مركز البيان للدراسات والتخطيط
Al-Bayan Center for Studies and Planning

الهجمات السيبرانية والأمن الوطني العراقي
بين المواجهة والإدارة

د.علاء عبيس راضي الجبوري

سلسلة اصدارات مركز البيان للدراسات والتخطيط

مركز البيان للدراسات والتخطيط
Al-Bayan Center for Studies and Planning

الهجمات السيبرانية والأمن الوطني العراقي: بين المواجهة والإدارة

سلسلة اصدارات مركز البيان للدراسات والتخطيط / قسم الابحاث / الدراسات الأمنية والعسكرية

الاصدار / ورقة بحثية

الموضوع / الأمن والدفاع، مكافحة التطرف والإرهاب

د.علاء عبيس راضي الجبوري / رئاسة الوزراء

عن المركز

مركزُ البيان للدراسات والتخطيط مركز مستقلٌ، غيرُ ربحيٍّ، مقرُّه الرئيس في بغداد، مهمته الرئيسة -فضلاً عن قضايا أخرى- تقديم وجهة نظر ذات مصداقية حول قضايا السياسات العامة والخارجية التي تخصّ العراق بنحو خاصٍ، ومنطقة الشرق الأوسط بنحو عام. ويسعى المركز إلى إجراء تحليلٍ مستقلٍّ، وإيجاد حلول عملية جليّة لقضايا معقدة تهمُّ الحقليْنِ السياسي والأكاديمي.

ملحوظة:

لا تعبّر الآراء الواردة في المقال بالضرورة عن اتجاهات يتبناها المركز، وإنّما تعبّر عن رأي كتابِها.

www.bayancenter.org
info@bayancenter.org
Since 2014

مقدمـــــة:

تختلف الدول في عملية إدارة التهديدات التي تتعرض لها في مختلف المجالات السياسية والاقتصادية والاجتماعية والأمنية، خاصةً في ظلّ تنوع وتعدد تلك التهديدات واختلاف أثرها من فترة إلى أخرى. لذا، فإنّ أسلوب إدارتها يشكل نقطة مفصلية في عملية الحفاظ على كيان الدولة من تلك التهديدات. طبيعياً ما تملكه الدول المتقدمة من تقنيات حديثة لمواجهة وإدارة التهديدات التي تواجهها ليست متوفرة بنفس القدر في الدول المتخلفة أو النامية، التي تفتقد إلى تلك التقنيات أو للخبرة في استخدامها، أو حتى لسوء استخدامها. ومن الملاحظ في الآونة الأخيرة توسّعاً كبيراً في نوعية الهجمات التي أصبحت تهديداً مباشراً وغير مباشراً على الأمن الوطني للدول، بمختلف أنواعها وأشكال نظمها السياسية، مع تفاوت النسبة بين تلك الهجمات والعلاقة بين الأثر والتأثير.

وتُعدّ الهجمات السيبرانية واحدة من تلك التهديدات التي أصبحت تقلق الدول، نظراً لآثارها المدمرة على بنيتها السياسية والاقتصادية والأمنية والتكنولوجية. فقد أدى التطور الهائل والمتسارع الذي شهده العالم إلى جعل أمن الدول الوطني معرضاً للاختراق بصورة مباشرة، سواء داخلياً أو خارجياً، وإن كانت النسبة بينهما متفاوتة. وبما توفره الهجمات السيبرانية من مزايا كبيرة مقارنة بغيرها من الحروب، سواء للجهة المنفذة أو من حيث الفوائد المُتحققة، فقد أصبحت الوسيلة الأكثر استخداماً في الوقت الحاضر، كما تُعَدّ الأداة المستقبلية الرئيسية، لا سيما بالنسبة للدول المتقدمة.

ويُعدّ العراق واحداً من الدول التي يتعرض أمنه الوطني، بين الفينة والأخرى، لمختلف أنواع التهديدات، سواء المباشرة المرئية أو غير المرئية ذات التأثير الكبير. فمنذ عام 2003، وما شهده من تدمير للبنى التحتية وحلّ مؤسساته العسكرية والأمنية، وما تبع ذلك من تأسيس مؤسسات جديدة في محاولة لسدّ الفراغ الأمني الذي نشأ آنذاك، ظلّت التهديدات مستمرة، لا سيما التقليدية منها، مما أدى إلى تعرض الأمن الوطني العراقي لاهتزازات متكررة. غير أن ما واجهه العراق في عام 2014، مع دخول تنظيم داعش الإرهابي على خط المواجهة ومحاولته تأسيس دولته المزعومة على أرض العراق، شكّل أكبر تلك الاهتزازات، والتي سعى العراق بكل السبل للتصدي لها، ونجح بالفعل في تحقيق النصر وهزيمة ذلك التنظيم الإرهابي ميدانياً عام 2017. ومنذ ذلك الحين، اعتمد العراق سلسلة من الاستراتيجيات والآليات في محاولات جادة للتعافي والحفاظ على أمنه الوطني.

ومع ذلك، لا يزال يواجه نوعاً جديداً من التهديدات، والمتمثل في الهجمات السيبرانية، والتي تستدعي توفر مجموعة من الآليات لإدارتها والسيطرة عليها، سواء من قبل الفواعل الرسمية أو غير الرسمية، وبأساليب مختلفة.

وتتمحور مشكلة الدراسة حول طرح الأسئلة الآتية:

1. ما هي آليات إدارة الهجمات السيبرانية التي يتعرض لها العراق؟
2. كيف يمكن الحد من الهجمات السيبرانية والتقليل من أثرها على الأمن الوطني العراقي؟
3. ما العلاقة بين الهجمات السيبرانية والأمن الوطني العراقي؟
4. ما هي استراتيجيات الحكومة في مواجهة تطور الهجمات السيبرانية؟
5. لماذا لا يتم إنشاء هيئة متخصصة للإشراف والرقابة والمتابعة على الجهات المعنية بالأمن المعلوماتي؟

ويقتضي الأمر اتباع مجموعة من الآليات المختلفة والمتطورة لمواجهة الهجمات السيبرانية، إذ إن الجميع مسؤول عن الأمن الوطني العراقي وفقاً لمكانته والمسؤوليات الملقاة على عاتقه. فالعلاقة بين الأمن الوطني وتلك الهجمات علاقة مباشرة، حيث يُعدّ مجرد التعرض لاختراق البيانات وسرقتها مؤشراً على ضعف أمن الدولة. لذا، ينبغي على الحكومة والسلطات التشريعية والقضائية وضع استراتيجيات شاملة والعمل على تنفيذها، بالإضافة إلى إنشاء جهة متخصصة للإشراف والرقابة والمتابعة على عمل الجهات المعنية بالحفاظ على الأمن الوطني العراقي.

وتتضمن هيكلية البحث الآتي:

المبحث الأول: الهجمات السيبرانية مقاربة مفاهيمية

المبحث الثاني: العراق في مؤشر الامن السيبراني

المبحث الثالث: آليات إدارة الهجمات السيبرانية في العراق

المبحث الأول: الهجمات السيبرانية مقاربة مفاهيمية

تعددت المفاهيم المرتبطة بالأمن السيبراني؛ إذ تتقارب بعض هذه المفاهيم في أحيان وتبتعد في أحيان أخرى، لكنها جميعها تسهم في تحقيق الهدف المنشود من البحث. فالعملية البحثية تتطلب إيضاح المفاهيم أولاً، ومن ثم ربطها مع بعضها لتكوين صورة نهائية للقارئ. من بين هذه المفاهيم: الفضاء السيبراني، والأمن السيبراني، والهجوم السيبراني، والجريمة السيبرانية. لذا، سيتم توضيح جميع هذه المفاهيم مع التركيز على الهجمات السيبرانية كمتغير مستقل، والأمن الوطني كمتغير تابع.

إذ أدى التطور السريع للفضاء السيبراني، بحكم الاستخدام الواسع جداً للإنترنت سواء من قبل الأفراد أو المنظمات المحلية والإقليمية والدولية، والمؤسسات الحكومية وغير الحكومية، إلى تنامي أهميته الحيوية، مما جعل الاستغناء عنه أمراً محالاً. غير أن هذا الفضاء عُرضة لعدة تحديات، لا سيما تلك الهجمات الإلكترونية التي تستهدف البنى التحتية للدولة الضحية. وبسبب الترابط العضوي بين الأمن السيبراني والفضاء السيبراني والبنية التحتية لأي دولة، فإن الأضرار المتعمدة فيه تمثل تهديداً للأمن الوطني للدولة المستهدفة. وهذا يفسر إدراج معظم دول العالم لموضوع الأمن السيبراني كأحد أولويات أمنها الوطني.[1]

ويتألف الفضاء السيبراني من نظم حاسوبية مختلفة متصلة بالشبكة ونظم اتصالات سلكية ولاسلكية متكاملة، وأضحى الفضاء السيبراني أحد سمات المجتمع الحديث، وهو ما يعمل على تعزيز وتمكين الاتصال السريع، وأنظمة القيادة والتحكم الموزعة، وتخزين ونقل البيانات بكميات هائلة ومجموعة من الأنظمة الموزعة بشكلٍ كبير، وأصبحت كل هذه الأشياء الآن من المسائل المسلم بها لدى المجتمع وأصبحت عاملاً أساسياً للأعمال التجارية، وحياتنا اليومية وتقديم الخدمات. ويمكن رؤية انتشار الفضاء السيبراني في كل مكان والاعتماد عليه حتى في الميادين العسكرية، حيث تعتمد الاتصالات، والقيادة والتحكم، والاستخبارات والعناصر الهجومية الدقيقة جميعها على العديد من «النظم السيبرانية» ونظم الاتصالات ذات الصلة، وقد أدى انتشار هذه الأنظمة المترابطة إلقاء قدر من التبعية والضعف على الأفراد والصناعات والحكومات والتي يصعب التنبؤ بها أو إدارتها أو تخفيفها أو منعها. وترى بعض الدول هذه التبعيات الضعيفة على أنها مصدر قلق ناشئ فيما يتعلق

1- مصطفى ابراهيم سلمان، الامن السيبراني واثره في الامن الوطني العراقي، مجلة العلوم السياسية والقانونية، جامعة ديالى، كلية القانون والعلوم السياسية، المجلد(10)، العدد(1)، 2021، ص159.

بالأمن القومي أو الدفاع الوطني، وكلفت قوات الأمن التابعة لها بالاستجابة لها، في حين أنشأت دول أخرى منظمات جديدة بالكامل منوطة بإدارة سياسات الأمن السيبراني الوطني أو تنسيقها، وهكذا نشأ الأمن السيبراني كمسألة شاملة هامة والتي تتطلب استجابات من الأفراد والشركات الخاصة والمنظمات غير الحكومية و»الحكومة برمتها» وكذلك مجموعة من الوكالات والهيئات الدولية.[2]

وتباينت التعاريف الخاصة بالفضاء السيبراني وتكاد تكون مسألة منطقية نتيجة عدة عوامل منها التوقيت الذي جرى فيها التعريف والباحث وبيئته الداخلية والخارجية وغيرها، إذ إن تعريف المعهد الوطني للمعايير والتقنية الأمريكي (NIST) عرف الفضاء السيبراني بأنه «الشبكة المترابطة من البنى التحتية لتكنولوجيا المعلومات، والتي تشمل الإنترنت وشبكات الاتصالات السلكية واللاسلكية والنظم الحاسوبية والمعالجات المدمجة وأجهزة التحكم....» [3].

اما مصطلح الأمن السىبراني فقد شاع في السنوات الماضية على نطاق واسع، وأخذ يحظى بشعبية متزايدة لاسيما بعدما استخدمه الرئيس الامريكي آنذاك (باراك أوباما) الذي يعد الرئيس الرابع والأربعون للولايات المتحدة الأمريكية والذي امتدت فترة حكمه من 20 يناير من عام 2009، وحتى 20 يناير من عام 2017، في خطابه الذي دعا فيه الشعب الأمريكي إلى الاهتمام بالأمن السيبراني لتعزيز أمننا القومي[4]، وكذلك تم تعريفه على أنه «النشاط أو العملية أو القدرة أو الإمكانية أو الحالة التي يتم بموجبها حماية نظم المعلومات والاتصالات والمعلومات الواردة فيها من وإلى أو الدفاع عنها ضد الضرر أو الاستخدام أو التعديل غير المصرح به أو الاستغلال، وايضاً تم تعريفه بأنه هو الجهد المستمر لحماية هذه الشبكات المتصلة معاً وكافة البيانات من الاستخدام غير المصرح به أو الذي يسبب الضرر على المستوى الشخصي، تحتاج إلى حماية هويتك وبياناتك وأجهزتك الحاسوبية على مستوى الشركة، يتحمل الجميع مسؤولية حماية سمعة المؤسسة وبياناتها وعملائها على مستوى الدولة، فإن الأمن القومي وسلامة المواطنين ورفاهيتهم على المحك[5].

2- ج .ةُ .ج إي تر مُبلاي، الأمن السيبراني منهج مرجعي عام، أكاديمية الدفاع الكندية، حلف الناتو، 2016، ص17.
3- المصدر نفسه، ص17.
4- مصطفى ابراهيم سلمان، الامن السيبراني وأثره في الامن الوطني العراقي، مصدر سبق ذكره، ص154.
5- مقدمة في الامن السيبراني، دورة تدريبية مقدمة من سايكو، ص8.

وبما أن الإجراءات المتخذة لتأمين شيءٍ ما يجب أن تكون متناسبة مع قيمة ما يُجرى تأمينه، فإنه يوجد مستويات مختلفة من الأمن اعتماداً على مقاييس القيمة والمخاطر. ومن ثم، فإن تأمين الفضاء السيبراني ينطوي على عدد من الاعتبارات للتخفيف من المخاطر والتهديدات، في الوقت الذي يتم فيه التشجيع على إمكانية الوصول والانفتاح عبر مختلف أنواع الشبكات والأجهزة المترابطة. ويُعد تحقيق التوازن الضروري بين إمكانية الوصول وقابلية الاستخدام والأمن التحدي الرئيسي للدول، وخاصة تلك المتخلفة.[6]

فلقد أصبح الأمن السيبراني يشكل جزءاً أساسياً من أي سياسة أمنية وطنية للدول. فقد بات معلوماً أن صناع القرار في الدول الكبرى، وعلى سبيل المثال لا الحصر الولايات المتحدة الأمريكية، والاتحاد الأوروبي، وروسيا، والصين، والهند، وبعض الدول العربية مثل المملكة العربية السعودية ومصر وغيرها، يصنفون الأمن السيبراني كأولوية في سياساتهم الدفاعية الوطنية. فضلاً عن ذلك، فقد أعلنت أكثر من 130 دولة حول العالم عن تخصيص أقسام وسيناريوهات خاصة بالحرب السيبرانية ضمن فرق الأمن الوطني.[7]

يُعدُّ الأمن السيبراني مجموعةً من الوسائل الهادفة إلى الحد من خطر الهجوم على البرمجيات، وأجهزة الحاسوب، والشبكات. فهو يتضمن الأدوات المستخدمة في مواجهة «القرصنة الإلكترونية»، وكشف الفيروسات، وتأمين الاتصالات عبر التشفير. ويرى الاتحاد الدولي للاتصالات الأمن السيبراني على أنه: «مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات وممارسات فضلى، وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين». في حين يُعرّف الإعلان الأوروبي للأمن السيبراني بأنه «قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات».[8]

6- ج ۀ ج إي تر مُبلاي، الأمن السيبراني منهج مرجعي عام، مصدر سبق ذكره، ص9.
7- عدنان مصطفى البار وخالد علي المرحي، أمن المعلومات والأمن السيبراني، كلية الحاسبات وتقنية المعلومات، جامعة الملك عبدالعزيز، المملكة العربية السعودية، ب، ت، ص1.
8- صفد الشمري، الأمن السيبراني في العراق، اصول رقمية، منصة التواصل الرقمي، العراق، بغداد، 2022، متاح على الرابط الالكتروني التالي https://dcc-iq.com/?p=41841 تاريخ الزيارة 15\9\2024

وإذا ما تطرقنا لمفهوم الهجوم السيبراني، فإن تعريفه يُعدُّ من المسائل الشائكة التي تُشكّل عائقاً أمام فقهاء القانون؛ إذ وجدوا صعوبة في وضع تعريف عام وشامل، حيث لا يوجد تعريف جامع ومقبول له حتى الآن. كما أنه لا يوجد تعريف دقيق وواضح للهجوم السيبراني نتيجة اختلاف مواقف الدول في مواجهته. لذا، يرى فقهاء القانون الدولي أن النقطة الجوهرية في اعتبار النشاط الإلكتروني هجوماً سيبرانياً تعتمد على النتائج التي يخلفها الهجوم.[9]

أما الجريمة السيبرانية، فهي تتوقف في الأساس على الغرض من استخدام المصطلح، إذ تتمثل في عدد محدود من الأعمال التي تمس سرية البيانات أو النظم الحاسوبية وسلامتها وتوافرها لأغراض مختلفة بحسب الجهة القائمة بها.[10]

المبحث الثاني: العراق في مؤشر الأمن السيبراني

بلغ الإنفاق العالمي على المنتجات الأمنية 125.2 مليار دولار في عام 2020، مسجلاً زيادة بنسبة 6% مقارنة بعام 2019. ومن المتوقع أن يصل الإنفاق العالمي على المنتجات والخدمات الأمنية إلى 174.7 مليار دولار بحلول عام 2024، بمعدل نمو سنوي مركب قدره 8.1% خلال الفترة 2020-2024. تجدر الإشارة إلى أن القطاعات الثلاثة الأكثر إنفاقاً على الأمن السيبراني هي القطاع المصرفي، قطاع التصنيع، والحكومات الفدرالية/المركزية.[11]

ووفقاً للدعائم الخمس للبرنامج العالمي للأمن السيبراني، والمتمثلة في التدابير القانونية، والتقنية والتنظيمية وبناء القدرات والتعاون ومدى وجود استراتيجيات وسياسات للأمن السىبراني، ومدى وجود خطط ومعايير وطنية يتم تنفيذها على أرض الواقع مثل توفير التدريب والتأهيل للكوادر في مجال الأمن السىبراني والجهود والمبادرات المبذولة في هذا الشأن، كما يشير إلى أحد أهم العوامل، وهو وجود بنية تشريعية وقانونية تدعم الأمن السيبراني.[12]

9- نبيله هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2013، ص 24 – 25.
10- دراسة شاملة عن الجريمة السيبرانية، مكتب الامم المتحدة المعني بالمخدرات والجريمة، 2013، ص22.
11- خالد وليد محمود، قراءة في مؤشر الأمن السيبراني لعام 2021، مركز الجزيرة للدراسات، قطر، الدوحة، 2022م، متاح على الرابط التالي https://www.aljazeera.net/opinions/2022/2/16 تاريخ الزيارة 6\10\2024م.
12- المصدر نفسه.

فإن العراق، خلال الفترة من 2019 إلى 2024، لم يرتقِ إلى مصاف الدول المتقدمة عالمياً أو عربياً في مجال الأمن السيبراني. إذ يعتمد المؤشر العالمي للأمن السيبراني على 25 معياراً لقياس التزام 193 دولة عضواً في الاتحاد الدولي للاتصالات بالأمن السيبراني، من خلال الركائز الخمس: القانونية، والتقنية، والتنظيمية، وبناء القدرات، والتعاون. في عام 2019، حصل العراق على المرتبة 129 عالمياً من أصل 193 دولة، وعلى المركز السابع عشر عربياً، متفوقاً على عدد من الدول التي سبقته بفارق نقاط. أما في مؤشر 2020، فقد تقدم العراق إلى المركز 107 عالمياً، مما يُعد قفزة أمنية مهمة في مجال الأمن السيبراني وحماية بيانات المواطنين، باعتبارها جزءاً لا يتجزأ من الأمن القومي العراقي.[13]

وحسب مركز الإعلام الرقمي العراقي، فقد شهد العراق تراجعاً في عام 2021، حيث تراجع 22 مرتبة عن آخر إحصائية، ليحصل على المرتبة 129 عالمياً في مؤشر الأمن السيبراني من أصل 182 دولة، بعد أن كان في المركز 107 في التقرير السابق. وأوضح المركز أن الأمن السيبراني وحماية بيانات المواطنين العراقيين هما جزء لا يتجزأ من الأمن القومي العراقي. كما أشار إلى أن العراق قد تراجع أيضاً على المستوى العربي، حيث حصل على المرتبة 17، متفوقاً فقط على مجموعة من الدول العربية الفقيرة جداً مثل موريتانيا، والصومال، وجزر القمر، وجيبوتي، واليمن، في حين تفوقت عليه بقية الدول العربية بما فيها سوريا، وفلسطين، وليبيا، ولبنان، والسودان.[14]

في نسخة 2021 التي أصدرها الاتحاد العالمي للاتصالات، جاءت الولايات المتحدة الأمريكية في المركز الأول بدرجة 100 %، بينما احتلت السعودية المركز الثاني بدرجة 99.5 %. أما ترتيب الدول العربية ضمن مركزها العالمي فجاء على النحو التالي:

13- رغد الحسيني، الأمن السيبراني وموقعه في العراق، وكالة ارض اشور، العراق، 2023، متاح على الرابط الالكتروني التالي https://ashourland.net تاريخ الزيارة 11\10\2024م.
14- العراق يتراجع عالمياً وعربياً في «الامن السيبراني»، تقرير مركز الاعلام الرقمي العراقي.

ت	الدولة	المرتبة عربياً	المرتبة عالمياً	الملاحظات
1	السعودية	الأولى	الثانية	لم تدرج دولة اليمن في هذه النسخة إذ حققت (6) مؤشرات فقط من أصل (77) مؤشراً، التي يعتمد عليها التصنيف في تقييم القدرات السيبرانية للبلدان، ويعود ذلك إلى أسباب عديدة منها عدم وجود كادر متخصص في الأمن المعلوماتي (السيبراني) وعدم اهتمام قيادات الدولة بقطاع أمن المعلومات والاتصالات بالشكل الكافي، وعدم وجود جهاز حكومي متخصص في تقديم خدمات الدفاع والأمن للفضاء السيبراني، بالإضافة إلى عدم وجود أطر وتشريعات قانونية متكاملة وحديثة تؤسس لقاعدة وطنية فاعلة للأمن السيبراني الوطني، وكذا ضعف التنسيق بين الأجهزة الحكومية ونظائرها في دول الجوار والعالم فيما يخص سبل تدعيم الأمن السيبراني لليمن.
2	الإمارات	الثانية	الخامسة	
3	عُمان	الثالثة	الحادية والعشرون	
4	مصر	الرابعة	الثالثة والعشرون	
5	قطر	الخامسة	السابعة والعشرون	
6	تونس	السادسة	الخامسة والأربعون	
7	المغرب	السابعة	الخمسون	
8	البحرين	الثامنة	الستون	
9	الكويت	التاسعة	الخامسة والستون	
10	الاردن	العاشرة	الواحد والسبعون	
11	السودان	الحادي عشر	مائة وواحد	
12	الجزائر	الثانية عشر	مائة وأربعة	
13	لبنان	الثالثة عشر	مائة وتسعة	
14	ليبيا	الرابعة عشر	مائة وثلاثة عشر	
15	فلسطين	الخامسة عشر	مائة واثنان وعشرون	
16	سوريا	السادسة عشر	مائة وستة وعشرون	
17	العراق	السابعة عشر	مائة وتسعة وعشرون	
18	موريتانيا	الثامنة عشر	مائة وثلاثة وثلاثون	
19	الصومال	التاسعة عشر	مائة وسبعة وثلاثون	
20	جزر القمر	العشرون	مائة وخمسة وسبعون	
21	جيبوتي	الواحدة والعشرون	مائة وتسعة وسبعون	

الجدول من إعداد الباحث بالاعتماد على بيانات متوفرة من مجموعة مصادر.

يلحظ الباحث أن مركز العراق في هذا المؤشر العالمي متدني جداً مقارنة بدول المنطقة بشكل خاص والدول العربية بشكل عام. ولعل ذلك يعود إلى مجموعة من الأسباب التي تتعلق في طبيعتها بالبنى التحتية. فضلاً عن ذلك، فإن سبب التراجع يعود إلى أن العراق لم يقدم إجابات على الاستبيان الذي جمعه فريق المؤشر، والذي تضمن بعض المعلومات والبيانات. وهذا يطرح عدة تساؤلات حول سبب هذا التجاهل من قبل الجهات المسؤولة عن ملف الأمن السيبراني في العراق. كما أن هذا التراجع في الملف الأمني السيبراني يعود إلى عدم وجود مؤسسة متخصصة بالأمن السيبراني في العراق. وما هو موجود لا يتعدى كونه مجرد أقسام في دوائر مختلفة تفتقر إلى التنسيق أو التعاون المحترف في هذا المجال، حيث تعمل كل جهة منها بشكل منفرد.

بينما جاءت السعودية متفوقة على البلدان العربية في هذا المؤشر لعام 2023، نتيجة عدة عوامل، منها عدد من المبادرات المتمثلة في إطلاق البوابة الوطنية لخدمات الأمن السيبراني «حصين» لتقديم خدمات وحلول سيبرانية مبتكرة، وتوفير برامج نوعية لبناء القدرات البشرية الوطنية وتعزيز تنافسيتها محلياً وعالمياً، وتمكين رواد الأعمال والمبتكرين في سوق الأمن السيبراني. كما تم إصدار تنظيمات لتعزيز الأمن السيبراني ومتابعة التزام الجهات الوطنية بها، بالإضافة إلى إطلاق مبادرات دولية لدعم الجهود وتوحيد المساعي المشتركة في مجال الأمن السيبراني. فضلاً عن ذلك، فقد بينت الهيئة الوطنية للأمن السيبراني أن هذه المرتبة تأتي انعكاساً للدعم اللامحدود والتمكين الذي توليه القيادة لقطاع الأمن السيبراني، وتأكيداً على التطوير المستمر الذي يشهده قطاع الأمن السيبراني في المملكة، وامتداداً لجهود الهيئة المبذولة في بناء وتعزيز قطاع الأمن السيبراني، والتي أسهمت بدورها في إحراز هذه المرتبة العالمية للمرة الثانية على التوالي.[15]

أما في مؤشر عام 2024م الصادر عن الاتحاد الدولي للاتصالات، فقد أظهر نتائج استثنائية للدول العربية، بما في ذلك العراق الذي يعيش أجواء مضطربة من التجسس والابتزاز الإلكتروني. وقد صنف التقرير الدول إلى خمس طبقات وفقاً لالتزامها بمتطلبات الأمن السيبراني التي حددها الاتحاد، فجاءت البحرين، مصر، الأردن، عمان، المغرب، قطر، والسعودية ضمن الطبقة الأولى نتيجة التزامها بتلك المؤشرات. أما العراق، فقد جاء في

15- السعودية الثانية عالمياً في مؤشر الأمن السيبراني، وكالة العربية الحدث، متاح على الرابط الالكتروني التالي
https://www.alarabiya.net/aswaq/economy/2023/06/20.

الطبقة الرابعة ما قبل الأخيرة، إلى جانب دول مثل لبنان، موريتانيا، جيبوتي، الصومال، فلسطين، والسودان، وسوريا. في حين احتلت اليمن الطبقة الخامسة منفردة بها، مما يعني وجود تخلف سيبراني يعانيه العراق، على الرغم من الإمكانيات المادية التي يمتلكها والمرصودة لهذا القطاع.[16]

يرى الباحث أن العراق، ومنذ هذه السنوات الخمسة، لم يحقق تقدماً في المؤشر العالمي، مما يعني وجود ضعف وعدم التزام في متطلبات تحقيق الأمن السيبراني. وهذا يتطلب العمل على تحسين الوضع من قبل مختلف الجهات الحكومية وغير الحكومية المعنية بهذا المجال. هناك دول عربية مجاورة تتمتع بمراكز متقدمة في المؤشر بفضل تفوقها في مجموعة النقاط، مما منحها مراكز أعلى وجعلها أقل تعرضاً لخطورة الهجمات السيبرانية، وبالتالي ساعد في حماية أمنها الوطني والقومي من آثار تلك الهجمات. الأمر الذي يتطلب في مجمله اتباع مجموعة من الآليات لإدارة الهجمات السيبرانية التي يتعرض لها العراق بين فترة وأخرى، وما سيتم الحديث عنه في المبحث التالي.

المبحث الثالث: آليات إدارة الهجمات السيبرانية في العراق

لا تزال الآليات المتبعة في العراق بمختلف أشكالها وأنواعها تحتاج إلى التكيف والتطور بما يتماشى مع التقدم التكنولوجي والتهديدات التي تفرضها الهجمات السيبرانية، أو حتى تلك التي تفوقها في حدتها. وهذه تعد نتيجة منطقية لمواجهة الهجمات المستمرة التي يتعرض لها العراق، سواء من الفاعلين الدوليين أو غير الدوليين (مثل الجماعات والمنظمات الإرهابية). فمجموعة الوسائل التقنية، والأدوات، والتنظيمات الإدارية، والتشريعات القانونية المتبعة، لم تعد كافية لمواجهة تلك الهجمات السيبرانية، مما يعرض المعلومات والبيانات في مختلف المؤسسات العراقية للخطر، وبشكل متكرر يتفاوت بين الزيادة والنقصان. وبالتالي، يتعرض الأمن الوطني العراقي للاختراق من قبل تلك الفواعل، سواء كانت دولية أو غير دولية، وإن كانت النسبة بينهما مختلفة لصالح الأخيرة في بعض الأحيان، مثل التنظيمات الإرهابية التي أصبحت تشكل تهديداً حقيقياً لأمن الدول، ومنها العراق.

16- بالتزامن مع ازمات التجسس والابتزاز تصنيف جديد فاضح للعراق بالأمن السيبراني، السومرية، 2024، متاح على الرابط التالي alsumaria.tv تاريخ الزيارة 12\11\2024

الآليات الحكومية لمواجهة تلك الهجمات السيبرانية، وإن كانت بنظر البعض ضعيفة أو غير كافية، إلا أنها جديرة بالاهتمام والبحث العلمي لبيان مدى اهتمام العراق الرسمي وغير الرسمي في هذه المسألة الحيوية التي تؤثر على الأمن الوطني العراقي. إذ إن هناك مجموعة من الآليات التي تتمثل في الآتي:

1- الآليـــة التشريعية

لا يوجد في العراق قانون خاص بحماية البيانات في الوقت الحالي، إذ تُطبَّق تشريعات الخصوصية القديمة والمتخلفة (التي لا تستطيع تغطية أركان الجريمة السيبرانية) إلى حد كبير، وتؤثر بأثر رجعي على الإنترنت. كما يفتقر القضاء العراقي إلى أي تشريع محدد بشأن الجرائم الإلكترونية، مما يعني أن القانون المدني العراقي القديم لعام 1951م وقانون العقوبات لعام 1969م يُستخدمان فيما يتعلق بالجرائم الإلكترونية. وقد أفضى غياب البيئة القانونية بشأن الفضاء الإلكتروني إلى تعقيد توفير الأمن السيبراني الشامل لكل من مؤسسات الدولة والشركات، في حين جعل محاكمة الظواهر الجديدة والمتنامية للجريمة السيبرانية أمراً صعباً بشكل مستمر.[17]

ولا يزال قانون الجرائم المعلوماتية (الإلكترونية) في أروقة مجلس النواب ولم يتم تشريعه نتيجة لعوامل سياسية، منها عدم الاتفاق على بعض المواد بين الأحزاب السياسية ومحاولة طرحه ضمن «سلة القوانين» أو في المقايضة التشريعية، حيث يتم التصويت عليه مقابل التصويت على قوانين أخرى من قبل الأحزاب السياسية المتبينة له. فضلاً عن ذلك، هناك عوامل دولية ضاغطة من قبل المنظمات الدولية لحقوق الإنسان، بالإضافة إلى ضغط الشارع العراقي والمطالبات الجماهيرية بعدم تشريعه، نتيجة ما أشيع حول القانون من سلبيات تتعلق بتقييد حرية الفرد العراقي إلكترونياً. وقد جاء مقترح القانون لتنظيم استخدام شبكات المعلومات وأجهزة الحاسوب والأجهزة والأنظمة الإلكترونية. وقد تم تقديم القراءة الأولى للقانون المقترح أمام مجلس النواب العراقي في يوم 27/7/2011م، ولكن لم تُجرَ القراءة الثانية للقانون حتى بعد مرور هذه السنوات العديدة على القراءة الأولى، ورغم المحاولات البرلمانية من قبل لجنة الأمن والدفاع، إلا أنه لا يزال خارج حسابات السلطة التشريعية.

17- هاشم شبر، تنظيم الجهد المؤسساتي والوزاري المشترك ازاء الامن السيبراني في العراق، مركز البيان للدراسات والتخطيط، العراق، بغداد، 2022، ص6.

2- الآليـــة الإدارية

تعد الآلية الإدارية جزءاً من التزامات الحكومة العراقية، كونها المسؤول الأول بالاشتراك مع السلطة التشريعية في حماية أمن العراق الوطني حسب الدستور العراقي النافذ لعام 2005م. فقد قامت وزارة الاتصالات في العام الماضي بإنشاء مشروع بوابات النفاذ الدولية من خلال وثيقة السياسات والمعايير لأمن المعلومات ومشاركة البيانات التي جرى إقرارها من قبل مجلس الوزراء. ويتمثل هذا المشروع في اعتماد إجراءين لمواجهة تلك التهديدات السيبرانية، وهما كالآتي:[18]

أ- الاجراء الأول: هو مقاومة هذه الهجمات عن طريق تحصين مواقع المؤسسات ووضع جدار ناري تقني عليها.

ب- الإجراء الثاني: اتخاذ إجراءات للحد من أضرار تلك الهجمات بعد حدوثها.

3- الآليـــة التعليمية

يُعد التعليم واحداً من الآليات المهمة في الحد من وتقليل مخاطر الهجمات السيبرانية وأثرها على الأمن الوطني العراقي. لذا، سعت الحكومة العراقية إلى تأسيس وإنشاء أقسام في الجامعات لتدريس مناهج الأمن السيبراني، فضلاً عن إقامة الورش من قبل الجهات الأمنية والاستخبارية في الجامعات للتوعية بمخاطر الهجمات وكيفية الوقاية منها بالنسبة للأفراد أولاً، والمؤسسات التعليمية ثانياً. لذا، يستلزم الأمر الاهتمام أكثر بهذه الآلية والمضي قدماً فيها بزخم كبير من أجل التعريف بمخاطر هذه المشكلة السيبرانية وآثارها على الأمن العراقي، وزرع ثقافة حماية البيانات والمعلومات لدى الفرد، مع توعية حول كيفية التعامل مع الروابط والفيروسات، خاصة لأولئك الذين يتعاملون مع المعلومات، وإيلاء أهمية كبيرة لها.

4- الآليـــة الاستراتيجية

تعد هذه الآلية واحدة من أكثر الآليات أهمية وضرورة ملحة، والتي نصت عليها وثيقة السياسات والمعايير لأمن المعلومات ومشاركة البيانات المقرّة من مجلس الوزراء العراقي. إذ أشارت الوثيقة إلى أن من بين السياسات التي يمكن اتباعها في سبيل تقليل الضرر هو إنشاء مستشارية الأمن الوطني الاستراتيجية للأمن السيبراني، التي تمتد للسنوات المقبلة.

18- انس العزاوي، إجراءات عراقية لمواجهة الهجمات السيبرانية، موقع الحل، 2022، متاح على الرابط الالكتروني التالي https://7al.net/2022/06/11 تاريخ الزيارة 15\11\2024م، وكذلك ينظر الى مركز التطوير الرقمي، العراق يعتمد إجراءين لمواجهة الهجمات السيبرانية، 2022.

5_الآليـــة الثقافية -المجتمعية- القطاعية

في كل الأزمات أو التحديات التي تواجهها الدولة، يكون الفرد هو الأساس في تجاوزها. وهي أيضاً مبدأ من المبادئ الأربعة التي حددتها الجمعية الأمريكية للإنترنت، والتي تمثل في الوعي. فالوعي المجتمعي والثقافة تجاه الهجمات السيبرانية قد تكون كفيلة للحد من تلك الهجمات أو آثارها، ولو بنسبة معينة. إذ أشارت الجمعية إلى أن على جميع الجهات المعنية في القطاعات المختلفة فهم المخاطر التي تهدد أمنها، ومدى تأثير تلك المخاطر عليها وعلى الآخرين في النظام البيئي المختص بالبنى التحتية لشبكة الإنترنت واستخداماتها. كما اشترطت مبدأ ينبغي على جميع الجهات المعنية تحمُّل مسؤولية مواجهة المخاطر الأمنية التي تهدد أمنها، مع الأخذ في الاعتبار الآثار المترتبة على اتخاذ إجراء ما، أو التقاعس عنه، والتعاون بإشراك جميع الجهات المعنية، بما في ذلك الأطراف المعنية خارج الحدود المحلية في حوار مستمر حول الأمن السيبراني لمواجهة التهديدات السيبرانية.[19]

إذ يواجه أمن المعلومات مجموعة من المخاطر الفنية والبشرية والطبيعية، وما يهمنا في هذه الفقرة هو النوع الثاني، المتمثل في المخاطر البشرية، والتي تقسم بدورها إلى قصدية وغير قصدية. لذا، يجب زرع ثقافة حماية المعلومات والتنبيه على العقوبات المترتبة في حال القصدية في تسريبها. هناك تهديدات كثيرة تحيط بأنظمة المعلومات، وتتعدد هذه التهديدات وتتنوع بتنوع هياكل الأنظمة المعلوماتية ونقاط الضعف فيها. ويمكن تقسيم تهديدات أمن المعلومات إلى ثلاث فئات رئيسية تحتوي كل فئة منها على عدد كبير من التهديدات، وتتمثل في الآتي:[20]

1- تهديدات فنية

وهي تلك التهديدات الناجمة عن الأخطاء الفنية في مختلف أنظمة أمن المعلومات، ومنها تهديدات عيوب التصميم في الأجهزة والبرامج والشبكات وعيوب التشغيل وعيوب تشتت المعلومات.

19- صفد الشمري، ما واقع الأمن السيبراني في العراق؟، جريدة الصباح، 2021م، متاح على الرابط الالكتروني التالي https://alsabaah.iq/48007-.html تاريخ الزيارة 9\12\2024م.
20- عدنان مصطفى البار وخالد علي المرحي، امن المعلومات والامن السيبراني، مصدر سبق ذكره، ص4.

2- تهديدات بشرية

ويقصد بها التهديدات الناتجة عن العنصر البشرى مباشرة. فقد يتسبب العنصر البشرى عمداً أو عن طريق الخطأ في الضرر أو إتلاف المعلومات أو تسريبها لجهات خارجية أو الوصول إلى معلومات والاطلاع عليها دون أن يكون له صلاحية لذلك. يمكن حصر أهم مصادر التهديدات البشرية للنظم المعلوماتية في الآتي:

أ - المستفيد النهائي الشرعي الفاسد.
ب - موظف المنشأة الفاسد.
ج - المستفيد النهائي الشرعي وموظف المنشأة غير الواعيين بالمخاطر الأمنية، بالرغم من أنهم غير فاسدين.
د - المؤسسات التجارية ذات النوايا المنحرفة، إذ قد يكون الدافع التنافس التجاري.

3- تهديدات طبيعية

ويقصد بها الكوارث الطبيعية التي ليس للإنسان أو التجهيزات الفنية دخل في حدوثها كالحرائق والزلازل وقد تلحق هذه الكوارث أضرار كبيرة بأنظمة المعلومات وقد تؤدى إلى انقطاع الخدمات الإلكترونية نهائياً، وبعد التعرف إلى أنواع التهديدات المعلوماتية، أصبحت الحاجة لأمن المعلومات ضرورية من أجل تحليل هذه التهديدات باختلاف أنواعها سواء كانت مركزية، بشرية أو طبيعية ووضع الخطط والبرامج اللازمة للحماية منها أو التخفيف من آثارها.

6_الآليـــة التقنية

تقع هذه المهمة على عاتق الجهات الحكومية ذات العلاقة المباشرة بالموضوع والمسؤولة عن حماية أمن العراق الوطني، ومنها مستشارية الأمن الوطني التي تحاول وضع استراتيجيات خلال السنوات الماضية لمعالجة وتقليل الهجمات. ففي واحدة من تلك الاستراتيجيات، وعبر دراسة لها، استراتيجية الأمن السيبراني في البلاد، أوضحت أن العراق ليس بعيداً عن التهديدات السيبرانية التي تتمثل في الجريمة الإلكترونية، التجسس السيبراني، الإرهاب الإلكتروني، وإساءة معاملة الأطفال واستغلالهم عبر الإنترنت. وضعت الدراسة عدة مراحل زمنية يتم من خلالها

تحديد الضعف الهيكلي في نظم المعلومات العراقية، وبالتالي 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. 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.[21]

7_الآليـــة التعاونية والتدريبية

تعد واحدة من الآليات الناجعة لحماية أمن العراق الوطني من الهجمات السيبرانية، إذ لا بد من ضرورة التعاون بين المؤسسات المعنية بالأمن في هذه الجزئية من خلال تبادل الخبرات والكوادر الأمنية بينها. فضلاً عن تعاون هذه المؤسسات مع المراكز والمؤسسات في القطاع الخاص ذات الاهتمام والتوجه الأمني بشكل عام، والسيبراني والرقمي بشكل خاص. ومنها على سبيل المثال لا الحصر: مركز الإعلام الرقمي العراقي، مركز التطوير الرقمي، منصة التواصل الرقمي، مجلس المسار الرقمي العراقي، مركز المعلومات الرقمية وغيرها.

ويتطلب واقع الأمن السيبراني العراقي، والمخاطر والتهديدات المستمرة التي تعترضه، إحداث هيئة وطنية موحدة لجميع التشكيلات والفرق الإلكترونية للأجهزة العراقية، التي يمكن أن تشكّل البنية التحتية الأساسية له، ضمن مسار الاستراتيجية الوطنية للأمن السيبراني، وبصلاحيات موسعة. ويعمل هذا الكيان على تأمين وضع البلاد في البُعد الخامس للحروب المعاصرة، إلى جانب تعديل النصوص التشريعية المرتبطة بمواجهة الجرائم السيبرانية، بما يتناسب مع المعطيات المعاصرة. كما ينبغي إرساء ثقافة عامة للأمن السيبراني على صعيدي المؤسسات والأفراد، وتشجيع البحث العلمي في هذا المجال، عن طريق افتتاح أقسام أو فروع علمية في الجامعات العراقية. إضافة إلى ذلك، ينبغي تحفيز الباحثين لإجراء دراسات حول الأمن السيبراني بناءً على ارتباطه بتخصصاتهم العلمية

21- انس العزاوي، إجراءات عراقية لمواجهة الهجمات السيبرانية، موقع الحل، 2022، متاح على الرابط الالكتروني التالي https://7al.net/2022/06/11 تاريخ الزيارة 17\12\2024م.

وتدريب وتنمية المهارات الرقمية بشكل مستمر لمواكبة المستجدات الإلكترونية على مستوى المنطقة والعالم.[22]

8-الآليـــة الإقليمية والدولية

رافق التطور الكبير في البرامج وتقنيات الحاسوب ضعف التشريعات العقابية، بل إنها في بعض الدول تكون معدومة، مما يجعل من الصعب الحد من هذه الهجمات. وقد أدى ذلك إلى ضعف الموقف الدولي بشكل عام في مواجهة هذا الخطر. فعلى سبيل المثال لا الحصر، كشفت دراسة حديثة للإنتربول أن (93) دولة من أصل (187) لا تمتلك تشريعات داخلية تجرم بعض الظواهر الإلكترونية، مثل تصوير الأطفال بشكل إباحي وغيرها من الظواهر الأخرى. وهذا يعني أنه إذا كانت الدول لا تمتلك التشريعات اللازمة لمعالجة هذه المشكلة ضمن قوانينها الداخلية، فكيف لها أن تتفاعل بجدية مع بعضها البعض لمواجهة الهجمات السيبرانية من خلال إبرام وتنفيذ الاتفاقات الخاصة بهذا الشأن؟ وبالتالي، يبرز هذا الاختلاف بشكل واضح في مواقف الدول من حيث تشريعاتها الداخلية التي تُعد ثغرة يمكن للمهاجمين استغلالها للدخول من خلالها.[23]

9-الآليـــة المفاهيمية

يتطلب من المعنيين بالأمن عموماً والأمن السيبراني بشكل خاص التمييز بين المفاهيم ذات الصلة وعدم الخلط بينها للعمل بفعالية. فهناك فرق بين الهجوم السيبراني والجريمة السيبرانية، إذ لا شك أن هناك تبايناً بين مفهوم الهجوم السيبراني والجريمة السيبرانية، اللذين يتم تبادلهما بشكل متكرر من قبل المهتمين في هذا المجال. الخلط بين هذين المصطلحين قد يؤدي إلى إثارة مشكلات جديدة قد تنتهي بخرق القانون الدولي، خاصة إذا تجاهلت الدولة المعتدى عليها تحديد نوع الاعتداء، سواء كان هجوماً سيبرانياً أم جريمة سيبرانية. فحق الدولة المعتدى عليها في حالة الهجوم السيبراني يختلف عن حقها في الرد على الجريمة السيبرانية، إذ أن الهجوم السيبراني يشمل فعلاً يهدف إلى التأثير على قدرات ووظائف شبكات الحاسوب لأهداف قومية أو سياسية، من خلال استغلال نقاط الضعف لتمكين المهاجم من اختراق الأنظمة والتلاعب بها.[24]

22- صفد الشمري، الأمن السيبراني في العراق، اصول رقمية، منصة التواصل الرقمي، العراق، بغداد، 2022، متاح على الرابط الالكتروني التالي https://dcc-iq.com/?p=41841 تاريخ الزيارة 20\12\2024

23- علي فاضل علي سليمان، حق الدفاع الشرعي على الهجمات السيبرانية، مجلة جامعة تكريت للحقوق، كلية القانون، جامعة تكريت، المجلد (4) العدد (4) الجزء (1)، السنة (4)، 2020، ص250.

24- Ian Traynor، Russia Accused of Unleashing Cyber War to Disable Estonia، Guardian London، May 17، 2007p32.

لذا، ينبغي التعامل مع الهجمات السيبرانية بوصفها أعمال حرب، لأنها تشبه الهجمات المسلحة التي ينظمها قانون الحرب. ويتضح أن الهدف من الهجوم السيبراني يعكس بوضوح أنه نتاج سياسة دولة، وليس مجرد فعل صادر عن فرد أو جماعة قرصنة. في المقابل، تُعرَّف الجريمة السيبرانية بأنها مخالفة تُرتكب ضد الأفراد أو الجماعات بدافع إجرامي، مثل الدخول غير المصرح به إلى الأنظمة، أو إتلاف البيانات المخزنة، أو اعتراضها ونقلها بشكل غير قانوني من جهاز حاسوب إلى آخر، كإدخال بيانات خاطئة أو العبث بها. كما عرّفها بعض الباحثين بأنها: "سلوك غير مشروع معاقب عليه قانوناً، صادر عن إرادة جرمية، ويستهدف معطيات الحاسوب.[25]

لذا، فإن الهجوم السيبراني يندرج ضمن اختصاص القانون الدولي العام، لأنه يمثل خرقاً لسيادة الدولة، بينما تقع الجريمة السيبرانية ضمن نطاق القانون الوطني وفقاً لمبدأ إقليمية القانون. وبالتالي، فإن ما يميز الهجوم السيبراني عن الجريمة السيبرانية هو أن الأول يهدف إلى إضعاف أو تدمير قدرات الدولة من خلال شبكات الإنترنت لتحقيق أهداف سياسية أو متطلبات الأمن القومي، في حين أن الجريمة السيبرانية تقتصر على تحقيق مكاسب مالية أو نقدية، مثل السرقة أو الاحتيال. في كلا الحالتين، تتحمل الدولة مسؤولية دولية عن أفعال مواطنيها التي تلحق الضرر بمصالح الدول الأخرى، مما يستوجب اتخاذ تدابير للحد من الهجمات السيبرانية.[26]

25- نائل عبد الرحمن صالح، واقع جرائم الحاسب في التشريع الاردني، مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الامارات العربية المتحدة، المجلد (1)، ط3، 2004، ص 192.
26- علي فاضل علي سليمان، حق الدفاع الشرعي على الهجمات السيبرانية، مصدر سبق ذكره، ص250.

الخاتمـــة:

تتطلب عملية إدارة التهديدات، بمختلف أنواعها وأشكالها ودرجات خطورتها، مجموعة من السياسات والآليات التي تتناسب مع طبيعة تلك التهديدات وتعمل على الحد منها قدر الإمكان. لذلك، تولي الدول، على اختلاف أنظمتها، أهمية كبيرة لهذه المسألة، ولا سيما في مجال الأمن السيبراني، حيث يُعدّ انعدامه واحداً من أخطر التهديدات العالمية. فوفقاً لتقرير المخاطر العالمية لعام 2023 الصادر عن المنتدى الاقتصادي العالمي، يحتل انعدام الأمن السيبراني المرتبة الثامنة من حيث شدة التأثير على المديين القصير والطويل. ولهذا السبب، نجد أن حكومات الدول المتقدمة، على وجه الخصوص، تُدرجه ضمن أولويات سياساتها، وتسعى، بالتعاون مع السلطة التشريعية، إلى سنّ مجموعة من القوانين لمعالجة هذه القضية، نظراً لتأثيرها المباشر على طبيعة النظام السياسي والاقتصادي والاجتماعي، وكذلك على العلاقة بين السلطات والأفراد، سواء من حيث تحقيق التوازن أو الإخلال به.

واجه العراق بعد عام 2003 مجموعة كبيرة من التهديدات في مختلف المجالات، كان أولها تهديد كيان الدولة بالكامل نتيجة التغيير الشامل الذي تعرض له جراء التدخل العسكري للولايات المتحدة وحلفائها. تلا ذلك تهديدات أمنية تمثلت في ظهور الفاعلين من غير الدول، وعلى رأسهم التنظيمات الإرهابية، بدءاً بتنظيم القاعدة ثم تنظيم داعش، واستمرت هذه التهديدات حتى تحولت إلى تهديدات سيبرانية تستهدف العراق ومؤسساته المختلفة بين الحين والآخر. وتشمل هذه التهديدات عمليات سرقة وتسريب بيانات ومعلومات حساسة تخص العديد من الوزارات، بالإضافة إلى استخدامها في المساومة والابتزاز، مستغلين ضعف البنية التحتية للمؤسسات العراقية. وبما أن التهديدات السيبرانية تشهد تطوراً متسارعاً، فإنه من الضروري تحقيق تطور سيبراني موازٍ لها أو يفوقها، بهدف منع هذه التهديدات أو على الأقل الحد منها.

ولمواجهة تلك التهديدات السيبرانية، سواء الصادرة عن دول أو جهات غير حكومية، لا بد من وضع استراتيجية شاملة تمتد على المديين القصير والطويل. ويجب أن تتضمن هذه الاستراتيجية مجموعة من الآليات الفعالة، مع إشراك مختلف الجهات المعنية لضمان حماية البيانات والمعلومات في المؤسسات الحكومية وغير الحكومية على حدٍ سواء.

الاستنتاجات والتوصيات:

توصل الباحث إلى مجموعة من الاستنتاجات، وعلى ضوء ذلك، هناك جملة من التوصيات نأمل أن تجد طريقها إلى المعنيين والمسؤولين، والتي تتمثل فيما يلي:

الاستنتاجات:

1. لا يزال العراق يحتل موقعاً ضعيفاً في مؤشر الأمن السيبراني مقارنة بالدول المتقدمة، ويعد ضعيفاً جداً مقارنة بالدول العربية الإقليمية.
2. يعاني العراق من التعرض إلى هجمات سيبرانية من جهات دولية وغير دولية نتيجة ضعف الإجراءات الخاصة بحماية المعلومات، إذ لم تكن التدابير الموضوعة كافية لضمان أمن وحماية الوجود العراقي في الفضاء السيبراني.
3. لم يؤسس العراق مؤسسة خاصة بالأمن السيبراني إلا في وقت متأخر جداً في الوقت الذي زادت التهديدات السيبرانية بدرجة كبيرة، لذلك جاءت تلك المؤسسة ضعيفة مقارنة بحجم التهديدات.
4. لم تأخذ الجهات غير الرسمية دورها المناط بها في مساعدة الجهات الحكومية في هذه المسألة فلم تبادر من ذاتها إلا حين طلب منها ذلك. ورغم هذا، فهي لا تزال ضعيفة جداً مقارنة بحجم التهديد السيبراني.
5. لا تزال استراتيجية الامن السيبراني العراقي هلامية غير واضحة في الكثير من ابوابها وجزئياتها فعند قراءتها والاطلاع عليها نجد سقفاً زمنياً للتنفيذ والمحدد بسنة من خلال معالجة المخاوف الفورية وثلاث سنوات بناء البنية التحتية وخمسة سنوات وما بعدها تطوير بالاعتماد على الذات، إلا أن ذلك واقعياً لم يحصل.

التوصيات:

1. يتطلب النص في استراتيجية الأمن السيبراني العراقي على صفة الإلزامية للجهات التنفيذية.
2. ضرورة إيلاء الاهتمام والدعم الكافي مادياً وتقنياً ومعنوياً لفريق الاستجابة للحوادث السيبرانية العراقي (CERT) من أجل القيام بمهامه في الأمن السيبراني وحماية البنية التحتية للإنترنت، ونشر الوعي في مجال حماية الخصوصية والحماية الذاتية.

3. العمل على تأسيس جامعة أو كلية للأمن السيبراني والتعاون مع الجامعات العالمية، من أجل تخريج مجموعة من الطلبة وبجودة عالية والاعتماد على النوعية وليس الكمية وضمن مواصفات وصفات تحددها السلطات والجهات صاحبة الاحتياج السيبراني.
4. ضرورة متابعة المؤشرات السيبرانية الصادرة من المراكز العالمية المعنية بالأمن السيبراني، وتحليل موقع العراق ضمن هذه المؤشرات على مدى خمس سنوات، من اجل تحليل اسباب التراجع في حالة حصولها او الاستثمار في حالة الصعود وتعزيزه.
5. بناء وزيادة الوعي السيبراني لمواجهة التحديات والتهديدات من أجل التعاون والتشارك مجتمعياً في هذه المسألة بحيث لا يؤثر على حماية وامن المعلومات وتصبح العملية عكسية يتعلم من خلالها البعض ليستغلها ويكون طرفاً في عملية التهديد.

قائمة المصادر

1. عدنان مصطفى البار وخالد علي المرحي، أمن المعلومات والأمن السيبراني، كلية الحاسبات وتقنية المعلومات، جامعة الملك عبدالعزيز، المملكة العربية السعودية، ب، ت.
2. العراق يتراجع عالمياً وعربياً في «الأمن السيبراني»، تقرير مركز الاعلام الرقمي العراقي.
3. علي فاضل علي سليمان، حق الدفاع الشرعي على الهجمات السيبرانية، مجلة جامعة تكريت للحقوق، كلية القانون، جامعة تكريت، المجلد (4) العدد (4) الجزء (1)، السنة (4)، 2020.
4. مركز التطوير الرقمي، العراق يعتمد إجراءين لمواجهة الهجمات السيبرانية، 2022.
5. مصطفى ابراهيم سلمان، الامن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم السياسية والقانونية، جامعة ديالى، كلية القانون والعلوم السياسية، المجلد (10)، العدد (1)، 2021.
6. مقدمة في الأمن السيبراني، دورة تدريبية مقدمة من سايكو، ص8.
7. نائل عبد الرحمن صالح، واقع جرائم الحاسب في التشريع الاردني، مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الامارات العربية المتحدة، المجلد (1)، ط3، 2004.

8. نبيله هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2013.
9. هاشم شبر، تنظيم الجهد المؤسساتي والوزاري المشترك ازاء الأمن السيبراني في العراق، مركز البيان للدراسات والتخطيط، العراق، بغداد، 2022.
10. انس العزاوي، إجراءات عراقية لمواجهة الهجمات السيبرانية، موقع الحل، 2022، متاح على الرابط الالكتروني التالي https://net.7al/2022/06/11
11. انس العزاوي، إجراءات عراقية لمواجهة الهجمات السيبرانية.، موقع الحل، 2022، متاح على الرابط الالكتروني التالي https://7al.net/2022/06/11
12. ج .ةُ .ج إي تر مُبلاي، الأمن السيبراني منهج مرجعي عام، أكاديمية الدفاع الكندية، حلف الناتو، 2016.
13. خالد وليد محمود، قراءة في مؤشر الأمن السيبراني لعام 2021، مركز الجزيرة للدراسات، قطر الدوحة، 2022م، متاح على-https://www.aljazeera.net/opinions/2022/2/16
14. رغد الحسيني، الأمن السيبراني وموقعه في العراق، وكالة ارض اشور، العراق، 2023، متاح على الرابط الإلكتروني التالي https://net.ashourland
15. السعودية الثانية عالمياً في مؤشر الأمن السيبراني، وكالة العربية الحدث، متاح على الرابط الالكتروني التالي https://www.alarabiya.net/aswaq/econo-2023/06/20/my
16. صفد الشمري، الأمن السيبراني في العراق، اصول رقمية، منصة التواصل الرقمي، العراق، بغداد، 2022، متاح على الرابط الالكتروني التالي https://dcc-iq.com/?p=41841
17. صفد الشمري، الأمن السيبراني في العراق، اصول رقمية، منصة التواصل الرقمي، العراق، بغداد، 2022، متاح على الرابط الالكتروني التالي .https://7al.net/2022/06/11
18. صفد الشمري، ما واقع الأمن السيبراني في العراق؟، جريدة الصباح، 2021م، متاح على الرابط الالكتروني التالي https://iq.alsabaah.com/48007-html.

19. Ian Traynor، Russia Accused of Unleashing Cyber War to Disable Estonia، Guardian London، May 172007 ،.

لِدولةٍ فاعلةٍ ومجتمعٍ مُشارِك

www.bayancenter.org
info@bayancenter.org