مجلة العلوم القانونية والسياسية

اسم المقال: الأمن السيبراني وأثره في الأمن الوطني العراقي
اسم الكاتب: أ.م.د. مصطفى ابراهيم سلمان الشمري
رابط ثابت: https://political-encyclopedia.org/index.php/library/1210
تاريخ الاسترداد: 2026/11/01 18:04 +03

الموسوعة السياسيّة هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترنت.
لمزيد من المعلومات حول الموسوعة السياسيّة - Encyclopedia Political، يرجى التواصل على info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسيّة - Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام المتاحة على الموقع https://political-encyclopedia.org/terms-of-use

تم الحصول على هذا المقال من موقع مجلة العلوم القانونية والسياسية جامعة ديالى ورفده في مكتبة الموسوعة السياسيّة مستوفياً شروط حقوق الملكية الفكريّة ومتطلبات رخصة المشاع الإبداعي التي ينضوي المقال تحتها.

كلية القانون والعلوم السياسية – جامعة ديالى
المجلد العاشر – العدد الأول– 2021 مجلة العلوم القانونية والسياسية

الأمن السيبراني وأثره في الأمن الوطني العراقي

Cyber Security and its Impact on the Iraqi National Security

الكلمة المفتاحية: الأمن السيبراني، الفضاء السيبراني، الأمن الوطني، العراق، الارهاب.

Keywords: Cyber security, cyberspace, national security, Iraq, terrorism.

أ. م. د. مصطفى ابراهيم سلمان الشمري
جامعة بغداد - مركز الدراسات الاستراتيجية والدولية
Assistant Prof. Dr. Mustafa Ibrahim Salman
University of Baghdad – Center of Strategic and International Studies
E-mail: dr.mustafa@cis.uobaghdad.edu.iq

ملخص البحث

Abstract

يُعد الأمن السيبراني من أكثر المسائل اهمية في حياتنا المعاصرة بحكم علاقته المباشرة بجميع مجالات الحياة العامة من سياسة واقتصاد وامن وثقافة وغيرها، وتعتمد عليه معظم دول العالم في مؤسساتها الرسمية وغير الرسمية لا سيما في بنيتها التحتية، وان الاهتمام به وتلافي نقاط الضعف تعد من اولويات الأمن الوطني لأية دولة، وتمثل الحرب السيبرانية الجيل الخامس من التطور المعاصر للحروب وأكثرها خطورة بحكم الاضرار الكبيرة التي تخلفها في البنية التحتية لأية دولة، وما يترتب عليه من مساس مباشر لحياة المواطنين.

وأصبح العراق لاسيما منذ العام 2003 بسبب الانفتاح على العالم والتطور في المجال التقني والمعلوماتي أكثر عرضة للهجمات السيبرانية.

المقدمـــــة

Introduction

أصبح الأمن السيبراني في عالمنا المعاصر أكثر من كونه مسألة مرتبطة بأمن المعلومات والتقنيات وشبكات الحاسوب وغيرها، بحكم علاقته المباشرة بالمجال السياسي والامني والاقتصادي والاجتماعي والثقافي، إذ تعتمد معظم – إنْ لم تكن جميع المؤسسات الحيوية لأية دولة على تقنيات المعلومات في عملياتها اليومية التي تعتمد بدورها على أنظمة الاتصالات والمعلومات وهذا يعني بالنتيجة انها تعتمد على الأمن السيبراني.

وقد ادى التطور السريع للفضاء السيبراني بحكم الاستعمال الواسع جدًا للأفراد والمنظمات المحلية والاقليمية والدولية والمؤسسات الحكومية وغير الحكومية إلى تنامي اهميته الحيوية، مما جعل الاستغناء عنه أمرًا محالاً، غير ان هذا الفضاء عُرضة لتحديات عدة لاسيما تلك الهجمات الالكترونية التي تستهدف البنية التحتية، وبسبب الترابط العضوي بين الأمن السيبراني والفضاء السيبراني والبنية التحتية لأية دولة جعل الاضرار المتعمد بها يمثل تهديدًا للأمن الوطني للدولة المستهدفة، وهذا يفسر لنا ادراج معظم دول العالم مسألة الأمن السيبراني كأحد أولويات أمنها الوطني.

ومنذ العام 2003 شهد العراق انفتاحاً وتطوراً ملحوظاً في المجال التقني والمعلوماتي، مما جعل مؤسساته الرسمية والخاصة أكثر عرضة للهجمات السيبراني، إذ نشطت عبره التجارة والوسائل غير المشروعة مما فرض تحديات جديدة أثرت بشكل مباشر في منظومة أمنه الوطني، وتستلزم معالجتها.

أهمية البحث: تكمن اهمية البحث في ان الأمن السيبراني أصبح من اهم قضايا الأمن الوطني لأية دولة بحكم علاقته المباشرة بمؤسساتها وبنيتها التحتية ومواطنيها، وان اي تعرض بالهجمات الالكترونية لها سوف يؤثر مباشرةً بأمنها الوطني، بل سوف يؤدي إلى خسائر كبيرة، وفيما يتعلق بالعراق فقد زادت اهمية الأمن السيبراني منذ العام 2003 بحكم الاستخدام الواسع للفضاء السيبراني هذا من جهة، وتصاعد الهجمات الالكترونية من جهة اخرى.

اشكالية البحث: يقوم البحث على اشكالية رئيسة مفادها انه بالرغم من الدور الذي تلعبه برمجيات الحاسوب ونظم الحماية المتنوعة في الحد من الهجمات السيبرانية، إلا انها ما زالت تتعرض باستمرار لهذه الهجمات بل انها في تزايد، وعليه فما هو الأمن السيبراني والفضاء السيبراني؟، وما علاقة الأمن السيبراني بالأمن الوطني؟، وما تأثيره في الأمن الوطني العراقي؟.

فرضية البحث: ينطلق البحث من فرضية مفادها ان الأمن السيبراني أصبح جزءًا مهمًا في استراتيجية الأمن الوطني لأية دولة، وعليه تبذل الدول جهودًا كبيرة لضمانه من كل التحديات، ولكنها في الوقت ذاته عرضة باستمرار للهجمات السيبرانية.

منهجية البحث: اعتمد الباحث على المنهج الوصفي التحليلي فهو من اهم مناهج البحث في العلوم السياسية كونه يعمل على وصف الظاهرة محل الدراسة، ومن ثم يعمل على تحليلها وفق مؤشرات علمية.

هيكلية البحث: بهدف الاحاطة بموضوع البحث فقد تناول ما يأتي:

المبحث الأول: مفهوم الفضاء السيبراني والامن السيبراني.

المبحث الثاني: علاقة الأمن السيبراني بالأمن الوطني.

المبحث الثالث: الأمن الوطني العراقي في ظل تحديات الأمن السيبراني.

المبحث الأول

Section One

مفهوم الفضاء السيبراني والامن السيبراني

The concept of cyberspace and cybersecurity

تعددت تعاريف الفضاء السيبراني والامن السيبراني، بل ان البعض لا يفرق بينهما للترابط الوثيق بينهما، وعليه سنوضح هذين المفهومين، وبيان أهداف الأمن السيبراني وأهميته، وعلى النحو الاتي:

المطلب الأول: مفهوم الفضاء السيبراني:

First Requirement: The Concept of Cyberspace:

يرتبط الفضاء السيبراني بالواقع الافتراضي وشبكات الاتصال الالكترونية وانظمة الحاسوب، ولهذا تعددت تعاريفه ومنها تعريف ادارة السلامة العامة الكندية بأنه: " العالم الالكتروني الذي تم إنشاؤه بواسطة شبكات مترابطة لتكنولوجيا المعلومات، والمعلومات متاحة على تلك الشبكات أي انها مشاعة عالميًا حيث يرتبط الناس معًا بتبادل الأفكار والخدمات والصداقة. علمًا ان الفضاء السيبراني ليس ثابتًا، بل هو نظام بيئي ديناميكي ومتطور ومتعدد المستويات للبنية التحتية المادية والبرمجيات واللوائح والأفكار والابتكارات والتأثيرات التي يتأثر بها عدد متزايد من المساهمين الذين يمثلون مجموعة من البشر النوايا"[(1)].

وقد عرف المعهد الوطني للمعايير والتقنية في الولايات المتحدة الفضاء السيبراني بأنه: "الشبكة المترابطة من البنى التحتية لتكنولوجيا المعلومات، والتي تشمل الإنترنت وشبكات الاتصالات السلكية واللاسلكية والنظم الحاسوبية والمعالجات المدمجة وأجهزة التحكم"[(2)].

وعليه فإن الفضاء السيبراني هو الفضاء الافتراضي الذي يستخدم الالكترونيات والطيف الكهرومغناطيسي لتخزين وتعديل وتبادل المعلومات عن طريق استخدام النظام الشبكي والبنية المادية المعنية، أي إنه غير ملموس إذ تجري الاتصالات والأنشطة المتعلقة بالإنترنت، كما ان الفضاء السيبراني هو وهمي حيث الكائنات الموجودة فيه غير ملموسة ولا تمثل العالم المادي، ذلك لأنها بيئة افتراضية تمامًا، ويتم تبادل المعلومات والاتصال بين أكثر من (7,2) مليار

شخص حول العالم لتوفير منصة مشتركة لتبادل الأفكار والآراء والخدمات والصداقة، فهو فضاء قابل للتوسع بلا حدود بحكم طبيعته إذ ينمو بشكل هائل دون النظر إلى أي حدود مادية أو سياسية[3].

المطلب الثاني: مفهوم الأمن السيبراني:

The Second Requirement: The Concept of Cybersecurity:

يُمثل الأمن السيبراني ظاهرة عالمية وتحديًا اجتماعيًا تقنيًا معقدًا للحكومات، ويتطلب مشاركة الأفراد، وعلى الرغم أن الأمن السيبراني هو أحد أهم التحديات التي تواجهها الحكومات اليوم، إلا ان الرؤية والوعي العام لا يزالان محدودين، ويُعزى ذلك إلى أن معظم الناس ينظرون إلى الإنترنت على أنه بيئة آمنة ويستخدمونها يوميًا في هواتفهم الذكية والأجهزة اللوحية وأجهزة الكمبيوتر الخاصة بهم، في الوقت ذاته فإن هناك عددًا كبيرًا من الهجمات الالكترونية وبشكل يومي التي أخذت تطال الجميع من دون استثناء، مما جعل الشركات والمؤسسات تتكبد تكاليف أعلى للتعامل مع حوادث الأمن السيبراني، واذا كان بعض هذه الهجمات غير ضارة فإن بعضها الاخر شديد التأثير والخطورة، وتزداد أهمية الحاجة إلى الأمن السيبراني نظرًا لاعتمادنا على تكنولوجيا المعلومات والاتصالات في جميع جوانب الحياة المجتمعية، ويعد الأمن السيبراني ضروريًا للأفراد والمؤسسات العامة والمنظمات غير الحكومية، ورغم تمتع مواقع البحث الخاصة بالعديد من الحكومات بأمان محدود ولكن مع ذلك يتم اختراقها، والذي شمل ايضا الوزارات والمؤسسات الادارية والأحزاب السياسية والبنية التحتية من طاقة ومياه والمنظمات غير الحكومية وحتى المنظمات الرياضية كانت هدفًا للانتهاكات وسرقة المعلومات، ويلاحظ انه غالبًا ما يركز الاهتمام بقضايا الأمن السيبراني على الحوادث وكيفية التعامل معها بعد وقوعها، في حين أن مسألة الاهتمام في تحسين الأمن السيبراني بالوقاية من الانتهاكات قد تخلفت عن الركب، وهذه تعد مفارقة كون ان العالم يعيش معركة مستمرة بين المتسللين والمدافعين عن حماية النظام العام، كما ان هناك مفارقة أخرى تتمثل في سعي الحكومات إلى حماية الأمن السيبراني وحث الشركات والمواطنين بأن يحموا أنفسهم، لكنها في

المقابل تريد الوصول إلى بيانات المواطنين والشركات لأغراض المراقبة خشية استعمالها من قبل الإرهابيين والمجرمين وهذا ينطوي على انتهاك للخصوصية[4].

ولابد من الاشارة إلى ان الأمن السيبراني يتعلق بالناس والأنظمة على حدٍ سواء، علمًا ان هذا التفاعل المعقد بينهما يتطلب معرفة عميقة بالأمن السيبراني والبنية التحتية لتكنولوجيا المعلومات وأنواع الهجمات الممكنة لفهم ما يجري، لا سيما وان الناس يؤدون دورًا في الحفاظ على الأنظمة وتحديثها للتأكد من جاهزيتها أمام الهجمات الالكترونية كي يتم اكتشافها فورًا واتخاذ التدابير ضدها، وهذا يتطلب المعرفة الضرورية بما هو مطلوب، إذ ان قلة المعرفة لدى المستخدمين يمكن أن تؤدي إلى حدوث ثغرات أمنية إضافية منها على سبيل المثال استعمال كلمات مرور ضعيفة، وتثبيت برامج غير موثوقة، واستخدام الأجهزة والتطبيقات غير الآمنة، ومن ثم فإن الطبيعة الاجتماعية – التقنية للأمن السيبراني تُعقد عملية إيجاد الحلول، فأغلب الناس تريد ان تكون آمنة فقط وتحميل الحكومة عبء المسؤولية، كما ان غالبية الناس تعتقد ان المخاطر المتعلقة بالأمن السيبراني بعيدة عنهم وبأنهم لن يكونوا هدفًا للهجوم وهذا ينطوي على مغالطة، فالواقع خلاف ذلك إذ يتطلب الأمن السيبراني معركة مستمرة بين المتسللين والمدافعين رغم ان تأثير بعض هذه الهجمات والتقنيات الجديدة غير واضحة، مما يجعل من الصعب اظهار النجاحات والدعوة للاستثمار في تدابير الأمن السيبراني، وفي الواقع ان الحكومات تواجه مهمة صعبة ذلك انها تواجه عدوًا غير معروف أو شخص ينكر المسؤولية في موقف يصعب فيه إثبات أنه الجاني هذا من جهة، ومن جهة أخرى أصبحت مسألة الأمن السيبراني بحكم طبيعتها مشكلة عابرة للحدود الوطنية[5].

وقد شاع مصطلح الأمن السيبراني في السنوات الأخيرة على نطاق واسع، وأخذ يحظى بشعبية متزايدة لاسيما بعدما استخدمه الرئيس الامريكي (باراك أوباما) في العام **2009** في خطابه الذي دعا فيه الشعب الامريكي إلى الاهتمام بالأمن السيبراني لتعزيز أمننا القومي[6]. كما عد التهديد القادم من الفضاء السيبراني من اكبر التحديات الامنية والاقتصادية التي تواجه الولايات المتحدة، ولهذا جعله في مقدمة اهتماماته، وعين لهذا الغرض مسؤول عن الأمن

السيبراني ويكون عضوًا في مجلس الأمن القومي الامريكي وان يكون على اتصال دائم به والتنسيق معه، ومن جانبه عد (جون مايكل ماكونيل) رئيس الاستخبارات الامريكية (2007 – 2009) ان الانترنت رفع بشكل غير مسبوق التحديات التي يتعرض لها النظام والامن القومي الامريكي التي يمكن ان تشمل مجالات سياسية وحيوية[7].

علمًا ان أهم التحديات التي تواجه مصطلح الأمن السيبراني هي الاستخدام غير المدروس للمصطلح، فلا يوجد تعريف واحد متفق عليه للأمن السيبراني فهناك من يعده متداخلًا مع أمن المعلومات مُدعيًا أن الأمن السيبراني هو فرع من أمن المعلومات، وهناك من يربط بين الأمن السيبراني والخاصية العالمية للإنترنت على اعتبار انه أوسع من أمن المعلومات الذي يهتم أساسًا بالسرية، وهناك من عرفه بأنه "الاسلوب والإجراءات المرتبطة بعمليات إدارة المخاطر الأمنية التي تتبعها المنظمات والدول لحماية سرية وسلامة وتوافر البيانات والأصول المستخدمة في الفضاء السيبراني، ويتضمن المفهوم إرشادات وسياسات ومجموعات من الضمانات والتقنيات والأدوات والتدريب لتوفير أفضل حماية لحالة البيئة السيبرانية ومستخدميها"[8]. وكذلك يُعرف بأنه " 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 بأسرع وقت ممكن بحيث لا تتوقف عجلة الانتاج، وبحيث لا تتحول الاضرار إلى خسائر دائمة"[9].

وقد عرف الاتحاد الدولي للاتصالات الأمن السيبراني بأنه "مجموعة من الأدوات والسياسات والمفاهيم الأمنية والحمايات الأمنية والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريبات والممارسات الفضلى والضمانات والتكنولوجيات التي يمكن استعمالها لحماية البيئة السيبرانية والمنظمة وأصول المستعمل"، ويقصد بالأصول هنا أجهزة الحاسوب ومستعمليه، وانظمة الاتصالات والخدمات والتطبيقات وجميع المعلومات الموجودة في الفضاء السيبراني بما يضمن سلامة الخدمة وسريتها واستمراريتها وحمايتها من المخاطر الأمنية المنتشرة في البيئة السيبرانية، وقد تنوعت اشكال الهجوم السيبراني منها: الفايروسات وأحصنة طروادة

والديدان الالكترونية والتجسس الالكتروني وسرقة الهوية والهجمات والاحتيال عبر الانترنت وغيرها، ونظرا لكثرتها وتنوعها فإن هناك حاجة ضرورية لمواجهتها عن طريق توسيع قاعدة المعرفة لتأمين الشبكات منها، ومن ابرز وسائل الحماية هي: التدقيق والمراقبة والحوسبة الآمنة وبرامج الحماية من الفايروسات وانظمة كشف الاختراق والحماية منه والجدران الواقية، وعليه فإن من الضروري اتباع اسلوب امني متعدد الطبقات، بحيث يكون الأمن شامل كل اجزاء النظام الالكتروني من انظمة وشبكات وتطبيقات لاسيما وان الأمن السيبراني هو عملية مستمرة ولا يوجد نظام امني واحد ينطبق على الجميع، وتشمل تقنيات الأمن السيبراني التشفير وضوابط النفاذ وسلامة النظام والتدقيق والإدارة والرصد والمراقبة[10].

وقد عرف المعهد الوطني للمعايير والتقنية في الولايات المتحدة الأمن السيبراني بأنه: "النشاط أو العملية أو القدرة أو الإمكانية أو الحالة التي يتم بموجبها حماية نظم المعلومات والاتصالات والمعلومات الواردة اليها والدفاع عنها ضد الضرر أو الاستخدام أو التعديل غير المصرح به أو الاستغلال"[11]. كما يعرف ايضاً بأنه: تقنيات وعمليات تم تصميمها لحماية الكمبيوتر وأجزاء وبرامج الكمبيوتر والشبكات والبيانات من الوصول غير المصرح به ونقاط الضعف التي يتم توفيرها عبر الإنترنت من قبل مجرمي الإنترنت والجماعات الإرهابية والمتسللين، ويرتبط الأمن السيبراني بحماية الإنترنت الخاصة بالأشخاص والمعدات الرقمية القائمة على الشبكة من الوصول غير المصرح به والتلاعب[12].

والملاحظ ان تعريفات الأمن السيبراني قد تعددت ولعل ابرزها فضلاً عما تقدم هو: الأساليب الدفاعية المستخدمة للكشف عن المتسللين المحتملين وإحباطهم، أو حماية شبكات الكمبيوتر والمعلومات التي تحتويها من الاختراق ومن الاضرار الخبيثة أو الاختلالات، ويعرف ايضاً بأنه الحد من خطر التعرض لهجمات ضارة على البرامج وأجهزة الكمبيوتر والشبكات، ويتضمن ذلك الأدوات المستخدمة للكشف عن الاختراقات وإيقاف الفيروسات ومنع الوصول إلى البرامج الضارة وفرض المصادقة وتمكين الاتصالات المشفرة وتشغيلها، وكذلك هو القدرة على حماية الفضاء السيبراني والدفاع عنه من الهجمات السيبرانية، كما يعرف بأنه: مجموعة

التقنيات والعمليات والممارسات وتدابير الاستجابة والتخفيف المصممة لحماية الشبكات وأجهزة الكمبيوتر والبرامج والبيانات من الهجوم أو الاضرار أو الوصول غير المصرح به وذلك للتأكد من السرية والنزاهة والتوافر، ويعرف أيضًا بأنه: فن ضمان وجود واستمرارية مجتمع المعلومات للشعب، وضمان وحماية المعلومات والأصول والبنية التحتية الحيوية في الفضاء السيبراني، والامن السيبراني هو ايضاً النشاط أو العملية أو القدرة أو الامكانية أو الحالة التي تحمي فيها أنظمة المعلومات والاتصالات والمعلومات الواردة اليها، وان يتم الدفاع عنها ضد الاضرار أو الاستخدام غير المصرح به أو التغيير أو الاستغلال، فضلاً عن ذلك يعرف الأمن السيبراني هو تنظيم وجمع الموارد والعمليات والهياكل المستخدمة لحماية الفضاء السيبراني والأنظمة الممكّنة للفضاء السيبراني من الحوادث التي تتعارض بشكل غير قانوني مع حقوق الملكية الفعلية، ويتميز الأمن السيبراني بالطابع الاجتماعي والفني متعدد التخصصات، وانه شبكة خالية من المقاييس أي ان الجهات الفاعلة في الشبكة الالكترونية متشابهة إلى حد كبير، ويتمتع بدرجات عالية من التغيير والترابط وسرعة التفاعل[13].

وعليه فإن الأمن السيبراني هو مزيج من العمليات والتقنيات والممارسات، والهدف منه حماية البرامج والتطبيقات والشبكات وأجهزة الكمبيوتر والبيانات من الهجوم، ويشمل الأمن السيبراني الأمن المادي للبرامج والتطبيقات والشبكات وأجهزة الكمبيوتر، وامن غير مادي أو معنوي يتعلق بالبيانات والمعلومات من أي هجوم واضرار متعمدة وسرقة للمعلومات والتحكم في الوصول الصحيح للأجهزة والتطبيقات والشبكات لحمايتها من الضرر الذي قد يحدث عبر الشبكات، ولعل أهم مجالات الأمن السيبراني هي: أمان التطبيق، و أمن المعلومات، وامن البريد الالكتروني، وأمن أجهزة المحمول، وأمن محركات البحث، وأمن اللاسلكي [14]. وتشمل استراتيجيات الأمن السيبراني إدارة الهوية وإدارة المخاطر وإدارة الحوادث[15].

المطلب الثالث: اهداف الأمن السيبراني وأهميته:

The third requirement: the aims and importance of cybersecurity:

يُعد الأمن السيبراني الآن جزءًا مهمًا لكل شرائح المجتمع من فرد واسرة، وكذلك للمنظمات والحكومات والمؤسسات والافراد، ومن الضروري حماية الاسرة ولاسيما الاطفال من عمليات الاحتيال عبر الإنترنت، ومن الضروري أيضًا حماية المعلومات المالية التي يمكن أن تؤثر على الوضع المالي لأي شخص، وتأتي هذه الضرورة من الاهمية المتزايدة للإنترنت الذي أصبح حاجة حيوية لجميع المؤسسات والمنظمات والافراد، فقد وفر الانترنت الكثير من فرص العمل والتعلم، وعليه لا بد من فهم كيفية حمايةً المؤسسات والافراد لأنفسهم من الاحتيال عبر الانترنت وسرقة الهوية لا سيما وان هناك العديد من التحديات التي تواجههم منها محدودية الموارد وضعف في مهارات الأمن السيبراني، وان التعلم المناسب عند استعمال الانترنت وحماية أنظمة الحاسوب يمكن ان توفر بيئة آمنة للأنترنت[16].

ويمكن تحديد أهم أهداف الأمن السيبراني بالآتي[17]:

1. الهدف الأول (السرية) التي تضمن أن الأفراد المصرح لهم فقط يمكنهم تلقي أو تغيير أو إدارة المعلومات.
2. الهدف الثاني (النزاهة) التي تضمن أن الأشخاص أو العمليات المصرح لهم فقط هم من يستطيعون إجراء أي تغييرات في النظام.
3. الهدف الثالث هو توفر النظام والمعلومات التي يديرها النظام ومشغليه مما يضمن أن الكيانات المرخص لها فقط يمكنها الوصول إلى المعلومات أو الموارد المخزنة أو المستخدمة في البنية التحتية للمؤسسات.

وعليه يحظى الأمن السيبراني بأهمية بالغة ذلك لأن الحكومات والمؤسسات العسكرية والشركات والمؤسسات المالية والطبية وغيرها تقوم بجمع ومعالجة وتخزين كميات كبيرة جدًا من البيانات على أجهزة الكمبيوتر والأجهزة الأخرى، وان الكثير من هذه البيانات معلومات حساسة كونها تتعلق بالملكية الفكرية أو معلومات أمنية أو شخصية أو بيانات مالية وان

الدخول غير المصرح به إلى هذه المعلومات والبينات لهُ عواقب وخيمة، لا سيما وان هذه المعلومات تنتقل بين المؤسسات والشركات عبر الشبكات إلى الأجهزة الأخرى، ونظرًا لارتفاع خطر الهجمات الالكترونية فإن الدول والمؤسسات والشركات تجد نفسها مضطرة لحماية بياناتها ومعلوماتها، بل أصبحت الهجمات الإلكترونية والتجسس الرقمي يمثلان أكبر تهديد للأمن القومي لأي بلد، بل إنه فاق خطر الإرهاب[18].

وللدلالة على اهمية الأمن السيبراني في عالمنا المعاصر ان مجرمي الانترنت يركزون في هجماتهم على البنية التحتية الحيوية لأنه في حالة حدوث هجوم ناجح عليها يمكنهم من الحصول على ربح مالي أو سياسي، مستغلين بذلك نقاط الضعف في هذه البنية كون بعضها يستعمل انظمة حماية الكترونية تجارية ومع المعرفة الجيدة بالتقنية يُمكن للمهاجم استغلال الثغرات الموجودة في هذه الانظمة، وما زاد من تعقيد الامور ان الحوادث في الفضاء السيبراني تواجه دائمًا مشكلة إسناد المسؤولية فمن الصعب تتبع مرتكبي الحادث، علاوة على ذلك أن التهديدات السيبرانية يصعب التنبؤ بها واتخاذ التدابير الوقائية في الوقت المناسب، مما جعل خطر تنفيذ الهجمات السيبرانية الناجحة يزداد لاسيما وانها غير مرئية، علمًا ان الهجوم السيبراني يتطور وفق خمس مراحل هي: العثور على ثغرة أمنية في النظام، والسيطرة على النظام أو جزء منه، وإدخال البرامج الضارة في النظام، وإصابة مكونات النظام الأخرى، والقيام بهجوم على النظام بأكمله أو على جزء خاص منه، وتتسبب الثغرات في الأمن السيبراني بحدوث مشكلات كبيرة لكل مالك أو مشغل للنظام، ومن أجل منع الحوادث السيبرانية فإن أفضل ما يمكن عمله هو تحسين الأمن السيبراني[19].

وجدير بالذكر ان بنيان الأمن السيبراني يقوم على محورين أساسين هما الادارة والحوكمة، ويقصد بالإدارة في سياق الأمن السيبراني هي: ادارة أمن المعلومات وتحليل مستوى جاهزية منظومة الأمن السيبراني من حيث التكامل الاستراتيجي، وتوسيع استراتيجية الأمن السيبراني، وتقليل المخاطر، والقدرة على التكيف لتسهيل حركة اتخاذ القرارات لمواجهة الهجمات الإلكترونية ضد الافراد والشركات[20]. علمًا ان الأمن السيبراني والإدارة يرتبطان ارتباطًا وثيقًا

فمن المسلم به أن الأمن السيبراني لا يقل أهمية عن الأمن المادي، وعلى الرغم من عدم وجود نموذج واحد لإدارة الأمن السيبراني، إلا ان هناك اتفاقاً عالمياً بان ادارة الأمن السيبراني ضرورية كونها تعمل على حماية البنية الأساسية الحيوية، فجميع بلدان العالم تدرك الحاجة إلى ادارة مواردها الحيوية وحمايتها بعناية، كما تعمل الحكومات والمنظمات العالمية على بذل كل جهودها لتوفير الأمن للبنية التحتية الحيوية لأنه يضمن رفاهية أي بلد وشعبه، لا سيما عندما أصبحت البنية التحتية الحيوية وأمن الطاقة وثيقة الصلة بالقرارات السياسية[21]. وأما الحوكمة فيقصد بها ضمن اطار الأمن السيبراني بانها " المبادئ والقواعد الإدارية وأساليبها المُتبعة في جهة ما لضبط سلطات اتخاذ القرار وتحديد أصحاب المسؤولية والمحاسبة في تنفيذ المهام والواجبات ذات العلاقة بحماية الجهة من الهجمات الالكترونية أو سوء استخدام الأصول المعلوماتية، مع ضمان استمرارية العمليات التشغيلية في حال وقوع حوادث أو كوارث"، أي ان الهدف من حوكمة الأمن السيبراني توجيه سلوكيات وقرارات الاشخاص ومراقبتهم وارشادهم بما يحسن ويرفع من كفاءتهم فضلاً عن تسهيل عمل الجهات ذات العلاقة وتنسيق جهودها[22].

المبحث الثاني

Section Two

علاقة الأمن السيبراني بالأمن الوطني

The relationship of cybersecurity to national security

قبل الحديث عن علاقة الأمن السيبراني بالأمن الوطني لا بد من التأكيد على مسألة مهمة وهي ان مفهوم الأمن الوطني يتسم بالعمومية لتأثره بحقائق متنوعة ومتغيرة ونسبية نابعة من العوامل الداخلية والخارجية، ويُعد الأمن في قمة الضرورة لأية دولة، لذلك تلجأ الدولة إلى العديد من التشريعات والاجراءات التي تكفل سلامة امنها الوطني بما يعززه داخليًا ويحميها من الاخطار الخارجية، وعليه فإن الأمن الوطني يساوي كيان الدولة وأساس بقائها[23]. ولهذا تعددت مفاهيم الأمن الوطني فهناك من يرى بأنه: "ما تقوم به الدولة للحفاظ على سلامتها ضد الاخطار الخارجية والداخلية التي تؤدي بها إلى الوقوع تحت سيطرة اجنبية نتيجة ضغوط خارجية او انهيار داخلي"[24]. وقد عرف الكاتب السياسي الامريكي (والتر ليبمان) الأمن الوطني بأنه " قيمة قد تزيد أو تنقص وذلك حسب قدرة الأمة على ردع أي هجوم أو هزيمته " أي ان الأمن الوطني يمثل قيمة متغيرة[25]. كما عرف (فرانك تراغر) و (فرانك سيموني) الأمن الوطني بأنه " ذلك الجزء من السياسة الحكومية الذي يهدف إلى خلق الظروف القومية والدولية اللازمة لحماية وتوسيع القيم الوطنية الحيوية ضد الخصوم الحاليين او المحتملين "، وعرفه (دونالد برينان) بأنه سلامة البقاء الوطني، وعليه فإن الأمن يركز بشكل أساسي على التحرر من كل اشكال الخوف والتهديد[26].

وقد أصبح الأمن الوطني لأية دولة وثيق الصلة بتكنولوجيا المعلومات والاتصال بحكم قدرتها في التأثير على اي مجتمع، فقد اختصرت وسائل التواصل الاجتماعي من فيسبوك وتوتير والفايبر والتيليجرام والواتس اب والسكايب واليوتيوب وغيرها الوقت والمسافة، وأخذت تحظى بتأثير فعال ومتنامي لدى معظم شعوب العالم، ويبرز في هذا الخصوص الحراك الشعبي والاحتجاجات الجماهيرية التي اخذت تنتظم على شكل مظاهرات وشكلت مصدر قلق للأنظمة الحاكمة، إذ لها دور في توجيه الرأي العام وتعبئة الشارع، وخير مثال على ذلك ما

تعرضت له البلدان العربية منذ العام 2011 التي تأثرت بما يسمى (الربيع العربي)[27]. علمًا ان هناك مجمعاً صناعياً الكترونياً آخذاً في الظهور، تمامًا مثل المجمع الصناعي العسكري في الحرب الباردة[28].

وتكمن المفارقة ان الاقتصاد الرقمي والمجتمع الاكثر تقدمًا في أي بلد يكون أكثر عرضة للتهديدات السيبرانية، وهذا يتطلب من الدول ذات الاقتصاد الرقمي والبنية التحتية الرقمية المتقدمة إيلاء المزيد من الاهتمام لحماية الفضاء السيبراني، لا سيما بعدما أصبح الأمن السيبراني مشكلة أمنية وطنية وجزءاً لا يتجزأ من منظومة الأمن الوطني لأية دولة، بل يجب أن تبنى استراتيجية الأمن الوطني السيبراني على استراتيجية الأمن الوطني، وتحتاج الدول إلى استراتيجيات مرنة وديناميكية للأمن السيبراني حتى تستطيع الرد على التهديدات السيبرانية، لا سيما وان الفضاء السيبراني دائم التغير والتطور وليس له حدود مادية، وهذا بدوره يفرض مسألة لا تخلو من الحساسية ألا وهي حماية البيانات مقابل مشاركة المعلومات، فالمواطنين لديهم حق مشروع في العيش في مجتمع مفتوح يتمتع بالتدفق الحر للمعلومات، وفي المقابل فإن الحكومات من واجبها حماية هذه المعلومات حفاظًا على الأمن والنظام العام، فمكافحة جرائم الإنترنت والحرب على الارهاب وغيرها تتطلب تبادل المعلومات وتفاعل يومي بين المواطنين والحكومة كونها أصبحت من الضرورات المعاصرة للأمن الوطني، ويمكن تقسيم الاستراتيجية الوطنية للأمن السيبراني على خمسة اقسام رئيسة وهي: العسكرية أي الحرب السيبرانية، والجرائم السيبرانية، وحماية البنية التحتية الحيوية، وادارة الأزمات، والدبلوماسية السيبرانية، كما ان الدول تصوغ استراتيجية امنها السيبراني بشكل مستقل بناءً على أفكارها وتصوراتها الأمنية[29].

وعليه فإن التطورات المعاصرة فرضت نفسها على دول العالم ضرورة تبني استراتيجية وطنية للأمن السيبراني على ان يراعى فيها التوازن بين متطلبات الأمن الاساسية وبين احترام خصوصية المواطنين وطبيعة الثقافة السائدة في البلد، علما ان هذه الاستراتيجية لا بد ان تكون ذات نهج شمولي أي لا تقتصر على الحكومة فحسب، بل من الضروري اشراك جميع أصحاب المصلحة وهم: الحكومة، والقضاء، والاجهزة الامنية، والمسؤولين عن البنية التحتية للأمن

السيبراني من القطاع العام والخاص، ومجهزي خدمة الانترنت وتكنولوجيا المعلومات، والمؤسسات التعليمية المختصة، والمواطنين، فضلا عن الهيئات الاقليمية والدولية المعنية بمجال الأمن السيبراني[30].

ومن اجل ضمان فاعلية ونجاح الاستراتيجية الوطنية للأمن السيبراني لا بد من توفر مجموعة من العناصر الاساسية لها ولعل أهمها: ضمان أعلى مستوى من التأييد والدعم الرسمي لها ماديا ومعنويا من قبل الحكومة، وتشكيل هيأة مختصة بالأمن السيبراني، وإشراك الهيئات الحكومية المعنية وضمان التعاون والتنسيق فيما بينها، واشراك أصحاب المصلحة الاخرين لاسيما القطاع الخاص الموثوق بهم لضمان عمل البنى التحتية الأساسية للأمن السيبراني، وتخصيص موارد لها في ميزانية الدولة الوطنية، وضرورة ان تتضمن الاستراتيجية خططاً قابلة للتنفيذ وأهداف قصيرة ومتوسطة وبعيدة المدى تسعى إلى تحقيقها، والإدارة الجيدة لمخاطر التهديدات السيبرانية لضمان استمرارية عمل هذه الاستراتيجية، ووضع خطة طوارئ لإدارة أزمات الأمن السيبراني، وتعزيز تبادل المعلومات بين القطاع الحكومي والخاص، وإجراء عمليات محاكاة وتدريبات عملية للأمن السيبراني، فضلاً عن تدريب كوادر مختصة وتنمية مهاراتهم، وتشجيع الابتكار والبحث والتطوير، ووضع قوانين واضحة تحد من الانشطة السيبرانية المحظورة معززة بقدرات تنفيذية تحد من الجريمة السيبرانية، ومواءمة الاستراتيجية الوطنية للأمن السيبراني بخطط واستراتيجيات الأمن السيبراني الإقليمية والدولية[31].

وقد اكتسبت الصراعات السياسية والعسكرية والاقتصادية بين الدول بُعدًا الكترونيًا بحيث يصعب التنبؤ بحجمها وتأثيرها، بل ان الحروب التي تدور رحاها في الفضاء السيبراني أكثر أهمية من الأحداث التي تجري على أرض الواقع، ذلك ان الانجازات المذهلة للتجسس السيبراني اظهرت المكاسب الكبيرة لعمليات اختراق اجهزة الكومبيوتر مقارنة بارتفاع اشكال التجسس التقليدية التي تتطلب ذكاء بشري وارتفاع نسبة الخطورة، مما جعل التجسس السيبراني على الساحة العالمية مصدر قلق للدول على امنها الوطني، فالهجوم السيبراني ليس غاية في حد ذاته ولكنه وسيلة قوية لمجموعة متنوعة من الغايات من الدعاية إلى التجسس، ومن تعطيل الخدمات

إلى تدمير البنية التحتية الحيوية، ويجادل البعض انه لم يحصل تغير في طبيعة التهديد للأمن الوطني، لكن الانترنت وفر آلية جديدة يُمكنه من زيادة سرعة الهجوم وحجمه وقوته، ذلك ان انتشار الانترنت وتزايد اعتماد العالم عليه سيترتب على الإضرار به تداعيات سياسية واقتصادية وعسكرية ملموسة لا سيما بعد التطور الملفت للهجمات السيبرانية كنتيجة طبيعية للنزاعات في العالم الحقيقي، مما سيؤدي دورًا رئيسًا في النزاعات المستقبلية[32].

ولعل أحد مفارقات مساحة الحرب السيبرانية هو أن اللاعبين الكبار والصغار يتمتعون بمزايا، فالدول القوية في تكنولوجيا المعلومات تستغل قوتها السيبرانية الفائقة، وفي المقابل تستغل الدول الصغيرة وحتى المتسللين من غير الدول قوة انتشار الانترنت لمهاجمة عدو أقوى، علاوة على ذلك فإن الدول التي تعتمد على الانترنت تمثل هدفاً مغرياً لأنها تملك الكثير لتخسره عندما تنهار شبكة الانترنت فيها، كما ان المساحة في الحرب السيبرانية متقاربة جدًا لان الجميع متجاور في الفضاء السيبراني، إذ تشكل الأجهزة والبرامج وعرض النطاق الترددي الحدود وليس الجبال والوديان والممرات المائية، كما انها لا تعتمد على الأسلحة القوية بل على الذكاء والابتكار، فضلاً عن ذلك ان أهم ميزة للمهاجم في هذه الحرب هي مدى امكانية الكشف عن هويته، إذ يخترق المتسللون الأذكياء شبكة الانترنت الدولية التي تشبه المتاهة، وتوجه الهجمات ضد حكومات دول لديها مشكلات دبلوماسية مع دول ما، أو لأنها ضعيفة من ناحية امكانية تنفيذ القانون، فمن الناحية النظرية يمكن مواجهة صراع سيبراني كبير ضد خصم غير معروف، وعلى المستوى التقني فهناك قلة خبرة في مواكبة هذا التهديد بل قد يكون من الصعب حتى معرفة مدى التعرض للهجوم السيبراني، وعلى المستوى السياسي فإن الطبيعة غير الملموسة للفضاء السيبراني تجعل حساب النصر والهزيمة صعبة للغاية[33].

ان الهجمات السيبرانية المعاصرة تستهدف القيادات السياسية والأنظمة العسكرية والمنشآت الحيوية والمواطنين العاديين في أي مكان من العالم في وقت السلم والحرب مستفيدين من امكانية إخفاء هوية المهاجم، والامثلة على ذلك كثيرة منها: تعرض البرازيل إلى هجمات سيبرانية في عامي 2005 و 2007 اغرقت مدنًا بأكملها في الظلام وأثرت في ملايين المدنيين،

وما زال مصدر الهجمات مجهولاً، كما تعرضت شبكات الكهرباء في الولايات المتحدة أيضًا لمثل هذه الهجمات في ايار 2009، ونظرًا للأهمية المتزايدة للأمن السيبراني وتأثيره المباشر في الأمن الوطني لأية دولة انشأت الولايات المتحدة قيادة متخصصة بالأمن السيبراني التي أعلنت أن الفضاء السيبراني هو المجال الجديد للحرب، كما ان الاولويات الثلاثة الأولى لمكتب التحقيقات الفيدرالي الأمريكي (FBI) هي مكافحة الإرهاب، والتجسس، والهجمات السيبرانية، ويأتي الهجوم على الكهرباء كونها من اهم البنى التحتية وان قطعها سيؤثر بلا شك على شبكات الكمبيوتر التي تعتمد عليها مما سيؤثر بالنتيجة على الأمن الوطني، فضلاً عن ذلك تعرض منشآت ايران النووية في العام 2010 إلى هجوم سيبراني – دودة الكمبيوتر من نوع Stuxnet – بحيث نجح نصف ميغابايت من رمز الكمبيوتر من الحاق اضرار تتجاوز فاعلية أي هجوم عسكري تقليدي، ونظرًا لتطور الأمن السيبراني من تخصص تقني إلى مفهوم استراتيجي، ولأن الهجمات السيبرانية يمكن أن تؤثر في الأمن الوطني على المستوى الاستراتيجي، فانه يجب على الدول وقادتها حشد جميع موارد الدولة بما يحمي الأمن السيبراني الاستراتيجي[34].

وجدير بالذكر ان الهجمات السيبرانية تُعد من أكثر الهجمات وضوحًا وإزعاجًا في القرن الحادي والعشرين لاسيما عندما تقترن بدوافع سياسية، وعليه عُدت الحرب السيبرانية بأنها "حرب الجيل الخامس"[35]. وبرزت بشكل واضح في العام 2017 تقريبًا، بحكم الاضرار الكبيرة التي تحدثها على نطاق واسع، فبغضون ساعات قليلة يمكن للهجمات السيبرانية ان تصيب أعدادًا كبيرة من الشركات والمؤسسات لمناطق جغرافية كبيرة ومتنوعة، ولعل أهم سمات الجيل الخامس من هذه الحروب السيبرانية هي: الذكاء التقني للمهاجمين والتطور والسرعة والنجاح والثراء وقدرة عالية على الاختفاء[36]. ولا تتقيد بحدود جغرافية، فضلاً عن الاستعمال الواسع للأجهزة الرقمية من حاسوب ومحمول وغيرها.

وعليه فإن الأمن السيبراني يعد مشكلة للفرد والمجتمع على حدٍ سواء، ويتعين معالجتها من قبل السياسيين كونها امن وطني بالمقام الأول، إذ يتفق جميع السياسيين على أن الأمن

السيبراني أمر مهم وينظرون إليه كمسألة تكنولوجية تحتاج إلى حل بشكل عام، فهو أكبر من مجرد مشكلة تكنولوجية ذلك أن القيم السياسية للدولة هي المقصودة في اي هجوم سيبراني، إذ يُنظر إلى الجريمة السيبرانية على أنها تهديد محتمل في كل مكان، وسيترتب عليها تأثير مدمر على الحياة، وفي حالة عدم وضع حد لها ستكون المخاطر كبيرة، علمًا ان هناك مشكلة يجب ان تؤخذ بنظر الاعتبار ألا وهي ان عدم وضوح المجرم في الغالب سيعقد من صياغة الأمن السيبراني بطريقة فعالة، ذلك ان الهجوم السيبراني سيعده البعض عملاً شريراً او ارهابيًا في حين يعده البعض الاخر بأنه عملا بطوليًا اعتمادًا على وجهة النظر[37].

ولذلك أصبح الأمن السيبراني أكثر أهمية في أذهان صانعي القرار في الدول، ولهذا تم وضع عقائد متعلقة بالأمن السيبراني في جميع دول العالم تقريبًا، ولكن واقع الحال يؤكد بأنه لا تزال هناك فجوة واضحة بين الدول من حيث الوعي، والفهم والمعرفة والقدرة، أخيرًا على نشر الاستراتيجيات، والقدرات والبرامج، المناسبة لضمان الاستخدام الأمن، والملائم لتكنولوجيا المعلومات والاتصالات كعوامل تضمن الأمن وتحقق التنمية الاقتصادية[38].

ومن الجدير بالذكر ان الدول المعتمدة على البنية التحتية للمعلومات والاتصالات يمكن لأي هجوم سيبراني ان يؤثر في طبيعة عمل مجتمعاتها، ولهذا يوصف الأمن السيبراني بأنه "حجر الزاوية لمجتمع المعلومات"، وعليه فانه يتطلب تخطيطًا استراتيجيًا متماسكًا ومفصلاً وتنظيمًا قانونيًا مناسبًا، وقد أخذت الدول تتبنى استراتيجيات وطنية للأمن السيبراني خاصة بها اعتبارًا من العام 2011، وتختلف الاستراتيجيات الوطنية للأمن السيبراني في كل دولة على حدة من حيث المحتوى والشكل والتنفيذ وغيرها، فلا يوجد حاليًا إطار وطني موحد لحماية الأمن السيبراني، ومع ذلك فإن وجود مثل هذه الاستراتيجيات وتنفيذها بشكل صحيح يمكن أن يساعد في حماية الأمن الوطني لأية دولة، كما يضمن التطور السليم للمجتمع، ويمكن أن تساعد الاستراتيجية الوطنية الفعالة للأمن السيبراني في حل النزاعات بين الدول وضمان السلام، وفي هذا الخصوص صرح (ينس ستولتنبرغ) الأمين العام لحلف الناتو بان الانترنت أصبح الآن جزءًا أساسيًا من جميع الأزمات والصراعات تقريبًا[39].

وتتباين الهجمات السيبرانية من حيث التأثير والحجم، إذ يستطيع أي هجوم ناجح على بعض مكونات البنية التحتية الحيوية أن يكون له تأثيرات كبيرة على الأمن الوطني والاقتصاد ومعيشة وسلامة المواطنين، إلا أنه من الصعب قياس التأثيرات الاقتصادية، إذ تختلف تقديرات تلك التأثيرات على نطاق واسع، ويرى بعض المختصين ان التكاليف تزداد بشكل كبير لا سيما مع التوسع المستمر في البنية التحتية لتكنولوجيا المعلومات والاتصالات، ولكن عمومًا تُعد باهظة[40]. وتشير بعض التقارير ان الخسائر العالمية المقدرة من جرائم الإنترنت تتجاوز (400) مليار دولار أمريكي في السنة، هذا الواقع دفع بالرئيس الامريكي حينها (باراك اوباما) إلى وصف الأمن السيبراني بأنه "واحد من أخطر تحديات الأمن الاقتصادي والوطني التي نواجهها كأمة"[41].

وتزداد تكلفة الجريمة السيبرانية بالارتفاع مع زيادة عدد الهجمات السيبرانية، وتقسم جرائم الهجمات السيبرانية إلى أربعة اقسام رئيسة هي تعطيل الأعمال، وفقدان المعلومات، وخسارة الإيرادات، وتلف المعدات[42].

علمًا ان مؤشرات الهجمات السيبرانية وجرائم الإنترنت كثيرة جداً لعل اهمها: انه في العام 2017 ارتفعت نسبة الهجمات السيبرانية بنسبة (600 %)، ويعزى هذا الارتفاع إلى زيادة عدد الأجهزة المرتبطة بالإنترنت، وتكمن المشكلة في أن الأمن لا يواكب وتيرة التهديدات المتزايدة، وركزت (31 %) من الهجمات السيبرانية على البنية التحتية، كما تم شن (91 %) من الهجمات السيبرانية برسائل احتيال عبر البريد الإلكتروني، وان (85 %) من جميع المرفقات التي يتم إرسالها بالبريد الالكتروني يوميًا ضارة للمستلمين المقصودين، وان (38 %) من المرفقات الخبيثة يتم ارسالها على انها ملفات لبرامج مايكروسوفت اوفس أو برامج أخرى، ويمكن أن تشل البرامج الضارة الأنظمة بالكامل أو تجعلها عديمة الفائدة، وان أي هجوم ناجح للبرامج الضارة سيؤدي إلى خرق للأمن السيبراني، ويمكن أن تنهار بسببه شركة بأكملها فضلاً عن تدمير سمعتها العامة، ويبلغ متوسط تكلفة هجوم البرامج الضارة (4,2) مليون دولار، ويتطلب من الشركات حتى تتمكن من الكشف عن خرق البيانات قرابة (6) أشهر، ففي العام

2017 شكلت الشركات الصغيرة التي لديها اقل من ألف موظف قرابة (61 %) من ضحايا خرق البيانات[43].

وفي الواقع ان العالم المعاصر يعتمد كليًا تقريبًا على التكنولوجيا القابلة للاختراق، ولهذا فإن كل (39) ثانية يقع هجوم للقراصنة في جميع أنحاء العالم، ويحصل مجرمو الانترنت على عائدات سنوية تقدر بنحو (5,1) تريليون دولار، وان (60 %) من عمليات الاحتيال تحصل عبر الأجهزة المحمولة، ويتم غسل (80) مليار دولار سنوياً، ويقدر عدد ضحايا الجرائم السيبرانية في العام 2018 قرابة (700) مليون شخص موزعين على (20) دولة، وان (43 %) من الجرائم السيبرانية تستهدف الشركات الصغيرة، ويقدر عدد الأجهزة الذكية المتصلة في جميع أنحاء العالم بحدود (17) مليار، وتم انفاق (96) مليار دولار على الأمن السيبراني في العام 2018 بزيادة قدرها (8 %) عن العام 2017، وكلفت الجرائم السيبرانية الشركات التجارية في العام 2019 قرابة (2) تريليون دولار، وهذا المبلغ هو أعلى بأربعة أضعاف مما كان عليه في العام 2015[44].

وفي موازاة ما تقدم لا بد من التأكيد على حقيقة مهمة وهي ان معدل الاتصال بالإنترنت من مجتمعات واجهزة ذكية المنتشرة على كوكب الارض تفوق القدرة على تأمينها بالشكل الصحيح، فعندما تم اختراع شبكة الانترنت العالمية في العام 1989، كان اول محرك بحث فعال في العام 1991، في حين وصل عدد محركات البحث في العام 2019 إلى قرابة (9,1) مليار، ورافق ذلك ارتفاع كبير في عدد مستخدمين الانترنت من (2) مليار في العام 2015 إلى (4) مليار في العام 2018، ويتوقع ان يرتفع العدد إلى (6) مليار في العام 2022، كما اكدت التقارير المختصة بالأمن السيبراني ان العالم سيحتاج إلى حماية (300) مليار كلمة مرور على مستوى العالم في العام 2020، لا سيما وان المحتوى الرقمي في العالم ارتفع من (4) مليار تيرابايت في العام 2016 إلى (96) مليار تيرابايت بحلول العام 2020، وبناءً على هذه المؤشرات فإن جرائم الهجمات السيبرانية الحقت اضراراً غير مسبوقة بحق المؤسسات الخاصة والعامة، وزادت من الإنفاق على أمن تكنولوجيا المعلومات، وما يؤكد ذلك

ان الإنفاق العالمي على أمن المعلومات بلغ أكثر من (114) مليار دولار في العام 2018 بزيادة قدرها (4,12 %) عن العام 2017، وارتفع إلى (124) مليار دولار في العام 2019 أي بزيادة تقدر بـ(7,8 %)، فضلاً عما تقدم وصلت الفدية إلى أبعاد وبائية وهي أسرع الجرائم السيبرانية نموًا التي تحصل عن طريق برمجيات خبيثة تصيب أجهزة الكمبيوتر وتقيد وصولها إلى الملفات، وتهدد في كثير من الأحيان بتدمير دائم للبيانات ما لم يتم دفع فدية، وقد وصفت وزارة العدل الأمريكية الفدية بأنها إنموذج وظائف جديد للجريمة السيبرانية وظاهرة عالمية، ففي العام 2016 كان معدل من وقع ضحية الفدية كل (40) ثانية، وارتفع المعدل في العام 2019 إلى ضحية كل (14) ثانية، ومن المتوقع ان يصل هذا العدد إلى (11) ثانية بحلول العام 2021، وقد ترتب على ذلك ارتفاعًا ملحوظًا في تكاليف الأضرار الناجمة عن الفدية العالمية، إذ ارتفعت من (5) مليار دولار في العام 2017 إلى (5,11) مليار دولار في العام 2019، ومن المتوقع ان تصل إلى (20) مليار دولار في العام 2021، وعموما فإن تقارير الأمن السيبراني تتوقع ان تصل تكلفة الأضرار الناجمة عن جرائم الانترنت العالمية بـ(6) تريليون دولار سنويًا بحلول عام 2021، بعد ان كانت (3) تريليون دولار في العام 2015، مما يُعد أكبر تحويل للثروة الاقتصادية في التاريخ[45].

وبناءً على المؤشرات السابقة صنف تقرير المخاطر العالمية للعام 2020 حرب الجيل الخامس بانها أعلى الحروب خطرًا في العام 2020، بعد ان أثرت الهجمات السيبرانية على مدن بأكملها وشملت القطاعين العام والخاص على حدٍ سواء، وما زاد من خطورتها صعوبة كشفها وملاحقتها ففي أعلى دولة بالعالم على الصعيد التقني وهي الولايات المتحدة فإن قدرة ما كشف منها وملاحقته وصلت ما نسبته إلى (05,0 %)، فضلاً عن ذلك هناك أكثر من (21) مليار جهاز متصل بالإنترنت في جميع أنحاء العالم وعددها سيتضاعف بحلول العام 2025، يرافق ذلك ارتفاع نسبة الهجمات على الأجهزة المرتبطة بالإنترنت إلى أكثر من (300 %)، ومن المتوقع ان تصل تكلفة الأضرار الناجمة عن جرائم الانترنت العالمية إلى (6) تريليون دولار بحلول العام

2021[46]. بعد ان كانت (3) تريليون دولار في العام 2015، مما يُعد أكبر تحويل للثروة الاقتصادية في التاريخ[47].

مما تقدم يتضح بان الأمن السيبراني أصبح وثيق الصلة بالأمن الوطني لأية دولة، وتزداد الخطورة كلما زاد اعتماد الدولة على تقنية المعلومات وارتباطها بالفضاء السيبراني، ذلك ان الهجمات السيبرانية يمكن لها ان تقوض الأمن الوطني، فأية فجوة تقنية ستؤدي إلى خسائر كبيرة للدولة في مؤسساتها الرسمية ولمواطنيها، بل انه يعرض هيبة الدولة وسمعتها الدولية إلى الخطر، إذ لا تقف هذه الخسائر عند الجانب المادي فحسب بل ستؤثر مباشرة ايضا على الجانب المعنوي إذ ستلحق ضررًا في نفسية المواطنين وقادتهم، كونه يولد قناعة عامة بضعف قدرة الدولة على حماية المواطنين ومؤسساتها، وعليه يمكن القول ان الأمن السيبراني يعد قضية أمنية وطنية ضرورية يجب فهمها بعناية وشمولية.

المبحث الثالث

Third Section

الأمن الوطني العراقي في ظل تحديات الأمن السيبراني

Iraqi national security in light of cybersecurity challenges

تنطلق استراتيجية الأمن السيبراني العراقي، من مبدأ اساس هو ضمان امن العراق وحماية وجوده في الفضاء السيبراني، وحماية بنية معلوماته الحيوية، وبناء مجتمع انترنت، موثوق به ورعايته، والتعامل مع التحديات السيبرانية، التي تهدد امن العراق الوطني وسلامته، عن طريق تبني مجموعة من الاجراءات تعمل على حماية، فضاء العراق السيبراني والدفاع عنه[48].

وبدأ تسجيل إحصائيات رسمية عن الجرائم السيبرانية في العراق منذ العام 2006، بسبب الانتشار السريع للخدمات والعمليات عبر الإنترنت، فارتفعت معها نسبة جرائم الإنترنت والانشطة المضرة بالنظام والمجتمع العراقي، بل ان نسبة القرصنة السيبرانية في العراق هي الأعلى في الشرق الأوسط، وتنوعت حالات الجرائم السيبرانية في العراق منها: الغش عبر الإنترنت، وغسيل الأموال، وتزايد مواقع القرصنة، والتجارة السيبرانية غير المشروعة، والتطفل على الشبكات، والجنس، والإرهاب الإلكتروني، وعند الرجوع إلى سجلات مكتب التحقيقات،

الجنائية العراقية للأعوام، 2006 – 2011، والخاصة بالجرائم السيبرانية نلاحظ أن حالات جرائم الإنترنت في العراق زادت، خلال تلك السنوات، بمعدل سنوي متوسط، قدره (2,246 %)، فخلال هذه المدة شهد العراق نموًا سريعًا لمستخدمي الإنترنت، وزادت بالوقت ذاته الجرائم السيبرانية، وتم ارتكاب معظم هذه الجرائم من قبل حاملي شهادات الثانوية بنسبة (4,63 %)، وبالدرجة الثانية من قبل حاملي شهادات البكالوريوس بنسبة (8,27 %)، والباقي بنسبة (8,8 %)، وكانت السرقة أعلى نسبة حالات الجريمة السيبرانية مقارنةً بالحالات الأخرى، وقد شكل الشباب أعلى نسبة هذه الجرائم، فمن إجمالي هذه الجرائم ارتكبها أشخاص تقل أعمارهم عن (24) عامًا بنسبة (8,44 %)، وقد احتل الذكور النصيب الاوفر فمن بين جميع الجرائم السيبرانية في العراق ارتكب الذكور ما نسبته (1,81 %)، وهذا مؤشر واضح على ان برامج الحماية من الجرائم السيبرانية يجب ان تركز على فئة الشباب والمراهقين[49].

فضلاً عن ذلك ان سوق الانترنت في العراق غير منظم بصورة صحيحة وبشكل كامل، ويُعزى ذلك إلى طبيعة المرحلة الانتقالية التي مر بها العراق، والاوضاع الامنية مما أدى إلى تضرر كبير في بنية الانترنت التحتية مما دفع بالمشتركين إلى تنويع مصادر التجهيز بخدمة الانترنت[50].

والملاحظ ان العراق في مراحله الاولية فيما يتعلق بمواجهة الجريمة السيبرانية، فهذه الجريمة ليست من اهتمامات المجتمع العراقي الرئيسة، علمًا ان وزارة التخطيط العراقية أعلنت انه في العام 2013 كان الجزء الرئيس من الجرائم السيبرانية المرتكبة قد استعملت مواقع التواصل الاجتماعي وفي مقدمتها الفيس بوك، وشملت هذه الجرائم الاختطاف والتهديد واختراق المعلومات الشخصية والمخدرات والاحتيال وغيرها، وتم القبض على بعض الأشخاص الذين ارتكبوا جرائم الإنترنت[51].

وجدير بالذكر انه بالتزامن مع الحرب على تنظيم داعش الارهابي منذ العام 2014 رصدت شركات امنية مختصة بالأمن السيبراني ان هناك حربًا سيبرانية في العراق يتم فيها استخدام وسائل التواصل الاجتماعي، لحشد المؤيدين ونشر الدعاية، ولجمع المعلومات، الامنية عن طريق مجموعة، من قراصنة الانترنت، الذين يعملون على خداع الناس بارسال رسائل تحوي

شفرات وبرامج ضارة عبر وسائل التواصل الاجتماعي، وما ان يتم فتحها حتى يبدأ المهاجمون على الفور بالتحكم الكامل بالجهاز، وسرقة الملفات أو استخدام كاميرة الكمبيوتر أو الميكروفون لمراقبة ما يجري للشخص المستهدف، وفي هذا الخصوص قال (أندرو كوماروف) الرئيس التنفيذي لشركة انتل كراولر (***Intel Crawler***) الامريكية المختصة في مكافحة التهديدات السيبرانية: "ان هناك بعض الجماعات في العراق تستخدم برامج ضارة، ومن الصعب التأكد من هويتهم، وقد استهدفوا بالفعل مدنًا وجماعات معينة وحتى عائلات معينة، أي ان كل الهجمات السيبرانية هي انتقائية للغاية وتتأثر في معظمها بالأطراف المحلية المتصارعة، واضاف إن المهاجمين يستهدفون ضحاياهم باستخدام وسائل التواصل الاجتماعي، ويقومون أيضًا بالبحث عن أجهزة التوجيه في داخل العراق لتخريبها بأدواتهم الخاصة، وقد تركزت غالبية هذه الهجمات في بغداد والبصرة والموصل وأربيل، وكانت الغاية منها جمع المعلومات عن المظاهرات المحلية، والاحزاب، والاتصالات بين السكان المدنيين أو الحكومة والعكس بالعكس"، علماً ان شركة انتل كراولر(*Intel Crawler*) جمعت معلوماتها من مراقبتها، لنشاط الفضاء السيبراني العراقي وعبر الاتصالات الامنية في المنطقة[52].

وفي السياق ذاته افاد تقرير لشركة انتل كراولر (*Intel Crawler*) في العام **2014** ان هناك جهات فاعلة تتخذ من العراق مقراً لها وتشارك في أنشطة غير مشروعة مختلفة في الفضاء السيبراني تعمل كمرتزقة وقد زادت بشكل كبير، ولديها علاقات بجماعات اخرى في كل من مصر ولبنان وليبيا وإيران وسورية، فضلاً عن دور الجماعات الإسلامية المنتشرة في العديد من الدول[53].

وقد رصد محللي الأمن السيبراني قيام جماعات مرتبطة بمنظمات ارهابية ومنها تنظيم داعش الارهابي بشن هجمات عبر الإنترنت على العديد من دول العالم، وشملت الأهداف وسائل الإعلام والمؤسسات الحكومية والجامعات والشركات والمنظمات غير الحكومية، فكان ذلك سببًا في إثارة نقاش لدى المختصين في الدوائر الغربية حول سعي المنظمات الارهابية إلى شن ما وصفوه بأنه "جهاد سيبراني" ضد الغرب، وفي هذا الخصوص أصدر مكتب التحقيقات

الفيدرالي الامريكي (*FBI*) تحذيرًا في 7/نيسان/2015 أكد فيه ان عمليات التشويش المستمر على محركات البحث يتم ارتكابها من قبل أفراد متعاطفين مع تنظيم داعش الارهابي، وقد أثرت هذه العمليات في محركات البحث ومنصات التواصل الخاصة بالمؤسسات الإخبارية والشركات التجارية والمؤسسات الدينية والحكومات الفيدرالية والمحلية في العديد من الدول الغربية، والى جانب الاضرار التي خلفتها فإن إزالة اثارها تكون مكلفة[54].

علمًا ان الحرب السيبرانية ضد تنظيم داعش الارهابي كانت بمثابة الاختبار العملي في المستقبل للحرب السيبرانية ضد الجماعات الإرهابية والحركات المتطرفة والعنيفة والمتمردين والعصابات الإجرامية العابرة للحدود الوطنية، إذ برز في هذه الحرب دور الهجمات السيبرانية في احباط العمليات الارهابية [55].

وفي الواقع ان التهديدات السيبرانية تمثل تحديات غير مرئية تؤثر في منظومة الأمن الوطني العراقي، فمع الانفتاح على العالم والتطور التكنولوجي الذي شهده العراق لاسيما في مجال الاتصالات والمعلومات لكن بالوقت ذاته يعاني العراق من ضعف في البنية التحتية الخاصة بالحماية الالكترونية من الهجمات السيبرانية مما جعل العراق مكشوفاً لدى الكثير من دول العالم لاختراقه والتجسس عليه لاسيما المتعلقة منها بالمؤسسات الامنية[56]. ولأجل ذلك عمل العراق مع شركائه الدوليين في مجال تطوير الأمن السيبراني للإفادة من خبراتهم، وفي هذا الخصوص قامت الحكومة العراقية بالتنسيق مع حلف شمال الاطلسي (الناتو) على تدريب (16) موظفاً من فريق الاستجابة للأحداث السيبرانية للمدة من 21 تشرين الثاني ولغاية 2/كانون الأول/2016 [57]. وتضمن البرنامج التدريبي جلسات نظرية ومختبرية عملية عن أساسيات الدفاع السيبراني، وحماية البيانات من التسرب، وتحليل الشفرات، والادلة الالكترونية، ورفع مستوى الخبرة التقنية لحماية الشبكة الوطنية، وزيادة الوعي بالأمن السيبراني، وستعمل هذه الدورات على تعزيز قدرات الدفاع السيبراني الوطنية العراقية [58].

وجدير بالذكر ان العراق احتل المرتبة (158) على الصعيد العالمي استنادًا إلى مؤشر الأمن السيبراني العالمي للعام 2017 (*Global Cybersecurity Index - GCI*) الصادر

من الاتحاد الدولي للاتصالات التابع إلى الأمم المتحدة كونه الوكالة المختصة في مجال تكنولوجيا المعلومات والاتصالات[59]. وفي العام 2018 احتل العراق وفق مؤشر الأمن السيبراني العالمي للعام 2018 المرتبة (107) على الصعيد العالمي من أصل (175) دولة شملها التقرير، والمرتبة (13) على صعيد الدول العربية [60]. وهذا يعني ان الأمن السيبراني في تطور ايجابي وهذه دلالة على نجاح القائمين عليه.

ولا بد من الاشارة إلى ان اجمالي خطوط خدمة الانترنت في العراق سواء المرتبطة بالهاتف النقال او اللاسلكي بلغت (15,297,411) في العام 2018[61]. وهذا مؤشر واضح على مدى الاستعمال الواسع لشبكات الانترنت في العراق، لا سيما اذا اخذنا بعين الاعتبار ان حجم سكان العراق قد بلغ قرابة (40) مليون انسان.

وبهدف تطوير استراتيجية العراق للأمن السيبراني انعقد في العاصمة العراقية بغداد في 5/اذار/2019 مؤتمر "العراق الإلكتروني والأمن السيبراني" بالتعاون مع المجلس الدولي للاستشارة الالكترونية (EC-Council) التابع لمفوضية الاتحاد الاوربي كونه المعني بمتابعة قضايا الأمن السيبراني وله دوره العالمي في هذا المجال، وكان الهدف منه تحديث وابتكار عمليات الأمن السيبراني الاستراتيجية والتكتيكية للحكومة العراقية، ومستقبل الحكومة الالكترونية، والتهديدات السيبرانية التي يتعرض لها العراق وسبل الدفاع السيبراني عنها، وزيادة الوعي لمنع الجريمة السيبرانية في العراق، فضلاً عن حماية البيانات، والتعامل مع الحوادث السيبرانية، واستعادة القدرة السيبرانية على العمل بعد الحوادث، ودور (EC-Council) في تقديم الدعم للعراق، ويأتي هذا المؤتمر في سياق خطط الحكومة العراقية للاستثمار في الحكومة الالكترونية، وتعزيز الأمن السيبراني العراقي[62].

وفي سياق التحديات السيبرانية تعرض العراق في 26و27/ايلول/2019 إلى هجوم سيبراني من قبل قراصنة طالت قرابة (30) موقعًا حكوميًا، أبرزها مواقع وزارة الدفاع والداخلية والخارجية والامن الوطني والصحة، وقد استغل المهاجمون بعض الثغرات فعملوا على تطبيق التغييرات على بيانات موقع البحث التي من شأنها توجيه المستخدمين إلى صفحة بحث مختلفة،

وعلى الرغم ان الجهات الحكومية نجحت في استعادة سريعة لبعض المواقع إلا ان بعضها أستغرق وقتًا أطول[63]. علمًا ان المهاجمين تمكنوا من الدخول إلى أجهزة الحواسيب الحكومية واختراق قاعدة البيانات التي من المفروض ان تكون محمية بشكل جيد مما سمح لهم بأخذ معلومات كثيرة، وقد حذرت لجنة الأمن البرلمانية من خطورة مثل هذا الاختراق مستقبلاً كونه سيؤدي إلى تسريب معلومات أمنية مهمة وحساسة[64].

وعمومًا يمكن تحديد أهم المشكلات التي يعاني منها الأمن السيبراني وشبكات الانترنت في العراق وسبل معالجتها بالآتي[65]:

1- ضعف القوانين والتشريعات الحكومية الخاصة بالأمن المعلوماتي والسيبراني، مما يتطلب تبني تشريعات قانونية فعالة يتم تطبيقها على القطاع الحكومي والخاص، وهنا يأتي دور الحكومة في تنفيذ اجراءات امنية محددة في وزاراتها ومؤسساتها فضلاً عن القطاع الخاص مما يعزز الأمن المعلوماتي والسيبراني على حدٍ سواء في العراق.
2- ضعف القدرات المهنية المحلية وقلتها في مجال أمن المعلومات المتقدمة والامن السيبراني، وهذا يتطلب العمل الجاد على تدريب وتطوير كوادر مهنية محترفة في القطاع الحكومي والخاص تؤهلها على مواجهة التحديات السيبرانية.
3- ارتباط منظومات الانترنت في العراق بالخارج مما يعني ان الأمن السيبراني العراقي مرتبط بالنتيجة بدول وشركات خارجية، وهذا يتطلب من الحكومة العراقية انشاء شراكة فعالة مع شركات محلية لإقامة علاقات موثوق بها وفعالة لسد النقص في هذا المجال.
4- قلة إدراك الشركات المحلية في مجال تكنولوجيا المعلومات بحجم المخاطر الامنية المعاصرة، وهذا يتطلب تنمية الوعي لديهم بان التحديات الامنية المعاصرة تختلف عن المرحلة السابقة، مما يستلزم البحث عن حلول جديدة مناسبة للتطورات الامنية المعاصرة، والابتعاد عن وسائل المعالجة التقليدية بهدف انشاء تكنولوجيا معلوماتية متقدمة في العراق تواكب التطور السريع.

الخاتمـــــــة

Conclusion

إن واقع عالمنا المعاصر يؤكد على حقيقة مهمة وهي الاعتماد المتزايد على تكنولوجيا المعلومات والاتصالات لتشمل معظم جوانب الحياة، مما فرض بدوره تحديًا سيكون حاضراً بقوة في القرن الحادي والعشرين ألا وهو ضرورة ضمان الأمن السيبراني من الهجمات السيبرانية، لا سيما وان هذه الهجمات غير مرئية ولكن في الوقت ذاته لها اثارها السلبية المرئية على الصعيد السياسي والاقتصادي والتكنولوجي والاجتماعي والثقافي، بل تكاد ان تكون مدمرة لاسيما اذا ما استهدفت البنية التحتية، ولهذا صُنفت الحرب السيبرانية بانها الجيل الخامس من تطور الحروب، واكثرها خطورة بحكم الضرر الكبير الذي يمكن أن تلحقه بقطاع واسع من المواطنين للدولة المُستهدفة، مما جعل القادة السياسيين امام عدو غير مرئي لكنه يتطلب في الوقت ذاته توفير كل الاستعدادات لمواجهته، وعليه فإن الغاية الاساسية من الأمن السيبراني هي تقليل المخاطر المتعلقة بالاعتماد على الفضاء السيبراني في ظل وجود تهديدات عدائية متنوعة وكثيرة وغامضة.

فضلاً عن ذلك كشف الأمن السيبراني عن حقيقة أخرى ألا وهي ان الناس هم أضعف حلقة في سلسلة الأمن السيبراني، ولذلك فانه يتطلب بناء ثقافة أمنية وزيادة الوعي بالمخاطر السيبرانية المعاصرة، وهذا بدوره يتطلب من الدول توعية شعوبها، وتبني استراتيجيات للأمن السيبراني ونظام أمني وقانوني مناسب يتم تطبيقه في المؤسسات الحكومية والقطاع الخاص، وبناء كوادر متقدمة في مجال التكنولوجيا والمعلوماتية والاتصال، وتخصيص مختبرات متقدمة لها تمكنها من التصدي بنجاح للتحديات السيبرانية المعاصرة.

وفيما يتعلق بالعراق فإن الانفتاح الذي شهده العراق لاسيما في المجال التقني والمعلوماتي، وتزايد الاعتماد عليه فرض عليه تحديات عدة، ونظرا لكون العراق مستهدف بالدرجة الاساسية من قبل التنظيمات الارهابية، فقد شهدت المؤسسات الرسمية وغير الرسمية خروقات وهجمات سيبرانية عدة، ومن هنا ظهرت تحديات أمنية معاصرة فرضت نفسها على العراق منها الارهاب

السيبراني والقرصنة السيبرانية والجريمة الالكترونية وغيرها، وهذا يتطلب بناء كوادر وطنية والاستفادة من المنظمات الدولية المختصة من أجل مواجهة هذه المخاطر.

الهـــوامـــش
Endnotes

(1) *Dan Craigen and Nadia Diakun-Thibault and Randy Purse, Defining Cybersecurity, Technology Innovation Management Review (Ottawa: Technology Innovation Management, October 2014), p.p. 13 – 14.*

(2) *North Atlantic Treaty Organization, Cybersecurity A Generic Reference curriculum, Brussels, 2016, p. 17.*

(3) *Rajesh Kumar Goutam, Importance of Cyber Security, International Journal of Computer Applications (New York: Foundation of Computer Science, Vol. 111, No. 7, February 2015), p. 14.*

(4) *Hans de Bruijn and Marijn Janssen, Building cybersecurity awareness: The need for evidence-based framing strategies, Government Information Quarterly (Amsterdam: Elsevier, Vol. 34, Issue 1, January 2017), p.p. 1 – 2.*

(5) *Ibid, p. 4.*

(6) *Daniel Schatz and Rabih Bashroush and Julie Wall, Towards a More Representative, Definition of Cyber Security, Journal of Digital Forensics, Security and Law JDFSL (United State: Florida, the Association of Digital Forensics, Security and Law, Vol. 12, No. 2, 2017), p.p. 53 – 54.*

(7) **د. منى الأشقر جبور، الأمن السيبراني: التحديات ومستلزمات المواجهة (بيروت: جامعة الدول العربية، 2012)، ص 3.**

(8) *Daniel Schatz and Rabih Bashroush and Julie Wall, op. cit., p.p. 55, 56, 66.*

(9) **د. منى الأشقر جبور، مصدر سبق ذكره، ص 3.**

(10) **الاتحاد الدولي للاتصالات، الأمن في الاتصالات وتكنولوجيا المعلومات، جنيف، 2009، ص13.**

(11) *North Atlantic Treaty Organization, Cybersecurity A Generic Reference curriculum, op. cit., p. 17.*

(12) *Rajesh Kumar Goutam, op. cit., p. 14.*

(13) *Dan Craigen and Nadia Diakun-Thibault and Randy Purse, op. cit., p.p. 14 – 17.*

(14) *Jitendra Jain and Dr. Parashu Ram Pal, A Recent Study over Cyber Security and its Elements, International Journal of Advanced Research in Computer Science (India: Rajasthan, Janardan Rai Nagar Rajasthan Vidyapeeth, Vol. 8, No. 3, 2017), p. 791.*

(15) *Kouroush Jenab and Saeid Moslehpour, Cyber Security Management: A Review, Business Management Dynamics (London: Society for Business Management Dynamics, Vol.5, No.11, May 2016), p. 17.*

(16) *Rajesh Kumar Goutam, op. cit., p. 14.*

(17) *Tadas Limba and others, Cyber security management model for critical infrastructure, The International Journal Entrepreneurship and Sustainability Issues (European Union: Entrepreneurship and Sustainability Center, Vol. 4, No. 4, June 2017), p. 560.*

(18) *Nate Lord, What is Cyber Security? Definition, Best Practices & More, Guardian, 15 July 2019.*

https://digitalguardian.com/blog/what-cyber-security

(19) *Tadas Limba and others, op. cit., p.p. 561 – 563.*

(20) *Daniel Jardim Pardini and Astrid Maria Carneiro Heinisch and Fernando Silva Parreiras, cyber security governance and management for smart grids in Brazilian energy utilities, Journal of Information Systems and Technology Management – Jistem USP (Brasil: Sao Paulo, Universidade de Sao Paulo, Vol. 14, No. 3, 2017), p. 385.*

(21) *Tadas Limba and others, op. cit., p.p. 560 – 561.*

(22) **فهد سعيد، رسائل في حوكمة الأمن السيبراني، 2019.**

https://www.linkedin.com/

(23) **د. نجدت صبري، الاطار القانوني للأمن القومي دراسة تحليلية (عمان: دار دجلة، 2011)، ص ص 39 – 41.**

(24) **د. أحمد فريجة و لدمية فريجة، الأمن والتهديدات الأمنية في عالم ما بعد الحرب الباردة، دفاتر السياسة والقانون (الجزائر، جامعة بسكرة، العدد 14، 2016)، ص 159.**

(25) د. محفوظ رسول، أمن الطاقة في العلاقات الروسية – الاوروبية (عمان: مركز الكتاب الاكاديمي، 2018)، ص 14.

(26) سيد أحمد قوجيلي، تطور الدراسات الامنية ومعضلة التطبيق في العالم العربي، دراسات استراتيجية (ابو ظبي: مركز الامارات للدراسات والبحوث الاستراتيجية، العدد 169، 2012)، ص ص 10 – 12.

(27) جوهر الجموسي، الافتراضي والثورة مكانة الإنترنت في نشأة مجتمع مدني عربي (الدوحة: المركز العربي للأبحاث ودراسة السياسات، 2016)، ص ص 87 – 89.

(28) *Jerry Brito and Tate Watkins, Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy, Harvard National Security Journal (United States: Cambridge, Harvard Law School, Vol. 3, 2011), p. 40.*

(29) *László KOVÁCS, National Cyber Security as the Cornerstone of National Security, Land Forces Academy Review (Romania: Sibiu, Nicolae Balcescu Land Forces Academy, Vol. 23, No. 2, 2018), p.p. 113 – 116.*

(30) للمزيد ينظر الاتحاد الدولي للاتصالات، تأمين شبكات المعلومات والاتصالات أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني: المسألة 1 – 22، (جنيف: 2014)، ص ص 24 – 26.

(31) للمزيد ينظر الاتحاد الدولي للاتصالات، دليل لوضع استراتيجية وطنية للأمن السيبراني: التزام استراتيجي بالأمن السيبراني، (جنيف: 2018)، ص ص 36 – 50.

(32) *Kenneth Geers, Strategic Cyber Security (Estonia: Tallinn, NATO Cooperative Cyber Defence Centre of Excellence, 2011), p. 9.*

* يقصد به حجم المعلومات والبيانات المرسلة في مدة زمنية معينة وكيفية التعامل معها عن طريق اتصال معين.

(33) *Ibid, p.p. 10 – 11.*

(34) *Ibid, p.p. 12 – 15.*

(35) *Jose Nazario, Politically Motivated Denial of Service Attacks, Cryptology and Information Security Series (Amsterdam: IOS Press, Vol. 3, 2009), p. 164.*

(36) *Check Point Software Technologies Ltd, 5th generation cyber attacks are here and most businesses Are Behind A New Model For Assessing and Planning Security, United States, 2018, p. 15.*

(37) *Hans de Bruijn and Marijn Janssen, op. cit., p.p. 4 – 6.*

(38) *Global Cybersecurity Index 2017 (Geneva: International Telecommunication Union, 2017), p. 1.*

(39) *Darius Štitilis and others, A model for the national cyber security strategy The Lithuanian case, Journal of Security and Sustainability Issues (Lithuania: Vilnius, Entrepreneurship and Sustainability Center, Vol. 6, No. 3, 2017 March), p.p. 357 – 358.*

(40) *Eric A. Fischer, Cybersecurity Issues and Challenges: In Brief, Report for Congress (Washington: Library of Congress, Congressional Research Service, No. R43831, August 2016), p. 3.*

(41) *Martha Finnemore and Duncan B. Hollis, Constructing Norms for Global Cybersecurity, The American Journal of International Law (Washington: American Society of International Law, Vol. 110, No. 3, July 2016), p.p. 430, 463.*

(42) *Kelly Bissell and Larry Ponemon, The Cost of Cyber Crime (United States: Michigan, Ponemon Institute, 2019), p.p. 10, 19.*

(43) *Cyber Defense Magazine, Cyber Security Statistics for 2019, 2019. https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/*

(44) *Ana Bera, 83 Terrifying Cybercrime Statistics, 2019. https://safeatlast.co/blog/cybercrime-statistics/*

(45) *Cybercrime Magazine, Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021, 2019. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/*

(46) *The Global Risks Report 2020 (Geneva: The World Economic Forum, 2020), p. 63.*

(47) *Cybercrime Magazine, Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021, op. cit.*

(48) **استراتيجية الأمن السيبراني العراقي، مستشارية الأمن الوطني، امانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات، ص ص 2 – 4.**

(49) *Sattar J. Aboud, An Overview of Cybercrime in Iraq, The research bulletin jordan ACM (Jordan: Center of Innovations in Computing and Engineering Machinery, Vol. II, Issue II, April 2012), p.p. 31 – 34.*

(50) الاتحاد الدولي للاتصالات، اعتماد تكنولوجيا المعلومات والاتصالات وآفاقها في المنطقة العربية (جنيف: 2012)، ص 54.

(51) *Sattar J. Aboud, Cybercrime in Iraq, International Journal of Scientific & Engineering Research (United States: Vol. 5, Issue 3, March 2014), p.p. 422 – 424.*

(52) *Mark Ward, Iraq conflict breeds cyber-war among rival factions, BBC News, 22 July 2014.*
https://www.bbc.com/news/technology-28418951

(53) *Nazan Osman, Cyberwarfare on the increase in Iraq, 2014.*
https://www.scmagazineuk.com/cyberwarfare-increase-iraq/article/1481055

(54) *Marco Macori, The Threat of Cyber Terrorism – A Risk Management Perspective, In book Cyber Security Policies and Critical Infrastructure Protection (Germany: Potsdam, Institute for Security and Safety, 2018), p. 232.*

(55) *Dr. Chris Bronk and Gregory S. Anderson, Encounter Battle: Engaging ISIL in Cyberspace, The Cyber Defense Review (New York: United States Military Academy West Point, Army Cyber Institute, Vol. 2, No. 1, Winter 2017), p. 105.*

(56) علي زياد العلي، التحديات غير المرئية للأمن الوطني العراقي، مركز البيان للدراسات والتخطيط، 2018*http://www.bayancenter.org/2018/06/4565/*.

(57) فريق الإستجابة للأحداث السبرانية، حلف الناتو يدرب خبراء عراقيين في مجال الدفاع السبراني، 2016*https://cert.gov.iq/library/events/6*.

(58) *Iraq Business News, NATO trains Iraqi Experts in Cyber Defence, United Kingdom, 12th December 2016.*
https://www.iraq-businessnews.com/2016/12/12/nato-trains-iraqi-experts-in-cyber-defence/

(59) *Global Cybersecurity Index 2017, op. cit., p. 64.*

(60) *Global Cybersecurity Index 2018 (Geneva: International Telecommunication Union, 2018), p. 58.*

(61) جمهورية العراق، وزارة التخطيط، إحصاءات الاتصالات والبريد لسنة 2018 (بغداد: الجهاز المركزي للاحصاء، 2019)، ص 17.

(62) *EC-Council, EC-Council Sponsors e-Iraq and Cybersecurity Event, 2019.*
https://blog.eccouncil.org/ec-council-sponsors-e-iraq-and-cybersecurity-event/
(63) *John J. Catherine, Iraq government websites hacked in 'largest operation' yet, 2019.*
https://www.kurdistan24.net/en/news/018ebfb3-1c36-4f5a-81d8-798da19ed435
(64) **صحيفة العربي الجديد، تحقيقات عراقية مكثّفة بعد هجوم إلكتروني على 30 موقعاً حكومياً، 29 ايلول 2019.**
(65) *Farook Al-Jibouri, Iraq Cyber Security Overview, and announcing our Cyber Security Framework, LinkedIn Corporation, 2016.*
https://www.linkedin.com/pulse/iraq-cyber-security-overview-announcing-our-framework-al-jibouri/

المصـــــــادر

References

المصادر باللغة العربية:

أولاً : الوثائق:

استراتيجية الأمن السيبراني العراقي، مستشارية الأمن الوطني، امانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات.

ثانياً : الكتب:

I. **جوهر الجموسي، الافتراضي والثورة مكانة الإنترنت في نشأة مجتمع مدني عربي (الدوحة: المركز العربي للأبحاث ودراسة السياسات، 2016).**

II. **د. محفوظ رسول، أمن الطاقة في العلاقات الروسية – الاوروبية (عمان: مركز الكتاب الاكاديمي، 2018).**

III. **د. منى الأشقر جبور، الأمن السيبراني: التحديات ومستلزمات المواجهة (بيروت: جامعة الدول العربية، 2012).**

IV. **د. نجدت صبري، الاطار القانوني للأمن القومي دراسة تحليلية (عمان: دار دجلة، 2011).**

ثالثاً : البحوث والدراسات:

I. **أحمد فريجة و لدمية فريجة، الأمن والتهديدات الأمنية في عالم ما بعد الحرب الباردة، دفاتر السياسة والقانون (الجزائر، جامعة بسكرة، العدد 14، 2016). د.**

II. **سيد أحمد قوجيلي، تطور الدراسات الامنية ومعضلة التطبيق في العالم العربي، دراسات استراتيجية (ابو ظبي: مركز الامارات للدراسات والبحوث الاستراتيجية، العدد 169، 2012).**

رابعاً : التقارير:

I. **الاتحاد الدولي للاتصالات، اعتماد تكنولوجيا المعلومات والاتصالات وآفاقها في المنطقة العربية (جنيف: 2012).**

II. **الاتحاد الدولي للاتصالات، الأمن في الاتصالات وتكنولوجيا المعلومات، جنيف، 2009.**

III. **الاتحاد الدولي للاتصالات، تأمين شبكات المعلومات والاتصالات أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني: المسألة 1 – 22، (جنيف: 2014).**

IV. الاتحاد الدولي للاتصالات، دليل لوضع استراتيجية وطنية للأمن السيبراني: التزام استراتيجي بالأمن السيبراني، (جنيف: 2018).

V. جمهورية العراق، وزارة التخطيط، إحصاءات الاتصالات والبريد لسنة 2018 (بغداد: الجهاز المركزي للاحصاء، 2019).

خامساً : الانترنت:

I. علي زياد العلي، التحديات غير المرئية للأمن الوطني العراقي، مركز البيان للدراسات والتخطيط، 2018. *http://www.bayancenter.org/2018/06/4565/*

II. فريق الإستجابة للأحداث السبرانية، حلف الناتو يدرب خبراء عراقيين في مجال الدفاع السبراني، 2016، *https://cert.gov.iq/library/events/6*

III. فهد سعيد، رسائل في حوكمة الأمن السيبراني، 2019.
https://www.linkedin.com/

سادساً : الصحف: Newspapers

I. صحيفة العربي الجديد، تحقيقات عراقية مكثّفة بعد هجوم إلكتروني على 30 موقعاً حكومياً، 29 ايلول 2019.

المصادر باللغة الانكليزية :

First- Books:

I. *Dan Craigen and Nadia Diakun-Thibault and Randy Purse, Defining Cybersecurity, Technology Innovation Management Review (Ottawa: Technology Innovation Management, October 2014).*

II. *Kenneth Geers, Strategic Cyber Security (Estonia: Tallinn, NATO Cooperative Cyber Defence Centre of Excellence, 2011).*

III. *Marco Macori, The Threat of Cyber Terrorism – A Risk Management Perspective, In book Cyber Security Policies and Critical Infrastructure Protection (Germany: Potsdam, Institute for Security and Safety, 2018).*

Second- Articles:

I. *Dr. Chris Bronk and Gregory S. Anderson, Encounter Battle: Engaging ISIL in Cyberspace, The Cyber Defense Review (New*

York: United States Military Academy West Point, Army Cyber Institute, Vol. 2, No. 1, Winter 2017).

II. *Daniel Jardim Pardini and Astrid Maria Carneiro Heinisch and Fernando Silva Parreiras, cyber security governance and management for smart grids in Brazilian energy utilities, Journal of Information Systems and Technology Management – Jistem USP (Brasil: Sao Paulo, Universidade de Sao Paulo, Vol. 14, No. 3, 2017).*

III. *Daniel Schatz and Rabih Bashroush and Julie Wall, Towards a More Representative, Definition of Cyber Security, Journal of Digital Forensics, Security and Law JDFSL (United State: Florida, the Association of Digital Forensics, Security and Law, Vol. 12, No. 2, 2017).*

IV. *Darius Štitilis and others, A model for the national cyber security strategy The Lithuanian case, Journal of Security and Sustainability Issues (Lithuania: Vilnius, Entrepreneurship and Sustainability Center, Vol. 6, No. 3, 2017 March).*

V. *Eric A. Fischer, Cybersecurity Issues and Challenges: In Brief, Report for Congress (Washington: Library of Congress, Congressional Research Service, No. R43831, August 2016).*

VI. *Hans de Bruijn and Marijn Janssen, Building cybersecurity awareness: The need for evidence-based framing strategies, Government Information Quarterly (Amsterdam: Elsevier, Vol. 34, Issue 1, January 2017).*

VII. *Jerry Brito and Tate Watkins, Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy, Harvard National Security Journal (United States: Cambridge, Harvard Law School, Vol. 3, 2011).*

VIII. *Jitendra Jain and Dr. Parashu Ram Pal, A Recent Study over Cyber Security and its Elements, International Journal of Advanced Research in Computer Science (India: Rajasthan, Janardan Rai Nagar Rajasthan Vidyapeeth, Vol. 8, No. 3, 2017).*

IX. *Jose Nazario, Politically Motivated Denial of Service Attacks, Cryptology and Information Security Series (Amsterdam: IOS Press, Vol. 3, 2009).*

X. *Kouroush Jenab and Saeid Moslehpour, Cyber Security Management: A Review, Business Management Dynamics (London: Society for Business Management Dynamics, Vol.5, No.11, May 2016).*

XI. *László KOVÁCS, National Cyber Security as the Cornerstone of National Security, Land Forces Academy Review (Romania: Sibiu, Nicolae Balcescu Land Forces Academy, Vol. 23, No. 2, 2018).*

XII. *Martha Finnemore and Duncan B. Hollis, Constructing Norms for Global Cybersecurity, The American Journal of International Law (Washington: American Society of International Law, Vol. 110, No. 3, July 2016).*

XIII. *Rajesh Kumar Goutam, Importance of Cyber Security, International Journal of Computer Applications (New York: Foundation of Computer Science, Vol. 111, No. 7, February 2015).*

XIV. *Sattar J. Aboud, An Overview of Cybercrime in Iraq, The research bulletin jordan ACM (Jordan: Center of Innovations in Computing and Engineering Machinery, Vol. II, Issue II, April 2012).*

XV. *Sattar J. Aboud, Cybercrime in Iraq, International Journal of Scientific & Engineering Research (United States: Vol. 5, Issue 3, March 2014).*

XVI. *Tadas Limba and others, Cyber security management model for critical infrastructure, The International Journal Entrepreneurship and Sustainability Issues (European Union: Entrepreneurship and Sustainability Center, Vol. 4, No. 4, June 2017).*

Third – Reports:

I. *Check Point Software Technologies Ltd, 5th generation cyber attacks are here and most businesses Are Behind A New Model For Assessing and Planning Security, United States, 2018.*

II. *Global Cybersecurity Index 2017 (Geneva: International Telecommunication Union, 2017).*

III. *Global Cybersecurity Index 2018 (Geneva: International Telecommunication Union, 2018).*
IV. *North Atlantic Treaty Organization, Cybersecurity A Generic Reference curriculum, Brussels, 2016.*
V. *The Global Risks Report 2020 (Geneva: The World Economic Forum, 2020).*

Fourth - Internet:

I. *Ana Bera, 83 Terrifying Cybercrime Statistics, 2019. https://safeatlast.co/blog/cybercrime-statistics/*
II. *Cyber Defense Magazine, Cyber Security Statistics for 2019, 2019. https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/*
III. *EC-Council, EC-Council Sponsors e-Iraq and Cybersecurity Event, 2019. https://blog.eccouncil.org/ec-council-sponsors-e-iraq-and-cybersecurity-event/*
IV. *Farook Al-Jibouri, Iraq Cyber Security Overview, and announcing our Cyber Security Framework, LinkedIn Corporation, 2016. https://www.linkedin.com/pulse/iraq-cyber-security-overview-announcing-our-framework-al-jibouri/*
V. *Iraq Business News, NATO trains Iraqi Experts in Cyber Defence, United Kingdom, 12th December 2016. https://www.iraq-businessnews.com/2016/12/12/nato-trains-iraqi-experts-in-cyber-defence/*
VI. *John J. Catherine, Iraq government websites hacked in 'largest operation' yet, 2019. https://www.kurdistan24.net/en/news/018ebfb3-1c36-4f5a-81d8-798da19ed435*
VII. *Mark Ward, Iraq conflict breeds cyber-war among rival factions, BBC News, 22 July 2014. https://www.bbc.com/news/technology-28418951*

VIII. *Cybercrime Magazine, Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021, 2019. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/*

IX. *Nate Lord, What is Cyber Security? Definition, Best Practices & More, Guardian, 15 July 2019. https://digitalguardian.com/blog/what-cyber-security*

X. *Nazan Osman, Cyberwarfare on the increase in Iraq, 2014. https://www.scmagazineuk.com/cyberwarfare-increase-iraq/article/1481055*

Cyber Security and its Impact on the Iraqi National Security

Assistant Prof. Dr. Mustafa Ibrahim Salman
University of Baghdad – Center of Strategic and International Studies

Abstract

Cyber security is one of the most important issues in our contemporary life by virtue of its direct relationship with all areas of public life, including politics, economy, security, culture, etc. Most countries of the world depend on it in their official and non-official institutions especially in their infrastructure. Thus, caring for it and avoiding its weaknesses is one of the security priorities of all countries. The cyber war represents the fifth generation of the contemporary wars and it is the most dangerous of which because of the great damage it causes to the infrastructure of any country and the consequent direct impact on the lives of citizens.

Iraq, especially since 2003 due to openness to the world and the development in the technical and information field, has become more vulnerable to cyber-attacks.

Journal of Juridical and Political Science
Web: www.lawjur.uodiyala.edu.iq