أمن المعلومات وحماية البنيات التحتية الأساسية والإتصالات

الصادق سعيد جبريل

أمن المعلومات وحماية البنيات التحتية الأساسية والاتصالات

الصادق سعيد جبريل

2013م

فهرسة المكتبة الوطنية أثناء النشر-السودان

005,8 الصادق سعيد جبريل 1977-

ص.أ

أمن المعلومات وحماية البنيات التحتية الأساسية والإتصالات

الصادق سعيد جبريل حامد-الخرطوم: ص.س , 2013م

248 ص:ايض, 24سم

ردمك 978-99942-75-93-9

1. أمن المعلومات
2. أمن الحاسبات الإلكترونية
3. أمن المعلومات

أ. العنوان

بسم الله الرحمن الرحيم

المقدمة

الحمد لله الذي بنعمته تتم الصالحات وأُصلي وأُسلم على سيدنا محمد (صلى الله عليه وسلم) وعلى آله وأصحابه والتابعين.

شهدت نهاية القرن العشرين وبداية القرن الحادي والعشرين تطوراً سريعاً لتكنولوجيا الاتصالات والمعلومات حتى بالكاد لا تجد دولة في العالم لا تعتمد على هذه التكنولوجيا في تطوير اقتصادها القومي وزيادة الإنتاجية وتنمية الموارد البشرية. فالمعلومات والاتصالات أصبحت كل شيء في حياة البشرية في عالم اليوم. على الرغم من الفوائد التي لا تحصى لهذه التكنولوجيا، إلا أن هنالك جوانب سالبة، تتمثل في الاستخدام السيِّئ لها لتحقيق الإضرار الاقتصادي أو الاجتماعي بالأفراد والجماعات والمنظمات والدول.

هذا الكتاب "أمن المعلومات وحماية البنيات التحتية الأساسية والاتصالات"، يناقش المهددات الأساسية لنظم الاتصالات والمعلومات والبنيات التحتية الحرجة المعتمدة على هذه النظم، ويحاول أن يلخص بعض المعالم الأساسية للتجربة البشرية في مجال حماية هذه النظم من المخاطر.

الفصل الأول من الكتاب يُناقش العوامل التقنية الأساسية التي ساعدت في تطور قطاع المعلوماتية والاتصالات، ويُعرّف بالمكونات الأساسية لنظم الاتصالات والطرق المختلفة لتخزين وإرسال البيانات، بالإضافة إلى المبادئ الأساسية في تصميم النظم، والتي يُعتقد على نطاق واسع أنها ساعدت بشكل كبير في عملية التطور والانتشار السريع لشبكات الاتصالات والإنترنت. الفصل الثاني يتعرض وبصورة مختصرة وشاملة؛ للمهددات والمخاطر التي يمكن أن تتعرض لها هذه النظم. نسبةً لاعتماد الكثير من جوانب الحياة اليومية والمكتبية والأنشطة الاقتصادية في عالم اليوم على المعلوماتية والاتصالات؛ لذلك يجب أن يكون في كل منظمة أو

مؤسسة إدارة متخصصة لأمن المعلومات وعلى رأسها شخص بمسمى مدير أمن المعلومات. هذه الإدارة والوظيفة الجديدة مُهمَّتُها في الأساس هي تلبية المتطلبات والاحتياجات اليومية المتزايدة للمعلوماتية والتخطيط للكوارث والجرائم والطوارئ بمفهومها الجديد. الفصل الثالث من الكتاب يستعرض المهام الأساسية والمسار المهني لمدير أمن المعلومات في المنظمة أو المؤسسة. الفصل الرابع يناقش المتطلبات الخاصة بعملية التخطيط لبناء الإطار العملي والقانوني لإدارة أمن المعلومات في المنظمة أو المؤسسة. الفصل الخامس يسرد ويُعرّف ببعض الوسائل التقنية التي يمكن أن تُستخدم لحماية فضاء المعلوماتية والاتصالات. الفصل السادس يناقش واجبات الدولة في عملية بناء الإطار القانوني للتحقيق في الجرائم المتصلة بقطاع المعلوماتية والاتصالات، وفي إصدار اللوائح والموجهات العامة التي يجب أن تلتزم بها المؤسسات في القطاعين العام والخاص لحماية هذه النظم.

الفصل السابع يسلط الضوء على بعض المشكلات المرتبطة بمواقع التواصل الاجتماعي (الجرائم، التحيُز السياسي، الاستخدام السالب لهذه الأدوات من قبل بعض أنظمة الحكم والجماعات السياسية المعادية لها). أيضاً يناقش هذا الفصل مشكلة النفاذ غير الآمن للأطفال على الإنترنت، ويقدم قائمة لبعض نُظم التحكم الأبوي، التي يمكن أن يستخدمها الآباء والمدرسون والمربون لمعرفة سلوكيات الأطفال على الإنترنت لمحاولة تقويمها. الفصل الثامن يتحدث عن دور الاتحاد الدولي للاتصالات والمنظمات المتحالفة معه في عملية حماية البنيات التحتية الحرجة للمعلوماتية والاتصالات. ويشرح الفصل مجهودات الاتحاد الدولي للاتصالات من خلال عرض وشرح الأجندة الدولية للاتحاد لحماية المعلوماتية والمشاريع المختلفة للاتحاد بهذا الخصوص. الفصول من التاسع وحتى الخامس عشر؛ تُلخص تجارب بعض الدول المتقدمة والطموحة في مجال حماية البنيات التحتية الأساسية والاتصالات. لقد شمل المسح كلاً من دولة قطر وأستراليا وماليزيا والولايات المتحدة والمملكة المتحدة واليابان، بالإضافة إلى مجموعة الاتحاد الأوروبي. لتلخيص تجربة كل دولة، تم التركيز في المسح على إعطاء مقدمة عامة توضح مدى اعتمادية الدولة على بنيات

المعلوماتية والاتصالات والخطط المستقبلية، ثم معرفة البنيات الحرجة المُعتمدة بواسطة الجهات التنفيذية في الدولة، ومعرفة الجهود المبذولة والمؤسسات القائمة على حماية المعلوماتية. بالإضافة إلى هذه العناصر، أيضاً شمل المسح التعرّف على المؤسسات المنوط بها تقديم خدمة الإنذار المبكر بالجرائم والمهددات، والجهود المبذولة بشأن حماية الأطفال عند النفاذ، والقوانين والتشريعات في مجال حل المنازعات المتصلة بالمعلوماتية والاتصالات. الفصل السادس عشر يلخص أهم الواجبات التي يجب على الجميع القيام بها لمواكبة عجلة التكنولوجيا في هذا المجال.

الكتاب لا يعتبر مرجعاً شاملاً في مجال حماية البنيات التحتية الحرجة للمعلوماتية والاتصالات؛ بل هو محاولة فردية لعرض ما يدور في هذا المجال. أيضاً يُمكن أن يُنظر إليه على أنه دعوة مفتوحة للمهتمين للولوج إلى الموضوعات وبصورة تفصيلية، وذلك باستخدام قائمة المراجع الأجنبية المُرفقة في نهاية هذا الكتاب. كثير من الموضوعات التي تم شرحها بصورة مبسطة هي في الأساس عبارة عن قوانين أو موجهات أو سياسات ومراجع أو موضوعات مُستحدثة تصلح أن تكون مجالاً مكتملاً للبحث العلمي والابتكار في المستقبل. في هذا الخصوص أيضاً يمكن أن يُنظر للكتاب على أنه فهرس وقائمة بالموضوعات المختلفة في هذا المجال، حيث يحتوي في هذا الخصوص على قائمة بأكثر من 200 مرجع أجنبي، وعلى عدد مقدّر من العناوين للمواقع التي تحتوي على أفكار ومواد تعليمية وإرشادية قيّمة، يمكن أن يستفيد منها القارئ في تقديرنا.

في الختام نشكر كل من ساهم في إتمام هذا العمل، ونخص بالشكر المهندسين: منير الصديق الفكي علي، عمر علي عمر حسن، ياسر عثمان، ومحمد حسين؛ وكل الإخوة والأخوات. كما يسعدنا استقبال مقترحاتكم على البريد الالكترونى للكتاب infosec014@gmail.com.

المحتويات

الفصل الأول

نبذة عن التطور التقنى لنظم الاتصالات والمعلومات

1.1 المقدمة

فيما لا شك فيه أن من أهم التطورات في نهاية القرن العشرين وبداية القرن الحادي والعشرين، هو التسارع في صناعة نظم الاتصالات والمعلومات والتي تم استخدامها وعلى نطاق وآسع في كل الأنشطة البشرية. قبل أن نُدلف إلى الجوانب الإيجابية والسلبية والمخاطر التي يمكن أن يتعرض لها الإنسان بصورة عامة عند استخدام هذه التكنولوجيا؛ نبدأ في هذا الفصل بمقدمة تعريفية بسيطة، نلخصُ فيها وبصورة مختصرة، بدايات هذا التطور، ونُعرّف بالعناصر الأساسية لهذه التكنولوجيا. في هذا الفصل نبدأ بمناقشة العوامل الأساسية التي ساعدت في عملية تطور نظم الاتصالات والمعلومات في الفقرة 2.1، ثم نعرّف نظم الاتصالات السلكية واللاسلكية في الفقرات 3.1 و4.1 على التوالي. في الفقرة 5.1 نُعرف علاقة التماثل بين عمليات الإرسال والتخزين؛ وفي الفقرة 6.1 نناقش متطلبات بناء مركز المعلومات Data Center ثم نتعرض لعملية تصميم نظم الاتصالات والمعلومات، بالاعتماد على الطبقات في الفقرة 7.1. وفي الفقرة 8.1 نُلخص وبصورة مختصرة مسيرة تطور شبكة الإنترنت.

2.1 الجوانب التقنية الأساسية التى ساعدت في تطور نظم الاتصالات والمعلومات

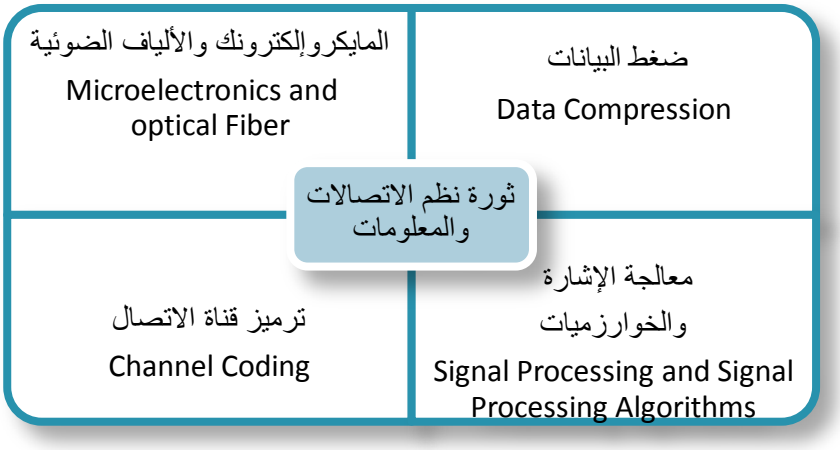
كتب كل من إدوارد أي لي (Edward A. Lee) وديفد جي مسار إشمت (David G. Messerschmit) من جامعة كلفورنيا بيركلي في افتتاحية كتابهما المشهور "الاتصالات الرقمية [1] Digital Communication" الطبعة الأولى في 1988م، فيما يمكن ترجمته إلى ما يلي:

> "لماذا نرسل إشارات الصوت والصورة بشكل رقمي؟ أليس في هذا ضياع لعرض النطاق؟!... وأن قيمة المُدوم الرقمي تساوي عشرة أضعاف قيمة المُدم العادي؟"

في مقدمة الطبعة الثانية [2] لنفس الكتاب، والتي تم نشرها في سنة 1994م، تم تغيير الجملة الافتتاحية إلى ما يمكن ترجمته إلى الآتي:

"... لفترة ليست ببعيدة، كان يُعتقد وعلى نطاق واسع، أن عملية إرسال الإشارة الصوتية وإشارة الصورة بشكل رقمي ضياع لعرض النطاق الترددي!.... حديثاً تغيرت هذه الفكرة، أو بالأحرى فإن كل نظم الاتصالات في عالم اليوم، متجهة وبسرعة لاستخدام الإرسال الرقمي."

هذا التغير الكبير في الجملة الافتتاحية إلى النقيض في المعنى من باحثين في فترة وجيزة (6 سنوات)؛ يعكس مدى التطور السريع الذي شهده هذا المجال في العقدين الأخيرين. في هذه الفترة الوجيزة تغيرت أُسُس ومعايير تصميم نظم إرسال الصوت والصورة من استخدام التكنولوجيا التماثلية إلى استخدام التكنولوجيا الرقمية. يعود هذا التقدم المذهل في الأساس إلى التطور السريع في البحث العلمي في المجالات الأساسية التي تشكل الأضلاع والركائز المهمة لثورة الاتصالات والمعلومات التي شهدها القرن العشرون والتي يوضحها الشكل 1.1.



الشكل 1.1: يوضح التطور فى المجالات الرئيسية التي ساهمت فى تقدم ثورة الاتصالات والمعلومات.

إذا أخذنا فقط عنصر عملية ضغط البيانات، نجد أنه أسهم إسهاماً فعالاً في زيادة وتحسين معامل كفاءة عرض النطاق Bandwidth Efficiency في نظم الاتصالات، وتقليل المساحة المطلوبة لحفظ البيانات في عملية التخزين. على سبيل المثال في حالة الإرسال التلفزيوني: قديماً كان عرض النطاق بالنسبة للقمر الصناعي المحدد بسعة قدرها 500 ميغا هيرتر يسع فقط لعدد 32 قناة تلفزيونية. في عالم اليوم وبفضل تقدم تكنولوجيا ضغط البيانات Data Compression، أصبح بالإمكان إرسال أكثر من عشرة أضعاف هذا العدد من القنوات على نفس عرض النطاق الثابت للقمر الصناعي. بما أن عملية ضغط البيانات وعملية فك شفرتها وإعادتها إلى وضعها الأول يحتاج إلى معالجة حاسوبية فائقة السرعة والدقة؛ في الجانب الآخر نجد أن التطور في أبحاث مجالات الميكروإلكترونك ومعالجات الإشارة والتقنيات الضوئية أسهم في توافر هذه المعالجات والتقنيات الفائقة السرعة، وبأسعار معقولة في متناول يد الباحث والمصمم والمستخدم النهائي للتكنولوجيا.

الأمر الآخر والذي له أيضاً علاقة مباشرة بمعالجة الإشارة والميكروإلكترونك؛ هو عملية الترميز من أجل اكتشاف الأخطاء في عملية إرسال البيانات في قناة الاتصال. هذه العملية تقتضي إضافة بيانات إضافية للمعلومات قبل عملية الإرسال، وذلك من أجل أن يتمكن نظام الاستقبال من اكتشاف الأخطاء التي يمكن أن تحدث في قناة الاتصال أثناء عملية نقل البيانات. نعود لنقول إن التطور في صناعة المعالجات وعلم الخوارزميات، كان لهما أيضاً الدور الريادي في تطور عملية الترميز.

قد يبدو للقارئ أن قصة تطور أيٍّ مجال من المجالات الأربعة السابقة مستقلة عن المجال الآخر، بينما الحقيقة تقول بغير ذلك، فقصة ازدهار أي مجال تحتوي بداخلها بعض تفاصيل ما يحدث في المجال الآخر، وهذا شأن كل العلوم الحديثة في عالم اليوم. فالتطور في مجال تصميم الخوارزميات ومعالجات الإشارة، أدى بصورة غير مباشرة إلى التطور في مجال تصميم خوارزميات ضغط البيانات. من جهةٍ أخرى؛ فإن التطور في صناعة المايكروإلكترونك، أسهم وبصورة فعالة في تدنى أسعار وحدات المعالجة الرقمية، مما سهَّل بدوره في التطور في مجال الترميز وزيادة سرعة

وحدات ضغط البيانات. فوق كل ذلك يمكن القول بأن التقدم التكنولوجي في هذه المجالات، لم يؤدِّ إلى الثورة والتقدم، وفي مجالات الاتصالات وتكنولوجيا المعلومات فقط؛ بل كان له الأثر الكبير في صياغة وتشكيل كل ما تم إنجازه من تقدم في نهاية القرن العشرين وبداية القرن الحادي والعشرين. فتكنولوجيا الميكروإلكترونك ومعالجات الإشارة والصورة، أُستخدمت في جميع المجالات الهندسية والصناعية والطبية والزراعية. بالتحديد يمكن أن نذكر عدداً من هذه المجالات فيما يلي:

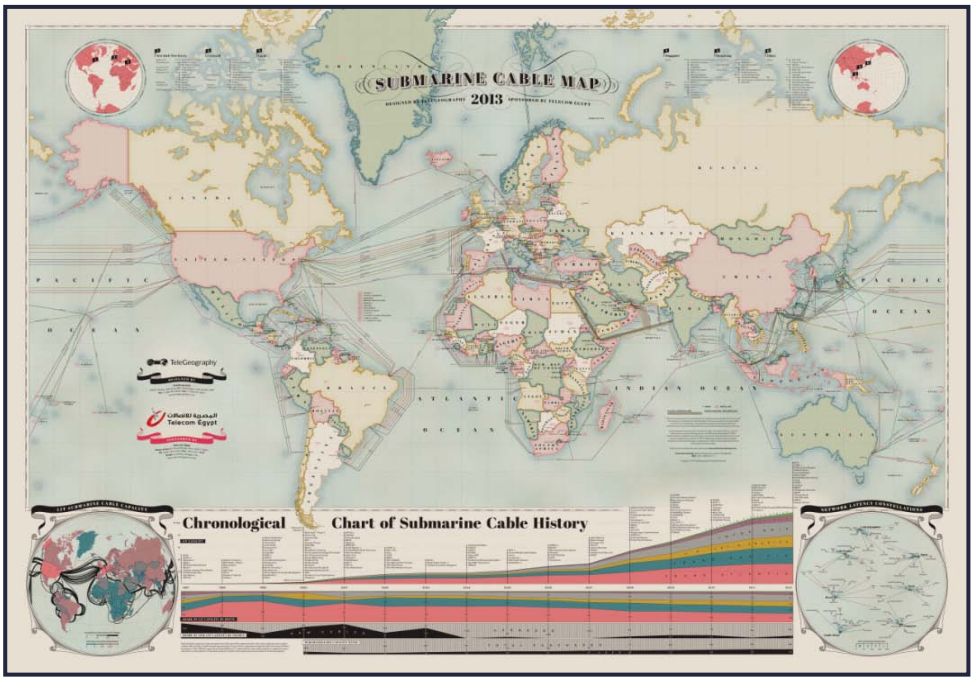
- مجالات الطب والهندسة الحيوية الطبية (الطب التشخيصي والطب العلاجي).
- مجالات الصناعة (الاختبارات بواسطة مقارنة الصورة والصوت).
- اختبارات المباني والأصول المدنية باستخدام التصوير والتكبير والحوسبة.
- استكشاف واستغلال الثروات الطبيعية والمعادن باستخدام تكنولوجيا الاتصالات ونظم التحكم.
- التطبيقات الأمنية ومنع الجرائم (مراقبة الشوارع والأماكن الإستراتيجية).
- التطبيقات الدفاعية (دقة التصويب، الاستكشاف بواسطة الرادارات).
- الأبحاث العلمية (القياسات، التحكم، الحوسبة والتحليل).
- زيادة كفاءة تشغيل العمليات الصناعية (نظم تشغيل الكهرباء ومراقبة العمليات الصناعية).
- قياس الجو والطقس والإنذار المبكر (كما في حالات الزلازل والفيضانات).
- اختبارات الجودة وتحديد المكونات والمواد الفعالة (استخدام محللات فورايرللقياسFourier Transform Infra-red Spectroscopy).
- ...إلخ

3.1 تطور الاتصالات السلكية

في شهر مارس من العام 1876م وبعمر29 سنة؛ تمكن العالم جرهام بيل من وضع الأُسس الأولية للاتصالات التلفونية باختراع جهاز التلفون (الهاتف الثابت) [3]. منذ ذلك التاريخ عرفت البشرية الاتصالات التلفونية، والتي مرّت بعد ذلك بعدة مراحل، أهمها الانتشار الواسع النطاق في الخمسينيات والستينيات من القرن العشرين. في هذه الفترة تم استخدام شبكة الهاتف كوسيلة للاتصال في كل الأغراض والنشاطات الإنسانية (الاقتصادية والاجتماعية والسياسية ...إلخ)، حيث عبرت الكيبلات التي تحمل الإشارات التلفونية الصحاري والمحيطات وأُستخدمت الوسائل المتطورة للتراسل الهاتفي مثل قنوات الأقمار الصناعية ونظم المايكروويف الأرضية. في العام 1977م بدأ العالم يستخدم الألياف البصرية بصورة محدودة، ولكن ما إن حل العام 1988م، حتى تم استخدامها في أول عملية ربط قاري بين القارة الأُوروبية والولايات المتحدة، بمسافة تقدر 150،3 ميلاً وبسعة تقارب 39000 مكالمة هاتفية، في آن واحد [4] [5]. من الناحية العملية وعلى نطاق واسع تعتبر بداية استخدام الألياف الضوئية، هي بداية المولد الحقيقي لعصر المعلوماتية والاتصالات الذي نعيش تفاصيله اليوم.

يمكن تلخيص أهم العوامل الأساسية التي أسهمت في تطور الاتصالات التلفونية ونقل البيانات والإنترنت في العقدين الأخيرين، في الانتشار الواسع للألياف البصرية (كيبلات الألياف الضوئية)، إذ ساعد التقدم المذهل في البحث العلمي على زيادة سرعة الإرسال عبر هذا الوسط، والذي لا يكاد يخلو من الكثير من التعقيدات التقنية المصاحبة لوسائط نقل البيانات الأُخرى. منذ الأيام الأُولى لاستخدام الألياف الضوئية وإلى يومنا هذا، هنالك دوماً زيادة متطردة في سعة الإرسال القصوى لهذا الوسيط في كل عام، وذلك بفضل التقدم في البحث العلمي والابتكار في هذا المجال. فمثلا حديثاً وبفضل ابتكار طرق حديثة لتعديل وتضمين البيانات، تمكن العلماء من الناحية المعملية من إرسال ما يعادل 1.05 بيتا بت في الثانية (Petabits/sec) [6] في نفس الوقت عبر الشُّعيرة الواحدة للألياف البصرية (1.05x10^15بت في الثانية)، أي ما

يعادل سعة حوالي 16مليار دائرة هاتفية (أيْ أن الشُعيرة الواحدة للألياف البصرية يمكن أن تحمل مكالمات لضعف عدد سكان الكرة الأرضية في آنٍ واحد). اليوم ومع تقدم التكنولوجيا لم تمتد شبكات الألياف البصرية لتغطي المساحات الشاسعة من الأراضي اليابسة للدول فقط!، بل امتدت بصورة شاسعة لتغطي المياه الدولية والإقليمية والمحيطات لتوفير الربط البيني بين جميع القارات والأقاليم الدولية والدول مع بعضها، كما هو موضح في الشكل 2.1، والذي وهو عبارة عن خارطة حديثة توضح مسارات الكوابل البحرية للألياف البصرية حول العالم.



الشكل 2.1: خارطة حديثة توضح مسار الكيبلات البحرية للألياف البصرية التي تربط بين القارات والأقاليم والدول المختلفة. الخريطة من موقع (www.TeleGeography.com)TeleGeography

4.1 تطور الاتصالات اللاسلكية

شهدت أنظمة الاتصالات اللاسلكية تطوراً ملحوظاً في القرن الماضي، وبمعدل نمو استثنائي في العقدين الأخيرين منه. يمكن إسناد بداية معرفة الإنسان بالاتصالات

اللاسلكية إلى أوائل أيام الثورة الصناعية، عندما قام العالم ماركوني بأول عملية إرسال لاسلكية لنقل الإشارة الصوتية في عام 1895م. في بدايات القرن العشرين، أسهمت كثير من العوامل الفنية والتقنية والظروف السياسية في الحد من استخدام نظم الاتصالات اللاسلكية على نطاقٍ واسع. عند نهاية الحرب العالمية الثانية، أسهم العمل البحثي الريادي للعالم الأمريكي كلود شانون [7] (Claude Shannon) عام 1948م في مجال حساب وتكميم سعة قناة الاتصال في تمكين المهندسين والمهنيين من الفهم الدقيق لأساسيات عمل هذه النظم وسعة قنوات الاتصال. هذا الفهم كان له الدور الكبير في التقدم والتسارع المذهل الذي شهده مجال الاتصالات اللاسلكية، والذي يعتبر القلب النابض للتطور في مجال الاتصالات اللاسلكية الذي نعيشه اليوم.

خلال الستينيات والسبعينيات من القرن العشرين، تم تطوير خوارزميات الترميز لقنوات الاتصالات الفضائية الخاصة بالتوابع الصناعية الفضائية العميقة (البعيدة) Deep Space Communication Channel، والترميز لقنوات التوابع الفضائية القريبة Near Space Communication channel.

التطور في مجال الاتصالات الفضائية العميقة كان بغرض استكشاف الآفاق في ما حول الكرة الأرضية والتوابع الشمسية المختلفة. أما التطور في مجال الاتصالات الفضائية القريبة؛ فكان بغرض بناء شبكات الترابط المعتمدة على الأقمار الصناعية الواسعة النطاق، وذلك لدعم شبكة الاتصالات الهاتفية والاستشعار المُبكر وقياس تقلبات الطقس على سطح الكرة الأرضية. في فترة السبعينيات والثمانينيات أيضاً، انتشرت أنظمة البث الإذاعي والتلفزيون وأنظمة المايكروويف الأرضية، وتم استخدام هذه النظم بصوره تجارية على نطاق واسع.

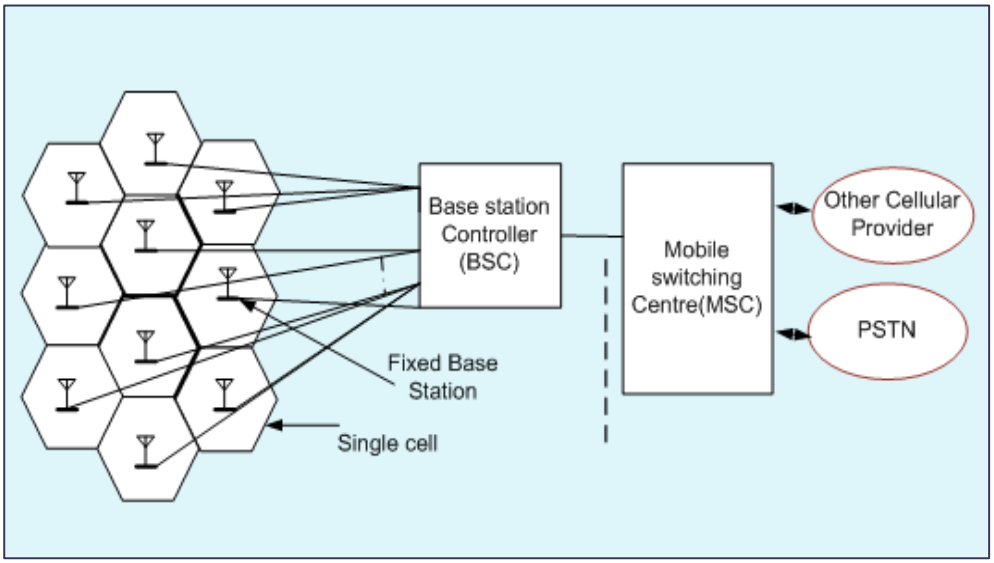
فيما لا شك فيه أن الجزء الأهم من عملية التطور في مجال الاتصالات اللاسلكية، هو الانتشار الواسع للأنظمة الخليوية والشبكات المحلية اللاسلكية Cellular Systems Networking and Wireless LANs في التسعينيات من القرن العشرين. التطور في هذه النظم يمكن تلخيصه فيما يلي:

تطور النظم الخليوية

يرجع تاريخ بداية معرفة الإنسان بهذه الأنظمة إلى أواخر الستينيات وأوائل السبعينيات من القرن العشرين، وذلك عندما تم تطوير مفهوم الاتصالات المتنقلة أو الخليوية في مختبر بيل Bell Lab في الولايات المتحدة [8]. يعتمد مفهوم الاتصالات الخليوية على تقسيم المنطقة الجغرافية المعنية بالتغطية إلى خلايا صغيرة، وتركيب وحدة ثابتة Base-Station في كل خلية لتقوم بدعم الوحدات المتنقلة Mobile Units داخل الخلية، وأيضاً دعم ربطها بالخلايا والنظم الهاتفيه الأُخرى. الشكل 3.1 يوضح المكونات الأساسية لنظام الهاتف الخليوي Cellular system.

من الناحية العملية، بدأ تركيب ما يُعرف بالجيل الأول First Generation للأنظمة الخليوية في الولايات المتحدة في العام 1978م، ثم بعد ذلك تم تشغيلها في كلٍ من اليابان وإسرائيل وبعض الدول الأُوروبية، وكثير من الدول الأُخرى في فترة الثمانينيات. من أهم سلبيات نظام الجيل الأول ضيق سعة التراسل وتقديمها لخدمة نقل الإشارات الصوتية وبعض الخدمات الأُخرى بصورة محدودة. مع نهاية الثمانينيات وبداية التسعينيات تم تركيب نظام ما يُعرف الجيل الثاني Second Generation، وهو جيل يعتمد على التكنولوجيا الرقمية والتي لها الكثير من الميزات الإيجابية على التقنية التماثلية التي أُستُخدمت في الجيل الأول [9]. أهم الخدمات التي تم تقديمها بواسطة نظم الجيل الثاني، هي نقل الرسائل النصية، بالإضافة لخدمة نقل الإشارات الصوتية بكفاءة وسعة تراسلية أكبر.

أسهم التقدم في مجال صناعة الشرائح الإلكترونية وتدني أسعارها، إلى انتشار الجيل الثاني من النظم الخليوية على نطاقٍ واسع، إذ تم تركيب هذا الجيل في أكثر من مائة دولة حول العالم في فترة زمنية وجيزة.



الشكل 3.1: يوضح المعمارية العامة لنظم الاتصالات الخليوية.

في العام 1998م وضع الاتحاد الدولي للاتصالات الموجهات والخصائص الأساسية، لما يُعرف بالجيل الثالث للنظم الخليوية، والتي كان من بينها تقديم خدمة تراسل البيانات والإنترنت بسعات عريضة، بالإضافة إلى نقل الصوت والرسائل. لتقديم هذه الخدمة كان يتطلب تغيير الكثير من مكونات نظام الجيل الثاني، والذي انتشر بصورة واسعة في ذلك الوقت، مما يعني مزيداً من الإنفاق المالي على قطاع الاتصالات. نسبة للعوامل الاقتصادية التي مرَّ بها العالم في هذه الفترة (الأزمة المالية في جنوب شرق آسيا)، فإن الكثير من الشركات العاملة في مجال بناء نظم الاتصالات، اتجهت إلى تطوير حلول جزئية لتتجنب بذلك عملية التغيير شبه الكلي لمكونات الجيل الثاني [9]. ساهمت الأبحاث العلمية بتطوير ما عرف في ذلك الوقت بالجيل (2.5) والذي احتوى فقط على بعض التعديلات البسيطة على مكونات الجيل الثاني، لتتمكن بذلك من نقل البيانات والإنترنت، بجانب خدمات نقل الصوت والرسائل النصية.

مع بداية تعافي العالم من الأزمة المالية التي ضربت دول جنوب شرق آسيا؛ بدأت العديد من الدول في تحديث بنيات الاتصالات الخليوية، وذلك بتركيب نظام الجيل الثالث الحقيقي (حسب مواصفات الإتحاد الدولي للاتصالات)، والذي احتوى على

وحدات صُمِّمت خصيصاً لنقل البيانات والإنترنت. من أكبر المشكلات التقنية التي واجهت هذا الجيل من الأنظمة الخليوية، هو ضيق سعة عرض النطاق وظهور تطبيقات جديدة تتطلب سرعة نقل بيانات عالية. في كثير من البلدان تم تحسين خصائص الجيل الثالث بزيادة سرعة نقل البيانات والإنترنت، وعرف الجيل الجديد بالجيل (3.5)، غير أنه من الناحية العملية يجب الإشارة إلى أنه من الناحية المعمارية ليس هنالك فرق بين الجيل الثالث والجيل الثالث ونصف أو (3.5) [10].

في العام 2008م، تم اعتماد خصائص نظام ما يعرف Long Term Evolution (LTE) المقترح بواسطة مجموعة المواصفات الأُوروبية 3GPP بواسطة الاتحاد الدولي للاتصالات، على أنها الخصائص والميزات الأساسية للجيل الرابع للنظم الخليوية [10-12]. من أهم هذه الميزات الآتي:

- زيادة سرعة نقل البيانات.
- تقليل زمن التأخير في عملية الإرسال (هذه الميزة مفيدة في عملية نقل مواد الوسائط المتعدده في الزمن الحقيقي).
- زيادة سعة نقل البيانات للنظام.
- تقليل التكلفة باعتماد معمارية مختصرة.
- الاستخدام الواسع لميزات برتكول الإنترنت (IPv4/IPv6).

تم الحصول عملياً على كل هذه الميزات باستخدام تقنية الهوائيات المتعددة Multiple Input Multiple Output (MIMO) وتقنية تقسيم الوصول الترددي أو ما يُعرف بـ Orthogonal Frequency Division Multiple Access (OFDMA)[13]. من الناحية العملية، تم تركيب هذا النظام في العام (2010-2011)، في كثير من البلدان حول العالم، ومن المتوقع أيضاً أن يتم تشغيله على نطاق واسع هذا العام والأعوام التالية، في كلٍّ من قطر والكويت وكثير من البلدان العربية. الجدول 1.1 يُلخص أهم الميزات الأساسية للأجيال المتعاقبة لنظم الاتصالات الخليوية.

الجدول 1.1: أهم الميزات الأساسية للأجيال المتعاقبة لنظم الاتصالات الخليوية

الجيل	مواصفة النظام الأساسية	خصائص الوصول المتعدد	الخدمات الأساسية التي يقدمها
الجيل الأول 1978م	Advanced Mobile System Phone (AMPS)	تقسيم الترددFDMA	تراسل المكالمات الصوتية
الجيل الثانى (2) 1990م	GSM، CDMA IS-one، (IS-95) 136	تقسيم الزمن/تقسيم الكود TDMA/ CDMA	تراسل المكالمات الصوتية والرسائل النصية.
الجيل (2.5) 1998م	CDMA2000 1x، EDGE/ EGPRS، GPRS	تقسيم الزمن/تقسيم الكود TDMA/ CDMA	تراسل المكالمات الصوتية والرسائل النصية والبيانات.
الجيل الثالث (3) 2001م	WCDMA/CDMA -EVDO/UMTS	تقسيم الزمن والكود بعرض نطاق واسع	تراسل المكالمات الصوتية والرسائل والبيانات.
الجيل(3.5)	HSDPA/HSDPA +/CDMA2000 1x EV-DO Revision A	تقسيم الكود بعرض نطاق واسع	تراسل المكالمات الصوتية والرسائل النصية والبيانات بسرعة عالية
الجيل الرابع (4) 2010م	LTE/LTE advanced[14]	تقسيم التردد OFDMA	تراسل المكالمات الصوتية والرسائل النصية والبيانات بسرعة عالية باستخدام الإنترنت برتكول

الشبكات اللاسلكية المحلية

تم تكوين مجموعة المواصفة 802.11 بواسطة المجلس الاستشاري لجمعية مهندسي الكهرباء والإلكترونيات (IEEE) في سنة 1991م، بغرض النظر في إمكانية وضع معايير ومواصفات ثابتة وعالمية لنظام شبكات لاسلكية، تكون بديلة ومتوافقة مع الشبكات السلكية ذات المواصفة IEEE 802.3. في العام 1997م تمكنت هذه المجموعة من إصدار المعيار IEEE 802.11، والذي عرف وانتشر على نطاق واسع باسم الويفاي Wi-Fi. اليوم وعلى نطاق العالم تقوم هذه التكنولوجيا بدعم

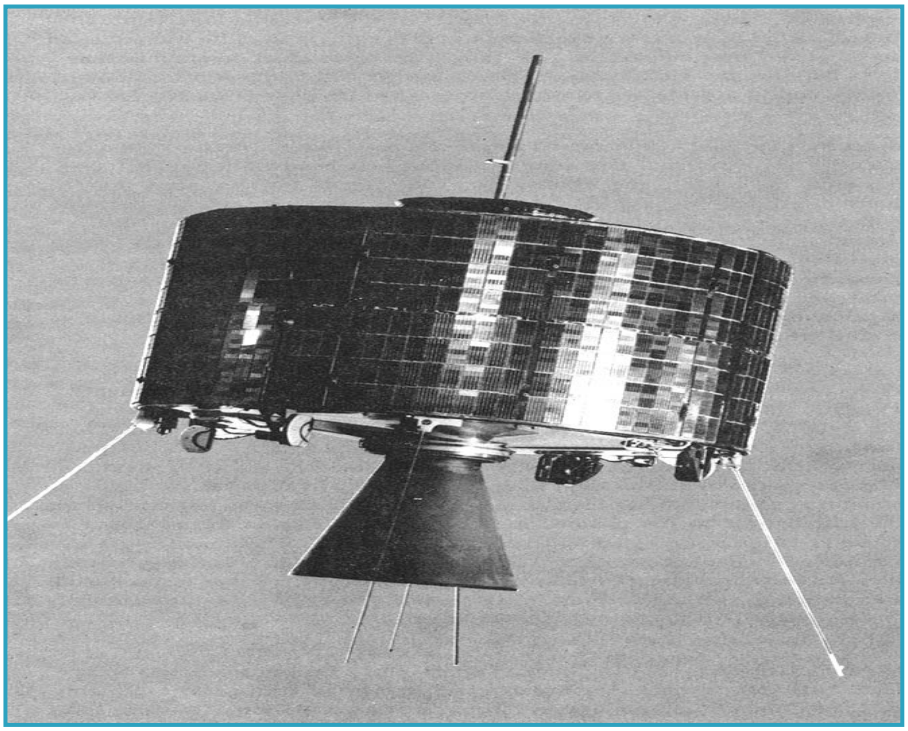
شبكات الوصول Access Networks إلى المنازل والمحال التجارية والملاعب وأماكن التجمعات العامة، إذ تقوم بربط المستخدم المتنقل في نطاق تغطيتها بالشبكة الثابتة عالية السرعة [8]. الجدول 2.1 يوضح خصائص الترابط للأنواع المختلفة للشبكات اللاسلكية المحلية Wireless Local Area Networks (WLANs)

جدول 2.1: يوضح الميزات الأساسية للأنواع المختلفة للشبكات المحلية

الموديل/ المواصفة	سرعة البيانات القصوى	تردد التشغيل
IEEE 802.11a	54 ميغا بت في الثانية	5 ميغا هيرتز
IEEE 802.11g	54 ميغا بت في الثانية	2.4 ميغا هيرتز
IEEE 802.11n	300 ميغا بت في الثانية	2.4،5 ميغا هيرتز

تطور وإنتشار وصلات الأقمار الصناعية أو التوابع الصناعية

يمكن إسناد بداية فكرة استخدام وصلات التوابع الصناعية، إلى الورقة التي نشرها العالم الإنجليزي أرثر كلارك (Arthar Clark)، والتي كانت بعنوان Extra-terrestrial Relays[15, 16]. تم نشر هذه الورقة في المجلة البريطانية Wireless World في أكتوبر من العام 1945م. بعد حوالي عشرين عاماً من ظهور الفكرة الأوَّلية في ورقة العالم كلارك، أي في أغسطس من العام 1964م، تم عملياً إطلاق القمر Syncom-3 (Synchronous Communication Satellite) الشكل 4.1 وهو أول قمر صناعي يعمل في المدار المتزامن مع الأرض Geostationary Orbit. تم إطلاق هذا القمر بواسطة وكالة الفضاء الأمريكية ناسا، وتم استخدامه لأغراض تراسل الاتصالات عبر المحيط الباسفيكي (الموقع: فوق خط الاستواء عند الخط الطولي 180 درجة شرق). في الحقيقة هنالك تجربتان عمليتان للإطلاق لكلٍ من Syncom-1 و Syncom-2 سابقتان لعملية إطلاق القمر Syncom-3، إلا أن الأخيرة تعتبر هي الناجحة، بسبب وصول القمر إلى المدار المستقر أو Geostationary Orbit.



الشكل 4.1: القمر الصناعي Syncom-3 -1964/8/19: المصدر موقع وكالة الفضاء الأمريكية (ناسا) (http://nssdc.gsfc.nasa.gov)

في أبريل من العام 1965م، تم إطلاق أول أقمار الجيل الأول لمنظمة إنتلسات Intelsat الدولية، والذي عُرف باسم الطائر الأول أو Early Bird على الموقع المداري المتزامن 28 درجة غرب. تم استخدام هذا القمر لأغراض تراسل خدمة الاتصالات التلفونية عبر المحيط الأطلسي. نسبة لارتفاع تكلفة صناعة وتشغيل الأقمار؛ فإنه وفي الأيام الأولى لظهور هذه التكنولوجيا واستخدامها؛ تم إطلاق مجموعة من الوحدات المملوكة لبعض المنظمات الدولية المتخصصة، والتي تم إنشاؤها خِصِّيصاً لهذا الغرض. الجدول 3.1 يضم أهم المنظمات الدولية العاملة في مجال تشغيل نظم الاتصالات المعتمدة على التوابع أو الأقمار الصناعية.

الجدول 3.1: قائمة بأهم المنظمات الدولية العاملة في مجال تشغيل نظم التوابع أو الأقمار الصناعية.

المنظمة/ الشركة	منطقة العمل

إنتلسات INTELSAT (2001-1964)	تعمل مجموعة إنتلسات اليوم على تشغيل عدد 52 قمراً صناعياً في مواقع مختلفة من العالم. (الشكل 5.1) لتقديم خدمات الاتصالات المختلفة. بدأت إنتلسات كمنظمة دولية لتشغيل الأقمار الصناعية في العام 1962م، وتم بيعها إلى القطاع الخاص في 2001م.
أربسات Arabsat 1976م-حتى الآن	تعمل مجموعة أربسات على تشغيل عدد 5 أقمار صناعية في المواقع المدارية 20، 26، 30.5، و34.5 درجة شرق لتغطية المنطقة العربية والشرق الأوسط وشمال أوروبا وهي منظمة مملوكة لمجموعة الدول العربية [17].
مجموعة SES S.A.	تمتلك هذه المجموعة عدد 54 قمراً صناعياً في المدار المتزامن وتغطي 99% من الكرة الأرضية. www.ses.com
مجموعة Eutelsat	تغطي المجموعة كل القارة الأوروبية والشرق الأوسط وجزءاً كبيراً من آسيا وأمريكا تغطي عدد 4500 بث تلفزيوني و 1100 بث راديوي.

أهم الخدمات التي توفرها الأقمار أو التوابع الصناعية:

1. خدمات الاتصالات لتلبية متطلبات التطبيقات المدنية والتي تشمل كلاً من الآتي:
   - خدمات البث التلفزيوني والإذاعي.
   - تراسل الاتصالات الصوتية (الهاتف).
   - خدمات النطاق العريض (نقل البيانات).
   - الإنترنت.
2. الخدمات العسكرية.
3. خدمات الإنذار المبكر
4. إدارة حركة الطيران
5. قياس الطقس.
6. الاستشعار عن بعد.
7. تحديد المواقع والمسح الجغرافي والزمن.

مجال صناعة وتشغيل الأقمار الصناعية لبناء شبكات الاتصالات من المجالات الدراسية الواسعة والمشوقة، والتي يصعب وصفها في فقرة صغيرة، لذلك نوصي القارئ المتشوق للتعمق والمعرفة في أن يستخدم المرجع رقم [18] المرفق.

الشكل 5.1: خارطة توضح المواقع الجغرافية للأقمار الصناعية المملوكة لمنظمة إنتلسات الدولية (المصدر موقع إنتلسات http://exnetapps.intelsat.com): تظهر الأقمار مصطفَّة على الموقع المداري المتزامن (36000 كيلومتر فوق خط الاستواء).

5.1 المكونات الأساسية لشبكات الاتصالات

شبكة الاتصالات هي عبارة عن نظام متكامل للربط بين المرسل والمستقبل، من خلال مجموعة من العناصر (الأجهزة والوصلات والمكونات البرمجية)، تُكوِّن مع بعضها نظاماً متكاملاً للتراسل. بصورة عامة، يمكن تصنيف المكونات الأساسية لشبكات الاتصالات في عالم اليوم إلى ثلاث مكونات أساسية حسب الآتي:

1. شبكة النقل Telecommunication Transmission Network: وهي البنية التحتية التي تربط بين الدول والمدن المختلفة والمواقع الكبرى داخل الدولة الواحدة. هذه البنية غالباً ما تكون من الألياف البصرية وأجهزة

الإرسال الخاصة بها أو من وصلات مايكرويف عالية السرعة (أرضية أو معتمدة على أقمار صناعية).

2. شبكة الوصول Access Network: وهي الشبكة التي تمكن المستخدم النهائي End-user من النفاذ إلى مواقع الخدمة والمعالجة والتبديل (Central office، Inter-Connection and Switching). في هذا النوع من الشبكات تُستخدم أنواع مختلفة من الوصلات مثل: كيبلات الهاتف العادية، كيبُلات الألياف الضوئية إلى المنازل Fiber-to-Home، كيبُلات DSL والإرسال اللاسلكي كما هو الحال في الأنظمة الخليوية.

3. شبكة الخدمة أو القلب Core Network، وهي الشبكة التي تربط وتتحكم في شبكة النقل Transmission Network وشبكة الوصول أو النفاذ Access Network وتتكون بشكل عام من العناصر الآتية:

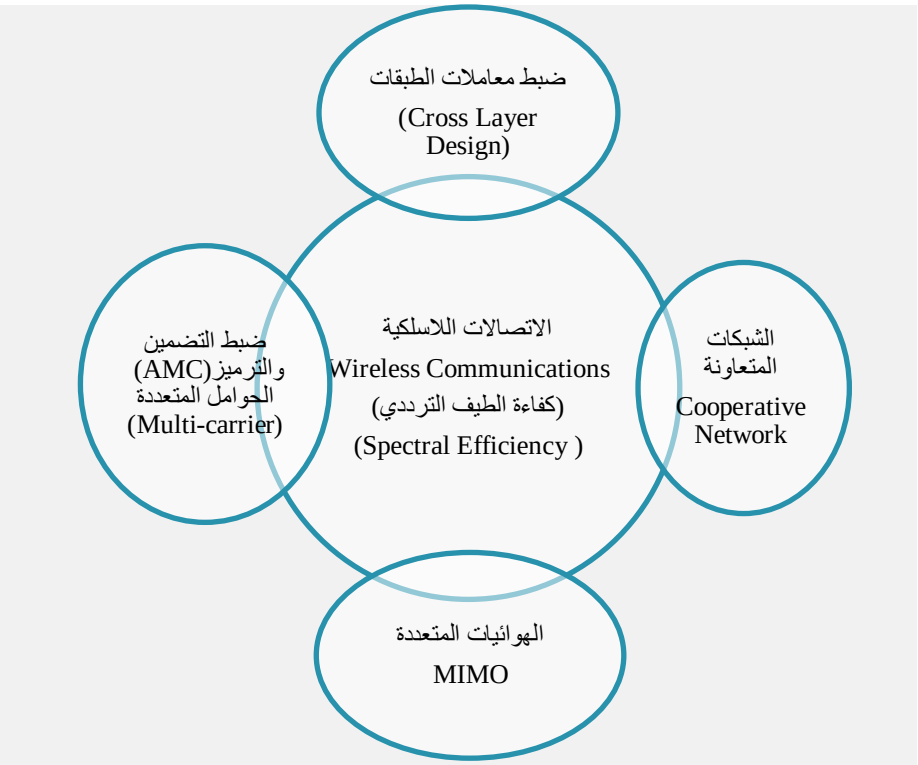
- عناصرالتبديل Switching Elements
- عناصر الترابط Interconnections
- مُخدمات الرسائل والإنترنت Internet and SMS Severs
- مُخدمات الحسابات والسيطرة Billing (Accounting) and Control System
- مُخدمات الخدمات الإضافية Value added Service Systems.

مع تقدم التكنولوجيا في مجال صناعة المعالجات ومعمارية الحاسبات Computer Architecture and Micropocessor، أصبح بالإمكان بناء كل عناصر شبكة الخدمة أو القلب Network Core وبكل سهولة وبكفاءة عالية، تفوق كل متطلبات التطبيقات المستخدمة اليوم. بالنسبة لشبكة النقل Transmission Network أيضاً يمكن القول إن النتائج التي تم التوصل إليها أخيراً في مجال السعة القصوى للألياف البصرية، تفوق أيضاً كل متطلبات المستخدم في الوقت الحاضر وفي المستقبل القريب. بالنسبة لشبكة الوصول Access Network والتي تعتمد على حلول توصيل الألياف الضوئية

إلى المنزل Fiber-to-Home أو تكنولوجيا الشبكات اللاسلكية؛ فيمكن القول إن كلاً منها مُرتبط بعدد من الإشكالات، فعملية بناء وتوصيل شبكات الألياف الضوئية إلى المنازل تعتبر حلاً هندسياً مثالياً، من حيث ميزة توفير السعات التراسلية العالية، لكن هذا الحل مرتبط بتكلفة عالية نسبياً، وخارج نطاق تحمل الكثير من الاقتصاديات في العالم اليوم (خاصةً الدول النامية والدول الفقيرة التي تعتمد على الاقتصاديات الأولية). أما بالنسبة للحلول اللاسلكية، فإنها رخيصة من ناحية التكلفة، لكن لها سعة محدودة (نسبة لمحدودية الطيف الترذُدِي وسرعة نقل البيانات في النطاق الترذُدِي المحدد)، وتعتبر مقيدة نسبياً للكثير من التطبيقات. هنالك الكثير من الجهود والأبحاث العلمية في عدة اتجاهات من أجل زيادة كفاءة نقل البيانات في وحدة الطيف الترددي، نذكر منها ما يلي:

- ضبط المعاملات في الطبقات المختلفة لموديل TCP/IP مع بعضها البعض Cross Layer Design(CLD).
- حلول الشبكات المتعاونة.Corporative Networks
- استخدام الهوائيات المتعددة Multiple Input Multiple output (MIMO).
- ضبط معاملات عملية التضمين والترميز Adaptive (AMC) Modulation and Coding واستخدام الحوامل المتعددة Multi-Carrier.

الشكل6.1: يوضح الاتجاهات البحثية في مجال الشبكات اللاسلكية من أجل زيادة كفاءة الطيف الترددي [19].



الشكل 6.1: الاتجاهات البحثية الأربعة في مجال الشبكات اللاسلكية لزيادة كفاءة الطيف الترددي.

6.1 التطور في أنظمة تخزين المعلومات

من وجهة مفهوم نظرية المعلومات، فإن عملية إرسال المعلومات في قنوات الاتصالات، تكاد تماثل عملية التخزين من حيث العمليات. قبل عملية الإرسال أو عملية التخزين، يعمد المهندسون إلى تقليل ما يُعرف بالمعلومات الزائدة أو Redundancy Data، وذلك لتقليل عرض النطاق المستخدم في حالة الإرسال أو تقليل مساحة التخزين في حالة حفظ المعلومات. مع التطور في مجال صناعة وحدات المعالجة والشرائح الإلكترونية، لم يتم التطور فقط في عملية إرسال المعلومات، بل أيضاً تطورت عملية تخزين المعلومات واسترجاعها. يمكن تلخيص الطرق الرئيسية لتكنولوجيا التخزين في العناصرالآتية:

- الشريط المغناطيسي Magnetic Tape
- القرص الصلب Hard Disk

- الأقراص الضوئية Optical Storage
- أدوات التخزين الخارجية Solid state Storage
- شبكة التخزين Storage Area Network
- صندوق الضوئيات Optical Jukebox
- مصفوفة الأقراص Disk Array

7.1 مركز المعلومات أو مستودع البيانات

مراكز المعلومات أو مستودعات البيانات هي عبارة عن منشآت بُنيت خصيصاً لتحمي أنظمة الكمبيوتر والاتصالات ومكونات تخزين المعلومات الخاصة بالبنيات الأساسية الحرجة. عملية اختيار الموقع ومواصفات المباني والمعدات الخاصة بمراكز البيانات، تعتبر من العمليات الهندسية الصعبة، لاعتمادها على الكثير من العوامل العامة والشروط الخاصة بطبيعة النشاط الاقتصادي. في الولايات المتحدة الأمريكية على سبيل المثال تقوم الحكومة بإلزام الشركات والمؤسسات الكبرى (مثل ميكروسوفت وإنتل وشركات النفط والجامعات الكبرى) ببناء مراكز للبيانات في مواقع متعددة تحددها الحكومة، لتتمكن من توفير درجة عالية من الحماية في الأمور التي تتعلق بالوصول الفيزيائي والكوارث الطبيعية. للمزيد من الحذر، قامت شركة قوقل المشهورة ببناء مراكز للبيانات في أماكن متفرقة من العالم، لتوفير درجة أعلى من الحماية. الولايات المتحدة من الدول التي تعرضت للكثير من التجارب الصعبة، والتي كان يتوقع فيها ضياع كمية كبيرة من المعلومات. على سبيل المثال في العام 2008م، كانت هنالك الكثير من الفيضانات بسبب التغير المناخي، حيث تأثرت بذلك بعض مراكز البيانات، لكن سياسة استخدام المواقع المتعددة، مكنت المؤسسات من استعادة المعلومات في فترة وجيزة، ومواصلة النشاط الاقتصادي ومن دون أية خسائر تذكر، وكذلك الحال في حادث11 سبتمبر الشهير في العام 2001م.

من أهم الاعتبارات التي يجب مراعاتها في تصميم مراكز البيانات:

1. اختيار الموقع المناسب (بعيداً من مواقع حدوث الفيضانات والكوارث وسهولة توفير الحماية الفيزيائية).
2. يجب أن يقاوم المبنى التأثيرات الفيزيائية (الزلازل والهجوم بغرض التدمير) بدرجة عالية.
3. إمداد المبنى بمصادر مستقرة للطاقة والخدمات (يفضل الإمداد من مصادر متعددة).
4. اختيار العناصر البشرية العاملة بعناية فائقة.
5. اختيار مواصفات معدات تخزين البيانات.
6. تزويد المبنى بشبكة اتصالات عالية الكفاءة.
7. تزويد المبنى بنظام لإطفاء الحريق والإنذار المبكر.
8. تزويد المبنى بنظام للحماية الفيزيائية.

عملية بناء وإدارة مركز المعلومات من العمليات المكلفة من الناحية الاقتصادية، وتعتبر خارج نطاق مقدرة الكثير من المؤسسات وبيوتات الأعمال التجارية الصغيرة، لذلك تعمد الكثير من الدول إلى بناء وإدارة مستودعات المعلومات العامة، والتي يمكن أن يستخدمها أصحاب الأعمال الصغيرة في عملية إدارة المخاطر التي يمكن أن يتعرض لها نشاطهم الاقتصادي. من ناحية عامة، فمن أهم القطاعات التي يجب أن تستخدم مراكز المعلومات في عملية إدارة المخاطر Risk Management ما يلي:

1. قطاع الإدارة الحكومية والحكومة الإلكترونية.
2. قطاعات التجارة الإلكترونية.
3. البنوك والمؤسسات المالية.
4. قطاعات صناعة وإدارة الطاقة.
5. قطاعات تكنولوجيا المعلومات وشركات الاتصالات الكبرى.
6. قطاعات الخدمات العامة (كهرباء، مياه، مواصلات).
7. قطاعات الأمن الوطني.
8. قطاعات التعليم (الجامعات والمعاهد العليا والمدارس).

9. قطاع إدارة الصحة.

إدارة مستودع البيانات

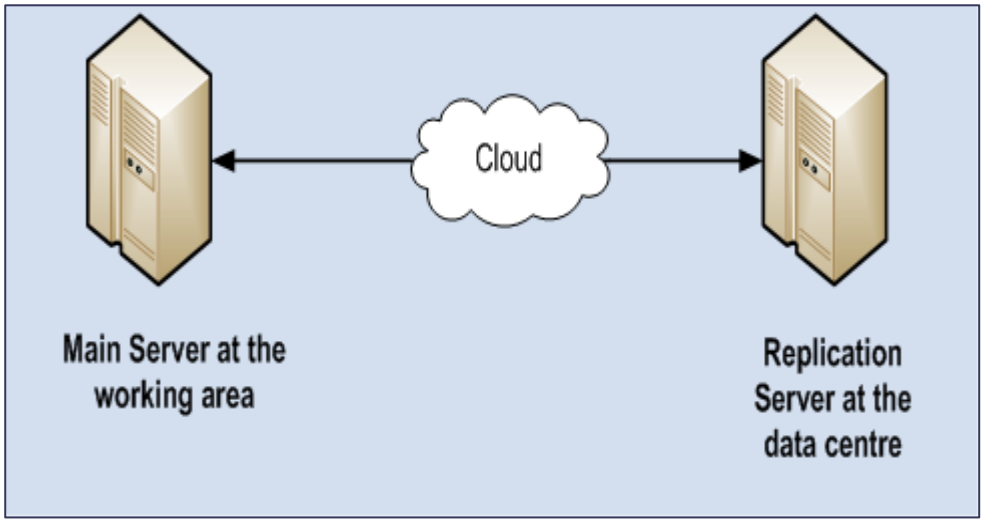
عملية إدارة مراكز البيانات من العمليات المعقدة والتي يجب تدريب العاملين عليها، وإكسابهم الخبرة العملية اللازمة للتعامل مع حالات الطوارئ، التي يمكن أن تقابلهم خلال فترة حياتهم العملية. يمكن تلخيص العمليات الأساسية لإدارة مراكز المعلومات في العناصر الآتية [20]:

- مراقبة المنشأة من الأخطار الآتية:
  - الاختراق.
  - الحريق.
  - تعطل مصادر الطاقة.
  - درجة الحرارة.
  - تسريب المياه.
  - مراقبة المبنى وجميع الأصول.
- الحماية من الشحنات الكهرومغناطيسية.
- النظافة العامة.
- المراجعة الدورية لخطط التعامل مع الكوارث.

النسخ المتماثل للبيانات

النسخ المتماثل في الحوسبة، هو عملية حفظ المعلومات بصورة متطابقة بين المخدم الرئيسي ومخدم النسخ المتماثل Main Server and Replication Server، وذلك لضمان الاتساق بين الموارد من أجل تحسين الموثوقية. مثلاً في الشكل 7.1 يعمل المخدم الرئيسي على التحكم في مصادر البيانات الخاصة بالنشاط الاقتصادي (حسابات كهرباء، عمليات صناعية...إلخ)، ويقوم بمطابقة المعلومات مع مخدم النسخ المتماثل. في حالة تعرض المخدم الرئيسي لأي عطل فني، يقوم مخدم النسخ المتماثل

Replication Server مقام المخدم الرئيسي إلى حين عودة المخدم الرئيسي إلى الخدمة. من ناحية عملية يمكن أن يتم تركيب هذه المخدمات في مواقع مختلفة (مراكز بيانات مختلفة)، كجزء من عملية إدارة المخاطر. فإذا تعرض أحد المواقع لكارثة ما، يتم تشغيل النشاط الاقتصادي من الموقع الآخر ومن غير تأثير يذكر على النشاط المعيَّن.



الشكل 7.1: يوضح نموذجاً مختصراً لعملية النسخ المتماثلData replication

طرق النسخ الاحتياطي للبيانات

عملية نسخ البيانات من العمليات الروتينية التي يجب أن تقوم بها إدارة نظام المعلومات في المؤسسة (كجزء من إجراءات عملية إدارة المخاطر)، إذ تقوم بأخذ نسخة كاملة من البيانات بغرض الأرشفة أوللرجوع إليها عند الحاجة (حالات الإتلاف أو الضياع أو الكوارث). هنالك عدة طرق للقيام بعملية النسخ نذكر منها:

- النسخ الكامل Full Backup
- النسخ التزايدي Incremental Backup

- النسخ التفاضلي Differential Backup
- نسخ دلتا العكسي Reverse Delta Backup

حسب التقديرات المالية وحسابات إدارة المخاطر في المؤسسة أو النشاط الاقتصادي، يجب أن يتم اختيار وتحديد الطريقة المناسبة لعملية النسخ.

8.1 تصميم نظم الاتصالات وتطوير المعايير العالمية

من أهم العوامل التي ساهمت في تطور نظم الاتصالات، عملية الاعتماد على الطبقات المنفصلة في التصميم. هذه الطريقة وعلى الرغم من الكثير من عيوبها المكتشفة حديثاً [21]؛ إلا أنها أسهمت إسهاماً فعالاً في عملية تطور الاتصالات وتسهيل عملية الربط البيني بين النظم المختلفة. ولما كانت هنالك حاجة عالمية لهذه المعايير، ليتفق عليها الجميع من أجل الاستخدام الأمثل لتكنولوجيا الاتصالات، والاستفادة القصوى منها في عملية استدامة التطور وزيادة رفاهية الإنسان؛ فإنه تجب الإشارة هنا إلى عدد من المنظمات الدولية، التي تقوم بدور صياغة المعايير العالمية في مجال صناعة الاتصالات وهي:

- الاتحاد الدولي للاتصالات International Telecommunication Union (ITU) والذي يضم عدداً من الأقسام المتخصصة في فروع ومجالات الاتصالات المختلفة.
- مجموعة تطوير الإنترنت Internet Engineering Task Force (IETF) والتي تقوم بوضع المواصفات والمعايير الخاصة بتقنية الاتصال عبر الإنترنت، أو ما يُعرف ببرتكولات الإنترنت Internet Protocols.
- المجموعة الأوروبية لمعايير الاتصالات European Telecommunications Standards Institute (ETSI).
- مؤسسة مهندسي الكهرباء والإلكترونيات Institute of Electrical and Electronics Engineers (IEEE).

- المؤسسة الأمريكية للمعايير American National Standards Institute (ANSI).

في كل دولة من دول العالم، هنالك أيضاً مؤسسة مهمتها تنظيم قطاع الاتصالات والمعلوماتية، وفي كثير من الأحيان تعمل هذه المؤسسات في الدول المختلفة على تبادل الخبرات فيما بينها، والتعاون مع الاتحاد الدولي للاتصالات، من أجل الوصول إلى مواصفات معيارية أفضل.

9.1 تطور شبكة الإنترنت

كلنا يتفق مع الرأي الذي يقول إن تاريخ الإنترنت يرجع إلى العام 1950م، والذي فيه تم اكتشاف الحاسب الرقمي، الذي بواسطته ولجت البشرية إلى هذا العصر. لكن يجب أن نقرّ أيضاً أن البداية العملية للإنترنت، كانت في العام 1969م عندما تم إرسال أول رسالة على شبكة أربانت ARPANET بين معمل البروفسور Leonard Kleinrock في جامعة كاليفورنيا، في لوس أنجلوس، ومركز البحوث في بجامعة استانفورد Stanford Research Institute (SRI)، أي بعد حوالي 19 سنة من اكتشاف الحاسب الرقمي. في الحقيقة، كانت هنالك العديد من المحاولات لإرسال حزم البيانات قبل هذا الموعد. ففي العام 1962م قدم الطالب وقتها Leonard Kleinrock رسالته لدرجة الدكتوراه بعنوان" Message Delay In Communication Nets With Storage" [22] والتي وضعت الأساس النظري واللبنات الأساسية لعملية إرسال وتبديل حزم البيانات Packet Switching. لقد تلت هذه الخطوة العديد من تجارب الإرسال، لكن تظل بداية الإرسال الحقيقية من شبكة أربانت هي تاريخ الميلاد الحقيقي لشبكة الإنترنت. لقد أسهمت الكثير من العوامل الإستراتيجية والسياسية في بقاء شبكة ARPANET (الشبكة الأولى والأُم للإنترنت) محدودة الاستخدام لدى الجيش الأمريكي وبعض المؤسسات البحثية والتعليمية المرتبطة به خلال فترة السبعينيات من القرن العشرين، وذلك نسبة للقيود المفروضة من الإدارة الأمريكية على تبادل وانتشار التكنولوجيا في ذلك والوقت.

في بداية الثمانينيات من القرن الماضي، وبالتحديد في العام 1982م، تم اعتماد المواصفة الأساسية لبرتكول TCP/IP، وبرز اتجاه قوي عند الكثير من مواقع اتخاذ القرار في الولايات المتحدة بتوسيع دائرة خدمات شبكة ARPANET، لتشمل أكبر عدد من المؤسسات، إذ تم الربط البيني بين شبكة العلوم للحاسبات والتي تعرف(Computer Science Network (CSNET وشبكة أربانت، ثم بعد ذلك سمحت المؤسسة الوطنية للعلوم الأمريكية National Science Foundation (NSF) للكثير من المؤسسات البحثية والتعليمية حول العالم، بالوصول إلى الكثير من موارد شبكة CSNET في العام 1986م. في الأعوام 1990م و1995م، تم اتخاذ خطوات جريئة بواسطة الكثير من المنظمات الدولية من أجل تشجيع استخدام الإنترنت على نطاق واسع في كل أنحاء العالم، فقد تم الاعتماد على مؤسسات تقديم خدمة الإنترنت Internet Service Providers (ISPs) ، لتقديم الكثير من الخدمات المباشرة للجمهور. من أهم الخدمات التي قدمتها منظومة شبكة الإنترنت في الأيام الأولى الآتي:

- البريد الإلكتروني والرسائل النصية السريعة.
- الوصول إلى الصفحات World Wide Web.
- إرسال مواد الوسائط المتعددة. Video and VOIP calls.
- مواقع النقاش المفتوحة Discussion Forums.
- التواصل الاجتماعي Blogs،Social Networking .
- التسويق Online Shopping.
- التعليم والبحوث.

الجدول 4.1 يوضح أسماء المنظمات الرئيسية التي تسهم في إدارة وتطوير الإنترنت في العالم. الجدول 5.1 يعرض أسماء لبعض أصحاب البحوث والأعمال الريادية التي أسهمت في تطور الاتصالات والإنترنت.

الجدول 4.1: قائمة بأسماء المنظمات التي تساهمت في تطور وإدارة الإنترنت.

المنظمة	الموقع	المهام
مجموعة الإنترنت للبحوث Internet Research Task Force (IRTF)	http://irtf.org/	البحوث والتطوير في الموضوعات ذات المدى الطويل
مجموعة عمل هندسة الإنترنت Internet Engineering Task Force (IETF)	http://www.ietf.org/	العمل على تحسين عمل الإنترنت من خلال وضع المواصفات التي تساعد في عمليات التصميم وإدارة الشبكات.
جمعية الإنترنت للتخصيص والترقيم Internet Assigned Numbers Authority (IANA)	http://www.iana.org/	إدارة نظام العنونة IP addressing والأسماء DNS Roots والتسجيل.
جمعية معمارية الإنترنت Internet Architecture (Board IAB)	http://www.iab.org/	IAB هو عبارة عن لجنة إشرافية تتبع إلى IETF وتقدم المشورة لجمعية الإنترنت
جمعية الإنترنت	http://www.internetsociety.org/	مجموعة عمل تتعامل مع الصعاب اليومية التي تواجه شبكة الإنترنت

الجدول5.1: قائمة ببعض أسماء أصحاب البحوث والأعمال الريادية في مجال تطوير الإنترنت

الاسم	المساهمة من أجل تطور الإنترنت
كلود شانون Claude Shannon (1916-2001م)	قدم نظرية المعلومات والتي أسهمت إسهاماً فعالاً في تطور نظرية الترميز
فينفار بوش Vannevar Bush (1890-1974م)	كان له دور فعال في تشجيع الشراكة بين الجامعات والمراكز البحثية والجيش من أجل قيام مشروع أربانت ARPANET
بول براون Paul Baran (1926-2011م)	تطوير مجال الشبكات الموزعة Developed the Field of Redundant Distributed Networks
دونالد ديفس Donald Davies (1924-2000م)	تطوير مفهوم إرسال حزم البيانات Packet Switching
ليكيلايدا J. C. R. Licklider	تطوير مفهوم الشبكات للأغراض العامة Universal

(1915-1990م)	Network
تشارلز هرتسفلد Charles Herzfeld (ولد في 1925م)	من أحسن المديرين لمشروع DARPA وساعد مساعدة فعالة في قيام مشروع ARPANET
بوب تايلر Bob Taylor (ولد في 1932م)	تطوير مفهوم Ethernet and the Xerox Alto
دوغلاس إنجلبرت Douglas Engelbart (1925-2013م)	تطوير وسائل تعامل الإنسان مع الحاسوب Human–Computer Interaction
لاري روبرتس Larry Roberts (ولد في 1937م)	قام بأول عملية ربط بين اثنين من أجهزة الحاسوب وقاد مشروع ARPANET في الأيام الأولى.

الفصل الثاني

المخاطر الأساسية على نظم الاتصالات والمعلومات

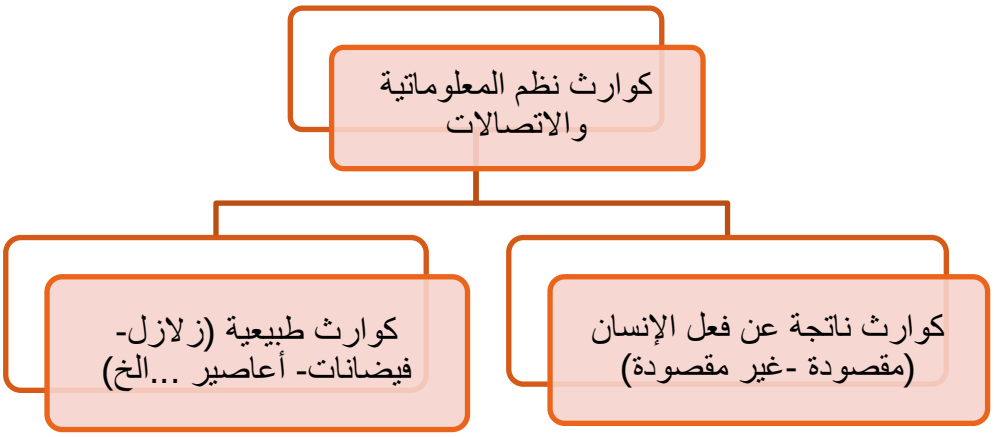
1.2 المقدمة

يُعرّف الخطر على أنه ضرر محتمل قد ينشأ عن بعض العمليات الحالية أو من بعض الأحداث في المستقبل. المخاطر موجودة في كل جوانب حياتنا اليومية ويجب أن تُوضع في اعتبارات التصميم من جميع أصحاب المهن والتخصصات الهندسية المختلفة. من وجهة نظر مفهوم نظم الاتصالات والمعلومات؛ فإن إدارة المخاطر تعني عملية فهم العوامل التي قد تؤدي إلى فشل النظم وسلامتها وإعداد الخطط اللازمة للتصدي لهذه المخاطر أو التقليل من أضرارها.

هذا الفصل من الكتاب يناقش بعض التصنيفات الأساسية للمخاطر التي يمكن أن تتعرض لها نظم الاتصالات والمعلومات في عالم اليوم. لتوضيح كل الآثار الاجتماعية والاقتصادية التي يمكن أن تنجم عن بعض هذه المخاطر، سوف نقوم في هذا الجزء باستعراض بعض الكوارث المعلوماتية الحقيقية، والمتصلة بنظم الاتصالات التي مرت بها بعض الدول والمنظمات، وذلك بغرض الاستفادة منها والتزود بخبراتها لمواجهة المستقبل. في بداية هذا الفصل سوف نتعرض إلى تصنيف شكلي لطبيعة المخاطر التي يمكن أن تتعرض لها نظم الاتصالات والمعلومات في الفقرة 2.2. في الفقرة (3.2) نناقش بعض الوقائع الحقيقية لكوارث نظم الاتصالات والمعلومات. وفي الفقرة 4.2 نناقش الهجوم الإلكتروني على دولة إستونيا. في الفقرة 5.2 يتم تسليط الضوء على بعض الإشكالات والتساؤلات التي برزت مع ظهور هذه الأنواع من المخاطر.

2.2 تصنيف المخاطر على نظم الاتصالات والمعلومات

بصورة عامة، يمكن تصنيف الكوارث التي يمكن أن تتعرض لها نظم المعلومات والاتصالات، إلى قسمين حسب الشكل 1.2. الجدول 1.2 يوضح بعض الأمثلة لهذه الأنواع المختلفة من الكوارث بصورة تفصيلية.



الشكل 1.2: التصنيف العام لكوارث المعلوماتية والاتصالات

الجدول 1.2: أمثلة من الواقع لبعض كوارث المعلوماتية والاتصالات.

طبيعة الكارثة	الوصف	بعض الأمثلة من الواقع
الاطلاع غير المقصود بفعل الانسان	الوصول إلى معلومات مصنفة بأنها سرية بصورة غير مقصودة.	ضياع وحدات تخزين معلومات ووقوعها في يدٍ أخرى. نشر المعلومات السرية نتيجة لخطأ في الإجراءات.
كوارث طبيعية	زلازل- أعاصير- فيضانات	انقطاع الكيبلات البحرية للألياف البصرية في اليابان في زلزال 2011م

		تأثر بعض مراكز البيانات Data centers للشركات الكبرى في ولاية واشنطون الأمريكية في العام 2007-2008م نتيجة للأعاصير والفيضانات. انهيار شبكة الاتصالات جزئياً في الصين بعد زلزال 2008م في إقليم تسشوان في الصين.
التأثير أو الاعتداء باستخدام برامج (بفعل الإنسان)	الفيروسات والبرامج المعادية بصورة عامة	محاولة التأثير أو الاعتداء على البرنامج النووي الإيراني بواسطة الفيروس Stuxnet [23] [24]. حادث Cyxymu في (هجوم ممنهج على مواقع التواصل الاجتماعي) 2008/8/7م[25] حادث الهجوم الإلكتروني على دولة إستونيا في 2007م حادث التأثير على النظم الحاسوبية المعتمدة على نظام النوافذ باستخدام برنامج زوتاب Zotob [26] في العام 2005م. حادث التأثير على نظام السلامة في المحطة النووية للكهرباء في ولاية أوهاو الأمريكية في العام 2003م[27]
انقطاع الكهرباء أو التشويش والاعتداء المتعمد (بفعل الإنسان)	انقطاع التيار الذي يزود بنيات الاتصالات والمعلومات- التشويش على قنوات الإرسال	تشويش قنوات البث الفضائي (التلفزيوني والإذاعي). انقطاع الكهرباء عن مراكز البيانات Data Centers. اختراق الشبكات وتغيير البيانات بصورة غير مصرح بها. حادث الاعتداء على مركز البيانات الخاص

		بالكهرباء في ولاية كالفورنيا الأمريكية في العام 2007م [28].
استغلال نطاق الإرسال (بفعل الإنسان)	استغلال نطاق الإرسال بصورة متعمدة أو غير متعمدة	الاعتداء والإرسال في نطاق التردد المملوك للغير.
أخطاء النظم (بفعل الإنسان)		أخطاء في تصميم البرامج. الأعطال الناتجة عند البرمجة الأولية للنظم System Configurations مثال لذلك عطل البرامج الذي أسهم في انقطاع الكهرباء في أجزاء كبيرة من الولايات المتحدة وكندا في العام 2003م [29] الأعطال الناتجة عن عملية تحديث النظم system upgrade
تعطيل خطوط الاتصالات (بفعل الإنسان)	انقطاع كيبلات– توقف نظم	انقطاع كيبلات الألياف البصرية في منطقة البحر المتوسط في العام 2008م تدمير منشآت الاتصالات.
الاحتيال (بفعل الإنسان)	الاحتيال باستخدام المواقع والرسائل الإلكترونية	إرسال رسائل الاحتيال Phishing Emails برمجة وإطلاق صفحات الاحتيال Phishing Websites. الاستفادة من بعض الأخطاء البشرية العفوية Social Engineering Attack.
التجسس أو التنصت	التنصت باستخدام أجهزة خاصة أو من	استخدام نظام PRISM بواسطة بعض الحكومات لجمع المعلومات من الإنترنت [30, 31].

الإلكتروني (بفعل الإنسان)	خلال نظم الاتصالات	تخوف الحكومة الأمريكية من بعض شركات الاتصالات الأجنبية في أن تستخدم أجهزتها في عمليات تنصت [32-34].

المخاطر الناتجة عن فعل الإنسان

بصورة عامة يمكن أن نُصنِّف المخاطر التي يمكن أن يُسببها الإنسان إلى الأقسام الآتية:

- مجموعات الجريمة المنظمة Organized Crime Groups والتي في الغالب تسعى إلى مهاجمة القطاعات المالية.
- مجموعات منظمة مدعومة من الدول State Sponsors، وهذه غالباً ما تسعى إلى سرقة المعلومات الاستخباراتية السرية ونتائج الأبحاث العلمية وخطط المؤسسات الحكومية
- مجموعات عدائية (ذات توجة سياسي أو أيدولوجي) تسعى للإضرار بالبنيات التحتية للدول.
- أفراد

3.2 أمثلة من الواقع لبعض وقائع كوارث المعلوماتية والاتصالات

نسبة إلى ارتباط الخطر بحدوث شيء ما في المستقبل، وأن هذا المستقبل لا يعلم خفاياه إلا خالق الكون. لذلك يجب التوضيح أولاً أن عملية إعداد الخطط البديلة للتقليل من آثار هذه المخاطر، عملية مهمة ولا تتعارض مع القيم والمبادئ الإنسانية، لكن يجب أن تتم وفق دراسات وتقييم مهني وعلمي. في هذه الجزئية نتعرض بالتفصيل لشكلين من أشكال المخاطر التي يمكن أن تتعرض لها نظم الاتصالات والمعلومات: انقطاع الوصلات البحرية الرابطة بين الدول والقارات، والاعتداء أو الهجوم الإلكتروني المُمنهج على الدول أو المنشآت والشركات الحيوية الكبرى.

انقطاع كيبلات الألياف الضوئية البحرية

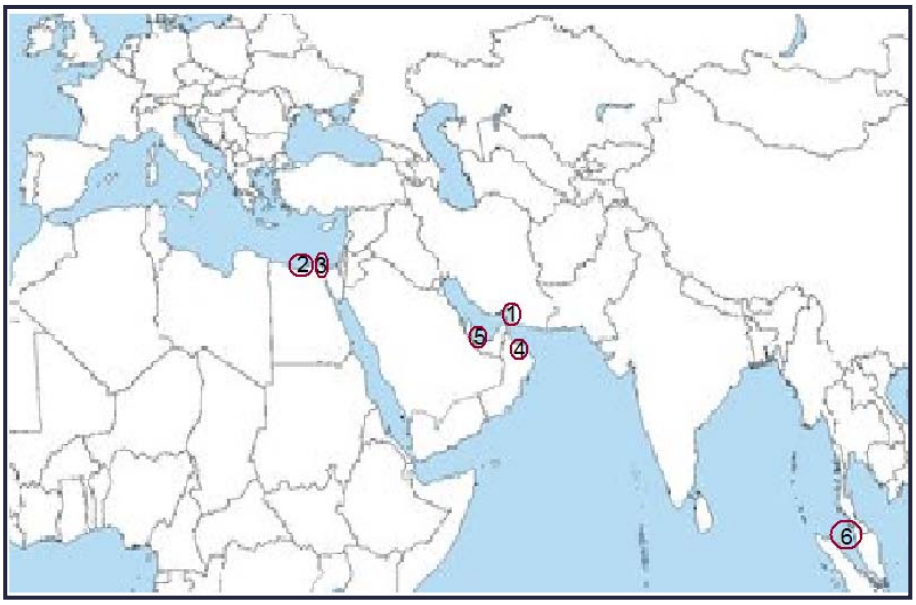
من أكبر الكوارث التي تصيب نظم الاتصالات اليوم، هي انقطاع خطوط التراسل الدولية أو الإقليمية فائقة السرعة، والتي تعتمد على تقنية الألياف البصرية. من الناحية العملية يمكن أن يكون الانقطاع بفعل فاعل، أو بسبب الظروف والكوارث الطبيعية المحيطة ببيئة العمل أو المنطقة التي يمر بها الكيبل.

كما ذكرنا في الفصل السابق، تُستخدم الألياف البصرية اليوم وبصورة واسعة لنقل البيانات وتطبيقات الإنترنت بين الأقاليم المختلفة للبلد الواحد، وتوصيل البلدان والقارات المختلفة مع بعضها البعض. لذلك يُعتبر انقطاع الألياف البصرية من الكوارث والمهددات الأمنية والمعلوماتية الكبرى في عالم اليوم. الجدول 2.2 يوضح وبصورة مختصرة بعضاً من حالات الأعطال الكارثية للكيبلات البحرية في منطقة الشرق الأوسط خلال العام 2008 م والآثار التقنية والاقتصادية المترتبة عليها.

الجدول 2.2: الأعطال الرئيسية للكيبلات البحرية خلال العام 2008 [35, 36] في منطقة الشرق الأوسط

التاريخ	مكان الانقطاع	الدول المتأثرة
23 يناير 2008	الوصلة البحرية Falcon التي تربط بين بلدان الخليج العربي والهند	تأثير في حركة الإنترنت
30 يناير 2008	الوصلات البحرية SEA-ME-WE4 في FLAG Telecom البحر المتوسط بالقرب من الإسكندرية	انقطاع الإنترنت في مصر بنسبة 70% و60% في الهند وتأثرت كل من الإمارات، قطر، البحرين، السعودية بنغلاديش والكويت بنسب متفاوتة
3 فبراير 2008	الوصلة البحرية Doha-Haloul بين دولة قطر والإمارات	-
4 فبراير 2008	الوصلة البحرية SEA-ME-WE4 بالقرب من جزيرة بيناغ الماليزية	-
19 ديسمبر	الوصلات FLAG Telecom	انقطاع الإنترنت في مصر

2008	و4 -SEA-ME-WE و-SEA 3- ME-WE بين جزيرة مالطة والإسكندرية	بنسبة 80% وتتأثر الاتصالات بين الشرق الأوسط وجنوب آسيا والعالم بنسبة 75%



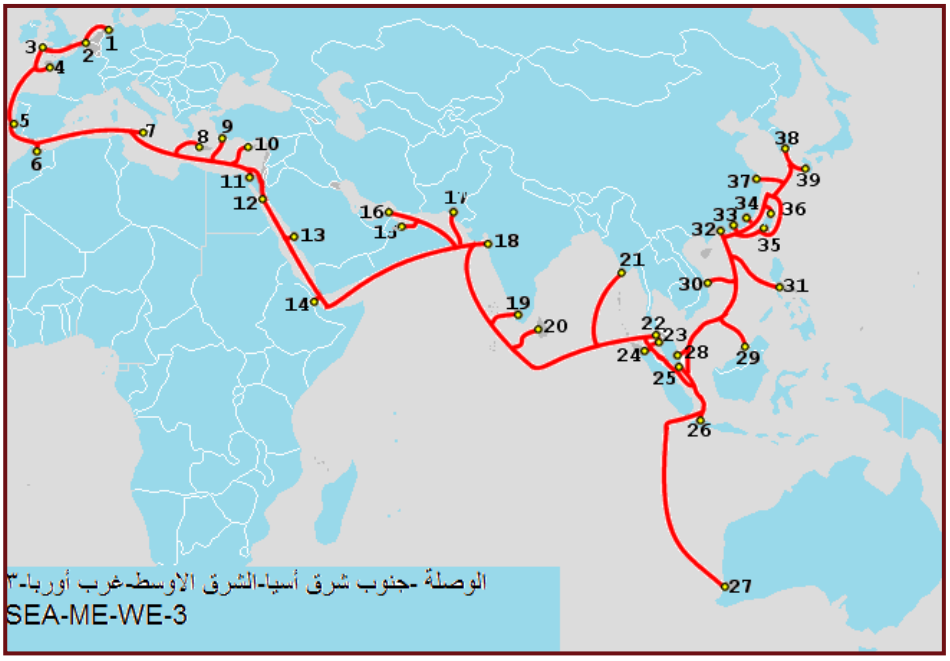
الشكل2.2:خارطة توضح مواقع أعطال الكيبلات البحرية خلال العام 2008م في منطقة الشرق الأوسط

جدول3.2: تعريف وشرح للأعطال الموضحة في الشكل2.2

الرقم	التاريخ	اسم الكيبل وموقع الإنقطاع
1	23 يناير	الوصلة فالكون (Falcon) بالقرب من بندرعباس (إيران)
2	30 يناير	الوصلة (SEA-ME-WE-4) بالقرب من الإسكندرية (مصر)
3	30 يناير	الوصلة فلاك (Flag) بالقرب من الإسكندرية (مصر)
4	1فبراير	الوصلة فالكون (Falcon) بين مسقط (عمان) ودُبي (الإمارات)
5	3 فبراير	الوصلة بين الدوحة (قطر) ومنطقة حلول (الإمارات)
6	4 فبراير	الوصلة (SEA-ME-WE-4) بالقرب من بيناغ (ماليزيا)

الجدول4.2: أطوال وخصائص الكيبلات البحرية التي تعرضت لكوارث أو قطع خلال العام 2008م [37]

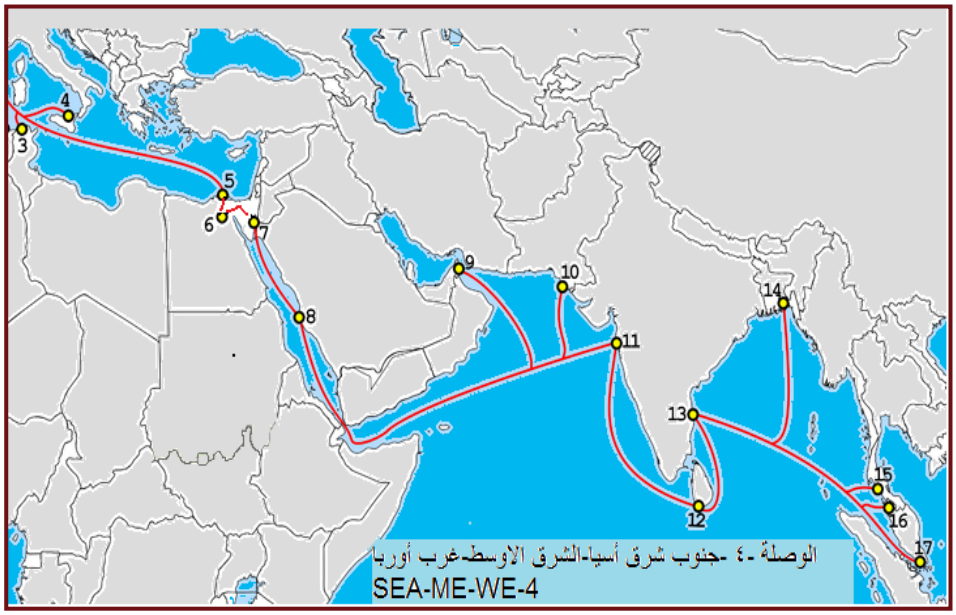
اسم الوصلة البحرية	الطول	المناطق التي تربطها
الوصلة البحرية Fiber-Optic Link Around the Globe (FLAG)	28000 كيلومتر	• أوروبا وأمريكا FA-1 • الشرق الأوسط وشبه القارة الهندية FALCON • أوروبا وجنوب شرق آسيا FEA • شمال آسيا FNAL
الوصلة البحرية South East Asia–Middle East–Western Europe 4' (SEA-ME-WE 4) الشكل2.4	18800كيلومتر	دول جنوب شرق آسيا وشبه القارة الهندية والشرق الأوسط و أوروبا
الوصلة البحرية South-East Asia - Middle East - Western Europe- 3 (SEA-ME-WE- 3) الشكل2.3	39000 كيلومتر	دول جنوب شرق آسيا والشرق الأوسط وغرب أوروبا



الشكل2.3 : خريطة توضح المسار الكامل للوصلة البحرية SEA-ME-WE-3 التي تغطي جنوب شرق آسيا والشرق الأوسط وأوروبا.

قائمة لتعريف النقاط الرئيسية التي تمر بها الوصلة البحرية SEA-ME-WE-3 حسب الشكل 2.3

1. نوردن- ألمانيا	**14. جيبوتي- جيبوتي**	**27. بيرث- أستراليا**
2. أوستند- بلجيكا	15. مسقط- عمان	28.ميرسغ- ماليزيا
3.قونهالى-المملكة المتحدة	16. الفجيرة، الإمارات	29.تنقوا- بروناي
4. بنمارش- فرنسا	17. كراتشي- باكستان	30. دا نانغ- فيتنام
5. سيسيمبرا- البرتغال	18. مومباي- الهند	31. باتانجاس- الفلبين
6. تطوان- المغرب	19. كوشين- الهند	32. تايبا- ماكاو
7. مازارا ديل فالو- إيطاليا	20. ماونت لافينيا- سريلانكا	33. هونغ كونغ
8. خانيا- اليونان	21. بيابون- ميانمار	34. شانتو-والصين
9. مارماريس- تركيا	22. ساتون-تايلاند	35. فانغشان- تايوان
10. يروسكيبو- قبرص	23. بينانج، ماليزيا	36. توشينج- تايوان
11. الإسكندرية- مصر	24. ميدان- إندونيسيا	37. شنغهاي- الصين
12. السويس- مصر	25. تواس وسنغافورة	38.كيوجي-كوريا الجنوبية
13. جدة- المملكة العربية السعودية	26. جاكرتا- إندونيسيا	39. أوكيناوا- اليابان



الشكل 4.2: خارطة توضح المسار الكامل للوصلة البحرية SEA-ME-WE-4 التي تغطي جنوب شرق آسيا والشرق الأوسط وغرب أوروبا.

قائمة لتعريف النقاط الرئيسية التي تمر بها الوصلة البحرية SEA-ME-WE-4 حسب الشكل 2.4

1. مارسليا- فرنسا	6. القاهرة- مصر	11. مومباي- الهند	16. ملقا - ماليزيا
2. عنابة- الجزائر	7. السويس- مصر	12. كولومبو- سريلانكا	17. تواس - سنغافورة
3. بنزرت- تونس	8. جدة-المملكة العربية السعودية	13. تشيناي- الهند	
4. باليرمو- إيطاليا	9. الفجيرة- الإمارات العربية المتحدة	14. كوكس بازار- بنجلاديش	
5. الإسكندرية- مصر	10. كراتشي- باكستان	15. ساتون- تايلاند	

الآثار الاقتصادية الناتجة عن انقطاع الكيبلات البحرية

لم يتحصل الباحث على دراسات إحصائية حقيقية بالآثار الاقتصادية والاجتماعية لهذه الأعطال؛ لكن يقدر بعض الخبراء القيمة الحقيقية لتأثر التجارة الدولية بهذه الأعطال بمليارات الدولارات، حسب تقدير حجم توقف الأعمال التجارية في البلدان المتأثرة.

فكثير من الدول مثل الولايات المتحدة وبريطانيا لها الكثير من الارتباطات التجارية مع الهند وباكستان ودبي في الإمارات العربية المتحدة، حيث تملك الكثير من الشركات العالمية أفرعاً إنتاجية وتسويقية في هذه البلدان المتأثرة، هذا بالإضافة إلى أن هنالك عامل مساهمة ثابتة لتكنولوجيا المعلومات والاتصالات في الإنتاج القومي لكل بلد من هذه البلدان المتأثرة، مما يعني أن أي عملية توقف للبنية المعلوماتية، سوف يكون لها تأثير مباشر على الإنتاجية الكلية [38, 39]. على الرغم من وجود الكثير من البدائل في وسائل الترابط والتراسل بين القارات المختلفة؛ إلا أن هذه المجموعة من الأعطال كان لها تأثير كبير على حجم التغطية في كثير من البلدان. الجدول 5.2، يوضح بعض التقديرات المعلنة بأعداد المتأثرين بهذه القطوعات حسب التقرير المنشور في المراجع [36, 37].

الجدول5.2: تقديرات بأعداد المتأثرين بالقطوعات

الدولة	تقديرات بعدد المشتركين المتأثرين
الهند	60،000،000
باكستان	12،000،000
مصر	6،000،000
السعودية	4،700،000
إيران	4،000،000
الإمارات	1،700،000
الجزائر	1،000،000
السودان	1،000،000
لبنان	400،000
سوريا	300،000
البحرين	-
بنغلاديش	-

المالديف	-

4.2 الهجوم الإلكتروني على دولة إستونيا

تقع دولة إستونيا في الجزء الشمالي من أوروبا، يحدُّها الخليج الفلندي من ناحية الشمال وبحر البلطيق من ناحية الغرب ومن الجنوب لادفيا ومن ناحية الشرق روسيا. انضمت إستونيا إلى الاتحاد الأوروبي في عام 2004م، وهي من الدول المتقدمة من الناحية الاقتصادية والتكنولوجية، إذ أنها من أوائل الدول التي استخدمت نظام الحكومة الإلكترونية e-Government على نطاق واسع.

بدأ هذا الهجوم الإلكتروني على إستونيا في 27 أبريل 2007م، واستمر لمدة ثلاثة أسابيع، وكان على ثلاث دفعات حسب الجدول 6.2. عند بداية الهجوم توقفت نُظم الاتصالات، الإنترنت، المصارف، المطارات، محطات القطار، نظم إدارة المياه وتوريد الغذاء والبث التلفزيوني [40, 41].

الجدول 6.2: يشرح طبيعة الهجوم الإلكتروني على إستونيا

الفترة	نوع الهجوم
27 أبريل 2007م	تنظيم مجموعة من الهجمات من نوع DDoS و ICMP Commands على مقدمي خدمات الإنترنت (ISPs) والمواقع الحكومية
30 أبريل 2007م	سرقة عناوين البريد الإلكتروني لأعضاء البرلمان وإرسال كمية من الرسائل لهم. وإيقاف خدمات البريد الإلكتروني لمدة يومين.
3-9 مايو 2007	الهجوم على المواقع الرسمية للدولة باستخدام تقنيات متطورة مثلSQL Injections

من الناحية العامة، نجد أن الهجوم استهدف القطاعات الحكومية والتجارية العامة، ولكن تم التركيز بصورة شديدة على القطاعات والمصالح الآتية [42, 43]:

- الدواوين الحكومية.
- البرلمان.
- الوزارات.
- الصحف اليومية والإخبارية بصورة خاصة.
- قنوات البث الإذاعي والتلفزيوني.
- مواقع الإنترنت الإخبارية الموالية للدولة.

تمكن المهاجمون من الإضرار بالبنية التحتية الأساسية للاتصالات والمعلومات، وتعطيل الكثير من القطاعات الحكومية والتجارية، والسيطرة على الكثير من وسائل الإعلام؛ وتمكنوا أيضاً من بث الكثير من الرسائل الكاذبة باسم الحكومة في الكثير من المواقع. من أهم القطاعات الحكومية والتجارية التي تم إيقافها [42]:

- مكتب رئيس الحكومة والبرلمان.
- كل الوزارات الحكومية.
- الأحزاب السياسية.
- ثلاث من الصحف اليومية.
- اثنان من أكبر البنوك.
- مقدمو خدمات الإنترنت.
- شركات الاتصالات.

أما التأثير التقني على شبكات الاتصالات؛ فكان كما يلي:

- إتلاف للموجهات Routers damaging .
- تغير جداول الموجهات Routing Tables Changed.
- تغير أجهزة العنونة أو ما يُعرف تقنياً بـ DNS Servers Overloaded.

- توقف خدمات البريد الإلكتروني E-mail Servers Failure.

الاستجابة الأولية

تجاه هذا الهجوم الإلكتروني والمعلوماتي الشامل، اتخذت الدولة مجموعة من الإجراءات الدفاعية، وذلك لتقليل حجم الأضرار إلى الحد الأدنى، فقام فريق الحاسوب للطوارئ والاستجابة الإستوني Estonian Computer Emergency Response Team (ECERT)(www.cert.ee/) بالإجراءات والعمليات الآتية [40, 41]:

- قفل جميع المواقع التي تعرضت للهجوم أمام المستخدمين من خارج الدولة.
- قطع 99% من عمليات الاتصال المزيفة من خارج البلاد.
- تحويل المهاجمين وفتح الطريق لهم لمهاجمة مواقع مزيفة أو مواقع مدمرة.
- مراقبة الاتصالات والإنترنت بواسطة نظم متطورة.
- حصار عمليات الإقلاع من مخدمات التسمية الرئيسية Blockade of Bots From Root Domain Name System(DNS) Servers
- إقناع مقدمي خدمات الإنترنت (ISPs) في البلدان والدول الأخرى، بوضع الحاسبات المشاركة في الهجوم في القائمة السوداء.
- تلقي العون التقني من كل من إسبانيا – إيطاليا - ألمانيا - سلفوفاكيا والكثير من البلدان الأخرى.
- ترك موقع رئيس البلاد سهلاً للهجوم، لتمكين المهاجمين منه، وذلك لتفادي مهاجمتهم لمواقع أخرى، قد تكون إستراتيجية وأكثر أهمية.
- تحليل مخلفات الهجوم بغرض الوصول للفاعل.
- تلقي المساعدة والدعم الفني من منظمة حلف شمال الأطلسي (NATO).

- دعت إستونيا في العام التالي (2008م) لاتفاقية مشتركة لمكافحة الهجمات المعلوماتية التي تعتمد على الكمبيوتر.

الخبرات المستفادة

التجارب المستفادة من هذا الحدث كثيرة، فهو أول تجربة لهجوم إلكتروني منظم لعدد من الأهداف داخل كيان سياسي معترف به دولياً. بعيداً عن حسابات الخسائر الاقتصادية والمعنوية التي لحقت بهذه الدولة، إلا أن مستوى الاستجابة والمساعدة الدولية، كان له الدور الأكبر في عملية احتواء الكارثة واستعادة الخدمات الأساسية في وقتٍ وجيز. الجانب الآخر والمهم، هو أن الكثير من الدول والمنظمات استفادت من هذا الدرس، وسعت بصورة حقيقية إلى دعم سياسات حماية البنيات التحتية الأساسية المعلوماتية والاتصالات [42]. على سبيل المثال قام الاتحاد الأوروبي بمراجعة وإعلان سياسة موحدة للدعم والحماية على نطاق الدول الأعضاء [44]. من ناحية أخرى، وعلى مستوى المنظمات الدولية، قام الاتحاد الدولي للاتصالات، بالكثير من المبادرات، وذلك من أجل تعزيز حماية المعلوماتية والاتصالات. للاطلاع على تجارب دول أُخرى مماثلة، يمكن للقارئ الرجوع إليها في المرجع رقم [45] المرفق في قائمة المراجع.

5.2 المخاطر على نظم المعلومات والإشكالات القانونية المصاحبة

فيما لا شك فيه أن موضوع أمن المعلومات والاتصالات وحماية البنيات التحتية الحرجة من الموضوعات الإستراتيجية الكُبرى، التي تشغل البشرية في عالم اليوم. في هذه الفقرة نتعرض لبعض من أهم الإشكالات التي تواجه العالم بهذا الخصوص، من خلال قراءة الواقع المعاش لطبيعة المخاطر التي تتعرض لها هذه النظم.

الحقيقة الأولى المرتبطة بالجريمة الإلكترونية في عالم اليوم، هي أنها في كثير من الحالات تكون متعدية للحدود السياسية، وأنها أصبحت من المهددات الاقتصادية والاجتماعية بالنسبة للكثير من الدول، التي تعتمد بصورة كبيرة على المعلوماتية. ففي حالة الهجوم على دولة إستونيا مثلاً، وإذا نظرنا إلى حجم الأضرار التي لحقت بالإنسان والمؤسسات الاقتصادية في هذه الدولة؛ قد لا يستغرب البعض منا نظرة الآخر إلى هذه الجريمة، على أنها تهديد للسلم والأمن الدوليين [40, 46, 47]. على

الرغم من كل الخسائر التي لحقت بهذه الدولة، إلا أنها لم تستطع أن تستخدم المادة 51 من ميثاق الأمم المتحدة، للدفاع عن النفس أو استخدام المادة 5 من معاهدة حلف شمال الأطلسي، للدعوة للدفاع المشترك أو حتى دعوة مجلس الأمن للقيام ببعض الإجراءات وفق المادة 41 من ميثاق الأمم المتحدة. حصل كل هذا العجز القانوني لأن كل هذه المواد تشترط تعرض الدولة لهجوم عسكري مسلح، وهو الشيء الذي لم يحدث لدولة إستونيا! [48, 49]. هذا العجز في تكنولوجيا القانون في تقديري، يجب الانتباه إليه ومناقشته من قبل المؤسسات الدولية ومُعالجته بوضع إطار قانوني دولي شامل يخاطب المشكلات الآتية:

1. تحديد المسؤولية عن الجريمة (أفراد – منظمات – دول أو جماعات مدعومة من بواسطة بعض الدول).
2. حفظ حقوق جميع الأطراف.
3. تحديد المسؤولية الثانوية والتي تشمل الجوانب الآتية:
   - مسؤولية شركات البرمجيات التي تركت الباب مفتوحاً للهجوم.
   - مسؤولية الأطراف التي أسهمت بشكل أو آخر في توفير البيئة المناسبة للقيام بالجريمة (مثلاً تقصير بعض الدول في محاربة جماعات الجريمة الإلكترونية داخل حدودها أو تقصير الدولة في تعقب الجماعات التي تقوم بالتشويش على الأقمار الصناعية من داخل أراضيها).
   - مسؤولية مقدمي خدمة الإنترنت.
   - مسؤولية مالك النظام الذي بدأ منه الهجوم في حالة وجود طرف ثالث.
4. دعم الموثوقية بين الدول بهذا الخصوص.
5. تعريف وتحديد مستويات التنسيق التقني والقانوني بين الدول.
6. الموائمة بين متطلبات الحرية الشخصية ومتطلبات التحقيق في الجرائم المتصلة بالمعلوماتية.

الجانب الآخر والذي أيضاً لا يقلُ أهميةً عن عملية وضع الإطار القانوني الدولي، هو عملية تطوير الحلول التقنية. هنا لا أقصد إيجاد أو تطوير حلول للمشكلات العارضة، كما تفعل العديد من الشركات؛ بل أقصد تطوير ووضع إطار شامل مماثل للذي قام بوضعه الاتحاد الدولي للاتصالات لإدارة شبكات الهاتف الثابت. مطلوب من اللجنة الدولية لتطوير الإنترنت IETF أن تُطور في المواصفات التقنية للبرتكولات الأساسية (DNS، IPv6،BGP) لتساعد في عملية تحقيق درجة عالية من الموثوقية في عملية الإسناد (نسب محتويات الجريمة إلى الجاني).

الفصل الثالث

مدير أمن المعلومات

1.3 المقدمة

وظيفة مدير أمن المعلومات Chief Information Security Office (CISO) هي وظيفة جديدة استحدثت مع تقدم ثورة المعلومات، واجتياحها لكل المجالات الحيوية والنشاطات الاجتماعية والاقتصادية للبشرية. على سبيل المثال في الجامعات الحديثة اليوم توجد الآلاف من الحواسيب المتصلة مع بعضها والمرتبطة بالعالم الخارجي عبر شبكة الإنترنت. هذه الحواسيب تحتوي في الغالب على كم هائل من المعلومات القيمة والحساسة من جميع النواحي؛ لذلك من المنطقي أن يكون هنالك جسم إداري معني بوضع السياسات واللوائح المنظمة للتعامل والتحكم في الوصول إلى هذه البيانات واستخدامها فيما يحقق المصلحة العامة للجامعة أو المؤسسة. في عالم المعلومات اليوم يقوم مدير أمن البيانات بالكثير من المهام والواجبات. تبدأ هذه الواجبات بتصنيف البيانات من حيث المحتوى، وتحديد صلاحيات الوصول والتعامل مع البيانات حسب الدرجات الوظيفية؛ وتنتهي إلى تحديد التكنولوجيا التي يمكن استخدامها لتحمي المؤسسة من الهجمات الإلكترونية والقرصنة ووضع السياسات العامة لإدارة المخاطر المعلوماتية التي يمكن أن تتعرض لها المؤسسة. في هذا الفصل نتناول الإطار العام لوظيفة مدير أمن المعلومات في الفقرة 2.3، ثم نناقش المهام الأساسية لهذه الوظيفة في الفقرة 3.3. في الفقرة 4.3 نقوم بتلخيص ومناقشة بعض متطلبات المسار المهني لهذه الوظيفة.

2.3 الإطار العام لوظيفة مدير أمن المعلومات

بصورة عامة يقوم مدير أمن البيانات بوضع السياسات العامة واللوائح لتحقيق الأهداف الآتية:-

- الخصوصية Confidentiality.

- توفير الخدمة Availability
- السلامة والأمان Integrity

الجدول 1.3 يوضح الجوانب الأساسية والإطار العملي العام الذي يجب أن يعمل من خلاله مدير أمن البيانات لتحقيق الأهداف المرجوة من نظام أمن المعلومات.

الجدول 1.3 الإطار العام الذي يجب أن يعمل من خلاله مدير أمن المعلومات

الدور القيادى لمدير أمن المعلومات CISO Role		
تحديد الإستراتيجيات والسياسات والجرائم الإلكترونية المتعلقة بالجوانب السياسية Stratigic Security (...,Cybercrime politics)	وضع سياسة أمن المعلومات وسياسة إدارة المخاطر واللوائح والنظم الداخلية Information Security (...,Risk management, Regulatary compliance)	الوسائل التقنية Technical Securit (...,Firewalls Network Security)

الجوانب التقنية

من أولى الخطوات والمهام التي يجب أن يقوم بها مدير أمن المعلومات، هي إقناع الإدارة العليا بالإنفاق على عملية جلب واستخدام الوسائل والمعدت التكنولوجية المناسبة وحجم النشاط الاقتصادي للمؤسسة التي يعمل بها. بصورة عامة يمكن تقسيم الوسائل التكنولوجية المستخدمة في أمن المعلومات وحماية البنيات الأساسية للمعلومات إلى الآتي:

- وسائل التحكم (يتم بها التحكم في بنيات المعلومات والاتصالات، مثل أجهزة التحكم في الشبكات والخدمات).
- وسائل المراقبة (مراقبة النظم والشبكات).
- وسائل التحقيق (وسائل تساعد على إجراء التحقيق في الجرائم الإلكترونية).

أهم نقطة تجب الإشارة إليها، هي أن هذه الوسائل متجددة ومتطورة مع تطور الجرائم المعلوماتية والتكنولوجيا، لذلك يجب أن يكون مدير أمن المعلومات شخصاً قادراً على الاطلاع المستمر (مدى الحياة)، وذلك لمواكبة المتغيرات السريعة في مجال تكنولوجيا المعلومات.

إدارة أمن المعلومات

يقصد بهذه الجزئية من الإطار العملي العام لأمن المعلومات، مقدرة الشخص على وضع الخطط المناسبة لعملية إدارة المخاطر Risk Management والإيفاء بالمتطلبات والمعايير الخاصة والعامة Regulatory Compliance في مجال أمن المعلومات. القطاعات والنشاطات الاقتصادية المختلفة في البلدان المختلفة، تخضع لمعايير تنظيمية مختلفة، فمثلاً قوانين أمن المعلومات في القطاع الصحي في الولايات المتحدة، تختلف تماماً عن القوانين التي تنظم أمن المعلوماتية في القطاع الصحي في الاتحاد الأوروبي. نفس الحالة تنطبق على قطاعات المختلفة مثل التعليم الجامعي والدفاع وقطاع إدارة المال والأعمال.

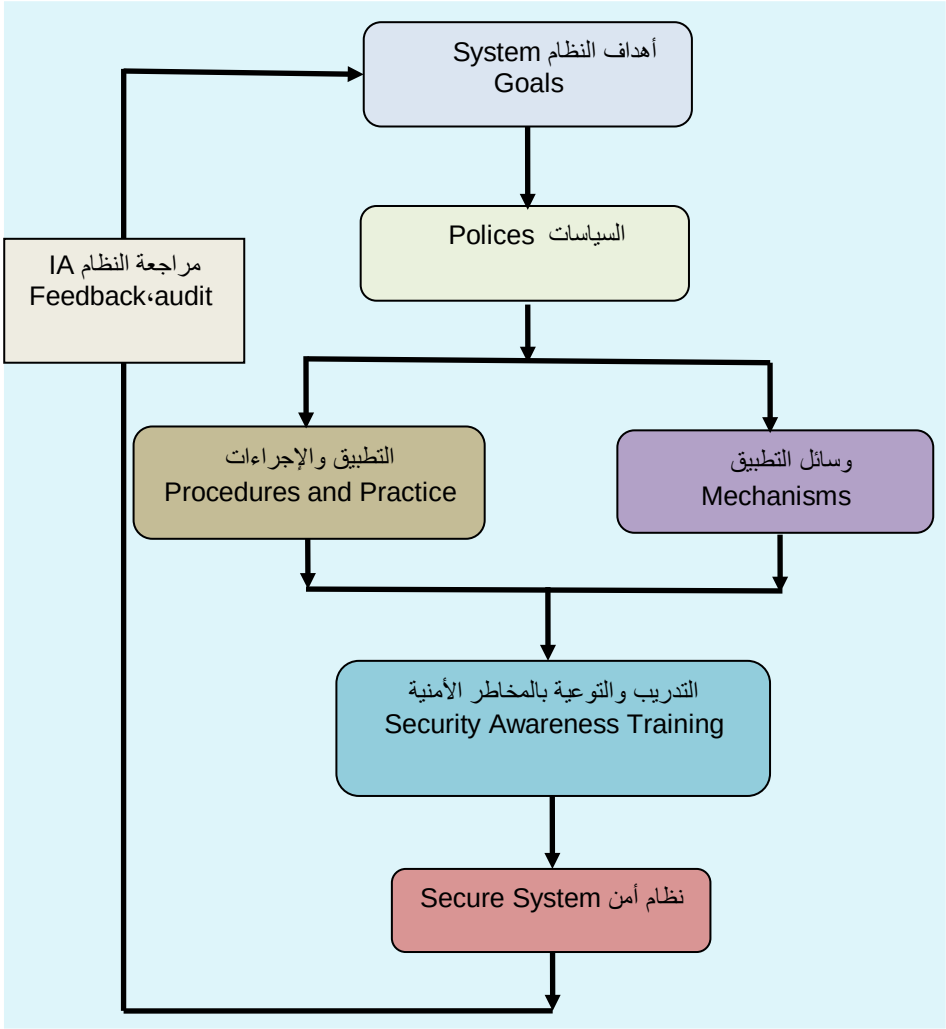
الإستراتيجيات

عملية إدارة إستراتيجية أمن المعلومات تعني معرفة البعد السياسي للمعلوماتية والجرائم الإلكترونية والتعاون الإقليمي والدولي في مجال الاستجابة للطوارئ والاختراقات. تساعد المعرفة بهذه الأمور والجوانب على تكوين رؤية بعيدة المدى من أجل وضع السياسات الصحيحة في الجوانب الآتية:

- تصميم السياسات.
- استخدام التكنولوجيا.
- تنمية الموارد البشرية.
- التعاون الدولي وتبادل الخبرات.

3.3 مهام مدير أمن المعلومات

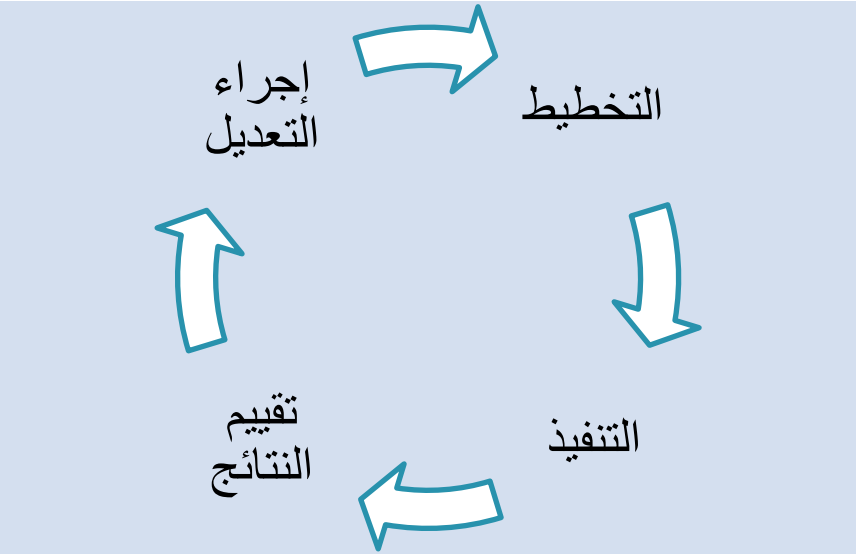
عملية أمن المعلومات تختلف باختلاف النشاط الاقتصادي، ففي الجامعة مثلاً تجب حماية البنية التحتية للمعلوماتية التي تخص الطلاب والعاملين، بالإضافة إلى نتائج البحوث والدراسات في المجالات الإستراتيجية، والمحافظة على أصول البنية التحتية بغرض الاستمرار في تقديم الخدمة التعليمية. في المجالات الصناعية يكون الهدف هو حماية البنية التحتية ومعلومات المجال الصناعي المهمة، وذلك لضمان الاستمرارية والتفوق الصناعي والمحافظة على الوضعية التجارية. القاسم المشترك في كل هذه العمليات هو المحافظة على البنية التحتية للمعلومات، والمحافظة على المعلومات الإستراتيجية للنشاط المعني؛ وفوق كل هذا وذاك، فإن العمل في مجال أمن المعلومات يتطلب التعلم المستمر من بيئة العمل وتجديد ومراجعة كل المدخلات التكنولوجية لعملية الأمن الإلكتروني، وذلك حسب بنية المخطط الموضح في الشكل 1.3. في البداية يجب تحديد الأهداف بكل دقة (تحديد البنيات والمعلومات التي يراد حمايتها). تلي هذه الخطوة عملية وضع السياسات العامة، ثم بعدها يتم اختيار المعدات التكنولوجية بالتوازي مع عملية اعتماد الإجراءات الخاصة بإدارة أمن المعلومات (إدارة المخاطر وتلبية المتطلبات الخاصة بالمواصفات والمعايير التي وضعتها الدولة). ثم بعد ذلك من المهم أيضاً أن تتم هنالك توعية عامة للكوادر البشرية العاملة بالمخاطر والسياسات واللوائح وطبيعة التعامل مع المعدات التقنية.



الشكل 3.1: الإطار العام لعملية إدارة أمن المعلومات.

تنتهي حلقة مهام إدارة أمن المعلومات بعملية التقييم والمراجعة، والتي فيها يتم تقييم كفاءة النظم والسياسات وسماع النصائح الخارجية، ليتم بعدها تحديث السياسات والاستمرار في عملية استدامة الاستقرار في الخدمات، كما هو موضح في المخطط أو النموذج في الشكل 2.3. في البداية يجب أن نبدأ بعملية التخطيط الشاملة والتي تأخذ في الحسبان كل الجوانب الأساسية لأمن المعلوماتية (من الحماية الفيزيائية إلى استخدام الوسائل التكنولوجية المعقدة وتوعية وتدريب الكادر البشري)، ثم يليها تنفيذ

الخطط والتقييم (تقييم داخلي وتقييم خارجي) والذي فيه تتم معرفة مواضع القصور ليتم تصحيحها بتعديل الخطة السابقة، وهكذا يجب أن تكون العملية مستمرة باستمرار النشاط الاقتصادي.



الشكل 2.3: مسار واستمرارية التطوير والتحديث في سياسات أمن المعلومات.

4.3 المسار المهني لمدير أمن المعلومات

من حيث المبدأ يمكن أن تكون لمدير أمن المعلومات في المؤسسة أية خلفية علمية من تخصصات العلوم والهندسة ونظم المعلومات، مع أخذ قدر عالٍ من التدريب العملي للقيام بالمهام. نسبة للتغير الديناميكي السريع الذي يشهده مجال المعلومات من حيث التطور التكنولوجي والمحتوى؛ فإن ميزة الذكاء وقابلية التعلم المستمر من بيئة العمل، هي أيضاً من الصفات الأساسية التي يجب أن تتوافر في كل الكوادر البشرية التي تعمل في هذا المجال. من ناحية التطور المهني فهنالك بعض الشهادات التي تؤهل الشخص مباشرة للعمل والمواكبة في هذا المجال، نذكر منها على سبيل المثال:

1. الشهادة الفنية لنظم أمن المعلومات. Certified Information Systems Security Professional (CISSP). هذه الشهادة عبارة عن معيار معترف به عالمياً، إذ أنها تغطي كل المتطلبات الصارمة للمواصفة المعيارية ISO /IEC17024، وذلك من حيث التصميم المعماري والمفهوم الإداري لنظم أمن البيانات وتحديد الموجهات الأساسية لبيئة العمل. تضم المحتويات الدراسية لنيل هذه الشهادة الموضوعات الآتية:

- التحكم بالوصول Access Control.
- أمن الاتصالات والشبكات Telecommunication and Network Security
- أمن المعلومات وإدارة المخاطر Information security governance and risk management
- سلامة تطوير البرمجيات Software Development Security
- التشفير Cryptography
- معمارية أمن المعلومات والتصميم Security Architecture and Design
- أمن وسلامة تشغيل النظم Operations Security
- استمرارية تشغيل النظم وخُطط الإفاقة والعودة من وضع الكارثة Business Continuity and Disaster Recovery Planning
- القوانين والنظم واللوائح والتحقيق Legal،Regulations ، Investigations and Compliance
- التحكم بالوصول الفيزيائي Physical (Environmental) Security

2. شهادة الاعتماد والتحكيم Certification and Accreditation Professional (CAP): وهي شهادة مهنية يتم فيها اختبار الشخص على المفاهيم والموضوعات الآتية:

- المفاهيم العامة لنظم أمن المعلومات.
- تصنيف نظم المعلومات.
- تنفيذ أساسيات التحكم في المعلومات.
- تقييم عملية التحكم في المعلومات.
- مراقبة نظام أمن المعلومات.
- إحكام نظام المعلومات.
- تطبيق نظام سيطرة على النظم.

3. شهادة ممارسة مهنة أمن المعلومات Systems Security Certified Practitioner (SSCP): لنيل هذه الشهادة يتم اختبار مقدرات الممتحن في الموضوعات الآتية:

- التحكم في الوصول Access Controls.
- التشفير Cryptography.
- اكتشاف البرامج والنشاطات الهدامة Malicious Code and Activity.
- المراقبة والتحليل Monitoring and Analysis.
- الاتصالات والشبكات Networks and Communications.
- الاستجابة للمخاطر وإعادة الخدمة Risk Response and Recovery.
- إدارة عمليات أمن المعلومات Security Operations and Administration

4. شهادة ممارسة مهنة التحقيق الإلكتروني Certified Cyber Forensic Professional (CCFP): لنيل هذه الشهادة يتم اختبار الشخص في الموضوعات الآتية:
    1. المبادئ القانونية والأخلاقية Legal and Ethical Principles المتصلة بمجال المعلوماتية.
    2. التحقيق Investigations.
    3. علوم التحقيق في الجرائم الإلكترونية Forensic Science.
    4. التحقيق الإلكتروني Digital Forensics.
    5. تطبيقات التحقيق Application Forensics
    6. التقنيات الحديثة Hybrid and Emerging Technologies
5. شهادة مطور البرامج الأمنية للتطبيقات Certified Secure Software Lifecycle Professional (CSSLP) والتي تُعنى بدراسة الأمور التي تتعلق بأمن التطبيقات.

6. الشهادة المهنية لأمن المعلومات والخصوصية للنظام الصحي HealthCare Information Security and Privacy Practitioner (HCISPP): لنيل هذه الشهادة يتم دراسة كثير من الأمور المتصلة بأمن المعلومات في المجال الصحي مثل:
    1. مقدمة عن المجال الصحي والرعاية الصحية.
    2. قواعد وأسس تنظيم المجال الصحي.
    3. أمن المعلومات والخصوصية في المجال الصحي.
    4. تطوير البرامج للقطاع الصحي.
    5. تقييم المخاطر على نظم المعلومات الصحية.
    6. إدارة المخاطر.
    7. إدارة المخاطر المتصلة بالطرف الثالث (المريض).

الفصل الرابع

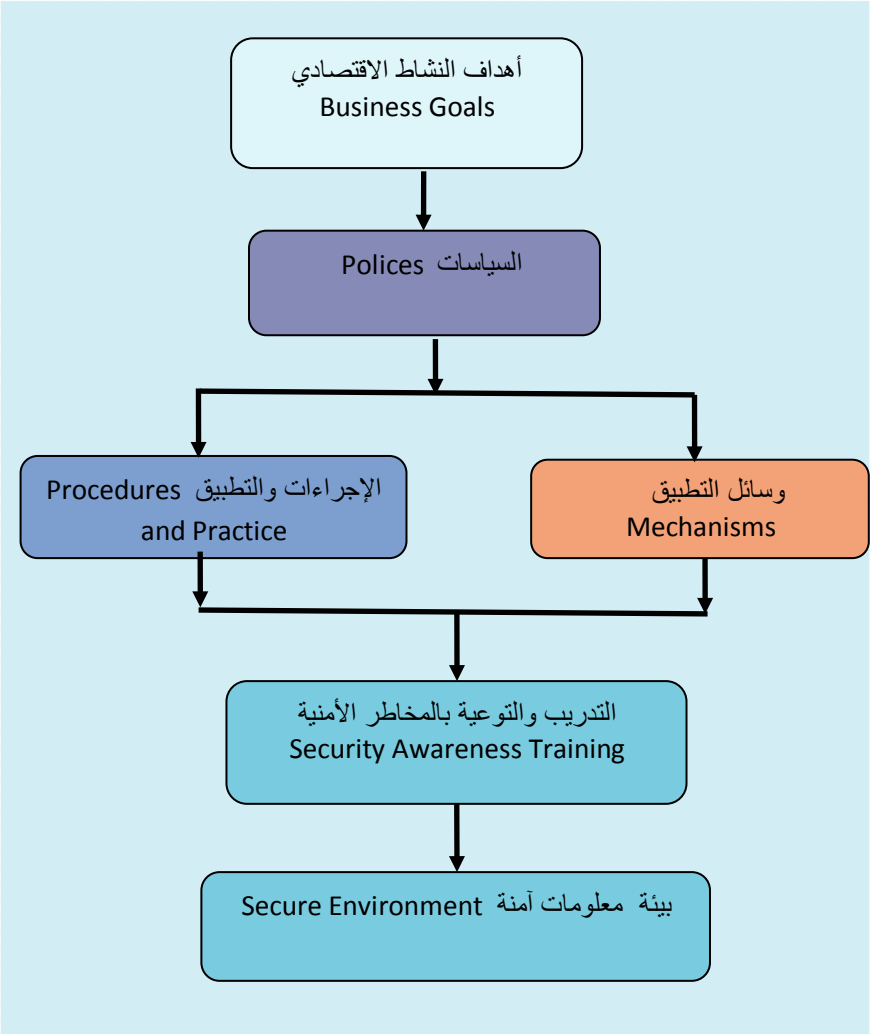
التخطيط وصياغة وبناء الإطار العملي والقانوني لحماية المعلوماتية

1.4 المقدمة

عملية إدارة أمن المعلومات من العمليات المعقدة والتي تحتاج إلى الكثير من العمل في كثير من الجوانب والمستويات الإدارية المختلفة. فالدولة يجب أن تضع أولاً الإطار القانوني الذي يحكم وينظم قطاع الاتصالات والمعلومات والأمور المتصلة بأمن المعلومات، ثم بعد ذلك يجب أن تطبق المؤسسات والمنظمات والقطاعات المختلفة هذه القوانين واللوائح، ثم تتبعها باللوائح الداخلية والسياسات الأمنية واستخدام التكنولوجيا المناسبة. في هذا الفصل نناقش العناصر الأساسية في عملية أمن المعلومات داخل المنظمات أو المؤسسات. في الفقرة 2.4 نناقش عملية التخطيط وبناء الإطار القانوني وفي الفقرة 3.4 ننافش موضوع التوعية والتعامل مع العنصر البشري. عملية التخطيط لاستمرارية الخدمات أو النشاط الاقتصادي يتم مناقشتها في الفقرة 4.4 والفقرة 5.4 تناقش الاستعداد للمخاطر وخطط التعافي من الكوارث.

2.4 التخطيط وبناء الإطار العملي والقانوني

في عالم اليوم ومع اختلاف الأنشطة البشرية التي تعتمد على المعلوماتية، فإنه يجب الإقرار بأن عملية وضع إطار ثابت للتخطيط لمهام أمن المعلومات عملية صعبة أو مستحيلة. اتفق الخبراء والمهنيون على إطار عملي عام وشامل موضح في الشكل 1.4 يمكن من خلاله لأيّ فني أو مهني متخصص من أن يضع الخطة التفصيلية لأمن المعلومات، وذلك اعتماداً على نوع وحجم النشاط الاقتصادي للمؤسسة وأهدافها العليا واللوائح والقوانين المنظمة للنشاط الاقتصادي في الدولة المعنية.



الشكل 1.4: الإطار العام لعملية إدارة أمن المعلومات.

حسب النموذج أو الإطار العام لعملية التخطيط لأمن البيانات والموضح في الشكل 1.4؛ فإن هذه العملية تبدأ بتحديد الأهداف العامة حسب النشاط الاقتصادي، فمثلاً عملية التخطيط لأمن المعلومات في المؤسسات التعليمية تختلف في الأهداف عن عملية التخطيط لأمن البيانات في المؤسسات الحكومية والخدمية الأُخرى، لذلك فإن عملية تحديد الأهداف هي عملية أساسية ومهمة في مرحلة تحديد الإطار القانوني. بعد عملية تحديد الأهداف يتم استخلاص السياسات العامة والتي منها يتم تحديد الوسائل التكنولوجية التي يجب استخدامها والإجراءات واللوائح التي يجب أن يتبعها الأفراد،

بالإضافة إلى إستراتيجيات التدريب والتوعية وذلك للوصول إلى البيئة المعلوماتية الآمنة في المؤسسة.

هذا هو الإطار العام لعملية التخطيط بصورة عامة، ويمكن للمُتخصص أن يستعين بالمنشورات والقوانين المنظمة للقطاع المعني في الدولة المحددة أو بعض المواصفات الدولية والإقليمية لتفصيل الخطط وتوضيحها بصورة أكثر. هنا يجب أن نشير إلى بعض المنشورات القيمة على سبيل المثال لا الحصر:

1. منشورات المركز الوطني الأمريكي للمواصفات والتكنولوجيا National Institute of Standard and Technology (www.NIST.gov) هذا الموقع يحتوي على الكثير والمفيد في مجال التخطيط لأمن المعلومات وحماية البنيات التحتية الحرجة والأساسية نذكر منها على سبيل المثال المواصفات القياسية الآتية:

- المواصفة NIST-SP800-12 توصف بصورة تفصيلية الموجهات العملية للتخطيط لأمن المعلومات التي يجب أن تتبعها المؤسسات في الولايات المتحدة [50].
- المواصفة NIST-SP800-13 توصف بصورة تفصيلية الموجهات العملية لأمن نظم إدارة الاتصالات Telecommunication Network Management[51]
- المواصفة NIST-SP800-30 والتي توصف بصورة تفصيلية التوصيات العامة بخصوص عملية إدارة المخاطر [52].
- المواصفة NIST-SP800-34 والتي توصف بصورة تفصيلية التوصيات العامة بخصوص عملية التخطيط لاستمرارية الخدمات [53].
- المواصفة NIST-SP800-37 والتي توصف بصورة تفصيلية الموجهات العامة بخصوص تطبيق نظام إدارة المخاطر [54].

- المواصفة NIST-SP800-53 والتي توصف بضورة تفصيلية عملية التحكم في نظم المعلومات الحكومية والمنظمات [55].
- المواصفة NIST-SP800-39 والتي توصف بصورة تفصيلية عملية إدارة المخاطر من حيث متطلبات التنظيم والأهداف [56].
- المواصفة NIST-SP800-82 والتي توصف بصورة تفصيلية الموجهات الأساسية لحماية نظم التحكم في العمليات الصناعية SCADA Systems [57].
- المواصفة NIST-SP800-66 والتي توصف بصورة تفصيلية الموجهات الأساسية لتطبيق معايير سلامة نظم المعلومات في المجالات الصحية (HIPAA) [58].

2. منشورات الاتحاد الدولي للاتصالات International Telecommunication Union (ITU) المتصلة بمجال السيبرسكيرتي CyberSecurity.
3. موارد مطلوبات شهادة أمن المعلومات CISSP.
4. منشورات الاتحاد الأوروبي المتعلقة بأمن المعلومات ونظم الاتصالات.
5. منشور الجمعية المفتوحة للتحكم في العمليات الصناعية Industrial Automation Open Networking Association وهو منشور مهم للعاملين في مجال التحكم في العمليات الصناعية [59].
6. المواصفة الأمريكية لحماية أنظمة الكهرباء للعام 2013م [60].
7. منشورات المجموعة الأمريكية المتحدة لتحليل بيانات وحركة الإنترنت Cooperative Association for Internet Data Analysis [61].
8. قاعدة بيانات الاستجابة للمخاطر المعلوماتية التابعة لجامعة بريتش كولمبيا الكنديةBritish Columbia Institute of Technology، Industrial Security Incident Database [62]

يجب أيضاً أن نشير إلى أن عملية أمن المعلومات وحماية البنيات التحتية الحرجة للمعلوماتية هي عملية تستهدف في المقام الأول التعامل مع العنصر البشري، لذلك يجب أن تكون من ضمن خطة أمن المعلومات في المنظمة أو المؤسسة عملية توعية ومشاركة Engagement للعناصر الفعالة في المؤسسة، وذلك من أجل التعريف بالإستراتيجية وزيادة كفاءة تنفيذها.

3.4 العوامل البشرية

العامل البشري هو العنصر الأهم في عملية أمن البيانات والبنيات التحتية الحرجة للمعلوماتية والاتصالات [63]. يمكن تقسيم المخاطر البشرية إلى نوعين:

1. العامل البشري الخارجي ونعني به االمورد البشري من خارج منظومة المؤسسة أو منظومة المعلومات.
2. العامل البشري الداخلي ونعني به المورد البشري الذي يتعامل بصورة مباشرة مع البيانات داخل المؤسسة.

من الصعب بمكان معرفة ما يمكن أن يعمله الإنسان في فضاء الإنترنت أو المعلومات، حينما يكون لوحدة ولا يراه أحد. عندئذ فقط يمكن أن نقول إن للقيم والمعتقدات (الأخلاق) دوراً فعّالاً في التحكم في التصرفات. هذه القيم والمعتقدات في كثير من الأحيان يمكن أن تهتز أو تنهار بسبب عوامل اجتماعية أو اقتصادية أو عدلية كثيرة. فالشخص الذي تم الاستغناء عن خدماته ضمن منظمة معينة، قد ينظر هو شخصياً إلى عملية فصله من العمل على أنها ظلم، أو أن الاستحقاق الذي ناله لا يُعادل ما قدمه من خدمات للمنظمة أو المؤسسة، وقد يشك في النظام العدلي القائم للمؤسسة أو البلد، بأنه قد لا يُوفر له الإطار الصحيح للتقاضي والعدالة. لذلك فإن مثل هؤلاء الأشخاص، قد يلجأ بعضهم لطرقه الخاصة لأخذ هذا الحق أو الإضرار بالمنظمة، بقدر ما يراه مناسباً لمقدار الظلم الذي لحق به. هذا كله بمظان أن هنالك أخلاقاً وقيماً، والتي لا يجوز أصلاً الاحتجاج بها أو الاعتماد عليها لحفظ حقوق الآخرين.

كيفية التحكم في العامل البشري

تقنياً وعملياً يمكن التحكم في العامل البشري بإحدى الوسائل الموضحة في المخطط الآتي:

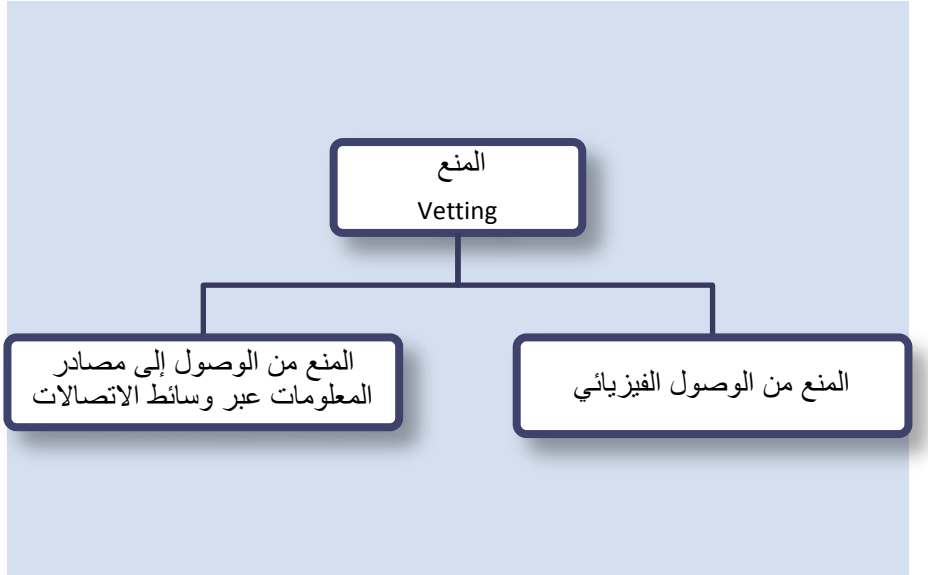
فالتدريب يخلق الوعي العام لدى العنصر البشري بالمعلومات وأهميتها في مجال النشاط الاقتصادي للمؤسسة [64]. على سبيل المثال الشخص المدرب يعرف جيداً متى وكيف يستخدم الإيميل الرسمي في المراسلات، وما هي طبيعة المعلومات المسموح بإرسالها حسب المستويات المختلفة للمخاطبات الرسمية. أيضاً يجب أن يعرف العنصر البشري كيف يتعامل مع مواقع الإنترنت المختلفة، والتي تطلب بعضاً من بياناته الرسمية. عموماً يجب أن تغطي عملية التدريب الفعالة الجوانب الآتية:

- التعريف بالمخاطر والآثار المترتبة على الهجمات الإلكترونية.
- وسائل وطرق الاختراق المعلوماتي.

المراقبة أيضاً من الوسائل الفعالة في التحكم في العامل البشري، حيث يمكن من خلالها تنفيذ وفرض السياسات والموجهات الخاصة بأمن المعلومات. يجب أيضاً من

الناحية العملية أن تصحب عملية المراقبة لوائح للعقاب، فالمراقبة من غير أسس ومعايير ثابتة للعقاب تعتبر عملية غير متناسقة (اعتباطية). لذلك يجب أن تضع المؤسسات والدول الأطر القانونية اللازمة لذلك.

المنع هو الوسيلة الأساسية في عملية أمن المعلومات والبنيات التحتية الأساسية للمعلوماتية. في كثير من الدول الغربية تسمى إدارة أمن المعلومات (Department of No) وذلك لكثرة استخدام لوائح المنع من قبل هذه الإدارة. تنقسم مستويات المنع إلى قسمين حسب المخطط الآتي:



كل الوسائل التقنية التي يمكن بها تحقيق عملية المنع سوف يتم مناقشتها في باب الوسائل التكنولوجية، لكن يبقى أن نشير هنا إلى أنه يجب أن تسبق عملية المنع عملية تصنيف شاملة للمعلومات والبيانات. هنالك عدة مناهج وطرق لعملية التصنيف، وبصورة عامة هناك نوعان يمكن الإشارة إليهما:

1. التصنيف حسب المستويات الإدارية، وهو تصنيف يصلح للمؤسسات الحكومية، وما يشبهها من منظمات. في التصنيف حسب المستويات الإدارية يتم تصنيف البيانات والمعلومات حسب الآتي:
   - معلومات حساسة (الأمور المالية والإدارية، تصاميم النظم، مواقع البنيات الأساسية).

- معلومات حساسة غير إستراتيجية (القرارات الإستراتيجية، معلومات الموارد البشرية).
- معلومات حساسة وإستراتيجية (معلومات المركز المالي، الأمن القومي، أماكن مستودعات المعلومات Data centers ...الخ).
- معلومات حساسة بصورة خاصة (البيانات الشخصية للأفراد وأمورهم المالية).

2. تصنيف المنظومات الصناعية، وفيه يتم تقسيم المعلومات إلى الآتي:
   - معلومات تخص ملكية النشاط الصناعي.
   - معلومات سرية خاصة بالنشاط الصناعي.

مهما كانت عملية التصنيف من حيث النوع أو النشاط الاقتصادي، يجب أن تسهم في النهاية في تسهيل وضع نظام إدارة قوي وفعال للمعلومات بما يحقق المصلحة العليا للمؤسسة. للذين يودون التفاصيل بصورة دقيقة عن نظم إدارة المعلومات يمكنهم الاطلاع على المواصفة الأمريكية NIST SP800-50 أو محتوى الشهادة CIISP الخاص بهذا الجانب.

4.4 التخطيط لاستمرارية الخدمات

نعني بمفهوم استمرارية الخدمات عملية إعادة خدمة نظام المعلومات أو منظومة العمل المعتمدة على المعلوماتية (البنية التحتية الحرجة) إلى الخدمة بصورة كلية أو جزئية، بعد حصول كارثة ما في النظام [65]. الكوارث على النظم المعلوماتية لها عدة أشكال نذكر منها الآتي:

- السرقة.
- الإتلاف أو الضياع الكلي كما في حادث 11 سبتمبر بالولايات المتحدة.
- التدمير أو توقف المنظومة الصناعية كما في حالة حادث تعطل وحدات العمل في المفاعل النووي الإيراني.
- عدم المقدرة على الوصول.

- ...إلخ (يمكن مراجعة الفصل المخصص لدراسة المخاطر).

يجب أن تُراعى في خطة استمرارية الخدمات الأهداف الرئيسية لمنظومة أمن البيانات (السرية، الخصوصية، توفر الخدمة). من أهم العناصر التي يجب أن تكون مشمولة في الخطة هي:

- سلامة مركز البيانات Data Center.
- استمرارية العمليات الموزعة.
- سلامة العنصر البشري -شبكات الاتصالات-مصادر الطاقة.

5.4 بناء وتطوير خطة التعافي من الكوارث

هي الموجهات والإجراءات التي تُمكن المنظمة أو المؤسسة من الاستجابة للمخاطر المعلوماتية وإعادة عملية تشغيل نظام المعلومات في فترة زمنية قصيرة [66]. من العوامل المهمة التي تجب مراعاتها في الخطة هي تكلفتها المالية وتأثيرها وعلاقتها بعملية التأمين وموافقتها للقوانين واللوائح المنظمة للنشاط الاقتصادي ويجب أن تكون مقنعة لكلٍّ من الآتي:

- الزبائن.
- الجهات التي تقوم بالمراجعة المعلوماتية.
- الجهات الحكومية المنظمة للنشاط الاقتصادي.
- العمال.
- المستثمرون.

العوامل الأساسية التي يجب أن تُراعى عند إعداد خُطة التعافي من الكوارث:

- رجوع النظام إلى الخدمة في زمن قياسي Timely Recovery of The Critical Operations
- تقليل الفاقد Minimize The losses

- الإيفاء بالمتطلبات والمعايير المحلية والعالمية Meet the Legal and Regulatory Requirement.

الفصل الخامس

التكنولوجيا المستخدمة فى حماية المعلوماتية

1.5 المقدمة

عملية استخدام التكنولوجيا في أمن المعلومات والاتصالات وحماية البنيات التحتية الأساسية الحرجة في عالم اليوم، تعتبر من الخطوات الأساسية التي يجب أن تقوم بها إدارة أمن المعلومات في المؤسسة أو المنظمة أو حتى تلك الجهات المنوط بها حماية المعلوماتية على مستوى الدول والمجموعات السياسية الإقليمية. هذا الفصل من الكتاب يتناول بالوصف أهم عناصر النظم التي تستخدم في أمن المعلومات. في الفقرة 2.5 يتم وصف أهم التقنيات المستخدمة في النظم المعلوماتية لتوفير ميزتي المراقبة والحماية من الوصول التخريبي إلى مستودعات المعلومات. في الفقرة 3.5 يتم وصف أهم نماذج نظم أمن المعلومات، والفقرة 4.5 تناقش أهم المعايير العالمية لتقييم النظم من حيث السلامة وقابلية الاختراق.

2.5 وسائل الحماية التقنية

مع تطور التكنولوجيا وزيادة اعتمادية الإنسان على المعلوماتية والاتصالات، تطورت الجريمة الإلكترونية وأصبح من غير الممكن الصبر على الخسائر المالية الناتجة من جراء الاعتداءات والاختراقات المعلوماتية. نتيجة لكل هذه المخاطر تم تطوير العديد من الوسائل التقنية التي يمكن أن تحارب وتحدَّ من هذه الظاهرة وبصورة فعالة. من أهم هذه التقنيات والتكنولوجيا الآتي:

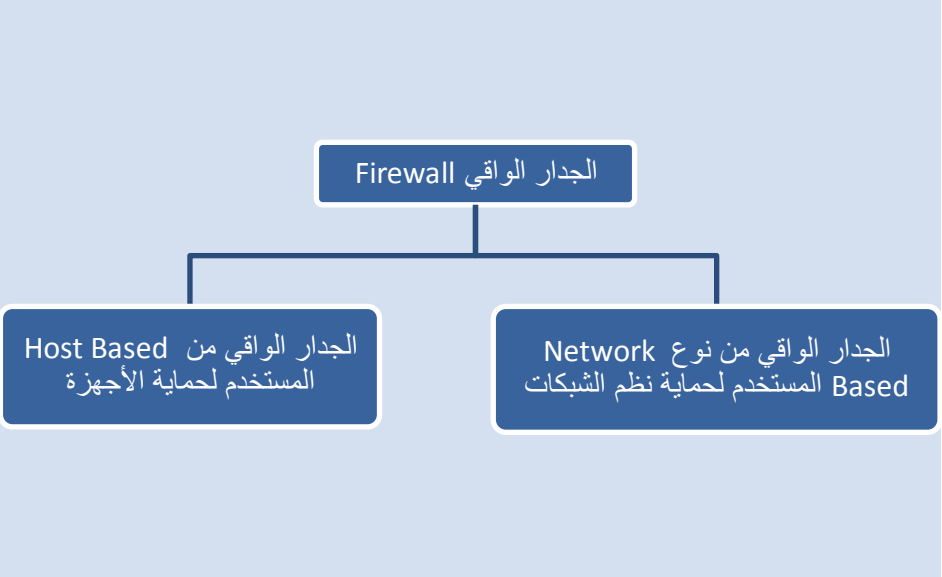
- الجدار الواقي Firewall
- كاشف الاختراق Intrusion Detections
- مضادات الفيروسات Anti-virus
- التحكم بالوصول Access Controls
- نظم التحقق Authentication Systems

- التشفير Encryption

طرق الإسناد Attribution Methods

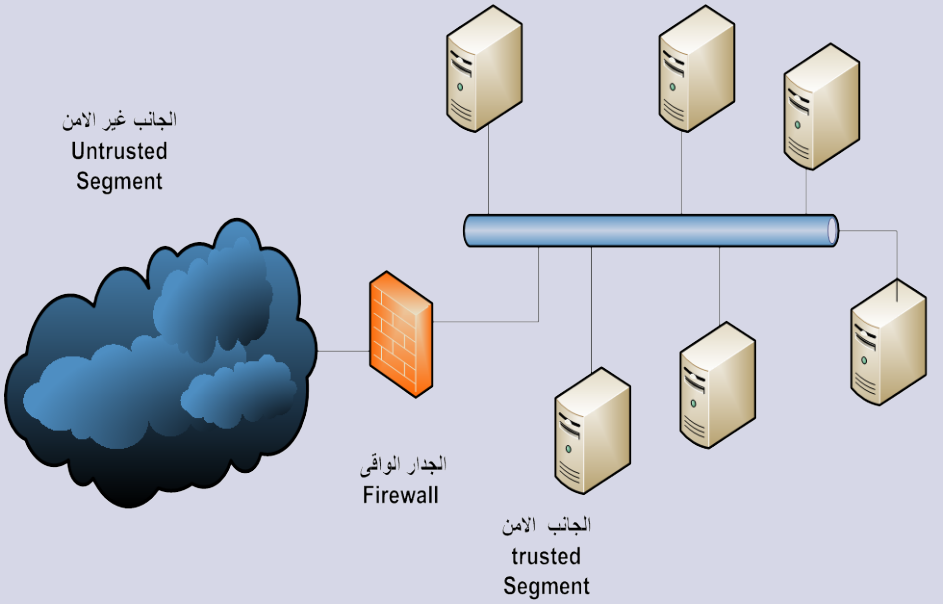
الجدار الواقي

الجدار الواقي هو أحد أهم الأدوات الفعالة في حماية شبكات المعلومات والاتصالات من الاختراق، ويتكون في الأساس من مكون برمجي Software منفصل، أو مكون برمجي معتمد على معمارية حاسوبية محددة Hardware Based System. الشكل 1.5 يوضح الأنواع المختلفة لأنظمة الجدار الواقي المستخدمة لحماية الأجهزة ونظم الشبكات.



الشكل 1.5: تصنيف نظم الجدار الواقي حسب الاستخدام.

يقوم الجدار الواقي المستخدم في حماية نظم الشبكات Network Based بالتحكم في حزم البيانات القادمة والمرسلة كما في الشكل 2.5 إذ يكون هو الحاجز بين الشبكة الآمنة والشبكة غير الآمنة، ويقوم بتحليل كل حزم البيانات، ويسمح بانتقالها حسب قواعد محددة يحددها المستخدم [67].



الشكل 2.5: استخدام الجدار الواقي من نوع Network Based لحماية المعلومات في الشبكة الخاصة.

ظهر الجيل الأول من أجهزة الجدار الواقي سنة 1989م، وكان يعمل على الطبقات الثلاث الأولى من الـ OSI System Model. اليوم مع تقدم التكنولوجيا يعمل الجيل الثالث من أجهزة الجدار الواقي على مستوى طبقة التطبيقات Application Layer إذ يقوم بالتحكم في الحزم المرسلة من كل التطبيقات وإليها. من أهم الخصائص التي يتم على أساسها تصنيف حزم البيانات هي:

- عنوان المرسل والمرسل إليه Source and Destination IP address.
- نوع البروتكول TCP/UDP.
- عنوان نهاية التطبيق (البرنامج) أو البورت Destination TCP and UDP ports
- عنوان بداية التطبيق (البرنامج) أو البورت. Source TCP and UDP ports

- المخرج الفيزيائي The Interface Where the Packet Arrives
- المدخل الفيزيائي The Interface Where the Packet is Destined

من أهم برمجيات الجدار الواقي المجانية والتي تعمل تحت نظم التشغيل Unix/Linux لينكس/ يونكس هي IPtable/IPchains، IPfilter، PF packet Filter ، NPF، IPFW. وأيضاً من أهم النظم والحزم التجارية Cyberoam، Eudemon، Microsoft's Internet Security and Acceleration (ISA) Server، Nortel Networks Alteon Switched Firewall System.

الجدار الواقي من النوع Host based firewall يستخدم لحماية الأجهزة داخل الشبكة من بعضها البعض ومن الأخطار الخارجية أيضاً. من أهم الأنظمة المستخدمة لهذا الغرض Internet Connection Firewall (ICF—included with Windows XP and Windows Server 2003). لأغراض الحماية المتكاملة للكثير من الأنشطة التجارية يُنصح باستخدام النوعين مع بعضهما.

كاشف الاختراق

نظم كشف الاختراق Intrusion Detections Systems (IDS) هي عبارة عن برامج تعمل على تجميع وتحليل كمية كبيرة من البيانات داخل الشبكة بغرض التعرف على أيّ اختراق أو تهديد من داخل أو خارج النطاق [68, 69]. من الأساسيات التي يتم على ضوئها تحليل البيانات هي:

- مراقبة وتحليل نشاطات المستخدمين.
- تحليل برمجيات النظم.
- معرفة وتتبع أنماط الاختراق.
- تحليل وتتبع النشاطات غير العادية.
- تتبع ومراقبة انتهاكات سياسة المستخدمين.

تم تطوير نظم كاشف الاختراق نتيجة للعدد المتزايد من الهجمات على المواقع والشبكات الرئيسية مثل وزارة الدفاع الأمريكية والبيت الأبيض ومنظمة حلف شمال الأطلسي. يوماً بعد يوم تتزايد أهمية حماية المعلومات، وذلك لأن تكنولوجيا الهجوم الإلكتروني أصبحت أكثر تطوراً من أي وقت مضى، وفي الوقت نفسه فإن هنالك سهولة في الوصول إلى أساليب وطرق الاختراق المستخدمة في الماضي من خلال شبكة الإنترنت.

من أهم برمجيات كشف الاختراق المجانية التي يمكن الاستعانة بها في عملية التعلم:

- برنامج Advanced Intrusion Detection Environment (AIDE)
- برنامجCARM-ng (Alert Correction، and Assessment Reaction Module - Next Generation)
- برنامج Bro NIDS ويستخدم لكشف الاختراق في الشبكات.
- برنامج OSSEC HIDS: يستخدم لكشف الاختراق على الأجهزة والبرامج.
- برنامج Prelude Hybrid IDS: يمكن أن يعمل على مراقبة الشبكات الكبرى والنظم الموزعة وباستخدام عناصر ومتغيرات متعددة.
- برنامج Samhain ويستخدم لحماية الأجهزة والنظم المعتمدة على نظام اليونكس.
- برنامج Snort: يستخدم لحماية أنظمة التحكم الإشرافي التي تستخدم في التحكم وإدارة نظم الإنتاج الصناعية [70].
- برنامج Suricata: تم تطوير هذا البرنامج بواسطة منظمة Open Information Security Foundation(OISF) في العام 2010م [71].

من المنتجات التجارية المشهورة في كشف الاختراق Network Intelligent Police (NIP)، Cisco IDS 4250، Cisco IDS 4230. جميع أنظمة كشف الاختراق تستخدام واحداً من اثنين من تقنيات الكشف:

- الطرق الإحصائية Statistical anomaly-based IDS [72].
- طرق مقارنة أنماط الاختراق Signature-based IDS [73].

مضادات الفيروسات

فيروس الحاسوب، هو عبارة عن مكون برمجي يصنع عمداً بغرض تغيير خصائص الملفات التي يصيبها، لتقوم بتنفيذ بعض الأوامر، إما بالإزالة أو التعديل أو التخريب وما شابهها من عمليات. أي أن فيروسات الحاسوب هي برامج تتم كتابتها بواسطة مبرمجين محترفين بغرض إلحاق الضرر بجهاز حاسوب آخر، أو السيطرة عليه أو سرقة بيانات مهمة منه، وتتم كتابتها بطريقة معينة. مضادات الفيروسات هي عبارة عن برامج معدة بواسطة خبرة عالية، وذلك لمسح الفيروسات والتخلص من آثارها التدميرية وباستعادة الملفات التالفة وما إلى ذلك من خصائص إيجابية. تعتمد مضادات الفيروسات على نظم برمجة ذكية، وقاعدة بيانات غنية بالأنماط المنتشرة للفيروسات، تتمكن من خلالها من اكتشافها وذلك بتتبعها للأنشطة وعمليات الحوسبة المختلفة.

التحكم بالوصول إلى المصادر المعلوماتية

التحكم في الوصول Access Controls في مجال المعلوماتية وأمن البيانات يعني تنفيذ تحكم انتقائي في عملية الوصول إلى مكان أو مورد ما من موارد البيانات، ويسمى الإذن بالوصول إلى البيانات أو المورد بالترخيص Authorization. هنالك طبقتان من نظم التحكم في الوصول يجب تطبيقهما على نظم المعلومات الإستراتيجية هما:

- التحكم بالوصول الفيزيائي Physical Access Control
- التحكم في الوصول للنظام System Access Control

نظم ووسائل التحقُّق

عملية التحقق هي عملية التعرف الإلكتروني والمصادقة، وذلك من أجل السماح للمستخدم بالوصول إلى موارد البيانات أو النظام بصورة عامة. النظم الإلكترونية في

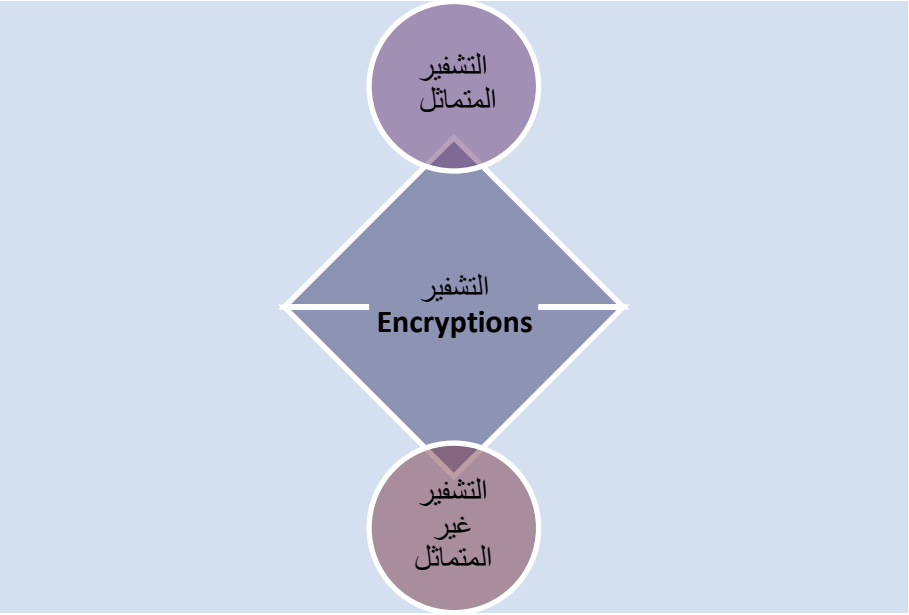
عالم اليوم تعتمد على عدة عناصر للتحقق الإلكتروني والمصادقة الإلكترونية نذكر منها ما يلي:

- المصادقة بناءً على شيء معروف للمستخدم مثل (كلمة المرور Password، رقم التعريف شخصي Personal Identification Number، نمط محدد Pattern كما في نظم الأندرويد).
- المصادقة بناءً على شيء مملوك بواسطة المستخدم (كرت الـATM، smart card، رقم الهاتف).
- المصادقة بناءً على عنصر أو شيء يعتبر جزءاً من المستخدم، أو ما يُعرف بالخصائص البيومترية Biometric characteristic مثل الآتي [74]:
  - بصمة اليد fingerprint recognition
  - التعرف على الوجه face recognition
  - التعرف على الصوت voice recognition
  - التعرف على طريقة الضغط على المفاتيح Keystroke Recognition
  - التعرف على طريقة الكتابة باليد Handwriting Recognition
  - التعرف على شكل اليد والأصابع Finger and Hand Geometry
  - بصمة العين Retinal Scan
  - التعرف على قزحية العين Iris Recognition

من الناحية العملية، فإن أغلب النظم اليوم تستخدم طرقاً متعددة العناصر للمصادقة Multi-factor Authentication وذلك لزيادة درجة الموثوقية في عملية الحوسبة.

تشفير المعلومات

التشفير هو عملية ترميز الرسائل أو المعلومات بطريقة ما، ليصعب التعرف عليها بواسطة الأشخاص غير المرخص لهم قراءتها. نظام التشفير يقوم بتشفير الرسالة أو المعلومات باستخدام ما يعرف بخوارزمية التشفير، إذ يتم تحويلها إلى نص مشفر غير قابل للقراءة. وعادة ما يتم هذا باستخدام ما يُعرف بمفتاح التشفير، والذي يحدد كيفية تشفير الرسالة. أي شخص غير مرخص له لا يمكن أن يرى النص المشفر ولا يمكنه تحديد الرسالة الأصلية. من الناحية الأخرى أيضاً، فإن أيَّ شخص مرخص له يمكنه فك شفرة النص المشفر باستخدام خوارزمية فك التشفير والتي تستخدم عادة ما يُعرف بمفتاح فك التشفير السري. عملياً هناك طريقتان للتشفير هما التشفير المتماثل والتشفير غير المتماثل.



1. التشفير المتماثل Symmetric-key Encryption وفيه يكون مفتاح التشفير هو نفسه مفتاح فك التشفير. من أهم الخوارزميات:-
   - خوارزمية Twofish
   - خوارزمية Serpent
   - خوارزمية Advanced Encryption Standard (AES)

- خوارزميات CAST5،Blowfish

2. التشفير غير المتماثل Asymmetric Key Techniques أو ما يعرف Public-key Encryption وفيه يتم توزيع مفتاح التشفير للكل مع إتاحة مفتاح فك التشفير للمستقبل المطلوب فقط. مثال لذلك:

- خوارزمية Diffie–Hellman key Exchange
- خوارزمية Digital Signature Standard (DSS)
- طرق تشفير ما يعرف ب Elliptic Curve Encryption
- خوارزمية Paillier Cryptosystem
- طرق ما يعرف Password-Authenticated key Agreement
- خوارزمية RSA
- خوارزمية McEliece Cryptosystem
- خوارزمية Merkle–Hellman Knapsack Cryptosystem

أيضاً من أهم التطبيقات التي تعمل بخوارزميات تشفير غير المتماثل:-

- تطبيق GPG
- تطبيق Internet Key Exchange
- تطبيق ZRTP،A Secure VoIP Protocol
- تطبيق Secure Socket Layer
- تطبيق SILC
- تطبيق SSH

طرق إسناد الجريمة المعلوماتية الى الجانى

نعني بالإسناد عملية نسب محتويات الجريمة إلى الجاني. هذه العملية تعتبر خطوه أساسية لعمل وتحقيق الأهداف المتصلة بالإطار القانوني، والذي سوف نتطرق له فيما بعد [75]. عملية إسناد الجريمة إلى الجاني من العمليات التقنية والتخصصية البحتة

التي لا تسمح المساحة في هذا الكتاب بتناولها بصورة تفصيلية، لكن هذا لا يمنع من أن نعطي القارئ فكرة أولية عن بعض من المتطلبات الأساسية لهذه العملية. مثلاً فيما يتعلق بنظم الشبكات، فإنه هنالك العديد من الطرق المتبعة لتحقيق عملية الإسناد الإلكتروني بصورة صحيحة ودقيقة. الجدول 1.5 يشرح بعض من طرق الإسناد المستخدمة في مجال أمن الشبكات ونظم الاتصالات.

الجدول 1.5: شرح لبعض طرق إسناد الجريمة الإلكترونية

طريقة الإسناد	الوصف/ شرح مبدأ العمل
طريقة Hash based IP traceback **[76]**	تقوم الموجهات أو Routers بحفظ قيم هاشت للحزم لتقوم بعد ذلك بالمتابعة العكسية لهذه القيم حتى تتمكن من الوصول إلى المصدر.
طريقة Overlay network for IP traceback**[77]**	في هذه الطريقة يجب أن ترسل جميع الموجهات (Routers) في الشبكة كل الحزم المشتبه بها إلى موجه مركزي ليقوم بعملية التحليل ليتمكن من تحديد المصدر.
طريقة Ingress Filtering**[78]**	في هذه الطريقة تقوم الموجهات على أطراف الشبكة بالتحقق من عناوين المصادر لجميع الحزم التي تدخل إلى الشبكة
طريقة ICMP return to sender	هذه الطريقة مفيدة في حالة الهجوم من نوع DOS حيث تقوم الموجهات بإيقاف سيل الحزم المرسلة إلى الضحية وإرسال حزم من نوع "لم يتم الوصول إلى المرسل إليه" في الاتجاه المعاكس وتتبعها حتى الوصول إلى المصدر.
طريقة Hackback**[78]**	تعتمد هذه الطريقة على إدخال نظام بمقدورة البحث عن الثغرات التي اعتمد عليها الجاني للقيام بالهجوم. فيقوم هذا النظام بتتبع هذه الثغرات للتمكن من الوصول

	إلى الجاني
طريقة Honeypots	هذه النوعية من الأنظمة تعمل على خداع الجاني حتى تتعرف علية بصورة أكثر.
طريقة Watermarking	تعتمد هذه الطريقة على أن تضع بعض الموجهات بصمات على البيانات حتى تتمكن في النهاية من الوصول إلى الجاني.
طريقة Probabilistic packet marking	تعتمد هذه الطريقة على قيام بعض الموجهات بإدخال معلومات عن مسار الحزمة بصورة اختيارية.

3.5 نماذج تصميم نظم أمن المعلومات

نموذج أمن المعلومات هو عبارة عن طريقة مجربة بالخبرة لتطبيق سياسات أمن المعلومات في القطاع أو النشاط الاقتصادي المحدد. نسبة لتعدد النشاطات البشرية التي تعتمد على المعلوماتية والاتصالات في عالم اليوم، لذلك ومن الناحية العملية نجد أن هنالك العديد من النماذج العملية لحماية المعلوماتية نذكر منها ما يلي:

- نموذج التحكم في الوصول Access Control List (ACL)
- نموذج Bell–LaPadula Model
- نموذج Clark–Wilson
- نموذج Context-based access control
- نموذج Graham-Denning Model
- نموذج Lattice-Based Access Control (LBAC)
- نموذج Brewer and Nash model
- نموذج Capability-BasedSecurity
- نموذج Multiple Levels of Security (MLS)
- نموذج Non-interference

- نموذج Role-Based Access Control (RBAC)

يمكن للمصمم أن يختار النموذج المناسب لتصميم نظام أمن المعلومات وذلك حسب مجال استخدام التطبيق.

4.5 معايير اختبار وتقييم نظم المعلومات

معايير تقييم وتحديد سلامة النظم المعلوماتية والاتصالات، تعتبر من العمليات الخاصة بالبلدان والمنظومات الإدارية والسياسية لكل دولة. الجدول 2.5 يوضح أهم المعايير الدولية، والتي أيضا تستخدم على نطاق واسع في عملية تقييم النظم.

الجدول 2.5: أهم المعايير التي يتم بها تقييم منتجات أمن المعلومات

المواصفة	الاعتماد
معايير السلامة لتقييم نظم الحاسوب Trusted Computer System Evaluation Criteria (TCSEC)	الولايات المتحدة
معايير تقييم تكنولوجيا المعلومات Information Technology Security Evaluation Criteria (ITSEC)	فرنسا- ألمانيا- المملكة المتحدة- الاتحاد الأوربي
المعايير المشتركة Common Criteria or CC	مواصفة دولية international standard (ISO/IEC 15408)
المعايير الكندية لتقييم سلامة النظم Canadian Trusted Computer Product Evaluation Criteria	كندا

الفصل السادس

التحقيق والمتابعة الإلكترونية والإيفاء بالمتطلبات والمعايير

1.6 المقدمة

الجريمة الإلكترونية من الجرائم المعقدة في عالم اليوم، وذلك نسبة لاعتمادها على عناصر التكنولوجيا والمعلوماتية الحديثة. لتعقب هذا الشكل الحديث من الجرائم، كان لا بد من استحداث مجال جديد يُعنى بدراسة كل الجوانب المتعلقة بهذه الجريمة. علم التحقيق والمتابعة الإلكترونية Digital Forensics هو المجال الذي يُعنى بدراسة جميع الأمور المتعلقة بالجريمة المعلوماتية في جميع مراحلها. في هذا الفصل نتناول في الفقرة 2.6 الجوانب الأساسية في مجال التحقيق الإلكتروني. الفقرة 3.6 تلخص وتُعرِّف عملية مراجعة نظم المعلومات ومطابقتها للمعايير؛ وفي الفقرة 4.6 نناقش عملية كتابة التقارير عن سلامة وأمن نظم المعلومات.

2.6 علم الأدلة الإلكترونية

في ظل الثورة العالمية السريعة في مجال المعلومات والاتصالات تطورت الجريمة المعلوماتية أو الإلكترونية، فتمَّ السطو على البنوك باستخدام تكنولوجيا الاتصالات والمعلومات. في السنوات القليلة الماضية نمت الجريمة المنظمة وانتشرت بصورة سريعة، خاصة تلك المرتبطة بالإرهاب وتجارة المخدرات والاتجار بالسلاح والدعارة المنظمة باستخدام الإنترنت. أُرتكبت أيضاً العديد من الجرائم التقليدية كالسرقة والنصب وخيانة الأمانة، وتزوير المحررات، والاعتداء على حرمة الحياة الخاصة، وعلى البيانات الشخصية، والتجسس. وظهرت جرائم ملازمة للتقنيات الحديثة، منها الغش الإلكتروني بالتلاعب في المدخلات وفي البرامج، والنسخ غير المشروع للبرامج، والعديد من الجرائم المتعلقة بالتجارة الإلكترونية والنظم، مثل

إتلاف الأجهزة الإلكترونية، وإتلاف السجلات المدونة على الحاسب الآلي، وبث الصور أو الأفلام الإباحية باستخدام وسائل الاتصالات، والقذف أو السب عن طريق الرسائل، وغسل الأموال [79].

تكمن الخطورة في هذه الظواهر الإجرامية الحديثة في أن الجريمة يسهل ارتكابها على هذه التكنولوجيا، وأن تنفيذها يتم في زمن وجيز أو أحياناً يتم في بضع ثوان. في حالاتٍ كثيرة في مثل هذه الجرائم الإلكترونية، يلجأ الجاني إلى محو آثار الجريمة وإتلاف أدِلتها عقب ارتكابه الجريمة، فضلاً عن أن مرتكبي هذه الجرائم، وبالذات في مجال الجريمة المنظمة، يلجأ البعض منهم إلى تخزين البيانات المتعلقة بالأنشطة الإجرامية في أنظمة إلكترونية، مع استخدام شفرات أو رموز سرية لإخفائها عن أعين الأجهزة الأمنية والعدلية. هذه المعضلة تثير كثيراً من المشكلات في عملية جميع الأدلة الجنائية وإثبات هذه الجرائم (نسب مخلفات الجريمة إلى الجاني).

علم الأدلة الإلكترونية، أو ما يعرف بالـ Digital Forensics هو أحد مجالات البحث العلمي الحديثة، ويُعنى بموضوع جمع الأدلة الإلكترونية، بغرض استخدامها في عملية الاستجابة والرد على الهجمات الإلكترونية أو استخدامها في عمليات وإجراءات التقاضي لاحقاً. يتفرع علم الأدلة الإلكترونية إلى التخصصات الآتية [80]:-

أهم العمليات التي يجب القيام بها عند القيام بعملية تحضير الأدلة الإلكترونية هي:

- حَجْر المصدر Seizure (وهذا غالباً ما يحتاج إلى أمر قضائي حسب الإطار القانوني للتقاضي في الدولة).
- جمع الأدلة Acquisition
- التحليل Analysis
- الإسناد Attribution
- رفع التقرير النهائي Reporting

بعض وسائل التحقيق الإلكتروني

توجد من الناحية العملية العديد من الوسائل الحديثة، التي تستخدم في عملية جمع الأدلة والتحقيق الإلكتروني (برمجيات ونظم متكاملة). الجداول أدناه 3.6-1.6 تلخص بعض البرامج المجانية (من مكتبة المصادر المفتوحة) والتي تستخدم في عملية تحضير وجمع الأدلة الإلكترونية، والتي يمكن الاستفادة منها في مجال التدريب والاستعانة بها عملياً في نطاق محدود:

الجدول 1.6: بعض أدوات جمع الأدلة من الحاسوب Computer Forensics tools

اسم البرنامج	بيئة العمل/ نظام التشغيل
SANS Investigative Forensics Toolkit - SIFT	Ubuntu
Digital Forensics Framework	Windows / Linux
The Sleuth Kit	Unix-like/Windows
Open Computer Forensics Architecture	Linux
CAINE	Linux
Dumpzilla	Windows / Linux

الجدول 2.6: بعض أدوات جمع الأدلة من وسائل التخزين Memory Forensics tools

اسم البرنامج	بيئة العمل/ نظام التشغيل
CMAT	Windows
Volatililty	Windows & Linux
Volatililty	Linux

الجدول 3.6: بعض أدوات جمع الأدلة في الشبكات Network Forensics tools

اسم البرنامج	بيئة العمل/ نظام التشغيل
WireShark	Windows / Linux
NetworkMiner	Windows / Linux

Tcpflow	Windows / Linux
NetSleuth	Windows

الإشكالات القانونية لعملية جمع الأدلة والتحقيق الإلكتروني

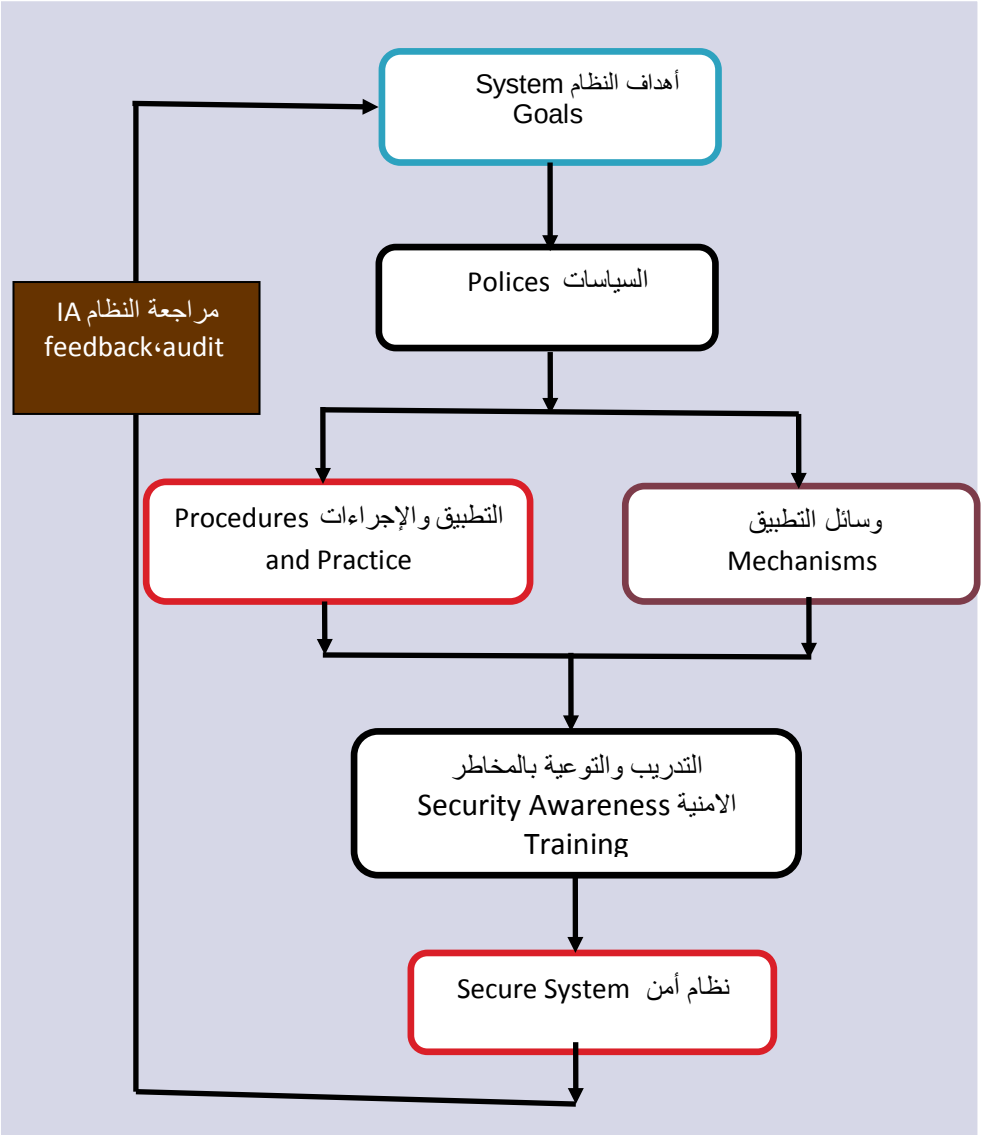
تُعاني الكثير من الدول من نقص كبير في الخبرة في مجالات التشريع وتطبيق وصياغة القوانين الخاصة بجرائم المعلوماتية والاتصالات والبنيات التحتية الحرجة، فالمؤسسات التشريعية والعدلية القائمة في كثير من البلدان تنقصها الخبرة والتدريب اللازم لبناء وتطبيق الموجهات القانونية الخاصة بهذا النوع من الجرائم المستحدثة. من أهم الإشكالات التي تُعاني منها الكثير من الدول في هذا الخصوص ما يلي:

- طبيعة الجرائم الإلكترونية غالباً ما تكون متعدية للحدود السياسية والإدارية للدول (Transnational). هذه الطبيعة تحد وبصورة كبيرة عملية التحقيق في الجرائم وتحقيق أهداف الإطار القانوني.
- تطوير وسائل (برامج ونظم متكاملة) ذات موثوقية كبير وفقاً لمعايير متفق عليها لتُستخدم في عمليات جمع الأدلة والتحقيق الإلكتروني. في الولايات المتحدة الأمريكية مثلاً هنالك معايير ثابتة لتطوير هذه الوسائل يمكن الاطلاع عليها في المرجع رقم [81].
- بناء الموجهات والأطر القانونية التي تحكم وتحدد متى وكيف تستخدم هذه الوسائل ودرجة الاعتمادية على مخرجاتها حسب الجرائم المختلفة. الاستخدام الاعتباطي لهذه الوسائل في كثير من الأحيان يؤدي إلى انتهاك حرية المعلومات وحرية الفرد، وهذا جانب سالب. في هذا المجال قامت أيضاً وزارة العدل الأمريكية بجهد كبير، وذلك بإصدار موجهات عامة بهذا الخصوص يمكن للقارئ الاطلاع عليها في المرجع رقم [82].

- تدريب وتأهيل الكوادر البشرية من (قضاء- ادعاء عام- محامين- لجان التشريع والعدل- رجال الشرطة المعلوماتية) التي تعمل في هذا المجال على مستوى الدولة.
- إعداد التشريعات اللازمة والخاصة بالعقوبات في ما يتعلق بالجرائم المعلوماتية.

3.6 المراجعة والمطابقة

عملية مراجعة نظم أمن المعلومات، هي عملية تقييم شاملة لمكونات النظام وخطط الطوارئ واختبارها لمعرفة مقدرتها على التصدي للكوارث المعلوماتية المحتملة، وأيضاً مطابقتها للمعايير والمواصفات وإصدار تقرير شامل بذلك [83]. بما أن أحد أهداف عملية المراجعة هو تقديم المشورة والنصيحة لإدارة أمن المعلومات في المنظمة أو المؤسسة، فإنه من الناحية العملية يجب أن تتوفر لجهاز أو جهة المراجعة المعرفة الكاملة بالتفاصيل التقنية والأُطر القانونية التي تم على أساسها صياغة الأهداف والسياسات العامة لأمن المعلومات في المؤسسة. كما هو موضح في الشكل 1.6، حيث تُمثل مخرجات عملية المراجعة (توصيات ونصائح) أهم مُدخلات عملية تعديل وصياغة الأهداف والسياسات المستقبلية.



الشكل 1.6: الإطار العام لإدارة أمن نظم المعلومات.

تشمل عملية المراجعة إجراء كلٍّ من الاختبارات الآتية:

1. المناعة ضد المخاطر Security Risks والتي تشمل بدورها اختبار كل من الآتي:
   - اختبار معمارية نظام (بالنسبة للاتصالات والشبكات)
   - اختبار السياسات واللوائح ومطابقتها للمواصفات والمعايير.

- اختبار سلامة البرمجيات.
- اختبار سلامة شبكات الاتصالات ومقدرتها على العمل في حالة المخاطر.

2. السيطرة على المعلومات Controlling Over Data
3. سلامة وحدات التخزين والتخرين في مكان بديل Adequacy of Backup and Off-site Storage

تبدأ عملية المراجعة بجمع الأدلة وتحليلها ومن ثم كتابة تقرير شامل بحالة نظام أمن المعلومات في المؤسسة أو المنظمة [84, 85]. من أهم الوسائل التقنية التي تستخدم في اختبار كفاءة نظم المعلومات ومناعتها ضد الاختراق؛ نظم تعرف بكواشف الاختراق Penetration Testing وهي نظم تقوم بالعمليات الآتية:

- تحديد قابلية النظام لبعض أنواع الهجمات.
- تحديد المخاطر الكبرى التي يمكن أن تحدث نتيجة لتوالي أو تسلسل وقوع مجموعة من المخاطر الصغيرة.
- تحديد مدى الخسائر في حالة وقوع بعض الأنواع المحددة من الهجمات.
- اختبار مدى وقدرة تصدي أجهزة حماية الشبكات للهجمات الإلكترونية والقرصنة المعلوماتية.
- تقديم الدليل المادي للإدارة العليا لزيادة الصرف المالي على قطاع أمن المعلومات.

الجدول 4.6 التالي يوضح بعض النظم، والبرامج التي تستخدم في اختبارات كشف الاختراق.

الجدول4.6: بعض النظم والبرامج التي تستخدم في اختبارات كشف الاختراق.

البرنامج	الإصدار الأخير
System Administrator's Integrated Network Tool (SAINT)**[86]**	2002م

Open Vulnerability Assessment System (OpenVAS)**[87]**	2013م
Metasploit Project**[88]**	2009م
Pentoo Penetration Testing tool**[89]**	2013م
BackBox**[90]**	2013م
IT Health Check(ITHC)**[91]**	2010م
Burp Proxy**[92]**	2013م
Nessus Vulnerability Scanner**[93]**	2012م
Ollydbg**[94]**	2012م
Nmap**[95]**	2012م

4.6 تقييم النظم: المتطلبات والمعايير

تختلف معايير عملية تقييم ومراجعة نظم المعلومات باختلاف البلدان، وذلك لاختلاف القوانين المنظمة لسلامة وأمن المعلومات في كل بلد. فيما يلي نستعرض أهم المعايير والمواصفات الواسعة الانتشار:

- المواصفة [96] Control Objectives for Information and Related Technology (COBIT): تم إعداد هذه المواصفة بواسطة اتحاد مراجعة نظم المعلومات (ISACA) في 1996. تمت مراجعة هذه المواصفة عده مرات، آخر إصدار منها يعرف بـ COBIT 5 تم إصداره في العام 2012م.
- المواصفة ISO17799/BS7799:2000 وهي مواصفة شاملة لإدارة أمن المعلومات تم إصدارها بواسطة هيئة المواصفات الدولية [97, 98] International Standard Organization.

- المواصفة Federal Information Security Management Act of 2002: وهي مواصفة أمريكية تعتمد على تفصيل مواد القانون الفيدرالي لأمن المعلومات للعام 2002م، والخاص بأمن المعلومات في نظم الحكومة الإلكترونية والخدمات الحكومية [99].
- المواصفة NIST-SP800 وهي سلسلة من المواصفات الخاصة بأمن الحاسوب والبيانات، وتشمل جميع مكونات أمن النظم من عمليات منع الاختراق إلى استعادة تشغيل النظم بعد الكوارث المعلوماتية [100].
- الاستعانة بقاعدة البيانات national Vulnerability Database الأمريكية (http://nvd.nist.gov/)، وهي مستودع غني بالخبرات الإنسانية في مجال بناء نظم أمن المعلومات ومكافحة الجرائم الإلكترونية.
- قانون التأمين والرعاية الصحية The Health Insurance Portability and Accountability Act of 1996 (HIPAA).

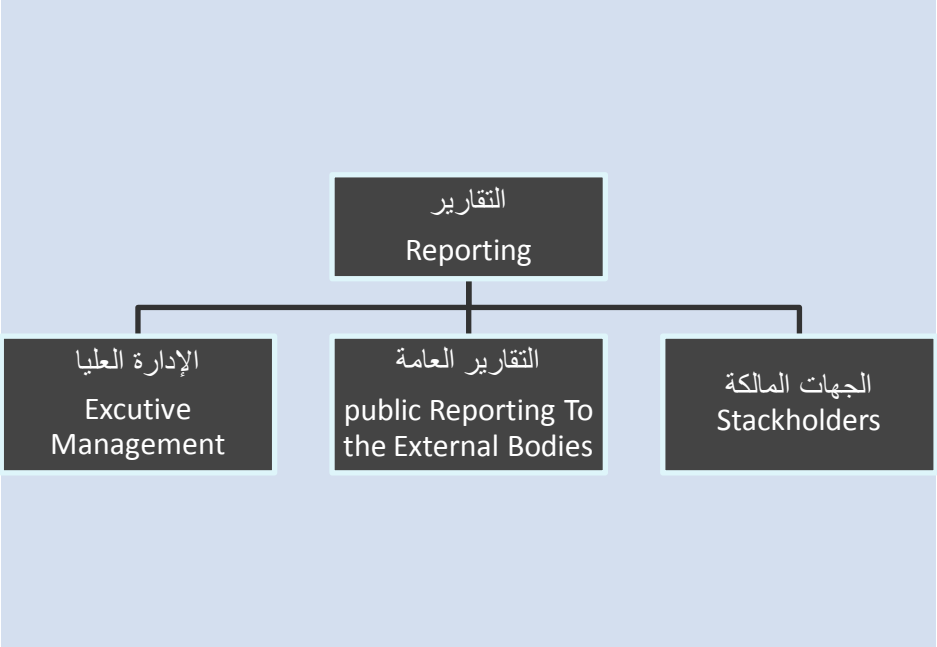
5.6 كتابة التقارير عن سلامة النظم

كتابة التقارير هي عملية إخبارية في المقام الأول، حيث تشمل إخبار الجهات الأساسية الموضحة في الشكل 2.6 عن بنية وحالة نظام أمن المعلومات. كتابة التقارير عن حالة النُظم المعلوماتية والبنيات الأساسية للاتصالات تشمل الإخبار عن كل الجوانب المتعلقة بالنظام في المؤسسة أو المنظمة. من أهم الجوانب التي يجب أن يركز عليها أي تقرير:

- تحقيق النظام للأهداف والسياسات المعلوماتية للمنظمة Policy Compliance.
- كفاءة نظام إدارة المخاطر Risk Management.
- كفاءة نظام الاستجابة للهجمات والمخاطر المعلوماتية Incident Response Management.

- التجاوزات والخروقات على السياسات العامة واللوائح في الفترة التي شملها التقرير.
- كفاءة التدريب وبناء القدرات.
- كفاءة والوسائل التكنولوجية المستخدمة في حماية الشبكات.

● كفاءة نظام تبادل الخبرات.



- الشكل 2.6: الجهات التي يجب أن يذهب إليها تقرير مراجعة نظام أمن المعلومات.

الفصل السابع

مواقع التواصل الاجتماعي وحماية الأطفال والأُسرة عند النفاذ

1.7 المقدمة

مواقع التواصل الاجتماعي هي تلك المواقع التي تعمل على خلق التواصل والتفاعل الاجتماعي بين المستخدمين في الفضاء الافتراضي، وذلك من خلال بوابات النقاش وتبادل المعلومات والأفكار. مع تقدم ثورة الاتصالات وانتشار الإنترنت عملت هذه المواقع على خلق أشكال وأنماط حديثة للتفاعل والتغير الاجتماعي والسياسي والاقتصادي في العالم [101]. هذا الفصل من الكتاب يتناول بعضاً من المهددات، والجوانب المرتبطة بأمن المعلومات وعلاقتها بشبكات التواصل الاجتماعي. الفقرة 2.7 تتناول التصنيفات الأساسية لمواقع التواصل الاجتماعي. الفقرة 3.7 تلخص بعض من المهددات التي يمكن أن تسببها هذه المواقع وفي الفقرة 4.7 تم التمهيد لمبدأ حاجة الإنسانية إلى الأطر القانونية، وذلك للتعامل مع الكثير من الإشكالات التي يمكن أن تنشأ نتيجة لتعامل الإنسان مع هذه المواقع. الفقرة 5.7 تناقش موضوع حماية الأطفال والأسرة عند النفاذ.

2.7 أقسام مواقع التواصل الاجتماعي

بصورة عامة، يمكن تصنيف مواقع التواصل الاجتماعي في عالم اليوم إلى قسمين هما:

الشكل1.7: تصنيف مواقع التواصل الاجتماعي (حسب الغرض من الموقع).

مواقع التواصل الاجتماعي للأغراض العامة

وهي مواقع تسمح بالنقاش وتبادل الأفكار في الموضوعات العامة (اجتماعية، مهنية، سياسية، اقتصادية، فنية،...إلخ). من أهم هذه المواقع:

- الفيسبوك (www.facebook.com).
- تويتر (www.twitter.com).
- لنكدلن (www.linkedin.com).
- ماي إسبيس (www.myspace.com)
- الواتساب (www.whatsapp.com) على شبكة الهاتف الجوال.
- ثريما Threema (https://threema.ch/e) على شبكة الهاتف الجوال.
- ...إلخ

مواقع التواصل الاجتماعي للأغراض التعليمية

وهى مواقع تم إنشاؤها حديثاً في الفترة (2011-2013) بواسطة منظمات أو اتحادات للجامعات بغرض تقديم الكورسات التعليمية الجامعية المجانية لكل العالم [102]. تقوم هذه المواقع بتشجع عملية التواصل الاجتماعي وتبادل الأفكار والتعاون بين الطلاب فيما يخُص المادة التعليمية. تعتبر تجربة هذه المواقع تجربة فريدة وحديثة في تقديم المواد الدراسية من حيث طريقة التدريس والإعداد وتلقي المساعدة العلمية في غرف النقاش الافتراضية. مع بداية العام 2013 أصدر المجلس الأمريكي للتعليم توصية بإمكانية اعتماد بعض شهادات هذه الكورسات في الجامعات الأمريكية. الجدول 1.7 يوضح قائمة ببعض من هذه المواقع. من المتوقع أن تغير هذه المواقع بصورة كبيرة في حياة البشرية على المدى القريب. فهي تستخدم تكنولوجيا الاتصالات والمعلومات لتوصيل المادة الدراسية لعدد كبير من الطلاب، فمثلاً في الكورس الواحد قد يشارك عدد 65000 طالب من جميع أنحاء العالم. هذا العدد في السابق قد لا يستطيع المحاضر الوصول إليه طوال العمر. العامل الآخر الذي جعلني شخصياً أعتقد بحتمية إسهام هذه المواقع في عملية التغيير، هو أنها تقدم مواد تعليمية عالية الجودة، يصعب على كثير من المؤسسات التعليمية المحلية في كثير من دول العالم الثالث توفيرها.

الجدول1.7: أهم المواقع التعليمية في العالم

الموقع	المكان (البلد المضيف)	عدد الجامعات/عدد الكورسات
موقع كورس إرا (www.Courera.org)	الولايات المتحدة	108جامعة من كل العالم/621 كورس
موقع أيدي إكس (www.edx.org)	الولايات المتحدة	32 جامعة من كل العالم
موقع إدنستي (www.udacity.com)	الولايات المتحدة	25 كورس
موقع إنفيرستي (www.iversity.org)	ألمانيا	8 كورس
موقع أوبنتو إستدى	استراليا	15 جامعة/ 27

(www.open2study.com)			كورس
موقع إسكوا (http://schoo.jp/)		اليابان	-
موقع فيونشا ليرن((http://futurelearn.com/)		المملكة المتحدة	21 جامعة
موقع فثدوكا (http://www.veduca.com.br)		البرازيل	18 جامعة

3.7 بعض المهددات في مواقع التواصل الاجتماعي

على الرغم من الفوائد غير المحدودة لهذه المواقع اجتماعياً واقتصادياً وعلمياً؛ إلّا أن هنالك الكثير من المخاطر والمحاذير [103, 104]، نذكر منها على سبيل المثال ما يلي:

- في مواقع النقاش وتبادل الأفكار يترك بعض المستخدمين الكثير من المعلومات القيمة التي يمكن أن يستفاد منها في الإضرار المعلوماتي.
- التعارف بين الأشخاص على مواقع التواصل الاجتماعي في بعض الأحيان قد يؤدي إلى اللقاء الشخصي مما قد يقود إلى بعض الأضرار و المخاطر.
- بعض المواقع مثل الفيسبوك Facebook وتويتر Twitter تتيح معرفة مكان الشخص في اللحظة المعينة، وهذا قد يقود إلى تسهيل ارتكاب بعض الجرائم التقليدية مثل السرقة والقتل والاحتيال.
- توفر بعض المواقع مثل linkelin معلومات قيمة عن المسار الوظيفي والمهني للمستخدم، مما قد يجعله عرضةً لبعض جرائم المعلوماتية والاحتيال الشبكي.
- المواد المقدمة في المواقع التعليمية معدّة بصورة مشوقة، لكن بالطريقة الغربية، وهذا قد لا يتفق مع بعض الثقافات والمعتقدات الأُخرى.
- في بعض الأحيان يمكن أن تنشأ علاقات في الفضاء الافتراضي بين أطراف لهم اختلافات كبيرة في العادات والتقاليد أو الأعمار، وهذا أيضاً قد يجلب بعض المشكلات للأطفال والقُصر بصوره خاصة.

- تستخدم هذه المواقع تكنولوجيا للبرمجة تعرف بالـ Anomaly Detection and Recommender Systems لبناء الروابط الاجتماعية من خلال تقديم اقتراحات لإضافة أفراد قد يكونون غير معروفين للمستخدم بصورة مباشرة، مما قد يعرضة لخطرٍ ما متصل بالمعلومات في المستقبل.
- انتحال الشخصيات. وهذه أصبحت من الأمور والجرائم اليومية الشائعة، فكثيراً ما نسمع أن شخصاً ما انتحل شخصية مسؤول مهم في الدولة، وقام بإصدار بيان أو إنشاء صفحة إخبارية باسمه.
- تأخذ بعض هذه المواقع قسطاً كبيراً من الوقت مما قد يُضر بالأنشطة الطبيعية والأساسية للإنسان في الجوانب الحياتية الأخرى.

- بالإضافة إلى كل هذه الإشكالات المصاحبة لمواقع التواصل الاجتماعي بصورة عامة؛ فإنه هنالك أيضاً عدة أشكالات متعلقة بالخصوصية والسرية خاصة بالتطبيقات التي تعمل على الهواتف الذكية مثل الواتساب والثريما.

4.7 الجوانب القانونية

مع تطور التكنولوجيا والاتصالات، فإنه من الأهمية بمكان أن تتطور تكنولوجيا القانون في كل الجوانب من تصميم العقود إلى إعداد الأدلة الجنائية للمحاكمات. مع زيادة عملية التواصل البشري عبر مواقع التواصل الاجتماعي، فإنه يجب الانتباه إلى أن هذا التواصل قد يُفرز الكثير من الأنشطة والمعاملات التي يجب أن تكون محكومة بالقانون.

استخدام مواقع التواصل الاجتماعي من قبل أنظمة الحكم

تمَّ استخدام مواقع التواصل الاجتماعي بصورة سالبة في كثير من البلدان والأنظمة غير الديمقراطية، نذكر منها الأحداث التالية على سبيل المثال:

- في العام 2008م قام شخص يدعى أحمد ماهر، بإنشاء مجموعة على الفيسبوك، لنقاش بعض الموضوعات السياسية التي تخص أحد البلدان العربية. في فترة وجيزة تضاعف عدد المشتركين في المجموعة بمتوالية

هندسية إلى حوالي 70 ألفاً، مما اضطر السلطات الأمنية في ذلك البلد للقيام بمتابعته والقبض عليه، لأخذ كلمة المرور لقفل مجموعة النقاش، وتقديمه للمحاكمة (يمكن الاطلاع على تفاصيل حركة 6- أبريل المرتبطة بهذه القضية من موقع الحركة على الإنترنت).

- في الأعوام 2011م و2012م، لعب موقع الفيسبوك Facebook دوراً فعالاً في إشعال الثوارت في كلٍّ من تونس ومصر وليبيا واليمن، لكن هنالك الكثير من الأدلة على أن الأنظمة القائمة في هذه الدول أيضاً استخدمت نفس الأدوات للإيقاع بالمعارضين والخصوم السياسيين.
- تستخدم بعض الدول نظاماً يعرف باسم Pyramiden، يقوم بجمع إحصائيات للمواضيع التي يتم نقاشها في مواقع التواصل الاجتماعي في بعض البلدان، لتقوم بعد ذلك القوات الإلكترونية أوالجيش الإلكتروني (Cyber Force) بالرد عليها بصورة مرضية ومقبولة للأنظمة السياسية الحاكمة.
- هنالك بعض من الأنظمة لا تسمح بعمل بعض من مواقع التواصل الاجتماعي.

نسبة لحداثة هذه المواقع وضخامة تأثيرها الإيجابي والسلبي على الشرائح المختلفة للمجتمعات في عالم اليوم، وللمساعدة في معرفة هذه الاتجاهات؛ فإن الجدول 2.7 يحوي بعض أهم المراجع التي يمكن الرجوع إليها بغرض الدراسة والتعمق ومواصلة البحث العلمي في هذا المجال.

الجدول 2.7: أهم المراجع التي يمكن الرجوع إليها بغرض المزيد من الدراسة.

المرجع	خلاصة المحتوى
Trust and privacy concern within a social networking sites: comparison of facebook and MySpace **[103]**	دراسة حالة بخصوص موضوع الخصوصية في مواقع التواصل الاجتماعي (مقارنة بين الفيسبوك وميسبيس)
Social networking sites and our	الورقة عبارة عن تقرير شامل تم إعداده

Live**[101]**	بواسطة مجموعة من الباحثين في مجال مواقع التواصل الاجتماعي بغرض الإجابة على الكثير من التساؤلات
MOOCs and the AI-Stanford like Courses: Two Successful and Distinct Course Formats for Massive Open Online Courses**[102]**	هذه الدراسة تسلط الضُوء على التطور في مجال تقديم الكورسات الجامعية المجانية من خلال الإنترنت
and ،How EdX Plans to Earn Revenue From Its Free ،Share Online Courses**[105]**	تتعرض الدراسة لطرق تحقيق الربح من خلال تقديم الكورسات المجانية.
What we're learning from online education**[106]**	المادة تقدم شرحاً مبسطاً للدروس المستفادة من تقديم الكورسات المجانية على الإنترنت.
Social Networking's Good and Bad Impacts on Kids**[107]**	الدراسة تناقش المخاطر التي يمكن أن يتعرض لها الأطفال على مواقع التواصل الاجتماعي.
Social networking and security risks**[108]**	الدراسة تتعرض لبعض المخاطر المرتبطة بأمن المعلومات في مواقع التواصل الاجتماعي.
Social Networking Statistics**[109]**	الموقع يعرض بعض الإحصائيات لبعض العوامل المهمة لمواقع التواصل الاجتماعي.

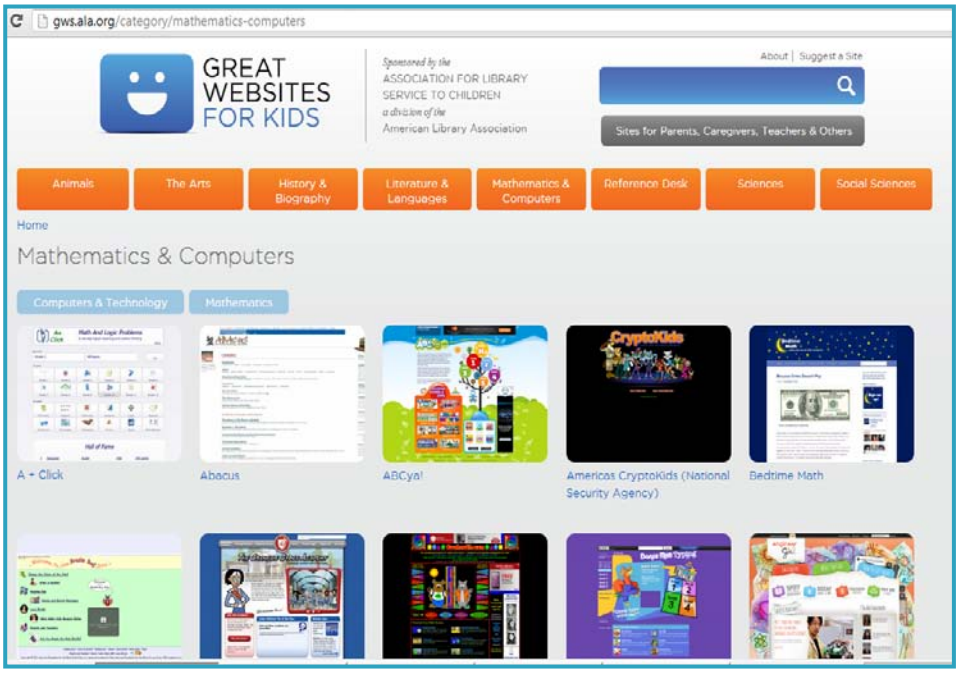
5.7 حماية الأطفال والأسرة عند النفاذ

تحدثنا في الفصول السابقة عن طرق ووسائل يستخدم أغلبها في حماية المؤسسات والمنظمات. في هذه الجزئية نتعرض لوسائل حماية الأطفال والأسرة من المخاطر التي يمكن أن تواجههم عند النفاذ على الإنترنت. نسبةً لحساسية هذا الموضوع وتداخله مع موضوع الحريات بكل مستوياتها في عالم اليوم، فسوف أتناول هذا

الموضوع من جوانب متعددة وأترك للقارئ حرية التقرير بشأن القيم والمبادئ التي يجب أن يتبعها. النقطة الأولى والتي هناك شبه إجماع دولي بشأنها هي مسألة حماية الأطفال عند النفاذ على الإنترنت. صحيح قد يختلف بعضنا مع بعض في تعريف الطفل من ناحية العمر أو تعريف معنى الحماية (من أيّ المواد يجب أن نحمى الطفل)، لكن يجب هنا أن نشير إلى وجود مسألة حماية الأطفال من العنف والإباحية ضمن قوانين الأمم المتحدة والتي تُعد ملزمة للجميع من الناحية الشكلية. عند مناقشة تجارب بعض الدول في مجال حماية المعلوماتية في هذا الكتاب (الفصل التاسع- الفصل الخامس عشر) تعرضنا لتجارب مختلفة لبعض الدول في موضوع حماية الأطفال عند النفاذ. هنالك من الدول من أضاف مسألة العنصرية والعنف اللفظي، وهنالك من اهتم بمسألة حماية خصوصية الأطفال، والتعامل مع بياناتهم الشخصية. يمكن إسناد أسباب الخلاف بين هذه الدول إلى الاختلافات العقائدية (القيم والأخلاق المكتسبة من عقيدة الإنسان).

مهما كانت درجة الاختلاف بين بعضنا في موضوع حماية الأسرة والأطفال عند النفاذ، فإن هذا الخلاف يجب أن لا يُشكل مصدر قلق للجميع لأنه فقط ناتج عن اختلاف معتقداتنا وعاداتنا وثقافاتنا. من كل التجارب المختلفة للدول التي تعرضنا لها، هنالك عوامل مشتركة في وسائل الحماية وهي عامل التوعية وعامل المنع. مثلاً التجربة البريطانية والتجربة الأسترالية ركزت بصورة كبيرة على عنصر التوعية بالمخاطر، وهذا أمر جيد من وجهة نظر الكثيرين لاعتماده على منهجية الإقناع.

من التجارب القيمة والعملية في مجال حماية الأطفال عند النفاذ، تجربة النوافذ إلى المواقع الآمنه للأطفال، وهي عبارة عن مواقع شاملة يمكن منها للطفل النفاذ إلى عدد كبير من المواقع المفيده والآمنة. الشكل 2.7 يوضع إحدى هذه النوافذ الآمنة والتي تُعرف Great Websites for Kids (http://gws.ala.org). هذه النافذة مدعومة من جمعية المكتبات الأمريكية، وتحتوي على أكثر من 700 موقع آمن للأطفال ضمن تصنيفات متعددة. الشكل 3.7 يوضح أيضاً نافذة تضم عدداً مقدراً من التصنيفات المتعددة للمواقع الآمنة والمفيدة للأطفال (http://www.kidsites.com/).



الشكل 2.7: دليل المواقع الآمنة للأطفال (http://gws.ala.org)

الشكل 3.7: دليل المواقع الآمنة للأطفال (http://www.kidsites.com).

البرامج المساعدة للأسرة فى التحكم فى سلوك الاطفال عن النفاذ على الانترنت

بالإضافة إلى وسائل التوعية والإرشاد إلى المواقع المفيدة، هنالك أيضاً العديد من الوسائل التقنية التي تساعد الأسرة والآباء والمدارس في عملية التحكم في المواد التي يمكن أن يتصفحها الأطفال على الإنترنت. الجداول 3.7-7.7 توضح بعضاً من هذه الوسائل والتقنيات.

الجدول 3.7: البرامج المساعدة على تحديد زمن بقاء الأطفال على الإنترنت [110].

اسم البرنامج	نظم التشغيل	الموقع
CSWEB	Windows ME Windows NT Windows 2000 Windows XP Windows Vista	www.securitysoft.com
Safe Eyes Parental Control Program	Windows 98، Windows ME Windows 2000 Windows XP Windows NT	www.onlinesafetysite.com
Covenant Eyes Internet Accountability and Filtering Software	Macintosh OS X Windows Vista Windows ME Windows NT، Windows 2000 Windows XP	www.covenanteyes.com
EyeTimer	Windows 98، Windows ME Windows NT، Windows 2000 Windows XP	www.familysafemedia.com
KidZui	Macintosh OS X	www.kidzui.com

	Windows ،Vista Windows XP	
Family Protector	Macintosh OS X	www.intego.com/contentbarrier
McGruff SafeGuard	Windows XP Windows 2000 Windows Vista	www.GoMcGruff.com
Optenet PC	،Windows 98 Windows ME Windows 2000 Windows XP	www.optenetpc.com
Net Nanny	Windows XP Windows 2000 Windows Vista	www.netnanny.com

الجدول 4.7: البرامج المساعدة على مراقبة الأطفال على الإنترنت [110]

اسم البرنامج	نظم التشغيل	الموقع
McGruff SafeGuard	Windows NT Windows 2000 Windows XP Windows Vista	www.ParentsOnPatrol.org.
SafeEyes	Macintosh OS X ،Windows 98 Windows 2000 Windows XP	www.internetsafety.com
WebBlocker	،Windows 95 ،Windows 98 Windows ME	www.thewebblocker.com

	Windows NT، Windows 2000 Windows XP	
Covenant Eyes Internet Accountability and Filtering Software	Macintosh OS X Windows Vista Windows ME Windows NT، Windows 2000 Windows XP	www.covenanteyes.com
Integrity Online/Everyware	Macintosh OS 9، Macintosh OS X Windows 95، Windows 98، Windows ME Windows NT، Windows 2000 Windows XP	www.integrity.com
A+ Internet Filtering for Families،	Macintosh OS 9 Macintosh OS X Windows NT Windows ME Windows Vista Windows NT Windows XP Windows 2000 Linux OS-independent	www.hedgebuilders.com

الجدول 5.7: البرامج المساعدة على حجب المحتويات الجنسية عن الأطفال عند تصفح الإنترنت[110]

اسم البرنامج	نظم التشغيل	الموقع
PureSight online child Safety	Windows 95 Windows 98	www.icognito.com

	Windows ME Windows NT Windows 2000 Windows XP	
ContentProtect	Windows 2000 Windows XP Windows Vista	www.contentwatch.com
KidZui	Macintosh OS X ،Windows Vista Windows XP	www.kidzui.com
The Internet Filter IF-2K	Macintosh OS X Windows ME ،Windows NT Windows 2000 Windows XP Linux	www.turnercom.com
Safe Access	Windows 2000 Windows XP Windows Vista	www.safeaccess.com
،iProtectYou	،Windows 95 ،Windows 98 Windows ME ،Windows NT Windows 2000 Windows XP	www.softforyou.com

الجدول 6.7: البرامج المساعدة التي يمكنها منع الأطفال من إرسال معلوماتهم الشخصية على الإنترنت [110].

اسم البرنامج	نظم التشغيل	الموقع
CyberSieve	Windows 95 Windows 98 Windows ME Windows NT Windows 2000 Windows XP	www.softforyou.com

Cyber Sentinel	Windows ME Windows NT Windows 2000 Windows Vista Windows XP	www.securitysoft.com
ContentProtect	Windows 2000 Windows XP Windows Vista	www.NetNanny.com
Integard	Windows Vista، Windows ME Windows 98، Windows 2000 Windows XP	http://en.kioskea.net
ModemLockDown	Windows XP Windows Vista	www.modemlockdown.com
SpectorPro	Windows 98، Windows ME Windows NT، Windows 2000 Windows XP	www.spectorsoft.com

الجدول 7.7: المتصفحات الخاصة بالأطفال [110].

اسم المتصفح	نظم التشغيل	الموقع
MyWeb	Windows 95 Windows 98 Windows ME Windows NT Windows 2000 Windows XP	www.myweb.com
SurfOnTheSafeside	Macintosh OS 9 Macintosh OS X Windows 3.1 Windows 95 Windows 98 Windows ME	www.surfonthesafeside.com

	Windows NT Windows 2000 Windows XP Linux OS-independent	
www.awesomelibrary.org	Macintosh OS 9 Macintosh OS X Windows 3.1 Windows 95 ،Windows 98 Windows ME ،Windows NT Windows 2000 Windows XP Linux OS-independent	Awesome Library for Kids Browser
parentalcontrols.aol.com	Windows Vista Windows 2000 Windows XP	Aol Parental Controls
www.kidzui.com	Macintosh OS X ،Windows Vista Windows XP	KidZui

الفصل الثامن

جهود الاتحاد الدولي للاتصالات فى مجال حماية المعلوماتية والاتصالات

1.8 المقدمة

الاتحاد الدولي للاتصالات International Telecommunication Union (ITU) هو منظمة دولية تُعنى بشؤون تنظيم وتطوير نظم الاتصالات على المستوى العالمي والإقليمي والدولي. يقوم الاتحاد بهذا الدور القيادي من المقر الدائم له في مدينة جنيف السويسرية ومجموعة من المكاتب الإقليمية المنتشرة في الأقاليم المختلفة حول العالم. هذه المكاتب تقوم بدور التنسيق للجهود والمبادرات، وتقديم الدعم اللازم لكثير من الدول النامية، وذلك من أجل الارتقاء بتكنولوجيا الاتصالات وتقانة المعلومات. نسبة للأبعاد الدولية للجريمة الإلكترونية في عالم اليوم، والذي شهد تطوراً رقمياً مذهلاً لم يسبق له مثيل من ذي قبل؛ كان لا بد للاتحاد من دور فعال في مجال أمن المعلومات وحماية البنيات التحتية الأساسية للاتصالات، التي يعتمد عليها العالم اليوم. الجريمة الإلكترونية عبر الإنترنت غالباً ما يكون لها بعد دولي. فمثلاً رسائل البريد الإلكتروني التي تحوي محتويات غير قانونية غالباً ما تصدر وتتنقل من خلال عدد من البلدان ويتم تخزينها أيضاً في بلدان مختلفة. لذلك يجب من الناحية العملية أن تتعاون كل هذه البلدان في عملية التحقيق في مثل هذا النوع من الجرائم.

الإجراءات القانونية القديمة لتتبع المجرمين بواسطة الشرطة الدولة، تعتبر أيضاً تقليدية إلى حدٍ ما ومعقدة، وغالباً ما تستغرق وقتاً طويلاً، وبالتالي إعداد إجراءات جديدة للتعاون الدولي للاستجابة السريعة للحوادث الإلكترونية، يعتبر أمراً مهماً جداً وحيوياً في عالم اليوم، الذي يعتمد على المعلوماتية. هذا الجزء يتناول بالشرح بعض مجهودات الاتحاد الدولي للاتصالات (ITU) في مجال أمن المعلوماتية Cyber-Security وحماية البنيات التحتية الأساسية الحرجة والاتصالات. في هذا الفصل تتم مناقشة الموجهات والأجندة الأساسية للاتحاد الدولي للاتصالات في مجال أمن

المعلومات في الفقرة 2.8. الفقرة 3.8 توضع أهم المشاريع التي يُنفذها الاتحاد في مجال المعلوماتية، والفقرة 4.8 تشرح مجهودات الاتحاد في مجال حماية الأطفال عند النفاذ على الإنترنت. وأخيراً الفقرة 5.8 تشرح مبادرة التعاون بين الاتحاد الدولي للاتصالات ومجموعة الشراكة الدولية من أجل التصدي لجرائم المعلوماتية أو ما يُعرف اختصاراً بـ Impact.

2.8 الموجهات العامة للاتحاد الدولي للاتصالات بخصوص أمن المعلوماتية

من أجل الوصول إلى فضاء معلوماتي آمن وبنيات تحتية أساسية مستقرة، تبنى الاتحاد الدولي للاتصالات ما يُعرف بالأجندة العالمية لأمن المعلومات Global Cyber-security Agenda (GCA) والتي تحتوي على الأهداف الأساسية الموضحة في الشكل 1.8. قبل أن نناقش أهم المشروعات التي قام بتنفيذها الاتحاد بناءً على هذه الأجندة، يجب أن نتعرض إلى هذه الأجندة بشيء من التفصيل المختصر من حيث الأهداف والمقاصد.

الشكل 1.8: الأجندة الدولية للاتحاد الدولي للاتصالات لحماية المعلوماتية.

بناء الإطار القانوني

يسعى الاتحاد إلى مساعدة الدول الأعضاء في مجال بناء تشريعات وطنية لأمن المعلومات تحتوي على إطار قانوني شامل (جمع للأدلة -وتحقيق – وقضاء ..الخ) للتعامل مع الجرائم الإلكترونية والمعلوماتية. أيضا يسعى الاتحاد إلى خلق نوع من التوافق بين التشريعات القانونية للدول والمجموعات الإقليمية المختلفة من أجل الوصول إلى بناء تشريعات عالمية للتعامل مع الجريمة االإلكترونية. من أهم الأنشطة الدولية للاتحاد في هذا المجال:

- مبادرة موائمة التشريعات واللوائح والنظم لدول الكاريبي والتي تُعرف اختصاراً [111](HIPCAR).
- مبادرة موائمة التشريعات واللوائح والنظم لدول شبة الصحراء الأفريقية والتي تُعرف اختصاراً بـ(HIPSSA) [112].

- مبادرة موائمة التشريعات واللوائح والنظم لدول الباسفيك والتي تُعرف اختصاراً بـ(ICB4PAC) [113].

تشجيع التعاون الدولي

يعمل الاتحاد الدولي بصورة لصيقة مع الدول الأعضاء، وينسق معها في جميع الموضوعات المتصلة بأمن المعلومات والاستجابة للمخاطر المعلوماتية وتنسيق الجهود على المستوى الدولي. في هذا الخصوص وقع الاتحاد اتفاقية تعاون وتكامل مع مجموعة الشراكة الدولية من أجل مكافحة جرائم المعلوماتية International Multilateral Partnership Against Cyber Threats والتي تُعرف اختصاراً بـ IMPACT، وذلك لتقوم مجموعة الشراكة الدولية ببعض مهام الاتحاد الدولي للاتصالات في مجال حماية المعلوماتية، كما سنأتي عليه لاحقاً [114]. من أهم نشاطات الاتحاد في مجال دعم وتنسيق التعاون الدولي:

- مساعدة الدول الأعضاء في إنشاء مراكز الحاسوب للطوارئ والاستجابة Computer Incident Response Teams (CIRT)
- يعمل الاتحاد مع مجموعة IMPACT على تقييم ومراجعة مقدرات مراكز الحاسوب للطوارئ والاستجابة في الدول الأعضاء.
- دعم المبادرات الوطنية والإقليمية والدولية في مجال حماية الأطفال عند النفاذ.
- دعم المبادرات الدولية في مجال توحيد القوانين والتشريعات الخاصة بحماية الاتصالات والمعلوماتية.

- تسهيل عملية الوصول إلى مصادر المعلومات القيمة والخاصة بعملية إعداد السياسات والتشريعات العامة في مجال أمن المعلومات والبنيات التحتية الحرجة.

بناء القدرات

يعمل الاتحاد الدولي للاتصالات بصورة لصيقة مع منظمة IMPACT وشركات الحلول الأمنية والبرمجيات على بناء القدرات البشرية للدول الأعضاء من خلال التدريب وإدارة عملية تبادل الخبرات [114]. من أهم الجوانب التي يقوم الإتحاد بمساعدة الدول فيها هي:

- بناء القدرات في مجال إدارة المعلومات.
- بناء الخبرات التقنية.
- تطوير البحوث والدراسات.
- دعم المشروعات الوطنية للدول الأعضاء في مجال نشر ثقافة أمن المعلومات.
- بناء القدرات في مجال سَنِّ القوانين والتشريعات الوطنية لتنظيم وإدارة قطاع المعلوماتية والاتصالات.

البناء التنظيمي

من ناحية البناء التنظيمي، فإن الاتحاد يعمل من خلال إدارة تطويرالاتصالات Communications Development ومنظمة IMPACT على الإشراف والتنسيق بين جميع للدول الأعضاء وتقديم الدعم الفني اللازم لكل دولة حسب احتياجاتها [115]. في مجال البناء التنظيمي ينصح الاتحاد كل الدول الأعضاء ببناء المنظمات الآتية على المستوى الوطني لكل دولة:

- إنشاء إدارة لتنسيق عمليات أمن المعلوماتية بين المؤسسات داخل الدولة National cyber-Security Coordinator
- بناء مركز حاسوب وطني للطوارئ والاستجابة (CIRT).
- بناء مركز لتنسيق ودعم الأنشطة والمبادرات المتصلة بأمن المعلوماتية والبنيات التحتية الحرجة.

التدابير التقنية والإجرائية

يعمل الاتحاد مع عدة أطراف دولية من أجل دعم وتطوير الوسائل التقنية لحماية المعلوماتية والبنيات الأساسية الحرجة. في هذا الخصوص يقوم الاتحاد بتركيز الجهود في المجالات الآتية [116]:

- تطوير المواصفات الخاصة بأنظمة حماية المعلوماتية والاتصالات بواسطة(ITU-T) ITU Standardization Sector.
- إعداد الدراسات والبحوث في مجال أمن المعلومات والاتصالات وذلك بواسطة ITU-T Study Group 17.
- التنسيق الدولي في مجال إدارة الترددات ITU Radio-Communications.
- الاستجابة للطوارئ بواسطة المركز الدولي للاستجابة Global Response Centre (GRC)

3.8 مشاريع الاتحاد الدولي للاتصالات في مجال أمن المعلوماتية

هنالك الكثير من المشاريع المتصلة بأمن المعلوماتية التي قام بتنفيذها الاتحاد للدول الأعضاء نذكر منها على سبيل المثال ما يلي:

- تنفيذ مشاريع إنشاء مركز حاسوب للطوارئ والاستجابة لكلٍّ من:
  1. يوغندا.
  2. زامبيا.
  3. كينيا.
  4. بوركينافاسو.
  5. بورندي.
  6. جاميكا.
  7. غانا.

8. ساحل العاج.
9. تنزانيا.
10. إنشاء مركز للتميز والابتكار لدول المنطقة العربية.
11. إنشاء مركز حماية البنيات التحتية الأساسية للدول الأقل نمواً.

- مشروع حماية الأطفال عند النفاذ على الإنترنت.

- إصدار المنشورات القيمة لتوضيح الإطار العام والموجهات التفصيلية لبناء النظم والمؤسسات التي تُعنى بحماية المعلوماتية والبنيات التحتية الحرجة.

الجدول 1.8 يوضح بعض من هذه المنشورات القيمة.

الجدول 1.8: يوضح قائمة بالمنشورات القيمة للاتحاد الدولي للاتصالات في مجال أمن المعلومات وحماية البنيات التحتية الأساسية للمعلوماتية والاتصالات.

اسم المنشور / التقرير	الملخص
The ITU National Cyber-security Strategy Guide**[117]**	يحتوى المنشور على الموجهات العامة التي يجب أن تستعين بها الدول من أجل بناء إستراتيجية وطنية لأمن المعلومات والاتصالات.
Service Catalogue**[118]** ITU-IMPACT	يحتوى المنشور على قائمة وشرح تفصيلي بالخدمات التي يقدمها الاتحاد الدولي للاتصالات ومجموعة الشركة الدولية من أجل مكافحة الجرائم المتصلة المعلوماتية.
ITU-IMPACT Partnership Prospectus (ALERT) Applied Learning for Emergency Response Team **[119]**.	تشرح الورقة تجربة عملية لفريق العمل من أجل التدارس بغرض التعامل مع حالات الطوارئ والاستجابة.
Cyber-security Guide for Developing Countries **[120]**.	يشرح دليل أمن المعلوماتية للدول النامية الخطوات العملية التي يجب أن تتبعها الدول لتكوين المؤسسات التي تحمي قطاع المعلوماتية والبنيات التحتية الحرجة.
Understanding cybercrime: Phenomena، challenges and legal	يشرح المنشور كيفية الاستجابة القانونية للجرائم المعلوماتية.

response **[121]**	
The ITU/UNODC Cybercrime: global challenge **[122]**.	يشرح المنشور المشكلات الخاصة بجرائم المعلوماتية.
security/CIIP -ITU National Cyber Self-Assessment Tool **[123]**	يشرح المنشور أدوات ووسائل التقييم الذاتي لمنظومة أمن المعلومات والبنيات التحتية الأساسية

4.8 مشروع حماية الأطفال عند النفاذ على الإنترنت

مشروع الاتحاد الدولي للاتصالات لحماية الأطفال عند النفاذ (www.itu.int/cop) هو جزء من الأجندة الدولية العامة لأمن المعلومات. تم عرض هذا المشروع على مجلس الاتحاد في العام 2008م، وتمت الموافقة عليه بواسطة الأمين العام ورؤساء الدول الأعضاء ومديري المنظمات الدولية الكبرى. الجدول 2.8 يُعرّف بأهم الأعضاء المشاركين/ الداعمين للمشروع [124]:

الجدول 2.8: الأعضاء المشاركون في مبادرة حماية الأطفال عند النفاذ.

اسم المنظمة	الموقع
الاتحاد الدولي للاتصالات ITU	www.itu.int/cop
التحالف الخيري لحماية الأطفال على الإنترنت Children's Charities' Coalition on Internet Safety	www.chis.org.uk/
منظمة حماية الأطفال الدولية Child Helpline International	www.childhelplineinternational.org
منظمة ECPAT	www.ecpat.net
الوكالة الأوروبية Network and Information Security Agency	www.enisa.europa.eu
اتحاد الإذاعات الأوروبية European	www.ebu.ch

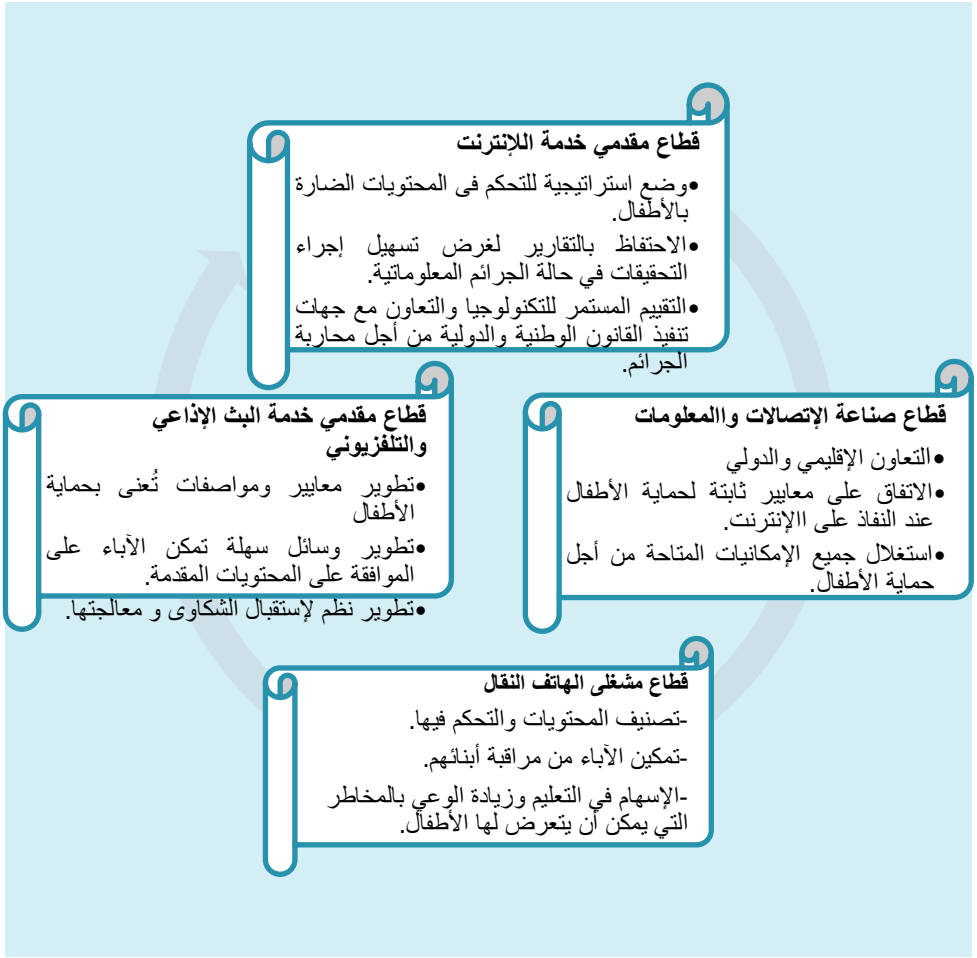
Broadcasting Union	
برنامج المفوضية الأوروبية لإنترنت أكثر أماناً European Commission Safer Internet Programme	ec.europa.eu/saferinternet
تحالف المنظمات غير الحكومية الأوروبية لسلامة الأطفال على الإنترنت European NGO Alliance for Child Safety Online	www.enacso.eu
معهد سلامة الأسرة على الإنترنت Family Online Safety Institute	www.fosi.org
جمعية GSM (GSM Association)	www.gsma.com
منظمة ikeepsafe	www.ikeepsafe.org
الشرطة الدولية International Criminal Organization Police	www.interpol.int
المركز الدولي للأطفال المفقودين والمستغلين International Centre for Missing& Exploited Children	www.icmec.org
منظمة optimal internet	www.optenet.com
ميكروسوت	www.microsoft.com
اتصالات إيطاليا	www.telecomitalia.com
اتصالات إسبانيا	www.telefonica.com
منظمة حماية لأطفال الدولية Save the Children	www.savethechildren.org
صندوق الأمم المتحدة للطفولة United Nations Children's Fund	www.unicef.org
مكتب الأمم المتحدة المعني بالمخدرات والجريمة United Nations Office on Drugs and Crime	www.unodc.org

معهد الأمم المتحدة لأبحاث الجريمة United Nations Interregional Crime and Justice Research Institute	www.unicri.it
معهد الأمم المتحدة لبحوث نزع السلاح United Nations Institute for Disarmament Research	www.unidir.org
مجموعة فودافون Vodafone Group	www.vodafone.com

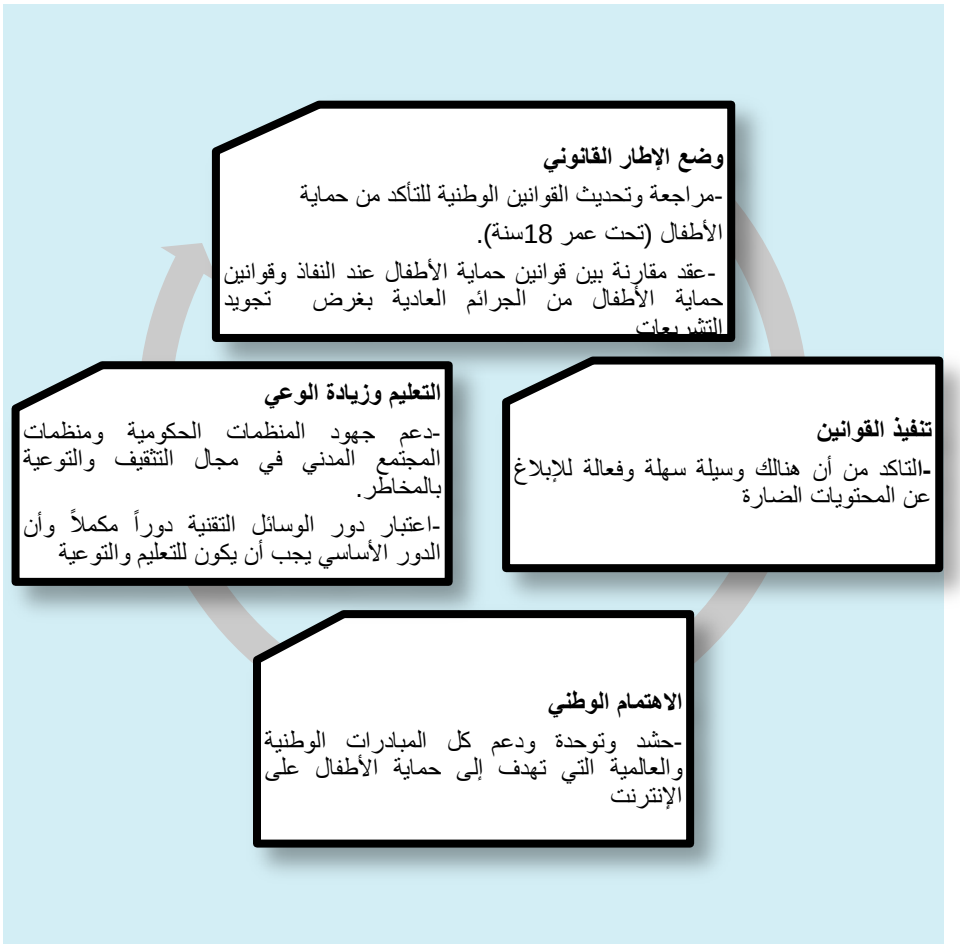
أهداف المشروع

- تحديد المخاطر ونقاط الضعف بالنسبة للأطفال في الفضاء السيبراني (أو المعلوماتي).
- خلق وعي عام بالموضوع من كل الجوانب.
- تطوير أدوات تقنية وطرق عملية للمساعدة في تقليل المخاطر.
- تبادل المعارف والخبرات.

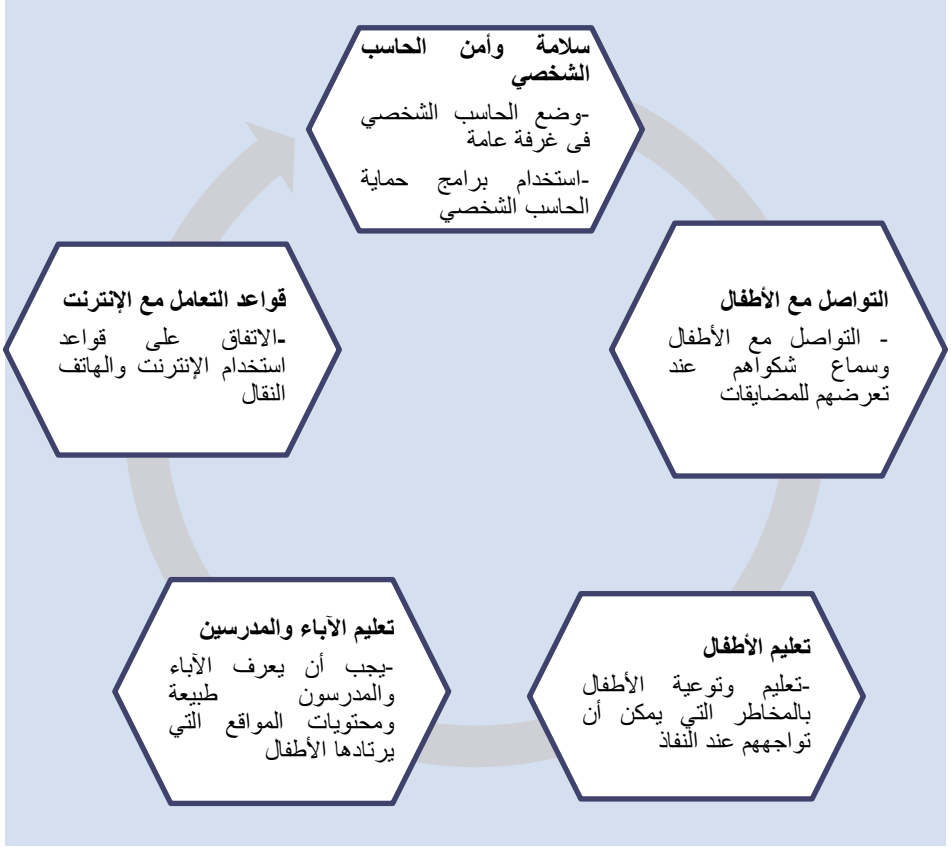
الأشكال التوضيحية 4.8-2.8 تشرح التوصيات العامة للاتحاد الدولي للاتصالات للحكومات والمدارس والآباء وقطاعات صناعة المعلوماتية والاتصالات بخصوص حماية الأطفال عند النفاذ على الإنترنت.



الشكل2.8: توصيات الاتحاد الدولي للاتصالات لقطاعات صناعة المعلوماتية والاتصالات الرئيسية بخصوص حماية الأطفال عند النفاذ.



الشكل 8.3: توصيات الاتحاد الدولي للاتصالات للدول بخصوص عملية حماية الأطفال عند النفاذ.



الشكل 4.8: واجبات الآباء والمدارس تجاه عملية حماية الأطفال عند النفاذ حسب توصية الاتحاد الاتحاد الدولي للاتصالات.

5.8 مجموعة الشراكة الدولية المتعددة الأطراف لمكافحة الإرهاب الإلكتروني

في إطار أجندة الاتحاد للأمن السيبراني الإلكتروني العالمي، في عام 2008م، وقع الاتحاد الدولي للاتصالات ومجموعة الشراكة الدولية المتعددة الأطراف لمناهضة التهديدات الإلكترونية (IMPACT) رسمياً مذكرة للتفاهم من أجل تكامل الأدوار وستصبح مدينة سيبرجايا Cyberjaya الماليزية هي المقر العالمي لبرنامج الأمن السيبراني. في 20 مايو 2011م وخلال القمة العالمية لمجتمع المعلومات World Summit of the Information Society(WSIS) المنعقدة في مدينة جنيف

السويسرية تم التوقيع على الاتفاق التاريخي بين الاتحاد الدولي للاتصالات (ITU) ومجموعة الشراكة الدولية المتعددة الأطراف لمكافحة الإرهاب السيبراني ليصبح بذلك IMPACT رسمياً الذراع الرسمي لمنظومة الأمم المتحدة والاتحاد الدولي للاتصالات لتنفيذ الموجهات العامة بخصوص الأمن السيبراني الإلكتروني. من الناحية العملية تُعد هذه القمة أول تجمع دولي يجمع الحكومات بالأوساط الأكاديمية وخبراء الصناعة، في تحالف شامل ضد التهديدات الإلكترونية. يقوم مركز IMPACT بالتنسيق بين حوالي 193 دولة عضواً في الاتحاد، ويقدم الخبرة والتسهيلات والموارد اللازمة للتصدي بفاعلية للتهديدات الإلكترونية، وأيضاً يقدم الدعم الفني اللازم لهيئات الأمم المتحدة والمنظمات الدولية.

يقدمم مركز IMPACT مجموعة من الخدمات القيمة للدول الأعضاء من خلال المنظومة الموضحة في الشكل 5.8.

الشكل 5.8: الخدمات الرئيسية التي يقدمها مركز Impact

المركز الدولي للاستجابة السريعة للطوارئ

يعمل المركز الدولي للاستجابة للطوارئ (GRC) على مساعدة الدول الأعضاء في جمع المجالات المتعلقة بالكوارث والطوارئ الخاصة بالنظم المعلوماتية والاتصالات. يعمل المركز بالتعاون مع مجموعة من الشركاء في مجالات الصناعة والدراسات العلمية. يقدم المركز أيضاً خدمة الوصول إلى Electronically Secure Collaborative Application Platform for Experts (ESCAPE)، وهو عبارة تطبيق يساعد الخبراء في كل العالم في عملية الوصول إلى الوسائل المتاحة وتبادل الخبرات في بيئة آمنة. الجدول 3.8 يوضح قائمة بالخدمات الأساسية التي يقدمها المركز الدولي للاستجابة والطوارئ GRC.

الجدول 3.8: الخدمات الأساسية لمركز الاستجابة والطوارئ الدولي

الخدمة المقدمة	الوصف/العدد
الوصول إلى ما يعرف (ESCAPE) Access to ESCAPE	من جهاز واحد في فضاء العنونة العام
الوصول إلى الأخبار والتقارير Ability to have Access to the Network Early Warning System (NEWS) and Data Visualization	✓
العدد الأقصى للمستخدمين الذين يمكنهم الوصول إلى (ESCAPE) Maximum number of ESCAPE portal accounts	5
Ability to invite local experts to the IMPACT expert Community	✓
Ability to escalate incidents to the IMPACT expert	✓

Community	
✓ Ability to upload malware for IMPACT analysis	
✓ Ability to receive periodic security news	
✓ Ability to receive periodic security reports (Generic)	
✓ Ability to subscribe to ESCAPE's content	
1 Minimum number of Computer Security Incident Response Team members nominated	

مركز توفيق السياسات والتعاون الدولي

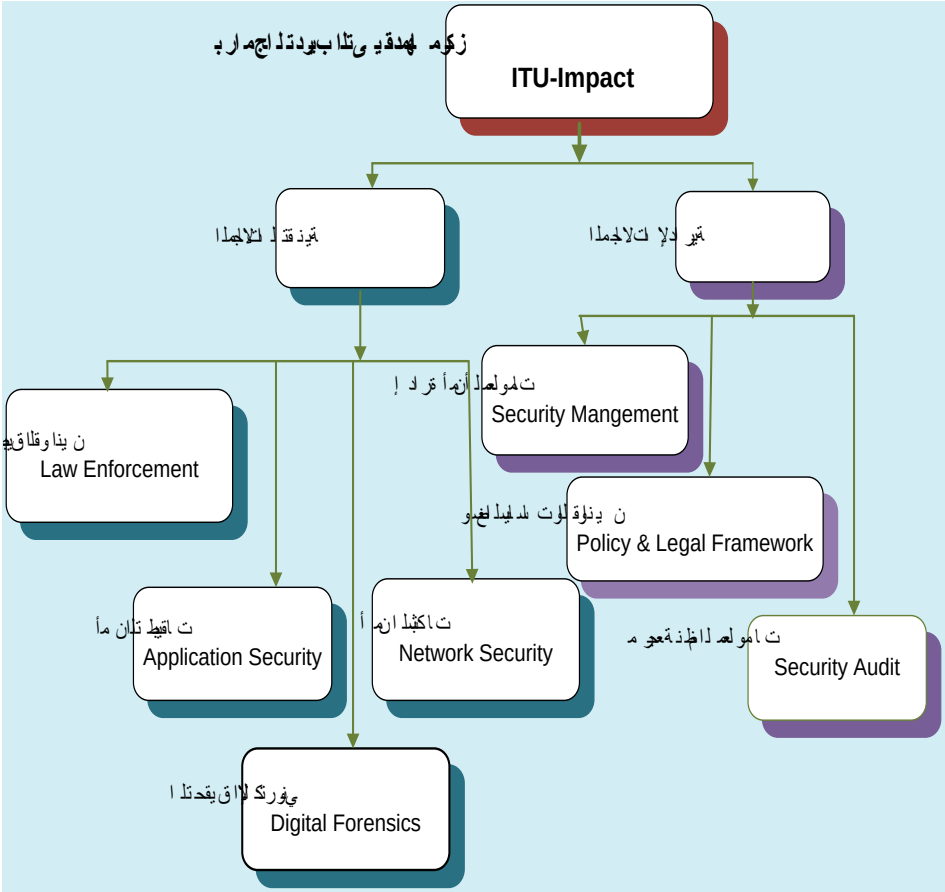
يقوم هذا المركز بالمهام الآتية:

- تشجيع المبادرات الدولية الساعية إلى مواءمة وتوفيق القوانين الدولية في مجال مكافحة جرائم المعلوماتية.
- العمل على زيادة الوعي العام الدولي حول ضرورة تضافر الجهود من أجل حماية المعلوماتية والفضاء الإلكتروني.
- تشجيع الجهود الدولية في مجال حماية الأطفال عند النفاذ.
- تشجيع التعاون الدولي.

مركز التدريب ورفع القدرات

يعمل مركز التدريب ورفع القدرات التابع لمنظمة Impact، على تقديم الدعم الفني والإداري للدول الأعضاء، من خلال مجموعة من البرامج التدريبية، التي يقدمها

المركز بالتعاون مع مجموعة من بيوتات رفع الكفاءة المهنية الدولية. الشكل 6.8 يوضح المجالات الأساسية للتدريب ورفع القدرات التي يقدمها مركز التدريب التابع لمنظمة Impact.



الشكل 6.8: المجالات الأساسية للتدريب التي يقدمها مركز التدريب التابع لمنظمة Impact

مركز تطوير بحوث أمن المعلومات

يعمل مركز البحوث والدراسات التابع لمنظمة Impact وبالتعاون مع عدد من بيوت الخبرة الدولية في مجال إنتاج نظم المعلومات على تطوير البحوث وتشجيع الابتكار في المجالات المتعدده لأمن المعلومات وحماية البنيات التحتية الحرجة للمعلوماتية والاتصالات.

الفصل التاسع
تجربة قطر

1.9 الخطة الوطنية والاتجاهات المستقبلية لبناء صناعة المعلوماتية

قطر من الدول العربية الغنية والطموحة في التقدم والازدهار والتميز في جميع المجالات الحيوية بالنسبه للإنسان في عالم اليوم. لتحقيق هذه الأهداف وصولاً إلى بناء أمة متحضرة عملت الدولة على تطوير نُظم الاتصالات والمعلومات لزيادة كفاءة الإنتاج. من أهم المشاريع التي قامت بتنفيذها الدولة في مجال المعلوماتية، هي إنشاء شبكة الخدمات الحكومية المتكاملة e-government، نافذة قطر التعليمية e-learning Patrol وتشجيع تطبيقات التجارة الإلكترونية e-bussies. أما في مجال الاتصالات فعملت الدولة على تحديث البنيات الأساسية لنقل المعلومات من خلال المشروع الوطني لشبكات السعات العريضة Qatar National Broadband Network (QNBN) والذي من المتوقع أن يتم الانتهاء منه في العام 2015م.

يعتبر مشروع إطلاق القمر الصناعي سهيل-1 من أهم وأكبر المشاريع الإستراتيجية للدولة في مجال الاتصالات يحث يوفر كثيراً من المؤسسات في للدولة درجة عالية من الاستقلالية في مجالات الاتصالات والبث الفضائي. تم إطلاق القمر بنجاح في نهاية أغسطس وبداية سبتمبر من العام (2013م). الشكل 1.9 يوضح جزءاً من التجهيز لعملية الإطلاق (المصدر قناة الجزيرة الإخبارية). من أهم الخدمات التي يقدمها القمر الصناعي سهيل-1

- تراسل الاتصالات الهاتفية
- البث التلفزيوني القياسي والبث التلفزيوني عالي الدقة High Definition Television (HDTV) and Standard Definition Television (SDTV) Channels
- الإنترنت.

يعمل القمر سهيل-1 من الموقع المداري المتزامن 25.5 درجة شرق، لفترة عمل طولها 15 سنة تقريباً ليغطى المنطقة العربية وشمال أفريقيا. تعمل الشركة المالكة سهيلسات على إطلاق القمر سهيل-2 في العام 2016 على الأكثر وذلك للإيفاء بمتطلبات خطة الدولة للعام 2022م

الشكل 1.9: جانب من عملية إطلاق القمر الصناعي سهيل-1 المملوك لشركة سهيلسات القطرية (المصدر: قناة الجزيرة الإخبارية).

2.9 القطاعات والمصالح الاستراتيجية

تم تعريف البنيات الأساسية Critical Sectors على أنها تلك القطاعات التي تضم الأصول الفيزيائية والمعلوماتية التي إذا توقفت أو تعطلت (أُتلفت أو دُمرت) يمكن أن يُؤدي ذلك إلى تأثير كبير على الصحة العامة والسلامة والأمن القومي والرفاه الاقتصادي لدولة قطر. بناءً على هذا التعريف، تم اعتماد القطاعات الآتية على أنها بنيات أساسية حرِجة:

- البنوك والقطاعات المالية Banking and finance.
- أصول الطاقة والشبكات Energy Facilities and Network.
- الحكومة Government.

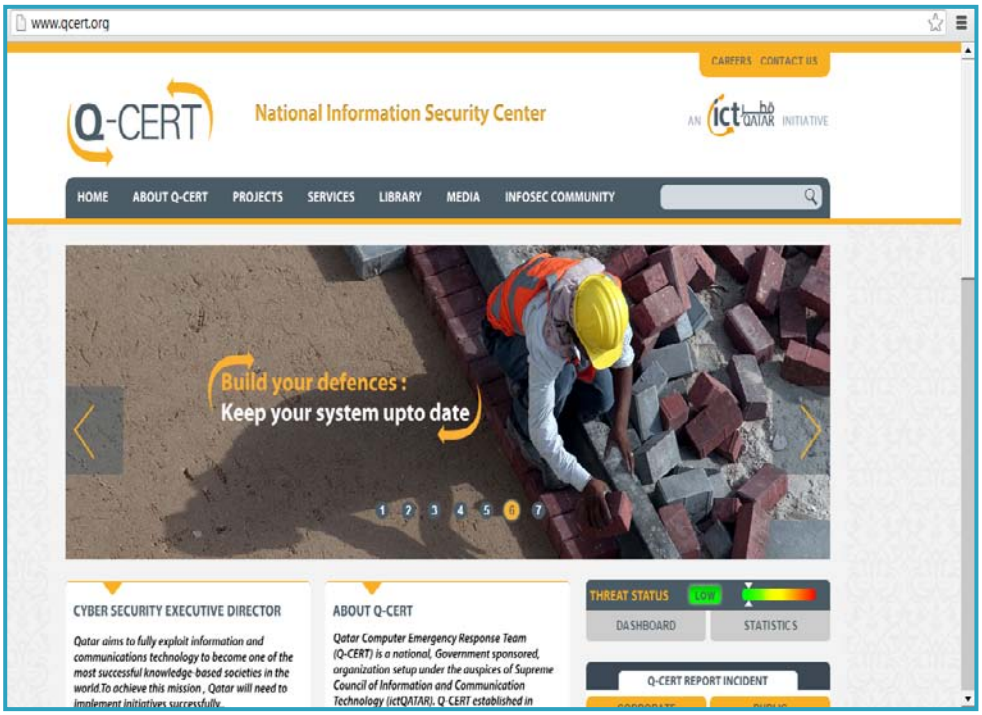
- الاتصالات وتكنولوجيا المعلومات ICT Sectors .
- خدمات الصحة Healthcare.
- المياه Water
- الغذاء Food
- المواصلات Transportations
- الإعلام Media
- المواد الخطرة Hazardous Materials

3.9 المبادرات في الماضي والحاضر

لأهمية موضوع أمن المعلومات وحماية البنيات الأساسية الحرجة، ودور هذه البنيات في نهضة وتقدم الشعوب في عالم اليوم، قامت الحكومة القطرية ممثلة في المجلس الأعلى للاتصالات وتكنولوجيا المعلومات Supreme Council of Information & Communication Technology بعدد من المبادرات في مجال تطوير عملية أمن المعلومات والاتصالات والبنيات الأساسية والحرجة. هذه المبادرات يمكن تلخيصها في الآتي:

1. تكوين فريق الحاسوب الوطني للطوارئ والاستجابة Qatar Computer Emergency Response Team (Q-CERT)، في العام 2005م (الشكل 2.9 يوضح الموقع الرئيسي) ليقوم بالمهام الآتية:
   - تحديد الأصول والبنيات التحتية الحرجة للمعلوماتية والاتصالات.
   - تطوير سياسات وخطط إدارة المخاطر.
   - منع الهجمات المعلوماتية وذلك بتطوير وسائل الحماية.
   - الاستجابة للطوارئ وتقديم الدعم التقني اللازم.
   - مساعدة القطاعات الحرجة Critical Sector في عمليات إعداد السياسات والتدريب ورفع القدرات.

- المساعدة في عملية تبادل الخبرات بين القطاع الحكومي والقطاع الخاص داخل الدولة.
- العمل على تبادل الخبرات مع المراكز الدولية والإقليمية.



الشكل 2.9: الموقع الرئيسي لفريق الحاسوب للطوارئ والاستجابة (www.qcert.org).

2. إعلان الموجهات العامة بخصوص أمن وسلامة نظم التحكم الأشرافي Supervisory Control and Data Acquisition (SCADA) System لحماية القطاعات الصناعية الإستراتيجية [125].
3. إعداد السياسة الوطنية لأمن المعلومات Government Information Assurance Policy [126]

4. إنشاء الشركة الوطنية للأقمار الصناعية سهيلسات لتطوير الاتصالات الفضائية المعتمدة على الأقمار الصناعية لتوفير درجة عالية من الاستقلالية والاستقرار في مجالات الاتصالات والبث الفضائي.

4.9 نبذة عن المنظمات والمؤسسات القائمة على حماية المعلوماتية

1. المجلس الأعلى للاتصالات وتكنولوجيا المعلومات (Supreme Council of Information & Communication Technology): تم إنشاؤه في العام 2004م ليقوم بإدارة وتنظيم قطاع الاتصالات وتقنية المعلومات ووضع السياسات العامة في مجال حماية البنيات الأساسية الحرجة في الدولة.
2. فريق الحاسوب الوطني للطوارئ والاستجابة Qatar Computer Emergency Response Team (Q-CERT)،: يعتبر فريق الحاسوب الوطنى للاستجابة والطوارئ الجهة التنفيذية في المجلس للاتصالات وتكنولوجيا المعلومات والمنوط بها إعداد وتنفيذ كل سياسات الدولة في مجال أمن المعلومات.

5.9 الإنذار المبكر والوعي العام

يقوم فريق الحاسوب للاستجابة والطوارئ ومن خلال عملية تبادل الخبرات مع المراكز الإقليمية والدولية بواجب الإنذار المبكر بالأخطار التي يمكن أن يواجهها المستخدمون للشبكات والبنيات الأساسية الحرجة للمعلوماتية والاتصالات. يعمل هذا الفريق من خلال المركز الوطني لأمن المعلومات على مراقبة حركة الإنترنت واستقبال البلاغات الخاصة بالجرائم والانتهاكات في مجال المعلوماتية على مدار 24 ساعة.

6.9 حماية الأطفال عند النفاذ

يعمل المجلس الأعلى للاتصالات في قطر ومن خلال مركز الحاسوب للطوارئ والاستجابة وبالتضامن مع المجلس الأعلى للتربية والتعليم على إقامة العديد من ورش العمل المتخصصة في مجال تقديم النصح والتوعية العامة بموضوع حماية الأطفال

عند النفاذ على الإنترنت. أيضاً من جهة أخرى يعمل المجلس وبالتضامن مع المجلس الاعلى للأُسرة والاتحاد الدولي للاتصالات على تطوير منهج تعليمي للأمن السيبراني، وذلك لمساعدة وتعريف المعلمين والدارسين أساسيات الاستخدام الآمن للإنترنت بغرض الاستفادة القصوى من الموارد المتاحة من خلالها [127].

بصورة عامة يمكن تلخيص المجهودات القطرية في مجال حماية الأطفال عند النفاذ على الإنترنت في الآتي:

- إنشاء صفحة إلكترونية تفاعلية على الإنترنت الشكل 3.9: لتقديم المواد التعليمية والإرشادية وتلقي الشكاوى وتوضيع السياسات العامة للدولة في مجال حماية الأطفال عند النفاذ.
- تعاون المجلس الأعلى للاتصالات مع المؤسسات التعليمية والمنظمات الوطنية من أجل رفع مستوى التوعية بقضايا حماية الأطفال في الفضاء المعلوماتي.
- تعاون المجلس الأعلى للاتصالات في الدولة مع الموسسات والمنظمات الدولية ذات الاختصاص.
- جهود جمعية حماية المرأة والطفل التابعة لمؤسسة قطر للإعمار.
- حملة التوعية الوطنية العامة بموضوعات الأمن المعلوماتي [128]

الشكل 3.9: الصفحة الرئيسية لموقع حماية الأطفال عند النفاذ (safespace.qa)

7.9 أهم القوانين والتشريعات

1. مشروع قرار بشأن لائحة تنظيم عمل مقدمي خدمة التصديق للعام 2010م [129]: ينظم القانون عمل المصادقة الإلكترونية على نطاق الدولة.
2. قانون المعاملات والتجارة الإلكترونية للعام 2010م [130]: ينظم هذا القانون المعاملات والتجارة الإلكترونية على نطاق الدولة.

8.9 بعض المواقع المهمة

الجدول 1.9: بعض المواقع المهمة للمعلوماتية والاتصالات في دولة قطر

إسم المؤسسة	عنوان الموقع	المهام الرئيسية
المركز الوطني لأمن المعلومات	www.qcert.org	تقديم الدعم التقني والنصح والإرشاد، وضع السياسات العامة والموجهات
المجلس الأعلى للاتصالات وتكنولوجيا المعلومات	www.ictqatar.qa	تنظيم قطاع المعلومات والاتصالات

موقع Safespace	www.safespace.qa	تقديم مواد تعليمية للتوعية في مجال حماية الأطفال عند النفاذ
موقع بوابة قطر الوطنية للتعليم الإلكتروني	www.elearning.ictqatar.qa	يقدم الموقع مواد تعليمية متخصصة في مجال التعامل مع تكنولوجيا المعلومات والاتصالات وتبادل الخبرات
موقع حكومي	portal.www.gov.qa	الموقع عبارة عن واجهة شاملة وآمنة لتقديم الخدمات الحكومية

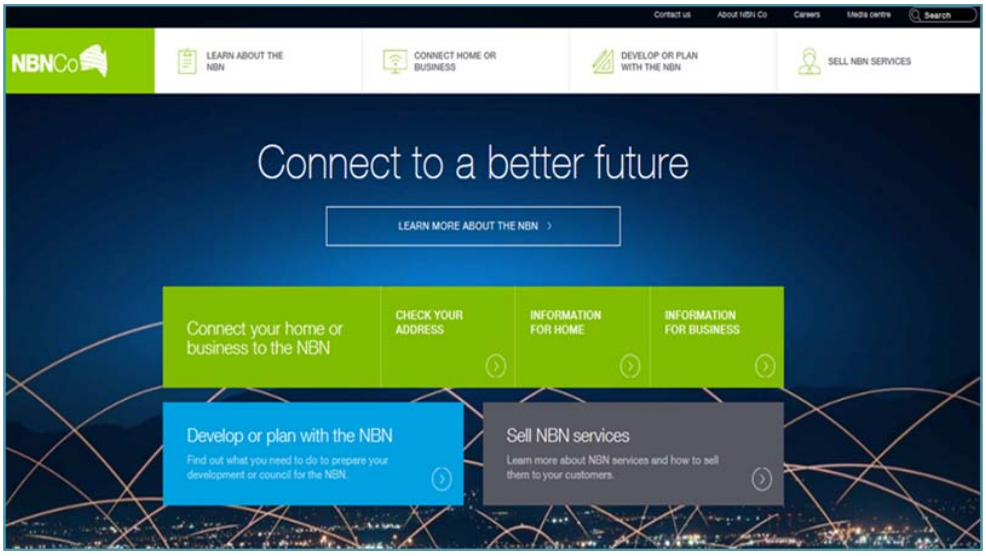
الفصل العاشر
تجربة أُستراليا

1.10 الخطة الوطنية والاتجاهات المستقبلية لبناء صناعة المعلوماتية

أستراليا من الدول المتقدمة التي تعتمد كل القطاعات فيها تقريباً بصورة كبير على بنيات الاتصالات ونظم المعلومات. نسبة لموقعها الجغرافي البعيد نسبياً من بقية العالم، سعت الدولة ومن الأيام الأولى لعصر المعلوماتية إلى بناء شبكة تراسل Telecommunication Transmission Network قوية وعالية الموثوقية لربط أستراليا بالولايات المتحدة واليابان والشرق الأوسط وبقية بلدان جنوب شرق أسيا، حيث تم استخدام كل من كيبلات الألياف الضوئية البحرية والأقمار الصناعية لتحقيق هذا الهدف.

في مجال بناء وتحديث شبكة الاتصالات الداخلية، قامت الدولة بالإعلان عن المشروع الوطني للربط باستخدام السعات العريضة National Broadband Network(NBN) بتكلفة قدرها 37 مليار دوالار أسترالي. يهدف هذا المشروع لربط ما يقارب 93% من المستخدمين بشبكة السعات العريضة التي تستخدم تكنولوجيا الألياف الضوئية إلى المنازل بحلول العام 2021م. أيضاً يهدف المشروع لتوصل المستخدمين في المناطق البعيدة بشبكة الجيل الرابع للنظم اللاسلكية (LTE). أيضاً يخطط المشروع لإطلاق اثنين من وحدات الأقمار الصناعية (Next-Generation of KA-Band Satellites) بسعة تراسل تصل إلى 80 قيغا بت في الثانية لكلٍ، وذلك لدعم موثوقية واستقرار عمل هذه الشبكات في أوقات الكوارث[131].

تعمل الهيئة الوطنية لمشروع شبكة السعات العريضة NBN Co التي تم إنشاؤها في 2009م على إدارة مشروع NBN[132]. الشكل 1.10 يوضح الموقع الرئيسي لهذه الهيئة لعكس وتوضيح جميع أنشطة المشروع للمجتمع الأسترالي.



الشكل 1.10: الموقع الرئيسي للهيئة الوطنية لبناء شبكة النطاق العريض (المصدر: http://www.nbnco.com.au/)

2.10 القطاعات والمصالح الإستراتيجية

في أستراليا تم تعريف البنيات التحتية الأساسية الحرجة للمعلوماتية والاتصالات على أنها تلك المرافق والخطوط الرئيسية للإمداد وتكنولوجيا المعلومات والاتصالات التي إذا دمرت أو عُطلت لفترة طويلة، يمكن أن تُأثر تأثيراً مباشراً على الصعيد الاجتماعي والرفاه الاقتصادي للأمة وفي قُدرات الدفاع الوطني والأمن القومي [133]. أي أن البنية التحتية للمعلومات هي جزء أساسي من منظومة الأمن القومي، على الرغم من أن الكثير من مُنشآتها مملوكة للقطاع الخاص، أو تتم إدارتها بواسطة القطاع الخاص.

في أستراليا تم إسناد مهام رئاسة لجنة حماية البنيات التحتية الأساسية للمعلوماتية والاتصالات إلى النائب العام Attorney-General's Department. تعمل هذه اللجنة من خلال شبكة موثوقة لتبادل المعلومات لحماية القطاعات الرئيسية الآتية:-

- الاتصالات (Telecommunications (Phone، Fax، Internet، Satellites) and Mass Communications، Cable
- الطاقة (غاز، وقود بترول، مصافي تكرير، خطوط نقل البترول، توليد ونقل الكهرباء).

- البنوك والتمويل والتجارة (Banking، Finance ، and Trading، Exchanges)
- قطاعات توريد مواد الغذاء الرئيسية (Bulk Production، Storage ، and Distribution)
- خدمات الطوارئ Emergency Services،
- قطاع الصحة (Hospitals، Public Health ، and Research and Development Laboratories)
- أماكن التجمعات العامة Mass Gatherings
- خدمات المواصلات (Air Traffic Control، Road، Sea، Rail ، and Inter-modal)
- الخدمات العامة (Water، Waste Water ، and Waste Management).

3.10 المبادرات في الماضي والحاضر

حماية البنية التحتية للمعلوماتية تتطلب مشاركة الجميع (المالك، المشغل، الجهات المنظمة، المنظمات المهنية واتحادات المصنعين) وتعاونهم المستمر مع كل المستويات الحكومية. لتحقيق هذا الهدف قامت الحكومة بوضع الموجهات والقواعد الأساسية التالية:

- الهدف الأساسي لحماية البنيات التحتية للمعلوماتية هو تقليل المخاطر على الصحة العامة والسلامة، ووزيادة الثقة، لضمان الأمن الاقتصادي في أستراليا والحفاظ على القدره التنافسية للدولة، وضمان استمرارية الخدمات الحكومة.
- • يجب تحديد البنية التحتية الحيوية المهمة، وتحليل المخاطر التي يمكن أن تتعرض لها وحمايتها.

- من الصعب حماية البنية التحتية للمعلوماتية من كل المخاطر لذلك تجب الاستعانة بوسائل إدارة المخاطر الحديثة لتحديد وإعداد الخطط البديلة في حالة تعرض البنية التحتية الحرجة للمعلوماتية للاعتداء أو التدمير.
- مسؤولية تحديد وسائل إدارة البنية التحتية للمعلوماتية تقع على عاتق كل من المالك والمشغل على حدٍ سواء.
- موضوع حماية البنيات التحتية المهمة يجب أن يأخذ في الحسبان استقلالية التجارة والقضاء والمصالح الحكومية المختلفة.
- موضوع حماية البنية التحتية للمعلوماتية يحتاج لتعاون مستمر بين المالك والمشغل والحكومة.
- يجب تبادل المعلومات المتعلقة بالتهديدات على البنيات التحتية للمعلوماتية بين كلٍّ من المالك والمشغل والحكومة بدرجة عالية من الموثوقية.
- يجب أخذ الحيطة عند الإشارة للتهديدات على البنيات التحتية القومية وذلك لعدم خلق قلق غير مبرر لقطاع السياحة والتجارة الدولية.
- الاعتماد على مخرجات البحوث العلمية لتصميم إستراتيجيات ذات درجة عالية من الموثوقية لتحجيم وتخطي المخاطر التي تواجة البنيات التحتية للمعلوماتية.

حماية البنيات التحتية للمعلوماتية وسياسة مكافحة الإرهاب

لجنة محاربة الإرهاب لها دور أساسي وفعّال في حماية البنيات الأساسية. بما أن مسؤولية حماية البنيات التحتية مسؤولية متبادلة بين القطاعات والمستويات المختلفة تحت إدارة النائب العام، لذلك قامت الحكومة بعمل الإجراءات الآتية:-

- تحديد البنيات التحتية الأساسية والمخاطر التي يمكن أن تتعرض لها.
- مساعدة القطاع التجاري في عملية إدارة المخاطر من خلال لجنة لتبادل المعلومات وإدارة المخاطر Trusted Information Sharing Network (TISN)

- تشجيع وتطوير الحلول المحلية والعالمية في مجال أمن وسلامة البنيات التحتية للمعلوماتية.

الأمن الإلكتروني

أصدرت الحكومة المركزية الأسترالية قانون للأمن الإلكتروني في عام2007م وخصصت كمية مقدرة من الموارد المالية لتمويل المبادرات في مجال زيادة الترابط والتعاون لمواجهة المخاطر والمهددات الإلكترونية للاقتصاد الأُسترالي. أيضاً تم تكوين لجنة للتنسيق بين الإدارات المختلفة E-Security Policy and Coordination (ESPaC) وذلك لصياغة الموجهات العامة للأمن الإلكتروني والتي تحتوي على النقاط التالية:

- تقليل التهديد والمخاطر الإلكترونية على قطاع المعلومات والاتصالات الحكومية.
- تقليل التهديد والمخاطر الإلكترونية للبنيات التحتية الأساسية.
- تعزيز حماية المستخدم العادي من خلال العمل على حمايتة من الهجمات الإلكترونية والاحتيال الإلكتروني.

4.10 نبذة عن المنظمات والمؤسسات القائمة على حماية المعلوماتية

في أُستراليا تتشارك المؤسسات الآتية مهمة حماية البنيات التحتية الحرجة للمعلوماتية:

1. مكتب النائب العام Attorney-General's Department: حيث يعمل قسم الأمن وحماية البنيات التحتية على تطوير التشريعات واللوائح والنظم التي تخدم أهداف الأمن الإلكتروني ومكافحة جرائم المعلوماتية والإرهاب.
2. مجموعة تبادل الخبرات والتي تعرف Trusted Information Sharing Network for Critical Infrastructure Protection: تم إنشاء هذه المجموعة لغرض تشجيع تبادل الخبرات بين القطاع العام والخاص في

مجالات أمن المعلومات وحماية البنيات التحتية الحرجة للاتصالات والمعلومات.

3. لجنة تنظيم سياسات الأمن الإلكتروني E-Security Policy and Coordination Committee (ESPaC): وهي لجنة تضم في عضويتها ممثلين لكل من وزارة الدفاع، المخابرات العامة، هيئة الاتصالات والتجارة الإلكترونية، شرطة الجرائم الإلكترونية، مكتب رئيس الوزراء، ومكتب التقييم القومي. يرأس هذه اللجنة النائب العام ومهمتها رفع الوعي ودعم البحوث والدراسات وتنسيق الجهود في مجال أمن المعلوماتية وحماية البنيات التحتية الحرجة.
4. وزارة الاتصالات والتجارة الإلكترونية: تسهم هذه الوزارة في حماية البنيات التحتية للمعلوماتية من خلال إدارة مجموعة تبادل الخبرات (TISN) حيث ترأس الوزارة مجموعة الخبراء والمستشارين والتي تقدم النصح والمشورة إلى TISN في الموضوعات التي تستجد في مجال أمن المعلومات والتي تضم بصورة خاصة المؤسسات الآتية:
   - مؤسسات الاتصالات والتجارة عبر الإنترنت.
   - المؤسسات التي تستخدم أنظمة التحكم الإشرافي Supervisory Control and Data Acquisition (SCADA)
   - خدمات الشبكات اللاسلكية .Wireless Services
5. لجنة الطوارئ والاستجابة لجرائم الحاسوب Computer Emergency Readiness Team : تم إنشاء هذه اللجنة في 2005م ضمن مكتب النائب العام لتقوم بالتنسيق على المستوى الداخلي والدولي في الشئون التي تتصل بأمن المعلومات وتقدم المشورة والدعم اللازمين.
6. إدارة الأمن والدفاع Defence Signals Directorate (DSD): تعمل هذه الإدارة على حماية نظم الاتصالات الرسمية للدولة وتقدم الدعم الفني اللازم

بما يختص بأمور تكنولوجيا أمن الشبكات والتشفير وتطوير الموجهات والسياسات العامة في مجال المعلوماتية.

7. الشرطة الفدرالية الأُسترالية (Australian Federal Police (AFP: مع إصدار قانون جرائم المعلوماتية في 2001م عملت الشرطة الأُسترالية على إنشاء مركز لجرائم التكنولوجيا المتقدمة Australian High Tech Crime Centre [134] (AHTCC) والذي يعمل على التحقيق في الجرائم الإلكترونية وتقديمها للقضاء.
8. المخابرات الأُسترالية (ASIO) Australian Security Intelligence Organization: تقوم أيضاً المخابرات العامة بجمع المعلومات المتعلقة بالجرائم الإلكترونية وتحليلها وتقديم النصح للدولة في هذا الخصوص.

5.10 الوعي العام والإنذار المبكر

بصوره عامة هنالك اثنتان من المؤسسات التي تقدم خدمات التوعية والإنذار المبكر هما:

1. إدارة الأمن والدفاع (Defence Signals Directorate (DSD: تعمل هذه الإدارة على تقديم خدمات التوعية والإنذار المبكر بالمخاطر لمؤسسات القطاع العام من خلال مشروع حصر جرائم المعلوماتية والاختراق الإلكتروني Information Security Incident Detection Reporting and Analysis Scheme وتحليلها (ISIDRAS) .

2. فريق الحاسوب الأسترالي للاستجابة والطوارئ Australian Computer Emergency Response Team (Aus-CERT): تم إنشاء هذا المركز بجامعة كوينزلاند ويقوم بتقديم الدعم الفني لمؤسسات القطاع الخاص وبعض من المؤسسات الحكومية وذلك من خلال المركز الوطني للتنبة بمخاطر الجرائم الإلكترونية.

6.10 حماية الأطفال عند النفاذ

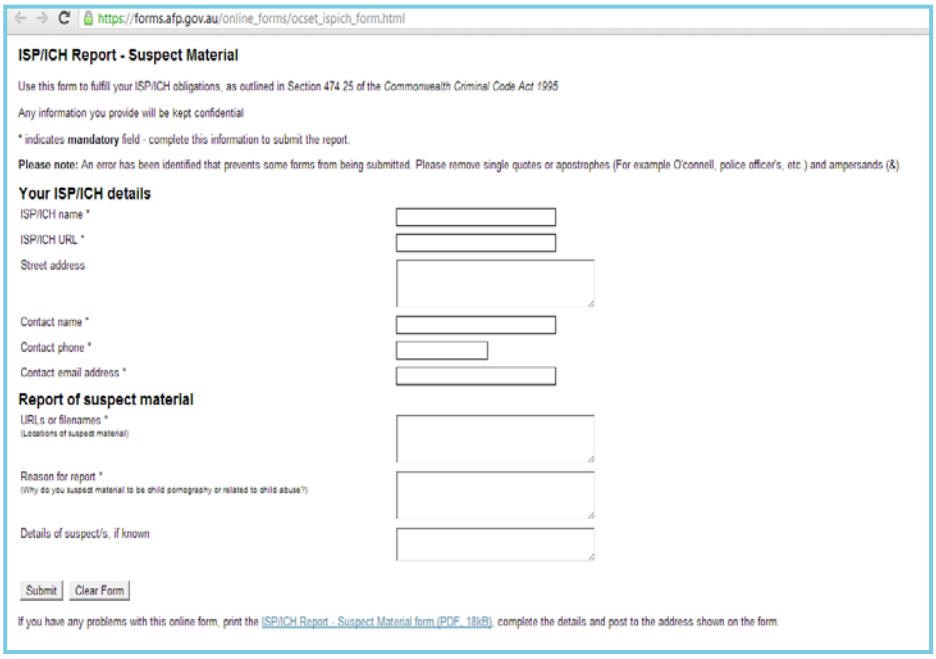
نسبة لاهمية هذا الموضوع وتصدره للأجندة الدولية، قامت أستراليا بسن عدد من القوانين والتشريعات التي تتعلق بحماية الأطفال على الإنترنت[135]. تقوم كل الأطراف في الدولة والمهتمة بموضوع حماية الأطفال (الآباء، المدرسون، المؤسسات التعليمية، مقدمو خدمة الإنترنت والشرطة الفيدرالية) بتطبيق هذه القوانين والسياسات واللوائح. مثلاً الشرطة الفيدرالية الأُسترالية تقوم بالتحقيق والتنسيق الجنائي فيما يخص جميع الجرائم الإلكترونية والمعلوماتية الخاصة بالأطفال، وهنالك فريق كامل مخصص لهذا الغرض. في كثير من الحالات تقوم الشرطة وبالتنسيق مع مقدمي خدمات الإنترنت بتحديد المواقع والصفحات التي تحتوي على المواد غير المتوافقة مع القانون الأُسترالي واتخاذ الإجراءات اللازمة بذلك مباشرة إذا كان المحتوى مستضافاً داخل أستراليا أو التعاون مع الهيئات الدولية في حالة المحتويات المستضافة (مخزنة) خارج البلاد.

تقوم الشرطة باستقبال البلاغات من المواطنين وهيئات حماية الأطفال في أستراليا على المواقع الإلكترونية الموضحة في الجدول1.10. الشكل 2.10 المرفق يوضح الشكل العام لنموذج تقديم البلاغات.

الجدول 1.10: يوضح المواقع الرئيسية للإبلاغ عن المحتويات المخالفة لقوانين حماية الطفل عند النفاذ.

عنوان الموقع	الجهة التي يتبع لها
https://forms.afp.gov.au/online_forms/ocset_form	الشرطة الفدرالية الأسترالية
http://www.thinkuknow.org.au/	منظمة thinkuknow
http://www.virtualglobaltaskforce.com/	مجموعة Virtual Global

Taskforce	
مجموعة مقدمي خدمة الإنترنت	https://forms.afp.gov.au/online_forms/ocset_ispich_form.html
هيئة الاتصالات والوسائط المتعددة	http://www.acma.gov.au
الجمعية الوطنية للوقاية من إساءة معاملة الأطفال وإهمالهم (NAPCAN)	http://napcan.org.au/



الشكل 2.10: يوضح نموذج البلاغات المعد بواسطة مجموعة مقدمي الإنترنت.

تعمل أيضاً الحكومة الأسترالية ومن خلال مشروع سيبر إسمارت (Cybersmart) على تقديم الكثير من المواد المفيدة في التوعية والتعليم للآباء

والمدارس والمدرسين والمهتمين بأمن المعلومات وحماية الأطفال عند النفاذ. الشكل 3.10 يوضح النافذة الرئيسية للموقع http://www.cybersmart.gov.au.

الشكل 3.10: يوضح الموقع الرئيسي لمشروع سيبر إسمارت (Cybersmart)

7.10 القوانين والتشريعات

من أجل الارتقاء بتكنولوجيا الاتصالات والمعلومات أصدرت الدولة الأسترالية القوانين والتشريعات الآتية:-

1. قانون المعاملات الإلكترونية لسنة 1999م، وهو قانون يُعنى بتنظيم المعاملات الخاصة التجارة الإلكترونية.
2. قانون جرائم المعلوماتية لسنة2001م والذي أُعتبر إضافة حقيقية للقانون الجنائي العام إذ أنه وضع الإطار العام للتحقيق في الجرائم الجنائية الإلكترونية وإصدار العقوبات اللازمة بحقها. ويغطي القانون الجوانب الآتية:
   - التغير غير المصرح به للمعلومات.
   - التعطيل غير المصرح به لأنظمة الاتصالات.
   - الوصول غير المصرح به للبيانات الخاصة.

- إتلاف البيانات المخزنة في النظم.
- امتلاك أو تزويد أو تطوير نظم أو بيانات بغرض ارتكاب الجريمة.

3. تعديل القانون الجنائي لسنة 1995 وذلك لإضافة فقرة الإرهاب.
4. قانون الرسائل غير المرغوب فيها (SPAM) لسنة 2003م: حيث يمنع هذا القانون إرسال الرسائل التجارية غير المرغوب فيها في البريد الإلكتروني أو الجوال للمستخدم من غير أخذ موافقته.
5. قانون الجرائم الجنسية ضد الأطفال Sexual Offences Against Children) Act 2010 : وضع هذا قانون القواعد الأساسية للعقوبات بشأن الجرائم الجنسية ضد الأطفال [136].
6. تعديل قانون اعتراض الاتصالات السلكية واللاسلكية وخدمات الاستخبارات2011م Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011 [137].
7. قانون شبكة السعات العريضة لسنة 2011م: وهو قانون يُعنى بموضوعات حرية المعلومات وإدارة قطاع الاتصالات باستخدام السعات العريضة[138].

8.10 بعض المواقع المهمة

الجدول 2.10: مواقع أهم الجهات التي تسهم في عملية إدارة أمن المعلومات والبنيات التحتية الأساسية للاتصالات

اسم المؤسسة	عنوان الموقع	المهام
Cyber-smart	www.cybersmart.gov.au	يقدم الموقع نصائح قيمة في مجال حماية الأطفال والأُسرة من الجرائم الإلكترونية على الإنترنت. يحتوى الموقع على

		الكثير من المواد التي يمكن الاستفادة منها في هذا المجال
Stay Smart Online	www.staysmartonline.gov.au/	يقدم هذا الموقع نصائح متخصصة لأصحاب الأعمال التجارية والعوائل ولجميع مستخدمي الإنترنت من أجل السلامة والأمان عند النفاذ
CERT	www.cert.gov.au/	يعمل هذا الموقع على تقديم الدعم التقني والتعامل مع البلاغات اليومية
Cyber Security	www.dbcde.gov.au/online_safety_and_security/cyber_security	يوفر الموقع الكثير من وسائل المساعدة للمستخدمين والمجموعات التجارية الصغيرة
Cyber-safety plan	www.dbcde.gov.au/funding_and_programs/cybersafety_plan	يقدم الموقع الكثير من المواد المفيدة للآباء والمدارس من أجل حماية الأطفال
The Easy Guide to Socialising Online	www.dbcde.gov.au/easyguide	يقدم الموقع نصائح بخصوص التعامل مع مواقع التواصل الاجتماعي ومحركات البحث ومواقع الألعاب
Online safety and security	www.dbcde.gov.au/online_safety_and_security	هذه الصفحة تعرض المواد المتعلقة بجهود الحكومة في مجال أمن المعلومات
OnSecure	www.onsecure.gov.au/	يقدم الموقع الدعم الفني المستجدات التقنية في مجال أمن المعلومات
ScamWatch	www.scamwatch.gov.au/	يقدم الموقع نصائح قيّمة للمستخدمين في موضوعات الخاصة بالاحتيال (phishing)
ThinkUKnow	www.thinkuknow.org.au/	يقدم هذا الموقع معلومات عن الدورات التدريبية للآباء والمعلمين من أجل مساعدة الأطفال على الإنترنت
The Trusted	www.tisn.gov.au/Pages/def	في هذا الموقع يتم تبادل المعلومات

Information Sharing Network	ault.aspx	بشأن الحماية الإلكترونية بين القطاع الخاص والحكومي

.

الفصل الحادي عشر
تجربة ماليزيا

1.11 الخطة الوطنية والاتجاهات المستقبلية لبناء صناعة المعلوماتية

ماليزيا هى إحدى دول جنوب شرق آسيا التي ازدهرت في فترة زمنية وجيزة، وذلك نتيجة لاتباع السياسات الحكيمة والاستغلال الأمثل للموارد الطبيعية. في العام 1997م تم وضع خطة قومية شاملة للتطوير بغرض تحقيق أهداف 2020م. هذه الخطة تحتوي على إستراتيجية شاملة للنهوض بقطاع المعلوماتية والاتصالات على النحو التالي:

- الاستفادة القصوى من ثورة المعلومات في تحقيق التنمية البشرية.
- تطوير وتحديث بنية نظم الاتصالات.

لتحقيق هدف الاستفادة القصوى من تكنولوجيا المعلومات والاتصالات، عملت الدولة على تطوير هذا القطاع بالدعم والتدريب للكوادر البشرية في كل المجالات المتصلة بتكنولوجيا المعلومات. أيضاً عملت على زيادة ثقة المستخدم النهائي بهذه التكنولوجيا من خلال اتخاذ القرارات الجريئة بحوسبة كل قطاعات الخدمات الحكومية والتجارية والقيام بواجب الحماية وذلك بإنشاء ودعم المؤسسات المعنية بأمن المعلومات.

في مجال تطوير بنية شبكة الاتصالات، قامت الدولة بإنفاق ما يعادل 4 مليارات دولار في مشروع عرف High Speed Broad band (HSBB) Network لتحديث كل بنيات شبكات الاتصالات إلى الجليل الثاني من تكنولوجيا الألياف الضوئية [139]. يهدف المشروع لتوصيل المستخدم النهائي بسعة قدرها 100 ميغا بت في الثانية للمنزل (المستخدم العادي) و1قيغا بت في الثانية للمحال التجارية أو المستخدم التجارى. في هذا المشروع تم تغير كل مكونات شبكة الاتصالات إلى تكنولوجيا حديثة (تعتمد على الألياف البصرية). في العام 2011م وعند حدوث زلزال اليابان لم تتأثر

خدمات المعلوماتية في ماليزيا، على الرغم من انقطاع الوصلة الدولية من ناحية الشرق وهذا يُعضد موثوقية التصميم الجيد للبنية التحتية للاتصالات.

من ناحية أخرى، عملت الدولة على تطوير قطاع الاتصالات عبر الأقمار الصناعية حيث تمتلك اليوم الشركة الماليزية)Malaysia East Asia Satellite MEASAT) عدد 5 أقمار صناعية في المدار المتزامن لتقدم مجموعة من الخدمات المختلفة في مجال الاتصالات والبث التلفزيوني والإذاعي وخدمات الإنترنت بسعات عرض مختلفة وحسب الطلب. أيضاً تعمل هذه الأقمار كوسيلة تراسل إسعافية للاتصالات في حالات الكوارث أو انقطاع الوصلات الرئيسية التي تربط ماليزيا بالعالم الخارجي.

2.11 القطاعات والمصالح الإستراتيجية

في ماليزيا تم تعريف المنشآت الحيوية الأساسية على أنها تلك الأُصول والنظم المادية والبرامج التي إذا تعطلت أو توقفت، يكون لها تأثير مدمر على كل من الآتي:

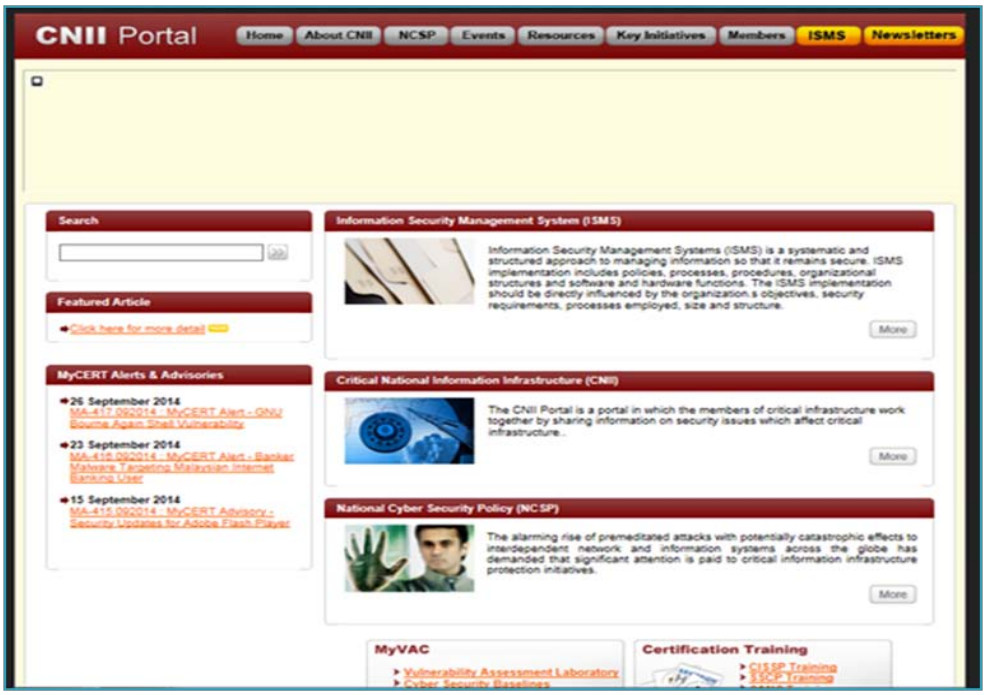
- الاقتصاد الوطني.
- المكانة الوطنية.
- الأمن القومي.
- مقدرة الحكومة على تسيير الأُمور العامة.
- السلامة والصحة العامة.

وفقاً لهذه المعايير تم اعتماد القطاعات الآتية على أنها تشكل بنيات حيوية أساسية وطنية[140] National Critical infrastructure

1. القطاع المالي Financial Sector
2. المياة والصرف الصحي Water and Sewerage
3. الاتصالات Communications
4. الطاقة Energy
5. خدمات الصحة والطوارئ Health and Emergency Services

6. الصناعة Industry
7. الحكومة المركزية Central Government
8. الخدمات الحكومية Government Services
9. المواصلات Transportation
10. الجيش Military

تعمل الحكومة الماليزية من خلال مؤسسة سيبرسكيورتي ماليزيا (cybersecurity Malaysia) على التنسيق بين الإدارات المختلفة لهذه القطاعات لقيادة عملية الابتكار وتشجيع عملية تبادل الخبرات بين الخبراء والمهنيين في هذه المؤسسات. هنالك موقع مخصص لتنسيق هذه الأنشطة (cnii.cybersecurity.my). الشكل 1.11 يوضح الموقع الرئيسي لتنسيق جميع الأنشطة في مجال حماية البنيات التحتية الحرجة. يحتوى الموقع أيضاً على الكثير من المواد القيمة (موجهات عامة، توصيات، تقارير عن حالات للاختراق،...الخ) والتي يمكن للقارئ أن يرجع إليها بغرض الاستفادة منها [141].



الشكل 1.11: الموقع الرئيسي لمجموعة حماية البنيات التحتية الوطنية الأساسية والحرجة في ماليزيا (المصدر: cnii.cybersecurity.my)

3.11 المبادرات في الماضي والحاضر

أطلقت الحكومة الماليزية ما عُرف بالأجندة الوطنية لتكنولوجيا المعلومات National IT Agenda (NITA) في العام 1996م كجزء من الإستراتيجية الرئيسية لإعداد الأمة لمواجهة تحديات عصر تكنولوجيا المعلومات. هذه الأجندة تحتوي على إطار يحدد الخطوط العريضة وجدول زمني للأعمال يهدف إلى ضمان التطوير المتوازن لتكنولوجيا المعلومات والبنية التحتية للاتصالات والتطبيقات. وفقاً لأجندة NITA فإن تحقيق النجاح لهذه الإستراتيجية يتطلب توفير قدر من الثقة والإيمان باستخدام تكنولوجيا الاتصالات والمعلومات في كل المجالات الحيوية. هذه الثقة يمكن أن تعزز عملياً من خلال تعزيز أمن وسلامة تكنولوجيا المعلومات، وذلك لتحويل المجتمع الماليزي إلى مجتمعٍ للمعلومات والمعرفة بحلول العام 2020م.

بجانب مشروع الأجندة الوطنية أنشأت ماليزيا ما يعرف بالمجلس القومي لتكنولوجيا المعلومات National Information Technology Council (NITC) [142]. هذا المجلس يُعنى في المقام الأول بتوسيع دائرة المشاركة بين القطاع العام والخاص، وذلك من أجل تنفيذ الأجندة الوطنية للمعلومات. بافتراض أن المعلومات هي من أهم أصول وركائز المجتمع الحديث، روجت الدولة لعدد من المفاهيم الحديثة مثل المجتمع الإلكتروني E-Community والخدمات الإلكترونية العامة E-Public Services والاقتصاد الإلكتروني E-Economy.

مؤتمر الأمن الإلكتروني الماليزي 2005م

احتضنت العاصمة الماليزية كوالالمبور مؤتمر قومى لأمن المعلومات في 2005م جمع بين المتخصصين وأصحاب القرار الحكومي وشركات الحلول الأمنية وذلك تحت رعاية وتنظيم كل من: وزارة التعليم والابتكار العلمي Ministry of Science، Technology and Inovation(MOSTI) ، وزارة الطاقة والمياه

والاتصالات Ministry of Energy، Water and Communications ، هيئة الاتصالات والوسائط المتعددة الماليزية Communications and Multimedia Commission، المركز القومي لأمن المعلومات والاستجابة السريعة للطوارئ National ICT Security and Emergency Response Centre، والمركز القومي لتطوير الإدارة والتحديث والتخطيط Malaysian Administrative Modernization and Management Planning. ناقش المؤتمر الموضوعات الخاصة بأمن البيانات بصورة عامة مع التركيز على النقاط التالية:

- فريق الحاسوب للاستجابة السريعةComputer Emergency Response Teams
- حماية البنيات التحتية الأساسية Critical Infrastructure Protection
- أمن الشبكات والتطبيقات Network and Application Security
- إدارة الأمن والإستراتيجيات Security Management and Strategy.
- مشاركة المعلومات Knowledge-Sharing.

استمر المؤتمر في عقد فعاليات سنوية منذ ذلك التاريخ، وذلك بغرض توفير بيئة مساعدة للخبراء والعلماء وقادة المؤسسات الحكومية، للاجتماع والتباحث حول جميع المستجدات في مجال حماية قطاع المعلوماتية والاتصالات [143].

السياسة الوطنية الماليزية لحماية فضاء المعلومات للعام 2007م

في العام 2007م أعلنتMOSTI عن السياسة الوطنية الماليزية لحماية الفضاء الإلكتروني National Cyber-Security Policy والتي تهدف في المقام الأول إلى تعزيز حماية البنيات الأساسية الحرجة وذلك بالتركيز على الجوانب والمحاور الآتية [144]:

1. تطوير عملية إدارة أمن المعلومات من خلال التشجيع على التعاون بين القطاعات المختلفة وتنسيق العمليات و تبادل الخبرات.
2. تطوير القوانين واللوائح التي تنظم عملية أمن المعلومات.

3. دعم عملية تطوير التكنولوجيا التي تستخدم في أمن المعلومات وحماية البنيات الحرجة وتطوير والموارد البشرية التي تخدم في هذا المجال.
4. العمل على نشر ثقافة أمن المعلومات.
5. دعم البحوث والدراسات والعمل على استقلال الدولة في هذا المجال.
6. التأكد من تنفيذ القوانين واللوائح.
7. دعم الجاهزية لمقابلة الكوارث.
8. العمل على تشجيع التعاون الدولي وتبادل الخبرات.

4.11 نبذة عن المنظمات والمؤسسات القائمة على حماية المعلوماتية

بصورة عامة في ماليزيا تم تقسيم مهام وعمليات حماية البنيات التحتية الأساسية (تنظيم العمليات، إدارة العمليات، منع الجرائم، وضع السياسات العامة) حسب الجدول 1.11.

الجدول 1.11: توزيع مهام حماية المعلوماتية والبنيات الحرجة بين القطاعات والإدارات الحكومية المختلفة في ماليزيا

المهام	الجهة الموكل إليها
التنظيم	هيئة الاتصالات والوسائط المتعددة
إدارة أمن البيانات في القطاع العام	وحدة الإدراة والتخطيط والتحديث
منع الجرائم والتحقيق في حالات الإختراق الإلكتروني	وحدة شرطة أمن المعلومات والجرائم الإلكترونية
وضع السياسات العامة	وزارة العلوم والتكنولوجيا
حماية البنيات الأساسية	وزارة الطاقة والمياه والاتصالات
الجمع بين القطاع العام والقطاع الخاص	مجموعة تداول وتبادل المعلومات Information Sharing Forum (ISF)

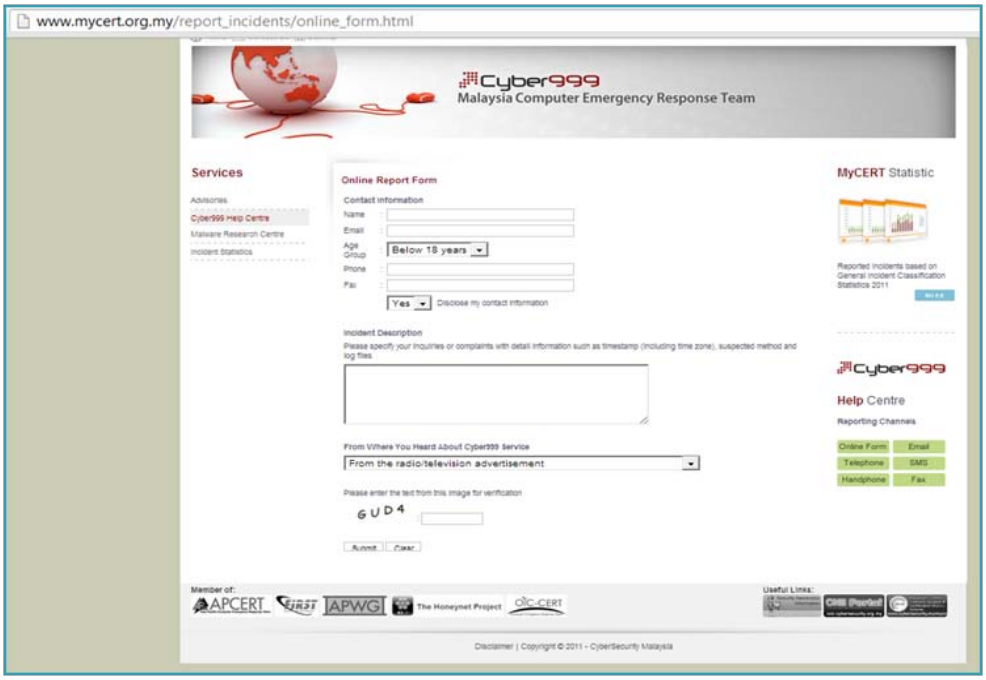
5.11 الوعي العام والإنذار المبكر

في ماليزيا تقوم المؤسسات الآتية بمهام زيادة الوعى العام والإنذار المبكر

فريق الحاسوب الماليزي للاستجابة والطوارئ

تم إنشاء هذا الفريق في سنة 1997م. عبر السنوات عمل هذا الفريق كمرجع أساسي في عملية الدعم التقني والفني لعملية أمن البيانات والإنترنت، إذ كان من أهم أهدافه تقليل احتمالية حوادث الاختراق الإلكتروني والخسائر الناتجة عنها. من المهام الأساسية لفريق الـ (MyCERT) [145] الآتي:

- يعمل كمرجع أساسي لتوفير الخبرة والمشورة للقطاعات الحكومية والخاصة والأفراد.
- يقوم بتجهيز ورفع التقارير عن جميع حالات الاختراق الإلكتروني للجهات الحكومية بغرض اتخاذ القرارات المناسبة.
- نشر الموجهات العامة بأمن البيانات وبالأخص كل ما يتعلق بمستجدات طرق الاختراق الإلكتروني وإستراتيجيات منع الاختراق.
- يعمل كنقطة مرجعية للدعم الفني حيث يوفر العديد من وسائل منع الاختراق.
- يعمل على التعليم والتدريب ورفع الوعي في المجتمع في مجال أساسيات الأمن الإلكتروني.
- يعمل على استقبال البلاغات من المجتمع والاستجابة للطوارئ على مدار الـ 24 ساعة. الشكل2.11 (www.mycert.org.my) يوضح الواجهة الرئيسية لإرسال البلاغات.



الشكل 2.11: الواجهة الرئيسية للبلاغات عن حالات الطوارئ الخاصة بالمعلوماتية (المصدر: www.mycert.org.my)

أمن معلومات ماليزيا

في العام 2005م تم تنظيم قطاع أمن المعلومات وذلك بتعريف وإضافة عدد من الصلاحيات الإضافية للجنة القومية لأمن الاتصالات والمعلومات National ICT Security and Emergency Response Centre (NISER) وتكوين ما يعرف بأمن معلومات ماليزيا Cyber-Security Malaysia [146]. اليوم يعمل مركز أمن معلومات ماليزيا تحت إشراف وزارة العلوم والتكنولوجيا والابتكار(MOSTI) ويقدم المشورة والدعم لكل القطاعات في الدولة ويعتبر نقطة تنسيق وتبادل للخبرات بين القطاع العام والخاص في هذا المجال. الشكل3.11 يوضع الصفحة الرئيسية لموقع Cyber-Security Malaysia. يقدم مركز أمن معلومات ماليزيا الخدمات الآتية :

- البحوث والدراسات التي تتعلق بطرق وتقنيات الاختراق الإلكتروني.

- البحوث والدراسات التي تتقلق بوسائل المراجعة والتحقيق الإلكتروني وتتبع الجرائم المعلوماتية Computer forensic technology.
- المراجعة المستمرة للسياسات والموجهات الخاصة بأمن المعلومات والاتصالات والتعاون المستمر مع المراكز العالمية والإقليمية في هذا المجال وذلك لمعرفة آخر المستجدات في مجال التهديدات الإلكترونية.
- تنمية القدرات في مجال أمن المعلومات.
- إدارة الجودة في مجال حماية البنيات التحتية للمعلوماتية والاتصالات.
- إدارة عملية تقييم الشهادات المهنية في مجال أمن المعلومات.

الشكل 3.11: الواجهة الرئيسية لموقع أمن معلومات ماليزيا (cyber-security Malaysia:www.cybersecurity.my)

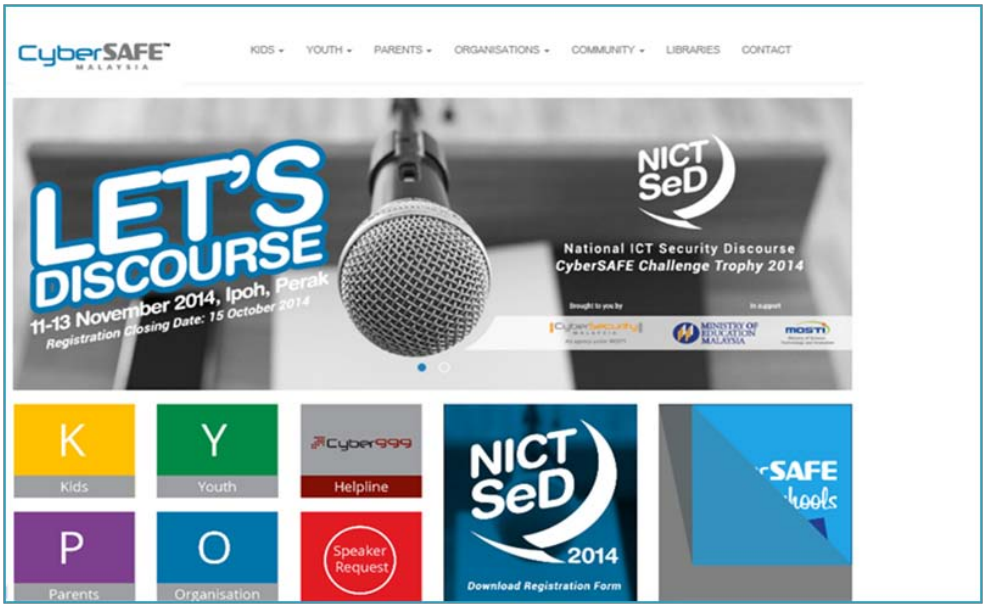
6.11 حماية الأطفال عند النفاذ

قامت الهيئة الماليزية للاتصالات والوسائط المتعددة في العام 2009م بتقديم مبادرة حماية الأطفال عند النفاذ وذلك لمساعدة الآباء، ولجعل النفاذ للإنترنت عملية آمنة

للأبناء. من أهم المخاطر التي تواجة الأطفال عند النفاذ والتي تم تحديدها بواسطة المبادرة:

- البلطجة Cyber-bullying
- الإباحية Pornography
- العنف Violence
- الاعتداء العنصري والكراهية Racial abuse and hate
- إدمان الألعاب عبر الإنترنت Online gaming & addiction
- الاحتيال والخداع عبر الإنترنت Online fraud & deception

استجابةً لهذه المبادرة، هنالك اليوم في ماليزيا العديد من المواقع التي تقدم النصح للآباء بخصوص المساعدة على سلامة الأطفال عند النفاذ على المواقع الإلكترونية. من أهم هذه المواقع موقع سيبرسيف الشكل CyberSafe 4.11 (www.cybersafe.my) والذي يحتوي على العديد من المواد القيمة في مجال توعية المجتمع بموضوعات حماية الأطفال عند النفاذ [147].



الشكل 4.11: الموقع الرئيسي لمنظمة سيبرسيف (www.cybersafe.my)

7.11 القوانين والتشريعات

منذ العام 1997م أصدرت الحكومة الماليزية عدداً من القوانين المتعلقة بالإشكالات في الفضاء الإلكتروني والمعلوماتية وذلك لتوفير إطار قانوني شامل لكل الموضوعات الخاصة بالمنازعات في مجال الاتصالات وأمن المعلومات وذلك بغرض زيادة الموثوقية لدى المستخدمين في القطاعين العام والخاص على حدٍ سواء. من أهم القوانين التي تم إصدارها:

1. قانون جرائم الحاسوب والمصادقة الإلكترونية لسنة 1997م: يُعرّف هذا القانون الإطار العام للجريمة الإلكترونية من حيث الشكل والدوافع والإدانة القانوينة التي يمكن أن تترتب عليها، والعقوبات الجزائية التي يمكن تقريرها [148].
2. قانون الاتصالات والوسائط المتعددة لسنة 1998م: يُعنى هذا القانون بتنظيم عمل الاتصالات وصناعات الوسائط المتعددة حيث يعطي هذا القانون هيئة الاتصالات والوسائط المتعددة السلطة التنفيذية لإدارة وتنظيم عمل شركات الاتصالات والوسائط المتعددة بما يحقق منفعة المستخدم والمصالح العليا للبلاد [149].
3. قانون التجارة الإستراتيجية لسنة 2010م: يُعنى هذا القانون بتنظيم عمليات التصدير والتحكم في العبور للمواد الضار والتي يمكن أن تستخدم في صناعة أسلحة الدمار الشامل [150].
4. قانون الخدمات البريدية لسنة2012م: ينظم هذا القانون عمل الخدمات البريدية [151].

8.11 بعض المواقع المهمة

الجدول 2.11: المواقع المهمة والمتخصصة في مجال أمن المعلومات والاتصالات

اسم المؤسسة	عنوان الموقع	المهام الرئيسية
موقع أمن معلومات ماليزيا	www.cybersecurity.my	هيئة استشارية تتبع لوزارة العلوم والتكنولوجيا والابتكار تقدم مجموعة من الخدمات التقنية في

		مجال أمن المعلومات
موقع فريق الحاسوب الماليزى للإستجابة والطوارئ	www.mycert.org.my	الاستجابة السريعة لحالات الاختراق والتهديد المعلوماتي
موقع Cyber Guru	www.cyberguru.my	مركز قومي للتدريب المهني في مجال أمن المعلومات.
موقع المؤتمر السنوي لأمن المعلومات في ماليزيا	www.csm-ace.my	عبارة عن تجمع سنوي لمناقشة قضايا أمن المعلومات في ماليزيا
موقع لجنة الترخيص والموثوقية	mytrustmark.cyber-security.my	لجنة حكومية تقوم بعملية الترخيص والتوثيق للمواقع التجارية والتجارة الإلكترونية
موقع لجنة حماية البنيات الأساسية للمعلومات والاتصالات	cnii.cybersecurity.my/main/about	تطبيق السياسات والموجهات في مجال أمن المعلومات
موقع سيبرسيف	www.cybersafe.my	يُقدم الموقع مجموعة من الإرشادات للآباء والمدرسين في مجال التعاملات الإلكترونية
موقع هيئة الاتصالات الماليزية	www.skmm.gov.my	إدارة وتنظيم قطاع الاتصالات في ماليزيا

الفصل الثاني عشر
التجربة الأمريكية

1.12 الخطة الوطنية والاتجاهات المستقبلية لبناء صناعة المعلوماتية

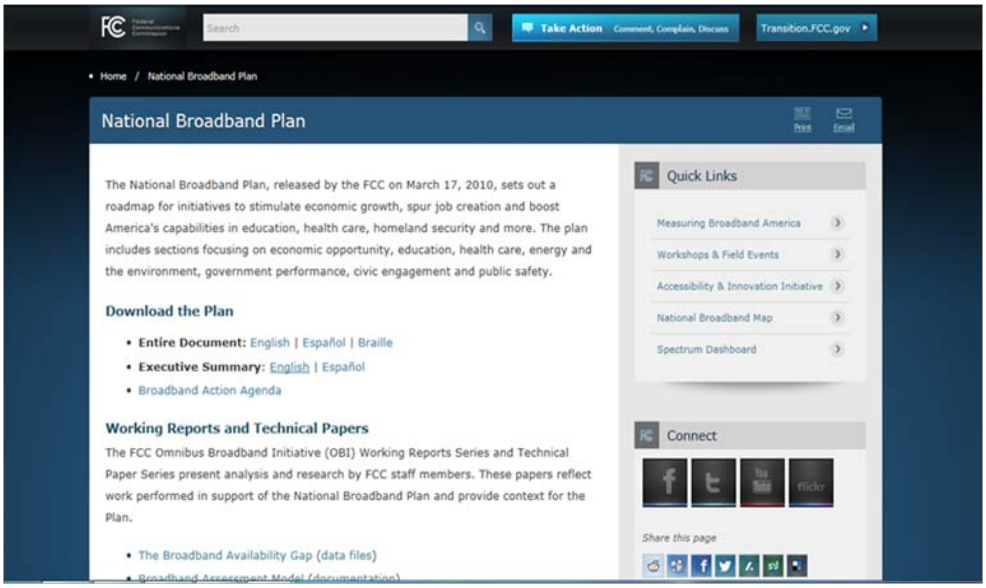
الولايات المتحدة هي الدولة الأولى والرائدة في مجال صناعة الابتكار في مجالات المعلوماتية والاتصالات في العالم. فهي الدولة التي بدأت عندها ثورة الإنترنت، والتي بدورها تعتبر الأساس لعملية التقدم في المعلوماتية في نهاية القرن العشرين وبداية القرن الحادي والعشرين. على الرغم من المسافة الشاسعة للتقدم التي تفصل الولايات المتحدة مع بقية البلدان المتقدمة في مجال المعلوماتية والاتصالات، إلا أن هنالك دائماً إصراراً من الإدارات الأمريكية المتعاقبة على تخصيص جزء كبير من الميزانية للبحوث والدراسات في هذه المجالات، وذلك للمحافظة على المكانة المتقدمة للدولة في قيادة عملية التميز والابتكار.

في العام 2010م، وضمن إستراتيجية الدولة للعام 2020م، وتنفيذاً لقانون الإنعاش الاقتصادي للعام 2009م American Recovery and Reinvestment Act؛ قامت الدولة بإعلان ما يُعرف بالخطة الوطنية للنطاق العريض National Broadband Plan والتي تهدف إلى الآتي:

1. ربط عدد 100 مليون منزل في الولايات المتحدة بسعة عرض نطاق تعادل 100 ميغا بت في الثانية بحلول العام 2020م.
2. يجب أن تتفوّق وتتقدم الولايات المتحدة في مجال صناعة وبناء شبكات الهاتف السيار على كل الدول في العالم.
3. يجب توفير سعة النطاق العريض لكل مواطن أمريكي.
4. كل التجمعات من (مدارس، ومستشفيات، ومبانٍ حكومية)، يجب أن توصل بسعة 1 قيقا بت في الثانية على الأقل.

5. استخدام التكنولوجيا اللاسلكية في عملية السلامة Every first responder interoperable، wireless،should have access to a nationwide broadband public safety network.
6. استخدام شبكات السعات العريضة في إدارة نظم الطاقة Every American should be able to use broadband to track and manage their real-time energy consumption.

تقوم الهيئة الفدرالية لتنظيم الاتصالات بالإشراف على تنفيذ هذه الخطة من خلال عملية مراقبة الإحصائيات والمؤشرات العامة. الشكل1.12 يوضع الموقع الرئيسي الذي يشرح مسار تنفيذ هذه الخطة: المصدر (www.Broadband.gov) .



الشكل 1.12:الموقع الرئيسي الذي يشرح مسار تنفيذ الخطة الوطنية للنطاق العريض في الولايات المتحدة (المصدر: www.Broadband.gov)

2.12 القطاعات والمصالح الإستراتيجية

في الولايات المتحدة تم تعريف البنيات الأساسية الحرجة بواسطة وزارة الأمن الداخلي Homeland Security على أنها تلك الأصول والبنيات والنظم التي تعتمد عليها الأمة في كثير من جوانب الحياة، وإذا تعطلت هذه الأصول فسوف يتعرض كلٌّ

من الاقتصاد والأمن القومي الأمريكي للخطر [152]. بناءً على هذا التعريف تم اعتماد القطاعات الإستراتيجية الآتية على أنها بنيات أساسية حرجة تجب حمايتها:

1. تقانة المعلومات Information Technology.
2. الاتصالات Telecommunications
3. قطاع الكيمياء Chemical Sector.
4. الأصول التجارية Commercial Facilities.
5. السدود Dams.
6. المفاعلات النووية التجارية والموادCommercial Nuclear Reactors، and Waste،Materials
7. المقار الحكومية Government Facilities.
8. نظم المواصلات Transportation Systems.
9. خدمات الطوارئ Emergency Services.
10. خدمات البريد والشحن Postal and Shipping Services.
11. الزراعة والأغذية Agriculture and Food.
12. الصحة العامة والعناية Public Health and Healthcare.
13. الطاقة Energy.
14. البنوك والمالية Banking and Finance.
15. الصناعات الدفاعية Defense Industrial Base.
16. الصناعات الإستراتيجية Critical Manufacturing.

3.12 المبادرات في الماضي والحاضر

بدأ الاهتمام في الولايات المتحدة بموضوع حماية المعلومات والبنيات التحتية للمعلوماتية والاتصالات منذ عام 1990م، وذلك نسبةً لاتجاه الكثير من جوانب الحياة الاجتماعية والاقتصادية للاعتماد بصورة مباشرة وأساسية على الإنترنت. في

الولايات المتحدة الأمريكية أيّ هجوم معلوماتي شامل، يمكن أن يؤثر تأثيراً كبيراً على الاقتصاد والأمن القومي للبلاد والعالم أجمع. نسبةً لهذه الحساسية، فقد قدمت الحكومة الاتحادية عدداً من المبادرات، واتخذت مجموعة من التدابير الوقائية لحماية البنيات التحتية الحرجة للمعلوماتية والاتصالات. هذه المبادرات والتدابير يمكن تلخيصها فيما يلي:

1. إنشاء اللجنة الرئاسية لحماية البنيات التحتية الحرجة Presidential Commission on Critical Infrastructure Protection (PCCIP) في سنة 1997م بواسطة الرئيس بيل كلنتون والتي تضم أعضاء من كل المؤسسات الحكومية والخاصة [153].
2. القرارات والتوجيهات الرئاسية رقم 62 (بخصوص محاربة الإرهاب) و63 (بخصوص حماية البنيات التحتية الحرجة) للعام 1998م لتطوير خطط تأمين البنيات التحتية القومية الحرجة [154].
3. الخطة القومية لأمن وحماية المعلومات للعام 2000م National Plan for Information Systems Protection.[155]
4. القرار الرئاسي القاضي بإنشاء إدارة الأمن الداخلي لسنة 2003م Homeland Security Executive Orders.[156]
5. القرار الرئاسي القاضي بإسناد مهمة حماية البنيات التحتية لإدارة الأمن الداخلي Homeland Security Presidential Directive / HSPD-7 للعام 2003 [157]م.
6. الإستراتيجية القومية للأمن الداخلي لسنة 2002م، والتي تهدف في المقام الأول إلى الحماية من الأخطار المتصلة بالإرهاب.
7. الإستراتيجية القومية لحماية الفضاء الإلكتروني National Strategy to Secure Cyberspace [158] والتي تهدف في المقام الأول إلى الآتي:
    - منع الهجمات الإلكترونية على البنيات الأساسية الأمريكية.
    - زيادة المناعة الوطنية ضد الهجمات والتخريب المعلوماتي.

- تقليل الأضرار وزمن إعادة الخدمة في حالة التعرض لبعض الهجمات.

8. الإستراتيجية القومية لحماية الأصول والبنيات التحتية الحرجة للمعلوماتية The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets [159].
9. الإستراتيجية القومية لتبادل المعلومات National Strategy for Information-Sharing [160]. نسبة للكثير من المشكلات التي واجهت هذه الإستراتيجية وظهور الكثير من الوثائق الرسمية والمراسلات على الإنترنت أو ما عرف بظاهرة ويكيليكس (Wikileaks)، تم تحديث الكثير من أهداف هذه الإستراتيجة في النسخة الجديدة التي تم إصدارها في العام 2012م [161].
10. إستراتيجية وزارة الدفاع للعمل في الفضاء المعلوماتي Department of Defense Strategy for Operating in Cyberspace [162]: تم إعلان هذه الإستراتيجية في العام 2011م وتهدف إلى الآتي:
    - التأكيد على أهمية استخدام وسائل الدفاع في مجال المعلوماتية.
    - الحث على استحداث وسائل جديدة للدفاع.
    - العمل على التعاون مع القطاعات الأخرى في هذا المجال.
    - بناء علاقات تعاون مع الدول الحليفة في هذا الجانب.
    - دعم الابتكار في هذا المجال.
11. الإستراتيجية القومية لمحاربة الجرائم العابرة Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security [163]: تم إعلان هذه الإستراتيجية في العام 2011م، وتهدف في المقام الأول إلى تعزيز محاربة الجرائم العابرة، والتي من ضمنها الجرائم المتصلة بالمعلوماتية.

12. الإستراتيجية العالمية للفضاء المعلوماتي International Strategy for Cyberspace: Prosperity، Security، and Openness in a Networked World: تم إعلان هذه الإستراتيجية في العام 2011م. [164, 165]. في هذه الإستراتيجية تم تحديد الدور الذي يمكن أو يجب أن تلعبه الولايات المتحدة على الصعيد الدولي في مجال أمن المعلومات والتحقيق في الجرائم الإلكترونية.
13. الإستراتيجية القومية لتعريف الوحدات والأجهزة في الفضاء المعلوماتي National Strategy for Trusted Identities in Cyberspace: تم إعلان هذه الإستراتيجية في العام 2011م بغرض زيادة الأمن المعلوماتي في مجال التجارة الإلكترونية [166].

4.12 نبذة عن المنظمات والمؤسسات القائمةعلى حماية المعلوماتية

في بداية الأمر أسندت الحكومة الأمريكية مهمة حماية المعلومات وبنيات الاتصالات الحرجة إلى مكتب إداري بوزارة التجارة عرف وقتها بمكتب حماية البنيات التحتية الحرجة للمعلوماتية Critical Infrastructure Assurance Office (CIAO). يعمل هذا المكتب بالتنسيق مع وحدة التحقيق الفدرالية Federal Bureau of Investigation (FBI) على التحقيق في جميع الجرائم المتصلة بالمعلوماتية. مع تطور التكنولوجيا وظهور مجموعة جديد من التهديدات أنشأت الحكومة وزارة للأمن الداخلي Department of Homeland Security (DHS) وأُسند إليها دور قيادة جميع الجهود والمبادرات المتصلة بحماية المعلوماتية وتنسيقها مع المنظمات الآتية:

1. مكتب حماية البنيات التحتية National Office of Infrastructure Protection (OIP): يقوم هذا المكتب بتنسيق الجهود في مجال حماية البنيات التحتية بين القطاعات المختلفة ويقدم الخدمات الآتية:
    - قيادة عمليات حماية البنيات التحتية.

- تطوير الخطة القومية لأمن البنيات التحتية الحرجة للمعلوماتية.
- تقييم وإدارة المخاطر.
- الإشراف على عملية تبادل الخبرات بين القطاعات المختلفة.
- جمع وتحليل المعلومات بشأن المخاطر المحتملة وتقديم النصح للحكومة الفيدرالية والقطاع الخاص.
- خلق علاقات دولية في هذا الشأن.

2. مكتب أمن المعلومات والاتصالات Office for Cyber-security and Communications (CS&C): يقوم هذا المكتب بالتنسيق بين القطاعات المختلفة بشأن عملية إدارة المخاطر المعلوماتية وإعداد الخطط بغرض التعامل مع الكوارث المتعلقة بنظم الاتصالات في حالة تعرض بنية شبكات الاتصالات للتدمير. من أهم موجهات هذا المكتب [167]:

- شبكة الاتصالات الوطنية يجب أن تقدم خدمة الاتصالات في حالة الطوارئ للحكومة الفدرالية (تحت كل الظروف).
- قسم أمن البيانات القومي يجب أن يعمل مع جميع الشركاء على المستوى الحكومي والقطاع الخاص والعالمي من أجل أمن البنيات التحتية وإدارة المخاطر.
- مكتب اتصالات الطوارئ Office of Emergency Communications (OEC) يجب أن يعمل على تطوير نظام يمكن أن يعمل في حالات الطوارئ لتقديم الخدمة لكل المستويات الإدارية في الحكومة الاتحادية.

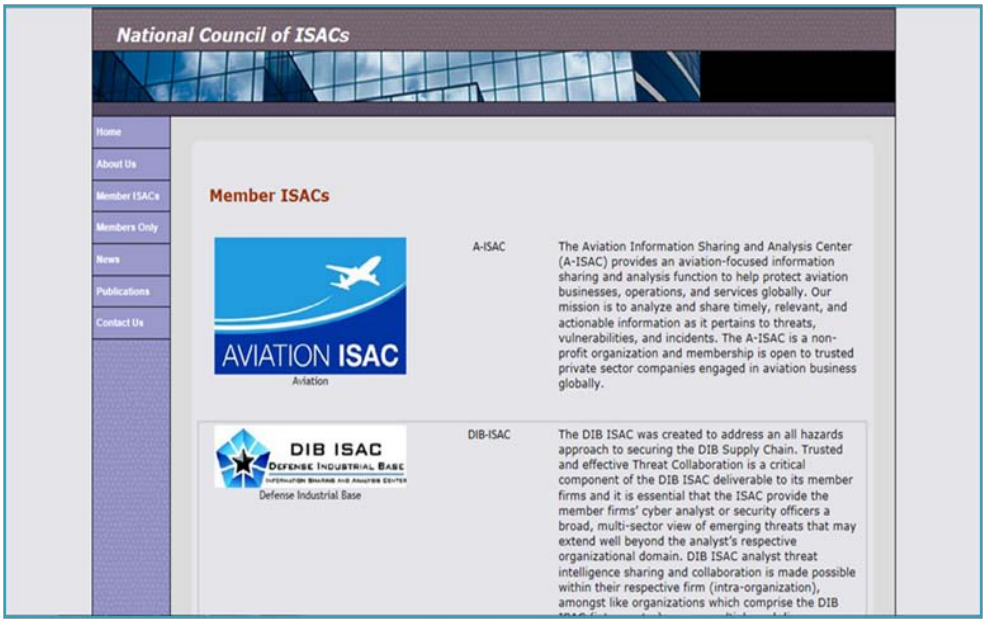
3. وزارة الخارجية US Department of State: تقوم وزارة الخارجية بالتنسيق مع وزارة الدفاع بتطوير ودعم المبادرات المتصلة بأمن المعلومات

والعمل مع جميع الشركاء (الحلفاء) من أجل تقليل المخاطر والهجمات الإلكترونية.

4. لجنة البرلمان الأمريكي للمعلوماتية Congressional Focus وهي لجنة مصغرة منبثقة من لجنة الأمن الداخلي وتهتم بالمسائل الآتية:
   - أمن الاتصالات والبنيات التحتية.
   - دعم البحوث في مجال أمن المعلومات والمخاطر.
   - التحقق من جاهزية نظم الاتصالات للعمل في حالة الطوارئ.
   - دعم أجهزة المخابرات وتشجيع تبادل الخبرات وتقييم المخاطر.

5. مكتب مراقبة الأداء الحكومي Government Accountability Office (GAO): يقوم هذا المكتب بإصدار تقارير لتقييم الموقف والحالات المتصلة بأمن المعلومات بصورة دورية.
6. مكتب الأمن الاجتماعي Defense Community: ويقوم بوضع السياسات المتصلة بأمن المعلومات في مجال الصناعات الإستراتيجية والحربية والدفاعية.
7. قسم جرائم الحاسوب والملكية الفكرية Computer Crime and Intellectual Property Section: يتبع هذا القسم لوزارة العدل ويقوم بإعداد الإستراتيجيات في مجال جرائم الحاسوب والملكية الفكرية.
8. برنامج حماية البنيات الأساسية الحرجة للمعلوماتية Protected Critical Infrastructure Information Program (PCIIP): يقوم هذا البرنامج بتنسيق عملية تبادل المعلومات بشأن المخاطر في القطاع الخاص.
9. مراكز تبادل الخبرات بين الأعضاء بشأن المخاطر Information Sharing and Analysis Centers (ISACs):

(http://www.isaccouncil.org/memberisacs.html) وهي مراكز تضم في عضويتها العديد من القطاعات الحكومية والخاصة: مثلاً المركز المخصص لشركات المعلوماتية يضم كلاً من Microsoft، Intel، CA ، Symantec، CSC، IBM، Oracle، Ebay، EWA-IIT، Harris ، Hewlett Packard، BAE Systems، IT، and VeriSign، Inc.: يقوم هذه المركز بتجميع المعلومات عن المخاطر المُستجدة في قطاع المعلوماتية وطرق التصدي لها ومشاركتها مع الأعضاء. هنالك مراكز لمشاركة المعلومات تضم قطاعات أخرى مثل قطاعات البنوك، قطاعات صناعات الكهرباء، قطاعات الاتصالات، قطاعات الطاقة، قطاعات التكنولوجيا النووية، قطاعات الصحة، قطاعات المال والأعمال، القطاعات البحرية، وقطاعات خدمات الطوارئ. تقوم كل هذه المراكز بنفس العمل كل مركز في مجاله. الشكل 2.12 يوضح النافذة الرئيسية لموقع المركز القومى لإدارة هذه الشبكة من المراكز.



الشكل 12.2: الموقع الرئيسي لإدارة شبكة مراكز تبادل الخبرات بين الأعضاء بشأن المخاطر. (http://www.isaccouncil.org/memberisacs.html)

10. مكتب InfraGard وهو عبارة عن مجموعة شراكة بين القطاع الخاص وFBI لدعم البحوث والدراسات ورعاية المبادرات الخاصة بأمن المعلومات وحماية البنيات التحتية الحرجة [168].

11. مكتب الحلفاء الوطنيين من أجل أمن المعلومات National Cyber Security Alliance (NCSA) وهو عبارة عن مجموعة شراكة بين الحكومة وقطاع صناعة المعلوماتية في الولايات المتحدة. يعمل هذا المكتب على زيادة الوعي بموضوع أمن البنيات التحتية من خلال الموقع (www.staysafeonline.org). الشكل 3.12.

الشكل 3.12: الموقع الرئيسي لمكتب الحلفاء الوطنيين من أجل أمن المعلومات National (www.staysafeonline.org) Cyber Security Alliance (NCSA)

5.12 الوعي العام والإنذار المبكر

أهم المؤسسات التي تقوم بواجب نشر الوعي العام والإنذار المبكر هي:

1. مركز تنسيق أمن المعلومات بجامعة جورج ميلان CERT Coordination Center، Carnegie Mellon (http://www.cert.org/): وهو عبارة عن مركز مدعوم من الحكومة الفدرالية لتطوير البحوث في مجال أمن المعلومات والاتصالات. تم إنشاء هذا المركز في 1988م بعد حادث Morris worm الذي عطل شبكة الإنترنت بنسبة 10%. يقوم هذا المركز بنشر تقارير دورية للجمهور عن حالات الاختراق وطرق التصدي لها.

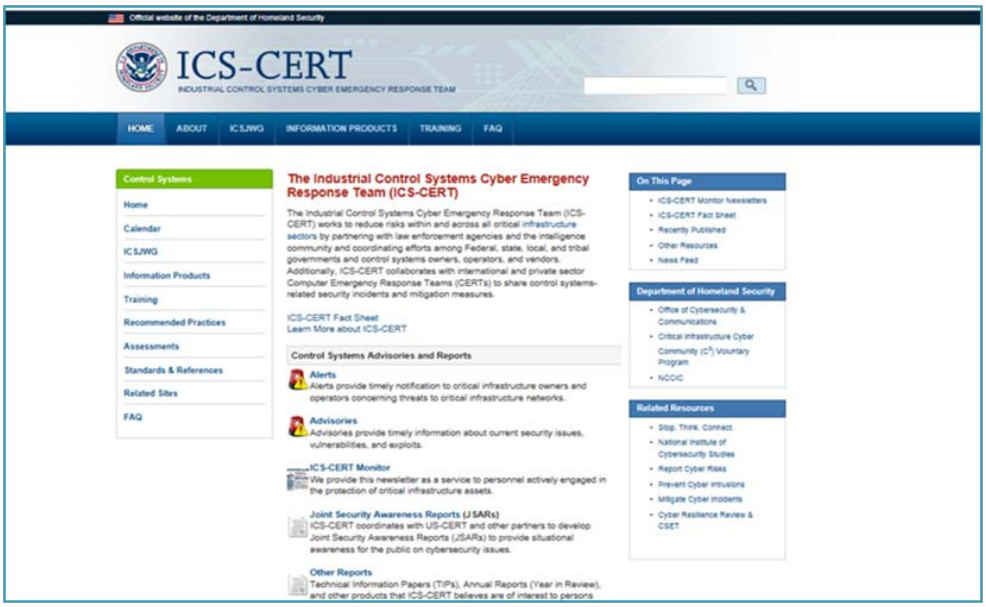
2. فريق الحاسوب للطوارئ والاستجابة الأمريكية US Computer Emergency Response Team (US-CERT): يتبع لجامعة جورج ميلان ومهمته منع الهجمات الإلكترونية وتقديم المساعدة والاستجابة السريعة في حالة تعرض أيٍّ قطاع لهجوم معلوماتي.

الشكل 4.12: الموقع الرئيسي لفريق الحاسوب للطوارئ والاستجابة الأمريكي

(المصدر: www.us-cert.gov)

3. وكالة التحقيق الفدرالية FBI: استناداً إلى سلطة القانون يقوم المكتب بعمل الاحتياطات الخاصة بحماية المعلوماتية والتحقيق في الجرائم المتصلة بالمعلوماتية والبنيات التحتية الحرجة والاتصالات.
4. موقع OnGuardOnline.gov (www.onguardonline.gov/) وهو موقع مدعوم من مراكز البحوث الحكومة وكبريات شركات التكنولوجيا يقدم نصائح ومواد تعليمية قيمة تُساعد المستخدم في حماية بياناتة الشخصية في عالم الإنترنت. الشكل 5.12 يوضح الصفحة الرئيسية للموقع.
5. فريق الحاسوب للطوارئ والاستجابة بخصوص قضايا أمن المعلومات في القطاع الصناعي Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). (http://ics-cert.us-cert.gov/). هذا الفريق متخصص في قضايا أمن المعلومات الصناعية، إذ يقوم بتقديم المشورة والدعم التقني ورفع الوعي العام في هذا الخصوص. الشكل 6.12 يوضح الصفحة الرئيسية للموقع.

الشكل 5.12: يوضح الصفحة الرئيسية لموقع الحماية عند النفاذ (www.onguardonline.gov/)



الشكل 6.12 يوضح الصفحة الرئيسية لموقع الاستجابة للطوارئ المتصلة بالقطاع الصناعي (http://ics-cert.us-cert.gov/)

6. مركز وزارة الدفاع لجرائم المعلوماتية Defense Cyber Crime Center (DC3) (http://www.dtic.mil) الشكل 7.12: يحتوي المركز على ثلاثة معامل كبرى تقوم بالوظائف الآتية:

- معمل التحقيق في جرائم المعلوماتية Defense Computer Forensics Laboratory (DCFL). يقوم هذا المعمل بالتحقيق في جميع الجرائم بالمتصلة بالمعلوماتية.
- معمل التدريب على التحقيق في الجرائم الإلكترونية Defense Cyber Investigations Training Academy (DCITA).
- مؤسسة أمن المعلوماتية Defense Cyber Crime Institute (DCCI). ينحصر دور هذه المؤسسة في البحث العلمي والابتكار.

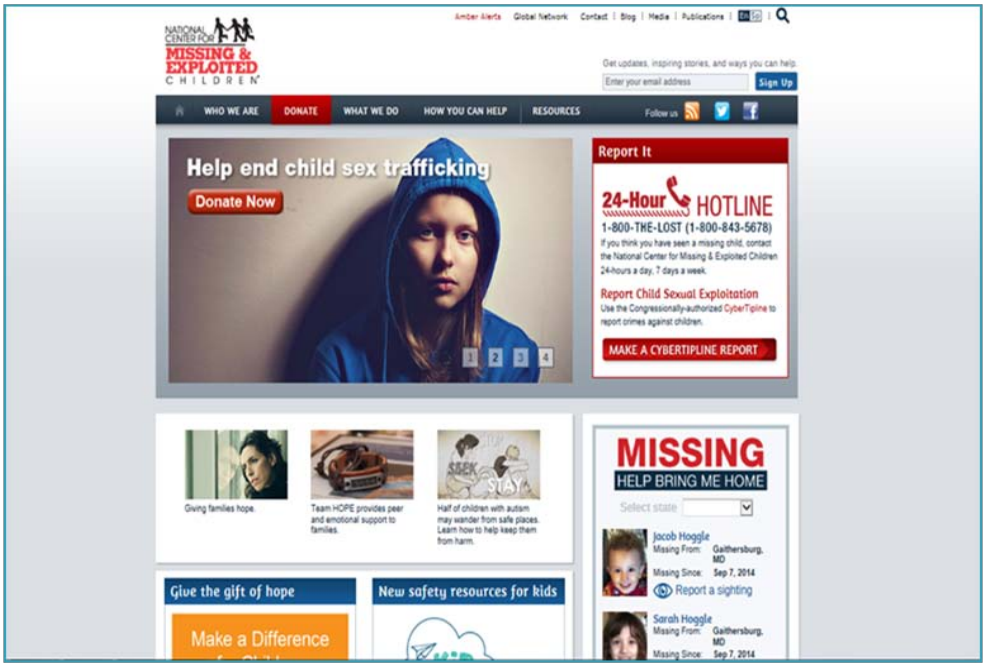
الشكل 7.12: مركز وزارة الدفاع لجرائم المعلوماتية (المصدر:www.dtic.mil)

6.12 حماية الأطفال عند النفاذ

أدركت الحكومة الأمريكية ومن وقت مبكر الأخطار التي يمكن أن يتعرض لها الأطفال عند النفاذ على الإنترنت حيث قامت بتشريع عدد من القوانين في هذا المجال نذكر منها ما يلي:

1. قانون حماية خصوصية الطفل لسنة 1998م Children's Online Privacy Protection Act والذي يلزم المواقع الإلكترونية في الولايات المتحدة بالعديد من الالتزامات تجاه عملية حفظ المعلومات الخاصة بالأطفال [169].
2. قانون حماية الأطفال على الإنترنت لسنة 2000م Children's Internet Protection Act: يلزم هذا القانون المدارس والمكتبات العامة بتطبيق عدد من الوسائل التقنية على شبكة الإنترنت وذلك للتحكم في المواد التي يمكن أن يطلع عليها الأطفال [170].
3. قانون حماية الأطفال للقرن الحادي والعشرين 2007م: يعتبر هذا القانون جزءاً مكملاً لقانون حماية الأطفال عند النفاذ على الإنترنت لسنة 2000م إذ أنه يعطي صلاحيات أكبر لمؤسسات التربية والتعليم في عملية التوعية والتعليم والتحكم في عملية نفاذ الأطفال على الإنترنت. للاطلاع على هذا القانون يمكن الرجوع إلى الوثيقة في المرجع رقم [171, 172].

هنالك أيضاً العديد من المنظمات التي تقدم الكثير والمفيد من المواد التعليمية التي تساعد في التوعية بالمخاطر التي يمكن أن يتعرض لها الاطفال عند النفاذ على الإنترنت. من أهم هذه المؤسسات المركز القومي لحماية الأطفال من الاستغلال National Center for missing and Exploited Children (http://www.missingkids.com/home) الشكل 8.12 يوضح الموقع الرئيسي لهذه المنظمة.



الشكل 8.12: الموقع الرئيسي لمركز حماية الاطفال من الاستغلال (المصدر: http://www.missingkids.com)

7.12 القوانين والتشريعات

منذ بداية عهد المعلوماتية بدأت الولايات المتحدة بإصدار القوانين التي تُنظم وتحفظ الحقوق ضمن مفاهيم الفضاء الإلكتروني. من أهم هذا القوانين:

1. قانون المستشارية الفيدرالية لسنة1972م Federal Advisory Committee Act (FACA) 1972 والذي يحدد ويحكم عملية تبادل المعلومات داخل القطاع الحكومي [173].
2. قانون س
3. سوء استخدام الحاسوب لسنة 1986م Computer Fraud and Abuse Act (CFAA) 1986: هذا القانون تمت مراجعته عدة مرات في فترات متقاربة (1994م و2001م) وذلك لإضافة فقرات لتشمل الأنواع المختلفة من جرائم الحاسوب والفيروسات وعمليات إرسال المحتويات الضارة [174].

4. التوجيه الرئاسي رقم 13010 لسنة 1996م والقاضي بإنشاء مفوضية حماية البنيات التحتية الحرجة [175].
5. قانون باترويت لسنة 2001م USA PATRIOT Act of 2001 والذي يعطي الحق لوكالة التحقيق الفدرالية في الوصول إلى بعض المعلومات الخاصة بالإرهابيين [176]. الجدير بالذكر أن الرئيس أوباما قام بالتمديد بالعمل بهذا القانون لأربع سنوات في 2011م [177].
6. التوجية الرئاسي رقم 13228 لسنة 2001م ;Executive Order 13228 EO 13228 والقاضي بإنشاء مكتب الأمن الداخلى ومجلس مكتب الأمن الداخلي [178].
7. التوجيه الرئاسي رقم 13231 لسنة 2001م Executive Order 13231 of October 16، 2001 والقاضي بحماية نظم المعلومات التي تعتمد عليها البنيات التحتية الحرجة [179].
8. قانون الأمن الداخلي Homeland Security Act 2002: يعطي هذا القانون الحق لوزارة الأمن الداخلي في الوصول إلى الكثير من البيانات الخاصة بالأفراد (في ظروف خاصة) وذلك من أجل حماية الأمة والبنيات التحتية الحرجة.
9. قانون حرية المعلومات :Freedom of Information Act (FOIA) يستثنى هذا القانون معلومات البنيات الأساسية الحرجة من عملية النشر أو إعطائها لأيّ جهة إلا بإذن [180].
10. قانون المخاطر على التأمين والإرهاب Terrorism Risk Insurance Act 2002. هذا القانون يحدد قيمة التعويض لشركات التأمين في حالة التعرض لهجوم إرهابي. تم تعديل هذا القانون في 2005م و2007م وتم التمديد للعمل به حتى العام 2014م [181]
11. قانون حماية الأطفال عند النفاذ للإنترنت للعام 2007م (Adam Walsh Child Protection and Safety Act)[182].

8.12 جدول لبعض المواقع المهمة

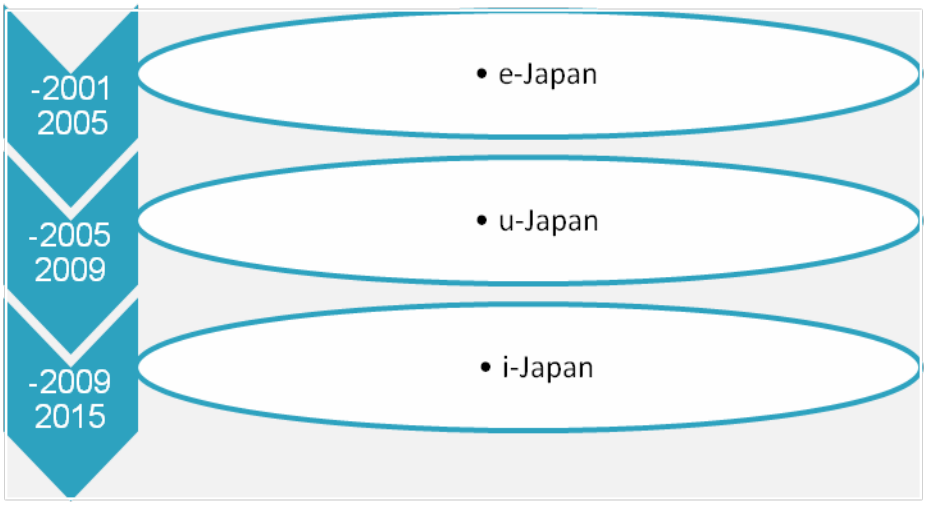
الجدول 1.12: المواقع المهتمة بالمعلوماتية في الولايات المتحدة.

اسم المؤسسة	عنوان الموقع	المهام الرئيسية
إدارة الأمن الداخلي Security Homeland	www.dhs.gov	تنسيق وإدارة حماية البنيات التحتية الأساسية للمعلوماتية والإتصالات في كل الولايات الأمريكية
مجموعة طوارئ الحاسوب والاستجابة الأمريكية US-cert	www.us-cert.gov	تقديم الدعم التقني عند الحاجة وتنسيق عملية تبادل الخبرات
مركز التنسيق بين مراكز الحاسوب للطوارئ CERT Coordination Center	www.cert.org	يقدم خدمات التنسيق بين بيوتات الخبرة وتطوير البرامج
منظمة onguardonline	www.onguardonline.gov	تقديم نصائح شاملة في مجال أمن المعلومات
وكالة التحقيقات الفيدرالية	www.fbi.gov	التحقيق في الجرائم المتصلة بالمعلوماتية وتقديم الدعم القانوني
الحلفاء الوطنيين من أجل أمن المعلوماتNational Cyber Security Alliance	www.staysafeonline.org	موقع تعليمي وإرشادي تدعمه شركات التقنية والمعلوماتية الكبرى في الولايات المتحدة
تجمع مراكز تبادل الخبرات بشأن المخاطر	www.isaccouncil.org	المساعدة في عملية تبادل الخبرات في مجال أمن المعلومات الخاصة بالأنشطة الاقتصادية المختلفة

الفصل الثالث عشر
تجربة اليابان

1.13 الخطة الوطنية والاتجاهات المستقبلية لبناء صناعة المعلوماتية

اليابان من الدول الأولى في العالم التي فطنت إلى مسألة بناء اقتصاد المعرفة ومجتمع المعلوماتية من وقت مبكر. في العام 2001م أعلنت الحكومة اليابانية عن برنامج E-Japan Strategy الذي يهدف في المقام الأول إلى تطوير وتحديث شبكات الاتصالات والاستفادة القصوى من إمكانيات تكنولوجيا المعلومات في عملية استدامة التطور والمحافظة على التفوق الاقتصادي [183]. بنهاية فترة برنامج E-Japan strategy وبتنفيذ جميع أهدافه الإستراتيجية؛ أعلنت الحكومة اليابانية عن مشروع U-Japan Strategy في العام 2005م والذي يهدف إلى العمل على استخدام تكنولوجيا الاتصالات والمعلومات في جميع جوانب الحياة اليومية للإنسان [184]. في العام 2009م تم الإعلان عن إستراتيجية i-Japan Strategy والتي تهدف إلى تطوير تطبيقات الحكومة الإلكترونية والاستفادة القصوى من تكنولوجيا الاتصالات والمعلومات في تطوير قطاع الصحة والموارد البشرية وتشجيع الابتكار [185].



2.13 القطاعات والمصالح الإستراتيجية

في اليابان تم تعريف البنيات الحرجة للمعلوماتية في قانون صدر العام 2005م. يُعّرف هذا القانون البنية الأساسية الحرجة على أنها الكيان التجاري أو المؤسسة الخدمة العامة التي لا يمكن الاستغناء عنها وتُشكل عاملاً ضرورياً في حياة السكان من ناحيةِ النشاط الاجتماعي والاقتصادي. في العام 2009م ومن خلال ما يعرف بالخطة الثانية لأمن المعلومات تم تحديد القطاعات الآتية على أنها قطاعات إستراتيجية [186].

1. الاتصالات Telecommunications
2. الخدمات الحكومية Government and Administrative Services
3. المالية Finance
4. الطيران المدني Civil Aviation
5. السكك الحديدية Railways
6. الخدمات اللوجستية
7. قطاع الكهرباء Electricity
8. الغاز Gas
9. الخدمات الطبية Medical Services
10. قطاع المياه Water

3.13 المبادرات في الماضي والحاضر

وضعت الحكومة اليابانية خطة عمل طموحة للترويج لفكرة مجتمع المعلوماتية والاتصالات المتطور في 1998م، بعد تنفيذ هذه الخطة تم إصدار خطة شاملة لأمن المعلومات في العام 2003م بواسطة وزارة الاقتصاد والتجارة والصناعة Ministry of Economy، Trade، and Industry (METI) . تعتبر هذه الخطة بمثابة الخطوة الثانية نحو إقامة مجتمع المعلوماتية. في سنة 2005م تم إصدار الإستراتيجية القومية لأمن المعلومات والتي تعتبر الأساس لكل المجهودات والأعمال الريادية:

الإستراتيجية الوطنية الأولى لأمن المعلومات

تهدف هذه الإستراتيجية إلى جعل اليابان مجتمعاً معلوماتياً متقدماً وتُؤسس أيضاً لشراكة فاعلة بين القطاع العام والخاص، فيما يتصل بأمن المعلومات وحماية البنيات التحتية الحرجة. أهم المهام التي تم تحديدها بواسطة الإستراتيجية:

- يجب وضع سياسة موحدة لأمن المعلومات ليتم تطبيقها على المؤسسات الحكومية المركزية والمحلية.
- إدارات البنيات الأساسية الحرجة يجب أن تضع في الاعتبار الاحتياطات اللازمة لاستمرار الخدمات تحت كل الظروف.
- الشركات العامة (القطاع الخاص) يجب أن تطبق مواصفات أمن المعلومات المطبقة في المؤسسات الحكومية.
- الحكومة يجب أن ترفع الوعي العام بموضوع أمن المعلومات من خلال التعليم والتدريب.

معايير قياس أمن المعلومات على مستوى الحكومة المركزية

أصدرت الحكومة معايير ومواصفات عامة لتقييم وقياس مستويات تطبيق سياسات ولوائح أمن المعلومات في القطاع الحكومي، حيث يتم دورياً تقييم نظم الحماية في المؤسسات وتقديم النصح اللازم بالإجراءات الإضافية التي يجب اتباعها.

4.13 نبذة عن المنظمات والمؤسسات القائمة على حماية المعلوماتية

في عام 2005م تم تكوين اثنين من المنظمات التي تتبع لأمانة مجلس الوزراء Cabinet Secretariat للقيام بدور أمن المعلومات والبنيات التحتية وهي:

1. المجلس الأعلى لسياسات أمن المعلومات The Information Security Policy Council (ISPC): تم إنشاء هذا المجلس في العام 2005م ليقوم بالمهام الآتية:
   - تطوير ومراجعة إستراتيجيات أمن المعلومات.
   - تقييم كفاءة نظم أمن المعلومات.

- تطوير موجهات السلامة العامة لنظم المعلومات.
- التوصية باستخدام نظم محددة.

2. المركز القومي للمعلومات National Information Security Centre (NISC): تم إنشاؤه أيضاً في 2005م ليقوم بالمهام الآتية [187]:
   - التخطيط وصياغة الإستراتيجيات الخاصة بالمعلوماتية للحكومة.
   - تعزيز أمن المعلومات في القطاع الحكومي.
   - مساعدة المؤسسات الحكومية في حالة تعرضها للاعتداء المعلوماتي.
   - تعزيز حمايتة البنيات التحتية والأصول المعلوماتية.
   - تعزيز ودعم عملية تبادل الخبرات.
   - الإسهام في تطوير الإستراتيجية الدولية لأمن المعلومات وخلق علاقات وصداقات دولية في هذا المجال.

أيضاً هنالك العديد من المؤسسات التي تساعد على حماية البنيات الحرجة منها:

3. وزارة الاقتصاد والتجارة والصناعة Ministry of Economy، Trade and Industry (METI): مهمتها تتنفيذ السياسات المتعلقة بأمن المعلومات والصادرة من رئاسة مجلس الوزراء، وذلك في المجالات المتصلة بالتجارة الإلكترونية e-Commerce والحكومة الإلكترونية e-Government وحماية البياناتData Protection، والبحوث والتطوير وتشجيع تطبيق السياسات الخاصة بأمن المعلومات في الشركات.
4. الشرطة الوطنية National Police Agency (NPA): تعمل الشرطة الوطنية من خلال مركز الجرائم المتطورة High-Tech Crime Technology Division (HTCTD) وشرطة المعلومات Cyber Forces. على محاصرة جرائم المعلوماتية ومراقبة أمن الإنترنت ووسائل الاتصالات على مدار الساعة. وتقوم أيضاً بجمع وتحليل الاختراقات وتعمل على تشجيع البحوث والتطوير والابتكار في هذا المجال.

5. وزارة الداخلية والاتصالات Ministry of Internal Affairs and Communications (MIC): تهتم بإنشاء البنيات التحتية للاتصالات والمعلومات.
6. مكتب تبادل الخبرات بين القطاعات الحكومية والقطاع الخاص CEPTOAR: مهمة المكتب تسهيل تبادل المعلومات المتعلقة بالاختراقات والجرائم الإلكترونية بين القطاع العام والخاص وتبادل الخبرات في هذا الشأن.
7. الجمعية اليابانية لأمن الشبكات Japan Network Security Association (JNSA): هي جمعية وطنية تم تكوينها في عام 2000م وتقوم بوضع المواصفات الخاصة بأمن الشبكات.

5.13 الوعي العام والإنذار المبكر

في اليابان تقوم المؤسسات الآتية بواجب الإنذار المبكر وزيادة الوعي العام:

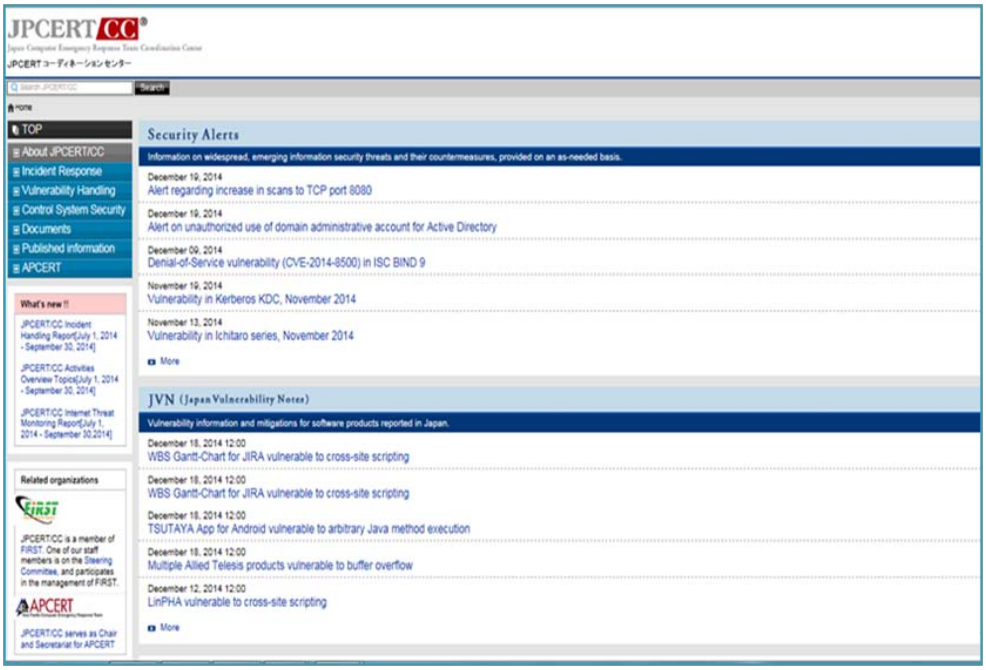
1. الفريق الوطني للاستجابة والطوارئ National Incident Response Team (NIRT).

تم إنشاء هذا الفريق في 2002م ويتبع لأمانة مجلس والوزراء ويضم مجموعة من الخبراء ليقوم بالمهام الآتية:

- فهم طبيعة الاختراقات الأمنية في مجال المعلومات وجمع البيانات عنها وتحليلها بغرض التنبؤ بما يحدث في المستقبل.
- تطوير موجهات عامة لتلافي الاختراق.
- يقوم بالمساعدة على الاستجابة السريعة.
- تطوير الخبرات في هذا المجال.

2. المركز الياباني لفريق طوارئ الحاسوب Japan Computer Emergency Response Team Coordination Center (JPCERT / CC) (http://www.jpcert.or.jp/english/)، الشكل 1.13. هذا المركز مستقل تم

إنشاؤه في سنة 1992م ليقوم بالتنسيق بين فرق الطوارئ المختلفة وشركات خدمات الاتصالات ومجموعات تطوير الحلول الأمنية والقطاع الحكومي. أيضا يقوم هذا المركز بالتنسيق مع المراكز الخارجية في هذا الخصوص.

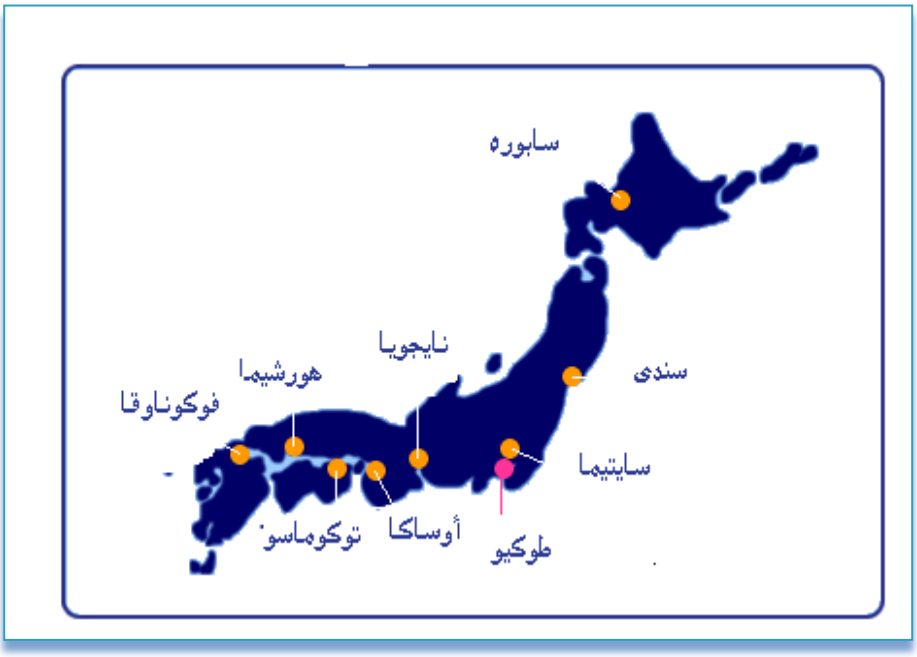


الشكل 1.13: المنفذ الرئيسي لموقع مركز الحاسوب للطوارئ والاستجابة الياباني (JPCERT / CC)

3. فريق الحاسوب لدول آسيا باسفك للاستجابة والطوارئ Asia Pacific Computer Incident (Emergency) Response Team (AP-CIRT/ APCERT): تم إنشاء هذا الفريق في 2003م ليقوم بالتنسيق بين فُرق الطوارئ والاستجابة للجرائم الإلكترونية في المنطقة. الشكل 2.13.

الشكل 2.13: الموقع الرئيسي لآسيا باسفيك سرت (AP-CIRT / APCERT) (http://www.apcert.org/)

4. مركز تحليل وتبادل معلومات الاتصالات Telecom Information Sharing and Analysis Center (www.telecom-isac.jp): وهو عبارة عن مركز لجمع المعلومات عن الحوادث الإلكترونية وتحليلها وتبادل الخبرات المستفادة منها. يضم المركز في عضويته كبريات شركات الاتصالات وصناعة المعلومات والأبحاث في اليابان.
5. قوات الدفاع المعلوماتي Cyber Force: تتبع هذا الفريق لجهاز الشرطة ويقوم بمراقبة الإنترنت على مدار الساعة. يقوم أيضاً هذا الفريق بدور الإنذار المبكر للجهات التي يمكن أن تتعرض لخطر أو أي هجوم إلكتروني ويعمل على إجراء الاختبارات الدورية للمؤسسات بغرض التعرف على مواضع الخلل فيها وتقديم النصح والإرشاد اللازم بذلك. الشكل 3.13 يوضح المواقع التي يعمل بها هذا الفريق (http://www.npa.go.jp).



الشكل 3.13: يوضح المواقع الجغرافية لمراكز القوة (الشرطة) المعلوماتية (Cyber Force) في اليابان: المصدر (http://www.npa.go.jp)

6. موقع الشرطة @police

تم إنشاء هذا الموقع بواسطة الشرطة الوطنية للتواصل المباشر بين الشرطة ومستخدمي الإنترنت حول ما يدور في العالم من اختراقات. أيضاً يقدم هذا الموقع مواد تعليمية للتوعية والتدريب واختبار مواضع الضعف.

6.13 حماية الأطفال عند النفاذ

اليابان من الدول الأولى في العالم التي اهتمت بموضوع حماية الأطفال عند النفاذ على الإنترنت حيث احتضنت أول حوار دولي إستراتيجي حول عملية حماية الأطفال في عام 2009م [188]. أهم مجهودات اليابان في هذا الخصوص يمكن تلخيصها في النقاط الآتية:

1. إصدار قانون سلامة استخدام الإنترنت لسنة 2008م (Act 79) [189] والذي يهدف إلى تحقيق كلٍّ من الآتي:
   - تعزيز محو الأمية في مجال استخدام الإنترنت للأطفال.
   - العمل على تقليل فرص الأطفال في التعرض للإحتيال أومشاهدة المواد الضارة على الإنترنت.
   - تشجيع المبادرات الخاصة بهذا المجال.
   - تشجيع وقياس فاعلية النظم المستخدمة في عملية الحجب.
   - تشجيع شركات تقديم خدمة الإنترنت ISPs ومراكز البحوث على ابتكار وتطبيق تقنيات متقدمة لحجب المواد الضارة بالأطفال.
2. مبادرة e-net Caravan (www.e-netcaravan.jp): قامت هذه المبادرة برعاية شركات الاتصالات الكبرى في اليابان، وكانت تستهدف كلاً من الآباء والمدارس والطلاب بالتوعية بالموضوعات الخاصة بالجرائم المعلوماتية الموجهة ضد الأطفال.
3. مبادرة هاتف خاص بالأطفال برعاية كل من شركة NTT docomo وSoftbank Mobile. تهدف المبادرة إلى تصنيع هواتف محدودة الإمكانيات للأطفال حيث يمكن التحكم في كثير من خصائصها بواسطة الآباء.
4. برنامج محو الأمية في مجال استخدام تكنولوجيا المعلومات للمدارس Improving ICT Literacy at School: وهو برنامج مدعوم من وزارات التعليم والرياضة والعلوم والتكنولوجيا ويهدف إلى تقديم المواد التعليمية المجانية بغرض رفع الوعي العام للأطفال.
5. إنشاء جمعية لمراقبة وتقييم محتويات الجوال Mobile Content Evaluation and Monitoring Association (http://www.ema.or.jp/en/index.html): تضم الجمعية في

عضويتها العديد من مؤسسات المجتمع المدني المهتمة بموضوع حماية الأطفال عند النفاذ [190].

6. إنشاء جمعية مراقبة الإنترنت Internet-Rating Observation (ROI) Institute: وهي منظمة مدنية معنية بتقييم محتويات الإنترنت وتصنيفها حسب الأعمار.
7. تكوين جمعية إنترنت آمنة لليابان Safer Internet of JAPAN في العام 2009م
8. الجمعية اليابانية لتعزيز سلامة الإنترنت Japan Internet Safety Promotion Association: هي جمعية تم إنشائها في 2009م وتعمل تحتها المجموعات البحثية الآتية [191]:

- فريق البحوث والدراسات والذي يركز على دراسة تاثير المواد الإباحية وغير القانونية على الأطفال في الجوانب الآتية:
  - العنف والبلطجة.
  - السلوك الجنسي.
  - الوعي الجنسي.
  - الانتحار.
- فرق محاربة المواد الإباحية للأطفال على الإنترنت Anti-Child-Pornography Working group: يعمل هذا الفريق على تبادل الخبرات مع الفرق الأخرى حول العالم بخصوص منع الإباحية.
- فريق المواقع الاجتماعية Community Site Working Group: يقوم هذا الفريق بدراسة تأثير مواقع التواصل الاجتماعي على الأطفال.
- فريق الهواتف الذكية Smartphone Working Group: يعمل الفريق على حماية الأطفال من خطر استخدام الهواتف الذكية من خلال التعاون مع مشغلي شبكة الهاتف.

- فريق الألعاب في مواقع التواصل الاجتماعي Social Game Working Group: يعمل الفريق على البحث في القضايا والمشكلات المصاحبة لهذه الألعاب.

الشكل 4.13: يوضح المواقع الرئيسى ل E-net Caravan initiative (www.e-netcaravan.jp)

7.13 القوانين والتشريعات

1. قانون الوصول غير المصرح به لموارد الحاسوب السنة 1999م Unauthorized Computer Access Law 1999: يغطي هذا القانون كل الجوانب التي تخص الاعتداء على المعلومات أو إتلافها.
2. قانون المصادقة الإلكترونية لسنة 2000م Act on Electronic Signatures and Certification Business (2000). يغطي هذا القانون كل الأمور الخاصة بالمصادقة والعمليات الإلكترونية.

3. القانون الأساسي لمجتمع المعلومات والإتصالات لسنة2001م: هو القانون الذي ينظم إنشاء شبكات الاتصالات والمعلومات على نطاق الدولة ويشجع عمليات التجارة الإلكترونية e-Commerce والحكومة الإلكترونية e-Government (www.e-gov.go.jp). ويعمل على حماية البيانات الشخصية ونتائج البحوث والابتكار.
4. قانون حماية الأطفال والمعاقبة بخصوص الأنشطة المتعلقة باستغلال الأطفال في البغاء وفي المواد الإباحية للعام 1999م Act on Punishment of Activities Relating to Child Prostitution and Child Pornography، and the Protection of Children [192].

8.13 بعض من المواقع المهمة

الجدول 1.13: المواقع المهمة للجهات المهتمة بموضوع أمن المعلومات في اليابان.

اسم المؤسسة	عنوان الموقع	المهام الرئيسية
@police	www.npa.go.jp	جمع المعلومات فيما يخص الجرائم الإلكترونية وتقديم الإرشادات للمستخدمين وتطوير البحوث في هذا المجال.
إدارة الحكومة الالكترونية	www.e-gov.go.jp	موقع إخباري عن كل ما يدور في مجال الحكومة الإلكترونية.
المجلس الوطني لسياسات أمن المعلومات	www.nisc.go.jp	وضع السياسات والموجهات العامة ومتابعة التنفيذ.
المركز الوطني للاستجابة والطوارئ	www.jpcert.or.jp	الإستجابة للطوارئ و تقديم الدعم التقني المباشر في حالات الاختراق والهجوم الإلكتروني.

مركز المراقبة والطوارئ لمجموعة جنوب شرق أسيا	www.apcert.org	الاستجابة للطوارئ وتقديم الدعم الفني المباشر في حالات الاختراق والهجوم الإلكتروني.
الجمعية اليابانية لأمن الشبكات	www.jnsa.org/en/about us	وضع المواصفات الخاصة بأمن الشبكات والمعلومات
مركز تبادل المعلومات والخبرات الياباني	www.telecom-isac.jp	تبادل الخبرات بين القطاع العام والخاص في مجال أمن المعلومات.
موقع لتبادل الخبرات	http://blog.jpcert.or.jp/	تبادل الخبرات بين المختصين في مجال أمن المعلومات

الفصل الرابع عشر
التجربة البريطانية

1.14 الخطة الوطنية والاتجاهات المستقبلية لبناء صناعة المعلوماتية

بريطانيا من الدول السبّاقة والرائدة في العالم، في مجال تطوير وبناء نظم المعلومات والاتصالات، فهي أول من بدأ بسنّ القوانين المنظمة لقطاع الاتصالات في بداية القرن العشرين. مع زيادة سرعة نقل البيانات باستخدام الألياف الضوئية واعتماد العالم بصورة شبه كلية عليها. قامت بريطانيا بتوفير البنيات والمتطلبات الأساسية لبناء هذه الشبكات، وتعتبر اليوم نقطة الالتقاء المحورية الثانية لشبكة الإنترنت بعد الولايات المتحدة Focal point for the Most of the world Submarine Cables (انظر الشكل 1.2 في الفصل الأول من هذا الكتاب) حيث تلتقي عندها معظم الكيبلات البحرية للألياف الضوئية.

في العام 2009م أصدرت كل من وزارة الثقافة والإعلام والرياضة ووزارة التجارة والابتكار والمهارات Department for Culture، Media and Sport، Department for Innovation and Skills،and Business تقريراً شاملا بعنوان بريطانيا الرقمية Digital Britain لتحديد المتطلبات الأساسية التي يجب الإيفاء بها في مجالات المعلوماتية والاتصالات لتحقيق الرؤية المستقبلية لبريطانيا[193]Future Britain. اهتم التقرير بدراسة الوضع الحالي للمعلوماتية والاتصالات، وتحديد المتطلبات المستقبلية في ما يخص الموضوعات الآتية:

1. تحديث البنيات التحتية للاتصالات.
2. دعم الصناعات المعلوماتية.
3. تطوير الخدمات العامة بالاستفادة من المعلوماتية والاتصالات.
4. تطوير البحوث والدراسات والتعليم ورفع قدرات الموارد البشرية.
5. أمن المعلوماتية والاتصالات.
6. تطوير خدمات الحكومة الإلكترونية.

يعتبر التقرير وثيقة قيمة من حيث المحتوى، إذ أنه تضمن نقاطاً تفصيليةً عن ما يجب فعله فيما يخص الموضوعات أعلاه [193]. في نفس العام تم إعداد خطة تفصيلية على مستوى الدولة لتنفيذ مشروع بريطانيا الرقمية Digital Britain، واحتوت الخطة على واجبات وجداول زمنية محددة لتنفيذها بحلول العام 2015م.

2.14 القطاعات والمصالح الإستراتيجية

في المملكة المتحدة تم تعريف البنية التحتية الأساسية بأنها هي البنية الخدمة الأساسية التي إذا تعطلت يمكن أن تُسبب خسارة كبيرة في الاقتصاد أو الاستقرار الاجتماعي والبشري. بناءً على هذا التعريف تم اعتماد القطاعات الخدمية الآتية على أنها بنيات أساسية حرجة [194, 195]:

1. الاتصالات Communications (اتصالات البيانات، الاتصالات الصوتية، البريد الإلكتروني والاتصالات اللاسلكية)
2. خدمات الطوارئ Emergency Services
3. قطاعات الطاقة بكل أشكالها (Electricity، Energy، Natural Gas ، Petroleum)
4. المالية والتمويل والبنوك والتجارة (Finance، Asset Management، Financial Facilities، Investment Banking، Markets ، Retail Banking)
5. الغذاء والعمليات المُصاحبة للإنتاج الغذائي (Food، Produce، Import، Process، Distribute، Retail)
6. الحكومة والخدمات العامة Government and Public Services
7. الصحة العامة (Health Care، Health، Public Health)
8. المواصلات (Air Transport، Marine، Rail، Road)
9. المياه (Mains Water، Water، Sewerage).

3.14 المبادرات في الماضي والحاضر

ركزت حكومة المملكة المتحدة على حماية البنيات الأساسية للمعلوماتية من نوعين من المخاطر هما: الإعتداء على الأُصول الفيزيائية والهجوم أو الاعتداء المعلوماتي، لذلك قامت الحكومة بالمبادرات الآتية:

1. إستراتيجية أمن المعلومات الوطنية: تبنى مجلس الوزراء هذه الإستراتيجية في العام 2003م، حيث تم تكوين جسم مركزي برئاسة الحكومة لحماية المعلوماتية Central Sponsor for Information Assurance (CSIA) حيث يقوم بالمهام الآتية:

- تمكين الحكومة من تقديم الخدمات للجمهور باستخدام تكنولوجيا الاتصالات والمعلومات.
- تقوية الأمن القومي للمملكة المتحدة من خلال تقوية أمن المعلومات والاتصالات.
- تطويرالاقتصاد والرفاه الاجتماعي من خلال تمكين الجمهور من الاعتماد على شبكات الاتصالات والمعلومات.

2. مبادرة حماية المعلومات الحكومية Government Data Security: تم تقديم هذه المبادرة في 2007م وذلك نسبة للخروقات المتعددة للأنظمة الحكومية.

4.14 نبذة عن المنظمات والمؤسسات القائمة

في المملكة المتحدة تقع مسؤولية حماية المعلومات والبنيات الأساسية للاتصالات على عاتق منظمة الأمن الداخلي، لكن هنالك العديد من المنظمات التي تساعد في هذه العملية منها:

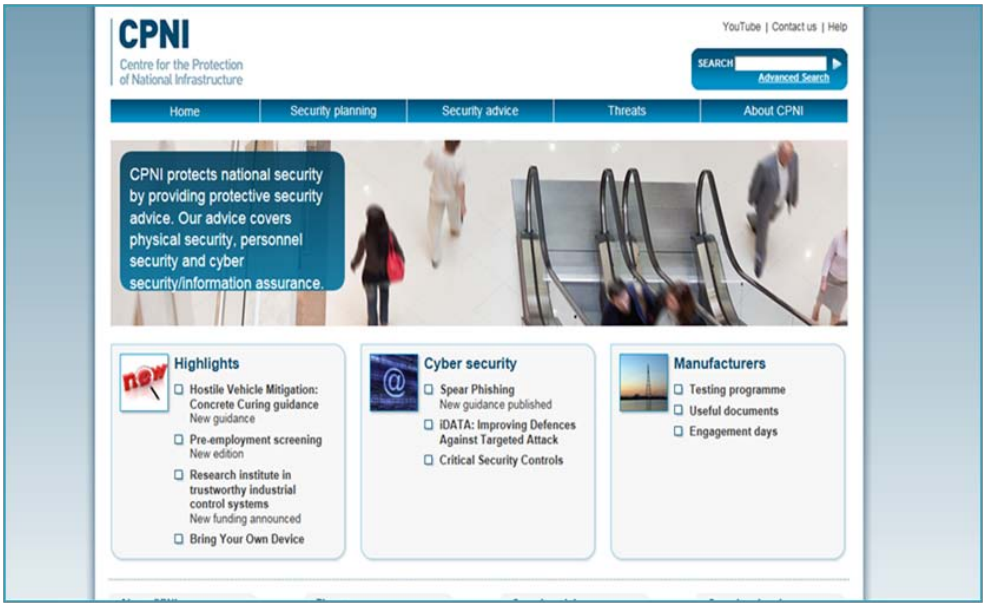
1. مركز حماية البنيات التحتية الوطنية Centre for the Protection of National Infrastructure (CPNI): تم إنشاء هذا المركز في العام 2007م ليقوم بحماية البنيات التحتية من الهجمات الإرهابية والإلكترونية

الشكل 1.14 يوضع الموقع الرئيسي. يقوم هذا المركز بدعم البحوث والدراسات العلمية وخلق علاقات مع المؤسسات العلمية والبحثية ذات العلاقة بموضوع أمن المعلومات ويقدم النصائح الدورية للمؤسسات الوطنية المعنية بتشغيل البنيات التحتية الحرجة في أحد الأشكال الآتية [194]:

- نصائح وجها لوجه يقدمها خبراء المركز للمؤسسات.
- التدريب الذي يقوم به المركز.
- معلومات على موقع المركز يمكن أن تستفيد منها المؤسسات.
- نصيحة مكتوبة في شكل تقرير يصدرة المركز.

أيضا بصورة عامة تقوم الوزارات والمؤسسات الآتية بتنفيذ ومتابعة توصيات المركز الوطني لأمن البنيات التحتية:

- مجلس الوزراء Cabinet Office.
- الحكومات المحلية ومنافذ الخدمات العامة.
- وزارة التجارة.
- وزارة البيئة والغذاء والتنمية الريفية Department for Environment، Food and Rural Affairs .
- وزارة المواصلات Department for Transport.
- وزارة الصحة Department of Health.
- إدارة مواصفات الأغذية Food Standards Agency.
- المالية Finance.
- خدمات الطوارئ Emergency Services.
- وكالة خدمات البحار والشواطئ Maritime and Coastguard Agency.
- الشرطة.



الشكل 1.14: الموقع الرئيسي لمركز حماية البنيات التحتية الوطنية.

2. مكتب Civil Contingencies Secretariat (CCS) وهو مكتب يخطط لدعم الحكومة في حالات الطوارئ ويقوم بمساعدة كل الوزارات في مجال إعداد الخُطط للتعامل حالات الكوارث.
3. هنالك أيضاً مجموعة من مؤسسات القطاع الخاص والتي تعمل جنباً إلى جنب مع مؤسسات القطاع الحكومي وتتبادل معها الخبرات في مجال أمن المعلومات. من هذه المؤسسات:

- المجلس الاستشاري لأمن المعلومات The Information Assurance Advisory Council.
- الجمعية البريطانية للحاسوب British Computer Society.
- المركز الوطني للحوسبة National Computing Centre.
- مؤسسة مراقبة الإنترنت Internet Watch Foundation
- نقابة الصناعة البريطانيةConfederation of British Industry (CBI)(www.cbi.org.uk).

- الجمعية المهنية لأمن المعلومات (http://www.iisp.org) Institute of Information Security Professionals(IISP): وهي عبارة عن جمعية مهنية تُعنى بالتدريب في مجالات أمن المعلومات وحماية البنيات التحتية الأساسية.
- الجمعية الأُوروبية للمعلومات European Information Society Group (EURIM) (also (http://www.eurim.org.uk/) Called The Information Society Alliance): تعمل هذه الجمعية مع المشرعين والمؤسسات الصناعية لتحديد تقنين العمليات أوالموضوعات الآتية:
    1. الخصوصية.
    2. حماية البيانات.
    3. المراقبة.
    4. المهارات وشبكات التعلم.
    5. العمل على أمن المعاملات الخاصة بالتجارة الإلكترونية.
    6. تحديد نقاط الضعف الاجتماعية والاقتصادية.
    7. حقوق الملكية الفكرية والتعامل العادل.
    8. التكافؤ بين الالتزامات القانونية على الإنترنت.

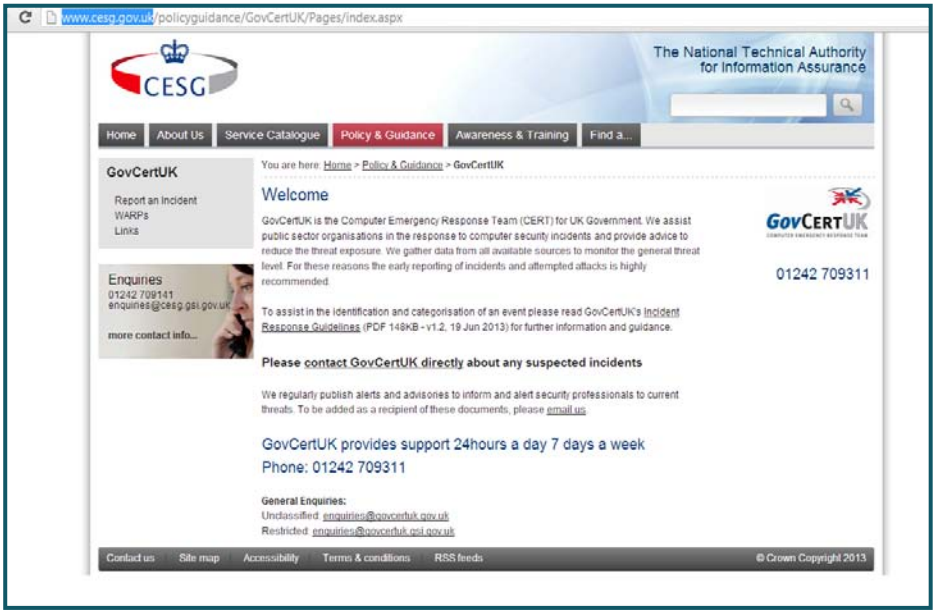
5.14 الإنذار المبكر والوعي العام

من أهم المنظمات التي تقوم بدور الإنذار المبكر وإشاعة الوعي العام في المملكة المتحدة هي:-

1. الفريق أو المجموعة المتحدة للأمن والاستجابة Combined Security Incident Response Team (CSIRTUK): وهي مجموعة تقوم

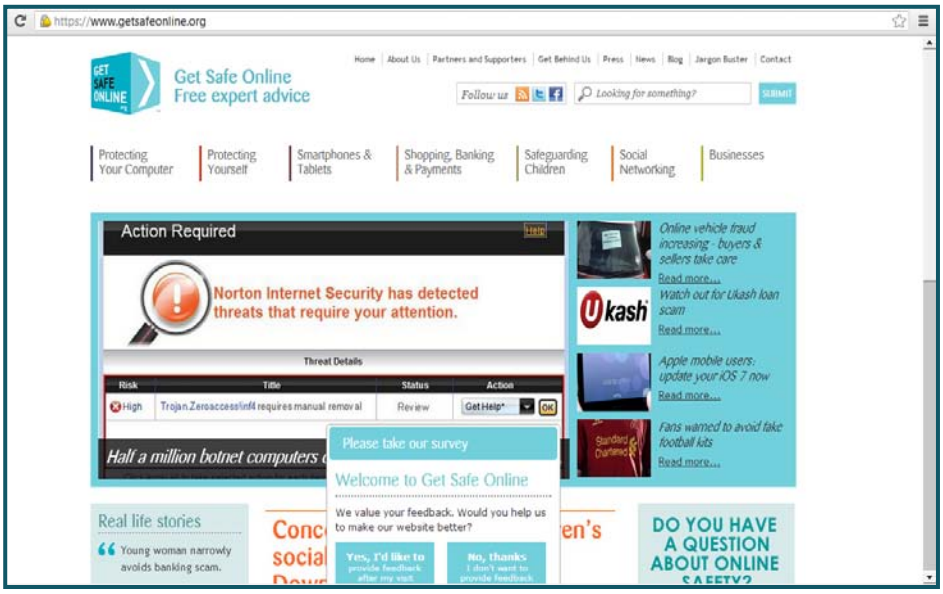
بمساعدة القطاع الخاص في مجالات أمن المعلومات وإدارة المخاطر والاستجابة للإختراقات الإلكترونية [196].

2. مجموعة GovCertUK (http://www.cesg.gov.uk) الشكل2.14: وهي مجموعة تقوم بمساعدة القطاع الحكومي في مجالات أمن المعلومات وإدارة المخاطر وتقديم الدعم التقني المباشر في الحالات الحرجة.
3. فريق وزارة الدفاع للاستجابة والطوارئ المعلوماتية Ministry of Defense Computer Emergency Response Team (MODCERT): هو عبارة عن فريق معلوماتي له عدة مراكز موزعة في مناطق مختلفة على طول البلاد. يقدم هذا الفريق النصح في الحالات الحرجة لمنظومات المعلومات ويعمل على تشجيع تبادل الخبرات بين المؤسسات وينسق بين كلٍّ من (CSIRTUK) وGovCertUK.



الشكل 2.14: الموقع الرئيسي للمجموعة المتحدة للأمن والاستجابة السريعة (http://www.cesg.gov.uk).

4. موقع GetSafeOnline الشكل 3.14: وهو موقع تعليمي يعمل على توعية المجتمع بموضوعات أمن المعلومات والاتصالات ويقدم النصائح العامة والتقنية حول الستخدام السليم للإنترنت.



الشكل 3.14: الموقع الرئيسي لمجموعة الوصول الآمن (GetSafeOnline) المصدر (https://www.getsafeonline.org/).

6.14 حماية الأطفال عند النفاذ

أنشأت الحكومة البريطانية مركز لحماية الأطفال عند النفاذ Child Exploitation and Online Protection Centre (CEOP) في أبريل 2006م وذلك لمقاومة الجرائم الخطيرة والمستحدثة ضد الأطفال. يعمل المركز على النطاق القومي والعالمي وبالتعاون مع مجموعة من المنظمات وبيوتات الخبرة المعلوماتية من أجل محاصرة الجريمة الإلكترونية (الجنسية). الشكل 4.14 يوضح الصفحة الرئيسية للمركز والتي يمكن التبليغ عبرها عن أي محتوى غير متوافق مع القانون ليتم بعد ذلك التعامل معه وبمساعدة الجهات القانونية الدولية إذا تطلب الأمر.

قام المركز بدعم برنامج تعليمي باسم ThinkUKnow (http://www.thinkuknow.co.uk/) الشكل 5.14 يوضح الموقع الرئيسي.

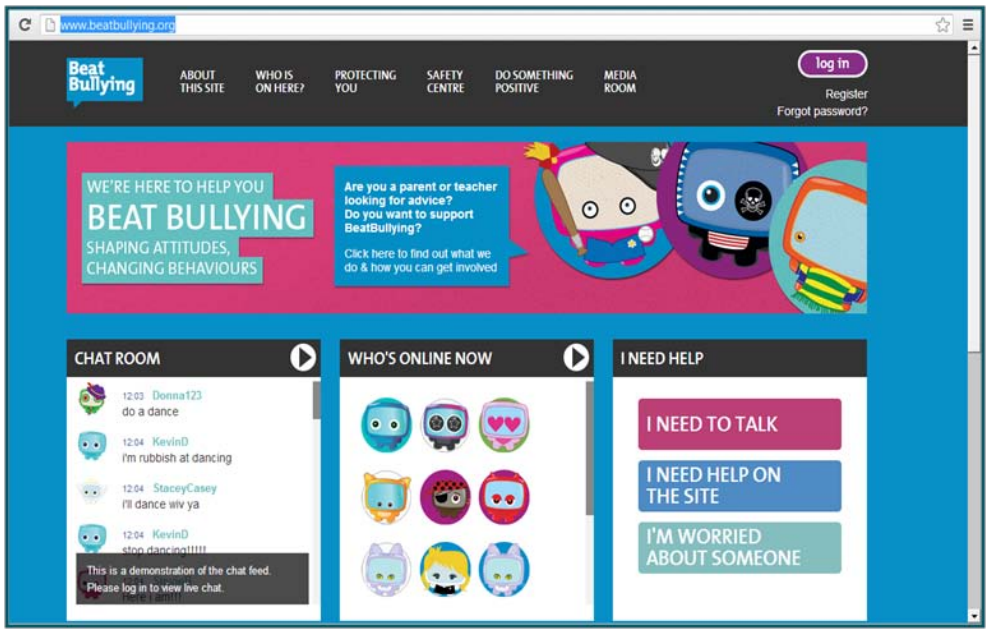
يساعد هذا الموقع الأعمار المختلفة من الأطفال على تصفح الإنترنت بسلام ويعلمهم كيفية التعامل مع مختلف التهديدات.

الشكل 4.14: الصفحة الرئيسية لموقع حماية الاطفال عند النفاذ.

الشكل 5.14: الموقع الرئيسي ThinkUKnow (http://www.thinkuknow.co.uk/)

هنالك أيضاً مجموعة محاربة البلطجة BeatBulling (http://www.beatbullying.org/) والتي تعمل على تقديم الاستشارات للآباء

والمدرسين وتقديم النصائح للأطفال في مجال محاربة البلطحة. الشكل 6.14 يبين الواجهة الرئيسية للموقع.



الشكل 6.14: الموقع الرئيسي لمجموعة محاربة البلطجة

7.14 القوانين والتشريعات

وضعت المملكة المتحدة العديد من التشريعات لحماية المعلومات والاتصالات والبنيات الأساسية نذكر منها ما يلي:

1. قانون الاحتيال والاتصالات للعام Telecommunications (Fraud) Act 1997:
2. قانون حماية البيانات :Data Protection Act 1998
3. قانون عام 2000م للاتصالات والإلكترونيات Electronic Communications Bill 2000: يشجع هذا القانون استخدام التشفير في المصادقة والأمور المتصلة بالتجارة الإلكترونية [197].
4. قانون الإرهاب :Terrorism Act 2000

5. قانون الشرطة والعدالة[198]:Police and Justice Act 2006
6. قانون منع استخدام الأطفال في المواد الإباحية 1996م Child Pornography Prevention Act: يُجرم هذا القانون استخدام الأطفال في المواد الإباحية [199].
7. قانون الجرائم الجنسية لسنة 2003م Sexual Offences Act: يحدد هذا القانون الجرائم الجنسية والأحكام والعقوبات المتعلقة بها ووسائل والوقاية وحماية الأطفال من الأذى [200].
8. قانون الطفل 2004م Children Act: صدر هذا القانون ليمهد لإنشاء مفوضية للأطفال والتي من خلالها يمكن الحكم على الخدمات المقدمة للأطفال والشباب من قبل السلطات المحلية وغيرها.

8.14 بعض من المواقع المهمة

الجدول 1.14: المواقع المهمة للجهات المهتمة بموضوع أمن المعلومات في المملكة المتحدة

اسم المؤسسة	عنوان الموقع	المهام الرئيسية
موقع مركز حماية البنيات التحتية	www.cpni.gov.uk /about/cni/	تحديد البنيات الحيوية وتقديم النصح والمشورة بخصوص أمن المعلومات
المنظمة الوطنية للتقنية وأمن المعلومات	www.cesg.gov.uk	الدعم التقني والمشورة
الجمعية البريطانية للحاسوب	www.bcs.org	التدريب و رفع القدرات
المركز الوطنى للحوسبة National Computing Centre	www.ncc.co.uk/	التدريب المهني ورفع القدرات المهنية
مؤسسة مراقبة الإنترنت	www.iwf.org.uk	مركز للإبلاغ من المحتويات المخالفة للقوانين
إتحاد الصناعات البريطانية	www.cbi.org.uk	الإسهام والدعم
الجمعية المهنية لأمن	www.iisp.org	هيئة للمواصفات والتدريب

المعلومات		وتنمية المهارات المهنية
GetSafeOnline	www.getsafeonline.org	نصائح عامة حول التعامل مع الإنترنت (مواقع التواصل الاجتماعي، التجارة الإلكترونية وأمن المعلومات).
saferinternet	www.saferinternet.org	شبكة مدعومة من الاتحاد الأوروبي متخصصة في مجال التصدي للجرائم الإلكترونية.
مركز حماية الاطفال عند النفاذ	ceop.police.uk	جمعية متخصصة في مجال حماية الأطفال عند النفاذ
ThinkUKnow	www.thinkuknow.co.uk.	شبكة تعليمية للنصح والإرشاد بخصوص حماية الأطفال عند النفاذ

الفصل الخامس عشر
تجربة الاتحاد الأوروبي

1.15 الخطة الشاملة والاتجاهات المستقبلية لبناء صناعة المعلوماتية

يعتبر الاتحاد الأوربي من المجموعات الدولية الأساسية المؤثرة في عالم اليوم من حيث الجهد والإسهام في مجال البحوث والدراسات المتعلقة ببناء نظم الاتصالات وتقدم ثورة المعلومات. في العام 2010م أعلنت المفوضية الأوروبية عن الأجندة الرقمية الأوروبية A Digital Agenda for Europe للعام 2020م والتي تهدف بصورة عامة إلى التطوير في المجالات والمحاور الآتية[201]:

1. بناء قطاع الاتصالات باستخدام شبكات السعات العريضة.
2. تطوير البنيات التحية للمعلوماتية للاتصالات.
3. تطوير الموارد البشرية ودعم سوق العمل بالخبرات.
4. تطوير سياسات أمن المعلومات.
5. تطوير قانون الملكية الفكرية.
6. تشجيع استخدام الحوسبة الموزعة.
7. دعم الصناعات الإلكترونية.

لتحقيق الأهداف العامة أعلاه، أعلنت المفوضية الأوروبية عن الأهداف والبرامج التفصيلية الخاصة والتي تشمل [202]:

- تغطية جميع دول الاتحاد بشبكة النطاق العريض Broadband Network بنهاية العام 2013م.
- تغطية جميع دول الاتحاد بشبكة النطاق العريض Broadband Network بسعة تفوق 30 ميغا بت في الثانية بنهاية العام 2020م.
- تغطية أكثر من 50% من الاتحاد الأوروبي بشبكة النطاق العريض Broadband Network بسعة تفوق 100 ميغا بت في الثانية بنهاية العام 2020م.

- تمكين 50% من سكان الاتحاد من إجراء المعاملات التجارية من خلال النوافذ الإلكترونية بنهاية العام 2015م
- تمكين 20% من سكان الاتحاد من إجراء المعاملات التجارية الدولية (خارج الحدود) من خلال النوافذ الإلكترونية بنهاية العام 2015م.
- تقليل قيمة التجول الدولي داخل دول الاتحاد إلى الصفر بنهاية العام 2015م.
- زيادة معدل استخدام الإنترنتregular internet usage من 60% إلى 75% بنهاية العام 2015م.
- تمكين 50% من سكان الاتحاد من إجراء المعاملات الحكومية من خلال نوافذ الحكومة الإلكترونية e-Government بنهاية العام 2015م.
- مضاعفة الإنفاق في مجالات البحوث والدراسات والتطوير المتصلة بتكنولوجيا المعلومات والاتصالات إلى 11 مليار يورو بنهاية العام 2020م.
- تقليل الطاقة المستهلكة في الإنارة بنسبة 20% بنهاية العام 2020م.
- تمكين المواطنين من إجراء جميع المعاملات الخدمية العابرة للحدود والمتفق عليها في العام 2011م من إجرائها من خلال النوافذ الإلكترونية بنهاية العام 2015م.

2.15 القطاعات والمصالح الإستراتيجية

موضوع حماية البنيات التحتية الحرجة للمعلوماتية والاتصالات من الموضوعات المهمة التي شغلت مراكز البحوث الأوروبية لفترة طويلة من الزمن. تم تعريف البنيات الأساسية الحرجة بواسطة الإدارة المركزية للاتحاد على أنها تلك الأصول الفيزيائية ونظم المعلومات والشبكات التي إذا أتلفت أو توقفت عن العمل لفترة قصيرة، يمكن أن تُحدث أثراً مدمراً على الصحة أو الأمن العام أو الاقتصاد لإحدى الدول الأعضاء. بناءً على هذا التعريف تم اعتماد المؤسسات الآتية على أنها بنيات أساسية حرجة:

- الطاقة Energy

- تكنولوجيا الاتصالات والمعلومات Information and Communication Technologies (ICT)
- المياه water
- الغذاء Food
- الصحة Health
- النظام المالي Financial System
- الإدارة المدنية Civil Administration
- نظم المواصلات Transport
- الكيميائيات والصناعات النووية Chemical and Nuclear Industry
- أبحاث الفضاء Space Research

3.15 السياسات العامة والمبادرات والبحوث

هنالك شبة إجماع بين دول الاتحاد الأوروبي على أن أمن البنيات التحتية الأساسية والحرجة مرتبط ارتباطاً مباشراً بأمن نظم المعلومات التي تعمل بهذه البنيات، لذلك ركزت رئاسة الاتحاد الأُوروبي على عملية تطوير نظم أمن المعلومات من خلال مجموعة من المبادرات والبحوث العلمية نذكر منها ما يلي:

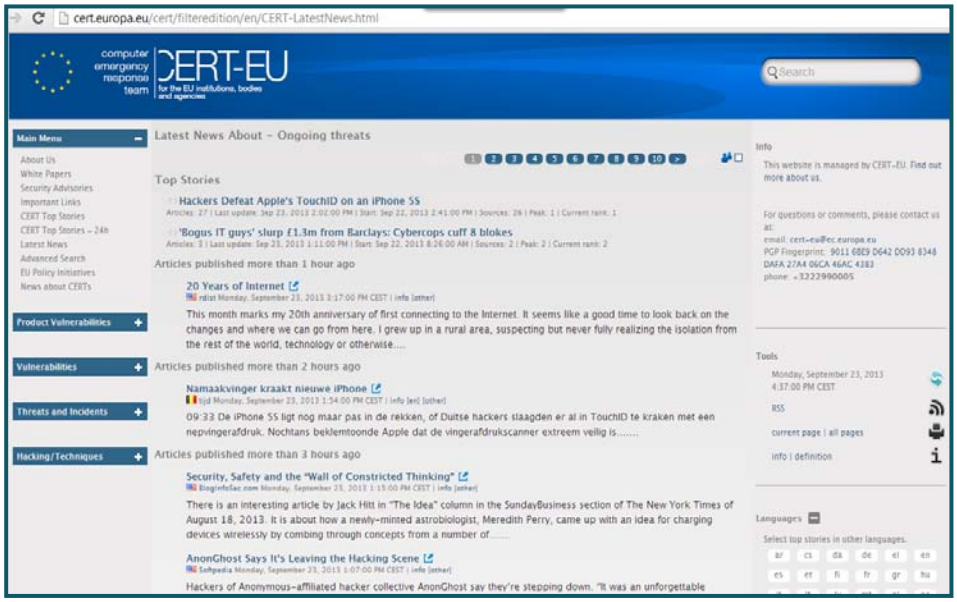
1. الورقة الخضراء لدراسة برنامج حماية البنيات التحتية الحرجة Green Paper on a European Program for CIP (EPCIP): ركزت هذه الورقة على دراسة الجوانب الآتية [203]:-
   - الأهداف الأساسية لبرنامج حماية أمن المعلومات.
   - وضع المبادئ الأساسية.
   - الإطار المطلوب تنفيذه.
   - تعريف وتحديد البنيات الحرجة.
   - الفرق بين ما هو وطني (خاص بالدولة) وما هو خاص بالاتحاد الأوروبي.

- ما هي واجبات المالك والمشغل والمستخدم للبنية الأساسية.
- دور عملية المراقبة والتقييم في سلامة البنيات التحتية.

2. إنشاء شبكة الإنذار الخاصة بالبنيات الأساسية الحرجة Critical Infrastructure Warning Information Network (CIWIN)(https://ciwin.europa.eu: وهى عبارة عن منظمة تمكن الدول الأعضاء في الاتحاد الأوروبي من تبادل الخبرات والبحوث والتجارب العملية في مجال أمن المعلومات وحماية البنيات التحتية الحرجة[204].
3. شبكة الاتحاد الأوروبي لأمن المعلومات European Network and Information Security Agency (ENISA). تعمل هذه الشبكة أو الوكالة على تقديم الدعم الفني لمراكز الحاسوب للاستجابة والطوارئ المعلوماتية للدول الأعضاء في الاتحاد في جميع المجالات المتعلقة بأمن المعلومات والتجارة الإلكترونية وأمن النظم الصناعية (Industrial Control systems/SCADA). أيضاً تساعد هذه الوكالة على رفع الكفاءة والخبرة لدول الاتحاد من خلال التدريب ومشاركة نتائج ومخرجات الدراسات والبحث العلمي [205].
4. مجموعات البحث الخاصة بتكنولوجيا أمن المعلومات Information Society Technologies (IST) FP6 and FP7. الهدف من هذا المجموعات البحثية هو زيادة وتشجيع المجتمع الأوربي على التطوير والابتكار في مجال أمن المعلومات.
5. البرنامج الأوروبي للبحث في موضوعات أمن المعلومات European Security Research Program (ESRP). هذا البرنامج عبارة عن مبادرة لدعم البحوث والدراسات في مجال أمن المعلومات.
6. مجموعة تنسيق البحث في موضوع البنيات المعلوماتية الحرجة Critical Information Infrastructure Research Co-ordination

(CI2RCO). يهدف هذا البرنامج إلى دعم وتنسيق الجهود البحثية بين الدول الأعضاء.

7. مركز الحاسوب للاستجابة والطوارئ الأوروبي EU Computer Emergency Response Team. يعمل هذا المركز وبالتنسيق مع المراكز العلمية والتقنية الأخرى والخاصة بالدول الأعضاء على التقليل من الأثر المدمر للهجمات الإلكترونية. الشكل 1.15 يوضح الصفحة الرئيسية لموقع الحاسوب للطوارئ والاستجابة التابع للاتحاد الأوروبي.



الشكل1.15: الصفحة الرئيسية لموقع الحاسوب للطوارئ والاستجابة التابع للاتحاد الأوربي.

4.15 حماية الأطفال عند النفاذ

لأهمية موضوع حماية الأطفال عند النفاذ على الإنترنت فقد أطلقت المفوضية الأوروبية حملات عدة لزيادة الوعي منذ عام 1999م [206]. تستهدف هذه الحملات كلاً من الأطفال والآباء والمدرسين وبيوتات التصنيع ومتخذي القرارات في الدول الأعضاء في الاتحاد بالتوعية والتعريف بالمخاطر الأساسية التي يمكن أن تواجه الأطفال على الإنترنت. يمكن تلخيص الأهداف الكلية لجميع المبادرات الأوروبية في الآتي:

- التعريف بالمخاطر في الفضاء المعلوماتي (الإنترنت).
- خلق وعي عام بهذه المخاطر.
- تطوير وسائل علمية لتقليل هذه المخاطر.
- تبادل الخبرات في المجالات التي يمكن أن تساعد في تقليل هذه المخاطر.

لتسهيل عملية تبادل الخبرات والتنسيق بين دول الاتحاد، تم إنشاء موقع شامل بالموضوعات الخاصة بالأمن عند النفاذ. الشكل 2.15 يوضح الصفحة الرئيسية لموقع (www.saferinternet.org) والذي يمكن من خلاله النفاذ إلى كل المواقع الخاصة بالسلامة عند النفاذ بالدول الأعضاء.

الشكل 2.15: الموقع الرئيسي للاتحاد الأوروبي للمساعدة على السلامة عند النفاذ.

5.15 القوانين والتشريعات

وضع الاتحاد الأوروبي العديد من التشريعات المُلزمة للدول الأعضاء لحماية المعلوماتية والاتصالات والبنيات الأساسية الحرجة نذكر منها ما يلي:

1. قانون حماية البيانات لسنة 1995م Data Protection Directive: يركز هذا القانون على جوانب حماية الخصوصية عند التعامل مع البيانات الشخصية للأفراد بواسطة مؤسسات الاتحاد الأوروبي. نسبةً لقصور هذا القانون في كثير من الجوانب الحديثة والمتعلقة بمواقع التواصل الاجتماعي وحوسبة الشبكات والتوافق مع القوانين العالمية الأخرى، فقد تم اقتراح قانون جديد في العام 2012م يحمل اسم General Data Protection Regulation (GDPR). من المتوقع أن يتم تنفيذ هذا القانون في العام 2014 م.[207-209].
2. قانون التحقق الإلكتروني لسنة 1999م Directive on Electronic Signature[210] يحدد هذا القانون الإطار القانوني على المستوى الأوروبي لاستخدام وسائل المصادقة الإلكترونية. ويهدف أيضاً إلى تسهيل استخدام المصادقة (التوقيعات) الإلكترونية، وفي أن تصبح معترفاً بها قانونياً داخل الدول الأعضاء [211].
3. قانون حماية الخصوصية لنظم الاتصالات 2002م Directive on Privacy Protection in the Electronic Communications Sectors: يهتم هذا القانون بجانب الخصوصية عند استخدام وسائل الاتصالات داخل الاتحاد (الدول الأعضاء). نسبةً للكثير من المتغيرات في مجال تكنولوجيا الاتصالات والمعلومات، فإنه تم إلحاق العديد من البنود في العام 2009م [212, 213].
4. اتفاقية (معاهدة) لشبونة 2007م Treaty of Lisbon: في هذه الاتفاقية تم وضع اللبنات الأولى في مجال إقامة المجتمع الأوروبي [214].
5. قانون حفظ البيانات 2006 Directive on Data Retention: يلزم هذا القانون شركات الاتصالات بحفظ بعض البيانات لفترة محددة بغرض استخدامها في عملية التحقيق في الجرائم المتصلة بالمعلوماتية والاتصالات [215, 216].

6. قانون Council Framework Decision on Attacks Against Information Systems 2005: يضع هذا القانون ويعرف الإطار العام للجرائم وللتعاون القانوني في المسائل المتصلة بالمعلوماتية داخل الدول الأعضاء، وذلك بالاعتماد على معاهدة قيام الاتحاد الأوروبي [217].
7. الاتفاقية الإطارية بشأن مكافحة الاستغلال الجنسي للأطفال والمواد الإباحية للأطفال Framework Decision on Combating the Sexual Exploitation of Children and Child Pornography 2003م: يحدد هذا الإطار الموجهات العامة للدول الأعضاء بشأن تحديد مدى العقوبات بشأن الجرائم المتصلة بالأطفال [218].
8. اتفاقية حماية الأطفال من الاستغلال الجنسي والاعتداء الجنسي 2007م Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse: تنص الاتفاقية في المادة 20 على أنه يجب على الدول الأعضاء اتخاذ التدابير التشريعية اللآزمة لضمان تجريم إقتناء المواد الإباحية من خلال تكنولوجيا المعلومات والاتصالات [219].
9. قرار الاتحاد بمكافحة المواد الإباحية على شبكة الإنترنت لسنة 2000م Council Decision to Combat Child Pornography on the Internet: يهدف هذا القرار إلى منع ومكافحة إنتاج وتجهيز وتوزيع وحيازة المواد الإباحية على شبكة الإنترنت [220].

6.15 بعض المواقع المهمة

الجدول 1.15: المواقع المهمة للجهات المهتمة بموضوع أمن المعلومات في الاتحاد الأوروبي

اسم المؤسسة	عنوان الموقع	المهام الرئيسية
شبكة الإنذار الخاصة بالبنيات الأساسية	www.ciwin.europa.eu/Pages	تبادل الخبرات العملية ونتائج البحوث والدراسات

الحرجة			
شبكة الأوروبي المعلومات	الاتحاد لأمن	www.enisa.europa.eu	وكالة متخصصة لتقديم الدعم الفني للدول الأعضاء في الاتحاد وذلك من خلال مراكز الحاسوب للطوارئ والاستجابة الموجودة في ظل دولة
مركزالحاسوب للإستجابة والطوارئ		www.cert.europa.eu	يعمل بالتنسيق مع المراكز الوطنية على منع وتقليل الهجمات الإلكترونية
موقع سلامة الإنترنت		www.saferinternet.org	يعمل الموقع على تقديم النصح والإرشاد على حماية الأطفال عند النفاذ
موقع تعلم اليوم		www.teachtoday.eu	تدريب المدرسين في مجال موضوعات حماية الأطفال عند النفاذ

الفصل السادس عشر

الاتجاهات المستقبلية في حماية البنيات التحتية الحرجة للمعلوماتية والاتصالات

1.16 المقدمة

في ختام هذا الكتاب نود أن نذكر ببعض المسلمات الأساسية، وهي أنه مع استمرار الحياة سوف يستمر التطور في التكنولوجيا لخدمة البشرية وقريباً سوف ينظر الجيل القادم إلى حياتنا اليوم على أنها حياة بدائية وأولية، فيها على سبيل المثال أن الإنسان لا يستطيع أن يرى ما يدور ما في داخل منزله من مكان العمل لعدم وجود شبكة بالمنزل مرتبطة بشبكة الهاتف أو الإنترنت، وفيها أيضاً أن السيارات يمكن أن تصطدم مع بعضها نتيجةً لأخطاء القيادة أو الأعطال البسيطة والبدائية التي يمكن تفاديها باستخدام المتحكمات الآلية ونظم المراقبة التي تعتمد على شبكات الاتصالات في الطرق. هذا كله استقراء أولي من منظور ضيق لبعض الاتجاهات البحثية في مجالات معالجة الصورة والمتحكمات الآلية وشبكات الاتصالات.

من المسلمات أيضاً أن هذا التطور سوف يكون مصحوباً ببعض التطور في مجالات الجريمة وبذلك تتطور المخاطر على البنيات الأساسية للمعلوماتية والاتصالات. في هذا الفصل نعرض بعض من الواجبات والموجهات الأساسية التي يمكن أن تساعد كل من الأفراد والمؤسسات والدول والمنظمات الدولية في مجابهة هذه المخاطر.

2.16 واجبات الدولة

يمكن بصورة عامة أن نلخص المهام الأساسية التي يمكن أن تقدمها الدولة في مجال حماية المعلوماتية وبنياتها في الآتي:

- دعم وتشجيع البحث العلمي والابتكار في مجال أمن المعلومات وحماية شبكات الاتصالات.

- بناء الأطر القانونية والتشريعات التي تحكم المنازعات ذات الصلة بالمعلوماتية والاتصالات من (تطوير وإصدار قوانين- تأهيل قضاة وادعاء عام ومحامين).
- تطوير وتحديث اللوائح والموجهات والمعايير المنظمة للعمل في هذا المجال (لوائح أمن المعلومات في القطاعات المالية، العسكرية، والقطاعات الحيوية والاساسية الأخرى).
- رفع الوعي العام بالمخاطر من خلال النوافذ الإعلامية المختلفة.
- العمل على تطوير الكوادر البشرية وتدريبها بصورة مستمرة لمواكبة المتغيرات فى مجال الجريمة الالكترونية.
- تحديد البنيات التحتية الأساسية الحرجة Critical Sectors والمعتمدة على المعلوماتية والاتصالات والعمل على حمايتها من المخاطر.
- خلق علاقة تواصل وتعاون بين القطاعات الحكومية المختلفة والقطاع الخاص (Information Sharing Forums) من أجل تبادل المعلومات والخبرات في مجال حماية المعلوماتية.
- التعاون مع المنظمات الدولية المهتمة بأمن المعلومات للاستفادة من خبراتها وتنسيق التحالفات الدولية الإستراتيجية في هذا الخصوص.
- العمل على حماية القيم والأخلاق والدين.
- تكوين فريق عمل وطني متخصص للتدخل والاستجابة السريعة لتقديم الدعم الفني للمؤسسات المختلفة في حال تعرضها للهجوم أو كارثة.
- تكوين آلية وطنية للإنذار المبكر بصورة فعّالة قادرة على التنبيه بالخطر في وقت وجيز ومناسب.
- العمل على تحديث بنيات المعلومات والاتصالات والاستفادة منها لزيادة الدخل القومى.
- العمل بصورة خاصة مع المنظمات الدولية لدعم مبادرات حماية للأطفال والأسرة في الفضاء المعلوماتي.

3.16 واجبات المؤسسات المهتمة بامن المعلومات فى الدولة

يمكن بصورة مختصرة تلخيص واجبات المؤسسات في حماية المعلوماتية والاتصالات في الآتي:

- تطبيق القوانين واللوائح والموجهات الصادرة من الدولة والخاصة بأمن المعلومات وحماية البنيات التحتية الاساسية.
- تطوير إدارة أو قسم أمن المعلومات وتأهيل الكوادر البشرية العاملة به ودعمها بالموارد المالية اللازمة.
- تطوير دراسات تحليل المخاطر Risk Analysis لمعرفة الاتجاهات المستقبلية.
- إعداد خطط للاستجابة لبعض المخاطر Disaster Recovery Plan.
- الاستعانة ببيوت الخبرة في عمليات المراجعة والتقييم والتطوير.
- العمل على تحديث السياسات بصورة دورية لمواكبة التطور السريع للجريمة الالكترونية.
- تطوير السياسات والنظم واللوائح الداخلية.
- استخدام الوسائل التقنية الحديثة للحماية.
- العمل على تبادل الخبرات والمعلومات بشأن المخاطر في مجال المعلوماتية مع القطاعات الأخرى ذات النشاط الاقتصادي المشابه.
- الاستجابة لنداءات وتوجيهات الإنذار المبكر الصادرة من المركز الوطني للإنذار المبكر بشأن المخاطر المحتملة في مجال المعلوماتية والاتصالات.

4.16 واجبات المنظمات الدولية العاملة فى مجال حماية المعلوماتية

بصورة عامة يمكن أن تقدم المنظمات الدولية العاملة في مجال أمن المعلومات وتطوير الانترنت الخدمات الآتية:

- تقديم الدعم الفني لبعض الدول في مجال إعداد السياسات الوطنية فى مجال أمن المعلوماتية وحماية البنيات التحتية الاساسية.
- العمل على توفير الدعم الفني للدول في حالات الكوارث والطوارئ ذات العلاقة ببنيات المعلومات والاتصالات.
- تطوير الإطار القانوني الدولي في مجال جرائم المعلوماتية العابرة للدول.
- المساهمة في مجال التحقيق المتصل بالجرائم العابرة للدول.
- العمل على تطوير إطار تقني يساعد في عمليات التحقيق فى الجرائم العابرة للدول من خلال التطوير في المواصفات القياسية لمعدات الاتصالات.
- العمل على حماية الأطفال والأسرة والأعراف الاجتماعية والمعتقدات.
- العمل على زيادة الوعي العام والإنذار المبكر.
- العمل على توفير غرفة للحوار بين الدول من أجل تطوير قوانين دولية في مجال أمن المعلومات وبنيات الاتصالات ومواءمة القوانين الداخلية للمجموعات الإقليمية.

5.16 واجبات الأفراد

يمكن تلخيص واجبات الفرد في النقاط الآتية:

- العمل على التطوير الذاتي من خلال الاطلاع المستمر لمواكبة المستجدات.
- الالتزام باللوائح والقوانين المنظمة للمعاملات.
- احترام القيم المجتمعية والأخلاق والمعتقدات عند استخدام نظم المعلومات والاتصالات وشبكات التواصل الاجتماعي.
- احترام قيم الأسرة والأطفال.
- استخدام وسائل التحكم الأبوي عند الضرورة.
- استخدام الوسائل التقنية المناسبة

قائمة الاختصارات

ACL	Access Control List
Aus-CERT	Australian Computer Emergency Response Team (Aus-CERT)
AES	Advanced Encryption Standard
AFP	Australian Federal Police
AHTCC	Australian High Tech Crime Centre
AIDE	Advanced Intrusion Detection Environment
AMC	Adaptive Modulation and Coding
AMPS	Advanced Mobile Phone System
ANSI	American National Standards Institute
AP-CIRT/ APCERT	Asia Pacific Computer Incident (Emergency) Response Team
ASIO	Australian Security Intelligence Organization
CAP	Certification and Accreditation Professional
CCFP	Certified Cyber-Forensic Professional
CDMA	Code Division Multiple Access
CEOP	Child Exploitation and Online Protection Centre
CIAO	Critical Infrastructure Assurance Office
CI2RCO	Critical Information Infrastructure Research Co-ordination

CIRT	Computer Incident Response Team
CISO	Chief Information Security Office
CISSP	Certified Information Systems Security Professional
CIWIN	Critical Infrastructure Warning Information Network
CLD	Cross Layer Design
COBIT	Control Objectives for Information and Technology Related
COP	Child Online Protection
CPNI	Centre for the Protection of National Infrastructure
CSNET	Computer Science Network
CSSLP	Certified Secure Software Lifecycle Professional
DCCI	Defense Cyber Crime Institute
DCFL	Defense Computer Forensics Laboratory
DCITA	Defense Cyber Investigations Training Academy
DNS	Domain Name System
DSD	Defence Signals Directorate
DSS	Digital Signature Standard
ECERT	Estonian Computer Emergency Response

	Team
EGPRS	Enhanced General Packet Radio System
ENISA	European Network and Information Security Agency
ESCAPE	Electronically Secure Collaborative Application Platform for Experts
ESPaC	E-Security Policy and Coordination
ESRP	European Security Research Program
ETSI	European Telecommunications Standards Institute
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FDMA	Frequency Division Multiple Access
FLAG	Fiber-Optic Link Around the Globe
GCA	Global Cyber-security Agenda (GCA)
GPRS	General Packet Radio System
GRC	Global Response Centre
HCISPP	HealthCare Information Security and Privacy Practitioner
HDTV	High Definition Television
HIPAA	Health Insurance Portability and Accountability
HIPCAR	Harmonization of ICT policies and

	legislation across the Caribbean
HIPSSA	Harmonization of the ICT Policies in Sub-Sahara Africa
HSBB	High Speed Broad band
HSDPA	High Speed Data Packet Access
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICB4PAC	
ICMP	Internet Control Message Protocal
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ICT	Information and Communication Technology
IDS	Intrusion Detections Systems
IEEE	Institute of Electrical And Electronic Engineering
IETF	Internet Engineering Task Force
IMPACT	International Multilateral Partnership Against Cyber Threats
INTELSAT	International Telecommunication Satellite
IRTF	Internet Research Task Force
ISACs	Information Sharing and Analysis Centers
ISP	Internet Service Providers
ISPC	The Information Security Policy Council

ITSEC	Information Technology Security Evaluation Criteria
ITU	International Telecommunication Union
JNSA	Japan Network Security Association
JPCERT / CC	Japan Computer Emergency Response Team Coordination Center
LAN	Local Area Network
LABAC	Lattice-Based Access Control
LTE	Long Term Evolution
My-CERT	Malaysian Computer Emergency Response Team
MEASAT	Malaysia East Asia Satellite
METI	and Industry ، Trade،Ministry of Economy (METI)
MIMO	Multiple Input Multiple Output
MLS	Multiple Levels of Security
MODCERT	Ministry of Defense Computer Emergency Response Team
MOSTI	Technology and ،Ministry Of Science Innovation
NATO	North Atlantic Treaty Organization
NBN	National Broadband Network
NEWS	Network Early Warning System

NIRT	National Incident Response Team
NISC	National Information Security Centre
NIP	Network Intelligent Police
NIST	National Institute of Standard and Technology
NSF	National Science Foundation
OFDMA	Orthogonal Frequency Division Multiple Access
OISF	Open Information Security Foundation
PCCIP	Presidential Commission on Critical Infrastructure Protection
Q-CERT	Qatar Computer Emergency Response Team
QNBN	Qatar National Broadband Network
RBC	Role-Based Access Control
SCADA	Supervisory Control and Data Acquisition
SEA-ME-WE-4	South-East Asia - Middle East - Western Europe- 3
SEA-ME-WE-4	South East Asia–Middle East–Western Europe 4
SDTV	Standard Definition Television
SRI	Stanford Research Institute
SSCP	Systems Security Certified Practitioner
SynCom	synchronous Communication satellite

TCP	Transmission Control Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TDMA	Time Division Multiple Access
TISN	Trusted Information Sharing Network
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System
WLAN	Wireless Local Area Network
WSIS	World Summit of the Information Society

المراجع الأجنبية

[1] D. G. Messerschmitt and E. A. Lee, *Digital Communication*, 1 ed.: Kluwer Academic Publishing, 1988.

[2] E. A. Lee and D. G. Messerschmitt, *Digital Communication*: Kluwer Academic Publishing, 1994.

[3] A. J. Whitaker. *Bell Telephone Memorial and Bell Homestead* .

[4] J. M., *Optical Fiber Communications*. London: Printiace Hall International, 1985.

[5] D. Forney. (2005, 18 Aug, 2013). *6.451 Principles of Digital Communication II*. Available: http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-451-principles-of-digital-communication-ii-spring-2005

[6] optics. (2013, 18 Aug). *NEC and Corning achieve petabit optical transmission*. Available: http://optics.org/news/4/1/29

[7] c. shannon, "A Mathematical Theory of Communication," *Bell System Technical Journal,*, vol. 27, pp. 379–423, July 1948.

[8] A. Goldsmith, *Wireless Communications*: Cambarge University Press, 2005.

[9] Rappaport, *Wireless Communications: Principles and Practice*: Dorling Kindersley, 2009.

[10] I. F. Akyildiz, D. M. Gutierrez-Estevez, and E. C. Reyes, "The evolution to 4G cellular systems: LTE-Advanced," *Physical Communication*, pp. 217-244, 2010.

[11] Per Beming, L. Frid, G. Hall, P. Malm, T. Noren, M. Olsson, and G. Rune, "LTE-SAE architecture and performance," *Ericsson 98 Review,* vol. 3, pp. 98-104, 2007.

[12] I. F. Akyildiz, D. M. Gutierrez-Estevez, and E. C. Reyes, "The evolution to 4G cellular systems: LTE-Advanced," *Physical Communication* vol. 3, pp. 217-244, 2010.

[13] Q. Li, G. Li, D. Mazzarese, B. Clerckx, and Z. Li" ,MIMO Techniques in WiMAX and LTE: A Feature Overview," *IEEE Communications Magazine,* May 2010.

[14] E. Dahlman, S. Parkvall, and J. Sköld, *4G LTE/LTE-Advanced for Mobile Broadband*, 1 ed.: Academic Press of Elsevier, 2011.

[15] A. C. Clarke. (Oct). *Extra-terrestrial relays*. Available: http://lakdiva.org/clarke/1945ww/1945ww_oct_305-308.html

[16] A. C. Clarke, "Extra-terrestrial relays," *Wireless World*, pp. 305-308, October 1945.

[17] arabsat. (Oct). *Arab satellite communications organization*. Available :http://www.arabsat.com/pages/Default.aspx

[18] D. Doddy, *Satellite Communications*, 3 ed.: McCrow-Hill, 2001.

[19] E. Saeid, "Precoder Design Based On inter-antenna Leakage Minimization for MU-MIMO," PhD, Electrical and Electronic

Engineering, Universiti Technology Petronas, Tronoh, Malaysia, 2013.
[20] SANS_Institute. (2002, Requirements for the Design of a Secure Data Center. Available: http://www.sans.org/reading-room/whitepapers/recovery/requirements-design-secure-data-center-561
[21] V. Kawadia and P .R. Kumar, "A cautionary perspective on cross-layer design," *IEEE Wireless Communications*, pp. 3-11, Feb 2005.
[22] L. Kleinrock, "Message Delay In Communication Nets With Storage," PhD, Electrical Engineering, MIT, 1962.
[23] G. Putic. (2013, Sept). *Stuxnet: An Effective Cyberwar Weapon*. Available: http://www.voanews.com/content/stuxnet-an-effective-cyberwar-weapon/1691311.html
[24] R. McMillan. (2010, Sept). *Siemens: Stuxnet worm hit industrial systems*. Available: http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems?taxonomyName=Network+Security&taxonomyId=142
[25] K. Hart. (2008, Aug). *Longtime Battle Lines Are Recast In Russia and Georgia's Cyberwar*. Available: http://msl1.mit.edu/furdlog/docs/washpost/2008-08-_14washpost_russia_georgia_cyberwar.pdf
[26] C. S. I. Operations. (2005, Aug). *Zotob Worm Information*. Available: http://www.cisco.com/web/about/security/intelligence/zotob-worm.html
[27] K. Poulsen. (2003, Aug). *Slammer worm crashed Ohio nuke plant network*. Available: http://www.securityfocus.com/news/6767
[28] R. McMillan. (2007, July). *Admin Faces Prison for Trying to Axe Power Grid*. Available: http://www.washingtonpost.com/wp-dyn/content/article/2007/12/15/AR2007121500062.html
[29] D. Verton. (2003 ,Sept). *Software failure cited in August blackout investigation*. Available: http://www.computerworld.com/s/article/87400/Software_failure_cited_in_August_blackout_investigation
[30] D. castro, "How Much Will PRISM Cost the U.S. Cloud Computing Industry ",ed: The information technology & innovation foundation, 2013.
[31] US_Government, "Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," D. o. n. intelligence, Ed., ed. Washington DC: Director of national intelligence, 2013.
[32] E. Messmer. (2013, Nov). *Don't trust the NSA? China-based Huawei says, 'Trust us*. Available:

http://www.computerworld.com/s/article/9243335/Don_t_trust_the_NSA_China_based_Huawei_says_Trust_us_
[33] J. Snyder. (2013, Nov .(*The Huawei security risk: Factors to consider before buying Chinese IT*. Available: http://searchsecurity.techtarget.com/feature/The-Huawei-security-risk-Factors-to-consider-before-buying-Chinese-IT
[34] B. Carlson. (2012, Nov). *Why is US Congress afraid of Chinese telecommunications giant Huawei*. Available: http://www.globalpost.com/dispatch/news/regions/asia-pacific/china/121009/huawei-ZTE-investigation-US-congress
[35] E. Zmijewski. (2008, Aug). *Mediterranean Cable Break*. Available: http://www.renesys.com/2008/01/mediterranean-cable-break/
[36] M. S. Media. (2008). *Mid East Communication Cables Cut, Companies Lose, Win Internet Providers*. Available: http://www.mathaba.net/news/?x=581059
[37] R. Drake. (2008, Aug). *The Submarine Cables – A Complete Guide to the 2008 Internet Outage*. Available: http://randomdrake.com/2008/02/12/the-submarine-cables-a-complete-guide-to-the-2008-internet-outage/
[38] R. S. a. c. Christof Gerlach, "Economic Impact of Submarine Cable Disruptions," APEC Policy Support Unit, Bangkok, Thailand2012.
[39] J. Oates. (2008, Aug). *Submarine cable cut torpedoes Middle East access*. Available: http://www.theregister.co.uk/2008/01/30/india_mideast_lose_internet/
[40] S. J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," *Berkeley Journal of International Law*, vol. 27, pp. 1-60, 2009.
[41] J. Davis. (2007, Aug). *Hackers Take Down the Most Wired Country in Europe*. Available: http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all
[42] S. Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Stephen Herzog*, vol. 4, pp. 49-60, 2011.
[43] M. W. C. Ashmore, "Impact of Alleged Russian Cyber Attacks," S. o. A. M. Studies, Ed., ed. Kansas :U.S. Army 2009.
[44] H. o. l. E. U. Committee, "Protecting Europe against large-scale cyber-attacks," London2009.
[45] E. Tikk, K. Kaska, and L. Vihul, "International cyber incidents: legal considerations," Cooperative Cyber Defence Centre of Excellence (CCD COE), Tallinn Estonia2010.

[46] S. Li, "When Does Internet Denial Trigger the Right of Armed Self-Defense," *THE YALE JOURNAL OF INTERNATIONAL LAW*, vol. 38, pp. 179-215, 2013.
[47] H. lobel, "The Law of War Implications of the Private Sector's Role in Cyber Conflict," *Texas international law journal*, vol. 47, pp. 618-640, 2012.
[48] M. C. Waxman, "Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions," *International Low Studies*, vol. 89, pp. 109-122, 2013.
[49] M. C .Waxman, "Comperhensive Ligal Approch for Cyber Security," PhD, Low, University of Tartu, 2011.
[50] B. Guttman and E. A. Roback, *An Introduction to Computer Security: The NIST Handbook*: NIST, 1995.
[51] J. Kimmins, C. Dinkel, and D. Walters, "Telecommunications Security Guidelines for Telecommunications Management Network NIST Special Publication 800-13," U. S. D. O. Commerce, Ed., ed. Gaithersburg,: U.S. DEPARTMENT OF Commerce, 1995.
[52] G. Stoneburner, A. Goguen, and A. Feringa, *Risk Management Guide for Information Technology Systems*. Gaithersburg: U.S. DEPARTMENT OF COMMERCE, 2002.
[53] M. Swanson, P. Bowen, A. W. Phillips, D. Gallup, and D. Lynes, "Contingency Planning Guide for Federal Information Systems," NIST Special Publication 800-34 Rev. 1May 2010.
[54] N.-J. t. force, *Guide for Applying the Risk Management Framework to Federal Information Systems*: U.S. Department of Commerce, 2010.
[55] NIST, *Recommended Security Controls for Federal Information Systems and Organizations* U.S. Department of Commerce 2009.
[56] NIST, *Managing Information Security Risk Organization, Mission, and Information System View*: U.S. Department of Commerce 2011.
[57] S. Carlos M. Gutierrez. (2007, Guide to Industrial Control Systems Security, Second Public Draft ,NIST Special Publication. Available: http://industryconsulting.org/pdfFiles/NIST%20Draft-SP800-82.pdf
[58] M. Scholl, K. Stine, J. Hash, P. Bowen, A. Johnson, C. D. Smith, and D. I. Steinberg. (2008, 2013). An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule *NIST Special Publication 800-66*. Available: http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf
[59] Industrial_Automation_Open_Networking_Association. (2006). *IAONA Handbook Network Security*. Available: http://www.vpi-initiative.com/download/IAONA-Security-Guide-15-draft.pdf

[60] US_Government. (2013, Aug). *Version 5 Critical Infrastructure Protection Reliability Standards*. Available: http://www.ferc.gov/whats-new/comm-meet/2013/041813/E-7.pdf
[61] US_Government. (Aug). *Cooperative Association for Internet Data Analysis*. Available: http://www.caida.org/home/
[62] I. S. I. D. British Columbia Institute of Technology. (Aug). *Industrial Security Incident Database*. Available: http://www.securityincidents.net/index.php/About/
[63] X. R. Luo, R. Brody, A. Seazzu, and S. Burd, "Social Engineering: The Neglected Human Factor for Information Security Management," *Information Resources Management Journal*, vol,18 . Sept 2011.
[64] T. Herath and H. R. Rao, "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems*, pp. 106-125, 2009.
[65] T. w. Bank, "World Bank Group Strategy for Information and Communication Technology," ed: World Bank Group 2012.
[66] N. Mayer, P. Heymans and R. Matulevičius (Aug). *Design of a Modelling Language for Information System Security Risk Management* Available: http://www.nmayer.eu/publis/RCIS07-CR_NMA-PHE-RMA.pdf
[67] D. Hucaby, D. Garneau, and A. Sequeira, *CCNP Security firewall 642-618 Official Cert Guide*. Indianapolis: Cisco Press, 2012.
[68] K. S. P. Mell, "Guide to Intrusion Detection and Prevention Systems," vol. NIST Special Publication 8 ,94-00U. S. D. o. Commerce, Ed., ed: National Institute of Standards and Technology, 2007.
[69] R. U. Rehman, *Intrusion Detection with SNORT: Advanced IDS Techniques Using SNORT, Apache, MySQL, PHP, and ACID* Prentice Hall, 2001.
[70] P. Weaver. (Aug). *SNORT IDS for SCADA Systems*. Available: http://www.snort.org/assets/114/Snort_RH5_SCADA.pdf
[71] O. I. S. Foundation. (2010, 2013). *Suricata (software)*. Available: http://www.openinfosecfoundation.org/index.php/download-suricata
[72] V. Jyothsna, V. V. R. Prasad, and K. M. Prasad, "A Review of Anomaly based Intrusion Detection Systems," *International Journal of Computer Applications*, vol. 28, pp. 26-35, Aug 2011.
[73] M. Uddin, K. Khowaja, and A. A. Rehman, "Dynamic Multi-Layer Signature Based Intrusion Detection System Using Mobile Agents " *International Journal of Network Security & Its Applications*, vol. 2, pp. 129-141, Oct 2010.
[74] F. F. I. E. Council. (Aug). *Authentication in an Internet Banking Environment*. Available: http://www.ffiec.gov/pdf/authentication_guidance.pdf

[75] S. McGee, R. V. Sabett, and A. Shah, "Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense," *Journal of Business & Technology Law*, vol. 8, 2013.
[76] H. Burch and B. Cheswick, "Tracing Anonymous Packets to Their Approximate Source," in *Proceedings of the 14th Systems Administration Conference*, New Orleans, Louisiana, 2000.
[77] Jeffrey Hunker, Bob Hutchinson, and J. Margulies. (2008, Jan). Role and Challenges for Sufficient Cyber-Attack Attribution .
[78] D. A. Wheeler, "Techniques for Cyber Attack Attribution," I. f. d. analyses, Ed., ed. Alexandria, Virginia: IDA, 2003.
[79] E. Casey, *Handbook of Digital Forensics and Investigation*: Elsevier Academic Press, 2010.
[80] A .M. Marshall, *Digital Forensics Digital Evidence in Criminal Investigation*: JohnWiley & Sons, Ltd, 2008.
[81] NIST, " Computer Forensics Tool Testing Project Handbook," U. D. o. Comerce, Ed., ed: US . Department of Comerce, 2012.
[82] J. Ashcroft, D. J. Daniels, and S. V. Hart, "Forensic Examination of Digital Evidence: A Guide for Law Enforcement," U. S. D. o. Justice, Ed., ed: U.S. Department of Justice, 2001.
[83] M. Damianides, "Sarbanes–Oxley and it Governance: New Guidance on it Control and Compliance," *Information systems Management*, pp. 77-85, 2005.
[84] R. Saint-Germain, "Information Security Management Best Practice Based on ISO/IEC 17799 " *The Info rmation Management Journal* pp. 60-66, Aug 2005.
[85] J. N. Ezingeard, McFadzean, E., & Birchall, D, "A model of information assurance benefits," *EDPACS*, pp. 1-16, 2005.
[86] SAINT. (20 Aug). *SAINT is a Vulnerability Assessment Tool*. Available: http://www.saintcorporation.com/
[87] OpenVAS. (20 Aug). *Open Vulnerability Assessment System (OpenVAS* .(Available: http://www.openvas.org/
[88] Metasploit. (20 Aug). *Metasploit Project*. Available: http://www.metasploit.com/
[89] Pentoo. (20 Aug). *Pentoo Penetration Testing tool*. Available: http://www.pentoo.ch/
[90] Blackbox. (20 Aug). *BackBox Penetration Testing tool*. Available: http://www.backbox.org/
[91] VMware. (20 Aug). *IT Health Check (ITHC)*. Available: http://www.vmware.com/company/acquisitions/ithc.html
[92] Burp. (Aug). *Burp Proxy*. Available: http://portswigger.net/burp/proxy.html
[93] T. N. Security. *Nessus Vulnerability Scanner*. Available: http://www.tenable.com/products/nessus

[94] OllyDbg. *OllyDbg Pen-test*. Available: http://www.ollydbg.de/
[95] Nmap. (Aug). *Nmap Pen-Test*. Available: http://nmap.org/
[96] ISACA. (20 Aug). *Control Objectives for Information and Related Technology*. Available: http://www.isaca.org/COBIT/Pages/default.aspx
[97] S. Direct. (20 Aug). *ISO 27002 - The Information Security Standard*. Available: WWW.STANDARDSDIRECT.ORG
[98] M. J. Kenning, "Security management standard — ISO 17799/BS 7799," *BT Technol J*, vol. 19, pp. 132-136, 2001.
[99] NIST. *Federal Information Security Management Act of 2002*. Available: http://csrc.nist.gov/groups/SMA/fisma/index.html
[100] NIST. *NIST-SP800*. Available: http://csrc.nist.gov/publications/PubsSPs.html
[101] K. N. Hampton, L. Sessions!Goulet, L. Rainie, and K. Purcell, "Social networking sites and our lives," Pew Internet ProjectJune 16 2011.
[102] C. O. Rodriguez. (2012, 19 Aug). *MOOCs and the AI-Stanford like Courses: Two Successful and Distinct Course Formats for Massive Open Online Courses* .
[103] C. Dwyer, S. R. Hiltz, and K. Passerini, "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace," in *Thirteenth Americas Conference on Information Systems*, 2007.
[104] M. Pagani, C. F. Hofacker, and R. E. Goldsmith, "The Influence of Personality on Active and Passive Use of Social Networking Sites," *Psychology & Marketing*, p. 441456, May 2011.
[105] S. Kolowich. (2013, 19 Aug). *How EdX Plans to Earn ,and Share, Revenue From Its Free Online Courses*. Available: http://chronicle.com/article/How-EdX-Plans-to-Earn-and/137433/
[106] D. Koller. (2012). *What we're learning from online education*. Available: http://www.ted.com/talks/daphne_koller_what_we_re_learning_from_online_education.html
[107] S. N. s. G. a. B. I. o. Kids. (2011, 19 Aug). *Social Networking's Good and Bad Impacts on Kids*. Available: http://www.apa.org/news/press/releases/2011/08/social-kids.aspx
[108] B. Dinerman, "Social networking and security risks," *GFI White Paper*, 2011.
[109] S. Browser Media, MacWorld. (2012, 19 Aug). *Social Networking Statistics*. Available: http://www.statisticbrain.com/social-networking-statistics/
[110] G. N. Wise. (Aug). *Keeping children safe on the Internet is everyone's job*. Available: http://kids.getnetwise.org/safetyguide/

[111] ITU. (2012, Aug). *Establishment of Harmonized Policies for the ICT Market in the ACP Countries*. Available: http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model-Policy-Guidelines-and-Legislative-Text_Cybercrime.pdf
[112] ITU. (2012, Aug). *Support for harmonization of the ICT Policies in Sub-Saharan Africa*. Available: http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/hipssa/Pages/default.aspx
[113] ITU. (2009, Aug). *Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries (ICB4PAC)*. Available: http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/ICB4PAC/Pages/default.aspx
[114] ITU. (Aug). *Capacity Building*. Available: http://www.itu.int/osg/csd/cybersecurity/gca/cap-build.html
[115] ITU. (Aug). *Organizational Structures*. Available: http://www.itu.int/osg/csd/cybersecurity/gca/org-struc.html
[116] ITU. (2009, Aug). *Technical and Procedural Measures*. Available: http://www.itu.int/osg/csd/cybersecurity/gca/tech-proced.html
[117] I. T. Union, "The ITU National Cybersecurity strategy guide," ed, 2011.
[118] ITU-IMPACT, "ITU-IMPACT Service Catalogue ", I. T. Union, Ed., ed, 2011-2012.
[119] ITU-IMPACT. (201 ,1Aug). *ITU-IMPACT Partnership Prospectus (ALERT) Applied Learning for Emergency Response Team*. Available: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/ALERT.pdf
[120] ITU. (2009, Aug). *Cybersecurity Guide for Developing Countries*. Available: http//:www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf
[121] ITU. (2012, Aug). *Understanding cybercrime: Phenomena, challenges and legal response* Available: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf
[122] UNODC/ITU. (Aug). *ITU/UNODC Cybercrime:The global challenge*. Available: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/cybercrime.pdf
[123] ITU. (2009, Aug). *ITU National Cybersecurity/CIIP Self-Assessment Tool*. Available: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-self-assessment-toolkit.pdf
[124] I. T. Union. (2010, Child Online Protection. Available: http://www.ictliteracy.info/rf.pdf/COP-Child_Online_Protection.pdf
[125] Q. ICT, "Controls for the Security of Critical Industrial Automation and Control Systems Guidelines," ed: ICT Qatar, 2012.
[126] S. C. o. I. a. C. T. (ictQATAR), "Government Information Assurance Policy," ed: Qatar Supreme Council of Information and Communication Technology (ictQATAR) 2012.

[127] H. Al-Jaber. (2012, Aug). *Protecting Qatar's Children in Cyberspace*. Available: http://www.ictqatar.qa/en/news-events/news/protecting-qatars-children-cyberspace
[128] Q. ICT. (2012, Aug). *Cyber safety awareness*. Available: http://www.ictqatar.qa/en/program/cyber-safety-awareness
[129] Q. Government, "The Bylaw Regulating the Work of Certification Service Providers," ed. Doha, Qatar: ICT-qatar, 2010.
[130] Q. Government, "Electronic Commerce and Transactions Law," ed. Doha: ICT-QATAR, 2010.
[131] M. Bingemann. (2010, Nov). *Satellite operators shortlisted for national broadband network* Available: http://www.theaustralian.com.au/technology/satellite-operated-shortlisted-for-national-broadband-network/story-e6frgakx-1225873722807
[132] N. _Co. (2009, Aug). *NBN CO*. Available: http://www.nbnco.com.au/
[133] E. M. Brunner and M. Suter, *International CIIP Handbook*: Center for Security Studies, ETH Zurich, 2009.
[134] A. F. P. (AFP). (July). *Australian High Tech Crime Centre*. Available: http://www.afp.gov.au/policing/cybercrime.aspx
[135] P .Holzer and A. Lamont, "Australian child protection legislation," *Australian Institute of family studies*, 14 Oct 2009.
[136] Austrilan_government. (2010, Aug). *Sexual Offences Against Children) Act 2010*. Available: http://www.comlaw.gov.au/Details/C2010A00042
[137] Austrilan_government. (2011, Aug). *Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2011*. Available: http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r4456
[138] Herald_Sun_News. (2011, Nov). *NBN bills finally pass lower house*. Available: http://www.heraldsun.com.au/archive/news/nbn-bills-finally-pass-lower-house/story-fn7x8me2-1226029602261
[139] B. H. Lee. (Sept). *TM HSBB: The Journey and the anticipatxion*. Available: http://www-mura.ist.osaka-u.ac.jp/ondm2010/pdf/ws2-3.pdf
[140] C. S. Malaysia. (2013, 27 Aug). *Critical National Information Infrastructure*. Available: http://cnii.cybersecurity.my/main/about.html
[141] C. malaysia. (Aug). *Critical National Information Infrastructure*. Available: http://cnii.cybersecurity.my/main/index.html
[142] NITC. (27 Aug). *National Information Technology Council of Malaysia (NITC Malaysia)*. Available: http://www.nitc.org.my/

[143] C. S. Malaysia. (26 Aug). *Cyber Security Malaysia Awards, Conference & Exhibition*. Available: http://www.csm-ace.my/
[144] T. a. I. Ministry of Science, "National Cyber Security," ed. Malaysia: Ministry of Science, Technology and Inovation, 2007.
[145] MyCert. (Aug). *Malaysian computer Emergency Response Team*. Available: http://www.mycert.org.my/en/
[146] C. Malaysia. (Aug). *CyberSecurity Malaysia*. Available: www.cybersecurity.my(
[147] CyberSafe-Malaysia. (Aug). *CyberSafe malysia*. Available: www.cybersafe.my
[148] M. Goverment. (Aug). *Digital signature (amendment) act 2001 ACT*. Available: http://www.skmm.gov.my/Legal/Acts/DIGITAL-SIGNATURE-ACT-1997-REPRINT-2002/DIGITAL-SIGNATURE-REGULATIONS-1998.aspx
[149] M. Govenment. (Aug). *Malaysian Communications and Multimedia Commission act*. Available: http//:www.skmm.gov.my/Legal/Acts.aspx
[150] Malaysian_govenment. (2010, Aug). *Strategic trade act 2010 (STA) [act 708]*. Available: http://www.skmm.gov.my/Legal/Acts/Strategic-Trade-Act-(STA)-Act-708.aspx
[151] Malaysian_govenment. (2012, Aug). *Postal services act 2012 act 741*. Available: http://www.skmm.gov.my/Legal/Acts/Postal-Services-Act-2012-Act-741.aspx
[152] H. security. (27 Aug). *Critical Infrastructure Sectors*. Available: http://www.dhs.gov/critical-infrastructure-sectors
[153] P. s. C. o. C. I. Protection, "Critical Foundations Protecting America's Infrastructures," 13 Oct 1977.
[154] J. D. Moteff, "Critical Infrastructures: Background, Policy, and Implementation," *Congressional Research Service*, 11 July 2011.
[155] *National Plan for Information Systems Protection Version 1.0 An Invitation to a Dialogue*, 2000.
[156] U. G. P. Office, "Homeland security act of 2002," U. S. G. P. Office, Ed., ed, 2002, pp. 2135 - 2321.
[157] W. Paper, "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets," ed: ISAC Council, 2004.
[158] U. Government, "National Strategy to Secure Cyberspace," ed. Washington: The White House, 2003.
[159] U. Government, "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets," ed. Washington: the white house washington, 2003.
[160] U. Government, "National Strategy for Information Sharing," ed: US Government, 2007.

[161] U. Government, "Natinal Strategy For Information Sharingand Safegarding," ed. Washginton :The WhiteHouse, 2012.
[162] US_Government. (2011, Aug 2013). Department of defense strategy for operating in cyberspace. Available: http://www.defense.gov/news/d20110714cyber.pdf
[163] US_Government. (2011, Strategy to combat transnational organized crime .Available: http://www.whitehouse.gov/sites/default/files/Strategy_to_Combat_Transnational_Organized_Crime_July_2011.pdf
[164] K. M. Finklea and C. A. Theohary, "Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement," Congressional Research Service2013.
[165] US_Government. (2011, Aug). *International l strategy for cyberspace*. Available: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
[166] US_Government. (2011, Aug). *National Strategy for Trusted Identities in Cyberspace (NSTIC or Strategy)*. Available: http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
[167] U. H. Security. (Aug). *Office of Cybersecurity and Communications*. Available: http://www.dhs.gov/office-cybersecurity-and-communications
[168] InfraGard. (Aug). *Learn More About InfraGard*. Available: https://www.infragard.org/FsafFT%2525252BDEUrq3EOQ9lsoJSt5VO98yZFD0ua36j7dev8%2525253D%21
[169] Cybertelecom. (Aug). *the Children's Online Privacy Protection Act (COPPA)*. Available: http://www.cybertelecom.org/privacy/coppa.htm
[170] U. F. C. Commission. (Aug). *Children's Internet Protection Act*. Available: http://www.fcc.gov/guides/childrens-internet-protection-act
[171] N. Willard. (2012, Aug). *Protecting Children in the 21st Century*. Available: http://www.districtadministration.com/article/protecting-children-21st-century
[172] Congress. (2007, Aug). *S. 49 (110th): Protecting Children in the 21st Century Act*. Available: http://www.gpo.gov/fdsys/pkg/BILLS-110s49is/pdf/BILLS-110s49is.pdf
[173] W. R. Ginsberg, "Federal Advisory Committees: An Overview " *Congressional Research Service*, 2009.
[174] I. L. Treatise. (28 Aug). *Computer Fraud and Abuse Act*. Available: https://ilt.eff.org/index.php/Computer_Fraud_and_Abuse_Act_(CFAA(
[175] *Executive order eo 13010 critical infrastructure protection*, 1996.

[176] US_Government. (2001, Sept). *USA Patriot Act of 2001*. Available: http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf
[177] FoxNews. (2011, Sept). *Obama Signs Last-Minute Patriot Act Extension*. Available: http://www.foxnews.com/politics/2011/05/27/senate-clearing-way-extend-patriot-act/%7Cdate
[178] US_Government. (2001, Sept). *Executive Order 13228 of October 8, 2001:Establishing the Office of Homeland Security and the Homeland Security Council*. Available: https://www.fas.org/irp/offdocs/eo/eo-13228.htm
[179] US_Government. (2001, Sept). *Executive Order 13231 of October 16, 2001 Critical Infrastructure Protection in the Information Age*. Available: https://www.fas.org/irp/offdocs/eo/eo-13231.htm
[180] US_Government. (Sept). *The Freedom of Information Act (FOIA)*. Available: http://www.foia.gov/
[181] March, "2013 Terrorism risk insurance report," 2013.
[182] U. Government, "Adam Walsh Child Protection and Safety Act," ed: US Government.
[183] Japan_Government. (2001, Aug). *e-Japan Strategy*. Available: http://www.kantei.go.jp/foreign/it/network/0122full_e.html
[184] Japan_Government. (2005, Aug). *U-japan*. Available: http://www.soumu.go.jp/menu_seisaku/ict/u-japan_en/
[185] J. G. of. (2009, Nov). *i-Japan Strategy 2015*. Available: http://www.kantei.go.jp/foreign/policy/it/i-JapanStrategy2015_full.pdf
[186] G. o. Japan, "The Second Action Plan on Information Security Measures for Critical Infrastructures ", T. I. S. P. Council, Ed., ed, 2009.
[187] G. o. Japan. (2013, Sept). *National Information Security Centre*. Available: www.nisc.go.jp
[188] ITU. (2009, Aug). *ITU/MIC Strategic Dialogue on Safer Internet Environment for Children*. Available: http//:www.itu.int/osg/csd/cybersecurity/gca/cop/meetings/june-tokyo/programme.html
[189] T. a. I. G. o. J. Ministry of Internal Affairs and Communications Ministry of Economy. (2009, Aug). *Workshop on Initiatives in Promoting Safer Internet Environment for Children*. Available: http://www.oecd.org/sti/ieconomy/43511802.pdf
[190] EMA. (Aug). *Mobile Content Evaluation and Monitoring Association*. Available: http://www.ema.or.jp/en/member_list_en.html
[191] JISPA. (Aug). *Japan Internet Safety Promotion Association* . Available: http://good-net.jp/english/

[192] G. o. Japan. (Sept). *Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children* Available: http://www.asianlii.org/jp/legis/laws/aopoartcpacpatpoc1999an52om2619991176/
[193] UK_Goverment, "Digital Britain," Department for Culture, Media and Sport and Department for Business, Innovation and Skills2009.
[194] U. Government. (29 Aug). *Centre for the Protection of the National Inferstructure* Available: http://www.cpni.gov.uk/about/cni/
[195] C. Office, "A Summary of the: Sector Resilience Plans for Critical Infrastructure 2010 / 2011," ed. London: Cabinet Office, 2011.
[196] M. J. West-Brown, D. Stikvoort, K.-P. Kossakowski, G. Killcrece, R. Ruefle, and M. Zajicek, *Handbook for Computer Security Incident Response Teams (CSIRTs)*. Pittsburgh, PA, 2003.
[197] U. _goverment. (2000, Sept). *Electronic Communications Act 2000*. Available: http://www.legislation.gov.uk/ukpga/2000/7/contents
[198] U. government ,2006) .Sept). *Police and Justice Act 2006*. Available: http://www.legislation.gov.uk/ukpga/2006/48/contents
[199] C. P. P. Act. (2001, Aug). *Governing pornography and child pornography on the Internet: The UK Approach*. Available: http://www.cyber-rights.org/documents/us_article.pdf
[200] U. government. (2003, Sept). *Sexual Offences Act 2003*. Available: http://www.legislation.gov.uk/ukpga/2003/42/contents
[201] E. commission, "A Digital Agenda for Europe " in *COM(2010) 245 final/2*, ed. Brussels: European commission, 2010.
[202] E. commission. (2012, Aug). *About our goals*. Available: https://ec.europa.eu/digital-agenda/node/1505
[203] C. o. t. e. communities, "Green paper on a european programme for critical infrastructure protection ", ed. Brussels: EU, 20.05
[204] E. States. (Sept). *Critical Infrastructure Warning Information Network*. Available: https://ciwin.europa.eu/Pages/Home.aspx
[205] E. States. (Sept). *European Network and Information Security Agency (ENISA)*. Available: www.enisa.europa.eu
[206] E .union. (2012, Sept). *The Protection of Childre n Online*. Available: http://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf
[207] D. P. Commissionor. (Aug). *EU Directive 95/46/EC - The Data Protection Directive*. Available: http://www.dataprotection.ie/docs/EU-Directive-95-46-EC/89.htm
[208] E. Union, "Directive 95/46/Ec of the European Parliment and the council of 24 october 1995," *official Journal of European communities*, 1995.
[209] E. commission, "Proposal for a regulation of the european parliament and of the council," Brussels25 Jan 2012.

[210] "Directive 1999/93/EC of the european parliament and of the council of 13 December 1999 on a Community framework for electronic signatures," *Official Journal of the European Communities*, 2000.
[211] Europa. (Aug). *Community framework for electronic signatures*. Available: http://europa.eu/legislation_summaries/information_society/other_policies/l24118_en.htm
[212] E. Union, "Directive 2009/136/ec of the european parliament and of the council of 25 November 2009," *Official Journal of the European Union*, 2009.
[213] EUROPA. (Aug). *Data protection in the electronic communications sector*. Available: http://europa.eu/legislation_summaries/information_society/legislative_framework/l24120_en.htm#amendingact
[214] E. Union. (2007). *Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community CIG 14/07* Available: http://www.consilium.europa.eu/uedocs/cmsUpload/cg00014.en07.pdf
[215] e. union, "Directive 2006/24/EC of the european parliament and of the council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications ervices or of public communications networks and amending Directive 2002/58/EC," *Official Journal of the European Union*, 2006.
[216] L. Feiler. (2008, Aug). *The Data Retention Directive*. Available: http://rechtsprobleme.at/doks/feiler-DataRetentionDirective.pdf
[217] E. Union, "COUNCIL FRAMEWORK DECISION 2005/222/JHA of 24 February 2005 on attacks against information systems," *Official Journal of the European Union*, 2005.
[218] E. union. (2003, Aug). *Council framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography* Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004F0068:EN:HTML
[219] C. o. Europe. (2007, Aug). *Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*. Available: http//:conventions.coe.int/Treaty/EN/treaties/Html/201.htm
[220] E. Union, "Council decision of 29 May 2000 to combat child pornography on the Internet," *Official Journal of the European Communities*, 2000.

ISBN 978-99942-75-93-9 ردمك