مركز البيان للدراسات والتخطيط
Al-Bayan Center for Planning and Studies

# الأمن المعلوماتي السيبراني

المهندس: أوس مجيد غالب العوادي

سلسلة إصدارات مركز البيان للدراسات والتخطيط

## عن المركز

مركزُ البيان للدرأسات والتخطيط مركز مستقلٌ، غيرُ ربحيّ، مقرّه الرئيس في بغداد. مهمته الرئيسة، فضلاً عن قضايا أخرى، تقديم وجهة نظر ذات مصداقية حول قضايا السياسات العامة والخارجية التي تخصّ العراق بنحوٍ خاصٍ ومنطقة الشرق الأوسط بنحوٍ عام. ويسعى إلى إجراء تحليل مستقلّ، وإيجاد حلول عمليّة جليّة لقضايا معقدة تهمّ الحقليْن السياسي والأكاديمي.

**آب/ اغسطس ٢٠١٦**



**www.bayancenter.org**
**info@bayancenter.org**

# الأمن المعلوماتي السيبراني (cyber security)

المهندس: أوس مجيد غالب العوادي *

**مقدمة:**

إن الانفتاح الذي شهده العراق في تكنولوجيا المعلومات والاتصالات في ظل التطور التكنولوجي العالمي المتنامي بعد سقوط النظام البائد الذي تزامن مع عدم وجود بنية تحتية متكاملة ومؤمنة لأنظمة المعلومات سواء أكانت أمنية أم مصرفية أم شخصية أدى إلى أن يكون العراق ساحة مفتوحة لكثير من دول العالم أو دول الجوار الإقليمي؛ لاختراقه والتجسس على المعلومات الخاصة بالمؤسسات الأمنية العراقية واستخدام العراق كساحة لشن الهجمات الإلكترونية لضرب أمن معلومات أي دولة كانت واختراقه، فضلاً عن استراق أي معلومة واستخدامها لأغراض المساومة، أي: لتنفيذ عمليات إرهابية وإسنادها، ومن الملاحظ أن أكثر المؤسسات العراقية تتعاقد لتجهيز معلوماتها من أقمار صناعية ذات مورد خدمة واقع خارج الحدود العراقية الذي يؤدي إلى مرور تلك المعلومات في خوادم تلك الدول، ورجوعها إلى العراق إذ يشكل هذا الإجراء خرقاً لأمن المعلومات العراقي، ولتلافي مثل هذه الخروقات الكبيرة التي تتعرض لها حركة المعلومات في العراق يتوجب بناء منظومة متكاملة لأمن المعلومات.

إن الوعي المتزايد بأهمية المعرفة المتكاملة بالمخاطر التي تخص جرائم المعلوماتية التي تصاحب كل عملية تطور جديد، أو إنتاج أجيال جديدة من التقنيات يسهم بدوره بتحول المجتمع الى مجتمع معلوماتي؛ ليزيد من اعتماد المؤسسات والبلدان والأفراد على أنظمة المعلومات والاتصالات، وهذا يعدُّ مصدراً من مصادر الخطر الرئيس، وعليه يجب مراعاة الجانب الامني والتركيز عليه في كل عملية تطور تكنلوجية، وينبغي للدولة تصميم البنية التحتية الخاصة بها وإدارتها بما يتوافق والمرتكزات الخاصة بأمن المعلومات والاتصالات. إن هذه الإدارة تمكن من خلق خدمات أخرى وتوليدها مثل (الحكومة الإلكترونية، والتعليم الإلكتروني، والصحة الإلكترونية).

* مهندس اتصالات ومعلومات – هيئة الاعلام والاتصالات

لا يخفى على الجميع أن أنظمة تكنولوجيا المعلومات هي أنظمة مترابطة شبكيا عن بُعد، ويمكن الوصول إليها نتيجة هذا الترابط؛ وبالتالي فإن احتمال تعرضها لهجمات سيبرانية أو اختراقها يكون وارداً ويمكن لهذا الاختراق الهجمات أن ينال من القدرة على المعالجة والتخزين وسرقة الرصيد المعلوماتي أو نسخه، وإلحاق الضرر بالسلع غير الملموسة والرمزية، فضلاً عن إلحاق الضرر بعملية صنع القرار لدى أي منظمة، ومن الملاحظ أن الدول ذات التنمية البشرية والاقتصادية القليلة تمتلك أمناً سيبرانياً عاليَ المستوى مثل: إرتيريا، والسودان، والأردن، ولبنان، وعُمان، وسواها من الدول الأخرى.

وسأقوم في هذا البحث بتوضيح مفهوم أمن المعلومات السيبراني على وفق التعريفات الدولية وأهمية هذا الموضوع من النواحي الأمنية، والاقتصادية، والمجتمعية، وحتى السياسية وأبعاد الأمن السيبراني، وأهم التحديات التي يمثلها، وسأبيّن أيضاً أنواع الجريمة السيبرانية، ووسائل سرقة المعلومات، وسأتطرق كذلك إلى الاختراق والفيروسات، وفي ختام البحث سأعرض استراتيجية عامة مقترحة للأمن المعلوماتي العراقي تتوافق والنهج العالمي المتبع والتوصيات والمقررات الدولية.

**لمحة تأريخية مختصرة:**

سأتطرق الى أهم المراحل التي ابتدأت منها جرائم المعلوماتية التي أدت الى ضرورة التفكير الجدي بوجود منظومة للأمن المعلوماتي لمعالجة هذه الجرائم والاختراقات:

بظهور استخدام الكمبيوتر وربطه بالشبكة في الستينيات إلى السبعينييات من القرن الماضي، ظهرت المعالجة الأولى لجرائم الكمبيوتر في شكل مقالات صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والتجسس المعلوماتي، وشكل هذا الموضوع التساؤل فيما إذا كانت هذه الجرائم مجرد حالة عابرة أو ظاهرة جرمية مستجدة، وهل هي جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في مجال المعلوماتية، فبقيت محصورة في إطار السلوك اللا أخلاقي دون النطاق القانوني ومع توسع الدراسات تدريجياً وخلال السبعينيات بدأ الحديث عنها كظاهرة جديدة.

وفي الثمانينيات ظهر نوع جديد من الجرائم السيبرانية ارتبط بعمليات اقتحام نظم الحاسوب عن بُعد، ونشر الفيروسات عبر شبكات الكمبيوتر الذي سبب تدمير الملفات والبرامج، حينها شاع اصطلاح (الهاكرز) المعبر عن مقتحمي النظم، وبقي الحديث دائماً عن دوافع هذه الجرائم محصوراً

في اختراق أمن المعلومات وإظهار التفوق التقني من قبل مرتكبي هذه الأفعال الذين لم يتعدوا فئة صغار السن العباقرة في هذا المجال، لكن بتزايد خطورة هذه الممارسات أصبح من الضروري إعادة تصنيف الفاعلين وتحديد طوائفهم ولاسيما بعد تحول الجريمة من مجرد مغامرة إلى أفعال تستهدف التجسس والاستيلاء على البيانات الاقتصادية والاجتماعية والسياسية والعسكرية.

شهدت فترة التسعينيات تطوراً هائلاً في مجال الجرائم التقنية وتغيُّراً في نطاقها ومفهومها؛ بفعل ما أحدثته شبكة الإنترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكات المعلومات حينما أصبحت مواقع الإنترنت التسويقية النشطة أكثر عرضة للهجمات التي ظهرت بسببها أنماط جديدة من الجرائم، مثل تعطيل النظام التقني ومنعه من القيام بعمله المعتاد الذي يتسبب بانقطاع النظام عن الخدمة لساعات، فتنتج عنه خسائر مالية بالملايين، وقد توسعت جرائم نشر الفيروسات عبر شبكة الإنترنت؛ لما تسهله من وصول إلى ملايين المستخدمين في الوقت نفسه، ليفتح الباب على مصراعيه لمختلف الأفعال غير السوية المتطورة بتطور التقنية، وقد سُجِّلَت عبر هذه المراحل مجموعةٌ من القضايا، منها: قضية (موريس الشهيرة) سنة ١٩٨٨ حينما تم نشر فيروس إلكتروني عُرِفَ بـ:(دودة موريس) عبر آلاف الكمبيوترات بوساطة الإنترنت، وفي عام ١٩٩٥ شهدت الأجهزة هجوماً عرف باسم (IP-SPOOFING) أدى إلى إيقاف عمل أجهزة أصلية وتشغيل أخرى وهمية، لتبرز قضية (الجحيم العالمي) التي اختص بها مكتب التحقيقات الفدرالية مكنتها من اختراق موقع البيت الأبيض الأمريكي، ومن ثم تلتها الكثير من الحوادث كحادثة شركة أوميغا، وفيروس مليسا، وغيرها من جرائم المعلوماتية المتعلقة بالأمن السيبراني.

أما في مرحلة ما بعد التسعينيات بعد عام ٢٠٠٠ فقد تطورت هذه الجرائم بنحوٍ أوسع، وتم استخدام المعلومات في الإرهاب المنظم من خلال ضرب البنى التحتية للدول سواء أكانت مرافق عامةً أم خدمات أم البنى العسكرية والاقتصادية المتمثلة بالبنوك، وغيرها.

# الفصل الأول

## تعريف الأمن السيبراني

يُعرَّف الأمن السيبراني على النحو المحدد في التوصية الاتحاد الدولي للاتصالات (ITU-T X.1205) بأنه: مجموعة الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية والمبادئ التوجيهية وتُهُج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وسبل الضمان والتكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرانية والمنظمة وأصول المستعملين. وتشمل المنظمة وأصول المستعملين تجهيزات الحواسيب الموصولة، والموظفين، والبنية التحتية، والتطبيقات، والخدمات، وأنظمة الاتصالات، والحصيلة الكلية للمعلومات المرسلة و/أو المخزنة في البيئة السيبرانية. ومن شأن خدمات الأمن السيبراني كفالة تحقيق والحفاظ على الخواص الأمنية للمنظمات وأصول المستعملين إزاء المخاطر الأمنية ذات الصلة في البيئة السيبرانية.

### التحديات التي يمثلها الأمن المعلوماتي:

بما أن المعلومات الرقمية تعدُّ اليوم ثروة ترتبط بثقافة الناس وتوجاهتهم الاجتماعية والسياسية والثقافية وترتبط ارتباطاً وثيقاً بسياسية الدول الاقتصادية والمنظومات الدولية فإن القضايا الاجتماعية والاقتصادية والسياسات العامة والاجتماعية والقضايا الإنسانية كافة تمثل تحدياً مهماً يواجه أمن المعلومات حيث تشكل تلك التحديات خطراً كبيراً ومعقداً ويحتاج التصدي له إلى وجود إرادة سياسية متماسكة وقرار جريء؛ لتصميم استراتيجية تطوير البنى التحتية للخدمات الرقمية، وتنفيذ استراتيجية قوية ومتماسكة وفعالة مع وجود حلول على المستويات الثقافية والقانونية والإدارية والتقنية كافة؛ وهذا بدوره ينعكس إيجاباً على المجتمع أجمع، ويسهم في زيادة النمو الاقتصادي المرغوب فيه.

لحماية أمن المعلومات وتضييق الفجوة الإلكترونية أمام الاختراقات يستلزم الآتي:

- بنى تحتية موثوقة وآمنة.
- سياسات لخلق الثقة.
- إطار قانوني مناسب.

- إدارة الأدوات الأمنية للمعلومات وإدارة المخاطر.
- إدارة أمنية قادرة على خلق الثقة في التطبيقات والاستخدامات المقدمة.
- فريق متخصص قادر على إدارة كل ما ورد في أعلاه ومدرب تدريباً عالياً، وذو معلومات محدثة وعلى اتصال مع فرق مشابهة في بقية بلدان العالم.

**ثانيا: أهمية الأمن المعلوماتي:**

إن أهم الأسباب التي دعت إلى ضرورة وجود مفهوم أمن المعلومات والدعوة إلى إيجاد الأطر التشريعية والقانونية والتنظيمية بما يتناسب والتحديات التي يواجهها المجتمع أو المنظمات أو الأفراد تتلخص فيما يأتي:

– الحاجة إلى الارتباط بنظم الاتصالات والإنترنيت وعدم إمكانية عزل الأجهزة عن الشبكات المحلية والشبكات واسعة النطاق لتوفير المعلومات لمن يحتاجها.

– اعتماد مختلف المؤسسات على فعالية المعلومات التي تزداد بازدياد التطورات التكنلوجية وبازدياد المتطلبات الخاصة بتلك المؤسسات.

– صعوبة تحدي الأخطار والتحكم بها أو متابعة المجرمين ومعاقبتهم؛ لعدم توافر الحدود الجغرافية حين استخدام الإنترينت والاتصالات الإلكترونية؛ لأنها تتيح الفرصة لاختراق الحدود المكانية.

– النمو المطّرد في الاستخدمات والتطبيقات الإلكترونية وظهور التجارة الإلكترونية والتسوق الشبكي والحكومة الإلكترونية والإدارة الإلكترونية التي تحتاج إلى بيئة معلوماتية آمنة.

**أبعاد الأمن المعلوماتي:**

**البعد السياسي:**

تقع على عاتق الدولة مسؤولية كبيرة لتحقيق الأمن الرقمي وذلك من خلال تعريف الإطار القانوني المناسب حيث لا يمكن الاقتصار على عملية البحث والتطوير للمؤسسات التعليمة فقط،

بل يجب تعزيز الثقافة الأمنية واعتبار الأمن المعلوماتي جزءاً لا يتجزأ من الخدمات التي تقدمها الدولة للمواطن فضلاً عن تقوية تطبيق الإجراءات القانونية التي تتعلق بجرائم المعلوماتية.

فعلى المستوى الاستراتيجي يجب تأمين الرقابة العامة، وتقاسم المعلومات بين المؤسسات المعنية، والإنذار وزيادة الوعي بأفضل الممارسات في مجال الأمن السيبراني، ويجب مراعاة التوافق بين القوانين التي تصدرها السلطة التشريعية التي تنظم قطاع الاتصالات والمعلومات وتحديد الجهات المسؤولة عن أمن المعلومات وإدامة المورد البشري، فضلاً عن صياغة التعليمات والأنظمة الخاصة بالأمن المعلوماتي وتشريعها وتحديثها.

إن عملية التثقيف التي تتبعها الدولة أو المؤسسات القطاعية التابعة لها لا ينبغي أن يقتصر دورها على إصدار مدونة سلوك أو تشجيع الثقافة الأمنية، بل يجب أن يتعدى ذلك إلى أن تكون تلك الثقافة ممارسَة على الأقل في مؤسسات الدولة، ومن ثم المنظمات والأفراد، ويجب أيضاً تشجيع ثقافة الإبلاغ عن تلك الجرائم.

إن الثقة بين الأطراف والمنظمات السياسية والفرقاء في المجال المالي والاقتصادي والسياسي والقانوني لها دور كبير في تطور الأمن المعلوماتي و إدامته، حيث إن الاستجابة على المستوى السياسي والاقتصادي والقانوني والتكنلوجي التي يعتمدها الفرقاء –المحتمل تضررهم من تلك الجرائم– يسهم في احتواء الجريمة السيبرانية والحد منها.

**البعد الاقتصادي:**

ليست الغاية من الأمن المعلوماتي كسب المال وإنما حماية الموارد الاقتصادية وتفادي خسارتها أو فقدانها، إن تقدير الربح الحاصل من أمن المعلومات غير متيسّر، وإن تقدير تكلفة الأمن التي تتمثل بالميزانات المرصودة، وتكلفة نواتج الأمن والتدريب، وبناء مراكز السيطرة، وغيرها من الأمور المتعلقة أمر ضروي إذْ إن حساب تكاليف أمن المعلومات والخسائر الناتجة عن الأخطاء والأعمال الخبيثة أمر صعب جداً؛ لأن احتياجات المؤسسة هي التي تحدد تلك التكاليف وهي التي تعتمد على الموجودات التي يراد حمايتها والأضرار الناجمة عن عدم كفاية الأمن واحتمال التعرض لهجمات أو اختراقات، حيث لا يمكن تحديد المخاطر التي تتعرض لها المؤسسة او الدولة وتقييمها، ولا يمكن أيضاً تحديد القيمة الاقتصادية للأمن المعلوماتي والمردودات المالية الناجمة عنه؛ و يقتضي التنويه

إلى أن القيمة الاقتصادية للأمن المعلوماتي يجب أن تفهم من باب اجتماعي واسع مع مراعاة تأثير التكنولوجيات الجديدة على الأفراد والمؤسسات والدول.

**البعد الاجتماعي:**

من المهم جداً أنْ يفهم المجتمع ولاسيما الأفراد الذين يستخدمون تكنولوجيا المعلومات والاتصالات أهمية الأمن المعلوماتي وكيفية اتخاذ الإجراءات والتدابير اللازمة للوقاية من الهجمات والاختراقات الإلكترونية وهذا يُلزم الجهات المعنية أن تقوم بحملات إعلامية وتثقيفية لخلق مجتمع معلوماتي مثقف أمنياً؛ إذْ يجب أن تشملَ تلك الإعلانات والحملات التثقيفية تدابير الأمن والوقاية وكيفية التعاطي مع جرائم المعلوماتية، ويجب بيان المخاطر المحتملة والمسؤولية الفردية التي تقع على عاتق الأفراد في التبليغ عن تلك الجرائم، ومن الضروري أيضاً التعريف بالتداعيات والمخاطر المحتملة عن تلك الهجمات؛ وبالنتيجة يستطيع كل الأفراد المستفيدون من شبكة المعلومات التمتع بالخدمات التي تتيحيها شبكات المعلومات والاستفادة من البنى التحتية والخدمات التي توفرها تلك الأسطح البينية دون تحمل مخاطر أمنية ناتجة عن جرائم المعلوماتية.

**البعد القانوني:**

من المفترض –منطقياً– وجود قاعدة تشريعية تشتمل على قوانين وأنظمة وتعليمات تخص التدابير الأمنية تمكن المعنين والمسؤولين عن أمن المعلومات اتخاذ الإجراءات والتدابير اللازمة والضرورية في حال تم انتهاك تلك التشريعات أو خرقها، إذْ يتحمل المذنبون المسؤولية الأمنية والجنائية؛ نتيجة لمخالفتهم أو محالوتهم انتهاك الأمن المعلوماتي لدولة معينة.

إن سن التشريعات الملائمة يشجع المستثمرين و الشركاء الاقتصاديين على الاستثمار كونه يعزز الثقة لديهم بإنشاء بنية تحتية سليمة وموثوقة خالية من الاختراقات، لأن الأمن المعلوماتي القائم على أساس الثقة والجودة يضع الأسس الصحيحة والسليمة لاقتصاد خدمات سليم.

إن الجدير بالملاحظة هو أن المتابع للإحصاءات الصادرة عن معهد أمن الحاسوب (CSI) أو الناتجة عن الفريق المعني بطوارئ الحاسوب والاستجابة لها (CERT) يجد أن التدابير الأمنية المتخدة حاليا غير فعالة بصورة كافية، وهي عاجزة في بعض الأحيان عن منع النشاط الإجرامي لجرائم المعلوماتية وذلك للأسباب الآتية:

١. طبيعة جرائم المعلوماتية التي تعتمد على البرامجيات المضرة (الخبيثة) والتحكم عن بعد.

٢. إمكانية المتسلل من انتحال شخصية المستخدمين الشرعيين وبذلك يكون القانون عاجزاً عن تحديد هوية مرتكب العمل الإجرامي.

٣. نقص الموارد البشرية والمادية داخل الخدمات المسؤولة عن مكافحة جرائم المعلوماتية.

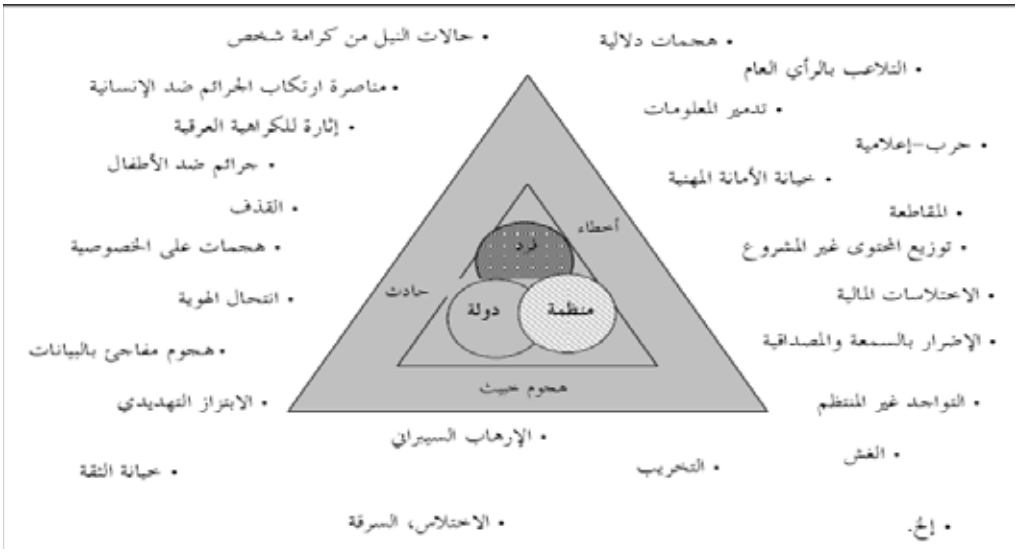
٤. الطبيعية غير الوطنية للجريمة المعلوماتية التي يصعب في ظلها اتخاذ إجراءات إلَّا في حال وجود تعاون قضائي دولي أو اتفاقيات ومعاهدات تلتزم بها الدول.

٥. التعريف غير الكافي والطبيعة المؤقتة لمعظم القرائن التي تتصل بتكنولوجيا المعلومات والاتصالات.

## الفصل الثاني

## جرائم المعلوماتية

تتكوّن الجريمة المعلوماتية أو الجرائم السيبرانية افتراضياً من مقطعين (Cyber Crime) الجريمة (Crime) والإلكترونية (Cyber) ويُستخدم المقطع الأخير لوصف فكرة من عصر المعلوماتية، فالجرائم الإلكترونية تعرّف قانونيا بأنها: ''المخالفات التي ترتكب ضد الأفراد أو المجموعات بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أي أذى مادي أو نفسي للضحية مباشر أو غير مباشر باستخدام شبكات الاتصالات و المعلوماتية''، وتُعدُّ الجريمة الإلكترونية ظاهرة اجتماعية متوافقة مع انتقال المجتمعات إلى المجتمع الرقمي حيث ينتقل فيها نشاط الناس من الواقع الفعلي المادي إلى الواقع الافتراضي، وتعدُّ جريمةً عابرةً للحدود الوطنية وتنماز بسهولتها وانخفاض تكاليفها والسرعة في تنفيذها وتوظيف الاتصالات في ارتكابها، فضلاً عن قلة الخطورة على الجناة وسرعة الكسب غير المشروع والفرص المتاحة لارتكابها وضعف الرقابة، ومن أهم العوامل التي ساهمت على انتشارها هي ضعف التشريعات، وضعف أدوات الحماية، وتوافر الفرصة لارتكابها، وغياب الحراسة والتقنية في انتشارها، وتنفيذها من قبل شباب يسعون للشهرة أو مجرمين محترفين يسعون للكسب والثراء.



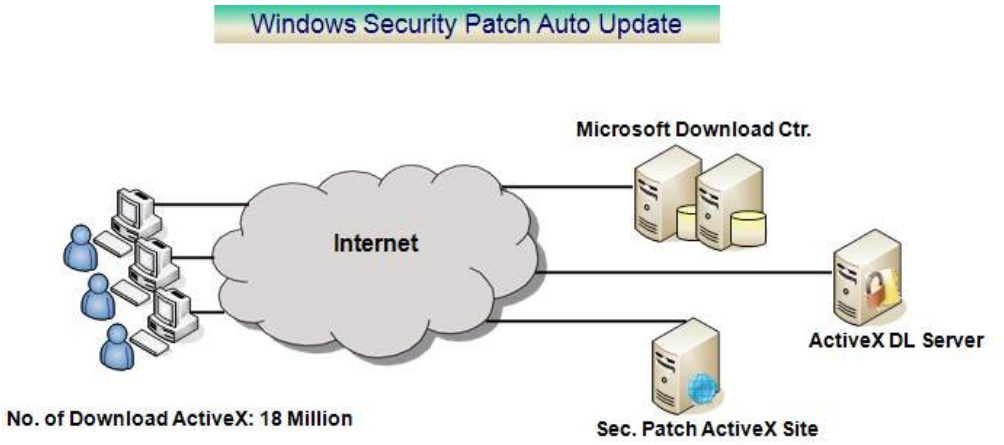

الشكل في أعلاه يوضح مخاطر جرائم المعلومات الشائعة.

## أنواع جرائم المعلوماتية:

### الجريمة ذات الصلة بالحاسوب:

إن الثغرات ونقاط التعرض في التكنولوجيا الرقمية تجتمع معاً لتحقيق بيئة من عدم الأمن، ومن الطبيعي أن يستغل المجرمون هذه الحالة وليست الشبكة الدولية للمعلومات (الإنترنيت) مستثنية من ذلك والدليل كثرة الجرائم الخاصة بالفضاء السيبراني؛ ولذلك حدَّتْ منظمةُ التعاون والتنمية في المجال الاقتصادي أنّ الجرائمَ ذات الصلة بالحاسوب بأنها: «أي سلوك غير مشروع وغير أخلاقي أو غير مرخص به ويشمل الإرسال ومعالجة المعلومات».

إن الجريمة ذات الصلة بالحاسوب يكون فيها النظام الحاسوبي هو الهدف، ووسيلة ارتكاب الجريمة في الوقت نفسه ويغطي هذا النوع جميع الجرائم التي تتعلق بشبكة الإنترنيت والفضاء السيبراني.




### ٢.جرائم غسيل الأموال والجرائم الاقتصادية:

إن التطوير المستمر والسريع لتكنولوجيا المعلومات والاتصالات يسمح للأفراد بالدخول في جرائم غسيل الأموال والجرائم الاقتصادية سواءٌ أكان العمل بمفردهم أمْ كان على مستوى منظمات، يسهم الإنترنيت في حيازته على أكبر كمٍّ من المعلومات الذي يمكن أيضا الحصول على أكبر كمٍّ من الضحايا الذين يقعون بيد الهاكرز (المخترقين)، إذْ من الممكن للتكنولوجيا الجديدة تسهيل جميع أنواع السرقات والتلاعب والتخريب والاحتيال والابتزاز والتهديد وغيرها من الأساليب التي تنضوي عليها جرائم المعلوماتية، ويعمد المجرمون في قطاع المعلومات على استخدام هويات زائفة لتفادي الملاحقة القضائية أو المسؤولية الجنائية أو الإرهابية من خلال انتحال هوية أشخاص آخرين.

يستخدم غاسلو الأموال الإنترنيت بزيادةٍ متصاعدة؛ للحصول على الأموال التي يتم توليدها بوساطة الأنشطة الإجرامية مثل التهريب، والتهرُّب الضريبي، والرشوة، وغير ذلك من الأنشطة الأخرى، وأن عمليات المقامرة و التجارة عبر شبكة الإنترنيت والعمليات المصرفية والعقارية، واستخدام الشركات كواجهات، والنقد الإلكتروني كلها عمليات غير مشروعة ومن الصعب رصدها.

### ٣.الجرائم الإرهابية السيبرانية:

حينما تكون الأنظمة المستهدفة جزءاً مهماً من البنية التحتية الحرجة والحساسة تكتسب الجريمة السيبرانية بعداً إرهابياً فـ(الطاقة، والمياه، والأغذية، والاتصالات، والخدمات المالية والمصرفية، والخدمات الطبية، وغيرها) كلها بنى تحتية حرجة وتشكل أساساً يمس حياة المواطنين بصورة مباشرة

و تمس كل أمن الدولة الاقتصادي والمجتمعي.

يعمد الإرهابيون إلى استهداف هذه البنى الحساسة والسيطرة عليها إلكترونيا عن بعد أو تخريبها من خلال البحث عن نقاط التعرّض والثغرات عبر شبكات الاتصال أو الإنترنيت أو الشبكات الداخلية لتلك الأنظمة والتسلل إليها.

إن الهجوم من النوع المتصل بالحاسوب لا يمكن استخدامه لبيان دوافع المهاجمين أو أهدافهم بأي قدر من اليقين وهذه إحدى المصاعب في مواجهة الجريمة السيبرانية إذْ يحتاج الاختصاصيون إلى مزيد من المعلومات؛ لتحديد قصد أبعاد الهجمات من خلال الفضاء عبر شبكات الإنترنيت أو الاتصالات التي تُعرَف بالهجوم عبر الفضاء السيبراني، وسواء أكان الإرهاب السيبراني يتم من طريق عملية زعزعة الأوضاع الاقتصادية أمْ تهديد البنية التحتية الحرجة أمْ لنشر أيديلوجية معينة أمْ التلاعب بالمعلومات فإنه ينطوي على تهديد جديد يجب أن يؤخذ بمنتهى الجدية لأنه يمكن أن يعرض حياة الناس وأمنهم إلى خطر كبير.

**٤ .جرائم متنوعة (عمليات مخادعة، أنشطة تجسس، التخابر، الابتزاز، التهديد والإيذاء):**

إن الأشكال الشائعة للجريمة المنظمة يمكنها أن تستفيد من تكنولوجيا المعلومات والاتصالات حيث إن شبكات الاتصال والإنترنيت تنماز بتيسرها للوصول والاتصال وتساعد المشغلين على أي نوع من التهريب، فضلاً عن عمليات النصب (الهجمات على الملكية، وأنظمة الحاسوب، والبنية التحتية، وسرقة البيانات، وسرقة حقوق النشر والتأليف، وسوى ذلك من الاحتيالات).

يستخدم المجرمون الإنترنيت بعدة طرق فبعظهم ينتحل هوية شخص آخر كي يقوم بالشراء على حساب الضحية وهذا يحصل –غالباً– في الاحتيال من طريق بطاقات الائتمان وتتحمل بموجبه الجهة التي تم الاحتيال عليها (النظام المصرفي أو التاجر) الكلفة المالية، وهناك طريقة أخرى في النصب تتمثل ببيع الألبومات أو جواز السفر لدول غير موجودة أصلاً، فضلاً عن منتجات غير موجودة.

إن شبكة الإنترنيت تسهل التجسس والتخابر فهي تيسّر الاعتراض غير المشروع للمعلومات التي تم تناقلها على الإنترنيت حيث يُعدُّ الانترنيت وسطاً قوياً يساعد على نشر طرق ارتكاب جرائم المعلومات والأفعال المنافية للقانون.

### ٥.الجرائم ضد الأشخاص:

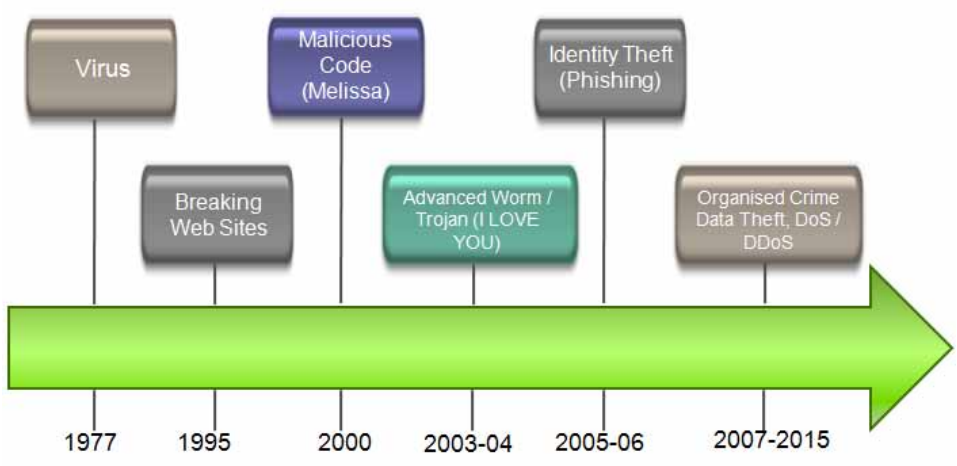
يخلق الإنترنيت إمكانية نشوء مجموعات أو أفراد يمارسون قضايا يعاقب عليها القانون قد تشمل تلك القضايا مواد خادشة للحياء أو أفلام عنف تحتوي على مشاهد حقيقة تتضمن تعذيباً لضحايا حقيقين حتى الموت وتعرف هذه الأفلام بأفلام سنف (snuff moves)، إذ من الممكن في بعض الأحيان تقاسم افلام الضحايا وصورهم حيث تنتشر خوادم الإنترنيت في بلدان تضعف فيها الرقابة، ويغيب عنها القانون، وتشمل هذه الجرائم مخالفات تمس سرية الشخص وصورته، والسرية المهنية، وحقوق سرية البيانات، وجرائم أخرى تتمثل برسائل خادشة يمكن أن يراها القاصرون.

### ٦.القرصنة:

تتمثل بالنسخ غير القانوني للمعلومات وتؤدي هذه الجريمة إلى خسارة بلايين من الدورلات سنوياً، وتكون على شكل خسائر صانعي البرمجيات والموسيقى وأفلام الفيديو، وقد لوحظ وجود زيادة كبيرة في عدد الأعمال العلمية والبحوث والدراسات والوثائق التي تم سرقتها بسبب وجودها على الإنترنيت وهناك عدد كبير من مخالفات الملكية الفكرية كتزيف أعمال المؤلف، وتصميم النماذج، والعلامات التجارية، وغيرها.

### ٧.التلاعب بالمعلومات

إن التلاعب بالمعلومات له أشكال متعددة منها تسريب الوثائق؛ لزعزعة استقرار شركة ما، وإرسال الطلبات بالرسائل الإلكترونية؛ للحصول على تبرعات خيرية عبر مواقع زائفة، ويُعَدُّ الإنترنيت أرضاً خصبةً جداً لشائعات المعلومات المضللة وهو يسهل عملية ارتكاب المخالفات ضد قانون وسائل الإعلام، والتحريض الجنائي، والدفاع عن الجرائم ضد الإنسانية، ومناصرة الإرهاب والتحريض عليه، وزرع العداء العرقي والطائفي والإهانات وغيرها من الأمور المختلفة.




شكل يمثل مراحل تطور الهجمات السيبرانية.

## الفصل الثالث

## وسائل سرقة المعلومات

تتعدد وسائل سرقة المعلومات فهناك عدة طرق وإمكانيات تتيحها تكنولوجيا الإنترنيت وهي في أغلب الاحيان تقوم على الخداع واستغلال نقاط التعرض والثغرات في التكنولوجيا، ومن أبرزهذه الطرق التنصت، وسرقة معلومات هوية شخص، معيّن أو منشأة معينة، واستخدام الفايروسات للدخول للمنظومات الإلكترونية والحاسبات، والحصول على مخرجات النظام بطرق غير مشروعة، والاختراق وغيرها من الأمور، وفيما يأتي شرح مختصر لما تم ذكره آنفا:

### ١. التنصت:

يعد التنصت من أقدم طرق سرقة المعلومات في الحاسبات حيث يحتوي على حزم البيانات أثناء مرورها أو تدفقها أو نسخها.

### ٢. سرقة معلومات هوية شخص معين:

تهدف هذ الطريقة إلى الحصول على معلومات سرية أو أمنية او الحصول على مبالغ

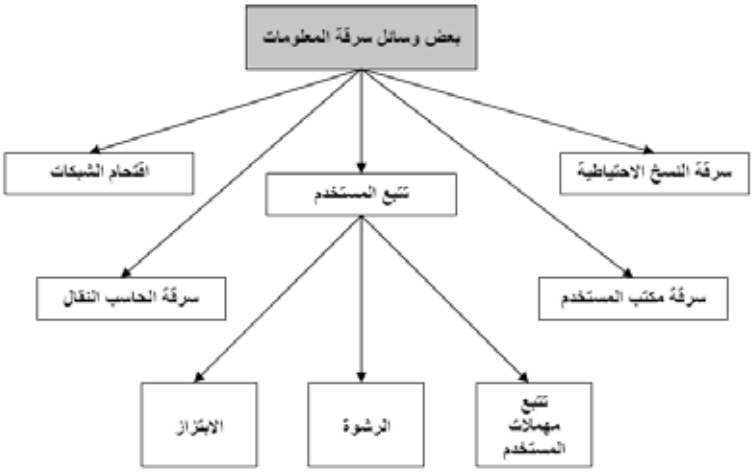
نقدية أو الدخول على قواعد البيانات منشأة معينة.

### ٣. استخدام الفيروسات للدخول غير المشروع إلى الحاسبات:

تنماز الفيروسات بمقدرتها على تغيير عمل الجهاز وأدائه دون علم صاحبه؛ وتنقسم على قسمين، الأول: يكون حميداً لا يدمر البرمجيات الخاصة بالحاسوب وممكن أن يحتل مساحة من الذاكرة ويظهر عبر رسالة في وقت محدد له أو يعطي إشارة بأن الذاكرة ممتلئة، والآخر خبيث يسعى إلى تدمير النظام والملفات، ويساعد كلا النوعين على سرقة البيانات بطريقة غير مشروعة.

### ٤. الحصول على مخرجات النظام بطرق غير مشروعة:

يتضمن ذلك سرقة وسائط التخزين ونسخها أو إرسالها خلال البريد الإلكتروني إما بتواطؤ أشخاص من المنظمة وإما من خلال المؤسسة المراد سرقة بياناتها وإما بالدخول غير المشروع إلى غرفة النظام.




**رسم توضيحي يمثل وسائل سرقة المعلومات**

**أنواع الهجمات السيبرانية:**

١- سرقة كلمات مرور المستخدمين للوصول إلى المعلومات وتتضمن:

- التخمين: وحينها تكون كلمة المرور باسم الزوجة أو الطفل أو نوع العمل ويسهل على المخترق تخمينها وتكون غير مؤمنة.
- الخداع الاجتماعي: حيث يظهر المخترق بمظهر المسؤول ويطلب كلمة المرور.
- الاستماع إلى حركة المرور (التجسس): حيث يستمع المخترق إلى بيانات غير محفزة مرسلة إلى الشبكة عبر بوتوكولات الاتصال.
- البرمجيات: وذلك من خلال تسريب حصان طروادة -مثلاً- الذي يقوم بدوره بتسريب المعلومات إلى حاسبة المهاجم.
- النفاذ إلى ملف تخزين كلمة المرور.
- السطو على كلمات المرور المرسلة بشكل محفز.
- التجسس عن طريق معرفة معلومات الاتصال.

٢- هجمات رفض أداء الخدمة: تتم من خلال رفض الخدمة من طريق تحميل النظام فوق طاقته حيث إن تزويد النظام ببيانات تفوق طاقته يؤدي إلى تصدع النظام بالكامل.

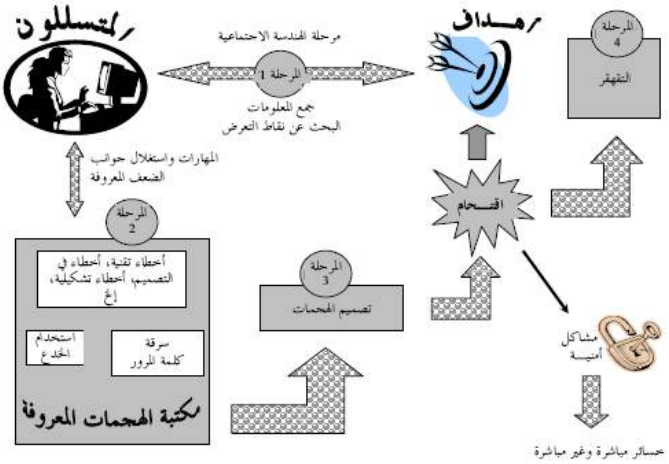
٣- الهجمات الطمسية: وتتمثل باستهداف صفحات الويب واستبدالها بصفحات أخرى، إذْ يقوم المهاجم بخلق موقع شبكي مماثل للموقع الأصلي؛ لاصطياد المشتركين واستدارجهم لمعرفة معلوماتهم أو بطاقات الائتمان الخاصة بهم، وغيرها.

٤- الهجمات الخداعية: تتم من خلال استخدام بوتوكالات النقل والتحكم (TCP/IP) في اختراق أمن النظام أثناء عمل العميل والخادم حيث يعمل البروتوكول أعلاه على تأمين وصلة ربط آمنة بين أي عميلين من خلال أرقام المنافذ ومحددات الهوية المنطقية حيث يقوم المهاجم بتخمين أرقام المنافذ التي تخص تبادل البيانات؛ وبالتالي يحل محل المستخدم القانوني ويخترق جميع

الجدران الواقية للوصول إلى قواعد البيانات للضحية ويستغل المتسللون البروتوكولات بما يأتي:

- شل الشبكات.
- إعادة توجيه البيانات نحو مقصد زائف.
- تحميل الأنظمة فوق طاقاتها من خلال غمرها برسائل متعددة.
- لمنع مرسل من إرسال بياناته.

٥- الهجمات على البنية التحتية الحرجة: ويتم ذلك من خلال الهجوم على البنية التحتية وما تحوية من شبكات كهرباء، وأنظمة صرف صحي، ومستشفيات وأنظمة التحكم الأمني، وغير ذلك.




رسم توضيحي يمثل مراحل الهجمات السيبرانية

**الاختراق:**

تفتقد كثير من المؤسسات إلى الوعي الأمني السيبراني وبالنتيجة لا تمتلك تلك المؤسسات على -مختلف توجهاها- منظومات أو برامج أو تقنيات تجنبها الاختراق السيبراني فتكون عرضة

لسرقة معلوماتها وبيانتها، أو إلحاق الضرر المادي في بناها التحتية، أو تهديد أمنها، وسأقوم فيما يأتي بشرح تفصيلي عن أهداف الاختراق وأساليبه ودوافعه والوقاية منه.

**أولاً: أهداف الاختراق وأساليبه:**

**الهدف من الاختراق:**

إن الهدف من الاحتراق هو الحصول على بيانات أو معلومات خاصة عن مؤسسة معينة أو فرد معيّن حيث يعمد المخترق إلى التعرف على الخدمات الخاصة بشبكة المواطن ومواطن الضعف والخلل في الأجهزة الملحقة كالحاسبات أو الهواتف النقالة الخاصة بالمواطن من خلال بوابات المعلومات والعبور الخاصة بالشبكة المحلية.

**دوافع الاختراق:**

أ- الدافع السياسي والعسكري:

إن الحروب المستمرة والتطورات السياسية والعسكرية المتزامنة مع التطورات التي شهدها قطاع الاتصالات والمعلوماتية في ظل الاحتياج المستمر والمتزايد لتكلنولوجيا الاتصالات والمعلومات لتلبية المتطلبات العسكرية للدول المتقدمة دعت إلى الاعتماد على هذه التكنولوجيا بصورة مفصلية، إذ أصبح موضوع التجسس و استراق المعلومات من طريق الاختراق يمثل ضرورة عسكرية بين الدول المتقدمة.

ب- الدافع التجاري:

نتيجة للمنافسة التجارية الكبيرة الحاصلة بين الشركات العالمية أصبحت عملية الاختراق مهمة لكثير من تلك الشركات؛ لغرض الاطلاع على معلومات الشركات المتنافسة لتحقيق أرباح تجارية فضلاً عن محاولة الدول ضرب اقتصاديات الدول الأخرى من خلال الاطلاع على معلومات تخص تلك الاقتصاديات وآليات نموها لغرض الحد منها.

ت- الدافع الفردي:

إن محاولات الاختراق على المستوى الفردي تبدأ بين الأفراد؛ بداعي التباهي بالنجاح في

اختراق أجهزة زملائهم الآخرين بدافع التحدي، لكنَّ هذه الحالة تحولت فيما بعد إلى هواية عند بعض الأفراد، إذْ شكل بعضهم منتديات لتعليم الاختراق، وقد ظهرت هذه المشكلة جلية بعد إقالة المبرمجين من بعض الشركات المعروفة الذين صبوا جام غضبهم على تلك الشركات لغرض النيل والثأر من شركاتهم التي أقالتهم.

### ٣- أنواع الاختراق:

يمكن تقسيم الاختراق على ثلاثة أنواع مهمة كما يأتي:

أ- اختراق الخوادم والأجهزة الرئيسة للشركات والمؤسسات أو الجهات الحكومية وذلك من طريق اختراق الجدار الناري للخوادم بعملية تدعى المحاكاة والتي تعني انتحال شخصية للدخول إلى النظام إذ إن عنوان الـ (IP) يحوي على عناوين المرسِل والمرسَل إليه وهذه العناوين تشكل مادة أساسية وثغرة كبيرة للمخترقين.

ب- اختراق الأجهزة الشخصية واستراق ما تحوية من معلومات، و تعدُّ هذه الطريقة شائعة جداً من قبل الهواة والمحترفين.

ت- التعرض للبيانات أثناء انتقالها والتعرف على شفرتها في حال كونها مشفرة، وهذه الطريقة شائعة لدى المحترفين الذين يحاولون سرقة أرقام بطاقات الائتمان البنكية وكشف الأرقام السرية لها.

### آلية الاختراق:

ذكرنا مسبقا أن الهجمات الإلكترونية التي تتم عبر الإنترنيت أو الفضاء السيبراني تنماز بسهولتها لأنَّ تلك الهجمات تتم عن بُعد، وأن عملية الاختراق لا تتم إلّا بوجود عاملين أساسيين، الأول هو البرنامج المسيطر، والآخر الخادم الذي يقوم بتسهيل عملية الاختراق.

حيث يكون الأول في جهاز المخترق والثاني في جهاز الضحية، ومن الجدير بالذكر أن طرق الاختراق تختلف وتتعدد وتتطور بتطور التقنيات، ولكن يبقى العنصر الأساس هو ضرورة وجود اتصال بين جهاز المخترق و جهاز الضحية، وأن ابرز اليات الاختراق تتم من طريق ما يأتي:

**١- أحصنة طروادة:**

و هو عبارة عن (Patch file) يتم إرسالة من قبل الشخص المخترق إلى الضحية ويزرع بعد استلامه في جهاز الضحية، ومهمته الأساسية البقاء صامتاً إلى حين التفعيل من قبل المخترق حيث يسيطر المخترق من خلال هذا الملف سيطرة تامة على جهاز الضحية ويقوم هذا الملف بتغيير اسمه بعد يوم أو يومين من دخوله إلى جهاز الضحية ومن الملاحظ أن حصان طروادة لا يعدُّ فايروساً وإنما يعدُّ ملفاً تجسسياً لكن تعاملة بعض المضادات كفايروس.

وتتم عملية إرسال حصان طروادة من خلال البريد الإلكتروني أو من خلال برنامج الـ(ICQ)، ويمكن إعادة تكوينه من طريق المايكرو الموجود ببرامج معالجة النصوص ويتم تفعيله بعد أن يعمد الضحية إلى فتح الروابط أو البرامج المرسلة، فيجد أنها لا تعمل وتعدُّ هذه العملية الخطوة الأولى للاختراق؛ ذلك لأن البرنامج يفتح بوابة اتصال بين جهاز الضحية وجهاز المخترق تُمكِّن الأخير من تحديث معلوماته والبدء بعملية الاختراق.

**٢- الـ (IP address):**

حين اتصال أي شخص بالإنترينت يكون الشخص المعني معرضاً إلى كشف كثيرٍ من المعلومات الخاصة به كعنوان الجهاز، وعنوان مزود الخدمة الخاص بالشخص، وتسجيل التحركات على الشبكة، وتوجد كثيرٌ من المواقع التي يزورها الشخص التي تفتح سجلاً خاصاً يتضمن عنوان الموقع، ونوع الكمبيوتر، والمتصفح المستخدم، وحتى نوع المعالج وسرعته ومواصفاته، وغيرها من التفاصيل، حيث يكون عنوان الـ(IP) كرقم الهوية الخاص بكل من يستخدم الإنتريت، ويتمكن المحترف من الولوج إلى الجهاز بعد معرفته للمعلومات الخاصة بالـ(IP) الخاص بالضحية، ويتمكن من السيطرة فقط في حال وجود اتصال بشبكة الإنترنيت لكن هذا الخيار لا يخدم المخترق؛ لأنَّ الخادم الخاص بمزود الخدمة يقوم بتغيير عنوان المشترك تلقائياً عند كل عملية دخول إلى الشبكة.

**٣- الـ (Cookies):**

هو عبارة عن ملفات صغيرة تضعه بعض المواقع التي يزورها المستخدم على القرص الصلب، ويتمكن هذا الملف من جمع بعض المعلومات والبيانات عن الجهاز وعدد المرات التي زار المستخدم فيها الموقع وتخزينها، وتسريع عملية نقل البيانات بين جهاز المستخدم والموقع؛ فالهدف الأولي من

هذا البرنامج تجاري، ولكنه يساء استخدامه من قبل المخترقين المحترفين.

**أساليب الاختراق:**

أ- يعمد المخترق إلى السيطرة على أبواب جدارن الحماية من خلال تحييد دور برامج الجدارن النارية.

ب- مهاجمة خدمات الملفات العامة للحصول على المعلومات التي تخص الشبكة.

ت- السعي للحصول على المعلومة من خلال طرق غير هجومية كالدخول كمستخدم طبيعي ثم يحاول المخترق الحصول على المعلومات التي تمكنه من الولوج بصورة مباشرة إلى الشبكة والاتصال بالخوادم الرئيسة لها وتعد هذه الطريقة من أنجع الوسائل؛ لأنها لا تثير الشكوك حول طبيعة الشخص المخترق من قبل مسؤولي أمن الشبكات، وهي تمكن المخترق من الحصول على المعلومات بأسرع وقت ممكن.

يحصل الاختراق من طريق الروابط المستخدمة من قبل مستخدمي الشبكة لأن تطبيقات الإنترنيت تحوي على اسم صاحب الحساب الخاص بدلاً من الاسم العام، وتُستغَل هذه المعلومة للحصول على معلومات أكثر عن الخوادم في الشبكة لاستخدامها.

**أ- الوقاية من الاختراق**

إن من أهم أساليب الوقاية للحد من عمليات الاختراق الإلكترونية للمنشآت والمؤسسات والمنظومات الإلكترونية ما يأتي:

١. تطبيق إجراءات أمنية مشددة من قبل الأفراد والمؤسسات لتحديد أهم المسائل التي يجب أن تتخذ لمواجهة الاختراقات.

٢. تشكيل فرق خاصة لمكافحة الاختراقات.

٣. الاستعانة بالمكاتب الاستشارية أو المؤسسات أو الشركات المعنية المتخصصة بأمن المعلومات والاتصالات لاتخاذ الاجراءات الامنية الملائمة واللازمة لطبيعة عمل المؤسسة؛ بهدف دعم وسائل الحد من الاختراقات وحماية مراكز المعلومات بوسائل فعالة ومتطورة؛

وبذلك نضمن صعوبة الاختراق من قبل الآخرين.

٤. توعية العاملين وتثقيفهم سواء أكانوا على مستوى أفرادٍ أم مؤسسات بخطورة الاختراق وضرورة الحذر منه، ويجب تدريب العاملين في مراكز المعلومات الخاصة بالمؤسسات على كيفية اكتشاف الاختراقات وإيقافها، والحد من أخطارها والأضرار التي من الممكن أن تلحقها وأساليب التعرُّف على مرتكبيها، فضلاً عن تدريبهم على الإجراءات الواجب اتباعها للحفاظ على المعلومات.

٥. استخدام أحدث النسخ والإصدارات الخاصة بالمتصفحات لتجنب الثغرات الإلكترونية الموجودة في الإصدارات القديمة التي توفر بيئة خصبة للمخترقين.

٦. تحميل وتنصيب أحدث برامج الحماية الخاصة بأنظمة التشغيل لتدارك المشاكل والاختراقات ويجب مراعاة تحديث هذه البرامج دورياً لغرض كشف الثغرات أو الفايروسات التي تساعد على عملية الاختراق.

٧. التحكم في ملفات المشاركة المحلية بين الحاسبات و محاولة إزالتها؛ لأنها أكبر مصدر للتهديد الأمني حيث تسمح لأي شخص بالدخول إلى الجهاز الخاص بالمستخدم ومشاركة المعلومات الموجودة في ملفات المشاركة.

٨. استخدام كلمات مرور من عدة أحرف ورموز يصعب التنبؤ بها بهدف حماية الجهاز من عملية الاختراق أو الاستخدام إلا بعد كتابتها بنحوٍ صحيح، ويجب مراعاة وجود كلمة مرور تسمح للآخرين الاتصال بالجهاز حين الاتصال بالشبكات.

٩. تجنب تحميل برامج أو ملفات مجهولة المصدر أو غير موثوقة، ويجب فحص الأقراص وشرائح الذاكرة والتأكد من خلوها من الفيروسات قبل استخدامها.

**الفيروسات:**

تعدُّ الفيروسات من أخطر مهددات الأمن المعلوماتي السيبراني؛ لذا فإن مؤشر وجود فيروس يمثل جريمة سيبرانية من جرائم الحاسب ويتعرض من قام بهذه الجريمة للعقوبة والقانون النافذ في الدول التي شرعت قوانين تخص جرائم المعلوماتية، فالفيروسات تهدف إلى السيطرة على الجهاز

والإضرار بالنظام وسرقة المعلومات وتمكين المخترقين من الوصول إلى المعلومات بسهولة وإتلاف محتويات النظام كافة.

الفايروس من وجهة نظر برمجية هي عبارة عن برنامج أو تطبيق يتم تصميمه بوساطة أحد المبرمجين؛ لتحقيق هدف معين من الأهداف التي تمت الإشارة إليها آنفا؛ لذلك تتم برمجته ليكتسب القدرة على التدمير أو فتح ثغرات للوصول إلى المعلومات وسرقتها أو السيطرة على أنظمة معينة ومن الممكن للفيروس استنساخ نفسة عدة مرات، أو اعادة إنشاء نفسه والانتشار، أو ربط نفسة ببرامج أخرى ومن أهم أنواع الفيروسات تتمثل بالآتي:

١. الديدان:

فيروسات تنمتز بالقدرة على استنساخ نفسها من وإلى الأقراص المرنة، أو عبر الشبكات وهي تنقسم على نوعين:

- النوع الأول: يدعى بالدودة المضيفة التي تستخدم الشبكة لنسخ نفسها على أجهزة الحاسوب الآلي المتصلة بالشبكة.
- النوع الثاني: يدعى الدودة الشبكية التي توزع أجزاءَها على عدة أجهزة و تمتد على الشبكة بعد تشغيل هذه الأجزاء، ومن أهم أضرارها إبطاء سرعة الجهاز.

٢. القنابل الموقوتة:

عبارة عن برامج تنتقل إلى الحاسب الآلي، وهي ملتصقة ببريد إلكتروني أو بملف معيّن يتم تحميله، ويبدأ عمل هذه الفيروسات بعد وقت لاحق أو مدة زمنية محددة أو بعد حدث معيّن يتم تحديده من قبل المبرمج ومن أهم آثارها حذف البيانات وتعطيلها وتخريبها.

٣. فيروسات الشبكة:

تنتشر هذه الفيروسات من طريق البريد الإلكتروني ولاسيما الرسائل التي تأتي لاحقا.

٤. باب المصيدة:

هو رمز يتم توزيعه حين تركيب باب الحماية كي يعطي المخترق الحرية في اختيار الوقت المناسب لعملية التخريب حيث يسمح هذا الرمز بالنفاذ من خلال الشبكات في ظل وجود نظم حماية معينة.

٥. فيروسات العتاد:

يعمل هذا النوع من الفيروسات على توليد ملايين العمليات الحسابية وعمليات الإدخال والإخراج المتوالية التي تؤدي إلى ارتفاع كبير في درجة حرارة وحدة المعالج المركزي واحتراقها.

٦. الباتشيات:(Trojans):

عبارة عن برنامج صغير قد يكون مدمجاً مع ملف آخر للتخفي حينما يتم تنزيله وفتحه يصيب الـ Registry ويفتح منافذ؛ مما يجعل جهاز المستخدم قابلاً للاختراق بسهوله وهو يعدُّ من أذكى البرامج، فمثلاً حينما نعمل تفحص (scan) فهناك بعض التورجن يفك نفسه على هيئة ملفات غير محددة فيمر عليها التفحص دون التعرف عليه و من ثم يجمع نفسه مرة ثانية.

٧. فيروسات التشغيل:

تنشط هذه الفيروسات في منطقة نظام التشغيل وهي من أخطر أنواع الفيروسات حيث إنها يمنعك من تشغيل الجهاز.

٨. الفيروسات المخفية:

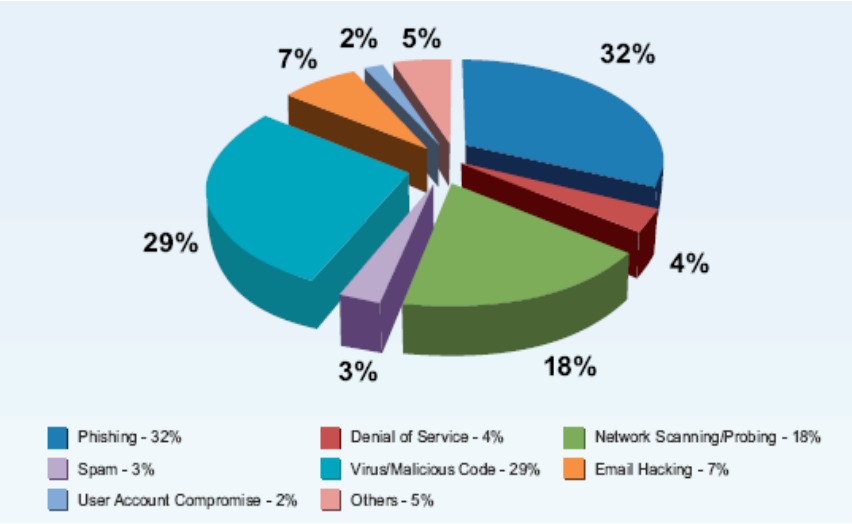
هي التي تحاول أن تختبئ من البرامج المضادة للفيروسات، وهي الفيروسات من السهولة كشفها والسيطرة عليها.

٩. الفيروسات المتحولة:

تتغير هذه الفيروسات من جهاز إلى آخر في أوامرها، التي تعد الأصعب على برامج كشف الفيروسات، وتكون مكتوبة بمستوى غير تقني فيسهل إزالتها بسرعة.

١٠. فيروسات الماكرو:

يشكل هذا النوع ضرراً كبيراً على برامج الأوفيس وهو فيروس يكتب بلغة الورد WORD ويصيب ملفات البيانات.




**مخطط بياني يوضح نسب الهجمات السيبرانية على مستوى العالم.**

**أهم أدوات الأمن المعلوماتي التي يجب اتباعها:**

**١- تقنيات تجفير البيانات:** تمكن هذه الأنظمة من الحفاظ على سرية المعلومات والتيقن من عدم كشفها وهي على نوعين:

- **تشفير تناظري:** وتيم بمفاتيح خاصة لأجل إزالة نص من النصوص، ويستخدم المشفر مفتاحاً في عمليتي فك وتشفير حيث يكون المرسل والمتلقي المفتاح تشفير الشفرة وفكها نفسه.
- **تشفير لا تناظري:** و يتم بمفاتيح عمومية، وبغض النظر عن نوع التشفير فهو يعتمد على قوة الخوارزمية التي تستخدم في تشفير المعلومة ويستخدم فيه زوج فريد من المفاتيح

ويشتمل على مفتاح عمومي ومفتاح خصوصي فيرسل المرسل بالمفتاح العمومي ويفك المستقبل بالمفتاح الخصوصي وينماز هذا التشفير برصانة عالية ويبلغ طول الشفرة ٢٠٤٨ بت.

**٢- بروتوكول إنترنت أمن.**

**٣- أمن التطبيقات:** يعني الحصول على النسخ الأصلية من النسخ البرمجية، ويتضمن تركيب نسخ جديدة من البروتوكولات المؤمنة.

**لحماية أمن المعلومات و تضييق الفجوة الإلكترونية أمام الاختراقات يستلزم الآتي:**

- بنى تحتية موثوقة وآمنة.
- سياسات لخلق الثقة.
- إطار قانوني مناسب.
- إدارة الأدوات الأمنية للمعلومات وإدارة المخاطر.
- إدارة أمنية قادرة على خلق الثقة في التطبيقات والاستخدامات المقدمة.
- فريق متخصص قادر على أدارة كل ما ورد في أعلاه ومدرب تدريباً عالياً وذو معلومات محدثة وعلى اتصال مع فرق مشابهة في بقية بلدان العالم.

# الفصل الرابع

## وضع استراتيجية وطنية مقترحة للأمن المعلوماتي (السيبراني) العراقي

**مقدمة:**

بعدما تم عرضه من توضيحات تخص خطورة الامن المعلوماتي وأهميته بصورة عامة ونظراً لعدم تبني مشروع وطني واضح المعالم يحدُّ من جرائم المعلوماتية، فضلاً عن عدم اكتمال القاعدة التشريعية المتمثلة بقانون الاتصالات والمعلوماتية العراقي حتى الوقت الحالي، اود أن اقترح استراتيجية وطنية للأمن السيبراني العراقي بما يتوافق والمنهج العالمي المتبع من قبل منظمات دولية مختصة مثل الاتحاد الدولي للاتصالات، ومؤسسات ودول اكتملت لديهم مثل هذه المشاريع حيث إن وجود خطة استراتيجة ونهج واضح يساعد صناع القرار على البدء بهذا المشروع الحيوي والمهم للدولة العراقية.

لذا يقتضي وضع خطة وطنية للأمن السيبراني وتنفيذها وجود استراتيجية شاملة تشمل استعراضاً عاماً أولياً لمدى كفاية الممارسات الوطنية الحالية والنظر في دور جميع أصحاب المصلحة (المؤسسات الحكومية، والقطاع الخاص، والمواطنين) في هذه العملية، ولأسباب تتعلق بالأمن القومي والرفاه الاقتصادي، تحتاج الحكومات –بصورة عامة– إلى المساعدة في عملية حماية البنية التحتية لمعلوماتها الحيوية، وتعزيز هذه الحماية وضمانها، فالبنية التحتية للمعلومات في عصرنا الحالي تشمل جميع قطاعات الصناعة في أي بلد، إذ إنها تتجاوز حدود البلدان، وإن شمولية البنية التحتية الحيوية للمعلومات تجعلها موجودة في كل مكان من شأنه أن يهيئ فرصاً ومزايا اقتصادية هائلة.

إن هذه المزايا تقترن أيضاً بكثيرٍ من حالات الاعتماد المتبادل والمخاطر المكلفة، وإن تكاليف جميع أصحاب المصلحة العاملين في خدمات المعلومات مثل بائعي البرمجيات ومشغلي الشبكات وموردي خدمات الإنترنت (ISPs) والمستعملين لها وإيراداتهم تتأثر بالبرمجيات الخبيثة والرسائل الاقتحامية، وتشمل هذه الآثار –على سبيل المثال لا الحصر– تكاليف التدابير الوقائية، وتكاليف العلاج، والتكاليف المباشرة لعرض النطاق والتجهيزات، وتكاليف فرص الازدحام. وعلى الرغم من أن البرامجيات الخبيثة ذات مضار كبيرة إلا أنها تولد تدفقات جديدة للدخل، بعضها شرعي وبعضها الآخر غير شرعي، حيث إنها تضفي الشرعية على نماذج للأعمال التجارية (مثل المنتجات المضادة للفيروسات والمضادة للرسائل الاقتحامية والبنية التحتية، وهي تفسح المجال أمام أعمال

إجرامية تجارية مثل (تأجير الشبكات الروبوتية، وتقاضي عمولات على المبيعات المتولدة عن الرسائل الاقتحامية، وخطط التلاعب بالأوراق المالية)؛ وبالتالي تؤدي هذه العوامل إلى حوافز مختلطة وأحياناً متعارضة لدى صانعي القرار تعمل على تعقيد التوصل إلى حلول جذرية متكاملة لهذه المشكلة.

إن التطور السريع والتغيُّرات التي أحدثتها تكنولوجيات المعلومات والاتصالات تحتاج إلى مزيدٍ من التركيز على التعاون المشترك لجميع الأطراف والشركاء سواءٌ أكانوا على المستوى المحلي أم الدولي، إن التواصل بين الحكومات في كثير من الأحيان والاضطلاع بدور قيادي في أمن الشبكات له أهمية حاسمة لضمان إشراك أصحاب المصلحة الآخرين المعنيين، ومنهم كذلك مشغلو البنية التحتية وموزّدوها، في عملية التخطيط ورسم السياسة بوجه عام، ومن خلال العمل المشترك بين الأطراف المعنية، يمكن لكل من الحكومة والقطاع الخاص أن يعززوا ويزيدوا من خبراتهم في إدارة المخاطر المتصلة بالبنية التحتية الحيوية للمعلومات، ومن شأن هذا الاندماج أن يضاعف من الثقة وأن يكفل تطوير السياسات والتكنولوجيات وتطبيقها بنحو ملائم وأكثر فعالية، ويسهم هذا الاندماج أيضاً بحماية البنية التحتية الحيوية للمعلومات وتعزيز الأمن السيبراني والتعاون والتنسيق بين الدول والشركاء على الساحة الدولية.

## أولا: الهدف من اقتراح الاستراتيجية الوطنية للأمن المعلوماتي

١. إقامة نظام وطني منسق للاستجابة لأمن الفضاء السيبراني لتلافي الحوادث السيبرانية وتتبعها وردعها والاستجابة لها والتعافي منها.

٢. إنشاء جهة تنسيق لإدارة الحوادث السيبرانية بحيث تضم هذه الجهة العناصر المهمة في الحكومة والعناصر الأساسية من مشغلي البنية التحتية والموردين بغية الحد من المخاطر.

٣. المشاركة في آليات مراقبة الحوادث والإنذار بوجودها والاستجابة لها وتقاسم المعلومات بشأنها.

٤. وضع الخطط والإجراءات والبروتوكولات بشأن الاستجابة لحالات الطوارئ، واختبارها، والتمرين عليها بما يكفل بناء الثقة بين المتعاونين من الجهات الحكومية وغير الحكومية وتعاونهم الفعال في وقت الأزمات.

**ثانيا : خطوات تحقيق الأهداف:**

يعد إنشاء قدرة وطنية لإدارة الحوادث مهمة طويلة الأجل تبدأ بإنشاء قدرة وطنية أو فريق وطني للاستجابة لحوادث الحاسوب (CIRT).

**١: تحديد أو إنشاء قدرات وطنية فرقة الـ(CIRT).**

أ- قد تؤدي المعالجة الفعالة والسريعة للحوادث السيبرانية الكبيرة إلى الحد من الأضرار التي تلحق بأنظمة المعلومات، فضلاً عن ضمان توافر وسائل فعالة للاستجابة وتقليل الوقت اللازم للانتعاش والحد من التكاليف، وهذا يكون بعد المواءمة والاشتراك بين القطاعين العام والخاص، إذ إن وجود فرقة استجابة لحوادث الأمن الحاسوبي المعينة وطنياً (CIRT) للعمل كجهة اتصال مع الحكومة أمر مهمٌ وضروري ولاسيما فيما يتعلق بالحوادث ذات الأهمية الوطنية حيث إن تنسيق الدفاع ضد الحوادث السيبرانية والتصدي لها والعمل مع سلطات إنفاذ القوانين له الأثر الفعّال في الحد من جرائم المعلوماتية.

ب- من الضروري أن تقوم فرقة الاستجابة لحوادث الأمن الحاسوبي (CIRT) بتوفير الخدمات والدعم؛ لتلافي القضايا ذات الصلة بالأمن السيبراني، والاستجابة لها، والعمل كجهة اتصال وحيدة للإبلاغ عن حوادث الأمن السيبراني، والتنسيق والاتصالات ذات الصلة، ويجب أيضاً أن تتضمن مهام هذه الفرقة الوطنية التحليل والإنذار، وتقاسم المعلومات، والحد من مواطن الضعف، والتخفيف ومعاونة جهود الانتعاش الوطنية للبنية التحتية للمعلومات الحرجة.

**المهام الملقاة على عاتق فرقة الاستجاب لحوادث الأمن الحاسوبي (CIRT):**

- رصد وتحديد النشاط الخارج على القياس.
- تحليل المخاطر السيبرانية ومواطن الضعف ونشر المعلومات المتعلقة بالإنذار بالأخطار السيبرانية.
- تحليل المعلومات المتعلقة بالحوادث ومواطن الضعف التي توزعها الجهات الأخرى وتجميعها، بما في ذلك الموردون لتكنولوجيا المعلومات، وخبراء التكنولوجيا؛ لتوفير تقييم يقدم لأصحاب المصلحة المهتمين.

• إقامة آليات اتصالات موثوق بها وتسهيل عملية الاتصال بين المعنيين لتقاسم المعلومات ومعالجة القضايا ذات الصلة بالأمن السيبراني.

• توفير معلومات الإنذار المبكر، بما في ذلك المعلومات المتعلقة بالحد من مواطن الضعف والمشاكل المحتملة.

• وضع استراتيجيات للحد والاستجابة، وتفعيل الاستجابة المنسقة للحوادث.

• تقاسم البيانات والمعلومات عن الحوادث والاستجابة المقابلة.

• تتبع المعلومات ورصدها لغرض تحديد الاتجاهات واستراتيجيات العلاج طويلة الأجل.

• نشر أفضل الممارسات العامة المتعلقة بالأمن السيبراني والتوجيهات المتعلقة بالاستجابة للحوادث وتلافيها.

**٢: إقامة آلية أو آليات داخل الحكومة للتنسيق بين المؤسسات المدنية والحكومية:**

أ- يتمثل أحد الأدوار الرئيسة للفرقة الوطنية للاستجابة لحوادث الأمن الحاسوبي في نشر المعلومات، بما في ذلك المعلومات عن مواطن الضعف والأخطار الحالية على المعنيين، وتمثل الوكالات الحكومية المعنية أحد أصحاب المصلحة المجتمعية ويتعين إشراكها في أنشطة الاستجابة.

ب- يمكن أن يتخذ التنسيق الفعال مع هذه المؤسسات المختلفة عدة أشكال منها -على سبيل المثال- ما يأتي: إقامة موقع على شبكة الويب لتبادل المعلومات أو توفير المعلومات من طريق قوائم المراسلات بما في ذلك النشرات الإخبارية وتقارير الاتجاهات والتحليل، أو إعداد المطبوعات التي تتضمن التنبيهات والأفكار المفيدة والمعلومات عن مختلف جوانب الأمن السيبراني بما في ذلك التكنولوجيات الجديدة ومواطن الضعف والأخطار والنتائج الناجمة عنها.

**٣: إقامة شراكات مع دوائر الدولة المعنية استعداداً لمواجهة الحوادث السيبرانية على المستوى الوطني وتتبعها والاستجابة لها:**

أ- يتعيّن أن تتعاون الحكومة والفرقة الوطنية للاستجابة لحوادث الأمن الحاسوبي مع القطاع الخاص، ونظراً لأن القطاع الخاص في كثير من البلدان يمتلك الجزء الأكبر من البنية التحتية الحيوية

للمعلومات وأصول تكنولوجيا المعلومات؛ لذا من الضروري على الحكومة العمل مع القطاع الخاص لتحقيق أعلى فائدة تخص الإدارة الفعالة للحوادث الناجمة عن جرائم المعلوماتية .

ب- تتيح العلاقات التعاونية مع القطاع الخاص -القائمة على الثقة- للحكومة اكتساب نظرة متعمقة في كثيرٍ من جوانب البنية التحتية الحيوية التي يملكها القطاع الخاص ويديرها، ويمكن للتعاون بين القطاعين العام والخاص والناس أن يساعد في إدارة المخاطر المرتبطة بالأخطار السيبرانية ومواطن الضعف والآثار الناجمة، وتحقيق التوعية بالأوضاع على مستوى العالم من خلال تقاسم المعلومات، والتوعية، والمشاركات المتبادلة.

التشجيع على تطوير ممارسات تقاسم المعلومات بين القطاع الخاص والحكومة بما يتيح تقاسم المعلومات التشغيلية في الوقت الفعلي.

خ- هناك بعض الوسائل لتشجيع الشراكة بين القطاعين العام و الخاص منها:

تحديد المنافع التي تعود على كل من الحكومة والقطاع الخاص.

وضع برامج تضمن حماية بيانات الملكية الحساسة وتنفيذها.

إنشاء فرق عمل مشتركة بين القطاعين العام والخاص بشأن إدارة المخاطر السيبرانية وإدارة الحوادث.

تقاسم أفضل أساليب وممارسات الاستجابة للحوادث وإدارتها ومواد التدريب الخاصة بها.

التعاون في تحديد الأدوار والمسؤوليات الخاصة بالحكومة والقطاع الخاص في إدارة الحوادث وفي وضع بروتوكولات متماسكة وقادرة على التنبؤ على مدار الوقت.

**٤: إقامة جهة أو جهات اتصال داخل المؤسسات الحكومية والقطاع الخاص والشركاء الدوليين لتسهيل التشاور والتعاون وتبادل المعلومات مع الفريق الوطني المسؤول عن الاستجابة للحوادث (CIRT):**

أ- يُعَدُّ تحديد جهات الاتصال الملائمة وإقامة علاقات عمل تعاونية لأغراض التشاور والتعاون وتبادل المعلومات عنصراً أساسياً للآلية المنسقة والفعالة الوطنية والدولية المعنية بالاستجابة للحوادث حيث إن لهذه العلاقات دوراً كبيراً في عملية الإنذار المبكر بالحوادث السيبرانية المحتملة وتبادل

المعلومات عن الأخطار والاستجابات فيما بين أطراف الاستجابة للحوادث والمعنيين الآخرين .

ب- يمكن أن توفر جهات اتصال محدَّثة وقنوات اتصال مع دوائر أصحاب المصلحة تبادل المعلومات الاستباقية وفي الوقت المناسب فيما يتعلق بالاتجاهات والأخطار والإسراع بالاستجابة، ومن الضروي إقامة اتصالات تستند إلى وظائف الإدارات وليس إلى الأفراد لضمان أن تظل قنوات الاتصال مفتوحة حتى حينما يترك الأفراد المنظمة، وتبدأ العلاقات في كثير من الأحيان ببناء الثقة مع أفراد معينين، إلا أنها يجب أن تتطور إلى ترتيبات أكثر التزاماً بالطابع النظامي والمؤسسي.

**٥: المشاركة في الأنشطة التعاونية وأنشطة تقاسم المعلومات على المستوى الدولي:**

يجب أن تشجع الحكومة التعاون مع المنظمات والموردين للتكنولوجيا والخبراء الآخرين المعنيين بهذا الموضوع على ما يأتي:

- الاستجابة المسبقة للحوادث بِعَدِّها قاعدة عالمية للسلوك.
- أن تعزز الحكومة الإمكانات لفرق الاستجابة لحوادث الأمن الحاسوبي للانضمام إلى المؤتمرات والمحافل الدولية والإقليمية بغية بناء القدرات؛ من أجل تحسين آخر ما توصلت إليه التكنولوجيا في الاستجابة للحوادث على المستوى الإقليمي.
- التعاون في مجال تنمية مواد CIRT على المستوى الوطني وإبلاغها إلى سلطات CIRT بفعالية.

**٦: وضع أدوات وإجراءات لحماية الموارد السيبرانية للكيانات الحكومية:**

أ- تتطلب عملية الإدارة الفعالة للحوادث وضع سياسات وإجراءات ومنهجيات وأدوات أمنية وتنفيذها لحماية الأصول السيبرانية للحكومة وأنظمتها وشبكاتها ووظائفها، ويمكن أن يتضمن ذلك بالنسبة لفرقة الاستجابة لحوادث الأمن الحاسوبي إجراءات التشغيل المعيارية، ومبادئ توجيهية للعملية الداخلية والخارجية، وسياسات أمنية للتنسيق مع المعنيين وتنفيذ شبكات المعلومات الآمنة لعمليات فريق CIRT، التي يتعيّن عليها -بوصفها جهة اتصال بشأن الاستجابة للحوادث- التنسيق مع المعنيين كافة، والمساعدة في التعاون مع فرق الاستجابة للحوادث الأخرى، ويتعين على الحكومة أن توفر التدريب المستمر لجميع الموظفين الجدد والحاليين بشأن الاستجابة للحوادث.

**٧: القيام من خلال الفريق الوطني للاستجابة للحوادث بإنشاء قدرة على تنسيق العمليات الحكومية للاستجابة للهجمات السيبرانية واسعة النطاق والتعافي منها:**

في حالة وقوع حادثة ترقى إلى مستوى الأهمية الوطنية فمن الضروري وجود جهة اتصال مركزية للتنسيق مع الكيانات الحكومية الأخرى ومع المعنيين الآخرين، مثل القطاع الخاص، ومن المهم وضع الخطط والإجراءات التي تكفل استعداد الفرقة الوطنية للاستجابة للحوادث للتصدي لأي حادث محتمل.

**٨: التشجيع على ممارسات الإفصاح التي تتسم بالمسؤولية من أجل حماية العمليات وسلامة البنية التحتية السيبرانية:**

من الملاحظ أنه من الممكن اكتشاف مواطن ضعف في منتجات تكنولوجيا المعلومات كالتجهيزات أو البرمجيات، وينبغي اتخاذ القرارات الخاصة بكشف المعلومات الخاصة بمواطن الضعف للجمهور على أساس كل حالة على حدة، بحيث لا يُساء استعمال هذه المعلومات، وينبغي إتاحة الوقت الكافي للبائعين قبل أي عملية من عمليات الكشف عن هذه المعلومات.

**ثالثا : آليات العمل:**

١. يجب أن يقتنع صناع القرار في العراق بالحاجة إلى إجراء وطني للتصدي للأخطار ومواطن الضعف في البنية التحتية السيبرانية الوطنية من خلال المناقشات على مستوى السياسات والتشريعات ووضع أو اقترح الأطر الكفيلة بذلك.

٢. تحديد شخص رئيس ومؤسسة رائدة يقع على عاتقها الجهد الكامل على المستوى الوطني.

٣. تحديد المكان الحكومي الذي ينبغي أن يؤسس في إطاره فريق استجابة لحوادث أمن الحاسوب (CERT) توكل إليه المسؤولية الوطنية في هذا المجال وتحديد المؤسسات الرائدة لكل جانب من جوانب الاستراتيجية الوطنية.

٤. تحديد الخبراء وواضعي السياسات الملائمين داخل الوزارات الحكومية، والسلطات الحكومية والقطاع الخاص وأدوارهم فيما يخص المشروع .

٥. إقامة آليات للتعاون فيما بين الحكومة العراقية وبقية الحكومات وكيانات القطاع الخاص على المستوى الوطني وتحديدها.

٦. تحديد الدول ذات المشاريع المماثلة والاستفادة من مشاريعها والآيات المتبعة فيها.

٧. المشاركة في تعزيز الجهود الدولية لمعالجة قضايا الأمن السيبراني، بما في ذلك تقاسم المعلومات وجهود المساعدة.

٨. ضرورة متابعة التوصيات والقرارت الخاصة بالموضوع التي تصدر من المؤسسات الدولية المعنية بالموضوع كالاتحاد الدولي للاتصالات.

٩. تأسيس إدارة متكاملة للمخاطر لغرض تحديد الجهود الوقائية المتعلقة بالأمن السيبراني ووضع الأولويات المتعلقة بها.

١٠. التقييم الدوري الحالة الراهنة للأمن السيبراني ووضع أولويات البرامج.

١١. تحديد متطلبات التدريب وكيفية تحقيقها.

**رابعا: إنشاء منظمة وطنية لإدارة الحوادث المراقبة والإنذار والاستجابة والانتعاش:**

من المهم أن تقوم الحكومة العراقية بإنشاء أو تحديد منظمة وطنية تعمل كجهة اتصال بين المؤسسات كافة لضمان الفضاء السيبراني وحماية البنية التحتية الحيوية للمعلومات تتضمن المهام الموكل إليها (المراقبة، والإنذار، والاستجابة، وجهود الانتعاش، وتيسير التعاون بين الكيانات الحكومية والقطاع الخاص والدوائر الأكاديمية والمجتمع الدولي).

إذ يقع على عاتق الحكومة الدور الأساس في معالجة الأمن السيبراني على المستوى الوطني وفي الإعداد لرصد الحوادث السيبرانية وإدارتها والاستجابة لها، وتتطلب الإدارة الفعالة للحوادث النظر في اعتبارات التمويل والموارد البشرية والتدريب والقدرات التكنولوجية والعلاقات بين الحكومات والقطاع الخاص والمتطلبات القانونية، ويعدُّ التعاون على جميع المستويات الحكومية ومع القطاع الخاص والدوائر الأكاديمية والمنظمات الدولية عنصراً ضرورياً لإدارة الحوادث ولاستثارة الوعي بالحوادث المحتملة والخطوات اللازمة صوب العلاج، وعلى الحكومة كذلك ضمان التنسيق بين الأطراف كافة.

## خامسا: الترويج لثقافة وطنية للأمن السيبراني:

نظراً لما أصبحت عليه الحواسيب الشخصية من قوة تتزايد باطّراد، وأن التكنولوجيات تتقارب في سماتها، وأن التوصيلات عبر الحدود الوطنية آخذة في التزايد؛ لذا ينبغي لجميع المعنيين الذين يقومون بتوريد تكنولوجيا المعلومات والاتصالات وإدارتها، الذين يستخدمون شبكات المعلومات فهم قضايا الأمن السيبراني وأن يتخذوا الإجراءات المناسبة لحماية شبكاتهم، ويجب على الحكومة أن توجه بضرورة نشر ثقافة الأمن السيبراني ودعم الجهود المساعدة على ذلك.

### أولا: الهدف من ترويج ثقافة الأمن السيبراني:

سأعرض أهم الأهداف في إطار ثقافة الأمن السيبراني التي ينبغي لها أن تؤخذ بنظر الحسبان من قبل الحكومة أو المؤسسات المعنية بهذا الموضوع.

١. الترويج لثقافة وطنية للأمن بما يتوافق وقرارات المنظمات الأممية مثل قرار الجمعية العامة للأمم المتحدة ٢٣٩/٥٧ والقرار ١٩٩/٥٨، لإرساء ثقافة عالمية لأمن الفضاء الحاسوبي وحماية البنى التحتية الحيوية للمعلومات.

٢. توعية القطاع الخاص والمجتمع المدني والأفراد، إذ ينبغي تدريب مستعملي الأنظمة الحكومية والخاصة، وإدخال تحسينات في المستقبل على الجوانب الأمنية، فضلاً عن أمور أخرى مهمّة تشمل الخصوصية، والرسائل الاقتحامية، والبرمجيات الضارة.

٣. تنفيذ تطبيقات الحكومة الإلكترونية وخدماتها من أجل تحسين عملياتها الداخلية وتوفير الخدمات الأفضل للقطاع الخاص والمواطنين.

٤. تناول مسألة أمن أنظمة المعلومات وشبكاتها من منظور آخر يشمل عناصر أخرى من قبيل تلافي المخاطر وإدارتها، وتوعية المستخدمين، وألّا يقتصر هذا الدور على المنظور التكنلوجي فقط.

٥. قيام البلدان بإبرام المعاهدات والاتفاقيات التي تعتمد على نهج متطور وشامل لتنفيذ الأمن السيبراني، من خلال إنشاء هيكل إدارة عالي المستوى لتنفيذ السياسات الوطنية، فضلاً عن الدعوة لتطبيق المعايير الدولية الخاصة بالموضوع.

٦. تشجيع الحكومة على تعزيز ثقافة للأمن على مستوى أممي ودولي وإقليمي من خلال المؤتمرات والنشاطات المختلفة.

**ثانيا: خطوات تحقيق الأهداف:**

**١. تنفيذ الخطة الأمنية شاملة للأنظمة التي تديرها الحكومة:**

تتضمن الخطوة الأولية إجراءً حكومياً رامياً لتأمين الأنظمة التي تديرها من خلال تنفيذ خطة أمنية وطنية تشمل إدارة المخاطر وتصميم مخطط للأمن وتنفيذه، وإعادة تقييم كل من الخطة وتنفيذها لقياس ما تحقق من تقدم وتحديد المجالات التي تحتاج إلى تحسينات في الخطة أو في تنفيذها، وينبغي أيضاً أن تتضمن الخطة أحكاماً تتعلق بإدارة الحوادث، التي تتضمن الاستجابة والمراقبة والإنذار والانتعاش ويجب أن تشمل الخطة كذلك التعاون بين الحكومة والقطاع الخاص والمجتمع المدني بشأن التدريبات والمبادرات الأمنية السيبرانية .

**٢. تنفيذ برامج ومبادرات التوعية الأمنية لمستخدمي الأنظمة والشبكات الحكومية التي تتضمن الآتي:**

أ- التوعية بالأمن السيبراني التي تتضن إشاعة ثقافة أمنية سيبرانية بين عامة الجمهور والمؤسسات المعنية وإقامة روابط مع المتخصصين الحكوميين في مجال الأمن السيبراني من أجل تقاسم المعلومات بشأن مبادرات الأمن السيبراني، فضلاً عن تنمية التعاون وتعزيزه في مجال المسائل المتصلة بالأمن السيبراني بين المؤسسات المعنية والأفراد.

هناك ثلاثة عناصر وظيفية يتعيّن النظر فيها لدى وضع برنامج للتوعية في هذا المجال:

- توعية أصحاب المصلحة وإشراكهم مما يؤدي إلى تعزيز الثقة بين القطاع الخاص والحكومة والأوساط الأكاديمية من أجل زيادة الوعي بالأمن السيبراني.

- التنسيق الذي من شأنه أن يكفل التعاون بشأن الحوادث والأنشطة المتصلة بالأمن السيبراني بين مختلف القطاعات الحكومية.

- تبادل الاتصالات والرسائل مع التركيز على تنمية الاتصالات الداخلية (داخل الوكالة

الحكومية المسؤولة عن هذا البرنامج) والاتصالات الخارجية (الوكالات الحكومية الأخرى، ودوائر الصناعة، والمؤسسات التعليمية، ومستعملي الحواسيب وعامة الجمهور).

**٣- التشجيع على إيجاد ثقافة للأمن داخل مؤسسات الأعمال التجارية:**

يمكن تحفيز ثقافة الأمن السيبراني داخل مؤسسات الأعمال التجارية من طريق عدد من السبل الحديثة؛ وذلك من خلال التعاون الحكومي والمبادرات مع روابط دوائر الأعمال التجارية أو الشراكات بين القطاعين العام والخاص، فضلاً عن تنفيذ مبادرات للتوعية والتدريب، ومن بين الأمثلة على هذه المبادرات: إتاحة المعلومات بطريقة مباشرة وغير مباشرة مثل الكتيبات الدالة، والكتيبات الإرشادية، والسياسات الأنموذجية والمفاهيم، وإنشاء مواقع على شبكة الإنترنيت موجهة بصورة خاصة إلى المنشآت التجارية الصغيرة والمتوسطة الحجم، وتوفير تدريباً وأدوات للتقييم الذاتي على بصورة مباشرة التي تهدف إلى خطوات استباقية لتحسين الأمن السيبراني.

**٤- دعم الخدمات الإرشادية التي تقدم للمجتمع المدني مع توجيه اهتمام خاص لاحتياجات الأطفال والشباب والأشخاص ذوي الاحتياجات الخاصة من خلال الآتي:**

أ- التعاون بين الحكومة مع قطاع الأعمال لتحفيز وعي المواطنين بالأخطار الناشئة والتدابير التي ينبغي استخدامها لمواجهتها من خلال تنظيم محافل محددة مثل يوم أو أسبوع أمن المعلومات، وتهدف معظم المبادرات إلى توعية الأطفال والشباب والأشخاص ذوي الاحتياجات الخاصة والطلاب سواء من خلال المدرسين أمْ الأساتذة أمْ الآباء أمْ من خلال التوزيع المباشر لمواد التوجيه. وتتنوع المواد التثقيفية المعروضة خلال هذه المحافل بدءاً من مواقع شبكة الويب أو الألعاب أو الأدوات على الخط مباشرة إلى البطاقات البريدية، أو الكتب الدراسية، أو الامتحانات و غيرها.

ب- يمكن للحكومة والقطاع الخاص أن يتبادلا الدروس التي اكتسباها من وضع الخطط الأمنية والتدريب، والعمل على تحسين أمن البنى التحتية المحلية للمعلومات.

**٥- الترويج لبرنامج وطني شامل للتوعية كي يتمكن جميع المشاركين -دوائر الأعمال والمستخدمين والمواطنين- من تأمين أدوارهم في الفضاء السيبراني:**

يوجد الكثير من مواطن الضعف في أنظمة المعلومات نتيجة لنقص الوعي بالأمن السيبراني

من جانب المستخدمين، ومديري الأنظمة وواضعي التكنولوجيات، والموردين والمدققين، وكبار موظفي المؤسسات المسؤولين عن المعلومات، ويمكن أن تشكل مواطن الضعف هذه مخاطر جسيمة على الهياكل الأساسية للحكومة، حيث إن نقص الوعي الأمني لدى مديري الأنظمة يشكل نقطة ضعف للخطة الأمنية للمؤسسة؛ لذا فإن تعزيز جهود القطاع الخاص في تدريب الموظفين واعتماد شهادات أمنية مقبولة على نطاق واسع للموظفين سوف تساعد في الحد من مواطن الضعف هذه، ومن ناحية أخرى فإن التنسيق الحكومي للأنشطة الوطنية للإرشاد والتوعية للتمكين من ثقافة الأمن سوف يبني أيضاً الثقة مع القطاع الخاص؛ لأن الأمن السيبراني عبارة عن مسؤولية مشتركة.

**٦- تعزيز الأنشطة المعنية بالتكنولوجيا الحديثة والبحث والتطوير:**

ينبغي للحكومة تشجيع الأنشطة المعنية بالتكنولوجيا والبحث والتطوير من خلال توجيه بعض جهودها صوب أمن البنية التحتية للمعلومات بتحديدها لأولويات البحوث والتطوير في المجال السيبراني، بتطوير المنتجات ذات الخواص الأمنية الذاتية، فضلاً عن معالجة التحديات التقنية الصعبة، ومن الممكن إتاحة الفرص لإشراك الطلاب في مبادرات الأمن السيبراني.

**٧- تنمية الوعي بالمخاطر السيبرانية والحلول المتاحة:**

يقتضي تناول القضايا التقنية تكاتف الحكومة وقطاع الأعمال التجارية والمجتمع المدني والأفراد المستخدمين في العمل معاً؛ لوضع التدابير التي تدمج بين المعايير واللوائح وتنفيذها.

تواصل المعنيين بالحكومة مع أدوات التكنولوجيا العالمية؛ لمعالجة مختلف احتياجات الأمن السيبراني حيث يوجد عدد من المنظمات ولجان الدراسات بما في ذلك لجنة الدراسات ١٧ لقطاع تقييس الاتصالات وغيرها من المؤسسات العالمية.

إن وجود مركز يُعنى بأمن المعلومات العراقي وإدارة الحوادث ومعالجتها والسيطرة على جرائم المعوماتية أمر مهمّ جداً وضروري في ظل ما يتعرض له العراق من هجمات إرهابية متمثلة بتنظيمات متطرفة تعتمد اعتماداً رئيساً على تناقل المعلومات والبيانات عبر الشبكات وعبر الفضاء السيبراني، إن سيطرة الحكومة العراقية من خلال إنشاء هذا المركز سيقلل من الجرائم الإرهابية بنسبة كبيرة جداً تصل إلى أكثر من ٧٠٪ ويساهم بتقليل نفقات الجهود العسكرية والخسائر البشرية نتيجة المواجهة المباشرة مع العدو، إن هذا المركز يحتاج إلى إرداة سياسية وقرار شجاع من قبل صنّاع القرار، ويجب

أن يرتبط هذا المركز بجهة محددة ومستقلة وغير خاضعة للضغوطات السياسية لغرض ضمان انسيابية العمل، ويكون ذلك من خلال تشريع قانون يتضمن الجوانب التنظيمية والفنية والإدارية والمالية كافة لإنشاء هذا المركز، ومن الجدير أن أنوه أيضاً إلى ضرورة اختيار المورد البشري الكفوء والمدرب تدريباً عالياً والموثوق من الناحية الأمنية، واتخاذ أعلى درجات الحيطة والحذر في اختيار العاملين في هذا المركز؛ لأن أي خرق من الممكن أن يشكل كارثة على أمن الدولة وخسائر كبيرة لا تُحمَدُ عقباها.

**المصادر باللغة العربية:**

- الاتحاد الدولي للاتصالات – مكتب السيطرة والتقييس ITU-T.

- الأمن في الاتصالات وتكنولوجيا المعلومات تحقيق في قضايا ذات صلة على تطبيق.

-الجرائم المعلوماتية المفهوم والأسباب / أ.د. ذياب موسى البداينة.

-جرائم المعلوماتية وطرق مواجهتها / الدكتور محمد علي قطب.

- الدكتور هلالي عبد الإله أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي.

-دليل الأمن السيبراني للبلدان النامية الاتحاد الدولي للاتصالات / ط ٢٠٠٧.

- العناصر الأساسية لتنظيم الجهود الوطنية لتحقيق الأمن السيبراني.

- قرارات مؤتمر المندوبين المفوضين العالمي المعنية بالموضوع P-P2014.

- كتاب الاختراق / محمد إسماعيل محمد.

-كمال احمد الكركي: النواحي الفنية لإساءة استخدام الكمبيوتر ورشة عمل في دورة جرائم التطور التقني.

- المرشد الأمريكي الصادر عام ١٩٩٤م، المعد من قبل قسم جرائم الحاسب الآلي والملكية الفكرية بإشراف الأستاذ Orin Kerr.

- مشروع دراسة الجوانب المالية لأمن الشبكات والبرمجيات الخبيثة والرسائل الاقتحامية ITUD1/144.

- مقررات مؤتمر تنمية الاتصالات العالمي WTDC-12.

- مقررات مؤتمر تقييس الاتصالات العالمي لعام ٢٠١٢.

- مهددات الأمن المعلوماتي وطرق مواجهتها / منصور بن سعيد القحطاني.

– هدى قشقوش: جرائم الكمبيوتر والجرائم الاخرى في مجال تكنولوجيا المعلومات . بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي بعنوان: الجرائم الواقعة في مجال تكنولوجيا المعلومات.

**المصادر باللغة الإنجليزية:**

- Auditing Information Systems. Hoboken, New jersey , John wiley of sons.

- http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_58_199pdf

- http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_57_239pdf.

- Vassilaki (Irini) Computer crimes and other crimes against inforation technology in Greec.

- WORLD TELECOMMUNICATION STANDARDIZATION Resolution 52 Resolution 50

- Yamaguchi (Atsushi):››computer crime and other crime against Information Technology In Japan›