

أهمية حماية المعلومات في ظل تصاعد هجمات القرصنة الإلكترونية:
دراسة ميدانية في المملكة العربية السعودية

Significance of Information Protection in the Face of Escalation
of Electronic Piracy Attacks: A field study in Saudi Arabia

إعداد الدراسة:

سلي محمد الخياط ٢٠٢١٢٠٠٥١٩٢ - قائد الفريق

٢٠٢٢٢٠٠٥٦٧٧	سعد محمد الشهراني	٢٠٢٢٢٠٠٦١٢٢	فارس راشد الزهراني
٢٠٢٢٢٠٠٥٥٧٩	محمد عبد الرحمن العضياني	٢٠٢٢٢٠٠٦١٤٧	حسن عمر الزبيدي
٢٠٢١٢٠٠٥١٣٧	خالد محمد حكيم	٢٠٢٢٢٠٠٦١٨٧	ماجد عوض السرحاني
٢٠٢٢٢٠٠٦٢٣٠	عبد الله محمد الفضلي	٢٠٢٢٢٠٠٥٧٢٠	جمانه هاني المتروك

منصور عبد الله الزامل ٢٠٢٢٢٠٠٦٠٨٢

إشراف:

د. وليد سليمان

الفصل الدراسي الثالث

الإهداء والشكر

نهندي ثمرة جهدنا المتواضع الى دوحة الأمل والحياة، ومن علمونا أن نرتقي سلم الحياة بحكمة

وصبر، برا واحسانا ووفاء لهم، والدينا الغاليين،

والى العقد المتين الى من كانوا عوناً لنا في رحلة بحثنا،

كما نحمد الله رب العالمين الذي خلق وهدى وسدد الخطى، فخرج هذا العمل بعونه وتوفيقه،

نحمده حمدا كثيرا في المبتدئ والمنتهى، ونتقدم بالشكر الجزيل والعرفان بالجميل لمشرفنا

الفاضل د/ وليد سليمان، حفظه الله،

الذي تشرفنا بإشرافه على هذا البحث، وكانت لملاحظاته القيمة وتوجيهاته السديدة وأخلاقه

الفاضلة ومعاملته الكريمة الأثر الكبير في وصول البحث الى هذه الصورة فله عظيم شكرنا

وتقديرنا وجزاه الله عنا خير الجزاء،

المستخلص

تشمل المعلومات المطلوب حمايتها مجالات واسعة، ومع ذلك تحتل المعلومات المرتبطة بالقطاعات الحكومية والمرتبطة كذلك بالقطاع الخاص أهمية خاصة كونها تتناول العديد من المجالات الحيوية والهامة في الدولة. وقد تأثر أمن المعلومات بالتطور التقني المتسارع للحاسب الآلي، والبرامج حيث واكب ذلك تطوراً موازياً في جرائم المعلومات وفي عمليات الاختراق والقرصنة. لذا كان الهدف من هذه الدراسة تحديد مدى أهمية حماية المعلومات في ظل تصاعد هجمات القرصنة الإلكترونية من خلال دراسة أمن المعلومات في ظل تطور التقنية الرقمية، والتعرف على القرصنة الإلكترونية وتأثيراتها. وتحديد التأثيرات الاقتصادية والعسكرية والسياسية التي قد تنشئ عن القرصنة الإلكترونية وسبل حماية البيانات والمعلومات المتعلقة بهذه القطاعات. وكذلك تحديد التشريعات والتنظيمات والضوابط التي سنتها المملكة العربية السعودية للحد من أضرار القرصنة الإلكترونية وتأثيراتها المدمرة اقتصادياً وسياسياً وعسكرياً. وقد جاءت النتائج مؤكدة لأهمية حماية المعلومات حيث ينبغي أن يكون هناك هيئة أو إدارة متخصصة تتولى مراقبة تنفيذ سياسات أمن المعلومات وتوفير وسائل الحماية المادية والتقنية الملائمة، وهو ما قامت المملكة العربية السعودية من خلال تأسيس وإنشاء الهيئة الوطنية للأمن السيبراني في العام ٢٠١٧م. والغرض من إنشاء هذه الهيئة حماية المصالح الوطنية الحيوية وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية وغير الحكومية. كما أكدت الدراسة تعدد طرق، وأساليب مكافحة جرائم المعلومات، تكشف عن خطورتها، وانتشارها، ومدى الجدية في مواجهتها.

Abstract

The information that needs to be protected covers a wide range of areas. However, the information that relates to the government and private sectors is of particular importance as it affects many vital and important areas of the country. Information security has been affected by the rapid technological development of computers and programs, as this has been accompanied by a parallel development of information crime, hacking and piracy. The objective of this study was therefore, to identify the importance of protecting information in the face of escalating electronic piracy attacks through examining information security in light of the development of digital technology and identifying electronic piracy and its impact. Identify the economic, military, and political implications that may arise from electronic piracy and ways to protect data and information in these areas. As well as define the laws, regulations and controls enacted by Saudi Arabia to limit the damage of electronic piracy and its destructive impact in economic, political, and military terms. The findings confirmed the importance of protecting information, as there should be a specialized body or department that monitors the implementation of information security policies and provides appropriate physical and technical means of protection which Saudi Arabia has done by establishing the National Cyber Security Authority. The purpose of establishing this authority is to protect vital national interests and national security, critical infrastructure, priority sectors, governmental and non-governmental services, and activities. The study also highlighted the diversity of methods and procedures used to combat information crime, revealing its seriousness, prevalence, and the extent to which it is taken seriously.

قائمة المحتويات

الإهداء والشكر.....	ب
قائمة المحتويات.....	هـ
قائمة الجداول.....	ز
المقدمة.....	١
الفصل الأول.....	٢
مشكلة الدراسة.....	٢
أهمية الدراسة.....	٢
الفصل الثاني: حماية المعلومات.....	٣
التمهيد.....	٣
تحديث القوانين المتعلقة بالقرصنة الإلكترونية.....	٣
الفصل الثالث: القرصنة الإلكترونية وعلاقته بحماية المعلومات.....	١١
التمهيد.....	١١
مفهوم القرصنة الإلكترونية.....	١١
تأثير القرصنة الإلكترونية على معلومات المؤسسات الحيوية للدولة.....	١٩
تأثير القرصنة الإلكترونية على الاقتصاد العالمي.....	٢٠
نظرة مستقبلية للقرصنة الإلكترونية في ظل التقدم التقني.....	٢٥
مستقبل العالم الأمني في ظل تصاعد عمليات القرصنة الإلكترونية.....	٢٧
الفصل الرابع: الإجراءات المنهجية للدراسة.....	٣٣
التمهيد.....	٣٣
منهج الدراسة.....	٣٣
أدوات الدراسة.....	٣٤
الأساليب الإحصائية المستخدمة.....	٣٤
الفصل الخامس: نتائج الدراسة الميدانية.....	٣٥

أولاً: البيانات الأولية.....	٣٥
ثانياً: تحليل بيانات المحور الأول – حماية المعلومات.....	٤٤
ثالثاً: تحليل بيانات المحور الثاني – القرصنة الإلكترونية.....	٤٦
رابعاً: تحليل بيانات المحور الثالث – صور الاختراقات.....	٤٨
الفصل السادس: تحليل النتائج والتصور المقترح.....	٥٠
المراجع العربية.....	٥٤
المراجع الأجنبية:.....	٥٦
ملاحق الدراسة.....	٥٧
ملخص الدراسة الإنجليزي - Summary.....	٦٦

قائمة الجداول

الجدول (١): الجنس.....	٣٥
الجدول (٢): العمر.....	٣٦
الجدول (٣): المسعى الوظيفي.....	٣٧
الجدول (٤): المؤهل العلمي.....	٣٨
الجدول (٥): الخبرات العملية.....	٣٩
الجدول (٦): مدى الاطلاع على استراتيجية الأمن السيبراني.....	٤٠
الجدول (٧): اسهام استراتيجية الأمن السيبراني في تحقيق التوجهات الحكومية وممكنات الحكومة الذكية.....	٤١
الجدول (٨): معدل ثبات فقرات المحور الأول- حماية المعلومات.....	٤٢
الجدول (٩): معدل ثبات فقرات المحور الثاني - القرصنة الإلكترونية.....	٤٢
الجدول (١٠): معدل ثبات الفقرات الخاصة - صور الاختراقات.....	٤٢
الجدول (١١): معدل ثبات فقرات الاستبيان ككل.....	٤٢
الجدول (١٢): معامل الارتباط بين محاور الدراسة.....	٤٣
الجدول (١٣): تحليل بيانات المحور الأول- حماية المعلومات.....	٤٤
الجدول (١٤): تحليل بيانات المحور الثاني - القرصنة الإلكترونية.....	٤٦
الجدول (١٥): تحليل بيانات المحور الثالث - صور الاختراقات.....	٤٨
الجدول (١٦): قدرة اللوائح والتشريعات المتعلقة بأمن المعلومات على معالجة التحديات والمخاطر الإلكترونية.....	٤٩

قائمة الأشكال

- الشكل (١): الجنس ٣٥
- الشكل (٢): العمر ٣٦
- الشكل (٣): المسعى الوظيفي ٣٧
- الشكل (٤): المؤهل العلمي ٣٨
- الجدول (٥): الخبرات العملية ٣٩
- الشكل (٦): مدى الاطلاع على استراتيجية الأمن السيبراني ٤٠
- الشكل (٧): اسهام أهداف استراتيجية الأمن السيبراني في تحقيق التوجهات الحكومية وممكنات الحكومة الذكية ٤١

قائمة الملاحق

ط	قائمة الملاحق
٥٧	استمارة الامتحان
٦٤	ملخص الدراسة العربي
٦٦	ملخص الدراسة الإنجليزي

المقدمة

إن قضية أمن وحماية المعلومات تعتبر من قضايا العصر الهامة نظراً لدورها الفاعل في تحقيق التنمية الاقتصادية والاجتماعية والإدارية والثقافية، حيث تعتمد عليها اغلب الاقتصادات سواء في الدول المتقدمة منها او الدول النامية بهدف تحسين الأداء، وخفض التكاليف، وتقديم أفضل الخدمات. وقد أصبحت المعلومات ثروة وطنية يجب الحفاظ عليها. ومع ازدياد أهمية هذه المعلومات ازدادت المخاطر التي تهددها، وتنوعت دوافع المجرمين تجاهها، وما يترتب عليها من تعرضها للخطر الجسيم. فالعديد من المعلومات والأنظمة والبنى التحتية المتصلة بالشبكات عرضة للخطر بين الحين والآخر، حيث تواجه بشتى انواع الخروقات، كما تتعرض لأنشطة إجرامية (هاكرز) تعطل خدماتها وتدمر ممتلكاتها، وتختلف هجمات الهاكرز من جهة لأخرى، ومن مكان لآخر ومن زمن الى زمن مستخدمة أدوات وآليات اختراق متجددة ومتطورة طول الوقت. لذلك تضافرت الجهود لمكافحة هذه الجرائم سواء التي تستهدف الحاسب الآلي وما يرتبط به من برامج، أو شبكة الإنترنت والأنظمة العاملة عليها، أو البريد الإلكتروني. وشملت اهم المخاطر او الجرائم التي تهدد امن المعلومات كالتلصص، وسرقة المعلومات، أو اعتراضها، وتشويهها، أو حتى تحويل مسارها. كما أصبح بالإمكان قرصنة هذه المعلومات واعتراضها، وكشف سريتها، مما يؤدي إلى خلق تحدٍ جديد أمام مختصي أمن المعلومات (الطاهري، ٢٠١٩).

ولقد شكلت التعاملات بالوسائل الإلكترونية قوة التطور في التبادل المعلوماتي بين الأفراد، والشركات، والجهات الحكومية. لذلك أصبحت حماية هذه الوسائل او المعلومات ضرورة من ضرورات التطور التقني في العصر الحديث. لذا سنحاول من خلال أطروحة (أهمية حماية المعلومات في ظل تصاعد هجمات القرصنة الإلكترونية) دراسة المخاطر على المعلومات والعمل لتحقيق أمنها خاصة في ظل تصاعد القرصنة الإلكترونية حاضراً ومستقبلاً، وازدياد وتيرة الهجمات السيبرانية في الآونة الأخيرة وما تسبب به من تأثيرات مدمره، أمنياً واقتصادياً، واستخدامها كذلك كأدوات إدارة حروب وصراعات المستقبل، بالنظر لما تتسم به من انخفاض في التكلفة، وصعوبة الجهات التي تقف ورائها. ولعل ما يفاقم من مخاطر هذه الهجمات هي العقوبات التي تحول دون تطبيق مبادئ القانون الدولي عليها، ما يجعل من الصعوبة معاقبة الجهات التي تقف ورائها.

الفصل الأول

مشكلة الدراسة

برزت في الآونة الأخيرة ظاهرة القرصنة الإلكترونية والتي تهدف بالأساس إلى الاستيلاء على المعلومات المهمة سواء بين الشركات المتنافسة أو بين الدول بعضها البعض، وتلك ظاهرة خطيرة يجب الحذر منها وخاصة في المؤسسات أو المنظمات الحيوية في الدولة التي تحتوي على معلومات خطيرة تمس أمن الدولة واستقرارها، ولذلك تكمن معضلة هذا البحث في (التعرف على أهمية حماية المعلومات في ظل تصاعد هجمات القرصنة الإلكترونية والتأثيرات المتعددة على المعلومات وخاصة في المؤسسات الحيوية والعلاقات بين الدول وسبل مكافحتها وما هو مستقبلها في ظل التقدم التقني).

أهمية الدراسة

تكمن الأهمية العلمية لهذه الدراسة في أنها إضافة معرفية من خلال تتبع الدراسات السابقة والمفاهيم والنظريات التي تناولت ظاهرة القرصنة الإلكترونية وأهمية حماية المعلومات ودوره في حماية المصلحة العامة ومصالح المستخدمين والمحافظة على سرية الاتصالات وأمن المعلومات، وفقاً لأعلى معايير الجودة والأمان. لذا يعتبر هذا البحث أداة قيمة للمؤسسات العامة والخاصة التي ترغب في تعزيز أمنها الإلكتروني وحماية المعلومات والحد من مخاطر القرصنة الإلكترونية التي قد تتعرض لها هذه القطاعات. كما تكمن أهمية هذا البحث في المساهمة في إيجاد طرق لمواجهة القرصنة الإلكترونية بطريقة أكثر فعالية، وفي التوعية المجتمعية حول أخطار استمرار القرصنة الإلكترونية في المستقبل بتهديد الإبداع والابتكار والسيطرة على معلومات وبيانات غاية في السرية قد تستخدم استخداماً سيئاً لتدمير دولة ما أو مجتمع معين. كما تكمن الأهمية العملية في أنها تسلط الضوء على أحد المواضيع الرئيسية المتمثل في حماية المعلومات للحد من القرصنة الإلكترونية في القطاعات الحكومية والخاصة للمملكة العربية السعودية. كما تسلط الضوء على جوانبه الإيجابية والمشكلات والتحديات التي تعترضه. وتعتبر هذه الدراسة ذات فوائد هائلة لهذه القطاعات المختلفة في المملكة العربية السعودية كونها تُوضح الدور الاستراتيجي لتطبيق استراتيجية أمن المعلومات في الحد من هجمات القرصنة الإلكترونية.

الفصل الثاني: حماية المعلومات

التمهيد

إن التأثيرات المتعددة للقرصنة الإلكترونية وهي التأثير على معلومات الدولة الحيوية، والتأثيرات الاقتصادية وأبرزنا التأثيرات على العلاقات بين الدول، ومن المعروف أن الحدود بين الجريمة والفعل غير الأخلاقي تبدو غير واضحة المعالم في بيئة الحاسب الآلي والإنترنت، وتميز وضبط هذه الحدود هو المسألة الجوهرية لتحديد قوة تأثير جرائم الكمبيوتر والإنترنت كالقرصنة الإلكترونية وخاصة مع شيوع استخدام الإنترنت وما حمله من أنشطة جديدة لا يزال الخلاف قائماً حول ما إذا كانت جريمة أم أنها مجرد ممارسة غير مقبولة كسلوك أخلاقي يتمثل في التجسس على الآخرين ومصالحهم لكنها لا ترقى إلى حد الجريمة. فعلى سبيل المثال، ثمة جدل واسع في هذه الأيام حول ما إذا كانت رسائل البريد الإلكتروني الإعلانية التي توجه بكميات كبيرة إلى المستخدم دون رغبته أو دون طلبها من قبيل ممارسة خاطئة أم فعلاً يوجب المساءلة، ومع استمرار التداعيات الخاصة بالقرصنة الإلكترونية والتي أصبحت شائعة بشكل كبير وأصبحت تؤثر على أمن الشركات من خلال الاطلاع على أسرار العمل أو المصالح برزت الحاجة إلى طرق لمواجهة تلك الظاهرة الخطيرة (حمد وأحمد، ٢٠١٦).

تحديث القوانين المتعلقة بالقرصنة الإلكترونية

حينما يتقدم المحتوى المعلوماتي للمجتمع وينتقل من الحالة الورقية التقليدية إلى الحالة الرقمية ويظل الواقع القانوني والتشريعي على حاله متخلفاً وعاجزاً عن استيعاب هذا التقدم فإن ذلك يشكل ولا ريب نقطة ضعف ويمكن أن تؤثر سلباً على المحتوى المعلوماتي المجتمعي بتفريعاته المختلفة ومن ثم على الأمن القومي، فالمجتمع الذي تلاحقه الجرائم المعلوماتية وهو غير مسلح بأدوات مقاومتها قد يجد نفسه في النهاية أمام قطاعات واسعة من الأفراد يتعرضون للتدمير المادي والمعنوي، ومؤسسات يهددها الانهيار واقتصاد تلاحقه خسائر بلا حصر ومجتمع تصوب نحوه سهام التفكك، (جوهرى وحسن، ٢٠١٩). وهذه ليست أفكاراً مرسلة بل واقعاً تؤكدته العديد من الإحصاءات والدراسات. ففي دراسة موسعة أجرتها شركة أي بي أم وهي الأولى في صناعة تكنولوجيا المعلومات عالمياً (وجد أن ٥٨ %) من مختلف المؤسسات من جميع أنحاء العالم

يعتقدون أن خسائر جرائم المعلوماتية تتعدى خسائر الجرائم المادية، وأظهر البحث أن خسائر الجرائم المعلوماتية تسبب بشكل رئيسي خسائر في إيرادات هذه المؤسسات، وخسارة العملاء الحاليين والمستقبليين، إلى جانب عدم إنتاجية الموظفين، وأن التهديد القادم من الأنظمة المعلوماتية غير المؤمنة في الدولة النامية خطر متنام أيضاً). وأن النسبة الأكبر من التهديدات المتعلقة بأمن المعلومات والجرائم المتصلة تأتي الآن من داخل المجتمعات والمؤسسات، وشيئاً فشيئاً تحول التحديث التشريعي إلى مطلب من متطلبات حماية أمن المعلومات وبالتالي الأمن القومي، وبات الفراغ أو الجمود التشريعي يشكل نقطة انكشاف وضعف للمحتوى المعلوماتي المجتمعي، لكن التشريعات والقوانين القديمة المنوط بها مواجهة الجرائم المعلوماتية وضبطها وتقليصها تعاني فراغاً واضحاً يشل حركة من يلاحقونها من رجال الشرطة والقانون ويشتت انتباه من يحققون فيها، وقد استحدث "الاتحاد الدولي للاتصالات" دليلاً إلكترونياً لتتبع المعايير الأمنية الخاصة بتكنولوجيا المعلومات والاتصالات لمكافحة الجريمة على الإنترنت، (ويعتمد على مفهوم أن تهض جهة مفردة بذلك التتبع، ما يمكن المعنيين من الرجوع إليها ومتابعتها بسهولة، ووصف الدليل بأنه "خريطة طريق" فيما يتعلق بمعايير الأمن الخاصة بتكنولوجيا المعلومات والاتصالات حيث يستطيع أن يلاحق المعلومات عن أحدث المعايير الأمنية المتجددة باستمرار، ثم يصحبها في قاعدة بيانات تُفتح أمام المعنيين، ما يُسهل مهمة البحث عن المعلومات المطلوبة، وفقاً للبيان الصحفي للاتحاد الدولي للاتصالات) وتم وضع الدليل بالتعاون المشترك بين "الاتحاد الدولي للاتصالات" و"الوكالة الأوروبية المختصة بأمن الشبكات والمعلومات" وأطراف دولية أخرى مهمة بشؤون الأمن المعلوماتي على شبكة الإنترنت، ويعرض الدليل أسماء المنظمات المعنية بتطوير المعايير وما تنشره من صيغ خاصة بأمن الإنترنت، ما يُجَنَّب تكرار الجهود، كما يسهل مهمة مهندسي أمن الشبكة الإلكترونية في كشف الثغرات التي تُمكن العابثين من تهديد أمنها، ويضم الدليل خمسة أقسام تُحدِّثُ بصفة مستمرة و تتناول منظمات تطوير المعايير الخاصة بتكنولوجيا المعلومات والاتصالات وأعمالها والصيغ المعتمدة لتلك المعايير وطرق إقرار الاتفاق على تلك المعايير، والحاجات المستقبلية. انظر نظم مكافحة جرائم المعلوماتية في المملكة العربية السعودية (التيامي، ٢٠٢١).

أ. مبررات سد الفراغ التشريعي

يتحدث القانونيون عن جملة من الأسباب التي يمكن اعتبارها من دواعي التغيير والتحديث في البيئة

القانونية والتشريعية، ومنها (سهولة إخفاء الجريمة، حيث إن الجرائم التي تقع على الحاسبات أو بواسطتها عبر الشبكات في أكثر صورها مستترة خفية لا يلاحظها المجني عليه غالباً أو يدري حتى بوقوعها، كما أن صعوبة الاهتداء إلى مرتكبي الجرائم الواقعة في ذلك السياق أو البحث عن دليل أو أثر تقليدي مثل المحررات المزورة في التزوير المادي، فعلى الإنترنت تتم جريمة التزوير دون تحديد شخص مرتكبها أو ضبط المحرر المزور)، كذلك تبرز طرق القراصنة من سهولة محو الدليل أو تدميره في زمن متناهي القصر، فضلاً عن سهولة تنصله من مسئولية هذا العمل حسبما تشهد بذلك وقائع عديدة مثل قيام الجاني بالتوجه إلى أي "مقهى إنترنت" والدخول على أحد المواقع وإرسال رسالة على البريد الإلكتروني لآخر تحوي عبارات سب وقذف ويقوم بمحو الدليل وإرجاع كل شيء كما كان عليه والانصراف) كذلك الضخامة البالغة لكم كبير من البيانات المتعين فحصها والإحجام عن الإبلاغ في مجتمع الأعمال مثل المصارف والبنوك ومؤسسات السمسرة حيث تخشى مجالس إدارتها عادة من أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القضائية حيالها إلى تضاؤل الثقة فيها من جانب المتعاملين معها، ويبرز أيضاً مشكلة نقص خبرة الشرطة وأجهزة الأمن وجهات الادعاء والقضاء.

ب. أبرز مظاهر الفراغ التشريعي

يمكن تلخيص مظاهر القصور التشريعي المختلفة التي تقف وراء حالة العجز الفاضح أمام

الجرائم المعلوماتية في النقاط التالية:

- (١) القصور في الإجراءات التشريعية المنظمة لعمل مقاهي الإنترنت والبرمجيات الصناعية ومقاييس إطلاق التقنية والقواعد التشريعية لنقل التكنولوجيا والتراخيص والاستثمار والضرائب وتنظيم حجية ومقبولية مستخرجات الحاسب ووسائل الإثبات التقنية والإثبات المدني وتنظيم الصور الإجرامية في ميدان الحاسب والإنترنت وتنظيم التجارة الإلكترونية، والتشريعات الضريبية التي تغطي المبادئ الخاصة بالضريبة في ميدان صناعة البرمجيات والأعمال على الإنترنت والتجارة الإلكترونية.
- (٢) انعدام وجود تصور واضح المعالم للقانون والقضاء تجاه جرائم الإنترنت لكونها من الجرائم الحديثة، وتلك مشكلة أكثر من كونها ظاهرة، ولانعدام وجود تقاليد بشأنها كما هو الشأن في الجرائم الأخرى

ويساعد على ذلك انعدام وجود مركزية وملكية عبر الإنترنت (القحطاني وآخرون، ٢٠١٤).

٣) المبدأ الأساسي الذي يحكم تطبيق القانون الجنائي هو إقليمية أو تطبيقه على نطاق محلي كمبدأ عريق له جذوره ومقوماته واستثناءاته لكن هذا المبدأ يعد محدوداً جداً بالنسبة للإنترنت لأن الجرائم المرتبطة بها عابرة للحدود.

٤) التشريعات العربية لم تعرف التفتيش واكتفت بالنص على أنه إجراء من إجراءات التحقيق وأن القواعد الشكلية الخاصة بالتفتيش لا تهدف إلى تحقيق مصلحة العدالة في ضمان صحة الإجراءات التي تتخذ لجمع الأدلة فحسب، وإنما تقيم بالإضافة إلى مقتضيات الإجراء سياجاً يحمي الحريات الفردية، وهناك قصور تشريعي في توضيح تفتيش أجهزة الحاسب وضبط المعلومات التي تحويها ومراقبة المعلومات في أثناء انتقالها كما إن الإجراءات الجنائية للجهات القائمة على التفتيش لا تحسم بوضوح مسألة ضبط برامج الحاسب والمعلومات الموجودة بالأجهزة وفقاً للشروط الخاصة بإجراءات التفتيش العادية (الشيتي، ٢٠١٩).

مما تقدم يتبين لنا كيف أن التشريعات ليست حاسمة في مسائل الاختراق الإلكتروني والقرصنة وذلك لاختلاف العمليات والأشخاص وعلى هذا فالشركات الكبرى عليها أن تبتكر في إيجاد حلول للاختراقات فعلى سبيل المثال، (مثال على ذلك تجربة (شركة أبل مآكنتوش) كبرى شركات الأجهزة الرقمية، في دراسة لحماية برامج الإنترنت إن خسائر الاقتصاد العالمي جراء قرصنة الإنترنت تصل إلى ما بين (٣٧٥- ٥٧٥) مليار دولار سنوياً، وتقدر اقتصاد الإنترنت بما بين تريليونين و(ثلاثة تريليونات دولار سنوياً)، وتتركز الأضرار الرئيسية لقرصنة الإنترنت في سرقة الحقوق الفكرية والجرائم المالية وسرقة المعلومات الخاصة بالشركات. وتشمل الخسارة التكلفة التي يتحملها مئات الملايين في العالم بسبب سرقة معلوماتهم الشخصية، (منهم أربعون مليوناً بالولايات المتحدة في العام الماضي، إضافة إلى سرقة حقوق الملكية الفكرية، وسرقة النقود والمعلومات الحساسة الخاصة بالشركات، والتكلفة التي تتحملها الشركات جراء التعافي من الأضرار. وذكرت الدراسة الخسارة في الوظائف التي تحملها الاقتصاد الأمريكي ربما تصل إلى فقدان خمسمائة ألف وظيفة). ويزداد الأمر تعقيداً بسبب خشية الشركات من الكشف عن جرائم قرصنة الإنترنت، ومن الشركات الأمريكية التي أعلنت عن تعرضها للقرصنة غوغل وفيسبوك وأبل ونيويورك تايمز. وتحمل الدول المتقدمة الكبرى النصيب الأكبر من خسائر قرصنة الإنترنت، وعلى رأسها

الولايات المتحدة والصين واليابان وألمانيا، ويقول مركز الدراسات الاستراتيجية والدولية (إن المعلومات التي يتم جمعها حول قرصنة الإنترنت غير كاملة بسبب عدم متابعة الكثير من الدول بصورة مستمرة عمليات القرصنة وعدم كشف الشركات عن ما تتعرض له من هجمات، ويوصي المركز بمواجهة القرصنة عن طريق تعاون دولي من خلال اتفاقية دولية لتطبيق القانون وتشديد العقوبات على جرائم القرصنة والتعاون مع منظمة التجارة العالمية، إضافة إلى تحديد الحكومات خسائر القرصنة وحصر الشركات المخاطر التي تواجهها، كما أن هناك مسؤولية تقع على المجتمعات للتصدي لهذه الجرائم، وتتمثل هذه المسؤولية في توعية الناس بمفهوم الجريمة الإلكترونية، (وأنها الخطر القادم والحرص على ألا يقعوا ضحية لها، يضاف إلى ذلك ضرورة التأكد من العناوين الإلكترونية التي تتطلب معلومات سرية خاصة كمعلومات البطاقة الائتمانية أو حساب البنك، ووضع أنظمة تشريعية متطورة لتنظيم البيئة القانونية والتنظيمية التي تخدم أمن تقنيات ونظم المعلومات، إلى جانب تطوير برمجيات أمنية ونظم تشغيل قوية تحد من الاختراقات الإلكترونية وبرمجيات الفيروسات وبرامج التجسس وذلك بشكل مستمر)

(١) اختيار برامج فعالة لمكافحة التجسس

إن حماية المعلومات أمر ليس بالصعب إذا تمت السيطرة عليه بشكل جيد وخاصة تلك المناطق التي يتسلل إليها القراصنة الإلكترونيين، وفيما يلي نوضح خطوات حماية المعلومات:

٣٦. البريد الإلكتروني: يعد البريد الإلكتروني أبرز الطرق للتسلل إلى الأجهزة المراد اختراقها ولذلك ينصح بالتالي:

(١) تثبيت برامج جيدة لمكافحة التجسس الإلكتروني الخاصة بالبريد الإلكتروني أمثلة على ذلك:

أ. مضاد الفيروسات القوي (Avast antivirus). الذي يقوم بتوفير الحماية الكاملة للهاتف والأجهزة

اللوحية من حيث مكافحة الفيروسات والبرمجيات الخبيثة.

ب. مضاد البرامج الخبيثة (Malware). يقوم أيضاً بالكشف وإزالة ملفات أحصنة طروادة، وبرنامج

(كاسبر سكاي) من أفضل البرامج للحماية من الفيروسات وملفات التجسس على الكمبيوتر والهواتف

في نفس الوقت،

ج. برنامج مضاد الاختيار (Norton antivirus). الذي يمتلك سمعة جيدة في الحماية من الفيروسات

ومكافحة الاختراق حيث هناك تاريخ كبير لهذه الشركة في مجال الحماية هذه الخبرة الكبيرة.

(٢) عدم فتح أي ملف مرفق مع رسالة من شخص مجهول، حتى وإن ظهر أنه ملف نصي أو صورة لا تحمل فيروس، لأنه يمكن التلاعب باسم الملف ليظهر الملف التنفيذي (Executable File) الذي يحمل فيروساً بمظهر ملف سليم يحمل صورة أو نصاً.

(٣) استخدام برنامج جدار الحماية لسد المنافذ غير الآمنة وتقليل الأخطار، مع تحديث جميع البرامج الخاصة (بالمتصفح الإنترنت، متصفح البريد الإلكتروني، المراسل الآتي، جدار الحماية، ونظام التشغيل (الويندوز) لتفادي الثغرات الأمنية المكتشفة بها (Kitsios, et al, 2022)

ب. تأمين وسائط التخزين: من المعلوم أن البيانات تحتاج إلى وسائل للحفظ، ولكن بطريقة خاصة سواء أكانت هذه المعلومات داخل وسائط التخزين الداخلية (مثل الأقراص الصلبة، الممغنطة، الضوئية إلخ) أو وسائط التخزين الخارجية أو ما يسمى شبكات التخزين، وبصفة عامة فإن أمن وسائط التخزين اكتسب أهمية عالية في السنوات الأخيرة، لذا يجب على المنشآت يجب أن تولي هذا الأمر مزيداً من العناية عند بناء مراكز معلومات جديدة أو عند التعامل مع وسائط التخزين الحالية. (حيث تتميز وسائط التخزين بتوزيع البيانات على عدة مراكز معلومات يتم الاتصال بتلك المعلومات عن بُعد، ومن أساسيات هذه البيئات وجود أدوات لمواجهة الكوارث، مثل تعدد نسخ البيانات. إلا أن هذه الأدوات أضافت نقاط ضعف للبيانات كما أوجبت وجود عدة مستويات من الأرقام السرية وعدة نقاط اتصال)، لذا يجب دراسة إجراءات الأمن في هذه البيانات ومن ثم تقويمها، لتدارك الثغرات الأمنية التي يمكن أن تكون محط اهتمام مسئول إداري أمن المعلومات (الشوابكة، ٢٠١٩).

ج. توفير مصدر احتياطي للطاقة الكهربائية. من ضمن البرامج المهمة في ضمان أمن أجهزة تقنية المعلومات (توفير مصدر احتياطي للطاقة الكهربائية؛ لذا يجب على مشغلي وإداري نظم المعلومات أن يكونوا على دراية وإدراك بأهمية وجود طاقة كهربائية مستمرة للأجهزة التي لا يمكن أن تقوم المنشأة بالعمل بدونها، ومن مصادر الطاقة الكهربائية، مزود الكهرباء المستمر ومولدات الطاقة الكهربائية الاحتياطية)

٢) مقترحات لحماية المعلومات من القرصنة الإلكترونية

إن أغلب دول العالم بما فيها الدول العربية ترفع حالياً شعار التحول إلى مجتمع المعلومات والمعرفة، وتنفذ خططاً واسعة النطاق لتحويل هذا الشعار إلى واقع، وفي خضم هذه الخطط يتم إنشاء سلاسل من قواعد البيانات القومية الكبرى، كما يجري تطوير شبكات الاتصالات ونشر الإنترنت عبر خطوط الاتصالات العادية والسريعة، وتتجه الأمور لتعميم خدمات نقل الصوت عبر بروتوكولات الإنترنت، وتنشط الدول في نشر مفاهيم وخدمات الحكومة الإلكترونية، وتصدر قوانين التوقيع الإلكتروني الذي يمهد الطريق صوب تفعيل أنشطة التجارة والأعمال الإلكترونية على نطاق واسع، وتتوسع في مبادرات توفير الحاسب لفئات المجتمع المختلفة بالمنازل والمدارس وللمهنيين، كما تتبنى عشرات من برامج التنمية المعلوماتية المتكاملة في مختلف الوزارات والهيئات والمؤسسات، كما أن تشييد بنية معلوماتية قومية واسعة المجال وتبني التوجه نحو مجتمع المعلومات نقل المجتمع والدولة والمؤسسات إلى مرمى المخاطر، وحتم عليها مواجهة التحديات الشاملة والواسعة النطاق في أمن المعلومات، بمعنى أن تحديات أمن المعلومات في مجتمع يمتلك بنية معلوماتية واسعة يجعله يواجه تهديدات في أمن المعلومات تتسم بالشمول والاتساع وعمق التأثير وتنوع الأدوات وتعدد مصادر الهجوم وأدواته وغزارة الأهداف التي تشكل إغراء ومناطق جذب لمن يستهدفونه (البابلي، ٢٠٢١)، ولذلك يجب العمل بهذه المقترحات التالية:

أ. أهمية إنشاء حماية خاصة قوية:

من الخطأ تخطيطياً وإدارياً أن تنشط أي دولة في تشييد بنية معلوماتية وطنية متعددة الأوجه والمستويات على هذا النحو ثم لا تطور سياسة أو استراتيجية وطنية لحماية هذه البنية وصيانة أمنها وأمن ما يتداول داخلها من بيانات ومعلومات، وتترك ذلك للتصرفات العفوية والمبادرات الفردية والمشروعات والخطط الجزئية المنفرطة التي تجري هنا أو هناك دون سياسة أو استراتيجية واضحة، فالبنية المعلوماتية الأساسية الشاملة تتطلب بالتبعية سياسة أمن معلوماتية شاملة، وليس هناك أدنى مبالغة في القول بأن المضي قدماً في تشييد بنية معلوماتية قومية ضخمة بلا استراتيجية أمنية شاملة وكافية يشكل خطراً جسيماً في مسيرة التنمية المعلوماتية، ويؤثر سلباً على الأمن الوطني، لأنه يجعل البنية المعلوماتية القومية وهي تتحول مع الزمن إلى مورد استراتيجي للدولة كياناً هشاً يمكن أن يتعرض لانكشاف أمني في كل أو بعض جوانبه.

ب. توقع المخاطر وإيجاد سبل مواجهتها:

بما أن مخاطر أمن المعلومات باتت ترقى إلى مستوى تهديد الأمن الوطني ككل، فإن وسائل المواجهة والحماية لا بد وأن تظل لها منظومة أمن وطني، لأنه من الخطأ أن تكون الأخطار والتهديدات شاملة وربما منسقة ومخططة أحيانا ثم تأتي سبل ووسائل مواجهتها جزئية وعفوية وخالية من التخطيط وتفتقر للتنسيق والرشد، وقد قدمت اليابان نموذجا لهذا المستوى من التعامل مع أمن المعلومات حينما أعلنت منذ أوائل (أكتوبر ٢٠٠٥ م) حيث البدء في تنفيذ برنامج شامل على مستوى مؤسسات وهيئات الدولة تعمل على تدريب مهندسين على صد عميات الاختراق والقرصنة الإلكترونية مثلما فعلت اليابان لحماية شركاتها الاقتصادية العملاقة.

ج. ابتكار وسائل جديدة متطورة للحد من القرصنة:

إن إدارة المعلومات المتداولة داخل البنية المعلوماتية الوطنية بما يدعم الأمن الوطني أمر يتطلب فهما ورؤية جديدة لأساليب ومناهج وأدوات تداول المعلومات بين أطراف المجتمع وبعضها البعض داخليا، وكذلك مناهج وأدوات وأساليب إدارة وتداول المعلومات بينها وبين الجهات الخارجية، كشركاء السياسة والتجارة والأعمال والتعليم والبحث العلمي وهذه قضية مهمة ومعقدة في آن معا، ولا يصح تركها لاجتهادات أفراد ومؤسسات وخبراء من هنا وهناك مهما علا شأنهم وتجاربهم وقدراتهم، بل تحتاج جهداً مؤسسياً لن يتحقق على النحو المطلوب إلا عندما تتبوأ قضية أمن المعلومات مكانها الصحيح كركيزة أساسية للأمن الوطني (دلالي، وبالبشير، ٢٠٢١).

د. توحيد المصطلحات في اللغة العربية:

حتى يمكن معالجة الكثير من الموضوعات المتعلقة بالتشريعات القانونية المطلوبة لمكافحة جرائم المعلومات. ومن خلال ما تقدم في هذا البحث يتضح لنا أن هناك تحد تقني كبير ضد القرصنة الإلكترونية الذين يهددون أمن المعلومات وخاصة الحيوية ويتمثل في ضعف البناء التحي المعلوماتي وانكشافه للتهديدات ووجود ثغرات أمنية كبيرة، حيث أن تعطيل النظم بفعل المخترقين وتخريب أو سرقة المعلومات يؤدي إلى اضطراب كبير في هيكل المعلومات، كما أن زيادة احتمالات وسهولة شن عمليات إرهابية معلوماتية لازالت قائمة وكبيره ولذلك كانت الحاجة إلى توفير الحماية لها، ومن ذلك سوف ننتقل إلى الفصل الرابع لتتعرف على نظرة مستقبلية للقرصنة الإلكترونية في ظل التقدم التقني، حيث التطرق إلى تحديات المجتمع المعلوماتي مستقبلاً،

مستقبل العالم الأمني في ظل تصاعد عمليات القرصنة الإلكترونية، مستقبل العالم الاقتصادي في استمرار
عملية القرصنة الإلكترونية.

الفصل الثالث: القرصنة الإلكترونية وعلاقته بحماية المعلومات

التمهيد

بعيداً عن ساحات المعارك حيث دوي المدافع وانفجارات القنابل وصوت الرصاص وتناثر الأشلاء وأساليب القتل البشعة، هناك ساحات معارك أخرى لا تقل ضراوة عن مثيلتها العسكرية لكنها لا تخلف جثثاً وإن كانت تخلف دماراً وخسائر مادية ومعنوية، إنها حروب الإنترنت حيث أشهرها حرب الهاكرز العظمى، فمثلما أدخل الحاسوب والإنترنت خدمات وتسهيلات جيدة للعالم إلا أنه أعطى عالم الجريمة أبعاداً جديدة فصار من الممكن ارتكاب جريمة اختراق أو سرقة أو تزوير عن بعد وأصبحت وسائل الأمن والحماية المحسوسة من حراسات وصناديق حفظ وأماكن تخزين لا تكفي وحدها لحماية المعلومات من اللصوص وظهرت الجرائم التي ترتكب باستخدام الحاسوب وشبكة الإنترنت ومن ذلك ظهرت القرصنة الإلكترونية حيث اختراق الأجهزة وسرقة المعلومات ومن خلال هذا الفصل سوف نتعرف على مفهوم القرصنة الإلكترونية، أهداف وطرق القرصنة الإلكترونية، مع التعرف على نماذج من عمليات القرصنة الإلكترونية (شلوش، ٢٠١٨).

مفهوم القرصنة الإلكترونية

القرصنة الإلكترونية بشكل عام هي الاختراق (القدرة على الوصول لهدف بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف، وحينما نتكلم عن الاختراق بشكل عام فنقصد بذلك قدرة المخترق على الدخول إلى جهاز شخص ما بغض النظر عن الأضرار التي قد يحدثها فحينما يستطيع الدخول إلى جهاز آخر فهو مخترق (Hacker)) (مصري، ٢٠٠٨). ويتضح ذلك أنه (عندما يقوم بحذف ملف أو تشغيل آخر أو جلب ثالث فهو مخرب (Cracker))، وهو الدخول على أجهزة الآخرين عنوة ودون رغبة منهم وحتى دون علم منهم بغض النظر عن الأضرار الجسيمة التي قد يحدثها سواء بأجهزتهم الشخصية أو بنفسياتهم عند سرقة ملفات تخصهم وحدهم فما الفرق هنا بين المخترق للأجهزة الشخصية والمقتحم للبيوت الآمنة المطمئنة (مصري، ٢٠٠٨). ومن القرصنة الإلكترونية (جرائم تدمير المواقع واختراق المواقع الرسمية أو الشخصية أو اختراق الأجهزة الشخصية واختراق البريد الإلكتروني للآخرين أو الاستيلاء عليه أو إغراقه والاستيلاء على اشتراكات الآخرين وأرقامهم السرية وإرسال الفيروسات وبرامج الاختراق والتجسس، ولعل جميع هذه الجرائم والأفعال مع اختلافها يجمعها أمر واحد وهو

كونها جميعاً تبدأ بانتهاك خصوصية الأشخاص وتضر مصالح الغير سواء كانوا مؤسسات عامة أو خاصة أو حيوية فهذا كله يعد من الجرائم الكبرى (المنشاوي، ٢٠٠٣). وللقراصنة مسميات متعددة تتمثل في:

ب) القبعات البيض

هم القراصنة الذين يعملون في المؤسسات الحكومية وشركات أمن المعلومات أو حتى منفردين لاكتشاف ثغرات البرامج والأجهزة والشبكات، والإبلاغ عنها من أجل سدها ومنع استغلالها من قبل المخترقين المجرمين. (وأشهر شخصية على مستوى العالم من هذا النوع هو الهاكر كيفن ميتنيك الذي اعتبرته وزارة العدل الأمريكية في يوم ما أكثر مجرم حاسوب مطلوب في تاريخ الولايات المتحدة" واعتقل وسجن أكثر من مرة قبل أن يتحول إلى هاكل أخلاقي ويصبح مستشاراً ومتحدثاً عاماً في أمن الحاسوب ومديراً لشركة "ميتنيك للاستشارات الأمنية"). وهناك القرصان أدريان لامو (المعروف باسم الهاكر المشرد) الذي كان يستخدم المقاهي والمكتبات ومقاهي الإنترنت أماكن لتنفيذ اختراقاته لمواقع إلكترونية لشركات شهيرة مثل نيويورك تايمز ومايكروسوفت وياهو، لكنه تحول أخيراً إلى مخترق أخلاقي ويعمل مستشاراً بأمن الحاسوب وساعد في تسليم سلطات الجيش الأمريكي برادلي مانغ المتهم بأنه مصدر تسريب فيديو غارة جوية على بغداد إلى موقع نشر الوثائق السرية الشهير ويكيليكس. ومن القراصنة البيض أيضاً ("ستيف وزنيك" الشريك المؤسس لشركة أبل الشهيرة، ولينوس تورفالدس مطور نظام التشغيل مفتوح المصدر "لينوكس"، وتيم بيرنرز-لي العقل المبدع وراء تطوير الشبكة العنكبوتية العالمية، وجولييان أسانج مؤسس موقع ويكيليكس) (Mokhor, et al, 2020).

ت) القبعات السود

هم النوع الشائع الذي تركز عليه عادة وسائل الإعلام، ويخترقون أمن الحاسوب من أجل مكاسب شخصية مثل سرقة بيانات بطاقات الائتمان أو البيانات الشخصية من أجل بيعها، أو حتى من أجل المتعة الذاتية مثل صنع روبوتات برمجية (بوتنت) يمكن استخدامها لشن هجمات الحرمان من الخدمة الموزعة ضد مواقع إلكترونية معينة. ومن أشهر هؤلاء القراصنة البريطاني غاري مكينون المتهم بتنفيذ أكبر عمليات اختراق ضد شبكات حواسيب حكومة الولايات المتحدة من بينها أنظمة حواسيب الجيش والقوات الجوية

والبحرية وإدارة الطيران والفضاء (ناسا) تسببت بأضرار لأنظمة الجيش (قدرت بسبعمئة ألف دولار) وإلى جانب مكينون، هناك جونثان جيمز (المعروف باسم كومريد) الذي اخترق وهو في الـ(١٥) عاماً من عمره شبكة ناسا ووزارة الدفاع الأميركية. (جورج هوتز الذي يعرف بكونه مخترق منصة ألعاب سوني بلايستيشن عام (٢٠١١م) وكيفين بولسون (المعروف باسم دارك دانتي) وهو أحد قراصنة الثمانينيات ذوي القبعات السود، واكتسب سمعته تلك لاختراقه خطوط الهاتف لمحطة إذاعة في لوس أنجلوس للفوز بجائزة كانت عبارة عن سيارة بورش (٩١١) جديدة من ضمن جوائز أخرى)، وهناك ألبرت غونزاليس (الذي اتهم بأنه العقل المدبر في أكبر سرقة لأجهزة الصراف الآلي وبطاقات الائتمان بالتاريخ، حيث يعتقد أنه وجماعته من القراصنة باعوا خلال الفترة من (٢٠٠٥ م) إلى (٢٠٠٧م) أكثر من (١٧٠) مليوناً من أرقام بطاقات الصراف الآلي وبطاقات الائتمان. والروسي فلاديمير ليفين الذي تمكن عام (١٩٩٤م) مستخدماً حاسوبه المحمول في شقته بمدينة سانت بطرسبرغ من تحويل عشرة ملايين دولار من حسابات عملاء في بنك "سيتي بانك" إلى حساباته الشخصية حول العالم)، وبعد اعتقاله تمت استعادة المال المسروق باستثناء أربعمئة ألف دولار. (وهناك روبرت تابان مورييس الذي أطلق في الثاني من (نوفمبر ١٩٨٨م) دودة حاسوب (برمجية خبيثة) عطلت نحو عُشر الإنترنت وأكثر من ستة آلاف نظام حاسوب، وقدرت قيمة الخسائر المالية لهذه العملية بنحو (١٥) مليون دولار) (عزت، ٢٠١٨).

ث) القبعات الرمادية

هم القراصنة الذين يقومون بأعمال قانونية، أو بمساعدة أمنية كما يملئ عليهم ضميرهم أحياناً، أو باختراق مؤذ في أحيان أخرى، وهم كذلك مزيج من القراصنة ذوي القبعات البيض وذوي القبعات السود، وهم عادة لا يخترقون لأغراض خبيثة أو لمصلحة شخصية، بل لزيادة خبراتهم في الاختراق واكتشاف الثغرات الأمنية.

١) أهداف وطرق القرصنة الإلكترونية

إن القرصنة الإلكترونية لم تأت إلا بأهداف وطرق محددة يسير عليها القراصنة نستوضحها مما يلي:

٣٦. أهداف القرصنة الإلكترونية:

للقرصنة الإلكترونية عدة أهداف تتلخص فيما يلي:

(١) أهداف سياسية وعسكرية. لقد أحدث التطور العلمي في مجال الحاسبات الآلية طفرة كبيرة في المجال التقني والمعلوماتي (فمنذ الحرب الباردة والصراع المعلوماتي والتجسس بين الدولتين العظمى على أشده ومع بروز مناطق جديدة للصراع في العالم وتغير الطبيعة المعلوماتية للأنظمة والدول أصبح الاعتماد كلياً على الحاسب الآلي وعن طريقه أصبح الاختراق للحصول على معلومات سياسية وعسكرية واقتصادية مسألة أكثر أهمية) (مصري، ٢٠٠٨).

(٢) أهداف تجارية. تمثل الأهداف التجارية حافزاً كبيراً للقرصنة الإلكترونية حيث الصراعات بين الشركات التجارية الكبرى مع بعضها البعض (وقد بينت الدراسات الحديثة أن عدداً من كبريات الشركات التجارية يجري عليها أكثر من خمسين محاولة للاختراق لشبكاتها كل يوم) (مصري، ٢٠٠٨).

(٣) أهداف فردية. تعد الأهداف الفردية هي الأخرى بمثابة منافسة بين الأفراد يستعرضون مهاراتهم ضد بعضهم البعض مثلها مثل المسابقات وقد بدأت أولى محاولات الاختراق الفردي بين طلاب الجامعات في الولايات المتحدة كنوع من التباهي بالنجاح في اختراق الأجهزة الشخصية لأصدقائهم ومعارفهم ما لبثت أن تحولت تلك الظاهرة إلى تحدي فيما بينهم في اختراق الأنظمة بالشركات ثم بمواقع الانترنت ولا يقتصر الدافع على الأفراد فقط)، كذلك وُجد أن هناك (مجموعات ونقابات أشبه ما تكون بالأندية وليست بذات أهداف تجارية، بعض الأفراد بشركات كبرى بالولايات المتحدة الأمريكية ممن كانوا يعملون مبرمجين ومحلي نظم تم تسريحهم من أعمالهم للفائض الزائد في العمالة فصبوا جم غضبهم على أنظمة شركاتهم السابقة مقتحميها ومخبرين لكل ما يقع عليه أيديهم من معلومات حساسة بقصد الانتقام).

ب. طرق القرصنة الإلكترونية:

لقد تم تقسيم طرق القرصنة الإلكترونية إلى ثلاثة أنواع تتمثل فيما يلي:

(١) اختراق المزودات والأجهزة الرئيسية المتحركة. حيث يتجه المخترق بشكل كبير إلى اختراق الجدران النارية التي عادة توضع لحمايتها (وغالباً ما يتم ذلك باستخدام المحاكاة (Spoofing) حيث أن حزم ال (IP) تحتوى على عناوين للمرسل والمرسل إليه وهذه العناوين ينظر إليها على أنها عناوين مقبولة وسارية المفعول من قبل البرامج وأجهزة الشبكة ومن خلال طريقة تعرف بمسارات المصدر (Routing source) فإن حزم ال (IP) قد تم إعطائها شكلاً تبدو معه وكأنها قادمة من كمبيوتر معين) (مصري، ٢٠٠٨). بينما هي في حقيقة الأمر ليست قادمة منه، ولكنها خادعة تخترق من يضغط عليها في الجهاز ويفتحها فهو بمثابة ملف تنفيذي يتجسس على صاحب الجهاز.

(٢) اختراق الأجهزة الشخصية والعبث بما تحويه من معلومات. وهي طريقة للأسف شائعة لسداحة أصحاب الأجهزة الشخصية من جانب ولسهولة تعلم برامج الاختراق وتعددتها من جانب آخر.

(٣) التعرض للبيانات أثناء انتقالها والتعرف على شفرتها أن كانت مشفرة. (وهذه الطريقة تستخدم في كشف أرقام بطاقات الائتمان وكشف الأرقام السرية للبطاقات البنكية (ATM) وفي هذا السياق نحذر هنا من أمرين لا يتم الاهتمام بهما بشكل جدي وهما عدم الكشف عن أرقام بطاقات الائتمان لمواقع التجارة الإلكترونية إلا بعد التأكد بالتزام تلك المواقع بمبدأ الأمان) من ناحية أخرى (فيقدر ما هو ذو أهمية أمنية عالية إلا أنه لا يؤخذ مأخذ الجد فالبعض عندما يستخدم بطاقات السحب الآلي من مكائن البنوك النقدية (ATM) لا ينظر خروج السند الصغير المرفق بعملية السحب أو انه يلقي به في أقرب سلة مهملات دون أن يكلف نفسه عناء تمزيقه جيداً) (مصري، ٢٠٠٨). ومن خلال النظر إلى ذات المستند سنجد أرقاماً تتكون من عدة خانات طويلة هي بالنسبة لنا ليست بذات أهمية (ولكننا سوف ندرك بأن تلك الأرقام ما هي في حقيقة الأمر إلا انعكاس للشريط المغنط الظاهر بالجهة الخلفية لبطاقة (ATM) وهذا الشريط هو حلقة الوصل بيننا وبين رصيدنا بالبنك الذي من خلاله تتم عملية السحب النقدي لأدركنا أهمية التخلص من المستند الصغير بطريقة مضمونة ونقصد بالضمان هنا عدم تركها لهاكرز محترف يمكنه استخراج رقم الحساب البنكي، بل والتعرف على الأرقام السرية للبطاقة البنكية (ATM).

٤. علاقة القرصنة الإلكترونية بالمعلومات. تعد المعلومات هي عنصر مهم في عمليات القرصنة حيث إن القرصنة أساساً تهدف إما للسيطرة على المعلومات سواء بتدميرها أو بالتعرف عليها وأصبحت بمثابة حرب بطريقة جديدة وأكثر تأثيراً من الحروب التقليدية، وسوف نستعرض ذلك كما يلي:

أ. اختراق سرية بطاقات الائتمان.

(١) حدثت عمليات سطو على بطاقات ائتمانية لشخصيات دولية بارزة، لكن في النهاية تسقط أقنعة اللصوص، ويتم تقديمهم للمحاكمة، (في أغلب الدول تتولي وزارة الداخلية، مهمة التصدي لعمليات القرصنة، والسطو على الحسابات المالية، وتحويل الأموال، والشراء الإلكتروني والجرائم كافة التي تقع بواسطة الإنترنت، عبر الاستعانة بأحدث الأجهزة والمعدات التكنولوجية المتطورة لكشف الجرائم، وضبط مرتكبها، سواء تم الاتصال بالإنترنت من خلال رقم الهاتف، أو لاسلكياً عبر القمر الصناعي، ومن خلال الدليل الرقمي للجهاز الحاسب المستخدم في تنفيذ الجريمة يتم ضبط الجناة) حيث أن (عمليات السطو الائتماني هذه لا تشكل ظاهرة في داخل الدولة، لكن (٩٩٪) من عمليات السطو على البيانات تتم خارج البلاد، أو عبر عصابات دولية أو من خلال مواقع محددة (إباحية أو غرف دردشة) يترادها ذوو الميول الإجرامية والإباحية، وتلتقي هذه الأفكار والميول، حيث يعرضون بيانات بطاقات الائتمان المسروقة للبيع، فيقوم البعض بشراء هذه البيانات، ثم استغلالها في الشراء الإلكتروني والتحويل غير المشروع للأموال).

(٢) مصر كانت مسرحاً لأخطر عمليات السطو المالي عبر الإنترنت، التي تمكنت الإدارة العامة للمعلومات والتوثيق بوزارة الداخلية من ضبطها (والبداية كانت بلاغاً تلقتة وزارة الداخلية المصرية من المباحث الفيدرالية الأمريكية بشأن إجراء تحويلات غير مشروعة للأموال من خلال أرقام تعريفية لبعض مستخدمي الإنترنت في مصر، وعلى الفور أصدر وزير الداخلية تعليماته بالتأكد من مصداقية البلاغ ومدي صدق ما تضمنه من معلومات، والعمل وفق الأطر الشرعية المتبعة في مصر، والسرية التامة في البحث والتحري، والحفاظ على سرية المعلومات والتحريات) وفي ذات السياق تم (التنسيق مع مختلف الأجهزة الفنية والرسمية في الدولة، وتبين بالبحث والتحري أن مرتكبي الواقعة هم (٢٤) شاباً من مركز دكرنس في المنصورة. واتسعت دائرة الاتهامات لتطال أكثر من (٥٠) شخصاً حتى الآن. وقد أحال النائب العام (٤٣) منهما إلى محكمة الجنايات أخيراً في هذه الواقعة، وقد تم

الحصول على البيانات كافة الخاصة بالواقعة من مزودي الخدمة الذين يلزمهم قانون الاتصالات بذلك في حالة ارتكاب جرائم الكترونية من خلالهم)، وقد ظهر من التحريات أن المتهمين (هم طلاب يترددون على المواقع الإباحية وغرف الدردشة، ويترددون على مقاهي الإنترنت، فالتقوا بشباب من الولايات المتحدة الأمريكية وعلى الإنترنت التقت المصالح، واتفق قراصنة أمريكا ودكرنس في المنصورة على إجراء تحويلات مالية غير مشروعة لكروت ائتمانية لمواطنين أمريكيين تم الحصول على بياناتها بالاحتيال، حيث كان يتم تحويل (٤٠٪) من المبالغ المسروقة إلى بنوك في الولايات المتحدة، وتحويل (٦٠٪) منها إلى مصر (حبيب، ٢٠٠٧).

ج. نماذج للحروب الإلكترونية بين الدول بطريقة القرصنة:

لقد مثلت القرصنة الإلكترونية عدة نماذج للحروب والصراع المعلوماتي بين الدول على سبيل المثال:

(١) في (يناير ٢٠١٠م) عطلت جماعة تطلق على نفسها اسم "الجيش الإيراني السيبراني" خدمة البحث على الإنترنت لمحرك البحث الصيني الشائع "بايدو"، وكان يتم تحويل مستخدمي محرك البحث إلى رسالة سياسية إيرانية، وكانت الجماعة ذاتها اخترقت "تويتر" في (ديسمبر ٢٠٠٩م) مع توجيه رسالة مشابهة.

(٢) في (أكتوبر ٢٠٠٩م) اكتشف فيروس "ستكسنت" وهو برمجية خبيثة معقدة مصممة لتعطيل أنظمة التحكم الصناعية من إنتاج سيمنز كالتى تستخدمها إيران وإندونيسيا إلى جانب دول أخرى، الأمر الذي أثار تكهنات بأنها سلاح إلكتروني حكومي استهدف برنامج إيران النووي.

(٣) في (يناير ٢٠١١م) أعلنت الحكومة الكندية تعرض وكالاتها لهجوم إلكتروني ضخم من بينها وكالة البحث والتطوير الدفاعي الكندية، وأجبرت الهجمات وزارة المالية ومجلس الخزانة الكنديين على فصل اتصالاتهما بالإنترنت. وفي (يوليو ٢٠١١م) أعلن نائب وزير الدفاع الأمريكي أن قراصنة إنترنت سرقوا (٢٤) ألف ملف من وزارة الدفاع في عملية واحدة خلال مارس/آذار، مضيفاً أن الوزارة تعتقد أن وراء الهجوم دولة وليس أفراداً أو مجموعة قراصنة.

(٤) في (أكتوبر ٢٠١٢م) اكتشفت شركة أمن المعلومات الروسية "كأبرشيك" هجوماً إلكترونياً عالمياً حمل اسم "أكتوبر الأحمر"، وقالت إنه يجري منذ عام (٢٠٠٧م) على الأقل ويعمل على جمع معلومات من سفارات وشركات

أبحاث ومؤسسات عسكرية وشركات طاقة وغيرها، مشيرة إلى أن أهداف الهجوم الرئيسية هي دول في أوروبا الشرقية ودول الاتحاد السوفياتي السابق وآسيا الوسطى، وبعض دول أوروبا الغربية وشمال أميركا.

(٥) في (إبريل ٢٠١٣م) مجموعة " أنونيموس " تشن هجوماً على مواقع إسرائيلية دعماً للأسرى والقضية الفلسطينية، وشملت القائمة مواقع البورصة الإسرائيلية، ورئيس الوزراء، ووزارة الدفاع، وموقع جهاز الأمن الداخلي (الشاباك)، والصناعات العسكرية الإسرائيلية، إضافة إلى موقع مكتب الإحصاء الرسمي، وموقع وزارة التربية والتعليم، وعشرات المواقع الأخرى وآلاف الحسابات الإسرائيلية على موقعي فيسبوك وتويتر، بالمقابل، أعلنت مجموعة قراصنة إسرائيليين أنها تمكنت من شن هجوم إلكتروني مضاد واختراق موقع "أنونيموس"، وهو ما أكدّه صبري صيدم مستشار الرئيس الفلسطيني لشؤون الاتصالات وتكنولوجيا المعلومات.

(٦) في (يناير ٢٠١٤م) اعترفت خدمة الاتصال المرئي "سكايب" بأنها تعرضت لاختراق، لكنها قالت إن بيانات المستخدمين لم تتضرر. جاء ذلك بعد يوم على إعلان الجيش السوري الإلكتروني المؤيد للرئيس بشار الأسد أنه تسلل إلى حسابات "سكايب" على مواقع للتواصل الاجتماعي.

(٧) في مارس (٢٠١٤م) هاجم مجموعة "ساير بيركوت" الأوكرانية تهاجم المواقع الإلكترونية لحلف الناتو، والمتحدثة باسم الحلف أونو لونغيكو تقول إن "الهجوم أدى إلى تعطيل مواقع الحلف لعدة ساعات"، كما قام قراصنة حاسوب يشنون هجوماً "عنيفاً" على موقع الرئاسة الروسية الجمعة، كما عطلوا العمل بموقع البنك المركزي الروسي وفقاً لما أعلنه المكتب الصحفي للكرملين. من خلال ما تقدم يتضح لنا أنه منذ توسع استخدام الكمبيوتر في الولايات المتحدة الأمريكية أولاً ثم في باقي أجزاء العالم والانتشار غير المسبوق للاتصالات، أصبحت المؤسسات الكبرى هدفاً لهجمات القراصنة بدوافع مختلفة، واستدعى ذلك الانتباه إلى القرصنة الإلكترونية وخاصة وأن الهجمات الإلكترونية تأتي على عدة أشكال وأن أكثرها فعالية هو أسلوب ابتدعه القرصان (الهاكرز)، ومن ذلك سوف ننتقل إلى الفصل الثاني والذي نتعرف من خلاله على تأثيرات القرصنة على المعلومات، حيث نتعرف على تأثير القرصنة الإلكترونية على معلومات المؤسسات الحيوية للدولة، تأثير القرصنة الإلكترونية على الاقتصاد العالمي، والتطرق إلى تأثيرات القرصنة الإلكترونية على العلاقات بين الدول.

تأثير القرصنة الإلكترونية على معلومات المؤسسات الحيوية للدولة

إن للقرصنة الإلكترونية تأثير كبير على مؤسسات الدولة ولاسيما الحيوية بحيث أن الاختراق قد يتسبب في الحصول على المعلومات السرية والتي لا يجب أن تكون معروفة ويكون ذلك من خلال ما يلي:

٣٧. اختراق الأجهزة الرئيسية

يتم اختراق الأجهزة الرئيسية للشركات والمؤسسات أو الجهات الحكومية باختراق (الجدران النارية) التي عادة توضع لحمايتها، (وغالباً ما يتم ذلك باستخدام المحاكاة (Spoofing) وهو مصطلح يُطلق على عملية انتحال شخصية للدخول إلى النظام، حيث إن حزم الـ (IP) تحتوي على عناوين للمرسل والمرسل إليه، وهذه العناوين ينظر إليها على أنها عناوين مقبولة وسارية المفعول من قبل البرامج وأجهزة الشبكة) ومن خلال طريقة تُعرف بمسارات المصدر (Source Routing) فإن حزم الـ (IP) قد تم إعطاؤها شكلاً تبدو معه وكأنها قادمة من كمبيوتر معين، (بينما هي في حقيقة الأمر ليست قادمة منه، وعلى ذلك فإن النظام إذا وثق بهوية عنوان مصدر الحزمة، فإنه يكون بذلك قد تم خداعه، واختراقه والحصول على كافة البيانات للمؤسسات الحيوية ومن ثم المساومة بها أو بيعها للدول الأعداء، ومثال هذه الطريقة مثل ما حدث مع شركة (Hotmail) عند اختراقها حيث نجح القراصنة في الوصول إلى معلومات النظام لاختراق الأجهزة الشخصية، والعبث بما تحويه من معلومات) وهي طريقة للأسف شائعة لعدم انتباه أصحاب الأجهزة الشخصية من جانب، ولسهولة تعلم برامج الاختراقات وتعددتها من جانب آخر. والتعرض للبيانات أثناء انتقالها والتعرف على شفرتها إن كانت مشفرة، وهذه الطريقة تستخدم في كشف أرقام بطاقات الائتمان وكشف الأرقام السرية للبطاقات البنكية أيضاً.

ب. أثر قدرة القراصنة من الحصول على المعلومات.

إن الوصول غير المصرح للمعلومات (السجلات) الحكومية الأمنية (تعد من الجرائم المعلوماتية، التي تستهدف المعلومات مباشرة، ومن أمثلة الوصول غير المصرح للسجلات الأمنية الاطلاع على السجلات الأمنية لأشخاص مطلوبين أمنياً، أو تزوير رخص قيادة السير، أو إصدار جوازات السفر، أو بطاقات الهوية، أو إلغاء المخالفات المرورية الخاصة بأشخاص معينين، أو الوصول إلى معلومات استخباراتية، أو ابتزاز أشخاص من الممكن أن يكونوا قيادات في مؤسسة حيوية (السرطان والمشهداني، ٢٠٠٨). ومن الجرائم التي تدخل ضمن هذا النوع، التطفل على أجهزة تقنية المعلومات بغرض الاكتشاف فقط، وفي هذه الحالة يكون غرض المتطفل النظر إلى المعلومات لإشباع غريزة الفضول فقط، ولكن هذا العمل يعتبر تعدياً على خصوصية الآخرين، لذا تعد من الجرائم التي تستحق العقاب. ومن الجرائم التي تقع ضمن هذا التصنيف، الدخول غير المصرح إلى مواقع الإنترنت وتعديل محتوياتها من بيانات وتصاميم. وفي جميع الحالات الإجرامية السابق ذكرها، يستعمل المجرم تقنية المعلومات للحصول على معلومات أو لتخريب نظم برامج التشغيل، ويعد مرتكباً للجريمة في هذه الحالة لأنه أعطى نفسه صلاحيات واسعة تخوله الوصول إلى المعلومات أو سرقتها والنظر إليها لاحقاً، ومما سبق يتضح لنا أن تأثير القرصنة الإلكترونية داخل (البنية المعلوماتية الوطنية) بما يدعم الأمن الوطني أمر يتطلب فهماً ورؤية جديدة لأساليب ومناهج وأدوات تداول المعلومات بين أطراف المجتمع وبعضها البعض داخلياً، وكذلك مناهج وأدوات وأساليب إدارة وتداول المعلومات بينها وبين الجهات الخارجية، كشركاء السياسة والتجارة والأعمال والتعليم والبحث العلمي والتصنيع، وهذه قضية مهمة ومعقدة، ولا يصح تركها لاجتهادات أفراد ومؤسسات وخبراء من هنا وهناك مهما علا شأنهم وتجاربهم وقدراتهم، بل تحتاج جهداً مؤسسياً لن يتحقق على النحو المطلوب إلا عندما تتبوأ قضية أمن المعلومات مكانها الصحيح كركيزة أساسية للأمن الوطني (العتيبي، ٢٠١٧).

تأثير القرصنة الإلكترونية على الاقتصاد العالمي

تشهد عمليات القرصنة الإلكترونية نشاطاً ملحوظاً في السنوات الأخيرة، على الرغم من الخطط المستمرة لكبرى شركات التأمين الإلكتروني للبرامج والمواقع الإلكترونية، حيث أصبحت القرصنة الإلكترونية

شبحا يدهام البنوك وشركات النفط على مستوى العالم، وتقدر خسائرها بمئات المليارات سنوياً، فمع تزايد نسبة الجرائم الإلكترونية وتنوع طرقها. حيث أنها تلحق خسائر مادية كبيرة وفادحة أكثر مما تسببه الجرائم التقليدية ليس فقط على مستوى الفرد بل تتعداه إلى مستوى المنظمات والجهات والمؤسسات وهذا بالطبع يؤثر بشكل سلبي على الاقتصاد حيث أن قطاع الاتصالات العالمي يواجه هجوماً شرساً من أشخاص أو مجموعات أو منظمات محترفة، وعلينا تدارك أن هدفها الرئيسي تحقيق ربح مادي، إضافة إلى أهداف أخرى، وذلك بالاستفادة من توسع استخدام الكمبيوتر والإنترنت، ويمكن حصرهم في مستويين (أولاً على مستوى الفرد؛ فقد أصبح الفرد ينجز تعاملاته ويدير أعماله وبحوثه ويتواصل مع العالم الخارجي بواسطة استخدام خدمات الاتصالات. في المقابل يتعرض هذا الفرد إلى بعض السلوكيات التي قد تصبح جريمة فيما لو تم التبليغ عنها، مثل سرقة الهوية الشخصية، زيادة الفواتير بتحويل فواتير المجرم للضحية، وعمليات احتيال، وسرقة بطاقة الانتماء الخاصة به، والابتزاز والتهديد، وتحويل أو نقل حسابه المصرفي (الحميدان، ٢٠١٣)، ونوضح تأثير القرصنة على الاقتصاد العالمي بشكل أكبر كما يلي:

٣٨. التأثير على مستوى الشركات:

إن الجرائم الإلكترونية تؤثر على الجانب المادي من الشركات من خلال:

- (١) الاطلاع على معلومات سرية لصفقة أو مناقصة أو أمور تسويقية خاصة والاستفادة منها.
- (٢) العبث بمخازن المعلومات الخاصة بالشركة بحذفها أو تعديلها أو تعطيل الوصول إليها.
- (٣) سرقة الأموال وتحويل حسابات مصرفية خاصة بالشركة.
- (٤) الغش في المعاملات الإلكترونية كالتغيير في المبيعات.
- (٥) عمليات الاحتيال.
- (٦) التهديد والابتزاز.
- (٧) اختراق الموقع الإلكتروني الخاص بالشركة.

ب. التأثيرات على البنوك:

تؤثر الجرائم الإلكترونية على البنوك من خلال:

(١) السطو الإلكتروني.

(٢) العبث بمخازن المعلومات الخاصة بالبنك بحذفها أو تعديلها أو تعطيل الوصول إليها.

(٣) نقل ملكية الأسهم.

(٤) اختراق الموقع الإلكتروني الخاص بالبنك.

ج. التأثيرات على المنظمات والمؤسسات والتي تؤثر على الجانب المادي لديهما:

(١) الاطلاع على معلومات سرية والاستفادة منها.

(٢) العبث بمخازن المعلومات الخاصة بالمنظمة، أو المؤسسة بحذفها، أو تعديلها، أو تعطيل الوصول إليها.

(٣) سرقة الأموال وتحويل الحسابات المصرفية الخاصة بالمنظمة أو المؤسس.

(٤) عمليات الاحتيال.

(٥) الابتزاز والتهديد.

(٦) اختراق الموقع الإلكتروني الخاص بالمنظمة أو المؤسسة.

ولقد باتت مشكلة الاختراق أكثر خطورة على المنظمات والمؤسسات عند عمليات الشراء الإلكتروني عبر التجارة الإلكترونية عبر موقع الشركة أو المؤسسة الرسمي حيث يستطيع بعض المخترقين سرقة حسابات الفيزا كارت للمشارك والحصول منها على الأموال.

د. تكاليف خسائر العالم جراء القرصنة الإلكترونية:

إن الجرائم الإلكترونية المنظمة (تكبد الشركات حول العالم خسائر سنوية بقيمة (٨٠٠ مليار دولار أمريكي)، وذلك في مؤشر لارتفاع معدلات الهجمات الرقمية إلى مستويات غير مسبوقة بنسبة (٤٢%) خلال عام (٢٠١٤م) وتمثل تهديدات الأمن الإلكتروني أبرز التحديات لاقتصادات العالم التي تعتمد بشكل كبير على أحدث التقنيات، حيث أسهمت هذه التهديدات المعقدة بشكل كبير ومتسارع في تعزيز الطلب على أنظمة بنية تحتية عالية الحماية لأمن المعلومات) ومن المتوقع أن يصل حجم الإنفاق على قطاع تكنولوجيا المعلومات في منطقة الشرق الأوسط إلى (٢٣ مليار دولار) بمعدل نمو سنوي قدره (١٠%). بالمقابل (تفيد التقارير الحديثة بأن منطقة

الخليج العربي ليست بمنأى عن خطر الجرائم الإلكترونية حيث تكبد الاقتصاد الخليجي خسائر بقيمة (٨٥٠) مليون دولار، جراء قرصنة البرمجيات التي باتت تهديدا حقيقيا للهيئات الحكومية ومجتمع الأعمال على السواء، ويدرك خبراء تكنولوجيا المعلومات بأن الأمن الإلكتروني يعتبر أكثر تعقيداً من مجرد شراء برمجيات مكافحة الفيروسات، التي تشهد تحديثاً مستمراً، حيث أن الأمر يتطلب استراتيجيات متكاملة لحماية الشبكات ضد التهديدات الواقعية. وقد كبدت القرصنة الإلكترونية الشركات العالمية الكبيرة خسائر بمليارات الدولارات سنوياً، حيث يقوم القراصنة بسرقة الملكية الفكرية وخطط التطوير والأبحاث وبيعها لشركات منافسة، وكان (آخر هذه العمليات ما حدث مع (Sony Pictures) حيث قام الهاكرز بتسريب بعض الأفلام التي لم تعرض بعد، وكان من المتوقع أن تجني أرباحاً طائلة عند عرضها في دور السينما. وبحسب شركة فورستر الأميركية للأبحاث، فإن التجسس يكلف الشركات الأميركية نحو (٥٠٠) مليار دولار سنوياً، حيث يقوم القراصنة بسرقة الملكية الفكرية وخطط التطوير والأبحاث وبيعها لشركات منافسة مقابل ملايين الدولارات) وتزايدت حالات اختراق البيانات، (إضافة إلى سرقة وفقدان أكثر من ملياري سجل للبيانات على مستوى العالم منذ عام (٢٠١٣م)، كما أنفق بنك (JP Morgan) حوالي (٢٥٠) مليون دولار هذا العام للحماية ضد هجمات القرصنة. ويشير خبراء إلى سرقة أكثر من (٣٧٥) مليون سجل خاص بالعملاء في النصف الأول من عام (٢٠١٤م) على مستوى العالم، بزيادة نسبتها (٣١%) على أساس سنوي، وأعلن تقرير (صدر مؤخراً عن شركة كاسبرسكي المختصة في أمن البيانات، أنه تم سرقة أو التجسس على مديري تنفيذيين ومختصين أثناء سفرهم للاستثمار في آسيا خصوصاً.

هـ. القرصنة الإلكترونية من خلال التطبيقات المجهولة.

انتشرت بشدة التطبيقات التجارية المجهولة المصدر التي تنتشر عبر الجوال حيث هناك العديد من الافراد الذين لا ينتبهون إلى خطورة التطبيقات المجهولة المصدر والمقرصنة وغير الموثوق بها، ويتعاملون معها كأنها أمر عادي، (في حين أن مثل هؤلاء القراصنة ينتظرون فقط مجرد فتحهم لهذه التطبيقات واتصالهم بالإنترنت، ليقوموا بسحب كافة المعلومات الشخصية والحساسة من على الأجهزة الذكية، ما قد يتسبب فيما بعد بتهديدات تطالبهم وتعمل على حدوث مشاكل وخسائر اقتصادية كثيرة)، كذلك الامر بالنسبة للشركات التي لازالت لا تولي انتباها وتنفق مبالغ جيدة من أجل حماية أمن معلوماتها وبياناتها الدقيقة والحساسة. أن خطورة القرصنة

الإلكترونية تهدد كلاً من الأفراد والشركات وتلحق الكثير من الضرر والخسائر الاقتصادية وغيرها، كذلك تبرز مشكلة تجربة التسوق الإلكتروني عبر الجوال من خلال الهاتف الذكي والتي هي في تطور مستمر، ومع تطورها تتطور أساليب القرصنة الإلكترونية (Ramli & Wibowo, 2022).

٢) تأثيرات القرصنة الإلكترونية على العلاقات بين الدول

القرصنة الإلكترونية لا تؤثر على الشركات والأفراد أو حتى الاقتصاد فقط، بل باتت تهدد العلاقات بين الدول وتشعل حروب إلكترونية بينها، وسوف نوضح بعض النماذج من تلك الحروب كما يلي:

أ. حرب القرصنة الإلكترونية الصينية الأمريكية. شهدت العلاقات الصينية الأمريكية حرباً من نوع جديد حيث التجسس الصيني على الولايات المتحدة الأمريكية في مجال المعلومات من خلال عمليات القرصنة ونتعرف على بعض صور القرصنة الإلكترونية كما يلي:

(١) هجوم الصين على الشركات الأمريكية

ذكرت وكالة أسوشييتد برس الأمريكية في عددها الصادر في (١٢/٥/٢٠١١م) أن خبراء أمن الإنترنت الأمريكيين ذكروا بأن عمليات القرصنة التي تتعرض لها مواقع الشركات والهيئات الحكومية الأمريكية تعود إلى (١٢) مجموعة من القراصنة الصينيين، ويحصلون على "دعم أو أوامر من الحكومة الصينية، حيث أن القراصنة الصينيون يقومون بهجمات ذات طابع احتلالي وسري لسرقة حقوق الملكية الفكرية والوثائق الأمريكية التي لا تقدر بثمن، ويمكن للجانب الأمريكي أحياناً بناءً على بعض العلامات الواضحة تحديد مكان وهوية هؤلاء القراصنة، وقد أشار جهاز الاستخبارات الأمريكية إلى أن عمليات القرصنة الصادرة من الصين تتزايد بصفة مستمرة، لكن من الصعب جداً توفير الدلائل على ذلك، ومع ذلك لا تريد الحكومة الأمريكية ربط عمليات القرصنة مباشرة بالحكومة الصينية. لكن المسؤولين والخبراء يشيرون في الخفاء إلى أنهم متأكدون من أن القراصنة على علاقة بالحكومة الصينية أو الجيش الصيني. وينتقد بعض خبراء أمن الإنترنت تهاون الحكومة الأمريكية في القيام بمزيد من الضغط على الصين لإجبارها على ملاحقة هؤلاء القراصنة وأن هذا يعتبر "تهديداً متصاعداً للأمن الاقتصادي الأمريكي".

ب. القرصنة الإلكترونية الإيرانية على الولايات المتحدة الأمريكية

زعمت الولايات المتحدة الأمريكية عام (٢٠١٢م) (أن قرصنة إيرانيين وراء هجوم إلكتروني استهدف أجهزة الكمبيوتر الخاصة بالبنوك الأمريكية، ومن المعروف أن إيران نفذت سلسلة من الهجمات الإلكترونية ضد أمريكا في السنوات الأخيرة، مما جعل أوباما يصدر قوانين جديدة تتيح لأمريكا وضع عقوبات اقتصادية على الدولة، التي تقدم على القرصنة الإلكترونية ضد مصالح الولايات المتحدة الأمريكية)، وكان رئيس جهاز الاستخبارات الأمريكي "جيمس كلابر" قد (أدان إيران على هجوم إلكتروني تعرضت له إحدى الشركات الأمريكية الكبرى وتدعى (Sands Casino) موضحاً أن إيران طورت قدراتها على القرصنة الإلكترونية في فترة وجيزة لم تتخطى العامين، وكان الجنرال الإيراني/ محمد أفاكيشي قد صرح رداً على التهديدات الأمريكية بشن حرب إلكترونية واسعة المدى ضد إيران، علماً بأن إيران جاهزة لمثل تلك الحرب ولديها الإمكانيات التكنولوجية، التي تجعلها ندا لواشنطن) ويرى بعض المحللين (أن حدة الهجمات الإيرانية الإلكترونية سوف تقل في الفترة القادمة خاصة بعد الاتفاق المبدئي، الذي ينص على رفع العقوبات الاقتصادية عن إيران تدريجياً، وهي العقوبات التي كانت دافعاً لهجمات إيران الإلكترونية كوسيلة ضغط وانتقام ضد الولايات المتحدة) ومن خلال ما تقدم في هذا البحث يتضح لنا مخاطر تأثير القرصنة الإلكترونية على العالم أجمع فهي حرب جديدة أخطر من الحرب التقليدية ولذلك يجب العمل على التأمين الجيد وخاصة في المؤسسات الحيوية والمصالح التجارية الكبرى، ومن ذلك سوف ننقل إلى الفصل الثالث للتعرف على طرق ووسائل حماية المعلومات من القرصنة الإلكترونية من خلال تحديث القوانين المتعلقة بالقرصنة الإلكترونية، اختيار برامج فعالة لمكافحة التجسس، مع بعض مقترحات للباحث لحماية المعلومات من القرصنة الإلكترونية

نظرة مستقبلية للقرصنة الإلكترونية في ظل التقدم التقني

بما أننا نعيش حالياً في عصر المعلومات والذي تنفذ فيه الدول خططاً واسعة النطاق لإنشاء سلاسل من قواعد البيانات الكبرى، في ظل واقع يفرض عليها تطوير شبكات الاتصال ونشر الإنترنت عبر خطوط الاتصالات العادية والسريعة والاتجاه لتعميم خدمات نقل الصوت عبر بروتوكولات الإنترنت وتنشط الدول في نشر مفاهيم وخدمات الحكومة الإلكترونية وتصدر قوانين التوقيع الإلكتروني الذي يمهد الطريق صوف تفعيل أنشطة

التجارة والأعمال الإلكترونية على نطاق واسع هذا غير تبني عشرات من برامج التنمية المعلوماتية المتكاملة في مختلف الوزارات والهيئات والمؤسسات، ولذلك كان هناك أهمية كبرى للحفاظ على السير في هذه التطورات التكنولوجية الجديدة ولهذا برزت الحاجة إلى استشراف مستقبل القرصنة الإلكترونية التي تهدد ذلك التقدم والتطور التكنولوجي من خلال التعرف على تحديات المجتمع المعلوماتي، مستقبل العالم الأمني والاقتصادي في ظل تصاعد عمليات القرصنة الإلكترونية.

لقد أدت ثورة المعلومات إلى ظهور أنماط جديدة من التحديات الأمنية. ولقد ظهرت تحديات جديدة للأمن بمفهومه التقليدي، هذه التحديات تتعلق بالاستعدادات اللازمة للتعامل مع المستجدات والمهددات الأمنية. ففي السابق كان من السهل على الدول إغلاق حدودها والتشويش على جيرانها وعدم استقبال بثهم التلفزيوني، ومنع الاتصالات معهم، وكانت غالبية المهددات الخارجية تأتي من دول الجوار لخلافات حدودية، أو أطماع في المصادر الوطنية، أو بسبب تحالفات عسكرية معينة. أما في المجتمع المعلوماتي فلم يعد بالضرورة أن تكون الدول متجاورة لكي تهدد بعضها أمنياً، فتطور نظم السلاح الذي يمكنه من الوصول لمسافات بعيدة، واستخدام تقنيات بسيطة لتدمير البناء المعلوماتي للدولة وتخريب نظمها الإدارية والعسكرية جعل حرب المعلومات حرب الجميع، وجيشها الجميع صغاراً وكباراً، هواة أو قراصنة أفراداً وجماعات. ويمكن القول إن الأمن في المجتمع المعلوماتي ما هو إلا نتيجة طبيعية لتطور المجتمع والانتقال إلى عصر التطور التكنولوجية الرقمية في التعامل بين الدول وبعضها البعض، إلا أنه يمكن القول إن سرعة انتقال التقنيات بين الدول، وتوافر البنية التحتية المعلوماتية الأساسية قد سرع في انتقال المجتمعات النامية إلى المجتمع المعلوماتي على الرغم من أنها غير منتجة تقنياً لهذه المعدات، ومتخلفة معلوماتياً. أصبحت المشاركة الدولية في كل شيء، في الحدود، والاقتصاد، والفضاء، والثقافة، الطعام، وفي التهديدات الأمنية كذلك، هناك مجموعة من التحديات التي نجمت عن المجتمع المعلوماتي منها التحديات على المستوى العالمي (محمود وكيطان، ٢٠٢١). والتحديات على المستوى الوطني، وذلك على النحو التالي:

٣٩. التحديات العالمية:

تشمل التحديات العالمية ما يلي:

(١) التحديات السياسية. إن الحاجة للمعلومة حاجة قوية، والقوة هذه ذات تأثير في القرار السياسي في أي مجتمع. فمن يملك المعلومة يملك القوة التي تؤثر على صانع القرار السياسي في أي مجتمع إن كان بحاجة إلى تلك المعلومة.

(٢) التحديات الاقتصادية. إن نقص الموارد الاقتصادية يعني الحاجة إلى المعلومات التي تطور اقتصاديات الدول، وحاجاتها المستقبلية، فتطوير صناعة الأسماك، والزراعة... إلخ. كل هذه التقنيات ذات تأثير في القطاع الاقتصادي للدولة.

(٣) التحديات التقنية (التكنولوجيا). هناك تحد تقني يتمثل بحاجة الدول والمجتمعات إلى المعدات والبرمجيات، وإلى تطوير إمكانياتها الذاتية في هذا المجال، وهذا التطوير بحاجة إلى المساعدة الفنية والاقتصادية الخارجية.

(٤) التحدي الأمني. ويتمثل في ضعف البناء التحتي المعلوماتي وانكشافه للتحديات ووجود ثغرات أمنية كبيرة. إن تعطيل هذا البناء أو تخريبه أو التعدي عليه قد يؤدي إلى اضطراب كبير في عمليات التواصل في مجالات المال والأعمال والعلاقات الاجتماعية بين الافراد... إلخ. كما أن زيادة احتمالات وسهولة شن عمليات ارهابية معلوماتية لازالت قائمة وكبيره. وقد بدأ الميل نحو مفهوم دولي للأمن وذلك لأن العالم يشترك في البناء الفضائي العام (وهو مشاع) وفي البنية المعلوماتية التحتية (مثل الإنترنت) مما جعل مهددات الأمن عالمية وتتطلب حلولاً عالمية، فمثلاً فيروس معين يهدد كل المستخدمين في كل الدول، ومن الممكن أن يخرب النظم والمعلومات في أي دولة. وازدادت الشراكة الدولية في الأمن مما يستدعي مزيداً من العولمة للقوانين.

ب . التحديات الداخلية:

تشمل التحديات التالية:

تحدي التنمية والديمقراطية وحقوق الانسان. ويشمل: تحدي التخلف وضغوطات النمو التي تقع على كاهل المجتمع، والفقر والأمية، والجريمة، والمشكلات الاجتماعية، والفساد الإداري والسياسي تحد من فرص التطور

والانتقال إلى المجتمع المعلوماتي، فلا بد من تطور البنى الاجتماعية والاقتصادية حتى تتمكن المجتمعات من دخول المجتمع المعلوماتي بيسر.

التحدي البشري ونقص الكفاءات. إن نقص الكفاءات على مستوى القيادة والتقنية بسبب عدم التأهيل وهجرة العقول إلى الخارج ومنح الدول الأخرى فوائد علمهم ونبوغهم بسبب التقدير المادي والمعنوي الذي يحصلون عليه، الأمر الذي جعل التعامل مع العصر القادم في ظل مشكلات متعددة داخلية يشكل تحدياً كبيراً.

التحدي الثقافي. إن السير ومواكبة المجتمع المعلوماتي والتفوق التقني في أي بلد يجب أن يتوافق مع المكتسبات الثقافية للدولة بحيث يتلاءم مع العادات والتقاليد الخاصة بالدولة بمعنى لا يصح في المجتمع الخليجي المحافظ أن يتم الاستثمار الإلكتروني على سبيل المثال بالمتاجرة في القمار أو الدعارة كما تفعل بعض الدول الأخرى، ولذلك فإن اختيار التكنولوجيا المعلوماتية الرقمية يجب أن تلائم المعتقدات الدينية والثقافية للدولة.

التحديات التربوية. يمثل النظام التربوي التحدي الأهم، وذلك من خلال نقل المجتمعات إلى المجتمع المعلوماتي، فنظام التعليم لابد أن يبنى على أسس المعلوماتية وتحويله من الاعتماد على النظم التقليدية إلى تكوين بناء معلوماتي تقني متكامل يشمل ذلك مهارات التدريس والمناهج.

التحدي الأمني. يشكل الأمن أساس التنمية في الدولة حيث أن التحول للمجتمع المعلوماتي يتطلب استقرار أمنياً قبل وأثناء عمليات التحول لمجتمع المعلومات، وتبرز التحديات الأمنية من حيث الحرص على سلامة قواعد المعلومات الخاصة بالأفراد العاملين في المجالات الحيوية في الدولة مثل المؤسسة العسكرية والوزارات والهيئات، كذلك يشمل التحدي تسريب المعلومات الهامة التي تهدد أمن الأوطان مثل المعلومات السرية لدى القيادات سواء المدنية أو العسكرية والتي تُبنى عملية القرصنة الإلكترونية عليها.

مستقبل العالم الأمني في ظل تصاعد عمليات القرصنة الإلكترونية

إن مستقبل العالم الأمني في ظل تصاعد عمليات القرصنة الإلكترونية هو أمر غاية في الأهمية للدول يجب أن تحرص على استشرافه وذلك وفقاً للتوقعات المستقبلية التالية:

أ. قد يأتي اليوم الذي يصبح فيه كل جهاز، بل وكل عملية، مرتبطاً بالشبكة العالمية، وذلك بدوره ينقلنا إلى سؤال هام وهو: هل سيستطيع المتسلل إلكترونياً، والذي ربما يكون في الطرف الآخر من الكرة الأرضية، قادراً على تعطيل نظام أمن المطار، أو فتح البوابات في مجمع عسكري؟ هل يستطيعون إيقاف محرك سيارة تسير بسرعة (٢١٠ كلم) على الطريق السريع، وبالتالي تسبب اصطدام مئة سيارة تمشي خلفها، أو تغيير طريق السير على الطريق السريع؟ وهل سيستطيع اللصوص والمستأجرون للقتل تتبع حركة ضحيتهم من خلال صفحات مواقع الإنترنت بحيث توفر لهم صور الأماكن العامة أو تفاصيل البيوت من الداخل؟ ستصبح تقنيات المعلومات محمولة في جيوبنا وعلى أجسامنا على شكل "بطاقات ذكية" تحمل ضمنها معلومات شخصية عن كل شخص يحملها، وأجهزة الاتصالات المحمولة كالهاتف الجوال، والنداء، وخدمات البريد الإلكتروني، ومعدات الحقيقة التخيلية وأجهزة تحسين السمع وغير ذلك من الأجهزة الجسمية. ويقوم عمال في شركة بوينغ للطائرات في (أيفريت بواشنطن) باستخدام تجهيزات جاهزة التصنيع للحقيقة التجميعية. وتشمل كل بزة من هذه الملابس نطاقاً للخصر يشتمل على جهاز حاسب شخصي يعمل بموجب برنامج وندوز، وغطاء لرأس يشتمل على جهاز لتحديد الموقع وشاشة العرض. ويشتمل إعداد الجهاز على يد توجيه إلكترونية تخلص العامل من النظر إلى المخططات الورقية وقوائم الغيار. وفي هذا المجال أيضاً قدمت دراسة مستقبلية تتوقع أنه سيتم التعاون بين شركة سوني وشركات أخرى لإنتاج جهاز كمبيوتر عالي الطاقة يمكن ارتداؤه يسمى: "المساعد المتحرك". يمكن تشغيل هذا الجهاز الذي يبلغ وزنه كيلو جراماً واحداً فقط بالصوت، ويستخدم مع شاشة تحمل على الرأس، وبإمكان مستخدم هذا الجهاز إجراء مكالمات هاتفية، وإرسال فاكسات والاتصال مع شبكة الإنترنت.

ب. لقد أنشأت التقنية الحديثة للمعلومات العديد من الاحتمالات للهجمات المستخدمة في حرب المعلومات، ويمكن أن تحدث العمليات في أي لحظة، كما يمكن أن تنطلق من أي مكان في العالم. فيمكن إعداد هذه الهجمات وتنفيذها من مكان الاستمتاع والراحة في البيت، أو المكتب، ودون الحاجة إلى تكاليف الجواسيس، والاختراقات الفعلية والتعامل مع المتفجرات. كما أن عدد الأهداف التي يمكن الوصول إليها هو عدد مدهل. ويمكن أن يقوم بهذه العمليات ممثلون حكوميون أو غير حكوميين، ومن قبل الأفراد أو الجماعات. كما أن تكلفة هذه العمليات قد تكون تافهة تماماً، وأما الخسائر التي تلحق بالضحايا فهي موجعة. إن تمويل العمليات العسكرية العادية هو أمر مكلف. وقد تبلغ كلفة طائرة نفثة مقاتلة واحدة أكثر من مئة مليون دولار. ومن ناحية

أخرى، فهناك تكلفة أخرى لكل من شرائح الكمبيوتر، وخزانات الوقود، والأقمار الصناعية للتجسس والقوات المسلحة الهائلة. (وبالمقارنة فإن مبلغاً يتفاوت ما بين (١٠:١) ملايين دولار يمكن أن يكون مبلغاً مربحاً جداً لتمويل فريق حرب معلومات تقني برواتب مغرية، بحيث يتألف الفريق من (٢٠:١٠) من المتخصصين بعمليات التسلل عبر أجهزة الكمبيوتر وشبكاته باستخدام آخر ما توصلت إليه تقنية الحاسبات الآلية). كما يمكن تحميل الأدوات التي يستخدمها هذا الفريق الفني في أعمالهم التسللية إلى أجهزة الكمبيوتر وشبكاته مجاناً من مواقع مختلفة على الإنترنت في مختلف أرجاء العالم. ولكن، هل يستطيع هذا الفريق التقني المتخصص تحقيق الأهداف ذاتها التي تحققها القوات العسكرية المعروفة وتسبب استسلام العدو أو قبوله للأمور السياسية المفروضة. ومن المتوقع أن يأتي اليوم الذي تصبح فيه الجريمة "مؤتمتة"، حيث يستطيع الفرد تحميل البرنامج الذي يريده من الإنترنت أو يشتريه من موقع من مواقعها ويقوم البرنامج بمختلف الخطوات التي تنفذ الجريمة دون اسم المجرم أو عنوانه أو أية تفاصيل عنه، ثم يقوم البرنامج ذاته بعد ذلك بمسح كافة آثار الجريمة بحيث لا يبقى لها أثراً على الأجهزة التي دخل إليها للضحية). وإن مثل هذه البرامج التي يمكن تسميتها: "التزوير في اللعبة" يمكن أن تحمل عناوين مثل: "تزوير شيكات قوائم الرواتب"، أو "البريد للتخريب"، كما أن امتلاك برنامج من هذا النوع لتنفيذ الجرائم هو أمر قانوني، وأما استخدامه وتنفيذه فلن يكون قانونياً، إلا أن احتمال القبض على أمثال هؤلاء المجرمين بالجرم المشهود ومتلبسين بالجريمة يكون ضئيل الاحتمال جداً. وستكون هذه البرامج مؤتمتة وآلية في كل خطوة من خطوات العمل والتنفيذ بدءاً من اختيار الضحية إلى تنفيذ الجريمة وإزالة آثار العدوان والجريمة. ويمكن أن يتم تصميم أمثال هذه البرامج بحيث لا يعرف المجرم ضحيته، ولا يعرف نوع الجريمة التي سيتم ارتكابها بالتحديد، ولا الطريقة التي ستستخدم لارتكاب هذه الجريمة، وكل ما يعرفه أنه سيحصل على مبلغ مليون دولار مثلاً، يوضع في حسابه البنكي خارج حدود البلد التي ينتمي إليها. كما يحتمل أن يشفر مطور البرنامج برنامجه بحيث يتجاوز كافة قوانين العقوبات على الجرائم، وقواعد تحري آثار الجريمة واكتشافها، والإجراءات القانونية التابعة لذلك.

ج. إن ما جلبته التقنية الحديثة هو مزيد من الخيارات والفرص لإجراء حروب معلومات. فهناك المزيد من الوسائل التي يمكن استغلالها في عمليات التخريب، وإلحاق الأضرار والأذى المتعمد والحرب

النفسية، وهناك المزيد من مختلف أنواع مصادر المعلومات التي يمكن مهاجمتها، وهناك المزيد من الأدوات التي يمكن استخدامها لتنفيذ هجمات قاتلة على مصادر المعلومات. ومن الملاحظ أيضاً أن هناك ازدياداً في نسبة الاعتماد على التقنية في المجتمع، وتزداد بهذا إمكانية احتمالات حدوث خسائر من الهجمات التقنية. وهناك الأدوات الجديدة التي يمكن استخدامها في الدفاع أيضاً، ولكن نادراً ما يكون الدفاع عملية ناجحة تماماً، وغالباً ما تتأخر تقنية الدفاع عن تقنية الهجوم. وغالباً ما يجد الغزاة والمتسللون طرقاً ملتوية لتجاوز منافذ الدخول والجدران النارية الدفاعية.

تشهد عمليات القرصنة الإلكترونية نشاطاً ملحوظاً في السنوات الأخيرة، على الرغم من الخطط المستمرة لكبرى شركات التأمين الإلكتروني للبرامج والمواقع الإلكترونية، حيث أصبحت القرصنة الإلكترونية شبحاً يدهم البنوك وشركات النفط على مستوى العالم، (وتقدر خسائرها بمبلغ (١٤٤) مليار دولار سنوياً، وفي منطقة الشرق الأوسط، فكل بنك يتعرض لما يقرب من (٥٠٠) هجمة إلكترونية في العام الواحد، وكل هجمة يقع ضحيتها من (١٠ إلى ١٥) عميلاً، وقد ارتفعت بنسبة (٦٥ %) في عام (٢٠١٥م) وقد انفقت منطقة الشرق الأوسط نحو (٢١٥) مليار دولار عام (٢٠١٤م) لحماية معلوماتها، وتتصدر الإمارات (بنسبة (٢٨ %) والسعودية بنسبة (٢١ %) في قائمة تلك الإنفاقات. ويؤكد خبراء مكافحة جرائم المعلومات والانترنت، أن هذه الجرائم انتشرت بشكل مخيف ينبئ بالخطر بسبب خواصها التي تميزها عن الجريمة التقليدية، موضحين أن ضحايا هذه الجرائم يتعرضون لتعطيل وتدمير لمخازن المعلومات الخاصة بهم وسرقة أموالهم والتهديد والابتزاز بما يؤثر بشكل سيئ في الاقتصاد)، وفي ظل ارتفاع تلك المعدلات بشكل لافت سوف يكون مستقبل العالم الاقتصادي كما يلي:

أ. استمرار الخسائر الاقتصادية. في حال عدم التعاون الجاد بين الدول لإيجاد حلول لمشكلة القرصنة الإلكترونية سيكون هناك استمرار للخسائر الاقتصادية نتيجة عمليات القرصنة (وقد كانت هناك قمة عبرت عن ذلك بين الرئيس الأمريكي باراك أوباما ورئيس الوزراء الصيني، وقد ناقشت القمة بكل صراحة قضية الهجمات الإلكترونية بشكل صريح بين البلدين على أعلى المستويات وخاصة في النواحي الاقتصادية حيث تبادل الهجمات الإلكترونية على كبرى المؤسسات والمنظمات الاقتصادية بين البلدين وحاولا إيجاد حلول لها). ربما هذه القمة جيدة لمناقشة تلك المشكلة الكبرى، ولكن الأهم من ذلك هو مدى تفاعل باقي دول العالم من أجل الحد من

استمرار الخسائر الاقتصادية. هناك أيضاً مشكلة أخرى تؤدي إلى الخسائر الاقتصادية نتيجة القرصنة الإلكترونية، ربما هذه المعلومات التي يتم جمعها حول قرصنة الإنترنت غير كاملة بسبب عدم متابعة الكثير من الدول بصورة مستمرة عمليات القرصنة وعدم كشف الشركات عما تتعرض له من هجمات.

ب. استمرار الخسائر الاقتصادية بدون تشريعات حقيقية معبرة عن حجم المشكلة. إن التعاون الدولي من خلال اتفاقية دولية لتطبيق القانون وتشديد العقوبات على جرائم القرصنة والتعاون مع منظمة التجارة العالمية، بدون تحديد خسائر القرصنة وحصر الشركات والمؤسسات التجارية المخاطر التي تواجهها سيؤدي أيضاً إلى استمرار عملية القرصنة واستمرار الخسائر الاقتصادية، لذلك هناك مسؤولية تقع على المجتمعات للتصدي لهذه الجرائم، وتتمثل هذه المسؤولية في توعية أصحاب وإداري المؤسسات والشركات الاقتصادية الكبرى بمفهوم الجريمة الإلكترونية، وأنها الخطر القادم والحرص على ألا يقعوا ضحية لها. يضاف إلى ذلك ضرورة التأكد من سبل الحماية للناوين الإلكترونية التي تتطلب معلومات سرية خاصة كمعلومات البطاقة الائتمانية أو حساب البنك، ووضع أنظمة تشريعية متطورة لتنظيم البيئة القانونية والتنظيمية التي تخدم أمن تقنيات ونظم المعلومات، إلى جانب تطوير برمجيات آمنة ونظم تشغيل قوية تحد من الاختراقات الإلكترونية وبرمجيات الفيروسات وبرامج التجسس وذلك بشكل مستمر، كل هذه العوامل إذا لم تُطبق ستستمر الخسائر الاقتصادية الكبيرة للشركات. ولذلك ومن خلال ما تقدم في هذا الفصل يتبين لنا أن استمرار عمليات الحروب الإلكترونية عن طريق القرصنة وقيام مخاطر دول كبرى بالاعتماد عليها في التلصص الاقتصادي والأمني والعسكري على الدول الأخرى بحاجة إلى تسخير إمكانيات الدول من أجل بناء طرق حماية أكثر تطوراً وأمناً لمواجهة تلك القراصنة، ولا مانع من الاستفادة من الخبرات والتجارب الأمنية للدول ذات التجارب الناجحة في الحماية واختيار الخبرات الوطنية ذات الكفاءة من أجل مزيد من أمن المعلومات، وإلا سيحدث ما لا يحمد عقباه من خسائر كبيرة مستوى مؤسسات الدول ولا سيما العسكرية واقتصادياً على مستوى المؤسسات الاقتصادية الهامة التي يؤثر سقوطها على سقوط الدولة بكافة مكوناته.

الفصل الرابع: الإجراءات المنهجية للدراسة

التمهيد

سيقوم الباحثون في هذا الفصل خطوات الدراسة الميدانية وإجراءاتها والتي تشمل منهاج الدراسة، ومجتمع وعينة الدراسة، وأداة جمع البيانات، وإجراءات الصدق والثبات والأساليب الإحصائية التي استخدمت في المعالجة والتحليل والتي سيتم توضيحها كما يلي:

منهج الدراسة

اعتمدت الدراسة على المنهج الاستقرائي في إعداد الجزء النظري، حيث سيتم استقراء المواضيع والدراسات المتعلقة بموضوع البحث وذلك لتكوين الإطار النظري. أما في الجانب العملي. واعتمدت الدراسة على المنهج الوصفي التحليلي في الحصول على كافة المعلومات والبيانات اللازمة لتحقيق أهداف الدراسة وأغراضها. ويتمثل المنهج الوصفي التحليلي فيما يلي:

- (١) المنهج الوصفي كونه منهجاً يناسب أهداف الدراسة الحالية. ويمثل المنهج الوصفي طريقة لوصف الموضوع المراد دراسته من خلال منهجية علمية صحيحة، وتصوير النتائج التي يتم التوصل إليها على أشكال رقمية معبرة يمكن تفسيرها. ويتضمن وصف متغيرات الدراسة المستقلة والمتعلقة في أهمية حماية المعلومات، والمتغير التابع المتمثل في تصاعد هجمات القرصنة الإلكترونية.
- (٢) المنهج التحليلي ويهدف إلى تحليل وتقييم أهمية حماية المعلومات في ظل تصاعد هجمات القرصنة الإلكترونية.

كما اعتمد الباحث إلى جمع البيانات بعدة طرق، أهمها:

- البيانات الثانوية، من خلال المراجعة والمسح للدراسات السابقة، والكتب والمقالات والتقارير والرسائل الجامعية، وشبكة الإنترنت، وذلك لوضع الأسس العلمية والإطار النظري لهذه الدراسة.
- البيانات الأولية من خلال المصادر الميدانية، حيث سيتم تطوير استبانة تشمل كافة محاور الدراسة.

أدوات الدراسة

لقد تم استخدام الاستبانة كأداة للدراسة لجمع آراء ووجهات نظر افراد العينة وسيتم توزيعها عن طريق البريد الالكتروني. ستشمل عينة الدراسة (١٠٠) من العاملين المختصين في الامن السيبراني في المملكة العربية السعودية. وسيتم استخدام برنامج (SPSS) لتحليل كافة البيانات الإحصائية التي تم جمعها من افراد العينة.

الأساليب الإحصائية المستخدمة

لقد تم استخدام الأساليب الإحصائية بناءً على طبيعة الدراسة، والأهداف التي سعت لتحقيقها، وسيتم التحليل للبيانات التي ستجمع من خلال أداة الدراسة (الاستبانة)، باستخدام جهاز الحاسب الآلي، عن طريق برنامج الحزم الاحصائية (SPSS). وتتمثل الأساليب الإحصائية التي سيتم تنفيذها في الدراسة بالآتي:

- النسب المئوية والتكرارات.
- معاملات الارتباط لإيجاد العلاقة بين المتغيرات.
- المتوسطات الحسابية والانحرافات المعيارية.
- اختبار T-test لإثبات صحة الفروض من عدمها.

الفصل الخامس: نتائج الدراسة الميدانية

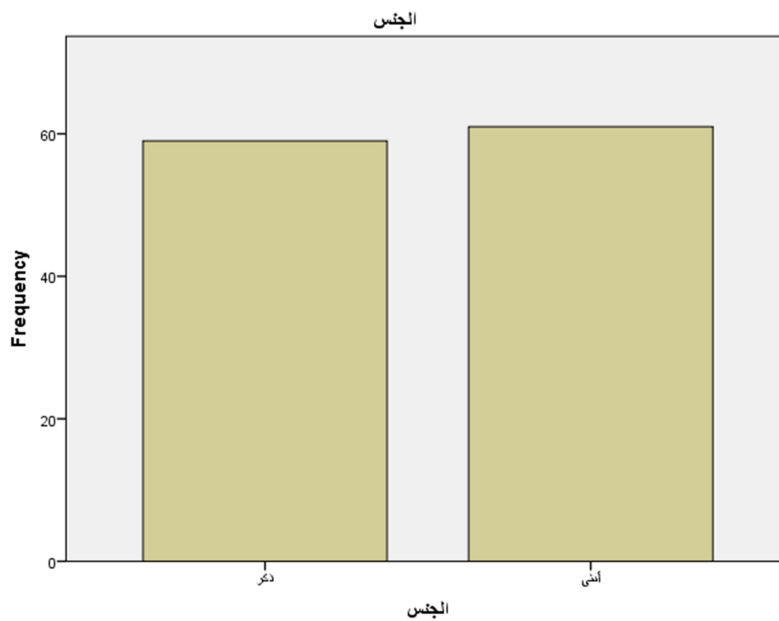
أولاً: البيانات الأولية

١. الجنس

الجدول (١): الجنس

البيان	التكرارات	النسب المئوية
ذكر	٥٩	%٤٩.٢
أنثى	٦١	%٥٠.٨
المجموع	١٢٠	%١٠٠

الشكل (١): الجنس



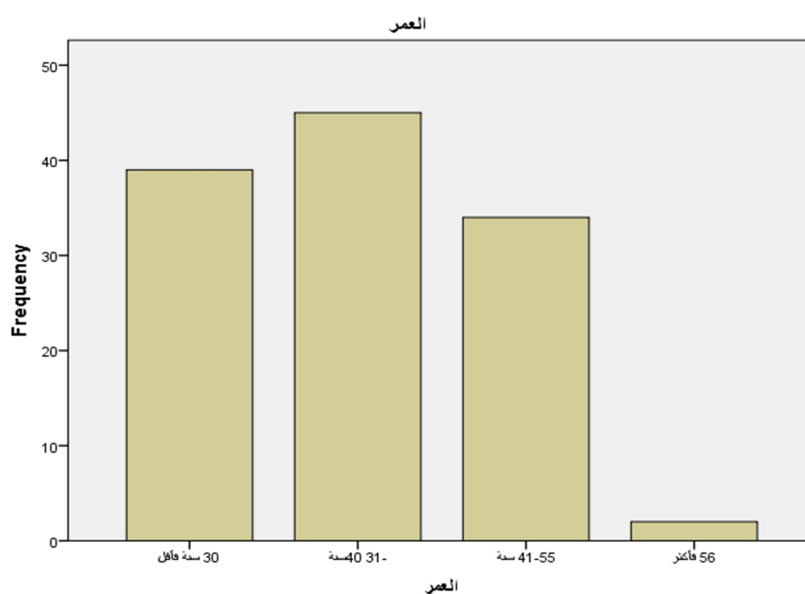
من الجدول والشكل أعلاه، يتضح أن نسبة الذكور إلى الإناث تقريبا متساوية، حيث بلغت نسبة الذكور (%٤٩.٢) في حين بلغت نسبة الإناث (%٥٠.٨) وهذه دلالة جيدة تخدم أغراض البحث.

٢. العمر

الجدول (٢): العمر

البيان	التكرارات	النسب المئوية
٣٠ سنة فأقل	٣٩	٣٢.٥%
٣١ - ٤٠ سنة	٤٥	٣٧.٥%
٤١ - ٥٥ سنة	٣٤	٢٨.٣%
٥٦ فأكثر	٢	١.٧%
المجموع	١٢٠	١٠٠%

الشكل (٢): العمر



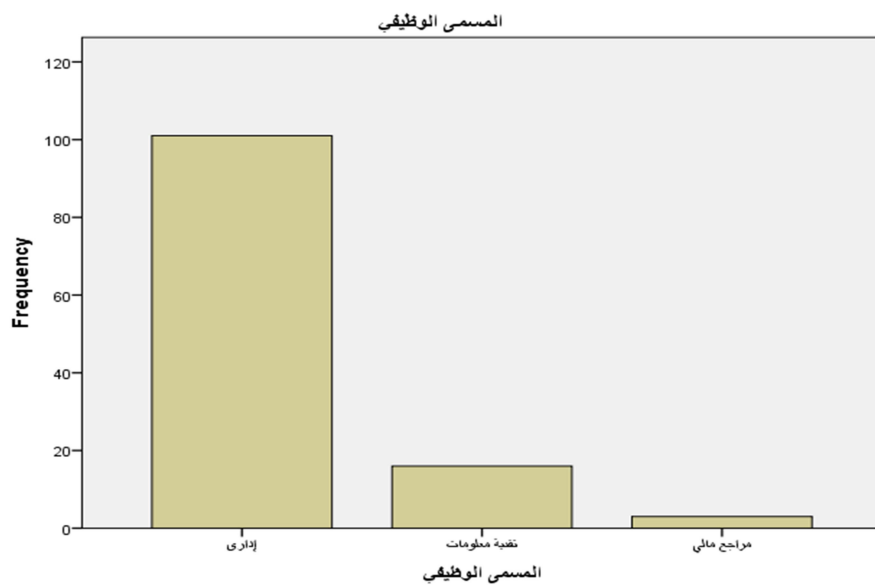
من الجدول والشكل أعلاه ، يتضح أن أغلب أعمار أفراد عينة الدراسة تراوحت ما بين (٣٠ إلى ٥٥) بنسبة وصلت إلى (٩٥%).

٣. المسمى الوظيفي

الجدول (٣): المسمى الوظيفي

البيان	التكرارات	النسب المئوية
إداري	١٠١	%٨٤.٢
تقنية معلومات	١٦	%١٣.٣
محاسب	٠	٠
مراجع مالي	٣	%٢.٥
المجموع	١٢٠	%١٠٠

الشكل (٣): المسمى الوظيفي



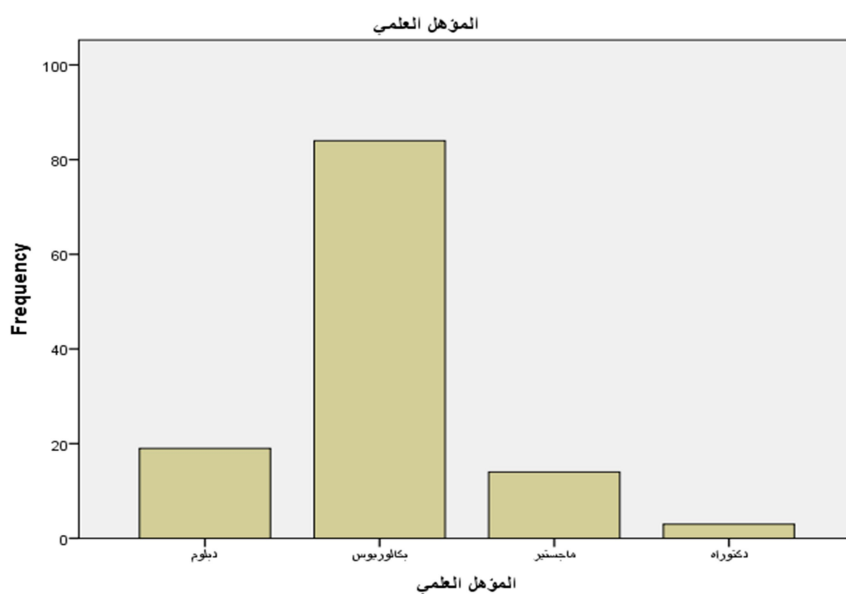
من الجدول والشكل أعلاه ، يتضح أن أغلب أفراد عينة الدراسة يعملون كإداريين بنسبة وصلت إلى (%٨٤.٢).

٤. المؤهل العلمي

الجدول (٤): المؤهل العلمي

البيان	التكرارات	النسب المئوية
دبلوم	١٩	%١٥.٨
بكالوريوس	٨٤	%٧٠
ماجستير	١٤	%١١.٧
دكتوراه	٣	%٢.٥
المجموع	١٢٠	%١٠٠

الشكل (٤): المؤهل العلمي



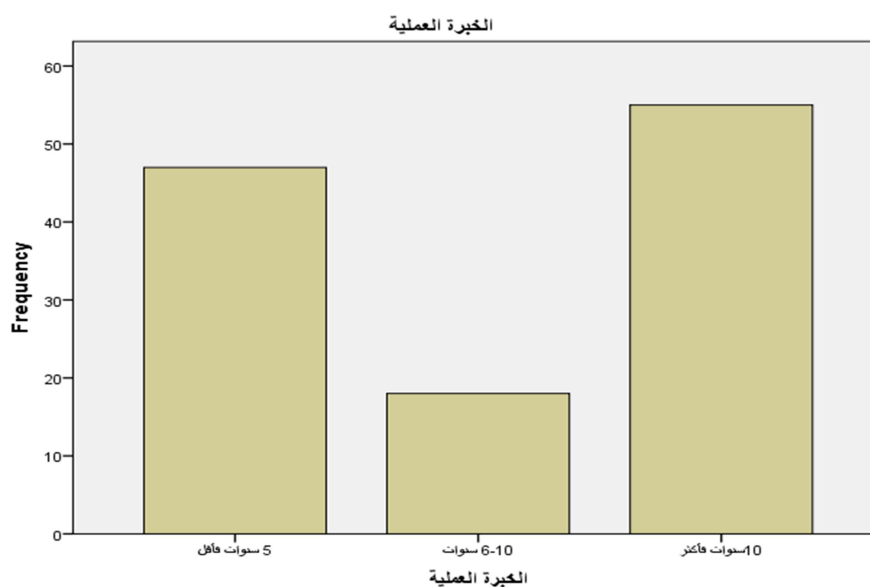
من الجدول والشكل أعلاه، يتضح أن أغلب أفراد عينة الدراسة لديهم مؤهل بكالوريوس بنسبة بلغت (٧٠%).

٥. الخبرات العملية

الجدول (٥): الخبرات العملية

البيان	التكرارات	النسب المئوية
٥ سنوات فأقل	٤٧	%٣٩.٢
٦ - ١٠ سنوات	١٨	%١٥
١٠ سنوات فأكثر	٥٥	%٤٥.٨
المجموع	١٢٠	%١٠٠

الجدول (٥): الخبرات العملية



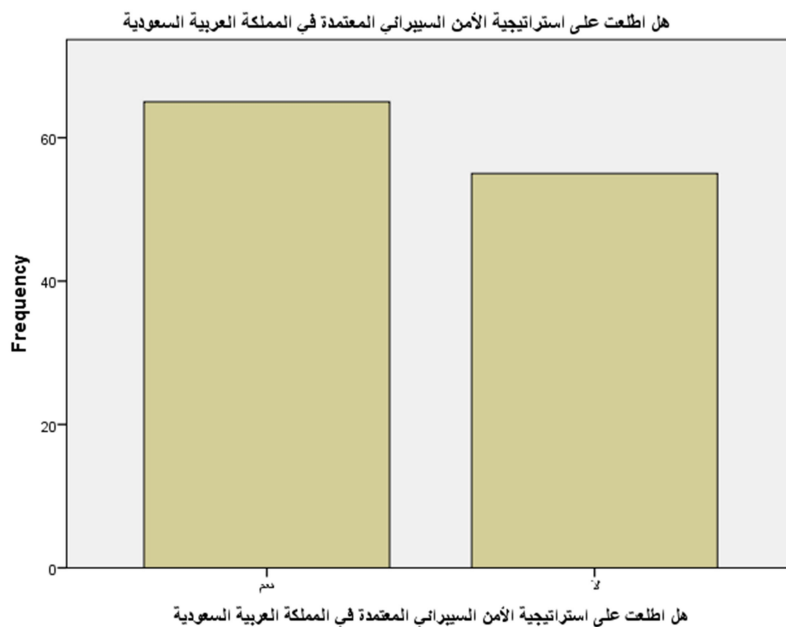
من الجدول والشكل أعلاه ، يتضح أن أغلب أفراد عينة الدراسة لديهم خبرة عملية وصلت إلى العشر سنوات بنسبة بلغت (٤٥.٨%).

٦. هل اطلعت على استراتيجية الأمن السيبراني المعتمدة في المملكة العربية السعودية

الجدول (٦): مدى الاطلاع على استراتيجية الأمن السيبراني

البيان	التكرارات	النسب المئوية
نعم	٦٥	%٥٤.٢
لا	٥٥	%٤٥.٨
المجموع	١٢٠	%١٠٠

الشكل (٦): مدى الاطلاع على استراتيجية الأمن السيبراني



من الجدول والشكل أعلاه، يتضح أن أغلب أفراد عينة الدراسة لديهم إطلاع على استراتيجية الأمن السيبراني المعتمدة في المملكة العربية السعودية بنسبة بلغت (%٥٤.٢) وهذا يخدم أغراض البحث بصورة مباشرة.

٧. هل أهداف استراتيجية الأمن السيبراني تسهم في تحقيق التوجهات الحكومية وممكنات الحكومة الذكية

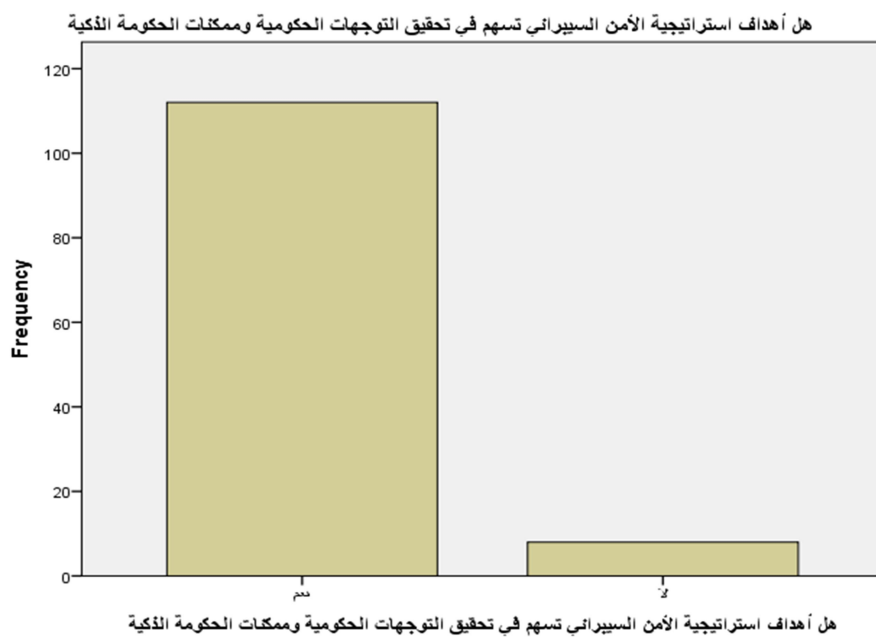
الجدول (٧): مدى اسهام أهداف استراتيجية الأمن السيبراني في تحقيق التوجهات الحكومية وممكنات

الحكومة الذكية

البيان	التكرارات	النسب المئوية
نعم	١١٢	%٩٣.٣
لا	٨	%٦.٧
المجموع	١٢٠	%١٠٠

الشكل (٧): مدى اسهام أهداف استراتيجية الأمن السيبراني في تحقيق التوجهات الحكومية وممكنات

الحكومة الذكية



من الجدول والشكل أعلاه، يتضح أن أغلب أفراد عينة الدراسة يرون أن استراتيجية الأمن السيبراني تسهم في تحقيق التوجهات الحكومية وممكنات الحكومة الذكية بنسبة بلغت (٩٣.٣%).

٨. ثبات الاستبيان

الجدول (٨): معدل ثبات فقرات المحور الأول- حماية المعلومات

معامل الثبات	
عدد العبارات	ألفا كرونباخ
١٠	٠.٩٧٠

من خلال الجدول أعلاه، نلاحظ أن معامل الثبات لفقرات المحور الأول قد بلغ ٠.٩٧٠ وهو معدل ثبات جيد.

الجدول (٩): معدل ثبات فقرات المحور الثاني – القرصنة الإلكترونية

معامل الثبات	
عدد العبارات	ألفا كرونباخ
١٤	٠.٨٦٧

من خلال الجدول أعلاه، نلاحظ أن معامل الثبات لفقرات المحور الثاني قد بلغ ٠.٨٦٧ وهو معدل ثبات جيد.

الجدول (١٠): معدل ثبات الفقرات الخاصة – صور الاختراقات

معامل الثبات	
عدد العبارات	ألفا كرونباخ
٦	٠.٨٧٠

من خلال الجدول أعلاه، نلاحظ أن معامل الثبات لفقرات المحور الثالث قد بلغ ٠.٨٧٠ وهو معدل ثبات جيد.

الجدول (١١): معدل ثبات فقرات الاستبيان ككل

معامل الثبات	
عدد العبارات	ألفا كرونباخ
٣٣	٠.٩٧٦

من خلال الجدول أعلاه، نلاحظ أن معامل الثبات لفقرات الاستبيان قد بلغ ٠.٩٧٦ وهو معدل ثبات جيد

ومناسب لأغراض البحث.

٩. معامل الارتباط بين محاور الدراسة:

الجدول (١٢) : معامل الارتباط بين محاور الدراسة				
صورالاختراقات	القرصنة الإلكترونية	حماية المعلومات		
٠.٥٥٩	٠.٥٧٢	١	معامل الارتباط بيرسون	حماية المعلومات
٠.٠٠٠	٠.٠٠٠		مستوى الدلالة	
١٢٠	١٢٠	١٢٠	العينة	
٠.٥١١	١	٠.٥٧٢	معامل الارتباط بيرسون	القرصنة الإلكترونية
٠.٠٠١		٠.٠٠٠	مستوى الدلالة	
١٢٠	١٢٠	١٢٠	العينة	
١	٠.٥١١	٠.٥٥٩	معامل الارتباط بيرسون	صورالاختراقات
	٠.٠٠١	٠.٠٠٠	مستوى الدلالة	
١٢٠	١٢٠	١٢٠	العينة	

من الجدول أعلاه، يتضح لنا هناك علاقة طردية قوية بين محاور الدراسة الثلاثة حيث جاءت قيمة معامل الارتباط بين المحور كالتالي: حماية المعلومات والقرصنة الإلكترونية بلغ معامل الارتباط (٠.٥٧٢) ويفسر ذلك بأنه كلما زادت القرصنة الإلكترونية كلما زادت عمليات حماية المعلومات والعكس صحيح. صور الاختراقات والقرصنة الإلكترونية بلغ معامل الارتباط (٠.٥١١) ويفسر ذلك بأنه كلما زادت صور الاختراقات كلما زادت القرصنة الإلكترونية والعكس صحيح. وهذا يدل على العلاقة القوية بين متغيرات الدراسة والتي تمثلت في حماية المعلومات والقرصنة الإلكترونية.

ثانياً: تحليل بيانات المحور الأول – حماية المعلومات

الجدول (١٣): تحليل بيانات المحور الأول- حماية المعلومات

م	التكرارات والنسب	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة	المتوسط المرجح	الانحراف المعياري	اتجاه العينة	رتبة السؤال
١	تكرارات	٤٠	٧١	٩	٠	٠	٤.٢١	٠.٥٨٨١	موافق	٧
	نسبة	%٣٠	%٦١	%٩	٠	٠				
٢	تكرارات	٦٨	٤١	٢	٩	٠	٤.٣٨	٠.٩٠٣١	موافق بشدة	٢
	نسبة	%٥٨	%٣١	%٢	%٩	٠				
٣	تكرارات	٥٩	٤٧	١٤	٠	٠	٤.٣٥	٠.٧١٢٤	موافق بشدة	٤
	نسبة	%٤٩	%٣٧	%١٤	٠	٠				
٤	تكرارات	٤٨	٥٨	٢	١٢	٠	٤.١٢	٠.٩٣٠٤	موافق	٨
	نسبة	%٣٨	%٤٨	%٢	%١٢	٠				
٥	تكرارات	٥٣	٥٨	٩	٠	٠	٤.٣٤	٠.٦٣٥٩	موافق	٦
	نسبة	%٤٣	%٤٨	%٩	٠	٠				
٦	تكرارات	٦٧	٥٣	٠	٠	٠	٤.٥٧	٠.٤٩٥١	موافق بشدة	١
	نسبة	%٥٧	%٤٣	٠	٠	٠				
٧	تكرارات	٣١	٨٠	٩	٠	٠	٤.١٢	٠.٥٣٤٤	موافق	٩
	نسبة	%٢١	%٧٠	%٩	٠	٠				
٨	تكرارات	٣٢	٧٤	١٤	٠	٠	٤.٠٨	٠.٥٩٤٦	موافق	١٠
	نسبة	%٢٢	%٦٤	%١٤	٠	٠				
٩	تكرارات	%٤٩	%٣٧	%١٤	٠	٠	٤.٣٨	٠.٦٤٤٧	موافق بشدة	٣
	نسبة	٤٨	٥٨	٢	١٢	٠				
١٠	تكرارات	٥٣	٥٨	٩	٠	٠	٤.٣٥	٠.٦١٢٤	موافق بشدة	٥
	نسبة	%٤٣	%٤٨	%٩	٠	٠				

من الجدول أعلاه، أن هناك اتفاق إجماع كامل بين أفراد عينة الدراسة بالموافقة على جميع فقرات المحور فجاءت الفقرة التي تنص على " عادة ما أشارك بياناتي الشخصية مع أي جهة دون التأكد من حماية بياناتي " في المرتبة الأولى بمتوسط حسابي بلغ (٤.٥٧) وانحراف معياري بلغ (٠.٤٩٥١)، في حين جاءت الفقرة التي تنص على " هناك برامج حماية للمستخدمين لحماية المعلومات من الاختراق " في المرتبة الثانية بمتوسط حسابي بلغ (٤.٣٨) وانحراف معياري بلغ (٠.٩٠٣١)، في حين جاءت الفقرة التي تنص على " أقوم بقراءة سياسة

الخصوصية عند تصفح المواقع الالكترونية والتطبيقات " في المرتبة الثالثة بمتوسط حسابي بلغ (٤.٣٨) وانحراف معياري بلغ (٠.٦٤٤٧)، وجاءت الفقرة التي تنص على " يلعب التهاون والإهمال الوظيفي دوراً مهماً في عمليات الاختراق وقلة حماية المعلومات وبالتالي قرصنتها " في المرتبة الرابعة بمتوسط حسابي بلغ (٤.٣٥) وانحراف معياري بلغ (٠.٧١٢٤)، في حين جاءت الفقرة التي تنص على " سبق وأن استخدمت بياناتي الشخصية بمواقع غير رسمية وغير معتمدة " في المرتبة الخامسة بمتوسط حسابي بلغ (٤.٣٥) وانحراف معياري بلغ (٠.٦١٢٤)، وهذا يدل على وجود موافقة على الأهمية التي يجب أن تتسم فيها حماية المعلومات نظراً لأهميتها وإمكانية استخدام هذه المعلومات في أعمال غير شرعية.

ثالثاً: تحليل بيانات المحور الثاني – القرصنة الإلكترونية

الجدول (١٤): تحليل بيانات المحور الثاني – القرصنة الإلكترونية

م	التكرارات والنسب	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة	المتوسط المرجح	الانحراف المعياري	اتجاه العينة	رتبة السؤال
١	تكرارات	٣٢	٦٧	٢١	.	.	٤.٠١	٠.٦٥٥٧	موافق	١٤
	نسبة	%٢٢	%٥٧	%٢١	.	.				
٢	تكرارات	٥٤	٥٥	١١	.	.	٤.٣٣	٠.٦٦٤٢	موافق	٦
	نسبة	%٤٤	%٤٥	%١١	.	.				
٣	تكرارات	٦٧	٤٤	٩	.	.	٤.٤٨	٠.٦٥٥٤	موافق بشدة	٢
	نسبة	%٥٧	%٣٤	%٩	.	.				
٤	تكرارات	٤٢	٦٦	١٢	.	.	٤.٢	٠.٦٣٢٥	موافق	١٣
	نسبة	%٣٢	%٥٦	%١٢	.	.				
٥	تكرارات	٤٥	٧٥	.	.	.	٤.٣٥	٠.٤٧٧٠	موافق	٥
	نسبة	%٣٥	%٦٥	.	.	.				
٦	تكرارات	٥٠	٦١	٩	.	.	٤.٣١	٠.٦٢٧٦	موافق	١٠
	نسبة	%٤٠	%٥١	%٩	.	.				
٧	تكرارات	٤٢	٦٩	٩	.	.	٤.٢٣	٠.٥٩٧٦	موافق	١١
	نسبة	%٣٢	%٥٩	%٩	.	.				
٨	تكرارات	٧٠	٣٨	١٢	.	.	٤.٤٨	٠.٦٩٩٧	موافق بشدة	١
	نسبة	%٦٠	%٢٨	%١٢	.	.				
٩	تكرارات	٥٠	٦١	٩	.	.	٤.٣١	٠.٦٢٧٦	موافق	٩
	نسبة	%٤٠	%٥١	%٩	.	.				
١٠	تكرارات	٤١	٦٧	١٢	.	.	٤.١٩	٠.٦٢٧٦	موافق	١٢
	نسبة	%٣١	%٥٧	%١٢	.	.				
١١	تكرارات	٥٧	٥٤	٩	.	.	٤.٣٨	٠.٦٤٤٧	موافق بشدة	٣
	نسبة	%٤٧	%٤٤	%٩	.	.				
١٢	تكرارات	٥٩	٤٧	١٤	.	.	٤.٣٥	٠.٧١٢٤	موافق بشدة	٤
	نسبة	%٤٩	%٣٧	%١٤	.	.				
١٣	تكرارات	٥٣	٥٦	١١	.	.	٤.٣٢	٠.٦٦١٥	موافق	٧
	نسبة	%٤٣	%٤٦	%١١	.	.				
١٤	تكرارات	٥٠	٦١	٩	.	.	٤.٣١	٠.٦٢٧٦	موافق	٨
	نسبة	%٤٠	%٥١	%٩	.	.				

من الجدول أعلاه، أن هناك اتفاق إجماع كامل بين أفراد عينة الدراسة بالموافقة على جميع فقرات المحور فجاءت الفقرة التي تنص على " تتطور عمليات القرصنة وسرعة فائقة باستخدام تقنيات حديثة ومعقدة " في المرتبة الأولى بمتوسط حسابي بلغ (٤.٤٨) وانحراف معياري بلغ (٠.٦٩٩٧)، في حين جاءت الفقرة التي تنص على " أرسل صوري الخاصة ومعلوماتي الخاصة لأصدقائي دون خوف من اختراق هكر لتلك المعلومات " في المرتبة الثانية بمتوسط حسابي بلغ (٤.٤٨) وانحراف معياري بلغ (٠.٦٥٥٤)، في حين جاءت الفقرة التي تنص على " لا يمكن القضاء على ظاهرة القرصنة الإلكترونية، ولكن يمكن التقليل من خطورتها " في المرتبة الثالثة بمتوسط حسابي بلغ (٤.٣٨) وانحراف معياري بلغ (٠.٦٤٤٧)، وجاءت الفقرة التي تنص على " اعي بخطورة القرصنة الإلكترونية وبضرورة حماية الخصوصية على أي موقع أقوم بزيارته " في المرتبة الرابعة بمتوسط حسابي بلغ (٤.٣٥) وانحراف معياري بلغ (٠.٧١٢٤)، في حين جاءت الفقرة التي تنص على " دائما ما تخترق أجهزتي بفيروسات بعد قيامي بتصفح الإنترنت بشكل دوري " في المرتبة الخامسة بمتوسط حسابي بلغ (٤.٣٥) وانحراف معياري بلغ (٠.٤٧٧٠)، وهذا يدل على وجود موافقة على أن القرصنة الإلكترونية أزمة تتفاقم زمن الأرشفة الإلكترونية كما أنه لا يمكن القضاء على هذه الظاهرة طالما كان هناك مشاركة للمعلومات عبر الإنترنت، بالإضافة إلى وجود تقنيات متجددة وبشكل دوري لعمليات القرصنة المستمرة.

رابعاً: تحليل بيانات المحور الثالث – صور الاختراقات

الجدول (١٥): تحليل بيانات المحور الثالث – صور الاختراقات

م	التكرارات والنسب	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة	المتوسط المرجح	الانحراف المعياري	اتجاه العينة	رتبة السؤال
١	تكرارات	٥٤	٥٧	١٩	٠	٠	٤.١٥	٠.٧١٢٤	موافق	٦
	نسبة	%٣٤	%٤٧	%١٩	٠	٠				
٢	تكرارات	٥٥	٥٤	١١	٠	٠	٤.٣٤	٠.٦٦٦٦	موافق بشدة	٣
	نسبة	%٤٥	%٤٤	%١١	٠	٠				
٣	تكرارات	٥٣	٥٨	٠	٩	٠	٤.٢٥	٠.٨٥٢٩	موافق	٤
	نسبة	%٤٣	%٤٨	٠	%٩	٠				
٤	تكرارات	٦٦	٥٤	٠	٠	٠	٤.٥٦	٠.٤٩٦٤	موافق بشدة	١
	نسبة	%٥٦	%٤٤	٠	٠	٠				
٥	تكرارات	٤٤	٦٤	١٢	٠	٠	٤.٢٢	٠.٦٤١٦	موافق	٥
	نسبة	%٣٤	%٥٤	%١٢	٠	٠				
٦	تكرارات	٦٢	٥٨	٠	٠	٠	٤.٥٢	٠.٤٩٩٦	موافق بشدة	٢
	نسبة	%٥٢	%٤٨	٠	٠	٠				

من الجدول أعلاه، أن هناك اتفاق إجماع كامل بين أفراد عينة الدراسة بالموافقة على جميع فقرات المحور فجاءت الفقرة التي تنص على "الاحتيال المالي الالكتروني" في المرتبة الأولى بمتوسط حسابي بلغ (٤.٥٦) وانحراف معياري بلغ (٠.٤٩٦٤)، في حين جاءت الفقرة التي تنص على "اختراق المواقع الحكومية ومواقع الشركات الحساسة" في المرتبة الثانية بمتوسط حسابي بلغ (٤.٥٢) وانحراف معياري بلغ (٠.٤٩٩٦)، في حين جاءت الفقرة التي تنص على "انتهاك خصوصية الغير" في المرتبة الثالثة بمتوسط حسابي بلغ (٤.٣٤) وانحراف معياري بلغ (٠.٦٦٦٦)، وهذا يدل على أن أهمية الحذر من الوسائل المختلفة للقرصنة ومحاربتها بشتى الوسائل المتاحة وفقاً لإجابات أفراد عينة الدراسة.

وعند تحليلنا للسؤال المتعلق بمدى قدرة اللوائح والتشريعات المتعلقة بأمن المعلومات والخصوصية على معالجة التحديات والمخاطر الالكترونية في ظل تصاعد عمليات الاختراق والقرصنة الالكترونية، ولماذا؟ كان اغلب الردود إيجابية حيث تمثلت هذه الردود بالجدول ادناه:

الجدول (١٦): بمدى قدرة اللوائح والتشريعات المتعلقة بأمن المعلومات والخصوصية على معالجة التحديات والمخاطر الالكترونية

البيان	التكرارات	النسب المئوية
نعم	٥١	%٤٢.٥
لا	٦٣	%٥٢.٥
إلى حد ما	٦	%٥
المجموع	١٢٠	%١٠٠

من الجدول أعلاه، يتضح أن هناك تفاوت في إجابات أفراد عينة الدراسة، حيث جاءت بلغ نسبة من أجابوا بنعم (٤٢.٥%)، في حين بلغت نسبة من أجابوا بلا (٥٢.٥) وجاءت نسبة من أجابوا إلى حد ما (٥%)، ويرجع ذلك إلى عدد من الأسباب أهمها:

- التطور المستمر.
- القدرة على العلاج ولكن مع وجود بطء في عمليات المعالجة.
- عدم وجود التثقيف العام عن الأمن السيبراني.
- التجدد المستمر في عمليات الاختراق.

الفصل السادس: تحليل النتائج والتصور المقترح

من خلال ما سبق ، يتضح أن نسبة الذكور إلى الإناث تقريبا متساوية. كما أن أغلب أعمار أفراد عينة الدراسة تراوحت ما بين (٣٠ إلى ٥٥) وغلب أفراد عينة الدراسة يعملون كإداريين ولديهم مؤهل بكالوريوس ولديهم كذلك خبرة عملية وصلت إلى العشر سنوات. كما وجد أن أغلب أفراد عينة الدراسة لديهم إطلاع على استراتيجية الأمن السيبراني المعتمدة في المملكة العربية السعودية وهذا يخدم أغراض البحث بصورة مباشرة. كما أن أغلب أفراد عينة الدراسة يرون أن استراتيجية الأمن السيبراني تسهم في تحقيق التوجهات الحكومية وممكّنات الحكومة الذكية. كما تم تحليل معدل الثبات للاستبيان ووجد أن معامل الثبات لفقرات المحور الأول وفقرات المحور الثاني والمحور الثالث والثبات لفقرات الاستبانة ذات معدل ثبات جيد ومناسب لأغراض البحث.

كما وجد عند تحليل معامل الارتباط بين محاور الدراسة ، أن هناك علاقة طردية قوية بين محاور الدراسة الثلاثة حيث جاءت قيمة معامل الارتباط بين حماية المعلومات والقرصنة الإلكترونية حيث بلغ معامل الارتباط (٠.٥٧٢) ويفسر ذلك بأنه كلما زادت القرصنة الإلكترونية كلما زادت عمليات حماية المعلومات والعكس صحيح. كما بلغ معامل الارتباط بين صور الاختراقات والقرصنة الإلكترونية (٠.٥١١) ويفسر ذلك بأنه كلما زادت صور الاختراقات كلما زادت القرصنة الإلكترونية والعكس صحيح. وهذا يدل على العلاقة القوية بين متغيرات الدراسة والتي تمثلت في حماية المعلومات والقرصنة الإلكترونية. ووجد أن تحليل محور الدراسة الأول أن هناك اتفاق إجماع كامل بين أفراد عينة الدراسة بالموافقة على جميع فقرات المحور فجاءت الفقرة التي تنص على " عادة ما أشارك بياناتي الشخصية مع أي جهة دون التأكد من حماية بياناتي " في المرتبة الأولى بمتوسط حسابي بلغ (٤.٥٧) وانحراف معياري بلغ (٠.٤٩٥١)، في حين جاءت الفقرة التي تنص على " هناك برامج حماية للمستخدمين لحماية المعلومات من الاختراق " في المرتبة الثانية بمتوسط حسابي بلغ (٤.٣٨) وانحراف معياري بلغ (٠.٩٠٣١)، في حين جاءت الفقرة التي تنص على " أقوم بقراءة سياسة الخصوصية عند تصفح المواقع الإلكترونية والتطبيقات " في المرتبة الثالثة بمتوسط حسابي بلغ (٤.٣٨) وانحراف معياري بلغ (٠.٦٤٤٧)، وجاءت الفقرة التي تنص على " يلعب التهاون والإهمال الوظيفي دوراً مهماً في عمليات الاختراق وقلة حماية المعلومات وبالتالي قرصنتها " في المرتبة الرابعة بمتوسط حسابي بلغ (٤.٣٥) وانحراف معياري بلغ (٠.٧١٢٤)، في حين جاءت الفقرة التي تنص على " سبق

وأن استخدمت بياناتي الشخصية بمواقع غير رسمية وغير معتمدة " في المرتبة الخامسة بمتوسط حسابي بلغ (٤.٣٥) وانحراف معياري بلغ (٠.٦١٢٤)، وهذا يدل على وجود موافقة على الأهمية التي يجب إن تتسم فيها عمليات حماية المعلومات.

إن هناك إجماع كامل بين أفراد عينة الدراسة بالموافقة على جميع فقرات المحور فجاءت الفقرة التي تنص على " تتطور عمليات القرصنة وسرعة فائقة باستخدام تقنيات حديثة ومعقدة " في المرتبة الأولى بمتوسط حسابي بلغ (٤.٤٨) وانحراف معياري بلغ (٠.٦٩٩٧)، في حين جاءت الفقرة التي تنص على " أرسل صوري الخاصة ومعلوماتي الخاصة لأصدقائي دون خوف من اختراق هاكل لتلك المعلومات " في المرتبة الثانية بمتوسط حسابي بلغ (٤.٤٨) وانحراف معياري بلغ (٠.٦٥٥٤)، في حين جاءت الفقرة التي تنص على " لا يمكن القضاء على ظاهرة القرصنة الإلكترونية، ولكن يمكن التقليل من خطورتها " في المرتبة الثالثة بمتوسط حسابي بلغ (٤.٣٨) وانحراف معياري بلغ (٠.٦٤٤٧)، وجاءت الفقرة التي تنص على " اعي بخطورة القرصنة الالكترونية وبضرورة حماية الخصوصية على أي موقع أقوم بزيارته " في المرتبة الرابعة بمتوسط حسابي بلغ (٤.٣٥) وانحراف معياري بلغ (٠.٧١٢٤)، في حين جاءت الفقرة التي تنص على " دائما ما تخترق أجهزتي بفيروسات بعد قيامي بتصفح الإنترنت بشكل دوري " في المرتبة الخامسة بمتوسط حسابي بلغ (٤.٣٥) وانحراف معياري بلغ (٠.٤٧٧٠)، وهذا يدل على وجود موافقة على أن القرصنة الإلكترونية أزمة تتفاقم زمن الأرشفة الإلكترونية كما أنه لا يمكن القضاء على هذه الظاهرة طالما كان هناك مشاركة للمعلومات عبر الإنترنت، بالإضافة إلى وجود تقنيات متجددة وبشكل دوري لعمليات القرصنة المستمرة.

كما وجد عند تحليل المحور الثاني المتعلق بالقرصنة الالكترونية ، أن هناك اتفاق إجماع كامل بين أفراد عينة الدراسة بالموافقة على جميع فقرات المحور فجاءت الفقرة التي تنص على " الاحتيال المالي الالكتروني " في المرتبة الأولى بمتوسط حسابي بلغ (٤.٥٦) وانحراف معياري بلغ (٠.٤٩٦٤)، في حين جاءت الفقرة التي تنص على " اختراق المواقع الحكومية ومواقع الشركات الحساسة " في المرتبة الثانية بمتوسط حسابي بلغ (٤.٥٢) وانحراف معياري بلغ (٠.٤٩٩٦)، في حين جاءت الفقرة التي تنص على " انتهاك خصوصية الغير " في المرتبة الثالثة بمتوسط حسابي بلغ (٤.٣٤) وانحراف معياري بلغ (٠.٦٦٦٦)، وهذا يدل على أن أهمية الحذر من الوسائل المختلفة

للقرصنة ومحاربتها بشتى الوسائل المتاحة وفقا لإجابات أفراد عينة الدراسة. وفي إجابة السؤال الأخير والمتعلق باللوائح والتشريعات المتعلقة بأمن المعلومات والخصوصية قادرة على معالجة التحديات والمخاطر الالكترونية في ظل تصاعد عمليات الاختراق والقرصنة الالكترونية، فيتضح أن هناك تفاوت في إجابات أفراد عينة الدراسة، حيث جاءت بلغ نسبة من أجابوا بنعم (٤٢.٥%)، في حين بلغت نسبة من أجابوا بلا (٥٢.٥) وجاءت نسبة من أجابوا إلى حد ما (٥%)، ويرجع ذلك إلى عدد من الأسباب أهمها التطور المستمر والقدرة على العلاج ولكن مع وجود ببطء في عمليات المعالجة ، وعدم وجود التثقيف العام عن الأمن السيبراني والتجديد المستمر في عمليات الاختراق.

لقد اكتسبت المعلومات أهميتها منذ أقدم العصور، ولكن نشأة الإنترنت والبريد الإلكتروني، وانتشار الحاسب الآلي، عزز هذه الأهمية، وأصبحت لا غنى عنها في جميع المجالات. ولكي تخدم المعلومات الغرض المرجو منها، لابد أن تكون متوفرة بصفة مستمرة ومحمية وموثوقة. وتشمل المعلومات المطلوب حمايتها مجالات واسعة، ولكن المعلومات الأمنية تحتل أهمية خاصة لأنها تتعلق بأمن الدول. وأولوية الحماية تكون لهذه المعلومات.. وتأثر أمن المعلومات بالتطور التقني المتسارع للحاسب الآلي، والبرامج حيث واكب ذلك تطوراً موازياً في جرائم المعلومات. وليس من السهل مقاضاة مجرم المعلومات، لإنعدام الشهود والأدلة المستخدمة ضد المتهمين ويصعب إثبات الدلائل لإستخدامها ضد المتهم كما أنه لا توجد قوانين بهذا الصدد في أغلب البلدان نظراً لجدة، وحدثة هذه الجرائم، ونظام جرائم المعلومات في مراحل التطبيق الأولى. وتختص جرائم المعلومات بخصائص منفردة لا تتوفر في الجرائم التقليدية، لأنها ترتكب عبر الإنترنت، وليس لها حدود جغرافية فهي تشمل آثارها كافة أنحاء العالم. كما تعرض أمن المعلومات للكثير من المخاطر، منها ما هو طبيعي، ومنها ما هو من صنع الإنسان.

إن البواعث التي تدفع المهاجمين لارتكاب جرائم المعلومات تختلف وتتعدد طرق، وأساليب مكافحة جرائم المعلومات، تكشف عن خطورتها، وانتشارها، ومدى الجدية في مواجهتها. كما ان موقف التشريعات العربية بخصوص حماية أمن المعلومات من المخاطر، لا تتعدى حدود ما تم تقريره على المستوى الدولي، وذلك لقناعة الدول العربية أن الحماية من هذه المخاطر تقع على كاهل المجتمع الدولي ككل نظراً لطابعها الدولي في أغلب الأحيان. وهناك اختلاف على تحديد الطبيعة القانونية للجريمة المعلوماتية، فهناك من يرى أن المعلومات ليس لها

قيمة مالية، وهناك من يرى أن للمعلومة قيمة مالية، ويمكن الاعتداء عليها شأنها في ذلك شأن المعاملات المالية الأخرى. ومن الصعب تطبيق النصوص التقليدية مثل : النصب، والسرقه، وخيانة الأمانة، والتزوير على حالات الجريمة المعلوماتية، لأن الجريمة المعلوماتية احتيال على الآلة، وليس على إنسان. إن أفضل طريقة لحماية المعلومات هي أن يكون لدى المنظمة هيئة أو إدارة متخصصة تتولى مراقبة تنفيذ سياسات أمن المعلومات وتوفير وسائل الحماية المادية والتقنية الملائمة. وليس لحرب المعلومات ميدان معركة محدد جغرافياً كالحروب التقليدية، بل يشمل مجالها جميع مجالات المعلومات، فهي حرب خفية، لا يُعرف فيها الطرف الآخر، أو الجهة التي قامت بالجريمة. وأسلحة حرب المعلومات متاحة للجميع، وقد تشن من أماكن متفرقة من العالم. والدول الأكثر تطوراً من الناحية التقنية، هي الأكثر تعرضاً لحرب المعلومات. ورغم كل الوسائل الوقائية، لا يوجد نظام أمن يحمي المعلومات حماية تامة وكاملة. وستتحول حروب المستقبل إلى حروب معلومات، وسوف يكون النصر فيها لمن يحقق التفوق المعلوماتي الآمن على الطرف الآخر. وهناك قلة في الدراسات المتعلقة بأمن المعلومات في جميع القطاعات المدنية والعسكرية وهذا يؤثر على سرية وأمن المعلومات وحفظها وتبادلها الأمر الذي يتطلب إجراء دراسات عن دور السياسات الأمنية في مواجهة جميع مهددات أمن المعلومات.

قائمة المراجع والمصادر

المراجع العربية

البابلي، عمار ياسر محمد زهير. (٢٠٢١). التحديات الأمنية المعاصرة للهجمات السيبرانية. الفكر الشرطي، مج ٣٠، ع ١١٨، ١٩ - ٨٣.

التيمني، مداخل زيد عبد الرحيم. (٢٠٢١). واقع الوعي المعلوماتي بالأمن السيبراني لدى الأفراد في المجتمع السعودي كما يدركها الخبراء المختصين بالأمن السيبراني. مجلة الخدمة الاجتماعية، ع ٦٧، ج ١، ٢٣ - ٢٣.

جوهري، عزة فاروق عبد المعبود، وحسن، طه محمد طه. (٢٠١٩). أمن المعلومات الرقمية وسبل حمايته في ظل التشريعات الراهنة. مجلة المركز العربي للبحوث والدراسات في علوم المكتبات، مج ٦، ع ١٢، ٨٥ - ١٣٢.

حبيب، أنس (٢٠٠٧). صحيفة أمريكية: الحرب الإلكترونية بين واشنطن وطهران لم تتوقف)، جريدة اليوم السابع المصرية <http://www.youm.com>

حمد، معاذ أحمد عبد الرازق، وأحمد، نصر الدين حسن. (٢٠١٦). أمن المعلومات ودوره في الحد من القرصنة الإلكترونية المركز القومي للمعلومات: دراسة حالة (رسالة ماجستير غير منشورة). جامعة، أم درمان، أم درمان.

دلالي، الجيلالي، وبالبشير، يعقوب. (٢٠٢١). رهانات الأمن السيبراني الوطني في ظل التحول الرقمي: قراءة في التأصيل المعرفي واستراتيجية المواجهة التشريعية. مجلة كلية القانون الكويتية، مج ١٠، ع ٣٧، ٥٢٥ - ٥٧٦.

شلوش، نورة. (٢٠١٨). القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول. مجلة مركز بابل للدراسات الإنسانية، مج ٨، ع ٢٤، ١٨٥ - ٢٠٦.

الشوابكة، عدنان عواد. (٢٠١٩). دور إجراءات الأمن المعلوماتي في الحد من مخاطر أمن المعلومات في جامعة الطائف. دراسات وأبحاث. مج. ١١، ع. ٤، أكتوبر ٢٠١٩. ص. ١٦٤-١٨٧.

الشيقي، إيناس إبراهيم (٢٠١٩) تقييم سياسات أمن وخصوصية المعلومات في المؤسسات التعليمية بالمملكة العربي السعودية دراسة تطبيقية على جامعة القصيم، ماجستير غير منشورة، جامعة القصيم.

الطاهري، عبد الفتاح. (٢٠١٩). الأمن المعلوماتي وعلاقته بالأمن القومي. مجلة الباحث للدراسات القانونية والقضائية، ع. ١٠، ٢١ - ٦٥.

العتيبي، عبد الرحمن بن بجاد (٢٠١٧) دور الأمن السيبراني في تعزيز الأمن الإنساني أطروحة ماجستير، جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية.

عزت، محمود. (٢٠١٨)، الفضاء السيبراني وتحديات الأمن المعلوماتي العربي، المجلة العربية العدد ٤٩٨.

القحطاني، عادل بن محمد ؛ مسعد، محمد رثيف مشرف. ؛ حرب، محمد خالد مناقش. ؛ المبرز، عبد الله بن إبراهيم مناقش. (٢٠١٤). تصور استراتيجي لتطوير أمن المعلومات تعزيزاً للأمن الوطني في المملكة العربية السعودية بالتطبيق على شركة سابك. أطروحة (ماجستير)-جامعة نايف العربية للعلوم الأمنية.

محمود، لى عبد الباقي، وكيطان، إسراء نادر. (٢٠٢١). المسؤولية الدولية عن الأضرار التي تحدثها الهجمات الإلكترونية. مجلة العلوم القانونية، مج ٣٦، عدد خاص، ٣٣٦ - ٣٦٢.

مصري، عبد القوي (٢٠٠٨). الجريمة الإلكترونية، الطبعة الأولى، (القاهرة: دار العلوم للنشر والتوزيع، ص (٦١).

المراجع الأجنبية:

- Kitsios, F.; Chatzidimitriou, E.; Kamariotou, M. (2022). Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry. *Sustainability*, 14, 1269.
- Mokhor, V., Honchar S. and Onyskova,A. (2020). Cybersecurity Risk Assessment of Information Systems of Critical Infrastructure Objects, *IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*, pp. 19-22.
- Sureshkumar, V and Baranidharan, B (2021). A study of the cloud security attacks and threats. *Journal of Physics: Conference Series*. 1-12.
- Vakulyk, O., Petrenko, P., Kuzmenko, I., Pochtovyi, M., & Orlovskiy, R. (2020). Cybersecurity as a Component of The National Security of The State. *Journal of Security & Sustainability Issues*, 9(3).
- Wibowo, E. & Ramli, K. (2022). Impact of Implementation of Information Security Risk Management and Security Controls on Cyber Security Maturity (A Case Study at Data Management Applications of XYZ Institute). *Jurnal Sistem Informasi*. 18. 1-17.

ملاحق الدراسة

استمارة الاستبيان



المملكة العربية السعودية
جامعة الجميع الذكية
كلية الإدارة العامة
قسم الإدارة

أهمية حماية المعلومات في ظل تصاعد هجمات القرصنة الإلكترونية:
دراسة ميدانية في المملكة العربية السعودية

عزيزي المشارك/المشاركة

السلام عليكم ورحمة الله وبركاته،،،

نقوم بإعداد دراسة ميدانية بعنوان " أهمية حماية المعلومات في ظل تصاعد هجمات القرصنة الإلكترونية :

دراسة ميدانية في المملكة العربية السعودية".

ونظرا لأهمية رأيكم في إثراء هذه الدراسة وتحقيق أهدافها من خلال خبراتكم العلمية والعملية. لذا نأمل منكم التكرم بالإجابة على الأسئلة الواردة في هذه الاستبانة بكل دقة، علماً بأن المعلومات التي سيرد ذكرها في هذه الاستبانة ستعامل بسرية تامة، ولن تستخدم إلا لأغراض البحث العلمي فقط.

شاكرين لكم حسن تعاونكم،،،

الباحثون

القسم الأول: المعلومات العامة

١. الجنس:

ذكر ()

أنثى ()

٢. العمر:

٣٠ سنة فأقل ()

٣١ - ٤٠ سنة ()

٤١ - ٥٥ سنة ()

٥٦ فأكثر ()

٣. المسمى الوظيفي:

مراجع مالي ()

تقنية معلومات ()

إداري ()

٤. المؤهل العلمي:

دبلوم ()

بكالوريوس ()

ماجستير ()

دكتوراه ()

٥. الخبرة العملية:

5 سنوات فأقل ()

٥-9 سنوات ()

١٠ سنوات فأكثر ()

٦. هل اطلعت على استراتيجية الامن السيبراني المعتمدة في المملكة العربية السعودية؟

☐ لا

☐ نعم

٧. هل أهداف استراتيجية الامن السيبراني تسهم في تحقيق التوجهات الحكومية وممكنات

الحكومة الذكية؟

☐ لا

☐ نعم

القسم الثاني: محاور الاستبانة

الرجاء تحديد العبارات التالية بما يتوافق مع آرائك:

غير موافق بشدة = ١ غير موافق = ٢ محايد = ٣ موافق = ٤ موافق بشدة = ٥

المحاور	١	٢	٣	٤	٥
المحور الأول: حماية المعلومات					
٨					كمية المعلومات التي يتم تداولها بشكل يومي كبيرة جداً
٩					٩- هناك برامج حماية للمستخدمين لحماية المعلومات من الاختراق
١٠					يلعب التهاون والإهمال الوظيفي دوراً مهماً في عمليات الاختراق وقلة حماية المعلومات وبالتالي قرصنتها
11					لقد تطور أمن المعلومات بشكل كبير في الآونة الأخيرة
12					هناك معرفة بالجهات المسؤولة عن حماية المعلومات ممثلة بالهيئة الوطنية للأمن السيبراني
13					عادة ما أشارك بياناتي الشخصية مع أي جهة دون التأكد من حماية بياناتي
14					تمتلك جهة عملي برامج حماية متطورة لحماية المعلومات
15					تقوم المواقع الإلكترونية والتطبيقات بطلب موافقتي قبل جمع بياناتي الشخصية
16					أقوم بقراءة سياسة الخصوصية عند تصفح المواقع الإلكترونية والتطبيقات
17					سبق وأن استخدمت بياناتي الشخصية بمواقع غير رسمية وغير معتمدة
18					أقوم بفتح رسالة وصلتني عبر البريد الإلكتروني من مصدر غير معروف
19					أتردد في الدخول إلى مواقع الإنترنت المجهولة خوفاً من الاختراق
20					أرسل صوري الخاصة ومعلوماتي الخاصة لأصدقائي دون خوف من اختراق هاتك لتلك المعلومات
21					أقوم بحظر كل من يصلني منه إزعاجات أو رسائل مشبوهة

المحور الثاني: القرصنة الإلكترونية					
22					دائماً ما تخترق أجهزتي بفيروسات بعد قيامي بتصفح الإنترنت

					بشكل دوري	
					من أبرز أسباب القرصنة جمع بيانات المستخدمين واستغلالها سياسياً واقتصادياً واجتماعياً وثقافياً	23
					تهدف شركات جمع البيانات، إلى خداع المستخدمين ودفعهم إلى الإدلاء ببياناتهم عبر تطبيقات تبدو حقيقية، ولكنها تحمل مهمات سرية لا يمكن للمستخدمين الاطلاع عليها	24
					تتطور عمليات القرصنة وسرعة فائقة باستخدام تقنيات حديثة ومعقدة	25
					تهدف شركات جمع البيانات، إلى خداع المستخدمين ودفعهم إلى الإدلاء ببياناتهم عبر تطبيقات تبدو حقيقية، ولكنها تحمل مهمات سرية لا يمكن للمستخدمين الاطلاع عليها	26
					يختلف مرتكبو جرائم القرصنة عن مرتكبي الجرائم الاعتيادية من حيث المبدأ وطريقة القيام بالعمل الاجرامي	27
					في الوقت الحالي لا يمكن وبأي شكل من الأشكال تجنب القرصنة الإلكترونية	28
					يمكن اعتبار القرصنة الإلكترونية في بعض الأوقات قرصنة أخلاقية	29
					لا يمكن القضاء على ظاهرة القرصنة الإلكترونية، ولكن يمكن التقليل من خطورتها	30
					اعي بخطورة القرصنة الالكترونية وبضرورة حماية الخصوصية على أي موقع أقوم بزيارته	31
					هناك قوانين رادعة لمعاقبة مرتكبي الجرائم الالكترونية او القرصنة والاختراق	32

القسم الثالث: صور الاختراقات

33. إن عملية الدخول الغير المشروع يمارسها الغير دون وجون حساب قانوني، وتعتبر اختراقا معلوماتيا يقع صاحبه تحت طائلة المسائلة القانونية؟ من وجهة نظرك ماهي الاختراقات التي يمكن التعرض لها حسب طبيعة عملك

ت	العوامل	درجة الاختراق		
		عالية	متوسطة	لا يوجد
١	اتلاف الوثائق الالكترونية والمعلومات الهامة			
٢	انتهاك خصوصية الغير			
٣	الاحتيايل المالي الالكتروني			
٤	اختراق وسرقة كلمات (السر) للبريد الالكتروني والحسابات والبطائق البنكية			
٥	ارسال الفيروسات الحاسوبية للشبكة واحداث اضرار فيها.			
٦	اختراق المواقع الحكومية الحساسة			
٧	أرسل صوري الخاصة ومعلوماتي الخاصة لأصدقائي دون خوف من اختراق هاكل لتلك المعلومات			
٨	أقوم بحذف الرسائل الخاصة أولا بأول			
٩	أقوم بحفظ كلمات السر الحساسة في جهاز الحاسب			
١٠	لا أسجل دخول لحساباتي الشخصية من أجهزة الآخرين			

34. هل تعتقد أن اللوائح والتشريعات المتعلقة بأمن المعلومات والخصوصية قادرة على معالجة التحديات والمخاطر المعلوماتية في ظل تصاعد عمليات الاختراق والقرصنة الالكترونية، ولماذا؟

.....

.....

مع خالص الشكر والتقدير،،،

ملخص الدراسة العربي

برزت في الآونة الأخيرة ظاهرة القرصنة الإلكترونية والتي تهدف بالأساس إلى الاستيلاء على المعلومات المهمة سواء بين الشركات المتنافسة أو بين الدول بعضها البعض، وتلك ظاهرة خطيرة يجب الحذر منها وخاصة في المؤسسات أو المنظمات الحيوية في الدولة التي تحتوي على معلومات خطيرة تمس أمن الدولة واستقرارها، ولذلك تكمن معضلة هذا البحث في (التعرف على أهمية حماية المعلومات في ظل تصاعد هجمات القرصنة الإلكترونية والتأثيرات المتعددة على المعلومات وخاصة في المؤسسات الحيوية والعلاقات بين الدول وسبل مكافحتها وما هو مستقبلها في ظل التقدم التقني). وتكمن الأهمية العلمية لهذه الدراسة في أنها إضافة معرفية من خلال تتبع الدراسات السابقة والمفاهيم والنظريات التي تناولت ظاهرة القرصنة الإلكترونية وأهمية حماية المعلومات ودوره في حماية المصلحة العامة ومصالح المستخدمين والمحافظة على سرية الاتصالات وأمن المعلومات، وفقاً لأعلى معايير الجودة والأمان. لذا يعتبر هذا البحث أداة قيمة للمؤسسات العامة والخاصة التي ترغب في تعزيز أمنها الإلكتروني وحماية المعلومات والحد من مخاطر القرصنة الإلكترونية التي قد تتعرض لها هذه القطاعات. كما تكمن أهمية هذا البحث في المساهمة في إيجاد طرق لمواجهة القرصنة الإلكترونية بطريقة أكثر فعالية، وفي التوعية المجتمعية حول أخطار استمرار القرصنة الإلكترونية في المستقبل بتهديد الإبداع والابتكار والسيطرة على معلومات وبيانات غاية في السرية قد تستخدم استخداماً سيئاً لتدمير دولة ما أو مجتمع معين.

وقد اعتمدت الدراسة على المنهج الاستقرائي في إعداد الجزء النظري، حيث سيتم استقراء المواضيع والدراسات المتعلقة بموضوع البحث وذلك لتكوين الإطار النظري. أما في الجانب العملي. واعتمدت الدراسة على المنهج الوصفي التحليلي في الحصول على كافة المعلومات والبيانات اللازمة لتحقيق أهداف الدراسة واغراضها. ويتمثل المنهج الوصفي التحليلي. المنهج الوصفي كونه منهجاً يناسب أهداف الدراسة الحالية. ويمثل المنهج الوصفي طريقة لوصف الموضوع المراد دراسته من خلال منهجية علمية صحيحة، وتصوير النتائج التي يتم التوصل إليها. ويتضمن وصف متغيرات الدراسة المستقلة والمتمثلة في أهمية حماية المعلومات، والمتغير التابع المتمثل في تصاعد هجمات القرصنة الإلكترونية. والمنهج التحليلي ويهدف الى تحليل وتقييم أهمية حماية المعلومات في ظل تصاعد هجمات القرصنة الإلكترونية.

واهم ما خلص اليه هذه الدراسة تتمثل في أهمية الحذر من الوسائل المختلفة للقرصنة ومحاربتها بشتى الوسائل المتاحة. لقد نجحت المملكة العربية السعودية في وضع استراتيجية الامن السيبراني التي بدورها حددت اللوائح والتشريعات المتعلقة بأمن المعلومات والخصوصية قادرة على معالجة التحديات والمخاطر المعلوماتية في ظل تصاعد عمليات الاختراق والقرصنة الالكترونية. وتعتبر اللوائح والتشريعات المتعلقة بأمن المعلومات والخصوصية قادرة على معالجة التحديات والمخاطر الالكترونية في ظل تصاعد عمليات الاختراق والقرصنة الالكترونية. وتعتبر الدول الأكثر تطوراً من الناحية التقنية، هي الأكثر تعرضاً لحرب المعلومات. ورغم كل الوسائل الوقائية، لا يوجد نظام أمن يحمي المعلومات حماية تامة وكاملة. وهناك حاجة الى اجراء المزيد من الدراسات المتعلقة بأمن المعلومات في جميع القطاعات المدنية والعسكرية وهذا يؤثر على سرية وامن المعلومات وحفظها وتبادلها الأمر الذي يتطلب إجراء دراسات عن دور السياسات الأمنية في مواجهة جميع مهددات أمن المعلومات.

ملخص الدراسة الإنجليزي - Summary

The phenomenon of electronic piracy has emerged, which is primarily aimed at stealing important information, whether between competing companies or between countries, and this is a dangerous phenomenon to be aware of, particularly in important institutions or organizations in the country that contain dangerous information that affects the security and stability of the state, and thus the dilemma of this study is to ((identify the importance of protecting information in the country

The scientific importance of this study lies in the fact that it adds to the body of knowledge by identifying previous studies, concepts, and theories that have addressed the phenomenon of electronic piracy and the importance of protecting information and its role in protecting the public interest and the interests of users, as well as maintaining the confidentiality of communications and the security of information while maintaining the highest standards of quality and security. Therefore, this study is considered a valuable tool for public and private entities that wish to improve their electronic security, protect the information, and reduce the risks of electronic piracy to which these sectors may be exposed. The importance of this study also lies in the fact that it contributes to finding ways to address electronic piracy more effectively and to raising community awareness of the dangers that a continuation of electronic piracy in the future poses by threatening creativity, innovation, and control over highly confidential information and data that can be maliciously used to destroy a country or a particular society.

The study relies on an inductive approach in preparing the theoretical part, extrapolating the issues and studies related to the research subject to form the theoretical framework. As for the practical part: The study relies on the analytical-descriptive approach to obtain all the information and data needed to achieve the study's objectives. The descriptive-analytical approach A descriptive approach is one that fits the objectives of this study. The descriptive approach is a way of describing

the subject under study through proper scientific methodology and presenting the results obtained. It includes a description of the independent variables of the study, represented by the importance of information protection, and the dependent variables, represented by the escalation of electronic piracy attacks. An analytical approach aimed at analyzing and evaluating the importance of information protection in relation to the escalation of electronic piracy attacks

The main conclusion of this study is that it is important to be wary of the various means of piracy and to fight them with all available means, according to the responses of the study participants. Saudi Arabia has managed to develop a cybersecurity strategy, which in turn sets regulations and laws related to information security and privacy and can address informational challenges and risks in the face of escalating electronic hacking and piracy. The countries that are more technologically advanced are the most exposed to information warfare

Despite all precautions, no security system fully protects information. More studies need to be conducted on information security in all civilian and military sectors. This concerns the confidentiality and security of information, as well as its preservation and sharing, which requires conducting studies on the role of security policy in addressing all information security threats.