رقم الترميز الدولي / ISSN (P): 2710-2653
ISSN (E): 2960-253X /
رقم الايداع الوطني / 2375 / 2019

تاريخ استلام البحث ٢٣ / ١٢ / ٢٠٢٤
تاريخ قبول البحث ١٤ / ٤ / ٢٠٢٥
تاريخ النشر ٣٠ / ٦ / ٢٠٢٥

الدور الدولي في تعزيز الأمن السيبراني

The international role in enhancing cybersecurity

م.د. رضوان حسن علي

Dr. Radwan Hassan Ali
رئاسة جامعة الكوفة
Presidency of the University of Kufa

radhwanh.almahmud@uokufa.edu.iq

IRAQI Academic Scientific Journals

https://iasj.rdd.edu.iq/journals/journal/view/229

الملخص

التعاون الدولي لتعزيز الأمن السيبراني يُعد أمرًا حيويًا في مواجهة التهديدات الإلكترونية التي تتجاوز الحدود الوطنية، تزايدت المخاطر السيبرانية بشكل كبير بسبب زيادة الاعتماد على التكنولوجيا الرقمية في جميع أنحاء العالم. لذلك، تتطلب معالجة هذه التهديدات تعاونًا بين الدول، المنظمات الدولية، والقطاع الخاص.

يتمثل التعاون الدولي في تبادل المعلومات والخبرات، وتطوير استراتيجيات مشتركة، وتعزيز التدريبات والقدرات الدفاعية، فضلاً عن إنشاء سياسات قانونية منسقة لمكافحة الجرائم الإلكترونية، بجانب ذلك، يُشجع التعاون بين القطاعين العام والخاص على تطوير حلول تقنية مبتكرة لمكافحة الهجمات السيبرانية، مما يعزز القدرة على التصدي للأخطار بشكل أسرع وأكثر فعالية.

الكلمات المفتاحية: " التعاون الدولي "، " الامن السيبراني "، " التهديدات"

Abstract

International cooperation to enhance cyber security is vital in addressing cyber threats that transcend national borders. Cyber security risks have significantly increased due to the growing reliance on digital technology worldwide. Therefore, addressing these threats requires collaboration between countries, international organizations, and the private sector.

International cooperation involves the exchange of information and expertise, the development of joint strategies, the enhancement of training and defense capabilities, as well as the creation of coordinated legal policies to combat cyber crimes. Additionally, cooperation between the public and private sectors fosters the development of innovative technological solutions to combat cyber attacks, thereby enhancing the ability to respond to threats more quickly and effectively.

Keywords: "International Cooperation", "Cybersecurity", "Threats"

المقدمة

يُعد الأمن السيبراني من المسائل الهامة في الوقت الحالي، وأصبح نجاح اي حكومة او مؤسسة يعتمد بشكل كبير على مدى تطور اجهزتها واستخدامها للتكنلوجيا المتقدمة وقدرتها على حفظ وحماية المعلومات، وخاصة وان اغلب الحكومات تتجه الى تحقيق اعلى مستويات التطور والتحول نحو العالم الرقمي وتنمية البنية التحتية الرقمية ووضع سياسات عامة فاعلة وقدرات عالية من اجل ارساء وترقية منظومة معلومات رصينة.

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

مباشر لحياة المواطنين .وأصبح العراق سيما منذ العام ٢٠٠٣ بسبب الانفتاح على العالم والتطور في المجال التقني والمعلومات أكثر عرضة للهجمات السيبرانية .

وبعد سقوط النظام السابق في العراق عام ٢٠٠٣ والتطور المتسارع في القضايا التكنلوجيا، فقد تعرض العراق الى الكثير من الهجمات السيبرانية، جعلت امنه السيبراني عرضه للمخاطر والاختراق والقرصنة، فضلا عن التحديات التي تواجهه والتي تؤدي بالضرورة الى عدم استقرار الامن السيبراني العراقي وعدم وضوح معالم لهذا الامن.

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

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

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

اشكالية البحث: تتمثل اشكالية البحث في تحديد وتحليل التحديات التي تواجه الامن السيبراني في العراق وكيفية تأثير تلك التحديات والتداعيات على الاستقرار الامني في البلاد، وبالرغم من التقدم المتسارع في التكنولوجيا فأن العراق يواجه تهديدات سيبرانية متزايدة تؤثر على البنى التحتية الحيوية وبالتالي التأثير على الامن الوطني، وعليه فمن الضروري توضيح ماهو الأمن السيبراني والفضاء السيبراني؟ وما هو الدور الدولي لتعزيز الامن السبيراني؟

فرضية البحث: يفترض البحث ان التحديات المتعددة التي تواجه الامن السيبراني في العراق مثل ضعف البنية التحتية التقنية، وقلة التدريب والوعي، ونقص التكنلوجيا، فضلاً عن التحديات القانونية والتنظيمية والاقتصادية،

تؤثر بمجملها على الاستقرار الامني، وعليه تبذل الدولة جهودًا كبيرة لضمانه من كل التحديات ولكنها في الوقت ذاته عرضة باستمرار للهجمات السيبرانية.

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

هيكلية البحث: بهدف الاحاطة بموضوع البحث فقد تناول ما يأتي المطلب الأول: مفهوم الامن السيبراني ومفهوم الفضاء السيبراني المطلب الثاني: الامن السيبراني اهدافه وأهميته، والمطلب الثالث تناول علاقة الامن السيبراني بالأمن الوطن، اما المطلب الرابع فكان حول الدور الدولي في تعزيز الامن السيبراني.

المطلب الأول: مفهوم الامن السيبراني ومفهوم الفضاء السيبراني

تعددت تعاريف الامن السيبراني والفضاء السيبراني، بل ان البعض لا يفرق بينهما للترابط الوثيق بينهم وعليه سنوضح هذين المفهومين وعلى النحو الاتي :

اولاً: مفهوم الامن السيبراني:

قد شاع مصطلح الأمن السيبراني في الفترات الأخيرة على نطاق واسع، وأخذ يحظى بشعبية واسعة سيما بعدما استخدمه الرئيس الامريكي الاسبق (باراك أوباما) في العام ٢٠٠٩ في خطابه الذي دعا فيه الشعب الامريكي إلى الاهتمام بالأمن السيبراني لتعزيز أمننا القومي[١].

كما عد التهديد القادم من الفضاء السيبراني من أكبر التحديات الامنية والاقتصادية التي تواجه الولايات المتحدة ولهذا جعله في مقدمة اهتماماته، وعين لهذا الغرض مسؤول عن الأمن السيبراني ويكون عضواً في مجلس الأمن القومي الامريكي وان يكون على اتصال دائم به والتنسيق معه. ومن جانبه عد (جون مايكل ماكونيل) رئيس الاستخبارات الامريكية (٢٠٠٧-٢٠٠٩) ان الانترنت رفع بشكل غير مسبوق التحديات التي يتعرض لما النظام والامن القومي الامريكي التي يمكن ان تشمل مجالات سياسية وحيوية .

ان أهم التحديات التي تواجه مصطلح الأمن السيبراني هي الاستخدام غير المدروس للمصطلح، فلا نجد تعريف واحد متفق عليه للأمن السيبراني فهناك من يعده متداخلا مع أمن المعلومات مؤكداً على أن الأمن السيبراني هو فرع من أمن المعلومات، وهناك من يربط بين الأمن السيبراني والخاصية العالمية للإنترنت على اعتبار انه أوسع من أمن المعلومات الذي يهتم أساسًا بالسرية، وهناك من عرفه: بأنه الاسلوب والإجراءات المرتبطة بعمليات إدارة المخاطر الأمنية التي تتبعها المنظمات والدول لحماية سرية وسلامة وتوافر البيانات والأصول المستخدمة في الفضاء السيبراني، ويتضمن المفهوم إرشادات وسياسات ومجموعات من الضمانات والتقنيات والأدوات والتدريب لتوفير أفضل حماية لحالة البيئة السيبرانية ومستخدميها، وكذلك يُعرف بأنه: النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات ويضمن امكانات الحد من

الخسائر والاضرار التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح اعادة الوضع إلى ما كان عليه بأسرع وقت ممكن بحيث لا تتوقف عجلة الانتاج وبحيث لا تتحول الاضرار إلى خسائر دائمة [٢]

وقد عرف الاتحاد الدولي للاتصالات الأمن السيبراني بأنه: مجموعة من الأدوات والسياسات والمفاهيم الأمنية والحمايات الأمنية والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريبات والممارسات الفضلى والضمانات والتكنولوجيات التي يمكن استعمالها لحماية البيئة السيبرانية والمنظمة وأصول المستعمل، ويقصد بالأصول هنا أجهزة الحاسوب ومستعمليه، وانظمة الاتصالات والخدمات والتطبيقات وجميع المعلومات الموجودة في الفضاء السيبراني بما يضمن سلامة الخدمة وسريتها واستمراريتها وحمايتها من المخاطر الأمنية المنتشرة في البيئة السيبرانية، وقد تنوعت اشكال الحجوم السيبراني منها: الفايروسات، وأحصنة طروادة، والديدان الالكترونية، والتجسس الالكتروني، وسرقة الهوية، والهجمات والاحتيال عبر الانترنت وغيرها ونظرا لكثرتها وتنوعها فإن هناك حاجة ضرورية لمواجهتها عن طريق توسيع قاعدة المعرفة لتأمين الشبكات منها ومن ابرز وسائل الحماية هي: التدقيق والمراقبة والحوسبة الآمنة وبرامج الحماية من الفايروسات وانظمة كشف الاختراق والحماية منه والجدران الواقية وعليه فإن من الضروري اتباع اسلوب امني متعدد الطبقات، بحيث يكون الأمن شامل كل اجزاء النظام الالكتروني من انظمة وشبكات وتطبيقات سيما وان الأمن السيبراني هو عملية مستمرة ولا يوجد نظام امني واحد ينطبق على الجميع، وتشمل تقنيات الأمن السيبراني التشفير وضوابط النفاذ وسلامة النظام والتدقيق والإدارة والرصد والمتابعة[٣]

وقد عرف المعهد الوطني للمعايير والتقنية في الولايات المتحدة الأمن السيبراني بأنه: النشاط أو العملية أو القدرة أو الإمكانية أو الحالة التي بموجبها حماية نظم المعلومات والاتصالات والمعلومات الواردة اليها والدفاع عنها ضد الضرر أو الاستخدام أو التعديل غير المصرح به أو الاستغلال[٤]، كما يعرف ايضاً بأنه: تقنيات وعمليات تم تصميمها لحماية الكمبيوتر وأجزاء وبرامج الكمبيوتر والشبكات والبيانات من الوصول غير المصرح به ونقاط الضعف التي يتم توفيرها عبر الإنترنت من قبل مجرمي الإنترنت والجماعات الإرهابية والمتسللين ويرتبط الأمن السيبراني بحماية الإنترنت الخاصة بالأشخاص والمعدات الرقمية القائمة على الشبكة من الوصول غير المصرح به والتلاعب[٥].

ونجد هناك العديد من التعريفات الخاصة بالأمن السيبراني سيما ان كل تعريف قد تناول الامن السيبراني من جهة ولعل ابرزها فضلاً عما تقدم هو :الأساليب الدفاعية المستخدمة للكشف عن المتسللين المحتملين وإحباطهم، أو حماية شبكات الكمبيوتر والمعلومات التي تحتويها من الاختراق ومن الاضرار الخبيثة أو الاختلالات، ويعرف ايضاً بأنه الحد من خطر التعرض لهجمات ضارة على البرامج وأجهزة الكمبيوتر والشبكات، ويتضمن ذلك الأدوات المستخدمة للكشف عن الاختراقات وإيقاف الفيروسات ومنع الوصول إلى البرامج الضارة وفرض المصادقة وتمكين الاتصالات المشفرة وتشغيلها، وكذلك هو القدرة على حماية الفضاء السيبراني والدفاع عنه من الهجمات السيبرانية، كما يعرف بأنه: مجموعة التقنيات والعمليات والممارسات وتدابير الاستجابة والتخفيف

المصممة لحماية الشبكات وأجهزة الكمبيوتر والبرامج والبيانات من هجوم أو الاضرار أو الوصول غير المصرح به وذلك للتأكد من السرية والنزاهة، ويعرف أيضًا بأنه: فن ضمان وجود واستمرارية مجتمع المعلومات للشعب، وضمان وحماية المعلومات والأصول والبنية التحتية الحيوية في الفضاء السيبراني، والامن السيبراني هو ايضاً النشاط أو العملية أو القدرة أو الامكانية أو الحالة التي تحمي فيها أنظمة المعلومات والاتصالات والمعلومات الواردة اليها وان يتم الدفاع عنها ضد الاضرار أو الاستخدام غير المصرح به أو التغيير أو الاستغلال، فضلاً عن ذلك يعرف الأمن السيبراني هو تنظيم وجمع الموارد والعمليات والهياكل المستخدمة لحماية الفضاء السيبراني والأنظمة الممكنة للفضاء السيبراني من الحوادث التي تتعارض بشكل غير قانوني مع حقوق الملكية الفعلية ويتميز الأمن السيبراني بالطابع الاجتماعي والفني متعدد التخصصات، وانه شبكة خالية من المقاييس أي ان الجهات الفاعلة في الشبكة الالكترونية متشائمة إلى حد كبير ويتمتع بدرجات عالية من التغيير والترابط وسرعة التفاعل[٦].

وعليه فإن الأمن السيبراني هو مزيج من العمليات والتقنيات والممارسات والهدف منه حماية البرامج والتطبيقات والشبكات وأجهزة الكمبيوتر والبيانات من الهجوم، ويشمل الأمن السيبراني الأمن المادي للبرامج والتطبيقات والشبكات وأجهزة الكمبيوتر، وامن غير مادي أو معنوي يتعلق بالبيانات والمعلومات من أي هجوم واضرار متعمدة وسرقة للمعلومات والتحكم في الوصول الصحيح للأجهزة والتطبيقات والشبكات حمايتها من الضرر الذي قد يحدث عبر الشبكات ولعل أهم مجالات الأمن السيبراني هي: أمان التطبيق وأمن المعلومات وامن البريد الالكتروني وأمن أجهزة المحمول وأمن محركات البحث، وأمن اللاسلكي وتشمل استراتيجيات الأمن السيبراني إدارة الهوية وإدارة المخاطر وإدارة الحوادث[٧]

ويشكل الامن السيبراني ظاهرة عامية وتحدياً اجتماعياً وتقنياً معقداً للحكومات، وعلى الرغم ان الامن السيبراني هو أحد لهم التحديات التي تواجه الامن المجتمعي اليوم، الا ان الرؤية والوعي لا يزالان محدودين، ويعزى ذلك الى ان معظم الناس ينظرون الى الانترنت على انه بيئة امنة ويستخدمونه يومياً على هواتفهم واجهزة الكومبيوتر الخاصة بهم، وفي ذات الوقت هناك العديد من الهجمات الالكترونية التي تطال الجميع دون استثناء، مما جعل الشركات والمؤسسات تتكبد تكاليف اعلى للتعامل مع حوادث الامن السيبراني.

وتزاد الحاجة الى الامن السيبراني نظراً لاعتماده على تكنلوجيا المعلومات والاتصالات في جميع جوانب الحياة المجتمعية، ويعد الامن السيبراني ضرورة ملحة للأفراد والمؤسسات والحكومات والمنظمات، ويلاحظ انه دائماً ما يتم التركيز والاهتمام بقضايا الامن السيبراني على الحوادث وكيفية التعامل معها بعد وقوعها في حين ان مسالة الاهتمام في تحسين الامن السيبراني بالوقاية من الانتهاكات.

ثانياً: مفهوم الفضاء السيبراني:

لقد عرف المعهد الوطني للمعايير والتقنية في الولايات المتحدة الفضاء السيبراني بأنه: الشبكة المترابطة من البنى التحتية لتكنولوجيا المعلومات، والتي تشمل الإنترنت وشبكات الاتصالات السلكية واللاسلكية والنظم

الحاسوبية والمعالجات المدمجة وأجهزة التحكم، وان الفضاء السيبراني يرتبط بالواقع الافتراضي وشبكات الاتصال الالكترونية وانظمة الحاسوب، ومن التعاريف الهامة ما ذكرته ادارة السلامة العامة الكندية بأنه: العالم الالكتروني الذي تم إنشاؤه بواسطة شبكات مترابطة لتكنولوجيا المعلومات، والمعلومات متاحة على تلك الشبكات أي انها مشاعة عالمياً حيث يرتبط الناس معاً بتبادل الأفكار والخدمات والصداقة، علماً ان الفضاء السيبراني ليس ثابتاً بل هو نظام بيئي ديناميكي ومتطور ومتعدد المستويات للبنية التحتية المادية والبرمجيات واللوائح والأفكار والابتكارات والتأثيرات التي يتأثر بها عدد متزايد من المساهمين الذين يمثلون مجموعة من البشر[٨] .

وعليه فإن الفضاء السيبراني هو الفضاء الافتراضي الذي يستخدم الالكترونيات والطيف الكهرومغناطيسي لتخزين وتعديل وتبادل المعلومات عن طريق استخدام النظام الشبكي والبنية المادية المعنية، أي إنه غير ملموس إذ تجري الاتصالات والأنشطة المتعلقة بالإنترنت، كما ان الفضاء السيبراني هو وهمي حيث الكائنات الموجودة فيه غير ملموسة ولا تمثل العالم المادي، ذلك لأنها بيئة افتراضية تماماً، ويتم تبادل المعلومات والاتصال بين أكثر من (٧,٢) مليار شخص حول العالم لتوفير منصة مشتركة لتبادل الأفكار والآراء والخدمات والصداقة، فهو فضاء قابل للتوسع بلا حدود بحكم طبيعته إذ ينمو بشكل هائل دون النظر إلى أي حدود مادية أو سياسية[٩]

المطلب الثاني : اهداف الأمن السيبراني وأهميته

أصبح الأمن السيبراني جزءاً هاماً لكل شرائح المجتمع من فرد واسرة، فضلا عن المنظمات والحكومات والمؤسسات، ومن الضروري حماية الاسرة والافراد من عمليات الاحتيال عبر الإنترنت ومن الضروري أيضاً حماية المعلومات المالية التي يمكن أن تؤثر على الوضع المالي لأي شخص.

اولا: اهداف الامن السيبراني

تأتي الضرورة من الاهمية المتزايدة للإنترنت الذي أصبح حاجة حيوية لجميع المؤسسات والمنظمات والافراد، فقد وفر الكثير من فرص العمل والتعلم، وعليه لا بد من فهم كيفية حمايةَ المؤسسات والافراد لأنفسهم من الاحتيال عبر الانترنت وسرقة الهوية سيما وان هناك العديد من التحديات التي تواجههم منها محدودية الموارد وضعف في مهارات الأمن السيبراني، وان التعلم المناسب عند استعمال الانترنت وحماية أنظمة الحاسوب يمكن ان توفر بيئة آمنة للأنترنت ومن الممكن تحديد أهم أهداف الأمن السيبراني[١٠]:

١. سرية المعلومات: ضمان أن المعلومات المتاحة فقط للأشخاص او الانظمة المخولين بالوصول اليها، مما يمنع الوصول غير المصرح به.

٢. سلامة البيانات: حماية البيانات من التعديل او التلف غير المصرح به، والتأكد من ان البيانات تبقى دقيقة وكاملة.

٣. التواتر: ضمان ان الانظمة والخدمات متاحة للمستخدمين المصرح لهم عند الحاجة، مما يمنع تعطيل قطاع الخدمة.

٤. المصادقة: التأكد من هوية الاشخاص او الانظمة التي تحاول الوصول الى المعلومات او الانظمة، من اجل الاطمئنان بأنهم الاشخاص المعنين والمصرحين بالدخول.

٥. التعقب والمساءلة: القدرة على تعقب الانشطة والاجراءات التي يتم تنفيذها داخل النظام لضمان ان جميع الانشطة يمكن مراجعتها وربطها بمستخدم معين.

٦. التشفير: استخدام تقنيات التشفير لحماية البيانات اثناء نقلها او تخزينها، مما يجعلها غير قابله للقراءة دون مفتاح التشفير الصحيح.

ثانياً: اهمية الامن السيبراني

يحظى الأمن السيبراني بأهمية بالغة ذلك بسبب قيام الحكومات والمؤسسات العسكرية والشركات والمؤسسات المالية والطبية وغيرها بجمع ومعالجة وتخزين كميات كبيرة جداً من البيانات على أجهزة الكمبيوتر والأجهزة الأخرى، وان اغلب هذه البيانات معلومات حساسة كونها تتعلق بالملكية الفكرية أو معلومات أمنية أو شخصية أو بيانات مالية وان الدخول غير المصرح به إلى هذه المعلومات والبينات لهُ عواقب وخيمة سيما وان هذه المعلومات تنتقل بين المؤسسات والشركات عبر الشبكات إلى الأجهزة الأخرى، ونظراً لارتفاع خطر الهجمات الالكترونية فإن الدول والمؤسسات والشركات تجد نفسها مضطرة لحماية بياناتها ومعلوماتها، بل أصبحت الهجمات الإلكترونية والتجسس الرقمي يمثلان أكبر تهديد للأمن القومي لأي بلد [١١].

وان اهمية الأمن السيبراني تأتي من ان مجرمي الانترنت يركزون في هجماتهم على البنية التحتية الحيوية لأنه في حالة حدوث هجوم ناجح عليها يمكنهم من الحصول على ربح مالي أو سياسي، مستغلين بذلك نقاط الضعف في هذه البنية كون بعضها يستعمل انظمة حماية الكترونية تجارية ومع المعرفة الجيدة بالتقنية يمكن للمهاجم استغلال الثغرات الموجودة في هذه الانظمة، وما زاد من تعقيد الامور ان الحوادث في الفضاء السيبراني تواجه دائمًا مشكلة إسناد المسؤولية فمن الصعب تتبع مرتكبي الحادث، فضلاً عن ذلك أن التهديدات السيبرانية يصعب التنبؤ بما واتخاذ التدابير الوقائية في الوقت المناسب ما جعل خطر تنفيذ الهجمات السيبرانية الناجحة يزداد سيما وانها غير مرئية، وان الهجوم السيبراني يتطور وفق خمس مراحل هي: العثور على ثغرة أمنية في النظام، والسيطرة على النظام أو جزء منه، وإدخال البرامج الضارة في النظام، وإصابة مكونات النظام الأخرى، والقيام بهجوم على النظام بأكمله أو على جزء خاص منه، وتتسبب الثغرات في الأمن السيبراني بحدوث مشكلات كبيرة لكل مالك أو مشغل للنظام، ومن أجل منع الحوادث السيبرانية فإن أفضل ما يمكن عمله هو تحسين الأمن السيبراني[١٢].

ان بنيان الأمن السيبراني يقوم على محورين أساسين هما الادارة والحوكمة :ويقصد بالإدارة في سياق الأمن السيبراني هي ادارة أمن المعلومات وتحليل مستوى جاهزية منظومة الأمن السيبراني من حيث التكامل الاستراتيجي، وتوسيع استراتيجية الأمن السيبراني، وتقليل المخاطر، والقدرة على التكيف لتسهيل حركة اتخاذ القرارات لمواجهة الهجمات الإلكترونية ضد الافراد والشركات، ان الأمن السيبراني والإدارة يرتبطان ارتباطاً وثيقاً فمن المسلم به أن الأمن السيبراني لا يقل أهمية عن الأمن المادي، وعلى الرغم من عدم وجود نموذج واحد لإدارة الأمن السيبراني إلا ان هناك اتفاقاً عالمياً بان ادارة الأمن السيبراني ضرورية كونها تعمل على حماية البنية الأساسية الحيوية، وان اغلب بلدان العالم تدرك الحاجة إلى ادارة مواردها الحيوية وحمايتها بعناية، وتؤكد الحكومات والمنظمات العالمية على بذل كل جهودها لتوفير الأمن للبنية التحتية الحيوية لأنه يضمن رفاهية أي بلد وشعبه، سيما عندما أصبحت البنية التحتية الحيوية وأمن الطاقة وثيقة الصلة بالقرارات السياسية، وأما الحوكمة فيقصد بها ضمن اطار الأمن السيبراني بانها: المبادئ والقواعد الإدارية وأساليبها المتبعة في جهة ما لضبط سلطات اتخاذ القرار وتحديد أصحاب المسؤولية والمحاسبة في تنفيذ المهام والواجبات ذات العلاقة بحماية الجهة من الهجمات الالكترونية أو سوء استخدام الأصول المعلوماتية، مع ضمان استمرارية العمليات التشغيلية في حال وقوع حوادث أو كوارث أي ان الهدف من حوكمة الأمن السيبراني توجيه سلوكيات وقرارات الاشخاص ومراقبتهم وارشادهم بما يحسن ويرفع من كفاءتهم فضلاً عن تسهيل عمل الجهات ذات العلاقة وتنسيق جهودها [١٣]

المطلب الثالث: علاقة الأمن السيبراني بالأمن الوطني

ان مفهوم الأمن الوطني يتسم بالعمومية لتأثره بحقائق متنوعة ومتغيرة ونسبية نابعة من العوامل الداخلية والخارجية، ويُعد الأمن في قمة الضرورة لأية دولة لذلك تلجأ الدولة إلى العديد من التشريعات والاجراءات التي تكفل سلامة امنها الوطني بما يعززه داخليًا ويحميها من الاخطار الخارجية، وعليه فإن الأمن الوطني يساوي كيان الدولة وأساس بقائها[١٤]

لذلك نجد هنالك العديد من المفاهيم التي فسرت الأمن الوطني، فهناك من يرى بأنه: ما تقوم به الدولة للحفاظ على سلامتها ضد الاخطار الخارجية والداخلية التي تؤدي جما إلى الوقوع تحت سيطرة اجنبية نتيجة ضغوط خارجية او انيار داخلي[١٥]. وقد عرف الكاتب السياسي الامريكي (والتر ليبمان) الأمن الوطني بأنه: قيمة قد تزيد أو تنقص وذلك حسب قدرة الأمة على ردع أي هجوم أو هزيمته، أي ان الأمن الوطني يمثل قيمة متغيرة، وعرفه (دونالد بريتان) بأنه: سلامة البقاء الوطني وعليه فإن الأمن يركز بشكل أساسي على التحرر من كل اشكال الخوف والتهديد[١٦]، كما عرفه (فرانك تراغر) و (فرانك سيموفي) الأمن الوطني بأنه ذلك الجزء من السياسة الحكومية الذي يهدف إلى خلق الظروف القومية والدولية اللازمة لحماية وتوسيع القيم الوطنية الحيوية ضد الخصوم الحاليين او المحتملين.

لقد أرتبط الأمن الوطني لأية دولة ارتباطاً وثيق الصلة بتكنولوجيا المعلومات والاتصال بحكم قدرتها في التأثير على اي مجتمع، فقد اختصرت وسائل التواصل الاجتماعي بمختلف مسمياتها الوقت والمسافة وأخذت تحظى بتأثير فعال ومتنامي لدى معظم شعوب العالم، ويبرز في هذا الخصوص الحراك الشعبي والاحتجاجات الجماهيرية التي اخذت تنتظم على شكل مظاهرات وشكلت مصدر قلق للأنظمة الحاكمة، إذ اذ لها دور في توجيه الرأي العام وتعبئة الشارع مثل ما حصل منذ عام ٢٠١١ ما سمي بالربيع العربي، علمًا ان هناك مجمعاً صناعياً الكترونياً آخذاً في الظهور، تمامًا مثل المجمع الصناعي العسكري في الحرب الباردة(١٧).

تكون المجتمعات الاكثر تقدماً ذات الاقتصاد الرقمي أكثر عرضة للتهديدات السيبرانية، الامر الذي يفرض إيلاء المزيد من الاهتمام لحماية هذا الاقتصاد من التعرضات والهجمات السيبرانية، سيما ان الأمن السيبراني أصبح مشكلة أمنية وطنية وجزءاً لا يتجزأ من منظومة الأمن الوطني لأية دولة، بل يجب أن تبنى استراتيجية الأمن الوطني السيبراني على استراتيجية الأمن الوطني، وتحتاج الدول إلى استراتيجيات مرنة وديناميكية للأمن السيبراني حتى تستطيع الرد على التهديدات السيبرانية، سيما وان الفضاء السيبراني دائم التغير والتطور وليس له حدود مادية وهذا بدوره يفرض مسألة لا تخلو من الحساسية ألا وهي حماية البيانات مقابل مشاركة المعلومات، فالمواطنين لديهم حق مشروع في العيش في مجتمع مفتوح يتمتع بالتدفق الحر للمعلومات، وفي المقابل فإن الحكومات من واجبها حماية هذه المعلومات حفاظًا على الأمن والنظام العام فمكافحة جرائم الإنترنت والحرب على الارهاب وغيرها تتطلب تبادل المعلومات وتفاعل يومي بين المواطنين والحكومة كونها أصبحت من الضرورات المعاصرة للأمن الوطني، ويمكن تقسيم الاستراتيجية الوطنية للأمن السيبراني على خمسة اقسام رئيسة وهي:

١- العسكرية أي الحرب السيبرانية.
٢- والجرائم السيبرانية.
٣- وحماية البنية التحتية الحيوية.
٤- وادارة الأزمات.
٥- والدبلوماسية السيبرانية.

ان الدول تصوغ استراتيجية امنها السيبراني بشكل مستقل بناءً على أفكارها وتصوراتها الأمنية، وعليه فإن التطورات المعاصرة فرضت نفسها على دول العالم ضرورة تبني استراتيجية وطنية للأمن السيبراني على ان يراعى فيها التوازن بين متطلبات الأمن الاساسية وبين احترام خصوصية المواطنين وطبيعة الثقافة السائدة في البلد، علما ان هذه الاستراتيجية لا بد ان تكون ذات نهج شمولي أي لا تقتصر على الحكومة فحسب، بل من الضروري اشراك جميع أصحاب المصلحة وهم الحكومة، والقضاء، والاجهزة الأمنية، والمسؤولين عن البنية التحتية للأمن السيبراني في القطاع العام والخاص ومجهزي خدمه الأنترنت وتكنلوجيا المعلومات، والمؤوسسات التعليمية المختصة والمواطنين فضلا عن الهيئات الاقليمية والدولية المعنية بمجال الأمن السيبراني (١٨)

ومن اجل ضمان فاعلية ونجاح الاستراتيجية الوطنية للأمن السيبراني لا بد من توفر مجموعة من العناصر الاساسية لها ولعل أهمها:

١. ضمان أعلى مستوى من التأييد والدعم الرسمي لها ماديا ومعنويا من قبل الحكومة.
٢. تشكيل هيأه مختصة بالأمن السيبراني.
٣. إشراك الهيئات الحكومية المعنية وضمان التعاون والتنسيق فيما بينها.
٤. اشراك أصحاب المصلحة الاخرين سيما القطاع الخاص الموثوق بحم لضمان عمل البنى التحتية الأساسية للأمن السيبراني وتخصيص موارد لها في ميزانية الدولة الوطنية.
٥. ضرورة ان تتضمن الاستراتيجية خططا قابلة للتنفيذ وأهداف قصيرة ومتوسطة وبعيدة المدى تسعى إلى تحقيقها والإدارة الجيدة لمخاطر التهديدات السيبرانية لضمان استمرارية عمل هذه الاستراتيجية ووضع خطة طوارئ لإدارة أزمات الأمن السيبراني.
٦. تعزيز تبادل المعلومات بين القطاع الحكومي والخاص وإجراء عمليات محاكاة وتدريبات عملية للأمن السيبراني.
٧. تدريب كوادر مختصة وتنمية مهاراتهم وتشجيع الابتكار والبحث والتطوير.
٨. وضع قوانين واضحة تحد من الانشطة السيبرانية المحظورة معززة بقدرات تنفيذية تحد من الجريمة السيبرانية.
٩. ملائمة الاستراتيجية الوطنية للأمن السيبراني بخطط واستراتيجيات الأمن السيبراني الإقليمي والدولي[١٩]

وبعد التطور الحاصل في تكنلوجيا المعلومات والاتصالات اكسبت الصراعات السياسية والعسكرية والاقتصادية بين الدول بُعداً الكترونياً بحيث يصعب التنبؤ بحجمها وتأثيرها، بل ان الحروب التي تدور رحاها في الفضاء السيبراني أكثر أهمية من الأحداث التي تجري على أرض الواقع، وان الانجازات المذهلة للتجسس السيبراني اظهرت المكاسب الكبيرة لعمليات اختراق اجهزة الكومبيوتر مقارنة بارتفاع اشكال التجسس التقليدية التي تتطلب ذكاء بشري وارتفاع نسبة الخطورة، الامر الذي جعل التجسس السيبراني على الساحة العالمية مصدر قلق للدول على امنها الوطني، فالهجوم السيبراني ليس غاية في حد ذاته ولكنه وسيلة قوية مجموعة متنوعة من الغايات من الدعاية إلى التجسس، ومن تعطيل الخدمات إلى تدمير البنية التحتية الحيوية، ويرى البعض انه لم يحصل تغير في طبيعة التهديد للأمن الوطني، لكن الانترنت وفر آلية جديدة يمكنه من زيادة سرعة الحجوم وحجمه وقوته، ذلك ان انتشار الانترنت وتزايد اعتماد العالم عليه سيترتب على الإضرار به تداعيات سياسية واقتصادية وعسكرية ملموسة سيما بعد التطور الملفت للهجمات السيبرانية كنتيجة طبيعية للنزاعات في العالم الحقيقي مما سيؤدي دوراً رئيسًا في النزاعات المستقبلية[٢٠].

المطلب الرابع / الدور الدولي في تعزيز الأمن السيبراني

ان الدور الدولي في تعزيز الأمن السيبراني يتمثل في التعاون المشترك بين الدول والمنظمات الدولية وكل الجهات المختصة من أجل تأمين الفضاء السيبراني، وحماية البنية التحتية الرقمية، والحد من التهديدات الإلكترونية التي يمكن أن تؤثر على الأمن الوطني والدولي، وتشمل الجهود الدولية في هذا المجال عدة محاور رئيسة[٢١]:

١. التعاون الدولي متعدد الأطراف: يعد تعاون الدول والمنظمات الدولية لمواجهة التهديدات السيبرانية العابرة للحدود من خلال تبادل المعلومات الاستخبارية حول الهجمات السيبرانية، مثل الفيروسات والبرمجيات الضارة، ومشاركة أفضل الممارسات الأمنية بين الدول.
٢. المنظمات الدولية: تلعب المنظمات الدولية دورًا حيويًا في تحديد سياسات الأمن السيبراني وتنسيق الاستراتيجيات العالمية لمواجهة الاخطار الامنية في الفضاء السيبراني ومن اهم هذه المنظمات هي:

• الاتحاد الدولي للاتصالات :(ITU) يعمل على وضع معايير عالمية للأمن السيبراني، ويسعى لتعزيز قدرات الدول في مجال حماية الفضاء السيبراني.

•الأمم المتحدة :من خلال منتديات مثل المنتدى العالمي للأمن السيبراني، تدعو إلى تبني سياسات أمنية مشتركة وتنظيم استخدام الفضاء السيبراني بما يتماشى مع المعايير الدولية.

•منظمة التعاون الاقتصادي والتنمية :(OECD) تروج لوضع سياسات ونظم أمن سيبراني فعّالة، وتدعم تبادل المعلومات بين الدول في مجال التهديدات السيبرانية.

٣. تعزيز القدرات الوطنية: تساهم الدول المتقدمة في دعم الدول النامية من خلال برامج تدريبية ومبادرات تهدف إلى رفع قدرات الحكومات والشركات في مجال الأمن السيبراني، مثل إنشاء مراكز استجابة للطوارئ وفرق الاستجابة للحوادث السيبرانية.(CSIRTs)
٤. وضع أطر قانونية وتنظيمية: تسعى العديد من الدول إلى التعاون في إنشاء أطر قانونية مشتركة لمكافحة الجريمة السيبرانية وتنظيم استخدام الفضاء السيبراني .على سبيل المثال:

• اتفاقية بودابست (2001) الخاصة بالجريمة الإلكترونية، التي تعد أول معاهدة دولية تهدف إلى التنسيق بين الدول لمكافحة الجرائم السيبرانية.

٥. حماية البنية التحتية الحيوية: تعمل الدول على تعزيز حماية البنية التحتية الحيوية) مثل الشبكات الكهربائية، والنقل، والاتصالات (عبر استراتيجيات أمنية مشتركة وتعاون دولي في رصد وتقييم المخاطر التي قد تهدد استمرارية عمل هذه البنية.

٦. الاستجابة للطوارئ السيبرانية: التعاون بين الدول لمواجهة الهجمات السيبرانية الضخمة أو الكوارث الرقمية مثل الهجمات المتقدمة المستمرة .(APT) يتم إنشاء شبكات من مراكز الاستجابة للطوارئ السيبرانية التي تعمل على التصدي للهجمات بسرعة وفعالية.

٧. البحث والابتكار: يتم تعزيز البحث العلمي والتقني في مجال الأمن السيبراني من خلال التعاون بين المؤسسات الأكاديمية والحكومية والشركات الخاصة على المستوى الدولي، بهدف تطوير تقنيات جديدة للكشف عن الهجمات والتصدي لها.

من خلال هذه الجهود، يسعى المجتمع الدولي إلى خلق بيئة سيبرانية آمنة ومستدامة تساهم في استقرار الاقتصادات، حماية حقوق الأفراد، وتعزيز الثقة في الفضاء الرقمي على المستوى العالمي.

الخاتمة

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

وعليه فإن الغاية الاساسية من الأمن السيبراني هي تقليل المخاطر المتعلقة بالاعتماد على الفضاء السيبراني في ظل وجود تهديدات عدائية متنوعة وكثيرة وغامضة، فضلاً عن ذلك كشف الأمن السيبراني عن حقيقة أخرى ألا وهي ان الناس هم أضعف حلقة في سلسلة الأمن السيبراني، ولذلك فانه يتطلب بناء ثقافة أمنية وزيادة الوعي بالمخاطر السيبرانية المعاصرة وهذا بدوره يتطلب من الدول توعية شعوبها وتبني استراتيجيات للأمن السيبراني ونظام أمني وقانونٍ مناسب يتم تطبيقه في المؤسسات الحكومية والقطاع الخاص وبناء كوادر متقدمة في مجال التكنولوجيا والمعلوماتية والاتصال، وتخصيص مختبرات متقدمة لها تمكنها من التصدي بنجاح للتحديات السيبرانية المعاصرة، وفيما يتعلق بالعراق فإن الانفتاح الذي شهده العراق لاسيما في مجال التقني والمعلوماتي وتزايد الاعتماد عليه فرض عليه تحديات عدة: ونظرا لكون العراق مستهدف بالدرجة الاساسية من قبل التنظيمات الارهابية فقد شهدت المؤسسات الرسمية وغير الرسمية خروقات وهجمات سيبرانية عدة ومن هنا ظهرت تحديات أمنية معاصرة فرضت نفسها على العراق منها الارهاب

الهوامش

([1]) Aniel Schatz and Rabih Bashroush and Julie Wall , Towards a More Representative , Definition of Cyber Security , Journal of Digital Forensics Security and Low JDFSL (United State Of Florida , The NO.2,2017.P.P.53-54.

[٢]) منى الاشقير جبور، الامن السيبراني : التحديات ومستلزمات المواجهة، بيروت الجامعة العربية، ٢٠١٢، ص ٣.

[٣]) الاتحاد الدولي للاتصالات، الامن في الاتصالات وتكنلوجيا المعلومات، جنيف، ٢٠٠٩، ص ١٣.

([4]) North Atlantic Treaty Organization ,Cyber Security A generic Reference Curriculum, Brussels ,2016.p.17.

([5]) Rajesh Kumar Contam , Importance of Cyber Security , International Journal of Computer Application (NEW YORK) Foundation of Computer Science , Vol. no 7 , February 2015 ,p.14.

([6]) Dan Craigen and Nadia Diakam – The banlt and Randy purse ,Defining , Cyber Security , Technology Innovation Management Review (Ottawa: Technology Innovation Management) October ,2014 ,p.p.13-14.

([7]) Jitendra Jain and Parashw Ram Pal ,A recent Study over Cyber Security and its Elements , International Journal of Advanced Research in Computer Science (India : Rajasihan , Janardan Rai Nagar Rajsthan Vidyapeeth Vol.8,No.3,2017) p791.

([8]) North Atlantic Treaty Organization , Cyber Security A Generic Renascence Curriculum op.cit, p.17.

([9]) Dan Cragen and Nadia Diakun , The fault and Randy Purse ,op-cit.p.p. 13-14.

([10]) Rajesh Kumar Contam , op. cit,p.14.

([11]) Nata Lord , What is Cyber Security ? Definition, Best Practices and More Guardian,15 july 2019, p16.

([12]) Jada Limba and Others, Cyber Security Management Model for Critical in Fra structure The International Journal Entrepreneurship and Sustainability Issues (European Union Entrepreneurship and Sustainability Center , vol .4, No 4 June 2017),p.560.

([13]) Jada Limba and Others, op.cit, p.561.

([١٤]) نجدت صبري ، الاطار القانوني للأمن القومي :دراسة تحليلية ، دار دجلة ،عمان ، ٢٠١١،ص ٤١.

([١٥]) احمد فريجة ولد مية فريجة ، الامن والتهديدات الأمنية في عالم ما بعد الحرب الباردة ، دفاتر السياسة والقانون ، العدد ١٤، الجزائر ، جامعة بسكرة ، ٢٠١٦، ص ١٥٩.

([١٦]) سيد احمد قوجيلي ، تطور الدراسات الأمنية ومعضله التطبيق في العالم العربي ، دراسات استراتيجية ، مركز الامارات للدراسات والبحث الاستراتيجية ، أبو ضبي ، العدد ١٦٩ ، ٢٠١٢، ص ١٢.

([17]) Jerry Brito and Take Watkins , Loving The Cyber Bomb? The Dangers of Threat Information in Cyber Security Policy, Harvard National Security Journal, Cambridge, Harvard Law School, united states, Vol.3,2011,p.40.

([18]) Laszlo Kovacs , National Cyber Security as The Cornerstone of National Security , Land Forces Academy Review , Sibiu Nicolai Bakes cu Land Forces Academy , Romania , Vol,23, No 2 ,2018, p.114.

([١٩]) للمزيد ينظر : الاتحاد الدولي للاتصالات ، دليل لوضع استراتيجية للأمن السيبراني : التزام استراتيجية بالأمن السيبراني ، جنيف ، ٢٠١٨ ، ص ٥٠.

([20]) Kenneth Gacers , Strategic Cyber Security , Estonia , Tallinn's NATO Cooperative Cyber Defense Centre of Excellence , 2019,p.9.

[٢١]) مجموعة مؤلفين ، تحولات في الدبلوماسية في القرن ٢١ ، ترجمة: اية محمد الغازي ، دار صفصافة للنشر والتوزيع ، مصر ، ٢٠١٧ ، ص ٣٧.

المصادر

المصادر باللغة العربية

١ – سيد احمد قوجيلي، تطور الدراسات الأمنية ومعضله التطبيق في العالم العربي، دراسات استراتيجية، مركز الامارات للدراسات والبحث الاستراتيجية، أبو ضبي، العدد ١٦٩، ٢٠١٢ .

٢– الاتحاد الدولي للاتصالات، دليل لوضع استراتيجية للأمن السيبراني: التزام استراتيجية بالأمن السيبراني، جنيف، ٢٠١٨.

٣– الاتحاد الدولي للاتصالات، الامن في الاتصالات وتكنلوجيا المعلومات، جنيف، ٢٠٠٩.

٤– احمد فريجة ولد مية فريجة، الامن والتهديدات الأمنية في عالم ما بعد الحرب الباردة، دفاتر السياسة والقانون، العدد ١٤، الجزائر، جامعة بسكرة، ٢٠١٦.

٥– مجموعة مؤلفين، تحولات في الدبلوماسية في القرن ٢١، ترجمة: اية محمد الغازي، دار صفصافة للنشر والتوزيع، مصر، ٢٠١٧.

٦– منى الاشقير جبور، الامن السيبراني: التحديات ومستلزمات المواجهة، بيروت الجامعة العربية، ٢٠١٢.

٧– نجدت صبري، الإطار القانوني للأمن القومي: دراسة تحليلية، دار دجلة، عمان، ٢٠١١.

المصادر باللغة الإنكليزية

1. Aniel Schatz and Rabih Bashroush and Julie Wall , Towards a More Representative , Definition of Cyber Security , Journal of Digital Forensics Security and Low JDFSL (United State Of Florida , The NO.2,2017.
2. Dan Craigen and Nadia Diakam – The banlt and Randy purse ,Defining , Cyber Security , Technology Innovation Management Review (Ottawa: Technology Innovation Management) October ,2014.
3. Jada Limba and Others, Cyber Security Management Model for Critical in Fra structure The International Journal Entrepreneurship and Sustainability Issues (European Union Entrepreneurship and Sustainability Center , vol .4, No 4 June 2017.
4. Jerry Brito and Take Watkins , Loving The Cyber Bomb? The Dangers of Threat Information in Cyber Security Policy, Harvard National Security Journal, Cambridge, Harvard Law School, united states ,Vol.3,2011.
5. Jitendra Jain and Parashw Ram Pal ,A recent Study over Cyber Security and its Elements , International Journal of Advanced Research in Computer Science (India : Rajasihan , Janardan Rai Nagar Rajsthan Vidyapeeth Vol.8,No.3,2017.
6. Kenneth Gacers , Strategic Cyber Security , Estonia , Tallinn's NATO Cooperative Cyber Defense Centre of Excellence , 2019.
7. Laszlo Kovacs, National Cyber Security as The Cornerstone of National Security, Land Forces Academy Review, Sibiu Nicolai Bakes cu Land Forces Academy, Romania, Vol,23, No 2 ,2018.

8. **Nata Lord, what is Cyber Security? Definition, Best Practices and More Guardian,15 july 2019.**
9. **North Atlantic Treaty Organization, Cyber Security A generic Reference Curriculum, Brussels ,2016.**
10. **Rajesh Kumar Contam , Importance of Cyber Security , International Journal of Computer Application (NEW YORK) Foundation of Computer Science , Vol. no 7 , February 2015.**