تأثير الأمن السيبراني على الأمن القومي العراقي - الفرص والتحديات

م.د. ياور عمر محمد
كلية القانون والعلوم السياسية- جامعة كركوك

The Impact of Cybersecurity on Iraqi National Security - Opportunities and Challenges

Dr. Yawar.O.Mohammad
University of Kirkuk-College of Law and Political Science

المستخلص: إن الاستخدام المتزايد لشبكات الانترنت أدى الى توسع دائرة التفاعلات الدولية عبر الفضاء السيبراني مما جعل الدول تولي اهتماماً كبيراً بالبنية التحتية الحرجة الخاصة بالأنظمة الالكترونية، وشبكات الاتصالات، والبرامج والأنظمة التي تحفظ المعلومات والبيانات المهمة التي تمس الأمن القومي للبلاد، ولاسيما إذا ما عرفنا إن الأمن القومي يشتمل على العديد من الجوانب منها الأمن الإنساني، والأمن الصحي، والأمن البيئي، هذا وإن التطور التكنولوجي أضاف مفاهيم جديدة للأمن القومي منها الأمن السيبراني، والإرهاب السيبراني، والهجمات السيبرانية، والحرب السيبرانية، لذا سعت الدول جاهدةً من أجل الحفاظ على أمنها القومي من المخاطر والتهديدات الحديثة إلى اتباع وسائل تكنولوجية حديثة بهذا الخصوص، من أجل ذلك، فكانت أولى هذه الخطوات هو إضافة الأمن السيبراني في خططها الاستراتيجية لتكون داعما لأمنها القومي، ولم يكن العراق بمعزل عن دول العالم في اتباع هذه السياسة بهذا الشأن. **الكلمات المفتاحية:** (الأمن السيبراني، الأمن القومي، التحديات، الفرص).

Abstract: The increasing use of the internet has led to a rise in international interactions through cyberspace, prompting nations to pay significant attention to the critical infrastructure of electronic systems, communication networks, and the software and systems that safeguard vital information and data related to national security. National security encompasses various aspects, including human security, health

security, and environmental security. Technological advancements have introduced new concepts to national security, such as cybersecurity, cyberterrorism, cyberattacks, and cyber warfare. To protect their national security from modern risks and threats, countries have adopted advanced technological means, with one of the first steps being the integration of cybersecurity into their strategic plans to support their national security. Iraq, like other countries, has also followed these important steps.

Key Words:(Cyber Security, National Security, Challenges, Opportunities)

المقدمة

شهد العقد الماضي من القرن الحادي والعشرين تطورات كبيرة وعلى كافة الأصعدة : السياسية والعسكرية والعلمية والتكنولوجية والاقتصادية، الامر الذي أثر بشكل مباشر على واقع الأمن القومي للدول، وأصبحت انعكاساتها تتجاوز التهديدات التقليدية للبلدان في مجال الأمن القومي، وقد كان للتطورات العلمية والتكنولوجية الدور الأساس في تطور مفهوم الأمن، إذ ساهمت هذه التطورات التكنولوجية الى تفاقم المخاطر والتهديدات التي تتعرض لها الدول كافة، ليس على صعيد الفواعل التقليدية التي كانت الدولة تمثل الفاعل الرئيس فيها على صعيد العلاقات الدولية فحسب، بل إن مصادر الخطر تعددت وتنوعت على أيدي قوى دولية جديدة، فطبيعة التهديدات الأمنية الناتجة عن هذا التطورات قد تغيرت بشكل كبير متمثلة في تطور هذه التهديدات ذاتها. وإن قطاع الاتصالات وتقنية المعلومات، أضحت ضمن دائرة التطور الحاصل في المجالات كافة، إذ لم تعد الحدود بين الدول حاجزاً، ولم تقف المسافات معضلة في التواصل، وأصبح الانسان بإكمال كافة أعماله بثواني عبر حاسوبه أو هاتفه الشخصي، فظهرت مفاهيم جديدة لم تكن موجودة فيما يخص الأمن ومنها الأمن السيبراني على وجه الخصوص،

الإرهاب السيبراني، والهجمات السيبرانية، والجريمة السيبرانية، وتسعى الدول بشتى الوسائل الى المحافظة على أمنها و ديمومتها والحفاظ على بنيتها التحتية الحرجة، وذلك عبر تعزيز مجموعة من المرتكزات بها منها: السياسية، والاقتصادية، والعسكرية، والاجتماعية، ومع تطور التكنولوجيا، وظهور مخاطر جديدة رافقت هذا التطور، أصبحت الدول تهتم بالتكنولوجية، واتخاذ الإجراءات اللازمة لدرء المخاطر والتهديدات التي تمس أمنها القومي؛ فقد سارعت العديد منها مع نهاية القرن العشرين وبداية القرن الحادي والعشرين الى وضع ملف جديد على أجندتها السياسية وخططها الاستراتيجية، ألا وهو الأمن السيبراني الذي ارتبط ارتباطاً وثيقاً بالأمن الوطني.

أهمية البحث: أصبحت قضايا الأمن القومي ومن ضمنها الأمن السيبراني من القضايا المهمة التي تواجه تحديات كبيرة، ونتيجة التطور التكنولوجي والتقدم في تقنيات الاتصالات، أصبح الأمن السيبراني أحد أبرز القضايا المعاصرة التي قد تساعد في تحقيق الامن القومي، لا سيما أن العالم أصبح توجهاتها في التعاملات الدولية تعتمد اعتماداً كبيراً على الفضاء السيبراني والذي انتقل اليها التفاعلات الدولية بصورة واضحة.

إشكالية البحث: تنطلق إشكالية البحث حول العلاقة بين الأمن القومي، والأمن السيبراني والتي تعزز القدرات الدولية في تحقيق الأمن لا سيما في العراق، وهنا تطرح الإشكالية تساؤلات عديدة، والتساؤل الرئيس في هذا المجال، ماهي التحديات والفرص التي تواجه الأمن القومي العراقي والتي تعد عائقاً أمام تحقيق أمن حقيقي في العراق؟ وماهي الآليات السيبرانية والأمنية المتبعة في تحقيقها؟ ويتفرع من هذا التساؤل الرئيس تساؤلات أخرى فرعية عدة يمكن أجمالها بالآتي:

١. ما المقصود بالأمن القومي؟ وما هو الأمن السيبراني؟

٢. ما هي التحديات والفرص التي تواجهها الأمن القومي العراقي؟

٣. ما هو تأثير الامن السيبراني على الأمن القومي؟

فرضية البحث: يستند البحث الى فرضية مفادها إنه كلما تزايد استعمال الفضاء السيبراني بشكل واسع واتخاذه كساحة للتفاعلات الدولية، أدى ذلك الى تزايد المخاطر والتهديدات التي يتعرض لها الأمن الوطني وهذا يشكل عائقاً وتحدياً مباشراً وكبيراً يؤثر على الأمن الوطني العراقي بصورة عامة، لذا فإن تحقيق أمن وطني وتعزيز فرص ديمومتها في العراق يرتبط ارتباطاً وثيقاً بالإمكانات والقدرات الوطنية في مواجهة التحديات، وبالتالي لا يمكن ضمان أمن حقيقي إلا عبر الاهتمام بالأمن السيبراني المرتبط بالأمن الوطني عبر آليات ووسائل التي تمكن الدولة من تحقيق امنها الوطني، ومواجهة التحديات أو تحقيق أهدافها عبر استغلال الجوانب الإيجابية للأمن السيبراني.

منهجية البحث: من أجل معالجة الإشكالية واثبات فرضية البحث وفق منهج علمي متكامل، اعتمد البحث على منهجيات عديدة: من أهمها المنهج الوصفي التحليلي للاستعانة في عرض وجمع المعلومات وتدقيق وتحليل ومعرفة الأمن الوطني والأمن السيبراني، عبر استعراض التحديات والفرص التي تواجه الامن الوطني العراقي، وفي محاولة لربط الاحداث مع بعضها البعض، مع إبراز الآليات السيبرانية والأمنية في تحقيق الأمن الوطني.

هيكلية البحث: انطلاقا من الفرضية المتعلقة بالبحث فقد تم تقسيم البحث الى مبحثين وخاتمة واستنتاجات: تناول المبحث الأول، مفهوم الأمن القومي والأمن السيبراني، بينما تناول المبحث الثاني: تأثير الأمن السيبراني على الأمن القومي.

المبحث الأول: دراسة في الإطار النظري

المطلب الأول: مدخل مفاهيمي: بعد الحرب العالمية الثانية شهد النظام الدولي تحولات كبيرة حول مفهوم الأمن بعيداً عن تركيز الدولة المنصب على الأمن الوطني، في اتجاه إعادة تصور واضح للاحتياجات الأمنية، وقد كان الدافع لهذا الوعي الجديد هو الادراك المتزايد للطبيعة المغايرة لتحديات الأمن في القرن الحادي والعشرين وهي التحديات التي حملت معها تهديدات أمنية معقدة ومتشابكة، لذا توسع مفهوم الأمن التقليدي، الى المعنى العالمي الواسع الذي يشمل:

الأمن البيئي، والأمن الصحي، والأمن الغذائي، والأمن الاقتصادي، والأمن الإنساني، ومن منطلق التطور التكنولوجي، وبعد ظهور شبكات الأنترنت (الفضاء السيبراني) ظهرت حاجة الدولة الى الحفاظ على بنيتها التحتية المرتبطة بشبكات الانترنت والفضاء الالكتروني، مما استوجب ظهور مفهوم جديد ألا وهو الأمن السيبراني[١].

أولا. الأمن القومي:

الأمن لغة: هو نقيض الخوف ويعني السلامة وهو مأخوذ من مصدر الفعل أمن والذي يعني اطمئنان النفس وسكون القلب، بينما التعريف الاصطلاحي للأمن: عرف من قبل دائرة المعارف البريطانية بأنه: "حماية الأمة" من القهر على يد قوة أجنبية "، وقد عَرّف هنري كيسنجر الامن بأنه:" أي تصرفات بَشِعَ وقد شهد مفهوم الامن تعريفات عديدة؛ لذا فقد تم تقسيمه من حيث العمومية الى أنواع عدة منها، الأمن العام، والأمن الخاص إذ يشمل الأمن العام كل الجوانب الحياة الإنسانية، مثل الأمن السياسي، والأمن الاقتصادي، والأمن البيئي، والأمن الصحي، والأمن الإنساني وغيرها من التفرعات الخاصة بالأمن وقد عرف هذا النوع من الأمن بالأمن الشامل أو بالأمن القومي الشامل[٢].

وقد يأتي الأمن بمعنى التحرر من الخوف ومثله قوله تعالى" وآمنهم من خوف [٣]، وقد يرتبط الأمن باللغة العربية بالمكان وهنا قد يشير الأمن الموضوعي الى المكان كما ورد قي قوله تعالى، "وإذ جعلنا البيت مثابةً للناس وَأمنا[٤] .

وعرف الأمن على مستوى الدولة أنه يعني القدرة على حفظ هذه الدولة على كيانها المستقل، وتماسكها الاجتماعي، والاقتصادي ضد القوى المعادية من الداخل والخارج، إلا إنه هناك عدة أنواع من الأمن أبرزها:[١]

١ . رشيد عمارة ياس، هيمن رؤوف سلام، الامن المجتمعي وفقاً لطروحات مدرسة كوبنهاغن، مجلة الدراسات السياسية والأمنية، المجلد٥ العدد الثاني، كانون الأول، السليمانية، ٢٠٢٢، ص١٨.

٢. رؤى عبدالله عبد الرحمن، أثر التنافس السيبراني الأمريكي الروسي على الامن العالمي في الفترة من٢٠١٥-٢٠٢٢، رسالة ماجستير غير منشورة جامعة التيلين، كلية الدراسات العليا، الخرطوم، ٢٠٢٤، ص١٦-ص١٧.

٣. القران الكريم: سورة قريش، الآية ٤.

٤ . القران الكريم: سورة البقرة الاية ١٢٥.

١. الأمن العسكري: وهي قدرة الدولة على حماية مواطنيها وابنائها واموالها وممتلكاتها من أية تهديدات خارجية قد تمس بها وتسبب الضرر.

٢. الأمن السياسي: وهو استقرار نظام الدولة وتقسيماتها التنظيمية، وحمايتها من الانهيار أو سد الثغرات فيها التي قد تكون مصدر تهديدها.

٣. الأمن الاقتصادي: وهو قدرة الدولة على المحافظة على رفاهية الافراد ومستواهم المعيشي، عبر توفير الموارد الرئيسة لهم.

٤. الأمن الاجتماعي وهو قدرة الدولة على المحافظة على تراثها ولغتها وثقافتها أو أنه مقدرة الدولة على حماية مجتمعها من الفساد والجرائم الاجتماعية التي تضر باستقرار المجتمع، وحمايته من الاخطار الخارجية التي قد تسبب له الضرر.

٥. الأمن البيئي: وهو عبارة عن حماية الموارد البيئية من التلوث والاستنزاف واستعمالها بطرقٍ سليمةٍ مما يخدم الدولة ومجتمعها.

إن الارتباط المتزايد بالفضاء الالكتروني(السيبراني)، فضلاً عن استخدامها من قبل الفاعلين من غير الدول، لا سيما الجماعات الإرهابية لتحقيق أهدافها التي تنال من الأمن القومي للدول، مما أدى الى نشوء نمط جديد من التهديدات على خلفية الهجمات السيبرانية على الأنظمة الالكترونية، والمنشآت الحيوية الخاصة بالبنية التحتية الحرجة للدول[٢]

ثانياً. الأمن السيبراني: إن التطورات التكنولوجية المتسارعة وزيادة الاعتماد على الفضاء السيبراني، كل ذلك فرض على النظام السياسي الدولي الى التركيز على مفهوم الأمن والذي امتد من حماية الدولة في التعرض للهجوم العسكري الى حماية المنشآت الحيوية للبنية التحتية من التعرض لهجمات عدائية عبر استعمال تكنولوجيا المعلومات المتطورة، وأصبحت قضية

١ . علاء عبد الرزاق محمد السالمي، المدخل الى الامن السيبراني، ط١(بغداد: الذاكرة للنشر والتوزيع، ٢٠٢١)، ص١٨.
٢ . احمد الكريدي، تحول مفهوم القوة في عصر المعلوماتية القوة الامريكية انموذجا، ط١ (الشارقة: الدار العربية للعلوم ناشرون، ٢٠٢٢٩، ص٢٣٨.

الأمن القومي السيبراني تدخل ضمن استراتيجيات الأمن القومي للعديد من الدول للعمل على الحيلولة دون تعرض بنيتها الأساسية للخطر القادم من ساحة جديدة والمتمثلة بالفضاء سيبراني[١]

نظراً للاعتماد على الفضاء السيبراني من قبل العديد من الدول، وتأثيره على الأمن القومي، ادى الى ظهور مفهوم الأمن السيبراني (Cyber Security)، وقد عرفته وزارة الدفاع الامريكية بأنه:" كافة الإجراءات التنظيمية المطلوبة لضمان حماية أمن المعلومات بجميع أشكالها (الالكترونية والمادية)، وأمن الأنظمة والشبكات، إذ يتم تخزين المعلومات والوصول اليها ومعالجتها ونقلها، بما في ذلك الاحتياطات المتخذة للوقاية من الجريمة والهجوم والتخريب والتجسس والحوادث" [٢]

ويشمل الأمن السيبراني حماية البيانات الرقمية وما يتعلق بها وهي تشمل: القضايا التي تندرج تحت أمن المعلومات، كحماية البنى التحتية، مثل شبكات الماء والكهرباء، والتي تعمل عن طريق الحواسيب، وكذلك الصواريخ الحربية والمعدات الطبية، والسيارات الحديثة، والتي أصبحت تعتمد على شبكات الانترنت بشكل أكبر، وايضاً حماية انترنت الأشياء التي تستعمل كاميرات المراقبة الرقمية فيها، وكذلك الأجهزة والأدوات المنزلية الذكية[٣].

وقد عرف الاتحاد الدولي للاتصالات الأمن السيبراني على أنه: "مجموعة وسائل تقنية وتنظيمية وإدارية التي يتم استعمالها لمنع الاستعمال غير المصرح بها، بهدف ضمان استمرارية عمل نظم المعلومات وحمايتها المعلومات، واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من مخاطر وتهديدات الفضاء السيبراني"، وتتباين مواقف الدول في مجال تعاطيها

١ . صفاء حسين علي، الحرب الالكترونية في المدرك الاستراتيجي الأمريكي، مجلة دراسات دولية، جامعة بغداد، العدد٨٢، بغداد، ٢٠٢٠، ص٢٣٤.

٢ . ايمان عبد القادر، أثر الفضاء السيبراني على الامن القومي العربي خلال الفترة من٢٠١١ حتى٢٠٢٣، مجلة الامن القومي والاستراتيجي الاكاديمية العسكرية للدراسات العليا والاستراتيجية العدد الثالث، مصر، يناير٢٠٢٤، ص١٠٧

٣. منصور عبد الكريم، ط١(القاهرة: دار الفاروق للاستثمارات الثقافية، ٢٠٢٢)، ص٥٥-ص٥٦.

للأمن السيبراني، فمنها من يضعه في مقدمة أولوياتها واهتماماتها، ومنهما من يتعامل مع الأمن السيبراني أنه مجال خطر، إلا إنه غير مهم ولا يشكل تهديداً لأمن للدولة [١]

لذا مع بروز المجتمع المعلوماتي، والفضاء السيبراني وتحول الأمن الى أحد القطاعات الخدمية التي تشكل قيمة مضافة، ودعامة أساسية، لأعمال الحكومات والافراد على حدٍ سواء، كما هو الحال مع التطبيقات الخاصة بالحكومة الالكترونية، والصحة الالكترونية، والتعليم عن بعد، والتجارة الالكترونية، وغيرها من النشاطات، إلا إن التأثيرات المتعددة للأمن السيبراني، ومضاعفاتها الخطيرة، لا تقف عند حدود الإساءة الى الافراد، والمؤسسات فحسب، بل تتعداها الى تعريض سلامة الدول والحكومات للخطر الامر الذي يجعل من مهمة القائمين على الموضوع تعقيداً وصعوبةً، فتحقيق الأمن وبناء الثقة في الفضاء السيبراني، تُعد من أساسيات تسخير تقنيات المعلومات والاتصالات، في مجال التنمية وخدمة المجتمعات الإنسانية[٢]

المطلب الثاني: علاقة الأمن السيبراني بالأمن القومي: إن الاهتمام بالأمن السيبراني نابع من التطور الكبير الذي حدث في تكنولوجيا المعلومات، وتقنية الاتصالات وتبادل المعلومات في العالم عبر استعمال شبكة الانترنت بمختلف أنواعها ويعد ذلك تطوراً خطيراً عالمياً وعربياً في مجال الأمن الداخلي والقومي ويعود ذلك الى أمرين وهما:[٣]

١. إن الكثير من الدول- بما فيها الدول العربية- بدأت التحول الى مجتمع المعلومات والمعرفة، واخذت بإعداد الخطط وتنفيذها على نطاق لتحويل هذا الشعار الى واقع عملي ملموس، بإنشاء مجموعة من قواعد البيانات القومية الكبرى، كما يجري الى تطوير شبكات الاتصالات، ونشر الانترنت عبر خطوط الاتصالات العادية والسريعة، وتعميم خدمات نقل الصوت عبر بروتوكولات الانترنت، وتشجيع الدول في نشر مفاهيم وخدمات الحكومة الالكترونية، وتشريع قوانين التوقيع الالكتروني الذي يمهد

١ . صدام مرير حمد الجميلي، الحروب الهجينة وأثرها في مستقبل الصراع العالمي، مجلة جامعة تكريت، كلية العلوم السياسية، العدد٣٤، تكريت، اذار ٢٠٢٤، ص١١-ص١٢.

٢ . يونس مؤيد يونس، استراتيجية الولايات المتحدة الامريكية للأمن السيبراني، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، بغداد، العدد ٥٥، ٢٠١٨، ص١٢٨.

٣. علاء عبد الرزاق محمد السالمي، المدخل للأمن السيبراني، ط١(بغداد: الذاكرة للنشر والتوزيع،٢٠٢١)، ص٢٢.

الطريق صوب تفعيل أنشطة التجارة والاعمال، والاقتصاد الالكتروني على نطاق واسع.

٢. إن البنية التحتية المعلوماتية المتكاملة واسعة المجال التي تُشييد من قِبل الدول، وتبني التوجه نحو مجتمع المعلومات، ونقل المجتمع والدولة والمؤسسات لتكون عرضة للمخاطر، وهذا يتطلب مواجهة التحديات الواسعة النطاق في أمن المعلومات، أي بمعنى آخر أن تحديات أمن المعلومات في مجتمع يمتلك بنية معلوماتية واسعة يجعله يواجه تهديدات في أمن المعلومات تتسم بالشمول والاتساع وعمق التأثير وتنوع الأدوات.

يبدو ان العلاقة واضحة بين الأمن السيبراني والأمن الوطني، لضمان حق الوصول الى كافة البيانات والمعلومات، ومصادر النظام، وذلك عبر آلية تحقق الهوية ورقابة تسمح بحصر مستخدمي النظام ضمن مجموعة أشخاص الذين أعطي لهم حق الولوج الى النظام، فالأمان في الفضاء السيبراني ليس إلا جزءاً من مكونات الأمن في المجتمع بشكل عام وهو الركيزة الأساسية من أجل تحقيق النمو والتطور والازدهار في مجتمع تسوده المعلومات بالدرجة الأساس، فقضية الأمن السيبراني، أصبحت من ضمن استراتيجيات الأمن القومي للعديد من الدول؛ للحيلولة دون تعرض بنيتها التحتية الحيوية للخطر الذي نتج من جراء قطع شبكة المعلومات الدولية، أو توقف شبكات الانترنت ووسائل البث الإذاعي أو تزوير الانتخابات أو التجسس السيبراني، أو سرقة الملكية الفكرية للاختراعات، أو اختراق أنظمة صواريخ العسكرية، كل هذه الأمور أصبحت مهددة للأمن القومي للدول[١]

وقد دفعت التهديدات السيبرانية المتزايدة لأمن الفضاء السيبراني العديد من الدول للعمل على بذل أقصى الجهود بصورة منفردة أو على شكل جماعات من أجل الحفاظ على الأمن السيبراني لديها، سواء كان عبر انشاء هيئات لمواجهة الطوارئ المعلوماتية أو تشريع قوانين لمكافحة الجريمة الالكترونية، أو انشاء قيادة لحماية الفضاء السيبراني، أو استحداث وحدات

١ . يونس مؤيد يونس، مصدر سبق ذكره، ص١٣٣

للحرب السيبرانية داخل الجيوش العسكرية، أو المشاركة في المناورات الالكترونية لتحسب القدرات الدفاعية أمام الهجمات السيبرانية، وبذلك أثر الفضاء الالكتروني على تغيير نمط القوة من حيث طبيعة وخصائص الأمن والصراع على المستوى الدولي، لذا لزم الأمر على الدول إعادة التفكير في مفهوم الأمن القومي للدولة، إذ إن الأمن السيبراني لم يقتصر فقط على البعد التقني، بل تعداه ذلك الى أبعاد أخرى في ظل تراجع سيادة الدولة وتزايد العلاقة بين الأمن والتكنولوجيا، وتأثيرها على المصالح الاستراتيجية للدول[١]

ونظراً لأتساع نطاق الفضاء السيبراني، وتبني الحكومات الالكترونية من جانب العديد من الدول، واتساع نطاق استخدام وسائل التكنولوجيا والاتصالات الحديثة حول العالم، أظهرت العلاقة الحقيقية بين الفضاء السيبراني والأمن العالمي، إذ أصبحت قاعدة البيانات القومية في حالة من الانكشاف الخارجي، وهذا مما يعرضها لخطر التعرض لهجمات سيبرانية، والدعاية والمعلومات المظللة، ونشر الشائعات أو الدعوة لأعمال تحريضية أو دعم المعارضة الداخلية للنظام الحاكم أو تقديم الدعم المادي والمعنوي لقوى المعارضة عبر الفضاء السيبراني.[٢]

المبحث الثاني: تأثير الأمن السيبراني على الأمن القومي. للأمن السيبراني تأثيرات على الأمن القومي، إذ إن المخاطر والتهديدات التي قد تتعرض لها البنية التحتية للدولة كبيرة، لا سيما بعد التحول في استخدام التكنولوجيا وتقنية الاتصالات الحديثة، في كافة المؤسسات السياسية والاقتصادية، والعسكرية، فثمة هجمة سيبرانية واحدة قد تؤدي الى تأثير كبير وخسائر فادحة في شبكات الطاقة ومحطات المياه والمصارف الحكومية والتعاملات التجارية.

المطلب الأول: تأثير الأمن السيبراني: لم يعد الاهتمام بالأمن السيبراني يقتصر على البعد التقني فقط وإنما تجاوز ذلك الى أبعاد أخرى ذات طبيعة سياسية، وعسكرية، واقتصادية، وثقافية واجتماعية، وغيرها من المجالات.

١ . دنيا جواد مطلك، احمد عبد الجبار عبدالله، انعكاسات تطور القوة المعلوماتية الامريكية في البيئة الداخلية، مجلة حمورابي، العدد٣٥، بغداد، ٢٠٢٠، ص١٥٤-ص١٥٥.

٢ . عادل عبد الصادق، الاقتصاد الرقمي تحديات السيادة السيبرانية، ط١(القاهرة: المركز العربي لأبحاث الفضاء الالكتروني،٢٠٢٠)، ص١٥

اولاً. التأثير على المجال السياسي:

إن أي نظام سياسي في أي دولة يسعى الى المحافظة على كيانها ومصالحها العليا وعلى استقرارها الخارجي المرتبط بالاستقرار الداخلي، وكذلك السعي الى خلق هامش من الرفاه الاقتصادي لمواطنيه، وفي ظل التطور التكنولوجي والثورة الرقمية، وظهور الفضاء السيبراني، أصبح المواطن قادراً عن التعبير عن رأيه السياسي، الذي أصبح لاعباً اساسياً وطرفاً مؤثراً في السياسة الداخلية والخارجية للدولة، إذ لا توجد صعوبات في الحصول على المعلومة ومعرفته بأمور بلده السياسية والقرارات المتخذة من قبل السلطة، كما إن الدول في المقابل زادت من استثماراتها في الفضاء السيبراني لغرض الوصول الى أكبر عدد من مواطنيها والتأثير عليهم ومحاورتهم عبر شبكات الانترنت، فضلاً عن استخدام الفضاء السيبراني في الترويج للحملات الانتخابية للرؤساء وتقديم توجيهاتهم، وطرح الأفكار السياسية بطرق مختلفة [١].

ثانياً. التأثير على المجال العسكري:

أحد أهم الابعاد المهمة في الفضاء السيبراني لكونه يعد العامل الأساس في الحفاظ على المؤسسات العسكرية عبر تأمين الاتصالات بين الوحدات عبر الشبكات العسكرية مما يسهل من تبادل المعلومات وتعبير الأوامر فيما بينها ومن أجل تحقيق ذلك فإن التحويل على شبكات الانترنت وتطويرها بات أمراً لا مناص منه، والتي قد تمثل نقطة ضعف إذا لم تكن مؤمنة بصورة صحيحة، إذ يمنع اختراقها، أو تدميرها والذي قد يؤدي الى تدمير البيانات العسكرية، أو قطع الاتصال بين الوحدات العسكرية وقياداتها، فضلاً الى إمكانية التحكم بالأسلحة المتطورة وخروجها عن السيطرة مثل الصواريخ الموجهة والطائرات بدون طيار وغيرها من الأجهزة والآلات الحديثة [٢].

١ . محمد محمود العمري، مدخل الى الامن السيبراني، ط١(عمان: دار زهران للنشر والتوزيع، ٢٠٢٠)، ص٣٨.
٢ . مازن حميد شلال، فراس جمال شاكر، الامن في النظام الدولي ما بين القوة التقليدية والقوة الجديدة، ط١(بغداد: دار كلمة للطباعة والنشر والتوزيع،٢٠٢٢)، ص٢٣٨

ويتوقف تحقيق الأمن القومي العسكري على الابتكارات الحديثة في المجال السيبراني في الوقت الحاضر عبر ربطها بوسائل الاتصالات الحديثة، وشبكات الانترنت، وقواعد البيانات، وأنظمة المعلومات العسكرية، التي تمكن مستخدميها من التحكم بها عن بعد، ويُعَد المحتوى الرقمي العسكري من أخطر الابعاد تأثيراً على الامن القومي لأي دولة في العالم، بالنظر لما تحتويه من معلومات حساسة رقمية والكترونية تخص الجانب العسكري والتسليحي للدول[١].

بدأت العديد من الدول الى ادخال الفضاء السيبراني ضمن استراتيجيات أمنها القومي لديها، وقد دفعت التهديدات الحديثة للفضاء السيبراني أغلب الدول على بذل الجهود بشأن الحفاظ على أمنها السيبراني سواء عبر انشاء هيئات متخصصة لمواجهة الهجمات السيبرانية واستحداث قوانين لمكافحة الجريمة السيبرانية، وإنشاء قيادة عسكرية لحماية الفضاء السيبراني، أو استحداث وحدات لتحسين القدرات الأمنية ضد الهجمات السيبرانية التي تتعرض لها[٢].

ثالثاً. التأثير على المجال الاقتصادي: يُعّد الفضاء السيبراني بنية جذابة لقطاعات المجتمع كافة، وأصبحت المعرفة المحرك الأساس للإنتاج والنمو الاقتصادي، كما إن التركيز على المعلومات والتكنولوجيا أصبح عاملاً من العوامل الأساسية للنهوض بالاقتصاد، وهذا ما دفع بالدول الى الاهتمام بالاستثمارات المعرفية، وأضحى عصرنة الاقتصاد مرتبط بالتحكم بالاقتصاد الرقمي من طرف مختلف الفاعلين الاقتصاديين والاجتماعيين.[٣]

لقد أدت الثورة المعلوماتية الى استعمال تقنيات المعلومات والاتصالات بصورة كبيرة وواسعة، لذا أرتبط الامن السيبراني ارتباطاً وثيقاً بالاقتصاد، فأصبح هذا الترابط واضحاً بين الاقتصاد والمعرفة، وازداد قيمة البيانات والمعلومات المتداولة والمخزونة، والمستعملة على كل المستويات، مما أتاح تقنيات المعلومات والاتصالات، الى تعزيز التنمية الاقتصادية لبلدان

١ . ماجد محمد الحنيطي، تكنولوجيا الصراعات الدولية المعاصرة، ط١(عمان: الآن ناشرون وموزعون،٢٠٢١)، ص٢٩.

٢ . عبد القادر الهواري، حرب اللاعنف وعلاقته بالفوضى الخلاقة، ط١(القاهرة: المجلس الأعلى للثقافة، ٢٠٢١)، ص١٨٢.

٣ . لامية طالة، التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها، مجلة معالم للدراسات القانونية والسياسية، كلية العلام والاتصال، المجلد٤، العدد٢، الجزائر،٢٠٢٠، ص٦٢

كثيرة، عبر الاستفادة من فرص الاستخدام التي تقدمها الشركات الدولية الكبرى، فضلاً عن دخول العالم عصر المال الالكتروني، ضمن بيئة متحركة، عبر أطلاق الخدمات المالية عبر المصارف، والمؤسسات المالية، في المجال الرقمي، وقد ربط المسؤولون عن قدرات الحكومات، وسياستها، بين الأمن والنمو الاقتصادي، بشكل واضح، وأصبح استهداف المعلومات والبيانات الاقتصادية، عبر عمليات التجسس الصناعي، والعسكري التقليدية، أو عن طريق الاعتداء وسرقة الملكية الفكرية، فضلاً عن التأثيرات المالية السلبية، والتي يتركها الاستهداف، على أنظمة المعلومات، وتعطيلها، مثل سرقة نتائج الأبحاث، أو غيرها من المعلومات[١]

وأصبح الفضاء السيبراني مسرحاً تجري فيها كافة الأنشطة الاقتصادية والمالية في ميدان التجارة والصناعة، وكذلك المعاملات المصرفية والبنكية بين الدول وبين الافراد ومن أجل تطور الاقتصاد الوطني ومواكبة التطورات الدولية القائمة على الاعتماد على التكنولوجيا، لذا يستوجب الامر الى الاهتمام بالأمن السيبراني في هذا المجال الحيوي الذي يهدف الى تحقيق التنمية للدول المرتبطة والعاملة على الشبكة الالكترونية القومية التي يخشى عليها من الاختراقات التي قد تعطل مسارات عمليات التنمية[٢].

رابعاً. التأثير على المجال الاجتماعي والثقافي:

ان التطورات التي شهدها القرن الحادي والعشرين في مجال شبكات الانترنت، ولا سيما مواقع التواصل الاجتماعي، إذ بلغ عدد المستخدمين لمواقع الانترنت أكثر من (٥) مليارات شخص مما جعل منه أكبر تجمع في العالم الافتراضي، مما أدى هذا الى افساح المجال أمام المستخدمين من تبادل المعلومات والخبرات والأفكار الجديدة، إلا إن ذلك يعد سلاحاً ذا حدين، الأول يخص تبادل العلم والمعرفة، والثاني يعرض أخلاقيات أفراد المجتمع للخطر لعدم السيطرة عليه ومراقبته، وقد يؤدي ذلك الى خطر يهدد السلم المجتمعي عن طريق نشر الأفكار المتطرفة

١ . منى الأشقر جبور، السيبرانية هاجس العصر، ط١(بيروت: جامعة الدول العربية، المركز العربي للبحوث القانونية،٢٠١٦)، ص٣٠.

٢ . نور الدين ملاك، التهديدات السيبرانية عبر الفضاء الأزرق وتأثيرها على الامن القومي للدول، جريدة الشعب الجزائرية ديسمبر، ٢٠٢١. ينظر الرابط: https://www.ech-chaab.com/ar/ تاريخ الزيارة١٩/١٠/٢٠٢٤.

وغيرها، لذلك يتوجب على الدولة ومؤسساتها الى نشر الوعي الثقافي بين المواطنين والمجتمعات بضرورة تجنب المخاطر من أجل تحقيق الامن السيبراني المجتمعي[١].

ولقد أصبح الفضاء السيبراني من الأدوات الحساسة في يد مختلف القوى والفاعلين، لما تقدمه من قدرات واسعة في نقل الاخبار والبيانات، وتوظيفها في مجال النشر والاقناع، وهذا جعل العديد من الدول والشعوب أمام خطر السيطرة والاختراق الناعم، الذي يعتمد على أساليب الاقناع، والتغلغل في عمق سيكولوجيا الافراد، مما يفرض على الدول استحداث أساليب حديثة، وتبني مسارات جديدة، يمكن عن طريقها حماية شعوبها من خطر الاختراق والتوجيه الخارجي[٢].

المطلب الثاني: فرص وتحديات الأمن السيبراني:

اولاً. الفرص التي تأمنها الأمن السيبراني: إن الانتشار الواسع للفضاء السيبراني ولشبكات الانترنت دور كبير في اتساع التنافس بين الدول والمجتمعات، وهذا أدى الى سرعة التواصل بين الشعوب وسرعة إيصال الاخبار وانتقال المعلومات وتداولها عبر شبكات الانترنت، لاسيما مع انتشار مواقع التواصل الاجتماعي (فيس بوك، يوتيوب، تويتر... غيرها)، لذا نجد أغلب الدول تبنت سياسات جديدة لدخولها في مجال الفضاء السيبراني عبر استعمال التقنيات الرقمية والتحول الى حكومة رقمية ويتم ذلك عبر التكامل الرقمي في أنظمتها الحكومية وتعد هذه السياسة فرصة في تعزيز تقدمها في مجال الأمن السيبراني، والعراق هو من أحد الدول التي اهتم بهذا المجال، ويمكن ايجازها بالآتي:[٣]

١. التعاون الدولي: التعاون مع الشركاء الدوليين وبشكل منتظم بشأن السياسات والعمليات التشغيلية، وتنسيق الإجراءات الهادفة لتعزيز الأمن السيبراني في جميع أنحاء العالم، وابرام الاتفاقات الثنائية والمتعددة الأطراف، وتبادل المعلومات حول قضايا الأمن السيبراني التي من شأنها دعم الاستعمال الآمن للفضاء السيبراني.

١ . مازن حميد شلال، فراس جمال شاكر، مصدر سبق ذكره، ص٣٣٨-ص٣٣٩.
٢ . احمد الكريدي، مصدر سبق ذكره، ص٣٥٣.
٣ . صلاح مهدي هادي، زيد محمد إسماعيل، الامن السيبراني كمرتكز جديد في الاستراتيجية العراقية، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، العدد٦٢، أيلول، بغداد، ٢٠٢٠، ص٢٩١-ص٢٩٢

٢. تطوير البنية التحتية: إعطاء الفرصة لإنشاء شركات تنافسية (عامة، وخاصة)، في مجال الأمن السيبراني، والاستثمار في مجال الأبحاث الرامية الى تطوير التقنيات مع الحلول المبتكرة في مجال الأمن السيبراني

٣. خلق فرص عمل جديدة: تطوير وصقل القوى العاملة في مجال الأمن السيبراني والحفاظ عليها عن طريق اجراء المسابقات في مجال الأمن السيبراني لاختيار أفضل المهارات العاملة فيها وتشجيعهم على متابعة مسيرتهم العلمية في هذا التخصص، تشجيع الافراد على استعمال أدوات وحلول على الانترنت للوقاية من الهجمات الالكترونية.

٤. تعزيز القدرات الدفاعية: ويتم ذلك عبر حماية البنية التحتية للمعلومات الحيوية الوطنية، لذا يجب العمل على تقييم المخاطر والتهديدات التي تواجهها البنية التحتية، وضع أطار قانوني لتعزيز سلامة وحيوية الفضاء السيبراني، ووضع الخطط الاستراتيجية وطنية للتصدي للأخطار، ومواطن الضعف في البنية التحتية السيبرانية، من قبل صانع القرار، وضع خطة للدفاع السيبراني وحماية البيانات من التسريب أو السرقة أو التخريب، وتحليل الأدلة الالكترونية عبر رفع مستوى القدرات والخبرات التقنية لحماية شبكة الانترنت الوطنية[١].

ثانياً. تحديات الأمن السيبراني:

يعد تحدي الأمن السيبراني من أبرز تحديات الأمن القومي في القرن الحادي والعشرين، إذ إن المفهوم الجديد للأمن لا يقتصر على الجوانب العسكرية، بل يشمل كل التهديدات والتحديات التي يمكن أن تشكل عائقاً أمام تحقيق الأمن القومي ومن ضمنها الاقتصاد الرقمي وتدقيق

١. رعد خضير صلبي، مجلة دراسات دولية، جامعة بغداد، مركز الدراسات الاستراتيجية والدولية، العدد٩٩، بغداد، أكتوبر ٢٠٢٤، ص٥٢٠- ص٥٢١.

المعرفة، فقد الغت تكنولوجيا المعلومات والاتصالات مفهوم الحدود الجغرافية، والسياسية والثقافية بين الدول[١].

فالتطورات الكبيرة في مجال التكنولوجيا، ودخول العالم العصر الرقمي في القرن الحادي والعشرين، وما نتج عن ذلك من تداعيات عديدة بسبب ظهور تهديدات ومخاطر وجرائم سيبرانية أصبحت تشكل تحدياً كبيراً للأمن القومي، لذا عد الفضاء السيبراني بمثابة المجال الخامس للحروب بعد (البر، والبحر، والجو، والفضاء الخارجي)، وهوما استدعى ضرورة وجود ضمانات أمنية ضمن هذه البيئة الرقمية، وقد تبلور ذلك بشكل أساس قي ظهور الأمن السيبراني (Cyber Security)، كبعد جديد في حقل الدراسات الامنية[٢].

وقد خلفت التكنولوجيا تحديات كبيرة وقفت عائقاً أمام تحقيق الدول لأمنها السيبراني، وفيما يلي أبرز هذه التحديات:[٣]

١. صعوبة معرفة مصدر الهجمات (الطرف المتعدي): على الرغم مما وصلت اليه التكنولوجيا من التطور الكبير في عمليات التتبع، إلاّ أن هناك تقدم في الوقت نفسه في عمليات التمويه والاختفاء، بصورة تجعل معرفة مصدر الهجمات شبه مستحيلة، إلا في حالة الهجمات الصغيرة والبسيطة التي يقوم بها أصحابها ضمن حدود الأخطاء، وليس في حالة شن الهجمات المعقدة التي تقوم بها الدول، أو بعض العناصر المدعومة من قبل الدول، إذ إن الهجمات الالكترونية التي شنتها روسيا الاتحادية على استونيا عام ٢٠٠٧، وعلى جورجيا عام٢٠٠٨، أو الهجمات الامريكية الإسرائيلية التي شنت على المفاعل النووي الإيراني عام ٢٠١٠، وهجمات كوريا الشمالية على شركة سوني(Sony)عام ٢٠١٥، والدور الأمريكي في قطع الانترنت عن كوريا الشمالية لمدة ١٠ ساعات، والاتهامات الامريكية التي وجهت الى روسيا

١ . اسلام فوزي، الامن السيبراني الابعاد الاجتماعية والقانونية تحليل سوسيولوجي، المجلة الاجتماعية القومية، المركز القومي للبحوث الاجتماعية والجنائية، المجلد٥٦، العدد٢، القاهرة، مايو٢٠١٩، ص٥٦

٢ . سالم محمد عبود، اساسيات الامن السيبراني، ط١(بغداد: دار الدكتور، ٢٠٢٢)، ص٤٢

٣. شريفة كلاع، الامن السيبراني واشكال التهديدات تحديات عالمية، ط١(عمان: الفا للوثائق ونشر واستيراد وتوزيع الكتب، ٢٠٢٣)، ص٨٥-ص٨٦.

لتدخلها في الانتخابات الرئاسية عام٢٠١٦، وغيرها من الهجمات التي لم يتم تبنيها صراحة من قبل الدول المعتدية، إذ إن بعض من هذه الدول أنكرت القيام بذلك، على الرغم من توفر الأدلة المرتبطة بالظروف السياسية وليس الفنية والقانونية .

٢. صعوبة منع الهجمات: إن ما يميز الفضاء السيبراني بان عملية التحديث للتكنولوجيا مستمرة، إذ يمكن اختراع وتطوير برامج فيروسات في معامل خاصة بصورة يومية، لم يتم الكشف عنها ولم يتم رصدها من قبل شركات الأمن السيبراني، فالبعض من هذه الهجمات تصيب المكون المادي مثل فيروس(ستاكسنيت). وبعضها وهو كثير يصيب الجانب البرامجي، وبعضها وهو أيضاً غير محدود يركز على المعلومات بهدف السرقة والتضليل أو التدمير والتخريب، كما وإن هذه الفيروسات تستغل الثغرات الحديثة التي تظهر في الأنظمة قبل أن يتم تحديثها ومعالجتها.

٣. القيود القانونية الخاصة بميثاق الأمم المتحدة: إذ تعد هذه التحديات التي تجعل قدرة الدولة على تحقيق أمن سيبراني عبر الفضاء السيبراني غير فعالة؛ ألا وهو القيود القانونية الخاصة باستخدام القوة في العلاقات الدولية، وفقاً لميثاق الأمم المتحدة ، إذ تنص (المادة٢ الفقرة٤) من ميثاق الأمم المتحدة على منع استخدام القوة في العلاقات الدولية أو التهديد باستخدامها، إلا في حالة توافقها مع مقاصد الأمم المتحدة، كما اشترطت المادة٥١ من الميثاق على ضرورة ابلاغ مجلس الأمن بأية تدابير هجومية سوف تتخذها الدولة في حالة الدفاع عن النفس، وبالنظر لأن الهجمات السيبرانية هي أحد اشكال استخدام القوة في العلاقات الدولية، أو التهديد باستخدامها فإنه ينطبق عليه ميثاق الأمم المتحدة والقيود التي تفرضها، وهو ما قد يكون عائقاً أمام نجاح الردع السيبراني وفاعليته[١].

٤. صعوبة تطوير نظام دفاعي سيبراني:

١ . شرفة كلاع مصدر سبق ذكره، ص٨٧-ص٨٨.

من التحديات الأمنية التي تواجهها الدولة هي معضلة الدفاع السيبراني، هي صعوبة تطوير نظام دفاعي سيبراني بحيث يضمن تأمين الأنظمة السيبرانية للدولة بشكل كامل ليحول دون تعرضها للهجمات، أو أن يوقفها فور وقوعها، فأغلب أنظمة الدفاع السيبراني تحقق قدراً من التأمين للأنظمة والشبكات السيبرانية لمدة ما الى أن يتم اكتشاف نقطة ضعف فيها ويمكن استهدافها والهجوم عليها وبعد ذلك تصبح بلا جدوى، فقوة النظام الأمني السيبراني وحمايته عبر مستويات مختلفة في الدفاع لا يوفر ضماناً كاملاً لتأمينه بشكل دائم، كما المعمول به أنه يتم تطوير أنظمة الدفاع فور وقوع هجمات وليس العكس، اذ يصعب على أية مؤسسة اكتشاف نقاط الضعف في أنظمتها الالكترونية دون وقوع هجوم فعلي يكتشفها[1]

٥. صعوبة تقييم المخاطر:

في حالة تعرض أية دولة للمخاطر والتهديدات فإن عملية تقييم المخاطر تعد من أحد العناصر الأساسية في صياغة عملية استراتيجية دفاعية محكمة لمواجهة خطر الأمن السيبراني، وان عملية تقييم المخاطر تنقسم الى ثلاث مراحل رئيسة وهي:[2]

أ. تحديد مدى قدرة الخصم على اكتشاف واستغلال نقاط الضعف في الأنظمة الالكترونية للدولة.

ب. تقدير حجم الآثار المترتبة على الهجوم إذا ما تمكن الخصم بالفعل من استغلال نقاط الضعف ومهاجمتها.

جـ. احتمالية اقدام الخصم على شن الهجوم وهي حالة يصعب معرفة نوايا الخصم من قبل الدولة الأخرى

1 . Brian Weeder: Cyber offence and Defence as Mutually Exclusive National Policy Priorties In Kerstin Vignardetal(eds.), Confronting Cyber Confict, Disarmament Forum, United Nations Institute For Disamament Research Accessed on: August 2,2o13,P23

٢ . فراس جمال شاكر، السيبرانية وتحولات القوة في النظام الدولي، ط١(عمان: دار أمجد للنشر والتوزيع، ٢٠٢٣)، ص ٣٢٥

٦. استخدام التنظيمات الإرهابية للفضاء السيبراني: إذ وظفت التنظيمات الإرهابية وجماعات الجريمة المنظمة للمجال السيبراني بغرض تحقيق أهدافهم فعلى سبيل المثال لا الحصر ما تقوم به التنظيمات الإرهابية بتوظيف الفضاء السيبراني عن طريق قيامها باستعمال مواقع التواصل الاجتماعي، من أجل تحقيق أهدافها عبر تلك المواقع كتنظيم داعش، إذ أصبحت لهذه التنظيمات مواقع الكترونية مثل(فيس بوك، يوتيوب، تيلكرام، تويتر) فضلاً عن استعمالها لمواقع أخرى وباللغة العربية، والانكليزية لبث أفكارها، وتبادل المعلومات، ونشر الصور ومقاطع الفيديو، وتجنيد الشباب عبر التواصل معهم، عن طريق هذه المواقع[١]

ثالثاً. الآليات الأمنية والسيبرانية لتحقيق أمن سيبراني قومي:

إن الأمن السيبراني للدول ومنها العراق يهدف بلا شك الى الحد من المخاطر والتهديدات الناجمة عن الهجوم على الأجهزة والحواسيب وشبكات الانترنت والبرامج والبيانات والمعلومات المخزونة وتحتوي على الأدوات المستعملة في مواجهة (القرصنة الالكترونية) وأجهزة وبرامج كشف الفيروسات، وتوفير الاتصالات المشفرة، فقد أعلن العراق وعبر مستشارية الامن الوطني عن (استراتيجية الأمن السيبراني العراقي)، منذ عام ٢٠١٧، لتوفير التدابير اللازمة والإجراءات والآليات الاستراتيجية لضمان أمن وحماية الوجود العراقي في الفضاء السيبراني، وحماية البنية التحتية، الحيوية للمعلومات والبيانات، وبناء مجتمع معلوماتي ضمن أطار شبكة الانترنت الموثوقة بها، والإرهاب والتجسس السيبراني، والصراع السيبراني، وقد وضعت استراتيجية تفصيلية تمثل خارطة طريق للأمن السيبراني، والمتمثلة بالحكومة الالكترونية الفعالة، والاطار التشريعي والتنظيمي لها، وأطار تكنولوجيا الأمن السيبراني، وثقافة الأمن السيبراني، وبناء القدرات، والبحث والتطوير نحو الاعتماد على القدرات والمصادر الذاتية، والجاهزية لحوادث الأمن السيبراني الى جانب التعاون الدولي، وقد جرى الإعلان عن فريق وطني مشترك في

١. مروان سالم العلي، التحديات الاستراتيجية للأمن الوطني في ظل المتغيرات الدولية، مجلة كلية العلوم السياسية، جامعة تكريت، العدد٢٠، تكريت، تموز٢٠٢٠، ص٤٩

مجال حماية الخصوصية والحماية الذاتية للأفراد والمؤسسات على شبكة الانترنت يعمل تحت أشراف وقيادة مستشارية الأمن الوطني العراقي ومن هذه الاستراتيجيات[١].

١. استراتيجيات الردع والدفاع السيبراني: فقد أهتمت الدول بالبيانات والمعلومات والأجهزة الحاسوب الخاصة ، وذلك لأهميتها الكبرى، وقد وجدت الدول طرق لحماية البيانات والمعلومات الخاصة بها، عبر الدفاع عن أصول بلدانها ضد الهجمات السيبرانية، أو ردع طرف الخصم عن القيام بشن هجمات معادية، فالدفاع يتضمن اتخاذ التحوطات اللازمة للتقليل من احتمال نجاح أي هجمة سيبرانية معادية، وإن الإجراءات المطلوبة تكون عن طريق عمليات منع العدو من الوصول الى غايته، او إزالة مواطن الضعف والخلل والقصور في الأجهزة والمعلومات المستهدفة، أو عبر المساعدة على التعافي السريع عند التعرض لأي هجمات سيبرانية، بينما عمليات الردع يقصد بها اقناع الخصم بان لا يشن أي هجوم، فالردع هو نهج يهدف الى اقناع الخصم بالعدول عن أي عمل عدواني قد يضرُ بمصالحه، أو ايهامه العدو بانه سوف يتكبد خسائر كبيرة في حالة قيامه بأي نشاط سيبراني معادي[٢]

٢. انشاء أنظمة الدفاع المتقدمة: إنَّ انشاء الجدران النارية، وأنظمة كشف التسلل، الجدران النارية Fire Walls وهي عبارة عن أنظمة معلوماتية – برامج توفر جداراً أمنياً ما بين شبكة الانترنت وشبكة المؤسسة، أو الحكومة الالكترونية، حتى يتم اجبار جميع العمليات (الخروج الدخول)، اليها عبر الشبكة، بان تمر عبر هذا الجدار الناري، والذي يمنع الاختراق، أو دخول متطفل يريد الوصول الى الشبكة، فهي برامج تقوم بصد محاولات الاختراق أو الهجوم الوافد من شبكة الانترنت لتهديد الشبكة الداخلية، أو النظم المعلوماتي[٣].

١. سالم محمد عبود، مصدر سبق ذكره، ص١٧٩.
٢ . هربرت لين، النزاع السيبراني والقانون الإنساني، المجلة الدولية للصليب الأحمر، المجلد٤٩، العدد٨٨٦، ٢٠١٢، ص٥٢٢-ص٥٢٣
٣. أميره عبد العظيم محمد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، كلية الدراسات الإسلامية والعربية القاهرة، العدد٣٥، الجزء٣، القاهرة، ٢٠٢٠، ص٢٦٤-ص٢٦٥

٣. التعاون الدولي ومشاركة المعلومات: نظراً لطبيعة الفضاء السيبراني العابر للحدود الجغرافية، فالتعاون الدولي في هذا المجال في غاية الأهمية ولتعزيز الموثوقية في استخدام تكنولوجيا المعلومات والاتصالات للحفاظ على أمنها عند الاستعمال، لذا فإن التعاون الدولي يتطلب تعاون يتعلق بالأمن السيبراني من أجل تبادل وجهات النظر الدولية، وافساح المجال أمام تبادل المعلومات وافضل الممارسات على المستوى العالمي السيبراني، والمساعدة في التحقيق والاحكام الإجرائية والموضوعية المشتركة ولمعالجتها على نحو يمكن الحفاظ على الامن السيبراني للدول المتعاونة، وفي عامي ٢٠٠٣ و٢٠٠٥، اتفقت الدول في القمة العالمية لمجتمع المعلومات على ضرورة وضع وسائل وأدوات تتسم بالفعالية والكفاءة على المستوى الداخلي والخارجي للنهوض بالتعاون الدولي بشأن الامن السيبراني[١].

٤. انشاء الأطر القانونية والهياكل التنظيمية: من أجل حماية الأمن السيبراني العراقي لابد من وضع استراتيجية للحد من الهجمات السيبرانية التي تتعرض لها أجهزتها وانظمتها الحاسوبية وشبكات الانترنت، والتي تهدد الأمن الوطني العراقي، لا سيما إن أكثر من ١٣٠ دولة حول العالم قامت بإنشاء مؤسسات وتشكيلات غير تقليدية مختصة بالحروب السيبرانية ضمن أطار فرق الأمن الوطني، وظيفتها محاربة الجرائم الالكترونية، فضلاً عن توفير الوسائل والتقنيات التكنولوجية لدعمها ليضع المسؤولية أما القطاعين العام والخاص اتجاه حماية الفضاء السيبراني الوطني العراقي، فضلاً عن التركيز بصورة خاصة على ضمان توفير أنظمة المعلومات، وتعزيز الخصوصية، وحماية سرية المعلومات الشخصية للمواطنين[٢]

٥. **الاستخبارات السيبرانية:**

---

١ . **السعيد عبد الحميد إبراهيم، القوانيين والاتفاقات الدولية في مواجهة الهجمات السيبرانية، ط١(القاهرة: دار العلم والايمان لنشر والتوزيع، ٢٠٢٥)، ص٣٠.**

٢ . سالم محمد عبود، مصدر سبق ذكره، ص١٧٧.

قيام الدولة في زيادة أنشطتها السرية والاستخباراتية المتصاعدة في ظل توظيف الفضاء السيبراني، وتوظيف برمجيات التجسس والرصد والتحول من توجه الهجمات السيبرانية من الخارج الى الداخل الى توظيف عملاء الاستخبارات أو الدبلوماسيين المقيمين بشن هجمات من الداخل الى داخل الدولة، إذ بدأت الدول بتكثيف نشاطها الاستخباري عن طريق استخدام وسائل الفضاء السيبراني عبر الرصد والمراقبة للمواقع الالكترونية لمتابعة أنشطة المنظمات الإرهابية وجماعات الجرائم المنظمة[١].

الخاتمة: إن ظهور شبكات الانترنت، واكتشاف الفضاء السيبراني، وتصاعد العامل التكنولوجي الذي أصبح عنصراً من عناصر قوة الدولة، وإن تنامي التفاعلات الدولية بين اللاعبين المؤثرين وعلى المستوى الإقليمي والدولي، أدى ذلك الى انعكاسات سلبية على الأمن القومي للدول، التي لم تعد قادرة على السيطرة على التهديدات والمخاطر السيبرانية التي تتعرض لها، ومع زيادة التعقيدات الأمنية في ظل تنامي المشكلات العابرة لحدود الدولة، لا سيما في الفضاء السيبراني مثل الإرهاب السيبراني، والحرب السيبرانية، والامن السيبراني، والردع السيبراني، والتي افرزت واقع يهدد الأمن القومي للعديد من الدول، والذي يعتمد على اتباع سياسات داخلية وخارجية للحد من هذه المخاطر وتلك التهديدات الأمنية، لاسيما مع ظهور فواعل من غير الدول، إذ اتجهت لنمط جديد من التهديدات باستخدام شبكات الانترنت، والفضاء السيبراني لتجد الدول تحديات لا يمكن تجاهلها، لاسيما بعد أن أصبح الهجمات على أجهزة وأنظمة الحواسيب، ومحطات الطاقة والمياه، والمصارف المالية، والبورصات والبنوك، نمط جديد واستهداف الدول وما تملكه من البيانات والمعلومات الخاصة والعامة، ومن أجل سرقة وتخريب أو تدمير هذه البيانات الحكومية وغير الحكومية، لذا توجب على الدولة والشركات، وكذلك الافراد الى اتباع وسائل وأدوات وبرامج حماية خاصة للحد من مخاطر الهجمات السيبرانية التي تشن والتي تكون أغلب مصادرها غير معروفة، لذا توصل البحث الى جملة من الاستنتاجات وهي على النحو الاتي:

١ . احمد محمود أبو الحسن، التهديدات السيبرانية وأثرها على حماية البنى التحتية الخدمات الحيوية، ط١(القاهرة: العلم والايمان للنشر والتوزيع، ٢٠٢٥)، ص٧٨.

١. تطور مفهوم الأمن القومي تجاه التهديدات الجديدة وغير التقليدية، واتساع نطاقه ليشمل الجوانب العسكرية، والسياسية، والاقتصادية، والاجتماعية والثقافية، والتكنولوجية، بما إن أجهزة الدولة الالكترونية مفتوحة أمام الجميع، وهذا بسبب عدم وجود حدود جغرافية في الفضاء السيبراني، فأصبحت أجهزتها عرضة للتهديدات والمخاطر وتحت دوافع وأسباب مختلفة، مما يستلزم تبني استراتيجية وطنية للأمن السيبراني في هذا المجال.

٢. للأمن السيبراني أثر كبير في تعزيز قوة الدولة، عبر ظهور شكل جديد للقوة وهو القوة الالكترونية/ السيبرانية.

٣. كلما زاد استخدام الفضاء السيبراني، وشبكات الانترنت، إذ أصبحت الدولة أكثر عرضة للمخاطر والتهديدات السيبرانية، وتعرض أمنها السيبراني لمزيد من التهديدات.

٤. إن الأمن السيبراني لم يعد ذات تأثير على بعد واحد وهو البعد العسكري، وانما امتد ليشمل الابعاد الأخرى السياسية، والاقتصادية، والاجتماعية، نظراً لتزايد التفاعلات الدولية في الفضاء السيبراني.

المقترحات:

١. سن القوانين والتشريعات اللازمة بكيفية التعامل مع المخاطر والتهديدات التي قد تتعرض لها الدولة، عبر شبكات الانترنت، لردع المخالفين من الافراد (القراصنة)، وعقد اتفاقات مع دول أخرى لنفس الغرض

٢. الدخول في تحالفات سيبرانية مع الدول، لا سيما المجاورة للحد من الاخطار والتهديدات التي تتعرض لها أي دولة من الدول المتحالفة

٣. انشاء قيادة سيبرانية موحدة واجبها متابعة كل ما يدور في الفضاء السيبراني الخاص بالدولة، ومسؤوليتها الأساسية هو تحقيق الامن السيبراني، وكيفية الحفاظ عليه من أي اختراق.

٤. التعاون بين الأجهزة والوزارات الدولة ذات العلاقة بالأمن السيبراني وتوحيد الجهود من أجل منع أو تقليل الخسائر عند تعرض الدولة لهجمات سيبرانية معادية.

٥. الاحتفاظ بالبيانات والمعلومات الوطنية في أجهزة وأنظمة حواسيب مؤمنة بشكل كبير، حتى تكون عصية عن الاختراق

٦. اختيار الكوادر العاملة ممن يحملون صفة الأمانة والإخلاص للوطن للعمل على الأجهزة الحكومية، لمنع تسريب المعلومات والبيانات الخاصة بالحكومة، وتدريبهم للعمل على شبكة الانترنت والأجهزة الحكومية التي تتناول المعلومات والبيانات الخاصة بالدولة.

المصادر:

القران الكريم:

١. سورة قريش ٤.

٢. سورة البقرة ١٢٥

أولا. الكتب العربية والمترجمة:

١. احمد الكريدي، تحول مفهوم القوة في عصر المعلوماتية القوة الامريكية انموذجا، ط١ (الشارقة: الدار العربية للعلوم ناشرون، ٢٠٢٢).

٢. احمد محمود أبو الحسن، التهديدات السيبرانية وأثرها على حماية البنى التحتية الخدمات الحيوية، ط١(القاهرة: العلم والايمان للنشر والتوزيع، ٢٠٢٥).

٣. سالم محمد عبود، اساسيات الامن السيبراني، ط١(بغداد: دار الدكتور، ٢٠٢٢)، ص٤٢

٤. السعيد عبد الحميد إبراهيم، القوانيين والاتفاقات الدولية في مواجهة الهجمات السيبرانية، ط١(القاهرة: دار العلم والايمان لنشر والتوزيع، ٢٠٢٥).

٥. شريفة كلاع، الامن السيبراني واشكال التهديدات تحديات عالمية، ط١(عمان: الفا للوثائق ونشر واستيراد وتوزيع الكتب، ٢٠٢٣).

٦. عادل عبد الصادق، الاقتصاد الرقمي تحديات السيادة السيبرانية، ط١(القاهرة: المركز العربي لأبحاث الفضاء الالكتروني،٢٠٢٠).

٧. عبد الرزاق محمد السالمي، المدخل الى الامن السيبراني، ط١(بغداد: الذاكرة للنشر والتوزيع، ٢٠٢١).

٨. عبد القادر الهواري، حرب اللاعنف وعلاقته بالفوضى الخلاقة، ط١(القاهرة: المجلس الأعلى للثقافة، ٢٠٢١).

٩. علاء عبد الرزاق محمد السالمي، المدخل للأمن السيبراني، ط١(بغداد: الذاكرة للنشر والتوزيع،٢٠٢١).

١٠. فراس جمال شاكر، السيبرانية وتحولات القوة في النظام الدولي، ط١(عمان: دار أمجد للنشر والتوزيع، ٢٠٢٣).

١١. ماجد محمد الحنيطي، تكنولوجيا الصراعات الدولية المعاصرة، ط١(عمان: الآن ناشرون وموزعون،٢٠٢١).

١٢. مازن حميد شلال، فراس جمال شاكر، الامن في النظام الدولي ما بين القوة التقليدية والقوة الجديدة، ط١(بغداد: دار كلمة للطباعة والنشر والتوزيع،٢٠٢٢).

١٣. محمد محمود العمري، مدخل الى الامن السيبراني، ط١(عمان: دار زهران للنشر والتوزيع، ٢٠٢٠).

١٤. منصور عبد الكريم، ط١(القاهرة: دار الفاروق للاستثمارات الثقافية، ٢٠٢٢).

١٥. منى الأشقر جبور، السيبرانية هاجس العصر، ط١(بيروت: جامعة الدول العربية، المركز العربي للبحوث القانونية،٢٠١٦).

ثانياً: البحوث والدوريات:

١. اسلام فوزي، الامن السيبراني الابعاد الاجتماعية والقانونية تحليل سوسيولوجي، المجلة الاجتماعية القومية، المركز القومي للبحوث الاجتماعية والجنائية، القاهرة، المجلد٥٦، العدد٢، مايو٢٠١٩.

٢. أميره عبد العظيم محمد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، كلية الدراسات الإسلامية والعربية القاهرة، العدد٣٥، الج٣، القاهرة، ٢٠٢٠.

٣. ايمان عبد القادر، أثر الفضاء السيبراني على الامن القومي العربي خلال الفترة من٢٠١١ حتى٢٠٢٣، مجلة الامن القومي والاستراتيجي الاكاديمية العسكرية للدراسات العليا والاستراتيجية العدد الثالث، مصر، يناير٢٠٢٤.

٤. دنيا جواد مطلك، احمد عبد الجبار عبدالله، انعكاسات تطور القوة المعلوماتية الامريكية في البيئة الداخلية، مجلة حمورابي، العدد٣٥، بغداد، ٢٠٢٠.

٥. رشيد عمارة ياس، هيمن رؤوف سلام، الامن المجتمعي وفقاً لطروحات مدرسة كوبنهاغن، مجلة الدراسات السياسية والأمنية، المجلد٥ العدد الثاني، السليمانية، كانون الأول، ٢٠٢٢.

٦. رعد خضير صلبي، مجلة دراسات دولية، جامعة بغداد، مركز الدراسات الاستراتيجية والدولية، العدد٩٩، بغداد، أكتوبر ٢٠٢٤.

٧. رؤى عبدالله عبد الرحمن، اثر التنافس السيبراني الأمريكي الروسي على الامن العالمي في الفترة من٢٠١٥-٢٠٢٢، رسالة ماجستير غير منشورة جامعة التيلين، كلية الدراسات العليا، السودان، الخرطوم، ٢٠٢٤.

٨. صدام مرير حمد الجميلي، الحروب الهجينة وأثرها في مستقبل الصراع العالمي، مجلة جامعة تكريت، كلية العلوم السياسية، العدد٣٤، تكريت، اذار ٢٠٢٤.

٩. صفاء حسين علي، الحرب الالكترونية في المدرك الاستراتيجي الأمريكي، مجلة دراسات دولية، جامعة بغداد، بغداد، العدد٨٢، بغداد، ٢٠٢٠.

١٠. صلاح مهدي هادي، زيد محمد إسماعيل، الامن السيبراني كمرتكز جديد في الاستراتيجية العراقية، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، العدد٦٢، أيلول، ٢٠٢٠.

١١. لامية طالة، التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها، مجلة معالم للدراسات القانونية والسياسية، كلية العلام والاتصال، الجزائر، المجلد٤، العدد٢، الجزائر، ٢٠٢٠.

١٢. مروان سالم العلي، التحديات الاستراتيجية للأمن الوطني في ظل المتغيرات الدولية، مجلة كلية العلوم السياسية، جامعة تكريت، العدد٢٠، تكريت، تموز٢٠٢٠.

١٣. نور الدين ملاك، التهديدات السيبرانية عبر الفضاء الأزرق وتأثيرها على الامن القومي للدول، جريدة الشعب الجزائرية ديسمبر، ٢٠٢١. ينظر الرابط: https://www.ech-chaab.com/ar/ تاريخ الزيارة١٩/١٠/٢٠٢٤.

١٤. هربرت لين، النزاع السيبراني والقانون الإنساني، المجلة الدولية للصليب الأحمر، المجلد٤٩، العدد٨٨٦، ٢٠١٢.

١٥. يونس مؤيد يونس، استراتيجية الولايات المتحدة الامريكية للأمن السيبراني، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، بغداد، العدد ٥٥، ٢٠١٨.

1.Brian Weeder: Cyber offence and Defence as Mutually Exclusive National Policy Priorties in Kerstin Vignardetal(eds.), Confronting Cyber Confict, Disarmament Forum, United Nations Institute for Disamament Research Accessed on: August 2,2o13, P23