مع عمل السلطة التنفيذية وهي تمثل الحل الأمثل لأزمتي التغلغل والمشاركة، إن أزمة الاندماج تتركز على انتظام النظام السياسي كونه روابط متفاعلة تكون بين الجماعات والمصالح التي تسعى لتحقيق مطالبها لدى

[1] قيراط، محمد مسعود .الإرهاب: دراسة في البرامج الوطنية واستراتيجيات مكافحته: مقاربة إعلامية Naif . Arab University (NAUSS), 2011.

[2] مصدر سابق

[1] مجموعة مؤلفين .المسألة الطائفية وصناعة الأقليات في الوطن العربي .المركز العربي للأبحاث ودراسة السياسات, 2017.

النظام، والأزمة تتصل بكيفية اصطفاف الوحدات الاجتماعية السياسية والدينية والعرقية كي تنسجم في كتلة متجانسة[1]

سادساً : أزمة التوزيع تتعلق هذه الأزمة بتوزيع المواد والثروات في العراق، وتوزيع مردودات الدخل القومي, وسعي النظام السياسي إلى إعادة توزيع المدخلات لصالح المواطنين، فهناك أكثر من ربع السكان يعيشون تحت خط الفقر[1].

سابعاً : ازمة الاقتصاد إن الكثيرين يربطون وجود التطرف والإرهاب بالأوضاع الاقتصادية فهي التي تصنع الأحداث، فقد انتشر الفقر والبطالة، وضاقت بالشباب موارد الرزق فلم يجدوا عملا، ولا بيتا مريحًا، أو حياة زوجية مستقرة، أو غذاءً، أو كساء لأولادهم مما دفع بهم إلى الإرهاب[2].

إن المجتمع يعاني من مشكلات عدة، كمشكلة السكان والديون والبطالة وارتفاع الأسعار، وعدم التناسب بينها وبين الأجور، وجرائم الاعتداء على المال العام وانحرافات المسؤولين وتهريب المال العام إلى الخارج، كل هذا دفع الشباب إلى التطرف حيث يوجد نوع من التنفيس عن الطاقات المكبوتة , إن عدم الاعتراف بالآخر، والسعي لإقصائه أو إلغائه أو تهميشه على المستوى الداخلي علاقة الحكومات بالشعوب أو على المستوى الدولي و فرض الاستتباع وإملاء الهيمنة قادت إلى ادعاء الأفضليات الى امتلاك الحقيقة، واعتبار الآخر المختلف هو الخصم والعدو اما على المستوى الدولي إن النظام السياسي الدولي يفتقر إلى الحزم في الرد بعقوبات دولية شاملة ورادعة و كذلك يفتقد الى تعاون دولب مشترك لتحييد ظاهرة التطرف ، وعلى المخالفات والانتهاكات التي تتعرض لها مواثيقه، فالتسيب الدولي هو الذي يفتح المجال واسعا أمام الغلو والتطرف من المغرر بهم دينيا أو سياسيا أو عقائديا .

تشكل المظالم وقود التطرف و تختلف باختلاف المواقع , و يكون مدفوعاً في كثير من الاحيان بدافع المخاوف الشخصية و الاحباط من العلاقات فضلاً عن غياب المساواة بين الناس لأن تحقيق العدالة الاجتماعية و السياسية و الاقتصادية والإنصاف بين مختلف أفراد المجتمع في مجال التعليم والصحة والعمل تجعله إنسانا سويا، وحينما يشعر الفرد بفقدان العدالة لا يتساوى مع الآخرين فإنه يصبح شخصا عدوانيًا تجاه الآخرين، الأمر الذي يؤدي إلى التطرف [2]

[2] جلبير الأشقر; دار الساقي; نعوم تشومسكي .السلطان الخطير ،2017

[1] المركز الوطني للوقاية للتطرف العنيف , الولايات المتحدة الامريكية .

ويتضح مما سبق التطرف هو مشكلة عالمية تؤثر على المجتمعات والأفراد في جميع أنحاء العالم. و ببساطة يمكن تعريف التطرف على انه مفهوم يشير إلى الانحراف عن المعايير الاجتماعية العادية والقيم الأخلاقية المتفق عليها، والانخراط في أفكار وسلوكيات متطرفة وغير متزنة تتسم بالعدوانية والعنف والتعصب.

يمكن أن يأخذ التطرف أشكالًا مختلفة، مثل التطرف الديني، الذي يتمثل في تبني أفكار دينية متطرفة والانخراط في سلوكيات عنيفة وإرهابية تستند إلى تفسيرات خاطئة للدين. ويمكن أيضًا أن يكون التطرف السياسي، الذي يتمثل في تبني أفكار سياسية متطرفة والانخراط في أعمال عنف وإرهاب لتحقيق أهدافهم. وبشكل عام، يمكن تحديد أي سلوكيات متطرفة بأنها تتخذ شكلاً من أشكال التعصب والعنف والتهديد بالعنف، وتتنافى مع المعايير الأخلاقية والاجتماعية المتفق عليها في المجتمعات المختلفة.ويتميز التطرف بأنه يمثل خطرًا على الأمن والاستقرار والسلم العام في المجتمعات، ويتطلب العمل الجماعي والتعاون بين جميع أفراد المجتمع لمواجهته ومنع انتشار.

المبحث الثاني : الامن السيبراني

اولا: نشاة الامن السيبراني :(شهد العالم في القرنين العشرين والحادي والعشرين ثورة تكنولوجية متسارعة رافقها انعكاسات على جميع مجالات الحياة البشرية، ومع هذه الثورة التكنولوجية ظهرت مصطلحات ومفاهيم جديدة، منها ما كان مرتبطاً بالجانب الإيجابي للتكنولوجيا ومنها الجانب السلبي والمخيف أيضاً، وبدأت الدول من جهة والمفكرين والعلماء من جهة أخرى في البحث والدراسة للوقوف على كل جانب إما بتعزيز قوتها الاقتصادية والعسكرية ونهضتها أو بدرء الأخطار المحتملة للمحافظة على أمنها واستقرارها، ومن ذلك السيبرانية بمفهومها العام والسعي إلى تحقيق الأمن السيبراني.)[1]

وفي دراسة نشأة الأمن السيبراني نجد أن معالمها تلازمت بمرحلتين نوعيتين تاريخياً :

(المرحلة الأولى منتصف الخمسينات من القرن العشرين واستحداث أجهزة الكمبيوتر كأداة لمعالجة وحفظ المعلومات رقمياً (Digital) وما ترافق من جهود عدد من الشركات الخاصة والعامة، حيث توجت هذه الجهود بتطوير وحدة المعالجة المركزية (CPU)، وذلك لتسهيل المهام الموكلة له، واستمر هذا التطور ليصبح جهاز الكمبيوتر من أساسيات العمل لدى الشركات والأفراد لما في ذلك من توفير للجهد والوقت)[2]

المرحلة الثانية: (وهي فعلاً ثورة تكنولوجية غيرت مجرى الحياة البشرية، ألا وهي ظهور شبكة الانترنت، حيث وفي ثمانينيات القرن الماضي، قادت الأبحاث التي أشرف عليها السير (تيم بيرنرز) لي في المنظمة الأوروبية للأبحاث النووية (CERN) إلى تطوير شبكة الويب، ونتج عن ذلك ربط مستندات النص التشعبي بنظام معلومات يمكن النفاذ إليه من أي موقع على الشبكة، ومنذ منتصف التسعينيات كان لشبكة الإنترنت تأثير ثوري على الثقافة والتجارة والتكنولوجيا وشمل ذلك ظهور التراسل الفوري وتطوّر البريد الإلكتروني والمكالمات الهاتفية عبر شبكة الإنترنت (VoIP) ومكالمات الفيديو وشبكة الويب التي تضمنت منتديات النقاش وشبكات التواصل الاجتماعي ومواقع التسوق عبر الإنترنت.[1]

و لقد رافق تلك الثورة انعكاسات على الجانب العسكري والتسلح لدى الدول، وأطلق البعض على ذلك مصطلح الحرب السيبرانية الباردة (Cyber Cold War) أو سباق التسلح السيبراني.

و نجد أنه أول ما نشأ في مجال السيبرانية هو الجريمة السيبرانية، حيث كانت على شكل جرائم وجهها الجناة تجاه المؤسسات المالية والمصرفية، أضف إلى ذلك الشركات المتخصصة ببرمجة نظم الاتصالات، وقد سارعت بعض الدول اتخاذ المواجهة والإجراءات التشريعية والقانونية لتجريم الأفعال وتحديد العقوبات الموقع الإلكتروني).[2]

وما لبث أن اتجهت الأنظار وخصوصاً في علم العلاقات الدولية إلى هذا التطور والأخذ به كمصدر قوة وسلاح جديد وأصبح الباحثون يركزون بشكل متزايد حول أثر التكنولوجيا على الأمن القومي والدولي، ويشمل ذلك تأثيرها على المفاهيم ذات الصلة كالقوة (power) والسيادة (sovereignty) والحوكمة (securitization) والأمنية العالمية (global governance)

و بنفس نفس الصعيد بدا الاهتمام بالدراسات والأبحاث المهتمة بمجال الهجمات السيبرانية، حيث يعد كل من الباحثان جون اركويلا وديفيد رونفليد من اول من ذهب للبحث في مسألة الهجمات السيبرانية في سنة 1997م، في كتاب "الحرب السيبرانية قادمة" حيث نجد أنهم تنبها إلى نظم الاتصال الرقمي ودوره في النزاع المسلح في المستقبل .

[1] محمد محمود العمري , المدخل الى الامن السيبراني ,دار زهران , عمان , 2020 , ص21

2 مصدر سابق , ص21

3 مصدر سابق , ص22

ولن نذهب بعيداً عن اطار السياسة وارتباط ذلك بالسيبرانية ، ذلك لأهميته على المستوى الدولى فقد كان لرؤساء الدول الكبرى رؤى استراتيجية خاصة بالمجال الامني السيبراني ، إذ اعتبرت الدول التي لديها قدرة سيبرانية تستحق الكتمان عليه باعتباره عنصر خاص و مهم للأمن القومي، لكن ومع تزايد التطور في هذا المجال قام العديد من أصحاب القرار و مسؤولي دول العالم بالتحضير لمواجهة المخاطر التي تنتج عن مثل هذا التطور، و لم يبق على ذلك النحو، فسرعان ما بادر قادة الدول و المسؤولون عن رغباتهم في عملية التطوير و زيادة دعم الجانب الخاص بالسيبرانية من منطلق الحق في الدفاع عن النفس

ثانيا: **مفهوم الامن السيبراني** يعطي التقرير الصادر عن ITU الامن السيبراني تعريفاً للعام 2010-2011م"، بأنه: مجموعة من المهام و الوسائل والسياسات والإجراءات الأمنية، و المبادئ التوجيهية، و المقاربات لإدارة المخاطر، و مجموعة من التدريبات و الممارسات التقنية و التي يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسة والمستخدمين .

بينما اتفق عدد من الكتاب على أنه: (عبارة عن مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها ويتضمن تنفيذ التدابير المضادة المطلوبة")[1]

فيما عرفه (إدوارد أمورسو (Amoroso Edward) بأنه: وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها وتوفير الاتصالات المشفرة".)[2]

أما(وزارة الدفاع الأمريكية "البنتاغون" وضعت تعريفاً دقيقاً المصطلح الأمن السيبراني، فاعتبرته: جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية من مختلف الجرائم الهجمات التخريب التجسس والحوادث

في حين اعتبر الإعلان الأوروبي الأمن السيبراني أنه:" قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات")[3].

---

[1] محمد محمود العمري , مصدر سبق ذكره,ص20.

[2] محمد محمود العمري , مصدر سبق ذكره,ص20

[3] مصدر سبق ذكره , ص21.

و يمككنا القول بأن تعريف وزارة الدفاع الأمريكية هو الأقرب إلى للصحة ، وذلك بأنه تحدث عن " جميع الإجراءات التنظيمية"، ولم يقتصر على جوانب محددة من الحماية المعلوماتية، كذلك أنه لم يعطي حماية خاصة لكل جانب من جوانب المعلوماتية، وإنما اعطاها جميعاً سواء كانت هذه المعلومات متعلقة بالبيانات أو المعتدية او بالمحتوية المادي للأنظمة المعلوماتية كذلك إلى أنه لم يخصص جريمة سيبرانية عن اخرى، وإنما شمل جميع الجرائم السيبرانية جميعا حسب كل هدف و غاية من ارتكابه.

ثالثا:فواعل الامن السيبراني :

امر مهم ان نتعرف على الفواعل الرئيسية في الأمن السيبراني، والتي تقسم إلى قسمين: الأول على المستوى الدولة و الثاني على مستوى اللادولة, وهنا تجدر بنا الاشارة إلى أن أستاذ العلوم السياسية جوزيف ناي من المفكرين الذين التفتوا لهذه الفواعل في عدة دراسات .

1-الفواعل الدولاتية (فواعل الدولة)

(بما أن الدولة هي الفاعل المحوري في تسيير الفضاء الافتراضي انطلاقاً من إمكاناتها المادية والبنيوية والبشرية والقانونية، تشير هنا أساساً إلى الاحتكار القانوني والمنظم للدولة للفضاء الافتراضي، من خلال مختلف أجهزتها)[1].

2-الفواعل اللادولاتية

ويقصد هنا الى الادوار التي تقزم بها الأفراد والجماعات والمنظمات غير الحكومية والشركات، والذين أصبحوا في وقتنا هذامؤثرين وبامتياز بحيث لديهم قدرة عالية في التحكم و كذلك في توجهات الدول وإدارتها وفق سياساتها من خلال الفضاء الرقمي، ومن ابرز هذه الفواعل هي :

الأفراد (Individuel):(حيث أصبح الفرد بفضل الفضاء السيبراني فاعلاً مؤثراً في العلاقات الدولية والفضاء السيبراني، وله القدرة والإمكانية على إحداث الثورة الرقمية، وتصبح هذه الثورة مجال استخدام للدولة نفسها، ومثال ذلك ما قام به المبرمج الأمريكي "مارك زوكربيرغ (Mark Zoukerberg) في العام 2004م حين أسس مع زملاؤه شبكة فاس بوك) لتستقطب أكثر من مليار مستخدم عبر العالم وتصبح أكبر موقع اجتماعي في العالم.[2] المنظمات غير الحكومية تعتبر هذه المنظمات شبكة الانترنت ووسائل التكنولوجيا الحديثة عنصر أساسي في عملها من

---

[1] مصدر سبق ذكره .

[2] محمد محمود العمري , مصدر سبق ذكره , ص153

خلال تعبئة الرأي العام، والضغط على الحكومات من خلال ترتيب الحملات الاجتماعية وتعبئة المجتمع المدني للضغط على الحكومات للتغيير في سياسات معينة، والأمثلة على ذلك كثرة مثل منظمات البيئة العالمية على اثر قرار الرئيس الأمريكي دونالد ترامب التخلي عن اتفاقيات التغير المناخي

(المجموعات الافتراضية (Default groups) ونذكر عن تلك المجموعات ما يقوم به القراصنة (Hackers)، حيث دائماً يسعون إلى تحقيق أهداف مختلفة منها السياسي الربحي المادي، الأيديولوجي) أيضاً نجد المنظمات الإجرامية والتي تقوم هذه المنظمات الإجرامية بعمليات القرصنة السيبرانية، وسرقة المعلومات واختراق الحسابات البنكية وتحويل الأموال، كما توجد سوق سوداء على الإنترنت المظلم (Dark internet لتجارة المخدرات والأسلحة والبشر)[1]

الشركات المتعددة الجنسيات: تمتلك بعض شركات التكنولوجيا موارد للقوة تفوق قدرة بعض الدول، ولا تنقصها سوى شرعية ممارسة القوة التي ما زالت حكراً على الدول، فخوادم شركات مثل: جوجل (Google) وفيسبوك (Facebook) ومايكروسوفت (Microsoft) ، تسمح لها بامتلاك قواعد البيانات العملاقة التي من خلالها تستكشف وتستغل الأسواق، وتؤثر في اقتصاديات الدول وفي ثقافة المجتمعات وتوجهاتها.

الجماعات الإرهابية وهذه الفئة تعتبر من أبرز الفواعل الدولية حيث أصبحت ومع تنامي ظاهرة الإرهاب تلجأ إلى الفضاء السيبراني في عمليات التجنيد والتعبئة والدعاية وجمع الأموال وغير ذلك ومحاولة جمع المعلومات حول أهدافها، إضافة إلى التعامل مع الأسلحة المختلفة والتواصل مع عناصرها في أماكن ودول بعيدة، رغم أن هذه الجماعات لم تصل بعد إلى مرحلة القيام بهجمات سيبرانية حقيقية على منشآت البنية التحتية للدول.[2]

رابعا:الارهاب السيبراني

هناك نوعين من االارهاب الاول المسمى بالارهاب النقي و الذي يكون بشكل مباشر و الاخر وهو الارهاب الذي يسمى الهجين و الذي يكون بشكل غير مباشر و يتمثل النوع الاخير بالتنسيق و التواصل و كذك جمع التبرعات و التجنيد الالكتروني و التدريب و نشر الافكار

[1] محمد محمود العمري , مصدر سبق ذكره , ص153

[2] محمد محمود العمري , مصدر سبق ذكره, ص32

المتطرفة و هذا ما سنتطرق اليه في بحثنا هذا **(نشر الأفكار المتطرفة الدعاية والإعلان):** (تستغل الجماعات الامتطرفة و الارهاب الفضاء السيبراني في جانب دعائي و اعلاني ذلك من خلال قيامها بث الأفكار المتطرفة من خلال وسائل التواصل الاجتماعي مثل الغرف الخاصة بالدردشة والتي يكون فيها جميع شرائح المجتمع موجودة و بالاخص الشباب ، أضافة إلى ذلك وجود عدد من المواقع و الصفحات الاكترونية التي تعود للجماعات المتطرفة ، وفي تقرير صادر عن احد الخبراء الأمنيين و المختصين في قضايا الإرهاب الرقمي جيف باردين حيثكشف أن تنظيم داعش الإرهابي كان يملك (90) ألف صفحة باللغة العربية على موقع التواصل الاجتماعي الفيسبوك و كذلك (40) ألف صفحة بلغات متعددة ، إضافة إلى موقعه الذي دشنه التنظيم بسبعة لغات لابتزاز الشباب بغرض ضمهم لصفوفهم فحوالي (3400) شاب انتمى لتنظيم داعش من خلال حملات التنظيم الالكترونية فحسب جمعية آفاق للأمن الداخلي في تونس أن عدد من المواقع الإلكترونية ذات التوجه المتطرف والإرهابي تحاول جذب ألف شاب تقريباً في السنة وهو يعادل (3) شبان يومياً، وهو رقم مرتفع يعكس مدى خطورة هذه الظاهرة التي تتزايد حدتها وهم يمثلون حوالي (40%) من مجموع الشباب المستقطب وهم من الطلبة االمميزين والتلاميذ المتفوقين الذين تتراوح أعمارهم بين (17) و (28) سنة والذين يدرسون الاختصاصات العلمية الطب الفيزياء والكيمياء، حيث تقوم هذه الجماعات بأستثمار مهاراتهم العلمية لأغراض تخريبية)[1]

خامسا:واقع الامن السيبراني دولياً و عربياً و مؤشر العراق منها

يعتمد مؤشر الأمن السيبراني العالمي خمسة ركائز للامن عن طريق تحليل 80 مؤشر فرعي القياس مستوى الأمن السيبراني لكل دولة، وهذه الركائز هي:

1. القانونية: التدابير القائمة على وجود المؤسسات والأطر القانونية التي تتعامل مع الأمن السيبراني والجريمة الإلكترونية

2- التقنية: التدابير القائمة على وجود المؤسسات الفنية والتعامل مع الأمن السيبراني.

3 – التنظيمية التدابير القائمة على وجود مؤسسات واستراتيجيات تنسيق السياسات التطوير الأمن السيبراني على المستوى الوطني.

4- بناء القدرات التدابير القائمة على وجود البحث والتطوير والتعليم وبرامج التدريب والمهنيين المعتمدين ووكالات القطاع العام التي تعزز بناء القدرات.

5- التعاون التدابير القائمة على وجود شراكات وأطر تعاونية وشبكات تبادل المعلومات.

ان العناصر أو المعايير أعلاه هي التي تحكم الاتحاد الدولي للاتصالات أثناء تقييم الدول وفقًا لمؤشر الأمن السيبراني. ومما يلاحظ وجود فجوات كبيرة في قدرات توفير وإتاحة الأمن السيبراني على مستوى العالم، إذ تمتلك مثلا الولايات المتحدة الأميركية والمملكة المتحدة بنى تحتية مغايرة تماما من حيث القدرة والكفاءة عن تلك الموجودة في دول مثل العراق وجيبوتي وبوروندي.

ومع ذلك، أظهرت دول مجلس التعاون الخليجي في هذا المؤشر أنها تفوقت بشكل جماعي على العديد من الدول الغربية الأخرى والبلدان الأكثر تقدما اقتصاديا من حيث قدراتها الأمنية السيبرانية واستدامة البنى التحتية البشرية وغيرها، بالإضافة إلى التدابير التعاونية لخلق بيئة تقنية آمنة الجزيرة

حيث صنّف المؤشر العالمي للأمن السيبراني "جي سي آي" (GSI) الذي أصدره الاتحاد الدولي للاتصالات التابع للأمم المتحدة لعام 2021 أربع دول عربية فقط في المستوى المرتفع. وتصدرت دول السعودية وقطر والإمارات والبحرين وعُمان الجهود في تحقيق الأمن السيبراني عربيا وعالميا، في حين وقعت باقي الدول في مرتبة متوسطة عالميا، أو تذيلت القائمة وفق المؤشر الذي شمل 175 دولة وقاس مدى التزام البلدان في مجال الأمن السيبراني وفقا للدعائم الخمس للبرنامج العالمي للأمن السيبراني . الجزيرة [11]

و نجد بأن العراق وعلى الرغم من التحسن الذي حدث في موقعه في مؤشر عام 2018 حيث شغل (107) عالمياً و (13) عربيا، فانه تراجع (22) نقطة في مؤشر العام 2020 ليكون (129) عالمياً من اصل (184) دولة و (17) عربياً بدرجة (71,20)، فضلاً عن تقاعس المؤسسات المعنية بالرد على اجاجات الاسئلة التي وجهت لها من فريق مؤشر الأمن السيبراني.

النتيجة الكلية	الاجراءات القانونية	الاجراءات التقنية	الاجراءات التنظيمية	بناء القدرات	اجراءات التعاون
20.17	0.00	6.56	7.75	2.14	4.6

[1] باسم خريسان , قراءة في مؤشرالامن الامن السيبراني 2020, مركز البيان للدراسات و التخطيط , بغداد , 2020

Global Cybersecurity Index 2020, International Telecom- munication Union Development Sector, ITUPublications, 2021, P74

وعند البحث عن اسباب هذا التراجع سوف تجد بأن الجهود الحكومية التي اتخذها العراق في مجال الأمن السيبراني لم تستمر وشهدت تراجع والتي شملت الاتي:

1) تراجع دور فريق الإستجابة للأحداث السبرانية، وهو فريق وطني مشترك مختص بمجال الأمن السيراني والاستجابة للحوادث السيرانية وحماية البنية التحتية للانترنت ونشر الوعي في مجال حماية الخصوصية والحماية الذاتية للافراد والمؤسسات على الانترنت يعمل تحت إشراف مستشارية الأمن القومي العراقي، ويحمل الفريق على عاتقه مسؤولية تأمين وحماية الشبكات ومراكز البيانات الوطنية والمواقع الرسمية التي تعمل في مجال الفضاء السيراني العراقي ويقوم بتنسيق الجهود الوطنية ودعم المؤسسات في القطاعين العام والخاص في حماية نفسها وخدماتها في الفضاء السيبراني.

2) لا يزال قانون جرائم المعلوماتية لم يصوت عليه بالرغم من القراءة الأولى له، وتبدل نسخه لعدة مرات بطريقة تثير مخاوفا على الحريات العامة.

3) عدد المؤتمرات وورش العمل والندوات عن الأمن السيبراني لا تزال محدودة جداً بالمقارنة مع دول الجوار مثل السعودية.

4) لا تزال الاموال المخصصة للأمن السيبراني قليلة بالمقارنة مع دول الجوار ومنها ايران التي خصصت مليار دولار سنوياً لهذا القطاع.

5) لا توجد بنية تحتية مادية وبشرية متكاملة في مجال الأمن السيبراني ولا توجد هيئة وطنية مسؤولة

6) لا نجد للعراق دور في المنتديات الدولية المعنية بالأمن السيبراني. [11]

المبحث الثالث: الامن السيبراني و دوره في مكافحة التطرف

ترجع أهمية الأمن السيبراني بالأساس إلى طبيعة الفضاء السيبراني على تعدد سماته وخصائصه. فهو عالم موازي للواقع المعاش، وهو أيضًا فيض رقمي من المعلومات ، بل ووسيط من خلال أجهزة الكمبيوتر وشبكات الاتصال.وعليه ، يتسم الفضاء السيبراني بغياب الحواجز المكانية والزمانية وضرورة وجود هيكل مادي من أجهزة الكمبيوتر وخطوط الاتصالات ، وعدم

[1] باسم خريسان , المصدر السابق.

تقيد الهجمات السيبرانية بالحدود الجغرافية، وصعوبة الكشف عن كثير من التهديدات السيبرانية قبل وقوعها، وفداحة الأضرار المترتبة على تلك التهديدات حال وقوعها .

ومن ثم يعتبر الأمن السيبراني أحد أبعاد الأمن القومي غير التقليدي ، بالنظر إلى تعدد التهديدات السيبرانية المحتملة وما قد ينتج عنها من خسائر سياسية وعسكرية واقتصادية فادحة. ومن هذا المنطلق، أولت نظريات العلاقات الدولية اهتمامًا بالغًا بالأمن السيبراني لتدفع الواقعية بأن الدول في سعي حثيث لتطوير قدراتها السيبرانية الهجومية بهدف استخدام الإنترنت كسلاح استراتيجي، وأن الفضاء السيبراني ساحة مفتوحة لمختلف الفاعلين بما في ذلك الفاعلين من غير الدول (مثل: الجماعات المتطرفة و التنظيمات الإرهابية، وجماعات القرصنة الإجرامية ، وشركات التكنولوجيا العملاقة) ، وأن هناك صعوبة في تقدير قوة الدولة السيبرانية لطابعها غير الملموس، ناهيك بتراجع فعالية الردع السيبراني، وتزايد أهمية الأساليب الهجومية على مثيلتها الدفاعية.[11]

أما النظرية الليبرالية، فتؤكد على أهمية التعاون لمجابهة التهديدات السيبرانية العابرة للقومية على الرغم من أن المنظمات الدولية المعنية بإدارة الإنترنت (مثل: منظمة الأيكانICANN ، والاتحاد الدولي للاتصالات) لا تستطيع التغلب على حالة الفوضى في النظام الدولي، علاوة على صعوبة تطبيق القانون الدولي على الفضاء السيبراني نظرًا لغياب الحدود الجغرافية التي تنطبق على الصراعات التقليدية. كما لم توفر الليبرالية إطارًا يمكن من خلاله فهم آلية تحقيق الردع السيبراني في ظل الإشكاليات التي تقوضه وفي مقدمتها صعوبة معرفة المهاجم ابتداءً. كما لم تحسم الليبرالية العلاقة الجدلية بين الأمن والخصوصية.

وعليه، يمكن القول إن النظريات الكبرى في مجال العلاقات الدولية قد تفشل في الإلمام بجميع أبعاد الأمن السيبراني، ولا سيما أنها تغفل البعد القيمي المعياري في تحليله. ومن ثم، فإنها قد تعجز عن تقديم أدوات تحليلية لفهم بعض التهديدات الأمنية غير التقليدية وفي مقدمتها التهديدات السيبرانية في ضوء التطورات التكنولوجية المتسارعة، وتنامي دور الفاعلين من النشطاء والجيوش الالكترونية والفاعلين من غير الدول في المجال السيبراني. فلعل الوجه المقابل للأمن السيبراني هو التهديد السيبراني الذي يأخذ صورًا متعددة، تشمل: الجريمة السيبرانية،

[1] نوران شفيق، أثر التهديدات الألكترونية على العلاقات الدولية دراسة في أبعاد الأمن الألكتروني (القاهرة: المكتب العربي للمعارف، 2016) ص. 11.

والإرهاب السيبراني، والحرب السيبرانية، والصراع السيبراني، والهجمات السيبرانية، والتجسس السيبراني، وغير ذلك. [12]

ولا شك أن أيًا من تلك التهديدات قادر على إلحاق خسائر اقتصادية ضخمة بالطرف الذي يتعرض لها ذلك أن تلك التهديدات مستويات ودرجات مختلفة ذات صور عدة، قد تشمل : قطع أنظمة الاتصال بين الوحدات الرسمية أو العسكرية وبعضها البعض أو تضليل معلوماتها أو سرقة معلوماتها السرية، والتلاعب بالبيانات الاقتصادية والمالية وتزييفها أو مسحها من أجهزة الحواسب، أو السيطرة على نظم الذكاء الاصطناعي وإنترنت الأشياء، وتوجيهها للقيام بأعمال تخريبية، او التلاعب بالراي العام او التاثير على الافراد وغير ذلك

وعليه أطلق مكتب مكافحة الإرهاب في الامم المتحدة العديد من المبادرات في مجال التقنيات الجديدة، من ضمنها مشروع بشأن استخدام وسائل التواصل الاجتماعي لجمع المعلومات مفتوحة المصدر والأدلة الرقمية لمكافحة الإرهاب والتطرف العنيف مع احترام حقوق الإنسان ومع استحداث مزيد من البرامج في ذلك المجال. كما يبرز أيضًا –بالتوازي مع ذلك–"برنامج أمن الفضاء السيبراني والتقنيات الحديثة" الذي تتمثل أهدافه الرئيسة في: تعزيز قدرات الدول الأعضاء والمنظمات الخاصة على منع الهجمات السيبرانية التي تقوم بها الجهات الفاعلة الإرهابية ضد البنية التحتية الحيوية، وتخفيف تأثير هذه الهجمات السيبرانية، وإصلاح الأنظمة المستهدفة في حالة حدوث تلك الهجمات[18]. مركز مكافحة الإرهاب بالأمم المتحدة، أمن الفضاء الإلكتروني، الأمم المتحدة[2].

وعلى تعدد تلك الجهود، فإنها تجد أواصرها في جملة من الاعتبارات منها استخدام التنظيمات الإرهابية لمختلف الأدوات التقنية لتخريب البنى التحتية الوطنية الحيوية مثل الطاقة أو أنظمة النقل أو المياه أو المرافق الحكومية أو الرعاية الصحية أو الاتصالات، ما يشكل مصدر قلق متزايدًا للدول الأعضاء في الأمم المتحدة. كما أعربت العديد من التنظيمات الإرهابية –بما في ذلك تنظيمي"القاعدة" و"داعش"– عن رغبتها في بناء قدرات سيبرانية هجومية تسمح لها بتنفيذ

[1] إيهاب خليفة، الحالة السيبرانية في نظريات العلاقات الدولية: الحاجة إلى مراجعة جديدة، بقلم خبير، مركز المعلومات ودعم اتخاذ القرار، العدد 23، ديسمبر 2021، ص ص. 8-11.

[2] https://cutt.ly/LwbeGCjh، تاريخ الاطلاع 26 سبتمبر 2023

هجمات مدمرة محتملة عن بعد، ما يزيد الحاجة إلى الاستثمار في أمن الدول الأعضاء وقدرتها على الصمود في مواجهة تلك الهجمات المحتملة، فضلًا عن القدرة على التخفيف والتعافي منها حال وقوعها ، وتقديم المسئولين عنها إلى العدالة. كما اعتمدت ظواهر عدة على شاكلة المقاتلين الأجانب، وتجنيد الإرهابيين، وانتشار المحتوى المتطرف العنيف،على الوصول العالمي للإنترنت. وقد أظهرت بعض الدراسات أن شهرة تنظيم "داعش" لم تكن لتتحقق لولا الإنترنت. وعلى مدار العقد الماضي، اكتسبت التطورات التكنولوجية أهمية متزايدة بالنظر إلى تأثيراتها الاقتصادية والسياسية العالمية، ليبرز في هذا الإطار البيانات الضخمة، والذكاء الاصطناعي، والمعالجة الحاسوبية، والتشفير، وشبكات الجيل الخامس، و"البلوكتشين"،وإنترنت الأشياء. وعلى تعدد مزايا تلك التقنيات التكنولوجية، فإنه من الممكن استخدامها من قبل التنظيمات الإرهابية لتحقيق أهدافها' وبجانب الجهود والقرارات الدولية الملزمة للدولة العراقية ، يبرز في سياق متصل بعض الاتفاقيات العربية وفي مقدمتها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. لتلك الاتفاقية بموجب القرار رقم 276 لعام 2014، بهدف تعزيز التعاون بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات بشكل عام والإرهاب السيبراني بشكل خاص. وهو ما يجد أواصره في اقتناع الدول العربية التي انضمت لتلك الاتفاقية بضرورة تبني سياسات جنائية مشتركة لحماية المجتمع العربي من جرائم تقنية المعلومات. والجدير بالذكر أن المادة الخامسة عشرة من تلك الاتفاقية تنص تحديدًا على الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات، وهي الجرائم التي تشمل: نشر أفكار ومبادئ جماعات إرهابية والدعوة لها، وتمويل العمليات الإرهابية والتدريب عليها، وتسهيل الاتصالات بين التنظيمات الإرهابية، ونشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية، ونشر النعرات والفتن، والاعتداء على الأديان والمعتقدات. ص المادة 15 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. انظر النص الكامل للاتفاقية على الرابط التالي[1]

تجربة العراق في الامن السيبراني

على صعيد العراق كشفت "تريند مايكرو" و هي شركة عالمية الرائدة في مجال الأمن السيبراني باكتشاف وحظر أكثر من 15 مليون تهديد عبر البريد الإلكتروني، وقامت بحماية أكثر من

[1] https://haqqi.s3.eu-north-1.amazonaws.com/2014-04/HRIDRL0149_ArabConventionCyberCrime.pdf

400 ألف مستخدم من التضرر من روابط خبيثة قاموا بالضغط عليها، كما استطاعت تحديد وإيقاف أكثر من نصف مليون هجوم لبرمجيات خبيثة في الدولة.

وبهذا الصدد، قال أسعد عُرابي، المدير العام لتريند مايكرو في منطقة الخليج العربي والأسواق الناشئة: "ساهمت التكنولوجيا في توفير العديد من الفرص لمؤسسات الدولة، إلا أنها في نفس الوقت شكلت تحديات أمنية جديدة، لذلك من الضروري المحافظة على جهود الاعتماد الآمن على التكنولوجيا في العراق، لتأمين المشهد الرقمي في البلاد من الهجمات الإلكترونية والمحافظة على العمليات والبيانات الحساسة".

وأضاف عرابي، أن "لدى تريند مايكرو التزام راسخ بتمكين الشركات العراقية ودعمهم بالأدوات والخبرات اللازمة لتحقيق أهداف التحول الرقمي، وتزويدهم بحلول أمنية متعددة الطبقات والمراحل الدفاعية"، وفقاً للتقرير السنوي.وسلط التقرير الضوء على أن "زيادة الفشل في إصلاح الثغرات الأمنية يضيف المزيد من الوقت والمال لجهود الشركات للإصلاح ويعرض المؤسسات لمخاطر إلكترونية غير ضرورية". [1] تعد الجماعات المسلحة أبرز مصادر التهديد في الحروب السيبرانية، إذ شهد العراق خلال فترات متقاربة هجمات إلكترونية من قبل هذه الجماعات على مواقع داخل العراق وخارجه. واستهدفت الهجمات منشآت ومؤسسات حكومية في إسرائيل وتركيا والسعودية، فضلاً عن مؤسسات إعلامية داخل العراق، أبرزها المواقع الإلكترونية التابعة لقنوات "UTV" وقناة "الفلوجة" العراقية .

و بهذا الصدد فأن هناك عديداً من علامات الاستفهام تدور حول طبيعة القدرات السيبرانية التي تمتلكها الجماعات المسلحة في العراق ، إذ إن الهجمات التي حصلت، وبخاصة تلك التي طالت

1 https://shafaq.com/ar/%D9%85%D8%AC%D8%AA%D9%80%D9%85%D8%B9/20-%D9%85%D9%84%D9%8A%D9%88%D9%86-%D8%AA%D9%87%D8%AF%D9%8A%D8%AF-%D9%81%D9%8A-%D8%A7%D9%84%D8%B9%D8%B1%D8%A7%D9%82-%D8%AA%D9%82%D8%B1%D9%8A%D8%B1-%D8%A7%D9%84-%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D9%8A%D9%83%D8%B4%D9%81-%D8%AD%D8%B5%D9%8A%D9%84%D8%A9-2022

مؤسسة الصناعات الدفاعية التركية ، والموقع الإلكتروني لقناة "أخبار كان" و"القناة 9" وهيئة الطيران الإسرائيلية، إلى جانب أهداف أخرى، "تحتاج إلى جهد دولة، وليس مجرد جماعات إلكترونية"

اضافة الى الحملات الدعائية في المنصات الموجودة على وسائل التواصل الاجتماعي و ابرزها على منصة تويتر و تليغرام والتي تتوعد بمزيد من الهجمات .

ومع ذلك، فالعراق لديه الإمكانية الكبيرة لتحسين موقفه ومرونته في مجال الأمن السيبراني، من خلال استغلال الكفاءات المطمورة بين اروقة مدنه وجامعاته ودوائره الحكومية والتي يتم زجها للعمل في أقسام مغايرة لاختصاصها إلا ما ندر ولا يتم التركيز عليها وتطويرها إلا بدورات فقيرة تقف بأول خطواتها وندوات نظرية لمواضيع مكررة بينما مجال الأمن الرقمي يحتاج الى تطبيقات عملية، ويمكن التحسين ايضاً بواسطة التعلم من أفضل الممارسات والابتكارات للمجتمع العالمي للأمن السيبراني.

إحدى الفرص التي يمكن للعراق الاستفادة منها هي المشاركة في مسابقة بلاك هات التي تعتبر أكبر حدث للأمن السيبراني في المنطقة، وبخطوة إيجابية شارك العراق بأسم فريق "لشركة عراقية" حصل فيها على المرتبة 139 عالميا في تلك المسابقة على مستوى الشرق الاوسط وافريقا والتي اقيمت في الرياض بالمملكة العربية السعودية للفترة 14-16 تشرين الثاني 2023، وهذا دليل على وجود عقول تمضي قُدُماً في ذلك المضمار ولكن ضمن قِطاع خاص لذلك نطمح ان يكون في المواسم القادمة ان يشارك فريق حكومي معتمد[1]

استراتيجية الامن السيبراني العراقي

حدّدت مستشارية الأمن الوطني في العراق، عبر دراسة لها، استراتيجية الأمن السيبراني في البلاد، وأوضحت أن العراق ليس بعيداً من التهديدات السيبرانية التي تتمثل في الجريمة الإلكترونية والتجسس السيبراني والإرهاب الإلكتروني وإساءة معاملة الأطفال واستغلالهم عبر الإنترنت. ووضعت الدراسة عدة مراحل زمنية يتم من خلالها تحديد الضعف الهيكلي في نظم المعلومات العراقية، بالتالي تقديم آليات جديدة لمعالجة هشاشة الأمن السيبراني في البلاد، وخصصت الدراسة المرحلة الأولى لزيادة الوعي بالأمن السيبراني، وتمتد لمدة سنة واحدة يجري خلالها تقديم مسودات قوانين تخص هذا المجال.

[1] . إيهاب عنانل باحث في مجال الذكاء الاصطناعي والأمن السيبراني – منصة التواصل الرقمي

أما المرحلة الثانية، ومدتها ثلاث سنوات، فتتضمن بناء البنية التحتية والقدرات بين باحثي أمن المعلومات، كما تتضمن المرحلة الثالثة والأخيرة، ومدتها خمس سنوات، تطوير الاعتماد على الذات من حيث التكنولوجيا ومراقبة آليات الامتثال للخطط والمعايير القياسية الموضوعة للأمن السيبراني العراقي.

وترى مستشارية الأمن الوطني أن هذه الدراسة تمثل محاولات لا غنى عنها لبناء أسس لا يشوبها الخلل للأمن السيبراني في العراق، ويرتبط التصنيف العالمي للدول في مجال الأمن السيبراني بقدرة الدولة على صد الهجمات الإلكترونية عندما تكون أنظمتها عالية الحماية، وألا تكون الدولة مصدراً لهجمات من هذا النوع على باقي الدول.

الخاتمة :

يتطلب واقع الأمن السيبراني العراقي، والمخاطر والتهديدات المستمرة التي تعترضه، إحداث هيئة وطنية موحدة لجميع التشكيلات والفرق الإلكترونية للأجهزة العراقية، التي يمكن أنْ تشكّل البنية التحتيَّة الأساس له، ضمن مسار الستراتيجية الوطنية للأمن السيبراني، وبصلاحيات موّسعة، يعمل على تأمين حال البلاد في البعد الخامس للحروب المعاصرة، إلى جانب تعديل النصوص التشريعيَّة المرتبطة بمواجهة الجرائم السيبرانيَّة، على وفق المعطيات المعاصرة، وإرساء ثقافة عامة للأمن السيبراني على صعيدي المؤسسات والأفراد، وتشجيع البحث العلمي المتعلق بهذا المجال، عن طريق افتتاح أقسامٍ أو فروعٍ علميَّة في الجامعات العراقيَّة، الى جانب تحفيز الباحثين لإجراء دراسات الأمن السيبراني، وبحسب ارتباطه بتخصصاتهم العلميَّة، وتدريب وتنمية المهارات الرقميَّة بشكلٍ مستمر، لمواكبة المستجدات الإلكترونيَّة، على مستوى المنطقة والعالم.

التوصيات :

ان العراق بحاجة للتكيف مع تحديات الفضاء السيبراني في مختلف المجالات ومنها المجال الأمني، وذلك من خلال العمل على اجراء الآتي:

1) وضع الإطار التنظيمي وإنشاء منظومة وطنية لحماية أمن الفضاء السيبراني وتأمين البني التحتية للاتصالات وتكنولوجيا المعلومات ونظم وقواعد البيانات والمعلومات القومية وبوابات الخدمات الحكومية والمواقع الحكومية على الإنترنت، وذلك بإعداد وتفعيل "فرق الاستعداد والاستجابة لطوارئ الحاسبات والشبكات" في القطاعات الحيوية على المستوي الوطني.

2) تطلب واقع الأمن السيبراني العراقي، والمخاطر والتهديدات المستمرة التي تعترضه، إحداث

هيئة وطنية موحدة لجميع التشكيلات والفرق الإلكترونية للأجهزة العراقية، التي يمكن أنْ تشكّل البنية التحتيَّة الأساس له، ضمن مسار الستراتيجية الوطنية للأمن السيبراني، وبصلاحيات موّسعة، يعمل على تأمين حال البلاد في البعد الخامس للحروب المعاصرة، إلى جانب تعديل النصوص التشريعيَّة المرتبطة بمواجهة الجرائم السيبرانيَّة، على وفق المعطيات المعاصرة، وإرساء ثقافة عامة للأمن السيبراني على صعيدي المؤسسات والأفراد .، ولا يمكن ربط هذا الفريق المهم بجهاز أمني بحت مثل جهاز المخابرات أو غيره من الأجهزة الأمنية الأخرى ذات الطبيعة التنفيذية المباشرة .

3) تنمية الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبراني في مختلف القطاعات، بالتعاون والشراكة مع القطاع الخاص والجامعات ومؤسسات المجتمع المدني، وبالتعاون مع الدول الصديقة والمنظمات الدولية والإقليمية ذات الصلة

4) تأسيس كليات واقسام علمية في الجامعات العراقية المدنية والعسكرية تختص بالأمن السيبراني و تمنح درجات علمية في تخصص الأمن السيبراني.

5) تشجيع ودعم وتنمية البحث العلمي والتطوير ودعم التعاون بين الجهات البحثية والشركات الوطنية، وبخاصة في مجال تحليل البرمجيات الخبيثة المتقدمة، وتحليل الأدلة الرقمية، وحماية وتأمين نظم التحكم الصناعية، وتطوير أجهزة وأنظمة تأمين النظم والشبكات

6) بناء وعي اعلامي وثقافي حول خطورة التهديدات السيبرانية .

7) بناء منظومة قانونية وقضائية تتعلق بالجرائم السيبرانية.

8) المشاركة في الجهود الدولية المتعلقة بالأمن السيبراني، مثل الاتفاقيات الدولية والمؤتمرات التي تعقد حول خطر التهديدات السيبراني وكيفية التعامل معها دولياً. الاهتمام الحكومي بالمؤشرات الدولية والاجابة الدقيقة بشفافية على الاستبيانات المعنية، وفق المعطيات الأمنية الممكنة.

9) انشاء مراصد ذات جنبة اجتماعية تكون بتماس مع النخب و المؤثرين دينياً و اجتماعياً و سياسياً شرط ان لا تنتهك حقوق الإنسان أوالقانون الدولي أوأية قوانين وطنية، وبما يكفل الحفاظ على الأمن القومي للدول وسلامة مواطنيها من جهة و بما يحفظ حرية الراي و التعبير بشكل متوازي من جهة اخرى .

الاستنتاجات :

يمكن الدفع بأن الإرهاب السيبراني بات جاذبًا لمختلف التنظيمات الإرهابية لأنه يتطلب عددًا أقل من الأشخاص والموارد، ويمكنها من استهداف أهداف واسعة النطاق، مع الحفاظ على مجهولية هوية الإرهابيين لا سيما مع إمكانية تواجدهم في أماكن بعيدة عن المواقع الفعلية المستهدفة. كما يمكن للإرهابيين الاختيار بين مجموعة واسعة من الأهداف التي يمكن النيل منها بسرعة دون الحاجة إلى استخبارات وتحضيرات واسعة وحواجز مادية يتحتم عبورها ونقاط تفتيش ينبغي تجاوزها

قائمة المصادر :

1) تيري إيغلتون. أوهام ما بعد الحداثة. المركز العربي للأبحاث ودراسة السياسات, 2019,

2) عبد الصمد الديالمي, دار الساقي. المدينة الإسلامية والأصولية والإرهاب: مقاربة جنسية.

3) نايل ممدوح أبو زيد "الوسطية حاجة ذاتية وضرورة إنسانية–دراسة قرآنية" , مجلة 12 العدد 3.

4) مجلة العلوم الأساسية Basic Science journal ISSN 2306-5249 وظائف العدد الثاني ٢٠٢١م / ١٤٤٢هـ (المؤيد أو الرافض).

5) أ. د. نايل ممدوح أبو زيد. الوسطية حاجة ذاتية وضرورة إنسانية–دراسة قرآنية. 2015.

6) مجموعة مؤلفين. المدينة العربية: تحديات التمدين في مجتمعات متحولة. المركز العربي للأبحاث ودراسة السياسات, 2020.

7) برهان غليون. نظام الطائفية من الدولة إلى القبيلة. المركز العربي للأبحاث ودراسة السياسات, 2017.

8) صالحي بن شريف; حنيفة. الأسرة و عنف الطفل: علاقة افتراضية أم حتمية؟. Insaniyat /إنسانيات. Revue algérienne d'anthropologie et de sciences sociales, 2008,

9) قيراط، محمد مسعود. الإرهاب: دراسة في البرامج الوطنية واستراتيجيات مكافحته: مقاربة إعلامية. Naif Arab University (NAUSS), 2011.

10–مجموعة مؤلفين. المسألة الطائفية وصناعة الأقليات في الوطن العربي. المركز العربي للأبحاث ودراسة السياسات, 2017.)

11-جلبير الأشقر ; دار الساقي; نعوم تشومسكي. السلطان الخطير . Dar al Saqi, 2017.

12) المركز الوطني للوقاية للتطرف العنيف , الولايات المتحدة الامريكية .

13) الدكتور محمد محمود العمري , المدخل الى الامن السيبراني ,دار زهران , عمان , 2020

14) الدكتور باسم خريسان , قراءة في مؤشرالامن الامن السيبراني 2020, مركز البيان للدراسات و التخطيط , بغداد , 2020 .

15) نوران شفيق، أثر التهديدات الألكترونية على العلاقات الدولية دراسة في أبعاد الأمن الألكتروني (القاهرة: المكتب العربي للمعارف، 2016)

16) إيهاب خليفة، الحالة السيبرانية في نظريات العلاقات الدولية: الحاجة إلى مراجعة جديدة، بقلم خبير، مركز المعلومات ودعم اتخاذ القرار، العدد 23، ديسمبر 2021

17) https://cutt.ly/LwbeGCjh، تاريخ الاطلاع 26 سبتمبر 2023

) north-1.amazonaws.com/2014-https://haqqi.s3.eu-

04/HRIDRL0149_ArabConventionCyberCrime.pdf

25)https://shafaq.com/ar/%D9%85%D8%AC%D8%AA%D9%80%D9%85%D8%B9/20-%D9%85%D9%84%D9%8A%D9%88%D9%86-%D8%AA%D9%87%D8%AF%D9%8A%D8%AF-%D9%81%D9%8A-%D8%A7%D9%84%D8%B9%D8%B1%D8%A7%D9%82-%D8%AA%D9%82%D8%B1%D9%8A%D8%B1-%D8%A7%D9%84-%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D9%8A%D9%83%D8%B4%D9%81-%D8%AD%D8%B5%D9%8A%D9%84%D8%A9-2022

18) . إيهاب عنانل باحث في مجال الذكاء الاصطناعي والأمن السيبراني – منصة التواصل الرقمي

)http://www.moqatel.com/openshare/Behoth/Mnfsia15/Extremity/sec01.doc_cvt.htm