الأمن السيبراني كمرتكز جديد في الاستراتيجية العراقية

م.و. صلاح مهدي هادي الشمري م.و. زيد محمد علي اسماعيل
كلية العلوم السياسية-جامعة النهرين

في ظل الاوضاع الأمنية غير المستقرة التي تشهدها منطقة الشرق الأوسط بشكل عام والعراق "بعد الاحتلال والغزو الأمريكي عام ٢٠٠٣" بشكل خاص ، كانت وما زالت ابعاد الإستراتيجية العراقية جامدة ومقتصرة على الجوانب السياسية والاقتصادية والعسكرية والأمنية ، ولم تتجاوزها في تصنيف الأحداث الأخرى المهمة لتشمل حماية أمن الدولة والمجتمع من تهديدات الثورة التكنولوجية الحديثة والمتمثلة بالأمن السيبراني . لذا كان على المخطط الإستراتيجي والأمني العراقي الاتجاه لوضع إستراتيجية لتحقيق الأمن السيبراني باعتباره خطر جديد لايمكن اغفاله إذا ما اراد الارتقاء بمستوى الاداء الإستراتيجي العراقي .

Abstract

In light of the unstable security conditions in the Middle East region in general and Iraq "after the American occupation and invasion in 2003" in particular, the dimensions of the Iraqi strategy were and still are rigid and limited to the political, economic, military and security aspects, and did not exceed them in classifying other important events to include protection of security The state and society are among the threats of the modern technological revolution, represented by cybersecurity. Therefore, the Iraqi strategic and security planner had the direction to develop a strategy to achieve cybersecurity as a new threat that could not be overlooked if he wanted to improve the Iraqi strategic performance.

This study will attempt to address the issue of cybersecurity as a new dimension in the Iraqi strategy .

الكلمات المفتاحية: الامن– السيبرانية – الاستراتيجية – الارهاب – الاختراق

المقدمة

في ظل الاوضاع الأمنية غير المستقرة التي تشهدها منطقة الشرق الأوسط بشكل عام والعراق "بعد الاحتلال والغزو الأمريكي عام ٢٠٠٣" بشكل خاص ، كانت وما زالت ابعاد الإستراتيجية العراقية جامدة ومقتصرة على الجوانب السياسية والاقتصادية والعسكرية والأمنية، ولم تتجاوزها في تصنيف الأحداث الأخرى المهمة لتشمل حماية أمن الدولة والمجتمع من تهديدات الثورة التكنولوجية الحديثة والمتمثلة بالأمن السيبراني . لذا كان على المخطط الإستراتيجي والأمني العراقي الاتجاه لوضع إستراتيجية لتحقيق الأمن السيبراني باعتباره خطر جديد لايمكن اغفاله إذا ما اراد الارتقاء بمستوى الاداء الإستراتيجي العراقي .

وتنطلق اهمية الدراسة من خلال تزايد الاهتمام العلمي بالتطور التكنولوجي للامن السيبراني من قبل الافراد والدول وتزايد خطورته على الابعاد العسكرية للقوة وبالتالي على الامن القومي للدولة في اطار مايسمى بـ " الفضاء السيبراني " .

اما اشكالية الدراسة تتمثل في تساؤل مفاده كيف يؤثر الامن السيبراني على استراتيجيات الدول ومنها العراق ، ويتفرع من هذا التساؤل تساؤلان رئيسيان هما (ماهي الاخطار والتهديدات الناجمة عن الامن السيبراني) و (هل يستطيع العراق من تحقيق الامن السيبراني كبعد جديد في إستراتيجية الأمن الوطني العراقي)

اما فرضية الدراسة فتنطلق من (ان انتقال الصراع الدولي الى الفضاء السيبراني زاد من احتمال حدوث حروب سيبرانية مما يتطلب من الدول وبالذات العراق زيادة الاهتمام بالتطور التكنولوجي وتكنولوجيا المعلومات لتحقيق الامن السيبراني للعراق) .

هذه الدراسة ستحاول التطرق إلى موضوع الأمن السيبراني كبعد جديد في الإستراتيجية العراقية ، وذلك من خلال تناول العناصر التالية :

- أولاً : مفهوم الأمن السيبراني
- ثانياً : الأمن السيبراني وانكشاف الذات "الاخطار والتهديدات"

١- الاختراق الالكتروني .

٢- الارهاب الالكتروني .

- ثالثاً : ضرورة الاستجابة لتحقيق الأمن السيبراني كبعد جديد في إستراتيجية الأمن الوطني العراقي

أولاً : مفهوم الأمن السيبراني :

تعتبر مهمة تحديد المصطلحات أول تحد يواجهه المفكرون ويتعرض له الباحثون في جميع التخصصات وشتى الدراسات ، وذلك لما تطرحه من إشكاليات تجعل من الصعوبة بمكان الاتفاق على تعريفات واضحة وشاملة وموحدة بين فرقاء المجتمع العلمي يمكن تعميمها على جميع الحقول المعرفية ، ويعد (الأمن السيبراني) واحداً من هذه المصطلحات التي تعرف تعدداً في التعريفات المقدمة لها .

فإذا كان مفهوم الأمن مفهوم واسع ، يطال جميع عمليات الدخول ، والخروج ، والبقاء ، أو التصرف ، في مكان ما ، فإنه في الفضاء السيبراني يشمل مختلف قواعد وأصول ضبط الاتصال ، وانتقال المعلومات ، وتخزينها وحفظها . كما يشمل أمن الموقع ، وأمن الأنظمة الالكترونية ، وعمليات استثمارها ، فضلاً عن أمن الاتصالات .

إن لفظة سيبار (**Cyber**) يونانية الأصل ، مشتقة من كلمة (**Kybernetes**) والتي تعني الشخص الذي يدير دفة السفينة (**Steersman**) ، وتستخدم مجازاً لتعبر عن المتحكم (**Governor**) . وقد استخدمها افلاطون من قبل للتعبير عن الحكم . وهناك من يرجع أصلها إلى منتصف القرن العشرين مع عالم الرياضيات الأمريكي (**Norbert Wiener's**) والذي استخدمها للتعبير عن التحكم الآلي .

ويعتبر (**Wiener's**) الأب الروحي المؤسس للسيبرنيتيقية (**Cybernetics**) وهو صاحب الكتاب الشهير : (**Cybernetics or control and communication in the Animal and the machine**) والذي عرف

فيه السيبرنيتيقية (Cybernetics) بأنها : (التحكم والتواصل عند الحيوان والآلة) ، كما أشار في نفس الكتاب إلى مسألة التواصل بين الإنسان والآلة ، واعتبر ان السيبرنيتيقية (Cybernetics) هي : (علم نقل الرسائل بين الإنسان والآلة ، أو بين الآلة والآلة) ، أو هي (علم القيادة أو التحكم في الأحياء والآلات ودراسة آليات التواصل في كل منهما) .

غير أنه وبعد الثورة التقنية الهائلة التي انطلقت بعد نهاية الحرب العالمية الثانية ، تغير مصطلح الآلات ليحل محله الكومبيوتر . ولذلك قام (وليام جيبسون William Gibson) في رواياته عن المستقبل باستخدام كلمة (الفضاء الإلكتروني) ، وأصبحت كلمة سايبر توضع أمام أي شيء وكل شيء مرتبط بشبكة الإنترنت .

وهذا يعني أن مصطلح سيبار أو الفضاء الإلكتروني وفي كثير من المراجع ، ظهر مع ظهور الإنترنت وتعميم استخدام الرقمنة ، موازاة مع كم هائل من المصطلحات مثل : (الفضاء الرقمي ، الدفاع الإلكتروني ، الهجوم الإلكتروني ، الجريمة الإلكترونية) وغيرها ، في حين ان الأمن السيبراني أو الإلكتروني ظهر حديثاً وهو يعني مجمل القوانين السياسية ، الأدوات ، النصوص ، المفاهيم وميكانيزمات الأمن وطرق تسيير الأخطار والممارسات التكنولوجية المتعلقة بتكنولوجيا المعلومات والاتصالات المستخدمة لحماية الدول والمنظمات والأشخاص . كما يعرف على انه الحالة المرغوب فيها لعمل أنظمة المعلومات والاتصالات والتي تمنحها القدرة على المقاومة والتصدي لكل ما ينجم عن الفضاء السيبراني ، والذي من شأنه أن يعرض المعلومات المخزنة أو المعالجة أو المنقولة للتلف أو التغيير أو التجسس .

قدمت وزارة الدفاع الأمريكية "البنتاغون" تعريفاً دقيقاً لمصطلح (الأمن السيبراني) ، إذ اعتبرته على انه : (جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع اشكالها الالكترونية والمادية من مختلف الجرائم ، والهجمات ، والتخريب ، والتجسس ، والحوادث) .

في حين اعتبر الإعلان الأوروبي (الأمن السيبراني) بأنه يعني : (قدرة النظام المعلوماتي على مقاومة محاولات الاختراق أو الحوادث غير المتوقعة ، التي تستهدف البيانات) .

وهذا ما ذهب إليه الكاتبان (Martti Lehto, Pekka Neittaanmaki) في كتابهما الموسوم : (Cyber Security: Analytics, Technology and Automation) إذ اعتبرا أن الأمن السيبراني عبارة عن : (مجموعة من الإجراءات التي تتخذ في الدفاع ضد الهجمات الإلكترونية "قراصنة الكومبيوتر" وعواقبها وتنفيذ التدابير المضادة المطلوبة) .

وهذا ما أكده (Richard A. Kemmerer) أستاذ الاتصالات في جامعة كاليفورينا ، الذي عرفه : (عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة) ، بينما عرفه (Edward Amoroso) بأنه : (وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات ، وتشمل تلك الوسائل والأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها ، وتوفير الاتصالات المشفرة) .(١)

وبحسب التعريف المعطى له في التقرير الصادر عن "الاتحاد الدولي للاتصالات" حول (اتجاهات الاصلاح في الاتصالات للعام ٢٠١٠ ٢٠١١) ، يعرف الأمن السيبراني على أنه : (عبارة عن مجموعة الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به ، وسوء الاستغلال ، واستعادة المعلومات الإلكترونية ، ونظم الاتصالات والمعلومات التي تحتويها ، وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات ، وتعزيز حماية وسرية وخصوصية البيانات الشخصية ، واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني) .(٢)

تأسيساً عليه ، يمكن تعريف الأمن السيبراني ، انطلاقاً من أهدافه ، بانه : (النشاط الذي يؤمن حماية الموارد البشرية ، والمالية ، المرتبطة بتقنيات الاتصالات والمعلومات ، ويضمن امكانات الحد من الخسائر والاضرار ، التي تترتب في حال تحقق المخاطر والتهديدات ، كما

يتيح اعادة الوضع إلى ما كان عليه ، باسرع وقت ممكن ، بحيث لا تتوقف عجلة الانتاج ، وبحيث ، لا تتحول الاضرار إلى خسائر دائمة) .(٣)

ثانياً : الأمن السيبراني وانكشاف الذات "الاخطار والتهديدات"

في البداية يمكن القول ، أن تهديدات الأمن السيبراني يمكن اعتبارها "تحديات غير مرئية" تؤثر على منظومة الأمن الوطني العراقي . فالتطور التكنولوجي الذي شهده العراق في مجال الاتصالات والمعلومات بعد عام ٢٠١٣م الذي تزامن مع ضعف الأمننة الإلكترونية في البنية التحتية الوطنية سواء أكانت (أمنية ، مصرفية ، شخصية) أدى إلى أن يصبح العراق منكشفاً إستراتيجياً لكثير من دول العالم ، لاختراقه والتجسس على المعلومات الخاصة بالمؤسسات كافة، واستخدام العراق كساحة لشن الهجمات الإلكترونية لضرب أمن معلومات أي دولة كانت واختراقه ، فضلاً عن استراق أي معلومة واستخدامها لأغراض المساومة ، وتنفيذ عمليات إرهابية . ومن الملاحظ أن أكثر المؤسسات العراقية تتعاقد لتجهيز معلوماتها من أقمار صناعية ذات مورد خدمة واقع خارج الحدود العراقية الذي يؤدي إلى مرور تلك المعلومات في خوادم تلك الدول ، ورجوعها إلى العراق ، إذ يشكل هذا الإجراء خرقاً لأمن المعلومات العراقي .(٤) وتتمثل أبرز هذه الاخطار والتهديدات بما يأتي :

١- الاختراق الالكتروني :

تفتقد كثير من مؤسسات الدولة العراقية إلى (الوعي الأمني السيبراني) ، إذ لاتمتلك تلك المؤسسات على مختلف توجهاتها منظومات أو برامج أو تقنيات تجنبها الاختراق فتكون عرضة لسرقة معلوماتها وبياناتها ، أو إلحاق الضرر المادي في بناها التحتية ، أو تهديد أمنها .

يعرف (الاختراق الإلكتروني) على أنه : (هجمات تستهدف شبكات الحاسوب ، فضلاً عن الشبكة الدولية للمعلومات "INTERNET" بمختلف انواعها واستخداماتها ، الهدف منه تعريض الأمن القومي لدولة ما أو مجموعة دول للخطر) .

إن الهدف من الاختراق هو الحصول على بيانات أو معلومات خاصة عن مؤسسة معينة أو فرد معين ، إذ يعمد المخترق إلى التعرف على الخدمات الخاصة بشبكة المواطن ، ومواطن الضعف والخلل في الأجهزة الملحقة كالحاسبات أو الهواتف النقالة الخاصة بالمواطن من خلال بوابات المعلومات والعبور الخاصة بالشبكة المحلية .

ويعد (التنصت الإلكتروني) من أهم أنواع الاختراق من حيث التنصت على المكالمات الخاصة ، إذ يتم من خلال برامج معدة لذلك الهدف .

وللاختراق الإلكتروني دوافع عدة ، أهمها : (٥)

- دوافع سياسية وعسكرية : إن الحروب المستمرة والتطورات السياسية والعسكرية المتزامنة مع التطورات التي شهدها قطاع الاتصالات والمعلوماتية في ظل الاحتياج المستمر والمتزايد لتكنولوجيا الاتصالات والمعلومات لتلبية المتطلبات العسكرية للدول المتقدمة دعت إلى الاعتماد على هذه التكنولوجيا بصورة مفصلية ، إذ أصبح موضوع التجسس واستراق المعلومات عن طريق الاختراق يمثل ضرورة عسكرية بين الدول المتقدمة . فعلى سبيل المثال في عام ٢٠٠١م تم اختراق مناطق صناعتية عسكرية كثيرة في (إيران) ، إذ تعتبر هذه المناطق الصناعية هي الأكثر حساسية ، من ضمنها اختراق (فايروس ستيكسنيت **STUXNE**) لأجهزة كمبيوترات خاصة بمعامل ومصانع تخصيب اليورانيوم ، إذ أشارت إيران إلى الولايات المتحدة الأمريكية و"إسرائيل" في تلك الواقعة الإلكترونية التي غيرت مفهوم الأمن التقليدي ، المرتبط بالتهديدات التقليدية ك (تهديد حدود الدولة) .(٦) وعلى صعيد (العراق) ، وتحديداً في ٢٠١٦/٩/٢٨م ، تعرض موقع "مستشارية الأمن الوطني" للاختراق الإلكتروني ، إذ نشر المخترقون صورة "كاريكاتورية" لمستشار الأمن الوطني "فالح الفياض" ، مع كتابة عبارة في الموقع : (ان موقعكم لم تقوموا بحمايته فكيف تحافظون

على أمن الشعب) . ويقدم الجدول رقم (١) اختراق المواقع الإلكترونية لـوزارت عراقية عدة بين عامي ٢٠١٦م ، ومطلع عام ٢٠١٧م .

ت	أسم الوزارة	تاريخ الاختراق
١-	موقع رئيس الوزراء العراقي	٢٠١٦/٣/٢٣م
٢-	موقع مجلس النواب العراقي	٢٠١٦/٦/٨م
٣-	وزارة الداخلية	٢٠١٦/٧/٣م
٤-	اختراق موقع الاستمارة الإلكترونية للتعيين على ملاك وزارة الصحة	٢٠١٦/٨/٢٢م
٥-	وزارة الاتصالات	٢٠١٦/١٠/١١م
٦-	وزارة الشباب والرياضة	٢٠١٧/٦/٢م
	الموقع الرسمي للمفوضية العليا المستقلة للانتخابات	٢/١٢ و ٢٠١٧/٢/١٣م

- دوافع اقتصادية : نتيجة للمنافسة التجارية الكبيرة الحاصلة بين الشركات العالمية أصبحت عملية الاختراق مهمة لكثير من تلك الشركات ، لغرض الاطلاع على معلومات الشركات المتنافسة لتحقيق أرباح تجارية فضلاً عن محاولة الدول ضرب اقتصاديات الدول الأخرى من خلال الاطلاع على معلومات تخص تلك الاقتصاديات وآليات نموها لغرض الحد منها .
- دوافع فردية : إن محاولات الاختراق على المستوى الفردي تبدأ بين الأفراد ، بداعي التباهي بالنجاح في اختراق أجهزة زملائهم الآخرين بدافع التحدي ، لكن هذه الحالة تحولت فيما بعد إلى هواية عند بعض الأفراد ، إذ شكل بعضهم منتديات لتعليم الاختراق ، وقد ظهرت هذه المشكلة جلية بعد إقالة المبرمجين من بعض الشركات المعروفة الذين صبوا جام غضبهم على تلك الشركات لغرض النيل والثأر من شركاتهم التي أقالتهم .

٢- الارهاب الالكتروني :

كانت بداية استخدام مصطلح الإرهاب الإلكتروني (Cyber terrorism) في الثمانينات من القرن العشرين على يد (باري كولين Barry Collin) والتي خلص فيها إلى صعوبة وضع تعريف شامل للإرهاب التكنولوجي . ولكنه تبنى تعريفاً للإرهاب الإلكتروني بأنه : (هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها سعياً لتحقيق أهداف سياسية أو دينية أو أيديولوجية ، وأن الهجمة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب) . ويعرفه (جيمس لويس James Lewiss) على أنه : (استخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البنى التحتية الوطنية المهمة كالطاقة والنقل والعمليات الحكومية ، أو بهدف ترهيب حكومة ما أو مدنيين) .

أما (دورثي دينينغ Dorothy Denning) فترى أن الإرهاب الإلكتروني هو : (الهجوم القائم على مهاجمة الحاسوب ، وأن التهديد به يهدف إلى الترويع أو إجبار الحكومات أو المجتمعات لتحقيق أهداف سياسية أو دينية أو عقائدية وينبغي أن يكون الهجوم مدمراً وتخريبياً ، لتوليد الخوف بحيث يكون مشابه للأفعال المادية للإرهاب) .

ووفقاً لوزارة الدفاع الأمريكية "البنتاغون" فإنها تعرف الإرهاب الألكتروني بأنه : (عمل إجرامي يتم الإعداد له باستخدام الحاسبات ووسائل الاتصالات ينتج عنها عنف وتدمير أو بث الخوف تجاه تلقي الخدمات بما يسبب الارتباك وعدم اليقين وذلك بهدف التأثير على الحكومة أو أو السكان لكي تمتثل لأجندة سياسية أو اجتماعية أو فكرية معينة) . وتبعاً لأحدى وثائق (حلف شمال الأطلسي NATO) فقد تم تعريف الإرهاب الإلكتروني على أنه : (هجوم بواسطة الإنترنت عن طريق استخدام ، أو استغلال شبكات الكومبيوتر أو الاتصالات مما يسبب دماراً من شأنه توليد خوف وترويع المجتمع، وفقاً لهدف أيديولوجي).

كما عرفه الدكتور (عادل عبد الصادق) على أنه يعني: (العدوان أو التخويف أو التهديد مادياً أو معنوياً باستخدام الوسائل الإلكترونية، الصادرة من الدول أو الجماعات، أو الأفراد عبر الفضاء الإلكتروني، أو أن يكون هدفاً لذلك العدوان بما يؤثر على الاستخدام السلمي له).

أما تعريفه إجرائياً فأنه يعني : (نشاط أو هجوم متعمد ذو دوافع سياسية بغرض التأثير على القرارات الحكومية أو الرأي العام باستخدام الفضاء الإلكتروني كعامل مساعد ووسيط في عملية التنفيذ للعمل الإرهابي أو الحرب من خلال هجمات مباشرة بالقوة المسلحة على مقدرات البنية التحتية للمعلومات ، أو من خلال ما يعد تأثيراً معنوياً ونفسياً من خلال التحريض على بث الكراهية الدينية وحرب الأفكار ، أو يتم في صورة رقمية من خلال استخدام آليات الأسلحة الإلكترونية الجديدة في معارك تدور رحاها في الفضاء الإلكتروني والتي قد يقتصر تأثيرها على بعدها الرقمي ، أو قد تتعدى أهداف مادية تتعلق بالبنية التحتية الحيوية) .(٧)

تحاول الجماعات الإرهابية الاستفادة من تكنولوجيا الإنترنت ، إذ يعتبر العديد منهم الفضاء الإلكتروني وسيلة للاتصال وتبادل المعلومات . فعلى سبيل المثال ، "تنظيم القاعدة" نادراً ما استخدم الإنترنت خلال سنوات تكوينه في تسعينات القرن العشرين . وكانت الرسائل التهديدية لـ(إسامة بن لادن) زعيم التنظيم تنتشر عن طريق تسجيلات صوتية أو شرائط فديو فيما بعد. ولكن مع مطلع القرن الحادي والعشرين، وبعد وقوع أحداث ١١ أيلول عام ٢٠٠١م، أفقدت العمليات العسكرية للجيش الأمريكي في أفغانستان تنظيم القاعدة ملاذاته الآمنة للتدريب البدني والتنظيم ، مما دفعه للتركيز على استخدام التكنولوجيا السيبرانية.

وهو الامر الذي أفرز تنظيماً يتبنى فكر (القرون الوسطى) ويحتضن تكنولوجيا (القرن الحادي والعشرين). ولكن لم تستخدم القاعدة الفضاء الإلكتروني للقيام بعمليات إرهابية سيبرانية، بل لتمرير المعلومات ، والوصول إلى العالم الأوسع بشكل لم يحدث من قبل لمثل هذه

المجموعة الصغيرة ، وكذلك لنقل رسائل (بن لادن) وغيره من قادة القاعدة إلى الملايين حول العالم .(٨)

وعلى صعيد تنظيم "داعش" الإرهابي فله ما يزيد عن (٥٠) ألف موقع إلكتروني ، و(٩٠) ألف صفحة باللغة العربية على مواقع التواصل الاجتماعي "فيس بوك" ، و (٤٠) ألفاً بلغات أخرى، وهذا ما ساهم في تجنيده حوالي (٣٤٠٠)(*) شاب شهرياً عبر حملاته الإلكترونية .(٩)

لقد استغل (تنظيم الدولة "داعش") الإرهابي الإنترنت في بث عمليات الإعدام التي كان يقوم بتنفيذها في الأسرى ، وذلك لبث الرعب والفزع في نفوس أهالي المدن التي كان يرغب في السيطرة عليها وهو ما تحقق جزئياً في هروب واستسلام مدن وقرى لتنظيم "داعش" الإرهابي خوفاً من تعرضهم لمصير من قبلهم ، كذلك استغل التنظيم في تجنيد العديد من الشباب حول العالم ، إذ بلغ عدد البلدان التي انضم منها أفراد إلى تنظيم الدولة "داعش" إلى (٧٠) دولة .

لقد سمحت ثورة الإنترنت الجماعات الإرهابية بإخفاء عملياتها بطرق جديدة ، أكثر تعقيداً عن سابقتها التقليدية . فالجماعات الإرهابية أصبحت تدرك أهمية الإنترنت من خلال ما يوفره من خدمات موثوق بها ، وشروط ميسرة ، وهويات افتراضية . فعلى سبيل المثال كانت "طالبان" تدير موقعاً دعائياً لعملياتها العسكرية وتفجيراتها الانتحارية ضد القوات الأمريكية في أفغانستان ، لأكثر من عام ، مع العلم بأن هذا الموقع الإلكتروني كان مملوكاً لشركة أمريكية في "تكساس"، إذ كانت تؤجر المواقع الإلكترونية بمبلغ (٧٠) دولار في الشهر ، تدفع بواسطة بطاقة الائتمان ، وكانت تتعامل مع نحو (١٦ مليون) حساب مستخدم .

كما استطاعت الجماعات الإرهابية استخدام الإنترنت في التواصل مع بعضها البعض عبر القارات ، والذي كان يستغرق شهوراً في الماضي ، هذا من جانب ، كما استطاعت الجماعات من جانب آخر تبادل المعارف بطرق جديدة ومبتكرة وهو ما يسميه خبراء الأمن (**TTPS**)، وهو اختصار لـ(تكتيكات وتقنيات وإجراءات) . فوصفات المتفجرات متوفرة بسهولة على

شبكة الإنترنت ، وكذلك طرق تجهيز "العبوات الناسفة" التي كان يتم استخدامها في مناطق الصراع من العراق إلى أفغانستان . وبذلك يكون الإنترنت قد وفر لهذه الجماعات مساحات افتراضية للتدريب بعيداً عن خطر قصف الطائرات بدون طيار .

كما وفر الإنترنت للجماعات الإرهابية مصدراً منخفض التكلفة لجمع المعلومات الإستخباراتية حول أهدافهم . فعلى سبيل المثال ، مكنت تقنية (Google Earth) جماعة (لشكر طيبة LASHKAR –E- TIBA) الباكستانية الإرهابية من التخطيط لهجمات "مومباي" عام ٢٠٠٨م . وكذلك في عام ٢٠٠٧م عندما قام مجموعة من الجنود الأمريكيين بالتقاط صور تذكارية في قاعدة عسكرية في العراق ، وكانت خلفهم مجموعة من طائرات الهليكوبتر ، ثم قاموا بتحميلها على الإنترنت ، ولم تكن الصور لتوضح نوعية الطائرات أو أي معلومات مفيدة للجماعات الإرهابية ، ولكن استطاعت بعض الجماعات الإرهابية استغلال (العلامات الجغرافية Geotags) التي حوتها الصور ، لتتمكن من تحديد موقع القاعدة العسكرية ، وتدمير أربعة من طائرات الهليكوبتر في هجوم بقذائف الهاون .

إن معالجة قضايا الأمن السيبراني على مستوى العالم يحتاج إلى عمل وتعاون جماعي ودولي . ورغم الإقرار بصعوبة تحقيق مثل هذا التعاون ، فإن الرغبة في حماية المصالح الخاصة ، وامتلاك قدرٍ من الثقة فيما بين الحكومات ، قد يمهد لتعاون دولي يعمل على تحجيم التهديدات السيبرانية المستقبلية .(١٠)

ثالثاً : ضرورة الاستجابة لتحقيق الأمن السيبراني كبعد جديد في إستراتيجية الأمن الوطني العراقي

ابتداءاً ، لابد لنا من القول ، إن مفهوم الاستجابة في أبسط صورها يمكن تعريفها على أنها : (قدرة الدولة على مواجهة التحديات والعقبات التي تفرزها البيئة الداخلية أو الخارجية ، تلك القدرة تكون مقرونة بفعل إستراتيجي مع إمكانيات مملوكة ، التي تساعد على إتمام الهدف تلافياً لأية فجوة إستراتيجية بهذا الخصوص) .(١١)

يقتضي وضع وتنفيذ خطة وطنية للأمن السيبراني وجود إستراتيجية شاملة تشمل استعراضاً عاماً أولياً لمدى كفاية الممارسات الوطنية الحالية والنظر في دور جميع اصحاب المصلحة (الهيئات الحكومية ، القطاع الخاص ، والمواطنين) في هذه العملية .

ولأسباب تتعلق بالأمن القومي والرفاه الاقتصادي ، تحتاج الحكومة إلى المساعدة في عملية حماية البنية التحتية لمعلوماتها الحيوية ، وتعزيز هذه الحماية وضمانها لايمكن الوصول إليه الا من خلال وجود إستراتيجية وطنية تعنى بالأمن السيبراني .(١٢)

إن إستراتيجية الأمن الوطني السيبراني بشكل عام هي : (كافة التدابير المتعلقة بسرية المعلومات والبيانات التي يتم معالجتها وتخزينها وإبلاغها عن طريق وسائل إلكترونية أو مشابهة، وحمايتها والنظم المرتبطة بها من التهديدات الخارجية أو الداخلية) . وتهدف هذه الإستراتيجية إلى تطوير وتنفيذ قدرات الأمن السيبراني لتحسين والحفاظ على المجالات الآتية : (١٣)

- حماية خصوصية المواطن وغير ذلك من البيانات من الضياع ، والتغييرات الضارة ، والاستخدام غير المصرح به .
- مرونة الخدمات الحكومية والنظم والبنية التحتية للتهديدات الإلكترونية .
- استمرارية الحكومة أثناء وبعد الحوادث السيبرانية الخطيرة .
- حماية أمن الخدمات الرقمية للمواطنين .
- تنسيق الاستجابة للتهديدات ضد البنية التحتية .
- أمن وسلامة البنية التحتية الأساسية للحكومة .

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

وقبل التطرق إلى ضرورة الاستجابة الملحة لوضع إستراتيجية وطنية شاملة للأمن السيبراني العراقي ، لابد من توضيح الترتيب العالمي للعراق وفقاً لنشرة الاتحاد الدولي للاتصالات ITU للأمن السيبراني لعام ٢٠١٧م ، إذ احتل العراق المرتبة (١٥٩) ، (عالمياً) في مستوى التأهب في مجال الأمن السيبراني . أما على (المستوى العربي) فقد احتل المرتبة (١٩) حسب التزامه بالتدابير التي يحددها الرقم القياسي العالمي للأمن السيبراني ، كما تشير البيانات في الجدول ادناه .

الدولة	الترتيب عربياً	الترتيب عالمياً
سلطنة عُمان	١	٤
مصر	٢	١٤
قطر	٣	٢٥
تونس	٤	٤٠
السعودية	٥	٤٦
الإمارات	٦	٤٧
المغرب	٧	٤٩
البحرين	٨	٦٥
الجزائر	٩	٦٨
الأردن	١٠	٩٣
السودان	١١	٩٦
سوريا	١٢	١٠٢
فلسطين	١٣	١٠٤
ليبيا	١٤	١٠٥
لبنان	١٥	١١٩

موريتانيا	١٦	١٢٥
الكويت	١٧	١٣٩
جيبوتي	١٨	١٤٠
العراق	١٩	١٥٩
جزر القمر	٢٠	١٦١
الصومال	٢١	١٦٢
اليمن	٢٢	١٦٤

الجدول من اعداد الباحث اعتماداً على المصدر الآتي : تصنيف الدول العربية في مجال الأمن السيبراني لعام ٢٠١٧ ، الشبكة الدولية للمعلومات (الانترنت) على الموقع : **https://www.3arabinsider.com**

وبالنظر إلى الجدول أعلاه ، يمكن القول ان جهود العراق في مجال تحقيق الأمن السيبراني تبقى ضئيلة ، إذ ينبغي على الأطراف المعنية من الجهات والمؤسسات الحكومية مثل : (وزارة الدفاع ، وزارة الداخلية ، وزارة الاتصالات ، وزارة التعليم العالي والبحث العلمي ، جهاز المخابرات الوطني العراقي ، مستشارية الأمن الوطني) وغيرها من المؤسسات ، أن تكون عالية الدراية والتخطيط والاطلاع وفق منظومة العمل الجمعي التواصلي مع الوزارات العراقية المختصة ناهيك حتى عن اللجان البرلمانية الأمنية والعمل على تكثيف الجهود والتعاون معاً للحيولة دون تمكين المغرضين من تحقيق أهدافهم وللحفاظ على سلامة أفراد المجتمع وشبكات البنية التحتية في المؤسسات وتدعيمها بكل وسائل الأمن والحماية ، لأن عملهم هو الأمن الشامل للعراق .(١٤)

إن أبرز الأهداف والوسائل والإجراءات التي يجب أن تتضمنها إستراتيجية الأمن الوطني السيبراني العراقي عند صياغتها وتشكيلها ، هي : (١٥)

أولاً : حماية البنية التحتية للمعلومات الحيوية الوطنية / ولتحقيق هذا الهدف ينبغي العمل على :

١- تقييم المخاطر التي تواجهها البنية التحتية للمعلومات الحيوية ، وتتضمن :

- وضع إطار زمني لإدارة المخاطر على البنية التحتية للمعلومات الحيوية وتقييم التهديدات ونقاط الضعف والعواقب وتطوير ملفات المخاطر .
- إجراء تقييمات منتظمة للمخاطر التي تواجه وزارت الدولة ، فضلاً عن مؤسسات القطاعات الحيوية فيما يتعلق بالبنية التحتية للمعلومات الحيوية .
- إجراء تقييمات حول مدى الترابط والاعتماد المتبادل بين مؤسسات الدولة لتحديد المخاطر المنهجية التي تواجهها .

٢- تنفيذ ضوابط ومعايير الأمن السيبراني للحد من المخاطر على البنية التحتية للمعلومات الحيوية ، وتتضمن :

- وضع نموذج ومعايير خاصة بالأمن السيبراني للبنية التحتية للمعلومات الحيوية ، يتضمن ضوابط محددة للأمن السيبراني .
- إجراء عمليات تقييم وتدقيق منتظمة لوزارت الدولة والمؤسسات الحيوية ، وذلك لقياس وتقييم فعالية برامج وضوابط الأمن السيبراني .
- وضع إستراتيجيات إدارة المخاطر لحماية الخدمات والأنظمة والمؤسسات الأكثر حيوية ، ومتابعة تنفيذ تلك الإستراتيجيات .
- تبادل المعلومات حول المخاطر وإستراتيجيات إدارة المخاطر بين مختلف قطاعات الدولة ، لتحديد أولويات إجراءات التخفيف من حدة تلك المخاطر واستثمار الموارد المتاحة .

٣- تحليل اتجاهات الأمن السيبراني والمخاطر التي تهدد البنية التحتية للمعلومات ، وتقديم التقارير للأطراف المعنية في الوقت المناسب . أي العمل على إنشاء مراكز عمليات أمنية خاصة بقطاعات أو مؤسسات بعينها أو مراكز معلومات للكشف عن التهديدات .

إن وجود مراكز تعنى بأمن المعلومات العراقي وإدارة الحوادث ومعالجتها والسيطرة على جرائم المعلوماتية أمر مهم جداً وضروري في ظل ما يتعرض له العراق من هجمات إرهابية

متمثلة بتنظيمات متطرفة تعتمد اعتماداً رئيساً على تناقل المعلومات والبيانات عبر الشبكات وعبر الفضاء السيبراني ، إن سيطرة الحكومة العراقية من خلال إنشاء هذه المراكز سيقلل من الجرائم الإرهابية بنسبة كبيرة جداً تصل إلى أكثر من (٧٠%) ويساهم بتقليل نفقات الجهود العسكرية والخسائر البشرية نتيجة المواجهة المباشرة مع العدو ، إن هذه المراكز تحتاج إلى إرادة سياسية وقرار شجاع من قبل صُناع القرار ، ويجب أن ترتبط هذه المراكز بجهة محددة ومستقلة وغير خاضعة للضغوطات السياسية لغرض ضمان انسيابية العمل ، ويكون ذلك من خلال تشريع قانون يتضمن الجوانب التنظيمية والفنية والإدارية والمالية كافة لإنشاء هذه المراكز ، ومن الجدير بالذكر أن ننوه أيضاً إلى ضرورة اختيار المورد البشري الكفوء والمدرب تدريباً عالمياً والموثوق من الناحية الأمنية ، واتخاذ أعلى درجات الحيطة والحذر في اختيار العاملين في هذه المراكز ، لأن أي خرق من الممكن أن يشكل كارثة على أمن الدولة وخسائر كبيرة لا تُحمد عقباها .(١٦)

٤- تعزيز استخدام المنتجات والخدمات التكنولوجية الموثوق بها ، من خلال : (١٧)

- وضع مبادئ توجيهية لتحديد المتطلبات الأمنية لمزودي خدمات تكنولوجيا المعلومات والاتصالات والأمن السيبراني .

٥- المراقبة المستمرة لأمن البنية التحتية للمعلومات الحيوية : أي وضع آلية لإجراء عمليات تشخيص ومراقبة مستمرة للشبكات من أجل تشكيل وعي أكبر بالمخاطر وتعزيز الإجراءات الوقائية والكشف عن الأجهزة المتضررة ومعالجتها .

ثانياً : الاستجابة للحوادث والهجمات الإلكترونية وحلها والتعافي منها ، من خلال تداول المعلومات في الوقت المناسب والتعاون واتخاذ الإجراءات اللازمة / ولتحقيق ذلك ينبغي القيام بما يلي :

١- تعزيز إمكانيات الإلمام والتحديث لوضع الأمن السيبراني .

٢- بناء قدرات الاستجابة للهجمات الإلكترونية وتحسينها باستمرار ، من خلال :

- وضع آلية للتنسيق وإدارة التعامل مع الحوادث الإلكترونية .
- إنشاء شبكة لتبادل المعلومات بين مراكز عمليات الأمن السيبراني ، وذلك لتيسير التعامل مع الحوادث وتبادل المعلومات وتوفير فرص التدريب .

٣- الحد من إمكانية تعرض البنية التحتية للمعلومات الحيوية لهجمات إلكترونية .

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

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

ثالثاً : وضع الإطار القانوني والتنظيمي لتعزيز سلامة وحيوية الفضاء الإلكتروني / ولتحقيق هذا الهدف ، ينبغي العمل على :

١- تعزيز قدرات العراق على مكافحة الجريمة الإلكترونية . ولتحقيق هذا الهدف ينبغي القيام ب

- تطوير قدرات جديدة للتحقيق في الأنشطة الإجرامية من خلال التدريب وتقنيات الأدلة الجنائية الحديثة واستخدام التكنولوجيا .
- سن قانون مكافحة الجريمة الإلكترونية لمنح القائمين على إنفاذ القانون سلطات جديدة ولتحديد الأفعال الإجرامية .
- جمع الإحصائيات المتعلقة باتجاهات الجرائم الإلكترونية وطرق ارتكابها .

٢- وضع وتنفيذ القوانين واللوائح والسياسات الوطنية للتعامل مع قضايا الأمن السيبراني والجريمة الإلكترونية .

٣- مراقبة وتعزيز الالتزام بالقوانين واللوائح والسياسات المتعلقة بالأمن السيبراني والجريمة الإلكترونية .

٤- بناء شراكات دولية متينة والحفاظ عليها لوضع معايير وقواعد الأمن السيبراني . ولتحقيق ذلك ينبغي القيام بإجراءات عدة أهمها :

- التعاون مع الشركاء الدوليين بشكل منتظم بشأن السياسات والعمليات التشغيلية لزيادة الوعي بالأمن السيبراني ، وتحديد التهديدات والتعامل معها ، وتنسيق الإجراءات الهادفة لتعزيز الأمن السيبراني في جميع أنحاء العالم .
- إبرام اتفاقيات ثنائية ومتعددة الأطراف لحث الجهات المختلفة على تبادل المعلومات حول قضايا الأمن السيبراني والإرتقاء بالتحقيقات الجنائية .

رابعاً : تعزيز ثقافة الأمن السيبراني التي من شأنها دعم الاستخدام الأمن والمناسب للفضاء الإلكتروني / من خلال : (١٨)

١- تعزيز وعي المجتمع بالأمن السيبراني باستخدام وسائل وقنوات متعددة . ولتحقيق هذا الهدف ينبغي القيام بعدد من الإجراءات هي :

- تعزيز الوعي الوطني بالأمن السيبراني والحفاظ عليه لدى مختلف فئات المجتمع (الأطفال ، الطلبة وأولياء الأمور ، وكبار السن ، وموظفي الحكومة) ، وغيرهم .
- إنشاء برامج للمنح والمكافآت ، وذلك لتكريم التميز في مجال الأمن السيبراني بتقديم إسهامات رئيسة في هذا المجال ، مثل تقديم الحلول أو الخدمات المبتكرة أو تنفيذ ضوابط الأمن السيبراني وإتباع أفضل الممارسات .

٢- تشجيع الأفراد على استخدام أدوات وحلول السلامة على الإنترنت للوقاية من الهجمات الإلكترونية .

٣- تطوير مناهج تثقيفية حول الأمن السيبراني وإتاحتها في المدارس والكليات والجامعات. إجراءات تحقيق هذا الهدف تتمثل بـ :

- العمل مع الجامعات والكليات على تطوير وتنفيذ مناهج وبرامج تثقيفية تتناول الأمن السيبراني على مستوى التعليم العالي والدراسات العليا .

- العمل مع المدارس على وضع برامج تعليمية حول السلامة على الإنترنت ، وتزويد المدرسين والإداريين بالمواد التي تدعمهم في تنفيذ مهمتهم .

إن الحفاظ على بيئة آمنة للأنشطة على الإنترنت أمر ضروري لتعزيز الثقة الرقمية ولتشجيع اقتصاد مزدهر عبر الإنترنت ، يجب أن يثق الأفراد ، بأن تعاملاتهم آمنة وأن معلوماتهم الشخصية في أمان . ويعد تعزيز الوعي والتشجيع على تبادل المعلومات بين الجهات الحكومية والشركات والمؤسسات من أهم الوسائل الفعالة في تحسين الأمن السيبراني . فضلاً عن ذلك ، يجب أن تقوم المؤسسات بجمع المعلومات الشخصية واستخدامها وحمايتها بصورة مناسبة ، الأمر الذي سيمكن المستخدمين من حماية أنفسهم ضد سرقة هوياتهم .

خامساً : تطوير وصقل الإمكانيات الوطنية للأمن السيبراني / من خلال :

١- تطوير قوى عاملة مهنية في مجال الأمن السيبراني والحفاظ عليها . ولتحقيق هذا الهدف ينبغي العمل على :

- تطوير نموذج كفاءة القوى العاملة في مجال الأمن السيبراني .
- تنظيم مسابقات في مجال الأمن السيبراني على الصعيدين المحلي والوطني لمختلف الفئات العمرية لاختيار أفضل المهارات القطرية وصقل مهاراتهم وتشجيعهم على متابعة مسيرتهم في مجال الأمن السيبراني .

٢- تعزيز فرص تأسيس الشركات ، وتنافسية كل من القطاعين (العام ، الخاص) في مجال الأمن السيبراني .

٣- الاستثمار في الأبحاث الرامية إلى تطوير وتسويق التقنيات والحلول المبتكرة في مجال الأمن السيبراني . ولتحقيق هذا الهدف ينبغي العمل على :

- وضع خطة عمل وطنية لإجراء الأبحاث وإحداث تطوير في مجال الأمن السيبراني ، وذلك لتعزيز الاستثمار في الحلول التي يمكن تحويلها بسرعة من مرحلة التطوير إلى مرحلة التنفيذ .
- تأسيس شراكات إستراتيجية مع الجامعات والمعاهد والمؤسسات البحثية داخل دولة قطر وفي الخارج فيما يتعلق بمشاريع الأبحاث والتطوير في مجال الفضاء الإلكتروني .

سادساً : تنمية الوعي بالمخاطر السيبرانية والحلول المتاحة / يقتضي تناول القضايا التقنية تكاتف الحكومة وقطاع الأعمال التجارية والمجتمع المدني والأفراد المستخدمين في العمل معاً ، لوضع التدابير التي تدمج بين المعايير واللوائح وتنفيذها .

فضلاً عن تواصل المعنيين بالحكومة مع أدوات التكنولوجيا العالمية ، لمعالجة مختلف احتياجات الأمن السيبراني إذ يوجد عدد من المنظمات ولجان الدراسات بما في ذلك لجنة الدراسات ١٧ لقطاع تقييس الاتصالات وغيرها من المؤسسات العالمية .

أخيراً يمكن القول ، يجب أن يقتنع صانع القرار العراقي بضرورة وجود إستراتيجية وطنية للأمن السيبراني كهدف للتصدي للأخطار ومواطن الضعف في البنية التحتية السيبرانية . هذه الأهداف تشكل مجتمعة الركيزة الأساسية للحماية من الهجمات الإلكترونية والاستعداد لمواجهتها واكتشافها والتعافي منها ، ولا شك أن لكل دولة خصوصيتها ، ولا يصح القول إن هناك إستراتيجية واحدة صالحة لجميع الدول ، فنقاط القوة والضعف تختلف من دولة إلى أخرى ، كذلك الفرص والتهديدات التي تواجهها .

الخاتمة

من هنا يمكن القول ، ان مسألة تحقيق الأمن السيبراني العراقي يعد أحد من أهم التحديات التي تواجه صانع الإستراتيجية العراقية في ظل التطورات التكنولوجية الحديثة والمتسارعة . وعلى الرغم من الجهود المبذولة في وقف الهجمات السيبرانية الإرهابية إلا أن العراق احتل عام

٢٠١٧م الترتيب (١٩) عربياً و (١٥٩) عالمياً وهو ما يشير إلى الحاجة لتعزيز الامكانيات وبذل المزيد من الجهود وتحسين القدرات في مجال مكافحة الهجمات والجريمة الإلكترونية وغيرها من التهديدات التي يمثل الانتصار عليها بمثابة نجاعة للإستراتيجية السيبرانية العراقية .

الهوامش

(١) د. بن مرزوق عنترة ، أ. حرشاوي محي الدين ، الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية ، ص٦٦ ، الشبكة الدولية للمعلومات (الانترنت) على الموقع : https://manifest.univ-ouargla.

(٢) عاد عبد المنعم ، أمن المعلومات والأمن القومي ، دراسات إستراتيجية ، مجلة السياسة الدولية ، العدد (٢١٣) ، مركز الاهرام للدراسات والبحوث الإستراتيجية ، القاهرة ، يوليو ٢٠١٨ ، ص٢٠٢ .

(٣) د. منى الأشقر جبور ، الأمن السيبراني : التحديات ومستلزمات المواجهة ، المركز العربي للبحوث القانونية والقضائية ، جامعة الدول العربية ، بيروت ، ٢٧ ٢٨ أغسطس (آب) ٢٠١٢ ، ص٢ .

(٤) علي زياد العلي ، التحديات غير المرئية للأمن الوطني العراقي ، مركز البيان للدراسات والتخطيط ، بغداد ، نشر بتاريخ ٢٠١٨/٦/٢٦م ، الشبكة الدولية للمعلومات (الانترنت) على الموقع :

http://www.bayancenter.org/2018/06/4565/

(٥) أوس مجيد غالب العوادي ، الأمن المعلوماتي السيبراني ، مركز البيان للدراسات والتخطيط ، بغداد ، آب / اغسطس ٢٠١٦ ، ص ١٩ ــ ٢٠ .

(٦) لمياء محمود ، الأمن القومي العربي كجزء من الأمن الإقليمي "الشرق أوسطي" : الأخطار وأدوار الفاعلين ، دراسات بحثية ، المركز الديموقراطي العربي للدراسات الإستراتيجية ، الاقتصادية والسياسية ، الشبكة الدولية للمعلومات (الانترنت) على الموقع : https://democraticac.de/?p=51048

(٧) الإرهاب الإلكتروني Cyber terrorism ، الموسوعة السياسية ، الشبكة الدولية للمعلومات (الانترنت) على الموقع : https://political-encyclopedia.org

(٨) محمد محمود السيد ، كيف سيواجه العالم تحديات "الأمن السيبراني" ، مجلة (السياسة الدولية) ، نشرت بتاريخ ٢٠١٤/٩/٢٤م ، الشبكة الدولية للمعلومات (الانترنت) على الموقع :

http://www.siyassa.org.eg/News/4925.aspx

(*) حسب تقرير للخبير الأمني في قضايا الإرهاب الرقمي (جيف باردين Jeff Bardin) .

(٩) د. بن مرزوق عنترة ، أ. حرشاوي محي الدين ، الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية ، مصدر سبق ذكره ، ص٦٨ .

(١٠) محمد محمود السيد ، كيف سيواجه العالم تحديات "الأمن السيبراني" ، مصدر سبق ذكره .

(١١) مكسيم لوفايفر ، السياسة الخارجية الأمريكية ، ترجمة : حسين حيدر ، الطبعة الأولى ، عويدات للنشر والطباعة ، بيروت ، ٢٠٠٦ ، ص٣٦ .

(١٢) الترويج لثقافة وطنية للأمن السيبراني ، الشبكة الدولية للمعلومات (الانترنت) على الموقع :
https://www.itu.int/dms_pub/itu-d/opd/stg/D-STG-SG01.22-2010-MSW-Adocx

(١٣) د.أحمد يوسف كيطان ، إستراتيجية الأمن الوطني السيبراني للصين : قراءة في قانون الأمن السيبراني الصيني ، مركز النهرين للدراسات الإستراتيجية ، نشرت بتاريخ ٢٠١٨/٤/١م ، الشبكة الدولية للمعلومات (الانترنت) على الموقع : **https://www.alnahrain.iq/post/242**

(١٤) د. حسين علاوي خليفة ، إستراتيجية الأمن الوطني العراقي ٢٠١٥ ٢٠١٨ : رؤية مستقبلية دراسة في ضوء البرنامج الحكومي الجديد ، مجلة قضايا سياسية ، العدد (٤٢) ، كلية العلوم السياسية ، جامعة النهرين ، بغداد ، ٢٠١٥ ، ص ١٥٩ ــ ١٦٠ .

(١٥) الإستراتيجية الوطنية للأمن السيبراني : دولة قطر ، وزارة الاتصالات وتكنولوجيا المعلومات ، قطر ، مايو ٢٠١٤ ، ص ٩ ــ ١٦ .

(١٦) أوس مجيد غالب العوادي ، الأمن المعلوماتي السيبراني ، مصدر سبق ذكره ، ص ٣٩ ــ ٤٠ .

(١٧) الإستراتيجية الوطنية للأمن السيبراني : دولة قطر ، مصدر سبق ذكره ، ص ١٠ ــ ١٦ .