الأمن السيبراني القوة الرابعة لتعزيز الأمن والدفاع
(البنية التحتية – الفوائد والمخاطر)

الباحث: احمد سالم علي حسين

ابن خلدون الجامعة

القسم: الأشعة والسونار/ المرحلة الثالثة

أشراف أ.د عبد القادر داود

ahmedalrawayiyu@gmail.com

الملخص:

يعد الأمن السيبراني أو ما أطلق عليه شخصياً بلقب "القوة الرابعة" واحدًا من أهم القوى العسكرية والأمنية بعد القوات البحرية، البرية، والجوية. أصبح الأمن السيبراني جزءًا أساسيًا في تعزيز الأمن والدفاع العراقي لمواجهة التهديدات الإلكترونية. يقوم الأمن السيبراني بحماية الأنظمة، الشبكات، البرامج، والبيانات في المؤسسات والشركات من الهجمات الإلكترونية التي تواجهها من الإرهاب الإلكتروني. ويُفهم الأمن السيبراني بأنه استخدام جميع الوسائل والإجراءات اللازمة لحماية المجال الإلكتروني من أي هجوم سيبراني. ويتضمن ذلك استخدام التقنيات والإجراءات والقواعد التنظيمية لمنع الوصول غير المشروع إلى المعلومات الإلكترونية، ويمنع بذلك استغلالها بطرق غير قانونية وغير أخلاقية.

الكلمات المفتاحية: (الأمن السيبراني، الذكاء الاصطناعي، الأمن والدفاع، البنية التحتية).

Cybersecurity is the fourth force for enhancing security and defense (Infrastructure – benefits and risks)

Researcher: Ahmed Salem Ali Hussein

Ibn Khaldun University

Department: Radiology and Ultrasound/Third Stage

Supervised by Prof. Dr. Abdel Qader Daoud

ABSTRACT:

Cybersecurity, or what I personally call the “fourth force,” is one of the most important military and security forces after the naval, land, and air forces. Cybersecurity has become an essential part of strengthening Iraqi security and defense to confront cyber threats. Cybersecurity protects systems, networks, programs, and data in organizations and companies from cyberattacks they face from cyberterrorism. Cybersecurity is understood as the use of all necessary means and procedures to protect the electronic domain from any cyber attack. This includes the use of technologies, procedures and organizational rules to prevent illegal access to electronic information, thus preventing its exploitation in illegal and unethical ways.

Keywords: (cybersecurity, artificial intelligence, security and defense, infrastructure).

مشكلة البحث:

مشكلة البحث في الأمن السيبراني في العراق تتمثل في عدة جوانب. أولاً، هنالك غياب شبه تام من ناحية الدعم المالي لتعزيز هذا القطاع وتطويره، مما يؤثر سلبًا على القدرة في مواجهة التهديدات السيبرانية. ثانيًا، تعاني البنية التحتية في البلاد من ضعف عام، مما يعرضها للهجمات الإلكترونية. وثالثًا، تعاني الأطراف المختلفة من نقص في التنسيق والتعاون المتبادل، وهذا يعيق الجهود الجماعية لتعزيز الأمن السيبراني.

بالإضافة إلى ذلك، لا يتلقى الأمن السيبراني الاهتمام الكافي في العراق، من مستوى المسؤولين إلى الأفراد، على الرغم من أهميته الكبيرة والتأثير الكبير الذي يمكن أن يكون له على الحروب الحديثة. لذلك يجب أن نركز على فهم الفوائد والمخاطر المترتبة بالأمن السيبراني، وضرورة تعزيزه وتطويره ونشر الوعي السيبراني. وبالإضافة إلى ذلك، هناك نقص في الخبرة المتوفرة في هذا المجال، وهذا يعيق القدرة على التصدي للتهديدات السيبرانية بفاعلية.

أهمية وفكرة البحث:

يكتسب هذا البحث أهميته من خلال فهم الأمن السيبراني، بالإضافة إلى الدور الحاسم الذي يلعبه في السلم والحرب كونه قوة رئيسية في هذا العصر، وخاصة بعد انتهاء العراق من الحروب والتأكيد على استعداده لأي طارئ بعد تأمين الجوانب البرية والجوية والبحرية. وليتبقى الجانب السيبراني. سيتناول هذا البحث البنية التحتية في ظل التحديات والتراخيات، واستكشاف الإيجابيات والسلبيات للأمن السيبراني، وفوائده ومخاطره الكبرى وتأثيرها على العراق بشكل خاص والعالم عمومًا، وذلك ضمن إطار معرفي. وكيف سنعمل أيضًا وفقًا لخطة زمنية محددة لنجاح التجربة السيبرانية، بالإضافة إلى بعض الإجراءات الاحترازية التي ستسهم في معالجة مشكل عدة، وكذلك التنبؤ والتوصيات التي سيتم التوصل إليها، والتي ستسهم في سد الفجوات والثغرات للأمن السيبراني العراقي على مستوى المؤسسات المدنية، المؤسسات العسكرية، الشركات، والأفراد حيث سيعزز أمان واستقرار البلاد. ومن المتوقع أن يكون لهذا البحث تأثير توعوي وتطويري على استراتيجيات الأمن السيبراني، وتعزيز القدرة التنافسية للعراق في هذا المجال، خاصه لو تم العمل بالجوانب التطبيقية والتوصيات المبتكرة، لأنه سيوسع آفاق إدراك القراء من المجتمع العراقي بشكل خاص لأولئك الذين سمعوا بالأمن السيبراني ولم يعرفوا معناه، فوائده، ومخاطره على الحاضر والمستقبل.

أهداف البحث: يسعى البحث إلى تحقيق الأهداف التالية:

- تعزيز الأمن والدفاع من خلال الأمن السيبراني بناءً على التوصيات في خلال فترة زمنية محددة.
- تأمين البنية التحتية من خلال معالجة التحديات الحالية.
- التوعية بشان الأمن السيبراني من خلال عرض أهميته ومخاطره ؛ لأن رفع الوعي والإدراكات سيقلل الهجمات.
- اعتماد فكرة مفادها هي أن الأمن السيبراني العراقي إذا لم يعتمد كقوة رابعة، فسيكون حلقة المواجهة الأضعف، وأول ما يتم اختراقه في حرب محتملة.

المقدمة:

هذا النوع من الأمن القومي يمكن أن يتواجد في جميع مؤسسات الدولة الخدمية والأمنية والشركات. ويجب على هذه المؤسسات والشركات أن تكون على دراية بأهمية الأمن السيبراني، وأن تبذل جهودًا فعالة لتعزيزه وتعزيز التحصينات لحماية معلوماتها وأنظمتها من الهجمات السيبرانية.

كما أن الأمن السيبراني المرتبط بالذكاء الاصطناعي مهم جدًا، حيث تعيش المجتمعات الحديثة في عصر رقمي متقدم، وتعتمد الكثير من العمليات والخدمات على التكنولوجيا الحديثة. ومع تزايد استخدام الإنترنت والأجهزة الذكية، أصبح الأمن السيبراني أكثر أهمية من أي وقت مضى.

كم أن الأمن السيبراني المرتبط بالذكاء الاصطناعي هو مجال يركز على استخدام التكنولوجيا الذكية والذكاء الاصطناعي لحماية الأنظمة والبيانات الحساسة من التهديدات السيبرانية. فالذكاء الاصطناعي يمكنه تحليل البيانات واكتشاف الأنماط غير العادية بشكل أسرع وأكثر دقة من الأنظمة التقليدية، مما يجعله أداة قوية في مجال الأمن السيبراني. تُستخدم تقنيات الذكاء الاصطناعي في مجال الأمن السيبراني بشكل واسع، مثل تحليل السلوك السيبراني وكشف التهديدات والاستجابة

الذكية للهجمات. كما يستخدم أيضًا في تصنيف وتصفية الرسائل الاحتيالية واكتشاف البرامج الضارة وتحليل الثغرات الأمنية بشكل فعال.

بعد كل ما ذكر سابقا، بات الاستثمار في الأمن السيبراني والمعلومات ضرورة حتمية في العصر الحديث، حيث بدأت الدول في الاستثمار في مجال التسلح الرقمي. يُعتبر استثمار الأمن السيبراني أحد العوامل الأساسية في مجال الأعمال والشركات والمؤسسات، سواء كانت صغيرة أم كبيرة. تتشارك الشركات والمؤسسات في استثمار وتوجيه النفقات نحو عملياتها الأساسية، وبالتالي يتعين عليها أيضًا الاستثمار في مجال الأمن السيبراني بشكل خاص بمنشآتها. فالميزانيات المخصصة للأمن السيبراني تلعب دورًا بارزًا في تعزيز تقدم الأعمال ونجاحها. وقد تم اللجوء إلى الأمن السيبراني بسبب أن نجاح أي شركة أو مؤسسة يعتمد بشكل كبير على معلوماتها. وبالإضافة إلى ذلك، فإن العديد من المعلومات والأنظمة والبنية التحتية المتصلة بالشبكات تتعرض للخطر بين الحين والآخر. وتواجه هذه المعلومات تحديات الاختراق والاستغلال الجرائمي. ولذلك، فإن الاستثمار في الأمن السيبراني يعد ضرورة لحماية المعلومات وضمان استدامة الأعمال ونجاحها في العالم الرقمي المتطور. وأن أهم مقومات الأمن السيبراني هو:

تأمين البنية التحتية ضد الهجمات السيبرانية

كمقدمة: تعد البنية التحتية الهياكل التنظيمية اللازمة لتشغيل المجتمع أو المشروع أو الخدمات والمرافق المختلفة لدعم الحياة الإقتصادية والاجتماعية. وتشمل البنية التحتية أيضًا الهياكل التنظيمية اللازمة لإدارة هذه المرافق وتطويرها وصيانتها. تعتبر البنية التحتية جوهرية لنمو الاقتصاد وتحقيق التنمية المستدامة في أي دولة أو منطقة. فهي تسهم في تحسين جودة الحياة للمواطنين وتعزيز فرص العمل وتعزيز الاستثمارات وتعزيز التجارة وتعزيز التواصل والتواصل بين المجتمعات المختلفة. علاوة على ذلك، فإن البنية التحتية تعمل كجسر للتنمية والتكامل الاجتماعي والاقتصادي والبيئي.

لذلك، يجب على الدول والمؤسسات الاستثمار في تحسين وتطوير بنيتها التحتية. يجب أن تكون هناك استراتيجيات وخطط مستدامة لتطوير البنية التحتية، مع التركيز على تحقيق التوازن بين الاحتياجات الحالية والمستقبلية. ويجب أن تشمل هذه الخطط تعزيز البنية التحتية الرقمية وتعزيز الاستدامة البيئية، وتحسين النقل، وتعزيز القدرات التكنولوجية، وتعزيز النمو الاقتصادي.

من الناحية الوظيفية للبنية التحتية يتمثل في تسهيل إنتاج البضائع والخدمات، وتوزيع المنتجات النهائية في الأسواق، بالإضافة إلى توفير الخدمات الاجتماعية الأساسية مثل المدارس والمستشفيات. على سبيل المثال، تسهم الطرق في نقل المواد الخام إلى المصانع. وفي الجانب العسكري، يشير هذا المصطلح إلى المباني والمنشآت الدائمة التي تدعم القوات العسكرية وتسهم في إعادة نشرها وتشغيلها. بشكل عام، البنية التحتية تشمل كل ما يلزم للحياة اليومية وتلعب دورًا هامًا في المجتمع، إذ إنها –إذا كانت موجودة وفعالة– تسهم في تسهيل العملية الاجتماعية.

التأمين: كمعادلة فأن (زيادة الهجمات السيبرانية على البني التحتية = ضعف الأمن والاقتصاد) وتعد البنية التحتية للمعلومات والاتصالات الحديثة أحد العوامل الرئيسية في تطور العالم الرقمي. ومع التقدم التكنولوجي المستمر، أصبحت الشبكات والأنظمة الحاسوبية جزءًا لا يتجزأ من حياتنا اليومية. ولكن مع زيادة استخدام الإنترنت وتزايد التهديدات السيبرانية، أصبح تأمين البنية التحتية أمرًا حاسمًا لضمان السلامة والسلامة الإلكترونية للمؤسسات والأفراد. يهدف الأمن السيبراني إلى حماية البنية التحتية الرقمية من الهجمات والاختراقات السيبرانية. يتضمن ذلك حماية الشبكات والأنظمة من الاختراق، وتأمين البيانات والمعلومات المخزنة، وتعزيز الوعي الأمني وتوعية المستخدمين بمخاطر السلامة الإلكترونية.

هناك العديد من الاستراتيجيات والتقنيات التي يمكن استخدامها لتأمين البنية التحتية للشركات أو المؤسسات وغيرهم بواسطة الأمن السيبراني: بدءًا من تطبيق سياسات وإجراءات الأمان القوية، إلى استخدام تقنيات التشفير والتوقيع الرقمي، التحقق باستخدام خطوتين، تطبيق نظم الاكتشاف

والاستجابة للحوادث، وبناء الجدران النارية لحماية الشبكات. بالإضافة إلى ذلك، يجب أن يتم تدريب الموظفين والمستخدمين على أفضل الممارسات في الأمان السيبراني، وتشجيعهم على استخدام كلمات مرور قوية وتحديث البرامج الخاصة بهم. يجب أيضًا نسخ الملفات والبيانات إلى مكان بعيد عن أي اتصال خارجي، وتحديد نقاط ضعف المؤسسة أو الشركة من خلال شركة تيم الخاصة بالشركة أو وأن يكون متخصصًا بأمن المعلومات. ويتعين أيضًا تنفيذ نظام المراقبة، ويجب أن يكون لدى المؤسسات خطة استجابة للأمن السيبراني في حالة وقوع هجوم أو اختراق. يجب أن تتضمن هذه الخطة إجراءات للتحقيق والاستجابة الفورية للتهديدات واستعادة البنية التحتية بأسرع وقت ممكن. تكامل هذه الاستراتيجيات والتقنيات يسهم في بناء بنية تحتية آمنة ومتينة ضد التهديدات السيبرانية.

باختصار، يعد تأمين البنية التحتية بواسطة الأمن السيبراني أمرًا حيويًا بالغا بالأهمية في العصر الرقمي الحالي. يجب أن تتخذ المؤسسات والأفراد إجراءات قوية لحماية الشبكات والأنظمة والبيانات المخزنة. كما يجب أن يتم توعية المستخدمين بأهمية الأمان السيبراني وتعزيز الوعي الأمني لتحقيق بيئة رقمية آمنة وموثوقة.

تعد الهجمات السيبرانية من أكبر التحديات الموجهة للعالم الرقمي في الوقت الحاضر. تشمل هذه الهجمات مجموعة متنوعة من الأنشطة التي يقوم بها المهاجمون للوصول إلى المعلومات السرية أو التأثير على الأنظمة الحاسوبية. فبعد معرفة الإجراءات الاحترازية، فيما يلي نظرة عامة على أشهر أنواع الهجمات السيبرانية:

١. الهجمات بواسطة البرمجيات الخبيثة: تعتبر البرمجيات الخبيثة من أكثر أدوات الهجمات السيبرانية شيوعًا. تشمل هذه البرمجيات الفيروسات وأحصنة طروادة وبرامج التجسس وأحصنة طروادة وأحصنة طروادة. تستهدف البرمجيات الخبيثة الأنظمة الحاسوبية والشبكات والأجهزة الذكية، وتلحق الضرر بالمعلومات وتسرق البيانات الحساسة.

٢. الهجمات بواسطة الاختراق: تتضمن هذه الهجمات اختراق الأنظمة الحاسوبية والشبكات بغية الوصول إلى المعلومات السرية أو تعطيل الأنظمة. قد يستخدم المهاجمون ثغرات في البرامج أو ضعف في إعدادات الأمان لتنفيذ هذه الهجمات.

٣. الهجمات بواسطة الهندسة الاجتماعية: تستخدم الهندسة الاجتماعية عرضًا مشوّقًا لخداع الأفراد وإقناعهم بالكشف عن معلومات سرية أو التفاعل مع رسائل أو روابط خبيثة. قد تتضمن الهندسة الاجتماعية الاحتيال الإلكتروني والتصيد الاحتيالي.

٤. الهجمات بواسطة الامتناع عن الخدمة: تهدف هذه الهجمات إلى تعطيل الخدمات عبر تعميق الشبكة بتكرار الطلبات الضارة أو زيادة حجم البيانات المرسلة إلى الخادم. يمكن أن تتسبب الهجمات بواسطة الامتناع عن الخدمة في تعطيل الشبكات والمواقع الإلكترونية.

٥. الهجمات بواسطة سرقة الهوية: تستهدف سرقة الهوية البيانات الشخصية للأفراد بهدف استخدامها في أنشطة غير قانونية مثل الاحتيال المالي وسرقة الهوية الرقمية.

٦. هجمات التجسس السيبراني: تستهدف هجمات التجسس السيبراني الحصول على المعلومات الحساسة والسرية من أنظمة وشبكات المؤسسات والدول. يستخدم المهاجمون تقنيات متقدمة لاختراق الأنظمة وسرقة المعلومات، وقد تكون هذه الهجمات طويلة الأمد وتستهدف الجوانب الحيوية للمؤسسات مثل: البحوث والتقنيات العسكرية والمعلومات الاقتصادية. تتطلب مكافحة هجمات التجسس السيبراني استخدام تقنيات تحليل الضوضاء وتعزيز الأمان وتطوير السياسات والإجراءات المناسبة لحماية المعلومات الحساسة.

ملاحظة: يجب على المستخدمين أن يكونوا متيقظين ويتبعوا أفضل الممارسات الأمنية لحماية أنفسهم من الهجمات السيبرانية. ينبغي أن يقوموا بتثبيت برامج مضادة للفيروسات وتحديث برامجهم بانتظام، واستخدام كلمات مرور قوية وعدم الاستجابة للرسائل الاحتيالية أو المشبوهة. وأن الحماية السيبرانية مسؤولية الجميع، ويجب أن نعمل جميعًا للحفاظ على سلامة بياناتنا الشخصية وأنظمتنا الحاسوبية.

تحديات ترهل البنية التحتية العراقية

كما قلنا سابقا فالبنية التحتية إحدى أهم الضروريات التي يمكن الاستغناء عنها بأي شكل من الأشكال لعملية النمو والتنمية الاقتصادية على حد سواء، إذ إن وجودها يعد من أهم عناصر جذب الاستثمار وتنمية الاقتصاد الوطني العراقي وتطوره؛ وبالتالي أن عملية التنمية الشاملة في العراق يجب أنه ترافقها خدمات للبنى التحتية موازية لما نطمح وأكثر من ذلك حتى. وهنالك عدة تحديات لنا منها صعوبة مواجهة الهجمات الحالية وصعوبة التعامل مع الهجمات المتطورة التي تستهدف البنية التحتية بشكل خاص، منها ضعف المردود المالي من البنى التحتية، والضعف المالي لتجهيزها، حيث أن الأموال وإن تواجدت لغرض البنية التحتية، فلا يتم صرفها بأتم شكل، ووضعنا الحالي خير مثال يضرب ويقاس. ومن ناحية أخرى، دخول البلد في حروب طويلة الأمد، وعقوبات اقتصادية دولية على العراق؛ وكل ذلك أدى إلى دمار تلك البنى التحتية وخرابها، فلم يكن هناك اهتمام كبير في مجال إعادة إعمار البنى التحتية للبلد؛ نتيجة انخفاض التخصيصات المالية السنوية المخصصة ضمن الموازنات العامة الاتحادية، وهو ما أثر سلبا على سياق عمل هذه المؤسسات والمرافق العامة الاستراتيجية للدولة. بالإضافة إلى ذلك وذاك، تداعيات الحرب مع تنظيم داعش التي أدت إلى انهيار كبير في البنى التحتية لمعظم المدن .وتواجه العراق تحديات استراتيجية تهدد الأمن الاستراتيجي، وتشمل هذه التحديات القطاعات الحكومية وغير الحكومية وتركز على البنية التحتية الأساسية وتأثيرها على الأمن الإدراكي للمواطنين، بما في ذلك التهديدات السيبرانية وزيادة عدد السكان التي تتطلب تخطيطا استراتيجيا.

التخريب بوساطة الهجمات السيبرانية

كأمثلة دولية: فأن اغلب الدول تسعى تغلبها على حساب دول أخرى لفرض نفسها أو لأغراض أخرى. حيث يتم استهداف البنية التحتية للدول سواء كانت مدنية أو عسكرية او هجمات إلكترونية، بما يؤدي إلى شلل أنظمتها وتدمير أنظمة التشغيل الخاصة، والتأثير على تدفق المعلومات بما يؤدي

إلى إرباك عمل البنية التحتية الحيوية، وينشأ عن مثل هذه الهجمات تعطيل العديد من مرافق الحياة في الدول وسيادة الفوضى، مثل استهداف محطات الطاقة والوقود والخدمات المالية والمصرفية ونظم الاتصالات والمواصلات، ومن أبرز الأمثلة على ذلك تعرض أوكرانيا خلال شهر جوان ٢٠١٧ لهجمة إلكترونية شملت محطات الطاقة، بالإضافة. إلى المؤسسات المالية وأحد أكبر المحطات، واختراق شبكة الكهرباء في أوكرانيا في كانون الأول/ديسمبر ٢٠١٥ والهجمات باستخدام فيروس حصان طروادة على شركات الطاقة التي تُوفّر الطاقة لمناطق كييف وعدة مدن اخرى. كان هذا أول هجوم إلكتروني ناجح على شبكة الكهرباء. لقد شهدت السنوات القليلة الماضية العديد من الهجمات الإلكترونية على بعض البنى التحتية الحرجة والمؤسسات العسكرية، وكما قالت مسؤولة أميركية كبيرة في مجال الأمن الإلكتروني، إنه "من المؤكد" أن القراصنة سيعملون على تعطيل البنية التحتية الحيوية في الولايات المتحدة، مثل خطوط الأنابيب والسكك الحديدية، في حالة حدوث صراع بين الدول المعادية لها.

كمثال محلي لعله قيد الحصول: فيعتبر تأمين البنية التحتية الاتصالية الخاصة بجميع العراقيين أمرًا بغاية الأهمية. فلو فرضنا أن تعداد العراق يبلغ ٤٠ مليون نسمة فأن معظم المنازل تمتلك كاميرات مراقبة، ويوجد هاتف لكل شخص، وكمبيوتر في كل دائرة من دوائر العراق، حيث لا تخلو من أجهزة الكمبيوتر لمتابعة المعلومات وما إلى ذلك. لذا، نواجه ١٠٠ مليون جهاز مختلف النوع متصل بشبكة الإنترنت، وبالتالي فإننا نواجه ١٠٠ مليون هجمة أمنية سيبرانية. وهذا في العراق بالخصوص. أما في العالم، فيتوقع وجود أكثر من ٢٥ مليار جهاز متصل بالإنترنت، مما يعني وجود ٢٥ مليار هجمة محتملة. وهنا يكمن أهمية الأمن السيبراني، حيث يحافظ على حساسية وأمان المعلومات الخاصة والعامة للمستخدمين، وذلك لآن اي معلومة قد تكون عادية للبعض ولكنها هي حلقة الوصل التي يحتاجها المخترق للقيام بعمله. ومن منطلق هذه المخاطر يجيب معرفة ما يلي:

مخاطر الأمن السيبراني المرتبط بالذكاء الاصطناعي

أ) مخاطر التطور على المعلومات والبيانات (كابوس المعلومات)

من منا من لم ينشر صورته على مواقع التواصل الاجتماعي، أو لم يشارك بفيديو، أو سجلت له مكالمة مع أحد الأشخاص أو ظهر على إحدى القنوات؟ بالأحرى... جميعنا.

ولأننا في عصر التطور الرقمي، عمل بعض الأشخاص على تطوير الجانب السلبي من هذا الذكاء، فمن خلال مكالمة، أو لقاء، أو فديو أن ينسخ بصمتك الصوتية وبصمتك الوجهية ويظهرك بصوتك ووجهك المعد بالذكاء الاصطناعي حيث لا يمكن تميزه على الناس الذين لا يعرفوك فتوضع بمواضع ابتزاز لا يحمد عقباها.

أبسط مثال للاستخدامات السيئة للذكاء الاصطناعي المرتبط بالأمن السيبراني، عندما تلقت والدة فتاة امريكية من ولاية اريزونا مكالمة مرعبة من ابنتها ذات ١٥ عاما، حيث كانت تصرخ بشدة وهي تطلب المساعدة، وذلك بعد أن خطفها مجهولي الهوية وبحسب صحيفة "ديلي ميل"، قالت الفتاة في المكالمة: "ساعديني يا أمي، أرجوك ساعديني"، وقالت الأم؛ إن الصوت كان مطابقا لابنتها وطريقتها في الصراخ والبكاء. ولكن لم تكن مخطوفة وإنما في رحلة تزلج ولكن المبتزون استعانوا بفيديوهات منشورة لها مسبقا وهي في المدرسة وما شابه ذلك، فاحتاجوا ثوان قليلة من صوتها ليستنسخوا بصمتها بنجاح ولم يحالفهم الحظ بالمال، ولم يتمكنوا من الحصول على قرش واحد لأن الأم اتصلت بزوجها، وفورا اتصل حتى تأكد بأن ابنته في مأمن وأن مكالمة المبتزين وهمية.

وهنا تكمن خطورة الذكاء الاصطناعي على تكوين شخصية بالذكاء الاصطناعي بفيديو واحد ،ومكالمة واحدة، او بصمة صوت واحدة لاستغلال الناس بإمور غير اخلاقية، واستغلاليات مالية وتهديدات وإلى ما شابه ذلك، ومن هذا المنطلق:

١) يجيب الحذر بما تشاركه على مواقع التواصل الاجتماعي من معلومات خاصة، حيث بعض المعلومات غير المهمة بالنسبة إليك قد تكون الوسيلة الأمثل في اختراق حسابك ، أو هاتفك ومعلوماتك الشخصية.

٢) عدم مصادقة الغرباء عل الصفحات الشخصية.

٣) عدم نشر المنشورات بصيغة عامة.

٢) مخاطر تطور الامن السيبراني على الاقتصاد (الكابوس الاقتصادي)

بدأت وتيرة الهجمات بالتسارع أكثر من أي وقت مضى، حيث تحولت لجريمة منظمة تدر مليارات الدولارات على الجهات التي تقوم بها. تم تصنيف الهجمات الإلكترونية على أنها خامس أعلى تصنيف للمخاطر في عام ٢٠٢٠، وأصبحت المعيار الجديد في القطاعين العام والخاص. تستمر هذه الصناعة المحفوفة بالمخاطر في النمو المتصاعد بإقبالنا لعام ٢٠٢٤ فبحسب سكاي نيوز العربية فخلال عام ٢٠٢٢ زادت الهجمات الإلكترونية بنسبة ٣٨ في المئة على صعيد عالمي، وقدرت التكلفة الإجمالية لهذه الهجمات، بنحو ٨.٤ تريليون دولار أميركي.

كما افادت دراسة اجرتها شركة سايبر سيكيورتي فينتشرز بقدرة الجرائم السيبرانية المستقبلية على قيادة اضخم عملية نقل للثروة الاقتصادية العالمية في التاريخ اجمع، والتي تبلغ تكلفتها في جميع انحاء العالم نحو ١٠.٥ تريليون دولار أمريكي بحلول ٢٠٢٥. ويعادل هذا الرقم الخيالي ثالث اضخم اقتصاد عالمي بعد الولايات المتحدة والصين فعلى كافة الشركات والمؤسسات أن تكون سباقة في أخذ الخطوة الأولى قبل أن تشن أي هجمة عليها، فبأخذ التدابير المناسبة باستعمال أحدث التكنلوجيا لتطوير المهارات والادوات اللازمة لتلك ووضع نصف المبالغ التي تقدر بخسارتها في الشركة جراء الهجمات بأخذها، ووضع واستثمارها في الامن السيبراني افضل حل يواجه معركة لن تنتهي إلا بقيام الساعة حيث ستكبدنا خسائر مالية كبرى من أجل الصمود ضد هذه الحرب لأن المهاجمون طوروا أنسهم في الامن السيبراني إضافة إلى تعزيزه بالذكاء الاصطناعي وصنع عدة برامج او

شفرات يمكن من خلالها كتابة الرموز المعتادة وغير المعتادة لأن الذكاء الاصطناعي بإمكانه توليد كلمات لا نهائية من الرموز المختلفة من الارقاء والحرف الكبيرة.

وهناك عدة امثلة على الخسائر التي تستهدف الشركات والافراد ومنها:

المثال ١:- في تموز ٢٠١٥ اكتشفت أحد الشركات المسماة last pass نشاطا غير معتاد لأول مرة على شبكتها، ولقد تبين أن هناك مجموعة من الإرهابيين الإلكترونيين المهاجمين قد سرقوا عنوان البريد الإلكتروني للمستخدمين ورسائل التذكير لكمات مرورهم، ولحسن الحظ لم يتمكنوا من معرفة البيانات المخزنة بسبب المصادقات المشفرة التي وضعتها الشركة. وكانت تلك أهم التدابير التي وضعتها الشركة لمواجهة الهجمات السيبرانية.

المثال ٢ :- تعرضت البيانات الشخصية الحساسة الخاصة بـ١٤٣ مليونا من عملاء شركة Equifax الائتمانية في الولايات المتحدة للخطر من قبل مجرمي الإنترنت، في واحدة من أكبر حوادث اختراق البيانات في تاريخ الولايات المتحدة. وعلى الرغم من أن قواعد بيانات الائتمان الاستهلاكي والتجاري لم تتأثر، إلا أن الشركة صرحت بأن القراصنة تمكنوا من الوصول إلى أرقام الضمان الاجتماعي وتواريخ الميلاد وعناوين خاصة بالعملاء في الفترة بين منتصف مايو ويوليو ٢٠١٧، بالإضافة إلى ذلك، تأثرت أرقام بطاقات الإتمان لحوالي ٢٠٩٠٠٠ من المستهلكين.

٣) مخاطر تطور الأمن السيبراني على منهجية الحروب الحديثة (الكابوس النووي)

تعتبر تكنولوجيا المعلومات محل اهتمام المؤسسات العسكرية والأمنية، وهو ما غير أشكال الحروب والمواجهة، هذا الأمر الذي جعل فضاء القوة السيبرانية ذا شأن وأهمية في الاستراتيجيات العسكرية والمدنية، وأصبح قوة قصوى تستطيع أن تأثر حتى في القوة الاخرى من القوة الأخرى البرية، البحرية، الجوية والفضائية، فقد تغيرت الحرب في عصر المعلوماتية من خلال ظهور مسرح جديد لها وهو الفضاء السيبراني، فمجريات الحروب بدأت بالتغير حالما انضم الامن السيبراني، حيث بدأ يوضع بالمقدمة بل أن اي حرب دولية يمكن أن يبدأ الامن السيبراني ويحولها من حرب الكترونية

إلي حرب برية وجوية وبحرية ونووية وذلك من خلال قيام قراصنة محترفين بشن هجمات إلكترونية بغرض السيطرة على نظم القيادة والسيطرة عن بعد، حيث يؤدي إلى إخراج منظومات الأسلحة عن سيرة القيادة المركزية، وإعادة توجيهها نحو المؤسسات الداخلية أو ضد دول صديقة، كمثال جوي يمكن السيطرة على الطائرات من دون طيار، وكمثال بري يمكن السيطرة على منظومة اطلاق الصواريخ وثال بحري السيطرة على الغواصات في أعماق البحار، أو السيطرة حتى على الفضاء من خلال الأقمار الصناعية العسكرية في الفضاء الخارجي وإخراجها عن سيطرة الدولة التابعة لها هذه الأسلحة والمعدات، إذ تزداد خطورة مثل هذه الهجمات إثر التطور التكنولوجي واعتماد اللوجستيات ونظم القيادة والتحكم وتحديد الأهداف، وإصابتها على برامج الكمبيوتر وشبكات الاتصال كما تقوم الهجمات السيبرانية بتدمير أنظمة إلكترونية لمنشآت حيوية عسكرية، وتعطيل أو إتلاف شبكات الدفاع العسكرية عن بعد، واختراق أو تعطيل أو تدمير شبكات القطاع الخاص ذا الصلة بالقطاع العسكري وقد تحدث الهجومات السيبرانية من أجل سرقة تصميمات الأسلحة العسكرية والتقنيات التكنولوجية الحديثة

وفكرة التشابك بين الجانب النووي وغير النووي (السيبراني) عميقة جدا، وذلك لأن الأسلحة النووية لم تعد منفصلة في حدود خاصة بسبب تعدد مهماتها وأصبحت انظمتها بذلك هدفا للاختراق، ففي أي نزاع محتمل يمكن أن يكون للخصوم حافز محتمل لمهاجمة اصول القيادة والتحكم عن بعد او ذات التحكم المزدوج، والتي تستخدم في العمليات النووية وغير النووية. الانظمة الحالية تعتمد الاشارات الرقمية بدلا من الاشارات التناضرية فقد اصبحت تعتمد بشكل اساسي على البروتوكلات القائمة على اساس الانترنيت.

كما يمكن شن الحرب النووية بهجمة الكترونية، حيث صرحت امريكا بان اي هجمة تطال اجهزتها الرادارية المتعلقة بالأمن النووي فأنها لا تترد بالرد بالسلاح النووي، وهذا سيشكل خطر عالمي مباشر

بشأن قيام اول حرب نووية عالمية وذلك بضغطات ازرار الكترونية من اطراف صديقة او معادية وسيحدث ما لا بحمد عقباه.

وجريمة الابادة النووية تعد أحد أكبر الجرائم بحق الانسانية ولا تقل شأنا بل أخطر حتى من جرائم التعدي الجنسي على القاصرات، جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية، جرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية عبر الإنترنت، الجرائم المعلوماتية ضد الدولة والسلامة العامة.

عواقب تأخر الاستثمار بالأمن السيبراني

يعد الاستثمار في الأمن السيبراني أفضل الوسائل لتأمين البنى التحتية، خاصة بعد الترهلات والتحديات التي رافقتها منذ سنوات عدة، ونحن الآن في خضم التحول الرقمي، ولقد بات الحفاظ على الأمن السيبراني العراقي، **والاستثمار الإجباري** في التقنيات الحديثة لضمان أمن نظام شركاتنا ومؤسساتنا وسلامتها أمرًا **حتميًا** من أجل الاستمرار والتطور والتوسع الذي يشهده هذا العالم.

وبتطور الامن السيبراني اعقبه تطور للمقرنصين والمهاجمين الالكترونيين وتفننوا وطفروا طفرة نوعية ضخمة، وباتوا الحد الفاصل في بقاء أي مؤسسة من عدمها وهذه المشكلة أكبر العقبات التي تواجه المؤسسات كافة.

وكمثال دولي:

فأن مدعي عام نيويورك أجبر كلية جامعية على الاستثمار في الحلول الأمنية بقيمة ٣.٥ مليون دولار على مدار الست الأعوام القادمة. هذا القرار أتى بعد تعرضها لهجوم فيروس فدية في عام ٢٠٢١ مسربا بيانات ٢٠٠ ألف شخص. وهذه الكلية الجامعية Marymount Manhattan College في نيويورك متخصصة بالفنون. تعرضت في عام ٢٠٢١ لهجوم فيروس فدية Ransomware.

وحسب ما كتبه حسام خطاب:

مجموعة الاختراق استغلت ثغرات مفتوحة في خادم الايميل Exchange Server، ونفذوا إلى بيانات آلاف الأشخاص. قدروا عددهم حينها بمائتي ألف. البيانات اشتملت على أرقام الضمان الاجتماعي، وأرقام الوثائق الحكومية، والسجلات الطبية، وأرقام البطاقات الائتمانية، وكلمات السر. دفعوا مبلغ الفدية لمجموعة الاختراق، وقضوا بعدها ثمانية أشهر في التحقيق ليقدموا تقريرهم للجهات الحكومية، ثم استهلت الجهات الحكومية تحقيقها، وتأكدوا بأن الكلية لم تطبق كثيرا من الضوابط الأمنية. الكلية كانت لا تحذف بيانات الطلاب بعد انتهاء الغاية منها. عدد طلاب الدفعة الواحدة لا يتعدى الألفين، وعدد الأشخاص المتضررين يؤكد هذا الجانب إذ أن بعض البيانات المخترقة تعود إلى ما قبل عشرة أعوام. ناهيك عن استخدام نسخ نظام تشغيل Windows قديمة، وعدم وجود برنامج دوري لفحوصات الاختراق وكشف الثغرات، وقلة التوعية الأمنية، وعدم تشفير البيانات الحساسة. الجهات الحكومية كانت على وشك تغريم الكلية بمليون دولار، إلا أنهم اتبعوا معهم نهجا مختلفا هذه المرة. فضلوا **إجبار** الكلية على الاستثمار في الأمن السيبراني كاستثمار طويل الأمد. ابرمت الكلية اتفاقا مع الجهات الحكومية على أنها ستستثمر ٣.٥ مليون دولار في الأمن السيبراني ما بين عامي ٢٠٢٣ و ٢٠٢٩. وإذا أخفقت الكلية في تنفيذ تعهداتها، عليها دفع غرامة المليون دولار مع فوائدها.

سلبيات الامن السيبراني:

من ناحية الامن والدفاع: أحد السلبيات الرئيسية للأمن السيبراني هو تعرض الحكومات والمؤسسات الحكومية والعسكرية للهجمات الإلكترونية. يمكن للمهاجمين القرصنة والوصول غير المشروع إلى معلومات حساسة وسرية، مما يعرض سلامة الدولة وأمنها للخطر. قد يتعرض أيضًا النظام العسكري للاختراق والتلاعب بالأوامر والتحكم في الأنظمة العسكرية الحيوية، مما يعرض الأمن القومي للتهديدات الكبيرة، كما انه ليس فعال دائما، وأسهم بإدخال العالم بحرب لم يبدأها احد حتى تنتهي،

فبعض الاختراقات ستكون هي الذريعة لبدأ حرب جوية وبرية وبحرية ونووية، وبعض الاختراقات قد تسهم في اطلاق صواريخ موجهه او نداءات بهجوم كاذب من صوت مزيف من قادة الدول والمراجع، حيث سيسهم الذكاء الاصطناعي ايضا بإيصال فيديو بالصوت وصورة القادة إلى الجنود، وسيتمكن الإرهاب الإلكتروني من تنفيذ خططه الإجرامية.

من ناحية الاقتصاد: يشكل الأمن السيبراني تحديًا كبيرًا على الاقتصاد، حيث تؤثر الهجمات السيبرانية سلبًا على الشركات والمؤسسات الحكومية، مما يهدد استقرار النظم الاقتصادية. وكذلك تعطل الخدمات الأساسية مثل الطاقة والماء والنقل نتيجة هذه الهجمات، مما يتسبب في خسائر فادحة للشركات وتأثير سلبي على النمو الاقتصادي. كما تؤثر الهجمات السيبرانية على الثقة في النظم المالية والتجارية، حيث يمكن أن تؤدي إلى سرقة الأموال أو التلاعب بها، مما يؤدي إلى فقدان الثقة وانخفاض الاستثمارات. وتجلب مكافحة الهجمات السيبرانية تكاليف اقتصادية هائلة، حيث يجب على الشركات والحكومات استثمار الكثير لتعزيز الأمان السيبراني وتنمية البنية التحتية اللازمة لحماية البيانات والأنظمة. يمكن أن تؤدي هذه التكاليف الإضافية إلى تباطؤ النمو الاقتصادي وانخفاض الاستثمار في مشاريع أخرى. بشكل عام، يمكن القول إن الأمن السيبراني يؤثر على الاقتصاد من خلال تعطيل الخدمات الأساسية وتهديد الثقة في الأنظمة.

من ناحية الأفراد: أحد السلبيات الرئيسية للأمن السيبراني أولًا، هو انتهاك الخصوصية. فعندما يتم اختراق الأنظمة الإلكترونية أو الشبكات، يمكن للمهاجمين الوصول إلى المعلومات الشخصية للأفراد مثل البيانات المصرفية أو المعلومات الحساسة الأخرى. ثانياً، يمكن أن يؤثر الاختراق الأمني على الصحة النفسية للأفراد، حيث يشعرون بالقلق والاضطراب والشعور بعدم الأمان. ثالثاً، قد يزيد الأمن السيبراني من احتمالية وقوع الاحتيال وفقدان الأموال أو البيانات الشخصية. لحماية أنفسهم، يجب على الأفراد أن يكونوا حذرين ويستخدموا كلمات مرور قوية وبرامج مكافحة الفيروسات وتطبيقات

الحماية. ينبغي أن يكونوا متوعين بالمخاطر المرتبطة بالأمن السيبراني ويتخذوا التدابير اللازمة للحفاظ على سلامتهم الرقمية.

مشاكل الأمن السيبراني في العراق:

١) أحد أكبر مشاكل الأمن السيبراني في العراق أنه سيكلفنا مبالغ طائلة في ظل الضعف المالي فضلا إلى ذلك سيكلف المجهود والوقت، بينما نحن في مرحلة متأخرة في ظل التطور العالمي المعلوماتي. وهذه احد أهم العوامل التي تؤثر على القدرة العراقية على مواجهة التهديدات السيبرانية. وأن التأمين على التكنولوجيا وتطوير القدرات السيبرانية يتطلب استثمارات كبيرة، وهو أمر يواجه صعوبة في ظل الضغوط المالية التي يعاني منها العراق حالياً. وبسبب هذه الصعوبات المالية، يصعب على العراق توفير الأجهزة والبرامج الحديثة لحماية الأنظمة ومواجهة الهجمات

٢) غياب الوعي العام بالأمن السيبراني، وكذلك غياب الثقافة السيبرانية وخاصة المتعلقة بالجرائم الالكترونية.

٣) تراجع الامن السيبراني العراقي كما نشر الاتحاد العالمي للاتصالات في سنة ٢٠٢١ حيث كان ترتيب العراق في المرتبة ١٧ عربيا و ١٢٩ عالميا، ويرجح ذلك التراجع إلى عدم تقديم المعلومات والبيانات إلى فريق الاتحاد العالمي للاتصالات حيث يعد هذا مشكلة ويؤدي إلى مشكلة أخرى وهي: تجاهل الجهات الرسمية المسؤولة عن ملف الامن والدفاع بملف الأمن السيبراني في العراق بينما يعد الشريان الرئيسي للأمن القومي العراقي.

ملاحظة: حلول المشكلة الأولى في التنبؤ، أما المشكلتان الثانية والثالثة في التوصيات.

الايجابيات المترتبة بوجود الأمن السيبراني في العراق:

١) ستكتمل معادلة منقوصة منذ الأمد وهي التعزيز بالقوة الرابعة= تعزيز الامن والدفاع. حيث سيسهم في الأمن السيبراني بإضافة قوته الأمنية إلى كافة المؤسسات، وإلى قوى العراق البحرية، الجوية، البرية.

٢) مواكبة التطور الأمني العراقي، والصعود بسلم التطور الأمني العالمي من خلال سد الثغرات الأمنية بواسطة الأمن السيبراني.

٣) مكافحة التحديات والتهديدات الإرهابية الناشئة وغير الناشئة.، والتي قد تستهدف الهياكل الحكومية، المؤسسات، البنية التحتية، والأفراد.

٤) بما أنه أحد اشكال الذكاء الاصطناعي والثورة الصناعية الرابعة فبالإمكان جعله مصدر توريد مال للدولة والشركات وذلك من خلال الاستثمار في تدابير وأجهزة وانظمة الأمن السيبراني للحد من الهجمات السيبرانية بقدر الإمكان، وأن اضافة الذكاء الاصطناعي للأمن السيبراني سيفرق في التكاليف وافضل من مَن يستخدمون الامن السيبراني بدون الاخير.

٥) إشعار الافراد في أمان اكثر عندما يعلمون انهم محميين من الهجمات الالكترونية.

٦) سيحافظ على امان الشركات وكافة مؤسسات الدولة الامنية او الخدمية.

٧) سيتم تعزيز الاستقرار الاقتصادي بشكل ممتاز، هذا سيتم حفظ البيئة الرقمية للشركات والمؤسسات كافة، مما يعزز الثقة ويسهم في تحقيق الاستقرار الاقتصادي.

٨) التعزيز من انتاجية الافراد والشركات لأنهم يجرون عمليات استباقية لمنع قبل وقوع اي هجمة من خلال مسح الفيروسات، وتحسين جدران الحماية والنسخ الاحتياطي الالي وغيرها من الاجراءات الاحترازية.

٩) سيدخل العراق في مرحلة متقدمة من الاستقرار الأمني، حيث أنه الخط الاحترازي العالمي الجديد وخط الدفاع الأول للأمن، حيث أن الأمن السيبراني ليس خيارا للعراق بعد الآن لتعزيز أمنه بل أصبح أولوية قصوى.

فوائد ضم الذكاء الاصطناعي للأمن السيبراني:

- تحسين وتوفير المساعدة لعامل الأمن البشري من خلال الاستجابة الفورية للهجمات.
- سيساعد في التنبؤ للتهديدات المستقبلية، ومعالجة أغلب التحديات الجديدة.
- سيقلل من وقت الاستجابة.
- سيتعامل مع عدد هائل من البيانات في آن واحد.

التوصيات والحلول المبتكرة لمشاكل الأمن السيبراني العراقي، وذلك لتعزيز الأمن والدفاع.

١) إنشاء قوانين خاصة بالأمن السيبراني ومن يخلفها يتحمل كافة التبعات القانونية.
٢) يجب تحسين البنية التحتية السيبرانية في العراق، و توفير أنظمة وشبكات سيبرانية آمنة ومحمية تمكن من اكتشاف ومنع الهجمات السيبرانية. يجب أيضًا توفير أدوات وبرامج متطورة لتحليل ورصد الأنشطة السيبرانية غير المشروعة.
٣) نشر الوعي السيبراني من خلاص التواصل الاجتماعي والدورات المتنقلة على كافة مؤسسات الدولة والشركات.
٤) تحديد يوم خاص في السنة للتوعية بالأمن السيبراني
٥) استحداث قسم الأمن السيبراني بشكل أوسع في الكليات الحكومية والأهلية
٦) التعاون المشترك من خلال:

أ) التعاون الداخلي بين وزارة التعليم العالي والبحث العلمي مع وزارة الدفاع بإلقاء محاضرات ودورات مشتركة سواءً في الكليات المدنية أو في مدرسة الحاسبات الالكترونية الخاصة بوزارة الدفاع.
ب) التعاون الخارجي بين العراق ودول العالم التي لها باع وخبرة في الأمن السيبراني كالدول الاوربية والاسيوية.

٧) إنشاء أكاديمية للذكاء الاصطناعي مشتركة بين وزارة الاتصالات ووزارة التعليم العالي والبحث العلمي الهدف منها إنتاج وتصدير حلول تعتمد على الذكاء الاصطناعي.

٨) نوصي بإجراء المزيد من الأبحاث التي تتضمن الذكاء الاصطناعي بشكل عام والامن السيبراني بشكل خاص وكذلك زيادة الإنفاق عليها من خلال الجوائز المالية والمعنوية لدعم وتشجيع الباحثين في هذا المجال.

٩) ادراج مجال الفضاء السيبراني ضمن مناهج التعليم في الجمهورية العراقية.

١٠) يجب على الرؤساء التنفيذين في مركز الأمن السيبراني أن يعدوا موجزا للعمل قبل نهاية كل سنة، وتقريرا يغطي العناصر التي تسهم في تعزيز الأمن والدفاع والصمود السيبراني وفق التحديات الناشئة.

بناء الجدار يبدأ بحجر صغير:

لن ينجح الأمن السيبراني لدينا ما لم نتبع الاستراتيجية السيبرانية العراقية ذات السقف الزمني التنفيذي المحدد والمعدة من قبل مستشارية الامن الوطني:

المرحلة الأولى(١ سنة) / معالجة المخاوف الفورية.

المرحلة الثانية (٣ سنوات) / بناء البنية التحتية.

المرحلة الثالثة (٥ سنوات وما بعدها) / تطوير الاعتماد على الذات.

تنبؤ:

أثق جيدا أن في حلول العقد القادم سيشهد العراق طفرة نوعية في ناحية الأمن والدفاع؛ فكمثال لوزارة الدفاع العراقية فأن الرفد المستمر للشباب وضخ الدماء الجديدة سيزيد من ناحية القدرة الانسانية

الدفاعية. كما أن إدماج الذكاء الاصطناعي ضمن الأمن السيبراني لمكافحة الإرهاب الإلكتروني سيزيد من القدرة الامنية السيبرانية.

سيكون العراق متعافي ماديا بعد سلسة الحروب في العقود الثلاثة الماضية، على عكس بقية الدول التي استفادت من فترة النقاهة في تطوير مؤسساتها، وذلك بتفعيلها لعدة ملفات منها الأمن السيبراني، فعلى سبيل المثال في الامن والدفاع فنذكر وزارة الدفاع ، فبعد الحرمان ل٣ عقود من خدمات هيئة التصنيع الحربي صوت البرلمان العراقي عام ٢٠١٩ على عودة الهيئة. يجب التعاون مع الدول التي لديها خبرة في تطوير جيوشها وتجهيزها بالمعدات الحديثة. سيساهم ذلك في تطوير صناعة الدفاع الذكية وزيادة إنتاج الأسلحة ستسهم في تقليل ميزانية الاستيراد. وسيتمكن من ضخ بعض الأموال في ناحية الأمن السيبراني الدفاعي. فالنفقات السنوية للسياسة الدفاعية في العراق بلغت حوالي ٥ مليارات دولار في الفترة من ٢٠١٥ إلى ٢٠٢١، وهو أمر يشكل عبئًا على ميزانيتنا، لأننا نستورد قرابة ٩٠% من حاجات القوات الأمنية من الخارج. فافتتاح مصنع الاعتدة الذي ينتج ٦٥ اطلاق سنويا قريبا، خط إنتاج المسدس الوطني، الطائرات المسيرة الذكية، وتعاوننا مع الدول العظمى التي لها باع في تطور جيوشها أول قطرات الغيث بتلك النبوءة.

من المتوقع أن يستفيد العراق من الاستثمار في الأمن السيبراني لزيادة ميزانية وزارة الدفاع. يجب أن يأخذ العراق في الاعتبار التحديات الجديدة مثل حرب الذكاء الاصطناعي والأمن السيبراني ، والتي لم يبدأها أحد حتى ينهيها، يعتبر الذكاء الاصطناعي حاليًا مفتاحاً هاماً في حماية المؤسسات الأمنية والمدنية ومعلوماتها. في العصر الصناعي الرابع والخامس المقبل ، يجب على العراق أن يدمج الأمن السيبراني المتصل بالذكاء الاصطناعي في جميع الشركات والمؤسسات والوزارات ، خاصة تلك ذات الأهداف الأمنية. ويجب أن يكتمل حلقة الأمن والدفاع بالتعاون من أجل مصلحة العراق. ومن المتوقع أن يشهد العراق تقدمًا أمنيًا في العقد المقبل إذا نفذ الخطة المعدة من قبل مستشارية الأمن الوطني وتطبيق توصياتي المذكورة سابقا.

الخاتمة:

في ختام بحثي، أولاً، لا يسعني إلا أن أكون قد وفقت وحققت هدفي المرجو في عرض الأمن السيبراني بشكل يلائم زيادة الوعي الأمني، خاصة بعد معرفة تبعاته السلبية والإيجابية، ومعرفة كيفية تعزيز الأمن والدفاع من خلال الإجراءات الاحترازية اللازمة لمواجهة الجوانب السلبية والكوابيس السيبرانية، وكيف للقوة الرابعة أن تكون سلاح ذو حدين، إما في تقدم الدولة أمنيا واقتصاديا، أو ذهابها ببنيتها التحتية وأفرادها ومؤسساتها واقتصادها إلى الهاوية. ثانيًا، إن التركيز الأكبر على الجوانب السلبية ليس إلا نتيجة الظروف والأحداث الحالية، فحتى عرض الجانبي السلبي قبل الجانبي الإيجابي لها غايات عدة. وكخلاصةً، لازلنا في مرحلة معالجة المخاوف الفورية والجوانب السلبية، فباعتماد الحلول سنصل إلى مراحل قد تكون خيالية بالنسبة للكثير، ولكننا أقرب من أي وقت مضى ، خاصة بعد تأمين الجوانب البرية والجوية والبحرية. فطريق الأمن السيبراني معبد، وبانتظار خطواتنا الجدية الأولى.

المصادر:

أولاً: الوثائق:

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

ثانيا: الكتب:

محمد سعد محمود (٢٠٢٠) الحرب السيبرانية: أدواتها وقودها خسائرها.

ثالثا: البحوث والدراسات:

شريفة كلاع(٢٠٢٢). الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني

علي زياد العلي(٢٠١٨).تحديات ترهل البنية التحتية العراقية. مركز البيان للدراسات والتخطيط.

خورخي فلوريس كاييخاس، وعائشة عفيفي، ونيكوالي لوزينسكي(٢٠٢١). الأمن السيبراني في مؤسسات منظومة الأمم المتحدة.

رم كولهاس (٢٠٢٢). البنية التحتية أهم بكثير من الهندسة.

د. غسان اللامي (٢٠١٣).تحليل مكونات البنية التحتية لتكنولوجيا المعلومات، دراسة استطلاعية في بيئة عمل عراقية.