مجلة جامعة تشرين – سلسلة العلوم الاقتصادية والقانونية

Cybersecurity Threats in Syria and Its Implications for International Relations

Ammar Yaseen Mrhej[***]

(Received 12 / 9 / 2024. Accepted 24 / 10 / 2024)

□ ABSTRACT □

Cybersecurity is a vital field that focuses on protecting electronic systems and data from cyber attacks and threats. This field includes the application of a set of procedures and techniques that aim to protect data and ensure the confidentiality and integrity of information. Awareness and training for users are an essential part of cybersecurity strategies, as they contribute to enhancing the level of awareness of potential risks and available protection methods. Common threats in this field include ransomware attacks, database hacking, and malware. Technologies used in information security, such as encryption and intrusion detection systems, contribute to building a comprehensive protection system against these threats. This study addresses the concept of cybersecurity, its objectives, and its importance, in addition to the main strategies that can be adopted in this field. The most prominent findings reached by the researcher are:
Emphasizing the importance of cybersecurity as a strategy to protect systems and data, which contributes to maintaining trust and business continuity. The main objectives include protecting data and ensuring confidentiality and integrity, while adapting to changing threats. Organizations face multiple challenges, including a shortage of qualified personnel and the complexity of new threats, which affects the effectiveness of cybersecurity strategies.

These results emphasize the importance of cybersecurity as a fundamental element in protecting information and enhancing digital security in the modern era.

Keywords: Cybersecurity, Cybersecurity Threats.

[***] **Ph.D., Department of Economics and Planning, Faculty of Economics, Tishreen University, Latakia, Syria. ammarmerhej@tishreen.edu.sy**

تهديدات الأمن السيبراني في سورية وتداعياته على العلاقات الدولية

عمار ياسين مرهج ***

(تاريخ الإيداع 12 / 9 / 2024. قُبِل للنشر في 24 / 10 / 2024)

□ ملخّص □

يمثل الأمن السيبراني مجالاً حيوياً يركز على حماية الأنظمة والبيانات الإلكترونية من الهجمات والتهديدات السيبرانية. يتضمن هذا المجال تطبيق مجموعة من الإجراءات والتقنيات التي تهدف إلى حماية البيانات وضمان سرية وسلامة المعلومات. تُعدّ التوعية والتدريب للمستخدمين جزءًا أساسياً من استراتيجيات الأمن السيبراني، حيث يسهمان في تعزيز مستوى الوعي بالمخاطر المحتملة وأساليب الحماية المتاحة.

تشمل التهديدات الشائعة في هذا المجال هجمات الفدية، اختراق قواعد البيانات، والبرامج الضارة. وتساهم التقنيات المستخدمة في أمن المعلومات، مثل التشفير وأنظمة اكتشاف التسلل، في بناء منظومة حماية شاملة ضد هذه التهديدات.

تتناول هذه الدراسة مفهوم الأمن السيبراني، وأهدافه، وأهميته، بالإضافة إلى الاستراتيجيات الرئيسية التي يمكن اعتمادها في هذا المجال. ومن أبرز النتائج التي توصل إليها الباحث:

التأكيد على أهمية الأمن السيبراني كاستراتيجية لحماية الأنظمة والبيانات، مما يسهم في الحفاظ على الثقة واستمرارية الأعمال. تشمل الأهداف الأساسية حماية البيانات وضمان السرية والسلامة، مع ضرورة التكيف مع التهديدات المتغيرة. تواجه المؤسسات تحديات متعددة، منها نقص الكوادر المؤهلة وتعقيد التهديدات الجديدة، مما يؤثر على فعالية استراتيجيات الأمن السيبراني.

تؤكد هذه النتائج على أهمية الأمن السيبراني كعنصر أساسي في حماية المعلومات وتعزيز الأمان الرقمي في العصر الحديث.

الكلمات المفتاحية: الأمن السيبراني، تهديدات الأمن السيبراني.

*** دكتوراه - قسم الاقتصاد والتخطيط - كلية الاقتصاد - جامعة تشرين- اللاذقية سورية. ammarmerhej@tishreen.edu.sy

مقدمة:

في عصر التكنولوجيا الرقمية، أصبحت المعلومات أحد أهم الأصول التي تمتلكها المؤسسات والدول على حد سواء. ومع تزايد الاعتماد على الإنترنت والتقنيات الحديثة، ظهرت تحديات جديدة تتعلق بحماية هذه المعلومات من التهديدات السيبرانية، خاصة في سياق الأزمات السياسية والاقتصادية. في سورية، حيث تعاني البلاد من صراعات متعددة، أصبحت التهديدات السيبرانية تمثل خطرًا إضافيًا يهدد الاستقرار الوطني والعلاقات الدولية.

الأمن السيبراني هو مجموعة من الممارسات والتقنيات التي تهدف إلى حماية الأنظمة والشبكات والبيانات من الهجمات السيبرانية، والتي قد تؤدي إلى فقدان البيانات أو سرقتها أو حتى تدمير الأنظمة. تتزايد أهمية الأمن السيبراني بشكل مستمر، حيث تشير الإحصائيات إلى أن عدد الهجمات السيبرانية في تزايد مستمر، مما يهدد الأفراد والشركات والدول. هذه الهجمات تتنوع بين الفيروسات، البرمجيات الخبيثة، هجمات حجب الخدمة، والاختراقات، وقد تكون لها تداعيات خطيرة على العلاقات الدولية، خاصة عندما تتورط دول في تنفيذ هجمات سيبرانية ضد أخرى.

تعتبر الحماية من التهديدات السيبرانية مسؤولية مشتركة بين الأفراد والشركات والحكومات. فالأفراد يحتاجون إلى توعية حول كيفية حماية معلوماتهم الشخصية، بينما يجب على الشركات الاستثمار في تقنيات الأمان وتدريب موظفيهم على الممارسات الآمنة. من جهة أخرى، ينبغي على الحكومات وضع تشريعات وسياسات تدعم الأمان السيبراني وتعزز التعاون الدولي لمواجهة هذه التهديدات المتزايدة.

في هذه الدراسة، سنستعرض مفهوم الأمن السيبراني وأهميته في السياق السوري، التهديدات التي تواجهه، والتداعيات المحتملة على العلاقات الدولية. كما سنتناول دور الأفراد والشركات والحكومات في تعزيز الأمان السيبراني وكيف يمكن للجميع العمل معًا لحماية المعلومات والبيانات في ظل بيئة مليئة بالتحديات.

الدراسات السابقة:

1. دراسة (كلاع، 2021) بعنوان: الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني [1]

هدفت الدراسة إلى تحليل طبيعة التحديات الأمنية في الفضاء السيبراني وكيفية تحقيق الأمن السيبراني الوطني، لحل المشكلة التالية: ما طبيعة التحديات الأمنية في الفضاء السيبراني وكيف يمكن تحقيق الأمن السيبراني الوطني؟ واعتمدت المنهج التاريخي والإحصائي، وتوصلت إلى أن من يمتلك القوة السيبرانية والتكنولوجيا المتقدمة سيسيطر على الفضاء السيبراني ويحقق الأمن السيبراني الذي يدعم السيادة الوطنية الكاملة للدولة.

2. دراسة (صيوح وآخرون، 2022) بعنوان: دور الأمن السيبراني في الاستراتيجية الأمنية الإيرانية [2]

هدفت الدراسة إلى تحليل كيفية توظيف إيران لتقدمها في مجال الأمن السيبراني لوضع استراتيجية أمنية فعالة لصد الهجمات السيبرانية، لحل المشكلة التالية: كيف تمكنت إيران من استخدام قدراتها السيبرانية لتعزيز استراتيجيتها الأمنية؟ واعتمدت المنهج الوصفي التحليلي وأسلوب دراسة الحالة، من خلال التركيز على إيران كنموذج. وتوصلت الدراسة إلى أن الفضاء السيبراني أصبح ساحة جديدة للصراع الدولي، مما يتطلب وضع استراتيجيات دفاعية فعالة للكشف عن الهجمات السيبرانية وصدها.

3. دراسة (محمد، 2024) بعنوان: التهديدات السيبرانية وجرائم المعلومات [3]

هدفت الدراسة إلى تقييم كفاية الآليات الدولية لمواجهة التهديدات السيبرانية للحد من آثارها، لحل المشكلة التالية: ما مدى كفاية الآليات الدولية في المجال لمجابهة التهديدات السيبرانية؟ واعتمدت المنهج الوصفي التحليلي، وتوصلت إلى أهمية تطوير وتعزيز ثقافة الأمن السيبراني والتوعية بالقوانين المتعلقة بالجرائم السيبرانية عبر وسائل الإعلام.

4. دراسة (Mahdi, 2023) بعنوان: Cyber Security (الأمن السيبراني) [4]

هدفت الدراسة إلى تحليل تأثير الجرائم الإلكترونية على الأمن السيبراني وتقييم التدابير الحالية لمنع هذه الجرائم وفهم الإرهاب السيبراني، لحل المشكلة المتعلقة بحماية الأدلة في ظل تزايد الجرائم الإلكترونية وتأثيرها على الأمن السيبراني. واعتمدت المنهجية على مراجعة الأدبيات وتحليل حالات دراسية لتقديم أمثلة عملية على التهديدات والتدابير. وتوصلت الدراسة إلى أن هناك زيادة ملحوظة في الجرائم الإلكترونية تتطلب استجابة فعالة، وأن الهجمات الإلكترونية يمكن أن تكلف المؤسسات مليارات الدولارات، مما يبرز أهمية الاستثمار في الأمن السيبراني.

5. دراسة (Institute, 2024) بعنوان:

Geopolitical Implications of Artificial Intelligence in Cybersecurity: A Comprehensive Analysis

(التداعيات الجيوسياسية للذكاء الاصطناعي في مجال الأمن السيبراني: تحليل شامل) [5]

هدفت الدراسة إلى تحليل التداعيات الجيوسياسية للذكاء الاصطناعي في مجال الأمن السيبراني، مع التركيز على المزايا والتحديات التي يطرحها هذا التفاعل، وكيفية تأثيره على العلاقات الدولية وديناميكيات القوة. تمثلت مشكلة البحث في التحديات المتعددة الأوجه التي يطرحها استخدام الذكاء الاصطناعي في الأمن السيبراني، بما في ذلك عدم التوازن في القوة، والحرب السيبرانية المدعومة من الدول، والمخاوف الأخلاقية والقانونية المتعلقة بالخصوصية وحقوق الإنسان. اعتمدت الدراسة على المنهج الشامل والمتعدد الأبعاد، الذي يجمع بين الأساليب النوعية والكمية، بما في ذلك مراجعات الأدبيات ودراسات الحالة لتحليل الأسس المفاهيمية، بالإضافة إلى الأساليب الكمية لتحليل البيانات التجريبية وتقييم فعالية تطبيقات الذكاء الاصطناعي في الأمن السيبراني. تم التوصل إلى أهم النتائج بأن الذكاء الاصطناعي له تأثير تحويلي على الأمن السيبراني، مما يعزز القدرات الدفاعية ويزيد من التوترات الجيوسياسية، ويبرز أهمية التعاون الدولي لضمان المرونة السيبرانية العالمية.

6. دراسة (Mohiuddin, 2024) بعنوان:

Emerging Cybersecurity Threats: Mitigation Strategies Trends, and Implications

(التهديدات الأمنية السيبرانية الناشئة: استراتيجيات التخفيف والاتجاهات والتداعيات) [6]

هدفت الدراسة إلى استكشاف أحدث الاتجاهات في تهديدات الأمن السيبراني الناشئة وتداعياتها على الأفراد والمنظمات والمجتمع، واقتراح استراتيجيات فعالة للتخفيف من حدتها. وتمثلت مشكلة البحث في الطبيعة الديناميكية والمتغيرة باستمرار للتهديدات السيبرانية، مما يتطلب فهمًا شاملاً لهذه التهديدات وتداعياتها وفعالية استراتيجيات التخفيف الحالية. واعتمدت الدراسة على المنهجية التي تشمل إجراء مراجعة شاملة للأدبيات الموجودة، وتحليل أوراق البحث الحديثة وتقارير الصناعة ودراسات الحالة ذات الصلة. وتم التوصل إلى أهم النتائج التي تؤكد على أهمية فهم ومعالجة التهديدات الناشئة للأمن السيبراني، والحاجة إلى نهج استباقي وتعاوني يشمل جميع أصحاب المصلحة، بالإضافة إلى أهمية البحث المستمر والتوعية والاستعداد لبناء نظام بيئي رقمي مرن.

مشكلة البحث:

تعتبر مشكلة الأمن السيبراني من القضايا الحيوية التي تواجه الأفراد والمؤسسات في عصر التكنولوجيا الرقمية.

إن الاعتماد المتزايد على التكنولوجيا والإنترنت في مختلف جوانب الحياة، مثل الأعمال التجارية، التعليم، والرعاية الصحية، يطرح تحديات جديدة تتعلق بحماية المعلومات والبيانات الحساسة.

استناداً لما سبق يمكن صياغة مشكلة البحث في السؤال الرئيس: كيف يمكن تعزيز الأمن السيبراني في سورية لحماية المعلومات والبيانات من التهديدات المتزايدة في ظل التطورات التكنولوجية المستمرة؟

يتفرع عن السؤال الرئيسي عدة أسئلة فرعية:

1- ما هي أهم الاستراتيجيات والتقنيات الفعالة لحماية المعلومات؟

2- كيفية رفع مستوى الوعي حول أهمية الأمن السيبراني في المجتمع.

أهمية البحث و أهدافه:

أهداف البحث:

1. توضيح مفهوم الأمن السيبراني.

2. دراسة أنواع التهديدات التي تواجه الأفراد والشركات.

3. تقديم استراتيجيات وتقنيات فعالة لحماية المعلومات.

4. رفع مستوى الوعي حول أهمية الأمن السيبراني في المجتمع.

أهمية البحث:

تتجلى أهمية هذا البحث في عدة جوانب:

1. رفع مستوى الوعي حول أهمية الأمن السيبراني وكيفية حماية المعلومات الشخصية.

2. يوفر البحث تحليلًا شاملًا للتهديدات السيبرانية الحالية والمستقبلية.

3. يقدم البحث استراتيجيات فعالة يمكن للأفراد والشركات اعتمادها لحماية بياناتهم.

4. يعزز البحث من فهم أهمية التعاون الدولي في مواجهة التهديدات السيبرانية.

فرضيات البحث:

1. تزايد الاعتماد على التكنولوجيا يزيد من الحاجة إلى استراتيجيات وتقنيات فعالة لحماية المعلومات.

2. الشركات التي تستثمر في تقنيات الأمن السيبراني تكون أكثر قدرة على تعزيز مستوى الأمان وحماية بياناتها.

3. رفع مستوى الوعي حول أهمية الأمن السيبراني في المجتمع يسهم في تقليل مخاطر التعرض للهجمات السيبرانية.

منهجية البحث:

اعتمد الباحث في دراسته على المنهج الوصفي التحليلي لوصف وتحليل مفهوم الأمن السيبراني في سورية واستراتيجياته، بهدف الوصول إلى نتائج تسمح باقتراح التوصيات.

حدود البحث:

تمثلت حدود البحث في دراسة مفهوم الأمن السيبراني في سورية، مع التركيز على أنواع التهديدات التي تواجه الأفراد والشركات، واستراتيجيات حماية المعلومات. واجه الباحث تحديات تتعلق بنقص البيانات المتاحة، وتباين مستوى الوعي حول الأمن السيبراني، بالإضافة إلى قلة الدراسات السابقة التي تعالج هذا الموضوع بشكل مباشر في السياق السوري.

النتائج والمناقشة:

مفهوم الأمن السيبراني:

يشكل الأمن السيبراني تحدياً عالمياً معقداً يتطلب تفاعل الأفراد والحكومات. ومع ذلك، فإن الوعي العام بأهمية الأمن السيبراني لا يزال محدوداً، حيث ينظرون إلى الإنترنت كبيئة آمنة، مما يعرضهم للكثير من الهجمات الإلكترونية المتزايدة. هذه الهجمات تتسبب في تكبد الشركات والمؤسسات تكلفة عالية للتعامل مع الحوادث، حيث تتراوح خطورتها بين غير الضارة والشديدة.

تتزايد الحاجة إلى الأمن السيبراني في سورية نظراً لاعتمادها على تكنولوجيا المعلومات والاتصالات في جميع جوانب الحياة. وعلى الرغم من وجود بعض المواقع الحكومية المحمية، إلا أنها لا تزال عرضة للاختراق، وتشمل ذلك الوزارات والبنية التحتية الأساسية. يشير ذلك إلى عدم كفاية الجهود الحالية لحماية البيانات والأنظمة لمواجهة التهديدات المتزايدة.[7]

تُطلق على الهجمات السيبرانية العديد من المصطلحات مثل الحرب الافتراضية أو الحرب السيبرانية أو الحرب الإلكترونية. تشير هذه المصطلحات إلى الهجمات التي يشنها القراصنة لاستهداف الملفات والمواقع الأخرى، بما في ذلك المواقع الإلكترونية للمنشآت الحيوية أو الحواسيب التابعة للوحدات العسكرية أو الاقتصادية للدول. تعكس هذه الهجمات طبيعة الصِّراع الحديث وتبرز أهمية تعزيز الأمن السيبراني كاستجابة فعالة للتحديات المتزايدة في الفضاء الرقمي.

من الواضح أن الأمن السيبراني لا يعد مجرد مسألة تقنية، وإنما هو قضية شاملة تتطلب وعياً جماعياً وتعاوناً دولياً لمواجهة التهديدات المتزايدة وتحقيق بيئة رقمية أكثر أماناً للجميع. ينبغي على الحكومات والشركات والمواطنين تعزيز جهودهم في مجال الأمن السيبراني وتبادل المعلومات والخبرات لمكافحة هذه التهديدات وحماية البنية التحتية الرقمية والمعلومات الحيوية.[2]

عرف المعهد الوطني للمعايير والتقنية في الولايات المتحدة الأمريكية الأمن السيبراني بأنه النشاط أو العملية أو القدرة أو الإمكانية أو الحالة التي يتم من خلالها حماية نظم المعلومات والاتصالات، بالإضافة إلى المعلومات الواردة إليها، والدفاع عنها ضد الضرر أو الاستخدام أو التعديل غير المصرح به أو الاستغلال.[7]

بينما عُرف الأمن السيبراني بأنه يتعلق بتقليل المخاطر المتعلقة بالهجمات الخبيثة على البرمجيات وأجهزة الكمبيوتر والشبكات. ويتضمن ذلك الأدوات المستخدمة للكشف عن الاقتحامات ووقف الفيروسات ومنع وصولها، فضلاً عن فرض إجراءات التوثيق وتمكين الاتصالات المشفرة.[8]

يُعتبر الهجوم السيبراني، المعروف أيضاً بالحرب الافتراضية أو حرب الإنترنت، مفهوماً حديثاً في سياق النزاعات الدولية. يشير هذا المفهوم إلى الأساليب الحربية التي تعتمد على تكنولوجيا المعلومات، حيث تستهدف الأنظمة الحاسوبية والمواقع الإلكترونية. تتضمن هذه الهجمات مجموعة من العمليات، مثل:

1- التسلل إلى أنظمة الحاسوب: اختراق الأنظمة للوصول غير المصرح به إلى البيانات الحساسة.

2- جمع البيانات: استحواذ غير قانوني على المعلومات الهامة.

3- تصدير البيانات: نقل المعلومات المستهدفة إلى جهات خارجية بشكل غير مشروع.

4- إتلاف أو تغيير البيانات: تدمير أو تعديل البيانات بطرق تؤثر على سلامتها.

5- تشفير البيانات: استخدام برمجيات خبيثة لتشفير المعلومات وطلب فدية لفك تشفيرها.

6- زرع برمجيات ضارة: نشر برمجيات خبيثة لأغراض التجسس أو التخريب.

تُعتبر هذه العمليات جزءًا من الهجمات على البنية التحتية الحيوية للمعلومات، التي تُعرّف بأنها الأنظمة الأساسية التي تدعم الوظائف الحيوية للمجتمع والاقتصاد. وبالتالي، يُنظر إلى الهجمات السيبرانية كأشكال متطورة من القرصنة الإلكترونية، تمثل تهديدًا متزايدًا للأمن القومي والاقتصادي للدول.[3]

أما الحرب الإلكترونية فهي فرع من فروع الحروب الحديثة يستخدم التكنولوجيا والأساليب الإلكترونية للسيطرة أو التأثير في نظم الاتصالات والمعلومات للخصم، بهدف تعطيل قدرته على القتال أو التحرك بفاعلية.[9]

مما سبق توصل الباحث إلى أن الأمن السيبراني هو مجموعة من التقنيات والممارسات التي تهدف إلى حماية الأجهزة والبيانات والبرامج من الهجمات الإلكترونية والاختراقات، بما في ذلك حماية نظم المعلومات والاتصالات والتصدي للتهديدات والاستغلال غير المصرح به.

أهمية الأمن السيبراني:

1- حماية البيانات الحساسة: تتعامل الحكومات والمؤسسات العسكرية والمالية والطبية مع كميات ضخمة من البيانات الحساسة، مثل المعلومات الشخصية والمالية والملكية الفكرية، مما يستدعي ضرورة حمايتها من الدخول غير المصرح به.

2- تأثير الهجمات الإلكترونية على الأمن القومي: تمثل الهجمات الإلكترونية والتجسس الرقمي تهديدًا أكبر للأمن القومي مقارنة بخطر الإرهاب، مما يجعل من الضروري تعزيز الأمن السيبراني.

3- استهداف البنية التحتية الحيوية: يركز مجرمو الإنترنت على البنية التحتية الحيوية، حيث يمكن أن يؤدي الهجوم الناجح إلى تحقيق مكاسب مالية أو سياسية، مما يزيد من أهمية حماية هذه الأنظمة.

4- استغلال نقاط الضعف: تعتمد بعض الأنظمة على حلول حماية تجارية قد تكون عرضة للاستغلال، مما يستدعي تحسين مستوى الأمان السيبراني.

5- صعوبة تتبع المسؤولية: تواجه الحوادث السيبرانية تحديات في تحديد المسؤولية، حيث يصعب تتبع مرتكبي الهجمات، مما يعقد جهود التحقيق والاستجابة.

6- تعقيد التهديدات السيبرانية: يصعب التنبؤ بالتهديدات السيبرانية، ويتطلب اتخاذ التدابير الوقائية في الوقت المناسب، مما يزيد من خطر الهجمات الناجحة.

7- مراحل الهجوم السيبراني: تتطور الهجمات وفق خمس مراحل، بدءًا من العثور على ثغرة أمنية وصولًا إلى تنفيذ الهجوم، مما يتطلب استراتيجيات متعددة لمنع الحوادث.

8- تحسين الأمن السيبراني كإستراتيجية وقائية: يعد تحسين الأمن السيبراني هو الحل الأمثل لمنع الحوادث السيبرانية وتقليل المخاطر المحتملة.

9- يحمي الأمن السيبراني مختلف أنواع البيانات الحساسة والمهمة من تعرضها للسرقة أو الإتلاف.

10- توفير بيئة عمل آمنة جداً خلال العمل عبر الشبكة العنكبوتية.

11- الحفاظ على المعلومات وتجانسها وسلامتها وذلك يكف الأيادي من العبث بها وتحقيق وفرة البيانات وجاهزيتها عند الحاجة إليها.

12- مقاومة التهديدات المتعمدة وغير المتعمدة والاستجابة والتعافي.

تتطلب هذه العوامل مجتمعة اهتماماً جاداً واستراتيجيات فعالة لتعزيز الأمن السيبراني في مختلف القطاعات. [7] و[10] و[11]

مما سبق توصل الباحث إلى أن أهمية الأمن السيبراني تُظهر ضرورة تكامل الجهود بين مختلف القطاعات لحماية البيانات الحساسة والبنية التحتية الحيوية. إن تطوير استراتيجيات فعالة لمواجهة التهديدات المتزايدة يُعد أمراً حيوياً لضمان استقرار وأمان المجتمعات في عصر التكنولوجيا الحديثة.

أهداف الأمن السيبراني:

يمكن تحديد أهم أهداف الأمن السيبراني بالآتي:

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.[7]

4- النشاط الذي يؤمن حماية الموارد البشرية، والمالية، المرتبطة بتقنيات الاتصالات والمعلومات.

5- ضمان إمكانيات الحد من الخسائر والأضرار.

6- إعادة الوضع لما كان عليه، بأسرع وقت ممكن، بحيث يمنع عجلة الانتاج عن التوقف، ومنع تحول الأضرار إلى خسائر.[8]

وإن أبرز الأهداف التي يعمل الأمن السيبراني على تحقيقها الآتي:[12]

1- أن يحافظ على أمن المجتمع واستقراره.

2- أن يحافظ على سلامة عمل قطاعات الدولة الإلكترونية من أي اختراق.

3- أن يحمى شبكة المعلومات بصورة علمية وتقنية محكمة.

4- أن يحفظ بيانات ومعلومات إلكترونية مهمة لأي جهة كانت.

5- أن يعمل على تشفير التعاملات الإلكترونية بحيث لا يستطيع أي مخترق الدخول إليها ويعتبر التشفير أحد أهم أساليب الحماية.

مما سبق توصل الباحث إلى أن أهداف الأمن السيبراني تُعد حيوية لضمان حماية المعلومات والأنظمة، حيث تساهم في تعزيز الثقة بين المستخدمين والمؤسسات. وإضافةً إلى الأهداف المذكورة، يمكن تضمين أهداف جديدة مثل:

1- تعزيز الوعي والتثقيف السيبراني للمستخدمين.

2- تطوير استراتيجيات استجابة سريعة للحوادث السيبرانية.

3- تعزيز التعاون الدولي لمكافحة التهديدات السيبرانية العابرة للحدود.

أبعاد الأمن السيبراني:

بهدف تحقيق أمن قومي متكامل للدول لمواجهة الهجمات السيبرانية ينطوي مفهوم الأمن أبعاداً كثيرةص تشمل أغلب النواحي الجوهرية في أي دولة ومنها:

1- البعد العسكري: أن يؤمن الأمن السيبراني للقوات العسكرية التواصل وتبادل المعلومات والأوامر عن بعد بصورة آمنة، مع لزوم أن يكون قادراً على صد أي محاولة اختراق، قد تصل إلى تدمير البيانات العسكرية لدولة العدو، بحيث يمس الأمن القومي كما حدث في إيران عند اختراق منشآتها النووية.[12]

2- البعد الاقتصادي: تظهر أهمية الأمن السيبراني بشكل أوسع وأكبر في المجال الإقتصادي لأن الفضاء الإلكتروني أصبح أساساً للتعاملات التجارية والمالية والإقتصادية وأصبح الحاسوب أداة لتسيير الصناعة والإقتصاد وهذا يستدعي الحرص على تحقيقه.[13]

3- البعد الاجتماعي: لقد جاء فى تقرير الاتحاد الدولى للاتصالات (ITY) 2010 بشأن الأبعاد الاجتماعية للأمن السيبرانى أن الثورة الرقمية غيرت كيفية التعامل التجارى، وكيفية عمل الحكومات. وأدت العولمة والتقدم التكنولوجى إلى إضعاف البنية التحتية وبالتالى جعلتها هدفاً محتملاً لهجمات إرهابية، حيث تُواجه البلدان مخاطر حقيقية؛ للأعداء أن يستغلوا مواطن الضعف التي تعانى منها أنظمة المعلومات الدقيقة. فهم يسعون إلى تعطيل البنية التحتية والموارد الأساسية من أجل تهديد الأمن القومى.[14]

4- البعد السياسي: هناك أمثلة كثيرة تدفع نحو الاهتمام بالبعد السياسي للأمن السيبراني، كالتسريبات المختلفة للوثائق الحساسة التي تؤدي إلى مشكلات معقدة على المستوى الخارجي والدولي، علماً أنه لا ينكر أحد الدور الفعال للشبكات التواصل الاجتماعي على المستوى السياسي كحملات انتخابية، تظاهرات افتراضية، حركات احتجاجية إلكترونية. ... كما يتم استغلال هذه المواقع من طرف العديد من الحكومات لتحقيق أهداف سياسية.[2]

5- البعد القانوني: يترتب على النشاط الفردي والمؤسساتي والحكومي في الفضاء السيبراني، نتائج قانونية، وموجبات تستدعي اهتماما خاص لحل النزاعات التي يمكن أن تنشأ عنها. وهو ما يستدعي مواكبة التحولات التي رافقت ظهور مجتمع المعلومات فظهرت حقوق أخرى، كحق النفاذ إلى الشبكة العالمية للمعلومات، وتوسعت بعض المفاهيم، لتشمل أساليب الممارسة الجديدة باستخدام تقنيات المعلومات والاتصالات، كالحق في إنشاء المدونات الالكترونية، والحق في إنشاء التجمعات على الانترنت، والحق في حماية ملكية البرامج المعلوماتية. كما ظهرت موجبات جديدة ذات انعكاسات اقتصادية مثل: موجب الاحتفاظ ببيانات الاتصالات، وموجب الإبلاغ عن مخالفات وجرائم خاصة بالمحتوى.

كل هذه التغيرات والتحولات تستدعي وجود ترسانة قانونية تنسجم مع التطورات الحاصلة، إن على مستوى الحقوق، أو على مستوى البيئات والعمليات.[8]

مما سبق توصل الباحث إلى أن الأبعاد المتعددة للأمن السيبراني تُظهر ضرورة تكامل الجهود بين المجالات العسكرية، الاقتصادية، الاجتماعية، السياسية، والقانونية لحماية الأمن القومي. إن الفهم الشامل لهذه الأبعاد يُعزز من قدرة الدول على مواجهة التهديدات السيبرانية بفعالية، ويؤكد على أهمية تطوير استراتيجيات متكاملة تضمن استقرار المجتمع وحمايته من المخاطر المحتملة في الفضاء الرقمي.

خصائص الأمن السيبراني:

بما أن الجريمة الإلكترونية تتم بمنهجية وأساليب جديدة ذات بعد تكنولوجي أعلى من الجرائم التقليدية كان لابد أن يأتي الأمن السيبراني للتغلب على هذه المشكلة من خلال مواكب التطور التكنولوجي ولذا تميز الأمن السيبراني بعدد من الخصائص منها الآتي:

1- الاكتشاف والتعقب: حيث يهدف الأمن السيبراني إلى اكتشاف الجريمة الإلكترونية وتعقب أثرها وبالتالي التغلب عليها.

2- السرعة وغياب الدليل: فصعوبات اثبات الجرائم الإلكترونية نظراً لاستخدام المخترقين وسائل تقنية حديثة أتى الأمن السيبراني بتقنيات حديثة عالية تفوق خبرة المجرم.

3- ضعف الأجهزة الأمنية والقضائية: تجاه التعامل مع الجرائم الإلكترونية نتيجة لنقص الخبرة الرقمية لدى الأجهزة الأمنية مما يعزز دور الأمن السيبراني في تحقيق الأمن الرقمي للمنظمات في حماية البيانات والبنى التحتية لتلك المنظمات.[15]

ويتميز الأمن السيبراني بمجموعة من الخصائص وهي الهيئة الوطنية للأمن السيبراني (2018):[11]

1- ضمان الوصول المنطقي إلى الأصول المعلوماتية والتقنية للمؤسسة، وذلك لمنع الوصول غير المصرح به وتقييد الوصول لما هو مطلوب لإنجاز الأعمال المتعلقة بالجهة.

2- قدرته على حماية أنظمة وأجهزة معالجة المعلومات بما في ذلك أجهزة المستخدمين والبنى التحتية للمؤسسة، وكذلك القدرة على حماية البريد الإلكتروني من المخاطر السيبرانية.

3- لديه قدرة على حماية وإدارة أمن الشبكات.

4- ضمان حماية أجهزة المؤسسة المحمولة بما في ذلك أجهزة الحاسب المحمول والهواتف الذكية والأجهزة الذكية اللوحية من المخاطر السيبرانية. وضمان التعامل بشكل أمن مع المعلومات الحساسة والمعلومات الخاصة بأعمال الجهة وحمايتها أثناء النقل والتخزين عند استخدام الأجهزة الشخصية للعاملين في المؤسسة.

5- السرية وسلامة البيانات والمعلومات ودقتها وتوافرها وفق السياسات والإجراءات التنظيمية للمؤسسة.

مما سبق توصل الباحث إلى أن خصائص الأمن السيبراني تُظهر أهمية التكيف مع التحديات المتزايدة في الفضاء الرقمي، حيث يتطلب الأمر تقنيات متقدمة واستراتيجيات فعالة لمواجهة الجريمة الإلكترونية. كما أن تعزيز الوعي والتدريب لدى الأجهزة الأمنية والمستخدمين يعد خطوة أساسية لضمان حماية فعالة ومستدامة للبيانات والبنى التحتية.

أنواع التهديدات السيبرانية:

تتنوع التهديدات السيبرانية وفقاً لنوعها وأهدافها، ويمكن تصنيفها إلى عدة فئات رئيسية:

1- التهديدات التي تلحق بمكونات الكمبيوتر: تشمل هذه التهديدات الأضرار التي قد تصيب المكونات المادية مثل وحدات الإدخال والإخراج، والأقراص الصلبة، والطابعات، بالإضافة إلى المكونات المعنوية مثل البيانات والمعلومات المخزنة. يمكن أن تتسبب هذه الجرائم في تدمير هذه المكونات كلياً أو جزئياً، أو نقل الفيروسات إلى حواسيب أخرى. من الأمثلة الشائعة على ذلك فيروس الفدية الذي يُستخدم لتشفير البيانات وطلب فدية لفك تشفيرها.

2- التهديدات التي تمس بشبكة المعلومات: تستهدف هذه التهديدات المواقع الإلكترونية بغرض تعطيلها أو التشويش عليها أو تعديل محتواها. وغالبًا ما تُستخدم عناوين IP مزيفة للدخول إلى الشبكة، مما يسهل نقل الفيروسات وإرسال الرسائل الضارة.

3- التهديدات التي تقع على البيانات والمعلومات: تشمل هذه الأفعال غير القانونية التي تستهدف وثائق أو نصوص موجودة على الشبكة بهدف سرقتها أو تعديلها أو إتلافها. من الأمثلة على ذلك انتهاك الملكية الفكرية للبرامج أو الأعمال الفنية والأدبية، حيث يمكن للمتطفلين مراقبة وتنصت الاتصالات الإلكترونية.[3]

المجالات التي تقع عليها التهديدات السيبرانية:

يمتد نطاق الجريمة السيبرانية ليشمل جميع جوانب حياة الأفراد والمجتمعات، بدءًا من التدخل في الحياة الخاصة وصولاً إلى الأمن القومي:

1- التهديدات السيبرانية وتأثيرها على الحياة الخاصة: مع ظهور العالم الإلكتروني، أصبحت حياة الأفراد الخاصة معرضة للخطر نتيجة توافر إمكانيات السطو والاطلاع على المعلومات الحساسة. يمكن أن تتضمن هذه التهديدات التهديد والمضايقة وانتحال الشخصية والاستدراج ونشر المحتوى غير اللائق.

2- التهديدات السيبرانية وتأثيرها على الأموال: شهدت المعاملات المالية تحولاً كبيراً نحو الشبكات الإلكترونية، مما أدى إلى تطور وسائل الدفع الإلكتروني. وهذا بدوره ساهم في زيادة الجريمة الإلكترونية بهدف الحصول على الأموال بطرق غير قانونية، مثل الاحتيال على بطاقات الائتمان وسرقة الأموال من البنوك وغسيل الأموال.

3- التهديدات السيبرانية وأمن الدولة: يُعتبر الأمن القومي للدولة خطاً أحمر لا يجوز المساس به، حيث إن الجرائم السيبرانية مثل الإرهاب والتجسس والجوسسة المضادة تمثل تهديداً مباشراً لوجود الدولة ومؤسساتها.[9]

مما سبق توصل الباحث إلى أن التهديدات السيبرانية تشكل تحدياً كبيراً للأمن الوطني في سورية، ولها تداعيات محتملة على العلاقات الدولية. فمع تزايد هذه التهديدات، يصبح من الضروري تعزيز التعاون الدولي وتطوير استراتيجيات فعالة لمواجهة هذه المخاطر وتعزيز الأمن السيبراني في جميع المجالات.

الردع السيبراني:

تمثل تهديدات الأمن السيبراني تحدياً متزايداً في المشهد الدولي، حيث أن هذه التهديدات لا تقتصر على الدول فقط بل تشمل أيضاً الأفراد والمنظمات على نطاق واسع. يتسارع الردع السيبراني كأداة أساسية في مواجهة هذه التهديدات، حيث يُفهم على أنه تكتيك يهدف إلى تثبيط الأعداء عن القيام بأعمال عدائية غير مرغوب فيها عن طريق تعزيز القدرات الدفاعية وخلق بيئة من الخوف من العواقب.

أولاً: استراتيجية الدفاع السيبراني: تتضمن أدوات الدفاع السيبراني طيفاً واسعاً من الأساليب، بما في ذلك البرامج الخبيثة، هجمات الخوادم، وهجمات عدم الخدمة الموزعة (DDoS). تنقسم هذه الأدوات إلى فئات متنوعة:

1. البرمجيات الخبيثة (Malware)
2. هجمات منصات الخوادم (Platform Attacks)
3. هجمات رفض الخدمة الموزعة (DDoS)

بينما تُعتبر البرمجيات الخبيثة أسلحة ضمن مخطط الحرب السيبرانية، فإن هجمات الخوادم ورفض الخدمة تعكس أساليب تنفيذ هذه الحرب.

ثانياً: الاستراتيجية في مواجهة التهديدات السيبرانية: من خلال التحليل، نجد أن الجرائم الإلكترونية تواصل تطورها دون حدود، حيث تسهم التكنولوجيا الحديثة في توفير أدوات دقيقة للإختراقات، مما ينتج عنه تعزيز فرص نجاح هذه الهجمات حتى ضد المنظمات العسكرية. وفي السياق السوري، تعتبر الجغرافيا السياسية والتوترات الحاصلة بيئة خصبة لتهديدات الأمن السيبراني.

في الحالة السورية، تتجلى المخاطر الناجمة عن الأزمات السياسية والاقتصادية في تراجع القدرة على مواجهة التحديات السيبرانية. تواجه سورية، كما هو الحال في دول أخرى، الحاجة الملحة لتطوير سياسات شاملة تهدف إلى حماية البنية التحتية الرقمية، وتعزيز الاستعدادات ضد الهجمات السيبرانية. لذا، من الضروري العمل على وضع استراتيجيات أمنية متعددة التخصصات تشمل عناصر تشريعية، تنظيمية، تقنية، وبشرية.

يساهم التعاون الدولي في تعزيز القدرات الوطنية في مواجهة المخاطر السيبرانية. من خلال الاستفادة من تجارب الدول الأخرى، يمكن لسورية أن تطوّر استراتيجيات فعالة في مواجهة التهديدات الرقمية. كما يتوجب أن تتم عملية تنفيذ هذه السياسات بحذر، مع التركيز على الحفاظ على حقوق الإنسان والحريات الفردية بشكل متوازن.[10]

مما سبق توصل الباحث إلى أن الردع السيبراني يمثل ضرورة أساسية لمواجهة التهديدات المتزايدة في الفضاء الرقمي. إن الفهم الدقيق لطبيعة هذه التهديدات وتطوير استراتيجيات شاملة يمكن أن يؤثر بشكل كبير على الأمن الوطني والعلاقات الدولية..

وقد أصبحت الاستراتيجيات السيبرانية تتشكل على مستويات متعددة، حيث تشمل الدفاع المسلح والجهات المدنية مثل وزارات العدل والداخلية والصناعة والاتصالات، بالإضافة إلى الجهات الاقتصادية كالشركات. وتعتمد هذه الاستراتيجيات على معايير محددة تتجلى بشكل خاص في السياق السوري الذي يواجه تحديات معقدة، مما يحتم تقييمها في إطار العلاقات الدولية.[1]

1- الثقافة الاستراتيجية: تشكل الثقافة الاستراتيجية إحدى العوامل الرئيسية في صياغة استراتيجيات الأمن السيبراني. تعتمد هذه الثقافة على المعتقدات المشتركة والتصورات التاريخية والهوية الوطنية، بالإضافة إلى العلاقات مع الدول الأخرى ومدى قبولها للمعايير الدولية. وفي حالة الدول الصغيرة مثل سورية، تمثل الحرب غير المتماثلة جزءًا من تجربتها التاريخية، مما يثير التساؤل حول ما إذا كان يمكن إدماج استراتيجية الدفاع السيبراني ضمن هذا الإطار. وفي المقابل، قد تجد الدول الكبرى عدم الحاجة لاعتماد استراتيجيات غير متماثلة في الفضاء السيبراني نظرًا لقوتها وتقديراتها المختلفة للوضع الدولي.

2- توصيف التهديدات: يجب أن يستند تطوير الاستراتيجيات السيبرانية إلى توصيف دقيق للتهديدات والتحديات المحدقة. يتطلب هذا الأمر فهماً شاملاً للأولويات الوطنية والتحديات الأمنية التي تواجه سورية، وخاصة في ظل الظروف الراهنة من الصراعات الداخلية والتهديدات الخارجية.

3- طبيعة الدولة: تؤثر طبيعة الدولة بشكل كبير في صياغة استراتيجيات الأمن السيبراني. فمن الضروري تحليل ما إذا كانت الدول الصغيرة تمتلك أهدافاً مماثلة لتلك التي تسعى إليها الدول الكبرى. هل تستطيع الدول الصغيرة، مثل سورية، المطالبة باستغلال أدوات القضاء السيبراني بنفس الطريقة التي تستخدمها الدول الكبرى لمواجهة التحديات المتشابهة؟

4- تأثير الدول الكبرى: تلعب الدول المسيطرة دورًا بارزًا في صياغة الاستراتيجيات الوطنية للدول الأخرى، حيث تفرض نماذج معينة وتوجهات استراتيجية. يمكن أن تؤثر هذه النماذج على كيفية تطوير الدول، بما في ذلك سورية، لاستراتيجيات الأمن السيبراني الخاصة بها. هنا يبرز أهمية التحليل المقارن الذي يمكن أن يكشف عن أوجه الاختلاف والتشابه بين الاستراتيجيات الوطنية وتأثيراتها على العلاقات الدولية.

5- المعايير الدولية: يعتمد تطوير المعايير الدولية للأمن السيبراني بشكل كبير على استراتيجيات الدول الكبرى. هذه المعايير تشكل إطارًا يجب أن يتكيف معه جميع الفاعلين في الغلاف السيبراني، بما في ذلك سورية. بالتالي، يمثل

التفاعل بين المعايير الدولية والاستراتيجيات الوطنية تحديًا إضافيًا يتعين على سورية مواجهته في سعيها لتعزيز أمنها السيبراني وضمان استقرار علاقاتها الدولية.

مما سبق نستنتج أن الحاجة الملحة لتحليل استراتيجيات الأمن السيبراني في سورية تظهر في إطار العلاقات الدولية، حيث يمكن أن تسهم في فهم أعمق للتحديات الراهنة وتعزيز القدرة على مواجهة المخاطر التقنية والسياسية.

تهديدات الأمن السيبراني في سورية وتداعياته في العلاقات الدولية:

تواجه سورية مجموعة من التحديات الجوهرية في مجال الأمن السيبراني، يمكن تلخيصها في النقاط التالية:

1- العنصر البشري: يُعتبر العنصر البشري من أبرز التحديات، حيث يتجلى ذلك في الصعوبات المتعلقة بالتحكم في ردود الفعل العاطفية وفهم القضايا الأمنية، التي تعتمد في النهاية على أحكام بشرية. يعتمد تصميم وإدارة أنظمة الأمن على الكفاءات البشرية، مما يجعلها عرضة للأخطاء وسوء الاستخدام. كما أن نقص المتخصصين في أمن المعلومات يمثل تحدياً كبيراً، مما يهدد قدرة الشركات على تأمين منظوماتها وأصولها.

2- المخاطر المرتبطة بالمنظمات: تتعرض المنظمات لمخاطر كبيرة عند استخدامها للفضاء السيبراني، مما يجعلها عرضة للهجمات والاختراقات.

3- ثغرات التشفير وكلمات المرور: تبقى تقنيات التشفير عرضة لنقاط الضعف، وكلمات المرور يمكن كسرها، مما يسهل عمليات الاختراق.

4- ابتكار الهجمات السيبرانية: يتطلب الابتكار المستمر في تقنيات الهجمات أن تتكيف استراتيجيات تقييم المخاطر التقليدية مع التهديدات الحديثة والمستقبلية.

5- تطور التهديدات: تظهر تقنيات جديدة تبث نقاط ضعف لم تكن موجودة سابقًا، حتى في الشركات التي تمتلك موارد كافية لمواجهة هذه التحديات.

6- توسع الهجمات السيبرانية: يُعزى توسع الهجمات إلى الزيادة الكبيرة في عدد الأجهزة المتصلة بالإنترنت (IoT) وارتفاع عدد مستخدمي الإنترنت، بالإضافة إلى تهديدات الدول فيما بينها التي أدت إلى تفشي الحروب السيبرانية والتجسس.

7- المرونة السيبرانية: تُعتبر المرونة السيبرانية ميزة حيوية للشركات، حيث تتطلب القدرة على التكيف مع التهديدات المتطورة واستعادة القدرات سريعًا بعد الهجمات. ومع ذلك، فإن العديد من الشركات لم تقم بإقامة تدريبات عملية لحل الأزمات.

8- الإطار التشريعي: يجب أن تكون القوانين المتعلقة بالأمن السيبراني مرنة وسريعة للتكيف مع التطورات المستمرة في الجرائم السيبرانية لضمان القدرة على مكافحتها بشكل فعال.

يتضح للباحث من خلال ما سبق من خلال استعراض التحديات الأساسية في الأمن السيبراني، أن العنصر البشري يُعتبر الحلقة الأضعف في سلسلة الحماية، مما يستدعي تعزيز الوعي والتدريب المستمر. كما أن الحاجة إلى تطوير الإطار التشريعي للتصدي للجرائم السيبرانية تُعد أمراً حيوياً لتمكين سورية من ضمان أمانها السيبراني وتعزيز استقرار علاقاتها الدولية.

وحول تهديدات الأمن السيبراني في سورية، يمكننا أن نستنتج أن الأمن السيبراني أصبح ضرورة ملحة أكثر من أي وقت مضى. فعلى الرغم من التقدم التكنولوجي السريع الذي يوفر فوائد متعددة، إلا أنه يحمل معه مجموعة من

المخاطر الجسيمة. تواجه سورية، مثل العديد من الدول الأخرى، تحديات كبيرة في حماية بياناتها ومعلوماتها الحساسة من الاختراقات والهجمات السيبرانية التي قد تهدد استقرارها وأمنها القومي.

تتطور العمليات السيبرانية المعقدة باستمرار، مما يعرض الأمن الحكومي والتجاري والأمن الشخصي للخطر. لذلك، يتعين على كافة الأطراف المعنية في سورية اتخاذ خطوات فعالة لتعزيز الأمن السيبراني في السياقات المختلفة.

تَعتبر توعية المستخدمين وتدريبهم على التعامل مع التهديدات السيبرانية من الخطوات الأساسية لتحقيق أمان أفضل. يتعين على الأفراد أن يكونوا مدركين للمخاطر المحتملة، وأن يتعلموا كيفية التعرف على الرسائل الاحتيالية والروابط الضارة، بالإضافة إلى فهم كيفية استخدام أدوات الحماية المتاحة.

علاوة على ذلك، يجب على الشركات والمؤسسات الحكومية تطوير استراتيجيات أمنية قوية لحماية أنظمتها وشبكاتها من الهجمات السيبرانية. يتوجب تخصيص المزيد من الموارد للاستثمار في تحسين إجراءات الأمان وتعزيز الحماية الاستباقية.

في السياق الدولي، يجب أن تتعاون الحكومات والمجتمع الدولي لإقامة إطار قانوني متين يهدف إلى مكافحة الهجمات السيبرانية عبر الحدود. ويتعين إنفاذ قوانين صارمة لمحاسبة المهاجمين وضمان تحقيق العدالة.

باختصار، تمثل تهديدات الأمن السيبراني تحدياً حقيقياً في ظل التطور التكنولوجي المستمر، ويتطلب الأمر جهوداً جماعية من الأفراد والمؤسسات للتعرف على هذه التهديدات والتصدي لها. إن مستقبل الأمن السيبراني في سورية يعتمد على قدرتها على حماية بيئتها السيبرانية والتكيف مع التغيرات السريعة، بما يضمن استقرارها وأمنها على الصعيدين الوطني والدولي.

الاستنتاجات والتوصيات:

الاستنتاجات:

1- الأمن السيبراني هو مجموعة من الاستراتيجيات والتقنيات التي تهدف إلى حماية الأنظمة والشبكات والبيانات من التهديدات الإلكترونية.

2- يعد الأمن السيبراني ضرورياً لحماية المعلومات الحساسة وضمان استمرارية الأعمال، مما يسهم في الحفاظ على الثقة بين المستخدمين والمزودين.

3- تشمل الأهداف الأساسية للأمن السيبراني حماية البيانات، ضمان سرية المعلومات، الحفاظ على سلامة الأنظمة، وضمان توفر الخدمات في جميع الأوقات.

4- تتضمن الاستراتيجيات الفعالة استخدام تقنيات التشفير، تطبيق سياسات الوصول، التدريب المستمر للموظفين، وتطوير خطط استجابة للحوادث.

5- يجب أن يكون الأمن السيبراني مرنًا وقابلًا للتكيف مع التهديدات المتغيرة، بالإضافة إلى كونه شاملًا ومتكاملًا لجميع جوانب التكنولوجيا المستخدمة.

6- تواجه المؤسسات تحديات متعددة مثل نقص الكوادر المؤهلة، تعقيد التهديدات الجديدة، والقيود القانونية والتنظيمية التي تؤثر على فعالية استراتيجيات الأمن السيبراني.

الاستنتاجات و التوصيات:

1- تطوير استراتيجيات وطنية: يُوصى بتطوير استراتيجيات وطنية شاملة للأمن السيبراني تشمل جميع القطاعات الحيوية في سورية، لتعزيز القدرة على مواجهة التهديدات.

2- زيادة الوعي والتدريب: يجب تعزيز برامج التدريب والتوعية للعاملين في مجال تكنولوجيا المعلومات والمستخدمين العاديين حول أهمية الأمن السيبراني وأساليب الحماية.

3- تعزيز التعاون الدولي: من الضروري تعزيز التعاون الدولي بين الدول لمشاركة المعلومات والخبرات المتعلقة بالتهديدات السيبرانية، مما يسهم في تحسين مستوى الأمن على الصعيد العالمي..

4- استثمار في التكنولوجيا: يتطلب الأمر استثمارًا مستمرًا في التقنيات الحديثة لمواجهة التهديدات المتزايدة وتحسين مستوى الحماية في المؤسسات.

5- تحديث التشريعات: يجب تحديث القوانين والتشريعات المتعلقة بالأمن السيبراني لتواكب التطورات السريعة في هذا المجال، مما يساهم في توفير إطار قانوني مناسب لحماية البيانات.

6- إنشاء فرق استجابة سريعة: يُنصح بإنشاء فرق متخصصة للاستجابة السريعة للحوادث السيبرانية لضمان التعامل الفوري مع أي تهديدات.

7- تقييم دوري للمخاطر: ينبغي إجراء تقييمات دورية للمخاطر لتحديد الثغرات وتحديث استراتيجيات الحماية وفقًا للتهديدات الحالية والمستقبلية..

بتطبيق هذه النتائج والتوصيات، يمكن تعزيز مستوى الأمن السيبراني في سورية وتحقيق حماية فعالة للأنظمة والمعلومات، مما يسهم في تحسين العلاقات الدولية ويعزز الثقة بين الدول في مواجهة التهديدات الإلكترونية.

References:

1- Kala, Sherifa. Cybersecurity and the challenges of espionage and electronic hacking of countries via cyberspace. Journal of Law and Human Sciences, University of Algiers, Volume (15), Issue (01), 2021, 292-314.
2- Sayyouh, Louay. Laiqa, Rami. Al-Hoshi, Ramadan. The Role of Cybersecurity in the Iranian Security Strategy. Tishreen University Journal of Economic and Legal Sciences. Syria, Volume (44), Issue (5), 2022, 367-380.
3- Mohamed, Al-Eidani. Cyber threats and information crimes. Article, Algeria, Journal of Ijtihad in Learning Law, Volume (13), Issue (01), 2024, 15-37.
4- Mahdi, Heba Salah. Cybersecurity. Journal of Sustainable Studies. University of Baghdad, Volume (5), Issue (2), 2023, 431-444.
5- Institute, Cyber. Geopolitical Implications of Artificial Intelligence in Cybersecurity: A Comprehensive Analysis. International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online), Vol. (11), No (3), 2023, 91-105.
6- Mohiuddin, Zafar. Emerging Cybersecurity Threats: Mitigation Strategies Trends, and Implications. article, 2024, 1-7.
7- Al-Shammari, Mustafa Ibrahim Salman. Cybersecurity and its impact on Iraqi national security. Journal of Legal and Political Sciences, University of Diyala, Volume (10), Issue (1), 2021, 149-190.
8- Samir, Bara. Cyber Security in Algeria: Policies and Institutions. Article, Algerian Journal of Human Security, Volume 2, Issue 2, 2017, 255-280.
9- Rahmouni, Mohammed. Characteristics of cybercrime and its areas of use. Article, Ahmed Draia University-Darrar, Al-Haqiqa Magazine, Volume 16, Issue 3, 2017, 432-451.
10- Moussa, Aish. Mohamed, Khemoud. Cybersecurity. Master's Thesis, Mouloud Mammeri University-Tizi Ouzou, Faculty of Law and Political Science, Department of Law, 2023, 134.
11- Ibrahim, Fatima Ali. Youssef, Rahab. El-Sayed, Walid Mahmoud. Cybersecurity and Digital Hygiene. Egyptian Journal of Information Sciences. Volume (9), Issue (2), 2022, 390-422.
12- Issa, Nawal. Azreen, Mohammed. The Importance of Cybersecurity in the Educational Process and Religious Values. Journal of the International City University (Majmaa), Issue (48), 2024, 205-238.
13- Jilali, Chouirb. Faiza, Murad. The concept of cyber warfare and cyber security. Article, Journal of Rights and Freedoms, Amar Telidji University of Laghouat, Faculty of Law and Political Science. Dr. Yahya Fares University of Medea, Faculty of Law and Political Science/ Sovereignty and Globalization Laboratory, Volume (11), Issue (1), 2023, 157-178.
14- Fawzi, Islam. (2019). Cybersecurity: Social and Legal Dimensions Sociological Analysis. Damanhour University, Socio-Legal Journal, Volume (56), Issue (2), 2019. 99-139.
15- Al-Khadri, Jihan Saad Mohammed. Cybersecurity and Artificial Intelligence in Saudi Universities "A Comparative Study". Journal of University Performance Development, Volume (12), Issue (1), 2020. 2735-3222.