ISSN: 1994-4217 (Print) 2518-5586(online)

Journal of College of Education

Available online at: https://eduj.uowasit.edu.iq

Assis. lect. Hussein Latif Hashem

Directorate of Education, Wasit Governorate

Email: hu32122hu@gmail.com

Keywords:

Electronic crimes ، Informatics Crime ، Hacker or Hacking ، Cyber Threats

A r t i c l e i n f o

Article history:

Received 5. May.2025

Accepted 11. Jun.2025

Published 10.May.2026

Internet crime and Cyber Security

A B S T R A C T

The aim of this research is to uncover the relationship between cybercrime and cyber security, particularly given that the scientific advancements witnessed worldwide in the field of communications technology have made social networks (the Internet) one of the most important means of committing crimes, requiring little physical effort.

Therefore, the research seeks to demonstrate the importance of cyber security in light of local and global data to reduce cybercrime, which has recently escalated, and to highlight the dangers of these crimes and the international and legislative efforts to combat them.

DOI: https://doi.org/10.31185/eduj.Vol63.Iss1.4522

جرائم الإنترنت والأمن السيبراني

م.م. حسين لطيف هاشم

مديرية تربية محافظة واسط

الملخّص:

يتجسد هدف البحث في الكشف عن العلاقة القائمة بين جرائم الانترنيت والأمن السيبراني، سيما وإن التطور العلمي الذي شهده العالم في مجال تكنولوجيا الاتصالات جعل شبكات التواصل (الانترنيت) من أهم الوسائل لتنفيذ الجريمة والتي لا تتطلب أي جهدا بدني يذكر.

لذا فإن البحث يسعى لبيان أهمية الأمن السيبراني في ضوء المعطيات المحلية والعالمية للحد من جرائم الانترنيت التي تفاقمت في المدة الأخيرة وبيان مخاطر تلك الجرائم والجهود الدولية والتشريعية لمكافحتها.

الكلمات المفتاحية: الجرائم الالكترونية ، الجريمة المعلوماتية ، الهكر أو الاختراق، التهديدات السيبرانية.

المقدمة: The Introduction

تعد الجريمة بشكل عام من الظواهر الاجتماعية التي لازمت الإنسان منذ القدم وعانى منها على مرور التاريخ ، ولعل جريمة القتل التي وقعت بين أبناء ادم (عليه السلام) دليل على قدم هذه الظاهرة ،فقد عانت منها المجتمعات البشرية إذ لا يخلو منها أي مجتمع من المجتمعات المتقدمة والنامية على حد سواء ، فكلما زاد عدد السكان زادت حاجاتهم وكثرت رغباتهم ومصالحهم ونزواتهم ، فالجريمة ما هي إلا صورة من صور تفاعل الإنسان مع بيئته ، إذ أنها تتباين من مجتمع إلى أخر من حيث نوع وكم الجريمة المرتكبة فضلاً عن تباينها داخل المجتمع الواحد جراء التغيرات الاقتصادية والاجتماعية والثقافية والدينية والسياسية والنفسية .

إن التطور العلمي الذي شهده العالم في مجال تكنولوجيا الاتصالات جعل شبكات التواصل (الانترنيت)من أهم الوسائل التي يتم من خلالها ممارسة الأنشطة التجارية والتعليمية والترفيهية وعلى المستوى الدولي وعلى مستوى الأشخاص ، اذ يكاد لا يخلو بيت من استخدام الانترنيت ، مما جعل هذه التقنية وسيلة مثالية لتنفيذ الجريمة والتي لا تتطلب أي جهدا بدني يذكر ، فقد مكن استخدام وسائل التواصل بفاعلية وسرعة عالية وتزايد استخدام الأشخاص لها عن طريق توظيف هذه الموقع والتعدي على الآخرين وجهلهم بالقوانين التي تحد من ذلك فضلاً عن وجود عامل مهم المتمثل بضعف الدور الرقابي للأسرة بمتابعة أبنائها ، إذ أصبحت هذه المواقع أدوات للابتزاز والتهديد والتشهير والسب والقذف بالآخرين .

من هنا جاءت أهمية هذا البحث الذي يمكن صياغة مشكلته بالسؤال الآتي:

ما أهمية الأمن السيبراني في الحد من جرائم الانترنيت أو ما تسمى بالجرائم الالكترونية؟

لذا فان فرضية البحث تكمن في الإجابة الآتية:

للأمن السيبراني أثر فعّال في الحد من معالجة جرائم الانترنيت وعلى كافة المستويات الشخصية والمجتمعية والقطاعات الاقتصادية ومؤسسات الدولة، سيما وان للأمن السيبراني أهمية في حماية أجهزة الكمبيوتر والشبكات وتطبيقات البرامج والأنظمة الهامة والبيانات من التهديدات الرقمية المحتملة.

تكمن أهمية البحث من طبيعة العلاقة القائمة بين جرائم الانترنيت والأمن السيبراني سيما وان الوتيرة السريعة للتحول الرقمي جلبت فرصا لا تصدق ومخاطر جسيمة ، مع قيام الشركات والهيئات الحكومية بتوظيف التكنولوجيا لتحقيق النمو والكفاءة ، فان المتطلبات الأساسية لاستراتيجيات الأمن السيبراني الفعالة تصبح واضحة بشكل متزايد ، ولقد حدث تحول كبير في التهديدات الالكترونية (الانترنيت) التي لم تعد افتراضية بل أصبحت حقيقة ملموسة يمكن أن تقوض الاستقرار العائلي هذا على مستوى الأسر أو العوائل مثلما تقوض مؤسسات الدولة المالية والأمنية والمخابراتية .

وفي ضوء ذلك فان منهجية البحث العلمي تتطلب صياغة عدد من المحاور التي يمكن اعتمادها للوصول إلى النتائج، وسيتم تناول تلك المحاور في ثلاث اتجاهات أو أنماط جميعها تشكل محتوى هذا البحث .

أولا: مفاهيم ومصطلحات Concepts and Terms

أ- جهاز الكمبيوتر Computer :

كلمة Computer كلمة انكليزية مشتقة من كلمة To Cmputer وهو آلة تعمل بالطاقة مجهزة بمجموعة مفاتيح كهربائية ودوائر الكترونية وفيها أقسام للتخزين وأخرى للتسجيل تعمل كعمليات حسابية بسرعة فائقة ودقة بالغة، وتطلق على الكمبيوتر تسميات متعددة منها العقل الالكتروني، الحاسب الالكتروني أو الحاسب الآلي والحاسوب (حجازي ،٢٠٠٤، ص٥٦)

ب- الانترنيت Internet

يعرف بأنه شبكة من شبكات الحاسبات الآلية وهي مكونة من كلمتين هما Inter Connection وكلمة Network ، وهذا يعني أن مئات بل الألف من الشبكات مربوطة مع بعضها البعض مكونة من حواسيب آلية مختلفة تم توصيلها ببعضها البعض بطريقة بسيطة تبدو كأنها قطعة واحدة، فالأنترنيت عبارة عن حاسب ألي يتحدث إلى أخر يرتبطان بواسطة سلك التلفون العادي أو أي نوع أخر من الكوابل. (جابر، ٢٠٠٤، ص٥١)

ج- جرائم الانترنيت (الالكترونية) Internet Crimes :

هي كل فعل أو نشاط غير مشروع فيه خروج عن القيم والقوانين الوضعية والدينية والأخلاقية والقانونية والمعيارية في معايير السلوك السوي (عبيد ،٢٠٢٢، ص٢٢)

د- الجريمة المعلوماتية Cybercrime:

تُعرف بأنها الأفعال التي تقع من قبل الشخص الطبيعي أو المعنوي مما من شأنه أن يشكل اعتداء على الحقوق المحمية قانوناً ناجمة عن الاستخدام غير المشروع لتقنيات نظم المعلومات سواء بطريقة مباشرة أو غير مباشرة وتؤدي إلى الإضرار بالمصلحة الاجتماعية (السعدون ،٢٠١٩، ص٤٢)

هـ- الهكر أو الاختراق Hacker or Hack:

يُقصد به اختراق مجموعة من الأنظمة والبرمجيات التي تدير عدد من مواقع أو مؤسسات الدولة والجهات ذات العلاقة أو الأفراد أو الشركات لأغراض التجسس أو تدمير البيانات أو تغيير المعلومات والتلاعب بالأرصدة المالية واختراق المواقع، وهو من مظاهر ما يسمى الجريمة الالكترونية. (جابر، ٢٠٢٢، ص٨٨)

و-السلوك المنحرف Deviant behavior:

هو كل فعل أو تصرف فيه خروج عن القيم والتقاليد المجتمعية والدينية والأخلاقية والقانونية والخروج عن معايير السلوك (عبد القادر،٢٠٢٠، ص٤١)

ز- مجال الانحراف الالكتروني Electronic Deviation Field:

هو المجال الأكثر شيوعاً وانتشاراً ويمثل هذا النوع من المجال عن طريق سلبية الاستخدام من قبل من اخترق شبكة تكنولوجيا لغرض الحصول على مكاسب، كالتلاعب بالمعلومات والمعطيات الرقمية والعبث فيها أو بيعها أو استغلالها داخل الشبكة المظلمة (الحيالي، ٢٠٢١، ص١٧).

ح- مواقع التحريض والتأثير Incitement and Influence Sites :

هي مجموعة من المواقع والبرمجيات التي تنقل عن عناصر الفكر والتطرف، إما لأشخاص طبيعيين أو معنويين يتبنون أفكاراً مضادة أو تتجه مع الجماعات والمذاهب الاجتماعية والسياسية هدفها إثارة المجتمعات المختلفة على تبني الأفكار الانقسامية إما بالتحريض المباشر أو غير المباشر (محمد ،٢٠٢٠، ص١٧٩)

ط- تسريب الإخبار والمعلومات Leaking News and Information :

هي شبكة تسمى شبكة التسريب ويتم من خلالها تسريب المعلومات ونشر المعلومات عبر ما يُسمى بالـ (الهاكر الأخلاقي) أو (القبعات البيضاء) أو الأفراد الذين يدخلون للحصول على المعلومات، وهي أكثر الشبكات تأثيراً، لما لها من علاقة مباشرة بين الحصول الأولي للمعلومة وتحويلها لغرض النشر العلني، أو ما يُسمى بالتسريبات المقصودة، من

خلال الدخول للنظام وتحديث ملف الأشخاص الحقيقين ويتلقى عليهم صلاحيات الدخول أو التشغيل المؤقت (جابر ،٢٠٢٢، ص٨٨)

ك- الأمن السيبراني Cyber Security :

هو مجموعة من المهمات، مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر، وتدريبات وممارسات وتقنيات تستخدم لحماية البيئة السيبرانية والمؤسسات والمستخدمين (الطيار ،٢٠٢٠، ص ٢٦٤)

ل- الفضاء السيبراني Cyber Space :

عبارة عن شبكة مترابطة من الهياكل الأساسية للمعلومات الحرجة والغير حرجة والذي يعمل على تقريب موارد المعلومات والاتصالات المترابطة باستخدام تكنولوجيا المعلومات والاتصالات، وهو يشمل جميع أشكال التدخلات الرقمية، التفاعلات، التواصل الاجتماعي، التخصصات الاجتماعية، أنشطة المعلومات، المحتويات، الاتصالات والموارد التي يتم نشرها من قبل الشبكات المترابطة (الهيئة الوطنية ،٢٠١٨، ص٣٣) .

م- تهديد Threat:

أي ظرف أو حدث من المحتمل أن يؤثر سلبا على أعمال الجهة (بما في ذلك مهمتها او وظائفها أو بمصداقيتها أو سمعتها) أو أصولها مستغلا أحد أنظم المعلومات عن طريق الوصول غير المصرح به إلى المعلومات أو تدميرها أو كشفها او تغييرها او حجب الخدمة ن وأيضا قدرة مصدر التهديد على النجاح في استغلال أحد نقاط الضعف الخاصة بنظام معلومات معينة (الهيئة الوطنية ،٢٠١٨، ص٣٤).

ثانيا: جرائم الانترنيت Internet Crimes :

إن من أهم جرائم الانترنيت هي جريمة الابتزاز الالكتروني ، وهي عملية تهديد وترهيب الطرف الأخر بنشر صور أو أفلام أو تسريب معلومات سرية ، مقابل دفع مبالغ مالية أو استغلال الضحية للقيام بأعمال غير مشروعة لصالح المبتزين لإعطاء معلومات سرية خاصة بجهة العمل أو غيرها من الأعمال غير القانونية ، وفي هذا السياق فان الابتزاز هو محاولة الحصول على مكاسب مادية أو معنوية عن طريق الإكراه المعنوي ، وبهذه الصورة فان الابتزاز يمتد ليشمل جميع القطاعات وبمسميات متعددة منها ما يسمى الابتزاز السياسي والابتزاز العاطفي وغيرها (الياسري ،٢٠٢٢ ، ص٥٨).

وبفعل التقدم الكبير في تكنولوجيا المعلومات فان جريمة الابتزاز الالكترونية تعد من الجرائم المستحدثة، وهذه الجريمة لها من يملكون التقنيات الحديثة لتنفيذ جرائمهم باستخدام إمكانياتهم التكنولوجية الحديثة ضد ضحايا اغلبهم من النساء لابتزازهم مادياً او جنسياً، وقد يكون الابتزاز موجه للسلطة العامة عندما يقوم الجاني باحتجاز شخص كرهينة، وهذا الشخص قد يكون مسؤولا أو مستثمر أجنبي أو ممثلين دبلوماسيين أو سياح أو غيرهم مما قد يؤثر على سمعة إي دولة من الدول .

من هنا فان جريمة الابتزاز الالكترونية هي ذات بعدين:

الأول: البعد المعنوي حيث الخوف والرعب للمجني عليه من خطر يراد إيقاعه بشخصه أو ماله أو شخص أو مال شخص يهمه .

الثاني: البعد المادي، حيث يسعى القائمون على هذه الجريمة الحصول على الأموال بطريقة غير قانونية وشرعية .

إن نشر ثقافة الانترنيت حسب ما يرى بعض المختصين يتطلب من الجهات التي تمتلك الخبرة المعلوماتية المتقدمة ونظم امن المعلومات أن يعدوا العدة لمواجهة المخاطر المترتبة على المعلوماتية ويتعين تضافر الجهود بين شرائح وفئات المجتمع المختلفة وبالتعاون مع كل الجهات المعنية وبالأخص وزارة التربية والتعليم العالي، ويكون هدف ذلك التعاون نشر ثقافة الانترنيت بتوعية الأسرة سواء الآباء منهم أو الأمهات لحماية أبنائهم من المخاطر الكامنة في شبكة الانترنيت.

ولذا فان نشر ثقافة الانترنيت أو المعلوماتية تتطلب التركيز على :

١- تحذير الأبناء من إعطاء معلومات شخصية عن أنفسهم للأشخاص الذين يتم التعارف بينهم عن طريق الانترنيت .

٢- تحذير الأبناء من مخاطر تنظيم لقاء مع احد الأشخاص من معارف الانترنيت وجهاً لوجه دون استشارة الوالدين أولا.

٣- تعليم الأبناء عدم الرد على ما يتلقونه من رسائل الكترونية مريبة .

٤- إرساء قواعد واضحة تنظم استخدام الأبناء لشبكة الانترنيت .

٥- استخدام أنظمة حماية برامج تتيح للآباء معرفة المواقع التي زارها الأبناء عند انشغال أو غياب الوالدين أو تمنعهم تلقائيا من الدخول إلى المواقع المحظورة .

٦- وضع جهاز الكمبيوتر في مساحات مفتوحة كالمكتبات المدرسية .

٧- وجود الرقابة للوالدين لمراقبة أفراد الأسرة .

ولتحقيق سلامة جميع مؤسسات الدولة وسلامة المجتمع العراقي والحد من جرائم الانترنيت وبما يعزز الأمن السيبراني ، لابد من تحقيق ما يسمى بالأمن المادي Physical Security والذي يتضمن التدابير الأمنية التي تم تصميمها لمنع الوصول غير المصرح إلى المرفق والمعدات والموارد التابعة للجهة المعنية ، وحماية الأفراد والممتلكات من التلف أو الضرر (مثل التجسس ، السرقة والهجمات الإرهابية) وينطوي الأمن المادي على استخدام طبقات متعددة من نظم مترابطة تشمل الدوائر التلفزيونية المغلقة CCTU ، حراس الأمن ، حدود أمنية ، الاقفال وأنظمة التحكم في الوصول والعديد من التقنيات الأخرى .

ولأن جريمة الابتزاز الالكتروني تعد من الجرائم الخطرة فقد أشار المشرع العراقي لهذه الجريمة والتي اسماها جريمة التهديد في المواد ٤٣٠ ، ٤٣١ و ٤٣٢ من قانون العقوبات العراقية المرقم ١١١ لسنة ١٩٦٩ ، حيث نصت المادة ٤٣٠ الفقرة الأولى ، يعاقب بالسجن لمدة لا تزيد على ٧ سنوات أو بالحبس كل من هدد أخر بارتكاب جناية ضد نفسه أو ماله أو ضد نفس أو مال غيره أو بإسناد أمور مخدشة بالشرف أو إفشائها وكان ذلك مصحوبا بطلب أو بتكليف بأمر أو الامتناع عن فعل مقصودا به ، وفي الفقرة الثانية يعاقب بالعقوبة ذاتها إذا كان التهديد في خطاب خال من اسم مرسلة أو كان منسوباً صدوره إلى جماعة سرية موجودة أو مزعومة .

وأشارت المادة ٤٣١ إلى انه يعاقب بالحبس كل من هدد أخر بارتكاب جناية ضد نفسه أو ماله أو ضد نفس أو مال غيره بإسناد أمور خادشه للشرف أو الاعتبار أو إفشائها بغير الحالات المبينة في المادة ٤٣٠ .

كما أشارت المادة ٤٣٢ كل من هدد أخر بالقول أو بالفعل أو بالإشارة كتابة أو شفاهاً أو بواسطة شخص أخر في غير الحالات المبينة في المادتين ٤٣٠ و٤٣١ يعاقب بالحبس مدة لا تزيد على سنة واحدة أو بغرامة .

في ضوء ذلك يمكن القول انه لا بد من إصدار قانون يخص الجرائم المعلوماتية وان يسعى إلى :

١- حماية المجتمع والأفراد من الجرائم الالكترونية.

٢- مكافحة الجريمة الالكترونية والتي تشكل تهديداً لأمن الدولة وسلامتها .

٣- زيادة الوعي العام بمخاطر الجريمة الالكترونية .

٤- تطوير قدرات العاملين على تطبيق القانون وتقديم الدعم التقني للسلطة القضائية لمواكبة أخر التطورات الحاصلة في مجال الجرائم المعلوماتية .

ثالثا: أهمية الأمن السيبرانيThe Importance Of Cyber Security

الأمن السيبراني هو مجموعة من الإجراءات والتقنيات التي تُستعمل لحماية الأنظمة الإلكترونية، مثل أجهزة الكمبيوتر والهواتف الذكية والشبكات والبيانات، من الهجمات أو الوصول غير المصرح به أو التلف أو السرقة .بمعنى أخر هو حماية كل ما هو متصل بالإنترنت من المخاطر الالكترونية.

ظهر الأمن السيبراني كمفهوم مع بداية استعمال الحواسيب والشبكات، لكن يمكن تحديد مراحل تطوره بدايات العام ١٩٧٠عندما بدأ الحديث عن حماية المعلومات مع ظهور أول الفيروسات التجريبية، مثل فيروس Creeper في شبكة ARPANETالتي كانت نواة الإنترنتت، بمعنى أخر لم يكن هناك شيء يُسمى الأمن السيبراني في عقد السبعينيات من القرن العشرين (الماضي).

في بداية الثمانينيات بدأ استعمال مصطلح أمن المعلومات وظهرت أولى برامج مكافحة الفيروسات، وفي العام ١٩٨٦ صدر أول قانون أمريكي لمكافحة جرائم الحاسوب .

وفي التسعينيات من القرن العشرين (الماضي) زادت الهجمات الالكترونية بتأثير انتشار الانترنيت، وبدأ يظهر مصطلح الأمن السيبراني لحماية الشبكات والبيانات المتصلة بالأنترنيت .

ومع بديات العام ٢٠٠٠ من القرن الحالي تطور الأمن السيبراني ليشمل حماية الهواتف الذكية، الأجهزة الذكية، منصات التواصل وحتى البنى التحتية للدول، وأصبح يحتل مساحة واسعة من الاهتمام نظريا ومهنيا وعمليا.

في ضوء ذلك يمكن التساؤل أين تكمن أهمية الأمن السيبراني؟ وما علاقته بالمجتمع وتحديدا الأسرة والأبناء؟

بالنسبة للآسرة فان الأمن السيبراني يشمل:

- حماية الأجهزة المنزلية من الفيروسات والاختراق .
- متابعة نشاط الأبناء على الانترنيت .
- ضبط إعدادات الأمان والخصوصية في التطبيقات والألعاب .
- توعية جميع أفراد الأسرة بالاستخدام الأمن للتقنية .

كما يؤدي الأمن السيبراني أثراً فعّالاً في حماية الأبناء من مخاطر الانترنيت أو المخاطر الالكترونية مثل :

- المحتوى غير المناسب.
- التنمر الالكتروني.
- محاولات الاختراق أو سرقة المعلومات.
- الاستدراج من الغرباء

ولمنع مثل تلك الاختراقات فان أهم الإجراءات التي يتبعها الأمن السيبراني لحماية الأنظمة والمعلومات، تشمل الآتية:

١- استعمال كلمات مرور قوية Use Strong Passwords تتكون من حروف وأرقام ورموز ويتم تغيرها بانتظام.

٢- تفعيل التحقيق بخطوتين Two Factor Authenticatiionوذلك بإضافة طبقة أمان إضافية للدخول إلى الحسابات .

٣- تحديث البرامج والنظامSoftware and System Update باستمرار لسد الثغرات التي قد يستغلها المخترقون.

٤- تثبيت برامج الحماية Firewall and Antivirus لرصد الفيروسات والهجمات ومنعها.

٥- النسخ الاحتياطي للبياناتData Backup لحمايتها من الفقد او الهجمات مثل فيروسات الفدية.

٦- عدم فتح الروابط أو الملفات المشبوهة Suspicious Files وخاصة التي تتصل عبر البريد الالكتروني أو الرسائل.

٧- تشفير البياناتData Encryption لتحصينها من السرقة أثناء الإرسال أو التخزين.

٨- توعية المستخدمين User Awarenessبتعليمهم كيفية استخدام الانترنيت.

رابعاً: أنواع المخاطر السيبرانية وتهديداتها Types Of Cyder Risks And Threats :

وهي العملية التي يمكن اعتمادها لمنع الآثار المترتبة على الأحداث وتقليلها التي قد تعطل سير العمل لضمان عدم تكرار حدوثها مستقبلا، وتوفير الموارد اللازمة لذلك، ووفقاً للمخطط (١) يبدو أن هذه الإدارة ترتبط ارتباطا مباشرا بالأمن السيبراني وبالتالي فان اعتمادها يعني الحد من جرائم الانترنيت (الجرائم الالكترونية)، فإدارة المخاطر تعني:

- درء الخطر أو الوقاية من عواقبه والعمل على عدم تكراره .
- الحماية من الآثار السلبية للمخاطر.
- الاستفادة من الفرص المتاحة.
- إضافة أقصى قيمة مستدامة ممكنة

ولضمان استمرارية الأمن السيبراني وقدرته وفاعليته في مكافحة جرائم الانترنيت ومنها الجرائم المعلوماتية، فان عملية إدارة المخاطر ووفقاً للمخطط (٢) يجب أن تنطلق من مبدأ تحديد المخاطر ثم تحليلها، تقيمها، معالجتها ثم المتابعة.

وان طبيعة العلاقة بين جرائم الانترنيت والأمن السيبراني تكشف محورين هامين من مخاطر الأمن السيبراني وهما:

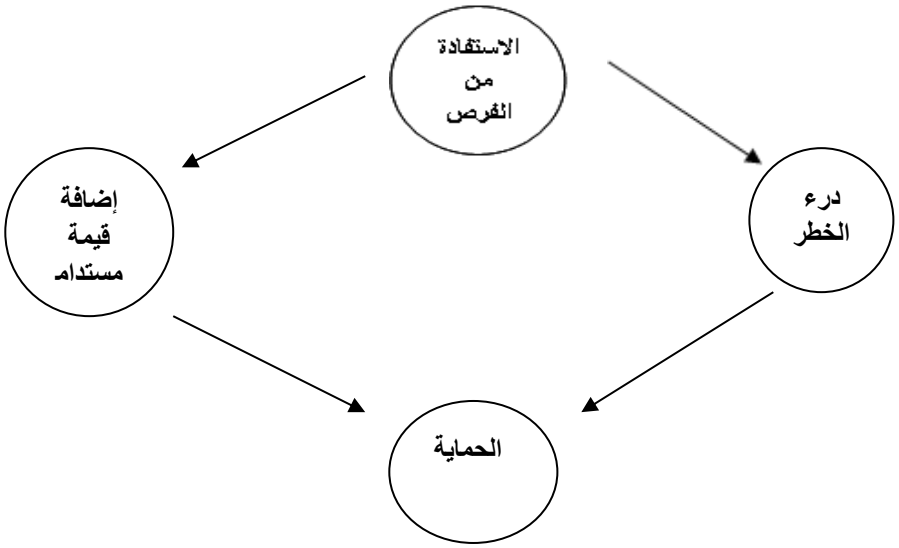
الأول : مجموعة مخاطر مرتبطة بالأداء.

الثاني: مجموعة المخاطر الأمنية .

ولذا فان تجاوز سلبيات هذين المحورين يعني إمكانية الحد من جرائم الانترنيت ومنها الجرائم المعلوماتية ، ويبين المخطط (٣) إن تلك المخاطر يمكن حدوثها في المستقبل ولربما تحدث أو لا تحدث وفي حالة حدوثها سيكون لها تأثيران احدهما ايجابي والأخر سلبي ، ويمكن توظيف ذلك ومعالجة ما يحدث من سلبيات وبما يعزز الأمن السيبراني ليكون قادرا وفاعلا في معالجة جميع المشكلات التي يسببها الانترنيت والتي هي جزء لا يتجزأ من الهجوم السيبراني Cyber-Attcck حيث الاستغلال المتعمد لأنظمة الحاسب الآلي والشبكات والجهات التي يعتمد عملها على تقنية المعلومات والاتصالات الرقمية بهدف إحداث أضرار فيها .

مخطط (١)

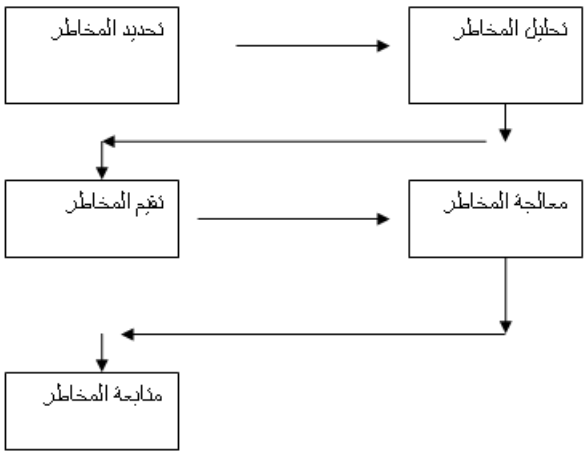
الهدف من إدارة المخاطر



الباحث بالاعتماد على المحتوى .

مخطط (٢)

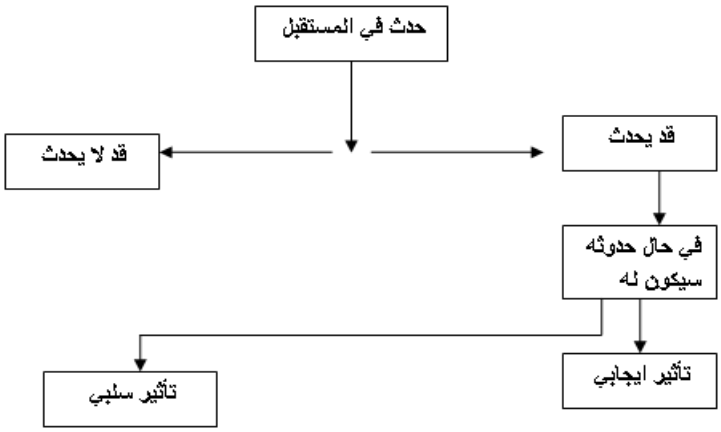
عملية إدارة المخاطر



المصدر: الباحث بالاعتماد على المحتوى .

مخطط (٣)

المخاطرة



المصدر: الباحث بالاعتماد على المحتوى .

هذا ما أكدت عليه الإستراتيجية الوطنية للأمن السيبراني في العراق لتوفير تدابير متماسكة وقوية وبما يتوافق وواقع الحال لمعالجة جميع العقبات التي تقف عائق في ما يسعى إليه الأمن السيبراني، اخذين بنظر الاعتبار إن أهم ما تؤكد عليه تلك الإستراتيجية هي

ضمان امن وحماية الوجود العراقي في الفضاء السيبراني، وحماية البنية التحتية الحيوية للمعلومات وبناء ورعاية انترنيت موثوق به .

إن إستراتيجية الأمن السيبراني الوطنية لدفع مخاطر الاختراق وجرائم الانترنيت وتعزيز تلك الإستراتيجية تتألف من خطط قصير، متوسطة وطويلة الأمد وجميعها تغطي الأولويات الوطنية وتعالج التعرض الوطني للمخاطر السيبرانية، وهناك العديد من التهديدات السيبرانية في جميع العالم تضر بالمصلحة الوطنية منها، الجريمة الالكترونية، الإرهاب الالكتروني، الصراع السيبراني، التجسس السيبراني وإساءة معاملة الأطفال واستغلالهم عبر الانترنيت. وهذه التهديدات لها القدرة على الأضرار بسلامة الدولة والمجتمع، وتعطل عمليات البنية التحتية الحيوية للمعلومات وتقويضها والعمليات الحكومية والأمن القومي .

في ضوء ذلك بات من الضروري تعزيز تلك الإستراتيجية بشكل منسق تستجيب بشكل ديناميكي نحو التهديدات التي تواجه الأمن القومي ومنها مخاطر الانترنيت، وبالتالي خلق رؤية وطنية للأمن السيبراني بما يتطابق وواقع الحال تتجه نحو مجتمع امن ومضمون ومرن وموثوق به وقادر على درء مخاطر الانترنيت وبما يحقق فرصاً لسكانه ويحمي المصالح الوطنية ويعزز التفاعلات السلمية والمشاركة الاستباقية في الفضاء السيبراني من اجل الرخاء الوطني .

جدير بالإشارة إلى أن الرؤية الوطنية تهدف إلى تعزيز القدرات في مجال الأمن السيبراني في العراق على نحو متناسق ومستدام ومتكامل من اجل التصدي والتخفيف من المخاطر السيبرانية في الفضاء السيبراني والتقليل من حدته ، وذلك يتطلب تعاوناً دوليا لتحقيق ما يأتي : (مستشارية الأمن القومي ، ٢٠١٩ ،ص٩)

١- تشجيع المشاركة الفعالة في جميع هيئات الأمن السيبراني الدولية ذات الصلة.

٢- تعزيز المشاركة الفعلية في جميع الفعاليات والمؤتمرات والمنتديات المتعلقة بالأمن السيبراني .

٣- تعزيز الموقع الاستراتيجي للعراق في مجال الأمن السيبراني باستضافة المؤتمرات الدولية والدورية .

٤- التواصل مع منصة الاتصالات العالمية ITU والعمل على تحديث الملف المتعلق بالوعي الأمني السيبراني العراقي.

٥- العمل على تكوين شراكة واتفاقيات بين فريق الاستجابة الالكتروني العراقي CERT وفرق الاستجابة الالكترونية الدولية الأخرى لأجل تطوير الفريق وتوسعة افقه ..

الاستنتاجات والمقترحات conclusions and Suggestions

أولا: الاستنتاجاتconclusions

١- مهما حاولت الدول ومنها العراق التحكم في المادة المعلوماتية التي تبث عبر الانترنيت، وفي ظل انعدام الرقابة المركزية على شبكة الانترنيت، فان ذلك لا يمنع من تسلل بعض مستعملي الانترنيت لتحقيق أغراضهم اللاأخلاقية والدنيئة.

٢- توجد العديد من المواقع التي لها دوافع سياسية أو اقتصادية أو اجتماعية تهدف إلى زرع الفوضى وبؤر الجريمة، سيما وان العديد من الحالات السلبية مثل اكتساب المعلومات التي تتعلق بمحاولة اختراق الشبكات المعلوماتية ترتبط بمراكز إستراتيجية في دول كبرى متقدمة .

٣- إن انعدام الرقابة على الانترنيت تؤدي إلى أثار اقل ما توصف أنها خطيرة ومدمرة، ولذا تحاول جميع الدول ومنها العراق ان تمنع تسرب المواقع المحظورة إلى شبكاتها المحلية بوسائل متقدمة، ومع ذلك فان الجريمة المعلوماتية تتقدم بصورة أسرع من سبل الحماية والوقاية .

٤-تعد الجريمة الالكترونية واحدة من أهم المظاهر الاجتماعية نظرا لانعكاسات السلبية على التنمية البشرية والنسيج الاجتماعي، مما يسبب ضعف الروابط الاجتماعية وتأثيرها في كافة الجوانب الاقتصادية والاجتماعية والأمنية .

٥-يعد الأمن السيبراني في ضوء التقدم التكنولوجي ضرورة حتمية لحماية البيانات والمعلومات من التهديدات الالكترونية التي تزداد يوما بعد يوم، سيما وان أحد التهديدات السيبرانية هو احتمال وجود محاولات لائتلاف أو تعطيل شبكة الكمبيوتر ونظام المعلومات الضعيفة التحصين .

٦- إن أبعاد تأثير التهديدات السيبرانية تكون متنوعة وهي تنطوي على مصادر التهديد الذي يقوم قبل الهجوم باستغلال ظروف وقوع حادث أو خرق أمنى معين وعادة فان مصدر التهديد يبدأ من خلال الرغبة في الاختراق والوصول إلى المعلومات الهامة أو الضوابط الأمنية بهدف الاستفادة من الخرق وعلى سبيل المثال لتحقيق مكاسب مالية .

ثانيا: المقترحات Suggestions

١- متابعة ومراقبة ومعالجة حالات الجرائم الالكترونية قبل حدوثها وهذا يتطلب دورا فاعلا من قبل الجهات الرسمية والمختصة لأي دولة من الدول.

٢- تفعيل كل القوانين التي تحد من الجريمة بكل أنواعها وجرائم الانترنيت في الخصوص والاستمرارية بالتوعية المجتمعية وتفعيل ما يسمى بالأمن السيبراني.

٣- وضع الرقابة على المواقع المحظورة التي تشكل خطراً مجتمعياً.

٤- مشاركة الأسرة والمؤسسات التربوية ومنظمات المجتمع المدني بوضع خطط علمية ووقائية للحد من الاختراق المحتملة وعلى مستوى الحاسوب الشخصي.

٥- إعداد خطة علمية منهجية لمواجهة تقنية الانترنيت او محاولة تكيفيها سلوكياً.

٦- على المجتمع والأسرة والفرد جعل شبكة الانترنيت ذات وجه ايجابية تقدم ما هو ذا فائدة حياتية مجتمعية.

قائمة المصادر:List Of Sources :

١- جابر، حيدر عباس، الجريمة المعلوماتية وآثارها في الأمن الوطني العراقي، رسالة ماجستير، كلية العلوم السياسية، جامعة النهرين، بغداد، ٢٠٢٠.

٢- جابر، عوض سيد وعبد الموجود أبو الحسن، الانحراف والجريمة في عالم متغير، سلسلة كتب مجالات الخدمة الاجتماعية ، القاهرة ، مصر ، ٢٠٠٤ .

٣- الهيئة الوطنية للأمن السيبراني، الضوابط الأساسية للأمن السيبراني ، عمان ، الأردن ، ٢٠١٨ .

٤-حجازي، عبد الفتاح بيومي ، الأحداث والانترنيت / دراسة معمقة على أثر الانترنيت، دار الفكر الجامعي، الإسكندرية، ٢٠٠٤ .

٥- الحيالي ، عبد الحميد، حقوق كل من الجهة الأمنية أو الفرد المتضرر، المركز العراقي لدعم حرية التعبير، المجلة الفصلية، العدد (٥)، بغداد، ٢٠٢١.

٦-الطيار، حسين بن سليمان بن راشد، الأمن السيبراني في منظور مقاصد الشارع، دراسة تاصيلية ، المملكة العربية السعودية، جامعة الطائف، مجلة الطائف للعلوم الإنسانية، المجلد ٦، العدد ٢١، ٢٠٢٠.

٧-الياسري، علاء نور حميد، تحليل جغرافي لواقع الجريمة الالكترونية في العراق باستخدام نظم المعلومات الجغرافية GIS ، أطروحة دكتوراه (غير منشورة) ، كلية الآداب، جامعة ذي قار، ٢٠٢٢.

٨- مستشارية الأمن الوطني، إستراتيجية الأمن السيبراني العراقي، أمانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات، بغداد ، ٢٠١٩ .

٩- عبيد، هشام، الآليات الدولية لمكافحة الجريمة الالكترونية، المركز الدولي للدراسات الإستراتيجية والاستخبارية، العدد (١٠)، المجلة الفصلية، بغداد، ٢٠٢٢.

١٠- السعدون، فهد خليف، الجرائم المعلوماتية – دراسة مقارنة، مجلة جامعة الأنبار للعلوم القانونية والسياسية، كلية القانون، جامعة الأنبار، العدد الثاني، السنة العاشرة، ٢٠١٩.

١١- عبد القادر، هيثم، الجرائم السبرانية – مفاهيم ونظريات، مجلة الأمن القومي العربي، العدد الرابع، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ٢٠٢٠.