اتجاهات في أمن المعلومات وأمانها

اتجاهات في أمن المعلومات وأمانها

أهمية تقنيات التَّعْمِية

(الشفرة)

ساري الخالد

العبيكان
Obeikan

© شركة العبيكان للتعليم، ١٤٣٨هـ

فهرسة مكتبة الملك فهد الوطنية أثناء النشر

الخالد، ساري محمد

اتجاهات في أمن المعلومات وأمانها./ ساري محمد الخالد.- الرياض، ١٤٣٨هـ

٢٤٠ص؛ ١٦,٥×٢٤سم.

ردمك: ٦-٠٠٥-٥٠٩-٦٠٣-٩٧٨

١- أمن المعلومات ٢- أمن الحاسب

أ. العنوان

ديوي: ٠٠٥,٨ ١٤٣٨/١٦٨٩

الطبعة الأولى

١٤٣٩هـ/٢٠١٨م

نشر وتوزيع العبيكان Obeikan

المملكة العربية السعودية - الرياض

طريق الملك فهد - مقابل برج المملكة

هاتف: ٤٨٠٨٦٥٤ ١١ ٩٦٦+، فاكس: ٤٨٠٨٠٩٥ ١١ ٩٦٦+

ص.ب: ٦٧٦٢٢ الرياض ١١٥١٧

www.obeikanretail.com


بسم الله الرحمن الرحيم

كلمة شكر

أتقدم بالشكر الجزيل للأستاذ الدكتور محمد مراياتي؛ لما قدمه من جهد كبير في مراجعة الكتاب وتصحيح ما وجب تصحيحه، وتقديم النصح في محتواه، وقيامه بإضافة فقرات مهمة عليه.

وأتقدم بالشكر الوافر لمؤسسة (العبيكان للنشر) لمساعدتها وتسهيلاتها في نشر الكتاب وتوزيعه.

ساري خالد

دمشق، 2016م.

المحتويات

المقدمة

الحمد لله ربِّ العالمين، والصلاة والسلام على سيِّدنا محمد وعلى آله وصَحبه أجمعين، أما بعد.

فلقد تطورت تكنولوجيا المعلومات والاتصالات تطورًا جعلها دائمة الوجود في حياتنا أفرادًا ومؤسسات وحكومات، فأصبحت في يد الصغير والكبير، وفي البيت والمدرسة والشركات والدواوين، ودخلت بشكل عميق في ثنايا الثقافة والاقتصاد والدفاع والمجتمع والمال، وفي المنظمات والمؤسسات الإقليمية والدولية، يرافق ذلك بزوغ أخطار وتحديات أمنية كبيرة تهدد الجميع، ويسعى هذا الكتاب إلى زيادة الثقافة العامة الضرورية لفهم هذه الأخطار والتحديات والتعامل معها، وإلى زيادة الوعي بأبعادها وبالمبادئ الأساسية التي تنظمها وتديرها.

من جهة أخرى، بُنِي علم أمن المعلومات على أساسيَّات ظَلَّت مُعتَمَدة بوصفها مبدأ عمل لمُمارسَة هذا العلم، إلا أن هناك أمورًا يجب الانتباه إليها على الرغم من تحقيق هذه الأساسيات أو تطبيقها من قِبَل العامِلِين في هذا الحقل، وهي ثغرات يَنبغي سَدُّها، وخاصة مع تعاظم قضايا أمن المعلومات وأمانها في الآونة الأخيرة، فكثيرًا ما يُنظَر إلى أمن المعلومات على أنَّه مجموعة من الإجراءات التطبيقيَّة لتأمين المعلومات الخاصَّة دون الالتفات إلى الحالة التي ستَكون عليها المعلومات بعد تطبيق هذه الإجراءات، ومن

هذه النقطة، يهتم هذا الكتاب بقياس ومعالَجة ومراقَبة الحالة التي تَدخُل فيها المعلومات بعد تطبيق إجراءات أمن المعلومات عليها، وتُسمَّى هذه الحالة (أمان المعلومات)[1]. ويُشار من قِبَل بعضهم إلى (أمان المعلومات) على أنَّه (أمن المعلومات) نفسه، ولكن من المفيد التمييز الواضح بين المصطلحين، فـ (أمان المعلومات) هو الوَضْعُ الجديد الذي تَدخُل فيه المعلومات بعد تطبيق إجراءات أمن المعلومات. علاوةً على ذلك، فقد أصبَحَت هناك مقاييس لهذه الحالة وإجراءات ضمن هذه الحالة تَتعامَل مع المعلومات لمتابعة الحفاظ على سريَّتها وسلامتها وتَوافرها لتجاري التطورات الطارئة.

يستعرض الكتاب في طرحه للموضوع تعاظم أهمية أمن المعلومات وأمانها في الآونة الأخيرة، وتفاقم المهددات وكثرة الاختراقات وتواترها على كل الأصعدة، ويأتي على ذكر حالات عالمية مختلفة بوصفها أمثلة لذلك.

ويُقدِّم (**الفصل الأول**) من هذا الكتاب مجموعة من المفاهيم الضروريَّة لاستيعاب الاتِّجاهات في أمن المعلومات وأمانها، ويُعالِج مفاهيم هذا الحقل، ويُقدِّمها بأسلوبٍ يوضحها أخذًا في الحسبان مفاهيم (أمان المعلومات)، ويُناقِش بعض المفاهيم المستجدة في هذا العلم، مثل مفاهيم (نماذج المعلومات الخاصَّة) التي قَسَّمت المعلومات إلى ثلاثة أشكال رئيسة بحسب الاهتمام وبحسب مُلّاكها، وأخيرًا يتعرض لمفاهيم وتعريفات عامة في تعمية (تشفير) المعلومات، والتعمية هذه من أهم التقنيات المستعملة لتحقيق أمن المعلومات.

ويبيّن (**الفصل الثاني**) تعاظم أهمية أمن المعلومات خلال السنوات القليلة الماضية، وذلك على كل المستويات من الفرد إلى المؤسسات والوزارات والشركات، في القطاع الخاص والمؤسسات المالية المختلفة، وخاصة البنوك، وكذلك على مستويات

---

(1) أمن المعلومات: Information Security وأمان المعلومات: Information Safety

أمن الدول ودفاعاتها، ولقد أصبح أمن المعلومات من القضايا اليومية في حياتنا وعلى كل المستويات والقطاعات.

أمّا (**الفصل الثالث**) فيَشرَح شرحًا مختصرًا عددًا من المقوِّمات الأساسيَّة التي تَبني علم أمن المعلومات، والداخِلة في استكمال الاتِّجاهات الجديدة فيه، ومن هذه المقومات ثلاثيَّة السرية والسلامة والتوافر، وأمن الشبكات، وأمن المعلومات الفيزيائي، والنفاذ إلى المعلومات، والتعمية.

ويقدم (**الفصل الرابع**) توضيحًا لمفهوم أمان المعلومات، ويشرح ثلاثة مقاييس لهذا الأمان، فقد أصبَحَ أمان المعلومات يُقاس بخيارات عدة من مستويات الأمان التي تُعيد اهتمامات الإنسان بمعلوماته الخاصَّة بحسب وجوده ضمن فئات المجتمع، إلى درجات الأمان التي تَنظُر إلى المعلومات وِفْقَ أهميَّتها وعواقب افتضاحها، وإلى مبدأ الأمان الذي يَقيس أمان المعلومات اعتمادًا على تكلفة اختراقها أو زمنه.

وأمّا (**الفصل الخامس**) فيبيّن بعض الأساسيَّات في إدارة أمن المعلومات، ويُطبّقها على نماذج المعلومات الثلاثة، ويُطبّق هذا الفصل إجراءات الأمن وإجراءات الأمان لكل نموذج من نماذج المعلومات بعد تَفصيل المراحل التي تَدرُس الوَضْع العام للمعلومات ومحيطها، وتُخمِّن الأخطار التي يُمكِن أن تُحيط بها، ويُمكِن اعتبار هذا الفصل دليلًا مبسطًا لتطبيق أمن المعلومات وأمانها من قِبل أي طرف: (من الفرد إلى المنظَّمة إلى الدولة).

ويستعرض (**الفصل السادس**) إحدى أهم تقنيات أمن المعلومات وأمانها، وهي تقنية التعمية واستخراج المعمى كما سماها علماؤها العرب القدامى الذين وضعوا أسسها، أو كما يدعوها بعضهم اليوم الشفرة وكسرها. فيأتي الفصل على مبادئها البسيطة وطرقها غير المعقدة لتسهيل فهمها، ومن ثم فهم الإجراءات المعيارية الأساسية المبنية عليها لتحقيق أمن المعلومات وأمانها.

ويشرح (**الفصل السابع**) بعض أهم الإجراءات المستعملة لتحقيق أمن المعلومات، مثل التوقيع الإلكتروني والبصمة الإلكترونية الخاصة بأي نوع من أنواع المعلومات، وإثبات هوية المرسل والمستقبل على شبكات نقل المعلومات وغيرها من الإجراءات الرئيسة.

ويُعالِج (**الفصل الثامن**) عددًا من القضايا المهمَّة في هذا الحقل، مع استعراض الحلول المناسِبة لها، فيعالج باختصار أمان معلومات القُصَّر، وأمان المعلومات الحَركيَّة، وحوادث الأمان.

ويتطرق (**الفصل التاسع**) إلى موضوعٍ متعاظمِ الأهميةِ في الآونةِ الأخيرةِ، وهو موضوع (الحروب السايبرية)، وملامح مستجداتها واهتمام الدول بالتعامل معها، وإنشاء الإدارات والتنظيمات والتجهيزات اللازمة لها.

إنَّ أهَم ما في هذا الكتاب هو أنه يقدم بعض المعارف الضرورية لزيادة الوعي بأمن المعلومات ومعرفة مصطلحاته وأساسياته اللازمة لنا جميعًا، خاصةً مع تعاظم قضايا هذا الأمن، ويُقدِّم طُرُقًا في أمان المعلومات تَتمثَّل في مشاهدة الحالة التي تَمرُّ فيها المعلومات بعد مرحلة أمنها ومتابَعتها.

وأخيرًا، يَجب أن أُنوِّه إلى أنَّ هذا الكتاب مِثْله مِثْل أيّ كتاب أَلَّفه بَشَر، فلا أُضفي عليه أيَّ صفة كمال، فما اكتَمَل إلا كتاب الله – عزَّ وجل – والحمد لله ربِّ العالمين.

ساري الخالد

2016م.

الفصل الأول

مفاهيم

يَشرَح هذا الفصل عددًا من المفاهيم الأساسيَّة في حقل أمن المعلومات، ويطرح مفاهيم أساسيَّة أخرى؛ لكي يكون القارئ مُمهَّدًا للتَعرُّف إلى الأفكار الواردة في هذا الكتاب.

1.1 أمن المعلومات

لقد تَعدَّدت التعاريف الرسميَّة لأمن المعلومات، وفيما يأتي تعريف أمن المعلومات المتوافِق مع اتِّجاهات هذا الكتاب. فأمن المعلومات Information security هو مُمارسَةُ العمل الذي يَتمثَّل في حماية المعلومات الخاصَّة من السرقة، أو الإفشاء، أو التخريب وإدخالها في وَضْعِ الأمان والمحافظة عليها، وتَقتَضي حماية المعلومات في هذا التعريف حماية محيطها ومحيط مالِكها أيضًا.

دورة حياة أمن المعلومات

2.1 أمان المعلومات

يحاول هذا الكتاب التمييز بين المصطلحَين (أمن المعلومات) و(أمان المعلومات)، حيث يَعدّهما بعضهم ذَوَي معنى واحد، ويَستنِد هذا الكتاب على مفهوم أن (أمان المعلومات) مختلِف عن (أمن المعلومات)، وإن (أمان المعلومات) Information safety، بالتعريف، هو الحالة (أو الوَضْع) التي تَدخُل فيها المعلومات الخاصَّة بعد اتخاذ إجراءات أمن المعلومات (أي بعد حمايتها من السرقة أو الإفشاء أو التخريب)، واتخاذ الإجراءات المستمرة لضمان أمان هذه المعلومات والتعامل مع المستجدات.

وكما تَمَّ تعريف (أمن المعلومات) فهو مُمارسَة عمل لحماية المعلومات الخاصَّة، أمّا (أمان المعلومات) فهو ضمان وَضْع المعلومات الخاصَّة بعد تأدية دور (أمن المعلومات). إنَّ مفهوم (أمان المعلومات) مهمٌّ للتمييز بين وَضْع المعلومات قبل تأدية وظيفة (أمن المعلومات) وبَعدها.

3.1 الطَرَف

الطّرَف هو الكائِن الذي يَتعامَل مع البيانات، سواء أكان فردًا Individual أم منظَّمةً Organization أم دولةً State أم طَرَفًا دوليًّا International party. والطّرَف الدولي هو مجموع دولتين أو أكثر.

4.1 الأصول الماديَّة والأصول غير المادية

الأصول الماديَّة Physical assets هي كُلُّ شيء مَلموس تَعود ملكيته إلى طرفٍ ما، مثل التجهيزات والشبكات وغيرها. أمّا **الأصول غير المادية** Logical assets فهي البيانات والمعلومات التي يَمتلِكها طرفٌ ما، ويَسعى العامِلون في حقل أمن المعلومات إلى حماية كلٍّ من الأصول الماديَّة والأصول غير المادية أيضًا.

5.1 البيانات والمعلومات

ثَمَّة اختلاف بين مصطلَحَي البيانات والمعلومات، فمن الناحية العامَّة في حقل تكنولوجيا المعلومات وَضَّحت بعض المراجع الفرق بين البيانات والمعلومات على أنَّ البيانات هي الحقائق (أو البيانات) الخام غير المنظَّمة وغير الجاهزة للاستعمال التي لم تُعالَج بعد، أمّا المعلومات فهي البيانات التي عولجت ورُتّبت، والتي أصبحت جاهزة للاستعمال [8، 7].

وفيما يلي تعريف لكلٍّ من البيانات والمعلومات يُوضِّح الفرق بينهما في سياق أمن المعلومات، **فالبيانات** Data هي مجموع المواد (الرقميَّة أو الورقيَّة) الموجودة التي تَعود ملكيتها إلى طرفٍ ما، والتي تَضم معلومات أو حقائق أو كليهما، وقد تَكون هذه الحقائق إمّا واضحة أو غير واضحة، وقد تُستعمَل أو لا تُستعمَل، وقد يُستفاد منها أو لا، وهي لا تَحمِل قيمة فعليَّة عند أي طرف. أمّا **المعلومات** Information فهي جزء البيانات الواضح

والمفهوم الذي يُمكِن استعماله والاستفادة منه، والذي يَحمِل قيمة فعليَّة عند طرفٍ ما، وقد تَكون المعلومات بالنسبة إلى طرفٍ ما مجرَّد بيانات، وقد تَكون البيانات بالنسبة إلى طرفٍ ما معلومات، وليس بالضرورة أن تَكون المعلومات نصوصًا مكتوبةً، فقد تكون عبارة عن صور فوتوغرافيَّة، أو تسجيلات صوتيَّة، أو تسجيلات فيديويَّة، أو مخططات ورسوم.

ثَمَّة نوعان من المعلومات هما: معلومات **عاديَّة** ومعلومات **خاصَّة**، فالمعلومات العاديَّة هي المعلومات العامَّة المشتَرَكة مع الآخرين التي لا تَنطوي على أي منفعة خاصَّة بطرف دون طرف آخر، والتي لا تَضم موادّ تُؤذي أطرافًا إذا أدرَكَتها أو توصلت إليها أطراف أخرى، ومن أمثلة المعلومات العاديَّة معلومات علميَّة، ومعلومات أدبيَّة، ومعلومات طبيَّة، وأخبار، وبرامج تلفازية، وأفلام سينمائيَّة، وأناشيد، ومواد الكتب أو الصحف أو الأقراص الحاسوبيَّة العامَّة. أمّا المعلومات الخاصَّة فهي المعلومات المرتبِطة بطرفٍ ما، التي يَعدّها هذا الطرف خاصَّة به، ولا يُريد أن يُشارِكه أحدٌ فيها، ولا يُريد أن يَطَّلع أحدٌ عليها إلا من أراد، ويَبتغي حمايتها من السرقة، أو الإفشاء، أو التخريب، ويَهتَم حقل أمن المعلومات بحماية المعلومات الخاصَّة فقط، ولا يَهدُف إلى حماية البيانات أو حتى المعلومات العاديَّة. ولذلك، لا تَرى منشورات حقل أمن المعلومات ضرورة في إضافة كلمة (خاصَّة) بعد كلمة (معلومات). وعليه، فإذا وَرَدت في هذا الكتاب كلمة (خاصَّة) بعد كلمة (معلومات) أم لم تَرِد، فيُقصَد ضمنيًّا أنَّ هذه المعلومات هي معلومات خاصَّة.

وقد تَكون المعلومات الخاصَّة مشتَرَكةً مع طرف أو أطراف عدَّة، وتُسمَّى عندها **معلومات خاصَّة مشتَرَكة**، أو تكون غير مشتَرَكة مع أي طرف، وتُسمَّى عندها **معلومات خاصَّة غير مشتَرَكة**، والمعلومات الخاصَّة المشتَرَكة هي المعلومات الخاصَّة التي يَتشارَك في استثمارها العاملون لدى طرف واحد أو أكثر، مثل معلومات قطاع الأعمال الخاصَّة، والطرف الوحيد الذي يُجيز قانونيًّا التشارُك في استثمار المعلومات الخاصَّة واستعمالها هو مالِك المعلومات (أو القيِّم إذا كان موكَّلًا بذلك من قِبَل مالِك المعلومات)

وإليه تَعود المنفعة الماليَّة من استثمارها، وصفة المعلومات الخاصَّة المشتَرَكة أنها مَسموح نَقلها وتداولها بين المُجَاز لهم فقط. أمّا المعلومات الخاصَّة غير المشتَرَكة فهي المعلومات الخاصَّة التي لا يَتشارَك مالِكها باستثمارها مع أحد أيًّا كان، مثل المعلومات الفردية الخاصَّة غير الحسَّاسة، وصفة المعلومات الخاصَّة غير المشتَرَكة أنها ممنوع نقلها ومن غير المَسموح أن يَستعمِلها إلا مالِكها.

للمعلومات الخاصَّة المشتَرَكة شكلان هما: **معلومات خاصَّة مشتَرَكة معدَّة للتخزين**، و**معلومات خاصَّة مشتَرَكة معدَّة للنقل**، واختصارًا IFTSPI. والمعلومات الخاصَّة المشتَرَكة المعدَّة للتخزين هي المعلومات الخاصَّة التي يَتشارَك في استثمارها أطراف عدَّة داخل أجهزة التخزين، سواء أكانت مخزَّنة في محيط إلكتروني أم في محيط يدوي. أمّا المعلومات الخاصَّة المشتَرَكة المعدَّة للنقل فهي المعلومات التي يَتشارَك في استثمارها أطراف عدَّة من خلال تَبادُلهم لها يدويًّا أو عبر شبكات رقميَّة.

6.1 نماذج المعلومات الخاصَّة

ثَمَّة ثلاثة نماذج للمعلومات الخاصَّة هي: **المعلومات ذات القيمة الماديَّة**، و**المعلومات ذات القيمة المعنويَّة**، و**المعلومات ذات القيمة المَجازيَّة**. المعلومات ذات القيمة **الماديَّة** هي المعلومات التي يُمكِن أن تَعود بنفعٍ مالي عندما تُستثمَر آنيًّا (أي في وقتها) مثل المعلومات الفرديَّة الخاصَّة التي تَضمّ أرقام الحسابات المصرفيَّة ورقم التعريف الشخصي ومعلومات الأعمال الخاصَّة، ومالِك المعلومات ذات القيمة الماديَّة قد يكون فردًا أو رئيس منظَّمة (تجاريَّة أو صناعيَّة) أو مسؤولًا حكوميًّا بالتفويض إذا كانت ملكيَّة المنظَّمة عامَّة. أمّا المعلومات ذات القيمة **المعنويَّة** فهي المعلومات التي لا تُقدَّر بثمن والتي قيمتها فوق ماديَّة، أي إنَّ أهميَّتها وحساسيَّتها تَفوقان أي قيمة ماليَّة مهما بَلَغ مقدار هذه القيمة، مثل المعلومات المصنَّفة سريَّة لدى القطاع العام أو الخاص، والمعلومات الدولية المصنَّفة سريَّة، ومالِك المعلومات ذات القيمة المعنويَّة هو

افتراضًا القيِّم المَعني بحماية هذه المعلومات، سواء في الدولة أو في الطرف الدولي، ولكنَّ المالِك الحقيقي للمعلومات ذات القيمة المعنويَّة هو السلطات العليا التي تَحكُم الدولة أو السلطات العليا المشارِكة بالمعلومات في الطرف الدولي، وأمّا المعلومات ذات القيمة **المَجازيَّة** فهي المعلومات التي تَحمِل أهميَّة بالنسبة إلى طرفٍ ما، ولكنَّها لا تَحمِل أي قيمة ماديَّة، وليست ذات قيمة معنويَّة، ولكنَّها في الوقت نفسه مهمَّة بالنسبة إلى ذلك الطرف، وتُعدّ من خصوصياته، مثل كلمات المرور الخاصَّة بصناديق البريد الإلكتروني، والمذكِّرات الشخصية. ومعنى كلمة (مَجازيَّة) هو أنَّ هذه المعلومات مَجازًا لها قيمة.

القيمة الماديَّة للمعلومات هي المكافِئ المالي الذي يُمكِن أن يُعيده استثمار تِلْك المعلومات في وقتها، وهذه القيمة تُساوي ذلك المكافِئ المالي آنيًّا. أمّا القيمة المعنويَّة فتُساوي منطقيًّا الـ (1) إنْ وُجِدَت أو الـ (0) إنْ لم تُوجَد، وكذلك القيمة المَجازيَّة.

7.1 المعلومات الرقميَّة والمعلومات الورقيَّة

المعلومات الرقميَّة Digital information هي المعلومات المخزَّنة في الأنظمة الحاسوبيَّة على شكل ملفات اثنانية، مثل الوثائق والصور والتسجيلات الصوتيَّة والفيديويَّة. أمّا **المعلومات الورقيَّة** فهي المعلومات المكتوبة أو المطبوعة على الورق، ومنها الوثائق والرسوم الورقيَّة، وتَنطبِق بعض الإجراءات المضادَّة على المعلومات الرقميَّة فقط، ويَنطبِق بعضها الآخر على المعلومات الرقميَّة والورقيَّة معًا.

8.1 ملكيَّة المعلومات

يجري تحديد الأصحاب الحقيقيين للمعلومات من خلال مفهوم **ملكيَّة المعلومات** Information ownership. في حقل أمن المعلومات، ثَمَّة ثلاثة أطراف تَتعامَل مع المعلومات هي: **المالِك**، **والقيِّم** Custodian، **والمستخدِم**. المالِك أو مالِك المعلومات هو الطرف الذي يَمتلِك المعلومات، ويَمتلِك قيمتها (سواء أكانت ماديَّة أم معنويَّة أم

مَجازيَّة)، ولديه كامل الحريَّة المطلقة في التصرُّف بهذه المعلومات، ويَتحمَّل أعباء سرقتها أو إفشاءها أو تخريبها إذا كان مسؤولًا بشكلٍ مباشر عن تخطيط الإجراءات المضادَّة وتطبيقها. أمّا القيِّم فهو عادةً الطرف الذي يَقَع على عاتقه مسؤولية الحفاظ على المعلومات وصيانتها من سرقتها أو إفشائها أو تخريبها، ولديه حقُّ الوصول إلى هذه المعلومات، وهو مسؤول مسؤوليَّة كاملة عن سرقة المعلومات أو إفشائها أو تخريبها إذا قام بتخطيط الإجراءات المضادَّة وتطبيقها، ومسؤول مسؤولية التخطيط فقط إذا قام بتخطيط الإجراءات المضادَّة، ولكنَّه لم يَقُم بتطبيقها، وكان تطبيقها سليمًا، ومسؤول مسؤوليَّة التطبيق فقط إذا قام بتطبيق الإجراءات المضادَّة، ولكنَّه لم يَقُم بتخطيطها، وكان تخطيطها سليمًا. أمّا المستخدِم فهو أي طرف يَستعمِل المعلومات لتحقيق أهداف مالِكها (كالموظَّف مثلًا أو مستخِدم خارج المنظَّمة) وأُعطي حَقَّ الوصول إلى هذه المعلومات من المالِك والقيِّم أو من أحدهما.

يُدعَى الطرف المقابِل لمالِك المعلومات – الذي لديه مصلحة أو منفعة من النفاذ إلى تِلْك المعلومات بشكل يُؤذي المصالح الماديَّة أو المعنويَّة أو المَجازيَّة لمالِك المعلومات – الخصم، ويَجب على مالِك المعلومات أن يَفترِض وجود الخصم حتَّى ولو لم يَكُن أصلًا؛ لأنَّ الأولويَّة الأساسيَّة في حقل أمن المعلومات هي حماية المعلومات في ظل وجود الخصم، ولأنَّ وجود فن أمن المعلومات غير ضروري إذا لم يَكُن هناك خصم (إضافة إلى التهديدات غير البشريَّة).

9.1 محيط المعلومات ومحيط مالِك المعلومات

محيط المعلومات Information environment هو الإطار الفيزيائي الذي يَضمّ المعلومات، ويَحفَظها، ويعالجها. ثَمَّة شكلان لطبيعة عمل محيط المعلومات هما **محيط إلكتروني** و**محيط غير إلكتروني (يدوي)**. المحيط الإلكتروني هو المكان والتجهيزات التي تَضم المعلومات الرقميَّة، وتَحفَظها فقط، مثل نظام حاسوبي أو أي أجهزة تخزين

رقميَّة أو أجهزة شبكة الاتصال الحاسوبية. أمَّا المحيط اليدوي فهو المكان الذي يَضم المعلومات الورقيَّة، ويَحفَظها فقط، مثل الخزنة الحديديَّة أو حافظات الملفات والوثائق الورقيَّة وجميع وسائط حفظ المعلومات بشكلها غير الرقمي؛ أي ما يسمى analog. أمَّا **محيط مالِك المعلومات** Owner environment فهو الإطار الفيزيائي الذي يُحيط بمالِك المعلومات وبمحيط المعلومات معًا، مثل: حجرة أو منزل أو منظَّمة أو دولة، ويَقَع محيط المعلومات داخل محيط مالِك المعلومات، وهو جزءٌ منه.

10.1 مفهوم التعمية (التشفير) أهم تقنيات أمن المعلومات

من المفاهيم الأساسية التي تُشكِّل عماد أمن المعلومات والاتصالات التعمية أو التشفير، وعلى الرغم من وجود كثير من المفاهيم التعموية، إلا أننا سنُعرِّف في هذه الفقرة الأساسيات منها فقط، وسوف نَتحدَّث عن المصطلحات الأخرى لاحقًا.

التعمية Cryptography بالتعريف: **علم حماية المعلومات السرِّية**، وهذا التعريف يرتبِط بالهدف الرئيس للتعمية، وهو الحفاظ على سرِّية المعلومات. أمّا في التعريف الاصطلاحي **فالتعمية هي تحويل المعلومات السرِّية من الشكل الواضح المقروء والمفهوم إلى شكل آخر طُلسمي وعشوائي وغير مفهوم، وذلك باستخدام خطة محدَّدة تَكفُل استرجاعها وإعادتها إلى هيئتها الأصلية الواضحة.** يُدعَى الشخص الذي يُمارِس علم التعمية **المُعمِّي** Cryptographer، والمُعمُّون هم عادةً إمّا باحثين أو رياضيين أو مبرمجين، ويُطلَق لقب المُعمِّي على كل من يعمل، ويُسهِم في حقل التعمية، والاختصاصي في التعمية هو الشخص الذي يُصمّم الخطط التعموية، ويحدّثها، ويضع الآليات المرتبطة بها (البروتوكولات).

جاء مصطلح "Cryptography" أساسًا من الكلمتين اليونانيتَي الأصل: "Kryptos" التي تَعني (مَخفيَّة أو كامنة أو محجوبة)، و"graphy" التي تَعني الكتابة، وبضَمِّهما معًا تُصبِحان كلمة واحدة "Kryptos graphy" أي (الكتابة المَخفيَّة) أو كما في الاصطلاح

العربي التراثي (التعمية)، ولقد دَرَج في هذه الأيام استعمال كلمة (تشفير) بدلًا من كلمة (تعمية)، وقد أَطلَق العلماء العرب الذين عملوا بهذا المجال في القرون الوسطى مصطلحات أخرى تُرادِف (التعمية)، مثل (تعمية الحروف) و(الترجمة) و(الكتابة الباطنة)[1]، لكن تَظَل كلمة (التعمية) المقابِل العربي السليم لمصطلح "Cryptography".

يَتمثَّل دور التعمية في حماية المعلومات السرِّية Secret Information ذات الطبيعة الخاصة، وهي المعلومات التي لا نُريد أن يَطَّلع عليها الآخرون (إلا مَن أَرَدنا مشاركته فيها)، ولا يَهمُّنا تعمية المعلومات التي لا نَراها خصوصية، ولا يَستفيد منها خصم. في الواقع، ثمة نوعان من المعلومات السرِّية:

- معلومات سرِّية فردية (غير مُشترَكة) Non-shared Secret Information: وهي المعلومات السرِّية الخصوصية المرتبِطة بطرف واحد فقط، وهو الشخص المُرخَّص له بقراءتها واستعمالها، ومن أمثلة هذا النوع: أرقام الحسابات المصرفية، وكلمات السر الخاصة بالبريد الإلكتروني الشخصي، والمذكرات اليومية...
- معلومات سرِّية جماعية (مُشترَكة) Shared Secret Information: وهي المعلومات السرِّية المتعلِّقة بأكثر من طرف واحد، ومن صفاتها أنها مفهومة ومُشترَكة بين شخصين أو أكثر، ولكنها مع ذلك تُعدّ سرِّية على بقية الأطراف غير المَعنية وغير المَرخَّص لهم بقراءتها واستعمالها، ومن أمثلة هذا النوع: المراسلات التي تَتم على مستوى الحكومات، كالمراسلات الدبلوماسية، أو العسكرية، أو الأمنية، أو الاستخباراتية، والمراسلات التي تَتم على مستوى المنظمات والشركات، كالصفقات السرِّية التجارية المتبادَلة، إضافة إلى تلك التي تَتم على مستوى الأفراد، كالرسائل العائلية الخاصة، وغير ذلك.

---

(1) (التعمية واستخراج المعمى عند العرب)، مراياتي ومير علم والطيان، الجزء الأول، منشورات مجمع اللغة العربية بدمشق.

وبالنسبة إلى الوجهة (المكان المقصود) التي ستَستَقر فيها المعلومات السرِّية بعد تعميتها، فثمة خياران: إمّا تخزينها Storing (أو إبقاءها) على القرص لحين استرجاعها واستعمالها لاحقًا، مثل المعلومات السرِّية الفردية، أو إعدادها للإرسال عبر الشبكة، مثل المعلومات السرِّية الجماعية التي غالبًا ما تكون مُضمَّنة في رسائل البريد الإلكتروني.

تُسمَّى المعلومات السرِّية التي نُريد حمايتها (تعميتها) **النص الواضح** Plaintext، وتُسمَّى أيضًا **النص الصافي** Cleartext، وتقنيًّا يُشير مصطلح النص الواضح إلى أيّ بيانات نصية مكتوبة بمحارف[1] ASCII القياسية مثلًا، وهي قابلة للقراءة والفهم، وتَضم حروف الأبجدية الإنجليزية (الصغيرة والكبيرة) والأرقام والإشارات والرموز وبعض محارف التحكُّم، مثل المحرف tab، ومحرف بداية السطر الجديد، وذلك في أغلب برامج تحرير النصوص العادية وتطبيقاتها، مثل برنامج Notepad في نظام Windows[2]. أمّا في علم التعمية، فتُطلِق مصطلح (النص الواضح) على كل ما نُريد حمايته، فقد يكون النص الواضح في التعبير التعموي عبارة عن رسالة جهّزها طرفٌ ما، تحوي معلومات نصية فقط مقروءة ومفهومة وذات دلالة، ومكتوبة بحروف اللغة الطبيعية (الأبجدية)، وهي مُعدَّة وجاهزة للإرسال عبر الشبكة ليتلقَّاها طرف ثانٍ، وكما ذكرنا سابقًا، تَندرِج الرسالة التي تحوي معلومات سرِّية تحت سقف المعلومات السرِّية الجماعية، وغالبًا ما يكون محتواها أمورًا تَتعلَّق بإرشادات دبلوماسية أو صفقات تجارية أو علاقات عائلية أو أي شيء خاص ومُشترَك بين طرفين أو أكثر، وقد يكون النص الواضح (الذي نَرغَب في تعميته) أيضًا عبارة عن ملف File؛ ملف نصي txt مثلًا، أو ملف صورة bmp، أو

---

(1) يَختلِف مصطلح محرف character عن مصطلح حرف letter. فالمحرف يمكن أن يُمثِّل حرفًا letter أو رقمًا numeral أو رمزًا symbol أو محرف تَحكُّم control character، أمّا الحرف فهو جزء من أبجدية منتهية ومحدودة، مثل الأبجدية الإنجليزية. ويمكننا أن نُسمِّي الحرف محرفًا، لكن لا نستطيع تسمية المحرف حرفًا؛ لأن مجموعة المحارف أوسع، وهي تشمل مجموعة الحروف.

(2) من الآن فصاعدًا سيَقتصِر استخدامنا لمصطلح النص الواضح plaintext ليعني كل ما نُريد حمايته من البيانات، سواء أكانت مقروءة أم غير مقروءة.

ملف صوتي mp3، أو ملف فيديوي avi، أو ملف تنفيذي exe، أو حتى سلسلة من الخانات الاثنانية (البتَّات bits)، وبتعبيرٍ آخر ملف اثنانيّ binary file. وسواء أكانت المعلومات أو محتويات الملف المُراد حمايته وتعميته مقروءة (حروف أبجدية مفهومة) أم غير مقروءة (محارف عشوائية مثلًا) يُطلَق عليها وعلى الملف بأكمله مصطلح النص الواضح، وفي رياضيات التعمية يُعرَّف النص الواضح بأنه دَخْل تابع التعمية وخَرْج تابع فك التعمية، وفيما يَتعلَّق بوجهة الملف المُعمَّى، يَبقى الخيار متاحًا بين تخزينه على وسائط التخزين الرقمية المختلفة أو إرساله عبر الشبكة إلى طرف آخر.

إذًا، يُطلَق مصطلح النص الواضح plaintext في التعبير التعموي على كل ما نُريد حمايته من المعلومات السرِّية الموجودة في الحاسوب، سواء أكانت نص رسالة أم ملفًّا اثنانيًّا[1]. وعلى كُلٍّ، يُعبَّر عن النص الواضح في التعمية التطبيقية بالبتَّات فقط سواء أكان رسالة نصية أم ملفًّا اثنانيًّا.

أمّا المعلومات السرِّية التي تمَّ تحويلها (تعميتها) إلى الشكل الطِّلسمي العشوائي غير المفهوم فتُدعَى **النص المُعمَّى** Ciphertext، ونقصد بعبارتنا إلى شكل غير مفهوم أنَّ المعلومات لا يمكن قراءتها، وليس لها دلالة أو معنى إن كانت نص رسالة، ولا يمكن مشاهدتها إن كانت ملف صورة، ولا يمكن سماعها إن كانت ملفًّا صوتيًّا، ولا يمكن تنفيذها إن كانت ملفًّا تنفيذيًّا، أو بتعبيرٍ آخر، لا يمكن استعمالها بالشكل الذي هي عليه، ولن يَتمّ تمييز نوعية النص المُعمَّى ومضمونه بعد التعمية، سواء أكان رسالة نصية أم ملفًّا اثنانيًّا؛ لأنه في الحالتين عبارة عن محارف ورموز مركَّبة عشوائيًّا، وعلينا أن نُميِّز بين ملف مُعمَّى Encrypted file وملف اثناني Binary file، فقد لا يكون للملف الاثناني امتداد، عندها يَتبادَر إلى الذهن أنه ملف مُعمَّى، وأنَّ محتوياته هي نص مُعمَّى بمجرَّد رؤية البيانات العشوائية الداخلية، وهذا غير صحيح؛ لأنَّه ليس كل ملف يحوي بيانات

(1) اصطلح مجمع اللغة العربية بدمشق على هذا المصطلح (اثاني) لكلمة Binary لتمييزها عن (ثنائي).

عشوائية غير مفهومة هو ملفًّا مُعمَّى، فقد يكون هذا الملف إمّا ملفًّا مضغوطًا أو حتى ملفًّا اثنانيًّا، إلا إذا تمَّ التأكد من أنَّ محتوياته هي نص مُعمَّى فعلًا، وأنها ناتج تعموي عن خوارزمية ما، ونَستطيع أن نَعدّ النص المُعمَّى بمنزلة بيانات؛ لأنه يحتوي ضمنيًّا على معلومات نَستفيد منها بمجرَّد فك تعميته، وأيضًا يُعرَّف النص المُعمَّى رياضيًّا بأنه دَخْل تابع فك التعمية وخَرْج تابع التعمية.

يمكن استخدام المصطلح Cryptogram، الذي يَعني **رسالة مُعمَّاة**، بوصفه مُرادِفًا لمصطلح Ciphertext فقط في حال كان مضمون الناتج التعموي مجرَّد رسالة نصية عادية[1]؛ أي لا نستطيع أن نُطلِقه على ملف مُعمَّى، وبمجمل الأحوال، نُطلِق مصطلح النص المُعمَّى Ciphertext على كل ما هو ناتج تعمية، سواء أكان في الأصل رسالة نصية أم ملفًّا اثنانيًّا؛ لأنَّ كلًّا من النص الواضح والنص المُعمَّى في النهاية عبارة عن بتّات في التعمية التطبيقية.

تُدعَى الخطة أو الطريقة التي تَقوم بتحويل النص الواضح إلى نص مُعمَّى ثم تحويله (استرجاعه أو إعادته) إلى النص الواضح مرةً أخرى **المُعمِّي**[2] Cipher (وتُكتَب أيضًا Cypher)، والمُعمِّي هو في الحقيقة مجموعة محدَّدة من الخطوات (أو خوارزمية، ولذا يُعرَّف في معظم الأحيان **بخوارزمية التعمية** Cryptographic Algorithm، ويُعرَّف في أحيان أخرى **بخطة التعمية** Cryptographic Scheme) تَعمَل وفق آلية معيَّنة ومنهج دقيق، ويَستعمِل المُعمِّي المفتاح والنص الواضح عند عملية التعمية لإنتاج النص المُعمَّى، ويَستعمِل المفتاح والنص المُعمَّى عند عملية فك التعمية لاستخراج النص الواضح، ويجب أن يَضمَن المُعمِّي استعادة المعلومات الأصلية كما كانت (قبل تعميتها)

---

(1) حتى لو كانت الرسالة موجودة في ملف نصي txt لا يمكن تسمية الملف المُعمَّى الناتج بـ cryptogram.

(2) يجب التمييز بين كلمة (مُعمِّي) المقابلة لمصطلح cipher و(مُعمِّي) المقابلة لمصطلح cryptographer.

دون تغيير، ولو على مستوى حرف واحد (أو بت واحد). ورياضيًّا، يُعرَّف المُعمِّي بأنه الخوارزمية الرياضية mathematical algorithm المُستخدَمة للتعمية وفك التعمية.

جاءَت كلمة (Cipher) من كلمة عربية الأصل هي (الصفر)، وكانت تُستخدَم عادةً في اللغات الأوروبية، في القرون الوسطى بعد انتقال مفهوم الصفر العربي إلى هناك، للإشارة إلى شيء غامِض وغير مفهوم؛ لأن مفهوم الصفر كان غامضًا لهم بالمقارنة مع الترقيم الروماني السائد في تلك الحقبة، ففي القرون الوسطى بأوروبا، عندما أراد الناس التعبير عن أمرٍ مُبهَم كاللغز، كانوا يدعونه Cipher.

من أهم مكوِّنات النظام التعموي الأساسية **المفتاح** Key[1] (وهو اختصارًا لعبارة **المفتاح التعموي** Cryptographic Key). والمفتاح هو وحدة البيانات التي تَتحكَّم في ناتج التعمية في كل مرة يتم تغييره (وهذا أمر ضروري)، وعلى الرغم من أن المفتاح وحدة من البيانات، يُصنَّف في باب المعلومات (كالنص الواضح) وليس في باب البيانات مع أنَّ حروفه عشوائية في بعض الأحيان، والسبب في ذلك التصنيف أنَّ المفتاح هو الوسيلة الوحيدة لاسترجاع المعلومات بعد تعميتها، وهو يُعَدّ من المعلومات السرِّية التي يجب حمايتها، وكما ذُكِر سابقًا، فالمفتاح هو الجزء المُستخدَم مع النص الواضح لإنتاج النص المُعمَّى، والمُستخدَم مع النص المُعمَّى لاستعادة النص الواضح، وذلك في طَوْر عمليتين عكسيتين: الأولى تُدعَى التعمية، والثانية تُدعَى فك التعمية.

يمكن أن يكون المفتاح كلمة، وتُسمَّى عندها كلمة المرور أو كلمة السر Password، أو عبارة، وتُسمَّى عبارة المرور Passphrase، أو مجموعة من الأرقام، وبالنسبة إلى صيغة المفتاح (أو بيانات المفتاح) فقد تكون مَقروءة ومفهومة وواضحة، مثل الكلمات العادية البسيطة التي يَختارها المستخدِم ليَسهُل عليه حفظها، وتَتألَّف تلك الكلمات عادةً من

(1) في الحقيقة، فضاء المفتاح هو أحد مكوِّنات نظام التعمية، وليس المفتاح الواحد، إذْ إنَّ المفتاح الواحد هو جزء من ذلك الفضاء.

حروف أبجدية عادية، وأحيانًا مزيج من الحروف والأرقام، وفي بعض الأوقات تُصبِح طويلة لغرض زيادة السرِّية، وقد تكون صيغة المفتاح غير مفهومة وغير واضحة، مثل السلاسل المحرفية المركَّبة بشكل عشوائي من الحروف والأرقام والرموز، ولكنها مع ذلك قابلة للطباعة، ولكل خطة تعمية **طول مفتاح** Key Length ثابت يُدعَى أحيانًا **حجم المفتاح** أو طوله Key Size. في الواقع، لا تَعدّ خطة التعمية كلمةَ المرورِ أو عبارةَ المرورِ على أنها مفتاح التعمية وفك التعمية النهائي.

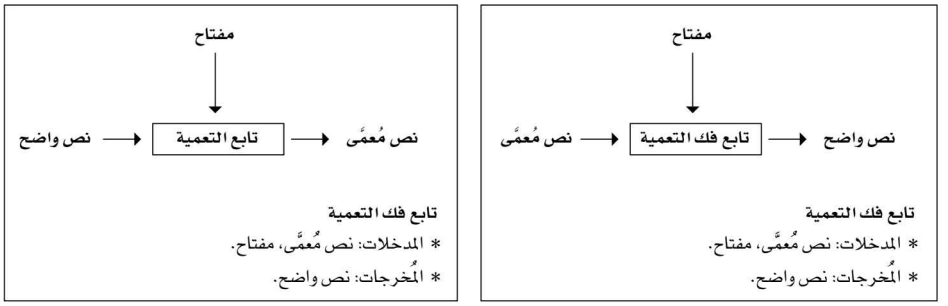
وبتعبيرٍ آخر، لا تَستعمِل خوارزمية التعمية السلاسل المحرفية المتغيِّرة الطول التي يُدخِلها المستخدِم مباشرةً، إنَّما تَقوم بإجراء عدد من العمليات عليها (كتوسيعها مثلًا) من أجل توليد بتّات المفتاح النهائي المستعمَلة لتنفيذ عملية التعمية وفك التعمية، وطول تلك البتات هو طول المفتاح الثابت، ويُسمَّى مجموع تلك العمليات عملية توليد المفتاح، ويَتم تنفيذها قبل تنفيذ عملية التعمية وفك التعمية، ورياضيًّا يُعرَّف المفتاح بأنه دَخْل تابع التعمية وتابع فك التعمية.

عملية التعمية Encryption هي عملية تحويل النص الواضح إلى نص مُعمَّى، وهي الجزء الأول من خطة التعمية. أمّا **عملية فك التعمية** Decryption فهي العملية العكسية التي تَقوم بتحويل النص المُعمَّى إلى نص واضح، وهي الجزء الثاني والمُكمِّل لخطة التعمية. وعلى نحوٍ أدق، عملية التعمية هي التابع الرياضي المستخدَم لتعمية النص الواضح، ويُسمَّى **تابع التعمية** Encryption function، ومُدخَلات تابع التعمية هي النص الواضح والمفتاح، ومُخرجاته هي النص المُعمَّى فقط.

أمّا عملية فك التعمية فهي التابع الرياضي المستخدَم لفك تعمية النص المُعمَّى، ويُسمَّى **تابع فك التعمية** Decryption function، ومُدخَلاته هي النص المُعمَّى والمفتاح ومُخرَجاته هي النص الواضح فقط. يُبيِّن الشكل (1-1) عمليتَي التعمية وفك التعمية من المنظور الرياضي، ويَرتبِط تابع فك التعمية بتابع التعمية وفق طريقة رياضية، بحيث

يُنفِّذ بدقَّةٍ تامة عكس ما يقوم به تابع التعمية، وذلك ليَضمَن استعادة المعلومات الأصلية الواضحة كما كانت، ويُرادِف مصطَلحَي encryption وdecryption مصطلحان آخران هما Encipherment وDecipherment على التوالي.

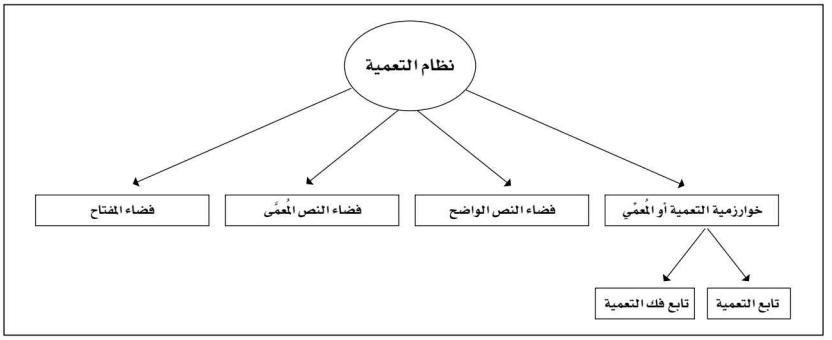
الشكل 1_1 عمليتَا التعمية وفك التعمية



يُشير المصطلحان **يُعمِّي**، و**يَفُك التعمية** إلى القيام بعمليتَي التعمية وفك التعمية، وثمة مصطلحان شائعان مرادفان يُؤدِّيان المعنى نفسه، هما Encipher وDecipher. تَستخدِم كتب التعمية ومراجعها زَوجَي المصطلحات السابقة بحسب الكاتب، والكتاب الذي يَستعمِل مصطلح (encrypt) ليَعني القيام بعملية التعمية يَستعمِل مصطلح (decrypt) ليَعني القيام بعملية فك التعمية، وكذلك هو الأمر بالنسبة إلى المصطلحين (encipher) و(decipher).

يَتكوَّن **نظام التعمية** Cryptosystem عمومًا من خوارزمية التعمية وإجمالي النصوص الواضحة والنصوص المُعمَّاة والمفاتيح الممكنة، ويُدعَى إجمالي النصوص الواضحة **فضاء النص الواضح** Plaintext Space، ويُدعَى إجمالي النصوص المُعمَّاة **فضاء النص المُعمَّى** Ciphertext Space، أمّا إجمالي المفاتيح الممكنة في المُعمِّي، فيُدعَى **فضاء المفتاح** Key Space، ويُقدِّم الشكل (1–2) صورة عن مُكوِّنات نظام التعمية.

الشكل (2_1) مخطط نظام التعمية.



بعد أن تَعرَّفنا إلى علم التعمية سنَتعرَّف الآن إلى علم (استخراج المعمى) كما سماه العرب واضعو هذا العلم[1] أو (تحليل التعمية) كما يسميه بعضهم الآن، **واستخراج المعمى** Cryptanalysis بالتعريف هو: **فَن وعلم اختراق حماية المعلومات السرِّية**، وبالتعريف العلمي **تحليل التعمية هو فك تعمية المعلومات السرِّية وتحويلها من الشكل العشوائي غير المفهوم إلى الشكل الواضح المقروء والمفهوم دون أي استخدام للمفتاح**، ويُمارِس هذا العلم مستخرج **التعمية** Cryptanalyst أو **مُحلِّلها**، وهو عادةً خبير في اللغة التي كُتِب بها النص الواضح، وفي الرياضيات التي تُعدّ الخبرة بها حاليًّا أكثر أهمية من اللغة بسبب تطبيق طرق التعمية المعقدة رياضيًّا.

إذًا، استخراج المعمى أو تحليل التعمية هو محاولة مُتعمَّدة لاستخراج النص الواضح من النص المُعمَّى دون امتلاك أو حتى معرفة بسيطة بالمفتاح الذي استُعمِل في تعميته، وتَتضمَّن المحاولة استخدام تقنيات عدة من أجل الوصول إلى الهدف المنشود، ويُشار إلى تلك المحاولة الموجَّهة في تحليل التعمية **بالهجوم** Attack، وثمة كثير من الأساليب والطرق لاسترجاع النصوص الواضحة، منها مثلًا كَشْف المفتاح المستخدَم،

---

(1) انظر: (علم التعمية واستخراج المعمى عند العرب) الجزءان الأول والثاني، منشورات مجمع اللغة العربية بدمشق، وترجمتهما للإنجليزية، منشورات مركز الملك فيصل للدراسات والبحوث الإسلامية.

أو إيجاد الحل العام، وقد يَتمّ الهجوم إمّا على نص مُعمَّى واحد فقط لاستعادة النص الواضح المقابل له أو على خطة التعمية المستخدَمة ككل؛ وذلك لاستعادة أي نص واضح، والمهمة الأصعب في الهجوم على خطة التعمية هي استنباط نقاط الضعف الموجودة بها واستغلالها في إيجاد طريقة عامة (الحل العام) لمعرفة المفتاح واستعادة النصوص الواضحة (أو استعادة النصوص الواضحة فقط دون الاهتمام بمعرفة المفتاح) بسهولة متى تَوافرت نصوص مُعمَّاة. أمّا حالة فقدان المفتاح من خلال حادثة لا تَتعلَّق أبدًا بتحليل التعمية (كإهماله أو إضاعته مثلًا) فتُدعَى **الافتضاح** Compromise.

بَقي علينا أن نُشير إلى وجود الفرق بين فك تعمية النص المُعمَّى وتحليل تعميته، فمن خلال فك تعمية النص المُعمَّى نَستعيد النص الواضح بواسطة استخدام المفتاح. أمّا من خلال استخراج تعميته فنَستعيد النص الواضح دون أي استعمال للمفتاح.

يُعرَف مصطلح تحليل التعمية أيضًا **باختراق المُعمِّي** Breaking a cipher، ويُطلِق الكثيرون في هذه الأيام مصطلحًا عاميًّا شائعًا يُفيد معنى تحليل التعمية هو (كسر الشيفرة). أمّا علماؤنا العرب الذين اشتغلوا بهذا المجال فقد أَطلَقوا تسميات عدة تُرادِف مصطلح تحليل التعمية، مثل (استخراج المُعمَّى) و(فك المُعمَّى) و(حل الترجمة) و(حل التعمية).

علم التعمية واستخراجها Cryptology **هو العلم الذي يَضُم كلًّا من علم التعمية وعلم تحليل التعمية.** جَوهَر هذا العلم هو الدراسة المشتركة للتعمية وتحليلها، ويُدعَى الشخص العامل في هذا المجال **خبير التعمية واستخراجها** Cryptologist. إنَّ عمل خبراء التعمية وتحليلها مُعقَّد جدًّا، حيث يقومون بتصميم خوارزميات وخطط التعمية، وفي الوقت نفسه يقومون بهجمات تحليلية عليها لاختبار قوتها والتأكد من حسن أدائها وسير عملها، وبكل تأكيد يَتطلَّب ذلك منهم الخبرة الرياضية الكافية، وسوف تَجِد

بعضهم يَستعمِل مصطلح (cryptology) بوصفه مرادفًا لمصطلح (cryptography) في بعض الحالات، وهذا خاطئ.

إنَّ استخدام التعمية لحماية المعلومات السرِّية الفردية ضَيِّق ومحدود جدًّا، وهو يقتصِر فقط على تأمين الملفات المخزَّنة على القرص؛ لئلا يقوم شخص آخر باستعمال الحاسوب والاطلاع على تلك الملفات؛ لذا فإنَّ أهم ما تُقدِّمه التعمية (وتقنياتها بلا شك) هو حماية المعلومات السرِّية الجماعية المتمثِّلة في الرسائل المتبادلة بين الأطراف المعنية.

يُعرَّف **الطرف** Entity أو **المُشارِك** Party بأنه جزء الاتصال القائم بين أطراف عدة، ومَهمّة الطرف قد تكون إرسال المعلومات أو استقبالها أو السيطرة عليها، وقد يُمثِّل هذا الطرف شخصًا ما أو محطة طرفية حاسوبية (مخدِّم)، وعندما تكون ثمة رغبة لدى طرفٍ ما في إنشاء رسالة سرِّية وتجهيزها للإرسال عبر الشبكة (مثل الإنترنت) إلى طرفٍ آخر، تَتشكَّل **بيئة الاتصال** Communication Environment أو **محيط الاتصال**، وتَتألَّف بيئة الاتصال بشكل افتراضي من ثلاثة مُشارِكين وقناة تبادل (إرسال واستقبال)، والمُشارِك الأول من بيئة الاتصال هو **المُرسِل** Sender، ويُعرَّف بأنه الطرف الأول من الاتصال القائم بين طرفين، وهو المُرسِل الشرعي الحقيقي للرسالة. أمّا المُشارِك الثاني من بيئة الاتصال فهو **المُستقبِل** Receiver، ويُعرَّف بأنه الطرف الثاني من الاتصال القائم بين طرفين، وهو المُستقبِل الشرعي المَعني بالرسالة، والمُشارِك الثالث من بيئة الاتصال هو **الخصم** Adversary، ويُعرَّف بأنه الطرف الثالث من الاتصال القائم بين طرفين، وهو الطرف غير الشرعي بينهم (الشاذ).

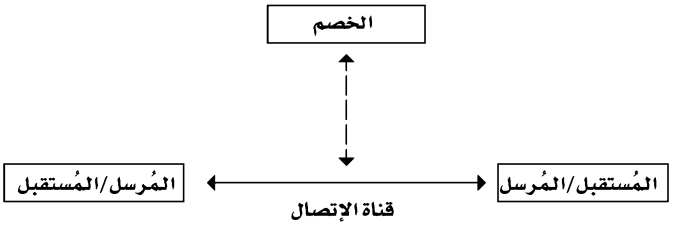
من الواضح أنَّ الخصم ليس المُرسِل أو المُستقبِل، إنّما هو دخيل لا علاقة له بالأصل في هذا الاتصال على خلاف المُرسِل والمُستقبِل، ويَقوم الخصم عادةً باختراق سرِّية (حماية) المعلومات المتبادَلة بين الطرفين الشرعيَين (المُرسِل والمُستقبِل)، وذلك من خلال أداء دور إمّا المُرسِل الشرعي أو المُستقبِل الشرعي أو كليهما، والهدف من قيامه بذلك هو قراءة الرسائل السرِّية المتبادَلة التي تَهمُّه، إضافة إلى التلاعب بهذه الرسائل

عن طريق تعديلها إمّا بإضافة معلومات مُزيَّفة أو بحذف معلومات محدَّدة أو تغيير بعض المعلومات، ويَتم كل هذا دون شك بعد أن يَتمكَّن الخصم من كَشْف مضمون الرسالة وقراءتها، ويُطلَق على الخصم تسميات عدة مرادفة، مثل **المهاجم** Attacker، و**المُعترِض** Interceptor، و**المُتطفِّل** Interloper، و**الدخيل** Intruder، و**المُناوِئ** Opponent، و**العدو** Enemy، و**المُتجسِّس** Tapper، و**المُتنصِّت أو المسترق** Eavesdropper.

أمّا **قناة التبادل** أو **قناة الاتصال** Communication Channel (واختصارًا تُدعَى فقط **القناة** Channel) فهي الوسيلة التي يَتم عبرها نَقْل المعلومات والرسائل من طرف إلى آخر، وتُشكِّل مجموعة قنوات الاتصال **الشبكة** Network. إنَّ أكبر وأشهر شبكة قنوات اتصال معروفة حاليًّا هي شبكة الإنترنت Internet، ولا تَفترِض التعمية أن تكون قناة الاتصال آمنة؛ لذا فهي تَعمَل، وتُؤدِّي دورها وفق ظروف القناة غير الآمنة، وإنَّ هذا الافتراض نابِع من افتراض المُرسِل والمُستقبِل الذي يَقضي بوجود الخصم في بيئة الاتصال التي يُشكِّلانها، حتى لو لم يكن هناك أصلًا.

في الشكل (1–3)، كَوْن قناة الاتصال تُعدّ قناة تبادل، فإنَّ المُرسِل هو مُستقبِل أحيانًا، والمُستقبِل هو مُرسِل أحيانًا، ولذا يَدُل الخط ذو الاتجاهين الواصل بين المُرسِل والمُستقبِل على ذلك، ويُشير الخط المنقَّط الذي يَصِل بين الخصم وقناة الاتصال إلى أنَّ الخصم هو طرف دخيل غير شرعي في قناة الاتصال. أمّا الاتجاهان المتعاكسان لهذا الخط المنقَّط فيَدُلّان على افتراض أنَّ الخصم يستطيع قراءة المعلومات المتبادَلة بين المُرسِل والمُستقبِل، وفي الوقت نفسه يستطيع التأثير فيها من خلال تعديلها.

الشكل (3_1) مخطط بيئة الاتصال الافتراضي



الفصل الثاني

تعاظم أهمية أمن المعلومات[1]

يستعرض هذا الفصل مشهدَ تعاظمِ أهميةِ أمن المعلومات وأمانها في الآونة الأخيرة، وتفاقمَ المهددات وكثرةَ الاختراقات وتواترها على كل الأصعدة، ويأتي على ذكر حالات عالمية مختلفة بوصفها أمثلة لذلك.

1.2 تطور المعلوماتية يرافقها تعاظم أخطار أمنها.

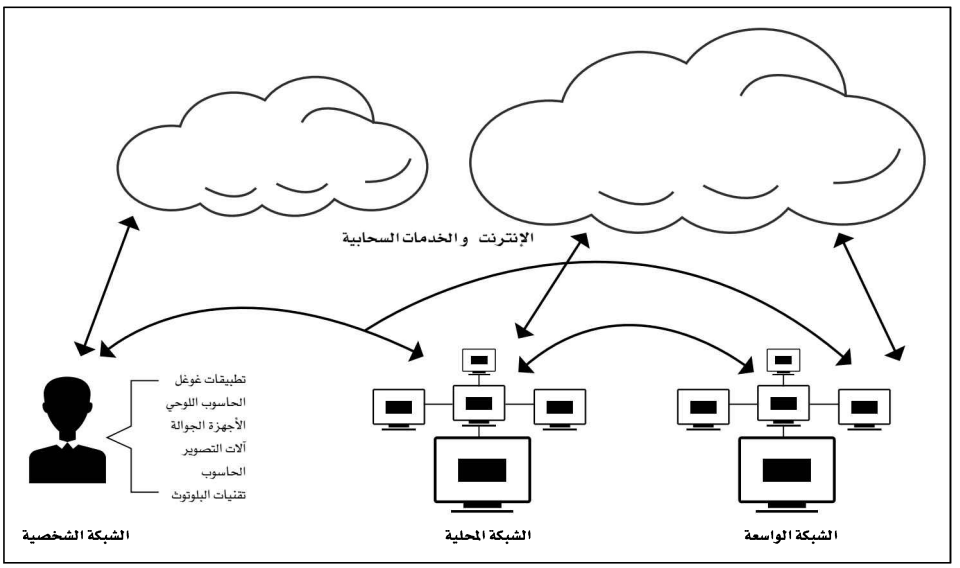
مع تطور الخدمات الإلكترونية، تطورت الأخطار والجرائم السايبرية (أو السيبرانية)، وظهرت طرق جديدة لارتكاب الجرائم في الفضاء السايبري أو السيبراني، وعلى المجتمع بأفراده ومؤسساته الاحتياط من وجود الجرائم السايبرية واتخاذ التدابير اللازمة لمواجهتها، فهي لن تتوقف، لا، بل ستتطور، وسيقع على عاتقنا اتخاذ الاحتياطات اللازمة في هذا المجال. لقد أصبح الفضاء السايبري واقعًا منذ منتصف

(1) اعتمدت الفقرات الأربع الأولى من هذا الفصل على تقرير اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا): الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية، توصيات سياساتية، 2015م.

التسعينيات، وأوجد بيئة جديدة تنتشر فيها الجرائم السايبرية، وقد عجزت القوانين الجزائية حتى الآن عن متابعة هذا التطور.

وظهرت تقنيات جديدة، مثل الصوت عبر الإنترنت (VoIP) Voice–over–IP، والحوسبة السحابية (انظر الشكل،Cloud Computing) التي يصعب معها تطبيق القانون التقليدي وإجراء التحقيقات القضائية؛ نظرًا لتشابكها وتعقيداتها، وأسهمت تقنيات الغفلية (تقنيات إخفاء الهوية الحقيقية للمستخدم) وتنامي تسويق البرامج المعلوماتية التي يستخدمها المخترقون في تطور الجرائم السايبرية، ولم يعد المخترقون يحتاجون إلى خبرات كبيرة؛ لأن برامج الاختراق أصبحت متوافرة وجاهزة، وقد أظهرت إحدى الدراسات أن (22%) فقط من الهجمات السايبرية معقدة، وتحتاج إلى محترفين.

نظام الأنظمة القادم في المعلومات والاتصالات (المعلوماتية)



Source: The Future of National and International Security on the Internet, Chapter 9, Maurice Dawson et al. 2014.

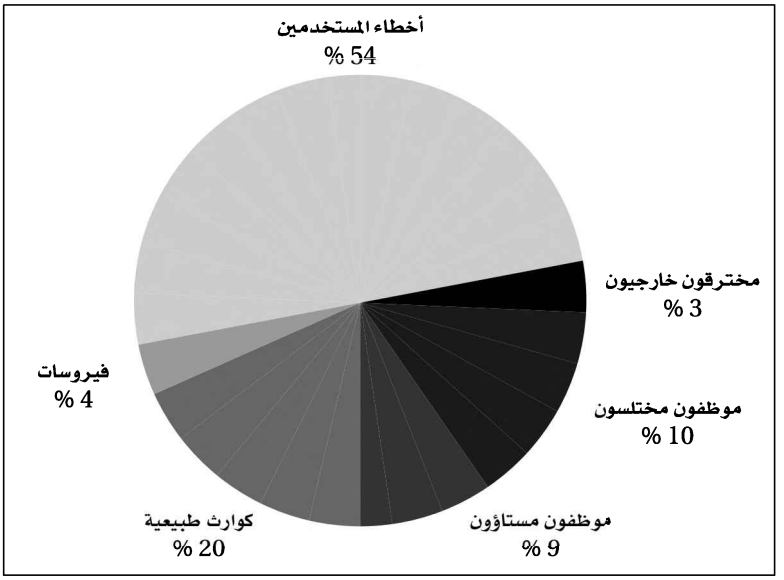
لقد بدأت الحكومات والشركات تعي تدريجيًّا أخطار الجرائم السايبرية وأهمية الأمن السايبري على الأمن الاقتصادي والسياسي للبلد وعلى مصالح العامة، وتبدو

الإنترنت جنة لمخترقي الشبكات بسبب ظهورهم عليها ظهورًا افتراضيًّا مُغْفَلًا دون اسم، وقد بات هؤلاء يعون ارتفاع عوائد الجرائم السايبرية، وتدني أخطار ونسب اكتشافها، وصعوبة إثباتها في بعض الدول، وبالفعل يتأتى عن الجرائم السايبرية خسائر مالية قد تكون مباشرة أو غير مباشرة، وهي خسائر فادحة تلحق بالأفراد والاقتصاد على حد سواء، فعلى سبيل المثال جرى عام 2012م تقدير قيمة الأضرار الناشئة عن الجرائم السايبرية في أستراليا، وكانت قرابة (2) مليار دولار.

وتظهر الدراسات أن نسبة مستخدمي الإنترنت الذين يقعون ضحايا الجرائم السايبرية تتراوح ما بين (1. 17%)، وهذه النسبة تزداد في الدول الأقل نموًّا، ووفق دراسة للأمم المتحدة، أكد مسؤولو تطبيق القانون في دول آسيا، في مسح صدر أوائل عام 2014م، أن الجرائم السايبرية في ازدياد، وبدرجات تتفاوت، وأن أخطار الجرائم السايبرية في مؤسساتهم قد ازدادت في الأشهر الأربعة والعشرين الماضية، ويبدي (44%) من المستخدمين في دول منطقة الشرق الأوسط وشمال إفريقيا مخاوف كبيرة من تعرض حسابات بريدهم الإلكتروني أو غيره من الحسابات على الإنترنت للاختراق، وهذه النسبة أعلى قليلًا مما هي عليه في العالم عمومًا، وهي (41%).

ويبدو أن الغالبية العظمى من الجرائم السايبرية في دول المنطقة العربية هي تلك التي تكون المعلوماتية فيها وسيلة ارتكاب الجريمة، وليس محلها، فوفق إحدى الدراسات عام 2011م، احتلت دولة الإمارات العربية المتحدة المرتبة (19) عالميًّا، في حين جاء لبنان في المرتبة (25) عالميًّا من حيث ترتيب الدول التي تتعرض لهجمات سيبرانية، وفي لبنان تحديدًا، لا تتجاوز جرائم التعدي على الأنظمة والبيانات (5%) من المجموع، في حين أن (95%) منها هي جرائم تقليدية بوسيلة معلوماتية، مثل الاحتيال والقدح، وكذلك في السودان، حيث لا تتجاوز نسبة جرائم التعدي على الأنظمة والبيانات (8%)، في حين تزيد نسبة جرائم شبكات التواصل الاجتماعي على (70%).

مثال حول تهديدات نظم المعلومات في بعض الأوساط:



المصدر: وزارة التربية والتعليم، عُمان.

في منطقة الشرق الأوسط، ومن خلال استطلاع قامت به شركة (PWC) عام 2014م، يعتقد (48%)، أن أخطار الجرائم السايبرية في مؤسساتهم قد ازدادت خلال العامين السابقين.

2.2 ارتفاع معدلات الجرائم السايبرية في دول منطقة الشرق الأوسط

ارتفعت نسبة الجرائم السايبرية في دول منطقة الشرق الأوسط، فعلى سبيل المثال، قد ارتفع معدل الجريمة الإلكترونية في دولة الإمارات العربية المتحدة بنسبة (25%) عام 2013م مقارنة بعام 2012م، وقد ارتفع معدل الجريمة السايبرية في كثير من الدول العربية بين عامي 2012 و2013 مثلًا، وتصدرت قضايا الاحتيال والابتزاز بهدف الحصول على المال ولأهداف غير الأخلاقية قائمة الجرائم المرتكبة، وذلك بحسب إحصاءات صادرة عن شرطة دبي، وقد ورد عن الإدارة العامة للتحريات والبحث الجنائي

أن «البلاغات ترد من كلا الجنسين ومن أعمار مختلفة، وتتركز بالنسبة إلى النساء على مواقع الزواج الإلكترونية، حيث يستغل الجاني إقبال الإناث من مختلف الأعمار على هذه المواقع لأغراض متعددة»، وارتفعت الجرائم السايبرية في دولة الكويت عام 2012م من (563) قضية إلى (997) قضية عام 2013م، وازداد عدد الجرائم السايبرية المبلغ عنها في سلطنة عُمان لدى سلطة التحقيق من أقل من (200) في نهاية عام 2011م إلى أكثر من (800) قضية في نهاية عام 2013م.

ومن صفات الجرائم السايبرية السرعة التي تتم بها، إذ قد تحدث الأضرار حتى قبل أن تعي الضحية باستهدافها، وهو ما قد لا يتيح للضحية الدفاع عن نفسها، ويقدر عدد ضحايا الجرائم السايبرية بنحو (559) مليون ضحية في العام، أو أكثر من (1,5) مليون ضحية في اليوم، وتشير بعض الإحصاءات إلى أن (72%) من مستخدمي الإنترنت من الرجال يقعون ضحية هذه الجرائم مقابل (65%) من مستخدمي الإنترنت من النساء، وتدل هذه الإحصاءات على أن الرجال هم عرضة لجرائم الإنترنت أكثر من النساء، وخاصة الفئة العمرية ما بين (18 إلى 31) سنة، ويرجع ذلك إلى استخدامهم للإنترنت مددًا زمنية أطول، ولجرأتهم بالدخول إلى مواقع مختلفة، وانخراطهم في سلوك محفوف بالأخطار عبر الإنترنت ما يعرضهم أكثر للاحتيال والسرقات والبرمجيات الخبيثة.

ويلاحظ ارتفاع الجرائم السايبرية ضد المرأة، وخاصة تلك التي تتعلق بالعنف ضدها، حيث إن (95%) من السلوك العدواني على الإنترنت كالتحرش، والمطاردة، واللغة المسيئة، والصور المهينة هي موجهة ضد النساء، وعادة ما تصدر من الشريك أو من شريك سابق، وفي دراسة حديثة أجراها الاتحاد الأوروبي عام 2014م، يظهر أن (4%) من النساء ما بين سن (18 و29) عامًا قد عانين خلال السنة السابقة ملاحقة عبر الفضاء السايبري (Cyberstalking) في حين أن (11%) من النساء اللواتي تمت مقابلتهن لغرض الدراسة، وهن في عمر (15) سنة فما فوق، قد تلقين نوعًا من الرسائل غير المرغوب فيها، كالرسائل الجنسية الهجومية عبر البريد الإلكتروني أو الرسائل

النصية (SMS)، أو التحرش غير اللائق عبر شبكات التواصل الاجتماعي، وتبقى الولايات المتحدة الأمريكية البلد الأول المنتج للبريد الواغل (أو غير المرغوب فيه)، ويقدر أن البريد الواغل قد استهلك عام 2012م قرابة (70%) من مجمل حركة البيانات على الإنترنت.

ويُعدّ مكتب التحقيقات الفيدرالي في الولايات المتحدة الأمريكية جرائم تكنولوجيا المعلومات من أهم الجرائم التي تواجهها الولايات المتحدة، ويعتقد نحو (60%) من أصحاب الأعمال في الولايات المتحدة أن الضرر اللاحق بهم من جراء الجرائم السايبرية يفوق الضرر الناجم عن الجرائم العادية، وأكد تقرير صادر عن الأوروبول عام 2011م حول تقييم أخطار الجريمة المنظمة أن تكنولوجيا الإنترنت أصبحت عاملًا أساسيًّا لتسهيل معظم أنشطة الجريمة المنظمة.

وهكذا لا بد من التساؤل عما إذا كانت هذه الوسيلة الجديدة للتواصل؛ أي الإنترنت، تعطي نتائج إيجابية أم أن عيوبها تفوق إمكاناتها، والجواب عن هذا السؤال رهن بنجاعة التدابير المتخذة في كل دولة لضمان الأمن والأمان السايبري.

3.2 التمييز بين تنظيم السلوك، والجرائم، والأمن في الفضاء السايبري

قد لا تكون جميع الاعتداءات في الفضاء السايبري مُجَرَّمَةً في القانون الجزائي في بعض الدول، وذلك على الرغم من الأضرار التي قد تنشأ عنها، وفي هذه الحالة، تُعدّ المضايقات والهجمات الإلكترونية سلوكًا غير ملائم يتطلب قواعد وخططًا لتنظيم السلوك في الفضاء السايبري، وعندها يجري التركيز على الأخطار العريضة الشخصية والاجتماعية الناتجة عن استعمال الحاسوب.

أما عندما تكون هذه الأفعال مُجَرَّمَةً جزائيًّا، فتُعدّ هذه الهجمات والمضايقات السايبرية جرائم سيبرانية، وتتطلب خطة وطنية ضمن إستراتيجية للأمن السايبري،

حيث يجري إعداد خطة لفضاء سيبراني آمن وموثوق وتنفيذها، بحيث تكون الدولة قادرة على مجابهة الهجمات على البيانات والأنظمة، ولا سيما الهجمات التي تطول البنية الأساسية الحساسة والأنظمة المعلوماتية للأمن القومي.

ويمكن القول: إن العمل على توفير الأمن والأمان وتنظيم السلوك في الفضاء السايبري يسهم حكمًا في مجابهة الجرائم السايبرية، ويؤكد الاتحاد الدولي للاتصالات في دراسة صادرة عنه أن وضع إستراتيجية لمكافحة الجرائم السايبرية هو عنصر لا يتجزأ من إستراتيجية الأمن السايبري.

4.2 الطابع الدولي للجرائم السايبرية

يُعدّ الطابع الدولي للجرائم السايبرية من أبرز الصفات التي تميزها، وهي بذلك تتحدى النظام القانوني المحلي والدولي، إذ يطغى في كثير من الأحيان الطابع الدولي على الجريمة السايبرية، فهي جريمة عابرة للحدود، وقد تتضمن أكثر من عنصر أجنبي، فالفعل الجرمي قد يحصل في بلد معين، وتتحقق النتيجة الجرمية في بلد آخر، مثل: حالة اختراق نظام معلوماتي عن بعد، وقد تتحقق النتيجة الجرمية في جميع البلدان، مثل: حالة نشر قدح وذم بحق شخص معين على موقع إلكتروني يمكن الوصول إليه من معظم دول العالم.

ولا تطول الجرائم السايبرية اليوم الأفراد فقط، بل أصبحت جرائم شاملة قد تأخذ شكل هجمات ضخمة منسقة تطول البنية الأساسية الحساسة للمعلومات في أكثر من دولة، أو شكل أنشطة إرهابية على الإنترنت، وعام 1998م، عمدت مجموعة الدول الصناعية الثماني التي هي أكثر تطورًا في العالم (G8) إلى إطلاق خطة عمل لمحاربة الجرائم السايبرية وإنشاء شبكة خبراء متاحة (7) أيام في الأسبوع على مدار (24) ساعة في اليوم؛ للمساعدة على التحقيقات المتعلقة بجرائم المعلوماتية، وكذلك تدريب أجهزة الأمن لدى تلك الدول وتجهيزهم.

5.2 مقتطفات من أخبار عالمية حول تعاظم أهمية أمن المعلومات وأمانها

19,7 مليار هجمة إلكترونية في العالم يوميًّا.

أعلن المركز الوطني للأمن الإلكتروني (الرياض) عن رصد محاولات هجوم إلكتروني تعرضت لها جهات حكومية ومحلية عدة عن طريق رسائل بريد إلكترونية لسرقة المعلومات، وكشفت شركة (سيسكو) العالمية عن تصديها لنحو 19,7 مليار هجمة إلكترونية يوميًّا في العالم، إضافة إلى افتقار العالم لأكثر من مليون مختص أمني في مجال الحماية الإلكترونية.

الاقتصادية، الثلاثاء 17 شعبان 1437هـ/ الموافق 24 مايو 2016م.

الهجمات الإلكترونية الخبيثة تتكاثر وتكبد الشركات 400 مليار دولار سنويًّا.

جيليان تيت من واشنطن.

بشكل عام، الهجمات الإلكترونية تتزايد بشكل كبير، وتكلف الشركات 400 مليار دولار سنويًّا، بحسب بيانات من (مايكروسوفت).

وقال توم بيرت، نائب المستشار العام في شركة (مايكروسوفت)، في مؤتمر نظمته (فاينانشيال تايمز) في واشنطن الأسبوع الماضي (مشيرًا إلى مشكلة تخلف التشريعات ضد الجرائم المعلوماتية): «لنفكر في حالة وجود شبكة برامج خبيثة في سنغافورة يديرها قراصنة في بلغاريا تسببوا في ضرر لشخص في أمريكا. من يملك السلطة القضائية؟ وما القوانين المستخدمة؟». «لا أحد يعرف، في الفضاء الإلكتروني، كما هي الحال في النظام المالي العالمي قبل عقد من الزمن، مجموعة كبيرة من النشاط الإجرامي في خطر أن يتم تجاهلها؛ لأن القواعد الوطنية غير مناسبة لعالم رقمي سريع النمو».

الاقتصادية، الأربعاء 13 رجب 1437هـ/ الموافق 20 إبريل 2016م.

مكتب أمن المعلومات الألماني ينصح بعدم دفع الفدى لقراصنة الكمبيوتر.

برلين – د ب أ.

هناك زيادة ملحوظة في نمط جديد من عمليات القرصنة والاحتيال عبر الإنترنت، حيث ينجح هؤلاء المحتالون في تهريب برامج إلى أجهزة الكمبيوتر الشخصي لضحاياهم تؤدي إلى تشفير الملفات الشخصية لهؤلاء الضحايا، ثم يطلبون منهم إرسال مال عبر خدمات تحويل أموال مجهولة مقابل استعادة الدخول على هذه الملفات.

ولكن مكتب أمن المعلومات الألماني ينصح الضحايا بعدم دفع أي أموال للمحتالين؛ لأنه حتى في حالة دفع الفدية لا يوجد ما يضمن للضحية استعادة الدخول على ملفاتهم.

والأفضل من وجهة نظر المكتب الاحتفاظ بنسخة احتياطية من هذه الملفات الشخصية المهمة على قرص صلب خارجي أو شريحة ذاكرة منفصلة بعيدًا عن جهاز الكمبيوتر، بحيث يمكن استرداد هذه الملفات في حالة تعرضها للسطو.

يُذكر أن برامج مكافحة الفيروسات تستطيع غالبًا التعرف إلى برامج التجسس التي تستهدف الحصول على فدية، لكنها لا تستطيع منع تشفير الملفات الشخصية. في الوقت نفسه، فإن الشخص الذي يقوم بعمل نسخة احتياطية من ملفاته المهمة بشكل منتظم يستطيع استعادة الحالة الأصلية للكمبيوتر الشخصي بسرعة معقولة بعد التعرض لعملية قرصنة.

صحيفة الرياض، الإثنين 24 ربيع الأول 1437هـ/ 4 يناير 2016م.

باحثون يخترقون شفرات نظام كمبيوتر كوريا الشمالية المضاد للتجسس.

ووفقًا لموقع independent البريطاني، تمكن مجموعة من الباحثين الدخول على هذا النظام والتعرف إلى تفاصيله الخفية، واكتشف مجموعة من الباحثين النظام السري الذي تعمل به أجهزة الكمبيوتر الخاصة بكوريا الشمالية، الذي تم تطويره من أجل الحفاظ على المعلومات المهمة بشكل سري ووقف تسريبها، وإبقاء الاتصالات مشفرة، وكانت منذ مدة قصيرة مجهولة للغاية، وهذا النظام يحمل اسم Red Star OS ويعتمد على برنامج

Linux وهو يبدو مشابهًا لنظام تشغيل Mac OS، ولكنه يحتوي على كل أنواع التكنولوجيا المتطورة التي تسمح لكوريا الشمالية بالسيطرة على طريقة استخدامه.

الاقتصادية، الأربعاء 19 ربيع الأول 1437هـ/ الموافق 30 ديسمبر 2015م.

الجريمة الإلكترونية... الإنترنت المنبر الأخطر للمتطرفين.

ابتزاز إلكتروني.

كشفت ختام بنت عاهد الشريدة ـ اختصاصية علوم الحاسب وأمن المعلومات بجامعة الأميرة نورة بنت عبدالرحمن ـ مشكلات الجرائم الإلكترونية قائلةً: أولًا: الاحتيال والجرائم المالية (Fraud and financial crimes): وتشمل مجموعة متنوعة من الاحتيال على الإنترنت، وذلك ما يسمى التَّصَيُّد (Phishing)، وكذلك الهندسة الاجتماعية (Social Engineering) التي تستهدف المستخدمين والشركات بشكل مباشر، ويشمل هذا النوع من الاحتيال ما يقوم به الموظفون الفاسدون في المؤسسات المالية من خلال إدخال بيانات خاطئة أو تعليمات غير مصرح بها، أو استخدام عمليات غير قانونية بهدف السرقة، وكذلك تعديل البيانات المخزنة أو حذفها، أو إساءة استخدام أدوات النظام الموجودة أو حزم البرامج أو كتابة شفرات برمجية لأغراض الاحتيال، مضيفةً أنه يأتي ثانيًا: الابتزاز الإلكتروني (Cyber extortion): ويكون ذلك بقطع الخدمة (DDOS) عن المواقع الإلكترونية وخوادم البريد الإلكتروني، أو نظم التشغيل للحاسبات، أو غيرها من هجمات القراصنة الخبيثة، ويكون هدفها الابتزاز المالي، وكذلك الإرهاب الإلكتروني (Cyber terrorism) وهي الاختراقات التي تشكل جهدًا منظمًا لإرهابيين إلكترونيين، أو وكالات مخابرات أجنبية، أو أي جماعات تسعى لاستغلال ثغرات أمنية محتملة في الأنظمة الحيوية، مبينةً أنه يأتي ثالثًا: الإرهابيون الإلكترونيون (Cyber terrorists): وهم الأشخاص الذين يدفعون حكومات أو منظمات لتلبية أهدافهم السياسية أو الاجتماعية من خلال إطلاق هجوم إلكتروني على أجهزة حواسيب وشبكات والمعلومات المخزنة عليها.

وأضافت: الحرب الإلكترونية (Cyber warfare) هي قائمة بالفعل بين كثير من الدول من خلال أجهزة الحاسوب وشبكات الإنترنت، ويعتقد محللون أن مثل هذا النوع من الهجمات قد يصبح القاعدة في الحروب المستقبلية بين الدول، حيث بدأت بعض الجيوش بتشكيل وحدات خاصة بالحروب، هدفها اختراق الدول الأخرى وتدمير بنيتها التحتية الإلكترونية، وربما يتم تكليف القادة العسكريين لقيادة مثل هذه الحروب مستقبلًا.

صحيفة الرياض، الأحد16 ربيع الأول 1437هـ/ 27 ديسمبر 2015م.

سرقة بيانات أربعة ملايين شخص بعد اختراق موقع (تولك تولك) البريطاني.

أعلنت شركة للاتصالات البريطانية (تولك تولك) أن بيانات عملائها في خطر بعد عملية القرصنة التي تعرض لها موقعها الإلكتروني الأربعاء الماضي.

الاقتصادية، الأحد 12 محرم 1437هـ/ الموافق 25 أكتوبر 2015م.

إجراءات عقابية لتعزيز أمن المعلومات في القطاع الخاص.

مراد أحمد وسام جونز ودنكن روبنسون من لندن وهانا كوتشلر وجينا كوهين من سان فرانسيسكو.

تعرضت الولايات المتحدة لهجمات قراصنة الكمبيوتر على نطاق أوسع بكثير، بدءًا من مجموعة متاجر التجزئة (تارجت) عام 2013م، التي فقدت سجلات 70 مليونًا من عملائها، إلى الهجوم المدمر على شركة أفلام سوني في العام الماضي.

تشهد تكلفة الهجمات الإلكترونية على الشركات تصاعدًا سريعًا، ووفقًا لمعهد بونيمون، وهو مجموعة أمريكية مختصة في بحوث الأمن الإلكتروني، ارتفعت التكلفة في المملكة المتحدة بنسبة 14 في المئة العام الماضي،

وتشير التقديرات إلى أن التكلفة على شركات الخدمات المالية ستصل إلى 8,5 مليون جنيه إسترليني لكل شركة هذا العام، أكثر من ضعف التكلفة البالغة ثلاثة ملايين جنيه

عام 2012م، ويتوقع أن تعاني شركات الطاقة والخدمات ارتفاعًا حادًّا، مع ارتفاع التكاليف لتصل إلى 6,5 مليون جنيه لكل مجموعة عام 2015م، مقارنة بـ 5,2 مليون جنيه العام الماضي.

غير أن الأثر المالي لشن هجمات على الشركات في المملكة المتحدة يختلف عن الأثر في الولايات المتحدة. وفقًا لمعهد بونيمون يكلف الاختراق العادي الشركة في المملكة المتحدة 6,3 مليون دولار؛ أي أقل من نصف المبلغ في الولايات المتحدة، البالغ 15 مليون دولار.

وبحسب تقرير صادر عن شركة برايس ووترهاوس كوبرز للخدمات المهنية، تعكف الشركات في جميع أنحاء العالم على تعزيز ميزانيات الأمن، مشيرًا إلى أنها زادت استثماراتها في هذا الجانب بنسبة 24 في المئة العام الماضي، وتحاول المصارف العمل معًا للتصدي لهذه المشكلة، وأنشأت لهذا الغرض (مركز تحليل وتبادل معلومات الخدمات المالية) الذي يتبادل البيانات المتعلقة بالتهديدات الأمنية، ولدى هذه الهيئة المختصة بالصناعة 5500 عضو، بما فيها بنك جيه بي مورجان تشيس، وسيتي جروب، وبنك ويلز فارجو، وإتش إس بي سي.

الاقتصادية، الإثنين 20 محرم 1437هـ/ الموافق 02 نوفمبر 2015م.

الفضاء الإلكتروني يعطي مفهومًا جديدًا للحرب.

عام 2014م، متوسط ما يسمى هجوم التهديد المتواصل استمر 205 أيام قبل أن يتم كشفه، وذلك وفقًا لشركة فايرآي للأمن الرقمي، وأكثر البلدان التي تعرضت للهجوم عام 2015م كانت الولايات المتحدة، وكوريا الجنوبية، واليابان، وكندا، والمملكة المتحدة وألمانيا، وقليل من الأشخاص في أوساط الدفاع الإلكتروني الغربي ترددوا في تحديد المجرمين الرئيسين: روسيا، والصين، مع إيران التي تلحق بسرعة.

يقول أحد كبار ضباط القيادة الإلكترونية العسكرية في الولايات المتحدة: إن واحدة من تكتيكات موسكو المفضلة هي تسليح عصابات الجريمة بأدوات قرصنة وبرمجيات خبيثة،

والتعاقد معها لتنفيذ عمليات ضد الخصوم، أو لحشد ما يسمى هجمات (العلم المزيف) لإرباك عمليات الإسناد.

ستيوارت بول روب، مسؤول الاستخبارات العسكرية السابق والرئيس التنفيذي حاليًّا لمجموعة استخبارات الأعمال KCS يقول: «إن التعقيد المتزايد لأدوات البرمجيات الخبيثة، والموارد المالية الكبيرة للدول التي تستخدمها، وانتشار العصابات الإجرامية المنظمة في هذا القطاع، يجعل من الصعب على نحو متزايد فهم مدى خطورة هذه القضايا تمامًا».

ويقول أحد كبار المسؤولين البريطانيين الذي هو على معرفة وثيقة بالقدرات الهجومية في المملكة المتحدة: «إن بإمكاننا إيقاف كل شيء في أي مكان نريده، لكننا لسنا في سبيلنا لفعل ذلك. جزء من المشكلة هو في معرفة الآثار التي تترتب على ذلك، وكيف سيستجيب الخصم، فلا أحد يريد حربًا فعلية».

الاقتصادية، الأربعاء 20 شوال 1436هـ/ الموافق 05 أغسطس 2015م.

قراصنة صينيون يستحوذون على معلومات حساسة عن موظفي «الاستخبارات الأمريكية».

كشفت مصادر أمريكية عن حصول قراصنة المعلوماتية على معلومات حساسة بينها تصاريح أمنية خاصة بالموظفين والمتعاقدين، إثر اختراق بيانات موظفين في الإدارة الأمريكية، بخلاف معلومات في غاية الخطورة عن موظفي وكالة الاستخبارات المركزية، وأشارت المصادر إلى أن المحققين يبحثون في هجومين إلكترونيين منفصلين، يعتقد بشكل كبير أن مصدرهما هو الصين، اخترقا سجلات الموظفين الحكوميين في قاعدة بيانات مكتب إدارة شؤون الموظفين.

وقال مسؤول أمريكي: إن قاعدة البيانات (حساسة جدًّا، وهي موصولة بجهات سيادية عدة»، في حين ذكر تقرير الصحيفة أن القاعدة ربما تحتوي على ملفات لبعض موظفي وكالة الاستخبارات المركزية، وكانت الإدارة الأمريكية قد أعلنت، الأسبوع الماضي، أنها

رصدت عمليات قرصنة معلوماتية طالت المعطيات الشخصية لأربعة ملايين موظف فيدرالي على الأقل، في هجوم إلكتروني ضخم يُشتبه بأن مصدره الصين.

الاقتصادية، الأحد 1436/8/27هـ/ الموافق 14 يونيو 2015م.

هجوم إلكتروني يستهدف مصلحة الضرائب الأمريكية.

واشنطن: أ. ف. ب.

اعترفت مصلحة الضرائب الأمريكية بأنها تعرضت لهجوم إلكتروني أسفر عن سرقة معطيات ضريبية تتعلق بنحو مئة ألف شخص، وقال مكتب الدخل الداخلي في بيان: إن القراصنة قاموا أولًا بجمع معلومات شخصية عن مكلفي الضرائب من طرف ثالث بينها تاريخ الميلاد والعنوان ورقم الضمان الاجتماعي، ثم استخدموا هذه المعطيات لدخول الخدمة الإلكترونية لمصلحة الضرائب، وأضاف البيان أنهم «حصلوا من مصدر خارجي على معلومات كافية لعبور عملية التعريف التي تتألف من مراحل عدة، بما في ذلك أسئلة التحقق من الهوية التي لا يمكن إلا لمكلف الضرائب الإجابة عنها»، وأوضح أن هذا الهجوم وقع بين شباط/ فبراير ومنتصف أيار/ مايو، مشيرًا إلى مئتي ألف اختراق سمح نصفها بسرقة معطيات.

ويأتي هذا الحادث في أوج تصاعد هجمات إلكترونية واسعة على شركات أمريكية كبرى بينها مصارف مهمة، يثير قلق البيت الأبيض.

الاقتصادية، الأربعاء 09 شعبان 1436هـ/ الموافق 27 مايو 2015م.

مخاوف من «حرب إلكترونية» تسير على خطى الحروب النووية.

في الشهر الماضي استضافت هولندا المؤتمر العالمي للفضاء السيبراني (الإلكتروني) لعام 2015م، الذي جمع ما يقرب من 2000 من المسؤولين الحكوميين والأكاديميين وممثلي الصناعات، وغيرهم. حيث تولى الباحث والكاتب الأمريكي جوزيف س. ناي الأستاذ في جامعة هارفارد، ومؤلف كتاب (هل انتهى القرن الأمريكي؟) رئاسة لجنة من المختصين لمناقشة الفضاء الإلكتروني والأمن، وقد ضمت اللجنة نائب رئيس شركة مايكروسوفت واثنين من الوزراء الأجانب.

وكان هذا المؤتمر الذي ضم أطرافًا متعددة من أصحاب المصلحة هو الأحدث في سلسلة من الجهود الرامية إلى إرساء قواعد الطريق من أجل تجنب الصراع السيبراني.

ويشير ناي في مقال له بعنوان (معايير دولية في الفضاء الإلكتروني) إلى أن القدرة على استخدام الإنترنت لإلحاق الضرر أصبحت الآن راسخة ثابتة.

ويضيف ناي: ثم ظهرت في أوائل التسعينيات الشبكة العنكبوتية العالمية، وتنامت من بضعة ملايين من المستخدمين آنذاك إلى أكثر من مليار مستخدم اليوم، وفي غضون ما يزيد على الجيل قليلًا، أصبحت شبكة الإنترنت الركيزة الأساسية للاقتصاد العالمي والحوكمة في مختلف أنحاء العالم.

وستضاف مليارات عدة أخرى من المستخدمين في العقود المقبلة، فضلًا على عشرات المليارات من الأجهزة (المتصلة بالإنترنت) التي تتراوح بين منظمات الحرارة إلى أنظمة التحكم الصناعية، وكل هذا الترابط المتعاظم يعني ضمنًا نشوء نقاط الضعف التي تستطيع الحكومات أو الجهات الفاعلة غير الحكومية استغلالها، وفي الوقت نفسه، بدأنا توًّا نتصالح مع العواقب المترتبة على ذلك فيما يتصل بالأمن الوطني، والواقع أن الدراسات الإستراتيجية للمجال السيبراني (الإلكتروني) تشبه الإستراتيجية النووية في الخمسينيات: فالتحليلات لا تزال غير واضحة حول معنى الهجوم، والدفاع، والردع، والتصعيد، والمعايير، والحد من التسلح.

ويُستَخدَم مصطلح (الحرب الإلكترونية) على نحو غير محكم على الإطلاق لوصف مجموعة واسعة من السلوكيات بدءًا من الاستطلاعات البسيطة وتشويه المواقع والحرمان من الخدمة إلى التجسس والتدمير، وهو في هذا يعكس تعريفات القواميس لكلمة (حرب) التي تشمل أي جهد منظم «لوقف أو إلحاق الهزيمة بشيء يُنظر إليه بوصفه خطرًا أو سيئًا» (على سبيل المثال الحرب على المخدرات).

وهناك أربع فئات رئيسة للتهديدات الإلكترونية للأمن الوطني، وكل منها تحتل مدة زمنية مختلفة، وتتطلب (من حيث المبدأ) حلولًا مختلفة: الحرب الإلكترونية والتجسس الاقتصادي، وهو ما يرتبط إلى حد كبير بالدول، وفئة الجريمة الإلكترونية والإرهاب

الإلكتروني، وهو ما يرتبط في الأغلب بجهات فاعلة غير تابعة لدولة، وتتبع أعلى التكاليف حاليًّا من التجسس والجرائم، ولكن الفئتين الأخريين ربما تصبحان أعظم تهديدًا على مدى العقد المقبل مقارنة بحالهما اليوم. وعلاوة على ذلك، مع تطور التحالفات والتكتيكات، ربما تتداخل الفئات بشكل متزايد.

ويختم ناي المقال مرجحًا أن يستغرق إبرام الاتفاقيات بشأن القضايا الخلافية مثل الاقتحام الإلكتروني لأغراض مثل التجسس وإعداد ساحة المعركة وقتًا أطول، وعلى الرغم من ذلك، فلا ينبغي لعدم القدرة على تصور اتفاقية شاملة للحد من التسلح الإلكتروني أن تمنع التقدم بشأن بعض القضايا الآن، فإن المعايير الدولية تميل إلى التطور ببطء، فقد استغرق الأمر عقدين من الزمان في حالة التكنولوجيا النووية، وكانت الرسالة الأكثر أهمية التي أبرزها المؤتمر الهولندي الأخير هي أن نقاط الضعف الإلكترونية الهائلة تقترب الآن من هذه النقطة.

الاقتصادية، الأحد 06 شعبان 1436هـ/ الموافق 24 مايو 2015م.

100 مصرف في العالم تتعرض لسرقات إلكترونية بمليار دولار.

تعرض أكثر من 100 مصرف ومؤسسة مالية في نحو 30 دولة إلى عمليات سطو إلكترونية (غير مسبوقة)، وقدرت شركة (كاسبرسكاي لاب) للأمن الإلكتروني حجم المسروقات خلال الهجمات التي بدأت منذ عام 2013م بنحو مليار دولار حتى الآن.

قال مركز تحليل الخدمات المالية وتبادل المعلومات، المسؤول عن تبليغ المصارف بأنشطة القرصنة الإلكترونية من جهته: إنه اطلع على تقرير (كاسبرسكاي لاب) منذ يناير الماضي، مؤكدًا أن المصارف بدأت في اتخاذ الإجراءات اللازمة لتجنب تلك الهجمات وحماية عملائها.

الاقتصادية، الثلاثاء 28 ربيع الثاني 1436هـ/ الموافق 17 فبراير 2015م.

العلوم والتقنية: 445 مليار دولار خسائر الهجمات الإلكترونية في العام الواحد.

إن تكلفة خسائر الهجمات الإلكترونية في العام الواحد قدرت بـ 445 مليار دولار عالميًّا، ومن المتوقع أن تتزايد فاتورة خسائر تلك الهجمات في المستقبل نتيجة التوسع في الخدمات الإلكترونية ودخول مفاهيم تقنية جديدة، وذلك يعزز الحاجة إلى تطوير جهود البحث العلمي في مجال أمن المعلومات لدعم المصالح الوطنية من خلال نقل وتوطين التقنيات وبناء القدرات وابتكار الخوارزميات الوطنية التي يمكن استخدامها بشكل آمن لحماية البيانات.

الاقتصادية، الأربعاء 21 جمادى الثاني 1437هـ/ الموافق 30 مارس 2016م.

فيروسات إلكترونية في محطة نووية ألمانية.

قالت الشركة المشغلة لمحطة الطاقة النووية في ألمانيا أمس الأول: إنه جرى اكتشاف أن المحطة التي تولد الكهرباء مصابة بفيروسات كمبيوتر، لكنها لا تشكل خطرًا على عمليات المنشأة؛ لأنها معزولة عن الإنترنت، وتدير شركة (آر. دبليو. إي) للمرافق محطة جوندريمينجن النووية التي تقع على بعد نحو 120 كيلومترًا شمال غرب ميونيخ، وقالت الشركة بحسب (سكاي نيوز): إن الفيروسات اكتشفت في الوحدة (ب) في المحطة في نظام للكمبيوتر جرى تعديله عام 2008م لإضافة برنامج لإظهار البيانات مرتبط بمعدات لنقل قضبان الوقود النووي.

واكتشفت أيضًا فيروسات في 18 محرك أقراص قابلًا للنزع في أجهزة كمبيوتر مكتبية تجري صيانتها بشكل مستقل عن أنظمة تشغيل المحطة.

الاقتصادية، الخميس 21 رجب 1437هـ/ الموافق 28 إبريل 2016م.

فيروسات تهاجم الهواتف الذكية تحت غطاء متاجر التطبيقات.

كثيرون هم المستخدمون الذين لا يقومون بتحميل التطبيقات على هواتفهم الذكية إلا إذا كان مصدرها متاجر التطبيقات الرسمية، مثل متجر أبل ومتجر جوجل بلاي؛ خوفًا

من أن تصيب هواتفهم إحدى البرمجيات الخبيثة أو برمجيات الفدية، لكن هذا الشيء لم يعد يكفي لحمايتهم، حيث بدأت البرمجيات الخبيثة وهجمات الفدية تلبس ثوب التطبيقات الرسمية في متاجر تطبيقات الهواتف الذكية والأجهزة اللوحية، وكشفت شركة Kaspersky لأمن المعلومات أن عدوى البرمجيات الخبيثة المستهدفة للأجهزة المتنقلة كانت هي الأكثر جدوى بالنسبة إلى مجرمي الإنترنت، حيث كانت تحدث عن طريق إحدى البرمجيات الخبيثة الموجودة في تطبيقات الأجهزة المتنقلة التي يتم تنزيلها من app- stores وكذلك من خلال وجود برمجية خبيثة في حزمة برامج أولية للهاتف، وذلك بسبب الإقبال المتزايد على خدمات الأجهزة المتنقلة في المنطقة، الذي أدى دورًا في جذب انتباه مجرمي الإنترنت الذين يقومون بتطوير أدواتهم بشكل مستمر.

الاقتصادية، الثلاثاء 19 رجب 1437هـ/ الموافق 26 إبريل 2016م.

أضرار الشركات في المملكة المتحدة بسبب الجرائم السايبرية:

أفادت (81%) من الشركات الكبيرة، و(60%) من المؤسسات الصغيرة في المملكة المتحدة بتعرضهم لاختراق معلوماتي عام 2013م، وكانت قيمة الضرر لأقسى حالات الجرائم السايبرية تقع بين (600) ألف ومليون جنيه إسترليني للشركات الكبيرة، وبين (65) ألف و(115) ألف جنيه إسترليني للشركات الصغرى، ويرى مسؤولو بنك إنجلترا أن الهجمات السايبرية أكبر تهديد للاستقرار المالي في المملكة المتحدة.

المصدر: تقرير اللجنة الاقتصادية والاجتماعية لغربي آسيا، الإسكوا.

أستراليا تخصص 230 مليون دولار لتطوير الأمن الإلكتروني.

كانبيرا – واس.

أعلنت الحكومة الأسترالية صباح اليوم الخميس عن تخصيص حزمة بقيمة 230 مليون دولار أسترالي لتعزيز إستراتيجية الأمن الإلكتروني وتطويرها؛ وذلك لحماية المصالح الأسترالية من أي اعتداءات أو هجمات إلكترونية.

ورأى مالكولم تيرنبول رئيس الوزراء الأسترالي في بيان أن عملية بناء بيئة موثوق بها وآمنة على شبكة الإنترنت يُعدّ أمرًا أساسيًّا للتطور ولمواجهة التحديات المستقبلية، ويُعدّ أمرًا أساسيًّا أيضًا في المجالات الاجتماعية والاقتصادية والإستراتيجية.

الخميس 14 رجب 1437هـ/ 21 إبريل 2016م.

الجريمة الإلكترونية.. مليارا دولار خسائر 12 ألف شركة حول العالم.

خلال المدة من تشرين الأول (أكتوبر) 2013 وشباط (فبراير) 2016م تم استهداف أكثر من 12 ألف شركة تجارية في جميع أنحاء العالم بعمليات الاحتيال هذه، التي تعرف أيضًا بمخططات رسائل البريد الإلكتروني الموجهة من الرئيس التنفيذي، وعادت هذه العلميات على المجرمين بمبلغ صافٍ يقدر بملياري دولار، وفقًا لمركز شكاوى جرائم الإنترنت، وهو فريق تحقيق واستخبارات داخل مكتب التحقيقات الفيدرالي يتعقب جرائم الكمبيوتر، وتعرضت لذلك شركات كبيرة وصغيرة في 108 بلدان، والخطر آخذ في التزايد، بحسب ما يقول مسؤولو إنفاذ القانون، ويقول مايكل تومبسون، رئيس فرقة عمل جرائم الإنترنت المالية في مكتب التحقيقات الفيدرالي في نيويورك: «لقد أصبح الأمر خارجًا عن السيطرة»، مضيفًا أن المجرمين «يصبحون أكثر جرأة»، من خلال إدخال أطراف ثالثة، مثل الشركات القانونية والمختصين الاستشاريين، لتنفيذ عمليات الاحتيال، وأصبحوا أكثر تطورًا في كيفية توريط الضحايا المحتملين.

الأحد 19 جمادى الأول 1437هـ/ الموافق 28 فبراير 2016م.

6.2 مقتطفات لمثال المملكة العربية السعودية

هجمات إلكترونية تسعى لاختراق أجهزة عددٍ من الجهات الحكومية.

أوضح المركز الوطني للأمن الإلكتروني أنه تم رصد محاولات هجوم إلكتروني تعرضت له جهات حكومية ومحلية عدة عن طريق رسائل بريد إلكترونية اصطيادي (Phishing email) تهدف إلى اختراق الأجهزة الإلكترونية وسرقة المعلومات عن طريق فتح المرفقات بالإيميل، ثم إرسالها إلى حسابات بريد إلكتروني أخرى،

وأكد المركز الوطني للأمن الإلكتروني على الجميع بضرورة الالتزام بمعايير السلامة الإلكترونية بعدم فتح مرفقات رسائل البريد الإلكترونية المشبوهة تلافيًا لأي أضرار قد تحدث من برمجيات خبيثة تحويها تلك المرفقات.

صحيفة الرياض، الأحد 08 شعبان 1437هـ/ 15 مايو 2016م.

مركز المعلومات الوطني يحذر من ثغرات إلكترونية في مواقع حكومية وصناعية.

حذر مسؤولون في المركز الوطني لأمن المعلومات من وجود ثغرات إلكترونية في مواقع حكومية وصناعية حساسة، مؤكدين أن بعض الشبكات الحكومية تعاني ضعفًا في قدرتها على مواجهة الاختراقات والتهديدات الإلكترونية، التي يسعى المركز الوطني لأمن المعلومات إلى معالجتها.

وأكد وجود تحديات تواجه الأمن الإلكتروني في المملكة على الرغم من إصدار مراسيم ملكية وسياسات تهدف إلى تنظيم أنشطة الأمن الإلكتروني والاستجابة للحوادث الإلكترونية، مشيرًا إلى أنه لا يوجد برنامج واضح لتنظيم السياسات الوطنية وتطويرها لحث الجهات على الالتزام بها.

الاقتصادية، الخميس 23 جمادى الأول 1437هـ/ الموافق 03 مارس 2016م.

كلمة الرياض

وقد واجهت المملكة هجمتين بارزتين: الأولى استهدفت الأنظمة الشبكية لشركة أرامكو، والثانية تم الهجوم فيها على قواعد البيانات في وزارة الخارجية.

الرياض، الأحد 10 صفر 1437هـ/ 22 نوفمبر 2015م.

مؤتمر مكافحة الجرائم المعلوماتية يوصي بـ:

القيام بحملات مستمرة لتوعية جميع فئات المجتمع بأنماط الجريمة المعلوماتية والتعريف بالجهات المعنية للإبلاغ عن تلك الجرائم، وبفتح باب الشراكة والتعاون داخليًّا

وخارجيًّا في مجال مكافحة الجرائم المعلوماتية، وبالتأكيد على قيام المربي بدوره تجاه الصغير وتفعيل الإجراءات النظامية لمحاسبته في حال تقصيره، وبإعداد أدلة إجرائية للضبط والتحقيق في الجرائم المعلوماتية، وإعداد برامج تربوية وإعلامية وتقنية لحماية الصغار من خطر الجرائم المعلوماتية، وحث الجهات الحكومية والأهلية على ضرورة تأمين التعاملات الإلكترونية وسلامتها وفق معايير وطنية محددة، وتحديد جهة مسؤولة عن حماية البنى التحتية المعلوماتية بالتنسيق مع الجهات الحكومية والأهلية، وبدعم المؤسسات التعليمية لتدريب الطلاب والمختصين في أمن المعلومات على أساليب مكافحة الجرائم المعلوماتية وطرقها.

الرياض، السبت 2 صفر 1437/ 14 نوفمبر 2015م.

هاكر سعودي يخترق 23 موقعًا حكوميًّا خلال ساعتين.

تمكن هاكر سعودي، فجر أمس السبت، من اختراق نحو 23 موقعًا إلكترونيًّا حكوميًّا خلال ساعتين، ما بين مواقع تعليمية، وأخرى صحية، ورياضية، وبلدية، ومرورية، وغيرها، مبررًا في رسالته أن سبب تلك الاختراقات هو تجاهل تلك المواقع الحكومية لرسائله عن هجوم محتمل.

عكاظ، الأحد 1436/11/01هـ/ 116 أغسطس 2015م.

الأمن الإلكتروني.. ومسؤولية العملاء:

استطاعت الجهات الأمنية في وقت وجيز أن تسقط شبكة من العمالة الآسيوية تخصصت في السطو على بيانات العملاء في أجهزة الصرف الآلي، للوصول إلى حسابات العملاء والسحب من أرصدتهم، وهي جريمة ذات خطورة عالية؛ لأنها تتضمن الدخول إلى النظام المصرفي التقني للمصارف، ومن ثم تنفيذ عمليات مالية تبدو في ظاهرها صحيحة، ولكنها نوع من استغلال البيانات والاختلاس المالي، بل الأخطر من ذلك أن هذا النوع من الجرائم جزء من الاحتيالات المالية في ساحات الإنترنت، وجزء من النشاط الإجرامي الذي تحذر منه الجهات المسؤولة عن مكافحة هذا النوع من الجرائم، التي امتدت واتسع نطاقها لتشمل معظم الجرائم المعروفة مع تميز في استخدام التقنية.

ولأهمية التوعية، فإن (الإنتربول) السعودي حذر في أوقات سابقة أكثر من مرة من تزايد ملحوظ في حالات الاحتيال الإلكتروني من خلال عمليات البيع والشراء عبر الإنترنت، حيث أوضح (الإنتربول) السعودي بلوغ قضايا التهديد والابتزاز عن طريق شبكة الإنترنت عالميًّا ما نسبته 18 في المئة من مجمل قضايا الجرائم الإلكترونية، وأن قضايا استغلال الأطفال سجلت ما نسبته 14 في المئة من مجمل الجرائم الإلكترونية، وأن قضايا اختراق البريد الإلكتروني تصدرت مجمل قضايا الإجرام الإلكتروني بما نسبته 27 في المئة، إضافة إلى قضايا السب والتشهير وإساءة السمعة والاختراق والاحتيال الإلكترونيين.

الاقتصادية، السبت 03 رمضان 1436هـ/ الموافق 20 يونيو 2015م.

أمن المعلومات يواجه «خطر الاختراق» من الخارج:

شدد (الدكتور زياد آل الشيخ) على أهمية أمن المعلومات للمواطن، وقال: أجرينا دراسة حديثة على المواقع غير الحكومية على شبكة الإنترنت، وهي نحو (7000) موقع عربي مصنفة على أنّها من أعلى المواقع زيارة عربيًّا، ومن خلال البحث اكتشفنا أنّ (2%) من هذه المواقع فيها فيروسات، وأنّ (5%) منها ممنوع الوصول إليها باستخدام برامج أمن المعلومات، وأن (5,6%) من هذه المواقع تعاني مشكلات استخدامها لأدوات قديمة غير محدثة، ومن ثم يصبح الموقع عرضةً للهجوم، ولهذا لا بد من الاهتمام بأمن معلومات المواطن والعمل على حماية معلوماته الخاصة.

ووضح (الدكتور محمد الشيبي) أنّ عملية الاختراق ـ بناءً على الإحصاءات العالمية ـ هي نحو (80%) من الداخل، و(20%) من الخارج.

الرياض، الثلاثاء 18 رجب 1434هـ/ 28 مايو2013م.

تقرير: السعودية في المرتبة 32 عالميًّا في عدد هجمات الإنترنت:

وضحت شركة (سيمانتك) الشركة العالمية، المتخصصة في مجال الأمن والحماية المعلوماتية، في مؤتمرها الصحافي الذي عقد أخيرًا في الرياض، بحضور كيفن إيزاك، المدير الإقليمي في شركة (سيمانتك) في منطقة الشرق الأوسط وشمال إفريقيا، أن

شركة (سيمانتك) أصدرت تقريرها الـ 13 حول تهديدات أمن الإنترنت ISTR، وبيّنت الإحصاءات التي تضمنت زيادةً متنامية في الهجمات والأنشطة الخبيثة في بلدان منطقة الشرق الأوسط، وأوضح التقرير أن السعودية تجاوزت الإمارات، لتتصدر القائمة في منطقة أوروبا والشرق الأوسط وإفريقيا من حيث عدد الأنشطة الخبيثة لكل مشترك في الإنترنت عبر الحزمة العريضة، خلال النصف الثاني من عام 2007م، وذلك بحصولها على نسبة 33 في المئة، حيث تحتل المملكة حاليًّا المركز 32 عالميًّا، بعد أن كانت في المركز 28 في حزيران (يونيو) من عام 2007م.

وفي السياق نفسه، خلُص تقرير تهديدات أمن الإنترنت ISTR، إلى أن شبكة الويب هي الآن الهدف والوسيلة الأساسية لشن الهجمات بدلًا من الهجمات الشبكية، وأن احتمال تعرض مستخدمي الإنترنت للإصابة بمجرد زيارتهم مواقع ويب المعتادة يزداد يومًا بعد يوم، ويستند التقرير إلى البيانات التي تم جمعها بواسطة ملايين الحسابات على الإنترنت، والبحوث الأساسية، والمراقبة الفاعلة للاتصالات بين المخترقين، وهو يوفر نظرة عامة عن حالة أمن الإنترنت في العالم.

ففي الماضي، كان على المستخدم زيارة المواقع المشبوهة عمدًا أو النقر على مرفقات البريد الإلكتروني الخبيثة ليصبح ضحية تهديد أمني. أما اليوم، فيمكن للمخترقين استغلال المواقع العادية التي تبدو سليمة واستخدامها وسيطًا لشن الهجمات على حواسيب المنازل والشركات، وقد لاحظت (سيمانتك) أن المهاجمين يستهدفون بشكل خاص المواقع التي يُرجَّح أن يثق بها المستخدمون، مثل مواقع الشبكات الاجتماعية.

وعام 2007م، اكتشفت (سيمانتك) 711,912 تهديدًا جديدًا مقارنة بتهديدات بلغت 125,243 في العام 2006م؛ أي بزيادة قدرها 468 في المئة. ويرفع ذلك العدد الإجمالي للتهديدات البرمجية الخبيثة التي اكتشفتها (سيمانتك) إلى1,122,311 حتى نهاية عام 2007م.

قاست (سيمانتك) إطلاق كل من البرمجيات السليمة والخبيثة خلال جزء من زمن التقرير، ووجدت أن 65 في المئة من التطبيقات الفريدة التي أطلقت في تلك المدة، وبلغ

عددها 54,609 تطبيقًا كانت مصنفة على أنها خبيثة، وهذه هي المرة الأولى التي تلحظ فيها (سيمانتك) تجاوز عدد التطبيقات الخبيثة لتلك السليمة.

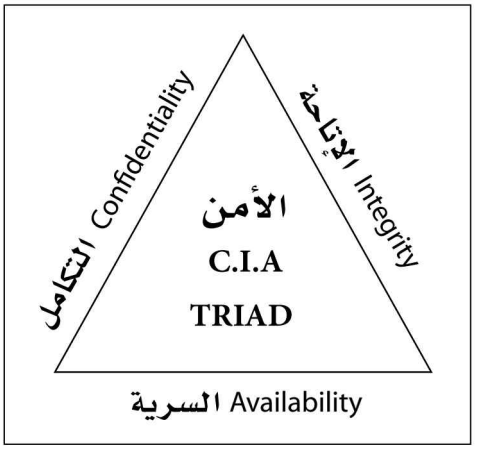
يقول ستيفن تريلينج، نائب الرئيس لشؤون تقنية الأمن والاستجابة لدى (سيمانتك): «لقد كانت النصيحة بتجنب مواقع الإنترنت المشبوهة أمرًا كافيًا في السنوات السابقة، أما اليوم فإن المجرمين يركزون على استغلال مواقع ويب السليمة لمهاجمة المستخدمين، ما يبرز أهمية الإبقاء على الأوضاع الأمنية قوية بغض النظر عن المكان الذي تذهب إليه والنشاط الذي تمارسه على الإنترنت».

الاقتصادية، السبت 19 جمادى الأولى 1429هـ/ الموافق 24 مايو 2008م.

الفصل الثالث

مقوِّمات أساسيَّة في أمن المعلومات

1.3 ثلاثيَّة السرية والسلامة والتوافر



يركز هذا النموذج الشهير في حقل أمن المعلومات على تحقيق ثلاثة شروط أساسيَّة تُدعَى **ثلاثيَّة** C.I.A أو C.I.A Triad، وهي اختصار **للسريَّة** Confidentiality **وسلامة المعلومات أو تكاملها** Integrity **وتوافرها أو إتاحتها** Availability. هذا يَعني أنَّه، لكي يُحقِّق أمن المعلومات أهدافه، يَنبغي المحافَظة على سريَّة المعلومات الخاصَّة، وعلى سلامتها، وعلى تَوافرها عند الحاجة إلى استثمارها، وتَقوم معظم خُطَط وإستراتيجيَّات أمن المعلومات (مهما كان نموذج هذه المعلومات) على تحقيق ثلاثيَّة C.I.A. تُعدّ بعض المراجع ثلاثيَّة C.I.A مجرَّد مفاهيم أساسيَّة في حقل أمن المعلومات، إلا أنَّها على الأصَح مجموعة مقاييس شَرطيَّة لتحقيق أهداف أمن المعلومات.

2.3 أمن الشبكات

من الأساسيَّات في حقل أمن المعلومات حماية المعلومات الخاصَّة التي تَنتقِل عَبْر الشبكات الحاسوبية أو النقالة، وهذا الأمر هو ما يَتكفَّل به أمن الشبكات، و**أمن الشبكة** Network security هو مجموعة من الإجراءات المضادَّة التي تَكفَل إدخال المعلومات الرقميَّة الخاصَّة المشتَرَكة المعدَّة للنقل في وَضْع الأمان عند مرورها عبر شبكة غير آمنة، وتَتمثَّل مجموعة الإجراءات المضادَّة في حماية الشبكة نفسها وفي حماية المعلومات الخاصَّة التي تَمرُّ عَبْرها. وعمومًا، يُؤدِّي أمن الشبكات دوره لحماية المعلومات الخاصَّة في المحيط الإلكتروني فقط.

ويُعَدُّ تصميم الشبكة الحاسوبيَّة المناسب أمرًا فعَّالًا في حمايتها، ومن طُرُق التصميم المُثلى للشبكة تقسيم الشبكة الحاسوبيَّة إلى شبكات صغيرة Network segmentation، وتركيب الجدران الناريَّة Firewalls وتركيب أنظمة اكتشاف التطفُّل [2، 11]. وإن **تقسيم الشبكة** الحاسوبيَّة الكبيرة في بيئةٍ ما إلى مجموعة من الشبكات الصغيرة، تُدعَى كلٌّ منها **الشبكة الفرعية** Subnet، يوفر مزيّة التّحكُّم في حركة المعلومات التي تَمرُّ عَبْر الشبكات الفرعيَّة بكل سهولة. أمّا **الجدار الناري** فهو مجموعة من البرامج الحاسوبيَّة التي تَتحكَّم في حركة المعلومات الخاصَّة التي تَنتقِل بين الشبكة الداخليَّة والشبكة الخارجيَّة وفقًا لمجموعة من القواعد الموضوعة، ويُمكِن النظر إلى الجدار الناري على أنه حاجز أمني يَقَع بين الشبكة الداخليَّة الآمنة والموثوقة في بيئةٍ ما (كشبكة داخليَّة في منظَّمة ما) والشبكة الخارجيَّة (كشبكة الإنترنت) ويَتحكَّم في دخول المعلومات وخروجها بينهما، وأمّا **نظام اكتشاف التطفُّل** Intrusion detection system فهو برنامج حاسوبي يَسعى إلى اكتشاف نشاط أي متطفِّل يُحاوِل الدخول إلى الشبكة الداخليَّة في بيئةٍ ما من خلال إصدار إنذارات تُنبِّه إليه.

ويُمكِن أيضًا حماية المعلومات الخاصَّة التي تَمرُّ عَبْر الشبكة بدلًا من حماية الشبكة نفسها، ومن أكثر الطُّرُق استخدامًا لحماية المعلومات الخاصَّة التي تَمرُّ عَبْر الشبكة هي الشبكات الخاصَّة الافتراضيَّة، **والشبكة الخاصَّة الافتراضيَّة** Virtual private network، واختصارًا VPN، هي مجموعة من البرمجيَّات والعتاديَّات التي تُكوِّن شبكة خاصَّة داخل شبكة عامَّة تُضاهي في عملها شبكة خاصَّة فيزيائيَّة، وتَستخدِم الشبكة الخاصَّة الافتراضيَّة تقنيَّة التعمية لحماية المعلومات التي تَمرُّ عَبْرها، ويُمكِن النظر إلى الشبكة الخاصَّة الافتراضيَّة على أنها نَفَق (أو أنبوب ضمن الشبكة العامة) تَمرُّ عَبْره المعلومات الخاصَّة بشكلها المعمَّى.

3.3 أمن المعلومات الفيزيائي

لا يَكفي أبدًا التركيز فقط على حماية المعلومات الخاصَّة دون الالتفات إلى حماية محيط مالِكها وحماية الأفراد الذين يتعامَلون معها، فتُدعَى حماية المعلومات الخاصَّة والأطراف الذين يتعامَلون معها ومحيط مالِكها، **الأمن الفيزيائي** Physical security، ويُعدّ الأمن الفيزيائي من الاهتمامات الرئيسة في حقل أمن المعلومات؛ لأنَّ تحقيقه يُمثِّل إطار الأمان الذي يُغطِّي المعلومات والأطراف الذين يتعامَلون معها ومحيط مالِكها، ويَشمَل الأمن الفيزيائي من حيث ترتيب الأولويَّة:

1. حماية الأطراف البشريَّة الذين يتعامَلون مع المعلومات الخاصَّة.
2. حماية المعلومات الخاصَّة.
3. حماية محيط مالِك المعلومات.

تُصنَّف حماية الأطراف في الدرجة الأولى في الأمن الفيزيائي؛ لأنَّ الأطراف البشريَّة (وخاصَّةً الخبيرة منها) تُعدّ المَسْنَد الذي تَتَّكِئ عليه جميع الأعمال التي تَتَّصِل بالمعلومات، فإذا حَصَل مثلًا، وتَضرَّرت المعلومات الخاصَّة، يُمكِن استعادتها من النُّسَخ الاحتياطيَّة منها، وإذا حَصَل، وتَضرَّرت المعدَّات والتجهيزات المتعلِّقة بالمعلومات

والموجودة جميعًا داخل محيط مالِك المعلومات، يُمكِن استبدالها من خلال شراء معدَّات وتجهيزات أخرى. أمّا الأطراف البشريَّة فلا يُمكِن تعويضها إلا بصعوبة بالغة، إذْ هي المحرِّك الأول في إدارة جميع الأعمال التي تَستثمِر المعلومات الخاصَّة؛ لذا فإذا حَصَل، وتَضرَّرت الأطراف البشريَّة تَضرَّر معها جميع تِلْك الأعمال، حتى ولو كانت هذه المعلومات والمعدَّات بحالة سليمة، وتَتضمَّن حماية الأطراف البشريَّة في الأمن الفيزيائي تأمينهم من جميع أشكال الأذى الجسدي أو النفسي الذي قد يَتعرَّضون له داخل محيط مالِك المعلومات.

والاهتمام الثاني في قائمة أولويَّة الحماية في الأمن الفيزيائي هو المعلومات الخاصَّة، وهي الحماية التي تتضمن إجراء النَّسْخ الاحتياطي لها وحماية هذه النُّسَخ، وتتضمن إتلافها وإتلاف جميع النُّسَخ بعد الانتهاء من استثمارها، و**النَّسْخ الاحتياطي للمعلومات** Backing –up information هو عملية إنشاء نُسَخ متطابقة (واحدة على الأقل أو أكثر) من النسخة الأصليَّة للمعلومات الخاصَّة بهدف استعمالها لاحقًا عند تَعرُّض النسخة الأصليَّة من المعلومات للتخريب، وتَتضمَّن هذه العملية إمّا نَسْخ أشرطة أو أقراص التخزين مرَّات عدَّة إذا كانت المعلومات رقميَّة، أو تصوير الوثائق والمستندات مرَّات عدَّة إذا كانت المعلومات ورقيَّة. أمّا **إتلاف المعلومات** Destroying information فهو عملية التخلُّص من المعلومات الخاصَّة عند الانتهاء تمامًا من استثمارها. إنَّ عملية إتلاف المعلومات ضرورية من أجل عدم استعمالها لاحقًا من قِبَل أفراد بشريَّة أخرى يُمكِن أن تَستغلَّها، وتُؤذي مالِكها، وتَتضمَّن عملية إتلاف المعلومات إمّا مَحو جميع المعلومات المخزَّنة على الأقراص الصلبة باستخدام برامج متخصِّصة، وإتلاف جميع الأشرطة والأقراص التي تَحتوي على المعلومات، وإتلاف جميع النُّسَخ أيضًا، وذلك من خلال تخريب هذه الأشرطة والأقراص وتمزيقها على نحوٍ مُحكَم، بحيث يَستحيل استعادتها أو استعادة المعلومات منها، وكلُّ ذلك بلا ريب إذا كانت المعلومات رقميَّة،

أو تمزيق الوثائق والمستندات التي تَحتوي على المعلومات الخاصَّة باستخدام معدَّات مخصَّصة لذلك أو إحراقها وإتلاف جميع النُّسَخ المصوَّرة إذا كانت المعلومات ورقيَّة.

والاهتمام الثالث في قائمة أولويَّة الحماية في الأمن الفيزيائي هو محيط مالِك المعلومات، ويَشتمِل محيط مالِك المعلومات على كلِّ المعدَّات والتجهيزات التي تَرتبِط من قريب أو من بعيد بالمعلومات، وتَتضمَّن هذه الحماية اختيار الموقع الفيزيائي المناسب للمعدَّات والتجهيزات التي سَتحتوي على المعلومات وتَقييد الوصول إليها إلا من قِبل الأطراف البشريَّة المُجَاز لها ذلك، وتَوفير الظروف البيئيَّة المناسبة للمحافظة على سلامة هذه المعدَّات والتجهيزات.

ويُمكِن تحقيق الأمن الفيزيائي باستخدام **ضوابِط الأمن الفيزيائي** Physical security controls، وهي مجموعة من الأدوات والأفراد البشريَّة والمواد الإعلاميَّة التحذيريَّة التي تُسهِم في تحقيق الأمن الفيزيائي، وثَمَّة ثلاثة أنواع من ضوابِط الأمن الفيزيائي هي: **ضوابِط رادِعة** Deterrent controls، **وضوابِط كَشْفيَّة** Detective controls، **وضوابِط وقائيَّة** Preventive controls، والضوابِط الرادِعة هي الضوابِط المُصمَّمة لتثبيط الأفراد عن السعي لانتهاك أمان المعلومات أو محيطها أو محيط مالِكها، ومن أمثلة هذه الضوابِط شارات إعلاميَّة تحذيريَّة في الأماكن الخارجيَّة لمحيط مالِك المعلومات تُنبِّه إلى أنَّ المكان مُراقَب بكاميرات التصوير. أمّا الضوابِط الكَشْفيَّة فهي الضوابِط المخصَّصة لاكتشاف أي انتهاك لأمان المعلومات أو محيطها أو محيط مالِكها عند وقوعه، ومن أمثلة الضوابِط الكَشْفيَّة أجراس الإنذار التي تُطلَق عند القيام بمحاولة اقتحام أو دخول غير مرخَّص في أحد أماكن محيط مالِك المعلومات، وأمّا الضوابِط الوقائيَّة فهي الضوابِط التي تُستعمَل لمَنْع الأفراد من انتهاك أمان المعلومات أو محيطها أو محيط مالِكها، ومن أمثلة ذلك الأقفال المركَّبة على أبواب الأماكن في محيط مالِك المعلومات والحرَّاس وكلاب الحراسة.

4.3 الولوج أو النفاذ إلى المعلومات

تَحتوي معظم المراجع في حقل أمن المعلومات على تفاصيل موسَّعة ودراسات كثيرة في طُرُق الولوج إلى المعلومات الخاصَّة والتَّحكُّم فيها، وسوف نَكتفي فيما يأتي بالحديث عن المفاهيم الأساسيَّة فقط.

تَتألَّف آلية الولوج إلى المعلومات من خمس عمليات أساسيَّة هي بالترتيب: **إثبات الهويَّة** Identification، **والتأكيد أو التحقق** Verification، **والمصادَقة** Authentication، **والترخيص** Authorization، **وضَبْط الوصول إلى المعلومات** Access control.

إثبات الهويَّة هو العملية التي يُقدِّم فيها طرفٌ ما هويَّته التي تَتضمَّن معلومات أساسيَّة عنه إلى الجهة المسؤولة عن مَنْحه إذن الولوج إلى المعلومات، وقد تَكون الجهة المسؤولة عن مَنْح إذن الولوج إلى المعلومات إمّا طرفًا بشريًّا أو برنامجًا حاسوبيًّا، وإنَّ عمليَّة إثبات الهويَّة هي مجرَّد ادِّعاء حامِل الهويَّة بملكيَّة هويَّته، ولا تَقتضي بالضرورة أن تَكون معلومات الهويَّة صحيحة، أو أنَّها تَعود فعلًا لحامِلها.

أمّا التأكيد أو التحقق فهي العمليَّة التي تَقوم فيها الجهة المسؤولة عن مَنْح إذن الولوج إلى المعلومات الخاصَّة بفَحص الهويَّة التي قَدَّمها الطرف البشري للولوج إلى المعلومات، ولا تَتضمَّن هذه العمليَّة إلا التأكُّد من أنَّ حامِل الهويَّة قد قَدَّمها فعلًا دون إثبات صحَّة ما فيها من معلومات أساسيَّة وصحَّة أنَّها تَعود فعلًا إلى حامِلها.

وأمّا المصادَقة فهي العمليَّة التي تَقوم فيها الجهة المسؤولة عن مَنْح إذن الولوج إلى المعلومات الخاصَّة بالتَّحقُّق من أنَّ المعلومات الأساسيَّة الواردة في الهويَّة المقدَّمة إمّا صحيحة بالكامل، وأنَّها تَعود فعلًا إلى حامِلها أو أنَّها مزوَّرة، ومن ثم التقرير رسميًّا بما سَبَق.

وأمّا الترخيص فهو العملية التي تَقوم فيها الجهة المسؤولة عن مَنْح إذن الولوج إلى المعلومات الخاصَّة بالسماح للطرف البشري الذي قَدَّم هويَّته، وتَمَّت المصادَقة رسميًّا على صحَّتها بالوصول إلى المعلومات الخاصَّة.

وأمّا ضَبْط الوصول إلى المعلومات فهو العمليَّة الأخيرة التي تَقوم فيها الجهة المسؤولة عن مَنْح إذن الولوج إلى المعلومات الخاصَّة بتحديد مستويات الوصول لجميع الأطراف (المستخدِمين) الذين يتعامَلون مع المعلومات الخاصَّة كُلٌّ بحسب حاجته من هذه المعلومات، وتَتضمَّن هذه العمليَّة تَقييد حريَّة وصول كل طرف بشري إلى المعلومات الخاصَّة التي لا يَحتاج إلى استثمارها.

5.3 التعمية من المقومات الأساسية لأمن المعلومات

تقنية التعمية (أو التشفير) هي المكوِّن الأساسي لأي مجموعة إجراءات في أمن المعلومات، وقد بَدَأ استعمال التعمية منذ القدم عندما أراد الإنسان أن يَحمي معلوماته الخاصَّة بطريقة لا يَحتاج فيها إلى إخفائها فيزيائيًّا، وكانت التعمية (ولا تزال) الأداة الفعَّالة لتَبادُل المعلومات العسكريَّة. أمّا الآن فقد أصبحت التعمية ضرورة لحماية أي معلومات خاصَّة، سواء أكانت عسكريَّة أم مدنيَّة عند خزنها أو تبادلها، وفي حقل أمن المعلومات تُعدّ تقنيَّة التعمية الأداة الرئيسة التي تَنطوي داخل أي مجموعة من الإجراءات المضادَّة لحماية المعلومات الخاصَّة المعدَّة للتخزين أو المعدَّة للنَّقل.

ثَمَّة نوعان من التعمية هما: **التعمية ذات المفتاح المتماثِل** Symmetric –key cryptography **والتعمية ذات المفتاح غير المتماثِل** Asymmetric–key cryptography 15. تَستخدِم التعمية ذات المفتاح المتماثِل المفتاح نفسه، ويُدعَى **المفتاح السرِّي** Secret key، من أجل تعمية النص الواضح وفك تعمية النص المعمَّى. أمّا التعمية ذات المفتاح غير المتماثِل فتَستخدِم مفتاحين مختلفين: الأول من أجل تعمية النص الواضح، ويُدعَى **المفتاح العام** Public key، والثاني من أجل فك تعمية النص المعمَّى، ويُدعَى **المفتاح**

الخاص Private key. جَاءَت التعمية بالمفتاح غير المتماثِل لحَلِّ مشكلة تَبادُل المفاتيح السريَّة في التعمية بالمفتاح المتماثِل عبر الشبكات غير الآمنة. أيضًا، ثَمَّة نموذجان للمعمِّيات التي تَستخدِم المفاتيح المتماثِلة، هما: **المعمِّيات الكتلوية** Block ciphers و**المعمِّيات التسلسليَّة** Stream ciphers، والمعمِّي الكتلوي هو المعمِّي الذي يقوم بتعمية النص الواضح كتلةً كتلة من البيانات حجمها 64 بتًّا أو أكبر. أمّا المعمِّي التسلسلي فهو المعمِّي الذي يَقوم بتعمية النص الواضح خانةً خانة (بتًّا بتًّا) من البيانات.

تُستخدَم التعمية أيضًا لأغراض غير أغراض حماية المعلومات من الاطلاع غير المشروع عليها، مثل الحفاظ على سلامة المعلومات من تغيير أي خانة أو حرف فيها، والتقنيَّة التي تُسهِم في الحفاظ على سلامة المعلومات هي **تابع البصمة أو الحشوة** Hash function، ويَأخُذ تابع البصمة كدَخْلٍ إمّا وسيطًا واحدًا هو معلومات فقط أو وسيطين هما: معلومات ومفتاح سرِّي، ويُعطي كخَرْجٍ قيمة تُدعَى **قيمة البصمة** Hash value، وعندما يَتِمّ تعديل أو إضافة أو إزالة بت واحد إلى المعلومات التي طُبِّقَ عليها تابع البصمة تَتغيَّر قيمة البصمة كليًّا، وذلك يَدلُّ بشكلٍ صريح على عملية تَلاعُب بتِلْك المعلومات.

ثَمَّة تقنيَّة مهمة من تقنيات التعمية ذات المفتاح غير المتماثِل هي **التوقيع الرقمي** Digital signature. تَستنِد هذه التقنيَّة إلى قيام مرسِل الرسالة بتوقيعها من خلال تطبيق تابع عليها باستخدام مفتاحه الخاص وإلحاق خَرْج هذا التابع (الذي يُعدّ بمنزلة التوقيع) بالرسالة، ومن ثم قيام مستقبِل الرسالة بتطبيق التابع نفسه عليها باستخدام المفتاح العام للمرسِل والتأكُّد من مطابقة خَرْج العملية مع التوقيع الملحَق مع الرسالة، والهدف الرئيس من التوقيع الرقمي هو مَنْع مرسِل الرسالة من نكرانها، إضافة إلى التأكد من شخصية المرسل، فمطابقة خَرْج تطبيق تابع التوقيع الرقمي باستخدام المفتاح العام لطرفٍ ما مع التوقيع الملحَق مع الرسالة يُلزِم مرسِل الرسالة بتَحمُّل مسؤوليات الرسالة ومضامينها ومَنْعه من نكران إرسالها.

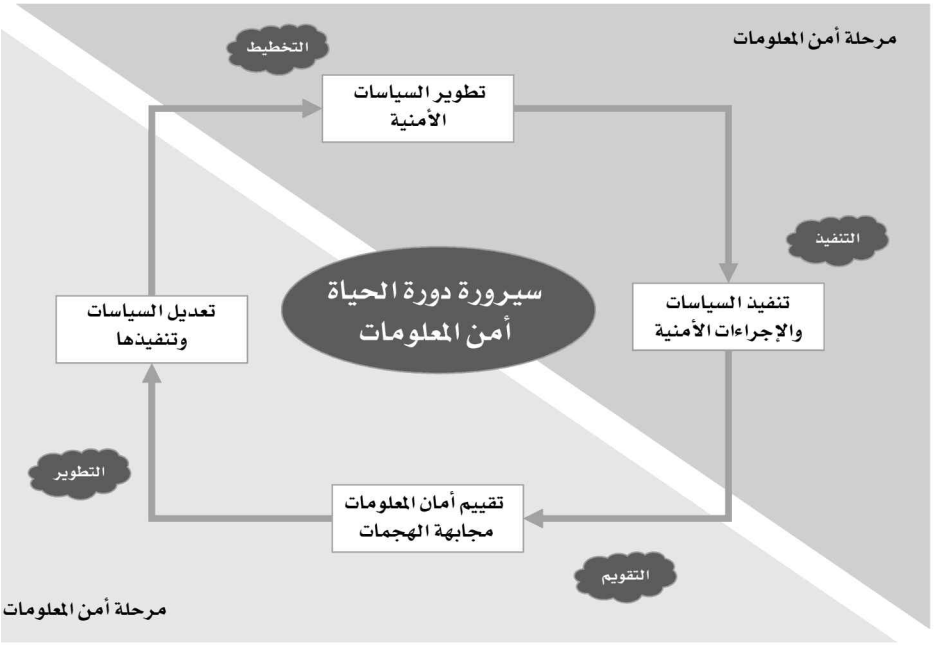
تُطبَّق تقنيَّة التعمية على كلٍّ من المعلومات الرقميَّة والمعلومات الورقيَّة، وتطبيق التعمية على المعلومات الورقيَّة يَقتصِر فقط على استخدام المعمَّيات التقليدية، وحديثًا، وبتَطوُّر علم التعمية وتَطوُّر خوارزمياتها وتعقيدها، أصبَحَت التعمية تُطبَّق على المعلومات الرقميَّة فقط، أمّا التقنيات الأخرى مثل توابع البصمة والتواقيع الرقميَّة، فلا تُطبَّق إلا على المعلومات الرقميَّة فقط.

الفصل الرابع

أمان المعلومات ومستوياته ومقاييسه

كما ذكرنا سابقًا، ثمة مرحلتان في عملية حماية المعلومات هما: مرحلة التعامل مع أمن المعلومات، ومرحلة التعامل مع أمان المعلومات، ويبيّن الشكل أدناه عناصر هاتين المرحلتين، وعادة لا يتطرق كثير من العاملين في حقل أمن المعلومات إلى آليَّةٍ لتقييس تفاصيل ومراتِب الحالة الأمنية التي تَدخُل فيها المعلومات بعد حمايتها، أو الحالة التي يجب أن تكون عليها المعلومات من حيث أمنها واستمرار هذا الأمن مع المستجدات والتطورات المضادة؛ أي مرحلة (أمان المعلومات)، فمعظم الألفاظ التي تُطلَق على المعلومات بعد حمايتها في هذا الحقل هي (آمنة) و(مؤمَّنة) و(مَحميَّة) و(حصينة) وما إلى ذلك من الألفاظ المرادِفة، ويُقدِّم هذا الفصل مقاييس لتقييم أمان المعلومات المَحميَّة، ولا تَرتبِط هذه المقاييس بطبيعة المعلومات، سواء أكانت رقميَّة أم ورقيَّة، فهي تسري على كلتا الطبيعتين.

يَعتمِد المقياس الأول على (**مستويات** أمان المعلومات) لقياس أمان المعلومات المَحميَّة تبعًا لفئات المجتمع أو تبعًا لفئات مالك المعلومات أو الطرف المعني بأمنها، ويُقيِّم المقياس الثاني (**درجات** أمان المعلومات) المَحميَّة من منظور أهميَّتها ومستوى حساسيَّتها أو مستوى سريتها أو خصوصيتها. أمّا المقياس الثالث فيُحدِّد **وَضْع** المعلومات المَحميَّة أو حالتها، آمنة أو غير آمنة، استنادًا إلى التكلفة الماليَّة والمدَّة الزمنيَّة لاختراق حمايتها بغَضِّ النَظر عن مراتِب هذا الأمان.



1.4 مستويات أمان المعلومات بحسب الجهة المالكة لها

تعتمد مستويات أمان المعلومات على الجهة المالكة لها، ويُمكِن التمييز بين أربع فئات رئيسة: الفرد – والمؤسسة أو المنظَّمة – والدولة – والعالم. الفرد هو المكوِّن الرئيس للمنظَّمة والدولة، والمنظَّمة قد تكون أحد مكوِّنات الدولة، وإن هناك تجمعات وتكتلات دولية لها معلومات خاصة بها، وتَحتاج المعلومات المرتَبِطة بكل فئة من هذه الفئات إلى

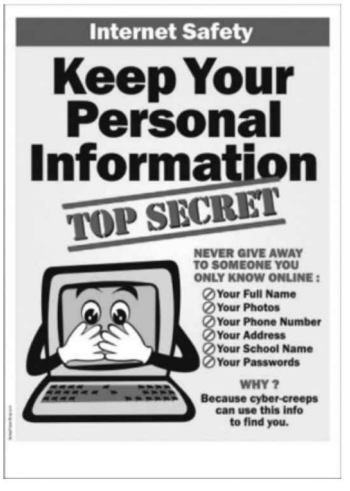
مستوى محدَّد من الأمان، إذْ ليسَ من الضروري توفير أمان تام وموحَّد الدرجة لكل الفئات، إذ إن لكل فئة متطلَّبات أمان معلومات معيَّنة تَختلِف عن تلك المطلوبة لبقيَّة الفئات.

ثَمَّة أربعة مستويات لأمان المعلومات تَشمَل جميع فئات المجتمع، وهي: **أمان المعلومات على مستوى الفرد، والمنظَّمة، والدولة، والعالَم.**

1.1.4 أمان المعلومات على مستوى الفرد

الفرد هو أصغر وحدة فاعِلة في المجتمع، وتَنحصِر أهميَّة أمان المعلومات في هذا المستوى ضِمْن نطاق الفرد فقط، وصفة بعض المعلومات في هذا المستوى أنَّها خاصَّة للفرد وغير مشتَرَكة مع الآخرين، والفرد هو الشخص الوحيد المخوَّل بقراءتها واستعمالها والاستفادة منها، والتخويل هنا مَمنوح من الفرد نفسه (أي مِنْه وإليه).

من الصعوبة تحديد جميع أشكال المعلومات المَطلوب حمايتها بالنسبة إلى الفرد، ولكن يُمكِن تعريف أنواع عامَّة للمعلومات التي تَخصُّ الفرد، ويَندرِج تحتها أيُّ شكل من تِلْك المعلومات. عمومًا، ثَمَّة نوعان من المعلومات التي تَخصُّ الفرد، هما: **معلومات فرديَّة خاصَّة غير حسَّاسة، ومعلومات فرديَّة خاصَّة حسَّاسة.**



المعلومات الفرديَّة الخاصَّة غير الحسَّاسة هي المعلومات المرتَبِطة بشخصٍ واحد فقط، وهو الطرف الوحيد المخوَّل بقراءتها واستعمالها والاستفادة منها، ولا تَحمِل في مضامينها أيَّ مظهر حسَّاس، بحيث إنَّ كتمانها لا يُؤدِّي إلى الجريمة المباشرة بحقِّ أيّ فرد آخر أو تهديد الأمن لدولة ما، وإنَّ إفشاءها يُؤدِّي إلى إيذاء مالِكها، ومن أمثلة المعلومات لهذا النوع: المذكِّرات اليوميَّة، وكلمات السرّ الخاصَّة بصناديق البريد الإلكتروني، وأرقام الحسابات المصرفيَّة، ورقم التعريف الشخصي PIN، وخطط شخصيَّة مستقبليَّة، وكما هو واضحٌ من التعريف، فإنَّ هذا النوع من المعلومات لا يَتضمَّن معلومات تُؤدِّي بتطبيقها إلى إيذاء أيّ فرد آخر جسديًّا، كالتخطيط مثلًا لعمليَّة قَتْل، أو اغتيالات سياسيَّة أو عسكريَّة، ولا تُؤدِّي إلى تهديد أمن دولة ما.

ولأن المعلومات الفرديَّة الخاصَّة غير الحسَّاسة لا تَحتوي على أيّ شكل من أشكال الجريمة المباشرة تجاه أيّ فرد آخر أو تهديد أمن دولة ما، فمن حقِّ الفرد الذي يَمتلِكها أن يَحميها بالطريقة التي يَختارها، وهذا الحقُّ الذي يَمتلِكه الفرد مبرَّر.

النوع الثاني من المعلومات التي تَخصُّ الفرد هو المعلومات الفرديَّة الخاصَّة والحسَّاسة، وهي المعلومات المرتَبِطة بشخصٍ (أو عدد من الأشخاص)، وهو الطرف الوحيد المخوَّل بقراءتها واستعمالها والاستفادة منها (من وجهة نَظَره الخاصَّة)، التي تَحمِل مظاهر حسَّاسة أو خطيرة، بحيث إنَّ كتمانها يُؤدِّي إلى إمكانية القيام بجرائم مباشرة أو تهديدات جديَّة لأمن أي دولة، وإنَّ إفشاءها يُؤدِّي إلى إحباط هذه الجريمة، وإنَّ المعلومات الفرديَّة الخاصَّة والحسَّاسة قد يشترك فيها أكثر من طرف (مجموعة من الأفراد يرتبطون بفرد)، خاصَّةً إذا كانوا يُشكِّلون عصابة، وتندرج مثل هذه العصابات تحت فئة الفرد؛ لأنها لم تَتكوَّن بطريقة نظاميَّة وشرعيَّة، فقد تَشكَّلت من خلال دعوة شخصٍ واحدٍ (هو الأصل) عددًا من الأفراد للانضمام إلى تنظيمه والائتمار بأوامره؛ ولذلك فهدف حماية المعلومات الخاصَّة الحسَّاسة من قِبَل هؤلاء الأفراد هو في النهاية هَدَف زَعيمهم نفسه؛ لأنَّهم يَعملون بتفكيره ومذهبه نفسه، وإنَّ إبقاء هذه المعلومات

الفرديَّة الخاصَّة الحسَّاسة (سريَّةً) يُؤدِّي إلى عواقِب وخيمة تَصِل درجة خطورتها إلى مستويات عالية إنْ لم يَتم إفشاؤها للمَعنيين.

لا يَمتلِك الفرد حق حماية معلوماته الخاصَّة الحسَّاسة مهما كانت ظروفه أو مَكانته الاجتماعيَّة، وإنَّ أفضل إجراء للتّعامُل مع هذه المعلومات هو القيام بإفشائها للمَعنيين وإجبار مالِكها على ذلك، أو اختراق أمانها إنْ لم يَكُن بالإمكان إفشاؤها مباشرةً.

2.1.4 أمان المعلومات على مستوى المنظَّمة

يُطلَق اسم (المنظَّمة) على أي منشأة أو شركة أو مؤسسة تَعود ملكيَّتها إلى فردٍ واحد أو عدد من الأفراد، وقد تَعود ملكيَّة المنظَّمة إلى الدولة، فثَمَّة نوع واحد من المعلومات التي تَخصُّ المنظَّمات (سواء أكانت تجاريَّة أم صناعيَّة أم خدمية) هو معلومات **الأعمال الخاصَّة** Private Business Information، وصفة معلومات الأعمال الخاصَّة في مستوى المنظَّمة أنَّها خاصَّة بالنسبة إلى المالِك (أو الأفراد المالِكين) وغير مشتَرَكة مع الآخرين، وهذا يَدلُّ على أنَّ مالِكي المنظَّمة هم المخوَّلون فقط بقراءة معلومات الأعمال الخاصَّة واستعمالها والاستفادة منها، ولا يَقتصِر التّخويل على المالِكين فقط، بل إنَّ موظَّفي المنظَّمة المخوَّلين من قبل مالِكيها يُمكِنهم قراءة معلومات الأعمال الخاصَّة واستعمالها أيضًا.

إنَّ معلومات الأعمال الخاصَّة التي تَمتلِكها المنظَّمة حسَّاسة بطبيعتها، وحساسيتها تَنبُع من أهميَّتها بالنسبة إلى مالِكيها؛ لأن فقدان هذه المعلومات أو إفشاءها أو تخريب جزء منها أو جميعها يُؤدِّي إلى خسائر كبيرة بالنسبة إلى المنظَّمة، وحجم هذه الخسائر يَعتمِد على درجة حساسيَّة معلومات الأعمال الخاصَّة ومقدار التخريب أو الإفشاء، ويَختلِف مضمون معلومات الأعمال الخاصَّة من منظَّمة إلى أخرى، فالمنشأة الصغيرة (كمكتب سياحة مثلًا) تَحتفِظ بأسماء العملاء المتعامِلِين معها، والشركة التجاريَّة (استيراد وتصدير مثلًا) تَحتفِظ بالعمليات والصفقات التجاريَّة التي أجرتها

أو ستَجريها مستقبلًا، والشركة الصناعية (معمل مثلًا) تَحتفِظ بالتصاميم والخطط المستقبليَّة لعمليات الإنتاج.

ومن حَقِّ المنظَّمة أن تَحمي معلومات الأعمال الخاصَّة التي تَمتلِكها مهما كان مضمونها أو درجة حساسيَّتها، وهذا الحقُّ مَكفول لأيّ منظَّمة، طالما أنها تَعمَل ضِمْن الإطار المشروع، والإطار المشروع يَعني أنَّ جميع معلومات الأعمال الخاصَّة التي تَحتفِظ بها المنظَّمة تَخصُّ مصالحها، ولا تَنطَوي على أي شكل من أشكال الجريمة المباشرة تجاه أي فرد أو تهديدات أمن دولة ما، وعليه يَنبغي أن تَندرِج سرقة هذه المعلومات أو إفشاؤها أو تخريبها ضمن جناية السرقة أو التخريب.

3.1.4 أمان المعلومات على مستوى الدولة

تُعدّ بعض المعلومات التي تَحتفِظ بها الدولة أهم بكثير وبكل المقاييس من المعلومات التي تَحتفِظ بها المنظَّمة أو الفرد، والسبب هو أنَّ الدولة تُمثِّل المجتمع الذي تَحكُمه، ومن ثم، فبعض المعلومات التيَ تحتفِظ بها الدولة وتَحميها مهمَّة بالنسبة إلى المجتمع ومرتَبِطة بأمنه، وهذا بلا شك بافتراض أنَّ الدولة التي نَتحدَّث عنها شرعيَّة. إذًا، يَجب أن تَحمي الدولة معلوماتها بشكل مناسب؛ لأنَّ الحفاظ على هذه المعلومات هو حفاظ على مصالح المجتمع ككل، وأنَّ سرقتها أو إفشاءها أو تخريبها هو تخريب لمصالح المجتمع ككل وتهديد لأمنه، ويَدلُّ هذا على أنَّ بعض المعلومات التي تَحميها الدولة حسَّاسة بطبيعتها.

والمعلومات التي تَحميها الدولة هي **المعلومات المصنَّفة سريَّة بكل مستويات هذه السرية**، فمثلًا من المعلومات التي تَحميها الحكومة الأمريكيَّة تحت بند المصنَّفة سريَّة الخطط العسكريَّة، والتصاميم الرئيسة للأسلحة، والأنشطة الاستخباراتيَّة، والمعلومات الاستخباراتيَّة عن دول أجنبيَّة، والمواد العلميَّة أو التكنولوجيَّة أو الاقتصاديَّة التي تَرتبِط بالأمن القومي، والمواد التي تَتعلَّق بإنتاج أسلحة الدمار الشامل واستخدامها. وفي

المملكة المتَّحدة تَعدّ الحكومة المعلومات التي تُهدِّد الاستقرار الداخلي لها أو للدول الصديقة، أو التي تُسبِّب تخريبًا للعلاقات مع الدول الصديقة، أو التي تُسبِّب تخريبًا طويل الأمد لاقتصادها الوطني، أو التي تُهدِّد بشكلٍ مباشر أمنها القومي، جميعها تحت بند المصنَّفة سريَّة. وأمّا في الصين، فالمعلومات التي تَحميها الحكومة تحت بند المصنَّفة سريَّة هي تِلْك المواد التي تَتعلَّق بالقرارات السياسيَّة الرئيسة، أو أنشطة القوات المسلَّحة، أو الأنشطة الدبلوماسيَّة، أو المرتبِطة بالاقتصاد الوطني، أو التي تَتعلَّق بالتكنولوجيا والعلوم.

من الطبيعي جدًّا أن تَحمي الدولة المعلومات التي تَمتلِكها، بل من غير الطبيعي ألا تَقوم بواجبها تجاه حماية المعلومات الحكوميَّة.

4.1.4 أمان المعلومات على المستوى الدولي

عندما يجري الحديث عن أمان المعلومات على المستوى الدولي، يُقصَد بذلك معلومات يَتجاوَز الاهتمام بها والاحتفاظ بسريَّتها حدود الدولة الواحدة، والمعلومات المطلوب حمايتها على المستوى الدولي لها شكلٌ واحد فقط هو معلومات خاصَّة تَتشارَك فيها أطراف دولية عدة، وتُدعَى **المعلومات الدوليَّة المصنَّفة سريَّة**. إنَّ أكبر تَجسيد لهذه المعلومات هو المعلومات الاستخباراتيَّة التي تَتضمَّن مصالح قوميَّة للدول التي تَمتلِكها، أو المعلومات العسكريَّة التي تَتعلَّق بخطَط دفاعيَّة فيما بينها، وأيضًا من المعلومات الدوليَّة المصنَّفة سريَّة تِلْك المتعلقة بمنظَّمات أو اتفاقيات دوليَّة خاصة، ومثال ذلك، المعلومات المصنَّفة سريَّة (بجميع مستويات تصنيفها السرِّي) المتبادَلة بين دول منظَّمة حلف شمال الأطلسي.

يَنطلِق الدافع لحماية المعلومات الدوليَّة المصنَّفة سريَّة من رَغْبة الدول التي تَمتلِكها في الحفاظ على مصالحها القوميَّة، وأوَّل هذه المصالح القوميَّة هو الأمان العام الذي يَتجسَّد في استقرار الدول المشارِكة وسلامتها، ومن ثم، فإنَّ سرقة هذه المعلومات

أو إفشاءها أو تخريبها سيُؤدِّي حتمًا إلى زعزعة استقرار الدول المشارِكة في استعمالها، وعليه، يَجب أن تَبذُل جميع الدول المشارِكة في هذه المعلومات أقصى ما لديها للحفاظ على سريَّتها وسلامتها وتَوافرها.

5.1.4 العلاقة بين مستويات أمان المعلومات

إنَّ مستوى أمان المعلومات المقصود بالتعاريف المذكورة أعلاه هو الحدُّ الأعلى المطلوب أن تَكون المعلومات فيه مَحميَّة، ومن المألوف أن تُحدَّد العلاقة بين مستويات أمان المعلومات بقانون **العلاقة التَراتُبيَّة** Hierarchical relationship الذي يَنصُّ عمليًّا على أن كل مستوى من مستويات أمان المعلومات المذكورة سهل الاختراق من قِبَل المستوى الذي يَعلوه، وصعب الاختراق من قِبَل المستوى الذي يَدنوه، فمثلًا، أمان المعلومات على مستوى المنظَّمة يَعني أنه يُمكِن للمعلومات المَحميَّة التي تَمتلِكها المنظَّمة أن تُختَرَق من قِبَل المستوى الأعلى (وهو الدولة أو دول أخرى متقدمة في هذا الحقل)، وفي الوقت نفسه لا يُمكِن اختراقها من قِبَل المستوى الأدنى (وهو الفرد أو شركات أصغر من المنظَّمة). أيضًا، أمان المعلومات على مستوى الدولة يَعني أنه قد يُمكِن للمعلومات المَحميَّة التي تَمتلِكها الدولة أن تُختَرَق من قِبَل المستوى الأعلى (وهو دول أخرى متقدمة في هذا الحقل)، وفي الوقت نفسه يَصعُب اختراقها من قِبَل المستوى الأدنى (وهو المنظَّمة أو الفرد).

إنَّ العلاقة السابقة بين مستويات أمان المعلومات ليسَت موضوعة أو مرسومة سابقًا (أو حتَّى موصَّى بها)، إنَّما هي علاقة طبيعيَّة عملية نابِعة من مقدار إمكانات وقدرات واهتمام كل مستوى (أي الفرد أو المنظَّمة أو الدولة أو العالَم)، فمثلًا لو كان الحديث عن أمان المعلومات على مستوى المنظَّمة يَتبيَّن أنَّ الدولة ببعض أو كل إمكاناتها تَستطيع أن تَخترِق أمان المعلومات التي تَمتلِكها منظَّمة إذا وجدَت الدولة ضرورة لذلك، وفي الوقت نفسه يصعب على الفرد أن يَخترِق أمان المعلومات التي تَمتلِكها منظَّمة. في

الواقع، يُفترض منطقيًّا أنَّ الفرد لن يُنفِق (أو يُضحِّي) بأموال طائلة لسرقة معلومات تَمتلِكها منظَّمة ما، فالقيمة الماديَّة لهذه المعلومات أقل من الأموال التي من المُمكِن أن يُنفِقها الفرد من أجل القيام بذلك، فلو كان الأمر كذلك، وأَنفَقَ الفرد أموالًا طائلة للاستحواذ على معلومات مَحميَّة للمنظَّمة قيمتها الماديَّة تَقلُّ عن الأموال التي أَنفَقَها ذلك الفرد، فهذا حتمًا ليس فردًا، وإنَّما منظَّمة لها أهداف وراء ذلك (أو فردًا يُمثِّل منظَّمة ما)، أو قد تكون هذه المعلومات ذات أهميَّة كبيرة بالنسبة إلى الفرد وأهميَّة أقل بالنسبة إلى المنظَّمة، ولنعطِ مثالًا آخر، وليَكُن عن أمان المعلومات على مستوى الدولة، فمن الممكن أن يُختَرَق أمان المعلومات التي تَمتلِكها دولة ما من قِبَل طرف دولي (دولة متقدمة في هذا الحقل)، أو من تعاون وكالتَي استخبارات أو أكثر؛ لأنَّ الدول المعنيَّة بعمليَّة التجسُّس والاختراق، التي تُمثِّلها وكالات الاستخبارات، ستَضَع إمكانات وموارد ضخمة للقيام بذلك، تَفوق ما تَمتلِكه الدولة المراد اختراق أمان معلوماتها من موارِد وإمكانات، وفي الوقت نفسه، سوف يَكون من الصعب على أي منظَّمة أن تَخترِق أمان المعلومات التي تَمتلِكها الدولة (إلا إذا كانت هذه المنظَّمة مَدعومة مثلًا من قِبَل وكالات استخبارات دول أخرى).

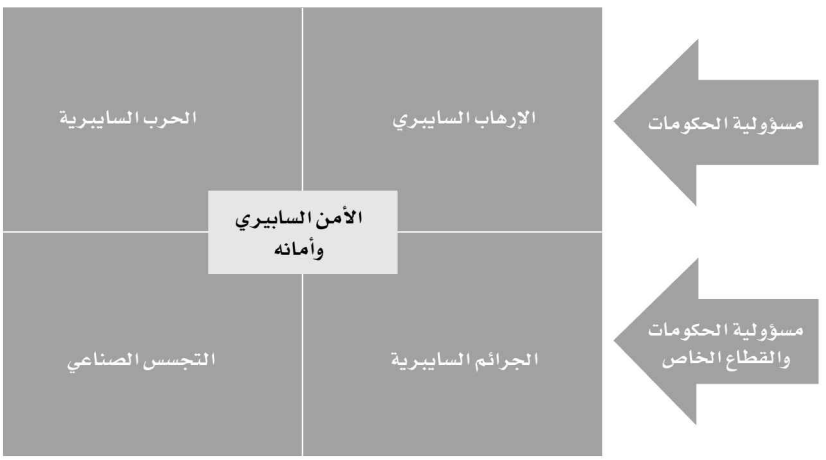
تُدعَى العلاقة بين الأطراف من مستوى الأمان نفسه **العلاقة التنافسيَّة** Competitive relationship، وقد يُحاوِل طرفٌ ما اختراق أمان معلومات طرف آخر من المستوى نفسه، ويَعتمِد نجاح محاولته على الإمكانات والموارِد المتاحة له للقيام بمحاولة الاختراق، ومن أمثلة هذه العلاقة التنافسيَّة قيام منظَّمة ما بسرقة معلومات ذات قيمة من منظَّمة أخرى، أو تَجسُّس دولة ما على دولة أخرى.

من المُمكِن تغيير مستوى أمان معلوماتٍ ما من خلال رفع هذا المستوى أو تخفيضه، فمثلًا يُمكِن أن يقوم فردٌ ما برفع مستوى أمان معلوماته ليَصِل إلى نفس مستوى أمان معلومات منظَّمة ما، ولكن مع هذا الإجراء ستَزداد تكلفة عمله، بمعنى آخر، سيَقوم الفرد الراغِب في رفع مستوى أمان معلوماته إلى نفس مستوى أمان معلومات منظَّمة

ما بدفع تكاليف إضافية قد تَصِل إلى التكاليف نفسها التي تَدفعُها المنظَّمة لحماية معلوماتها السريَّة، وقد يَبدو ذلك غباءً من الفرد إلا إذا كانت هذه المعلومات التي يُريد حمايتها ذات قيمة ماديَّة أكبر من تِلْك التكاليف الجاهِزة لدفعها، أو أنَّ هذا الفرد مدفوع للقيام بذلك، وهو مكلَّف بحمايتها، ومثال آخر على تغيير مستوى أمان المعلومات هو أن تَقوم منظَّمة ما بتخفيض مستوى أمان معلوماتها - إلى مستوى أمان معلومات الفرد - بعد أن تَرى أنَّها ليست ذات أهميَّة بالغة، ولا تَستحِق التكاليف المدفوعة لحمايتها.

ثمة تصور آخر للعلاقة بين مستويات الأمن والأمان المعلوماتي (السايبري) وهو بتصنيفه بحسب نوع التهديد والجهة المسؤولة عن الحماية ضده، ويبين الشكل توصيفًا مبسطًا لهذا التصور.

نموذج في مسؤوليات الأمن السايبري (مسؤولية الفرد محدودة)



2.4 درجات أمان المعلومات من حيث سريتها

لقد تَمَّ فيما سبق تَعَرُّفُ مستويات أمان المعلومات الأربعة التي ترسم الحدود الفاصلة بين حالات أمان المعلومات وفقًا لمتطلَّبات كل فئة من فئات المجتمع، ولقد حُدِّدت العلاقة التي تَربط بين هذه المستويات، ويُمكِن لمستويات أمان المعلومات أن

تُعطي فكرة عن أهميَّة المعلومات ومستوى حساسيَّتها بالنسبة إلى كل فئة من فئات المجتمع، ولكنَّ قياس أمان المعلومات من مَنظور أهميَّتها ومستوى حساسيَّتها من خلال درجات أمانها.

تقاس درجات أمان المعلومات من منطلَق قيمتها الماديَّة أو المعنويَّة أو المَجازيَّة، التي تَتطلَّب رَد فعل مناسِب يَتمثَّل في القيام بإجراءات لحمايتها، ويَتحدَّد مستوى هذه الإجراءات وفعاليتها اعتمادًا على القيمة الماديَّة أو المعنويَّة أو المَجازيَّة لتِلْك المعلومات. إذًا، فالقيمة تُحدِّد الدرجة المطلوبة من الأمان والكافية لكل طرف مَعني بتِلْك المعلومات، وهذا يَعني أن نَترُك مسألة إضفاء درجة أمان محدَّدة للمعلومات إلى المعلومات نفسها. أمّا الإجراء المقابِل والسليم للقيام فعليًّا بعمليَّة تحقيق هذه الدرجة من الأمان فهو من مهام الطرف الذي يَمتلِك تِلْك المعلومات.

يَندرِج أمان المعلومات مهما كانت قيمتها الماديَّة أو المعنويَّة أو المَجازيَّة في ثلاث درجات تُدعَى درجات أمان المعلومات، ودرجات أمان المعلومات هي:

1. الدرجة الأولى: **أمان المعلومات المطلَق.**
2. الدرجة الثانية: **أمان المعلومات العادي.**
3. الدرجة الثالثة: **أمان المعلومات المتكيِّف.**

1.2.4 الدرجة الأولى: أمان المعلومات المطلَق

الأمان المطلَق هو أقصى درجات الأمان الذي يُضفيه الطرف المالِك للمعلومات، فليسَ من السهل توفير الأمان المطلَق لأيّ معلومات مُراد حمايتها، فتكلفة وَضْع السياسات والخطط وتجهيز الأدوات اللازمة لإيجاد الأمان المطلَق باهظة جدًّا.

ومن صفات المعلومات المَحميَّة بدرجة الأمان المطلَق أنها ذات حساسيَّة عالية جدًّا، وتَحتوي على مواد يُمكِن، إذا تمَّ افتضاحها عَمْدًا أو عن غَير قَصْد، أن تُؤدِّي إلى

كوارث يُخيِّم تأثيرها السلبي على الأمن لدولة ما، أو قد تُسبِّب حربًا بين دولتين أو أكثر، فهي عادةً معلومات لا تَرتبِط بفرد أو منظَّمة، بل هي ذات أهميَّة كبرى على مستوى الدولة أو على المستوى الدولي، وأنَّ مستوى تصنيفها (بالنسبة إلى الدولة أو العالم) هو (سري للغايةUltra-Secret) أو (**سرِّي جدًّا** Top Secret) فقط، وإنَّ أمثلة المعلومات المَحميَّة بدرجة الأمان المطلَق قليلة، ومن تِلْك الأمثلة الخطط العسكريَّة، ومواعيد إطلاق العمليات العسكريَّة، وتصاميم الأسلحة والمعدَّات الحربيَّة، والمواد المتعلِّقة بإنتاج أسلحة الدمار الشامل واستخدامها، والمَحميَّة جميعها تحت مستوى التصنيف (سرِّي جدًّا) كما في الولايات المتَّحدة الأمريكيَّة، أو المعلومات العسكريَّة التي تَتعلَّق بخطَط دفاعية متَّفَق عليها بين دولتين أو أكثر والمَحميَّة أيضًا تحت مستوى التصنيف (سري للغاية) أو (سرِّي جدًّا) كتِلْك المتبادَلة بين دول منظَّمة حلف شمال الأطلسي.

إنَّ أهم ما يُذكَر في درجة أمان المعلومات المطلَق أنَّ صفة الأمان فيها (ثابِتة ودائِمة) مهما تَغيَّرت الظروف المحيطة، وأنَّ الأمان نفسه يَمتدُّ لمدة زمنيَّة طويلة، ومن الضروري جدًّا أن نُولي اهتمامًا لموضوع (المدة الزمنيَّة) التي يَجب أن تَظل المعلومات في غضونها مَحميَّة، ويَجب عند اعتماد درجة الأمان المطلق لحماية معلوماتٍ ما أن يَتم أيضًا تحديد المدة الزمنيَّة التي يَنبغي أن تَبقى المعلومات في غضونها مَحميَّة، والأهم من ذلك أن يَتم الحفاظ على مستوى نوعيَّة الإجراءات المتَّخَذة نفسه مهما تَقادَم الزمن ضمن المدة المحدَّدة لذلك.

إنَّ عددًا من حكومات الدول يَقوم بتمديد المدة الزمنيَّة لإبقاء المعلومات ذات مستوى التصنيف (سري للغاية) أو (سرِّي جدًّا) مصنَّفة سريَّة، وتَقوم أحيانًا بتعديل مستوى تصنيفها السرِّي، بل وحتَّى إلغاء تصنيفها سريَّة، وتَتَّبِع تِلْك الحكومات معايير محدَّدة لإلغاء تصنيف المعلومات سريَّة، ومن بين هذه المعايير مرور زمن معيَّن أو وقوع حدثٍ ما كما هو الحال في الولايات المتحدة الأمريكية، فقد يَفترِض الأمر التنفيذي ذو الرقم 13526 الذي أَصدَره الرئيس الأمريكي Barack Obama عام 2009 أن يَتم إلغاء

تصنيف المعلومات سريَّة تلقائيًّا عند مرور مدة زمنيَّة معيَّنة أو وقوع حدثٍ ما، والأمر التنفيذي نفسه يَنصُّ على عدم إبقاء المعلومات مصنَّفة سريَّة إلى أجل غير مسمَّى، ويَعتقِد Arvin Quist [1] أنَّ عملية إلغاء تصنيف المعلومات سريَّة بعد مرور زمن معيَّن أو وقوع حدثٍ ما، ضروريَّة من أجل تَفادي التكاليف الإضافيَّة غير الضروريَّة لإبقاء المعلومات مصنَّفة سريَّة، ولكنَّ ذلك الاعتقاد غير صحيح في بعض الحالات؛ لأنَّه من المُمكِن أن يُعَاد استخدام المعلومات المصنَّفة سريَّة ذات المستوى (سري للغاية) أو (سرِّي جدًّا) في أوقات لاحقة ولو بصيغةٍ أخرى، فمثلًا لو كانت هذه المعلومات تَتعلَّق بتصاميم أسلحة، يُمكِن أن يُعاد استخدامها لتطوير تِلْك الأسلحة وإضافة التحسينات عليها، وأيضًا لو تَمَّ رفع الحماية عن المعلومات ذات المستوى (سرِّي جدًّا) التي تَشرَح خطَّة العمل العسكري لدولة ما في حربٍ ما بعد نشوبها وانتهائها (استنادًا إلى مبدأ إلغاء تصنيف المعلومات سريَّة بعد وقوع حدثٍ ما)، فقد يَستفيد أعداء الدولة المَعنيَّة من تفاصيل خطَّة العمل العسكري، ويَستثمِرونها لاحقًا في حروب أخرى، ولكن ثَمَّة معلومات، وإنْ كانت ذات حساسيَّة عالية، وتَتطلَّب حماية مطلَقة يَمكِن بسبب طبيعتها قَبول المعايير التي تَقتضي إلغاء تصنيفها سريَّة عند مرور زمن معيَّن أو وقوع حدثٍ ما، مثل موعد إطلاق عمل عسكري ضد دولةٍ ما، كما سَنرى لاحقًا في درجة أمان المعلومات المتكيِّف.

والسؤال الذي يَجب أن يُطرَح الآن هو: (ما **الإجراءات** التي يَنبغي أن تُتَّخَذ لحماية المعلومات في درجة الأمان المطلَق؟)، فلا يُمكِن الإجابة بدقَّة وبالتفصيل عن هذا السؤال بسبب اختلاف الظروف بين طرف وآخر (أي بين دولة أو منظَّمة دوليَّة وأخرى)، ولكن يُمكِن تحديد صفة هذه الإجراءات ونوعيَّتها على نحوٍ عام، وفي البداية يَجب أن يَتم وَضْعُ الخطَط لحماية المعلومات في درجة الأمان المطلَق من قِبَل خبراء متخصِّصين وبالتنسيق مع الجهات العليا المالِكة للمعلومات، بعدها يَنبغي تخصيص

(1) Arvin S. Quist: هو موظَّف متخصِّص في أمن المعلومات وفي تصنيفها، يَعمَل لدى مختبر Oak Ridge الوطني التابع لوزارة الطاقة الأمريكيَّة.

الأدوات والبرامج اللازمة لحماية المعلومات، على أن تكون على مستوى عالٍ من القوَّة والاحترافيَّة، والأهم من ذلك ألا يَتم توظيف و(استعارة) الأدوات والبرامج المطروحة تجاريًّا، وبمعنى آخر، يجب أن يَتم استخدام أدوات وبرامج خاصَّة ومختلفة كليًّا (سواء من ناحية التصميم أو من ناحية القوة والكفاءة) عن جميع ما هو معروف لدى العامَّة سواء أكانوا أفرادًا أم منظَّمات (أو حتَّى عن تِلْك الأدوات والبرامج المستخدَمة في بعض المؤسسات الرسميَّة الحكوميَّة المتوسطة أو الصغيرة التي لا يَمُتّ عملها بأي صلة بالأمن القومي)، فمثلًا عندما أَقرَّ المعهد القومي للمقاييس والتكنولوجيا في الولايات المتَّحدة الأمريكيَّة خوارزميَّة التعمية DES بوصفها مقياسًا فيدراليًّا، أجازَها للاستعمال في حماية الاتصالات الحكوميَّة غير المصنَّفة سريَّة فقط (إضافة إلى الاتصالات التجاريَّة للأفراد والمنظَّمات)، وحَيَّد عنها جميع المعلومات المصنَّفة سريَّة، الذي صَرَّح بأنَّ لها أدوات تعمويَّة خاصَّة لحمايتها، وسوف يَقتضي ذلك دون شك أن تَكون تكاليف تصميم الخطَط وتجهيز الأدوات والبرامج ووَضْعُها باهظة جدًّا، وعليه فسوف يَتم استخدام أموال من ميزانيَّة الدولة (أو ميزانيَّات دول عدَّة متحالِفة ومعنيَّة بالأمر) لتغطية تِلْك التكاليف الباهظة، وذلك مبرَّر جدًّا؛ كون المنفعة النهائيَّة من كل ذلك ستَصُبُّ في مصلحة الأمن الوطني للدولة أو الدول المتحالِفة.

2.2.4 الدرجة الثانية: أمان المعلومات العادي

النموذج الشائع من الأمان الذي يُضفَى إلى المعلومات الخاصَّة على نحوٍ واسع هو أمان المعلومات العادي، ولا تَعني كلمة (العادي) أنَّ الإجراءات المستخدَمة لحماية المعلومات في هذه الدرجة عاديَّة، أو أنَّ المعلومات نفسها من مستوى عادي، بل هي اصطلاح يُميِّز هذا الأمان العادي عن ذلك الأمان المطلَق الذي نُضفيه إلى المعلومات الفائقة الأهميَّة، ولكلمة (عادي) في اصطلاح (أمان المعلومات العادي) دلالة مهمة هنا، وهي أنَّ إجراءات الحماية المستخدَمة وعلى مستويات عدَّة (الفرد – المنظَّمة – الدولة

- العالَم) متعارَفة من ناحية التخطيط والتطبيق والنتائج المتوقَّعة من تنفيذها (وإنْ اختلَفَتْ شدَّة تِلْك الإجراءات بين الفرد أو المنظَّمة أو الدولة أو حتَّى الطرف الدولي).

على الرغم من أنَّ أمان المعلومات في الدرجة الثانية عادي، إلا أنَّ أهميَّة المعلومات نفسها تَختلِف بحسب اختلاف الأطراف المَعنيَّة بها وبحسب مستويات هذه الأطراف، فقد تَكون أهمية المعلومات على مستوى المنظَّمة أكبر بكثير من أهمية المعلومات على مستوى الفرد، وأهمية المعلومات على مستوى الدولة أكبر بكثير من أهمية المعلومات على مستوَيَي الفرد والمنظَّمة، وهذا الأمر طبيعي بسبب اختلاف أهمِّيات مضامينها، فعلى سبيل المثال، المعلومات الاستخباراتيَّة التي تَمتلِكها دولةٌ ما أهم بكثير من أرقام الحسابات المصرفيَّة التي يَمتلِكها فردٌ ما، إذ إنَّ خصم دولةٍ ما يَستطيع دفع أموال بعشرات أضعاف المال الذي قد يَمتلِكه فرد للحصول على المعلومات الاستخباراتيَّة لتِلْك الدولة، ولكنَّ الصفة المشتَرَكة بين هذه المعلومات المتعدِّدة المستويات (الفرد - المنظَّمة - الدولة - العالَم) والمَحميَّة بدرجة الأمان العادي هي أنَّ هذه المعلومات ذات حساسيَّة عاديَّة، ومعظمها لا يُؤدِّي إلى كوارث تُؤثِّر سلبًا في الأمن القومي لدولة ما، أو تُسبِّب حربًا بين دولتين أو أكثر، إذا تمَّ افتضاحها عَمْدًا أو عن غَير قَصْد، ولكن يُمكِن القول: إنَّ جميع المعلومات المرتبِطة بالفرد أو بالمنظَّمة، ومهما كانت طبيعتها ومدى أهميَّتها وعواقب افتضاحها، مَحميَّة تلقائيًّا بدرجة الأمان العادي.

أمّا بالنسبة إلى مستوَيَي الدولة والعالم، فجميع المعلومات المرتبِطة بهما والمصنَّفة سريَّة ومن مستويات التصنيف (**سرِّي** Secret) وما دون؛ أي (**خاص** Confidential) و(**محدود** Restricted) كما في قوانين دول عدَّة، ومهما كانت طبيعتها ومدى أهميَّتها وعواقب افتضاحها، مَحميَّة تلقائيًّا بدرجة الأمان العادي، ومن المُلاحَظ أنَّه لم يُشمَل في تبويب المعلومات المصنَّفة سريَّة بالنسبة إلى الدولة والعالَم ومن مستوى التصنيف (سرِّي جدًّا) ضمن درجة الأمان العادي؛ لأنَّ المعلومات المصنَّفة سريَّة من مستوى التصنيف (سري للغاية) أو (سرِّي جدًّا) بالنسبة إلى الدولة والعالَم مَحميَّة عادةً بدرجة الأمان المطلَق.

إنَّ صفة الأمان في درجة أمان المعلومات العادي (ثابِت ومؤقت)؛ أي إنَّ مستوى الحماية المخصَّص للمعلومات في هذه الدرجة ثابِت مهما تَغيَّرت الظروف المحيطة، وإنَّ الحماية نفسها تَستمرُّ مدة زمنيَّة مؤقَّتة ومحدَّدة مسبقًا وقابِلة للتمديد تلقائيًّا لحين الانتهاء من استثمار المعلومات، و(قابِلة للتمديد) تَعني أنه يُمكِن أن تَمتدّ المدة الزمنيَّة لأطول مِمَّا خُطِّطَ لها إنْ احتاجَ الأمر، دونَ القيام بإعادة التخطيط مرةً أخرى، والنقطة الجوهريَّة هنا هي أنَّ المدة الزمنيَّة المخطَّط لها في درجة الأمان العادي، ستَنتَهي بمجرَّد أن يُحقِّق مالِك المعلومات الغرض من هذه المعلومات، ويَجب التمييز هنا بين حالة (تخفيض مستوى أو رفع الحماية كليًّا عن المعلومات) في درجة الأمان العادي، وحالتها في درجة الأمان المتكيِّف الذي سنأتي عليه لاحقًا.

تَختلِف إجراءات حماية المعلومات في درجة الأمان العادي بين كل طرف على المستوى نفسه (أي على مستوى الفرد أو المنظَّمة أو الدولة أو العالَم) وبين كل طرف من كل مستوى من المستويات، فقد تَكون الطُّرُق التي يَستخدِمها فردٌ ما لحماية معلوماته مختلفة كليًّا عن الطُّرُق التي يَستخدِمها فردٌ آخر لحماية معلوماته (وهذا على مستوى الفرد). وكذلك على المستويات الأخرى؛ أي إنَّ «إجراءات حماية المعلومات في درجة الأمان العادي تَختلِف باختلاف كل طرف عن الآخر على المستوى نفسه وباختلاف كل مستوى عن الآخر» أمّا بالنسبة إلى تفاصيل تِلْك الإجراءات، مثل تصميم الخطَط ووَضْعها والأدوات والبرامج، فالأمر عائدٌ لتقدير الطرف المالِك للمعلومات، ولكن مهما اختلَفَت تقديرات الأطراف في ذلك، إلا أنَّها ستَستخدِم آليات وَضْع الخطَط المتعارَفة والأدوات والبرامج المطروحة تجاريًّا لحماية معلوماتها.

3.2.4 الدرجة الثالثة: أمان المعلومات المتكيِّف

ثَمَّة شكل من المعلومات مستخدَم في الشؤون الحياتيَّة العامَّة التي تَحتاج إلى حماية واهتمام من أصحابها، تَفرِض طبيعتها عليهم فيما بعد إمّا رفع مستوى حمايتها أو

تخفيض مستوى حمايتها أو إهمال حمايتها، وإنَّ الأساس في هذه المعلومات أنَّها مَحميَّة بإحدى الدرجتين السابقتين (الأولى أو الثانية)، لكنَّ الظروف المحيطة بمالِكها تَفرِض تغيير مستوى الاهتمام بها، فإمّا أن يَقوم مالِكها برفع مستوى حمايتها أو تخفيضه أو حتَّى إلغاء الحماية كليًّا. إذًا، تَحتاج مثل هذه المعلومات إلى حماية يَتكيَّف مستواها مع مستوى أهميَّة تِلْك المعلومات بالنسبة إلى مالِكها في ذلك الزمن وفي ذلك الظرف، ومن ثم، فإنَّ أفضل حماية لمثل تِلْك المعلومات هي الحماية المتكيِّفة.

أمان المعلومات في هذا النوع من الحماية يَتكيَّف مع الزمن والأحداث المحيطة بمالِك تِلْك المعلومات، فمن المُمكِن أن تَزداد أهميَّة المعلومات (التي قد تَكون في ذلك الوقت مَحميَّة بالدرجة الثانية، وهي الحماية العاديَّة) لتَصِل إلى مستوى ذي حساسيَّة عاليَّة جدًّا، ومن ثم، سيَتطلَّب أن تُصبِح المعلومات مَحميَّة بالدرجة الأولى، وهي الحماية المطلَقَة، أو أن تَقل أهميَّتها (التي قد تَكون في ذلك الوقت مَحميَّة بالدرجة الأولى) لتَصِل إلى مستوى عادي، وذلك لا يَتطلَّب إلا أن تُصبِح المعلومات مَحميَّة بالدرجة الثانية، وقد تَقلُّ أهميَّة المعلومات لتَصِل إلى مستوى يُمكِن من خلاله أن تُرفَع الحماية كليًّا عنها.

يَتكيَّف أمان المعلومات في هذه الدرجة مع عامِلَين اثنين هما: الزمن، والأحداث المحيطة، ويَعني التكيف مع الزمن أنَّ المعلومات قد تُصبِح مع مرور الزمن إمّا ذات أهميَّة كبيرة، أو قد تَفقد أهميَّتها لتُصبِح عديمة القيمة، أمّا أن يَكون أمان المعلومات متكيِّفًا مع الأحداث المحيطة فيَعني أنَّها قد تُصبِح عند حدوث أمرٍ ما إمّا ذات أهميَّة كبيرة، أو قد تَفقد أهميَّتها لتُصبِح عديمة القيمة. إذًا، نَستطيع القول ممَّا سَبَق: إنَّ صفة الأمان في درجة أمان المعلومات المتكيِّف (متغيِّرة).

ومن الأمثلة الواقعيَّة على رَفْع مستوى حماية معلوماتٍ ما من الدرجة الثانية إلى الدرجة الأولى القيام برَفْع مستوى حماية معلومات عسكريَّة عند نشوب حرب، فيَجب التذكير هنا بأنَّ بعض المعلومات العسكريَّة عادةً مصنَّفة سريَّة لدى كثير من حكومات

الدول، وليس بالضرورة أن يَكون مستوى تصنيفها (سري للغاية) أو (سرِّي جدًّا) إلا عند نشوب حرب.

من البدهي ملاحظة أنَّ رَفْع مستوى حماية معلوماتٍ ما من الدرجة الثانية إلى الدرجة الأولى لا يُمكِن أن يَتم إلا من خلال أطراف كبرى تَستطيع تَحمُّل التكاليف الباهظة لإجراءات الحماية المطلَقة ذات الدرجة الأولى كحكومة ما.

من أمثلة تخفيض مستوى حماية معلوماتٍ ما من الدرجة الأولى إلى الدرجة الثانية خطَّة عسكريَّة لحرب متوقَّعة تَكون من الأساس مَحميَّة بالدرجة الأولى قبل نُشوب الحرب، يُمكِن بعد انتهاء الحرب تخفيض مستوى حمايتها إلى الدرجة الثانية، أو حتَّى رفع الحماية عنها، وذلك من أجل تَفادي التكاليف الباهظة في إبقائها مَحميَّة بالدرجة الأولى، وفي هذا المثال تَكيَّف أمان المعلومات (والمعلومات هي هنا الخطَّة العسكريَّة) مع عامِل الأحداث المحيطة، حيث أجازَ حَدَث وقوع الحرب أن تُصبِح تِلْك المعلومات مَحميَّة بالدرجة الثانية.

تُماثِل عبارة (تخفيض مستوى حماية معلوماتٍ ما من الدرجة الثانية) معنى (رَفْع الحماية كليًّا عن المعلومات)، وذُكِرَ في 2,2,3 أنَّ المعلومات المَحميَّة بالدرجة الثانية، وهي الحماية العاديَّة قد تَكون إمّا لأفراد أو منظَّمات (أو حتَّى مؤسَّسات رسميَّة حكوميَّة لا يَمتُّ عملها بأي صلة بالأمن القومي)، وإنَّ الأمثلة على تخفيض مستوى حماية معلوماتٍ ما من الدرجة الثانية كثيرة جدًّا، ومنها رَفْع الحماية كليًّا عن كلمات السرّ الخاصَّة بصناديق البريد الإلكتروني بعد إغلاقها، وأرقام الحسابات المصرفيَّة بعد إقفالها، وهذا بلا شك بالنسبة إلى الأفراد، فمن المُلاحَظ أنَّ أمان المعلومات السابقة يَتكيَّف مع عامل الأحداث المحيطة، كإغلاق صناديق البريد الإلكتروني أو إقفال الحسابات المصرفيَّة، وأمّا بالنسبة إلى المنظَّمات، فمن أمثلة تخفيض مستوى حماية معلوماتٍ ما من الدرجة الثانية قيام مكتب حوالات ماليَّة برَفْع الحماية كليًّا عن المعلومات التي

تَتضمَّن قيمة مبلغ حوالة ماليَّة مرسَلة بعد تسلّمها من قِبَل صاحِبها، وهنا أمان معلومات القيمة الماليَّة للحوالة يَتكيَّف مع عامِلَي الزمن والأحداث المحيطة معًا (فإمّا أن تَمُر مدة زمنيَّة معيَّنة دون أن يَقوم صاحب الحوالة الماليَّة بتسلّمها، وعندئذٍ يَتم إرجاع قيمتها إلى الفرع الخاص بالبلد المرسِل، أو أن يَقَع حَدَث تسلّم الحوالة الماليَّة من قِبَل صاحِبها، وفي كلتا الحالتين تُصبِح معرفة قيمة الحوالة الماليَّة من قِبَل آخرين غير صاحِبها عديمة الفائدة)، ويَقوم كثير من مكاتب الحوالات الماليَّة بإخفاء تفاصيل قيمة الحوالة الماليَّة ومرسِلها عن جميع الأشخاص باستثناء صاحِبها، والسبب كما يُعتَقَد، هو من أجل حماية صاحبها من قيام لصٍّ ما بالترصُّد له لسرقة حوالته الماليَّة بعد معرفته بقيمتها التي قد تَكون كبيرة بالنسبة إلى اللِّصّ (التي قيمتها بالنسبة إلى اللِّصّ تستحِق عناء التَّرصُّد لصاحِب الحوالة الماليَّة وسرقتها منه)، ومثال آخر عن تخفيض مستوى حماية معلوماتٍ ما من الدرجة الثانية بالنسبة إلى المنظَّمات هو رَفْع الحماية كليًّا عن جميع معلومات العمليات التجاريَّة أو الصناعيَّة لشركة ما بعد انتهاء عملها.

أمّا بالنسبة إلى رَفْع الحماية كليًّا عن معلومات مَحميَّة بالدرجة الأولى فمثاله المعلومات التي تَتضمَّن موعد بدء العمليات العسكريَّة لدولة ما ضد دولة أخرى، المصنَّفة من مستوى التصنيف (سري للغاية) أو (سرِّي جدًّا) تَكون في الأساس مَحميَّة بالدرجة الأولى؛ أي الحماية المطلَقة، ولكن في أثناء نُشوب الحرب وبعده تَفقد هذه المعلومات قيمتها المعنويَّة بشكل كامل، وعليه ليسَ بالضرورة إبقاؤها مصنَّفة سريَّة، ويُمكِن تَداولها.

يَعتمِد اختيار **إجراءات** حماية المعلومات في درجة الأمان المتكيِّف على مستوى الحماية الجديد المقرَّر للمعلومات بعد تغيير درجة أمانها، فإذا كانت المعلومات مَحميَّة بدرجة الأمان المطلَق، وتَمَّ تخفيض مستوى حمايتها لتُصبِح مَحميَّة بدرجة الأمان العادي، يَنبغي اعتماد إجراءات الحماية المتعارَفة في درجة الأمان العادي، وأمّا إذا كانت المعلومات مَحميَّة بدرجة الأمان العادي، وتمَّ رَفْع مستوى حمايتها لتُصبِح مَحميَّة

بدرجة الأمان المطلَق، يَنبغي عندها اعتماد إجراءات الحماية المخصَّصة للمعلومات ذات الحساسيَّة العالية جدًّا، أو المعلومات المصنَّفة سريَّة، ومن مستوى التصنيف (سرِّي جدًّا). وعند رَفْع الحماية كليًّا عن المعلومات (مهما كانت درجة أمانها السابق)، فيُمكِن عندها إلغاء إجراءات الحماية عنها.

3.4 الأمان وعلاقته بالتكلفة أو بالزمن

عَرَّف Bruce Schneier قاعدة عامَّة لقياس أمان المعلومات المعمَّاة بخوارزميَّة تعمية، تَستنِد إلى تكلفة كسر الخوارزميَّة والمدة الزمنيَّة المطلوبة لذلك، ويُمكِن تطبيق تِلْك القاعدة لقياس أمان المعلومات المَحميَّة مهما كانت قيمتها الماديَّة أو المعنويَّة أو المَجازيِّة، ومن هنا يُمكِن طَرْح مبدأ قياس أمان المعلومات استنادًا إلى عامِلَين اثنين هما: التكلفة الماليَّة والمدة الزمنيَّة، وهذا المبدأ هو (مبدأ الأمان بالتكلفة أو بالزمن).

يَنصُّ (مبدأ الأمان بالتكلفة أو بالزمن) على ما يأتي: إذا كانت التكلفة الماليَّة المطلوبة لاختراق أمان معلوماتٍ ما أكبر من القيمة الماليَّة الفعلية[1] لتِلْك المعلومات، فالمعلومات آمنة، وإذا كانت المدة الزمنيَّة المطلوبة لاختراق أمان معلوماتٍ ما أطول من المدة الزمنيَّة التي يَنبغي أن تَظل المعلومات في غضونها مَحميَّة، فالمعلومات آمنة، ويُرادِف مَعنى أن تَكون المعلومات آمنة في المبدأ السابق معنى أنَّ النظام الذي يَحتوي على تِلْك المعلومات آمن وحصين من جميع الهجمات التي يُمكِن أن تُشَنّ عليه، خاصةً إذا كان نظامًا حاسوبيًّا، وإنَّ الأساس في (مبدأ الأمان بالتكلفة أو بالزمن) هو المقارَنة بين طرفين في كل من الحالتين (**الأمان بالتكلفة**) و(**الأمان بالزمن**)، ففي حالة (الأمان بالتكلفة) عنصر المقارَنة هو المال، أمّا في حالة (الأمان بالزمن) فعنصر المقارَنة هو الزمن، وأمّا طَرفَا المقارَنة في الحالة الأولى فهما التكلفة الماليَّة لاختراق

(1) القيمة الماليَّة الفعليَّة للمعلومات هي القيمة الماليَّة الحقيقيَّة الآنيَّة لتِلْك المعلومات (أي قيمتها الماليَّة في وقتها).

أمان المعلومات والقيمة الماليَّة للمعلومات المَحميَّة، وطَرفَا المقارَنة في الحالة الثانية هما المدة الزمنيَّة لاختراق أمان المعلومات والمدَّة الزمنيَّة لإبقاء المعلومات مَحميَّة، وسوف نَتحدَّث عن كِلتا الحالتين (الأمان بالتكلفة) و(الأمان بالزمن) من المبدأ السابق بالتفصيل.

1.3.4 قياس الأمان بالتكلفة

تَعني هذه الحالة أنَّه إذا تَجاوزَت التكلفة الماليَّة لاختراق أمان معلوماتٍ ما القيمة الماليَّة الفعليَّة التي تَحمِلها تِلْك المعلومات، عندها يُمكِننا اعتبار تِلْك المعلومات آمنة من الناحية الاقتصادية، فكلَّما ازدادَت التكلفة الماليَّة المطلوبة لاختراق أمان المعلومات، ازدادَ أمان المعلومات، ومن المُمكِن أن يُوجَد أطراف قادرون على دفع تكاليف ماليَّة أكثر للوصول إلى المعلومات المَحميَّة، وتَعود مَهمَّة زيادة التكلفة الماليَّة لاختراق أمان معلوماتٍ ما إلى الطرف المالِك لتِلْك المعلومات، وتَتمثَّل مَهمَّته في تمديد مجال الأمان من خلال تعزيز إجراءات أمن المعلومات ورَفْع كفاءة أدوات حماية تِلْك المعلومات.

لا يَنطبِق قياس أمان المعلومات بالتكلفة إلا على المعلومات ذات القيمة الماديَّة، فالشركة التجاريَّة المتنافِسة مع شركة تجاريَّة أخرى تَستطيع أن تَدفَع أموالًا لقاء الوصول إلى معلومات ذات قيمة ماليَّة عالية بالنسبة إليها، إذا ارتَأتْ أنَّ مقدار الأموال المستعِدَّة لدَفْعها أقل من القيمة الماليَّة لتِلْك المعلومات، أمّا المعلومات ذات القيمة المعنويَّة، كالمعلومات المصنَّفة (سريَّة للغاية) أو (سرية جدًّا) لدى حكومات الدول (التي تَحمِل على سبيل المثال أهميَّة كبيرة على مستوى الدولة أو على المستوى الدولي)، فلا تَنطبِق عليها هذه الحالة، فمن المُمكِن أن تَقوم دولة ما (أو دول عدَّة مشارِكة) بدَفْع أموال كثيرة لقاء الحصول على معلومات مصنَّفة سريَّة لدولة أخرى، إلا إذا كانت هذه المعلومات

المصنَّفة سريَّة ذات طابع اقتصادي (كمشروعات تجاريَّة مستقبليَّة حكوميَّة) ومن غير المعقول إنفاق أموال لاختراق أمانها أكثر من قيمة تِلْك المعلومات[1].

2.3.4 قياس الأمان بالزمن

خلافًا للحالة السابقة المرتَبِطة بالمال، تَرتبِط هذه الحالة بالزمن، وتَعني أنَّه إذا كانت المدَّة الزمنيَّة المطلوبة لاختراق أمان معلوماتٍ ما أطول من المدة الزمنيَّة المطلوب أن تَبقى تِلْك المعلومات في غضونها مَحميَّة، عندها يُمكِننا اعتبار تِلْك المعلومات آمنة أمانًا كافيًا، فكلَّما طَالَت المدة الزمنيَّة المطلوبة لاختراق أمان المعلومات، ازدادَ أمان المعلومات.

يَنبغي أن يَتم تقدير المدة الزمنيَّة المطلوبة لاختراق أمان معلوماتٍ ما على نحوٍ مختلف من الجهتين: جهة الطرف المالِك للمعلومات، وجهة الطرف المخترِق، ويَجب على الطرف المالِك للمعلومات المَحميَّة أن يَضَع تَصوُّرًا يرى فيه أنَّ المدة الزمنيَّة التي ستَأْخُذ من وقت الطرف المخترِق للوصول إلى تِلْك المعلومات قصيرة، ويَنبغي للطرف المخترِق أن يَضَع تَصوُّرًا يرى فيه أنَّ المدة الزمنيَّة التي ستَأْخُذ من وقته لاختراق أمان تِلْك المعلومات طويلة؛ أي إن تقديرات المدة الزمنيَّة لاختراق أمان المعلومات لدى الجهتين هي التي تحدد أمان المعلومات في حالة (الأمان بالزمن).

يَنطبِق قياس أمان المعلومات بالزمن على المعلومات ذات القيمة الماديَّة والقيمة المعنويَّة والقيمة المَجازيَّة، وبالنسبة إلى المعلومات ذات القيمة الماديَّة، فمثلًا إذا كان الوقت الذي ستَستغرِقه شركة تجاريَّة ما لاختراق أمان معلومات ذات قيمة ماليَّة معتَبَرة من شركة تجاريَّة أخرى أطول من المدَّة الزمنيَّة المخطَّط أن تَظل المعلومات

---

(1) قد تَقوم دولة ما بدفع تكاليف ماليَّة ضخمة يَتجاوَز مقدارها قيمة المعلومات المصنَّفة سريَّة ذات الطابع الاقتصادي لدولة أخرى إذا كان هَدَف الأولى استثمار تِلْك المعلومات لتدمير اقتصاد الثانية.

في غضونها مَحميَّة، عندها ستَكون معلومات الشركة التجاريَّة الأخرى آمنة، أمّا إذا استطاعَت الشركة التجاريَّة الأولى الوصول إلى معلومات الشركة التجاريَّة الثانية في الوقت الذي تَكون فيه هذه المعلومات مَحميَّة، فعندها تَكون الشركة التجاريَّة الثانية قد تَكبَّدَت خسائر ماليَّة من جَرَّاء ذلك، وتَحصَل هذه المحاولات كثيرًا في عالَم الأعمال، وبالنسبة إلى المعلومات ذات القيمة المعنويَّة (كالمعلومات المصنَّفة سريَّة لدى كثير من الدول والمنظَّمات الدولية)، فيَنبغي للأطراف المالِكة لهذه المعلومات أن تَحميها لحين مرور زمن معيَّن أو وقوع حدثٍ ما، وأكبر مثال على هذا هو العبارة التي تَنصُّ على أن يَتم إلغاء تصنيف المعلومات على أنها سريَّة تلقائيًّا بعد مرور زمن معيَّن أو وقوع حدثٍ ما في الأمر التنفيذي ذي الرقم 13526 الذي أصدَرَه الرئيس الأمريكي عام 2009م، وأمّا بالنسبة إلى المعلومات ذات القيمة المَجازيَّة (مثل كلمات السرّ الخاصَّة بصناديق البريد الإلكتروني أو المذكِّرات الشخصيَّة)، فإذا كان مثلًا الوقت الذي سَيستَغرِقه طرفٌ ما محاولًا اختراق أمان كلمات السرّ الخاصَّة بصناديق البريد الإلكتروني لطرفٍ آخر أكبر من المدَّة الزمنيَّة المخطَّط أن تَبقى كلمات السرِّ مَحميَّة ودون تغيير، فعندها كلمات السرّ تِلْك آمنة.

الفصل الخامس

إدارة أمـن المـعـلومـات وأمانها

لقد تَعدَّدت الاصطلاحات التي تُشير إلى مجموع العمليَّات الآتية: كيفيَّة تَقييم المعلومات وإدارة الأخطار ووَضْع الإجراءات المضادَّة التي تَكفَل حماية المعلومات في حقل أمن المعلومات، فمِنْ هذه الاصطلاحات مصطلح (**أمن العمليَّات** Operations security) الذي استخدَمَته حكومة الولايات المتَّحدة الأمريكيَّة لاحتواء العمليَّات المذكورة، وإنَّ معظم المنشورات في هذا الحقل تُسمِّي مجموع العمليَّات المذكورة **إدارة الأخطار** Risk management، ولكن لأنَّ مجموع هذه العمليَّات يَهدُف في النهاية إلى وَضْع المعلومات في حالة الأمان (بغَضِّ النظر عن مستويات هذا الأمان) ويَندرِج ضِمْن توجيهٍ واحدٍ يَقوده، فيُمكِن تَسميته: (**إدارة أمن المعلومات** Information security management)، وإدارة أمن المعلومات هي مجموع العمليَّات التي تَضمَن إدخال المعلومات وإبقاءها في وَضْع الأمان من خلال تَقييمها، وتَحديد الأخطار التي تُحيط بها وبالمحيط الذي يَحتويها، وتخطيط وتطبيق إجراءات الأمن التي تَحميها، وتخطيط وتطبيق إجراءات الأمان التي تُحافِظ على إبقائها في وَضْع الأمان، ويَتمثَّل الهدف الأساسي لإدارة أمن المعلومات في حماية المعلومات من السرقة أو الإفشاء أو التخريب، ويُدعَى الفرد الذي يَتولَّى إدارة أمن المعلومات **مدير أمن المعلومات**، ومدير أمن المعلومات هو إمّا مالِك المعلومات الذي

يَمتلِك قيمتها بالكامل، ويَتحمَّل مسؤولية سرقتها أو إفشائها أو تخريبها، أو القيِّم الذي تَقَع على عاتقه مسؤوليَّة سرقة المعلومات أو إفشائها أو تخريبها.

تُطبَّق إدارة أمن المعلومات على نماذج المعلومات الخاصَّة الثلاثة، وهي المعلومات ذات القيمة الماديَّة، أو المعنويَّة، أو المَجازيَّة، ويُدعَى تطبيق إدارة أمن المعلومات على هذه النماذج الثلاثة: إدارة المعلومات ذات القيمة الماديَّة، أو المعنوية، أو المجازية على التوالي.

1.5 مفاهيم أساسيَّة

سوف يَتم الحديث فيما يأتي عن المفاهيم الأساسيَّة المرتَبِطة بإدارة أمن المعلومات.

1.1.5 تحديد المعلومات وتقييمها

لا بد عند تطبيق إدارة أمن المعلومات من معرفة المعلومات الخاصَّة المرَاد حمايتها وتحديدها، التي تَتطلَّب إجراءات أمن وإجراءات أمان محدَّدة تَتناسَب مع قيمتها أو مع الأخطار ومستوى الأمن المطلوب لها. إنَّ الخطوة الأساسيَّة في تطبيق إدارة أمن المعلومات هي تحديد المعلومات وتقييمها، ويَتم تحديد المعلومات الخاصَّة بتمييزها ضمن مجموعة من المعلومات العاديَّة أو البيانات المتوافِرة، ومن ثم إثبات أهميَّتها إمّا ماديًّا أو معنويًّا أو مجازيًّا بالنسبة إلى الطرفين مالِك المعلومات والخصم معًا، ومعنى (إثبات أهميَّتها بالنسبة إلى الطرفين) تأكيد وجود طرف آخر (وهو الخصم) لديه مصلحة أو منفعة من الوصول إلى هذه المعلومات تُؤذي المصالح الماديَّة أو المعنويَّة أو المَجازيَّة لمالِك المعلومات، وبعد تحديد المعلومات، تُقيَّم إمَّا ماديًّا أو معنويًّا أو مجازيًّا، والهدف من تقييم المعلومات هو ضمان عدم تَجاوز التكلفة الماليَّة لتطبيق إجراءات الأمن وإجراءات الأمان، والموضوعة جميعًا لحمايتها وإبقائها في وَضْع الأمان، فقيمة

المعلومات نفسها، سواء أكانت هذه القيمة ماليَّة (إذا كانت المعلومات ذات قيمة ماديَّة) أم اعتباريَّة (إذا كانت المعلومات ذات قيمة معنويَّة أو ذات قيمة مَجازيَّة)، وتُساعِد عملية تقييم المعلومات على تَوقُّع كَم التهديدات الموجَّهة إليها بشكلٍ مباشر ووَضْع تَصوُّر مبدئي حول مستوَيَي إجراءات الأمن وإجراءات الأمان الواجب تطبيقها، وإن مَهمَّة تحديد المعلومات وتقييمها، يَنبغي أن يَقوم بها مالِك المعلومات.

2.1.5 التهديدات

إنَّ مفهوم التهديدات المحتَمَلة والموجَّهة بشكلٍ مباشر إلى المعلومات أو إلى المحيط الذي يَحتويها ضروري لتكوين فكرة مبدئيَّة عن الأخطار الناجِمة عن تنفيذ تِلْك التهديدات من خلال الثغرات الكامِنة في محيط المعلومات، لتكوين تَصوُّرات مبدئيَّة حول إجراءات الأمن التي يُمكِن تخطيطها وحول إجراءات الأمان، و**التهديد** Threat، في حقل أمن المعلومات، هو أيّ شيء محتَمَل ومتوقَّع يُمكِن أن يُسبِّب سرقةً أو إفشاءً أو تخريبًا للمعلومات، ويُؤكِّد التعريف السابق أنَّ التهديد محتَمَل الحدوث في أيّ وقت، ومتوقَّع بالنسبة إلى مالِك المعلومات، ولكنَّه خارج عن إرادته وسيطرته، وسوف يُسبِّب تنفيذ التهديد لمالِك المعلومات خسائر إمّا ماديَّة أو معنويَّة أو مَجازيَّة، ويُمكِن أن يأتي التهديد إمّا من مصدر بشري، ويُسمَّى **تهديدًا بشريًّا** أو من مصدر غير بشري، ويُسمَّى **تهديدًا غير بشري**.

ثَمَّة أربعة أشكال رئيسة للتهديدات البشريَّة هي: **تهديد الهاكرز** Hackers threat، و**البرامج الخبيثة** Malicious code ، و**برامج التجسُّس** Spyware، و**تهديد المطَّلِعين المخادِعين** Malicious insiders threat.

الهاكر – بحسب تعريفه في حقل أمن المعلومات – هو أي شخص يَستطيع النَّفاذ خِفيةً إلى الأنظمة الحاسوبيَّة والعَبَث بالبرامج والمعلومات المخزَّنة فيها دون أن يَكون مخوَّلًا بذلك، وتُمثِّل أفعال الهاكرز تهديدًا بالغًا للمعلومات الرقميَّة فقط، ويَخترق

الهاكرز الأنظمة الحاسوبيَّة إمّا من أجل التَّفاخُر بخبرتهم في هذا المجال أو من أجل منفعة ماليَّة عائِدة من طرف ثالث يَعملون لمصلحته أو لحسابهم الخاص، ويَجب على الطرف المالِك للمعلومات أن يَفترِض وجود الهاكرز، حتَّى ولو لم يَشعر بهم أو بنتائج أفعالهم، ووجود الهاكرز ليس مقرونًا بأي حدث أو زمن، بل هم موجودون سواء أَردْنا حماية المعلومات أم لم نرد، وسواء تَمَّت حمايتها أم لم تتمّ. إذًا، التهديد الذي يُمكِن أن يَأتي من الهاكرز هو نفاذهُ خِفيةً إلى النظام الحاسوبي وسرقة المعلومات الرقميَّة المخزَّنة فيه أو إفشاؤها أو تخريبها.

التهديد الثاني الذي يُمكِن أن يُطلِقه البشر هو البرامج الخبيثة، مثل **الفيروسات** Viruses **والديدان** Worms **وأحصنة طروادة** Trojan horses، وهي برامج حاسوبيَّة تُؤدِّي أعمالًا تخريبيَّة عندما تُنفّذ داخل النظام الحاسوبي، ويُوجَّه التهديد الصادِر عن البرامج الخبيثة نحو المعلومات الرقميَّة فقط (كما هو الهاكرز)، وتَنتشِر البرامج الخبيثة إمّا تلقائيًّا أو بمساعدة غير شعوريَّة من المستخدِم الجاهِل بوجودها، ويَتراوَح أذى البرامج الخبيثة بين إظهار رسائل مزعجة على الشاشة إلى تهيئة أجهزة التخزين في الحاسوب وتدمير البيانات دون إرادة المستخدِم، وتَتمّ صناعة البرامج الخبيثة من قِبَل أطراف لديها نيات انتقاميَّة تَتجلَّى في التخريب الذي تُسبِّبه تِلْك البرامج داخل حاسوب الضحيَّة، ويُمكِننا استنتاج أنَّ البرامج الخبيثة بحَدِّ ذاتها، وما تَقوم به من أذى وتخريب داخل الأنظمة الحاسوبيَّة تُعدّ تهديدًا للمعلومات الرقميَّة فقط، ومن ثم الأنظمة أو المنظومات التي ترتبط بها.

برنامج التجسُّس هو البرنامج التنفيذي المركَّب على حاسوب المستخدِم الضحيَّة دون علمه، الذي يُراقب أنشطة المستخدِم ويجمع معلوماته، مثل ضربات المفاتيح، ولقطات الشاشة، وتسجيلات الكاميرا والمايكروفون و/أو الملفات، ثمَّ إرسالها إلى الطرف الذي يُدير ذلك البرنامج، وإنَّ عمليَّة جَمْع المعلومات وإرسالها إلى الطرف الذي يُدير برنامج التجسُّس هي بحَدِّ ذاتها تهديد للمعلومات الرقميَّة.

والتهديد البشري الرابع والأكثر خطورة هو تهديد المطَّلِعين المخادِعين، والمطَّلِعون المخادعون هم الأفراد المُجَاز لهم قانونيًّا استعمال المعلومات من قِبَل مالِك المعلومات، الذين يَستخدِمون تِلْك المعلومات خِفيةً لأغراض شخصيَّة سيِّئة، وهم من الأفراد المؤتَمَنين على المعلومات من قِبَل مالِك المعلومات والموجودين داخل محيطه، وقد يَكون المطَّلِعون المخادِعون إمّا أفرادًا ضِمْن البيت الواحد لمالِك المعلومات أو موظَّفين ذوي صلاحيَّات واسعة في منظَّمة ما (قيِّمين أو مستخدِمين) أو أفرادًا مسؤولين عن حماية المعلومات المصنَّفة سريَّة وحفظها في دولة ما (قيِّمين)، ويُعدّ تهديد المطَّلِعين المخادِعين الأكثر إيذاء؛ لأنَّه يَتضمَّن خيانة الثقة التي يَمنحَها مالِك المعلومات لهؤلاء المطَّلِعين. إذًا، يَقوم المطَّلِعون المخادِعون بسرقة المعلومات المؤتَمَنين عليها من قِبَل مالِك المعلومات أو إفشائها أو تخريبها، وتُمثِّل أفعالهم هذه تهديدًا للمعلومات الرقميَّة والورقيَّة.

وقد تَأتي التهديدات أيضًا من مصادر غير بشريَّة، وتُسمَّى عندها التهديدات غير البشريَّة، مثل الكوارث الطبيعيَّة والحوادث غير المتوقَّعة، ومن أمثلة الكوارث الطبيعيَّة الزلازل والفيضانات والعواصف، ومن أمثلة الحوادث غير المتوقَّعة زيادة الطاقة الكهربائيَّة في أجهزة تخزين المعلومات والحرائق وانهيارات الأبنية، وإذا وَقعَت الكوارث الطبيعيَّة أو الحوادث غير المتوقَّعة، فسوف تُسبِّب تخريبًا لمحيط المعلومات أو لمحيط مالِك المعلومات أو لكليهما، ومن ثم للمعلومات نفسها، وإنَّ وقوع الكوارث الطبيعيَّة والحوادث غير المتوقَّعة يُعدّ تهديدًا للمعلومات الرقميَّة والورقيَّة.

ثَمَّة نوع من التهديدات من المصدر البشري، يُدعَى **التخريب المتعمَّد للممتلَكات** Vandalism، ويَأتي تهديد التخريب المتعمَّد للممتلَكات من احتمال قيام أحد ما من داخل محيط مالِك المعلومات (كالمنزل أو المنظَّمة) عَمْدًا بتخريب أجهزة تخزين المعلومات إذا كانت المعلومات رقميَّة، أو تخريب الخَزْنات الحديديَّة أو حافظات الملفات والوثائق إذا كانت المعلومات ورقيَّة، وعلى الرغم من أنَّ التخريب في هذا التهديد يكون للممتلَكات،

وليس للمعلومات، إلا أنَّ الأذى الناتج عن ذلك التخريب سيَصِل للمعلومات في نهاية الأمر.

أخيرًا تُصَنَّفُ التهديدات وفق ثلاثة أصناف بحسب تواتر وقوعها وبحسب الأثر الذي يمكن أن تُحدِثَهُ، ويبين الشكل هذا التصنيف.

دارة الأخطار المعلوماتية من المنظور العملي

الوتيرة + الأثر	الوتيرة Likelihood		الأثر Impact		التصنيف
	عالي High	+	عالي High	=	عالي High
	عالي High	+	مخفض Low	=	متوسط Medium
	مخفض Low	+	مخفض Low	=	مخفض Low

المصدر: حسن الحربي، 2014م.

3.1.5 الثغرات

عندما تُوجَد عيوب في محيط مالِك المعلومات الخاصَّة تُؤدِّي باستثمارها من قِبَل الخصم إلى سرقة المعلومات أو إفشائها أو تخريبها، فنحن بصَدَد مفهوم الثغرات، **والثغرة** Vulnerability، في حقل أمن المعلومات، هي نقطة الضعف المحتَمَلة الموجودة في محيط مالِك المعلومات، التي يُمكِن استغلالها لسرقة المعلومات أو إفشائها أو تخريبها، وثَمَّة نوعان من هذه العيوب هما: **عيب أمن** Security flaw، و**عيب أمان** Safety flaw، وعندما تَكون الثغرة موجودة في محيط مالِك المعلومات قبل تطبيق إجراءات الأمن، تُسمَّى عندها عيب أمن، وعندما تَكون الثغرة موجودة في محيط مالِك المعلومات

بعد تطبيق إجراءات الأمن (أي بعد إدخال المعلومات في وَضْع الأمان) تُسمَّى عندها عيب أمان، وقد تُوجَد الثغرة، إمّا في محيط المعلومات الإلكتروني كالنظام الحاسوبي، وتُسمَّى عندها **ثغرة إلكترونيَّة**، أو في محيط المعلومات اليدوي كالخزنة الحديديَّة التي تَحتوي على وثائق ورقيَّة، وتُسمَّى عندها **ثغرة يدويَّة**، ومن أمثلة الثغرة الإلكترونيَّة عدم وجود برنامج مضاد فيروسات في نظام حاسوبي، وتُعدّ هذه الثغرة في الوقت نفسه عيب أمن، أو وجود برنامج مضاد فيروسات غير محدَّث في نظام حاسوبي، وتُعدّ هذه الثغرة في الوقت نفسه عيب أمان، ومن أمثلة الثغرة اليدويَّة عدم وجود قفْل على خزنة حديديَّة تَضُم معلومات ورقيَّة، وتُعدّ هذه الثغرة في الوقت نفسه عيب أمن، أو وجود قفل غير مُحكَم (أي غير آمن، ويمَكِن كَسْره بسهولة) على خزنة حديديَّة تَضُم معلومات ورقيَّة، وتُعدّ هذه الثغرة في الوقت نفسه عيب أمان، وقد تُوجَد الثغرة في محيط مالِك المعلومات كالمنزل أو المنظَّمة، ولكن لأنَّ محيط المعلومات هو جزء من محيط مالِك المعلومات، فاحتمال وجود الثغرة في محيط المعلومات هو احتمال وجودها نفسه في محيط مالِك المعلومات، وقد يكون إحداث الثغرة إمّا مقصودًا، وتُسمَّى **ثغرة متعمَّدة** Intentional vulnerability، أو غير مقصود، وتُسمَّى **ثغرة عرضيَّة** Accidental vulnerability، ومن أمثلة الثغرة المتعمَّدة تعطيل برنامج مضاد فيروسات في نظام حاسوبي، ومن أمثلة الثغرة العرضيَّة إهمال أو نسيان إحكام قفْل الخزنة الحديديَّة التي تَضم المعلومات الورقيَّة على نحوٍ متكرِّر.

وكما هو واضحٌ من تعريف الثغرة السابق، فإنَّ الثغرة بحدِّ ذاتها لا تُسبِّب سرقةً للمعلومات أو إفشاءها أو تخريبها، إلا إذا قابَلها تهديدٌ ما يَستغلُّها، وإنَّ التقاء الثغرة مع التهديد المقابِل هو ما سيُشكِّل الخطر الحقيقي على المعلومات، وهذا ما سيَتمّ الحديث عنه فيما يلي.

4.1.5 الأخطار

إنَّ الأخطار الحقيقيَّة على المعلومات ليست بإطلاق التهديدات وحدها، وهي ليست فقط بوجود الثغرات في محيط مالِك المعلومات، بل هي التقاء الثغرات مع التهديدات المقابِلة لها معًا، و**الخطر** Risk في حقل أمن المعلومات، هو احتمال حدوث أذى حقيقي للمعلومات أو محيطها أو محيط مالِكها، يُسبِّب في النهاية سرقة تِلْك المعلومات أو إفشاءها أو تخريبها. إذًا، يَتشكَّل الخطر في محيط مالِك المعلومات عندما تُوجَد فيه ثغرة ما، وفي الوقت نفسه يُطلَق تهديد مقابِل يَستغلُّ تِلْك الثغرة، ويُمكِننا أن نَنظُر إلى الخطر بصيَغ عدَّة، فمثلًا يُمكِن القول: إنَّ الخطر يَتشكَّل بتَقاطُع الثغرة مع تهديد مقابِل، أو أنَّ الخطر = الثغرة + التهديد، وإنَّ أمثلة تَشكُّل الأخطار كثيرة، ومن أبسطها وجود ثغرة إلكترونيَّة (ولتَكُن عدم وجود برنامج مضاد للفيروسات) في محيط معلومات إلكتروني (وليَكُن نظامًا حاسوبيًّا) مع إطلاق تهديد (وليَكُن برنامجًا خبيثًا أو فيروسًا) يُشكِّلان خطرًا على تِلْك المعلومات.

يُدعَى الخطر عند تَشكُّله باسم شكل التهديد البشري المقابِل، عندما يَكون التهديد بشريًّا، مثل خطر الهاكرز، وخطر المطَّلِعين المخادِعين، ويُدعَى الخطر عند تَشكُّله خطرًا غير بشري، عندما يكون التهديد غير بشري، أمّا التهديد المتمثِّل في التخريب المتعمَّد للممتلَكات فيُدعَى الخطرُ المقابِلُ له عند تَشكُّله خطرَ التخريب المتعمَّد للممتلَكات.

وتَتراوَح أساليب التَّعامُل مع الخطر بين محاولة الابتعاد عنه أو تقليل احتمال تَشكُّله أو قَبوله ونَقله إلى طرفٍ آخر، وثَمَّة أربعة خيارات للتَّعامُل مع الخطر ومَنْعِ تَشكُّله هي: **اجتناب الخطر** Risk avoidance، و**تخفيف الخطر** Risk mitigation، و**قَبول الخطر** Risk acceptance، و**تحويل الخطر** Risk transference [17، 13].

الخيار الأول هو اجتناب الخطر، ويَتم تَبنِّي هذا الخيار عندما تَكون المنفعة العائِدة من محاولة مَنْعِ تَشكُّل الخطر أقل بكثير من تكلفة مَنْعِ تشكُّله، ويَتم تطبيق هذا الخيار من

خلال اجتناب العوامل التي قد تُؤدِّي إلى تَشكُّل الخطر، ومن أمثلة اجتناب الخطر قيام إدارة منظَّمة ما بمَنْع موظَّفيها من تَبادُل رسائل بريد إلكتروني مع خارج المنظَّمة تَجنُّبًا لإرسالهم (سواء عَمْدًا أو عن غَير قَصْد) رسائل تَحوي معلومات أعمال خاصَّة.

والخيار الثاني من خيارات التَّعامُل مع الخطر ومَنْعِ تشكُّله هو تخفيف الخطر، وهو الأكثر شيوعًا، ويَتم تطبيق هذا الخيار من خلال اتِّخاذ إجراءات مضادَّة وقائيَّة متمثِّلةً في سَدِّ الثغرات الموجودة في محيط مالِك المعلومات ومَنْعِ تهديدات محدَّدة من استغلالها، ومن أبسط أمثلة تخفيف الخطر القيام بتركيب برنامج مضاد فيروسات في نظام حاسوبي للحماية من فيروس محدَّد.

والخيار الثالث هو قَبول الخطر، ويَتم قَبول الخطر عندما تَكون احتمالات تَشكُّله ضعيفة جدًّا، مثل احتمال وقوع زلزال شديد القوة في منطقة غير زلزالية تاريخيًّا، أو عندما تَكون تكلفة تَشكُّل الخطر صغيرة جدًّا مقارنةً بتكلفة تطبيق الإجراءات المضادَّة.

والخيار الرابع والأخير هو تحويل الخطر، ويَتم تطبيق هذا الخيار من خلال تحويل الخطر إلى طرف ثانٍ يَقبَل تَحمُّل أعباء تَشكُّل الخطر، والمثال الأبرز لهذا الخيار هو قيام شركة تأمين بتَحمُّل أعباء تَشكُّل الخطر مع مالِك المعلومات عن طريق قيام مالِك المعلومات بشراء بوليصة تأمين منها.

5.1.5 الإجراءات المضادَّة

المَهمَّة الأساسيَّة في إدارة أمن المعلومات هي تطبيق الإجراءات المضادَّة التي تَكفُل إحباط تَشكُّل الأخطار، **والإجراءات المضادَّة** Countermeasures في حقل أمن المعلومات، هي مجموعة من الأفعال العمليَّة والتنظيمية أو الإدارية التي تَهدُف إلى إحباط تَشكُّل الأخطار على المعلومات أو محيطها أو محيط مالِكها من خلال سَدِّ الثغرات ومَنْع التهديدات من استغلالها، والأفعال العمليَّة هي الأدوات التي يَتم استخدامها، مثل

البرامج الحاسوبيَّة والأنشطة، مثل حماية الأبنية التي تَحتوي على المعلومات الخاصَّة سواء رقميَّة أم ورقيَّة وبناء الأسوار حول تِلْك الأبنية، وما إلى ذلك. أمّا الأفعال الإدارية فتَعني السياسات التي تُلزِم الاضطلاع بالمسؤوليَّات المتعلِّقة بحماية المعلومات، والنصائح والتوجيهات المرتَبِطة بكيفيَّة الحفاظ على سلامة المعلومات، التي يَتم إصدارها من قِبَل المَعنيين والموجَّهة نحو الأفراد.

ولا يُمكِن في حقل أمن المعلومات الجزم بمواجَهة جميع التهديدات القائمة، ولكن يَكفي لمَنْع تَشكُّل الخطر سَدّ الثغرات التي من المُمكِن أن تَستغلّها التهديدات، وعمومًا فإن هَدَف تطبيق الإجراءات المضادَّة هو سَدّ الثغرات فقط؛ لأنَّ سَدّ الثغرة يُعدّ بحَدِّ ذاته مواجَهة للتهديد القائِم، ولكن من ناحية المَعني بحماية المعلومات، فمثلًا لا يُمكِن مواجَهة تهديد فيروس ما من خلال مقاوَمة انتشاره عالميًّا عَبْر الشبكة، ولكن يُمكِن سَدّ الثغرة التي قد يَستغلُّها تهديد ذلك الفيروس بتركيب برنامج مضاد فيروسات للحماية منه.

ثَمَّة نوعان من الإجراءات المضادَّة هما: **إجراءات أمن** Security measures، و**إجراءات أمان** Safety measures، وإجراءات الأمن هي الإجراءات المضادَّة التي يَتم تطبيقها من أجل إدخال المعلومات في وَضْع الأمان، وتُطبَّق إجراءات الأمن مرَّة واحدة على الأقل، ويُمكِن إعادة تطبيقها من جديد في حال تَمَّ تعديلها كليًّا أو جزئيًّا، وتُحاوِل إجراءات الأمن معالجة عيوب الأمن. أمّا إجراءات الأمان فهي الإجراءات المضادَّة التي يَتم تطبيقها بعد إدخال المعلومات في وَضْع الأمان، وتُطبَّق إجراءات الأمان باستمرار وعلى نحوٍ دوري بهَدَف إبقاء المعلومات في وَضْع الأمان، وتُحاوِل إجراءات الأمان معالجة عيوب الأمان التي قد تَظهَر عند ظهور تهديدات جديدة، وتَتَّخِذ الإجراءات المضادَّة (سواء أكانت إجراءات أمن أم إجراءات أمان) إمّا شكل **إجراءات وقائيَّة** Preventive measures أو شكل **إجراءات علاجيَّة** Remedial measures، والإجراءات الوقائيَّة هي الإجراءات المضادَّة التي تَسعى إلى مَنْع تَشكُّل الأخطار من خلال سَدِّ الثغرات التي

يُمكِن أن تَستغلّها تهديدات مقابِلة، أمّا الإجراءات العلاجيَّة فهي الإجراءات المضادَّة التي تُحاوِل تفكيك خطر (أو أخطار) بعد تَشكُّله من خلال القيام بسَدِّ الثغرة التي سَبَق، واستغلَّها التهديد واستعادة المعلومات السليمة إذا اختُرِقَ أمانها وإعادة محيط المعلومات إلى ما كان عليه قبل تَشكُّل الخطر، وتَتعامَل الإجراءات العلاجيَّة مع حوادث الأمان أيضًا (انظر الفقرة 3.8).

2.5 أمن المعلومات ذات القيمة الماديَّة

المعلومات ذات القيمة الماديَّة هي المعلومات التي يُمكِن أن تُعيد منافع ماليَّة عندما تُستثمَر آنيًّا، كأرقام الحسابات المصرفيَّة، ومعلومات الأعمال الخاصَّة، والمشروعات الاقتصاديَّة، ومالِك هذه المعلومات هو إمّا فردًا أو منظَّمةً أو حكومةً، وأمن هذه المعلومات هو تطبيق إدارة أمن المعلومات، كما تَمَّ تعريفها على المعلومات ذات القيمة الماديَّة، ويَتألَّف أمن المعلومات ذات القيمة الماديَّة من خمس مراحل هي:

1. المرحلة الأولى: تحديد المعلومات وتقييمها ماديًّا.
2. المرحلة الثانية: تحديد التهديدات المحتَمَلة وتحليلها.
3. المرحلة الثالثة: تحديد الثغرات وتحليلها.
4. المرحلة الرابعة: تقييم الأخطار.
5. المرحلة الخامسة: تطبيق الإجراءات المضادَّة.

1.2.5 المرحلة الأولى: تحديد المعلومات وتقييمها ماديًّا

تُعدّ هذه المرحلة مهمة جدًّا؛ لأنها تَرسم الإطار العريض حول المعلومات ذات القيمة الماديَّة التي يَنبغي الاهتمام بها وحمايتها من السرقة أو الإفشاء أو التخريب، والخطوة الأولى من هذه المرحلة هي تحديد المعلومات ذات القيمة الماديَّة، ويَتم تحديد ذلك من خلال تمييزها من بين مجموعة من المعلومات العاديَّة أو البيانات المتوافرة،

ومن ثمَّ إثبات أهميَّتها بالنسبة إلى الطرفين مالِك المعلومات والخصم معًا، ويَقتضي إثبات أهميَّة المعلومات ذات القيمة الماديَّة بالنسبة إلى الطرفين تأكيد وجود طرف آخر لديه مصلحة ماليَّة في الوصول إلى هذه المعلومات تُؤذي المصالح الماليَّة لمالِك المعلومات، ويَنبغي أيضًا معرفة هؤلاء الخصوم المحتَمَلين، وهم الأطراف البشريَّة المعروفون بالنسبة إلى مالِك المعلومات، مثل قريب أو صديق أو صاحب منظَّمة ما منافِسة (سواء أكانت تجاريَّة أم صناعيَّة) أو حكومة دولة ما منافِسة، وقد يَكون الخصم طرفًا بشريًّا مجهولًا مثل الهاكرز.

الآن، وبعد تحديد المعلومات ذات القيمة الماديَّة ومعرفة الخصوم المحتَمَلين، يَجب تجميع كل هذه المعلومات مع بعضها، ويَعني ذلك جَمْع المعلومات (سواء أكانت رقميَّة أم ورقيَّة) في مكان واحد دون النَّظَر إلى نسبة أهميَّة بعض المعلومات منها عن الأخرى، والسبب في ذلك هو أنَّ ثَمَّة معلومات منها قد تَعود بنفعٍ مالي صغير، لكنَّها مرتَبِطة بشكلٍ أو بآخر بمعلومات أخرى من الطبيعة نفسها تَعود بنفعٍ مالي كبير، بحيث لو تَمَّت سرقة المعلومات ذات النفع المالي الصغير أو إفشاؤها أو تخريبها سيُؤثِّر مع الوقت (عاجلًا أم آجلًا) في المعلومات ذات النفع المالي الكبير، وسيُسبِّب أذًى، ومن ثم يَجب تطبيق الإجراءات المضادَّة نفسها على المعلومات ذات النفع المالي الصغير والكبير، وعمليًّا يَتضمَّن تجميع كل هذه المعلومات تجميع الملفات التي تَحتوي على المعلومات في الحاسوب وتَضمينها في وسائط تخزين المعلومات الرقمية نفسها إذا كانت هذه المعلومات رقميَّة، أو تجميع الملفات التي تَحتوي على المعلومات في مكان واحد إذا كانت هذه المعلومات ورقيَّة، وإنَّ الهدف النهائي من تَجميع كل المعلومات ذات القيمة الماديَّة معًا هو تجهيزها بالكامل لتطبيق إجراءات الأمن وإجراءات الأمان عليها.

الخطوة الثانية من هذه المرحلة هي تقييم المعلومات ماديًّا، والهدف الأساسي من هذا التقييم هو ضَمان عدم تَجاوُز التكلفة الماليَّة لتطبيق الإجراءات المضادَّة النَّفْع المالي الذي يُمكِن أن تُعيده المعلومات عندما يَتم استثمارها، ويَتم تقييم المعلومات

ماديًّا من خلال حساب النَّفْع المالي من استثمار جميع هذه المعلومات آنيًّا، فعلى سبيل المثال، لو كانت المعلومات ذات القيمة الماديَّة عبارة عن أرقام الحسابات المصرفيَّة الشخصيَّة لطرفٍ ما، يكون النَّفْع المالي من استثمار هذه المعلومات آنيًّا مساويًا مجموع الأموال النقديَّة الموجودة في المصارِف، التي تَرتبِط بها أرقام الحسابات تِلْك، ولو كانت المعلومات ذات القيمة الماديَّة عبارة عن الأسرار الصناعيَّة لمنتَجٍ ما جديد، يكون النَّفْع المالي من استثمار هذه المعلومات آنيًّا مساويًا الأرباح الصافية التي يُمكِن أن تَعود بها صناعة المنتَج وبَيْعه. إذًا، لكل معلومات ذات قيمة ماديَّة طريقتها الخاصَّة في حساب النَّفْع المالي من استثمارها آنيًّا، ويتولى هذه المهمَّة مالِك المعلومات أو مدير أمن المعلومات، والمهم في النهاية هو أن تَكون التكلفة الماليَّة لتطبيق الإجراءات المضادَّة أقل من النَّفْع المالي من استثمار المعلومات آنيًّا.

2.2.5 المرحلة الثانية: تحديد التهديدات المحتَمَلة وتحليلها

تُحدِّد المعلومات ذات القيمة الماديَّة طبيعة التهديدات المحتَمَلة الموجَّهة بشكلٍ مباشر إليها وإلى محيطها، والخطوة الأولى من هذه المرحلة هي استقصاء جميع التهديدات المحتَمَلة، وتَنقسِم التهديدات المحتَمَلة والموجَّهة بشكلٍ مباشر إلى المعلومات ذات القيمة الماديَّة وإلى محيطها إلى قسمين هما: **تهديدات متعمَّدة** Intentional threats، و**تهديدات غير متعمَّدة** Unintentional threats، والتهديدات المتعمَّدة هي تهديد الهاكرز، وبرامج التَجسُّس، وتهديد المطَّلِعين المخادِعين، والتخريب المتعمَّد للممتلَكات، أمّا التهديدات غير المتعمَّدة فهي التهديدات غير البشريَّة.

الخطوة الثانية من هذه المرحلة هي تحليل التهديدات المحتَمَلة، فإنَّ الدافع وراء التهديدات المتعمَّدة هو الحصول على المنافع الماليَّة مهما كان مقدارها من خلال الوصول إلى المعلومات ذات القيمة الماديَّة، مهما كانت كَميَّتها، أمّا التهديدات غير المتعمَّدة فتؤدي على الأغلب إلى تخريب تِلْك المعلومات، وتَقَع من باب المصادفة، ويَنبغي

تركيز الاهتمام على التهديدات المتعمَّدة؛ لأنَّها تَقَع بنسبة أكبر من وقوع التهديدات غير المتعمَّدة، والسبب في ذلك هو أنَّ مُطلِقِي هذه التهديدات يُدرِكون أنَّ ثَمَّة منافع ماليَّة من الحصول على المعلومات ذات القيمة الماديَّة أو من إفشائها أو تخريبها، أمّا مُطلِقو التهديدات غير المتعمَّدة فيُوجِّهونها إلى جميع المعلومات سواء أكانت خاصَّة أم عامَّة، وسواء أكانت معلومات أم بيانات؛ لأنَّ دافعهم هو الإيذاء فقط.

وللهاكرز منافع ماليَّة من إدراك المعلومات ذات القيمة الماديَّة، وقد تَتَحقَّق هذه المنافع، إمّا بالحصول على هذه المعلومات، أو بإفشائها أو تخريبها لمصلحة أطراف أخرى، ويُوجَّه تهديد الهاكرز المتعمَّد في هذا النموذج من المعلومات الخاصَّة إلى المعلومات فقط، أمّا برامج التَجسُّس فتُطلِقها أطراف محدَّدة لها منافع ماليَّة أيضًا من إدراك المعلومات ذات القيمة الماديَّة، وتَتَحقَّق منافعهم هذه بالحصول على هذه المعلومات لمصلحتهم أو لمصلحة أطراف أخرى من خلال تركيبهم لتِلْك البرامج في حواسيب الضحايا، ويُوجَّه التهديد المتعمَّد المتمثِّل في برامج التَجسُّس في هذا النموذج من المعلومات الخاصَّة إلى المعلومات فقط، وأيضًا المطَّلِعون المخادِعون لهم منافع ماليَّة من الوصول إلى المعلومات ذات القيمة الماديَّة، وتَتَحقَّق منافعهم الماليَّة من خلال سرقة هذه المعلومات أو إفشائها أو تخريبها لمصلحتهم أو لمصلحة أطراف أخرى يتعامَلون معها، ويَقَع التهديد المتعمَّد الصادر عن هؤلاء بكثرة في المنظَّمات، ويُوجَّه تهديدهم المتعمَّد في هذا النموذج من المعلومات الخاصَّة إلى المعلومات وإلى محيطها أيضًا[1]، وأمّا التخريب المتعمَّد للممتلَكات فقد يقوم به أطراف لهم مصالح ماليَّة من قيامهم بهذا التخريب تَرتبِط بأطراف خارج محيط مالِك المعلومات، ويُسبِّب التخريب المتعمَّد للممتلَكات إيذاءً مباشرًا للمعلومات ذات القيمة الماديَّة، ويُوجَّه هذا

(1) السبب في أنَّ تهديد المطَّلِعين المخادِعين يُوجَّه إلى محيط المعلومات أيضًا هو أنَّ المطَّلِع المخادِع قد يَقوم أيضًا، من باب الأذى، بتخريب محيط المعلومات، سواء أكانت المعلومات رقميَّة أم ورقيَّة.

النوع من التهديد للممتلَكات في هذا النموذج من المعلومات الخاصَّة إلى المعلومات، وإلى محيطها، وإلى محيط مالِكها.

تُطلَق البرامج الخبيثة إلى جميع الأنظمة الحاسوبيَّة عَبْر الشبكات، وليسَ لمُطلِقي البرامج الخبيثة أيّ مصالح ماليَّة مباشرة، إلا أنَّ مصالحهم العامَّة تَتَحقَّق من خلال إصابة تِلْك البرامج للأنظمة الحاسوبيَّة، مسبِّبةً تخريبًا على الأقل للبيانات على نحوٍ عام، وللمعلومات ذات القيمة الماديَّة على نحوٍ خاص، ويُوجَّه التهديد المتمثِّل في البرامج الخبيثة في هذا النموذج من المعلومات الخاصَّة إلى المعلومات وإلى محيطها، وأمّا التهديدات غير البشريَّة فتُطلَق مصادفةً، وعلى أساس إطلاقها العَرَضيّ، فقد تُسبِّب تخريبًا لجميع المعلومات دون تحديد (سواء أكانت خاصَّة أم عاديَّة، وسواء أكانت ذات قيمة ماديَّة أم غيرها) وللبيانات على نحوٍ عام.

3.2.5 المرحلة الثالثة: تحديد الثغرات وتحليلها

قَبْل تحديد الثغرات، يَنبغي معرفة محيط المعلومات الذي يَضمّ المعلومات ذات القيمة الماديَّة، وتُساعِد عملية جَمْع هذه المعلومات على معرفة محيط المعلومات، والخطوة الأولى من هذه المرحلة هي تحديد الثغرات، ويَتم ذلك من خلال فَحْص كامِل محيط المعلومات (سواء أكان محيطًا إلكترونيًّا أم محيطًا يدويًّا) من أجل اكتشاف الثغرات التي يُحتَمَل أن تُوجَد فيه، وسوف تَكون الثغرات المحتَمَل وجودها في محيط المعلومات عيوب أمن؛ لأنَّ ظهورها سيَكون قبل تطبيق إجراءات الأمن، وتَختلِف آلية فَحْص محيط المعلومات الذي يَضم المعلومات ذات القيمة الماديَّة بين محيط المعلومات الإلكتروني ومحيط المعلومات اليدوي، فإذا كان محيط المعلومات إلكترونيًّا (مثل الأنظمة الحاسوبيَّة وشبكاتها)، عندها يُمكِن استعمال أدوات الفحص المؤتَمَتَة التجاريَّة التي تُساعِد على اكتشاف الثغرات التي يَستخدِمها الخصوم في شَنِّ هجماتهم، وإذا كان محيط المعلومات يدويًّا (مثل الخزنة الحديديَّة التي تَحتوي على الملفات

والوثائق الورقيَّة)، عندها يَنبغي فَحْص محيط المعلومات يدويًّا، وإنَّ عملية فَحْص محيط المعلومات اليدوي يدويًّا سهلة على خلاف المحيط الإلكتروني الذي يَتطلَّب أدوات حاسوبيَّة خاصَّة لفَحْصه، وبعد فَحْص محيط المعلومات، يَجب فَحْص محيط مالِك المعلومات الذي يَتَمثَّل في الإطار الفيزيائي الذي يُحيط المعلومات أيضًا، وذلك بهدف التَّأكُّد من عدم وجود عيوب أمن فيه، مثل هَشاشة الجدار الأسمنتي للغرفة وقابليَّة وقوعه على محيط المعلومات ومقاوَمة مناخ الغرفة للظروف الجويَّة، مثل ارتفاع درجة الحرارة ومقاوَمة الغرفة للحرائق.

الآن، وبعد تحديد الثغرات المحتَمَلة الموجودة في محيط المعلومات الإلكتروني أو اليدوي أو في محيط مالِك المعلومات، يُمكِن في الخطوة الثانية من هذه المرحلة تحليل هذه الثغرات من خلال مطابَقة التهديدات المقابِلة معها، فمثلًا لو كانت الثغرات التي تَمَّ تحديدها في الخطوة الأولى إلكترونيَّة، يُمكِن وَضْع تهديد الهاكرز، وبرامج التجسُّس، والبرامج الخبيثة، وتهديد المطَّلِعين المخادِعين، والتخريب المتعمَّد للممتلَكات في قائمة التهديدات المحتَمَلة، أما إذا كانت هذه الثغرات يدويَّة، فيُمكِن وَضْع تهديد المطَّلِعين المخادِعين، والتهديدات غير البشريَّة، والتخريب المتعمَّد للممتلَكات في قائمة التهديدات المحتَمَلة، ولو كانت الثغرات مكتَشَفة في محيط مالِك المعلومات، يُمكِن وَضْع التهديدات غير البشريَّة في قائمة التهديدات المحتَمَلة، ويَجب في الخطوة الثانية من هذه المرحلة أيضًا تحديد فيما إذا كانت الثغرات التي تَمَّ اكتشافها في الخطوة الأولى هي ثغرات متعمَّدة أم ثغرات عرضيَّة؛ لأنَّ التأكيد بأن تَكون الثغرة متعمَّدة هو التأكيد بوجود خصمٍ ما يُحاوِل إحداثَها وفقًا لمصالح خاصَّة به أو بأطراف أخرى، وإنَّ التأكيد بأن تَكون الثغرة عرضيَّة هو تأكيد بأنَّ هناك إهمالًا غير مقصود قد يَكون بسيطًا، ولكن يُؤدِّي تَجاهُله إلى استغلال الثغرة من قِبَل تهديدٍ ما مقابِل.

4.2.5 المرحلة الرابعة: تقييم الأخطار

من الصعب إضفاء قيمة ماليَّة محدَّدة لخطرٍ يهدد المعلومات ذات القيمة الماديَّة، وقبل الحديث عن تقييم الأخطار، يَنبغي أولًا ترتيب الأخطار على المعلومات ذات القيمة الماديَّة وفق مقدار الأذى الذي يُسبِّبه تَشكُّل الخطر، والترتيب الأساسي لهذه الأخطار من الأشَدِّ إلى الأخَفِّ وخيارات التَّعامُل مع كل واحد منها هو:

1. خطر الهاكرز، ويَتمّ التّعامُل معه بخيار (تخفيف الخطر).
2. خطر برامج التجسُّس، ويَتمّ التّعامُل معه بخيار (تخفيف الخطر).
3. خطر المطَّلِعين المخادِعين، ويَتمّ التّعامُل معه بخيار (اجتناب الخطر).
4. خطر البرامج الخبيثة، ويَتمّ التّعامُل معه بخيار (تخفيف الخطر).
5. خطر التخريب المتعمَّد للممتلَكات، ويَتمّ التّعامُل معه بخيار (تحويل الخطر).
6. خطر الحوادث غير البشرية، ويَتمّ التّعامُل معه بخيار (تحويل الخطر).

ويجري تقييم الأخطار على المعلومات ذات القيمة الماديَّة بتطبيق الخطوات الخمس الآتية:

1. الخطوة الأولى: إعداد قائمة كاملة بالثغرات التي تَمَّ اكتشافها في المرحلة الثالثة.
2. الخطوة الثانية: إعداد قائمة بالتهديدات المحتَمَلة ومطابقَتها مع قائمة الثغرات المعدَّة في الخطوة الأولى وإعداد قائمة بالأخطار التي يُحتَمَل تَشكُّلها من استغلال قائمة التهديدات المحتَمَلة المعدَّة في هذه الخطوة لقائمة الثغرات المعدَّة في الخطوة الأولى.
3. الخطوة الثالثة: ترتيب قائمة الأخطار وفقًا للترتيب الأساسي للأخطار الحقيقيَّة على المعلومات ذات القيمة الماديَّة من الأشَدِّ إيذاءً إلى الأخَفِّ إيذاءً والمذكور في الفقرة السابقة.

4. الخطـوة الرابعـة: إضفـاء مجمل القيمـة الماديَّة للمعلومات، لـكل خطر يُحتَمَل تَشـكُّله في القائمة المعدَّة في الخطوة الثالثة، والآن إذا احتَوَت قائمة الأخطار المحتَمَل تَشـكُّلها والمعدَّة في الخطوة الثالثة على خطر واحد على الأقل، يَجب علـى مديـر أمـن المعلومات أنَّ يُقرِّر رسـميًّا وبشـكلٍ صريح تطبيـق الإجراءات المضادَّة.
5. الخطـوة الخامسـة: تحديـد أسـاليب التّعامُـل مـع كل خطر في قائمـة الأخطار المعدَّة في الخطوة الثالثة وفقًا لخيارات التّعامُل مع كل خطر.

بَعْد تقييم الأخطار في الخطوات الخمس السابقة، يُمكِن الانتقال إلى المرحلة الخامسة والأخيرة من أمن المعلومات ذات القيمة الماديَّة، لتطبيق الإجراءات المضادَّة بحسب أساليب التّعامُل مع كل خطر والمحدَّدة في الخطوة الخامسة من تقييم الأخطار.

5.2.5 المرحلة الخامسة: تطبيق الإجراءات المضادَّة

يَجري في هذه المرحلة تطبيق الإجراءات المضادَّة التي تَكفل مَنْع تَشكُّل الأخطار. عمومًا، ثَمَّة نوعان من الإجراءات المضادَّة سيَتم تطبيقهما في هذه المرحلة، هما: إجراءات أمن، وإجراءات أمان، وتَضمَن إجراءات الأمن إدخال المعلومات الخاصَّة في وَضْع الأمان، أمّا إجراءات الأمان فتَضمَن إبقاء المعلومات الخاصَّة في وَضْع الأمان.

يَنبغي قَبْل كلِّ شيء أن يُدرِك مدير أمن المعلومات المكلف بالتطبيق ضرورة الموازَنة بين القيمة الماديَّة للمعلومات وتكلفة تطبيق إجراءات الأمن وإجراءات الأمان، وإنَّ تكلفة تطبيق هذه الإجراءات لا تَشمَل تكلفة وَضْعها وتخطيطها؛ لأنَّ هذه الإجراءات مخطَّطة وموضوعة مسبقًا، ولذا تَنطوي التكلفة فقط على تطبيقها، وفي البداية يَجب أن يَختار مدير أمن المعلومات تطبيق جميع الإجراءات المضادَّة، ويَقوم بحساب تكلفة ذلك، وإذا كانت تكلفة تطبيق الإجراءات المضادَّة أكبر من القيمة الماديَّة للمعلومات، فعندها يَنبغي اختيار عدد أقل من إجراءات الأمن وإجراءات الأمان، وبعدها حساب

تكلفة تطبيقها من جديد، وتَعود آليَّة اختيار الإجراءات المضادَّة ذات التكلفة الأقل لتطبيقها إلى مدير أمن المعلومات؛ لأنَّ هذا الأمر له احتمالات متعدِّدة مثل تَوافُر أو عدم تَوافُر بعض الإجراءات في المُتناوَل لتطبيقها وجَواز أو عدم جَواز تطبيق بعض الإجراءات من قِبَل السلطات الحكوميَّة.

إن إجراءات أمن المعلومات ذات القيمة الماديَّة هي بالترتيب:

1. اختيار الموقع الفيزيائي المناسِب (أي محيط مالِك المعلومات) إمّا للأجهزة والمعدَّات الحاسوبيَّة التي ستَحتَوي على المعلومات إذا كانت المعلومات رقميَّة، أو للمعدَّات اليدويَّة التي ستَحتفِظ بالوثائق والمستندات التي تَضمّ المعلومات إذا كانت المعلومات ورقيَّة.
2. توظيف الأفراد الموثوقين والمؤتَمَنين المفوَّض إليهم استعمال المعلومات الخاصَّة.
3. إذا كانت المعلومات الخاصَّة رقميَّة ومشتَرَكة، وتتطلب التواصل في بيئة كبيرة (كمنظَّمة مثلًا)، يَنبغي عندها حماية الشبكة الحاسوبيَّة التي سيَتم عَبرها تَبادُل المعلومات الخاصَّة من خلال اختيار إحدى طُرُق التصميم المُثلَى للشبكة لحمايتها، كتَقسيم الشبكة، وتركيب جدار ناري، وتركيب نظام اكتشاف التطفُّل، أو استعمال شبكة خاصَّة افتراضيَّة.
4. تركيب برامج موثوقة مضادَّة للبرامج الخبيثة وبرامج التَجسُّس في الأنظمة الحاسوبيَّة التي تُخزِّن المعلومات إذا كانت المعلومات رقميَّة.
5. نَسْخُ جميع المعلومات الخاصَّة احتياطيًّا من خلال إجراء نُسَخ رقميَّة عدَّة إذا كانت المعلومات رقميَّة، أو تصوير الوثائق والمستندات التي تَضمّ المعلومات مرات عدَّة إذا كانت المعلومات ورقيَّة.
6. حماية مَضمون جميع المعلومات الأصليَّة من خلال تَعميتها (تشفيرها) باستخدام إحدى المُعمِّيات المعياريَّة أو التجاريَّة الموثوقة أو المطورة محليًّا،

ومفتـاح سـرِّي طويل نسـبيًّا ومختَلَط المحـارِف إذا كانت المعلومـات رقميَّة، أو الاحتفـاظ بهـا في خزنـة حديديَّة مُحكَمـة الإقفال إذا كانـت المعلومات ورقيَّة. بعدهـا، يَنبغـي حماية مَضمون جميـع المعلومات الرقميَّة المنسـوخَة من خلال تَعميتهـا بالمعمِّـي نفسـه الـذي اسـتُعمِلَ في تَعميـة المعلومـات الأصليَّـة، ولكن بمفتـاح سـرِّي ومختَلِف عن المفتاح السـرِّي الذي اسـتُخدِم لتعميـة المعلومات الأصليَّة، والهدف من اسـتعمال مفتاح سـرِّي مختَلِف هو تَفادي مشـكلة نَسـيان المفتـاح السـرِّي الـذي اسـتُعمِلَ لتَعميـة المعلومـات الأصليَّـة أو ضَياعـه، وأمّـا حمايـة مَضمـون جميع المعلومات الورقيَّة المنسـوخَة فتَتمّ من خلال الاحتفاظ بهـا فـي خزنة حديديَّة أخـرى مُحكَمة الإقفال على أن تَكـون موضوعة في مكان مختلـف عن مكان الخزنة التي تَحتوي على المعلومات الورقيَّة الأصليَّة، ويَنبغي الاحتفـاظ بالمفتاحيـن السـرِّيَّين اللذَيـن اسـتُخدِما لتَعميـة جميـع المعلومات الأصليَّـة والمنسـوخَة في مكان آمـن للعودة إليهما من قِبَل الأطراف المشـارِكة فـي اسـتعمال المعلومات إذا كانت هذه المعلومات مشـتَرَكة، أو الاحتفاظ بهما لدى مالِك المعلومات شخصيًّا إذا كانت هذه المعلومات غير مشتَرَكة.

7. أمّـا إذا كانـت المعلومـات ورقيَّـة فيَنبغـي الاحتفـاظ بالمفتاحيـن اليدويَّيـن للخزنتَيـن اللتَيـن تَحويـان جميـع الوثائـق والمسـتندات التـي تَضـمّ المعلومات الأصليَّـة والمنسـوخة في مكان آمن جدًّا، بحيث تَسـهُل العـودة إليهما إذا كانت المعلومات مشتَرَكة أو في مكان سرِّي لا يَعلمُه إلا مالِك المعلومات شخصيًّا إذا كانت المعلومات غير مشتَرَكة.

أمّا إجراءات أمان المعلومات ذات القيمة الماديَّة فهي بالترتيب:

1. اسـتخدام ضوابِـط الأمن الفيزيائي فـي محيط مالِك المعلومـات الذي يَحتوي علـى المعـدَّات والأجهـزة الرقميَّـة أو المعـدَّات اليدويَّـة التي تَضـمّ المعلومات الرقميَّة أو الورقيَّة.

2. فَحْص محيط المعلومات دوريًّا من خلال استعمال أدوات الفَحْص المؤَتمَتة التجاريَّة التي تُساعِد على اكتشاف الثغرات في الأنظمة الحاسوبيَّة وفي الشبكة الداخليَّة لمنظَّمة ما مثلًا إذا كانت المعلومات رقميَّة، أو التَّأكُّد من سلامة محيط المعلومات بالنَّظَر إليه بالعين المجرَّدة وتَحديد فيما إذا كانت ثَمَّة عيوب فيه أم لا إذا كانت المعلومات ورقيَّة.
3. تحديث البرامج المضادَّة للبرامج الخبيثة وبرامج التَّجسُّس باستمرار.
4. التَّحقُّق من الخلفية الائتمانية للموظَّفين الموكَّلين باستخدام المعلومات الخاصَّة في منظَّمة ما، مثلًا بين مدةٍ وأخرى، ويَتم ذلك من خلال تَركيب برامج تَجسُّس في الأنظمة الحاسوبيَّة التي يَتم فيها استخدام المعلومات الخاصَّة واستثمارها، التي يَعمَل عليها هؤلاء الموظَّفون لتسجيل جميع أنشطتهم على هذه الأنظمة الحاسوبيَّة؛ وذلك بهَدَف حماية المعلومات الخاصَّة من أن تَتم سرقتها وتسريبها لخارج محيط مالِك المعلومات، واستعمال التسجيلات ونتائج المراقبة كدليل إدانة للموظَّف الذي أَقدَم على هذه الخطوة من الخيانة والسرقة، ولا يُعدّ هذا انتهاكًا لخصوصيَّة الفرد؛ لأنَّ المعلومات الخاصَّة والأنظمة الحاسوبيَّة التي تَضمّها ليست ملكًا لهذا الفرد.

وعليه فإنَّ أي أمر يَقوم به الموظف مستخدِمًا المعلومات الخاصَّة أو النظام الحاسوبي الذي يَضمّها خارج صلاحيات عمله يُعدّ انتهاكًا من قِبَله لأمان هذه المعلومات، ولا يَملك أي حَقّ للشكوى من التجسُّس عليه، الآن لمَنْع الموظَّف من تركيب برمجيات تَمنَع برامج التَّجسُّس في النظام الحاسوبي الذي يَعمَل عليه من أداء عملها داخل محيط مالِك المعلومات، يُمكِن استخدام برامج متخصِّصة تَمنَع أي تلاعب سواء إضافة أو إزالة أو تعديل لأي برنامج في النظام الحاسوبي.

5. تطبيـق آليَّـة متكامِلـة للولوج إلـى المعلومات الخاصَّـة، بحيث تَمْنَـح الموظَّفين داخـل منظَّمـة ما حَقّ الوصول إلى المعلومات التـي يَحتاجون إليها فقط، وتُقيِّد حريَّتهم بالوصول إلى المعلومات التي لم يُرخَّص لهم استعمالها.
6. إتلاف المعلومات الخاصَّة الرقميَّة أو الورقيَّة عند الانتهاء من استثمارها على نحوٍ يَستحيل استرجاعها كليًّا أو جزئيًّا.

3.5 أمن المعلومات ذات القيمة المعنويَّة

المعلومات ذات القيمة المعنويَّة هي المعلومات التي تَفوق أهميَّتها وحساسيَّتها أي قيمة ماديَّة لها مهما بَلَغ مقدار هذه القيمة، وهذا يُشير إلى أنَّ المعلومات ذات القيمة المعنويَّة هي المعلومات المصنَّفة سريَّة لدى حكومات الدول، والمعلومات الدوليَّة المصنَّفة سريَّة التي يَتشارَك بها طرف دولي، ويَعني ذلك أنَّ ملكيَّة المعلومات ذات القيمة المعنويَّة جماعيَّة، وتَعود إلى دولة أو إلى طرف دولي، وأمن المعلومات ذات القيمة المعنويَّة هو تطبيق إدارة أمن المعلومات عليها، ويتألَّف هذا الأمن من خمس مراحل أيضًا هي:

1. المرحلة الأولى: تحديد المعلومات وتقييمها معنويًّا.
2. المرحلة الثانية: تحديد التهديدات المحتَمَلة.
3. المرحلة الثالثة: تحديد الثغرات.
4. المرحلة الرابعة: تقييم الأخطار.
5. المرحلة الخامسة: تطبيق الإجراءات المضادَّة.

1.3.5 المرحلة الأولى: تحديد المعلومات وتقييمها معنويًّا

يَتمّ تحديد المعلومات في هذه المرحلة من خلال اختيار المعلومات المصنَّفة سريَّة فقط (إذا كانت متعلِّقة بدولة ما) أو المعلومات الدوليَّة المصنَّفة سريَّة (إذا كانت

متعلِّقة بطرف دولي) من بين مجموعة من المعلومات الخاصَّة الأخرى[1]. ليسَ من مهام مدير أمن المعلومات إضفاء أو إلغاء صفة السريَّة على المعلومات الخاصَّة الحكوميَّة أو المعلومات الخاصَّة المرتَبِطة بطرف دولي، إنَّما تَقتصِر مَهمَّته في هذه المرحلة فقط في اختيار المعلومات الخاصَّة التي قَامَت السلطات الحكوميَّة العليا في الدولة أو السلطات العليا في الطرف الدولي رسميًّا بإقرارها مصنَّفة سريَّة، ويُمكِن تحديد الخصوم المحتَمَلين الذين لهم مصلحة في إدراك هذه المعلومات على أنَّهم الأعداء القائِمون الظاهريون والمَخفيون لدولة معنيَّة أو للمجموعة التي تُشكِّل طرفًا دوليًّا.

على خلاف العمليَّة التي تَمَّ فيها تقييم المعلومات ماديًّا، لا توجد عمليَّة واضحة وسهلة تَستطيع تقييم المعلومات معنويًّا.

2.3.5 المرحلة الثانية: تحديد التهديدات المحتَمَلة

تَختلِف التهديدات المحتَمَلة والموجَّهة إلى المعلومات ذات القيمة المعنويَّة وإلى محيطها عن التهديدات المحتَمَلة والموجَّهة إلى المعلومات ذات القيمة الماديَّة وإلى محيطها، فالتهديدات المحتَمَلة والموجَّهة إلى المعلومات ذات القيمة الماديَّة وإلى محيطها تَحتوي على جميع أشكال التهديدات البشريَّة والتهديدات غير البشريَّة، أمّا التهديدات المحتَمَلة والموجَّهة إلى المعلومات ذات القيمة المعنويَّة وإلى محيطها فلا تَحتوي إلا على ثلاثة أشكال منها، والسبب يَعود إلى طبيعة المعلومات الخاصَّة التي تَقتصِر هنا على المعلومات المصنَّفة سريَّة بمستوياتها المختلفة، فالمعلومات المصنَّفة سريَّة عمومًا، سواء أكانت حكوميَّة أم مرتَبِطة بطرف دولي بعيدة كل البعد على أن تَكون مخزَّنة أو مشارَكًا بها في الطُّرُق التقليديَّة نفسها المستخدَمة في تخزين أو مشارَكة المعلومات ذات القيمة الماديَّة أو حتَّى المعلومات ذات القيمة المَجازيَّة، وهي قد تَكون

(1) تُترَك حماية المعلومات الخاصَّة الأخرى غير المعلومات المصنَّفة سريَّة إلى جهات حكوميَّة عاديَّة يُمكِنها استعمال أدوات مناسبة لذلك.

مشارَكًا بها في شبكة داخل محيط مالِك المعلومات، ولكنَّها بالتأكيد معزولة تمامًا عن الشبكة الخارجيَّة كالإنترنت، وهذا نابعٌ من إدراك المَعنيين بإقرار سريَّة هذه المعلومات لأهميَّتها البالغة.

عمومًا، ثَمَّة ثلاثة تهديدات محتَمَلة وموجَّهة إلى المعلومات ذات القيمة المعنويَّة هي: تهديد المطَّلِعين المخادِعين، والتهديدات غير البشريَّة، والتخريب المتعمَّد للممتلَكات، وإنَّ احتمال وقوع التهديدات غير البشريَّة والتخريب المتعمَّد للممتلَكات ضعيف بسبب حِرْص الحكومة أو الطرف الدولي على التأمين الفيزيائي الشديد للمعلومات ومحيطها ومحيط مالِكها، أمّا تهديد المطَّلِعين المخادِعين فهو التهديد الأكثر وقوعًا في كثير من الدول، وإنَّ أمثلة وقوع ذلك كثيرة، ومن هذه الأمثلة ذلك الذي شَكَّل قضيَّة شَغَلت الرأي العام الأمريكي في منتصف عام 2013م عندما قَام الموظَّف السابق في وكالة الأمن القومي الأمريكيَّة Edward Snowden بتصوير الوثائق الورقيَّة المصنَّفة سريَّة التي احتَوَت على ممارسات الوكالة بمراقبة الاتصالات الهاتفيَّة والمعامَلات الإلكترونيَّة عبر الإنترنت، ثمَّ تسليمها إلى الصحافة العالميَّة لنَشرها، فقد أَحرَج الأمر الذي قَام به Snowden الحكومة الأمريكيَّة أمام الرأي العام الأمريكي والرأي العام العالمي، وسَبَّب أذًى كبيرًا لأمن الجيش الأمريكي (على حَدِّ قولهم) وخسائر وَصَلت قيمتها لبلايين الدولارات، وأيضًا من أمثلة وقوع تهديد المطَّلِعين المخادِعين الوثائق الورقيَّة المصنَّفة سريَّة وبعضها من مستوى التصنيف (سرِّي جدًّا) التي تَمَّ تسريبها ونَشْرَها في موقع WikiLeaks الإلكتروني.

3.3.5 المرحلة الثالثة: تحديد الثغرات

تُحَدَّدُ الثغرات في هذه المرحلة بالأسلوب نفسه الذي تَمَّ فيه تحديد الثغرات في أمن المعلومات ذات القيمة الماديَّة، وذلك من خلال فَحْص كامِل محيط المعلومات (سواء أكان محيطًا إلكترونيًّا أم محيطًا يدويًّا) من أجل اكتشاف الثغرات التي يُحتَمَل

أن تُوجَد فيه، وعلى ما يُعتَقَد أنَّ الثغرات التي يُمكِن أن تَستغلّها التهديدات غير البشريَّة والتخريب المتعمَّد للممتلَكات والموجَّهة إلى المعلومات ذات القيمة المعنويَّة ضعيفة نسبيًّا بسبب مَتانة محيط مالِك المعلومات، ولكنَّ الثغرة التي يُمكِن أن يَستغلَّها تهديد المطَّلِعين المخادِعين، والتي تَتمثَّل في إهمال الحَذَر من قيام أحد القيِّمين أو أحد المستخدِمين للمعلومات الخاصَّة المصنَّفة سريَّة (الحكوميَّة أو الدوليَّة) بخيانة الثقة وسرقة هذه المعلومات أو إفشائها أو تخريبها، فهي جَليَّة.

4.3.5 المرحلة الرابعة: تقييم الأخطار

في البداية يَنبغي معرفة الأخطار على المعلومات ذات القيمة المعنويَّة وترتيبها قبل تقييمها، والأخطار الحقيقيَّة على المعلومات ذات القيمة المعنويَّة وترتيبها بحسب مقدار الأذى الذي يُسبِّبه تَشكُّل تِلْك الأخطار من الأشدِّ إلى الأخفِّ وخيارات التَّعامُل مع كل واحد منها هي:

1. خطر المطَّلِعين المخادِعين- ويَتم التّعامُل معه بخيار (اجتناب الخطر).
2. خطر التخريب المتعمَّد للممتلَكات- ويَتم التّعامُل معه بخيار (اجتناب الخطر).
3. الخطر غير البشري- ويَتم التّعامُل معه بخيار (اجتناب الخطر).

تَنطوي جميع خيارات التّعامُل مع الأخطار على المعلومات ذات القيمة المعنويَّة تحت (اجتناب الخطر)؛ لأنَّ المَعنيين بهذه المعلومات، المُمثَّلين بالسلطات العليا، سواء في الدولة أو في الطرف الدولي، لا يُريدون تَدخُّل أي جهة كانت لمَنْع تَشكُّل الخطر إلا الأطراف البشريَّة الموظَّفة والمُجَازة من قِبَلهم.

ولأنَّ خطر التخريب المتعمَّد للممتلَكات والخطر غير البشري صغيران بالنسبة إلى خطر المطَّلِعين المخادِعين، يُمكِن تَركيز الاهتمام على الخطر الأخير، والآن إذا كان هناك احتمال قيام أحد القيِّمين أو المستخدِمين للمعلومات المصنَّفة سريَّة (مهما كانت درجة وظيفتهم) بخيانة الثقة، عندها يُمكِن إقرار ذلك بوصفه تهديدًا محتَمَلًا

واعتبار إهمال الحَذَر منه كثغرة وإقرار احتمال تَشكُّل الخطر رسميًّا، ولكن على خلاف الخطوة الرابعة في تقييم الأخطار على المعلومات ذات القيمة الماديَّة، التي يَجب فيها إقرار تطبيق الإجراءات المضادَّة، يَنبغي هنا تطبيق إجراءات الأمن قبل مراحل تحديد التهديدات وتحديد الثغرات وتقييم الأخطار، ومن ثمَّ تطبيق إجراءات الأمان بعد مرحلة تقييم الأخطار، والسبب في اتِّخاذ هذه الخطوة الاستباقيَّة هو أنَّ أهميَّة المعلومات ذات القيمة المعنويَّة تَتطلَّب القيام بإجراءات احتياطيَّة قبل مناقشة جميع التهديدات والثغرات والأخطار المحتَمَلة، فإذا تَمَّ بعدها الإحساس باحتمال إطلاق تهديد ووجود ثغرة مسبقًا، يُمكِن عندها التّعامُل مع الخطر المشكَّل ضمن إجراءات الأمان، وليس إجراءات الأمن، وهذا لا يَعني دون شك تطبيق إجراءات الأمان فقط عند الإحساس باحتمال تَشكُّل خطر، بل إنَّ محاولة مَنْع تشكُّل خطر تَقَع ضمن إجراءات الأمان، إذْ يَنبغي تطبيق إجراءات الأمان على نحوٍ دوري فَوْر تطبيق إجراءات الأمن، وقد يَعتقِد بعضهم أنَّ تكلفة تطبيق إجراءات الأمن قبل مراحل تحديد التهديدات وتحديد الثغرات وتقييم الأخطار قد تَكون أكبر من قيمة المعلومات نفسها، ولكنَّ هذا الأمر غير صحيح؛ لأنَّه أولًا، المعلومات ذات القيمة المعنويَّة محدَّدة مسبقًا ومقرَّرة بصفة معلومات مصنَّفة سريَّة أو معلومات دوليَّة مصنَّفة سريَّة. وثانيًا، لا يَهتَم المعنيُّون بهذه المعلومات بأيّ تكلفة ماليَّة ضخمة يَتحمَّلونها لتطبيق إجراءات الأمن قبل تقييم الأخطار؛ لأنَّ هذه المعلومات تَرتبِط بالمصلحة العامَّة للمجتمع.

5.3.5 المرحلة الخامسة: تطبيق الإجراءات المضادَّة

إنَّ هذه المرحلة هي أهم مرحلة في أمن المعلومات ذات القيمة المعنويَّة؛ لأنَّها تُشكِّل حاجزَين أساسيَّين أمام سرقة المعلومات أو إفشائها أو تخريبها، وهذان الحاجزان هما إجراءات الأمن وإجراءات الأمان، ولكن على الرغم من احتواء هذه المرحلة على كلٍّ من إجراءات الأمن وإجراءات الأمان، إلا أنَّه، وكما ذَكرنا سابقًا، يَجب تطبيق إجراءات

الأمن قبل مراحل تحديد التهديدات وتحديد الثغرات وتقييم الأخطار، فإجراءات الأمن هي الحاجِز الأول الذي يَسعى إلى تأخير محاولة سرقة المعلومات المصنَّفة سريَّة أو إفشائها أو تخريبها، وأمّا إجراءات الأمان فهي الحاجز الثاني الذي يَستطيع مَنْع المطَّلِعين المخادِعين من القيام بأيّ محاولة ضارة.

إجراءات أمن المعلومات ذات القيمة المعنويَّة هي بالترتيب:

1. اختيار الموقع الفيزيائي الآمن، إمّا للأجهزة والمعدَّات الحاسوبيَّة التي ستَحتوي على المعلومات إذا كانت المعلومات رقميَّة، أو للمعدَّات اليدويَّة التي ستَحتفِظ بالوثائق والمستندات التي تَضم المعلومات إذا كانت المعلومات ورقيَّة، ويَنبغي أن يَكون الموقع الفيزيائي آمنًا من التهديدات غير البشريَّة، كالكوارث الطبيعيَّة والحوادث غير المتوقَّعة، وآمنًا من الهجمات البشريَّة مهما كان مَصدرها، ولإضافة هامش أمان إلى المكان الفيزيائي للمعلومات ذات القيمة المعنويَّة، يَنبغي أن يَكون الموقع مَخفيًّا عن الأعين، بحيث لا تُوجد شارات أو لافتات تَدلُّ على صفته أو على ماذا يَحتوي.
2. استخدام ضوابِط الأمن الفيزيائي الكَشفيَّة والوقائيَّة في محيط المكان الذي يَضم المعدَّات والأجهزة الرقميَّة أو المعدَّات اليدويَّة التي تَضم المعلومات الرقميَّة أو الورقيَّة، والسبب في عدم استخدام الضوابِط الرادِعة هو احتواؤها على أدوات ومواد إعلاميَّة تَدلُّ على طبيعة المكان، وذلك يُخالِف الإجراء الأول السابق.
3. تَوظيف أفراد موثوقين ومؤتَمَنين جدًّا بوصفهم قيِّمين أو مستخدِمين للمعلومات المصنَّفة سريَّة أو المعلومات الدوليَّة المصنَّفة سريَّة، ويَتم هذا الإجراء من خلال دراسة السيرة الذاتيَّة والتَحقُّق من الخلفيَّة الائتمانيَّة لكل فرد منهم قبل إسناد المَهام إليهم.

4. عَـزْلُ جميع الأنظمة الحاسـوبيَّة المخطَّط لها أن تَضـم المعلومات ذات القيمة المعنويَّة عن أي شبكة خارجيَّة أو داخليَّة، وعدم تَركيب أي برامج لا تَمُتّ بصلة (من قريب أو من بعيد) للتّعامُل مع هذه المعلومات في الأنظمة الحاسوبيَّة التي ستُخزِّنها، وذلك إذا كانت المعلومات الخاصَّة رقميَّة.
5. الاحتفـاظ بالمعلومـات الرقميَّة على وسـائط تخزين تَكون صالحـة مدة طويلة جـدًّا، وهذا يَعني أنه يَنبغي أيضًا مجاراة الصناعة الحديثة لوسـائط التخزين باسـتمرار؛ لمتابعـة حِفْـظ المعلومات الخاصَّـة الرقميَّة المخطَّط لهـا أن تَبقى مَحميَّة مدَّة طويلة.
6. عدم نَسْخِ أيٍّ من المعلومات الرقميَّة أو تصوير الوثائق والمستندات التي تَضم المعلومات الورقيَّة.
7. حماية مضمون جميع المعلومات المصنَّفة سـريَّة من خلال تَعميتها باستخدام أدوات تَعمويَّـة موثوقـة وقويَّـة وخاصَّـة بهـذه المعلومـات وغيـر معروفـة تجاريًّا ومفتـاح سـرِّي طويل نسـبيًّا ومختَلَط المحـارِف إذا كانت المعلومـات رقميَّة، أو الاحتفـاظ بهـا في خزنـة حديديَّة مُحكَمَـة الإقفال إذا كانـت المعلومات ورقيَّة. بعدهـا، يَجـب الاحتفـاظ بالمفتاح السـرِّي الرقمـي أو المفتاح اليـدوي مع أكثر القيِّمين ائتمانًا.

أمّا إجراءات أمان المعلومات ذات القيمة المعنويَّة فهي بالترتيب:

1. فَحْـص محيط مالِك المعلومات دوريًّا؛ للتَأكُّد من سـلامته وخُلوِّه من أي عيوب أمان والتَّحقُّق من عدم وجود أي ثغرة مهما كانت صغيرة.
2. التَّحقُّـق باسـتمرار مـن الخلفيـات الائتمانيَّـة لجميـع القيِّميـن والمسـتخدِمين للمعلومـات ذات القيمـة المعنويَّة؛ للتَأكُّد من اسـتمراريَّة أمانتهم تجاه التّعامُل مـع هـذه المعلومـات، وأفضل الطُّرُق للتحقُّـق من الخلفيـات الائتمانيَّة للقيِّمين

والمستخدِمين هي مراقبتهم فيما يَتعلَّق بتَحرُّكاتهم المرتَبِطة من قريب أو من بعيد بتَعامُلهم مع المعلومات ذات القيمة المعنويَّة.

3. تطبيق آليَّة دقيقة لولوج المستخدِمين إلى المعلومات الخاصَّة ذات القيمة المعنويَّة، بحيث تَمنَح المستخدم الذي يَحتاج فعلًا إلى هذه المعلومات، وبترخيص من رؤسائه، حَقّ الوصول المحدود، وتُقيِّد حريَّة وصول المستخدِمين إلى المعلومات التي لا يَحتاجون إليها أصلًا في عَمَلهم، ولم يُرخَّص لهم ذلك من رؤسائهم.
4. إتلاف جميع المعلومات الخاصَّة ذات القيمة المعنويَّة الرقميَّة أو الورقيَّة عند الانتهاء من استخدامها على نحوٍ يَستحيل تمامًا استرجاعها كليًّا أو جزئيًّا.

4.5 أمن المعلومات ذات القيمة المَجازيَّة

عندما تَكون ثَمَّة معلومات شخصيَّة تَخصُّ طرفًا بشريًّا ليست ذات قيمة معنويَّة وفي الوقت نفسه لا تَحمِل قيمةً ماديَّةً، فهذه المعلومات هي معلومات ذات قيمة مَجازيَّة، وأمثلة هذه المعلومات كثيرة، منها حسابات صناديق البريد الإلكتروني، والمذكِّرات الشخصيَّة، وما إلى ذلك. ولهذا النوع من المعلومات أيضًا إدارة أمن معلومات تُطبَّق عليها، ويُدعَى تطبيقها أمن المعلومات ذات القيمة المَجازيَّة.

إنَّ عمليَّة تحديد المعلومات المجازية وتقييمها بسيطة، وتَتم من خلال اختيار المعلومات التي تَحتوي على خصوصيَّات شخصيَّة فقط، ولكنَّها لا تَحمِل أي قيمة ماديَّة. مما لا شك فيه، فلن تَكون ثمّة معلومات ذات قيمة مَجازيَّة مختَلَطة مع معلومات ذات قيمة معنويَّة، ولكن إذا كانت المعلومات الخاصَّة ذات القيمة المَجازيَّة تَرتبِط من قريب أو من بعيد بمعلومات ذات قيمة ماديَّة، يَنبغي عندها عَزْلُ المعلومات ذات القيمة الماديَّة عنها لتطبيق أمن المعلومات ذات القيمة الماديَّة عليها، ويَتم تقييم المعلومات ذات القيمة

المَجازيَّة بأنها لا تَحمِل أي مؤشِّر مادِّي، إلا أنَّها تَدلُّ على أنَّ هذه المعلومات شخصيَّة فقط.

وعلى الرغم من اختلاف المعلومات ذات القيمة المَجازيَّة عن المعلومات ذات القيمة الماديَّة، إلا أنَّ التهديدات الموجَّهة إليها هي التهديدات نفسها الموجَّهة إلى المعلومات ذات القيمة الماديَّة، والسبب هو أنَّ طبيعة محيط مالِك المعلومات ذات القيمة المَجازيَّة قريبة جدًّا من طبيعة محيط مالِك المعلومات ذات القيمة الماديَّة، وهذا يَقتضي أيضًا أنَّ الثغرات التي يُمكِن أن تُوجَد في محيط مالِك المعلومات ذات القيمة المَجازيَّة هي نفسها الموجودة في محيط مالِك المعلومات ذات القيمة الماديَّة. أما التهديدات المحتَمَلة الموجَّهة إلى المعلومات ذات القيمة المَجازيَّة فهي: تهديد الهاكرز، والبرامج الخبيثة، وبرامج التَجسُّس، والتهديدات غير البشريَّة، ولم يُذكَر تهديد المطَّلِعين المخادِعين والتخريب المتعمَّد للممتلَكات في السَّرْد السابق؛ لأنَّ الحافِظ الوحيد للمعلومات ذات القيمة المَجازيَّة هو مالِكها فقط، ولا تَستدعي طبيعة هذه المعلومات أن تَكون مؤتَمَنة مع أيِّ كان، وإنَّ مالِكها سيَشعُر بانتهاك خصوصيَّته الشخصيَّة إذا اخترق أحدٌ غيره هذه المعلومات.

بعد تعرُّف التهديدات المحتَمَلة والثغرات التي يُمكِن أن تَستغلَّها تِلْك التهديدات، يُمكِن ترتيب الأخطار الحقيقيَّة على المعلومات ذات القيمة المَجازيَّة المحتَمَل تَشكُّلها بحسب مقدار الأذى الذي قد تُسبِّبه من الأشدِّ إلى الأخفِّ، وعَرْض خيارات التّعامُل مع كلٍّ منها على النحو الآتي:

1. خطر الهاكرز- ويَتم التّعامُل معه بخيار (تخفيف الخطر).
2. خطر برامج التَّجسُّس- ويَتم التَّعامُل معه بخيار (تخفيف الخطر).
3. خطر البرامج الخبيثة- ويَتم التّعامُل معه بخيار (تخفيف الخطر).
4. الخطر غير البشري- ويَتم التّعامُل معه بخيار (قَبول الخطر).

وتَتمثَّل الإجراءات المضادَّة في أمن المعلومات ذات القيمة المَجازيَّة في مجموعة من التدابير الاحترازيَّة، ومهمَّة هذه التدابير ضَمان عدم اختراق أي طرف بشري للمعلومات ذات القيمة المَجازيَّة العائِدة لطرف بشري آخر، وتَدمُج هذه التدابير إجراءات الأمن وإجراءات الأمان معًا، والسبب في تسمية مجموعة الإجراءات المضادَّة هنا التدابير الاحترازيَّة هو أنَّ الإجراء المضادّ بحَدِّ ذاته (سواء أكان إجراء أمن أم إجراء أمان) ذو تكلفة ماليَّة، ولو كانت قليلة، أمّا التدبير الاحترازي فهو ليس سوى فِعْل لا يَحتاج إلى ممارسة أو خبرة، وتكلفته الماليَّة قليلة تَصِل إلى الصفر في أغلب الأحيان، وعمومًا التدابير الاحترازيَّة لحماية المعلومات ذات القيمة المَجازيَّة، وهي بالترتيب:

1. تَركيب برنامج تجاري موثوق (وقليل التكلفة) مضادّ للبرامج الخبيثة وبرامج التَجسُّس في النظام الحاسوبي الذي يُخزِّن هذه المعلومات إذا كانت المعلومات رقميَّة.
2. نَسْخُ جميع المعلومات الرقميَّة ذات القيمة المَجازيَّة والاحتفاظ بها في قرص ليزري أو مُخزِّن بيانات بعيد عن النظام الحاسوبي.
3. حماية مضمون جميع المعلومات ذات القيمة المَجازيَّة من خلال تَعميتها باستخدام إحدى المُعميِّات التجاريَّة العاديَّة ذات التكلفة الماليَّة القليلة ومفتاح سرِّي قصير وآمن إذا كانت المعلومات رقميَّة، أو الاحتفاظ بها في مكان آمن قريب من مالِكها وبعيد عن الأعين وعن متناوَل الأيدي إذا كانت المعلومات ورقيَّة.
4. تَحديث البرنامج المضادّ للبرامج الخبيثة وبرامج التَجسُّس باستمرار.
5. إتلاف المعلومات الخاصَّة ذات القيمة المَجازيَّة الرقميَّة أو الورقيَّة عند الانتهاء من استخدامها على نحوٍ يَستحيل استرجاعها.

5.5 المعيار العالمي في إدارة حماية المعلومات ISO 27001/2

طوّرت منظمة المقاييس الدولية ISO سلسلة من المعايير أو المواصفات الدولية متخصصة بأمن المعلومات، وهي ISO27001 وISO27002، التي يطلق عليها نظم إدارة حماية المعلومات (المتطلبات)، إذ تعطي المواصفة ISO27001 نموذجًا عامًّا لتطبيق نظم إدارة حماية المعلومات وتشغيلها وتحسينها Information Security Management ISMS System. إن غاية منظمة ISO التنسيق بين معايير ISO27001 لإدارة حماية المعلومات مع معايير نظم الإدارة الأخرى مثلًا ISO9001:2000 التي تتعلق بنظم إدارة الجودة، وكذلك ISO14001:2004 التي تخاطب نظم إدارة البيئة.

تزود مواصفة ISO27001 وISO27002 إدارات المنظمات الصناعية والخدمية بتوجيهات لتطبيق نظم إدارة حماية المعلومات ISMS، فضلًا على حصولها على شهادة الطرف الثالث[1] الدولية لإثبات كفاءة المنظمة في حماية معلوماتها، التي تعمل طبقًا لمتطلبات المعايير الدولية، إضافة إلى مراقبة نظام ISMS واستدامته من قبل منظمة ISO، وبهذا يعالج نظام إدارة حماية المعلومات كل أطوار الهيكل التنظيمي، والسياسات، وخطط النشاط، والمسؤوليات، والممارسات، والإجراءات، والعمليات، وأخيرًا مصادر المعلومات.

إن التطبيق الفعّال لـ ISO27001 وISO27002 يوفر للإدارة العليا وسائل المراقبة والسيطرة على حماية المعلومات، ويقلل من أخطار العمل الناشئ عن عدم الحصول على المعلومات بالدقة المطلوبة، وكذلك من خطر تسرب المعلومات، فبعد تطبيق المنظمة المواصفة تضمن حماية معلوماتها رسميًّا للتواصل مع الزبون وشرعية (قانونية) المنظمة، إضافة إلى إرضاء متطلبات أصحاب المصالح لدى المنظمة.

تُعدُّ المواصفتان ISO27001 وISO27002 قاعدةً لتقييم نظام إدارة حماية المعلومات (ISMS) المتكامل، وإنها الوثيقة التي تقيّم أي نظام لإدارة حماية المعلومات.

---

(1) وهي الجهة المانحة للشهادة ISO27001.

عمليات المعالجة ISO27001:2013 وفوائد تطبيقها:

تُعَدُّ المواصفة ISO27001 التي صدرت عام 2005م، ثم تطورت لتصدر عام 2013م، والمواصفة ISO27002 معيارَي الحماية الدولي الرسمي المقدم لأي منظمة ترغب في الحصول على شهادة مستقلة لنظام إدارة حماية المعلومات، لهذا تحدد المواصفة المتطلبات الإلزامية لتأسيس نظام ISMS وتطبيقه وتوثيقه، وتحديد متطلبات التحكم لحماية المعلومات التي ستطبق وفق حاجات المنظمة الخاصة بها، وتشمل المواصفة الأولى منهما (11) مركزًا للتحكم و(39) هدفًا للسيطرة، إضافة إلى (133) موقعًا للسيطرة متوافقًا مع المواصفة ISO17799 التي تعمل من خلال أنموذج (PDCA) Plan – Do – Check – Act الذي يقوم بعمل التحسين المستمر، ويشتمل على مرحلتي أمن وأمان المعلومات الذي وصفناه باختصار في مطلع الفصل، وبهذا تستند المواصفة ISO27001 في عملها على تسعة أجزاء للمعالجة التي حددها تحالف صناعة حماية شبكات الإنترنت [1] CSIA يمكن تلخيصها فيما يأتي:

1. تعريف المجال لنظام إدارة حماية المعلومات ISMS.
2. تعريف سياسة حماية المعلومات.
3. تقييم الأخطار/ التحليل.
4. إدارة الخطر.
5. تحديد الأهداف للسيطرة والسيطرة الفعلية عليها/ التطبيق.
6. تجهيز بيان (كشف) التطبيق.
7. تطبيق ISMS وتشغيله.
8. استمرار المراقبة ومراجعة ISMS.
9. إدامة ISMS وتحسينه.

---

(1) Cyber Security Industry Alliance.

أما المعيار الثاني ISO27002، لمنظمة المواصفات الدولية ISO، فيُطبّق بوصفه تعليمات تساعد على تطبيق ISO27001 لإنجاز نظام ISMS بشكل فعال من خلال الآتي:

1. تقييم الأخطار والمعالجة.
2. سياسة الحماية.
3. تنظيم حماية المعلومات؟
4. إدارة الموجودات.
5. حماية معلومات الموارد البشرية.
6. حماية الطبيعة والبيئة.
7. إدارة العمليات والاتصالات.
8. السيطرة على دخول قواعد البيانات.
9. الحصول على نظم المعلومات، والتطوير، والإدامة.
10. إدارة حوادث لحماية المعلومات.
11. إدارة استمرارية العمل.
12. الالتزام (الالتزام بتطبيق بنود المواصفة).

وتجدر الإشارة في نهاية هذه الفقرة إلى أن ثمة فوائد ومنافع عدة واضحة من العمل على الحصول على شهادة المواصفة ISO27001:2005.

6.5 توجهات عامة عالمية في تحقيق الأمن والأمان المعلوماتي

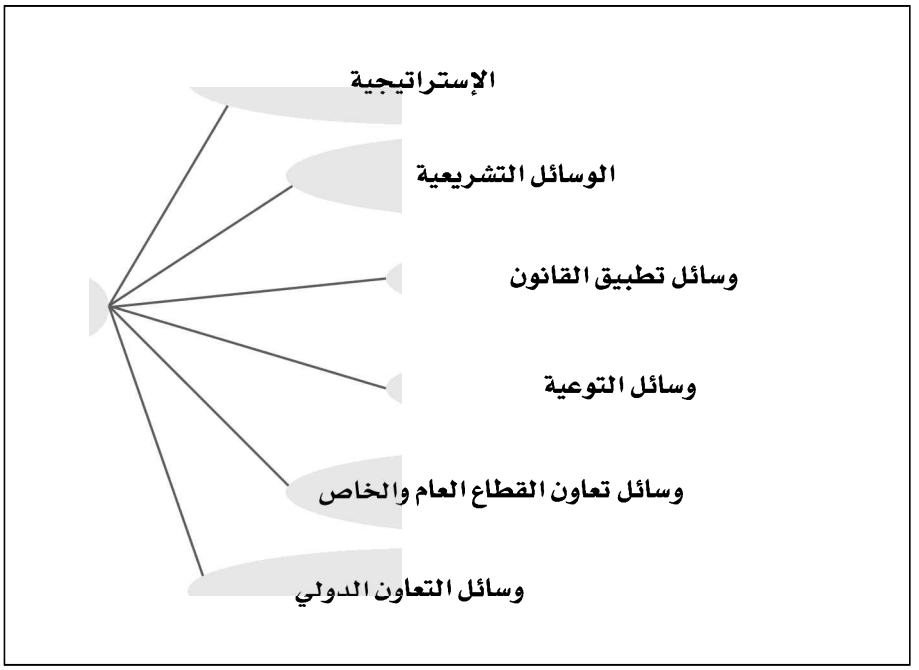
فيما يأتي لمحة عن الجهود العامة المبذولة على الصعيد العالمي المتمثلة في خمسة أنواع من التوجهات نبوّبها فيما يأتي[1]، ويبيّن الشكل توضيحًا لمعالمها الرئيسة:

(1) المصدر: اللجنة الاقتصادية والاجتماعية لغربي آسيا، الإسكوا.

1. التوجهات التشريعية:

- تطبيق التشريعات التقليدية على الجرائم المعلوماتية (السيبرانية).
- تحديث التشريعات.
- التقيد بالحياد التقني للتشريع.
- تحقيق التوازن في التشريع والتنسيق مع الآليات الأخرى.

إطار عام للسلامة السيبرانية في المنطقة العربية



2. التوجهات في تطبيق القانون والتنظيم:

- وضع سياسة خاصة بالسلامة المعلوماتية.
- إيجاد المحاكم المتخصصة وأجهزة التحقيق المتخصصة.
- استعمال الأدلة الرقمية في التحقيقات الجزائية.
- إنشاء مراكز الاستجابة السريعة لطوارئ الحاسوب.

3. التعاون بين الدول:

- تفعيل التعاون القضائي الرسمي وغير الرسمي.
- إيجاد حلول لتنازع الاختصاص القضائي.

4. التوجهات التقنية والإدارية والتنظيمية:

- اعتماد نموذج للأمن المعلوماتي (السيبراني).
- تفعيل التوجهات التقنية الخاصة بمقدمي الخدمات التقنية والشركات.
- تفعيل التوجهات المرتبطة بالعوامل الاجتماعية.

5. التوجهات المتعلقة بالتوعية والتدريب:

- توعية المستخدمين.
- توعية فئات خاصة في المجتمع.
- التدريب.

الفصل السادس

التعمية واستخراج المعمى أهم تقنيات أمن المعلومات[1]

(الشفرة وكسرها)

1.6 لمحة تاريخية.

يذكر علماء تاريخ هذه التقنية أن أنواعًا من سُبُل إخفاء المعلومات وسترها قد عرفتها الحضارة المصرية على ضفاف النيل في حدود عام 1900 قبل الميلاد، وتداولتها الحضارات الأخرى المجاورة.

واصطنع العرب في جاهليتهم الرمز، والملاحن، والمعاريض، وأمثالها؛ ليخفوا معانيهم ومراميهم، فلا يفهم عنهم إلاَّ الفَطِن ذو النباهة، فلما جاء الإسلام، واستبحر العمران، وازدهرت الحضارة العربية، وتشابكت مصالح الدولة التي امتدت أطرافها، وكثرت صلاتها بالدول الأخرى، تهيَّأت الأسبابُ المُسْعِفَةُ ليخطو العرب خطواتٍ فساحًا،

(1) بعض فقرات هذا الفصل مستقاة من مقالات للدكتور محمد مراياتي.

فيبدعوا في طرائق إخفاء أغراضهم ومقاصدهم، ويسلكوا في سبيل ذلك أساليب متنوعة مبتكرة، فيها الرمز، والألغاز، والملاحن، والتعمية، والمحاجاة، والتورية، وما إليها.

التعميةُ لغةً: الخفاءُ والالتباسُ، وهي في الاصطلاحِ: تحويلُ نصٍّ واضحٍ إلى آخرَ غيرِ مفهومٍ باستعمالِ طريقةٍ محدّدةٍ، يستطيعُ مَنْ يعرفُها أن يفهمَ النصَّ، واستخراجُها عكسُ ذلك، يجري فيه تحويلُ النصِّ المُعَمَّى إلى نصٍّ واضحٍ لِمَنْ لا يعرفُ مُسْبَقًا طريقةَ التعميةِ المستعملة[1].

إن علمَ التعميةِ واستخراجَ المعمى واحدٌ من علومٍ كثيرةٍ تدينُ للعربِ ولادةً ونشأةً وتطورًا، وهو ليس كغيرِه من العلوم التي ترجم العربُ بعضَ أصولِها، ثم أغنَوها، وطوّروها كالرياضياتِ والفيزياء والفلسفةِ، وإنما هو علمٌ عربيُّ المولدِ، يعودُ الفضلُ إلى العربِ في ابتكارِه، ووضعِ أُسُسِهِ، وإرساءِ قواعدِه، وتطويرِه إلى أن بلغ مرحلةً ناضجةً، وغدا ما وضعُوه فيه مرجعًا قبسَ منه المشتغلون بالتعميةِ من بعدُ، فالعربُ أوَّلُ من كتب في طرائقِ التعميةِ الرئيسةِ التي ما انفكَّ العالمُ يستخدمُ بعضَها حتى يومنا هذا، وهم أوَّلُ مَنْ وضع المنهجيّاتِ الأساسيةَ في علمِ استخراجِ المُعَمَّى، ودوَّنوا فيهما مصنَّفاتٍ مُسْتَقِلَّةً على غايةٍ من الأهميةِ منذ القرنِ الثالثِ الهجريِّ، وجُلُّها باقٍ في خزائنِ مكتباتِ العالمِ ينتظرُ مَنْ ينفضُ عنه غبارَ القرونِ، فسبقوا بذلك الغربيين نحوًا من سبعةِ قرونٍ، ومهَّدوا لهم، وتركوا بصماتٍ واضحةً في آثارهم، تشهدُ بفضلِ العربِ وريادتِهم.

كان للعرب والمسلمين مدارس في الفكر العلمي، منها ما اتبع مدارس قديمة، ومنها ما كان أصيلًا، فمن المدارس العربية الإسلامية الأصيلة مدرسة علماء الجبر، وعلماء المثلثات، ومدرسة علماء اللسانيات والصوتيات، ومدرسة علوم الإدارة وغيرها، وقد

---

(1) قال الزمخشري في (أساس البلاغة) (ت ع ب): «استخراج المُعَمَّى مَتْعَبَةٌ للخواطر». وإيراده هذا الكلام في مفتتح كلامه عن المادة يدل على ما يلاقيه المستخرج من تعب في حلّ التعمية، وعلى دقة في استخدام مصطلحي الاستخراج والمعمى.

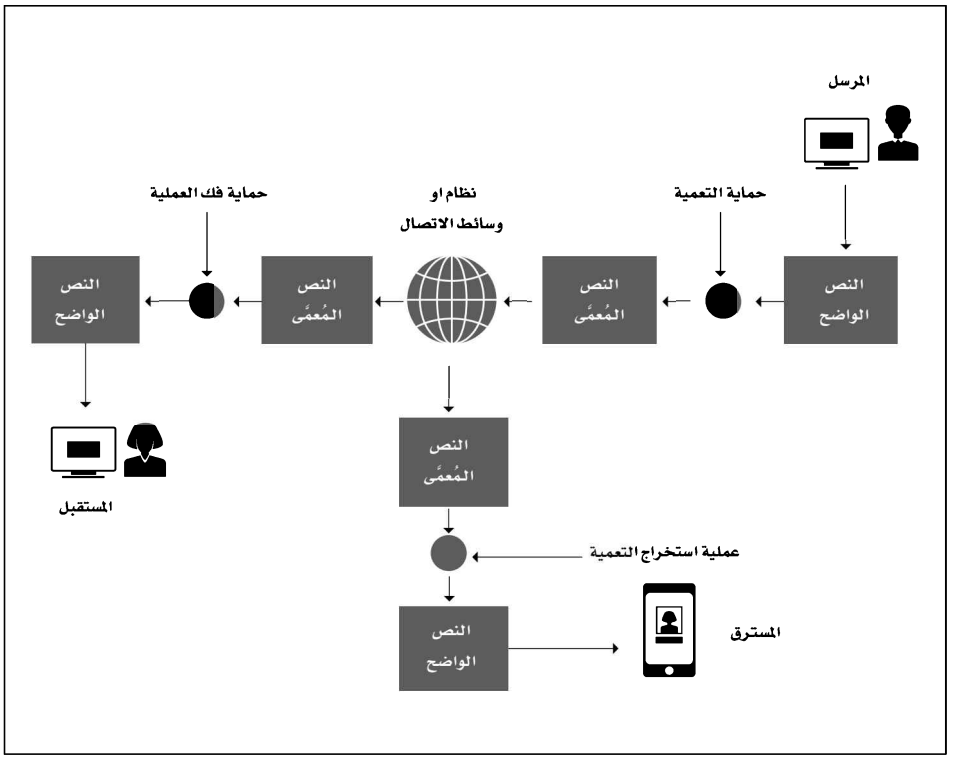
أضافت دراسة في جزأين، نشرت في 1200 صفحة من مجمع اللغة العربية بدمشق[1]، مدرسة علمية جديدة لم تكن معروفة قبلًا لطبيعة عملها، وهي المدرسة العربية في علوم التعمية (المعروفة الآن بعلوم الشفرة أو الكتابة السرية).

يعالج علم التعمية واستخراج المعمى مسألتين: تتناول الأولى طرق إخفاء المعلومات المرسلة من جهة إلى أخرى، وذلك لمنع المُسْتَرِق من الاطلاع على فحواها، وتتعلق الثانية باستخراج المعلومة من قبل المُسْتَرِق، وهذه المعركة بين المُعَمّي والمُستخرج قائمة سجالًا منذ أكثر من ألفي عام، فالأول يحاول ابتداع طريقة يَظُنُّ أنها لا تُستخرج، ويعمل الثاني جاهدًا على استخراجها، ويشارك في هذا التباري رياضيون، وفيزيائيون، ومعلوماتيون، ولغويون، وإلكترونيون، وغيرهم.

أخذ التخاطب عن بُعد أشكالًا مختلفة أهمها التراسل، وقد تطورت طرق التراسل ووسائلها مع الزمن لتأخذ حاليًّا أشكالًا مختلفة عدة، منها الرسائل البريدية، والتلكس، والبريد الإلكتروني، والتواصل عبر الجوالات، أو الهاتف المحمول بما في ذلك شبكات التواصل الاجتماعي وغيرها. أما وسائط التراسل فهي بريدية وسلكية ولاسلكية، وفي كثير من الأحيان يضطر الإنسان إلى إخفاء المعلومات التي يريد إرسالها إلى الطرف الآخر بهدف عدم اطلاع أي مُتطفل أو مُسْتَرِق على المعلومات المُرسلة، وهذه المعلومات قد تكون مهنية، أو تجارية، أو سياسية، أو دبلوماسية، أو عسكرية، أو... لذلك يقوم المُرْسِل بتعمية (تشفير) نص الرسالة قبل إرسالها للمُسْتَقْبِل الذي (يفكها) فور وصولها إليه لمعرفته بطريقة التعمية المتفق عليها مع المُرْسِل. أما المُسْتَرِق فيسعى إلى أخذ نسخة عن الرسالة خلال مسيرتها بين المتراسلين، ويحاول (استخراج تعميتها) على الرغم من عدم معرفته بطريقة التعمية المتفق عليها بين المُرْسِل والمُسْتَقْبِل، وهناك

(1) (التعمية واستخراج المعمى عند العرب) الجزء الأول والجزء الثاني، تأليف الدكاترة: محمد مراياتي، ويحيى مير علم، وحسان الطيان.

إذًا رغبة من قبل المتراسلين في تعقيد طريقة التعمية وجعلها مستحيلة (الاستخراج) يقابلها محاولة من المُسْتَرِق لنقض الطريقة واستخراجها؛ بغية الحصول على المعلومات المخفية فيها نظرًا لأهميتها، ويمثل الشكل مراحل عملية التواصل هذه:



عرفت التعميةُ في تاريخِها الطويلِ طرقًا عِدَّةً، يمكنُ إرجاعُ معظمِها إلى إحدى طريقتين هما:

أ. تعميةُ المعاني بالتوريةِ: هذه الطريقة لا تتبعُ قواعدَ محددةً، بل تعتمدُ على فطنةِ المتراسلينَ وخبرتهم وثقافتِهم(1)، وهي إلى العملِ الأدبيّ أو البديعي أقربُ منها إلى التعميةِ العلمية بمفهومِ هذا الكتاب، ولذلك سنتجاوز معالجةَ هذا اللونِ من المُعَمَّى على كثرةِ ما اجتمع من أصولِه الخطيةِ، ومن الأمثلة عليها: التورية،

والرمز، والألغاز، والملاحن، والمعاياة، والمحاجاة، وما إليها، فلن نتطرق لهذه الطرق في هذا الكتاب.

ب. التعميةُ بمعالجةِ الحروفِ: وتقومُ على اتِّباعِ طرقٍ تلتزمُ قواعدَ محددةً تخصُّ كُلًّا منها، وتدخل في منهجياتها مبادئ رياضياتية وخوارزميات معالجة محددة، وهذه الطرق هي المعنية بمعنى التعمية في هذا الكتاب.

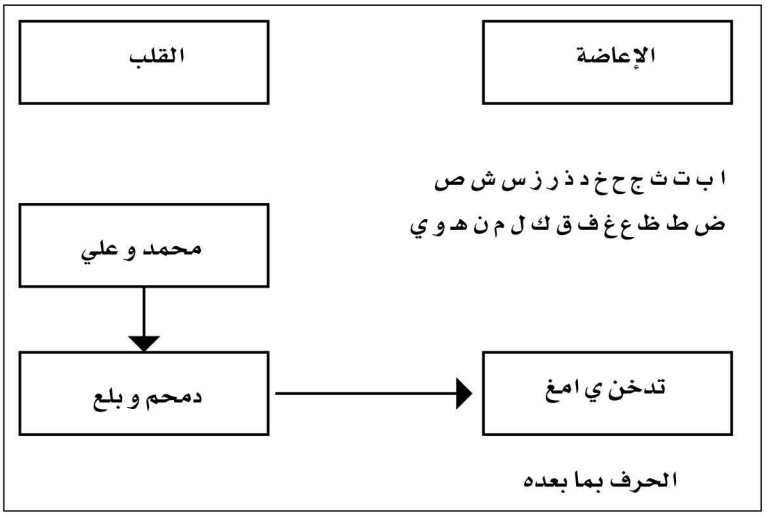
2.6 طرق التعمية الأساسية

أتينا سابقًا على التعاريف والمصطلحات الأساسية في علم التعمية واستخراج المعمى، ونتطرق في هذا الفصل إلى شرحٍ مبسطٍ وأمثلةٍ على الاستعمال والتطبيق.

تُقسَّم طرق التعمية التقليدية التي لم يُضَف إليها شيء جديد مهم حتى أوائل القرن العشرين، إلى أربعة أنواع، ذكرها الكندي واضع هذا العلم في مخطوطته، التي تُعدّ أول مرجع معروف في هذا العلم، وهي: التعمية بتبديل مواقع الحروف transposition، والتعمية بالإعاضة substitution، والتعمية بإضافة حروف (أغفال) nulls أو حذف حروف، ومثالُ ذلك أن تزيدَ حرفَ القافِ مثلًا بعد كلِّ ميمٍ، وحرفَ الشينِ بعد كلِّ لامٍ... إلخ، فَنُعَمِّي (محمد والد علي) على الشكلِ الآتي: (مقحمقد والشد علشي)، **والتعميةُ المركَّبةُ** Composite Cipher وتكونُ باستعمالِ طريقتينِ أو أكثرَ من الطرقِ الثلاثِ السابقةِ في آنٍ واحدٍ.

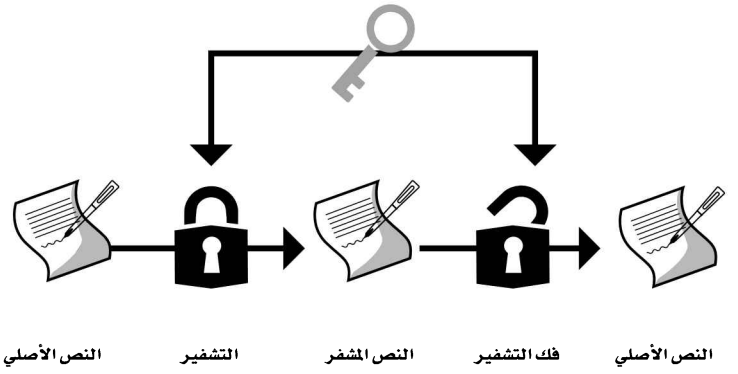
يبين الشكل الآتي شرحًا مبسطًا لعملية تعمية الكلمات: (**محمد وعلي**) باستعمال عمليتين متتاليتين: الأولى تغيير موقع الحروف في الكلمةTransposition كقلب المواقع مثلًا، حيث تصبح **محمد= دمحم**، وتصبح **علي = يلع**.

التعمية: تعريف ومثال

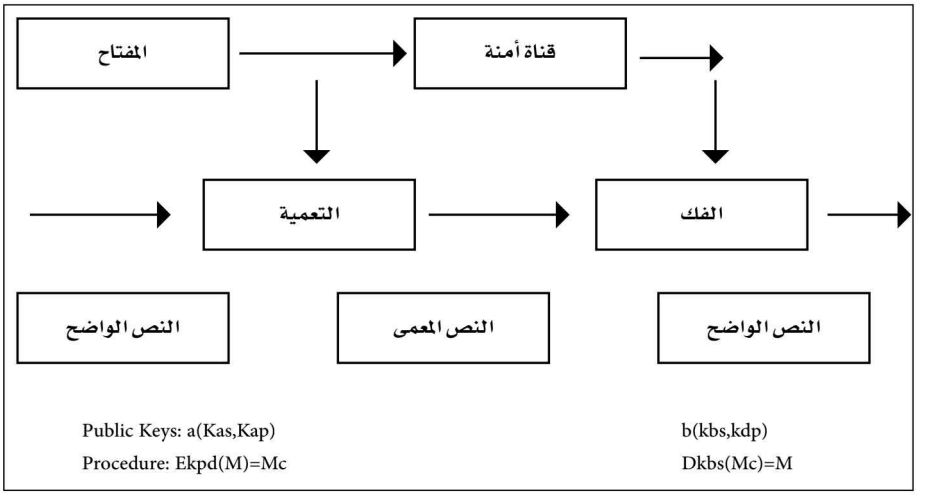


أما الطريقة الآتية فستكون باستعاضة شكل كل حرف بشكل حرف آخر ضمن الأبجديةSubstitution ، كأن يُستعاض عن الحرف بالحرف الذي يليه في الأبجدية: فتصبح **دمحم** = **ذنخن**، وتصبح **يلع** = **امغ**.

وتُقسَّم طرق التعمية إلى نوعين: متناظرة Symmetric وغير متناظرة Asymmetric، ففي التعمية المتناظرة يكون المفتاح المستعمل للتعمية المفتاح نفسه المستعمل لفك التعمية، ومن ثم فلا بد من إيجاد طريقة آمنة لإيصال المفتاح بين المتراسلين، ومن أمثلة التعمية المتناظرة نجد المعيار الأمريكي للتعمية DES وبعض مشابهاته.

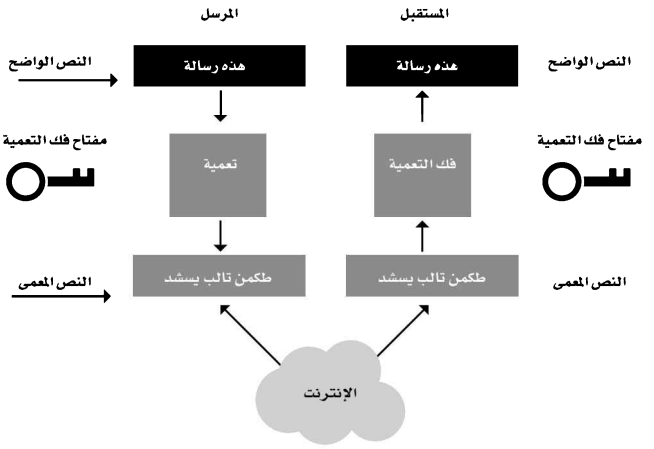


التعمية المتناظرة، التعمية بالمفتاح المعلن



أما في التعمية غير المتناظرة فيكون مفتاح التعمية مغايرًا لمفتاح فك التعمية، وتسمى هذه الطريقة أيضًا التعمية بالمفتاح المعلن Public Key؛ لأن لكل مراسل مفتاحين: أحدهما خاص وسري يحتفظ به لنفسه، والثاني معلن وفي متناول العامة، وعلى الرغم من وجود علاقة بين المفتاحين إلا أنه من غير الممكن عمليًّا حساب أحدهما لدى معرفة الآخر.

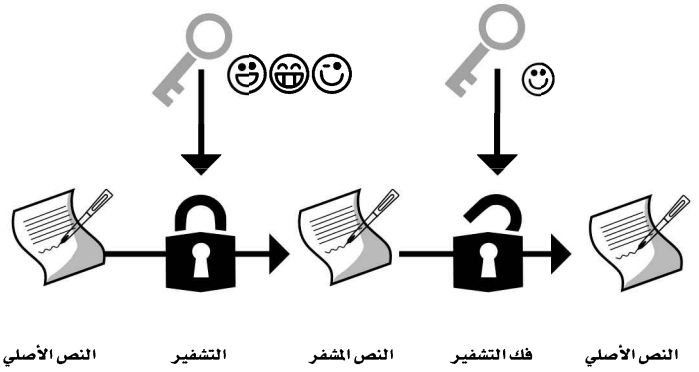
طريقة التعمية المتناظرة



من المألوف استعمال طريقتي التعمية معًا للاستفادة من ميزات كلٍّ منهما والإقلال من مساوئهما؛ لأن التعمية المتناظرة سريعة وآمنة أكثر من التعمية غير المتناظرة التي تحتاج إلى حسابات طويلة، وهي غير آمنة إذا كان مفتاحها قصيرًا، ومن جهة أخرى، فإن التعمية المتناظرة تحتاج إلى تبادل مسبق للمفتاح على عكس التعمية غير المتناظرة.

ويُستعمَل في معظم النظم العملية الموجودة في الأسواق التعمية بالمفتاح المعلن بهدف تبادل المفتاح السري اللازم للقيام باستعماله في التعمية المتناظرة، ويتم ذلك لكل مبادلة على الشبكة، ويسمى هذا المفتاح مفتاح جلسة المبادلة Session Key، وتجري تعمية المعلومات المتبادلة باستعمال التعمية المتناظرة ومفتاح الجلسة.

التعمية غير المتناظرة أو بالمفتاح المعلن



1.2.6 مبادئ وأمثلة في طرق التعمية المتناظرة الرئيسة:

ومن أهم طرق التعمية بالتبديل ما يكون بجمع حروف الرسالة، بعد ترميزها وفق نظام رقمي معين، جمعًا دائريًّا مع حروف مفتاح متفق عليه بين المتراسلين، فمثلًا إذا رمَّزنا حروف اللغة العربية بالأرقام العشرية من /1/ إلى /28/ بحسب ترتيب أبجد، وكان المفتاح المتفق عليه هو: (كليلة ودمنة) = B، تكون عملية التعمية بهذه الطريقة وفق ما يأتي:

- The clear message M, the encrypted message E(M), and the two keys (Ks,Kp) are represented by positive integers numbers.
- The keys are generated

n=q*p r=(q-1)(p-1) 77=11*7 60=(11-1)(7-1)

e<r e&r have no common divider e=37 or 11,19 etc

e*d=1 mod (r) 37d=1 mod(60) d=13

Ks=(d,n) Kp=(e,n) Ks=(13,77) Kp=(37,77)

- It is difficult to find d knowing n and e if q and p are of 100 digits.
- E(M)=M**e mod(n)
- M=E(M)**d

نظام ترميز عشري													
أ	ب	ج	د	ه	و	ز	ح	ط	ي	ك	ل	م	ن
1	2	3	4	5	6	7	8	9	10	11	12	13	14
س	ع	ف	ص	ق	ر	ش	ت	ث	خ	ذ	ض	ظ	غ
15	16	17	18	19	20	21	22	23	24	25	26	27	28

ولتكن الرسالة المُراد تعميتها هي: (يكثف العمل صباح الغد) = A

الرسالة الواضحة A	ي	ك	ث	ف	ا	ل	ع	م	ص	ب	ا	ح	ا	ل	غ	د
المفتاح B	ك	ل	ي	ل	هـ	و	د	م	هـ	ك	ل	ي	ل	هـ	و	د
ترميز الرسالة الواضحة	10	11	23	17	1	12	16	13	18	2	1	3	1	12	28	4
ترميز المفتاح	11	12	10	12	5	6	4	13	5	11	12	10	12	5	6	4
ترميز الرسالة المعمّاة بالجمع الدائري	21	23	5	1	6	18	20	26	23	13	13	13	13	17	6	8
الرسالة المعماة C	ش	ث	هـ	ا	و	ص	ر	ض	ض	ث	م	م	م	ف	و	ح

مثال على الجمع الدائري بأساس 28 «إذا تجاوزت النتيجة 28 فيطرح منها 28»:

$1 = 17 + 12$ $\quad$ $6 = 28 + 6$ $\quad$ $5 = 23 + 10$

فيكون النص المُعَمَّى هو: | C = (شثها وصرضض ثممم مفوح) |

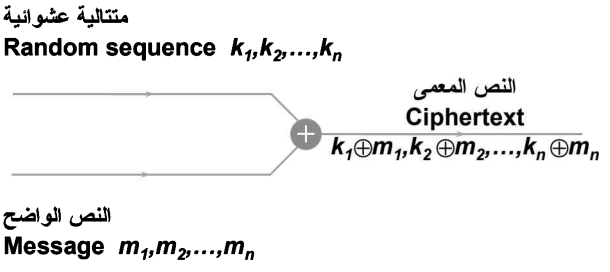
وبهذا، فعملية التعمية التي يقوم بها المُرْسِل هي الآتية:

$$C = A \rho B$$

حيث A هي النص الواضح وB هي المفتاح وC هي النص المُعَمَّى، أما المُسْتَقْبِل الذي يعرف المفتاح فيقوم بالعملية الآتية:

$$A = C \sigma B$$

تعمية فيرمان Vernam Cipher



كلا الرسالة والمفتاح متتالية من الخانات الإثنانية
The message and key are bit strings

حيث r هي عملية الجمع الدائري بالقياس /28/: modulo 28 وs عملية الطرح، أما المُسْتَرِق فسيحاول استخراج التعمية عن طريق اكتشاف المفتاح المستعمل، وهذا ممكن إذا كانت الرسالة أطول من المفتاح بمرات عدة، وهي أسهل إذا كان المفتاح جملة مفيدة.

واقترح فيرنام Gilbert Vernam عام 1917م، خلال الحرب العالمية الأولى، استعمال مفتاح عشوائي غير ذي معنى، طوله يساوي طول النص الواضح، وقد أُثبت رياضياتيًّا عام 1948م أن هذه الطريقة غير قابلة للاستخراج، وبهذا تكون منظومة التعمية هذه هي الوحيدة التي أُثبت رياضياتيًّا أنها آمنة، شريطة عدم استعمال المفتاح نفسه أكثر من مرة واحدة، وعدم حصول المُسْتَرِق على المفتاح بطرق أخرى، وتكون المفاتيح في سِجلّ، تحوي كل صفحة منه مفتاحًا، وتستعمل الصفحة مرة واحدة تتلف بعدها، ومن هنا أتت تسمية الطريقة بـ (سِجلّ المرة الواحدة) one time pad، ويمكن أن نفهم بسهولة سبب استحالة استخراج هذه التعمية لمن لا يعرف المفتاح مما يأتي: إن النص الذي ستعميه يمكن أن ينتج عنه أي نص، وذلك بحسب المفتاح الذي تستخدمه، فيمكن لكلمة (محمد) أن تعطي بحسب المفتاح، على حد سواء، كلمة (حشلم) أو كلمة (شخشك) أو كلمة (سامر) أو أي كلمة ذات أربعة حروف، ولذلك كان من المستحيل على من لا يعرف المفتاح نفسه أن يستخرج كلمة (محمد) الأصلية، ولهذه الخاصية استخدمت طريقة التعمية هذه في (الهاتف الأحمر) بين موسكو وواشنطن، الذي قيل فيه: إن أشرطة تسجيل مغناطيسية، محروسة بعناية، تنقل باستمرار بين واشنطن وموسكو بالطائرة.

لذا كانت سيئة نظام تعمية فيرنام أو نظام (سِجلّ المرة الواحدة) في ضرورة توزيع سِجلّ المفاتيح بين المتراسلين مسبقًا، وهذه عملية صعبة ومكلفة وغير آمنة، فهي أولًا صعبة أو مكلفة؛ لأنه يجب إرسال سِجلّ المفاتيح لكل المستقبلين قبل التراسل، على أن تكون هذه السجلات مختلفة عن بعضها، ويجب حفظها لدى المُسْتَقْبِل طوال مدة التراسل، وهي ثانيًا غير آمنة؛ لأن هناك احتمال استراق سِجلّ المفاتيح خلال عملية التوزيع أو خلال مدة الحفظ لدى المُسْتَقْبِل، وعملية التوزيع هي عن طريق المراسل أو البريد أو الوسائط السلكية أو اللاسلكية، وهي كلها عُرضة للاستراق، وحفظها مدة من

الزمن لدى المُسْتَقْبِل قبل استعمالها يعرضها أيضًا للاستراق، وهنا يأتي ميكانيك الكم ليحل هذه المشكلة، ويضمن توزيع المفاتيح العشوائية بأمان تام كما سنرى.

لنستعمل الآن نظام ترميز اثناني بدل النظام العشري، كما هو مبين في الجدول الآتي:

نظام ترميز اثناني						
2^4	2^3	2^2	2^1	2^0	الحرف	الرمز العشري
0	0	0	0	1	أ	1
0	0	0	1	0	ب	2
0	0	0	1	1	ج	3
0	0	1	0	0	د	4
0	0	1	0	1	ه	5
0	0	1	1	0	و	6
0	0	1	1	1	ز	7
0	1	0	0	0	ح	8
0	1	0	0	1	ط	9
0	1	0	1	0	ي	10
0	1	0	1	1	ك	11
0	1	1	0	0	ل	12
0	1	1	0	1	م	13
0	1	1	1	0	ن	14
0	1	1	1	1	س	15
1	0	0	0	0	ع	16
1	0	0	0	1	ف	17
1	0	0	1	0	ص	18
1	0	0	1	1	ق	19
1	0	1	0	0	ر	20
1	0	1	0	1	ش	21
1	0	1	1	0	ت	22
1	0	1	1	1	ث	23
1	1	0	0	0	خ	24
1	1	0	0	1	ذ	25
1	1	0	1	0	ض	26
1	1	0	1	1	ظ	27
1	1	1	0	0	غ	28

الجمع الدائري

$0 \rho 0 = 0$ $\quad$ $1 \rho 1 = 0$

$0 \rho 1 = 1$ $\quad$ $1 \rho 0 = 1$

ليكن النص الواضح هو (محمد) فترميزه وفق النظام الاثناني (01101 – 01000 – 01101 – 00100) = A فإذا كان المفتاح متتالية عشوائية اثنانية، طولها طول المفتاح (0010110101000110101 1) =B، وكان الجمع الدائري في الحقل /2/ (modulo 2).

تكون عملية التعمية كما يأتي: C = A ρ B ويبعث المُرْسِل C للمستقبل.

النص الواضح	م	ح	م	د
ترميز النص الواضح A	01101	01000	01101	00100
ترميز المفتاح B	010011	00011	10101	00101
ترميز الرسالة المعماة بالجمع الدائري C	00110	01011	11000	00001
الرسالة المعماة	و	ك	خ	ا

فإذا جمع المُسْتَقْبِل جمعًا دائريًّا C مع B فيحصل على النص الأصلي A وتبقى المسألة هنا هي توزيع سِجلّ المفاتيح، وهو متتالية عشوائية اثنانية آمنة بين المتراسلين، ومن ثم نصل إلى الهدف المنشود في نظام غير قابل للاستخراج، وهنا يأتي ميكانيك الكم ليقدم الحل لهذه المشكلة، وهو يكمن في قناة اتصال محمية من كل استراق يستحيل تجسسها دون شعور المتراسلين بذلك، حيث تكون الفوتونات المستقطبة حاملة للمعلومة (1) أو (0) بحسب استقطاب الفوتون.

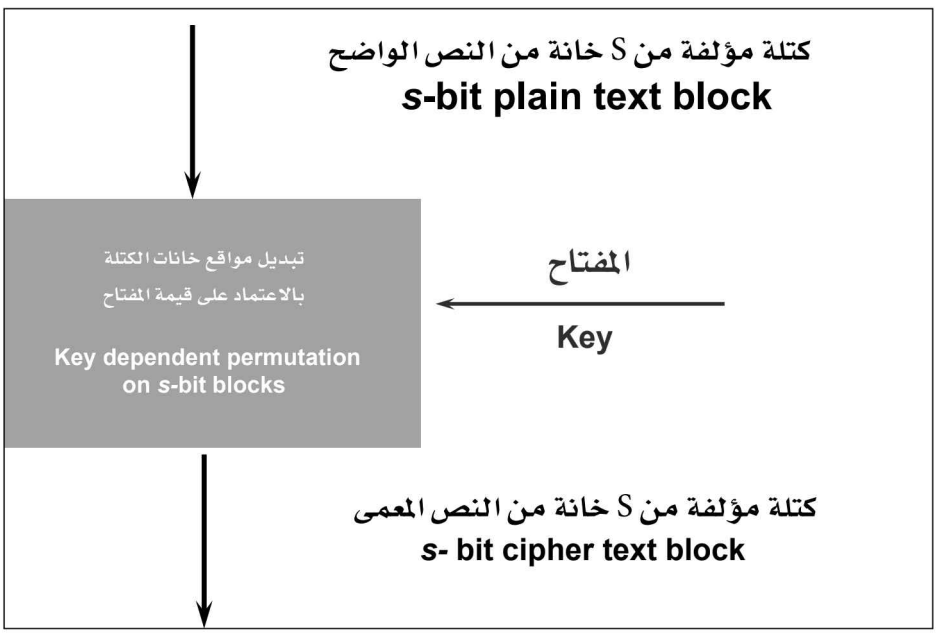
وقد حقق ميكانيك الكم أخيرًا تقدمًا عظيمًا في هذا الاتجاه لم يستطع الرياضياتيّون وحدهم تحقيقه، وتستخدم وسائل التعمية الكمومية فوتونات ضوئية إفرادية، وتعتمد على مبدأ هايزنبرك في الارتياب لتحقيق هدفها في التعمية غير القابلة للاستخراج، بل إن مجرد الاستراق يصبح غير ممكن دون تنبيه المتراسلين، وتسمح تقنية التعمية الكمومية أيضًا بتحقيق عمليات أخرى، مثل التحقق من هوية المُرْسِل، ومثل فكرة الأوراق النقدية غير القابلة للتزوير، وغيرها. والجدير بالذكر أن شركة IBM قد طرحت للعامة

حاسوب كمومي أوليًّا في إبريل من عام 2016م يمكن تجربته عن طريق موقعها على الإنترنت في مثل التعمية الكمومية[1].

وتتميز التعمية الكمومية بأنها تعتمد مبدأ (سِجلّ المرة الواحدة) وهو غير قابل للاستخراج، وتحقق نقل المفتاح العشوائي بين المتراسلين بأمان؛ لأنها تنبه المتراسلين إلى وجود مسترق عند حدوث الاستراق.

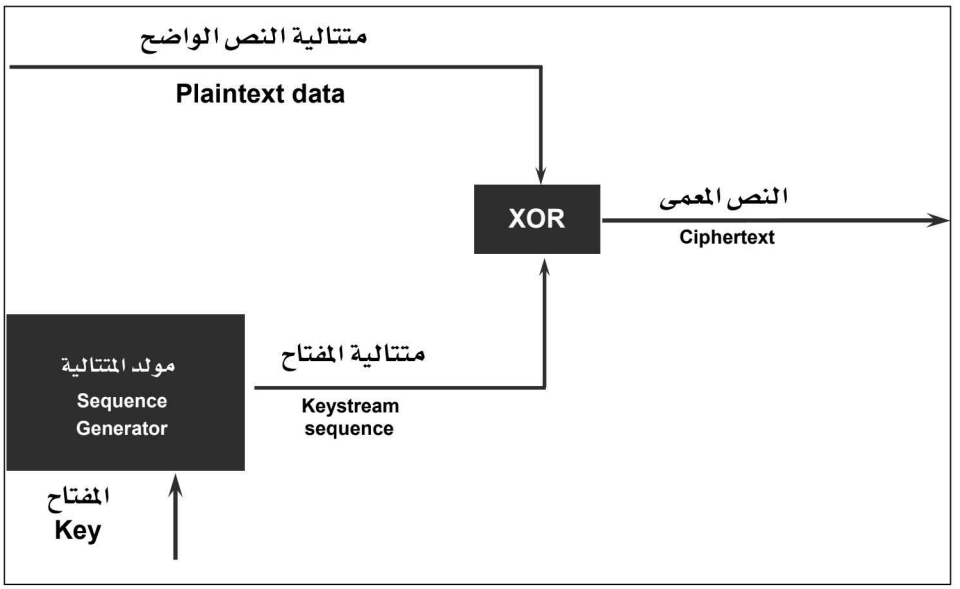
وتجدر الإشارة إلى أن التعمية المتناظرة الحديثة تستخدم نظامين من أنظمة التعمية، وهما التعمية التسلسلية stream cipher والتعمية الكتلوية block cipher، ويبين الشكلان الآتيان شرحًا لهذين النظامين، وفي كلا النظامين تكون الرسالة والمفتاح مرمزتين اثنانيًّا؛ أي باستعمال (1) و(0).

نظام تعمية كتلوي متناظر Symmetric Block Cipher System



(1) جريدة الرياض، الأربعاء 04 شعبان 1437هـ/ 11 مايو 2016م.

التعمية التسلسلية (متتالية إثنانية) Stream Cipher



2.2.6 الوسائل والعلوم المستخدمة في التعمية واستخراجها

إن الوسائل التي كانت مستخدمة في علوم التعمية في القرون الوسطى هي الورق، والقلم، والخرز الملون، وعقد الأصابع، وشبكات الاتصالات البريدية، وغيرها، أما الآن فلا يزال الورق والقلم مستعملًا إلا أن الأجهزة الميكانيكية (المسننات) طغت في أواسط القرن العشرين، أما الأجهزة الإلكترونية والحواسيب وشبكات الاتصال الإلكترونية، فأصبحت هي الغالبة الآن.

وتقع أسس علوم التعمية في مجالات متعددة أهمها الرياضية، مثل علم الأرقام، وعلم الإحصاء والاحتمالات، والجبر البولي، ونظرية التعقيد، ومعالجة الإشارة، ونظرية الألعاب، وغيرها، وتليها الأسس اللسانية من علوم الصوتيات، والصرف، والنحو، والدلالة، واللسانيات الحاسوبية، يضاف إليها أيضًا علوم الإدارة، وعلوم الإلكترونيات، والمعلوميات، وميكانيك الكم.

3.6 طول المفتاح وقوة التشفير.

تُعدّ عملية توليد المفاتيح أكثر العمليات حساسية في التعمية، فحتى يكون نظام التعمية سريًّا قدر الإمكان يجب أن تكون المفاتيح أعدادًا عشوائية حقًّا وغير قابلة للتنبؤ من قِبَل مستخرجي التعمية، إن مثل هذه الأعداد المطلوبة تختلف عن تلك التي تولدها الحواسيب خوارزميًّا باستعمال المتتاليات المحدودة شبه العشوائية من أجل استخدامها في الألعاب وفي عمليات تمثيل النظم الطبيعية Simulations، إذ إن الأعداد العشوائية حقًّا لا يمكن استخراجها إلا من (الضجيج) البيئي لعالمنا الفيزيائي، لكن توليد مثل هذه الأعداد العشوائية عالية الجودة في الحاسوب أمر صعب.

ومن المفيد ملاحظة أن نظام التعمية الوحيد الذي أثبت علماء التعمية سريته التامة، هو ما يسمى (سِجلّ المرة الواحدة) (OTP) One Time Pad الذي يكون فيه طول المفتاح العشوائي مساويًا لطول الرسالة نفسها، ففي هذا النظام تستخدم سلسلة عشوائية لتعمية الرسالة خانة خانة (Bit for Bit) أي إن الخانة (Bit) الرابعة والثلاثين من المفتاح تُستخدَم لتغيير الخانة الرابعة والثلاثين من الرسالة، والمفتاح يجب أن يكون عشوائيًّا حقًّا، فلا يقبل أن يكون سلسلة شبه عشوائية مولدة عن طريق خوارزمية محددة؛ لأنه عندها ستكون التعمية قابلة للكسر، ولكن نادرًا ما يجري استخدم نظم التعمية بـ (سِجل المرة الواحدة) OTP؛ لأنها غير عملية، إذ يجب على المفتاح أن يكون بطول الرسالة، ويجب إرساله للمستقبل عبر قناة سرية، والأنكى من ذلك أنه يستعمل مرة واحدة، وإلا فهو معرّض للاستخراج.

وعلى الرغم من اعتقاد كثير من الناس أن طول المفتاح هو العامل الحاسم في قوة التعمية، إلا أن هناك صفة لا تقل أهمية ألا وهي جودة تصميم نظام التعمية، ولنأخذ على سبيل المثال التعمية بالإعاضة البسيطة التي يُستعاض فيها مثلًا عن كل الألفات

بالسينات، وكل الباءات بالكافات، وكل التاءات بالفاءات، وهكذا... إن عدد الطرق هذه التي يمكن بها ترتيب الألفبائية العربية المؤلفة من 28 حرفًا يُعطى بالعلاقة:

28! (أي 1x2x3x 4x5x.....x26x27x28)، هذه الكمية تساوي (0488, 3 ×10 29) وهذا العدد من المفاتيح الممكنة يُعدّ (فضاء مفتاح) مقبولًا نسبيًّا، ويتطلب معدات حاسوبية ضخمة لكسره إذا أردنا فحص كل المفاتيح الممكنة حتى الوصول إلى النص الواضح، إلا أنه يمكن استخراج هذا النوع من التعمية دائمًا دون الحاجة لأكثر من ورقة وقلم رصاص، ويكون ذلك بأن نتفقد ببساطة الحرف الأكثر تواترًا في النص المعمى وافتراضه ألفًا (في حال اللغة العربية) وبعدها نتفقد الحرف الثاني الأكثر تواترًا، ونفترضه لامًا، وهكذا حتى نستخرج التعمية. إذًا، فعلى الرغم من أن (فضاء المفتاح) في هذه الطريقة كبير إلا أن الطريقة ضعيفة للغاية.

والحقيقة أن نظم التعمية ذات التصميم الجيد تحتاج في كسرها إلى جهد يتناسب مع طول المفتاح، ففي حالة التعمية الكتلوية (أو المقطعية) Block cipher تكون هذه العلاقة أسية، فعندما نزيد طول المفتاح خانة واحدة (1 Bit) يتضاعف عمل المستخرج في تجربته جميع المفاتيح الممكنة، وعندما نضاعف طول المفتاح، فيجب أن نربع كمية الجهد المطلوب، فمن أجل مفتاح طوله 128Bit نحتاج وسطيًّا إلى 2128 (7, 1 1038 x) عملية حسابية لاستخراج هذه التعمية.

ومن جهة أخرى تكون خوارزميات التعمية بالمفتاح المعلن أقل حساسية لطول المفتاح، فعادةً يكون فضاء المفاتيح تحت أسي، ولكن فوق خطي، وهذا يعني أن مضاعفة طول المفتاح يزيد كمية الجهد المطلوب لاستخراج التعمية كثيرًا، إلا أن هذه الكمية هي أقل من مربع الجهد، فإذا استعملنا خوارزمية التعمية بالمفتاح المعلنRSA على سبيل المثال نجد أن الخوارزميات الحديثة للتحليل إلى العوامل الأولية لا تعتمد تجربة كل الأعداد الأولية الأصغر الممكنة للوصول إلى تحليل العدد، بل تستعمل طرقًا أكثر جدوى

بكثير، وكذلك فطريقة ديفي- هلمان هي تحت أسية، وبغية إعطاء فكرة للمقارنة بين التعمية غير المتناظرة وتلك المتناظرة، فإن التعمية بمفتاح طوله3000 Bit بطريقة RSA أو ديفي- هلمان تطلب لاستخراجها تقريبًا الكمية نفسها من الجهد الذي تتطلبه طريقة التعمية المقطعية ذات مفتاح بطول 128 Bit.

التعمية المقطعية صعبة المنال نسبيًا على المستخرجين، وعلى الرغم من ذلك، فقد قامت شركة Electric Frontier Foundation منذ 20 عامًا ببناء حاسوب تفرعي خاص (أي مجموعة من الحواسيب تعمل على التوازي) أمكنه استخراج تعمية رسالة مشفرة بخوارزمية DES بمدة حساب تقل عن أسبوع، وذلك عن طريق تجريب كل المفاتيح الممكنة لفضاء مفتاح بطول 56 خانة Bit 56 .

إن استخراج المعمى بطريقة تجريب المفاتيح جميعها (طريقة القوى العمياء) ليست الطريقة الوحيدة، فأهل هذا العلم يستطيعون استخدام أدوات إحصائية ورياضياتية قوية لإيجاد طرق مختصرة ككشف بعض تراكيب النص المعمى، ويمكن تبويب طرق استخراج المعمى في ثلاثة أنواع، وذلك تبعًا لمدى معرفتنا لمعلومات عن النص الواضح والنص المشفر المقابل له.

ففي بعض الحالات يكون كل ما يعرفه المستخرج هو النص المعمى فقط، ومن ثم يكون لديه القليل من المعلومات التي يمكن أن تساعده على تخمين المفتاح، وفي هذه الحالة يمكن حتى لطرق التعمية سيئة التصميم أن تصمد أمام الهجوم بمعرفة النص المشفر فقط، ولكن إذا وصل إلى علم المستخرج على الأقل جزء من النص الواضح، مثلًا أن النص يبدأ بجملة: (عزيزي السيد سامر) فإن فرص النجاح تزداد بشكل كبير، فعلى الأقل يمكن للمستخرج أن يجرب عددًا من المفاتيح المختلفة حتى يصل إلى مفتاح منها يفك به تعمية (عزيزي السيد سامر) حتى إذا عرف المستخرج لغة النص الواضح فقط (مثلًا الروسية أو الفرنسية أو العربية) فإن هذه المعلومة ستساعده كثيرًا، فإذا

كانت الرسالة بالإنجليزية فالمعروف أن أكثر الكلمات تواترًا هي «The» من أجل هذا وبغية الحماية من استخراج التعمية بالكلمة المحتملة تقوم بعض نظم التعمية بالضغط الإلكتروني للرسالة قبل تعميتها بهدف إخفاء التراكيب التي يسهل التنبؤ بها.

يعرف المستخرج عادةً معلومات تزيد عما ذكرناه أعلاه، فإذا قام أحدهم بسرقة (بطاقة ذكية) تحتوي على دارات تعمية، فإنه ربما يستطيع تجريب بلايين الرسائل المنتقاة بدقة لهذه البطاقة ثم دراسة النصوص المعماة الناتجة، فمثل هذه الطريقة في الاستخراج باستعمال نصوص واضحة منتقاة يمكنها أن تكسر بسهولة نظام تعمية سيئ التصميم، ولنضرب مثالًا آخر حول نظام المفتاح المعلن، إذ يمكن للمستخرج أن يكتب رسالة، ثم يقوم بتعميتها بالمفتاح المعلن (المتاح للجميع) وبعدها يقوم بتحليل النص المعمى الناتج.

لقد جرى تطوير طريقتين فعالتين جدًّا في استخراج المعمى ألا وهما طريقة الفروق (أو الطريقة التفاضلية) والطريقة الخطية، وقد استعمل كلا المنهجين لكسر عدد من طرق التعمية المعروفة، وكذلك للبرهنة على إمكانية كسر معيار التعمية DES بسرعة تفوق بمئات بل آلاف المرات عن تلك التي تقوم على تجربة جميع المفاتيح الممكنة.

إن طريقة الاستخراج بالفروق تعتمد على تعمية عدد كبير من أزواج النصوص الواضحة ذات الفروق المنتقاة بدقة من أجل إيجاد أزواج النصوص المعماة المقابلة التي تتمتع بعدم تشابه محدد، فعند الوصول إلى زوج من هذه الأزواج، فإنه ستُكشَف للمستخرج معلومات حول المفتاح المستخدم، أما في طريقة الاستخراج الخطية والمطورة في شركة ميتسوبيشي اليابانية فيجري البحث عن الترابط بين النص الواضح والنص المعمى والمفتاح الموجودة أكثر مما يتوقع، ثم القيام بعد ذلك بإجراء إحصائيات على عدد كبير من الأزواج، نص واضح – نص معمى، وذلك بهدف إيجاد انحيازات تكشف معلومات عن المفتاح.

4.6 أمان خوارزميات التعمية

ثمة ثلاثة مداخل رئيسة لقياس أمان خوارزميات التعمية:

- إذا كانت التكلفة المالية المطلوبة لكَسر الخوارزمية أكبر من القيمة الفعلية التي تَحمِلها المعلومات المُعمَّاة فهي آمنة.
- إذا كانت المدة (الزمن) المطلوبة لكَسِر الخوارزمية أكبر من المدة التي يَنبغي أن تكون المعلومات في غضونها محمية (مُعمَّاة) فهي آمنة.
- إذا كان مقدار المعلومات المطلوبة لكَسِر الخوارزمية أكبر من مقدار المعلومات المُعمَّاة فهي آمنة. (المعلومات التي قد تكون ضرورية لكَسِر خوارزمية التعمية تَتمثَّل مثلًا في تفاصيل دقيقة عن الخوارزمية، ونتائج لهجمات تمَّت مسبقًا، وتحليلات ضخمة لعمل الخوارزمية، و... إلخ).

عمومًا، يجب أن تُبنَى خوارزمية التعمية، بحيث يَنبغي أن تَبقى المعلومات المحمية بها (مهما كان مستوى حساسيتها) أقل قيمة من تكلفة كسرها.

1.5.6 نماذج تقييم أمان خوارزميات التعمية

يمكننا تقييم أمان خوارزميات التعمية من خلال تصنيفها إلى نموذجين أساسيين: **خوارزميات آمنة بلا قيد** Unconditionally Secure Algorithms، و**خوارزميات آمنة حسابيًّا** Algorithms Computationally Secure.

الخوارزمية الآمنة بلا قيد.

تُعدّ خوارزمية التعمية آمنة بلا قيد إذا لم تتوافر معلومات كافية لاستعادة النص الواضح من نص معمّى مقابل، ويُفتَرَض في الخصم، في نطاق هذا النموذج، أن يمتلك موارد حسابية (وغير حسابية، زمن كافٍ - راحة - مال - ...) غير محدودة من أجل أن يشن هجومًا على الخوارزمية لكسرها، ولكن يظل مع كل تلك الموارد غير قادر على

استعادة النص الواضح، وإنَّ أمان هذه الخوارزميات هو أمان مطلق (غير مشروط)؛ لذا تُسمّى السريّة التي تقدّمها **السريّة المثالية** Perfect Secrecy. إنَّ مستوى السريّة المثالية هو هدف لكل مصمم خطة تعمية، وليس ثمّة خوارزمية تعمية تستطيع أن تحقق مثل هذا الأمن المطلق إلا خوارزمية (سِجلّ المرة الواحدة) one–time pad.

ثمّة شرطان أساسيان ليكون نظام التعمية المتماثل آمنًا بلا قيد: الأول، أن يكون المفتاح عشوائيًّا تمامًا، وأن يكون طوله مساويًا على الأقل لطول الرسالة، وألا يُستخدَم مرة ثانية، والثاني، ألا تتوافر المعلومات اللازمة للتيقّن من حقيقة النص الواضح المسترجع بعد كسر تعمية النص المعمّى المقابل؛ أي يجب أن يتوافر عدد كبير من النصوص الواضحة المقبولة بوصفها حلولًا للنص المعمّى، بحيث لا توجد طريقة لتحديد النص الواضح الأصلي الحقيقي من بين تلك النصوص الواضحة المسترجعة.

وكما قلنا: إنَّ نظام (سِجلّ المرة الواحدة) هو أكبر مثال عن خوارزمية تعمية متماثلة آمنة بلا قيد، أمَّا بقية خوارزميات التعمية المتماثلة فلا تقدّم الأمان المطلق، إذ إنها من النموذج الثاني.

بالنسبة إلى خطط التعمية بالمفتاح العلني فهي بالتأكيد لا تقدّم الأمان المطلق، والسبب هو: بتوافر النص المعمّى $c \in C$ والمفتاح العلني $e \in K$، يمكن استرجاع النص الواضح $m \in M$ عن طريق تعمية جميع عناصر فضاء النص الواضح M بالمفتاح e ومقارنة النتائج بالنص المعمّى الموجود، وإذا تطابقت نتيجة تعمية أحد النصوص الواضحة m بالمفتاح e مع نص معمّى c فذلك هو المطلوب (دون الحاجة إلى اكتشاف المفتاح الخاص $d \in K$).

الخوارزمية الآمنة حسابيًّا.

تُعدّ الخوارزمية آمنة حسابيًّا، وتُدعى حينها **الخوارزمية القويّة** Strong Algorithm، إذا تعذر كسرها مع وجود الموارد الحسابية الآنية على الأقل أو المستقبلية، وإنَّ جميع

خوارزميات وأنظمة التعمية الحالية المتماثلة وغير المتماثلة (ماعدا نظام: سِجلّ المرة الواحدة one–time pad) هي أمثلة عن نموذج الخوارزمية الآمنة حسابيًّا، وعمومًا تهتم تقنيات التعمية الحديثة، وتركّز على هذا النموذج فقط.

تتصف خوارزمية التعمية بأنها **قابلة للكسر** Breakable إذا استطاع طرفٌ[1] ما أن يكتشف، أو أن يصوغ طريقة لاستعادة النص الواضح من النص المعمّى المقابل دون معرفة ولو جزئية بالزوج المفتاحي (e، d) في إطار زمني معيّن، ويتحدد الإطار الزمني بالمدة التي تصغر المدة التي تكون في غضونها المعلومات المعمّاة ذات أهمية، وإنَّ هذا الإطار الزمني هو تابع لعمر أهمية المعلومات المحمية التي تحمل قيمة ما، وعلى سبيل المثال، لو تم التخطيط لدى قيادة جيش في بلدٍ ما لشن حرب على بلدٍ آخر في وقت معيّن، ووجبَ أن تكون هذه المعلومات سريّة (معمّاة) إلى وقت تنفيذ الهجوم؛ أي لنقل: 48 ساعة، فإنَّ عمر أهمية هذه المعلومات هو 48 ساعة بالتمام، ولن يستفيد الخصم، بعد اعتراضه وحصوله على هذه المعلومات المعمّاة، من معرفة مضمونها ومحتواها حتى ولو بعد ثانية من مرور الـ 48 ساعة؛ لأنَّ هذه المعلومات تكون قد فقدت أهميتها، والإطار الزمني لكسر حماية تلك المعلومات يتحدد بين 1 ثانية و47،59،59 ثا/ د/ سا.

ينبغي أن تُصمَّم خوارزميات التعمية الحديثة، بحيث تكون غير **قابلة للكسر** Unbreakable مع توافر الموارد الحسابية الآنية المتوقّع أن تزداد، وتتضاعف في المستقبل القريب.

تزداد الثقة في أمن خوارزمية التعمية إذا ما تصدَّت وبشكل دائم لعمليات التحليل المختلفة التي يقوم بها خبراء كبار في علم تحليل التعمية، وإنَّ مثل الخوارزميات التي يمضي عليها سنوات، ولم تنجح أي عملية تحليل لاختراق أمنها تُعدّ أفضل من تلك

(1) قد يكون هذا الطرف خصمًا، وقد يكون مصمم الخوارزمية نفسه الذي يقوم بهذا العمل بهدف اكتشاف نقاط الضعف.

الخوارزميات الحديثة التي يُعلن مصمموها أنها الأفضل، وأنها تقدّم أمنًا أكثر، ولا يمكن أن تُكسَر.

ينص الافتراض الأساسي في التعمية على أن تكون فضاءات النص الواضح M والنص المعمّى C والمفتاح K ومجموعة توابع التعمية $\{Ee: e \in K\}$ وتوابع فك التعمية $\{Dd: d \in K\}$ معروفة للجميع دون استثناء، لكنَّ الشيئين اللذين يجب على طرفي الاتصال الاحتفاظ بهما سرًّا هما النص الواضح m والزوج المفتاحي (e, d)[1]، وما يخالف هذا الافتراض هو التفكير في وجوب اعتماد أمان الخوارزمية على جعل الطريقة التي تعمل بها سرًّا، وتُدعى مثل هذه الخوارزمية **الخوارزمية المقيَّدة** Restricted algorithm.

مما لا شك فيه، فإنه لا أحد يستخدم الخوارزميات المقيّدة في هذه الأيام، إذ إنها غير كفأة لمقاييس الحماية المطلوبة للمعلومات السريّة، ومع ذلك تبقى مستعملة داخل كثير من التطبيقات المنخفضة السريّة لأغراض تتصف فيها حماية المعلومات بأنها مجرد أداة ثانوية ملحقة، ومن الصعب جدًّا استعمال الخوارزميات المقيّدة في تراسل المعطيات المحمية عبر الشبكة؛ لأن ذلك يتطلب إعداد شبكات اتصال خاصة لنقل تلك الخوارزميات بأمان إلى الأطراف الأخرى، ومن صفات الخوارزميات المقيّدة أنها لا تخضع لبحوث تحليلية، وهي على الأغلب للاستخدام الشخصي فقط.

ولقد تَعرَّف المجتمع التعموي الحديث منذ نشوئه إلى مجموعة من المبادئ الأساسية لبناء أي خطة تعمية، وسُميّت هذه المبادئ **مبادئ** Kerckhoffs، وأصبحت افتراضات ومتطلبات في الوقت نفسه لأي نظام تعمية، ونصَّ أحد تلك المبادئ على إرشاد يخالف استعمال الخوارزميات المقيّدة، حيث دعا إلى أن تكون تفاصيل الخوارزمية علنية وصريحة وغير سريّة.

---

(1) إذا كان $e = d$ فيجب الاحتفاظ بهما معًا؛ كونهما تركيبة واحدة، وإذا كان $e \neq d$ فيجب الاحتفاظ بالمفتاح d فقط، أمّا المفتاح e فينبغي أن يكون علنيًّا.

2.5.6 مبادئ Kerckhoffs في أمان خوارزمية التعمية

نَشَر عالِم اللغة وخبير التعمية البروفيسور الهولندي Auguste Kerckhoffs عام 1883م مقالة بعنوان (La Cryptographie Militaire) باللغة الفرنسية، التي تعني (التعمية العسكرية)، احتوت على ستة مبادئ أساسية لبناء خطط التعمية العكسرية، ولكن بسبب تحقيقها لمعظم مقاييس أمن المعلومات، تم تعميمها لتشمل خطط التعمية المدنية، وبسبب تغيّر الظروف والحالات من عصر Kerckhoffs إلى عصرنا هذا؛ أي بعد قرن ونيّف، تم تعديل تلك المبادئ لتلائم الأوضاع الحالية مع الحفاظ بجوهرها؛ لذا سنسرد هذه المبادئ كما أعلنها Kerckhoffs ثم سنشرحها بتفسير حديث.

المبدأ الأول: يجب أن يكون نظام التعمية غير قابل للكسر، إن لم يكن نظريًّا فعمليًّا على الأقل. كما نعلم أنه ليس ثمة نظام تعمية آمن بلا قيد إلا نظام (سِجلّ المرة الواحدة)، أو أي خطة تشابهه، وهو النظام الوحيد الذي بُرهِن على أنه غير قابل للكسر على المستويين النظري (الرياضي) والعملي، وفيما يتعلّق بهذه الأوقات، يمكن فهم المقصد الذي أراده Kerckhoffs من هذا المبدأ أن يكون نظام التعمية آمنًا حسابيًّا على الأقل، وصعب الكسر للوقت الآني، وهذا ما ينتهجه اليوم مصمّمو أنظمة التعمية وخوارزمياتها، وتتعلّق الصعوبة العملية لكسر خوارزميات التعمية بناحيتين: الأولى، التعقيد الحسابي بالنسبة إلى كسر خوارزميات التعمية المتماثلة. والثانية، المعضلة الرياضية بالنسبة إلى كسر خوارزميات التعمية غير المتماثلة.

المبدأ الثاني: يجب ألا يُحدِث اكتشاف تفاصيل عمل نظام التعمية أي مشكلة لدى مستخدميه. هذا المبدأ هو المبدأ الشهير في مجتمع التعمية، وهو الشرط الأساسي الذي يجب أن تحققه خوارزمية التعمية، وإنّه لواضح من نص المبدأ أن وقوع تفاصيل عمل نظام التعمية كاملةً بأيدي الخصم ينبغي ألا يخترق أمن المعلومات التي تم تعميتها به، وإضافة إلى ذلك، ينبغي ألا تصنع معرفة تطبيقه (source code) أيضًا أي مشكلة،

وينص هذا المبدأ في الوقت الحالي على أنه يجب أن تكمن سريّة نظام التعمية فقط في المفتاح الذي يستخدمه المشاركون في الاتصال، وليس في تفاصيل عمل النظام، ويجب إذًا على مصمّم خوارزمية التعمية أن يجعل جميع الأسرار الضرورية لأمان المعلومات التي ستعمَّى بها قدر الإمكان متمثّلة فقط في المفتاح الذي سيتم استخدامه، ثم يجب عليه بعدها أن ينشر الخوارزمية للعلن؛ كي يتم إخضاعها للبحث والدراسة، حتى من قِبَل الخصوم، من أجل استكشاف نقاط الضعف غير المُدركة وتحسينها. في الواقع، الوضع مختلف جدًّا بالنسبة إلى وكالة الأمن القومي الأمريكي NSA، إذ إنَّ الوكالة لم ولن ترغب أبدًا في نشر خوارزميات وأنظمة التعمية التي لديها للعلن، والسبب ليس لأنَّ السريّة التي تتبعها في ذلك قد حسّنت من أمن خوارزمياتها ونتائج عملها في التعمية، إنما لكي لا يستفيد أعداء الولايات المتحدة من خبرتها ومعرفة تفاصيل تلك الخوارزميات، وقد تكون الوكالة في هذا الأمر على صواب؛ لأنَّ مقراتها تضم أفضل وأذكى خبراء التعمية وتحليلها في العالم، وهؤلاء الخبراء هم الذين يتولون مهمة تصميم أنظمة التعمية، وهم الذين يحاولون كسرها من أجل اختبارها واكتشاف نقاط الضعف فيها.

المبدأ الثالث: ينبغي أن يكون المفتاح المستخدم في النظام سهل التذكّر، وقابلًا للتغيير في أي وقت. إنَّ سهولة حفظ المفتاح المستخدم أمر ضروري في جميع الأوقات، وينبغي أن يكون المفتاح، عندما يتم الاتفاق عليه بين طرفي الاتصال، سهل الحفظ دون تدوينه على أي وسيلة، ومن ثم سهل التذكّر في كل مرة يتم استعماله، وتحقق خوارزميات التعمية المتماثلة الحديثة هذا الأمر، إذ تمكّن المستخدم من أن يصنع مفتاحه الخاص من كلمة سر سهلة الحفظ والتذكّر، وأمّا بالنسبة إلى خوارزميات التعمية غير المتماثلة فيتولّى مهمة إنشاء المفتاح أحيانًا نظام التعمية نفسه، وقد يتطلّب تخزينه على وسيطٍ ما نظرًا لكبر حجمه، ولكن لا يعني ذلك أن يكون سهل التخمين، فيجب أن يحقق المفتاح العشوائية وسهولة الحفظ معًا، إضافة إلى ذلك، ينبغي لنظام التعمية أن

يكون ديناميكيًّا فيما يتعلّق بإمكانية تغيير المفتاح المستخدم إلى مفتاح جديد، وذلك عند رغبة المشاركين في الاتصال.

المبدأ الرابع: يجب أن تكون الرسائل المعمّاة سهلة النقل عبرَ التليغراف. لقد انخفض استخدام التليغراف في الوقت الحالي، فينبغي أن تكون الرسائل المعمّاة بالشكل الذي يسمح بنقلها عبرَ وسيلة الاتصال بسهولة ودون أخطاء[1]، وهذا يشير إلى أنه يجب على تلك الرسائل المعمّاة أن تضم محارف الأبجدية المعرّفة في وسيلة الاتصال فقط، ويتحقق هذا المبدأ حاليًّا من خلال استعمال نظام الترميز بالأساس 64، حيث تُرمَّز فيه الرسائل المعمّاة قبل نقلها إلى الأطراف الأخرى، ويَسهُل إرسال الرسائل المرمّزة واستقبالها بالنظام Base64 دون أخطاء، وذلك لقابلية تعريف محارفه في وسيلة الاتصال (البريد الإلكتروني).

المبدأ الخامس: ينبغي أن تكون خطة التعمية سهلة التداول والنقل، وينبغي ألا يتطلّب استعمالها جهدًا أكثر من شخص واحد فقط. لقد صاغَ Kerckhoffs هذه المبادئ لبناء خطط تعمية عسكرية، وإذا كانت خطة التعمية عبارة عن آلة، وليست خوارزمية أو طريقة رياضية، فينبغي أن تكون سهلة الحمل والنقل، وفيما يخص العمل الميداني في أثناء الحرب، يتطلّب هذا المبدأ أن تكون خطة التعمية قابلة لتداولها بين المعنيين (ضباط الجيش) سواء كانت آلة أم طريقة رياضية، وأمّا للوقت الحالي فخطة التعمية متمثّلة في الطريقة الرياضية فقط. وهذه الطريقة هي مجموعة من الخطوات المرتّبة ترتيبًا ثابتًا وواضحًا، وإنَّ هذا التمثيل يجعلها سهلة التداول والنقل والنشر، وأيضًا ينبغي ألا يتطلّب استعمال خطة التعمية جهدًا أكثر من شخص واحد، فإذا كانت الخطة آلة تعمية، فمن الضروري ألا تحتاج إلى أكثر من شخص لإنجاز تعمية رسالة ما (وهذا شيء مهم لاعتبارات عدة، منها عدم توافر أكثر من شخص في مكان العمل

(1) قد ينجم الخطأ عن مشكلة في مسار شبكة الاتصال أحيانًا، وهذا الأمر لا علاقة له بالمبدأ.

خاصةً إذا كان هذا المكان حربيًّا)، وإن كانت الخطة رياضية فمن الضروري أيضًا أن تكون سهلة الاستعمال من قِبَل شخص واحد، وتجدر الإشارة إلى أن خوارزميات التعمية المتماثلة الحديثة صعبة التطبيق يدويًّا، ولهذا فإن البرمجيات الحاسوبية تجعل تنفيذها أسهل.

المبدأ السادس: ينبغي أن يكون نظام التعمية سهل الاستخدام، بحيث لا يتطلّب معرفة بإجراءات وقواعد كثيرة، ولا جهدًا ذهنيًّا. من الواضح أن هذا المبدأ يرتبط بالمبدأ السابق، إذ إنه من سهولة نظام التعمية سيُتاح استعماله من قِبَل شخص واحد، وعلى الرغم من أن المبدأ الأول ينص ضمنيًّا على أن تكون خطة التعمية متينة وصعبة الكسر ومعقّدة، إلا أنها ينبغي أن تكون سهلة الاستخدام في الوقت نفسه، وهذا ما ينص عليه المبدأ الحالي، وليسَ على مستخدم النظام، في أثناء تعمية أو فك تعمية رسالة، أن يبذل جهدًا ذهنيًّا كبيرًا لإنجاز المهمة، وأيضًا ليسَ عليه أن يكون ملمًّا بقواعد وإجراءات من أجل إتمام عملية التعمية أو فك التعمية، ونفترض دائمًا أن مستخدم النظام لا يفقه شيئًا بتفاصيله الرياضية الداخلية، ومن ثم فعليه فقط أن يقوم بإدخال المفتاح والنص الواضح أو النص المعمّى وإنجاز بعض الخطوات البسيطة، وثمة طرق تقليدية تتطلّب من مستخدميها أن يمتلكوا بعض الخلفيات الرياضية، مثل معمّي Hill ومعمّي Playfair، وأمّا في خوارزميات التعمية المتماثلة الحديثة فلا يمكن أبدًا تطبيقها يدويًّا حتى ولو توافرت لمستخدميها خلفيات متعددة عنها، وذلك بسبب تعدد خطواتها المعقّدة، وتتطلّب هذه الخوارزميات الحديثة بالتأكيد برمجيات حاسوبية لتطبيقها (باستثناء بعض أنظمة التعمية غير المتماثلة التي يمكن تطبيقها يدويًّا دون استعمال البرمجيات)، حيث لا تأخذ من المستخدم وقتًا أكثر من إدخاله النص الواضح أو النص المعمّى والمفتاح.

إذًا، أهم مبدأ من تلك المبادئ الستة السابقة هو المبدأ الثاني الذي يوصي بأن تكون تفاصيل عمل خطة التعمية معروفة للجميع، وألا تكون تلك المعرفة مصدر تهديد لأمن المعلومات المعمّاة بها، وأن تكمن سريّة النظام بأكمله في المفتاح المستخدَم،

وثمة مبدأ شهير في مجتمع التعمية وأمن المعلومات يخالف مبدأ Kerckhoffs الثاني، وهو مبدأ **الأمن عبر التعتيم** Security Through Obscurity.

ينص مبدأ الأمن عبر التعتيم على استعمال سريّة تفاصيل عمل نظام التعمية، إضافة إلى سريّة التطبيق، لتحقيق أمن المعلومات، ومن المحتمل جدًّا أن تكون أنظمة التعمية التي تعتمد على مبدأ الأمن عبر التعتيم حساسة تجاه الهجمات الكامنة، وقد تمتلك نقاط ضعف كثيرة، وعلى الرغم من ذلك، يعتقد مصمّمو تلك الأنظمة أنها آمنة، وإن كان ثمة عيوب بها فهي غير ظاهرة وغير معروفة، ومن غير المحتمل أن يكتشفها الخصوم ومحللو التعمية، والخوارزميات المقيّدة هي خيرُ مثال على مبدأ الأمن عبر التعتيم.

لنكن أكثر وضوحًا بشأن سريّة المفتاح المستخدَم، ونصَّ الافتراض الأساسي في التعمية على أن يكون فضاء المفتاح K معروفًا، فهذا يعني أن جميع عناصره معروفة بدلالة حجمه وأبجدية التعريف المستخدمة، لكن الموضوع هنا يكمن في أن تتمثل سريّة المفتاح في العجز الذي يواجهه الخصم في العثور عليه من بين مجموعة كبيرة من المفاتيح. إذًا المفتاح موجود، وهو عنصر من أحد عناصر فضاء المفتاح المرافق لنظام التعمية؛ لذا فمن أجل تعقيد المهمة أمام الخصم، يقوم مصمّمو الخوارزميات بجعل فضاء المفتاح ضخمًا قدر الإمكان دون التساهل في قوة الخوارزمية نفسها.

يُعمِّم Bruce Schneier مبدأ Kerckhoffs الثاني ليشمل جميع أنظمة الأمن الأخرى، وإنَّ كل سر يبقى سرًّا في نظام أمني ما لديه بالتأكيد نقطة ضعف محتملة قابلة للهجوم، وينبغي أن تكون الأسرار المطلوب الاحتفاظ بها في النظام الأمني، هذا إن اقتضى الاحتفاظ بها، من المستويات التي إذا تم اختراقها (ولو بالمصادفة) لا تسبب خسائر كبيرة، وهذا الأمر مشابه جدًّا لنظام تعمية قوي، إذ يسعى مصمم الخوارزمية إلى أن يجعل جميع الأسرار المرتبطة بالنظام كامنة بشكل كلي تقريبًا في المفتاح السري

المستخدم، وإذا تم اكتشاف المفتاح فينبغي أن يكون ثمة بديل لإصلاح هذا الخرق؛ البديل هو توليد مفتاح جديد واستعماله، وأمّا الخسارة الكبيرة في نظام التعمية المقيّد فهي اختراق المعلومات المعمّاة به بعد التعرّف إلى تفاصيله، وهذا ما سيحدث إذا تم اعتبار النظام نفسه سرًّا. وكقاعدة عامة «كلما امتلك النظام الأمني أسرارًا أكثر في مضامينه، كان ضعيفًا وعُرضة للهجوم، وكلما كانت أسراره أقل، كان أكثر قوة».

6.6 مبادئ استخراج المعمى و(الهجمات) على إجراءات التعمية أو خدماتها

لقد عرّفنا استخراج المعمى أو تحليل التعمية مسبقًا، (**أو كسر الشفرة**) cryptanalysis or code breaking على أنّه فك تعمية المعلومات السريّة المحمية دونَ معرفة المفتاح المستعمل، وتُدعى المحاولة المقصودة في نطاق تحليل التعمية الهجوم التعموي، وبالتعريف، فـ**الهجوم التعموي** Cryptographic Attack **هو المحاولة المتعمَّدة لتعطيل خدمة ما أو أكثر من خدمات التعمية أو إفساد بروتوكول تعمية أو اختراق أمن خوارزمية تعمية.**

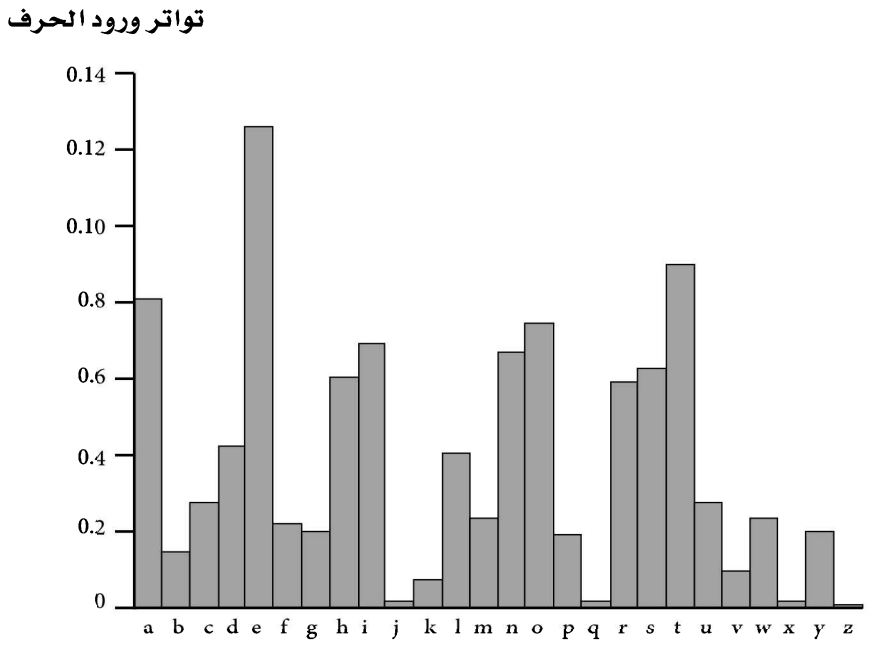
علم استخراج المعمى أكثر تعقيدًا من علم التعمية، ويحتاج إلى معارف في الرياضيات واللسانيات (وفي أيامنا إلى أدوات معلوماتية جبارة).

وأثبتت البحوث أخيرًا أن يعقوب الكندي، فيلسوف العرب (801–873 م) هو مؤسس هذا العلم،

وواضع أول كتاب فيه بعنوان (رسالة في استخراج المعمى) وهي رسالة مذهلة في معلوماتها[1].

(1) (التعمية واستخراج المعمى عند العرب) الجزء الأول والجزء الثاني، تأليف الدكاترة: محمد مراياتي، ويحيى مير علم، وحسان الطيان.

تواتر ورود حروف اللغة الإنجليزية



ويذكر الكندي أن طرق استخراج المعمى تعتمد على ثلاثة مبادئ: **الأول** هو إحصاء تواتر الحروف، أو الأشكال، أو الرموز في النص المعمى بالإعاضة، ومقارنته مع إحصاء تواتر الحروف في اللغة التي كتب بها النص المعمى كالعربية مثلًا، ويقدم الكندي إحصاءه لتواتر الحروف في اللغة العربية، ويذكر أن هذا المبدأ لا ينطبق إلا عندما يكون النص طويلًا إلى حد يسمح فيه عدد الحروف بانطباق القانون الإحصائي عليه (قانون الأعداد الكبيرة في الإحصاء!).

أما المبدأ **الثاني** فهو الاستفادة من تقارن الحروف وتنافرها في اللغة، فهناك حروف تتوالى كثيرًا مثل الألف واللام في (ال) التعريف، حيث تواترها عالٍ جدًّا؛ لذلك يجب البحث عن هذا التقارن في النص والاستفادة منه في استخراج المعمى، وهناك حروف لا تقترن تقديمًا، وأخرى تقترن تأخيرًا؛ أي لا تأتي قبل بعضها أو بعد بعضها،

ويعطي الكندي في رسالته دراسة وافية ومدهشة عن اقتران الحروف وتنافرها، وعن الكلمات الثنائية والثلاثية الأكثر تواترًا في اللغة العربية، مثل (من، عن، أن، في..) و(إلى، على، بلا،...).

أما المبدأ **الثالث** فهو (الكلمة المحتملة) probable word؛ أي ما يُستعمَل في الرسائل أو النصوص من عبارات الاستهلال والألقاب وما إليها، وهذه المبادئ الثلاثة لا تزال صحيحة ومستعملة في استخراج المعمى حتى يومنا هذا، ويُعدّ الكندي مخترع هذا العلم وواضع مبادئه.

وكما سبق هناك طرق غير قابلة للاستخراج، مثل طريقة (سِجلّ المرة الواحدة) وهي الطريقة الوحيدة التي تمَّ البرهان على أنها لا تُستخرج، أما طرق التعمية الأخرى فيمكن استخراجها نظريًّا، ويعتمد ذلك على الوسائل والوقت المتاح للمستخرج. على أن بعض الطرق تحتاج إلى وقت ووسائل غير متوافرة؛ لذلك تُعدّ غير قابلة للاستخراج عمليًّا.

والخلاصة هي أن ثمة أربعةِ مبادئ أساسية في استخراجِ المُعَمَّى أو حلِّ التعميةِ، درجَ العربُ على استخدامِها،

وبرعوا فيها منذ مدة مبكرةٍ على نحوٍ مدهشٍ، وهذه الطرقُ هي:

1. استعمالُ عددِ الحروفِ المستخدمةِ لتحديدِ اللغةِ المُعَمَّاة.
2. استعمالُ تواترِ ورودِ الحروفِ في النصِّ.
3. استعمالُ تواترِ ورودِ ثنائياتِ الحروفِ وثلاثياتها وغيرِها، أو ما سمَّوه ائتلاف الحروفِ وتنافرها.
4. استعمالُ الفواتح التقليديةِ المُحْتَمَلَةِ للرسائلِ، وهو ما سُمِّي حديثًا الكلمة المُحْتَمَلَة الورودِ.

يشتمل الملحق رقم (2) على ثلاثة أمثلة تراثية في استخراج المعمى.

من طرق استخراج التعمية التي تستعمل المفتاح المتناظر:

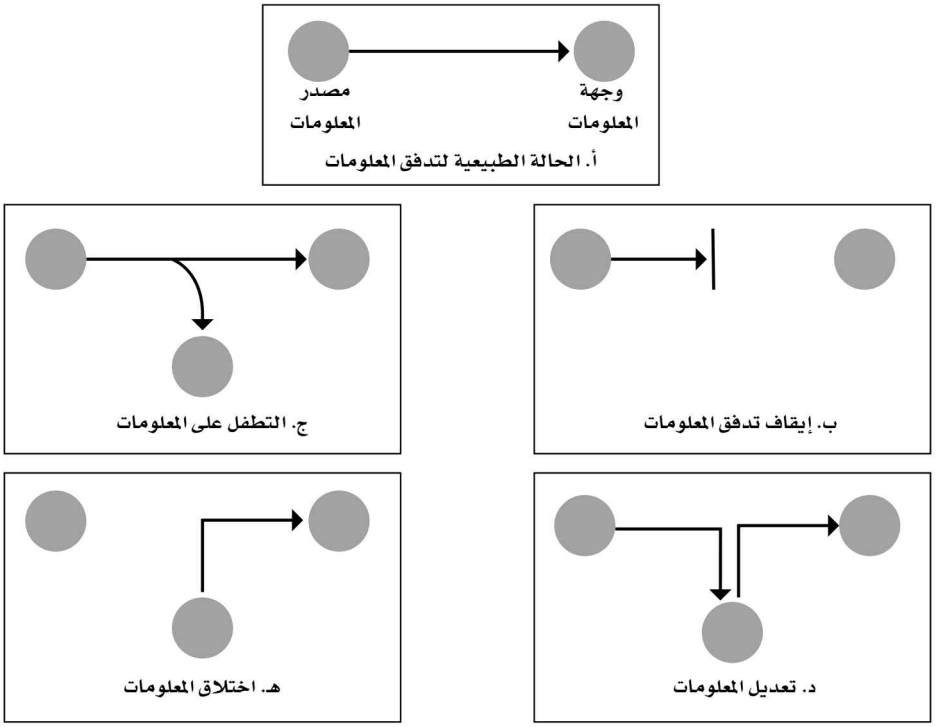
- التحليل (الأعمى) أو تجربة كل المفاتيح باستعمال حواسيب عملاقة.
- التحليل التفاضلي، وقد استخدم في استخراج تعمية المعيار الأمريكيDES ذي المفتاح القصير.
- التحليل الخطي.

وسنتطرق فيما يأتي إلى أهم (الهجمات) المنشورة في استخراج المعمى والهجمات على خدمات التعمية بشكل عام ضمن إطار أمن المعلومات، وإنَّ تصنيف هجمات التعمية متعدد ومتنوع، حيث إنَّ كل مرجع يعتمد على نموذج ما، وسوف نسرد في الفقرة الآتية هجمات التعمية وفق ثلاثة نماذج رئيسة: الهجوم على **خدمات التعمية**، والهجوم على **بروتوكولات التعمية**، والهجوم على **خوارزميات التعمية**.

1.6.6 الهجوم على خدمات التعمية

يتمثّل الهجوم على خدمة ما من خدمات التعمية في تعطيل أداء هذه الخدمة وعملها، ويتمثل نجاح الهجوم في عدم استطاعة المستخدم الشرعي تلقّي هذه الخدمة، ويُصوِّر Stallings في مرجعه مبدأ هذه الهجمات انطلاقًا من أنَّ الحالة الطبيعية لأداء الخدمة وإتمامها تتمثّل في تدفّق المعلومات بشكل سليم ومباشر من مصدرٍ ما إلى وجهةٍ ما؛ أي عندما تصل المعلومات سليمة إلى المكان المقصود تكون الخدمة قد أُدّيت. يعرِّف الشكل (1-4 أ) الحالة الطبيعية لتدفّق المعلومات Normal flow دون أي هجوم.

الشكل (4_1) الهجمات المحتملة على خدمات التعمية.



- **إيقاف تدفّق المعلومات** Interruption. عندما تتدفّق المعلومات عبر الشبكة من مصدرٍ ما إلى وجهةٍ ما يقوم المهاجم باعتراضها ومنع إيصالها إلى تلك الجهة المطلوبة، ويُعَدّ هذا الهجوم هجومًا على خدمة **توافر المعلومات** Availability[1]. يوضّح الشكل (4–1 ب) هذا الهجوم.
- **التطفّل على المعلومات** Interception. عندما تتدفّق المعلومات المحمية من مصدرٍ ما إلى وجهةٍ ما يقوم المهاجم بالتجسس عليها، والحصول على نسخة صافية واضحة منها، ويُعدّ هذا الهجوم هجومًا على خدمة **السريّة** confidentiality. يعطي الشكل (4–1 ج) صورة عن هذا الهجوم.

(1) في الحقيقة، إنَّ خدمة توافر المعلومات ليست من خدمات التعمية، ولكن الهجوم عليها يُعدّ جزءًا من الهجمات الموجَّهة على خدمات التعمية.

- **تعديل المعلومات** Modification. عند تدفّق المعلومات وفق المسار الطبيعي لها يعترضها المهاجم ليقوم بتعديلها، إمّا بإضافة بيانات أخرى عليها، أو إزالة بيانات منها، أو استبدال بيانات، ثم يرسلها بعد ذلك إلى وجهتها الطبيعية المفترَضة، ويُعدّ هذا الهجوم هجومًا على خدمة **سلامة البيانات** Data integrity. انظر الشكل (1–4 د).
- **اختلاق المعلومات** Fabrication. ليس ثمة تدفق لمعلومات حقيقية إلى وجهة طبيعية شرعية، فيقوم المهاجم في هذه الحالة باختلاق بيانات وتركيبها وإرسالها إلى وجهة ما على أنها معلومات قادمة من مصدر شرعي حقيقي، ويُعدّ هذا الهجوم هجومًا على خدمة **استيقان منشأ البيانات** Authentication. انظر الشكل (1–4 هـ).

2.6.6 الهجوم على بروتوكولات التعمية

قبل الحديث عن الهجمات المحتملة على بروتوكولات التعمية، دعنا نعرّف أولًا البروتوكول التعموي باختصار. يُعرَّف **البروتوكول التعموي** Cryptographic Protocol كما جاء في بأنه سلسلة من الخطوات المرتّبة ترتيبًا واضحًا، حيث يستعمل تقنية التعمية وتقنيات أخرى مرتبطة بها من أجل إنجاز مهمة ما، مثل إيصال المعلومات السريّة إلى أصحابها الحقيقيين والكشف عن الخصوم الواقعين في وسط قنوات الاتصال، ويقوم بتلك الخطوات طرفان أو أكثر من الأطراف الشرعية المشاركة، وقد تكون بعض الأطراف غير شرعية؛ لذا يهتم البروتوكول التعموي بالكشف عنها وفضحها.

ويتمثل الهجوم على بروتوكول التعمية في إحباط وإفشال خطوة ما أو أكثر من خطواته، ويتمثل أيضًا في المشاركة في هذا البروتوكول بوصفه طرفًا شرعيًّا دون علم بقية الأطراف، وإنَّ بروتوكولات التعمية كثيرة ومتنوعة، والهجمات عليها متنوعة، ولها

أشكال عدة، وثمّة نوعان عامان من الهجمات المعروفة على بروتوكولات التعمية هما: الهجوم السلبي، والهجوم الفعّال.

1.2.6.6 الهجوم السلبي Passive Attack

يُسمى أيضًا **الهجوم غير الفعّال**. يقوم الخصم أو المهاجم في هذا النوع بمراقبة قناة الاتصال التي يجري فيها تنفيذ البروتوكول بين الأطراف الشرعية المشاركة، والفائدة التي يجنيها هي الحصول على المعلومات المتبادلة وقراءة الرسائل دون أن يُكتشَف (أو على نحوٍ أدق دون أن يُكتشَف وجوده)، فإنَّ الخصم في هذه الحالة لا يأتي بأي حركة تفسد إتمام البروتوكول، وهو بذلك يُعدّ طرفًا غير محسوس به في هذا البروتوكول، ومن صفات هذا الهجوم أنه صعب الكشف، ولهذا عادةً ما تسعى بروتوكولات التعمية إلى أن تمنعه بدلًا من أن تكتشفه؛ لذا من الضروري جدًّا على بروتوكول التعمية أن يتوقّع جميع الاحتمالات التي قد يصادفها، خاصةً إذا كانت حالات اختراق أو تلاعب، وثمّة نوعان من الهجمات السلبية: التجسس، وتحليل الحركة.

التجسّس Tapping.

إنَّ هذا الهجوم هو أبسط هجوم معروف، وليس في هذا الهجوم أي معلومات محمية أو معمّاة (على الرغم من أنها قد تكون سريّة)، إذ تمر المعلومات والرسائل بشكلها الطبيعي عبر قناة اتصال عادية (من المفترض أنها غير آمنة)، ويتجسّس المهاجم ببساطة على قناة الاتصال للاطلاع على المعلومات المتبادلة بين طرفين شرعيين، ومن أمثلة هذا الهجوم: التجسّس على محادثة هاتفية، أو الاطلاع على رسالة بريد إلكتروني عادية غير معمّاة، ويُمكن صد هذا الهجوم بسهولة من خلال استعمال تقنية التعمية، سواء لحماية المحادثات الهاتفية أو لحماية التبادلات الإلكترونية، ويُسمَّى هذا الهجوم أيضًا **تحرير محتوى الرسالة** Release of message contents.

تحليل الحركة Traffic Analysis.

يفترض هذا الهجوم تعمية المعلومات والرسائل التي تمر عبر قنوات الاتصال غير الآمنة، ويراقب المهاجم في هذا النوع حركة الاتصالات والرسائل المعمّاة الجارية بين الأطراف الشرعية، ويقتصر عمل المهاجم من خلال مراقبته لحركة الاتصالات المعمّاة على محاولة معرفة المكان الذي تصدر منه الرسائل، والمكان الذي ستتوجه إليه، وطول تلك الرسائل، وزمن إرسالها، والاستفادة من النماذج التكرارية لنصوص بعضها، إضافة إلى معرفة تطابقها مع الأحداث الخارجية للمتصلين، مثل عقد اجتماع في زمنٍ ما، وينبغي أن تُساعد جميع المعلومات السابقة المهاجم على تخمين طبيعة الاتصالات على الأقل، والأفضل أن تُساعده على اكتشاف مضمون بعضها. وكقاعدة، كلما كان عدد الرسائل التي يتم رصدها واختبارها أكبر، زادَ احتمال نجاح هذا الهجوم، ويتطلّب هذا الهجوم جهدًا ووقتًا كبيريَن نسبيًّا لكي ينجح، وهو في بعض الأحيان صعب التطبيق بالنسبة إلى الأفراد العاديين، وتستخدم استخبارات بعض الدول هذا النوع من الهجوم للتجسّس على اتصالات الدبلوماسيين الأجانب المقيمين على أرضها.

2.2.6.6 الهجوم الفعّال Active Attack

يتميّز الهجوم الفعّال بالنشاط حيال الأذى الذي يسببه في أثناء تنفيذ بروتوكول ما أو حتى في وقت لا يتم من خلاله تنفيذ أي بروتوكول، ويحاول الخصم في الهجوم الفعّال التأثير في مجريات الاتصال القائم بين طرفين شرعييَن عبر خط قناة غير آمنة، وتتضمن الحركات التي قد يقوم بها الخصم في الهجوم الفعّال: -1 تعديل رسالة ما من خلال استبدال بياناتها أو حذف أجزاء منها أو إضافة بيانات إليها. -2 إنشاء رسائل ومعلومات جديدة ومزيّفة وإرسالها إلى طرفٍ ما على أنها قادمة من طرف شرعي. -3 خداع أحد طرفي الاتصال (أو كليهما) وإيهامه بأنه طرف شرعي. -4 إعاقة

تنفيذ الاتصال أو حتى تخريب القناة بأكملها. -5 قد يستطيع المهاجم أحيانًا الوصول إلى حاسب المستخدم وتخريب بياناته (يتم هذا عن طريق إصابة الحاسب بفيروس).

إذًا، تتطلّب الهجمات الفعّالة من الخصم التأثير في خطوة واحدة أو أكثر من خطوات البروتوكول، وفي أحيان أخرى التأثير في أحد طرفي الاتصال أو كليهما، والتلاعب بهما دون تنفيذ أي بروتوكول[1]، ولذلك تُعدّ الهجمات الفعّالة أكثر خطورة من الهجمات السلبية بسبب تأثيرها التخريبي، وليس بالضرورة أن يكون المهاجم طرفًا خارجيًّا غير شرعي، فقد يكون أحد الأطراف الشرعية المشاركة، وقد يكون مدير النظام، وفي هذه الحالة يُسمّى المهاجم **الغشّاش** Cheater، ومن المحتمل أيضًا أن يُوجَد أكثر من مهاجم ينفّذون مهمة واحدة، وخلافًا لنمط الهجوم السلبي يمكن اكتشاف وقوع الهجوم الفعّال بسهولة (وهذا بسبب نشاطه التفاعلي المحسوس)؛ ولذلك تسعى تقنيات التعمية إلى اكتشاف هذا الهجوم ومنع وقوعه، **وثمّة ثلاثة أنواع من الهجمات الفعّالة** هي: هجوم انتحال الشخصية، وهجوم الشخص الذي في الوسط، وهجوم إعادة التشغيل.

أ. هجوم انتحال الشخصية Attack Impersonation.

يُسمّى أيضًا **التنكّر** Masquarade، وينتحل الخصم في هذا الهجوم هوية أحد الأطراف الشرعية المشاركة في الاتصال، ثم يراسل الأطراف الأخرى على أنه ذلك الطرف الذي انتحل اسمه بوصفه مشاركًا حقيقيًّا في الاتصال، ويحدث هجوم انتحال الشخصية في عالم الواقع كثيرًا، والدليل على ذلك هو تلك المحاولات التي يخدع فيها الخصم الأطراف عبر الاتصال بهم هاتفيًّا والتحدّث معهم على أنه أحد الأقارب أو الأصدقاء بهدف سلب بعض المعلومات والإيقاع بهم، وينجح الهجوم في هذا الشكل من خلال استعمال تقنيات تقليد الأصوات بعد تسجيلها، وأمّا الحالات الأكثر واقعية فتكمن في غرف الدردشة على الإنترنت، وثمّة كثير من الناس الذين يقعون ضحايا عمليات

(1) ما يقصد هنا هو البروتوكول التعموي فقط.

احتيال وخدع ينفّذها خصوم بإحكام ضدهم، وتتمثّل هذه الخدع أحيانًا في تنكّر الفتاة بهوية شاب والتحدّث مع شاب آخر على هذا الأساس أو العكس، وأحيانًا تكون نتيجة هذا الاحتيال أكثر خطورة من مجرّد ضحايا حديث الحب والغرام وسلب المعلومات، فقد يكون هذا الهجوم انتحال شخصية بهدف تنفيذ عملية منظمة والإيقاع بأطراف بريئة، ومع الأسف تحدث هذه الحالات كثيرًا في عالم الواقع.

يمكن صَدّ هذا الهجوم في حالات معينة من خلال استخدام أحد تمثيلات[1] بروتوكول **التحدّي والرد** Challenge and Response Protocol، فمثلًا لو كان الطرفان المشاركان في الاتصال يعرفان بعضهما مسبقًا (أقارب أو أصدقاء مثلًا)، بإمكانهما الاستيقان من بعضهما عن طريق تنفيذ هذا البروتوكول، ويُسمّى الاستيقان في هذه الحالة استيقان الطرف أو إثبات الهوية (انظر 1-4)، ولنفترض في هذا التمثيل من بروتوكول التحدّي والرد أنَّ بوب يرغب في مراسلة أليس، فلكي يستيقن كلٌّ من أليس وبوب من هوية بعضهما يحتاجان إلى تنفيذ خطوات البروتوكول على النحو الآتي:

1. ترسل أليس رسالة إلى بوب تحتوي على كلمة ما طالبةً منه تعميتها بالمفتاح السرّي الذي تشاركه به.
2. يقوم بوب بتعمية الكلمة وإرسال الناتج برسالة إلى أليس مُرفقة بكلمة أخرى جديدة طالبًا منها تعميتها بالمفتاح السرّي نفسه.
3. تتحقق أليس من صحة الناتج، وتتأكد من أنه بوب نفسه، ثم تُعمّي الكلمة التي أرسلها بوب، وبعدها ترسل الناتج إليه.
4. يتحقق بوب من الناتج، ويتأكّد بذلك من أنها أليس نفسها.

---

(1) ثمّة أكثر من تمثيل لبروتوكول التحدّي والرد، انظر الفصل الثاني من:
Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, John Wiley & Sons, 2001.

ثمّة حالة يَفشل فيها هذا الشكل من البروتوكول تمامًا، فلو استطاع خصمٌ ما الحصول على المفتاح السرّي من بوب بطريقة أو بأخرى، وهو المفتاح المشترك مع أليس، لتَمَكّن من تنفيذ بروتوكول التحدّي والرد بنجاح والحديث مع أليس على أنه بوب، وبالإمكان تنفيذ بروتوكول التحدّي والرد على هذا النحو في غرف الدردشة وفي رسائل البريد الإلكتروني.

ب. هجوم الشخص الذي في الوسط Man-In-The-Middle Attack.

ويُعرَف اختصارًا بـ MITM. يقع هذا الهجوم عندما يتصل الطرفان الشرعيان عبر قناة غير آمنة في ظل استعمال تقنية التعمية بالمفتاح العام، ويتركّز الخصم في هذا الهجوم في وسط قناة الاتصال محاولًا قراءة الرسائل السريّة المتبادلة وتعديلها (إن رغبَ في ذلك) دون علم الطرفين الشرعيين المشاركين. معياريًّا، يُعدّ هجوم الشخص الذي في الوسط ناجحًا في بروتوكولات تبادل المفاتيح العامة التي لا تستعمل أي طريقة للاستيقان.

ولإيضاح فكرة هذا الهجوم جيدًا، سوف نستعرض بروتوكول تبادل المفاتيح العامة الأساسي مع محاولة الخصم خداع أليس وبوب. يرغب أليس وبوب في تبادل الرسائل السريّة من خلال استعمال كُلٍّ منهما المفتاح العام للآخر.

1. ترسل أليس إلى بوب مفتاحها العام. يعترض الخصم الرسالة، ويستبدل ذلك المفتاح بالمفتاح العام الخاص به، ثم يرسله إلى بوب، ويحتفظ بالمفتاح العام لأليس.
2. يرسل بوب إلى أليس مفتاحه العام. يعترض الخصم الرسالة، ويستبدل ذلك المفتاح بمفتاح عام آخر خاص به، ثم يرسله إلى أليس، ويحتفظ بمفتاح بوب العام.

3. عندما ترسل أليس رسالة إلى بوب، تُعمّيها بمفتاحه العام. ولأن المفتاح العام الذي استعملته أليس عائدٌ للخصم، يعترض هذا الأخير الرسالة، ويفك تعميتها باستخدام مفتاحه الخاص، ثم يقرؤها، ويعدّل عليها إن تطلّب الأمر، وبعد ذلك يُعمّيها باستعمال المفتاح العام لبوب، ويرسلها إليه.
4. يستقبل بوب الرسالة في ظرف مدة زمنية عادية ومقبولة (أي لا يوجد فيها أي تأخير).
5. يكرّر الخصم الخطوة (3) مع بوب.

لن يلحظ أيٌّ من بوب وأليس أن ثمّة طرفًا ثالثًا غير شرعي يتجسس على رسائلهما، ويقرؤها دون رقيب. يعلم كلٌّ من بوب وأليس أنهما يتحدّثان عبر قناة غير آمنة، ويستخدمان التعمية من أجل تأمين اتصالاتهما، ولكنهما لا يدركان وجود شخص ثالث يطّلع على أسرارهما.

ومن أجل جعل الاتصال آمنًا، يجب أن يضمن كلا الطرفين سلامة المفاتيح العامة التي يتبادلانها، ولكن لا يعني ذلك أن عليهما تبادلها بطريقة سريّة أو عبر قناة آمنة، فالبروتوكول الذي يقترح هذا الحل يُعدّ فاشلًا بكل المقاييس، والمفاتيح العامة، كما هو واضحٌ من اسمها، ينبغي أن تكون على مرأى من الجميع ودون تحفّظ.

يمكن إحباط هجوم الشخص الذي في الوسط من خلال تنفيذ بروتوكول **الضم** Interlock Protocol. اقترح Rivest وShamir بروتوكول الضم من أجل اكتشاف وجود الخصم الواقع في وسط قناة الاتصال، ولا يمنع هذا البروتوكول الخصم من محاولته تلك، ولكنّه يُنذر الطرفين من أول مرة بوجوده. (انظر أيضًا المرجع).

ثمّة فرق بين هجوم الشخص الذي في الوسط وانتحال الشخصية المذكور سابقًا، ويمكن التمييز بين هاتين الهجمتين من خلال النظر إلى عدد المشاركين في الاتصال، وإنَّ عدد المشاركين في هجوم الشخص الذي في الوسط هو ثلاثة (أليس - بوب -

الخصم)، وأمّا في هجوم انتحال الشخصية فعدد المشاركين هو اثنان فقط (المرسل / المستقبل / الخصم)؛ لأنَّ الخصم ينتحل هوية إمّا المرسل أو المستقبل.

ج. هجوم إعادة التشغيل Replay Attack.

يسجّل الخصم في هذا الهجوم رسائل قديمة من بروتوكول ما عن طريق حفظ خطوات عدة منه، ثم إعادة استعمالها لاحقًا من أجل إعادة تنفيذ تلك الخطوات مع أحد الطرفين الشرعيَين اللذين قاما بتنفيذ البروتوكول نفسه سابقًا، ويسجّل الخصم في هذا الهجوم الخطوات، ويحتفظ بالمعلومات والمراسلات المطلوبة في أثناء تنفيذ البروتوكول بين الطرفين الشرعيَين دون علمهما، ويتضح من ذلك أن للمهاجم مهمتين: الأولى تتم ضمن إطار هجوم كامن، وهي المهمة التي يسجّل فيها المعلومات والمراسلات، والثانية تتم ضمن إطار هجوم فعّال يخدع فيها أحد الطرفين.

يمكننا أن نعدّ هجوم إعادة التشغيل جزءًا من هجوم انتحال الشخصية؛ وذلك لأن عدد المشاركين في كلتا الهجمتين نفسه، ولكن في هجوم إعادة التشغيل سيبدأ الخصم بالتنفيذ، ومن ثم سيكون هو المرسل، وعلى نحوٍ أدق، يمكننا اعتبار هجوم إعادة التشغيل حالة أو مثالًا عن هجوم انتحال الشخصية، ونستطيع صد هجوم إعادة التشغيل من خلال استعمال **الأختام الزمنية** Timestamps.

د. هجوم الحرمان من الخدمة Denial-of-Service Attack.

ثمة هجوم يرتبط ببروتوكول اتصال، ولكن ليس له علاقة بالتعمية، وهو هجوم الحرمان من الخدمة، ويُشَنّ من وسط قناة الاتصال على شبكة حاسوبية، فيؤدي إلى تحميلها بما يفوق طاقتها، ومن ثم إلى نقص الموارد المتاحة، ومن ثم منع المستخدم الشرعي من الاستفادة من تلك الموارد، ومن الأمثلة الواقعية على هذا الهجوم: منع الخصم وصول الرسائل إلى الطرف المعني بها، أو قيامه بتعطيل الشبكة بأكملها من خلال تحميلها رسائل تفوق طاقتها من أجل الحط من مستوى أدائها.

ثمة أشكال أخرى من الهجمات على بروتوكولات التعمية، ومن الممكن أن تظهر هجمات جديدة، ولكن كيف نعرف أن الهجوم هو هجوم على بروتوكول تعموي! عندما يقوم الهجوم على قناة الاتصال، ويُوجَّه على أحد تقنيات التعمية أو خدماتها فهو افتراضيًّا هجوم على بروتوكول تعموي، والتنفيذ لا يتم إلا في وسط قناة الاتصال سواء أكان سلبيًّا أم فعالًا.

3.6.6 الهجوم على خوارزميات التعمية

يُطبَّق هذا الهجوم على خوارزميات التعمية وخططها. إنَّ هذا النوع ليس بإستراتيجية لإحباط بروتوكول أو إفساد خدمة ما، وإنما طريقة عملية من أجل الوصول إلى الهدف النهائي، وهو الحصول على النص الواضح، ويتمثّل الهدف النهائي في الهجوم على خوارزميات التعمية في استعادة النص الواضح لنص معمّى مطلوب، وأما الهدف الوسيط فيتمثّل في الحصول على المفتاح المستعمل (أو استنتاجه) من أجل استعادة أي نص واضح مستقبلي، وقد يتمثّل الهدف الوسيط أيضًا في استنتاج (أو ابتكار) خوارزمية بديلة تسمح بالوصول إلى الهدف النهائي، وكما هو جلي، فإن الهدف الوسيط يُعدّ أهم من الهدف النهائي؛ كونه سيصبح وسيلة دائمة ومتوافرة للوصول إلى الهدف النهائي بسهولة، ويَفترض الهجوم على خوارزميات التعمية أنَّ المهاجم على معرفة تامة بالخوارزمية المستعملة.

ثمة **ستة أنماط رئيسة** من الهجمات الموجَّهة على خوارزميات التعمية هي: هجوم النص المعمَّى فقط، وهجوم النص الواضح المعلوم، وهجوم النص الواضح المختار، وهجوم النص الواضح المختار المتكيِّف، وهجوم النص المعمّى المختار، وهجوم النص المعمّى المختار المتكيِّف، وسوف نتحدث هنا عن النمط الأول فقط بوصفه مثالًا على هذا النوع من الهجوم على خوارزمية التعمية، وفي حال الرغبة في الاطلاع على الأنماط

الخمسة الأخرى، فيمكن العودة إلى المرجع: (المدخل إلى علم التعمية، تأليف: ساري خالد 2015م)[1]، ولكن تذكّر أن المهاجم في كل نوع لديه اطلاع تام على خطة التعمية[2].

هجوم النص المعمّى فقط Ciphertext–only Attack.

يمتلك المهاجم في هذا النمط النص المعمّى فقط c (أو مجموعة من النصوص المعمّاة c_1، c_2،....، c_i) المقابل لنص واضح m تم تعميته بمفتاح e:

$$c = E_e(m)$$

حيث $m \in M$ ، $c \in C$، $e,d \in K$.

يقتصر عمل المهاجم (محلل التعمية) على دراسة خصائص النص المعمّى c إمّا من أجل استعادة النص الواضح المقابل m بوصفه هدفًا نهائيًّا، أو لاستنتاج المفتاح d لفك تعمية نصوص مستقبلية معمّاة بالمفتاح e.

يمكن نمذجة هجوم النص المعمّى فقط على النحو الآتي (انظر المرجع):

إذا توافر للمهاجم $c_1 = E_e(m_1)$، $c_2 = E_e(m_2)$، ....، $c_i = E_e(m_i)$ حيث $m \in M$ ، $c \in C$، $e,d \in K$، فعليه أن يقوم باستنتاج إمّا كهدف نهائي m_i، m_1، m_2،....، m_i أو كهدف وسيط d أو خوارزمية بديلة من أجل استعادة m_{i+1} من $c_{i+1} = E_e(m_{i+1})$.

يُعدّ هجوم النص المعمّى فقط (بالنسبة إلى محلل التعمية) أضعف هجوم؛ لأنه يتضمن امتلاك المهاجم للنص المعمّى فقط، وفي المقابل، تُعدّ خوارزميات وخطط التعمية التي ينجح كسر تعمية النصوص المعمّاة بها عن طريق هذا الهجوم ضعيفة جدًّا.

---

(1) كتاب (المدخل إلى علم التعمية)، تأليف: ساري خالد، 2015م.

(2) ثمة حالات ليست فيها خوارزمية التعمية معلومة للمهاجم، تتجسّد مثل هذه الحالات كثيرًا في المعمّيات الكلاسيكية.

وينجح هذا الهجوم عند حصول المهاجم على النص الواضح m للنص المعمّى c؛ أي عند توصّله للهدف النهائي، ويُعدّ ناجحًا بنسبة أكبر إذا استطاع المهاجم استنتاج المفتاح d أو اكتشاف خوارزمية بديلة.

إنَّ لموضوع هجوم النص المعمّى فقط تشعّبات عدة، فمثلًا لو كان النص المعمّى الذي يمتلكه المهاجم ذا قيمة لاكتفى فقط باستعادة النص الواضح المقابل بوصفه هدفًا نهائيًّا دون الحاجة إلى اكتشاف المفتاح d، أمّا لو كان النص المعمّى مجرد وسيلة (أي ليس ذا قيمة) لكانَ على المهاجم دراسة خصائصه من أجل استعادة النص الواضح المقابل، ولكن ليس كهدف نهائي إنما من أجل إيجاد طريقة لاستنتاج المفتاح والاستفادة منه لفك تعمية رسائل مستقبلية معمّاة به، أو ابتكار خوارزمية ما لاستعادة أي نص واضح من نص معمّى دون الحاجة حتى إلى معرفة المفتاح، وبمجمل الأحوال، يعتمد الهدف النهائي لهجوم النص المعمّى فقط على رغبة محلل التعمية.

الفصل السابع

إجراءات معيارية في أمن المعلومات

1.7 بعض إجراءات أمن المعلومات على الشبكات

تزداد أهمية إجراءات الأمن السايبري للمعلومات على الشبكات الحاسوبية بشكل سريع، فقد قُدِّر حجم هذا السوق بأكثر من 75 بليون دولار عام 2015م، وحجمه عام 2020 بـ 170 بليون دولار[1] وتوجد من أجل كل نوع من أنواع المهددات إجراءات معاكسة لحماية المبادلات الإلكترونية.

1. فللحماية من الدخول أو النفاذ غير المشروع إلى المعلومات المخزونة والاطلاع عليها، تستعمل وسائط مختلفة تمنع هذا الدخول غير المشروع، مثل: كلمات السر Passwords، والبطاقات المغناطيسية الشخصية Magnetic Cards، والبطاقات الذكية Smart Cards، والخصائص البيولوجية للأفراد (بصمات الأصابع، شبكية العين، تعرف الصوت،...).

(1) http://cybersecurityventures.com/cybersecurity_market_report/.

2. أما الدخول إلى الشبكات فيمكن التحكم فيه عن طريق استعمال تجهيزات أو برمجيات منع الدخول غير المشروع إلى الشبكات، ومنها: جدران النار Firewalls، والمرشحات Routing Filters، والمُخدِّم الوكيل أو البروكسي Proxy ، والفصل الفيزيائي للشبكة المحمية عن شبكة الإنترنت.
3. وللحماية من التنصت ومن تحليل الاتصالات، وبهدف تحقيق السرية والخصوصية Confidentiality or Privacy يُستخدم التشفير (التعمية)، حيث تخزن هذه المعلومات في الذواكر وفي الأقراص والأشرطة المغناطيسية بشكل معمى لا يمكن الاطلاع عليه إلا لمن يملك مفتاح التعمية، وعند التراسل بين جهتين باستعمال الشبكات الحاسوبية، تُعمى المعلومات المرسلة أيضًا، وتستعمل أيضًا تقانات الحشو بالأغفالTraffic Padding والتحكم بالتوجيه Routing Control من أجل الحماية من تحليل الاتصالات.
4. أما حماية المعلومات من التغيير أو التعديل بهدف ضمان صحتها Integrity فيتم باستعمال التعمية أيضًا وباستعمال التوقيع الإلكتروني Digital Signature، وسنأتي فيما بعد على شرح لتكنولوجيا التشفير والتوقيع الإلكتروني المستعملة في المبادلات الاقتصادية.
5. والقضية الرابعة المهمة في المبادلات الإلكترونية على الشبكات الحاسوبية هي التحقق من هوية المتراسلين Authentication، منعًا من حدوث تقمص للشخصيات الحقيقية أو الاعتبارية. والتكنولوجيا المستعملة في ذلك هي التوقيع الإلكتروني، ويمكن استعمال بعض التكنولوجيات الخاصة بالتحكم في الدخول إلى النظم، مثل كلمة السر، والبطاقات المغناطيسية أو الذكية، أو عبر تعرف الخصائص البيولوجية التي أتينا على ذكرها فيما سبق.
6. وللحماية من إنكار حدوث الاتصال Non-Repudiation أي أن ينكر المرسل أنه قام بالمبادلة الإلكترونية أو أن ينكر المستقبل أنه تسلّم هذه المبادلة، فتستعمل أيضًا تكنولوجيا التوقيع الإلكتروني، ويستفاد في هذا المجال

مـن طـرف ثالث على الشـبكة يقـوم مقام كاتـب العدل فـي المبـادلات الورقية Notarization، وتوجد الآن كثير من الشركات على الإنترنت تقوم بهذه الوساطة بين الجهات التي تجري مبادلات اقتصادية فيما بينها، وذلك بتوثيق الطرفين وتوثيق مبادلاتهما.

7. أخيـرًا، لا بـد مـن مراقبـة مـا يجـري وتسـجيله ضمـن النظـم المعلوماتية من إجـراءات واتصـالات بهـدف العودة لهذا السـجل عنـد حدوث أي طـارئ أو أي خرق أمني للنظام Auditing، ويتم ذلك عادة عبر برمجيات خاصة تقوم بشكل آلـي بعمليـات، مثل سـجلات المراقبـة Audit Trails، ومتابعة الحـوادث الأمنية Security Events Tracking.

ويلخص الجدول الآتي آليات تأمين الخدمات الأمنية المطلوبة للتبادلات الإلكترونية للمعلومات:

جدول آليات توفير الخدمات الأمنية المطلوبة لحماية الاتصالات الحاسوبية

	Mechanisms الآليات							
	Encryption تعمية	Digital Signature التوقيع الإلكتروني	Access Control التحكم بالنفاذ	Data Integrity صحة البيانات وتكاملها	Authenti_cation التحقق من الهوية	Traffic Padding رصد انسياب المعلومات	Routing Control التحكم في مسار المعلومات	Notarization التسجيل الرسمي
Confidentiality السرية	√	*	*	*	*	√	√	*
Integrity الصحة والتكامل		√	*	√	*	*	*	*
Authentication صحة الهوية	√	√	*	*	√	*	*	*
Access Control التحكم في النفاذ	*	*	√	*	*	*	*	*
Non_repudiation عدم نكران التعامل	*	√		√	*	*	*	√

2.7 أنظمة الحماية المعيارية

إن الهدف المبتغى من مختلف الأجهزة والبرامج المعلوماتية، كالمخدم الوكيل proxy servers وجدران النار Firewalls، على سبيل الذكر لا الحصر، هو إيقاف الفيروسات المعلوماتية، وتثبيط عزيمة المخربين والقراصنة، وتقليص النفاذ للمواقع غير المرغوب فيها، ولهذا الغرض هناك إجراءات أساسية عدة متمثلة في إدراج كلمة السر المعماة (Encrypted Password) على مستويات مختلفة، واستعمال الشهادات المصادق عليها (Certificates) والإمضاء أو التوقيع الرقمي أو الإلكتروني (Digital signature) أو تثبيت مضاد فيروس (Antivirus).

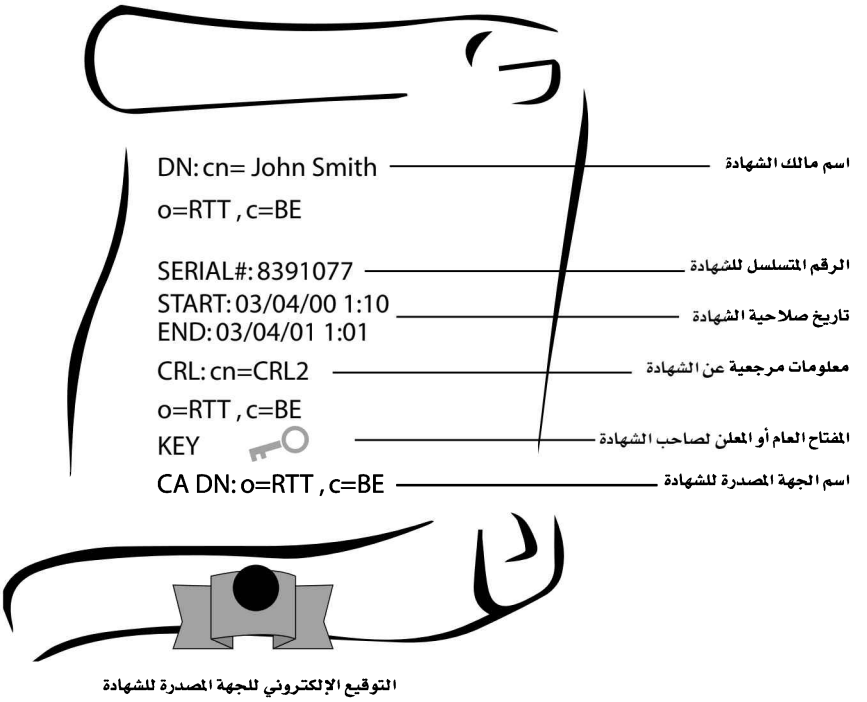
3.7 إجراءات التعمية أهم آليات الحماية.

تستخدم التعمية في إجراءات عدة في أمن المعلومات، بل في معظم هذه الإجراءات، ومن هذه الإجراءات ما ذكرنا سابقًا من آليات السرية، والحفاظ على صحة المعلومات وتكاملها، وإثبات هوية المتراسلين، وستبيّن الفقرات الآتية أهمية التعمية في إجراءات أمن المعلومات وأمانها بشكل مبسط:

4.7 إجراء استعمال الشهادات المعتمدة.

إن التحقق من الهوية داخل شبكة الإنترنت أمر في غاية التعقيد؛ ذلك أن الأطراف المتصلة لا يمكنها أن تلتقي ماديًّا كما هو الحال في أثناء المقابلة المادية، وهذا ما يمكّن الكثير من الأشخاص من استراق الرسالة أو القيام بتشخيص نفسه على شخص أو كيان آخر؛ أي انتحال شخصية غير شخصيته.

الشهادة الرقمية CA



إن شهادة الاعتماد، سواء للأشخاص أو لمواقع الإنترنت، يجب أن تشترك في الهوية بواسطة (**المفتاح العام**) ولا يَعرِفُ (**المفتاحَ الخاص**) الموافق إلا من يملك شهادة الاعتماد، ويسمح (**المفتاح الخاص**) للمالك باستعمال (**الإمضاء الرقمي**) أو فك شفرة المعلومات المشفرة باستعمال (**المفتاح العام**) الموافق، فعندما ترسل شهادة الاعتماد الشخصية لأشخاص آخرين، فإنك تمنح لهم المفتاح العام الشخصي، ومن ثم يمكن لهم أن يرسلوا لك المعلومة المعماة التي لا يمكن لأحد سواك أن يفك تعميتها أو قراءتها، وذلك باستعمال مفتاحك الخاص.

5.7 إجراء التحقق من هوية المخدم

تمنع عملية التحقق من هوية المخدم انتحال الشخصية، حيث يطلب الزبون الشهادة الرقمية للمخدم، فعند إرسال المخدم لشهادته الرقمية يسأل الزبون نفسه الأسئلة الآتية التي يجب أن يكون جواب كل منها (نعم) حتى يتم نجاح التحقق من هوية المخدم، السؤال الرابع من الأسئلة الآتية ليس جزءًا من تقنية الـ SSL وإنما أضيف لمنع نوع من الاختراق للأمن يدعى (رجل في الوسطMan in The Middle) وهذه الأسئلة هي:

عملية إقامة اتصال آمن باستعمال المنتج SSL/TLS

- **هل تاريخ اليوم ضمن مدة صلاحية الشهادة؟**

في حال كان الجواب لا، تُنهى عملية التحقق عند هذا الحد وإعادة رسالة خطأ.

- **هل مصدر الشهادة الرقمية هو CA موثوق أي مصدر شهادات موثوق بالنسبة إلى الزبون؟**

يملك كل زبون SSL قائمة لمصدري الشهادات الموثوقين بالنسبة إليه، تحتوي هذه القائمة على حقل (Distinguished Name (DN يحوي الاسم المميز لمصدر الشهادة، يفحص هذا الشرط بالبحث عن مصدر شهادات موثوق في القائمة المخزنة لدى الزبون يتطابق حقل DN لديه مع حقل DN الموجود في الشهادة، في حال تجاوز هذا الشرط ينتقل إلى السؤال الثالث.

- **هل المفتاح العام العائد لمصدر الشهادة يفك تشفير التوقيع الرقمي، وهل المعلومات المرسلة في الشهادة تتناقض مع التوقيع؟**

للتحقق من التوقيع الرقمي يقوم الزبون بالخطوات الآتية:

1. يفك الزبون شيفرة التوقيع الرقمي للجهة المصدرة CA بواسطة المفتاح العام الذي من المفترض وجوده في قائمة مصدري الشهادات الموثوقين.
2. يطبق الزبون تابع الاتجاه الواحد المستخدم من قِبل الـ CA المصدرة للشهادة على البيانات المرسلة من المخدم، ويتم بعد ذلك المطابقة بين التوقيع الرقمي المرسل مع الشهادة وقيمة التابع الناتجة :

- نستنتج في حال التطابق أن المعلومات المرسلة في الشهادة صحيحة، ويُنتقَل إلى السؤال الرابع.
- ينتج عدم التطابق إما بسبب تغيير في الشهادة، أو أن المفتاح العام المستخدم في فك التشفير لا يتوافق مع المفتاح الخاص المستخدم في تشفير المعلومات، وفي هذه الحالة تُرفَض الشهادة.

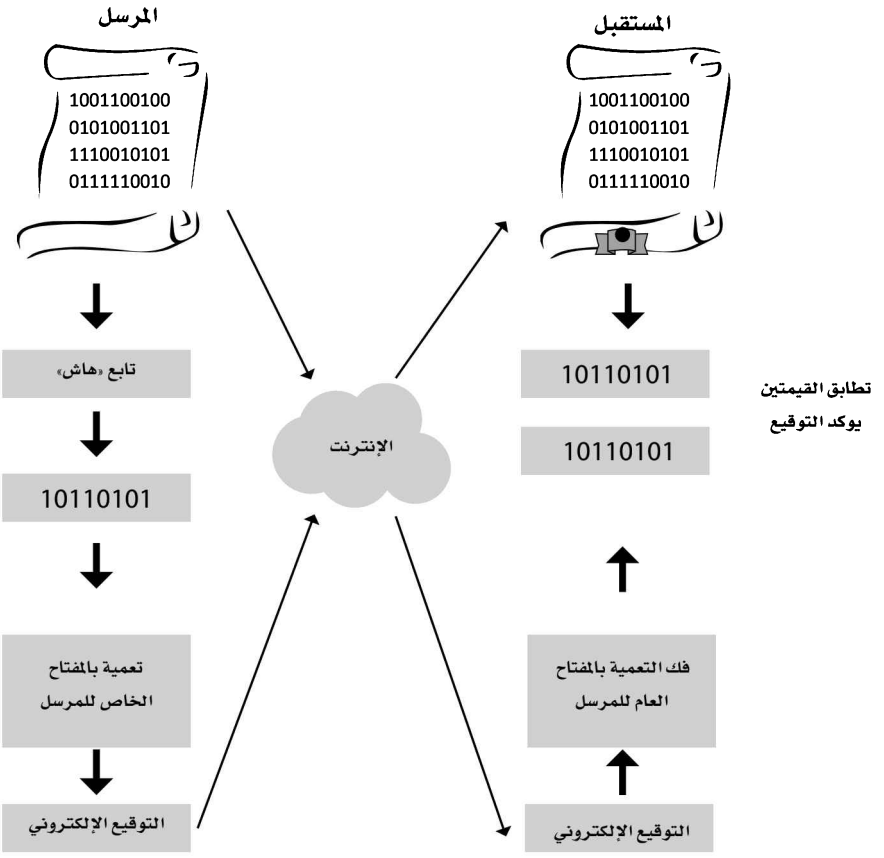
- **هل اسم النطاق في الشهادة الرقمية يطابق اسم نطاق المخدم؟**

ذكرنا سابقًا أن هذا السؤال ليس من تقنية SSL وإنما أضيف لمنع نوع من الاختراق يدعى (رجل في الوسط Man in The Middle)، حيث يتحقق الزبون من أن اسم النطاق المسجل في الشهادة الرقمية يطابق اسم النطاق الذي يتصل معه حاليًّا، وهو الحل الوحيد المطروح لمنع هذا النوع من الاختراق.

6.7 إجراء الإمضاء الرقمي أو التوقيع الإلكتروني

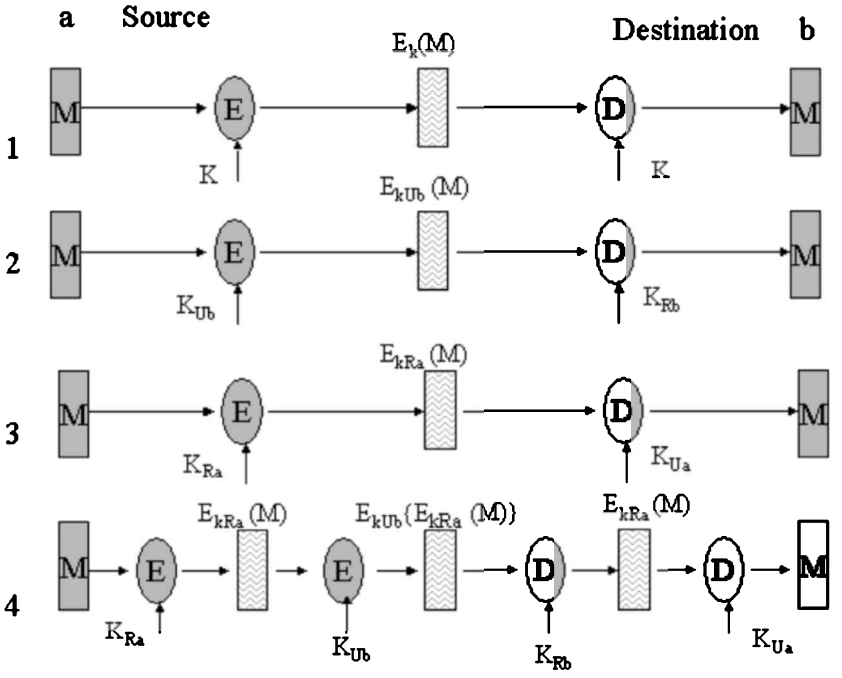
تحتوي الرسائل المرسلة عبر شبكات الاتصال أحيانًا على أوامر خاصة ومهمة، مثل طلب صرف مستحقات مالية من المصارف، وفي هذه الحالة يجب إثبات صحة الرسالة المستقبلة والوثوق بها، وطريقة التوثيق في حالة تسلم الرسائل باليد هي إمضاء المُرْسِل على الوثيقة، أما في حالة الانتقال عبر شبكات الاتصالات، فإن التوثيق في هذه الحالة يتم بالإمضاء الرقمي digital signature، وهو عبارة عن رسالة معماة بالمفتاح المعلن تستعمل من أجل التوقيع الإلكتروني طريقة التشفير بالمفتاح المعلن، ويقوم المرسل ولنسمِّه (سامر) باختصار الرسالة مستعملًا تابع اختصار أو (بصمة) وهو تابع رياضياتي محدد Hash Function، ثم يشفر المختصر الناتج مستعملًا مفتاحه الخاص السري، وبعدها يرسل الرسالة الأصلية مع تشفير مختصرها إلى المستقبل ولنسمِّه (سليم)، ويقوم المستقبل (سليم) بإجراء عملية اختصار الرسالة نفسها مستعملًا تابع الاختصار نفسه، ويقارن النتيجة مع ناتج فك تشفير المختصر المرسل له الذي حصل عليه باستعمال المفتاح المعلن للمرسل (سامر)، فإذا كانت نتيجة المقارنة التطابق يكون هذا إثباتًا على أن الرسالة مرسلة من (سامر)، وأنه لم يُجرِ عليها أي تعديل.

إرسال وثيقة موقعة توقيعًا اللكترونيًا



هناك أربعة ترتيبات أساسية تستخدم فيها طريقتا التشفير المتناظرة وغير المتناظرة لتأدية الوظائف الأمنية المطلوبة للتبادلات الإلكترونية، ولتحقيق الاتصال بين المرسل a والمستقبل b وهي المذكورة أدناه، والمبينة في الشكل الآتي:

1. الطريقة التقليدية التي تشفر فيها على سبيل المثال النصوص المخزونة أو الرسائل المتبادلة على الشبكات.
2. طريقة التشفير بالمفتاح المعلن التي تستعمل لتبادل معلومات قصيرة مشفرة، كالمفاتيح السرية.



3. طريقة التشفير بالمفتاح المعلن في حالة التوقيع الإلكتروني لتحديد هوية المرسل.
4. طريقة التشفير بالمفتاح المعلن في حالة سرية المعلومات (أي تشفيرها) + توقيع إلكتروني + هوية المرسل.

ومما لا شك فيه، يمكن دمج الطريقة 1 مع أيٍّ من الطرق الثلاث الأخر 2 و3 و4.

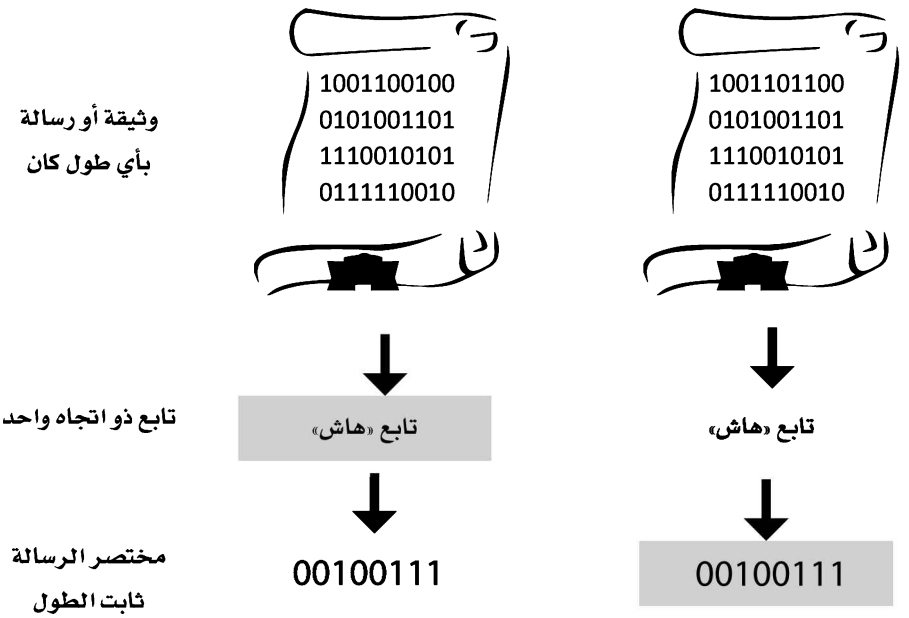
والأشكال السابقة تشرح الطريقة المستعملة لإجراء التوقيع الإلكتروني، حيث ينطلق المرسل (سامر) من نص الرسالة الواضح، ويستخرج ملخصًا لهdigest ، ثم يُشفِّر هذا الملخص باستعمال مفتاحه السري، وبعد ذلك يرسل الرسالة الواضحة وناتج تشفير ملخصها إلى (سليم)، ويفكّ (سليم) تشفير ملخص الرسالة باستعمال مفتاح

(سامر) المعلن، ويقوم بحساب ملخص الرسالة، ويقارن نتيجة الحسابين، فإذا تطابقتا يكون (سامر) هو مرسل الرسالة، وتكون الرسالة غير معدلة.

7.7 توابع البصمة (هاش)

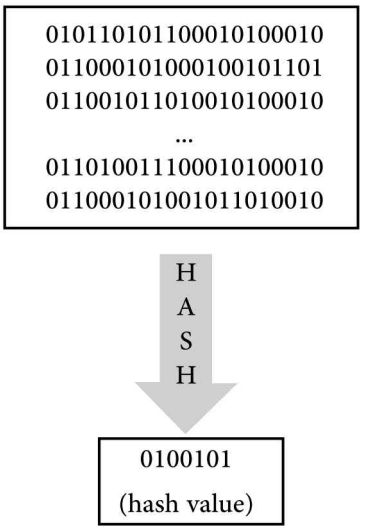
مثلما تُؤمِّن التعمية المتماثلة أو المتناظرة والتعمية غير المتماثلة (أي التعمية بالمفتاح السرِّي والتعمية بالمفتاح العلني) خدمة السرِّية Confidentiality، تؤمِّن توابع البصمة بنوعيها خدمتَي سلامة البيانات Data Integrity واستيقان الرسالة Message Authentication (أو استيقان منشأ البيانات Data Origin Authentication).

تابع «هاش» المستعمل لفحص عدم حصول تغير في الرسالة



إن تغيرت خانة «بت» واحد في الوثيقة يغير مختزلها أو بصمتها كليًا

يأخُذ **تابع البصمة** Hash Function (ويُدعَى أيضًا **تابع الضغط** Compression Function و**تابع التقليص** Contraction Function)[1] كدخل إمّا وسيطًا واحدًا (رسالة طولها يساوي m بت) أو وسيطين (رسالة طولها يساوي m بت ومفتاح سري طوله يساوي k بت)، ويعطي كخرج قيمة طولها يساوي n بت، حيث n < m، تُدعَى **ترميز البصمة** Hash Code أو **نتيجة البصمة** Hash Result أو **قيمة البصمة** Hash Value أو **الدمغة** Imprint أو **البصمة الرقمية** Digital Fingerprint أو **خلاصة الرسالة** Message Digest أو ببساطة **بصمة** Hash.



أبسَط مثال على تابع البصمة هو تابع يقوم بالجمع الاثناني لبايتات سلسلة دخل (ولتكن رسالة) وتحويلها إلى بايت واحد طوله يساوي 8 بتات (وهو قيمة البصمة)، ويمكننا تمثيل هذا المثال وفق الإجراء الرياضي الآتي:

$$Message = X_1 || X_2 || X_3 || \ldots || X_{t-1} || X_t$$

(1) في الحقيقة، إنَّ تابع الضغط (أو كما يُسمَّى تابع التقليص) هو الجزء الأساسي والمكوِّن لتابع البصمة، وليس هو تابع البصمة نفسه، ولكن سُمِّي تابع البصمة بهذين الاسمين انطلاقًا من المبدأ العام لعمل تابع البصمة الذي يقوم بعملية الضغط، وهي تحويل سلسلة كبيرة ومتغيِّرة إلى سلسلة صغيرة وثابتة.

HashValue = 0

For i = 1 to t

HashValue = HashValue $\oplus X_i$

Next i

حيث Message: رسالة طولها يساوي t بايت، وX_1، X_2، X_3، ...، X_t: البايتات التي تُشكِّل الرسالة، وHashValue: كلمة غير مؤشَّرة طولها يساوي 8 بتات، وهي قيمة البصمة المطلوبة، و⊕: عملية الجمع الاثناني.

نمطَا توابع البصمة.

في البداية تنقسم توابع البصمة إلى نوعين رئيسين، هما: **توابع البصمة غير المزوَّدة بمفتاح** Unkeyed Hash Functions و**توابع البصمة المزوَّدة بمفتاح** Keyed Hash Functions. تأخذ توابع البصمة غير المزوَّدة بمفتاح دخلًا واحدًا فقط هو الرسالة، بينما تأخذ توابع البصمة المزوَّدة بمفتاح دخلين، هما: الرسالة والمفتاح السرِّي.

يَتميَّز تابع البصمة H (بنوعيه غير المزوَّد بمفتاح والمزوَّد بمفتاح) بخاصتين أساسيتين:

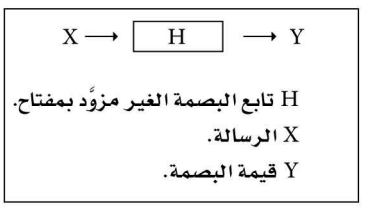
1. **الضغط** Compression: يقوم تابع البصمة H بضغط سلسلة بتية x ذات طول متغيِّر ومنتهٍ طولها يساوي m بت إلى سلسلة بتية y صغيرة وثابتة طولها يساوي n بت، حيث $n < m$.
2. **سهولة البصم** Ease of Computation: في حال H غير مزوَّد بمفتاح، وبتوافر تابع البصمة H وسلسلة بتية x، من السهولة حساب البصمة $H(x)$. وفي حال H مزوَّد بمفتاح، وبتوافر تابع البصمة H وسلسلة بتية x ومفتاح سري k، من السهولة حساب البصمة $Hk(x)$.

ثمة نمطان رئيسان من توابع البصمة: النمط الأول هو **ترميز اكتشاف التعديل** Modification Detection Code ، واختصارًا MDC (ويُعرَف هذا النمط أيضًا **بترميز اكتشاف التلاعب** Manipulation Detection Code ، **وترميز سلامة الرسالة** Message Integrity Code ، واختصارًا MIC). والنمط الثاني هو **ترميز استيقان الرسالة** Message Authentication Code، واختصارًا MAC (ويُعرَف هذا النمط أيضًا **بترميز استيقان البيانات** Data Authentication Code، واختصارًا (DAC)، وسوف نتحدَّث عن كل نمط من هذين النمطين بالتفصيل[1].

ترميز اكتشاف التعديل MDC.

الـ MDCs هي توابع بصمة غير مزوَّدة بمفتاح، ويستطيع نمط الـ MDC تأمين خدمة سلامة البيانات data integrity فقط، ويأخذ هذا النمط دخلًا واحدًا فقط هو الرسالة، وتُسمَّى **الصورة الأمامية** Preimage، ويُعيد كخرج قيمة هي قيمة البصمة. انظر الشكل (5-1)، وانطلاقًا من ذلك، يمكننا تمثيل تابع البصمة غير المزوَّد بمفتاح H على النحو الآتي:

$$H: M \rightarrow R$$



حيث M: فضاء الرسالة، وهو المجموعة التي تضم قيَم الدخل (قيمة الدخل هي أي رسالة طولها يساوي m بت)، وR: فضاء البصمة، وهو المجموعة التي تضم قيَم الخرج

(1) يمكن أن يأتي المصطلح MDC (ومرادفاته) بمعنى (تابع حساب ترميز اكتشاف التعديل) و(ترميز اكتشاف التعديل) في الوقت نفسه. كذلك، يمكن أن يأتي المصطلح MAC (ومرادفاته أيضًا) بمعنى (تابع حساب ترميز استيقان الرسالة) و(ترميز استيقان الرسالة)، ويتم تمييز ذلك بحسب سياق النص.

(قيمة الخرج هي أي قيمة بصمة طولها يساوي n بت)، و n < m. يُلاحَظ هنا أنَّ طول قيمة الدخل الذي يساوي m بت كبير ومتغيِّر، ولكنه منتهٍ، أمّا طول قيمة الخرج الذي يساوي n بت فهو صغير وثابت لجميع قيَم الدخل.

الشكل: تابع البصمة غير المزوَّد بمفتاح (MDC).

يُقسّم نمط الـ MDC إلى نوعين:

8.7 بعض المنتجات التقليدية المتوافرة للتبادل الآمن للمعلومات على الشبكات

توجد حاليًّا منتجات ومعايير عدة لتوفير الوظائف اللازمة لضمان أمن الاتصالات على الإنترنت، ومنها أمن المبادلات الإلكترونية والتجارة الإلكترونية.

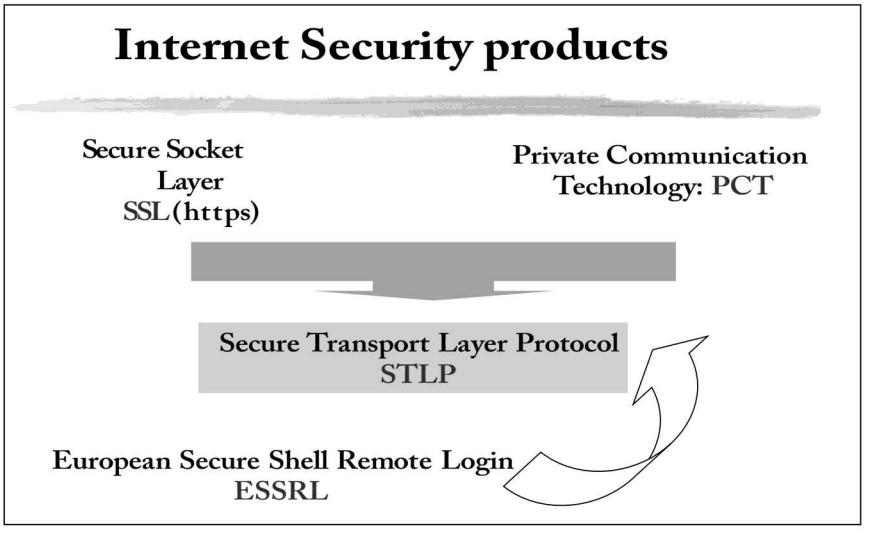
تُصمّم هذه المنتجات من جمع خوارزميات عدة في منتج واحد، فمثلًا المنتج:

Pretty Good Privacy (PGP)

يتألف من جمعٍ لخوارزمية التشفير المتناظرة IDEA مع خوارزمية المفتاح المعلن RSA إضافة لخوارزمية تابع الاختصار (أو البصمة أو هاش) The MD5 Hash function ، ويبين الشكل المرفق بعض هذه المنتجات والخوارزميات الداخلة في تصميمها.

وتتوافر على الإنترنت بعض المعايير الأمنية المتداولة، مثلSecure Socket Layer (https SSL) ومثل Private Communication Technology PCT ، علمًا أنه يجري أخيرًا دمج هذين المعيارين مع المعيار الأوروبيEuropean Secure Shell Remote Login ESSRL في معيار واحد هو Secure Transport Layer Protocol STLP كما هو مبين في الشكل الآتي:

مثال يبيّن بعض منتجات أمن التواصل عبر الإنترنت


Internet Security products
Secure Socket Layer SSL(https)
Private Communication Technology: PCT
Secure Transport Layer Protocol STLP
European Secure Shell Remote Login ESSRL

الفصل الثامن

قضايا

ثَمَّة عدد من القضايا الحسَّاسة في أمن المعلومات، وسيَستعرِض هذا الفصل بعض هذه القضايا، ويَدرُس أبعادها، ويُقدِّم إجراءات تُسهِم في علاجها، فبعض هذه القضايا تتعلق **ببعدٍ آخر للأمان المتعلق بالمعلومات والاتصالات** غير **أمان المعلومات** الذي تعرضنا له في صلب الكتاب، ألا وهو أمان الأشخاص أنفسهم نتيجة تداولهم للمعلومات على شبكاتها، مثل أمان القُصّر، وأمان الأشخاص نتيجة وجود معلومات على شبكات الاتصال حول تحركاتهم.

1.8 أمان معلومات القُصَّر

مع تَطوُّر وسائل الاتِّصال الحديثة عَبْر الإنترنت، ومع ازدياد تَعلُّق القُصَّر بها، واستخدامِهم لها بوصفها وسائل ترفيه أكثر مِمَّا هي وسائل اتِّصال، ازدادَت عمليات اصطياد هؤلاء القُصَّر بكثافة، والقاصِر بحَسْب تعريفه في الشبكة الدوليَّة لحقوق الطفل CRIN هو من لم يَتجاوَز سن 18[1]، سواء أكان ذكرًا أم أنثى. إنَّ أخطار استعمال القُصَّر

(1) تَدعو CRIN أيضًا القاصر من لم يَتجاوَز سن 18 سنة.

لوسائل الاتِّصال عَبْر الإنترنت كثيرة جدًّا. يُدعَى تطبيق الحلول المثاليَّة لمواجهة أخطار استعمال القُصَّر لوسائل الاتِّصال عَبْر الإنترنت **أمن معلومات القُصَّر**، وسيَتم فيما يأتي تعداد هذه الأخطار، ومن ثم سيَتم الحديث عن أسبابها، وبعدها ستُقدَّم الحلول لمواجَهتها.

تَتضمَّن أخطار استعمال القُصَّر لوسائل الاتِّصال عبر الإنترنت جميع العواقِب السيّئة التي يُمكِن أن تَأتي من ذلك، وتُسمَّى (أخطارًا) لأنَّ القُصَّر لديهم اندفاعات ومجازَفات غير شعوريَّة نحو الخطر، وهي:

1. سَرِقة مجرمين لمعلومات شخصيَّة من القاصِر تَتعلَّق باسمه الكامِل وجنسه وعمره وعنوانه التفصيلي ومعلومات أخرى عن عائلته، مثل أسمائهم ومهنَتَي والديه وأوقات غيابهم جميعًا عن المنزل، وما إلى ذلك من المعلومات المشابِهة، وتُسرَق هذه المعلومات إمّا من خلال غرف الدردشة الكثيرة أو من خلال وجودها أساسًا على صفحة خاصَّة بالقاصِر في أحد مواقع الشبكات الاجتماعيَّة، ويستفيد المجرمون من هذه المعلومات بطُرُق عدة، فقد يَقوم المجرم الذي سَرَق معلومات حقيقيَّة تفصيليَّة من القاصِر دون شعوره، إمّا بخَطْفِ القاصِر وطَلب فدية من أهله، أو سرقة منزله عند معرفة عدم وجود أحد في المنزل، أو بيع هذه المعلومات إلى جهات إجراميَّة أخرى.
2. استدراج القاصِر للانضمام إلى تَنظيم ما، سواء أكان هذا التنظيم عبارة عن شبكة دعارة للقُصَّر أم تَنظيم إرهابي، خاصَّةً إذا كان القاصِر يَتجاوَز سن 15 سنة، ويجري استدراج القاصِر للانضمام إلى أيّ تنظيم عن طريق، إمّا غرف الدردشة أو صفحات الشبكات الاجتماعيَّة، ويَنتُج عن الانضمام إلى شبكة دعارة إقناع القاصِر (سواء أكان ذكرًا أم أنثى) بتصوير نفسه عاريًا وإرسال الصور إلى هذه الشبكة سرًّا، ويَتضمَّن انضمام القاصِر إلى شبكة تَبادُل صور فاحِشة معه، وذلك يُسبِّب أضرارًا نفسيَّة له، وقد يَتجاوَز هذا الأمر

مجـرَّد انضمام افتراضي لشـبكة دعارة على الإنترنـت وتَبادُل الصور إلى تَردُّد القاصِـر فعليًّا على شـبكة الدعـارة وانضمامه إليها عمليًّـا. أمّا حالات انضمام القاصِر إلى التنظيمات الإرهابيَّة عبر الإنترنت فهي كثيرة جدًّا، فها هي جميع وسـائل الإعـلام تتحـدث فـي أنحاء العالـم عن انضمـام الكثيرين مـن القُصَّر مِمَّـن غُرِّر بهم بدوافع دينيَّة إلى تنظيمات إرهابيَّة، ويَنتُج عن انضمام القاصِر افتراضيًّـا لهذه التنظيمات الإرهابيَّة في معظم الأحيان اسـتدراجه للانضمام فعليًّـا إليهـا وتَجنيده في عمليات انتحاريَّة وحروب إرهابيَّة ضد دولٍ ما، وهناك أمثلة انضمام القُصَّر للتنظيمات الإرهابيَّة عبر الإنترنت.

3. تَثقيـف القُصَّـر بمعلومـات خاطِئـة، إمّـا عَمْدًا أو عـن غير قَصد، وقـد تَتضمَّن هـذه المعلومـات أمورًا سـيّئة تَتعلَّق بالصحة العامَّة، أو بالحيـاة الاجتماعيَّة، أو بمخالَفـة الأنظمـة والقوانين النافِذة في البلد الذي يَعيش فيـه القاصِر، ويَنتُج عـن التثقيـف بمعلومات خاطِئة ظهور سـلوكيَّات سـيّئة للقاصِـر مرتَبِطة بالأمر الـذي تَـمَّ تَلقّي معلومـات عنه، وأحيانًا قد يُسـيء القاصِر فَهْم هـذه المعلومات بسبب عدم تَوافُقها مع عمره.

أمّا أسباب انتشار أخطار استعمال القُصَّر لوسائل الاتِّصال عبر الإنترنت فهي:

1. فُضول القُصَّر وحُب استطلاعِهم لكل ما هو موجود على شبكة الإنترنت، إذ يَندفِع القُصَّر لرؤية كل شيء ومطالَعته في الإنترنت، ويَتضمَّن هذا الاندفاع مُحاوَلة التفاعُل والتواصُل مع الأشخاص دون النظَر إلى حقيقة أعمارهم وجنسهم وجنسياتهم، ودون معرفة أهدافهم الحقيقيَّة من هذا التَفاعُل، وإنَّ براءَة القاصِر في معظم الأحيان تَجعلُه يُقدِّم معلومات شخصيَّة تفصيليَّة عنه وعن عائلته دون إدراك الخطر الذي يُمكِن أن يَأتي من ذلك الأمر، فالقاصِر يُقدِّم معلوماته الشخصيَّة التفصيليَّة من باب تَكوين أصدقاء، والمجرِم يَستغلُّ هذا الاندفاع من القاصِر ورغبته في تَكوين أصدقاء، ويُقدِّم نفسه للقاصِر على أنه صديق من عمره نفسه وحتَّى جنسه، وله الهوايات نفسها ليَسرِق منه تِلْك المعلومات.
2. الكَبْتُ النفسي ومن ثم الجنسي للقاصِر خاصَّة إذا كان في سِن البلوغ. يَسعى بعض القُصَّر في سِن البلوغ للتخفيف عن كَبْتهم الجنسي إلى شبكة الإنترنت لمُطالَعة المواد الإباحيَّة، وتَنتظِر معظم مواقع الإنترنت الفاحِشة هؤلاء القُصَّر؛ ليُقدِّموا لهم المواد الإباحيَّة ولاستغلالهم.
3. التأثير الإعلامي في القُصَّر، إذ يَتفاعَل القاصِر مع وسائل الإعلام بشكلٍ كبير. فعندما يَتلقَّى القاصِر إعلامًا يُؤثِّر في اندفاعه الديني، يَلجأ إلى الإنترنت، وتستغله الصفحات المتطرِّفة في الشبكات الاجتماعيَّة لحَقْنه بأفكار تُؤدِّي به في النهاية إلى الانضمام إلى أصحابها.
4. عَدَم مُتابَعة الأهل لأبنائهم. كثيرًا ما تَقَع الحوادث التي يَذهَب القُصَّر ضَحيتها من وراء إهمال الأهل لأبنائهم الذين يَمضون ساعات كثيرة ومتواصِلة على شبكة الإنترنت، وأيضًا يَتجلَّى إهمال الأهل في عدم مُتابَعة أبنائهم الذين يَستخدِمون وسائل الاتِّصال التي أصبحت متوافِرة في جميع الأنظمة الحاسوبيَّة والهواتف الخلويَّة.

إنَّ الحلول المثاليَّة لمواجَهة أخطار استعمال القُصَّر لوسائل الاتِّصال عَبْر الإنترنت ليسَت كثيرة، ولكنَّها تَشمَل الأساليب لاستباق حدوث أي أخطار واحتوائها عند حدوثها، والحلول المثاليَّة لمواجَهة أخطار استعمال القُصَّر لوسائل الاتِّصال عَبْر الإنترنت هي:

1. تَركيب برامج حاسوبيَّة متخصِّصة تَمْنَع الأطفال من الولوج إلى أي موقع إنترنت باستثناء مواقع الإنترنت المَسموحَة من قِبَل الأهل. تَستطيع هذه البرامج أن تَضَع حاجزًا بين ولوج الطفل وأي موقع إنترنت يَرغَب الأهل في حَجْبه، وتَستطيع بعض هذه البرامج أن تُسجِّل جميع أنشطة الطفل في أثناء عَمَله على الإنترنت للاطِّلاع عليها فيما بعد، ويَبقى على الأهل التأكُّد من سلامة مواقع الإنترنت التي يَسمَحون لأطفالهم بالولوج إليها، وهذه المهمَّة ليسَت بالأمر الصعب، حيث يَستطيع الوالدان أن يُلقيا نظرة سريعة على هذه المواقع قبل البَتّ في السماح بالولوج إليها، ويُمكِن اختصار الطريق على الأهل من خلال إتاحَة مواقع الأطفال، كالألعاب والترفيه والرسوم المتحرِّكة فقط ضمن المواقع المَسموح بالدخول إليها في إعدادات تِلْك البرامج، وفي الواقع طُبِّقَت بعض القيود على استخدام الأطفال للإنترنت في بعض البلدان، وأشهرها الولايات المتَّحدة الأمريكيَّة، فعام 2000 سَنَّ الكونغرس الأمريكي قانون CIPA الذي يَنصُّ على أنه يجب على المدارس والمكتبات الحاصِلة على حسوم من استعمال خدمة الإنترنت فَرْض قيود على الإنترنت لمَنْع الأطفال من الولوج إلى مواقع الإنترنت المؤذية والفاحِشة (4).
2. مراقَبة سلوك القاصِر بعد استعماله الإنترنت على المدى القصير. إنَّ أي تَغيُّر في سلوك القاصِر بالتزامُن مع جلوسه الطويل على الإنترنت يَدلُّ على حدوث تأثير فيه يُمكِن أن يُؤذيه فيما بعد، ويَجب على الأهل اتِّباع أسلوب يُمكِّنهم من استدراج القاصِر لإخبارهم عن أنشطته في الإنترنت واتِّصالاته مع أصدقائه، وإذا كان الأهل على دراية تقنيَّة لا بأس بها في الحاسوب، يَستطيعون زراعة

برنامج تَجسُّس خَفي في حاسوب القاصِر لمتابَعة أنشطته كاملةً، وهناك برامج تجاريَّة لهذا الغرض موجودة بكثرة على الإنترنت.

3. تَوعيـة القُصَّـر اجتماعيًّـا ودينيًّا. تَتضمَّن تَوعية القاصِـر اجتماعيًّا تَعليمه عدم التعاطي مع أشخاص قد يكونون مشبوهين أو غير معروفين لديه، وعدم إعطائهم معلومـات شَـخصيَّة تفصيليَّة عنه، ويَندرِج تحـت تَوعية القاصِر اجتماعيًّا عدم تَزويد مواقع الإنترنت بالمعلومات الشخصَّية حتَّى ولو كان ذلك اختياريًّا، ولقد طُبّقت فعلًا قوانين تَمْنع أصحاب مواقع الإنترنت طَلَب معلومات من الأطفال إلا بموافقة الأهل، فعام 1998م أحدَثَت الولايات المتَّحدة الأمريكيَّة قانون COPPA الـذي يُلـزِم مديري مواقـع الإنترنت ومشـغِّليها بالحصـول على موافَقـة والدَي الطفل الذي يَقلُّ عمره عن 13 عامًا قبل تَجميعهم معلومات شخصيَّة منه (5). أمّـا تَوعيـة القاصِر دينيًّا فتَتضمَّن تَذكيره بوجوب التحلِّي بالأخلاق الإسـلاميَّة والتقيُّد بالتعاليم التي تُحرِّم مشـاهدة المواد الإباحيَّة ومخالَفة شَرْع الله – عز وجـل – وإشـعاره بأنَّـه مراقَـب مـن الله – عـز وجل – حتَّـى ولـو كان مختليًا مع نفسه، وتَتضمَّن تَوعية القاصِر دينيًّا تَذكيره بالإثم الذي يُمكِن ارتكابه من وراء تَصديق الجماعات المتطرِّفة والالتحاق بها.

2.8 أمان المعلومات الحَركيَّة

ثَمَّة معلومات خاصَّة تَتضمَّن تفاصيل عن انتقال فرد أو أفراد عدَّة أو نَقْل مادة ما من مكان إلى آخر، وتُدعَى **المعلومات الحَركيَّة**، وتَتألَّف المعلومات الحَركيَّة من ستَّة عناصر، هي:

- الهَدَف، وهو إمّا فردًا أو أفرادًا أو مادة ما.
- المكان الأصل الذي يُوجَد فيه الهَدَف.
- المكان المَقصود الذي سيَنتقِل إليه الهَدَف.

- مخطَّط الطريق الكامِل الذي سيَسلُكه الهدف من المكان الأصل إلى المكان المقصود.
- وسيلة الانتقال (أو النقْل) سواء أكانت سيَّارة أم قطارًا أم باخرة أم طائرة.
- موعد الانتقال (أو النقْل) محدَّدًا بالتاريخ (اليوم، والشهر، والسنة) وبالوقت (الساعة، والدقيقة).

صفة المعلومات الحَركيَّة أنَّها مؤقَّتة، بمعنى أنَّه يَنتهي الاهتمام بحمايتها بمجرَّد وصول الهدف إلى المكان المَقصود، ويَقتضي ذلك أنَّ الأمان الذي يُمكِن أن نُدخِل فيه هذه المعلومات هو الأمان العادي ذو الدرجة الثانية، وعليه، فإنَّ صفة الأمان في هذه الدرجة (ثابِتة وآنية)، وذلك يَعني أنَّ مستوى حماية المعلومات الحَركيَّة ثابِت، ولكنَّه يَستمرُّ مدة زمنيَّة إلى حين وصول الهَدَف إلى المكان المَقصود، ومن أمثلة المعلومات الحَركيَّة المتعلِّقة بفرد، المعلومات الخاصَّة التي تَتضمَّن انتقال موكب رئيس دولة من مكان إلى آخر، أو سَفَر مسؤولين كبار من مكان إلى آخر، وعُبورهم بالطائرة أجواء بلدان محدَّدة، وما إلى ذلك، ومن أمثلة المعلومات الحَركيَّة المتعلِّقة بمادة ما المعلومات الخاصَّة التي تَتضمَّن نَقْل أسلحة من مكان إلى آخر (أو من بلد إلى آخر)، أو المعلومات الخاصَّة التي تَتضمَّن نَقْل أموال نقديَّة من مكان إلى آخر، وثَمَّة أمرٌ مهم يَنبغي التركيز عليه فيما يَخصُّ المعلومات الحَركيَّة، وهو أنَّ هذه المعلومات قد تُستخدَم نفسها على نحوٍ متكرِّر، أو قد يَتغيَّر فيها واحد أو أكثر من عناصرها، فعلى سبيل المثال، قد يُعاد استخدام المعلومات الحركيَّة المتعلِّقة بانتقال موكب مسؤول كبير من منزله إلى مقرِّ عمله (أو بالعكس) يوميًّا بالعناصر نفسها؛ أي إنَّه سيَنتقِل من منزله (المكان الأصل) إلى مقرِّ عمله (المكان المقصود) أو بالعكس، وسيَسلُك الطريق نفسه المخصَّص لذلك وبوسيلة الانتقال نفسها وتمامًا موعد هذا الانتقال نفسه، وأحيانًا ولأسباب أمنيَّة، قد يَقوم المَعنيُّون بحماية موكبه بتَغيير أحد العناصر، مثل مخطَّط الطريق أو موعد الانتقال أو أحيانًا وسيلة الانتقال.

يُمكِن حماية المعلومات الحَركيَّة وإدخالها في وَضْع الأمان من خلال تَطبيق أمن معلومات عليها، يُدعَى **أمن المعلومات الحَركيَّة**، ويَتمثَّل أمن المعلومات الحَركيَّة في حمايتها من أجل حماية الهَدَف من أي خطر قد يُوجَّه إليه عند انتقاله (أو نَقْله) المتمثل في سَعي مجرمين لإيذاء الهَدَف إذا كان فردًا أو إيذاء الهَدَف أو سَرقته إذا كان عبارة عن مادَّة ما، ويُقَاس نجاح أمن المعلومات الحَركيَّة بالسلامة التامَّة لوصول الهدف إلى المكان المَقصود على نحوٍ متكرِّر، ويَتم تَحقيق أمن المعلومات الحَركيَّة من خلال تطبيق الإجراءات الآتية:

1. وَضْع الخطَّة الكامِلة لانتقال (أو نَقْل) الهَدَف من قِبَل خبراء متخصِّصين في مجال أمن الهَدَف وسلامة انتقاله (أو نَقْله). يُفتَرَض في الخبراء المتخصِّصين في مجال أمن الهَدَف وسلامته أنَّهم يَستطيعون رَسْم مخطَّط الطريق الكامِل ووسيلة الانتقال (أو النقْل) الملائمة وموعد الانتقال (أو النقْل) بما يَتناسَب مع أهميَّة الهَدَف وأخطار الطريق واعتبارات أخرى، مثل إطلاق تهديدات سابقة للهَدَف.
2. عَدَم تَسجيل المعلومات الحَركيَّة رقميًّا أو ورقيًّا، في وسائل أو وسائط معلوماتية يمكن النفاذ إليها.
3. الاحتفاظ بالمعلومات الحَركيَّة بين مجموعة صغيرة جدًّا من الأفراد ذوي العلاقة بانتقال (أو نَقْل) الهَدَف، ويَجب أن يُختار هؤلاء الأفراد على أساس الثقة التامَّة بأمانتهم، ويَجب أن يُغيَّروا باستمرار؛ لكيلا يَحدُث تَسريب للمعلومات الحَركيَّة من قِبَل أحدهم لأي سببٍ كان، مثل إقدام واحد منهم أو بعضهم على الخيانة.
4. تَغيير واحد أو أكثر من عناصر المعلومات الحَركيَّة باستمرار.
5. استعمال وسائط اتصالات مشفرة (معماة) بمستوى آمن من مستويات التشفير (التعمية).

3.8 حوادث الأمان

لا يَعني أنَّ تطبيق إجراءات الأمن ثمَّ إجراءات الأمان على المعلومات خاصَّة (مهما كان نموذجها) يَجعلها آمنة دومًا، فمن المُمكِن أن يَحدُث اختراق لأمان المعلومات حتَّى بعد تطبيق جميع إجراءات الأمن وجميع إجراءات الأمان بحذافيرها وبمهنيَّة عالية، فلا يوجَد وَضْعٌ مثالي لأمان المعلومات، بحيث تَكون هذه المعلومات آمنة بشكل تام، وإذا كانت الإجراءات المضادَّة مطبَّقة على نحوٍ عالٍ من الاحتراف وبمتابعة مستمرَّة، فعندها لا يَصِل أمان المعلومات إلى الوضع المثالي، وإنَّما إلى حَدٍّ قريب منه، وإذا حَدثَت اختراقات لأمان المعلومات المماثِّلة، إمّا بسرقة هذه المعلومات أو إفشائها أو تخريبها، فنحن بصَدَد مفهوم حوادث الأمان Safety incident، وقد يَتساءَل القارئ عن سَبَب تَسمية هذه الحوادث بـ (حوادث الأمان) بدلًا من (حوادث الأمن)، فلا يوجَد في حقل أمن المعلومات حوادث أمن؛ لأنَّ وقوع أي سرقة أو إفشاء أو تخريب للمعلومات الخاصَّة قبل تطبيق إجراءات الأمن تحديدًا سَبَبه عدم تطبيق أمن معلومات رسميًّا عليها، فوقوع أي سرقة أو إفشاء أو تخريب للمعلومات الخاصَّة قبل تطبيق أمن معلومات لا يَمتُّ بصِلة لحقل أمن المعلومات، وإنَّ السَبَب الرئيس لوقوع حوادث الأمان هو عَدَم تطبيق إدارة أمن المعلومات بشكلٍ مناسِب، ولقد وُضِعَت مراحل إدارة أمن المعلومات لكل نموذج من نماذج المعلومات الخاصَّة على نحوٍ مثالي، ولكن سوء التطبيق لجميع هذه المراحل يُمهِّد لوقوع حوادث الأمان.

ثَمَّة إجراءان علاجيّان للتعامُل مع حوادث الأمان، هما:

1. مراجعة الآليَّة التي تَمَّ عَبْرها تطبيق إدارة أمن المعلومات، ومن ثم تَغييرها، فالإجراء العلاجي الأول يَنبغي أن يَكون مراجعة هذه الآليَّة لاكتشاف مواضِع الخطأ في التطبيق ومعرفتها، فوَضْعُ آليَّة جديدة لتطبيق مراحل إدارة أمن المعلومات تَتفادَى مواضِع خطأ التطبيق تِلْك.

2. تغيير مضامين جميع المعلومات الخاصَّة فَوْر وقوع حادث الأمان. سوف يَتعرَّض مالِك المعلومات الخاصَّة إلى أذى وخسارة كبيرين بمجرَّد وقوع حادث الأمان؛ لـذا يَجـب عليـه أن يُغيِّر عند وقوع حـادث الأمان مضامين المعلومات الخاصَّة فورًا، وعند ذلك ستَفقِد مضامين هذه المعلومات القديمة أهميَّتها بعد تغييرها، وتَتراوَح عملية تغيير مضامين المعلومات الخاصَّة ما بين السـهولة والصعوبة، وذلك بحسـب كل نموذج من نمـاذج المعلومات، فمن أمثلة المعلومات الخاصَّة ذات القيمـة الماديَّـة التـي يُمكِن تغييـر مضامينها معلومات الأعمـال الخاصَّة، وأرقـام التعريف الشـخصي، وتُغيَّر مضامين معلومات الأعمـال الخاصَّة مثلًا بتغيير الخطَط المسـتقبليَّة لمشروعات تجاريَّة أو التصاميم الرئيسة لمنتجات صناعيَّة.

أمّـا أرقـام التعريـف الشـخصي فتُغيَّـر بـكل سـهولة من خـلال تبديلهـا بأرقام أخـرى، وأمّا تغيير مضامين المعلومات الخاصَّـة ذات القيمة المعنويَّة فيَتطلَّب جهودًا كبيرة وصعبة، إذ سيَشـمَل تغيير مضامين المعلومات المصنَّفة سـريَّة، كتصاميم الأسلحة، ومواعيد الهجمات الحربيَّة، وتغيير في مضامين المعلومات الدوليَّـة المصنَّفـة سـريَّة، كمحتويـات معلومـات اسـتخباراتيَّة مشـتَرَكة، وأمّا تغييـر مضامين المعلومـات الخاصَّة ذات القيمـة المَجازيَّة فلا يَحتـاج إلا إلى جهـدٍ يَتمثَّـل في تغييـر محتويات مِثْل كلمـات المرور لحسـابات صناديق البريد الإلكترونـي، وما إلى ذلك، وإنَّ تغيير مضامين جميع المعلومات الخاصَّة يَقطَع الطريق في أغلب الأحيان أمام الخصم للاسـتفادة من المعلومات التي حَصَل عليهـا؛ لـذا فـإنَّ أهم شـيئين في هـذا الإجراء همـا الحِرص على سـريَّة عمليَّة تغييـر مضامين المعلومات الخاصَّة، والإسـراع في تطبيـق إدارة أمن معلومات عليها من جديد.

الفصل التاسع

الحروب السايبريَّة

يُمثِّل العالَم الرقمي بيئة جديدة على العالَم الحقيقي في التعاطي مع المعلومات، وقد أصبح هذا العالم الرقمي فضاءً متكاملًا له معطيات يَتم من خلالها التفاعُل معه، وبعد أن تحوَّل إلى بيئة رسميَّة معتَمَدة، أصبح هذا العالَم الرقمي يُعرَف باسم **الفضاء السايبري** Cyberspace، ويُعرَّف هذا الفضاء بأنه البيئة الافتراضيَّة التي يَتم فيها تَبادُل المعلومات الرقميَّة عبر شبكات حاسوبيَّة، ويُمكِن تَصوُّر الفضاء السايبري كمجموعة ضخمة من شبكات الأنظمة الحاسوبيَّة المتَّصلة مع بعضها، ومثلما تَقَع حروب تقليديَّة في عالَم الواقع (كالتي تَحدُث في البر، والبحر، والجو، والفضاء) تَقَع حروب افتراضية في الفضاء السايبري تُسبِّب أذى وخسائر قد تُضاهي تلك الناتجة عن الحروب التقليديَّة، وتُدعَى **الحروب السايبريَّة** Cyberwars، والحرب السايبريَّة هي الهجمات الافتراضيَّة الموجَّهة من قِبَل منظَّمات أو دول لاختراق أو لتعطيل أو تخريب أنظمة أو شبكات حاسوبيَّة لمنظَّمات أو دول أخرى [27، 28]، ويُدعَى الهجوم الذي يَتم إطلاقه في الحرب السايبريَّة **الهجوم السايبري** Cyberattack.

تَحدُث الحروب السايبريَّة بشكل مفاجئ، وتُشَنُّ هجماتها في مواعيد سريَّة، ولأنَّ عنصر المفاجأة في وقوعها وعدم معرفة مُطلِقها والحجم الكبير لخسائرها تكون ذات

آثار بالغة، ويُماثِل بعضها تلك المرتَبِطة بأي عمل إرهابي، وتُدعَى الحرب السايبريَّة عندها **الإرهاب السايبري** Cyberterrorism.

ولقد كان الحديث عن الحروب السايبريَّة في الأوساط الدوليَّة الرسميَّة خافتًا، إلا أنه بعد اكتشافه والتَعرُّض لكثير من الهجمات السايبريَّة الموجَّهة عمدًا إلى دول بحدِّ ذاتها، أصبح الحديث عن تلك الحروب وعن ضرورة اكتساب مقدرات سايبريَّة علنيًّا.

وتَتَّجه كثير من بحوث أمن المعلومات الحديثة نحو التَعمُّق في مجال الحروب السايبريَّة من خلال دراسة دوافعها (أسبابها) وآلية خوضها، ومعرفة الأطراف المشارِكة فيها، ونتائج وقوعها، ولا شَكَّ أنَّ تطوير أي دراسة أو بحث يَتعلَّق بالحرب السايبريَّة سيزيد من إدراك المعطيات المرتَبِطة بها، وسيُمكِّن الطرف المَعني بها (سواء منظَّمة أو دولة) من تلافي آثارها السلبية أو التخفيف منها على الأقل، والتَصدِّي لها كلَّما وَقَعت.

1.9 دوافع الحروب السايبريَّة

لم تَنشأ الحروب السايبريَّة في الفضاء السايبري بلا سبب، فقد كانت هناك دوافع وأسباب عدَّة وجيهة وراء قيامها، ولم تَكُن هذه الحروب السايبريَّة لو لم تَحدُث ثورات تكنولوجيَّة عَمَّت أرجاء العالم، فالمعرفة والخبرة المتزايدة في النفاذ خفيةً إلى شبكات الحاسوب والأدوات البرمجيَّة التي طُوِّرت خصيصًا لاختراق تلك الشبكات أحدثت معطيات أو ممكنات قيام تلك الحروب، ولَعلَّ دوافع الحروب السايبريَّة مترابطة نسبيًّا، إلا أنَّ وراء كل دافع هدفًا أو غرضًا معيَّنًا جَعَل هذه الدوافع ذات صيغة شبه رسميَّة في عالم الفضاء السايبري، ودوافع الحروب السايبريَّة هي:

1. **حماية الفضاء السايبري العسكري.** تَنطلِق معظم دول العالم في التعامل مع الحروب السايبريَّة من حماية فضائها السايبري العسكري أولًا، الذي تَعدّه الواجهة الأماميَّة في التَصدِّي للهجمات السايبريَّة قبل خوض تلك الحروب، وعلى هذا الاعتبار أنشأَت بعض الدول هيئات سايبريَّة رسميَّة مهمَّتها الدفاع

عن المنشآت العسكريَّة المرتبطة بشبكات الحاسوب [30، 31]، ولَعلَّ السبب الرئيس وراء إنشاء هذه الهيئات هو الوعي بأنَّ الهجمات السايبريَّة قد أصبحت ذات تهديد أكبر على الأمن القومي لبلدٍ ما من التهديدات التقليديَّة.

في الحقيقة، لم تَكُن قرارات إنشاء الهيئات السايبريَّة الدفاعيَّة إلا مدخلًا لإنشاء هيئات سايبريَّة هجوميَّة متلازمة مهمَّتها شَنُّ الحروب السايبريَّة وإطلاق الهجمات الإلكترونيَّة القادرة على تعطيل المنشآت العسكريَّة التقليديَّة المرتَبِطة بالشبكات الحاسوبيَّة لبعض الدول، وعلى هذا الأساس تَبنَّت الهيئات السايبريَّة لمعظم الدول إستراتيجيَّتَي الدفاع السايبري والهجوم السايبري الأساسيتين في عملها، واعتَبَرت تلك الهيئات السايبريّة الرسميَّة أنَّ تطبيق الإستراتيجيَتين معًا ضروري للحفاظ على الأمن القومي، وبالأخص حماية التجهيزات العسكريَّة المرتبطة بالشبكات الحاسوبيَّة، على الرغم من نكرانها لتطبيق إستراتيجيَّة الهجوم السايبري، وقد تطوّر الأمر إلى أبعد من ذلك من خلال تَعاون بعض الدول معًا لتطوير سيناريوهات ردع هجمات سايبريَّة تُطلَق على نحوٍ تدريبي من أجل الاستعداد للتصدِّي للهجمات السايبريَّة الحقيقيّة، وخصّصت دول أخرى ميزانيات ماليَّة ضخمة لتطوير قدرات تلك الهيئات السايبريَّة على أداء عملها وتزويدها بالقوَّة المطلوبة في صراع الفضاء السايبري، وانطلاقًا من مبدأ مشارَكة المجتمع المدني في حماية الفضاء السايبري، شَجَّعت دول أخرى شركات محليَّة متخصَّصة في أمن المعلومات على المساهَمة في إغناء هذا القطاع وتطوير شركات جديدة للعمل فيه.

2. **تعطيل منشآت البنية التحتيَّة الحيويَّة.** مع ارتباط مرافِق البنية التحتيَّة الحيويَّة (مثل شبكات الطاقة الكهربائيَّة، وشبكات توزيع المياه، والمواصلات، والمؤسسات الماليَّة، والصحيَّة، والاتصالات، والدفاع، والمؤسسات الحكوميَّة بشكلٍ عام) بالشبكة الحاسوبيَّة، ازدادَت الهجمات السايبريَّة الموجَّهة لتعطيل تلك المرافِق، وقد تَعدَّى الأمر إلى وقوع تعطيل فَعَّال لمنشآت حسَّاسة ذات

أهميَّة قوميَّة [37، 33]، وردًّا على وقوع هذه الهجمات، أنشأَت بعض الدول هيئات سـايبريَّة مهمَّتها فقط حماية المرافِق الحيويَّة المرتَبِطة بشبكات الحاسوب، بل حتَّى إنَّ دولًا أخرى أسَّسَت هيئات سايبريَّة متخصِّصة في حماية الفضاء السايبري الحكومي والبنى التحتيَّة ومستقلَّة عن تلك الهيئات السايبريَّة المتخصِّصة في حماية الفضاء السايبري العسكري.

3. **النزعَة إلى التَفوُّق السايبري.** يَرغَب عدد من حكومات الدول إلى التفوُّق السايبري والحفاظ على هذا التفوُّق من خلال خَوض حروب سايبريَّة وإطلاق هجمات سايبريَّة حقيقيَّة، ولكنَّ الهدف الحقيقي لتلك الدول في السعي إلى التَفوُّق السايبري هو صَدُّ الهجمات السايبريَّة المستقبليَّة الموجَّهة إليها، وذلك عن طريق اكتشاف العيوب السايبريَّة للخصوم مسبقًا في أثناء إطلاق الهجمات السايبريَّة إليهم.
4. **مكافحة الإرهاب.** لا شَكَّ أنَّ الإرهاب العالمي بأنواعه ومصادره المختلفة أصبحَ يَستعمِل الفضاء السايبري لنشر مفاهيمه وعقيدته وإدارة تنظيماته، ومن ذلك تقوم الحكومات، كما يَسعى بعض (الهاكرز) كمجموعات مستقلَّة غير حكوميَّة متعدِّدة الجنسيات، للتَصدِّي للمنشورات والرسائل الإلكترونيَّة التي تَبثُّها التنظيمات الإرهابيَّة من خلال حَظْرها ومَنْعها من الانتشار كرَدٍّ فعل إيجابي في الوقوف ضد الإرهاب.
5. **اكتساب منافع شخصيَّة أو ماديَّة.** يَشنُّ بعض الأفراد أو المنظَّمات (التجارية أو الصناعيَّة) حربًا سايبريَّة ضد أفراد أو منظَّمات أخرى، وذلك للحصول على منافع شخصيَّة أو منافع ماديَّة، وتَتمثَّل معظم الهجمات السايبريَّة، التي تُطلَق من قِبَل الأفراد أو المنظَّمات، في نَشر برامج خبيثة أو زَرع برامج تَجسُّس في حواسيب الضحايا، وتُؤدِّي البرامج الخبيثة أو برامج التَجسُّس عملها من خلال آليَّة يَضعها الطرف (أو الأطراف) الذي أطلقها، بحيث تُحقِّق الهدف من وراء إطلاقها.

6. **إجراء بحوث علميَّة لتطوير حلول مستقبليَّة.** ليسَت جميع الهجمات السايبريَّة موجَّهة دائمًا ضدَّ أطراف معيَّنة لكسب المنافع الشخصيَّة أو الماديَّة، أو ضدَّ دول بعينها لإيذائها، إنَّما يُطلَق بعضها من قِبَل شركات متخصِّصة في أمن المعلومات وأمن الفضاء السايبري من أجل رسم سيناريوهات محدَّدة في كيفيَّة التَعاطي مع هذه التهديدات أو الهجمات، ووَضع الحلول التقنيَّة المناسبة لمواجهتها، ومن ثم تطبيق هذه الحلول في برمجياتها، ومن المُلاحَظ أنَّ هذه التهديدات السايبريَّة وحلول مواجهتها، المطوَّرة من قِبَل شركات أمن معلومات تجاريَّة، قد لا تُقارَن أبدًا مع تلك التهديدات والهجمات السايبريَّة المطوَّرة من قِبَل مجموعات متخصِّصة واحترافيَّة تَعمل مع حكومات دول كبرى.

2.9 أطراف الحروب السايبريَّة

لم يَعُد امتلاك تكنولوجيا المعلومات والعمل عليها صعبًا، ولم يَعُد الدخول إلى بعض شبكات الحاسوب (ومنها الشبكة الدوليَّة الإنترنت) إلا كفعل تحريك فأرة الحاسوب من مكانها؛ ولذلك لم يَعُد مستعصيًا على أي جهة – سواء أكانت فردًا، أم منظَّمة، أم مجموعة أفراد يُمثِّلون دولة ما بصفة رسميَّة – أن تخوض حربًا سايبريَّة في أي وقت كان ومن أي مكان، على أن يَتوافر الوصول إلى الشبكة الحاسوبيَّة والهدف وامتلاك الخبرات والبرمجيات المناسبة، فأدوات الحرب، وتحديدًا تلك التي يُشَنُّ بها هجوم، أصبحت برمجيات صغيرة تُوضَع في وسائط تخزين صغيرة.

وثَمَّة أطراف محدَّدة تَقود أي حرب سايبريَّة وتُوجِّهها، وعمومًا تَندرِج هذه الحروب السايبريَّة تحت ثلاثة مستويات هي: **الحروب السايبريَّة بين الأفراد** Individual cyberwar، **والحروب السايبريَّة بين المنظَّمات** Organizational cyberwar، **والحروب السايبريَّة بين الدول** International cyberwar، وثَمَّة حروب سايبريَّة أخرى تَحدُث بين أطراف من مستويات مختلفة.

1.2.6 (الحروب) السايبريَّة بين الأفراد

في حقيقة الأمر، لا توجد حرب سايبريَّة بين الأفراد، فعندما يشنّ فردٌ ما هجومًا سايبريًّا على فرد آخر يُسبِّب له أذى، عندها يُعدّ الطرف أو الفرد المستهدَف مجرَّد ضحيَّة، وتُدعَى هذه الحالةُ **الجريمةَ السايبريَّةَ** Cybercrime، والجريمة السايبريَّة هي الجريمة أو الهجوم أو الفعل المؤذي الذي يُستخدَم فيه الحاسوب للنفاذ إلى الشبكات الحاسوبيَّة لإلحاق الضرر بفرد أو بمجموعة من الأفراد، ويُدعَى الطرف أو الفرد الذي يَقترِف الجريمة السايبريَّة **المجرم السايبري** Cybercriminal، ومهما كان عدد أفراد الطرف المستهدَف في الجريمة السايبريَّة، فهم في النهاية مجرَّد ضحايا، وليسوا أطراف حرب حقيقيين.

أحيانًا يخرج الأذى أو الضرر الذي يُسبِّبه المجرم السايبري عن نطاق الفضاء السايبري ليدخل أحيانًا في نطاق الجريمة الحقيقيَّة، كجناية القتل العَمد، أو الاغتصاب، أو السرقة. وهذا دون شك عندما يُستعمَل الحاسوب (أو الشبكة الحاسوبيَّة) بوصفه وسيلة مؤقَّتة في إتمام الجريمة، كأنْ يُخزَّن دليلٌ ما على جريمة قتل في حاسوب.

ثَمَّة نوعان أساسيان من الجرائم السايبريَّة التي تُقترَف هما: **جرائم سايبريَّة نشيطة** Active cybercrimes و**جرائم سايبريَّة كامنة** Passive cybercrimes، والجرائم السايبريَّة النشيطة هي الجرائم السايبريَّة التي يَنجُم عنها إيذاء حواسيب الضحايا (الأفراد الآخرين من الحرب السايبريَّة المفتَرَضة) عن طريق نَشر البرامج الخبيثة، مثل الفيروسات والديدان وأحصنة طروادة وإطلاق هجمات الحرمان من الخدمة. أمّا الجرائم السايبريَّة الكامنة فهي الجرائم السايبريَّة التي تَتمثَّل في سرقة المعلومات الفرديَّة الخاصَّة، مثل كلمات السر لحسابات البريد الإلكتروني، ومواقع الشبكات الاجتماعيَّة، وأرقام التعاريف الشخصيَّة، وأرقام الحسابات المصرفيَّة، وتُقترَف الجرائم السايبريَّة الكامنة بشكلٍ كبير عن طريق استعمال برامج التَجسُّس. عمومًا تُعدّ

الجرائم السايبريَّة بنوعيها النشيط والكامن تهديدًا بشريًّا موجَّهًا نحو جميع الأطراف من جميع المستويات.

ولا يُمكِن الاستهانة بنتائج وقوع الجرائم السايبريَّة، فبعد انكشاف الضرر والأذى اللذين يُمكِن أن تُسبِّبهما الجرائم السايبريَّة، يشير أحد التقارير الدوليَّة إلى أنَّ تلك الجرائم تُكبِّد الاقتصاد العالمي ما يُقارِب 445 بليون دولار أمريكي سنويًّا بحسب تقديرات عام 2005م.

2.2.9 الحروب السايبريَّة بين المنظَّمات

تَمتلِك المنظَّمات (سواء أكانت تجاريَّة أم صناعيَّة) خصائص تجعلها أكثر احتمالًا لأن تَدخُل في حروب سايبريَّة بين بعضها مما هو الحال بين الأفراد كأطراف مستقلَّة، ولأنَّ المنظَّمة (مهما كان عملها) أساس بناء اقتصاد دولة، يُعدّ استهدافها من قِبَل أي منظَّمة منافِسة أخرى في الدولة نفسها أو في دولة أخرى حدثًا ممكنًا في معظم الأحيان [20، 21]. إنَّ المنظَّمة التي تُخصِّص ميزانيَّة ماليَّة كبيرة لوضع إستراتيجيَّة أمن معلومات خاصَّة بها تستطيع أن تَتصدَّى للهجمات السايبريَّة الموجَّهة من قِبَل أي منظَّمة أخرى (منافِسة أو غير منافِسة)، أو على الأقل تُخفّف من الآثار السلبيَّة للهجمات التي قد تتلقاها فعلًا.

تسعى الهجمات السايبريَّة بين المنظَّمات إلى تحقيق الهدفين الرئيسين الآتيين:

1. الحصول على معلومات الأعمال الخاصَّة للاستفادة منها في اكتساب منافع ماليَّة، ويَتم هذا عادةً عن طريق اختراق أنظمة حواسيب المنظَّمة المستهدَفة، أو زرع برامج تَجسُّس فيها، ومن ثم تحميل معلومات الأعمال الخاصَّة التي تحتوي على تفاصيل صناعة منتجات معيَّنة أو تصاميم مستقبليَّة أو صفقات تجاريَّة.

2. تخريب منشآت البنية التحتيَّة المتَّصلة بشبكات الحواسيب للمنظَّمة المستهدَفة وتكبيدها خسائر كبيرة، ويَتُم ذلك من خلال نشر فيروس أو دودة في أنظمة حواسيب المنظَّمة تُعطِّل عمل معدَّات البنية التحتيَّة أو تُدمِّرها، وتَشتدُّ الحروب السايبريَّة بين المنظَّمات عندما تَتطوَّر هذه المنظَّمات، وتصبح أكثر إنتاجًا وذات إيرادات ماليَّة كبيرة، وعلى هذا الأساس، تُحاوِل كل منظَّمة أن تَرفَع من مستوى حماية معلوماتها من خلال وضع ميزانية ماليَّة ضخمة لتخطيط ورسم المعايير التي تَضمَن تطبيق ممارسات جيدة في أمن المعلومات، وتوعية موظَّفيها المسؤولين عن تلك المعلومات بأهميَّة التقيُّد بالمعايير المرسومة للحفاظ على نجاح المنظَّمة ككل.

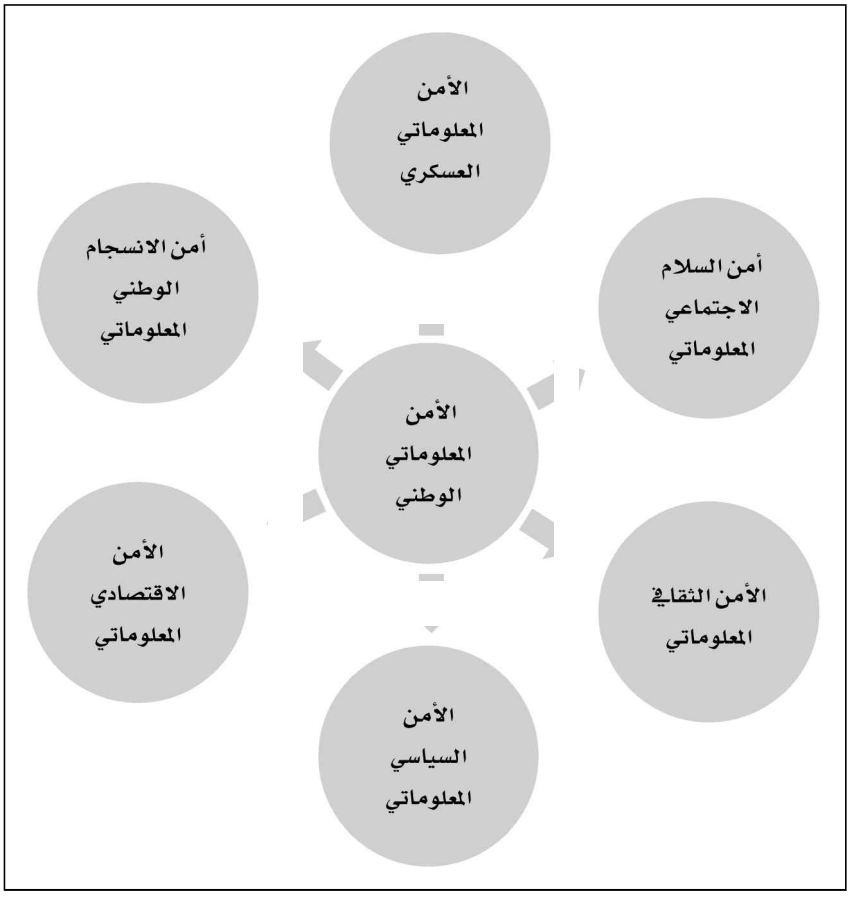
3.2.9 الحروب السايبريَّة بين الدول

إنَّ الحروب السايبريَّة التي تَحدُث بين الدول هي أوضح تجسيد لمفهوم (الحرب السايبريَّة)، فالحرب التقليديَّة عادةً ما تَقع بين دولتين أو أكثر، ولكن ليس ثَمَّة حرب تقليديَّة (بكل معنى الكلمة) تَحدُث بين أفراد أو بين منظَّمات. لذلك، وعلى نحوٍ مشابه للحروب التقليديَّة التي تَقع بين الدول، تَحدُث حروب سايبريَّة بينها، وفي بعض الأحيان، تَحدُث حروب سايبريَّة بين دول صديقة، إلا أنَّ الاعتراف بخوضها لا يُعلَن من قِبَل أي طرف منها، وقد يعود ذلك إلى أسباب دفاعيَّة تَتمثَّل مثلًا في اختبار أنظمة الحماية السايبريَّة للدولة التي شَنَّت الحرب ضدَّ دولة صديقة.

تشتمل الحروب السايبريَّة بين الدول التعرض إلى ستة أنواع من الأمن والأمان الوطني المعلوماتي، ويبيّن الشكل تمثيلًا مبسطًا لذلك.

الأمن المعلوماتي الوطني

(أمن المعلومات والاتصالات)



تَتشابه أهداف الحروب السايبريَّة بين الدول، من حيث المستهدفات المعلوماتية، مع أهداف الحروب السايبريَّة بين المنظَّمات، ولكن على نطاقٍ أوسع، وعلى العموم، ثَمَّة أيضًا ثلاثة أهداف رئيسة للحروب السايبريَّة بين الدول هي:

1. الحصول على المعلومات المصنَّفة سريَّة (مهما كان مستوى تصنيفها السرِّي) للدولة المستهدَفة، ويشمل ذلك المعلومات العسكرية، والأمنية، والاقتصادية، والاجتماعية، وغيرها.

2. تعطيل منشآت البنية التحتيَّة الحيويَّة للدولة المستهدَفة.
3. الحرب الإعلامية باستعمال الإعلام الجديد من خلال الفضاء السيبرياني.

تختلِف شدَّة الحروب السايبريَّة التي تحدُث بين الدول باختلاف المهارات العلميَّة للدولة المصدَر والدولة الهدف، والإمكانيات المتمثِّلة في المعدَّات والأدوات البرمجيَّة التي تَمتلِكها الدولة المصدَر، ويشهد العالم اشتداد قوَّة الحروب السايبريَّة بين الدول، وما قد يُصيب الدولة المستهدَفة هو تخريب منشآت بنيتها التحتيَّة الحيويَّة، هذا إن كانت هذه المنشآت متَّصلة بشبكات حاسوبيَّة، وقد يكون للحرب السايبريَّة أثر مادِّي في الدولة المستهدَفة، وهذا قَلَّما يَحدُث إلا في حالات محدَّدة.

4.2.9 الحروب السايبريَّة بين أطراف مختلفة المستويات

من الممكِن أن تَقَع حروب سايبريَّة بين أطراف من مستويات مختلفة، فقد يَحدُث أن يَشنَّ فرد أو مجموعة من الأفراد هجومًا سايبريًّا على منظَّمة ما بهدف الحصول على منافع شخصيَّة أو مكاسب ماليَّة، وقد يقوم فرد أو مجموعة من الأفراد بشَنِّ هجوم سايبري على مؤسسات دولة ما، ويَحدُث أيضًا أن تَخوض دولة ما حربًا سايبريَّة ضد مجموعة من الأفراد أو منظَّمة ما أو منظَّمات عدَّة، عمومًا عندما تَحدُث حروب سايبريَّة عدَّة معًا في الفضاء السايبري بين أطراف من مستويات مختلفة وعبر قارَّات العالم، يُمكِن أن نَدعو مجموعها **الحرب السايبريَّة العالميَّة** World cyberwar.

3.9 مقوِّمات الحروب السايبريَّة

إنَّ لكل حرب تقليديَّة في عالم الواقع معطياتها الخاصَّة، ولكن جميع الحروب التقليديَّة لديها عناصر تُؤسِّس لقيامها، وفي المقابل، تَمتلِك الحروب السايبريَّة مقوِّمات موحَّدة خاصَّة بها، ومقوِّمات الحروب السايبريَّة هي المكوِّنات أو العناصر (الماديَّة وغير الماديَّة) التي تُؤسِّس بمجموعها قيام تلك الحروب، ولكل حرب سايبريَّة معطياتها

الخاصَّة المتمثِّلة مثلًا في دوافع قيامها والنتائج المتوقَّعة من خوضها، ولكن مقوِّمات أي حرب سايبريَّة هي:

1. **البيئة** Environment.
2. **الطرف** Entity.
3. **الإستراتيجيَّة** Strategy.
4. **الأداة** Tool.

وعلى الرغم من أنَّ مقوِّمات أي حرب سايبريَّة موحَّدة، إلا أنَّ عواملها متغيِّرة، ويعني ذلك أنَّ الطرف أو الإستراتيجيَّة أو الأداة قد تَتغيَّر من حرب سايبريَّة إلى أخرى.

1.3.9 البيئة

تَتنوَّع البيئات الواقعيَّة التي تَحدُث بها الحروب التقليديَّة، فمن الممكِن تحديد بيئة أي حرب تقليديَّة بمجرَّد وقوعها، سواء في البر أو على البحر أو في الجو أو الفضاء، ولكن الحروب السايبريَّة لا تَقَع إلا في بيئة افتراضيَّة واحدة هي الفضاء السايبري، والفضاء السايبري، كما عُرِّف سابقًا، هو البيئة الافتراضيَّة التي يَتم فيها تَبادُل المعلومات الرقميَّة عبر شبكات حاسوبيَّة. يَصِف التعريف السابق الشكل العام للفضاء السايبري، ولكن من الناحية الفيزيائيَّة، الفضاء السايبري هو المجموع الأكبر لشبكات الحواسيب، التي تُعرَف باسم الإنترنت.

عندما تَقَع حرب تقليديَّة بين دولتين، تعرِف كلٌّ منهما حدودها (البريَّة، أو البحريَّة، أو الجويَّة) المرسومة التي لا تتجاوَزها إلا في حالة هجوم، وتُحافِظ على ثباتها في حالة دفاع، ولكن في بيئة الحروب السايبريَّة (التي هي الفضاء السايبري) لا توجد حدود بين أي طرف في أثناء قيامها، فالاستطلاع والتخطيط والهجوم (أو حتَّى الدفاع) في الفضاء السايبري يُمكِن أن تَتم جميعها من أي مكان في العالم وفي أي وقت، وهذه الحريَّة شبه المطلقة في التَحكُّم في شَنِّ حرب سايبريَّة وإدارتها من أي مكان في العالم

جَعلَت كل من لديه المعرفة والخبرة الكافيَتَين مع أدوات مناسبة قادرًا على خوضها، ومن أهم خصائص الحروب السايبريَّة شنُّ الهجمات فيها من قِبَل أطراف موجودين فيزيائيًّا عبر قارَّات العالم دون أن يَلتقوا أبدًا.

إنَّ الفضاء السايبري هو البيئة الوحيدة التي تَجري فيها أي حرب سايبريَّة؛ لذا فمن المهم أن يُدرِك الطرف (سواء أكان المصدَر أم الهدف) جميع خصائص الشبكة الحاسوبيَّة التي يعمل عليها، وأن يُحاوِل سَدَّ الثغرات المكتشَفة، ويُعالِج نقاط الضعف في هذه الشبكة إذا كان يُمثِّل الطرف الهدف، أو أن يَكتشِف ثغرات ونقاط ضعف الشبكة الحاسوبيَّة للطرف الهدف إذا كان يُمثِّل الطرف المصدَر. وأخيرًا، ينبغي للطرف المصدَر والطرف الهدف أن يَعُدّا الفضاء السايبري ساحة الحرب السايبريَّة التي من الواجب السيطرة عليها والتَحكُّم فيها على النحو الذي يُحقِّق الغاية.

2.3.9 الطرف

يُعدّ الطرف البشري (سواء أكان فردًا أم منظَّمةً أم دولةً) المقوِّم الأهم من مقوِّمات أي حرب سايبريَّة، فدون الطرف البشري لا يُمكِن أبدًا إشعال أي حرب سايبريَّة. والطرف البشري (واختصارًا الطرف فقط) هو المحرِّك الأساسي في الحرب السايبريَّة، إذْ لا يُمكِن أن تُوجَد إستراتيجيَّة في الحرب السايبريَّة (سواء أكانت هجومًا أم دفاعًا) دون أن يَرسُمها الطرف، ولا يُمكِن أن تَتحرَّك أدوات الحرب السايبريَّة وحدها، وتُؤدِّي دورها دون أن يَستثمرها الطرف، وكل ذلك دليلٌ على أنَّ مقوِّم الطرف هو أهم مقوِّمات أي حرب سايبريَّة.

على العموم، ثَمَّة طرفان أساسيان في أي حرب سايبريَّة، هما: **الطرف المصدَر** Source entity و**الطرف الهدف** Target entity، والطرف المصدَر هو الطرف البشري الذي يُؤدِّي دور المهاجم أو الذي يقوم بعملية الهجوم السايبري على الطرف الهدف في الحرب السايبريَّة. أمّا الطرف الهدف فهو الطرف المستهدَف الذي يَتلقَّى الهجوم

السايبري من الطرف المصدَر، الذي يُؤدِّي دور المدافِع أو الذي يقوم بعملية الدفاع في الحرب السايبريَّة، وقد يكون الطرف المصدَر فردًا أو منظَّمةً أو دولةً أو مجموعها، وقد يكون الطرف الهدف في الوقت نفسه فردًا أو منظَّمةً أو دولةً أو مجموعها.

يتَّصفُ كلٌّ من الطرف المصدَر والطرف الهدف بخصائص تُميِّزهما عن بعضهما، وهذه الخصائص تُمكِّنُ من التَعرُّف إلى كل طرفٍ فيما إذا كان طرفًا مصدَرًا أو طرفًا هدفًا، وخصائص الطرف المصدَر هي:

1. حيازة دافع للقيام بحرب سايبريَّة ضدَّ الطرف الهدف. لا بُدَّ أن يَمتلِك الطرف المصدَر دافعًا قويًّا ليُقرِّر القيام بهجوم سايبري على طرف معيَّن، ويحثُّ أحد الدوافع التي تَمَّ سردها سابقًا أي طرف على أن يَخوض حربًا سايبريَّة متى وُجِد هذا الدافع.
2. التَّمتُّع بمعرفة علميَّة ومهارة مكتَسَبة في المجال، وتجهيزات في الفضاء السايبري تَجعله يَتجرَّأ لشَنِّ هجوم سايبري على الطرف الهدف، وإذا لم تَتوافَر عوامل المعرفة العلميَّة والخبرة العمليَّة في خوض تجربة الحرب السايبريَّة لدى الطرف المصدَر، لن يستطيع عندها أن يَشنَّ هجومًا سايبريًّا على الطرف الهدف، أو أن يَخوض حربًا سايبريَّة ضدَّه، بل حتَّى من الممكِن أن يُصبِح الطرف المصدَر طرفًا هدفًا دون أن يدري إذا لم يَمتلِك المعرفة الكافية الخاصَّة بالحروب السايبريَّة.
3. السَّعي نحو معرفة نتائج الهجوم السايبري على الطرف الهدف، والاستطلاع حول نجاحه أو فشله. يَكتسِب الطرف المصدَر ثقة كبيرة في نفسه إذا عَلِم بنجاح هجومه على الطرف الهدف، وهذا الأمر سيُشجِّعه على شَنِّ هجمات سايبريَّة أخرى على الطرف الهدف نفسه وشَنِّ هجمات سايبريَّة على أطراف هدف أخرى أو خوض حرب سايبريَّة ضدَّها.

4. التَحـوُّل إلـى موقف الطرف الهدف تلقائيًّـا. بمجرَّد أن يَشـنَّ الطرف المصدَر هجومًا سـايبريًّا على الطرف الهدف سيَتحوَّل بدوره تلقائيًّا إلى طرف هدف، وسيَسـعى إلـى أن يَصدّ الهجمات السـايبريَّة التي قد تأتي مـن الطرف الهدف الآخـر الـذي بدوره قد تَحوَّل إلى طرف مصدَر، والأمـر برمَّته طبيعي جدًّا؛ لأنَّ مبدأ الحرب بشـكل عام يَعتمِد على أسـلوب الهجوم والدفاع في الوقت نفسه أو الصَدِّ والرَدِّ.

أمّا خصائص الطرف الهدف فهي:

1. حيـازة سـبب يَجعلـه فـي موقـف الطـرف الهـدف، كأن يكون قـد أطلـقَ هجومًا سـايبريًّا سـابقًا، وكان في موقف الطرف المصدَر، وبعدها وبدافع انتقامي من الطرف الآخر، أصبح في موقف الطرف الهدف. وهذا يُحتِّم الآن على الطرف الهـدف أن يَتوقَّـع في أي وقت تَلقِّي هجوم سـايبري، وأن يكون مسـتعدًّا لحماية بنيته السايبريَّة.
2. امتـلاك بنيـة سـايبريَّة ضعيفـة تَجعله عُرضةً لهجوم سـايبري. وهذا بلا شـك إن لم يَسـتطِع الطرف الهدف صَدّ الهجوم السـايبري والدفاع عن منشآته التي تَسـبَح في الفضاء السـايبري، فعندما لا يكون الطرف (سـواء أكان مصدَرًا أم هدفًا) محصَّنًا على نحوٍ جيد، سيُصبح عُرضةً لأي هجوم سايبري، سواء أكان بدافـع انتقامـي أم لا؛ لذا يَنبغي للطرف الهـدف أن يُعزِّز من دفاعاته الرقميَّة؛ لكي يكون جاهزًا في حال قام بالردِّ، ومستعدًّا في حال قام بالصدِّ.
3. الاسـتعداد للدفاع عن بنيته السـايبريَّة من هجمات سـايبريَّة مسـتقبليَّة أخرى بعد أن تَلقَّى الهجوم السايبري الأول من الطرف المصدَر، ومن ثمَّ التَحوُّل إلى أن يكون في موقف الطرف المصدَر، وهذا دون شك إنْ لم يكُن الطرف الهدف قد بادَر مسبقًا بهجوم سايبري على الطرف المصدَر.

إنَّ دراسة سلوك طرفَي الحرب السايبريَّة مهم جدًّا لمعرفة (أو على الأقل تَوقُّع) نتائجها، فالحرب السايبريَّة لا تقوم إلا بوجود نشاط سايبريّ بين طرفين، فلولا نشاط الطرفين المصدَر والهدف معًا لما كان هناك حرب سايبريَّة، فمن الممكِن أن يشنّ طرف واحد هجومًا سايبريًّا على طرف آخر لا يُحرِّك ساكنًا. عندها، لا يُؤسِّس هذا الهجوم السايبري حربًا سايبريَّة، وإنَّما يُسمّى (هجومًا سايبريًّا)، وفي المقابل، إذا كانت الهجمات السايبريَّة متبادَلة بين طرفين، عندها تكون قد وَقَعت حربٌ سايبريَّة.

3.3.9 الإستراتيجيَّة

يَعتمِد ربح الحروب التقليديَّة أو خسارتها على فعاليَّة الإستراتيجيَّة الموضوعة لخوض الحرب، سواء أكانت هذه الإستراتيجيَّة هجومًا أم دفاعًا، فعندما يَفوز طرف ما في حرب على طرف آخر، فإنَّ ذلك دليلٌ على أنَّ إستراتيجيَّة الحرب للطرف الفائز أكثر فعاليَّة من إستراتيجيَّة الحرب للطرف الخاسر (وهذا إنْ كان هو أيضًا يُطبِّق إستراتيجيَّة ما)، وفي الحرب التقليديَّة لا تحتاج بعض الدول إلا إلى إستراتيجيَّة لتُهاجِم بها طرفًا آخر فقط دون أن تَعوز إستراتيجيَّة أخرى للدفاع (وهذا عندما تكون الدولة متفوقة حربيًّا)، وبعض الدول الأخرى لا تحتاج إلا إلى إستراتيجيَّة لتدافع بها (على الأقل) عن نفسها من هجمات طرف آخر أو أطراف أخرى. أمّا في الفضاء السايبري فلا بُدَّ لكل طرف (سواء أكان فردًا، أم منظَّمة، أم دولة) أن يَمتلِك إستراتيجيَّتين معًا: واحدة للدفاع السايبري، وواحدة للهجوم السايبري؛ ليَخوض أي حرب سايبريَّة.

ثَمَّة إستراتيجيَّتان أساسيَّتان لخوض أي حرب سايبريَّة هما: **إستراتيجيَّة الدفاع السايبري** Cyber defense strategy **وإستراتيجيَّة الهجوم السايبري** Cyber offense strategy. وإستراتيجيَّة الهجوم السايبري هي الخطة المرسومة من قِبَل أي طرف، التي ينبغي أن يَضمَن تطبيقها شَنّ هجمات سايبريَّة ناجحة على الطرف الخصم، ولا بُدَّ أن يكون لدى كل طرف في الحرب السايبريَّة إستراتيجيَّتا الدفاع السايبري والهجوم

السايبري معًا، ويجب أن تكون الإستراتيجيَّتان مكمِّلتين لبعضهما، بمعنى أنه إذا طُبِّقَت إستراتيجيَّة الهجوم السايبري مثلًا، ينبغي أن تحتوي إستراتيجيَّة الدفاع السايبري على سيناريوهات لكل آليَّة هجوم؛ لكي تكون مستعدَّة للصَدِّ وحماية البنية السايبريَّة للطرف الذي وَضعهما، ولا تَختلِف إستراتيجيَّتا الدفاع السايبري والهجوم السايبري عن بعضهما من حيث السياسات العامة والأدوات، فكلتاهما تُطبَّقان في الفضاء السايبري نفسه ومن قِبَل الطرف نفسه.

ولا يُمكِن التَنبُّؤ بفوز طرف ما أو خسارته في أي حرب سايبريَّة، ولكن إذا اُعتمدت معايير محدَّدة في رسم إستراتيجيتَي الدفاع السايبري والهجوم السايبري وتطبيقهما، يُمكِن عندها توقع الفوز في الحروب السايبريَّة، وإذا لم تَضمَن معايير نجاح إستراتيجيَّة الهجوم السايبري نجاح أي هجوم سايبري، ينبغي على الأقل أن تَضمَن معايير نجاح إستراتيجيَّة الدفاع السايبري حماية البنية السايبريَّة.

معايير نجاح إستراتيجيَّة الدفاع السايبري هي:

1. أن تُراعي احتمال التَعرُّض لأقوى هجوم سايبري. عند رسم إستراتيجيَّة الدفاع السايبري، يجب على واضعيها أن يستعدوا لاحتمال مواجهة أكبر هجوم سايبري، وهذا السقف الأعلى من التشاؤم يَضمَن الحماية من الهجمات السايبريَّة الأقل حدَّة.
2. أن تكون قابلة للتعديل في حال لم يَنجَح تطبيقها في حماية البنية السايبريَّة كليًّا أو جزئيًّا. ينبغي أن تكون إستراتيجيَّة الدفاع السايبري مرنة قدر الإمكان للتعديل، خاصَّةً في أثناء وقوع الحرب السايبريَّة؛ لأنَّ تعديلها جزئيًّا قد يَقلِب الموازين، ويَتحوَّل الطرف الذي وَضعها من خاسر إلى فائز.
3. أن تحتوي على توقع سيناريوهات حصول هجمات سايبريَّة متعدِّدة الإمكانيَّات ومن أطراف مختلفة. إنَّ وضع إستراتيجيَّة دفاع سايبري، بحيث تكون موجَّهة للتعامل مع طرف معيَّن أو طرف ذي خصائص معيَّنة قد يؤدي إلى الفشل؛ لذا

يجب على إستراتيجيَّة الدفاع السايبري أن تُحاكي هجمات ذات قوى متفاوتة ومن أطراف مختلفة.

4. أن تكون بسيطة وواضحة قدر الإمكان منذ البداية وعند تطبيقها. إذا احتَوَت إستراتيجيَّة الدفاع السايبري على خطوات كثيرة وتفاصيل معقَّدة، فسوف يكون من الصعب على الأشخاص الموكَّلين بتطبيقها فهمها واستيعابها، عندما يقومون بدراستها، أمّا عند التطبيق العملي لهذه الإستراتيجيَّة في أثناء وقوع الحرب، فسوف يُعاني هؤلاء الأشخاص الموكَّلين بتطبيقها بطئًا في التنفيذ، وسوف يَتمتَّع الأشخاص الموكَّلون بتطبيق إستراتيجيَّة الدفاع السايبري بمرونة كافية إذا كانت هذه الإستراتيجيَّة سريعة التنفيذ.
5. أن يُرافِقها إستراتيجيَّة دفاع سايبري أخرى رديفة وبديلة لها في حال فَشِل تطبيق الإستراتيجيَّة الأساسيَّة؛ لذا يجب وضع إستراتيجيَّة دفاع سايبري بديلة وجاهزة للتطبيق فورًا إذا واجَه تطبيق الإستراتيجيَّة الأساسيَّة شللًا تامًّا.

أمّا معايير نجاح إستراتيجيَّة الهجوم السايبري فهي:

6. أن تكون مرسومة وفق أفضل الممارسات العالمية في وضع إستراتيجيَّات الهجوم السايبري. مما لا شك فيه، فإنه لا تُقارَن إستراتيجيَّات الهجوم السايبري للدول الماهرة في الحروب السايبريَّة مع تلك الموضوعة من قِبَل أفراد أو منظَّمات، حتَّى ولو امتَلكوا خبرة كبيرة في هذا المجال، مراقبة سلوك أي هجوم سايبري وتحليله من أي أطراف قويَّة في هذا المجال يُمكِّن من استخلاص بعض أو جميع خطوات إستراتيجيَّاتها في الهجوم السايبري، ومن ثم دراستها والاستفادة من دورها.
7. أن تَضم سيناريوهات متنوِّعة ومتعددة لهجمات سايبريَّة، بحيث إنْ لم تَنجَح إحداها تَنجَح الأخرى. إنَّ التَنوُّع في سيناريوهات الهجمات السايبريَّة ضروري لكي يَتحقَّق التأثير في أكبر قد مَمكِن من أنظمة شبكات حواسيب الطرف

الهدف، ومن المُمكِن عمليًّا أن يَفشَل تطبيق سيناريو ما لهجوم سايبري على طرفٍ، ويَنجَح على طرفٍ آخر، وهذا كلّه بسبب اختلاف مستويات حماية البنية السايبريَّة لدى كل طرف.

8. أن يتطلَّب تطبيقها استعمال أقل عدد مَمكِن من الأدوات. من الضروري التنويع في استعمال الأدوات البرمجيَّة اللازمة في الهجوم السايبري، ولكنَّ كثرة هذه الأدوات أو تعقيدها أو تطبيقها دفعةً واحدة قد يُؤدِّي إلى الخسارة في الحرب السايبريَّة، ومن ناحيةٍ ثانية، يُؤدِّي استعمال جميع الأدوات البرمجيَّة في هجوم سايبري واحد إلى كَشف جميع القدرات المتوافرة في هذا المجال، ومن ثم يؤدي إلى إضعاف قوَّة أي هجوم سايبري مستقبلي واحتمال الخسارة في الحرب السايبريَّة.

9. أن تُحدَّث على نحوٍ دوري. ينبغي أن تُواكِب إستراتيجيَّة الهجوم السايبري تَنوُّع الحروب السايبريَّة وتَطوُّرها على مستوى العالم، وأن تَتماشى مع تَطوُّر أسلحة الحروب السايبريَّة، وبالتحديد تلك الأدوات الخاصَّة بشَنِّ الهجوم السايبري، فإذا لم تُحدَّث إستراتيجيَّة الهجوم السايبري لأي طرف دوريًّا، فلن يُكتَب له النجاح بسبب تَطوُّر إستراتيجيَّات الدفاع السايبري للأطراف الأخرى وتحديثها.

والخلاصة، لا يُمكِن لأي طرف أن يفوز في حرب سايبريَّة إذا لم تَكُن إستراتيجيَّتا الدفاع السايبري والهجوم السايبري الخاصَّتان به ناجحتين، حتَّى ولو امتَلَك أدوات الحروب السايبريَّة، فالتخطيط الجيِّد لهاتين الإستراتيجيتين يُسهِم في الفوز، ولكنَّ لا يَضمَنه إلا إذا كانت آليات تطبيقهما ناجحةً أيضًا.

4.3.9 الأداة

لا يُمكِن إطلاق أي هجوم سايبري أو خوض حرب سايبريَّة دون امتلاك الأدوات اللازمة لذلك، وأدوات الحروب السايبريَّة بالمعنى التقني هي الأدوات البرمجيَّة التي يَتم العمل عليها في الفضاء السايبري، ويجري يوميًّا إنتاج أدوات برمجيَّة خاصَّة بالحروب السايبريَّة وتطويرها؛ لذا لا يُمكِن حَصر جميع تلك الأدوات البرمجيَّة في حديث واحد، وعمومًا ثَمَّة نوعان أساسيَّان من أدوات الحروب السايبريَّة، هما: **أدوات الدفاع السايبري** Cyber defense tools و**أدوات الهجوم السايبري** Cyber offense tools. من البدهي إدراك أنَّ أدوات الدفاع السايبري تَخصُّ الطرف الهدف، وأدوات الهجوم السايبري تَخصُّ الطرف المصدَر، ولكنَّ ذلك لا يعني أبدًا عدم امتلاك الطرف المصدَر أدوات الدفاع السايبري أيضًا، أو عدم امتلاك الطرف الهدف أدوات الهجوم السايبري؛ لذا فمن المنطقي أن يَمتلِك كلٌّ من الطرف المصدَر والطرف الهدف النوعين معًا.

تتألَّف أدوات الدفاع السايبري من **أدوات الحماية** Protection tools، و**أدوات الفحص** Scan tools، و**أدوات المراقبة** Monitoring tools. تَتولَّى أدوات الحماية مهمَّة الحفاظ على أمان شبكة الحواسيب المتَّصلة بالإنترنت وجميع الشبكات الحاسوبيَّة التي تَربُط منشآت البنية التحتيَّة الحيويَّة، وأمّا أدوات الفحص فتَتولَّى مهمَّة فحص أنظمة الحواسيب المرتَبِطة ببعضها والتأكُّد من عدم وجود ثغرات قد تُؤدِّي إلى اختراق تلك الأنظمة الحاسوبيَّة، وأمّا أدوات المراقبة فتَتولَّى مراقبة حركة مرور البيانات الداخلة والخارجة من الشبكة الحاسوبيَّة الداخليَّة وإليها؛ للتأكُّد من عدم وجود أنشطة مشبوهة أو غير طبيعيَّة، وإنَّ أدوات الدفاع السايبري الثلاثة السابقة هي الأساسات التي تُبنَى عليها أي آلية دفاع سايبري، وهي المفاصل التي تَرتكِز عليها إستراتيجيَّات الدفاع السايبري.

أمّا أدوات الهجوم السايبري فتتألَّف من **أدوات الاختراق** Hacking tools، و**أدوات التعطيل** Disruption tools، و**أدوات التَجسُّس** Spy tools. تقوم أدوات الاختراق بعملية اختراق أنظمة حواسيب الطرف المستهدَف، ويَتم ذلك من خلال البحث عن ثغرات في شبكة حواسيب الطرف الهدف، وأمّا أدوات التعطيل فهي البرامج الصغيرة التي تُرسَل إلى شبكة حواسيب الطرف الهدف لكي تُسبِّب تخريبًا وأذى في أنظمة الحواسيب المتَّصلة بتلك الشبكة وفي كل ما يَتَّصل بها أيضًا من منشآت البنية التحتيَّة، وأمّا أدوات التَجسُّس فهي أخطر الأدوات التي يَستعملها الطرف المصدَر، والتي تقوم بعملية تسجيل جميع أنشطة أو معلومات وبيانات الطرف الهدف خفيةً، ومن ثم إرسالها إلى الطرف المصدَر.

تَختلِف صفات أدوات الدفاع السايبري عن صفات أدوات الهجوم السايبري، فمن الضروري امتلاك جميع أدوات الدفاع السايبري وتطبيقها معًا لكي تُحمَى البنية السايبريَّة لأي طرف. أمّا أدوات الهجوم السايبري فيُمكِن استعمال أي مجموعة منها (أو جميعها) لإطلاق هجوم سايبري، فمن المُمكِن لإطلاق هجوم سايبري أن تُستعمَل مثلًا أدوات الاختراق وحدها دون استعمال أدوات التعطيل أو أدوات التَجسُّس، وكذلك الأمر مع أدوات التعطيل وأدوات التَجسُّس.

الملحق (1)

قائمة بمعايير (مواصفات دولية) وبأفضل الممارسات في إدارة أمن المعلومات وأمانها

يمكن الوصول لتفاصيلها من الإنترنت

Short list of 20 standards and good practices that are in use in the EU

Telecommunications market:

1 ISO/IEC 27001/2

2 ISO/IEC 24762:2008 Guidelines for ICT and disaster recovery services

3 ISO/IEC 27005 Information security risk management

4 ISO/IEC 27011 Information security management guidelines for telecommunications

5 BSI BS25999_1 Business Continuity

6 ITU_T X.1051 (02/2008)

7 ITU_T X.1056 (01/2009)

8 ITU_T X.800 (1991)

9 ITU_T X.805 (10/2003)

10 ISF Standard of Good Practice 2007

11 CobiT

12 ITIL Service Support

13 ITIL Security Management

14 IT_Grundschutz_Kataloge

15 KATAKRI

16 NIST SP 800_34

17 NIST SP 800_61

18 FIPS_200

19 UK NICC Minimum Standard ND1643

20 PCI DSS 1.2

Source: The European Union Agency for Network and Information Security (ENISA): Shortlisting network and information security standards and good practices.

الملحق (2)

مستويات سرية المعلومات في النظام الأمريكي

1. Core secrets أسرار عظمى

The highest level of classification. Information at this level is released only to select government individuals (Used by the NSA exclusively).

2. Top Secret سري للغاية

The highest security level outside of the NSA framework. "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe. It is believed that 1.4 million Americans have top secret clearances.

3. Secret سري

This is the second-highest classification. Information is classified Secret when its unauthorized disclosure would cause "serious damage" to national security. Most information that is classified is held at the secret sensitivity.

4. Confidential مؤتمن – خاص

This is the lowest classification level of information obtained by the government. It is defined as information that would "damage" national security if publicly disclosed, again, without the proper authorization.

5. Unclassified (غير سري) متاح

الملحق (3)

مواقع إلكترونية مفيدة في أمن المعلومات

http://www.infosyssec.org/infosysec/index.htm

http://www.certicom.com

http://www.counterpane.com

http://www.cs.purdue.edu/coast/

http://www.sans.org

http://www.icsa.net/

http://www.itpolicy.gsa.gov

http://www.bs.org/

http://www.rsa.com

http://www.telstra.com.au/info/security.html

https://www.cisecurity.org/

https://www.sans.org/security_training/by_location/all

https://www.pcisecuritystandards.org/

https://www.enisa.europa.eu/

http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref2048

http://www.pwc.com/gx/en/issues/cyber_security/information_security_survey.html

الاتحادات والمنظمات المتخصصة في أمن المعلومات

ISSA: (www.issa.org)

مؤسسة SANS : (www.sans.org)

الاتحاد العالمي لحماية الحاسوب (International Computer Security Association)

ICSA: (www.icsa.net)

قائمة المصطلحات

تعمية	Cryptography
مُعمي (للأشخاص)	Cryptographer
نص واضح	Plaintext
نص مُعمَّى	Cipher text
رسالة مُعمَّاة	Cryptogram
مُعمي (من أصل عربي، وهي كلمة الصفر)	Cipher
خوارزمية التعمية	Cryptographic Algorithm
خطة التعمية	Cryptographic Scheme
مفتاح	Key
مفتاح تعموي	Cryptographic Key
عملية التعمية	Encryption
عملية فك التعمية	Decryption
تعمية	Encipherment
فك تعمية	Decipherment
يُعمِّي	Encrypt
يَفُك التعمية	Decrypt
يُعمِّي	Encipher
يَفُك التعمية	Decipher
نظام تعمية	Cryptosystem

فضاء النص الواضح	Plaintext Space
فضاء النص المُعمَّى	Ciphertext Space
فضاء المفتاح	Key Space
استخراج المعمى (كسر الشفرة)	Cryptanalysis
مستخرج التعمية أو كاسر للشفرة	Cryptanalyst
هجوم	Attack
افتضاح	Compromise
كسر التعمية	Breaking a cipher
علم التعمية واستخراجها	Cryptology
خبير التعمية واستخراجها	Cryptologist
مُرسِل	Sender
مُستقبِل	Receiver
خصم	Adversary
مُهاجِم	Attacker
مُعترِض	Interceptor
مُتطفِّل	Interloper
دخيل	Intruder
مُناوِئ	Opponent
عدو	Enemy
مُتجسِّس (مسترق)	Tapper
مُتنصِّت	Eavesdropper
سرِّية	Confidentiality
سرِّية	Secrecy
خصوصية	Privacy

سلامة البيانات	Data Integrity
استيقان طرف	Entity Authentication
إثبات هوية	Identification
استيقان مُتبادَل	Mutual Authentication
خوارزمية آمنة بلا قيد	Unconditionally Secure Algorithm
خوارزمية آمنة حسابيًّا	Computationally Secure Algorithm
سرِّية مثالية	Perfect Secrecy
خوارزمية قوية	Strong Algorithm
خوارزمية مقيَّدة	Restricted Algorithm
الأمن عبر التعتيم	Security Through Obscurity
بروتوكول تعموي	Cryptographic Protocol
هجوم سلبي	Passive Attack
تجسُّس (استراق)	Tapping
تحليل الحركة	Traffic Analysis
هجوم فعّال	Active Attack
غشّاش	Cheater
هجوم انتحال الشخصية	Impersonation Attack
تنكُّر	Masquerade
بروتوكول التحدي والرد	Challenge and Response Protocol
هجوم الشخص الذي في الوسط	Man in the Middle Attack
بروتوكول الضم	Interlock Protocol
هجوم إعادة التشغيل	Replay Attack
ختم زمني	Timestamp
هجوم الحرمان من الخدمة	Denial of Service Attack

هجوم النص المُعمَّى فقط	Ciphertext_only Attack
هجوم النص الواضح المعلوم	Known_plaintext Attack
هجوم النص الواضح المختار	Chosen_plaintext Attack
هجوم النص الواضح المختار المتكيِّف	Adaptive_chosen_plaintext Attack
هجوم النص المُعمَّى المختار	Chosen_ciphertext Attack
هجوم النص المختار	Chosen_text Attack
هجوم النص المُعمَّى المختار المتكيِّف	Adaptive_chosen_ciphertext Attack
تحليل التعمية باستعمال السوط	Rubber_hose Cryptanalysis
الهجوم بشراء المفتاح	Purshase_key Attack
النظام العشري	Decimal System
النظام الاثناني	Binary System
رقم اثناني	Binary Digit
بت	Bit
النظام الثماني	Octal System
رقم ثماني	Octal Digit
ثُمانية	Octet
النظام الست عشري	Hexadecimal System
رقم ست عشري	Hexit
نظام الترميز بالأساس 64	Radix64 Encoding System
عملية على مستوى البت	Bitwise Operation
بايت	Byte
رباعية	Nibble
ثنائية	Crumb
كلمة	Word

كلمة مضاعفة	Doubleword
كلمة رباعية	Quadword
بت أكثر دلالة	Most Significant Bit
بت أقل دلالة	Least Significant Bit
بت ندية	Parity Bit
بت ندية زوجي	Even Parity Bit
بت ندية فردي	Odd Parity Bit
نمط بيانات صحيحة معرَّفة	Defined Integral Data type
نمط بيانات صحيحة غير معرَّفة	Nondefined Integral Data Type
عدد صحيح مؤشَّر	Signed Integer
عدد صحيح غير مؤشَّر	Unsigned Integer
بت إشارة	Sign Bit
المعامِل المنطقي Not	Not
المعامِل المنطقي And	And
المعامِل المنطقي Or	Or
المعامِل المنطقي Xor أو عملية الجمع الاثناني	Xor
إزاحة بتات	Bit Shift
تدوير بتات	Bit Rotation
مُعمِّي كتلي	Block Cipher
تشويش	Confusion
نثر	Diffusion
تأثير الانهيار	Avalanche Effect
الكمالية	Completeness
معيار الانهيار الصارم	Strict Avalanche Criterion

معيار استقلال البت	Bit Independence Criterion
صندوق تعويض	Substitution Box
صندوق تعويض مثالي	Perfect S_box
صندوق تبديلة	Permutation Box
تبديلة الضغط	Compression Permutation
تبديلة التوسيع	Expansion Permutation
تبديلة صرفة	Straight Permutation
مَعمِّي مركَّب	Product Cipher
مرحلة	Round
تابع المرحلة	Round Function
مُعمِّي كتلي تكراري	Iterated Block Cipher
خوارزمية جدولة المفتاح	Key Schedule Algorithm
مفتاح رئيس	Main Key
مفتاح فرعي مرحلي	Round Subkey
توسيع مفتاح	Key Expansion
شبكة تعويض وتبديلة	Substitution_Permutation Network
نمط عملية	Mode of Operation
نمط جدول الترميز الإلكتروني	(Electronic Codebook Mode (ECB
نمط سلسلة الكتل المُعمَّاة	(Cipher Block Chaining Mode (CBC
نمط التغذية الخلفية بالنص المعمَّى	(Cipher Feedback Mode (CFB
نمط التغذية الخلفية بالخرج	(Output Feedback Mode (OFB
نمط العداد	(Counter Mode (CTR
حشو	Padding
استعارة النص المعمَّى	Ciphertext Stealing

قيمة ابتدائية	Initialization Vector
انتشار الخطأ	Error Propagation
نمط سلسلة الكتل	Block Chaining Mode (BC)
قيَم اختبار	Test Vectors
مقاطعة مفتاح	Key Interruption
تحليل التعمية التفاضلي	Differential Cryptanalysis
تحليل التعمية الخطي	Linear Cryptanalysis
مفتاح ضعيف	Weak Key
مفتاح شبه ضعيف	Semi-weak Key
مفتاح محتمَل أن يكون ضعيفًا	Possibly Weak Key
مُعمِّي تسلسلي	Stream Cipher
سلسلة مفتاحية	Keystream
بذرة	Seed
مولِّد السلسلة المفتاحية	Keystream Generator
مولِّد المفتاح الجاري	Running Key Generator
مُعمِّي تسلسلي متزامن	Synchronous Stream Cipher
مُعمِّي تسلسلي ذاتي التزامن	Self-synchronizing Stream Cipher
التعقيد الخطي	Linear Complexity
مولِّد بتات	Bit Generator
مولِّد بتات عشوائية	Random Bit Generator (RBG)
مولِّد بتات شبه عشوائية	Pseudorandom Bit Generator (PRBG)
تابع البصمة	Hash Function
تابع الضغط	Compression Function
تابع التقليص	Contraction Function

ترميز البصمة	Hash Code
نتيجة البصمة	Hash Result
قيمة البصمة	Hash Value
دمغة	Imprint
بصمة رقمية	Digital Fingerprint
خلاصة الرسالة	Message Digest
بصمة	Hash
تابع بصمة غير مزوَّد بمفتاح	Unkeyed Hash Function
تابع بصمة مزوَّد بمفتاح	Keyed Hash Function
ترميز اكتشاف التعديل	(Modification Detection Code (MDC
ترميز اكتشاف التلاعب	Manipulation Detection Code
ترميز سلامة الرسالة	(Message Integrity Code (MIC
ترميز استيقان الرسالة	(Message Authentication Code (MAC
ترميز استيقان البيانات	(Data Authentication Code (DAC
صورة أمامية	Preimage
تابع بصمة وحيد الاتجاه	(One way Hash Function (OWHF
تابع بصمة مقاوِم التصادم	Collision Resistant Hash Function ((CRHF
مقاوَمة إيجاد الصورة الأمامية	Preimage Resistance
مقاوَمة إيجاد الصورة الأمامية الثانية	2nd Preimage Resistance
مقاوَمة التصادم	Collision Resistance
تابع بصمة ذو مقاوَمة ضعيفة للتصادم	Weak Collision Resistant Hash Function
تابع بصمة ذو مقاوَمة قوية للتصادم	Strong Collision Resistant Hash Function
تابع بصمة وحيد الاتجاه الضعيف	Weak One Way Hash Function

تابع بصمة وحيد الاتجاه القوي	Strong One Way Hash Function
قيمة الـــMAC	MAC Value
مقاوَمة الحساب	Computation Resistance
تابع وحيد الاتجاه	One_Way Function
تابع وحيد الاتجاه ذو باب خلفي	Trapdoor WOF
تقوية MD	MD_strengthening
MDC ذو طول بصمة أحادي	Single_length MDC
MDC ذو طول بصمة ثنائي	Double_length MDC
هجوم يوم الميلاد	Birthday Attack

المراجع

1. "About: What is Wikileaks?." WikiLeaks. 10 July 2014 <https://wikileaks.org/About.html>.
2. Andress, Jason. The Basics Of Information Security: Understanding the Fundamentals Of InfoSec in Theory and Practice. Massachusetts: Syngress Press, 2011.
3. Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition, John Wiley & Sons, 1996.
4. "Children's Internet Protection Act." FCC. 27 July 2014 <http://www.fcc.gov/guides/childrens_internet_protection_act>.
5. "COPPA – Children's Online Privacy Protection Act." COPPA. 27 July 2014 <http://www.coppa.org/coppa.htm>.
6. Data Encryption Standard (DES), FIPS PUB 46_3. Washington, D.C.: US Department of Commerce/National Institute of Standards and Technology, 25 Oct. 1999.
7. "Data vs. Information." Diffen. 16 May 2014 <http://www.diffen.com/difference/Data_vs_Information>.

"Difference between Data and Information." *Difference Between – Know and Clarify yourself.* 16 May 2014 <http://www.differencebetween.info/difference_between_data_and_information>.

"Edward Snowden." *Biography.* 10 July 2014 <http://www.biography.com/people/edward_snowden_21262897>.

Presidential Documents. *Executive Order 13526 of December 29, 2009: Classified National Security Information.* Washington, D.C.: Federal Register, vol. 75, no. 2, 5 Jan. 2010: 707_731.

Gattiker, Urs. E, *The Information Security Dictionary.* Kluwer Academic Publishers, 2004.

HMG Security Policy Framework. London: Cabinet Office, ver. 11.0, October 2013.

Peltier, Thomas R., Peltier, Justin, and Blackley, John. *Information Security Fundamentals*. Boca Raton: CRC Press LLC, 2005.

Quist, Arvin S. "Security Classification of Information: Volume 2. Principles for Classification of Information." *Federation of American Scientists*. Apr. 1993. 9 Mar. 2014 <http://www.fas.org/sgp/library/quist2/chap_8.html>.

Schneier, Bruce. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. New York: John Wiley & Sons, Inc., 2nd edition 1996.

Security Within The North Atlantic Treaty Organization (NATO), NATO Unclassified. North Atlantic Council, Document C-M (2002) 49, 17 June 2002.

Solomon, Michael G. and Chapple, Mike. *Information Security Illuminated*. Boston: Jones & Bartlett, 2005.

State Secrets: China's Legal Labyrinth. New York: Human Rights in China (HRIC), 2007.

Stewart, James M., Tittel, Ed, and Chapple, Mike. *CISSP: Certified Information Systems Security Professional, Study Guide*. Alameda: SYBEX Inc., 3rd edition 2005.

"The Convention." *CRIN*. 24 July 2014 <https://www.crin.org/en/home/rights/convention>.

Winkler, Ira. *Zen and the Art of Information Security*. Rockland: Syngress, 2007.

H. X. Mel, Doris M. Baker, "Cryptography Decrypted, «Addison Wesley, 2001.

Ronald L. Rivest and Adi Shamir, How to Expose an Eavesdropper, Communications of ACM, 1984.

Microsoft Safety &security center http://www.microsoft.com/security/default.aspx .

William Stallings, Cryptography and Network Security: Principles and Practice, Second Edition, Prentice Hall, 1999.

http://www.ourwatch.org.uk/safety_advice/mobile_internet_and_identity_safety .

8. Andress, Jason and Winterfeld, Steve. Cyber Warfare: Technics, Tactics and Tools for Security Practitioners. Massachusetts: Syngress Press, 2011.
9. "Cyberwar." The RAND Corporation. 16 February 2015 <http://www.rand.org/topics/cyberwar.html>.
10. "Cyberwar." Oxford Dictionaries. 16 February 2015 <http://www.oxforddictionaries.com/definition/english/cyberwar>.
11. "Latest viruses could mean 'end of world as we know it, 'says man who discovered Flame." The Times of Israel. 16 February 2015 <http://www.timesofisrael.com/experts_we_lost_the_cyber_war_now_were_in_the_era_of_cyber_terror>.

12. "U.S. Cyber Command." U.S. Strategic Command. 22 February 2015 <http://www.stratcom.mil/factsheets/2/Cyber_Command>.

13. "Aman's Cyber Consulting Services – Protect your organization from advanced cyber-attacks." Aman. 22 February 2015 <http://www.aman.co.il/englishsite/about/services/cyber_security.aspx>.

14. "Cyber-attacks a bigger threat than Al Qaeda, officials say." Los Angeles Times. 22 February 2015 <http://articles.latimes.com/2013/mar/12/world/la-fg-worldwide-threats-20130313>.

15. "Obama Order Sped Up wave of Cyberattacks against Iran." The New York Times. 22 February 2015 <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0>.

16. "S. Korean military to prepare with U.S. for cyber warfare scenarios." Yonhap News Agency. 22 February 2015 <http://english.yonhapnews.co.kr/national/2013/04/01/20/0301000000AEN20130401004000315F.HTML>.

17. "Germany to invest 100 million euros on internet surveillance: report." Kazinform. 22 February 2015 <http://www.inform.kz/eng/article/2567203>.

18. "South Korea raises alert after hackers attack broadcasters, banks." global post. 22 February 2015 <http://www.globalpost.com/dispatch/news/thomson-reuters/130320/south-korea-police-investigating-server-outages-at-major-tv-net>.

19. "The Real Story of Stuxnet." IEEE Sprectrum. 23 February 2015 <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>.

20. "Centre of Excellence for Cyber Security Research and Development in India (CECSRDI)." PERRY4LAW Organization. 23 February 2015 <http://perry4law.org/cecsrdi/?p=735>.

21. Fritz, Jason, How China will use cyber warfare to leapfrog in military competitiveness. Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies: Vol. 8: Iss. 1, Article 2. 2008.

22. "Hundreds of ISIS social media accounts shut down." CNN Money. 23 February 2015 <http://money.cnn.com/2015/02/10/technology/anonymous-isis-hack-twitter>.

23. Even, Shmuel, and Siman-Tov, David, Cyber Warfare: Concepts and Strategic Trends. Tel Aviv: The Institute for National Security Studies, 2012.

24. "Cybercrime." Techopedia. 2 March 2015 <http://www.techopedia.com/definition/2387/cybercrime>.

25. Rouse, Margaret. "Cybercrime." TechTarget. 2 March 2015 <http://searchsecurity.techtarget.com/definition/cybercrime>.

26. Sandle, Paul. "Cybercrime costs global economy $445 billion a year: report." Reuters. 2 March 2015 <http://www.reuters.com/article/2014/06/09/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609>.

27. T. Rasmussen, Gideon. "Cyberwar- A Threat to Business." Gedion T. Rasmussen. 4 March 2015 <http://www.gideonrasmussen.com/article-14.html>.

28. Barker, Ian. "How US organizations are losing the cyberwar." Betanews. 4 March 2015 <http://betanews.com/2014/10/07/how-us-organizations-are-losing-the-cyber-war/>.

29. Siciliano, Robert. "In Business, the Cyber war Between the U.S. and China and Russia Is Tense." Entrepreneur. 4 March 2015 <http://www.entrepreneur.com/article/238411>.

30. "Why Syria's Air Defenses Failed to Detect Israelis." IMRA. 4 March 2015 <http://www.imra.org.il/story.php3?id=36291>.

31. "36 governments sites hacked by Indian Cyber Army." Tribune. 5 March 2015 <http://tribune.com.pk/story/83967/36-government-websites-hacked-by-indian-cyber-army>.

32. ISO/IEC 27001, Information technology- Security techniques - Information Security Management Systems (ISMS)- Requirements, 2005, 34.

33. ISO/IEC 27002, or BS 17799, Information technology - Security techniques- Code of practice for information security management, 2005, 115.

34. Mobile, internet & identity safety,

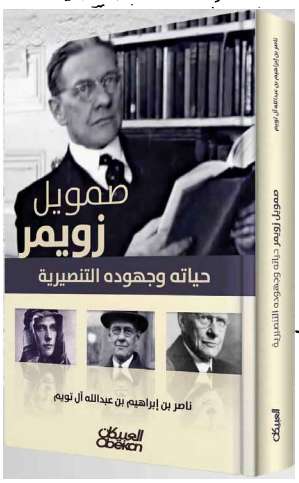
مراجع

1. لورنس إم. أوليفا، (أمن تقنية المعلومات نصائح من خبراء) ترجمة د. محمد مراياتي، سلسلة ترجمة كتب بإشراف مدينة الملك عبدالعزيز للعلوم والتقنية والمنظمة العربية للترجمة.
2. مراياتي، مير علم، طيان (علم التعمية واستخراج المُعَمَّى عند العرب) الجزء الأول، مطبوعات مجمع اللغة العربية بدمشق، 1987م.
3. محمد مراياتي، يحيى مير علم، حسان الطيان، (علم التعمية واستخراج المعمى عند العرب، الجزء الثاني، دراسة وتحقيق لثماني رسائل مخطوطة)، منشورات مجمع اللغة العربية، دمشق، 1997م.
4. مراياتي، مير علم، طيان (أصالة العرب في علم التعمية واستخراج المُعَمَّى)، ندوة التراث العلمي العربي للعلوم الأساسية، طرابلس، ليبيا، 1990م.

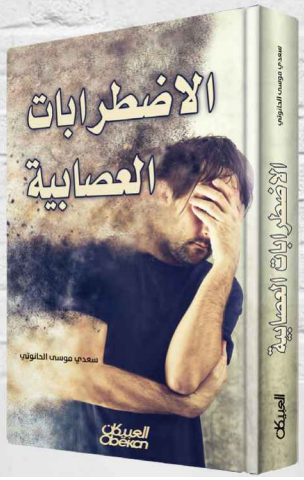
1. 2013 US State of cybercrime Survey.
2. PWC, "The Global State of Information Security Survey 2014".
3. Homeland Security, Cyber Security Publications at :http://www.dhs.gov/cybersecurity publications
4. Homeland Security, Critical Infrastructure Security at: http://www.dhs.gov/topic/critical-infrastructure-security

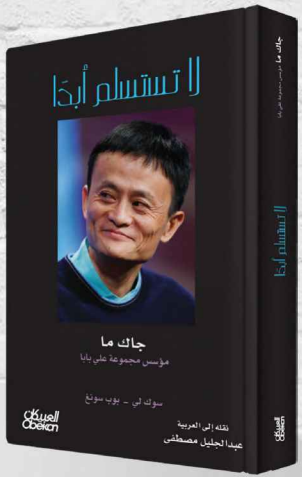
5. ENISA : The European Union Agency for Network and Information Security , publications .
6. GSMA, "The Mobile Economy 2014 Report , The Arab States" , https:// gsmaintelligence.com/research/
7. The International Society of Security Awareness Professionals http://www. iasapgroup.org/
8. Rebecca Herold, "Managing an Information Security and Privacy Awareness and Program and Training Program", CRC 2011
9. Maurice Dawson, University of Missouri – St. Louis, USA; Marwan Omar, Nawroz University, Iraq; Jonathan Abramson, Colorado Technical University, USA; Dustin Bessette, National Graduate School of Quality Management, USA. 2014.
10. IT Security, Threats and Data Breaches, Perception versus Reality: Time to Recalibrate. Empower business through security. ISTR report. kaspersky.com/ business.

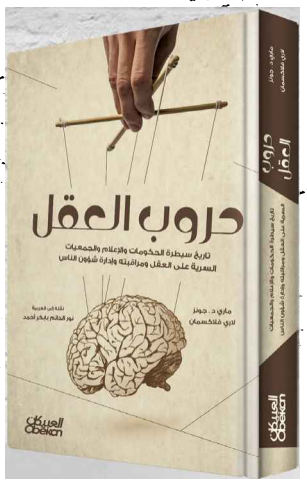
أحدث الإصدارات

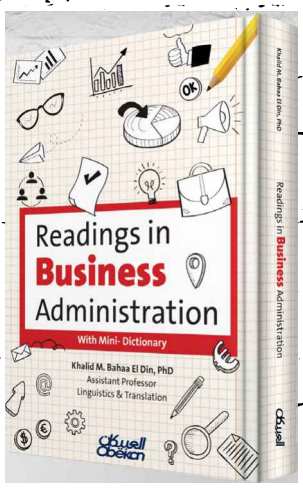


أحدث الإصدارات

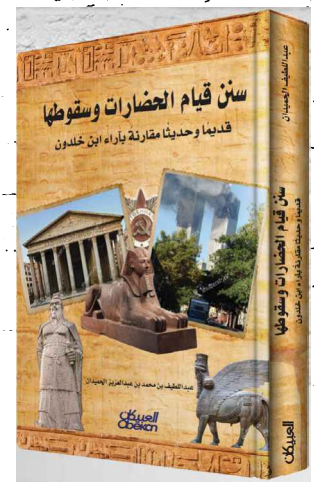








أحدث الإصدارات



أحدث الإصدارات