مجلة العلوم الإنسانية والطبيعية
مجلة علمية محكمة (التصنيف: NSP)
معامل التأثير العربي للعام 2024 = 0.44

HNSJ Humanities & Natural Sciences Journal
ISSN: (e) 2709-0833
www.hnjournal.net

عنوان البحث

التحديات التي تواجه الأمن السيبراني

هيله عبد المجيد عبد الحافظ العودة[1]

[1] كلية الحقوق، الجامعة الإسلامية في لبنان.

HNSJ, 2025, 6(7); https://doi.org/10.53796/hnsj67/46

المعرف العلمي العربي للأبحاث: https://arsri.org/10000/67/46

تاريخ الاستقبال: 2025/06/07م تاريخ القبول: 2025/06/15م تاريخ النشر: 2025/07/01م

المستخلص

يُعد الأمن السيبراني أحد أهم التحديات العالمية في ظل الثورة الرقمية والتطور المتسارع لتقنيات المعلومات والاتصالات. فقد أدى الاعتماد المتزايد على الأنظمة الرقمية إلى بروز تهديدات سيبرانية متنامية تشمل الاختراقات، سرقة البيانات، الهجمات الخبيثة، والابتزاز الإلكتروني، وهو ما يضع الأفراد والمؤسسات والدول أمام مخاطر متصاعدة. تكمن أبرز هذه التحديات في تعقيد الهجمات الإلكترونية الحديثة وصعوبة اكتشافها والتصدي لها، إضافة إلى نقص الكفاءات البشرية المتخصصة في المجال، وضعف الوعي الأمني لدى المستخدمين، فضلاً عن التحديات القانونية والتنظيمية المرتبطة بالامتثال للمعايير المحلية والدولية. كما أظهر البحث أن التكنولوجيات الحديثة مثل الذكاء الاصطناعي وإنترنت الأشياء تمثل سلاحًا ذا حدين، فهي قادرة على تعزيز قدرات الحماية كما يمكن استغلالها لتطوير هجمات أكثر خطورة. توصلت الدراسة إلى أن مواجهة هذه التحديات تتطلب تبني استراتيجيات شاملة تتضمن تطوير البنية التحتية السيبرانية، تعزيز التشريعات المحلية والدولية، الاستثمار في تدريب وتأهيل الكوادر المتخصصة، إلى جانب نشر الوعي المجتمعي بأهمية الأمن السيبراني كجزء من الأمن القومي في القرن الحادي والعشرين.

الكلمات المفتاحية: الأمن السيبراني، الهجمات الإلكترونية، الذكاء الاصطناعي، إنترنت الأشياء، التشريعات السيبرانية.

RESEARCH TITLE

Challenges Facing Cybersecurity

Abstract

Cybersecurity has emerged as one of the most pressing global challenges in the era of the digital revolution and the rapid advancement of information and communication technologies. The growing reliance on digital systems has led to escalating cyber threats, including intrusions, data theft, malicious attacks, and electronic extortion, exposing individuals, organizations, and states to increasing risks. Among the most significant challenges are the complexity of modern cyberattacks and the difficulty of detecting and countering them, the shortage of qualified professionals in the field, and the lack of sufficient security awareness among users. In addition, legal and regulatory challenges remain concerning compliance with national and international data protection standards. The study further highlights that emerging technologies such as artificial intelligence and the Internet of Things constitute a double-edged sword: while they can strengthen defensive capabilities, they can also be exploited to develop more advanced and dangerous attacks. The research concludes that addressing these challenges requires comprehensive strategies that include strengthening cybersecurity infrastructure, enhancing local and international legislation, investing in training and capacity-building for specialized personnel, and raising societal awareness of the importance of cybersecurity as a key component of national security in the twenty-first century.

Key Words: Cybersecurity, Cyberattacks, Artificial Intelligence, Internet of Things, Cyber Legislation.

المقدمة

لقد أحدثت تكنولوجيا المعلومات والاتصالات ثورة عالمية في جميع جوانب الحياة، وعلى المستوى الاجتماعي كان لها تأثير كبير على سلوك المجتمع وهويته، فضلاً عن نشر آلية الشبكة بين المجموعات البشرية المتمثلة في وسائل التواصل الاجتماعي عبر أجهزة الكمبيوتر والهواتف المحمولة، وقد أدى ذلك إلى تغييرات كبيرة في الأسس الاجتماعية الرئيسية، مثل الحياة الخاصة، والثقافة، والإعلام، والاجتماعات، وإقامة العلاقات الاجتماعية.

أما على مستوى الاقتصاد العام، فقد أدى انتشار تكنولوجيا المعلومات والاتصالات إلى تسريع التحول نحو الاقتصاد الرقمي القائم على المعرفة، وهكذا دخل لنا العصر الرقمي، حيث أدت البرمجيات المبتكرة والتطبيقات الذكية إلى العديد من الانتصارات الإدارية وريادة الأعمال، فضلاً عن تبني التقدم التكنولوجي على نطاق واسع في القطاعات الاقتصادية الحيوية مثل الطاقة والسياحة والخدمات المصرفية والتمويل.

وفي ضوء ذلك، يمكن اعتبار تحدي الأمن السيبراني أكبر تحدي للأمن القومي في القرن الحادي والعشرين، نظراً لأن الأمن الحديث لا يشير إلى الجوانب العسكرية فحسب، بل يتتبع تطور جميع التهديدات والتحديات التي يمكن أن تشكل تهديداً، إضافة الى إنه لقد تم القضاء على فكرة الحدود الجيوسياسية والثقافية بين الدول بفضل تكنولوجيا المعلومات والاتصالات، مما يعرض السيادة الوطنية للخطر، ومن الأمثلة على ذلك قرصنة المواقع الحكومية الرسمية والتجسس على بيانات الاستخبارات الوطنية.

كما يبدو التحدي الفكري والثقافي أحد المداخل الرئيسية للتهديدات السيبرانية، حيث يتضح من الغزو الفكري لوسائل التواصل الاجتماعي، ونشر ثقافة العنف والحصرية، وتشجيع النشاط الإجرامي تحت ستار التعصب والطائفية، أو الدين، ذريعة للمحتوى الإلكتروني القائم على نشر المعرفة والتقديم الحضاري.

أولاً_ أهمية البحث:

يندرج موضوع البحث ضمن الدراسات الأمنية والإستراتيجية، التي برزت كحقل مركزي في العلاقات الدولية، خاصة بعد نهاية الحرب الباردة، وما عرفته من نقاشات جديدة لتوسيع مفهوم الأمن ليشمل قضايا ومجالات متعددة: سياسية، اقتصادية، اجتماعية، ثقافية، بيئية وسيبرانية.

ثانياً_ إشكالية البحث

تعد تكنولوجيا المعلومات والاتصالات أداة حيوية في التنمية الاقتصادية والاجتماعية للدول النامية، إلا أنها تواجه تحديات كبيرة في مجال الأمن السيبراني. فالتهديدات الإلكترونية تتزايد بشكل مستمر وتشمل الاختراقات والاختراقات الضارة وسرقة البيانات والتجسس الإلكتروني والهجمات الإلكترونية الضارة والاحتيال الإلكتروني والابتزاز الإلكتروني والاستخدام غير المشروع لتكنولوجيا المعلومات والاتصالات. الأمر الذي يثير لدينا الإشكالية المركزية التالية:

ما مدى قدرة التشريعات المحلية في الدول النامية على الإحاطة بالجريمة السيبرانية والتعويضات التي وضعتها في ضمان الحقوق هل تعتبر كافية؟

ثالثاً_ منهج البحث:

لمعالجة الإشكالية الرئيسة التي تم ذكرها أعلاه قمنا باتباع المنهج التحليلي: في معالجة إشكالية البحث من خلال تحليل النصوص القانونية الخاصة بالطبيعة الدولية لجرائم الارهاب السيبرانية العابرة للحدود، وبيان الدور الدولي في التعاون في

مواجهة هذه الجريمة، وكشف الممارسات الحقيقة والفعلية لمرتكبيها.

رابعاً_ خطة البحث

من أجل معالجة الإشكالية قمنا بتقسيم البحث إلى:

المبحث الأول/ نشأة الأمن السيبراني وتطوره.

المطلب الأول/ مفهوم الأمن السيبراني.

المطلب الثاني/ دور الأمن السيبراني.

المبحث الثالث/ تحديات الأمن السيبراني.

المطلب الأول/ التحديات على الصعيد الداخلي.

المطلب الثاني / التحديات على الصعيد الخارجي.

المبحث الأول

نشأة الأمن السيبراني وتطوره

لقد شهد العالم في السنوات الأخيرة سباق تسلح جديد وغير تقليدي، يقوم على إنشاء وتطوير برامج تكنولوجية متقدمة تستخدم لأغراض مختلفة في العالم الافتراضي الذي يسمى "الفضاء السيبراني". يشير الفضاء السيبراني أو الفضاء الإلكتروني إلى العالم الرقمي والإلكتروني الذي يمتد عبر خطوط وقنوات الاتصال المختلفة على الإنترنت. وهو مساحة ملموسة وغير ملموسة من جزء أو من مجموع الحواسيب، وشبكات المعلومات المحوسبة، وبرامج ومضامين، ومعطيات مرور ورقابة، والذين يستخدمون كل ذلك، يعرف أيضاً بأنه مجال يتميز باستخدام الإلكترونيات والطيف الكهرومغناطيسي لحفظ البيانات وتعديلها وتبادلها بواسطة أنظمة الشبكة والبنية التحتية المرتبطة بها [1].

وللفضاء السيبراني خصائص عديدة في نطاق الحروب والنزاعات تستطيع الدولة أو الأفراد من خلالها من توجيه هجمات بسرعة عالية ضد الأعداء المتواجدين على مسافات طويلة جداً دون تعريضهم للخطر، حيث تتميز الهجمات الموجهة من خلال هذا الفضاء الافتراضي بالصمت، والتكلفة المنخفضة، وسرعة الأداء، تأثير القوة، صعوبة معرفة هوية المهاجم وخلفيته الأيديولوجية وغيرها من الصفات التي تجعل هذه الهجمات خطيرة للغاية.

إن توجيه الهجمات عبر هذا الفضاء لا يحتاج الى كميات هائلة من المعدات والموارد، بل كل ما تحتاجه هو شخص لديه معرفة ودراية كافية في أحداث الضرر والأذى في الأنظمة عبر التسلل الى الأجهزة البعيدة من بواسطة استخدام الفضاء السيبراني، كما أن توجيه الهجمات عبر هذا الفضاء قد تتفوق على المعارك والحروب التقليدية من حيث الخسائر المادية والأضرار التي تترك أثرها على الدول والمجتمعات. **لاستيضاح ما سبق ذكره، سنقوم بتقسيم هذا المبحث إلى** مطلبين، سوف نتحدث في **المطلب الأول عن مفهوم الأمن السيبراني**، أما في **المطلب الثاني سوف نتحدث عن دور الأمن السيبراني**.

[1] خالد وليد محمود، الهجمات عبر الانترنت، ساحة الصراع الالكتروني، المركز العربي للأبحاث ودراسة السياسات، قطر، 2013، ص 4.

المطلب الأول

مفهوم الأمن السيبراني

تطلق كلمة "سيبراني": على كل ما يتعلق بالشبكات الإلكترونية الحاسوبية، وشبكة، الإنترنت، والفضاء السيبراني يعني الفضاء الإلكتروني((Cyberspace)) وهو يعني كل ما يتعلق بشبكات الحاسوب، والإنترنت، والتطبيقات المختلفة (كالواتساب، والفيس بوك، وغيرها من مئات التطبيقات)، وكل الخدمات التي تقوم بتنفيذها (كتحويل الأموال عبر النت، والشراء أون لاين، وغيرها من آلاف الخدمات في جميع مجالات الحياة على مستوى العالم).[2]

وعليه، يقصد بالأمن السيبراني" Cyber Security " حماية الأشياء من خلال تكنولوجيا المعلومات مثل الأجهزة والبرمجيات ويشار إليها" ICT " وذلك اختصار Information and Communication Technologies، والقول بالأمن السيبراني يعني اتخاذ التدابير اللازمة لحماية الفضاء السيبراني من الهجمات السيبرانية، وذلك من خلال مجموعة من الوسائل المستخدمة تقنيا وتنظيميا وإداريا في منع الوصول غير المشروع للمعلومات الإلكترونية ومنع استغلالها بطريقة غير قانونية ونظامية، وبذلك فإنه يهدف إلى الحفاظ على استمرارية الأنظمة والمعلومات المتوفرة بها، وحمايتها بكل خصوصية وسرية من خلال إتباع التدابير والإجراءات اللازمة لحماية البيانات[3].

هناك العديد من التعاريف التي قُدمت لمفهوم الأمن السيبراني اصطلاحاً، منها حيث يعرف بأنه" مجموعة من الإجراءات المتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة". أيضاً يمكن تعريفه أنه: "مجموع الأطر القانونية والتنظيمية والهياكل التنظيمية والوسائل التكنولوجية الوطنية والدولية التي تهدف إلى حماية الفضاء السيبراني الوطني كما تركز على حماية بيانات الأفراد ومؤسسات الدولة من الاستخدام غير المصرح به أو أي أذى يلحق بشبكة البيانات"[4]

وهذا ما ذهب إليه الكاتبان Neittaanmäki Pekka, Lehto Martti في كتابهما Cyber Security: Analytics, Technology and Automation حيث عرفا الأمن السيبراني أنه: "عبارة عن مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة."[5]

بينما عرفه (إدوارد أمورسو Amoroso Edward) بأنه": وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة".[6]

وفي التقرير الصادر عن الاتحاد الدولي للاتصالات حول اتجاهات الإصلاح في الاتصالات لعام 2010-2011 عرف الأمن السيبراني بأنه": مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات

---

[2] على زياد العلى، على حسين حميد، تكتيكات الحروب الحديثة: الأمن السيبراني والحروب المعززة والهجينة، العربي للنشر والتوزيع، القاهرة، 2023، ص 24.

[3] ايمن احمد الحديدي، الأمن السيبراني في ظل الانفجار المعرفي، ط1، دار اليازوردي للنشر والتوزيع، الأردن، 2022، ص 41.

[4] حازم محمد خليل، استغلال الفضاء السيبراني في الحروب غير التقليدية: دراسة في الوكالة السيبرانية والإرهاب السيبراني، المجلة العلمية لكلية الدراسات الاقتصادية والعلوم السياسية، المقالة 7، المجلد 8، العدد 15، بغداد، 2023، الصفحة 265-302.

[5] هبه جمال الدين، الأمن السيبراني والتحول في النظام الدولي، مجلة كلية الاقتصاد والعلوم السياسية المجلد 24، العدد 1 – الرقم المسلسل للعدد 94، يناير 2023، بغداد، ص189-230

[6] ماجد عزيز إسكندر، التوظيف السياسي للهجمات السيبرانيَّة ومخاطرها على الأمن القومي، ط1، مركز الأمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، 2023، ص 28.

لإدارة ا لمخاطر، وتدريبات وممارسات فضلى وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين".[7]

وقدمت وزارة الدفاع الأمريكية تعريفاً دقيقاً لمصطلح الأمن السيبراني فاعتبرته "جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية، من مختلف الجرائم: الهجمات، التخريب، التجسس والحوادث." في حين اعتبر الإعلان الأوروبي الأمن السيبراني أنه" قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات."[8]

ويعرف الأمن السيبراني بأنه "مجموعة من الوسائل التقنية والتكنولوجية والعمليات التي يتم استخدامها لحماية الشبكات والأجهزة والبرامج والبيانات ومن الهجمات أو التسلل الغير مسموح به ويعرف أيضا بأنه أمن تكنولوجيا المعلومات أو حماية المعلومات، كما يعرف أنه "النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصال كما يحد من الأضرار في حال حصول هجمات أو تهديدات سيبرانية ويعيد الوضع إلى ما كان عليه بأسرع وقت. [9]

وعرف 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 الحماية البيئة السيبرانية والمنظمة وأصول المستعمل"، ويقصد بالأصول هنا أجهزة الحاسوب ومستعمليه، وأنظمة 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 أشكال الهجوم السيبراني منها الفايروسات وأحصنة طروادة والديدان الإلكترونية والتجسس الإلكتروني وسرقة الهوية والهجمات والاحتيال عبر الأنترنت وغيرها، ونظرا لكثرتها وتنوعها فإن هناك حاجة ضرورية لمواجهتها عن طريق توسيع قاعدة المعرفة لتأمين الشبكات منها ومن أبرز وسائل الحماية هي: التدقيق والمراقبة والحوسبة الأمنة وبرامج الحماية من الفايروسات وأنظمة كشف الاختراق والحماية منه والجدران الواقية، وعليه فإن من الضروري اتباع أسلوب امني متعدد الطبقات بحيث يكون الأمن شامل كل أجزاء النظام الإلكتروني من أنظمة وشبكات وتطبيقات، لاسيما وان الأمن السيبراني هو عملية مستمرة ولا يوجد نظام أمني واحد ينطبق على الجميع، وتشمل تقنيات الأمن السيبراني التشفير وضوابط النفاذ وسلامة النظام والتدقيق والإدارة والرصد والمراقبة[10].

من خلال التعاريف السابقة يمكن معرفة جوانب الأمن السيبراني، حيث يمكن تقسيمهم إلى ثلاث هي حماية بيانات الأشخاص الإلكترونية؛ ومن خلالها حماية الشركات ومؤسسات الدولة وبياناتها وعملائها؛ ثم حماية الأمن القومي وسلامة المواطنين ورفاهيتهم وخصوصيتهم لا لاستخدام هذه البيانات بطرق غير شرعية أو ضد أصحابها [11].

والملاحظ يمكن إيجاز التعريفات التي أوردناه للأمن السيبراني والتي قد تعددت في تعريف خاص بنا بأنه: الأساليب

---

[7] أحمد مصطفى ناصف، دمج الأمن السيبراني في منظومة الأمن القومي: الأمن السيبراني والأمن القومي، إدارة الأعمال مجلة الأهرام، المجلد6، العدد 178، القاهرة، 2022، ص 48 – 55.

[8] عادل عبد الصادق، الإرهاب السيبراني والأمن القومي في بيئة متغيرة، مجلة السياسة الدولية، العدد 578، العدد227، القاهرة، 2022 ص 244 – 247.

[9] إسلام فوزي، الأمن السيبراني: الأبعاد الاجتماعية والقانونية: تحليل سوسيولوجيا، المجلة الاجتماعية القومية، المجلد56، عدد2، بغداد، 2019 ص 99 – 139.

[10] ينظر في تفصيل ذلك، تقرير الاتحاد الدولي للاتصالات، الأمن في الاتصالات وتكنولوجيا المعلومات، جنيف، 2009، ص13.

[11] محمد الصغير مسيكة، الفضاء السيبراني وتحديات الأمن القومي للدول، مجلة العلوم القانونية والاجتماعية، المجلد7، العدد4، 2022، بغداد، ص 447 – 462.

الدفاعية المستخدمة للكشف عن المتسللين المحتملين وإحباطهم، أو حماية شبكات الكمبيوتر والمعلومات التي تحتويها من الاختراق ومن الأضرار الخبيثة أو الاختلالات وعليه يمكن رؤية أن الأمن السيبراني مفهوم أوسع من أمن المعلومات، فالأمن السيبراني يهتم بأمن كل ما هو موجود على السايبر من غير أمن المعلومات، بينما أمن المعلومات لا يهتم بذلك، كما أن أمن المعلومات يهتم بأمن المعلومات الفيزيائية " الورقية"، بينما لا يهتم الأمن السيبراني بذلك. عليه يشكل الأمن السيبراني جزءا أساسيا من أي سياسة أمنية وطنية فقد أصبحت الدول تصنف مسائل الدفاع السيبراني كأولوية في سياساتها الدفاعية.

المطلب الثاني

دور الأمن السيبراني

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 أن 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 الإلكترونية 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 الآخر شديد التأثير والخطورة[12].

وتزداد أهمية الحاجة إلى الأمن السيبراني نظرا للاعتماد على تكنولوجيا المعلومات والاتصالات في جميع جوانب الحياة المجتمعية، حيث يعد 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 أيضاً الوزارات والمؤسسات الإدارية 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 أن العالم يعيش معركة مستمرة بين المتسللين والمدافعين عن حماية النظام العام، كما أن 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[13].

ولابد من الإشارة إلى أن الأمن السيبراني يتعلق بالناس والأنظمة على حد سواء، علمًا أن هذا التفاعل المعقد بينهما يتطلب معرفة عميقة بالأمن السيبراني والبنية التحتية لتكنولوجيا المعلومات وأنواع الهجمات الممكنة لفهم ما يجري، لا سيما وأن الناس يؤدون دورا في الحفاظ على الأنظمة وتحديثها للتأكد من جاهزيتها أمام الهجمات الإلكترونية كي يتم اكتشافها فورا واتخاذ التدابير ضدها، وهذا يتطلب المعرفة الضرورية بما هو مطلوب.

إن قلة المعرفة لدى المستخدمين يمكن أن تؤدي إلى حدوث ثغرات أمنية إضافية منها على سبيل المثال استعمال كلمات

---

[12] مصطفى ابراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 1، جامعة ديالى، العراق، 2021، ص 154.

[13] هانس بروجن وآخرون، بناء الوعي بالأمن السيبراني: الحاجة إلى استراتيجيات تأطير قائمة على الأدلة، مجلة السفير، المجلد.34، الإصدار 1، أمستردام، 2017، ص. 1-2.

مرور ضعيفة، وتثبيت برامج غير موثوقة واستخدام الأجهزة والتطبيقات غير الأمنة ومن ثم فإن الطبيعة الاجتماعية التقنية للأمن السيبراني تُعقد عملية إيجاد الحلول، فأغلب الناس تريد أن تكون آمنة فقط وتحميل الحكومة عبء المسؤولية، كما أن غالبية الناس تعتقد أن 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 أن تأثير بعض هذه الهجمات والتقنيات الجديدة غير واضحة مما يجعل من الصعب إظهار النجاحات والدعوة للاستثمار في تدابير الأمن السيبراني وفي الواقع إن الحكومات تواجه مهمة صعبة ذلك أنها 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[14].

وقد شاع مصطلح الأمن السيبراني في السنوات الأخيرة على نطاق واسع، وأخذ يحظى بشعبية متزايدة لاسيما بعدما استخدمه الرئيس الأمريكي "باراك أوباما" في العام 2009 في خطابه الذي دعا فيه الشعب الأمريكي إلى الاهتمام بالأمن السيبراني لتعزيز أمننا القومي[15].

كما عد التهديد القادم من الفضاء السيبراني من اكبر التحديات الأمنية والاقتصادية التي تواجه الولايات المتحدة، ولهذا جعله في مقدمة اهتماماته، وعين لهذا الغرض مسؤول عن الأمن السيبراني ويكون عضوا في مجلس الأمن القومي الأمريكي وان يكون على اتصال دائم به والتنسيق معه، ومن جانبه عد "جون مايكل ماكونيل" رئيس الاستخبارات الأمريكية (2007 – 2009) إن الإنترنت رفع بشكل غير مسبوق التحديات التي يتعرض لها النظام والأمن القومي الأمريكي التي يمكن أن تشمل مجالات سياسية وحيوية[16].

ويعتبر الأمن السيبراني وجها لإحدى وجوه واقع العلاقات الدولية المعاصرة والتي وضعت مفهوم الأمن الوطني أو القومي كمحرك لهذه العلاقات ومعياراً للسيادة الوطنية كما أصبح هاجسا لكافة الدول اعتبارا بهدفها الأسمى في حماية سلمها وأمنها والتزاما باحترامها للأمن والسلم الدوليين بالموازاة مع محاربة الجريمة الإلكترونية والاحتيال الإلكتروني وغيرها من المخاطر التي يأتي الأمن السيبراني على رأسها.

المبحث الثالث

تحديات الأمن السيبراني

تتزايد تحديات الأمن السيبراني مع تقدم التكنولوجيا، خاصة مع تطور الذكاء الاصطناعي. ويعزى ذلك إلى أن الذكاء الاصطناعي قد يسهم في تعزيز قدرات الهجمات السيبرانية وجعلها أكثر تطوراً وتعقيداً، في الوقت الذي يُمكن أن يُستخدم أيضاً في رفع إمكانات مواجهة تلك التهديدات من ناحية أخرى، كسلاح ذو حدين[17].

من الأوجه الإيجابية لتقنيات الذكاء الاصطناعي في التفاعل مع التهديدات السيبرانية المتقدمة أنه يمكن لتلك التقنيات –لا سيما تلك التي تتصل بتحليل البيانات– أن تسهم في اكتشاف الأنماط غير المعتادة والتصرفات المشبوهة في الشبكات السيبرانية، الأمر الذي يمكن أن يساعد في الكشف المبكر عن هجمات محتملة، كما أنه يمكن لتكنولوجيا الاستجابة

---

[14] هانس بروجن وآخرون، بناء الوعي بالأمن السيبراني، مرجع سابق، ص 4.

[15] دانيال شاتز وآخرون، تعريف الأمن السيبراني، مجلة الطب الشرعي الرقمي والأمن والقانون JDFSL، جمعية الطب الشرعي الرقمي والأمن والقانون، المجلد. 12، العدد 2، فلوريدا، 2017، ص 53.

[16] منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، مصر، 2009، ص 3.

[17] مقال منشور على موقع سكاي نيوز العربية، رابط الموقع، https://www.skynewsarabia.com/ تاريخ الزيارة، 1-11-2024.

التلقائية أن تكون فعالة في الحد من تأثير الهجمات السيبرانية، من خلال تطوير أنظمة تقوم بعزل الأنظمة المتضررة تلقائياً لمنع انتشار الهجمات[18].

ومع زيادة عدد الأجهزة المتصلة بالإنترنت (انترنت الأشياء)، يصبح أمان هذه الأجهزة أمراً بالغ الأهمية، وهنا يمكن استخدام تقنيات التشفير والتحقق الثنائي لضمان أمان التفاعل بين هذه الأجهزة والنظم السيبرانية الأخرى، ضمن الأوجه الإيجابية كذلك. كما يمكن باستخدام التحليل البياني تطوير نماذج تنبؤ متقدمة لتحديد الثغرات المحتملة في الأنظمة والتطبيقات.

وبالنظر لناحية الأوجه السلبية، فيمكن للمهاجمين استغلال الذكاء الاصطناعي لتطوير أساليب هجمات أكثر تطوراً وتعقيداً، كما يمكن أن يتيح لهم استخدام تقنيات التعلم الآلي لتحليل البيانات واكتشاف الثغرات والأنماط غير المألوفة في الأنظمة السيبرانية، وهذا يجعل من الصعب اكتشاف هذه الهجمات بسبب تعقيد الأساليب المستخدمة. **لاستيضاح ما سبق ذكره، سنقوم بتقسيم هذا المبحث إلى مطلبين، سوف نتحدث في المطلب الأول عن التحديات على الصعيد الداخلي، أما المطلب الثاني سوف نتحدث عن التحديات على الصعيد الخارجي.**

المطلب الأول

التحديات على الصعيد الداخلي

توجد العديد من التحديات لاتي تواجه الأمن السيبراني على الصعيد الداخلي ستناولهم على النحو الآتي:

أولاً: تطوير البنية الإدارية

ترتبط الثقة في الأمن السيبراني، بقدرة الأجهزة المعنية على ضبط الأمور، كما ترتبط بوضوح المسؤوليات، والمرجعيات المعنية بإقرار الحقوق وحمايتها، وبالقدرة على الردع والملاحقة لكل عمل جرمي، أو تصرف يعرض استقرار المعاملات، والأمن السيبراني. وتتطلب المكافحة الفاعلة أجهزة متخصصة، وعناصر تتميز بالكفاءة والقدرة على الإحاطة بجوانب كيفية إدارة أنظمة المعلومات وطرق معالجة البيانات، والحقوق المتصلة بها. وتعرف البنية التحتية على أنها مجموعة الوسائل والقدرات التي يتم تنسيقها عادة بواسطة منظمة مركزية للمعلومات يحددها القانون الدولي، يضاف إلى ذلك، ضرورة وجود مرجعية، تشرف على توثيق الحقوق، وإرساء قواعد متينة للثقة في العاملين في مجال معالجة المعلومات والأنظمة المتصلة بها، كما الحقوق الناشئة عنها، في سجلات خاصة ذات قيود موثوقة [19].

وعليه يمكن رؤية ضرورة إيجاد أجهزة إدارية متخصصة تتولى إعطاء شهادات خاصة للأشخاص الذين يتولون مراقبة المعلومات، وحفظها، ومعالجتها، كما تتولى تسجيلهم في سجلات خاصة، وتلزمهم بقواعد لحماية المعلومات والأنظمة فتشجيع الاستثمار، والإبداع، والاختراع، في أسواق العمل المتصلة بوسائل الاتصالات، يرتكز على تحديد واضح للحقوق والموجبات، كما على آليات محددة لحماية الحقوق الناشئة من هذا النشاط كما كان عليه الحال مع إقرار قوانين الملكية الفكرية، وحقوق المؤلف، والعلامات التجارية، والسجلات التي تثبت الملكية، في عصر ما قبل الإنترنت. وفي ذلك أيضًا، حفاظ على حقوق المستخدمين لاسيما حقهم في تطبيق القوانين المرعية الإجراء.

---

[18] جلال محمد الزغبي واسامة احمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية، مرجع سابق، ص98.

[19] بارام جيل، الحرب السيبرانية ومستقبل الصراع الإيراني الإسرائيلي، مجلة آفاق للأبحاث السياسية والقانونية، المجلد، 6، العدد59، الجزائر، 2020، ص 107 – 109.

ثانياً: الحفاظ على الخصوصية

يعتبر الحفاظ على الحق في الخصوصية من أساسيات تعزيز الثقة في الأمن السيبراني والافادة من طاقات تقنيات المعلومات والاتصالات على المستويات الاجتماعية والاقتصادية والثقافية فالتحديات الحالية التي تطرحها وسائل معالجة البيانات وجمعها، واستخدامها، واستثمارها لابد وأن تكون ذات انعكاسات سلبية على استخدام الإنترنت، ومروحة التقنيات المتصلة بها، سواء تجارياً، أو اجتماعياً، أو حكومياً، ولا بد للإطار التشريعية والتنظيمية، من أن تمكن المستخدمين من فهم حقيقة ما يجري من ممارسات تطال بياناتهم الشخصية، والمعلومات التي يضعونها على الإنترنت. كما لابد من تمكينهم من ممارسة حقوقهم في إدارتها، بالشكل الذي يؤدي إلى إمكانية الحفاظ على خصوصيتهم وعلى حقوقهم الفكرية، والصناعية والأدبية. وفي هذا المجال، يمكن للتشريعات الوطنية أن تسترشد بالقواعد الدولية، والمبادئ التي سبق إقرارها، على المستوى العالمي، كجزء من أساسيات المحافظة على نمو واستقرار، الأمن السيبراني. [20]

وعليه، إن الأمن السيبراني يعمل على الحفاظ على خصوصيتهم، وعلى حقوقهم الفكرية والصناعية والأدبية الإطار القانوني الذي يوفر حماية الحق في الخصوصية، والبيانات الشخصية والحريات الفردية، وبعض الفئات العمرية، كالأطفال والشباب، والملكية الفكرية.

ثالثاً: التحليلات الجيدة

يمكن لكل مؤسسة في كل صناعة الاستفادة من التحليلات الجيدة حيث انه من السهل أن تضع المؤسسة يدها على التهديد إذا قيمت المخاطر الخاصة بها، ولديها صورة تاريخية جيدة للمخاطر التي تعرضت لها في الماضي. عندما يكون لديها بيانات جيدة يمكن رؤية المخاطر بوضوح ومراقبة المواقف التي قد تشكل تهديداً والتحرك بسرعة عند وجود مشكلة. في الواقع يمكن أن تساعد البيانات الجيدة حتى بعد اختراق البيانات أو الهجوم عليها. [21]

رابعاً: الدفاع ضد التهديدات الداخلية

بينما تميل معظم تهديدات المنظمة إلى الظهور من الخارج إلا أن بعض التهديدات تأتي أحيانا من داخل المؤسسة نفسها، وفقاً لاستطلاع خرق بيانات الذي أجرته إيجريس تشعر 95٪ من الشركات بالقلق من حدوث خرق داخلي. لا يعني هذا بالضرورة أن هناك جهات فاعلة سيئة في الشركات؛ ففي معظم الأحيان تكون التهديدات الداخلية عن طريق الخطأ. على سبيل المثال التهيئة الخاطئة أو الحلول غير المعتمدة أو الاختيارات السيئة من قبل الموظفين. ومع ذلك في بعض الأحيان يتورط ممثل داخلي في نشاط ضار مثل التجسس أو السرقة. وجد الاستطلاع أيضا أن 61٪ من قادة تكنولوجيا المعلومات يعتقدون أن موظفيهم وضعوا بيانات الشركة الحساسة في خطر ضار في العام الماضي، ومهما كانت أسباب التعرض للمخاطر يجب أن تكون مميزات الأمن السيبراني الجيدة قادرة على التنبيه بسرعة إلى الأخطاء أو إساءة الاستخدام التي قد تعرض البيانات أو الشبكات للخطر. [22]

---

[20] عبد المنعم منيب، الحرب السيبرانية والصراع بين الدول، التقرير الاستراتيجي التاسع عشر الصادر عن مجلة البيان: ما بعد الإنسانية – العوالم الافتراضية وأثرها على الإنسان، الجزائر، 2022، ص 231 – 249.

[21] شريفة كلاع، الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، المجلد15، العدد1، الجزائر، 2022، ص 292 – 314.

[22] نورة شلوش، القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول، مجلة مركز بابل للدراسات الإنسانية، المجلد8، العدد2، بابل العراق، 2018، ص 185 – 206.

خامساً: إدارة المخاطر عبر النظام البيئي بأكمله

إن البائعون والشركاء والمقاولون هم مصدر مهم للمخاطر على الأعمال، وغالبا ما يكون لديهم إمكانية الوصول إلى البيانات والشبكات المؤسسية، ولكن ليس من الممكن دائما مطالبتهم بالالتزام بمعايير محددة أو أفضل الممارسات، وليس من المستغرب أن تكون الجهات الخارجية مصدراً كبيراً للمخاطر، حيث وجد تقرير بونيمون لعام 2019 أنه عندما تتسبب أطراف ثالثة في حدوث خرق تزداد التكلفة بأكثر من 370 ألف دولار ومع ذلك وفقاً لدراسة معيار إدارة مخاطر البائع لعام 2019 أيضا التي أجرتها شركة بروتيفيتي فإن 4 مؤسسات فقط من أصل 10 لديها عملية ناجحة تماما لإدارة مخاطر الموردين، وعليه يجب أن تتيح مميزات الأمن السيبراني مراقبة وإدارة المخاطر التي يشكلها البائعون، كما يجب أن تسمح هذه المميزات بمراقبة وإدارة المخاطر بغض النظر عن مكان حدوثها، خارج الشركة أو داخل المؤسسة أو في سلسلة التوريد أو غيرها.[23]

سادساً: الأمن وسلامة المعلومات في الأمن السيبراني

يهدف الأمن السيبراني إلى تعزيز حماية جميع ما يتعلق بالدولة إلكترونياً وأفراداً لحماية هذه الأنظمة الإلكترونية وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية وجميع مكوناتها المحيطة بالمجتمع من أجهزة وبرمجيات ومدات وجميع ما يؤثر على تقدم هذه الخدمات، وما تحويه من بيانات، فأصبحت هذه أيضاً من أهم الأولويات المهمة والحيوية لجميع دول العالم لأنهم يريدون أن يحافظوا على بيانات مواطنيهم وحفظ ممتلكاتهم وبياناتهم الإلكترونية، وأخذ كثير من الدول على عاتقها وخاصة الدولة المتقدمة في الكثير من الاهتمامات والاحتياطات والتعمق في هذا التخصص الذي يمس حياة مواطنيهم، فأنشأوا الكليات والمعاهد ومراكز البحوث حتى يتم معرفة كل شيء يقوم بتوفير الحماية لمواطنيهم ولمجتمعاتهم.[24]

المطلب الثاني

التحديات على الصعيد الخارجي

توجد على الصعيد الخارجي عدة تحديات للأمن السيبراني ستناولهم وفق الآتي:

أولاً: التعاون لتعزيز الأمن

في هذا المجال، لا بد من إيجاد الإطار التشريعي والتنظيمي الحاضن، الذي يشجع مبادرات التعاون، إلا إن استمرارية عمل تقنيات المعلومات والاتصالات، وفي مقدمها الإنترنت، كما استقرار الأمن السيبراني، وستعان سياسات المعالجة الثغرات الأمنية، ولمواجهة الأخطار والحد من آثار الأعمال الجرمية، وبالتالي لابد من دعم الجهود الآيلة إلى وضع معايير دولية، كما لا يد من دعم إقرار الأطر القانونية والتنظيمية والإفادة من أفضل الممارسات والتجارب الناجحة، التي تعزز الثقة في الأمن السيبراني، وتؤمن بيئة لنمو النشاط الاقتصادي، والاجتماعي في الأمن السيبراني. [25]

وفي هذا الإطار، يمكن رؤية أنه لابد من الابتعاد من السياسات التي تتعارض وطبيعة عمل الإنترنت المفتوحة، وإمكاناتها التي تشكل أرضية للإبداع، والنمو الاقتصادي والاجتماعي، بحيث لا تتحول هذه السياسات، إلى أدوات تحيق الانسياب الحر للمعلومات، والوصول اليها، تحت ذريعة تحقيق الأمن والحمارة على خط مواز، لابد لسياسات الأمن أن تعزز

---

[23] جيهان أحمد عبدالعال، الحروب السيبرانية دراسة في المفهوم والنشأة ومعادلات النجاح، المجلة العلمية للدراسات التجارية والبيئية، المجلد13، عدد2، 2022، القاهرة، ص 287 – 310.

[24] ضحى لعيبي كاظم السدخان، البعد الجيو سياسي للأمن السيبراني، مجلة العلوم الإنسانية، مجلد5، العدد1، بابل العراق، 2021، ص 188 – 233.

[25] أحمد جلال محمود، أثر التهديدات غير التقليدية للأمن على العلاقات الدولية المعاصرة: الأمن السيبراني في الشرق الأوسط حالة دراسة من 2010–2020، المؤتمر الدولي: مستقبل منطقة الشرق الأوسط – رؤية مصر 2030، 2020، ص 38 – 84.

المبادرات الفردية والجماعية العاملة على تحقيق الأمن والحماية.

فنجاح خطط الحماية والأمن السيبراني، يفرض ترابطاً وتكاملا بين استراتيجيات الأمن وسياساته، كما يفترض إمكانية وصول الجمهور اليها، ليس فقط على المستوى الوطني، وإنما على المستويين الإقليمي والعالمي أيضًا. كذلك، هنالك حاجة لمشاركة الجميع، في وضع الحلول، بحيث تأتي هذه الأخيرة ناجعة ومؤسسة لتفاهم اجتماعي وسياسي، بما يعزز فرص نجاحها وفعاليتها. كما انه لا بد لمتخذي القرار، أن يأخذوا مقترحات القطاعات المهنية، والاختصاصيين، والمجتمع المدني، وغيرهم، بعين الاعتبار، لدى صياغة التشريعات، ووضع الأطر التنظيمية. [26]

ثانياً: تعزيز وحماية الانسياب العالمي الحر للمعلومات

يرتكز اقتصاد الإنترنت، كما نموها، بشكل أساسي على الانسياب الحر للمعلومات. وإذا كانت الدول المختلفة، مدعوة إلى وضع سياسات تعزز هذا الانسياب، وتشجعه، وتدعمه، إلا أنها في المقابل، مدعوة إرضاء إلى تأمين الإطار القانوني الذي يوفر حماية الحق في الخصوصية والبيانات الشخصية والحريات الفردية، وبعض الفئات العمرية، كالأطفال والشباب، والملكية الفكرية. ومن هنا، ضرورة التفاتها إلى الأمن السيبراني، والعمل على إرساء قواعد ثابتة له. ويتصل انسياب المعلومات، بالطبيعة المفتوحة للإنترنت التي تتكل بدورها على اعتماد مقاييس ومعايير تقنية عالمية. وترد في هذا الإطار أيضا، سياسات المنافسة، والسوق المفتوح، والتنوع، والخدمات العابرة للحدود، التي تسمح بتأمين خدمات، بكلفة معقولة، تساهم في إتاحة الإنترنت للجميع.[27]

ويمكن رؤية إن الأمن السيبراني هو الإطار القانوني الذي يوفر حماية الحق في الخصوصية. والبيانات الشخصية، والتحريات الفردية، وبعض الفئات العمرية كالأطفال والشباب والملكية الفكرية.

ثالثاً: تغطية أكبر للتهديدات الخارجية

تأتي العديد من التهديدات من خارج المؤسسات أنفسها تميل هذه التهديدات الخارجية إلى أن تأخذ شكل القرصنة والتصيد الاحتيالي، كما تميل إلى الظهور في مؤسسة بعدة طرق، على سبيل المثال بيانات الاعتماد المسروقة، ورفض الخدمة، وتطبيقات الويب المخترقة، ومرفقات البريد الإلكتروني، 93٪ من رسائل البريد الإلكتروني العشوائية هي الآن أدوات لبرامج الفدية. يجب أن يكون النظام الأساسي الأمني قادراً على مراقبة التهديدات والإخبار عند تعرض المؤسسات والشركات للاختراق أو الاستهداف من خلال نشاط ضار. [28]

وعليه إن استقرار الأمن السيبراني، يستدعي سياسات لمعالجة الثغرات الأمنية، ومواجهة الأخطار والحد من آثار الأعمال الجرمية، إن الدول أصبحت ترتب أمورها لمواجهة حروب المستقبل التي تعتمد على التخريب والتدمير من خلال الأمن السيبراني، وهذا أصبح جزء من مكتبات واستراتيجيات الدول المتقدمة، لمواجهة هذه الحروب أو القيام بها، وأصبحت عمليات مقاومة هذه الحروب جزء لا يتجزأ من استراتيجيات الدفاع لدول كثيرة.

---

[26] لامية طالة، الإرهاب السيبراني والأمن القومي: قراءة في تحولات الاستراتيجية الدفاعية، المجلد35، العدد4، الجزائر، 2021، ص 353 – 366

[27] عبدالكريم اسماعيل، تأثير الفضاء الافتراضي علي الأمن القومي، مجلة البحوث والدراسات، المجلد19، العدد1، بغداد، 2022، ص 141 – 160.

[28] جيلالي شويرب، مفهوم الحروب السيبرانية والأمن السيبراني، مجلة الحقوق والحريات، المجلد11، العدد1، الجزائر، 2023، ص 157 – 178.

الخاتمة

الأمن السيبراني أصبح ضرورة ملحة في عالمنا الحديث مع الاعتماد المتزايد على التكنولوجيا والإنترنت في جميع مناحي الحياة. ومع تصاعد التهديدات الإلكترونية وتطور أساليب الهجوم، أصبحت الدول والمؤسسات والأفراد أكثر عرضة للمخاطر التي تهدد بياناتهم وأمنهم، ففي ظل هذه التحديات، من الضروري التحرك بشكل عاجل لتطوير استراتيجيات شاملة لحماية الفضاء السيبراني، وضمان استمرارية العمليات الحيوية، وحماية الخصوصية والبيانات الحساسة.

في نهاية البحث توصلنا الى العديد من الاستنتاجات والتوصيات التالية:

أولاً_ الاستنتاجات

1. تصاعد التهديدات السيبرانية: التطور المستمر في أساليب الهجوم الإلكتروني يجعل الأنظمة التقليدية غير كافية لحمايتها.
2. فجوة الوعي والمهارات من خلال ضعف الوعي الأمني لدى الأفراد والمؤسسات يمثل نقطة ضعف كبيرة يمكن للمهاجمين استغلالها.
3. نقص الكفاءات المؤهلة في مجال الأمن السيبراني يزيد من تعقيد التصدي للهجمات.
4. تعقيد التكنولوجيات الحديثة حيث إن الانتشار الواسع لتقنيات مثل إنترنت الأشياء والذكاء الاصطناعي والحوسبة السحابية أدى إلى زيادة مساحة الهجمات المحتملة.

ثانياً_ التوصيات

1. تعزيز الوعي والتثقيف الأمني من خلال إطلاق حملات توعية تستهدف الأفراد والشركات لرفع مستوى المعرفة بممارسات الأمن السيبراني، وإدراج برامج تدريبية في المدارس والجامعات لتأهيل جيل واعٍ بالتهديدات السيبرانية.
2. تطوير البنية التحتية السيبرانية من خلال الاستثمار في أنظمة حماية متقدمة تعتمد على الذكاء الاصطناعي لتحليل ورصد الهجمات، وتأمين البنية التحتية الحيوية مثل شبكات الطاقة والمستشفيات ضد الهجمات الإلكترونية.
3. تعزيز القوانين والتشريعات من خلال تحديث القوانين الوطنية لمواكبة التطورات التكنولوجية وضمان الحماية القانونية لضحايا الجرائم السيبرانية، ودعم التعاون الدولي لوضع إطار قانوني شامل لمكافحة الجرائم الإلكترونية العابرة للحدود.

قائمة المصادر والمراجع

أولاً_ الكتب

1. خالد وليد محمود، الهجمات عبر الانترنت، ساحة الصراع الالكتروني، المركز العربي للأبحاث ودراسة السياسات، قطر، 2013.
2. على زياد العلى، على حسين حميد، تكتيكات الحروب الحديثة: الأمن السيبراني والحروب المعززة والهجينة، العربي للنشر والتوزيع، القاهرة، 2023.
3. ايمن احمد الحديدي، الأمن السيبراني في ظل الانفجار المعرفي، ط1، دار اليازوردي للنشر والتوزيع، الأردن، 2022.

4. ماجد عزيز إسكندر، التوظيف السياسي للهجمات السيبرانيَّة ومخاطرها على الأمن القومي، ط1، مركز الأمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، 2023.

5. منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، مصر، 2009.

6. عبد المنعم منيب، الحرب السيبرانية والصراع بين الدول، التقرير الاستراتيجي التاسع عشر الصادر عن مجلة البيان: ما بعد الإنسانية – العوالم الافتراضية وأثرها على الإنسان، الجزائر، 2022.

7. أحمد جلال محمود، أثر التهديدات غير التقليدية للأمن على العلاقات الدولية المعاصرة: الأمن السيبراني في الشرق الأوسط حالة دراسة من 2010–2020، المؤتمر الدولي: مستقبل منطقة الشرق الأوسط – رؤية مصر 2030، 2020.

ثانياً_ المجلات

1. حازم محمد خليل، استغلال الفضاء السيبراني في الحروب غير التقليدية: دراسة في الوكالة السيبرانية والإرهاب السيبراني، المجلة العلمية لكلية الدراسات الاقتصادية والعلوم السياسية، المقالة 7، المجلد 8، العدد 15، بغداد، 2023.

2. هبه جمال الدين، الأمن السيبراني والتحول في النظام الدولي، مجلة كلية الاقتصاد والعلوم السياسية المجلد 24، العدد 1 – الرقم المسلسل للعدد 94، يناير 2023، بغداد.

3. أحمد مصطفى ناصف، دمج الأمن السيبراني في منظومة الأمن القومي: الأمن السيبراني والأمن القومي، إدارة الأعمال مجلة الأهرام، المجلد6، العدد 178، القاهرة، 2022.

4. عادل عبد الصادق، الإرهاب السيبراني والأمن القومي في بيئة متغيرة، مجلة السياسة الدولية، العدد 578، العدد227، القاهرة، 2022.

5. إسلام فوزي، الأمن السيبراني: الأبعاد الاجتماعية والقانونية: تحليل سوسيولوجيا، المجلة الاجتماعية القومية، المجلد56، عدد2، بغداد، 2019.

6. مصطفى ابراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 1، جامعة ديالى، العراق، 2021.

7. هانس بروجن وآخرون، بناء الوعي بالأمن السيبراني: الحاجة إلى استراتيجيات تأطير قائمة على الأدلة، مجلة السفير، المجلد.34، الإصدار 1، أمستردام، 2017.

8. بارام جيل، الحرب السيبرانية ومستقبل الصراع الإيراني الإسرائيلي، مجلة آفاق للأبحاث السياسية والقانونية، المجلد، 6، العدد59، الجزائر، 2020.

9. شريفة كلاع، الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، المجلد15، العدد1، الجزائر، 2022.

10.نورة شلوش، القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول، مجلة مركز بابل للدراسات الإنسانية، المجلد8، العدد2، بابل العراق، 2018.

11.جيهان أحمد عبدالعال، الحروب السيبرانية دراسة في المفهوم والنشأة ومعادلات النجاح، المجلة العلمية للدراسات التجارية والبيئية، المجلد13، عدد2، 2022.

12.ضحى لعيبي كاظم السدخان، البعد الجيو سياسي للأمن السيبراني، مجلة العلوم الإنسانية، مجلد5، العدد1، بابل العراق، 2021.

13.لامية طالة، الإرهاب السيبراني والأمن القومي: قراءة في تحولات الاستراتيجية الدفاعية، المجلد35، العدد4، الجزائر، 2021.

14.عبد الكريم اسماعيل، تأثير الفضاء الافتراضي على الأمن القومي، مجلة البحوث والدراسات، المجلد19، العدد1، بغداد، 2022.

15.جيلالي شويرب، مفهوم الحروب السيبرانية والأمن السيبراني، مجلة الحقوق والحريات، المجلد11، العدد1، الجزائر، 2023.

16.محمد الصغير مسيكة، الفضاء السيبراني وتحديات الأمن القومي للدول، مجلة العلوم القانونية والاجتماعية، المجلد7، العدد4، 2022، بغداد.

17.دانيال شاتز وآخرون، تعريف الأمن السيبراني، مجلة الطب الشرعي الرقمي والأمن والقانون JDFSL، جمعية الطب الشرعي الرقمي والأمن والقانون، المجلد. 12، العدد 2، فلوريدا، 2017.

ثالثاً_ التقارير

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

رابعاً_ المواقع الالكترونية

مقال منشور على موقع سكاي نيوز العربية، رابط الموقع، https://www.skynewsarabia.com/ تاريخ الزيارة، 1-11-2024.