

القرصنة الإلكترونية: أنواعها أشكالها وطرق التصدي لها

E-piracy: its types, forms, and ways to confront it

بوغرة الصالح

كلية الحقوق والعلوم السياسية

جامعة تيارت

bougherara@gmail.com

بن شريف أحلام *

كلية الحقوق والعلوم السياسية

جامعة تيارت

bencherifahlam@gmail.com

تاريخ القبول: 2012/05/09

تاريخ الاستلام: 2012/03/22

Abstract: This paper deals with the subject of electronic piracy. We often hear the word piracy, and we imagine the gangs of theft and robbery of ships, and the imprisonment of his crew, which is exactly what the pirates of the electronic systems do, but with modern means and without endangering themselves. Electronic hacking or computerization is a process of computer hacking that occurs over the Internet often because most computers in the world are connected via this network or even through internal networks connected to more than one computer. This operation is carried out by one or several people who are proficient in computer programs and their management methods; That is, they are high-level programmers who can, by means of software, help penetrate a computer and identify its contents, through which the other connected devices are hacked into the same network.

Keywords: hacking, technological, informatics, electronic, digital, social networking sites.

ملخص: تتناول هذه الورقة موضوع القرصنة الإلكترونية، فكل ما يتبادر إلى أذهاننا كلمة قرصنة، فإننا نتخيل عصابات سرقة السفن البحرية والسطو عليها، ونهب ما فيها وأسر طاقمها، وهو ذاته ما يفعله قرصان الأنظمة الإلكترونية بالضبط، لكن بوسائل حديثة، ودون أن يعرض نفسه للخطر. فالقرصنة الإلكترونية أو المعلوماتية هي عملية اختراق لأجهزة الحاسوب تتم عبر شبكة الإنترنت غالباً، لأن أغلب حواسيب العالم مرتبطة عبر هذه الشبكة، أو حتى عبر شبكات داخلية يرتبط فيها أكثر من جهاز حاسوب، ويقوم بهذه العملية شخص أو عدة أشخاص متمكنين في برامج الحاسوب وطرق إدارتها، وهم ذوي مستوى عالٍ يستطيعون بواسطة برامج مساعدة اختراق حاسوب معين والتعرف على محتوياته، وحتى اختراق باقي الأجهزة المرتبطة معها في نفس الشبكة.

الكلمات المفتاحية: القرصنة، التكنولوجيا، المعلوماتية، الإلكترونية، رقمية، مواقع التواصل الاجتماعي.

بن شريف أحلام / بوغرارة الصالح: القرصنة الإلكترونية: أنواعها أشكالها وطرق التصدي لها

المقدمة:

يشهد العالم حاليا ثورة هائلة في تكنولوجيا المعلومات حيث دخلت تطبيقاتها مختلف ميادين الحياة، فبدأت ظاهرة القرصنة والاختراق مع بداية ظهور الحاسبة الإلكترونية، وازدادت بشكل كبير مع استخدام تقنية الشبكات؛ حيث يشمل الاختراق الهجوم على شبكات الحاسوب من قبل مُخترقي الأنظمة الإلكترونية ومنتَهكي القوانين، كما يبيّن التطوُّر الحاصل في مجال سِرِّة المعلومات التي تغطّي الإنترنت بالإضافة إلى تقنيات أخرى كالاتّصالات، كم أن عمليات القرصنة تتطوّر وبسرعة فائقة باستخدام تقنيات حديثة ومعقّدة مما يستوجب التصدي لها.

الإشكالية التي يتناولها المحور :

من خلال هذا نطرح إشكالية هذه المداخلة على النحو التالي:

ماهي القرصنة الالكترونية وماهي أنواعها وأشكالها ؟

وماهي الطبيعة الموضوعية لهذا النوع من الجرائم ،وماهي خصائصها ومخاطرها وسمات مرتكبها ودوافعها؟

أهم المحاور التي تتناولها الورقة البحثية :

أولا: مفهوم القرصنة الالكترونية:

- تعريف القرصنة الإلكترونية
- تصنيف قرصنة المعلومات والطرق المتبعة في ذلك

ثانيا: أسباب القرصنة الالكترونية والحماية القانونية والمعلوماتية لها :

- الأسباب التي تدفع إلى ارتكاب جرائم القرصنة المعلوماتية
- الحماية القانونية والالكترونية من القرصنة المعلوماتية

أهداف الورقة البحثية :

- ✓ التعريف بهذا النوع من الجرائم (جريمة القرصنة الالكترونية)
- ✓ التوعية والتحسيس من مخاطر التعرض لها
- ✓ محاولة التصدي لهذا النوع من الجرائم مع تقديم حلول
- ✓ معرفة كيفية حماية المعطيات المقدمة الكترونيا

أولاً: مفهوم القرصنة الإلكترونية

هناك عدة مصطلحات يمكن أن تستخدم للتعبير عن الظاهرة الجرمية الناشئة في بيئة الحواسيب الإلكترونية والشبكات كسوء الاستخدام ، الاحتيال ، الجريمة المعلوماتية ، جرائم القرصنة ، الاختراق وجرائم الانترنت.

إن اختيار المصطلح يتعين بارتباط البعدين التقني والقانوني ، فإذا عدنا للحقيقة الأولى المتصلة بنشأة وتطور تقنية المعلومات نجدها تشمل فرعين جرى بحكم التطور تقاربهما واندماجهما هما الحوسبة والاتصالات ، فتقوم الحوسبة على استخدام التقنية لإدارة وتنظيم ومعالجة البيانات في إطار تنفيذ مهام محددة تتصل بعلمي الحساب والمنطق، إما الاتصال فقائم على وسائل تقنية لنقل المعلومات بجميع دلالاتها الدارجة.

يتبين لنا من ذلك إن من الصعوبة إيجاد مصطلح شامل يعبر عن كل الحالة الجرمية المرتكبة التي يقوم بها المخترقون ، فإذا وصفنا جريمة معينة بأنها جريمة اتصالات فليس بالضرورة إن تكون مرتبطة بالحاسوب أو الانترنت وإنما مقتصرة على سرقة خطوط هاتفية مثلاً ، وإذا وصفنا حالة أخرى بأنها جريمة حاسوب فليس بالضرورة إن يكون لها علاقة بأجهزة الاتصال وإنما قد تكون زرع برنامج فيروس في حاسوب ما.

لذا يجب إن يكون المصطلح المستخدم لوصف جرائم المعلوماتية شاملاً لمعنى الجريمة بكل تفاصيلها وتفرعاتها.

1- تعريف القرصنة الإلكترونية

قراصنة الإنترنت، أصبح الاسم المرعب لمستخدمي الشبكة العنكبوتية، حيث أصبح "الأمن الإلكتروني" أكثر ما يبحث عنه مستخدمو تلك الشبكة، ليتعداه الأمر إلى الدول التي بات همّها الشاغل هي الأخرى حفظ أمنها الإلكتروني، ولعلّ تسريب وثائق "ويكيليكس" ونشرها يُعدُّ أكبر عملية قرصنة شهدتها الشبكة العنكبوتية، حيث تعتبر عملية القرصنة هذه سياسيةً بحثة، ناهيك عن آلاف عمليات القرصنة التي تحدث يومياً ولأهداف مختلفة؛ منها المالي وآخر انتقامي وفضائي وما إلى هنالك من أسباب تدعو القراصنة إلى مثل هذه الأفعال¹.

¹ أمل المرشدي ، بحث قانوني حول جريمة القرصنة الإلكترونية <http://www.mohamat.net/law/dl.52.com>

بن شريف أحلام / بوغرارة الصالح: القرصنة الإلكترونية: أنواعها أشكالها وطرق التصدي لها

إن مفهوم القرصنة الإلكترونية يشير بالضرورة إلى استخدام وسائل الاتصال تكنولوجيا المعلومات الحديثة في ممارسات غير مشروعة تهدف إلى التحايل على الأنظمة المعالجة الآلية للبيانات وكشف البيانات الحساسة المصنفة أو تغييرها والتأثير على سلامتها أو حتى إتلافها، فالقرصنة ما هي إلا عملية دخول غير مصرح به إلى أجهزة الغير وشبكاتهم الإلكترونية، أي أن توجه هجمات آلة معلومات الكمبيوتر أو خدماته بقصد المساس بالسرية أو المساس بسلامة المحتوى أو تعطيل قدرة وكفاءة أنظمة الكمبيوتر وبشكل خاص المعلومات المخزنة داخله، فالقرصنة إذن تعني الوصول بطريقة غير مشروعة من خلال ثغرات في نظام الحماية الخاص بالهدف.²

2- أنواع القرصنة

تتنوع وتختلف القرصنة حسب الدافع والغاية منها فنجد القرصنة الانتقامية والقرصنة السياسية، القرصنة الذاتية وقرصنة الهواة، القرصنة الاحترافية وغيرها نلخصها في التالي:

أ- القرصنة الانتقامية

والتي غالباً ما تكون بين دول على خلاف سياسي، وهو ما يمكن رؤيته بين إيران أو كوريا الشمالية أو حتى مجموعات مؤيدة للقضية الفلسطينية من جهة وبين دولة الاحتلال الإسرائيلي، حيث تمّ تسجيل أكثر من هجوم إلكتروني شنه قراصنة إيرانيون استهدفوا خلاله صحف ومواقع إلكترونية إسرائيلية.³

ب- قرصنة سياسية: ربما يُعدُّ هذا النوع أشهر عمليات القرصنة على الإنترنت، حيث تؤكد الإحصائيات أن 58% من كل البيانات المسروقة كانت تتم من قبل مجموعات ناشطة في مجال القرصنة السياسية، وعلى رأس مجموعات القرصنة لأغراض سياسية مجموعة "أنونيموس" والتي حققت العديد من النجاحات في السيطرة على عدد من المواقع السياسية، بالإضافة لتمكّنها من سرقة كميات كبيرة من البيانات من بعض الشركات الخاصة والمؤسسات

² الموقع الخاص بالأكاديمية العربية البريطانية للتعليم العالي.

³ د أحمد شربتجي، د. وقائي بغدادي، الحماية وتأمين الانترنت التحدي القادم وأساليب المواجهة، سلسلة العلوم والتكنولوجيا، الهيئة المصرية العامة للكتاب القاهرة، سنة 2010، ص51.

الحكومية، حيث يؤكد خبراء على أنّ القرصنة لأغراض سياسية أصبحت إحدى آليات الاحتجاج السياسي، مشيرين إلى أنّه من الصعب تطوير نظم دفاعية محددة ضد هذه الهجمات الإلكترونية لأن مجموعات القرصنة السياسية تستخدم وسائل وأساليب خاصة يتم ابتكارها لكل مناسبة بعينها⁴.

ج- قرصنة ذاتية: في هذا النوع من القرصنة تقوم بعض الدول بـ "قرصنة نفسها" لتكون هذه العملية مقدمة لاتهام دول أخرى بهذه القرصنة، وهذا ما يُمكن مشاهدته من خلال الاتهامات الأمريكية وبعض الدول الغربية لروسيا بأنها تقوم بالتدخل بانتخابات هذه الدول، وذلك في محاولة لإشغال فتيل أزمة فيما بينها.

د- قرصنة الهوية: وفي قرصنة الهوية أو الفضائح يقوم بعض القراصنة باختراق المواقع الشخصية للشخصيات العامة بغية جمع معلومات أو صور أو محادثات خاصة بهذه الشخصية ليقوما بعد ذلك بنشرها على العلن، وفي بعض الحالات يتم ابتزاز تلك الشخصيات مقابل الحصول على مبلغ من المال.

أما في القرصنة المالية يقوم القراصنة باستغلال الثغرات الأمنية للبنوك أو ماكينات الصرف الآلي ليقوموا بتحويل ملايين الدولارات إلى حساباتهم الشخصية، أو يقوموا بعمليات شراء من الإنترنت دون أن يقوموا بدفع أية مبالغ.

هـ- قرصنة مستحدثة: يبرز هذا النوع من القرصنة من خلال استهداف الذات عبر المنصّات الإعلامية لدول العدو وذلك بهدف تحقيق جملة من الأهداف السياسية والعسكرية، وربما تظهر الحالة -القطرية - الخليجية- كواحدة من أبرز عمليات القرصنة الذاتية، حيث تمّ قرصنة وكالة الأنباء القطرية من قبل الإمارات -في حال صحّت ادعاءات الدوحة- وتمّ من خلال هذه القرصنة نشر أخبار من شأنها تأزيم العلاقات بين الدولتين الجارتين.

وبعد عملية القرصنة هذه اندلعت الأزمة الخليجية التي ما تزال ممتدة حتى يومنا هذا، وهنا يؤكد مراقبون أنّ الأخبار التي نُشرت على وكالة الأنباء القطرية أو التلفزيون القطري كانت من قبل القراصنة التابعين للإمارات، ولو لم يكن ذلك؛ لكانت الإمارات تفهمت بأنّ ما تمّ عرضه ناتج عن عملية قرصنة، غير أنّ مراقبين يؤكدون أن الإمارات كانت تسعى إلى هذه الأزمة وكانت عملية الاختراق هذه مجرد وسيلة لإشغال فتيل الأزمة الخليجية.

⁴ محمد سامي الشوام، ثورة المعلومات وانعكاساتها على قانون العقوبات، مطابع الهيئة للكتاب، مصر 2008، ص 38.

بن شريف أحلام / بوغرارة الصالح: القرصنة الإلكترونية: أنواعها أشكالها وطرق التصدي لها

ويقوم بعملية القرصنة أشخاص هواة ومحترفين ،تم تعريفهم كالتالي: أشخاص لهم القدرة على التعامل مع أنظمة الحاسب الآلي والشبكات ،بحيث تكون لهم القدرة على تخطي أي إجراءات أو أنظمة حماية ،اتخذت لحماية تلك الحسابات أو الشبكات وهؤلاء المخترقين يتم تصنيفهم إلى نوعين أولهم : هم الهاكرز HAKERS وهم أشخاص لهم القدرة الفائقة على اختراق الأجهزة والشبكات أيا كانت إجراءات وبرامج الحماية التي تم اتخاذها، إلا أنهم لا يقومون بأي من الإجراءات التي تؤدي إلى إلحاق أضرار نتيجة الاختراق جهاز أو شبكة أما CRACKERS الكراكرز فهؤلاء يطلق عليهم المخربين وهم يتشابهون مع الهاكرز في قدرتهم الفائقة على الاختراق وتخطي إجراءات وبرامج الحماية ، إلا أنهم يقومون بالعبث بالمعلومات المخزنة على تلك الحسابات والشبكات و سنأتي إلى تصنيفهم في التالي:

2- أصناف القرصنة

يمكن تصنيف القرصنة إلى صنفين وهما كالتالي:

أ- الهاكرز HACKERS:

يعتمد الهواة على برامج التجسس الجاهزة والمتاحة في كل مكان، سواء عن طريق الشراء أو التحميل من شبكة الإنترنت، ويقوم الهاكرز بزرع ملفات التجسس patches Trojans& في حواسيب الضحايا عن طريق البريد الإلكتروني أو ثغرات الويندوز التي يكتشفها البرنامج، هذا الصنف من الهاكرز أهدافه طفولية؛ حيث يسعى لإثبات نجاحه في استخدام هذه البرامج وانضمامه إلى قائمة الهاكرز؛ بهدف التفاخر بين الأصحاب كشخص يمتلك مواهب يفقدها بعضهم، وهؤلاء كل ما يشغلهم هو التسلّل إلى حواسيب الآخرين وسرقة بريدهم الإلكتروني، والتلاعب في إعدادات هذه الأجهزة، مع ترك ما يفيد أنهم فعلوا ذلك كشكل من أشكال الغرور والتباهي بالنفس،

في التعريف الذي تقدمه الموسوعة الإلكترونية المفتوحة "ويكيبيديا" يعرف الهاكرز بأنهم "مجموعة من المبرمجين الأذكياء الذين كانوا يتحدون الأنظمة المختلفة ويحاولون اقتحامها، وليس بالضرورة أن يكون في نيتهم ارتكاب جريمة أو حتى جنحة، ولكن نجاحهم في الاختراق يعتبر نجاحا لقدراتهم ومهارتهم".

غير أنه بالنسبة لعامة الناس يبقى "الهكرز" مجرد فتية يقومون بالسطو على المواقع والشبكات متسببين بالأذى والخسائر المادية والأمنية والمعنوية، إلى جانب تشويههم صورة مؤسسات كبرى وعالمية جراء هزيمتها أو عجزها عن صد هجمات ينفذها مراهقون، وهذا صحيح إلى حد كبير، لكن معرفة الدوافع يمكنها أن تقود إلى فهم سيكولوجية الهاكر وبيئته، ويمكنها أيضا أن توضح أن عمل القراصنة هو -في أحد وجوهه- محرك حقيقي للإبداع التكنولوجي.⁵

• مهارات الهكرز

للهمكر مهارات، وهي أنهم يستطيعون اختراق مواقع الشركات، واختراق وفك كلمة السرّ، سواء الخاصة بالبريد الإلكتروني، أو موقع شركة على الإنترنت، أو فك "السيريل نمبر" عند تثبيت برنامج.

لهذا النوع من الفتية الشغوفين بتكنولوجيا الحاسوب والإنترنت أو المهووسين فيهما والمعروفين اختصارا بالقراصنة أو الهكرز "ثقافة ونمط تفكير"، يصعب على غير المنخرط في هذا العالم تخيل وجود هذا التصنيف وواقعيته ما لم يدخل في حوار مع الجهات التي تتعامل مع المشاكل التقنية التي يتسبب بها القراصنة، أو مع المعجبين بهم وبفتوحاتهم.

في التعريف الذي تقدمه الموسوعة الإلكترونية المفتوحة "ويكيبيديا" يعرف الهكرز بأنهم "مجموعة من المبرمجين الأذكياء الذين كانوا يتحدون الأنظمة المختلفة ويحاولون اقتحامها، وليس بالضرورة أن يكون في نيتهم ارتكاب جريمة أو حتى جنحة، ولكن نجاحهم في الاختراق يعتبر نجاحا لقدراتهم ومهارتهم".⁶

"إذا كان التلفون بالنسبة لمعظم الناس هو هاتف ذكي فهو بالنسبة للهكر حاسوب صغير قادر على القيام بمهام مغايرة لما صمم أساسا لأجله".

ب- المحترفون الكراكرز: Crackers

⁵ علي السيد الباز، الحكومة الإلكترونية والادارة المحلية، الادارة المحلية الإلكترونية العربية : متاح عبر: www.arabia/law/info.com

⁶ علي سد الباز، المرجع السابق، ص 45.

بن شريف أحلام / بوغرارة الصالح: القرصنة الإلكترونية: أنواعها أشكالها وطرق التصدي لها

أما المحترفون أو الكراكرز فهم الفريق الأخطر؛ لأنهم يعلمون ماذا يريدون، وماذا يفعلون، وكيفية الوصول إلى أهدافهم باستخدام ما لديهم من علم يطوّرونه باستمرار، بالإضافة إلى استخدام البرامج الجاهزة المتطورة، إلا أنهم يعتمدون على خبرتهم في لغات البرمجة والتشغيل، وتصميم وتحليل وتشغيل البرامج بسرعة، كما أنّ هوايتهم الأساسية معرفة كيفية عمل البرامج لا تشغيلها.⁷

إنّ أهداف هذا الفريق أكبر وأخطر من الفريق السابق؛ فأهدافهم المصارف وسحب الأموال من حساب العملاء، أو الولوج إلى أخطر المواقع وأكثرها حساسية، والتلاعب ببياناتها أو تدميرها.

ج- مبالون للتحدي

يقول خبير في أمن المعلومات سمعنا منه لأول مرة مصطلح "ثقافة الهاكرز" للجزيرة نت إن هؤلاء "يميلون بطبيعتهم إلى التحدي، لذا فهم يتدعون دائما طرقا جديدة للعمل". ويمضي الخبير -الذي فضل عدم الإفصاح عن هويته- قائلا إن "فلسفة الهاكر قائمة على مخالفة القوانين" التي تبعها الناس، وعلى ما سماه "التفكير خارج الصندوق"، إلى جانب "التحيز للإبداع في تناول المعلومة بطريقة مخالفة للساند". ويعطي الخبير على ذلك مثلا "إذا كان التلفون بالنسبة لمعظم الناس هو هاتف ذكي فهو بالنسبة للهاكر حاسوب صغير قادر على القيام بمهام مغايرة لما صمم أساسا لأجله".⁸

والهاكر مجهول الهوية والاسم في الأغلب، لكنه يعرف من نتائج أفعاله، ومن الاسم المستعار الذي يستخدمه أثناء قيامه بهجوم ما أو إعلان مسؤوليته عنه.. هذا ما قاله مهندس برمجيات يعمل في إحدى الشركات الكبرى بالدوحة.

د-هاكرز" باتجاهين

⁷ معتوق عبد اللطيف، الاطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن مذكرة لنيل شهادة الماجستير في العلوم الجنائية سنة 2011، منشورة، 36.

⁸ ريموتر "السعودي" ريموتر" لديه "هاشتاغ- وسم- وصفحة وتويتر، ويمكنك التعرف عليهم مناعمالهونصوصه".

هو فتى دون الـ18 في الأغلب، تختفي عيناه خلف نظارات سميقة، محب للعزلة، قليل الكلام والاختلاط حتى مع أفراد عائلته، مهووس بالحاسوب، ويقضي ساعات طويلة أمام شاشته، أما لوحة المفاتيح التي يستخدمها فضاع لونها الأصلي، واختفت أغلبية حروفها لكثرة الاستخدام.

تلك هي الصورة النمطية لقرصان الحاسوب، وهي صورة تعكس الواقع في كثير من الأحيان، إلا أن الأفعال التي يأتي بها عباقرة الزمن الرقمي هؤلاء ستبقى مصدر تهديد دائم للمؤسسات، لكن مصائر المنخرطين فيها يمكن أن تسير في اتجاهات متعارضة⁹.

"سيرتا الصحفي الأسترالي المثير للجدل جوليان أسانج، والهاكر الأميركي ستيفن ميتنيك تعطيان فكرة عن طريقين يمكن أن يسلكهما "الهاكر": طريق مواجهة المؤسسات ومقارعتها برؤية سياسية، أو طريق التوبة عن الإجرام الإلكتروني، وتسخير العبقرية الرقمية استثماريا أو في خدمة المؤسسات"

سيرتا الصحفي الأسترالي المثير للجدل جوليان أسانج، والهاكر الأميركي ستيفن ميتنيك تعطيان فكرة عن طريقين يمكن أن يسلكهما "الهاكر": طريق مواجهة المؤسسات ومقارعتها برؤية سياسية، أو طريق التوبة عن الإجرام الإلكتروني، وتسخير العبقرية الرقمية استثماريا أو في خدمة المؤسسات.

أسانج بدأ قرصنة الحاسوب -حسب مصادر متطابقة- عام 1987 وهو في الـ16، وكان يستخدم اسم "منداكس"، وقد شكل مع اثنين من رفاقه مجموعة تدعى القرصنة الأخلاقية أو المخربين العالميين، وقاموا باختراق مواقع حكومية أميركية كبرى، بينها وزارة الدفاع (البنتاغون) ومنشآت تتبع لها كالقوات البحرية، إضافة إلى وكالة الفضاء الأميركي (ناسا) وشركات "زيروس"، وفي بلده أستراليا اخترقت مجموعة القرصنة الأخلاقية مواقع الجامعة الوطنية، وشركة الاتصالات وسيتي بنك وشركات أخرى.

3- مجموعات.. قرصنة نضالية

⁹ علي سيد الباز، المرجع السابق، ص36.

بن شريف أحلام / بوغرارة الصالح: القرصنة الإلكترونية: أنواعها أشكالها وطرق التصدي لها

تأثر القرصنة في أنحاء العالم بالمشاكل المحلية لمجتمعاتهم وكذلك بالقضايا السياسية التي تشغل اهتمام الناس. وسخروا قدراتهم التقنية والعمليات التي ينفذونها في سبيل نصرة قضايا سياسية أو اجتماعية أو فكرية بعينها. وهناك عدة قرصنة يعملون كمجموعات في أرجاء العالم بينهم "غارديينز أوف بيس" الذين هاجموا "سوني إنترتينمنت" وهذه أبرز المجموعات.

أ- أنونيموس Anonymous أو القرصنة المجهولون

وهي مجموعة غير مركزية من القرصنة المنتشرين في العالم والتي أصبحت ذات ثقل كبير في ما تسمى الحرب الإلكترونية، ونفذت العديد من الهجمات الإلكترونية المؤثرة مثل تسريب آلاف رسائل البريد الإلكتروني الخاصة بالرئيس السوري بشار الأسد، ومهاجمة مواقع حكومية أمريكية وبريطانية وأخرى للناتو، إلى جانب مهاجمتها مواقع إلكترونية حكومية إسرائيلية في كل مرة تشن فيها إسرائيل عدوانا عسكريا ضد قطاع غزة.

إنَّ عمليات القرصنة تتطوّر وبسرعة فائقة باستخدام تقنيات حديثة ومعقّدة؛ ممّا جعل النّظرة إليها تتغيّر كليّاً عمّا كانت عليه في المراحل السّابقة، فلا يمكن فعليا تحديد الفترة الزمنية لأول عملية اختراق، وذلك لأنّ مفهوم الاختراق قديما لم يكن يعني مجرد اختراق شبكة حاسوب أو موقع إلكتروني، وإنما كان اختراق أي جهاز لتحقيق هدف خاص يسمى اختراقا، في عام 1903 كان الفيزيائي جون أمبروز فلمنج يستعد لعرض إحدى العجائب التكنولوجية المستجدة وهي نظام تلغراف لاسلكي بعيد المدى ابتكره الإيطالي جوليلمو ماركوني، في محاولة لإثبات أن رسائل شفرة مورش يمكن إرسالها لاسلكيا عبر مسافات طويلة، وكان ذلك أمام جمهور غفير في قاعة محاضرات المعهد الملكي الشهيرة بلندن.

وقبل بدء العرض بدأ الجهاز ينقر مكونا رسالة، كانت في البداية كلمة واحدة ثم تحولت إلى قصيدة ساخرة بشكل غير لائق تتهم ماركوني "بخداع الجمهور"، فقد تم اختراق عرض ماركوني وكان المخترق هو الساحر والمخترع البريطاني نيفيل ماسكيلين الذي قال لصحيفة تايمز إن هدفه كان كشف الثغرات الأمنية من أجل الصالح العام.¹⁰

¹⁰ الموقع الإلكتروني: <http://etudiantdz/cybernetatach.com/vb/html/>

في عام 1932 تمكن خبراء التشفير البولنديون ماريان ريجيوسكي وهنري زيجلاسكيوجيرزيروزيكي من فك شفرة جهاز إننيغما الذي استخدمه بشكل خاص الألمان خلال الحرب العالمية الثانية لإرسال واستقبال رسائل سرية.

في عام 1971 ابتكر جون درابر-الملقب بكابتن كرننتش- وصديقه جو إنغريسيا الصندوق الأزرق الذي استخدماه للتحايل على نظام الهاتف وإجراء مكالمات هاتفية بعيدة المدى مجانا.

إن بداية القرصنة الالكترونية تعود إلى الستينات إذ ارتبط ظهورها إلى ظهور أولى الحواسيب الالكترونية إلا أن أول عملية قرصنة كانت في سنة 1878 بإحدى شركات الهاتف المحلية الأميركية وفي نظر خبراء المعلوماتية أن الفترة ما بين 1980 إلى 1989 فترة العصر الذهبي للقرصنة الالكترونية. وفي عام 1981 تشكلت مجموعة قراصنة "نادي فوضى الحاسوب" في ألمانيا، ومجموعة "أسياد البرامج" (وير لوردز) في أميركا التي تتألف من العديد من المتسللين المراهقين ومخترقي الهاتف والمبرمجين والعديد من قراصنة الحاسوب الذين يعملون في الخفاء. وفي عام 1988 ظهرت "دودة موريس" -إحدى أوائل ديدان الحواسيب المعروفة التي أثرت في البنية التحتية للإنترنت وانتشرت في الحواسيب وعلى نطاق واسع داخل الولايات المتحدة، واستغلت الدودة نقطة ضعف في نظام يونيكس "ناون 1" واستنسخت ذاتها بانتظام وتسببت بإبطاء أداء الحواسيب لدرجة عدم القدرة على استخدامها¹¹.

وعند اعتقال مطور هذه الدودة روبرت تابان موريس أصبح أول قرصان يدان تحت قانون "احتيال الحاسوب وإساءة الاستخدام"، وهو الآن أحد القراصنة الأخلاقيين (أصحاب القبعات البيضاء) حيث يعمل بروفيديسورا في معهد ماساتشوستس للتكنولوجيا، كما أن أشهر الحروب الالكترونية هي حرب الهاكرز العظمى والتي كانت بين 1990 و1994 بين فريقين من الهاكرز المحترفين، حيث سعى كل فريق لاختراق حواسيب الآخر في صيف عام 1994 تمكن قرصان روسي يدعى فلاديمير ليفين من اختراق بنك "سي تي بنك" الأميركي وتحويل عشرة ملايين دولار من حسابات عملاء إلى حساباته الشخصية في فنلندا وإسرائيل مستخدما حاسوبه

¹¹ محمد سامي الشوا، المرجع نفسه، ص29.

بن شريف أحلام / بوغرة الصالح: القرصنة الإلكترونية: أنواعها أشكالها وطرق التصدي لها

المحمول. حكم عليه بعد اعتقاله بالسجن ثلاث سنوات، واستعادت السلطات كافة المبلغ المسروق باستثناء أربعمائة ألف دولار.

كما شهدت سنة 2000 أول حرب إلكترونية دولية بين العرب المسلمين ضد اليهود وكان نتيجتها اختراق وتعطيل الكثير من المواقع الإسرائيلية، كما شهدت الهند مصيرا مماثلا من قبل الهاكرز الباكستانيين وكذلك الحرب الأميركية الصينية عام 2001 بسبب أزمة طائرة التجسس الأميركية في الصين وراح ضحيتها الكثير من المواقع والشبكات.

ولعل أشهر القراصنة على الإطلاق هو الأمريكي كيفن ميتنيك الذي يعتبر أشهر هاكلر في التاريخ وكذا القرصان الذي لقب بـ the menetor والذي قام بنشر دراسة شهيرة بعد عملية اعتقاله أصبحت تعرف باسم بيان الهاكر وهو بيان رسمي لأهداف ووجهات نظر القرصان، نشرت في المجلة الإلكترونية PHRACK ولا تزال الدراسة تعتبر أشهر ما كتب قرصنة الحاسوب وكثيرا ما تستخدم لتبين طريقة تفكير وعمل القرصان.

ويقسم المهتمون بمتابعة تكنولوجيا المعلومات وأخبارها قرصنة الإنترنت عادة إلى قسمين: القرصنة الأخلاقيين (القبعات البيض)، والقرصنة المجرمين (القبعات السود)، ويضاف إليهما أحيانا قسم ثالث هم أصحاب القبعات الرمادية.

ب- القبعات البيض

هم القرصنة 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 الأميركية في يوم ما "أكثر مجرم حاسوب مطلوب في تاريخ الولايات المتحدة" واعتقل وسجن أكثر من مرة قبل أن يتحول إلى هاكلر أخلاقي ويصبح مستشارا ومتحدثا عاما في أمن الحاسوب ومديرا لشركة "ميتنيك للاستشارات الأمنية"¹².

¹² طوبي ميشال عيسى، التنظيم القانوني لشبكة الانترنت، دارصادر للمنشورات بيروت، ط1 2000، ص383.

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 أخيرا إلى هاكل أخلاقي ويعمل مستشارا 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 في يوليو/تموز 2007.

ومن القراصنة البيض أيضا "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، وجوليان أسانج مؤسس موقع ويكيليكس.

ج- القبعات السود

وهم 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) وتسبب بأضرار لأنظمة الجيش قدرت بسبعمائة ألف دولار، وإلى جانب مكينون، هناك جونثان جيمز (المعروف باسم كومريد) الذي اخترق وهو في الـ 15 عاما من عمره شبكة ناسا ووزارة الدفاع الأميركية. وجورجهوتز الذي يعرف بكونه مخترق منصة ألعاب سوني بلايستيشن 3 عام 2011. 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 911 جديدة من ضمن جوائز أخرى¹³.

¹³ هلال عبد الله، المرجع نفسه، ص 64.

بن شريف أحلام / بوغرارة الصالح: القرصنة الإلكترونية: أنواعها أشكالها وطرق التصدي لها

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 2005 إلى 2007 أكثر من 170 مليوناً من أرقام بطاقات الصراف الآلي وبطاقات الائتمان، والروسي فلاديمير ليفين الذي تمكن عام 1994 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 أربع مائة ألف دولار، وهناك روبرت تابان موريس الذي أطلق في الثاني من نوفمبر/تشرين الثاني 1988 دودة حاسوب (برمجية خبيثة) عطلت نحو عُشر الإنترنت وأكثر من ستة آلاف نظام حاسوب، وقدرت قيمة الخسائر المالية لهذه العملية بنحو 15 مليون دولار.

د- القبعات الرمادية

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

ثانياً: الأسباب التي تدفع إلى ارتكاب جرائم القرصنة المعلوماتية

يختلف مرتكبو جرائم القرصنة المعلوماتية عن مرتكبي الجرائم الاعتيادية من حيث المبدأ وطريقته القيام بالعمل الإجرامي، لكن في النهاية يبقى الطرفان مخالفين للقانون؛ لذا يستحقان العقاب بما اقترفوا من جرائم.

وهناك عدّة أسباب تدفع إلى ارتكاب الجرائم المعلوماتية، يُمكن أن أختصرها بالآتي:

1-حبُّ التعلُّم:

يعتبر حبُّ التعلم والاستطلاع من الأسباب الرئيسة التي تدفع إلى ارتكاب مثل هذه الجرائم؛ لأنَّ المُخترِق يعتقد أنَّ أجهزة الحاسوب والأنظمة هي ملك للجميع، ويجب ألاَّ تبقى المعلومات حكراً على أحد؛ أي: إنَّ للجميع الحقَّ في التعرُّف والاستفادة من هذه المعلومات¹⁴.

2- المنفعة المادية

قد تكون مُحاولات الكسب السريع، وجَنِّي الأرباح الطائلة دون تعب، ولا رأس مال، من الأسباب التي تدفع إلى اختراق أنظمة إلكترونية كالتّي تستخدمها المصارف عن طريق الدُّخول إلى الحسابات المصرفية، والتلاعب فيها، أو الاستخدام غير المشروع لبطاقات الائتمان.

3- التسلية واللهو

عددٌ غير قليل من مُخترقي الأنظمة يتَّخذون من عملهم هذا وسيلة للمرح والتَّسلية، وتقضية أكبر وقت مُمكن في أنظمة وحواسيب الآخرين، ويكون هذا الاختراق غالباً سَلَمياً، ودون أن يَحْدث تأثير يُذكر.

4- الدوافع الشخصية

يعتبر مُحيط الإنسان والبيئة التي يعيش فيها من العوامل المؤثرة في سلوكه وتصرفاته، وغالباً ما تدفع مشاكل العمل إلى رغبةٍ في الانتقام ووجود أنظمة إلكترونية تسهِّل له القيام برغباته، فيَعْبث بِمُحتوياتها إلى درجة التَّخريب، أو يكون الدافع التحدي وإثبات الجدارة أمام الآخرين بِحيث يفتخر هذا الشخص بأنَّ في استطاعته اختراق أيِّ حاسوب أو أيِّ نظام، ولا يستطيع أحدُ الوقوف في وجهه.

2- وسائل الحماية من القرصنة الالكترونية¹⁵:

1. استخدام أحدث برامج الحماية من الهاكرز والفيروسات، وقُم بعمل مسَّح دوريٍّ وشامل على جهازك في أوقات مُتقاربة، خصوصاً إذا كنت ممن يستخدمون الإنترنت بشكل يومي.

¹⁴ جميل عبد الباقي، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة 2001، ص 56.

¹⁵ محمد زكي، المرجع السابق، ص 110.

2. لا تَدْخُل إلى المواقع المشبوهة، مثل: المواقع التي تُعَلِّم التجسُّس، والمواقع التي تُحارب الحكومات، أو المواقع التي تحوي أفلامًا وصُورًا خليعة؛ لأنَّ الهاكرز يستخدمون أمثال هذه المواقع في إدخال ملفات التجسُّس إلى الضحايا؛ حيث يتمُّ تنصيب ملفِّ التجسس (الباتش) تلقائيًا في الجهاز بِمُجرَّد دخول الشخص إلى الموقع!
3. عدم فتح أيِّ رسالة إلكترونية من مصدر مجهول؛ لأنَّ الهاكرز يستخدمون رسائل البريد الإلكتروني لإرسال ملفات التجسُّس إلى الضحايا.
4. عدم استقبال أيَّة ملفات أثناء الشات (من أشخاص غير موثوق بهم، وخاصةً إذا كانت هذه الملفات تحمل امتداد (exe) مثل (love.exe) أو أن تكون ملفات من ذوات الامتدادين، مثل (Ali.pif.jpg):، وتكون أمثال هذه الملفات عبارة عن برامج تزرع ملفات التجسُّس في جهازك، فيستطيع الهاكرز بواسطتها من الدُخول إلى جهازك، والتسبُّب في الأذى والمشاكل لك.
5. عدم الاحتفاظ بأيَّة معلومات شخصية داخل جهازك، كالرسائل الخاصة، أو الصُّور الفوتوغرافية، أو المملَّقات المهمَّة، وغيرها من معلوماتٍ بَنَكِيَّة، مثل أرقام الحسابات، أو البطاقات الائتمانية.
6. قُمْ بوضع أرقام سَرِيَّة على مملَّقاتك المهمَّة؛ حيث لا يستطيع فتحها سوى مَنْ يعرف الرِّقْم السريَّ فقط، وهو أنت.
7. حاول قُدِّر الإمكان أن يكون لك عددٌ معيَّن من الأصدقاء عبر الإنترنت، وتوخَّ فهم الصِّدق والأمانة والأخلاق.
8. حاول دائمًا تَغْيِير كلمة السِّرِّ بصورة دوريَّة، فهي قابلة للاختراق.
9. تأكَّد من رَفْع سلك التوصيل بالإنترنت بعد الانتهاء من استخدام الإنترنت.
10. لا تقم باستلام أيِّ ملف وتَحْمِيله على القرص الصلب في جهازك الشخصي إن لم تكن متأكَّدًا من مصدره.

الختامة

يوماً بعد يوم تزداد مخاطر الجرائم المعلوماتية وتتوسع دائرتها لتشمل كافة مرافق الحياة العامة وبدأت تهدد الاقتصاد العالمي نتيجة الخسائر الكبيرة الناتجة عنها ، واطخر ما في

الأمران اغلب مرتكبي هذه الجرائم يبقون مجهولي الهوية وهذا الأمر يتيح لهم الاستمرار والتفنن بطرق التلاعب بموارد الآخرين عن طريق السيطرة على أنظمتهم الالكترونية.

وما يدعوا للقلق إن الكثير من البلدان ومنها العراق لا يملك لحد الآن تشريعاً صريحاً يجرم ظاهرة القرصنة مع وجود بعض المحاولات لإصدار قانون عربي موحد يخص جرائم المعلوماتية بكافة تفرعاتها وقد يكون سبب تأخير إصدار مثل هكذا تشريع يعود لعدم وجود دعاوى قضائية في محاكم العراق كافة ضد مرتكبي جرائم القرصنة والاختراق ، وهذا لا يعني عدم وجود جرائم معلوماتية بل إن عدداً غير قليل من المواقع الالكترونية العراقية تتعرض للهجوم سنوياً وخصوصاً مواقع وكالات الأنباء والمواقع الحكومية ، وان سبب عدم رفع الدعاوى يعود لصعوبة معرفة الفاعل.

لذا يجب وضع دراسة مستقبلية لما قد يحصل جراء تطور هذه الجرائم خصوصاً في هذه المرحلة التي يقبل فيها العراق على تنفيذ مشروع الحكومة الالكترونية وقد بدأت بالفعل بعض الوزارات بالخطوات الأولى لتنفيذ هذا المشروع الأمر الذي يستدعي الإسراع بإصدار قوانين صارمة تردع أي شخص يحاول العبث بالوثائق الرسمية.

في السنوات الأخيرة انتشرت القرصنة الإلكترونية بصورة كبيرة تنبئ بالخطر بسبب خواصها التي تميزها عن الجريمة التقليدية، ذلك أن ضحاياها يتعرضون لتعطيل وتدمير مخازن المعلومات الخاصة بهم وسرقة أموالهم والتهديد والابتزاز، مما يتسبب للاقتصاد بأضرار كبيرة.

ومع تزايد نسبة الجرائم الإلكترونية وتنوع طرقها فقد أصبحت تلحق خسائر مادية كبيرة وفادحة أكثر مما تسببه الجرائم التقليدية، ليس فقط على مستوى الفرد بل تتعداه إلى مستوى المنظمات والجهات والمؤسسات، فجرائم القرصنة أصبحت تدار إلكترونياً وتوجد على الشبكة الإلكترونية لفتح قنوات تواصل جديدة بهدف استقطاب شريحة أكبر من الناس وزيادة أرباحها.

ورغم أن الجريمة الإلكترونية تتم عبر استخدام أدوات مثل الحاسوب أو الإنترنت فإنها لا تختلف في طبيعتها عن الجرائم التقليدية.

بن شريف أحلام / بوغرارة الصالح: القرصنة الإلكترونية: أنواعها أشكالها وطرق التصدي لها

ومحاربة الجريمة الإلكترونية تحتاج إلى وقفة طويلة وقوية من قبل الدول والأفراد، بهدف تأمين استخدام أجهزة الحاسوب وشبكة الإنترنت.

قائمة المراجع

1. علي السيد الباز ،الحكومة الالكترونية والادارة المحلية.الادارة المحلية الالكترونية العربية : متاح عبر: www.arabia/law/info.com
2. الموقع الالكتروني: <http://etudiantdz/cybernetatach.com/vb/html>
3. أمل المرشدي ، بحث قانوني حول جريمة القرصنة الالكترونية <http://www.mohamat.net/law/dl.52.com>
4. جميل عبد الباقي ،الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية ،القاهرة2001،ص56.
5. أحمد شربتجي ،د. وقائي بغدادي، الحماية وتأمين الأنترنت التحدي القادم وأساليب المواجهة ،سلسلة العلوم والتكنولوجيا ،الهيئة المصرية العامة للكتاب القاهرة ،سنة2010 ، ص51.
6. ريموتر"السعودي "ريموتر" لديه "هاشتاغ- وسم- وصفحة وتويتر، ويمكنك التعرف عليهم من أعماله ونصوصه".
7. طوبي ميشال عيسى، التنظيم القانوني لشبكة الأنترنت، دار صادر للمنشورات بيروت، ط1 2000،
8. محمد سامي الشوام، ثورة المعلومات وانعكاساتها على قانون العقوبات ،مطابع الهيئة للكتاب ،مصر2008.
9. معتوق عبد اللطيف ،الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن مذكرة لنيل شهادة الماجستير في العلوم الجنائية سنة2011 ،منشورة
10. الموقع الخاص بالأكاديمية العربية البريطانية للتعليم العالي.