وزارة التعليم العالـــــــي والبحث العلمـــــــي

جامعة عبد الحميد ابن باديس-مستغانم-

كلية العلوم الاجتماعية

قسم علوم الإنسانية

شعبة علوم الإعلام والاتصال

تخصص وسائل الإعلام والمجتمع

رسالة مكملة لنيل شهادة الماستر في علوم الاعلام والاتصال الموسومة ب:

واقع القرصنة الالكترونية في الجزائر

دراسة ميدانية على عينة من ضحايا القرصنة الالكترونية بلدية عمي موسى ولاية غليزان

-من إعداد الطالبين :

* مكي يوسف

* دوار محمد

-تحت إشراف الأستاذة والدكتورة:

*صفاح أمـــــال

لجنة المناقشة:

د- صفاح أمال	أستاذة محاضر -جامعة مستغانم-	مقرراً
د- العربي بوعمامة	أستاذ محاضر -جامعة مستغانم-	رئيساً
د- عبو نريمان	أستاذة محاضر -جامعة مستغانم-	مناقشاً

السنة الجامعية: 2017-2018.

اهداء

إلى من تكبد عناء دراستي وسهر على توفير كل ما أوتي في سبيل رؤية ثمرة جهده....إلى من علمني العطاء دون انتظار والدي

إلى من كان دعاؤها سر نجاحي

والدتي

إلى الذين تفهموا انشغالي في البحث

إخوتي

إلى كل زملاء دفعة الماستر 2018م

أهدي هذا العمل.

مـكـي يــوسف

مقدمة:

لا شك أن الجرائم المعلوماتية جرائم ولدت نتيجة لإساءة استخدام شبكة الانترنت، التي ظهرت أخيرا على الساحة الدولية حيث لم يكن لها وجود قبل ذلك ونتيجة لظهور تلك الشبكة فقد ظهرت معها جرائم المعلوماتية التي تمثلت في جرائم الاعتداء على ذات جهاز الكمبيوتر أو على البيانات المعلوماتية التي توجد على هذا الجهاز أو على الشبكة ذاتها.

والملاحظ أن هذه الجرائم الالكترونية ما كانت أجدا في الحسبان إذ أن التاريخ البشري لم يمر قط قبل ذلك بمثل تلك التجارب، ومع اختراع الحاسوب تحول العمل اليدوي إلى الحاسوب الذي يرتبط عادة بحواسيب أخرى عبر شبكات صغيرة أو كبيرة.

وبالتالي أصبحت المعلومات في خطر دائم لأن اختراق أي جهاز يعني إمكانية الدخول إلى الأجهزة الأخرى التي ترتبط عبر شبكة واحدة، هذا المر جعل العالم ينفتح على نوع جديد ممن الجرائم والتي تعرف بسرقة المعلومات أو كما يصطلح عليها القرصنة الالكترونية والتي أصبحت تشكل جناية لا تقل خطورة وتأثيرا عن باقي أنواع الجرائم الأخرى خاصة في البلدان العربية وفي الجزائر على وجه الخصوص. ولهذا تطرقنا في دراستنا حول "**واقع القرصنة الإلكترونية في الجزائر دراسة ميدانية ببلدية عين موسى**" ، وحتى نتمكن من معالجة إشكالية السابقة الذكر قمنا برسم خطة تضمنت الإطار المنهجي بتحديد الإشكالية والتساؤلات وحصر الأسباب الذاتية والموضوعية التي كانت وراء تسليط الضوء على زاوية ضحايا القرصنة الإلكترونية، بالإضافة إلى منهج الدراسة ومجتمع البحث والعينة، ثم تحديد أداة المقابلة ولضبط الدراسة ومتغيراتها حددّت المفاهيم والوقوف على الدراسات السابقة التي تتشارك في طرحنا للموضوع وأخيراً تعليق عليها ، أمّا الإطار النظري فقد تضمن فصلين، خصصنا الفصل الأول القرصنة الإلكترونية من خلال تعريفها وذكر نشأتها، ومظاهرها، وخصائصها، ولنتطرق في الفصل الثاني إلى القرصنة الإلكترونية في الجزائر. ويشكل الإطار التطبيقي المنعطف الرئيسي للدراسة بإجراء دراسة ميدانية على ضحايا القرصنة الإلكترونية عن طريق المقابلة، وتحليل نتائجها، وفي الأخير وضع خاتمة للدراسة.

الاطار المنهجي

1- الدراسة الاستطلاعية

تعرف الدراسة الاستطلاعية على أنها تلك الأبحاث الأولية التي يلجأ إليها الباحث، عادة لتدليل صعوبات التي يواجهها على مستوى استكشاف الظواهر محل الدراسة أو التعرف عليها بصورة جيدة بعد اكتشافها [1].وعلى هذا الأساس فإن الدراسة الاستطلاعية لموضوع دراستنا كانت بداية بالقراءة الأولية من خلال استعراض مختلف الأدبيات السابقة سواء كانت ذات صلة مباشرة أو غير مباشرة لموضوع الدراسة، ولتحقق من جوانب المراد معرفتها وكشفها على مستوى موضوعنا ،قمنا بدراسة استطلاعية على عينة مماثلة لعينة البحث الحالي في الخصائص، حيث خصصنا مجال الاستكشاف على المبحوثين الذين تعرضون للقرصنة الإلكترونية، إذ تمت الدراسة الاستطلاعية بتاريخ 2017/12/07 حيث تم اجراء مقابلة مع عينة من المبحوثين قوامها 5 مفردة مشتملة على كلاّ الجنسين ذكور وإناث على مختلف المستويات. وقد توصلنا إلى أهم النتائج على النحو التالي :

- ✓ إن مختلف المبحوثين تعرضن للقرصنة بطريقة غير مباشرة.
- ✓ إن مختلف المبحوثين الذين تعرضن للقرصنة هم فئة الشباب.

[1]-أحمد بن مرسلي، **مناهج البحث في علوم الإعلام و الاتصال**، ط(3)، ديوان المطبوعات الجامعية، الجزائر،2007، ص ص48-49.

اشكالية الدراسة :

إن التطور الحاصل في تكنولوجيا الإعلام والاتصال، وظهور الشبكة العالمية الأنترنت بكل ما حملته من تقدم وخدمات، لم يمر على العالم بسلام، لأنه بقدر ما أحدث آثار ايجابية وغير نمط حياة المجتمعات وساهم في التطور والرقيب قدر ما كان له أثر سلبي على حياة الناس ومصالح الدول بأسرها، كل هذا تجلى في تطويع الأنترنت والوسائل الالكترونية لتكون عالمنا من عوالم الجريمة والقرصنة والكثير من السلبيات لهذه الأخيرة، إذ ظهرت إلى الوجود. وعلى هذا الفضاء السيبرني بما يسمي القرصنة الالكترونية ،التي تعد الابن الغير الشرع الذي جاء نتيجة للتزاوج بين ثورة تكنولوجيا المعلومات....مع العولمة.

أو المارد الذي خرج من القمقم. ولا تستطيع العولمة أن تصرفه بعد أن أحضرته الممارسة السيئة لثورة تكنولوجيات المعلومات، فإن تمكن سهولة الانتاج المعلومات الرقمية لها قد خلقت سوقا للنسخ الغير قانوني، ويستاثر هذا النسخ تغيرات كثيرة من ملايين الدولارات الامريكية كخسائر يدخلها ناشرو البرمجيات والموسيقي وأفلام الفيديو وقد لوحظ أيضا وجود زيادة كبيرة في عدد الأعمال العلمية و الأكاديمية التي تلجأ إلى سرقة الأفكار فقط بمجرد نسخ وثائق موجودة من الويب هناك عدد كبير من مخالفات الفكرية المحتملة ،و كتزييف أعمال مؤلف ما بما في ذلك البرمجيات و التصميم و النموذج والعلامة التجارية الجزائر كغيرها من الدول الأخرى عرفت حضور متميز لهذه التكنولوجيات و استخدامها في جل المجالات هذه الاخيرة مؤخرا و استخدام قوي من طرف شبابها إذ تعيش نوعا من هذه الآفة خاصة في هذه الآونة الأخيرة: وفي ضوء هذا السياق نطرح الإشكال التالي: **كيف تتجلى أثار القرصنة الإلكترونية على ضحاياها ؟**

ومن خلال هذا نتوصل إلى عدّة أسئلة فرعية تتمحور فيما يلي :

1. ماهي أشكال القرصنة الإلكترونية التي تعرض لها أفراد العينة؟.
2. ماهي أثرها ونتائجها؟
3. ماهي السبل المستخدمة لمواجهتها؟
4. ما هي أفضل سبل الحماية من القرصنة الالكترونية؟

أسباب اختيار الموضوع:

ان الانطلاق الاولية لكل دراسة تسترعي الوقوف على الاسباب الذاتية و الموضوعية.

1.الأسباب الموضوعية:

- كون الظاهرة المعالجة متفشية بكثرة في الجزائر إلى درجة أنها أصبحت أمر عادي.

- المراتب التي تحتلها الجزائر في هذا المجال حيث تصنف على رأس الدول العربية في القرصنة الالكترونية.

- تزويد المكتبة الجامعية بمذكرة تعالج الظاهرة محل الدراسة.

- محاولة منا بتحسيس الرأي الجزائري بمدى خطورتها على المدى البعيد والقريب.

- التعرف على مساعي الدولة في الحد من هذه الظاهرة.

2.الأسباب الذاتية:

- فضولنا للكشف عن جوانب الظاهرة عن قرب.

- التعرف أكثر على فئة القراصنة في الجزائر والتعرف على وجهة نظرهم.

– إيمانا منا بأن شباب اليوم هم دعائم المستقبل ويمكنهم توجيه إمكانياتهم ومجهودهم الفكري من عمل سلبي إلى عمل ايجابي تستفيد منه الجزائر في المستقبل القريب والبعيد.

أهمية الدراسة:

إن دراستنا لموضوع القرصنة الإلكترونية تعزز أهمية علمية وأكاديمية تمثل فيما يلي:

1/ تشكل المواضيع الدراسات الإعلامية المرتبطة بالمجتمع موضوعاً حيوياً مؤسسياً، ومن هنا تكمن أهمية الدراسة في تسليط الضوء على القرصنة الالكترونية، بإعتبار هذا الأخير ذو دور فعال ورئيسي في تحقيق العملية للمقرصنين .

2/المستجدات الاتصالية التي وفرتها البيئة التكنولوجية الحديثة في ظل الميديا الجديدة.

3/تحديد المتغيرات التي ستحدثها القرصنة الالكترونية، من خلال التحديات التي تفرضها على ضحايا والمؤسسات.

4/اعتبار دراستنا هي امتداد لدراسة الباحثين سابقين من خلال إسقاطها على الزاوية معينة من الضحايا مما قد تعطي نتائج جديدة في ظل الوسائط الحديثة.

أهداف الدراسة:

أي دراسة تجرى في البحث العلمي فأنها تتطلب البلوغ أهداف يسيطرها الباحث وفق طبيعة الدراسة ومن الاهداف التي نرمي الوصول اليها في دراستنا هي:

1- التعرف على ظاهرة القرصنة في المجتمعات الجزائرية .

2- الكشف عن سلبياتها وما تخلفه من خسائر مادية ومعنوية على ضحاياها سواء كانوا مؤسسات أو أفراد.

3- محاولة توعية الشباب وخاصة مستعملي الانترنت بخطورة الوضع على مستقبلهم وعلى بلدهم.

4- الرغبة في الكشف عن تأثيرات القرصنة.

حدود الدراسة:

- ✓ **الحدود الموضوعية:** تقتصر الدراسة على القرصنة الإلكترونية في الجزائر.
- ✓ **الحدود البشرية:** الفئة الذين تعرضن للقرصنة.
- ✓ **الحدود المكانية:** ولاية غليزان "بلدية عمي موسى".
- ✓ **الحدود الزمنية:** امتدت الدراسة من بداية أكتوبر 2017إلى غاية أفريل 2018.

تحديد المفاهيم والمصطلحات:

القرصنة الإلكترونية:

إجرائياً: هي عبارة عن استخدام غير معترف به يكون بقصد إحداث خلل للملفات أو صور أو معلومات شخصية سواء تعلقت بأشخاص أو مؤسسات يكون صاحبها غير معروف ويتم استعمال هذه الملفات المقرصنة لخدمة أغراض ذاتية .

الفيروسات:

هي عبارة عن برنامج يقوم بالإحداث أضرار لجهز الحاسوب ماإن دخل إليه.ويتم الوقايةمنه بلإستخدام عدة طرق وذللك بتفعيل الجدار الناري كمثال.

تعريفها:

هي عبارة عن مجموعة من التعليمات التي تتكاثر بمعدل سريع جدا وتصيب النظام المعلوماتي بالشكل.

ويعرفه **الدكتور محمد سامي الشوا:** "الفيروس هو عبارة عن خلية مغناطيسية نائمة ومبرمجة تنشأ في وقت محدد لتخريب البرنامج الأصلي ومنتشرة في الأجهزة الأخرى التي تضمنتها الشبكة بحيث تفسر ما تحتويه من معلومات".

كما عرفه بعض المختصين في المجال المعلوماتي بأنه: برنامج يصممه بعض المختصين بهدف تخريب مع إعطائه القدرة على ربط نفسه ببرامج أخرى ثم تتكاثر وتنشر داخل النظام حتى يتسبب في تدميره تماما"[2].

ويعرفه آخرون بأنه: "مرض يصيب الحاسب الآلي، فهو ليس فيروسا بالمعنى البيولوجي المعروف، ولكنه برنامج معين يتم تسجيله أو زرعه على الأقراص أو الأسطوانات الخاصة بالحاسب ويظل هذا الفيروس لفترة محددة ثم ينشط فجأة في توقيت معين ليدمر البرامج والبيانات المسجلة والمخزنة في داخل الحاسب ويشمل أثره التخريبي لإتلاف والحذف والتعديل"[3]

إجرائياً: هي عبارة عن برنامج يقوم بالإحداث أضرار لجهاز الحاسوب ما إن دخل إليه. ويتم الوقاية منه بالإستخدام عدّة طرق وذلك بتفعيل الجدار الناري كمثال.

2.مفهوم الانترنت:

للوقوف على حقيقة الانترنت يجب معرفة خلفية وأبعاد المفهوم في حد ذاته حيث أن مفهوم الانترنت ونظرا لبعض الغموض الذي يكتنفه ارتأينا دراسة من زاويتين لغة واصطلاحا.

– التعريف اللغوي:

انترنت Internet هي كلمة منحوتة من كلمتين Inter / Net فكلمة Interconnoction أخذ الجزء الأول منها وهو Inter وتعني الشبكة وكلمة Net هي ترجمة حرفية لكلمة Net work وهي تعني ربط أكثر من شيء ببعضه البعض.

وهناك أنواع من الشبكات تشكل جزء من الانترنت هي:

---

[1]–محمد العريان، **الجرائم المعلوماتية**، كلية الحقوق، جامعة الاسكندرية، 2004، ص56.

[3] – عبد الفتاح بيومي حجازي، **التجارة الإلكترونية وحمايتها القانونية**، دار الفكر الجامعي، الاسكندرية،2006،ص79.

الشبكة الداخلية "الانترنت":

وهي شبكة تعمل داخل المؤسسة لكنها تستخدم معايير الانترنت وبالتالي الانترنت هي انترنت صغيرة ولكن للاستعمالات الداخلية للمؤسسة.

الشبكة الخارجية "الاكسرانت":

هي شبكة داخلية تسمح لبعض الشركات الخارجية بالدخول لها لأسباب استراتيجية وعادة ما يكون الوصول للمعلومات فيها جزئيا.

التعريف الاصطلاحي:

هي عبارة عن حاسب آلي يتحدث إلى حاسب آلي آخر يربط بينهما بواسطة سلك هاتف العادي أو أي نوع آخر من الكوابل، إذ كانت الحواسيب موجودة في أماكن بعيدة ومنفردة فيمكن استخدام الأقمار الصناعية الربط بينهما ليتحقق بذلك الاتصال الدولي عبر الانترنت وحتى داخل البلد الواحد فهي تحتاج إلى الوصلات الوسطية.

وبالتالي يمكن تعريف الانترنت على أنها:

شبكة عالمية من الحاسبات الآلية تعرف بشبكة الاتصال العالمية ووسيلة تتواصل عبرها الكمبيوترات، ليس لأنها ترتبط بها مجموعة اختيارية من الحواسيب التي تغطي العالم أجمع، فحسب أيمن سيد درويش، فإن الانترنت اسم لنظام ضخم منتشر في جميع أنحاء العالم تألف من أناس، معلومات، حواسيب ضخمة ومعقدة إلى درجة يصعب على الإنسان العادي فهمها".[4]

1- أيمن سيد درويش، **المرجع الكامل لخدمات الأنترنت**، سوريا، شعاع النشر والعلوم، ط1، 1998.ص 10.

ويقول الأستاذ "**أرتود ديفور**" الانترنت ظاهرة تعددت العبارات في وصفها منها: الشبكات، الفضاء الالكتروني.

أما الباحثان "**بون نورتن وكاتن سميث**" يقولان أن الانترنت ليست حاسوبا ضخما يجلب كل الأشياء إلى مكان واحد مركزي، بل هي شبكة عالمية على نطاق عالمي في الشبكات العالمية الحاسوبية المختلفة والمتمثلة ببعضها البعض بواسطة وصلات الاتصال هذه الشبكة مكونة من منظمات ومؤسسات متفرقة تشمل الدوائر الحكومية والجامعات والشركات التجارية.[5]

3. تعريف المعلومات:

نبين في هذا المطلب تعريفا للمعلومات وما قيل في شأنها، وتعريفا للبيانات باعتبارها عنصر مكمل للمعلومات.

والمعلومة Information كلمة شاع استعمالها منذ خمسينات القرن الماضي في مجالات مختلفة وسياقات شتى مما جعل لها في الاستعمال الدارج مفاهيم متنوعة.[6]

لغويا: مشتقة من كلمة علم ودلالتها فيها، وتدور بوجه عام حول المعرفة التي يمكن نقلها واكتسابها.[7]

المعلومة اصطلاحا:

هناك مئات من التعريفات التي أدلى بها باحثون من تخصصات وثقافات مختلفة لفهم وإدراك المعنى المراد بمصطلح المعلومات.

2_ يون نورتن وكاتن سميث، **التجارة على الأنترنت**،(ترجمة مركز التعريب و البرمجة)، بيروت، الدار العربية للعلوم، ط1، 1997، ص10.

[6] - محمد سامي شوا، **ثورة المعلومات وانعكاساتها على قانون العقوبات**، دار النهضة العربية،1994، ص73.

[7] - **المعجم الوسيط**، ج1، ط2، مجمع اللغة العربية، 1985، ص647.

ويعرف الأستاذ "catala" بأنها: "رسالة ما معبر عنها في مشكل يجعلها قابلة للنقل أو الإبلاغ للغير، ويعرفها البعض الآخر بأنها" رمز أو مجموعة رموز تنطوي على إمكانية الإفضاء إلى معنى[8]

شركة ما والاحتفاظ بسريته أو بالنظر إلى الأمرين معا كما هو الحال بالنسبة للرقم السري للبطاقة الائتمانية ويقلل الطابع السري في هذه الحالات المختلفة من استخدام المعلومات ويقهرها فقط على دائرة المؤتمنين عليها والذين يجدون أنفسهم هكذا منقعين بحق الاستئثار عليها.

– الاستئثار أمر ضروري لأنه في جميع الجرائم التي تنطوي على اعتداء قانوني على القيم، يستأثر الفاعل بسلطة تخص الغير وعلى نحو مطلق والاستئثار في مجال المعلومات يمكن أن يرد على الولوج في المعلومة والمخصص لمجموعة محددة من الأشخاص، لذا فإن الاستئثار ينظر إلى المعلومة بوصفها من قبيل الأسرار ويمكن أن يرد الاستئثار أيضا بالنسبة لشخص بمفرده باعتباره صاحب سلطة التصرف في المعلومة، وعندئذ يكون لمؤلف المعلومة أو صاحبها.[9]

تعريف البيانات

لغة: مصدرها الفعل بين أي أظهر واتضح وأفصح عن وعبر عنها القرآن الكريم في سورة الرحمن وقال تعالى: "الرحمان 1.2.3.4.

وقوله "عَلَمَه' البَيَانَ" تعني حقائق أو أشياء معروفة يقينا ويمكن منها الوصول إلى نتيجة معينة.

---

[9] محمد سعيد خشبة، **مقدمة في التجهيز الإلكتروني**، القاهرة، جامعة الأزهر، ص78.

اصطلاحا: للبيانات تعريفات عدة يستخلص منها أنها عبارة عن كلمات وأرقام ورموز وحقائق وإحصاءات خام لا يوجد أي صلات بينهما وهي صالحة لتكوين فكرة أو معرفة بواسطة الإنسان أو الأدوات والأجهزة التي يسخرها لذلك وهي ما تسمى بالمعالجة الآلية، وكثيرا ما تستخدم البيانات كمرادف للمعلومات رغم الاختلاف في المعنى والمفهوم والدلالة.

البعض يقول أن البيانات هي المعطيات المتصلة بجهة معينة، والمعلومة هي المعنى المستخلص منها بعد معالجاتها، فالبيانات هي المداخلات للنظام المعلوماتي ومن قبيل ذلك تعرف البيانات بأنها: "مجموعة من الحقائق تعبر عن مواقف وأفعال معينة حدثت في الماضي أو الحاضر أو ستحدث في المستقبل سواء أكان التعبير بالكلمات أو الأرقام أو الأشكال أو الرموز، وتعريف المعلومات بأنها: "بيانات خضعت للتشغيل والتحليل والتفسير لتحقيق زيادة المعرفة لمتخذي القرارات ومساعدتهم لتحقيق أغراض معينة وتمكينهم من الحكم السديد على الظواهر والمشاهدات.

ويطلق البعض كلمة البيانات على "مجموعة الحقائق أو المشاهدات أو القياسات التي تكون عادة على هيئة حروف أو أرقام أو أشكال خاصة تصف أو تمثل فكرة أو موضوع أو هدف أو شرط أو أية عوامل أخرى.

وهي بهذا المعنى تشكل المادة الخام التي يتم تشغيلها للحصول على شكل أكثر فائدة واستخداما، وهو المعلومات أي أن البيانات هي المادة الخام التي تشتق منها المعلومات.[10]

البريد الالكتروني:

يعد البريد الالكتروني من الوسائل التكنولوجية الحديثة التي تستهدف تسهيل تبادر المعلومات على الفور، ويمكن أن تكون هذه البيانات في شكل نصوص، أو أصوات أو رسوم، يتم ذلك باستخدام نظم البريد التي تعتمد على الحاسب الالكتروني في استقبال الرسائل وتخزينها ونقلها إلى أماكن بعيدة، ويوجد نظامان أساسيان للبريد

[10] - محمد سعيد خشبة، **مقدمة في التجهيز الإلكتروني**، المرجع السابق، ص79.

الالكتروني يسمى الأول: Store – and –foruard ويتعامل مع الصوت والنصوص المطبوعة، ويسمى النظام الثاني: Facsimile ويتعامل مع الرسوم فقط.

أمن المعلومات:

اصطلاحاً:

إجرائياً: هي مخطط تقوم به الدولة لحماية المعلومات من القرصنة على مستوى الداخلي أو الخارجي من خلال الوضع استراتجيات متعددة ومرقبة تامة على مستو مستخدمي الأنترنت.

منهج الدراسة :

يقصد بالمنهج في العلوم الإنسانية طريقة تصور وتنظيم البحث، فالمنهج يتدخل بطريقة أكثر أو أقل إلحاحاً بأكثر أو أقل دقة في كل مراحل البحث [11] .وتختلف تقسيمات المناهج من الباحث إلى أخر، إلاّ أنّ المنهج المعتمد في دراستنا هو **المنهج الوصفي المسحي** وهو الذي يحاول أن يصور أو يوثق الظروف أو الاتجاهات الحالية. وهذا يعني أنه يفسر ما هو موجود في هذه اللحظة. ويعني الباحثون في هذا النمط من المسوح الوصفية باكتشاف الوضع الحالي في المجال قيد الدراسة [12].في حين يعرفه **موريس أنجرس** بأنه مجموعة منظمة من العمليات تسعى لبلوغ الهدف[13].ويسعى الباحث إلى إتباعها في إطار الإلتزام بتطبيق قواعد معينة [14].وعلى هذا الأساس فقد اعتمدنا على **المنهج المسحي وصفي** وذلك أنه الأنسب للمناهج العلمية الملائمة للدراسات الوصفية بصفة عامة، ولمستخدمي القرصنة الإلكترونية بصفة خاصة لأن المنهج يستهدف تسجيل وتحليل وتفسير الظاهرة في وضعها الراهن

---

[11] -أحمد عظيمي، **منهجية كتابة المذكرات والأطروحات الدكتورة في علوم الإعلام والاتصال**، ديوان المطبوعات الجامعية، الجزائر، 2009، ص52.

[12] -روجرز ويمر وجوزيف دومينيك، ترجمة: صالح أبو إصبع، فاروق منصور، **مدخل إلى مناهج البحث الإعلامي**، ط(1)، مركز الدراسات الوحدة العربية، بيروت، 2013، ص325.

[13] -موريس أنجرس، ترجمة: بوزيد صحراوي وأخرون، **منهجية البحث العلمي في العلوم الإنسانية "تدريبات علمية "**، دار القصبة ، الجزائر، 2004، ص98.

[14] -مصطفى عمر السيد أحمد، **البحث العلمي وإجراءاته ومناهجه**، د.ط، مكتبة الفلاح، القاهرة، 2002، ص166.

بعد جمع البيانات الكافية واللازمة عنها وعن عناصرها من خلال مجموعة من الإجراءات المنظمة التي تحدد نوع البيانات ومصدرها وظروف الحصول عليها [15]. ولتدقيق أكثر اخترنا **المسح بالعينة** وذلك نظراً لحجم الجمهور الكبير الذي يستلزم الدراسة الجزئية من خلال وصف **مجتمع البحث "وهم القرصنة** " والمتمثلة أساساً في **"ضحايا القرصنة الإلكترونية"** على مستوى ولاية مستغانم وذلك بربط كل المتغيرات المذكورة في موضوعنا السابق ذكره.

أداة الدراسة:

لقد أملت علينا طبيعة الدراسة والمنهج المستخدم أن نجمع البيانات الميدانية من خلال **المقابلة** التي تدخل ضمن أدوات البحث العلمي حيث يستخدمها الباحث في جمع المعلومات من الأشخاص الذين يملكونها وبيانات أخرى غير موثقة .

المقابلة لغة: مشتقة من الفعل قابل وهي بذلك المواجهة من حيث قياسها على مواجهة الشخص أي مقابلته وجها لوجه.[16]

وتعرف المقابلة على أنها تبادل لفظي بين شخصين يهدف للحصول على أنواع من المعلومات لاستخدامها في بحث علمي أو للاستعانة بها في عمليات التوجيه والتشخيص وتكون في ثلاث صيغ وهي المقابلة المقننة والمقابلة شبه المقننة والمقابلة غير ،والعلاج المقننة.[17]

- **مجتمع البحث والعينة:**

يعرف **مجتمع البحث** على أنه المجتمع الذي يشمل جميع العناصر والمفردات المشكلة أو الظاهرة قيد الدراسة[18].ومن ثم فإن مجتمع الأصلي المعني للدراسة هم ضحايا القرصنة الإلكترونية ب: بلدية عمي موسى، إذ

---

[15]–محمد منير حجاب ،**الموسوعة الإعلامية**، مجلد1، دار الفجر للنشر والتوزيع، مصر، 2003، ص544.

[16]- أحمد بن مرسلي، **مناهج البحث في علوم الإعلام و الاتصال**، المرجع السابق، ص213.

[17] - بلقاسم سلاطنية الجيلالي حسان، **أسس البحث العلمي**، الكتاب الأول، ديوان المطبوعات الجامعية، الجزائر، 2007، ص107.

[18]–ربحي مصطفى عليان، عثمان غنيم، **مناهج وأساليب البحث العلمي النظرية والتطبيق**، دار الصفاء للنشر والتوزيع، عمان، 2009، ص39.

مكننا هذا الأخير من **تحديد العينة** والتي يقصد بها الجزء الذي يتم اختياره من الكلّ، وانطلاقاً من هذا فإن عينة الدراسة تتمحور في ضحايا القرصنة الإلكترونية، وهي العينة غير الإحتمالية أي عينة **قصدية** التي يتعمد الباحث أن تتكون من وحدات معينة[19].وعلى هذا الأساس فقد اخترنا عينة التي تمثلت في 7 ضحايا للقرصنة الإلكترونية ومتخصص في محاربة الجريمة المعلوماتية، وكذا خبير في تكنولوجيا الإعلام والاتصال.

دراسات سابقة :

الدراسة الأولى :

- دراسة نوال بنت علي محمد قيسي تحت عنوان الجرائم الالكترونية وهي مذكرة مكملة لنيل شهادة ماجستر في العلوم الاجتماعية جامعة الامام محمد بن سعود المملكة العربية السعودية

تتمحور اشكالية الدراسة حول أشكال القرصنة وتحديد أهم الجرائم المعلوماتية شيوعا خاصة جرائم القرصنة

في هذا المقال اختارت الباحثة الانطلاق من التساؤلات الفرعية على النحو الأتي :

[19]-إسماعيل محمود حسن، **مناهج البحث الإعلامي** ، ط(1)، دار الفكر العربي، القاهرة، 2011، ص ص139-153.

1- ماهي أشكال القرصنة الالكترونية ؟

2- ماهي السبل المستخدمة لمواجهتها ؟

3- ما سبل الحماية منها ؟

تهدف هذه الدراسة الى الكشف عن أثار القرصنة من خلال اختيار عينة تتكون من 15 ضحية للقرصنة الالكترونية بالاعتماد على أداء المقابلة واستعانت الباحثة بالمنهج المسح الوصفي .[20]

الدراسة الثانية :

- دراسة صغير يوسف تحت عنوان الجريمة المرتكبة عبر الانترنت وهي مذكرة مكملة لنيل شهادة ماجيستر في علوم الاعلام والاتصال تخصص اعلام وتكنولوجيا الاتصال الحديثة جامعة مولود معمر تيزي وزو 2013 تمحورت اشكالية الدراسة حول اثار الجريمة الالكترونية وكيفية مواجهتها وفي هذا المقام اختار الباحث الانطلاق من التساؤلات الفرعية على النحو التالي

1- ما مفهوم الجريمة الالكترونية ؟

2- ماهي الاثار الناتجة عنها ؟

3- ماهي الاحتياطات الواجب اتخاذها للحماية منها ؟

تهدف هذه الدراسة للكشف عن أثار القرصنة الالكترونية وأهم السبل للحماية من خلال اختيار عينة تتكون من 35 مفردة من ضحايا القرصنة ، باعتماد على أداة المقابلة وقد استعان الباحث بالمنهج المسح الوصفي ليتوصل بذلك الى النتائج أهمها :

1- القرصنة الالكترونية نشاط اجرامي يتمثل في استلاء على ملك الغير عن طريق اللهو أو السرقة دون اللجوء الى العنف أو الترهيب .

[20] نوال بنت علي محمد القيسي ، الجرائم الالكترونية دراسة عينة من ضحايا القرصنة مذكرة ماجيستر في العلوم الاجتماعية جامعة الامام محمد بن سعود الاسلامية ، السعودية 2011/2010

2- القرصنة الالكترونية تلحق أذي مادي ومعنوي سواء بالأفراد أو المؤسسات فهي ايذاء لسمعة ضحية ومساس به من خلال سرقة ملفاته الشخصية وقد تكون محاولات الكسب السريع وجني أرباح الطائلة دون تعب سبب في اخراق أنظمة المؤسسات والمساس بها ماديا

3- تحميل برامج الحماية على الجهاز وتجنب المواقع المشبوهة وعدم فتح الرسائل المجهولة احتياطات وجب اتخاذها للحماية من الهاكرز [21]

[21] يوسف صغير الجريمة المرتكبة عبر الانترنت ، دراسة عينة من ضحايا القرصنة مذكرة ماجيستر في علوم الاعلام والاتصال ، تخصص الاعلام وتكنولوجيا الاتصال الحديثة ، جامعة مولود معمري ، تيزي وزو 2012/2011

الاطار النظري

المبحث الأول: مفهوم القرصنة :

كثر الحديث في عصرنا الحاضر عن القرصنة الالكترونية، فأصبح من الطبيعي سماع هذا المصطلح أو قرصنة البرامج أو القرصنة المعلوماتية، وغيرها من المصطلحات المرادفة لهذه التسميات والقرصنة، والقرصنة بمعناها الدقيق هي: "كل عمل عنف غير مرخص به يرتكب بقصد النهب من قبل سفينة خاصة ضد سفينة أخرى في أعالي البحار".

إلا أن لفظ القرصنة في وقتنا الحاضر أصبح وصفا يطلق على نهب المصنفات المنشورة للغير من خلال الحصول على نسخة منها دون الحصول على موافقة مالكها.[22]

وقد عرفت قرصنة برامج الحاسوب بأنها الاستيلاء على ملك الغير عن طريق النهب أو السرقة، دون اللجوء إلى العنف أو الترهيب أو التهويل أو القتل، وهي مخالفة للقرصنة التي كان يمارسها الأقدمون عن طريق البر والبحر، كونها تمارس بهدوء نظرا للتطور التكنولوجي لوسائل التبليغ والبث وتعد مداخيلها مهمة جدا.

ولا يدخل في نطاق القرصنة الالكترونية استيلاء الفاعل على المكونات المادية المستخدمة في الحاسب والتي قد تحتوي تلك البرامج والبيانات كاستيلائه على الأقراص المدمجة مثلا أو الأشرطة أو الأقراص اللينة فلا يكاد ذلك يخرج عن اعتباره غصبا في مجال الفعل الضار والعادي الذي يقع على الأشياء المادية.

ولعل أهم ما تتميز به القرصنة الالكترونية أن الفاعل رغم حصوله على البرامج والبيانات الالكترونية المملوكة للغير إلا أنه لا يخرجها في الوقت ذاته من حيازة ذلك الغير ولا يحول بالتالي بينه وبين الانتفاع بها.

ويكون الفاعل في قرصنة البرامج والبيانات الالكترونية إما إعادة إنتاجها أو نسخها للاستفادة منها أو لبيعها والحصول على منفعة مادية منها.[23]

---

[22]- سامي علي حامد عياد، **الجريمة المعلوماتية وإجرام الانترنيت**، دار الفكر الجامعي، الإسكندرية، 2007، ص78

ومنه يمكن تعريف القرصنة الالكترونية على أنها: "عملية اختراق لأجهزة الحاسوب تتم عبر شبكة الانترنت غالبا لأن أغلب حواسيب العالم مرتبطة عبر هذه الشبكة أو حتى عبر شبكات داخلية يرتبط عنها أكثر من جهاز حاسب ويقوم بهذه العملية شخص أو عدة أشخاص متمكنين في برامج الحاسوب وطرق إدارتها أي أنهم مبرمجون ذو مستوى عال يستطيعون بواسطة برامج مساعدة اختراق حاسوب معين للتعرف على محتوياته ومن خلالها يتم اختراق باقي الأجهزة المرتبطة معها في نفس الشبكة.[24]

---

[23] - عايد رجا الخلايلة، **المسؤولة التقصيرية الالكترونية**، المسؤولة الناشئة من إساءة استخدام الفرد الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، ط1، الإصدار الأول، 2005، ص100.101

[24] - سامي علي حامد عياد، **الجريمة المعلوماتية وإجرام الانترنيت**، المرجع السابق، ص79.

المبحث الثاني: نشأة القرصنة الالكترونية:

بدأت ظاهرة القرصنة والاختراق مع بداية ظهور الحاسبة الالكترونية وازدادت بشكل كبير مع استخدام تقنية الشبكات حيث يشتمل الاختراق الهجوم على شبكات الحاسوب من قبل مخترقي الأنظمة الالكترونية ومنتهكي القوانين، كما يبين التطور الحامل في مجال سرية المعلومات التي تعطي الانترنت بالإضافة إلى تقنية أخرى كالاتصالات فإن عمليات القرصنة تطورت بسرعة فائقة[25]، وأصبح من الشائع جدا العثور على مواقع بالانترنت خاصة لترويج البرامج المقرصنة مجانا أو بمقابل مادي رمزي.

وأدت قرصنة البرامج إلى خسائر مادية باهظة جدا وصلت في العام 1988 إلى 11 مليار دولار أمريكي في مجال البرمجيات وحدها.

ولذلك سعت الشركات المختصة في صناعة البرامج إلى الاتحاد وإنشاء منظمة خاصة لمراقبة وتحليل سوق البرمجيات ومن ذلك منظمة اتحاد برمجيات الأعمالBusines software Alliance أو ما تعرف اختصارا بـ ASA، والتي أجرت دراسة تبين منها أن القرصنة على الانترنت ستطغى على أنواع القرصنة الأخرى، ودق هذا التقرير ناقوس الخطر للشركات المعنية فبدأت في طرح الحلول المختلفة لتفادي القرصنة على الانترنت.

ومنها تهديد بعض الشركات بفحص القرص الصلب لمتصفحي مواقعهم على الانترنت لمعرفة مدى استخدام المتصفح للمواقع لبرامج مقرصنة إلا أن تلك الشركات تراجعت عن هذا التهديد اثر محاربته من قبل جمعيات حماية الخوصصة لمستخدمي الانترنت.

كما قامت بعض تلك الشركات بالاتفاق مع مزودي الخدمة لإبلاغهم عن أي الموقع مخصصة للبرامج المقرصنة تنشأ لديهم وذلك لتقديم شكاوي ضدهم ومقاطعتهم إن أمكن أو إقفال تلك المواقع على الأقل.

---

[1]-. سامي علي حامد عياد، **الجريمة المعلوماتية وإجرام الانترنيت**، المرجع السابق، ص80.

والقرصنة عربيا لا تختلف كثيرا عن القرصنة عالميا إن لم تسبقها خطوات خاصة في ظل عدم توفر حقوق الحماية الفكرية أو في عدم جدية تطبيق هذه القوانين إن وجدت.

وتحاول سرد أهم حالات القرصنة التي حدثت عبر التاريخ كما يلي:

في عام 1985م قام شخص يدعى "روبيرتو سوتو" كولومبي الجنسية بسرقة خط تيلكس حكومي، ليرسل مجموعة رسائل عبره إلى مصاريف في المملكة المتحدة ومنها إلى دول أخرى ونتج عن هذه الرسائل نقل 13.5 مليون دولار من أرصدة الحكومة الكولومبية WORM.

وفي عام 1988 قام أحد طلاب جامعة "كورل" بزراعة برنامج في شبكة حواسيب حكومية انتشر خلالها في 6000 حاسوب وبعد أن تم كشفه تم طرده من الجامعة وحكم عليه بإيقافه على العمل 3 أعوام وتغريمه بمبلغ 10.000 عشرة آلاف دولار.

City Banks مجموعة من القراصنة الروس قام بنقل مبلغ 10 ملايين دولارا إلى حسابات مصرفية في مختلف دول العالم في عام 1994 وكان زعيم العصابة "فلادميرليفين" يستخدم حاسوب الشخصي لتحويل الأموال إلى حسابات في كل من فلندا وإسرائيل، وقد تم إيقافه في الولايات المتحدة الأمريكية وحكم علية بالسجن لمدة ثلاث سنوات.[26]

المبحث الثالث: مظاهر القرصنة الالكترونية:

[26] - سامي علي حامد عياد، **الجريمة المعلوماتية وإجرام الانترنيت**، المرجع السابق، ص ص80-81.

أ/ **تقليد برامج الحاسوب:** يقصد بتقليد برامج الحاسوب محاكاة برنامج معين يصنع أو إنتاج نسخ على مثاله بحيث تبدو عند تسويقها كالأصل.

ب/ نسخ برامج الحاسوب: وتعد هذه الصورة أهم صور القرصنة على البرامج وتتمثل في عملية النسخ الكلي أو الجزئي، سواء على طريق المحاكاة أم النسخ المباشر، حيث تقوم بعض الشركات بنسخ البرامج وبيعها دون ترخيص الشركة المنتجة، ويتم كذلك سرقة البرنامج الأصل عن طريق إزالة معالم وتغيير هيئته وإعادة تجهيزه على نحو يبدو وكنتيج جديد.[27]

2- عايد رجا الخلايلة، مرجع سبق ذكره، ص102،103.

وهناك نوعان يمكن أن يرد بهما نسخ البرامج هما النسخ المباشر أو ما يطلق عليه النسخ الحرفي، ويقصد به قيام مرتكب هذا الفعل بنسخ البرنامج بصفة كاملة أو بيعه دون الحصول على ترخيص بذلك من الجهات المعينة.

والنسخ غير القانوني للبرامج ويقصد به كل استخدام غير مسموح به للبرامج.

ج/ أسلوب الهندسة العكسية: يقصد به قيام بعض الشركات المتخصصة في تصنيع وإنتاج أجهزة لأداء وظائف معينة تؤديها أجهزة أخرى موجودة في الأسواق، حيث تكون الطريقة المتبعة في تصنيع وإنتاج الأجهزة الجديدة مختلفة عن طريقة تمنيع أو إنتاج الأجهزة الأصلية.

---

[27] -عايد رجا الخلايلة، **المسؤولة التقصيرية الالكترونية**، المرجع السابق، ص ص102،103

المبحث الرابع: خصائص الجريمة الإلكترونية

فيما يلي مجموعة من خصائص الجرائم الإلكترونية والتي تؤدي إلى ارتكاب الجريمة الإلكترونية منها:

1–الازالة (Removable) الجريمة الإلكترونية لا تتطلب الإزالة فيمكن نسخها فقط.

2–التوافر (Available) المعلومات في كل مكان جاهزة.

3–القيمة (Valuable) :معلومات بطاقات الائتمان والحسابات المصرفية والتصاميم قيمة.

4–المتعة (Enjoyable) كثير من الجرائم الإلكترونية ممتعة من مثل سرقة الموسيقى والمال.

5–الديمومة (Durable) المعدات والبرامج المسروقة يمكن أن تستخدم لفترة طويلة.

6–سرعة التنفيذ لا يتطلب تنفيذ الجريمة الإلكترونية الوقت الكثير وبضغطة واحدة على لوحة المفاتيح يمكن أن تنتقل ملايين الدولارات من مكان إلى آخروهذا لا يعنى أنها لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة.

7– التنفيذ عن بعد لا تتطلب الجريمة الإلكترونية في أغلبها (إلا جرائم سرقة معدات الحاسب) وجود الفاعل في مكان الجريمة بل يمكن للفاعل تنفيذ جريمته وهو في دولة بعيدة كل البعد عن مكان الجريمة سواء كان من خلال الدخول للشبكة المعنية أو اعتراض عملية تحويل مالية أو سرقة معلومات هامة أو تخريب الخ[28].

8–إخفاء الجريمة إن الجرائم التي تقع على الحاسبات الآلية أو بواسطتها (كجرائم الإنترنت) جرائم مخيفة، إلا أنه تلاحظ آثارها والتخمين بوقوعها.

[28]- عايد رجا الخلايلة، المسؤولة التقصيرية الالكترونية، المرجع السابق، ص ص103-104.

9- الجاذبية: نظرا لما تمثله سوق المعلومات والحاسب والإنترنت من ثروة كبيرة للمجرمين أو للإجرام المنظم فقد غدت أكثر جذباً لاستثمار الأموال وغسيلها وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن الدخول إلى الشبكات وسرقة المعلومات وبيعها أو سرقة البنوك أو اعتراض العمليات المالية وتحويل مسارها أو استخدام أرقام البطاقات.

10- عابرة للحدود الدولية (Transnational)إن ربط العالم بشبكة من الاتصالات من خلال الأقمار الصناعية والفضائيات والإنترنت جعل الانتشار الثقافي وعولمة الثقافة والجريمة أمرا ممكناً وشائعاً لا يعترف بالحدود الإقليمية للدول ولا بالمكان ولا بالزمان أصبحت ساحتها العالم أجمع

11- جرائم ناعمة تتطلب الجريمة التقليدية استخدام الأدوات والعنف أحياناً كما في جرائم الإرهاب والمخدرات والسرقة والسطو المسلح إلا أن الجريمة الإلكترونية تمتاز بأنها جرائم ناعمة لا تتطلب عنفاً فنقل بيانات من حاسب إلى آخر أو السطو الإلكتروني على أرصدة بنك ما لا يتطلب أي عنف أو تبادل إطلاق نار مع رجال الأمن.

12-صعوبة إثباتها تتميز الجريمة الإلكترونية عن الجرائم التقليدية بأنها صعبة الإثبات وهذا ا رجع إلى افتقاد وجود الآثار التقليدية للجريمة وغياب الدليل الفيزيقي (بصمات، تخريب، شواهد مادية) وسهولة محو الدليل أو تدميره في زمن متناه القصر، يضاف إلى ذلك نقص خبرة الشرطة والنظام العدلي وعدم كفاية القوانين القائمة[29]

[29] - عايد رجا الخلايلة، المسؤولة التقصيرية الالكترونية، المرجع السابق، ص 104.

المبحث الأول: واقع القرصنة الالكترونية في الجزائر :

إن القرصنة الالكترونية في الجزائر يمكن أن تدخل على المدى القريب والمتوسط من مؤثراتها، فتأثيرها يشابه والأزمة المالية العالمية المستفحلة حاليا فقد تم دق ناقوس الخطر بمناسبة احتفال تسليم شهادات الكفاءة لممثلي شركة IpBaick ، هذه الشركة العالمية المتخصصة في ميدان أمن الشبكات المعلوماتية ضمن تكوين مهندسين في الإعلام الآلي، ومن هنا تجلت الخدمات المضمونة من IpBaick في ميدان أمن الشبكات المعلوماتية، حيث أوضح ممثلوا هذه الشركة أن خدماتهم تضمن أقصى الأمن في تسيير شبكات المؤسسات.

* أما في الجزائر فأرادوا ممثلوا شركة IpBaick إجراء عملية تحسيس حول ظروف وإشكالية تأمين شبكات المعلوماتية في الجزائر ثم مناقشتها بقوة، حيث أوضحوا أن في الجزائر خطر الاعتداء المعلوماتي، وأوضحوا أن خطر الاعتداءات المعلوماتية ضد مواقع رسمية جزائرية يشكل تهديدا واقعا، ولحد الآن لا يوجد أي برنامج خاص بالجزائر مما يثير مخاوف أن تكون منظومتنا المعلوماتية لدى المؤسسات مقرصنة أو معتدي عليها.[30]

وأضافوا أن أخطار القرصنة في الجزائر موجود في أي زمان ومكان ومنذ عامين تمكن الجزائريون من حل شفرة TPS رغم أنه حتى ذلك الحين كان الروس هم في الطليعة هذا الميدان.

كما أوضح الرئيس مدير العام "نوار حرز الله" بأنه منذ وقت قريب فأن المواقع الالكترونية لمؤسسات الدولة كانت مستهدفة في كل حين موضحا بأن عدد الاعتداءات على مختلف مواقع web قد بلغت 3000 اعتداء في الشهر، وفي هذا الميدان فإن بعض المعتدين أو الهاكرزظ يظهرون وبعضهم يبدي افتخارا بإمضاء قرصنته لأكبر عدد من المواقع وذلك الغرور تسبب لهؤلاء الأشخاص بعقوبات مستحقة.

والملاحظة فإذا كانت الجزائر لا تزال في مؤخرة التقنية التكنولوجية فهي عكس ذلك في مجال القرصنة الالكترونية.

---

[30]- www.el-massa.com/ar/centent/view/27763/41.

فحسب المعطيات المنشورة من قبل الهيئات المختصة والصحافة الوطنية فالجزائر على رأس البلدان العربية في ميدان القرصنة.

كما أنه اختراق البرامج المعلوماتية يهم القراصنة الجزائريين وذلك لنزع الشفرة لباقات القنوات التلفزيونية الرقمية.

وعلى سبيل المثال فإن منتدى تبادل الشفرات دخول للباقات التلفزيونية المشفرة فإن الجزائريون يوجدون على رأس القائمة، ففي متوسط40 ألف متصل يوميا، 9 آلاف منهم جزائريون ويستعملون القرصنة كلمات سرية عن طريق برامج معروفة في هذا الميدان والمتواجدة في السوق الوطنية.

ويرى الخبير في التكنولوجيا الإعلام والاتصال السيد "قرار يونس" أن تطور تقنيات الإعلام والاتصال صاحبته أضرار منها القرصنة الالكترونية وفي السياق ذكر المتحدث أن درجة خطورة القرصنة في الجزائر قليلة مقارنة بمثيلتها من الدول خاصة في مجال التجارة الالكترونية التي لم تشرع بعد في استعمالها، إلا أنه ألم على ضرورة التفكير من الآن في تنظيم هذه العملية وتحصين المواقع وتأمينها من خلال التطبيق الصارم للإجراءات خاصة ما تعلق بقرصنة البرامج، حيث يبقى تطبيق عقوبات على المخالفين متفاوت رغم أن القانون يمنع أي نوع من القرصنة سواء كانت الكترونية أو كلاسيكية.

وحسب السيد "قرار" فإن التكتم عن ظاهرة القرصنة وعدم التبليغ وتقديم شكاوي عن حالات القرصنة خوفا من المشاكل التي قد يواجهها القائمون على الانترنت، يبقى عائقا أمام محاربة الظاهرة.[31]

من جهتها قالت باحثة بمركز البحث في الإعلام العلمي والتقني "**سيريست**" أن القرصنة الالكترونية في الجزائر منتشرة بصفة واسعة، وإن معظم البرامج المستعملة من قبل الجزائريين هي برامج مقرصنة ابتداء من أنظمة التشغيل منها نظام "الوندواس" ومختلف طبعاته المستعملة. وذكرت "للمساء" أن استعمال البرامج غير المقرصنة يعد جد ضئيل في الجزائر.

[31]- IBDI.

ويقتصر عن بعض المؤسسات الدولة والذي يبقى غير كاف لأن البرامج المقرصنة تباع في الأماكن العمومية دون حسيب أو رقيب وتقتنى بسهولة، كما أن الإقبال عليها واسع نظرا لتمنها الزهيد مقارنة بتلك الأصلية.

ويعود ذلك كما أضافت إلى عدم استيعاب أهمية الأمن المعلوماتي والثغرات والعيوب التي تحتوي عليها البرامج المقرصنة والتي تهدد أمن الأنظمة المعلوماتية، بينما يجب حسبها الذهاب نحو مصادر المجانية " Open sour" المعروفة بأمنها وإمكانية معرفة ثغراتها.

واعتبرت الباحثة أن أحسن طريقة لمواجهة القرصنة هو سن سياسة وطنية لتشجيع هذه الأنظمة الحرة ووضع مصلحة لأمن المعلومات والرقابة من الاختراقات والهجومات التي تهدد شبكات المعلوماتية الوطنية والتي تمس بوابات المواقع الجزائرية.

خاصة أن ما طرأ في السنوات الأخيرة من تطور في وسائل النسخ والإنتاج الالكتروني تجاوز الحدود حيث تباع النسخ المقرصنة غالبا بأسعار منافسة للنسخة الأصلية.

قيم السيد "**خليل**" وهو تقني سامي في الإعلام الآلي أنه مؤخرا بدأت الجزائر تعرف القرصنة الالكترونية، وبدأت تتعرض لبعض الهجمات من بعض القراصنة، لكن ذلك لا يجعل منها مستهدفة من قبلهم مثل باقي الدول في العالم ولعل ذلك راجع إلى قلة أو انعدام في بعض الأحيان استعمال التكنولوجيا الحديثة.[32]

أما السيد "**مصطفى يوسف تومي**" فصرح بأنه يوجد الكثير من القراصنة في الجزائر منهم من ألقي القبض عليهم ومعظمهم بسبب أمور سياسية مثل قرصنة البريد الالكتروني للرئيس الجزائري.

---

[32] فضيل دليو، التحديات المعاصرة، مخبر علم الاجتماع الاتصال، جامعة منتوري ، ص ص15.14.

-

أما السيد "فؤاد حلوان" فأفادنا بأنه صنفت الو.م.أ وللمرة الثانية على التوالي الجزائر في القائمة السوداء لأعلى نسبة تقليد والقرصنة للمنتجات الأمركية خاصة شركة مايكروسوفت حيث تمثل نسبة القرصنة البرمجيات 80% و85%، والقرصنة منتشرة بشكل ملفت للانتباه وكأنها أمر عادي.[33]

المبحث الثاني: الأسباب التي تدفع لارتكاب جرائم القرصنة:

يختلف مرتكبو جرائم المعلوماتية عن مرتكبي الجرائم الاعتيادية من حيث المبدأ وطريقة القيام بالعمل الإجرامي، لكن النهاية يبقى الطرفان مخالفين للقانون لذا يستحقوا العقاب بما اقترفوا من الجرائم.

وهناك عدة أسباب تدفع لارتكاب الجرائم المعلوماتية يمكن أن نختصرها في الآتي:

[33] - عمر يوسفي، التكنولوجيا الرقمية وحقوق المؤلف والحقوق المجاورة، دراسة وصفية تحليلة، شهادة ماجستير، 2008، ص127

- ***حب التعلم:***

يعتبر حب التعلم والاستطلاع من الأسباب الرئيسية التي تدفع لارتكاب مثل هذه الجرائم لأن المخترق يعتقد أن أجهزة الحاسوب والأنظمة هي ملك للجميع ويجب أن لا تبقى في المعلومات حكرا على أحد أي أن للجميع الحق بالتعرف والاستفادة من هذه المعلومات.

- ***المنفعة العامة:***

قد تكون محاولات الكسب السريع وحتى الأرباح الطائلة دون تعب ولا رأس مال من الأسباب التي تدفع لاختراق أنظمة الكترونية كالتي تستخدمها المصارف عن طريق الدخول إلى الحاسبات المصرفية والتلاعب فيها أو الاستخدام غير المشروع لبطاقات الائتمان.

وتنتشر الآن في الانترنت عشرات مواقع القرصنة التي تتضمن مختلف الأنواع من البرامج (الألعاب، نظم التشغيل، البرامج الخدماتية...) التي تجلب مجانا أو بأثمان بينما قد تقدر ثمنها في السوق بعشرات الآلاف من الدولارات، ويصطلح على تسمية هذا المواقع في المجتمع انترنت الموازي، بمواقع (warez) .[34]

- ***التسلل واللهو:***

عدد غير قليل من مخترقي الأنظمة يعتبرون من عملهم هذا وسيلة للمرح والتسلية وتقضيه أكبر وقت ممكن في أنظمة وحواسيب الآخرين ويكون هذا الاختراق غالبا سلميا ودون أن يحدث تأثير يذكر.

- ***الدوافع الشخصية:***

---

[34] - عمر يوسفي، التكنولوجيا الرقمية وحقوق المؤلف والحقوق المجاورة، **المرجع السابق**، ص121.

يعتبر محيط الإنسان والبيئة التي يعيش فيها من العوامل المؤثرة في سلوكه وتصرفاته وغالبا ما تدفع مشاكل العمل إلى رغبة بالانتقام ووجود أنظمة الكترونية تسهل له القيام برغباته فيعبث بمحتوياتها إلى درجة التخريب، أو يكون الدافع التحدي واثبات الجدارة أمام الآخرين بحيث يفتخر هذا الشخص بأن استطاعته اختراق أي حاسوب أو أي نظام ولا يستطيع أحد الوقوف بوجهه.

ولعل السبب الرئيسي وراء بعض عمليات القرصنة هو الدافع الاقتصادي حيث أن هناك من العاملين في مجال القرصنة من يحاول الدفاع علانية عن هذه الأعمال بغية إضفاء الشرعية عليها، مبررا توزيع النسخ المجانية من البرامج عبر الانترنت بالمساهمة في نشر المعلوماتية التي تفكرها شركات البرمجيات الكبيرة التي تطالب بمبالغ باهظة مقابلها، وذلك بتوفيرها بأسعار معقولة لعامة الناس.

ومعروف أن هذه العملية التجارية ببضاعتها الجاهزة تكسب بعض القراصنة أموالا طائلة لأنها لم تكلفهم جهدا كبيرا من العمل واستثمارات مالية أو بشرية ذات بال.

وحسب السيد "**حلوان فؤاد**" أن السبب الرئيسي في ذلك القرصنة يرجع إلى انعدام الرقابة وحماية حقوق الملكية الفكرية في بلادنا فأسواقنا أغرقت بالمنتجات المقلدة والمقرصنة ولكن لا يوجد أي عقوبات أو رقابة.[35]

أما السيد "تومي يوسف مصطفى" فقال : بأنه لا يمكن أن نقول أن هناك أسباب واضحة وخاصة أن الدول الأوربية ربع أطفالهم قراصنة حسب الإحصائيات وهذا إضافة إلى التطور التكنولوجي وخاصة البرامج التي تسهل الحصول على الرقم الخاص بالجهاز الحاسوب.

---

[1]-عمر يوسفي، التكنولوجيا الرقمية وحقوق المؤلف والحقوق المجاورة، **المرجع السابق**، ص122.

وقد أكد لنا السيد "محمد" أنه من أهم أسباب القرصنة الالكترونية من بينها : حب التعلم ولهذا المنفعة المادية وذلك من خلال الكسب السريع وجني الأرباح إضافة إلى التسلية واللهو بحيث يعتبرون عملهم هذا مجرد وسيلة للمرح، إضافة إلى الدوافع الشخصية المؤثرة في سلوك وتصرفات القرصان أو الهاكرز.[36]

المبحث الثالث: تصنيف القراصنة:

إن أفضل التصنيفات القراصنة الانترنت هو ذلك التصنيف الذي أورده "ويليم فوستروخ ودافيدكوف" في مؤلفهم جرائم الكمبيوتر، حيث تم تقسيم قراصنة الانترنت إلى فئتين: **المخترقون** و**المحترفون** الحاقدون (الكراكرز) علما أن بين الاصطلاحين تباينا جوهريا، متطفلون يتحدون إجراءات أمن النظم والشبكات، لكن لا تتوافر لديهم في الغالب دوافع حاقدة أو تخريبية وإنما ينطلقون من دوافع التحدي وإثبات المقدرة.

[36] - عمر يوسفي، التكنولوجيا الرقمية وحقوق المؤلف والحقوق المجاورة، المرجع السابق، ص 125.

- **الكراكرز** فإن اعتداءاتهم تعكس ميولا لجريمة خطرة تنبئ عنها رغباتهم في إحداث التخريب، إلا أن يعن الدراسات والمعالجة في حقل الجرائم الانترنت نعتمد هذا التميز دون أن يؤثر هذا التمييز على مسؤولية مرتكبي الأنشطة من كلا الطائفتين ومسائلهم عما يلحقونه من أضرار بالمواقع المستهدفة باعتداءاتهم.

حيث يعمد الكثير من مستخدمي شبكة الانترنت من الفضوليين إلى التسلل أو اختراق أجهزة أشخاص أو مؤسسات دون استئذان، فيبدأ بعضهم على سبيل التجربة والفضول وعندما يتمكن يعجبه الأمر وينساق فيه إلى حد بعيد، فيدخل أجهزة مستخدمي انترنت لا يعرفهم شخصيا ولا يعرف حتى مكان تواجدهم لسرقة أسرارهم والاستيلاء على ملفاتهم الخاصة، أو للتخريب ويتحول بذلك فضول العابث إلى اختراق احترافي، قد لا تصده حتى برامج اكتشاف حدوث الاختراقات والحماية منها.

ولقد كثر الحديث عن وقائع عملية كما في حالته اختراق أحد الصبية الذي يبلغ من العمر 14 سنة نظاما الكمبيوتر العائد للبنتاغون والآخر لا يتجاوز عمره 17 سنة تمكن من اختراق كمبيوترات العديد من المؤسسات الإستراتجية في أوربا والو.م.أ.[37]

ولعل السمة المميزة لقراصنة الانترنت هو تبادلهم للمعلومات فيما بينهم وتحديد التشارك في وسائل الاختراق وآليات نجاحها واطلاعهم بعضهم البعض على مواطن الضعف في نظم الشبكات والكمبيوتر، حيث تجري عمليات التبادل للمعلومات فيما بينهم وبشكل رئيسي عن طريق النشرات الإعلامية الالكترونية ومجموعات الأخبار[38]

---

[37] - عمر يوسفي، **التكنولوجيا الرقمية وحقوق المؤلف والحقوق المجاورة**، المرجع السابق، ص126.

[38] - عمر يوسفي، التكنولوجيا الرقمية وحقوق المؤلف والحقوق المجاورة، المرجع السابق، ص127.

- **أشهر قراصنة الانترنت في الجزائر:**

موريش، ماستر، أوكسيد، ماكسي32، هيزوكا4، انجل25، دي زاد... هي أسماء مستعارة ورموز أشهر قراصنة لانترنت بالجزائر ومعروفين في العالم أجمع عبر الشبكة العنكبوتية بفريق "دي زاد: Team DZ) وقد استطاع هذا الفريق وكلهم من الشباب العبقري في مجال التحكم شبه الكامل في تقنيات وأسرار الإعلام الآلي إلى درجة سمحت لهم باختراق أكثر المواقع تحصينا في أي بقعة على الكرة الأرضية، سيما منها الإسرائيلية والصهيونية العنصرية.

*القرصان "**انجل**" الذي يسكن بإحدى ضواحي عاصمة الشرق قسنطينة وهو من مواليد 1976 حيث بلغ عدد اختراقاته في هذا المجال أزيد من 150 موقع، دمرها جميعا ووضع بديلها عبارات تعكس موقفه من تلك المواقع، ومن بين المواقع المخترقة هي مواقع إسرائيلية، ومواقع دنمركية، وقد أوضح القرصان "أنجل" المتخرج من جامعة

قسنطينة في مجال الطاقة والذي تعلم وأتقن تقنيات الإعلام الآلي أنه اخترق مواقع هولندية مساندة لإسرائيل المغتصبة للأراضي العربية إضافة إلى مواقع شيعية إيرانية متطرفة.

وهناك أيضا القرصان الجزائري "Hisok4" "هيزوكا" والقاطن بولاية مستغانم، هذا القرصان تمكن بمفرده من اختراق آلاف المواقع في العالم أجمع وهو من أخطر وأقوى القراصنة المعروفين في العالم والدليل على ذلك ورود اسمه في مئات المواقع المدمرة من طرفه.[39]

كما يوجد قرصان جزائري آخر والذي يعرف بـ "co_2" وهذا أيضا يعد من أشد القراصنة ذكاء وفتكا، ويبقى ربما أخطر القراصنة الجزائريين على الإطلاق ، هو الذي رسم لاسمه أيضا بـ "crusty" حيث تمكن هذا القرصان من تدمير أزيد من ثمانية ألاف موقع في مدة زمنية محدودة، وإبلاغ صوت المستضعفين إلى العالم من المظلومين في فلسطين خاصة.

وهناك أيضا قرصان من مدينة المدية والذي يملك شهادة في الدراسات التطبيقية الجامعية لاعلام الالي للتسيير حيث يملك ألقاب عديدة يعرف بها ولعل من بينها DANKI، ناس ملاح وقباح، سرمد، ذبيح القدر، أما في قرصنة الاجهزة فيعرف باسم فتاة لم يرد أن يفصح عن الاسم، وعن أسباب قيامه بعمليات القرصنة قال لنا "سرمد": أن الدوافع الأولى هو حب التطفل والاطلاع على المعطيات الشخصية لآخرين.

أما بالنسبة إليه فلقد كانت بينه وبين مجموعة من الشباب تحدي حيث أنهم استهانوا به وانقصوا من قدراته العلمية وبأنه شخص غير كفؤ لممارسة الإعلام الآلي وكانت تلك البداية.

وقد وضح "سرمد" أنه يوجد أنواع للقرصنة؟ فهناك قرصنة على الأجهزة والقرصنة على المواقع، وقد أعطى لنا مثال تطبيقي على كيفية قرصنة موقع الكتروني.

---

[39]- www.echoroukonline.com,le 25/01/2018,à 12:45.

وعن المواقع الأكثر استهدافا من طرفه فقال بأنه استهدف المواقع التي تهين شخص النبي صلى الله عليه وسلم، إضافة إلى مواقع مصرية عندما كانت الحرب الالكترونية بيننا وبينهم، إضافة إلى بعض المنتديات والمواقع الإباحية.[40]

المبحث الرابع: إحصائيات القرصنة الالكترونية في الجزائر:

ومن بين العمليات الكبرى المشهورة للقراصنة الجزائريين سواء كانوا في داخل الوطن أو خارجه، وهو أشهر قرصان جزائري والمدعو "Maure"، حيث تمكن هذا القرصان من تحقيق نجاح لم يبلغه أحد قبله فلقد تمكن من دخول أو اختراق موقع البنك المركزي الإسرائيلي والذي كان جد مؤمنا وبدل فيه محتوى الصفحة الأولى الافتتاحية.[41]

صرحت شركة **ميكروسوفت** أن قرصنة برامجها المعلوماتية في الجزائر ونسبة التعاملات غير الشرعية في هذا المجال = 95% أي ما يقارب40 مليون دولار.

---

[40] IBDI..-

[41]- http://3w.bladi.dz.com/articles/1883/1/la-securiteinformatique-en Algérie/page1html.le 15/03/2018,à 14:25.

وحسب شركة Bsines Softeware Alliance=BSA نسبة القرصنة للبرامج المعلوماتية يقدر بـ 84% في الجزائر وهذا بإدخال صناعات البرامج كلها وليس فقط لميكروسوفت بل لكل المنتجين لها بخسائر تقدر بـ 86 مليون دولار.

أما في الميدان الصحفي البصري يضيعون للجزائر ما يقارب 25 مليون دينار أي 290ألف أورو كل عام كحقوق مؤلف وهذا حسب الديوان الوطني لحقوق المؤلف الذي يحاول إحالة الظاهرة لعمليات المراقبة.

وبين 20% و30% من الأشرطة المسموعة و50% من الأقراص المضغوطة في السوق الجزائرية هي مقلدة وتم تصنيعها على أساس برامج مقلدة، هذا ما وضح المدير العام المساعد للديوان الوطني للحقوق المؤلف "محمد امزيان زنتر" لوكالة الأنباء الفرنسية.

إضافة إلى أنه 90% من المؤسسة تعمل ببرامج مقلدة[42].

المبحث الخامس: المنظومة القانونية ومكافحة القرصنة الالكترونية:

إن الحكومة قد صادقت على منظومة لمكافحة الجريمة المعلوماتية ولهذا التهديدات التي تمثلها هذه المنظومة ضرورية لحماية اقتصاد البلد والوطن غير أنه يجب إيجاد وسائل تنفيذها وأخيرا، فإن حماية الفرد يجب أن يكون موضع قانون إذ أن الانترنت مجال غير معروف حيث تكون المعلومات تتداول بدون أن نعرف هي حقيقة أم لا.[43]

وقد كشف "**جمال بوزيتي**" مدير مركز البحوث القانونية والقضائية في تصريح له لجريدة الأجواء أنه عن قرب الانتهاء من المرسوم القانوني الخاص بإنشاء هيئة وطنية لمحاربة الجريمة المعلوماتية وسيدخل حيز التطبيق خلال أيام القليلة القادمة، وصرح بوزيتي على هامش الملتقى الدولي حول الجريمة المعلوماتية أن الجريمة المعلوماتية ستتفاقم خلال

---

[42] - http://www.dzmag.info/plus-dinfo/technologie/mafia-crew-purate-des-sites -Algeriens-impartents96.le 13/04/2018, à08:36.

[43] http://actu-voila.fr/Article-hightech.040816142509.2puo3x2.html,le 14/04/2018,à12:45.

السنوات المقبلة في الجزائر وستشكل خطرا أكبر على المجتمع لذلك فالدولة قد اتخذت الإجراءات اللازمة للحد من تفاقمها في المجتمع وهو السبب الذي جاء من أجله المرسوم التنفيذي الخاص بإنشاء هيئة وطنية لمحاربة الجريمة المعلوماتية والذي تم الانتهاء منه تقريبا ولم يبقى الكثير ليدخل حيز التنفيذ وفي سياق متصل دعا "بوزيتي" المواطنين إلى الاعتماد على الشركات والمنظمات الوطنية في الجزائر من أجل إنشاء وتسيير مواقعهم الالكترونية.

وهذا من أجل التحكم في سلامتها وعدم تعرضها إلى القرصنة وسهولة معالجة أي انتهاك في حقها دون العودة إلى الشركات أخرى أجنبية موجودة خارج الوطن.

وأضاف ذات المتحدث أنه تم تكوين حوالي 50 قاض في إطار كيفية معالجة القضايا الخاصة بالجريمة المعلوماتية التي تزداد انتشارا كل سنة في بلادنا.[44]

وحسب الأخصائيين فإن القرصنة الالكترونية للجزائريين قليلة على عكس ما يروج عنه فغالبية من يحترفون القرصنة هم مجموعة مبتدئين، وعلى هذا الأساس سنت الجزائر خلال السنة الجارية قانون للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، و ذلك في خطوة نحو ردع جرائم المعلوماتية، خاصة ما يتعلق منها بتسخير الوسيلة التكنولوجية للترويج للإرهاب والدعاية، وبذلك تكون الحكومة قد أخذت أول خطوة نحو سد الفراغ القانوني الذي كان موجودا في مكافحة الجريمة المعلوماتية.

ويعد هذا القانون الذي يأتي في سياق مكافحة الإرهاب الالكتروني بمثابة إطار قانوني مهم يحدد في بابه الأول تعريف وتحديد الجرائم المعلوماتية، ثم ينتقل إلى إمكانية الحد منها ومواجهتها بعد أن أصبحت تلك الجرائم من بين الجرائم التي تهدد أمن وسلامة المجتمعات حيث جاء في 19 مادة و06 فصول تؤكد في مجملها على احترام مبدأ محافظة على السرية الاتصالات إلا في استثناءات حددها المشروع.

2- العدد 1031) ص03. هناء طالبي، وزارة العدل تعلن عن قرب الانتهاء من الهيئة الوطنية لمحاربة الجريمة المعلوماتية، (2010/05/06،

وقد تضمن القانون المتعلق بجرائم المعلوماتية مثلما اشرنا سابقا 19 مادة و06 فصول.

الفصل الأول: تعريف هذا الموضوع من حيث الاصطلاح وكذلك مجال تطبيق هذا القانون تحت عنوان: "احترام مبدأ حرية المراسلة والاتصال" وهذا ما عدى المجالات الاستثنائية كجمع وتسجيل محتوى هذه المرسلات من أجل تحريات وتحقيقات والحجز أو القبض في مجال نظام المعلوماتية.

الفصل الثاني: تضمن مراقبة الاتصالات الالكترونية لأهداف احتياطية والأخذ بالحسبان خطورة التهديد المحتمل وأهمية الأهداف المحمية.[45]

وعلى هذا الأساس فلعمليات المراقبة الالكترونية لا يمكن العمل بها إلا بموجب تصريح من جهة قضائية مختصة.

إن مراقبة الاتصالات الالكترونية مسموح بها في أربع حالات هي:

* الاحتياط لحدوث جرائم موصوفة بالأعمال الإرهابية أو تخريبية وجرائم ضد أمن الدولة في هذه الحالة يرخص لضباط الشرطة القضائية من طرف النائب العام لمجلس القضاء).

* وفي حالة وجود معلومات حول إمكانية إصابة نظام معلوماتي يمثل تهديد المؤسسات الدولة وذلك من أجل الدفاع عن الوطن أو من أجل النظام العام.

*ومن أجل البحث والتحقيق معلومات قضائية في حالة وجود صعوبات في الوصول إلى نتائج الأبحاث الجارية بدون اللجوء إلى المراقبة الالكترونية.

---

[45] المرجع السابق، ص31. هناء طالبي، وزارة العدل تعلن عن قرب الانتهاء من الهيئة الوطنية لمحاربة الجريمة المعلوماتية،

الفصل الثالث: تضمن قواعد الإجرائية المتعلقة بالتحقيقات وكذلك القبض في حالة الجرائم المتعلقة أو المرتبطة بتكنولوجيا الإعلام والاتصال.

الفصل الرابع: أقر الالتزامات التي تقع على عاتق المتعاملين في مجال الاتصال الالكتروني وتحديدا الالتزام بحفظ وضمان المعطيات المتعلقة بالأعمال غير الشرعية التي تسهل للشرطة العلم بهذه الجرائم وتحديد هوية القائمين بها.[46]

الفصل الخامس: هناك مشروع قانون يفترض إنشاء منظمة وطنية ذات عمل تنسيقي في مجال ومحاربة الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال لتنشيط وتنسيق عمليات الاحتياط ضد جرائم المعلوماتية إضافة إلى مساعدة الهيئات القضائية وكذلك مصالح الشرطة القضائية في التحقيقات التي تجريها في مواضع الجرائم، بالإضافة إلى جمع المعلومات والخبرات القضائية هذه المنظمة ستكون المكلفة كميزة لهذا المشروع بتجادل المعلومات مع نظراء جانب من أجل مكافحة هذه الأنواع الخطيرة من السلوكات الإجرامية.

الفصل السادس: عرف القواعد القانونية والتنسيقات الدولية عن طريق توسيع اختصاص المحاكم الجزائية تحديدا من أجل ما يعرف بالجرائم المتعلقة بتكنولوجيات الأعلام والاتصال تحديدا حينما تكون هذه الجرائم مرتكبة من طرف أشخاص ذو حصانة، ومن أجل أهداف إستراتيجية للجزائر.

وبالحديث عن التنسيق الدولي يتضمن القانون مجموعة من المبادئ العامة المتعلقة تحديدا بالمساعدة وتجادل المعلومات على أساس التبادل.[47]

تدابير لتسيير مقاهي الانترنت في الجزائر:

وفي هذا الصدد اعتبر عميد الشرطة بمديرية الشرطة القضائية "**عبد القادر مصطفاوي**" القرصنة الالكترونية هي جريمة من الجرائم المنصوص عليها في المادة 394 من قانون العقوبات الذي يعتبرها مساسا بأنظمة المعالجة الآلية

[46] - هناء طالبي، وزارة العدل تعلن عن قرب الانتهاء من الهيئة الوطنية لمحاربة الجريمة المعلوماتية، المرجع السابق، ص32.

[47] -www.bladi-dz.com/articles/1883/1/la -securité,le 14/03/2018,à 15:30.

للمعطيات "كل دخول إلى نظام معلوماتي وتغيير معطياته أو سرقتها أو تخريبها"، حيث تعالج هذه الجرائم المرتبطة بالتطور التكنولوجي كيفية الجرائم على مستوى الشرطة القضائية التي تقوم بمعاينة هذا النوع من الجرائم والبحث عن المجرمين وتقديمهم أمام العدالة، وذلك بالاعتماد على تقنيات تحقيق حديثة وتقنيين مختصين ومحققين تم تكوينهم في هذا المجال من خلال خمس دورات تكوينية تم تنظيمها منذ 2002[48].

ولا يزال الإحجام عن تبليغ مصالح الشرطة عن الجرائم الالكترونية المرتكبة، عائقا يحول دون التعرف على المجرمين والضحايا الذين يتعرضون للقرصنة فضلا عما ينجز عن الجرائم الكلاسيكية المرتكبة عن طريق الوسائل التكنولوجيا الحديثة للإعلام والاتصال من مشاكل كالترهيب عن طريق رسائل التهديد والرسائل المخلة بالحياء واستعمال التكنولوجيات الحديثة للترويج للإرهاب.

وفي هذا الإطار أشار محافظ الشرطة "عبد القادر مصطفاوي" في اللقاء الذي خص به "المساء" إلى أن مصالح الشرطة القضائية تقوم بحملات تحسيس للمواطنين وتوعيتهم من أجل رفع شكاوي عند تعرضهم للقرصنة أو التهديد وتمكين الشرطة من التحقيق في الميدان، مؤكدا على ضرورة وضع تدابير تنظيمية تخص تسيير مقاهي الانترنت وتجميد المواقع الإباحية المفتوحة التي تستعمل في غياب الرقابة الصارمة على هذه الأخيرة.

- **إنشاء مركز وطني للمراقبة تدفق المعلومات:**

ثمن السيد "**قرار يونس**" وهو خبير في تكنولوجيا الإعلام والاتصال الوصاية المتعلقة بإنشاء مركز وطني لمراقبة تدفق المعلومات الذي سيكون جاهزا السنة المقبلة والذي سيضبط أكثر تبادل المعلومات ويحمي المشاركين من أي قرصنة من خلال جمعه كل ممولي الانترنت.

واعتبر المختص في المعلوماتية المركز الذي سيتم استحداثه مركزا ذكيا يؤمن المعلومات من خلال وضع نقطة التقاء بين مختلف الممولين المراقبة المحتويات ومنع المواقع غير المرغوبة فيها سواء من قبل الممول أو من قبل الدولة التي

---

[48] - -www.el-massa.com/ar/centent/view/27763/41,le 12/03/2018,à 12:12.

لها الحق في الاطلاع على ما يجري عبر الشبكة العنكبوتية، خاصة أن الجزائر تعتبر الوحيدة التي لها الحرية المطلقة في دخول المواقع واستعمالها.[49]

آخر إحصائيات قضايا الجريمة المعلوماتية :

كشف "**مختار لخضاري**" مدير الشؤون الجزائية وإجراءات العفو بوزارة العدل عن نسجيل 12 قضية لجرائم معلوماتية طرحت على المحاكم، و20 شخص متابع منذ بداية السنة الجارية، ومع وضع88 شخص رهن الحجز مما يستدعي مناقشة كيفية محاربة هذه الجريمة نظرا لأخطارها على الأمن الوطني وسلامة الأشخاص، أوضح "**مختار لخضاري**" خلال ملتقى دولي دول الجريمة المعلوماتية نظم بفندق الشراطون تحت الرعاية السامية لوزير العدل وحافظ الأختام "الطيب بلعيز" أن قضايا الدخول غير المشروع مع إتلاف المعطيات تشكل نسبة ù34 والدخول غير المشروع 1.29، إدخال معطيات خلسة 21%، المتاجرة في المعطيات المتحصل عليها من دخول غير مشروع 2%، أما عن مرتكبي هذه الجرائم فيتراوح منهم ما بين 25 و 30 سنة بأعلى نسبة 68% ولهم معرفة بالمعلوماتية، كالطلبة والتنفيس وعلاقته بالضحية غالبا مهنية، في حين تكون الدوافع غالبا مادية بنسبة 65% لكن هناك دوافع أخرى كالانتقام أو الفضول أو التحدي وحسب ذات الإحصائيات يشير ذات المتحدث، فالضحية في الغالب تتمثل في إدارات عمومية ومؤسسات ذات طابع صناعي وتجاري بنسبة60%وشركات خاصة بنسبة 20% وباقي النسبة تمثلها شركات أجنبية وهيئات عمومية.

وقد تحدث المشاركون عن تطور تكنولوجيا الإعلام والاتصال وتوسع نطاق استعمالها وسواء على المستوى الدولي أو الوطني، والذي يعد من العوامل التي أدت إلى اتساع الجريمة المعلوماتية أو ارتكاب الجرائم الكلاسيكية من نصب، تمويل الإرهاب والإشادة بالأعمال الإرهابية.

---

[49]- هناء طالبي، وزارة العدل تعلن عن قرب الانتهاء من الهيئة الوطنية لمحاربة الجريمة المعلوماتية، المرجع السابق، ص 35.

الاعتداء على أخلاق القصر وكذلك التضليل خاصة على الأعمال المدربية والتخويف على شبكة الانترنت كتلقي رسائل مشينة أو صور خليعة وللإشارة فقد حضر الملتقى قضاة من الأقطاب الجزائية المتخصصة وقضاة من النيابة، والتحقيق والحكم ومختصون جامعيون، وكذلك مجموعة من الخبراء الجزائريين والأجانب من الولايات المتحدة الأمريكية وفرنسا وانجلترا.[50]

- **أهم سبل الحماية:**

يرى الخبراء أن هناك احتياطات للحيلولة دون التعرض للقرصنة الالكترونية والفيروسات خاصة:

1. شراء برامج أصلية، والمغلقة بغلاف الشركات المنتجة أو من الوكيل المعتمد أو من مورد ذات سمعة طيبة.

2.لا يتم النسخ لأي برنامج على جهاز الحاسب الآلي إلا إذا كان القرص المحصل عليه البرنامج جيدا ومغلقا.

3. لا يتم قبول أي قرص كهدية من شركة أو جهة مجهولة أو مورد غير معروف.

4. يجب استخدام برامج مسح الفيروسات VIRUS SCAN، وذلك لتأكد من أن البرامج سليمة، وذلك قبل تحميل البرامج على القرص الصلب.

5. إذا تم استخدام أحد الأقراص على جهاز حاسب إلى آخر، غير الحاسب المستعمل، فلا بد من التأكد من أن القرص لم يصب بفيروس من الحاسوب الآخر.

*** ويضيف الباحثون إلى الإجراءات السابقة الإجراءات العملية ونلخصها:**

---

[50] المرجع السابق، ص38. هناء طالبي، وزارة العدل تعلن عن قرب الانتهاء من الهيئة الوطنية لمحاربة الجريمة المعلوماتية،-

1. عدم فتح الملفات وهذه طريقة تحول دون التعرض لأوبئة الفيروسات خاصة عندما تكون منتشرة وتكون من الأنواع الخطرة حتى لو كان البريد الالكتروني مثلا من مصدر ذا ثقة فيجب التحوط وتوخي الحذر ذلك أن أحدث الفيروسات قد احتلت قوائم الرسائل الالكترونية وبعثت بدلا منها رسائل جديدة، ملحق به الشحنة التدميرية للبرنامج ولذلك يفضل مراجعة الملفات بصورة مستمرة بحثا عن الفيروسات وإبادتها.[51]

2.ضرورة توخي الحذر والحيطة الدائمين، فهناك دائما فيروسات جديدة بصفة تكاد أن تكون يومية، ولذلك لا بد من البحث عن الحلول الدائمة والمستمرة.

كما يجب اتخاذ احتياطات للحماية من الهاكرز منها:

1. استخدام أحدث برامج الحماية من الهاكرز والفيروسات وقم بعمل مسح دوري وشامل على جهازك في فترات متقاربة خصوصا إذ كان جهازك متصل بالانترنت بشكل يومي.

2.لا تدخل إلى مواقع مشبوهة مثل المواقع التي تعلم التجسس والمواقع التي تحارب الحكومات أو المواقع التي تحوي أفلاما وصورا خليعة لأن الهاركز يستخدمون أمثال هذه المواقع في إدخال ملفات التجسس إلى الضحايا حيث تنصب ملف التجسس (الباتش) تلقائيا في الجهاز بمجرد دخول الشخص إلى الموقع.

3.عدم فتح رسالة الكترونية من مصدر مجهول لأن الهاكرز يستخدمون رسائل البريد الالكتروني لإرسال ملفات التجسس إلى الضحايا.

4. عدم استقبال ملفات أثناء (الشات CHAT) من أشخاص غير موثوق بهم وخاصة إذا كانت هذه الملفات تحمل امتداد (EXE) مثل: (LIVE.EXE) أو أن تكون ملفات من ذوي الامتدادين مثل:(

[51] - هناء طالبي، وزارة العدل تعلن عن قرب الانتهاء من الهيئة الوطنية لمحاربة الجريمة المعلوماتية، المرجع السابق، ص39.

ahmed.pif.jpg) وتكون أمثال هذه الملفات عبارة عن برامج ملفات التجسس في جهازك فيستطيع الهاكرز بواسطتها من الدخول إلى جهازك وتسيب الأذى والمشاكل لك.

5. عدم الاحتفاظ بأية معلومات شخصية في داخل جهازك كالرسائل الخاصةأو الصور الفوتوغرافية أو الملفات المهمة وغيرها من المعلومات بنكية مثل أرقام الحسابات أو البطاقات الائتمانية..[52]

6. قم بوضع أرقام سرية على ملفاتك المهمة حيث لا يستطيع فتحها سوءا من يعرف الرقم السري فقط وهو أنت.

7. حاول قدر الإمكان أن يكون لك عدد معين من الأصدقاء عبر انترنت وتوفي فيهم الصدق والأمانة والأخلاق.

8. حاول دائما تغير كلمة السر بصورة دورية فهي قابلة للاختراق.

9. تألم من رفع سلك التوصيل بالانترنت بعد انتهاء من استخدام الانترنت.

10. لا تقم باستلام أي ملف وتحميله على القرص الصلب في جهازك الشخصي إن لم تكن متأكدا من مصدره.[53]

[52] المرجع السابق، ص42. - هناء طالبي، وزارة العدل تعلن عن قرب الانتهاء من الهيئة الوطنية لمحاربة الجريمة المعلوماتية،

[53] هناء طالبي، وزارة العدل تعلن عن قرب الانتهاء من الهيئة الوطنية لمحاربة الجريمة المعلوماتية، المرجع السابق، ص43.

الاطار التطبيقي

السمات العامة :

1-توزيع المبحوثين حسب الجنس:

الحنس	التكرار	النسبة المئوية
الذكور	**7**	**%77.78**
الإناث	**2**	**%22.22**
المجموع	**9**	**%100**

*نلاحظ من خلال الجدول أعلاه أن أغلبية المبحوثين من فئة الذكور التي قدرت مفردتهم ب: 7مفردة أي ما يعادل 77.78% من عينة البحث، مقارنة بفئة الإناث الذين قدر مفردتهم ب: 2 مفردة بنسبة 22.22%، والزيادة في عدد الذكور تؤكد بأنها الغالبية العظمى الذين تعرضن للقرصنة الإلكترونية بدلا من الإناث الذين لا يصرحن بإجابتهم بأنهم تعرضن للقرصنة الإلكترونية خوفا من تشويه صورتهم الشخصية.

2-توزيع العينة حسب السن:

السن	التكرار	النسبة المئوية
23-18	**1**	**%11.11**
28-23	**3**	**%33.33**
33-28	**5**	**%55.56**
المجموع	**9**	**%100**

*نلاحظ من خلال الجدول أن أكبر نسبة فيما يتعلق بمتغير السن هي الفئة التي تتراوح أعمارهم ما بين 55.56سنة والتي تقدر ب: 5 مفردة، تليها الفئة العمرية المتراوحة سنهم ما بين 23-28 سنة وهو ما يمثل نسبة 33.33% في حين تحتل الفئة العمرية من 18-23 سنة المرتبة الثالثة ب :1 مفردة أي ما يمثل 11.11% .ومن هنا نفسر ان المبحوثين أكثر عرضة للقرصنة بدرجة كبير هم الفئة العمرية التي تتراوح أعمارهم ما بين 28-33 وتليها الفئة التي

تتراوح أعمارهم ما بين 23-28 سنة من خلال الولوج إلى مواقع غير معروفة أصحابها.أم الفئة التي تحتل أدنى المرتبة هم فئة الشباب .

3-توزيع أفراد العينة حسب مستوى التعليمي؟

المستوى التعليمي	التكرار	النسبة المئوية
مستوى متوسط	2	%22.22
مستوى ثانوي	3	%33.33
مستوى جامعي	4	%44.45
المجموع	9	%100

* نلاحظ من خلال الجدول أعلاه أن مستوى المبحوثين تمثل في مستوى جامعي الذي قدر ب: 4 مفردة أي ما يعادل نسبة 44.45% وتليها نسبة 33.33% من مستوى ثانوي، أما مستوى متوسط أحتل المرتبة الأدنى أي ما يقدر ب: 2مفردة ما يعادل 22.22%.

4-توزيع أفراد العينة حسب الحالة الاجتماعية:

الحالة الاجتماعية	التكرار	النسبة المئوية
متزوج	5	%55.56
أعزب	3	%33.33
مطلق	1	%11.11
المجموع	09	%100

*نلاحظ من خلال الجدول أعلاه أن الفئة الأكثر تعرضاً للقرصنة الإلكترونية هم المتزوجين الذين قدرت مفردتهم ب: 5 أي ما يعادل نسبة 55.56%، وتليها نسبة 33.33% العزب، أما الفئة المطلقين تحتل المرتبة الأخيرة والتي قدرت بنسبة 11.11 .

المحور الأول: كيفية تعرض المبحوثين للقرصنة الإلكترونية:

س1: كيف تم تعرضك للقرصنة؟

المبحوث الأول:

صاحب 24 سنة طالب جامعي أجب على سؤال بأنه تعرض للقرصنة من خلال الولوج إلى مواقع غير معروفة أصحابها.

المبحوث الثاني:

البالغ من العمر 18 سنة وهو تلميذ في السنة الثالثة نهائي حيث أجب بأنه تعرض في العديد من المرات إلى القرصنة من خلال استخدامه للأنترنت بمجانية .

المبحوث الثالث:

البالغ من العمر 33 سنة وهو بائع الملابس أجب هو الآخر بأنه تعرض للقرصنة نتيجة مجانية الأنترنت وكذلك استخدام الملاحقات التنفيذي مع البريد الإلكتروني.

المبحوث الرابع :

البالغة من العمر 27 سنة وهي عاملة بمقهى الأنترنت تعرضها للقرصنة باستخدام آليات التهديد والتشهير بصورها الشخصية على مستوى حسابها في الفيس بوك.

التحليل :

من خلال المبحوثين 1.2.3.4 والتي كانت من جنس 3 ذكور و أنثى واحدة والمتراوحة أعمارهم بين 18-33 سنة نجد أن هناك اختلاف في تعرضهم للقرصنة حيث تركزت معظم الإجابات على مجانية الأنترنت وكذلك استخدام مواقع غير معروفة أصحابها وكذلك ملحقات ذات طابع التنفيذي مع البريد الإلكتروني والتي تتمظهر القرصنة جلياً في

التشهير بالصور والتهديد، حيث أن القرصنة اصبحت في الوقت الحالي خطراً على حياة الشخصية سواءً كانوا متعلمين أو غير متعلمين من مختلف الأعمار وذلك عن طريق عملية إختراق لأجهزة الحاسوب عن طريق شبكة الأنترنت والتي تتميز هذه الأخيرة بسهولتها ومجانيتها وأكثر استقطاباً للمجتمع فأصبحت وسيلة سهلة للتحقيق عملية القرصنة الإلتكرونية خصوصاً بعد دخول الفيس بوك إلى المجتمع الجزائري الذي أعطى منبراً للقرصنة الإلكترونية بنمط جديد سواء عن طريق الصور ملفات مما يؤدي إلى اختراق خصوصية.

س2: ماهي المخلفات الناتجة عن تعرضك لهذه الجريمة المعلوماتية؟

من خلال اجابات المبحوثين عن المخلفات الناتجة عن تعرضهم للجريمة الإلكترونية هي اعتراض البريد الإلكتروني قبل وصوله إلى المرسل وإرسالها باسم آخر وكذلك زرع ملفات التجسس مما يؤدي إلى مخلفات ناتجة عن تعرض لهذه الجريمة الإلكترونية من خلال المساس بالشخصية وايذاء السمعة وهو ما أكده المبحوث رقم 4 والذي أجب "أنني تعرضت للإهانة كبرى بين كل من يعرفني وأصبحت في نظري المجتمع مجرم على جريمة لم ارتكبها اطلاقاً. كمّا أكد المبحوث رقم 5 "إنني تعرضت لسرقة الملفات الشخصية التي أدت إلى ايذاء سمعة، وكذلك ايذائي ماديا وعقلياً".

التحليل:

لقد سببت القرصنة الإلكترونية العديد من المخلفات على نفسية المبحوثين وتعدت بذلك إلى محيط اجتماعي المنتمي إليه من خلال غرس سلوكات وتصرفات تبقى راسخة في ذهنه مما تؤدي إلى أمراض نفسية واحباط كبير في الفرد مما يؤدي إلى عواقب وخيمة على سمعة المادية والمعنوية بطريقة مباشرة أو غير مباشرة تجعل من مستخدمي القرصنة وسيلة تحقق لهم دوافع عديدة سواء في حب التعلم أو الدوافع الشخصية كالإنتقام أو التسلية واللهو ةالتي في نظر القانون الجزائري محضورة يعاقب عليها بسن قوانين متعددة.

س3: ما موقفك من القرصنة؟

من خلال ايجابات المبحوثين نجد أن موقفهم سلبي حيث يعتبرون أن القرصنة نشاط ايجرامي وجريمة كبرى في حق الضحايا تستهدف حياتهم الشخصية خصوصا أن المجتمع الجزائري مجتمع عمي موسى مجتمع متماسكا ومحافظ على

شرفه خصوصا اذا مست هده الجريمة الفردية وهو ما أكده المبحوث رقم 01 الذي أجاب بطريقة تحكمية ان الجريمة الالكترونية موقفهما الصاعد لا يستدعي التفكير مثلها مثل جريمة القتل كما أكد المبحوث رقم 02 ان استخدام تقنية الحاسب الالي بطرقة سلبية تستدعي اتخاذ موقف سلبي كون هذه الاخيرة تهدف لتنفيذ فعل اجرامي يمس الجانب المادي والمعنوي للافراد

التحليل :

ان الجريمة الالكترونية اصبحت اليوم واقعا يفترض الالمام بجوانبه خصوصا أن موقف المجنمع الجزائري " **عمي موسى** " يبقى مناقضا تماما لهذه الظاهرة التي اصبحت تمس شرائح مختلفة من المجتمع خصوصا هذه الاخيرة اصبحت تحقق منفعة تنطي تحت الربح بالسريع دون أي تعب ولا رأس المال الامر الذي جعلها تفوق مؤشر التزايد يوميا دون أي رقابة من طرف الدولة

س4 كيف تمكن الهاكرز من دخول الى جهازك؟

تمركزت معضم اجابات المبحوثين الى ان الهكر تمكن من دخول الى جهازك عن طريق نوافذ سرية وفيروسات متعددة مجهولة أصحابها هو ما أكدته المبحوثة رقم 04 أن الهكرز تمكن من دخول جهاز حاسوب عن طريف نوافذ سرية وهي عبارة عن ملفات واسعة تحتوي على فيروسات والتي كانت تصلني راسائل من عدة اسماء حيث أنه بمجدر فتحها للحاسوب تصبح مخترق كما اضافت في نفس السياق المبحوث رقم 05 و 03 تم اختراق جهاز الحاسوب كوني كنت استخدم البريد الالكتروني دون دراية مني كوني لا اعلم معلومات كافية وخبرة في هذا التخصص

التحليل :

لقد تنوعت اختراقات الهاكرز او ما يلقبه العديد بالقرصان عدة طرق سواء باستخدام الفايروس أو نوافذ سرية أو ملفات التجسس في جهاز الضحية أو عن طريق نوافذ سرية كأم صاحبها أصبح مالك ثاني للحاسوب بطريقة خفية تجعل العلاقة بين الانترنت والضحية والهاكرز علاقة تأثير وتأثر مؤثر يبقى فيها الفرد المتعرض لهذه الجريمة الضحية واحدة لا غير .

س5 : ماهي الاشياء التي يبحث عنها الهاكرز ؟

تمركزت معضم اجابات المبحوثين الى ان الهاكرز يبحث للحصول على المعلومات والصور الشخصية بدافع الابتزاز لاغراض مالية أو انحرافية حيث أجابة المبحوثة رقم 04 أن أهم الاشياء التي يبحث عنها الهاكرز هي التهديد بنشر الصور على الانترنت خصوصا عند عدم الاستجابة لمطالب انحرافية أو مالية بالستخدام اتصالات مجهولة يطلب فيها المتصل مبلغ مالي مقابل نشر صورها على مواقع التواصل الاجتماعي كما أكد المبحوث 07 ان اهم ما يبحث الهاكرز عنه هو اثبات القدرة على الاختراق وجعل من ذلك فرصة لتحقيق النصر قد تكون من اتفه الاسباب حيث تم التعرض للقرصنة نتيجة لمناوشات دارت ببيني وبين صديقي على عدم قدرته على قرصنت ملفاتي الشخصية

التحليل :

ان الاشياء التي يبحث عنها الهاكرز ليست ذات دوافع انسانية وانما عكس ذلك تهدف الا التسلية عن طرق نشر الصور وتهديد الاشخاص لمشاركتها في مواقع التواصل بالاجتماعي والتي تتعدد اسبابها بين ذاتية شخصية وأخرى بدافع الغيرة والانتقام أو بدافع مادي لتحقيق الربح السريع الذي يستغرق وقت طويل في جمعه عن طريق مهنة شريفة فأصبح الهاكرز مثال حي أموال طائلة في ضرف ثواني

س6: ماهي الأشياء التي تساعدهم على اختراق جهازك ؟

من خلال ايجابات المبحوثين 05 و 06 و 07 ان الاشياء التي تساعد الهاكرز على اختراق جهاز الحاسوب على أنه متصل بشبكة الانترنت وعن طريق استخدامهم برامج net bus ,net buster , web cracker التي ظهرت لهم هذه التطبيقات جزء من الجهاز الحاسوب

التحليل :

هناك عدة أشياء تساعد الهاكرز على اختراق جهاز الحاسوب خصوصا بالستخدام البرامج الاربعة السابق ذكرها بالإضافة الى المعرف التي يملكها الهاكرز في اغلب الاحيان تكون له صلة وثيقة مع الضحية .

س7: ماهي أهم الاحتياطات التي يجب اتخاذها للحماية من الهاكرز ؟

أكد المبحوثين 01 و 02 04 07 أن اهم الاحتياطات التي يجب اتخاذها هي وضع برنامج anti –virus وتجنب دخول الى مواقع مشبوهة وفتح الرسائل المجهولة

التحليل :

تتعدّد احتياطات حماية من الهاكرز بالستخدام عدة طرق سواء ارتبطت بجهاز الكمبيوتر أو بالفرد أهمها تفعيل البرنامج جدار ناري وكذلك وضع الحارس الانتقائي وعدم الاحتفاظ بأية معلومات شخصية في حسابك الخاص وصور فتوغرافية وكانت احياطات بسيطة الى أنه ينبغي جعلها قاعدة أساسية تتصل اتصال مباشر بحماية خصوصية المستخدمين في مواقع التواصل الاجتماعي .

المحور الثاني :واقع محاربة الجريمة الإلكترونية.

- **مقابلة مع اخصائي في محاربة الجريمة الالكترونية :**

س1 من هم هؤلاء القراصنة ؟

ما يروج عنه فغالبية من يحترفون القرصنة هم مجموعة مبتدئين او لصوص جريمة المعلوماتية هوايتهم المساس بالافراد و المؤسسات سواء ماديا او معنويا

التحليل :

ان الحديث عن القراصنة ليس قضية او مصطلح جديد وانما هم أشخاص خارجون عن القانون اصبحت الانترنت متنفس لهم في تحقيق عملية القرصنة بسرعة فائقة والتي يطلق عليها بجرائم ناعمة تتطلب استخدام أدوات العنف الغير

الملموس ويرجع ذلك الى افتقار الاثار التقليدية وغياب الدليل الفزيقي وأصبح كل من يبحث عن الربح السريع يمتهن مهنت القرصنة وهي مهنة غير معترفة بها قانونيا

س2 :ماهي القوانين التي شرعت للردع من هذه الظاهرة ؟

وأجاب المبحوث على هذا السؤال :

التحليل :

تسعى الجزائر كغيرها من الدول الى سن العديد من القوانين في اطار محاربة الجرائم المعلوماتية واذا اردنا الحديث فان القانون 2016 في المادة 19 من الفصل السادس الى بناء ارضية قانوينة من خلال منظومة تسعى الى مكافحة هذه الجريمة في اطار بناء عمل تنسيقي لمحاربة جرائم تكنولوجيا الاعلام من خلال تنشيط وتنسيق عمليات الاحتياط ضد الجرائم المعلوماتية اضافة الى مساعدة الهيئات القضائية .وكذلك تسخير الوسيلة التكنولوجية للترويج للارهاب و الدعاية

كما سنت الجزائر قانون للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، و ذلك في خطوة نحو ردع جرائم المعلوماتية، خاصة ما يتعلق منها بتسخير الوسيلة التكنولوجية للترويح للإرهاب والدعاية، وبذلك تكون الحكومة قد أخذت أول خطوة نحو سد الفراغ القانوني الذي كان موجودا في مكافحة الجريمة المعلوماتية.

ويعد هذا القانون الذي يأتي في سياق مكافحة الإرهاب الالكتروني بمثابة إطار قانوني مهم يحدد في بابه الأول تعريف وتحديد الجرائم المعلوماتية، ثم ينتقل إلى إمكانية الحد منها ومواجهتها بعد أن أصبحت تلك الجرائم من بين الجرائم التي تهدد أمن وسلامة المجتمعات حيث جاء في 19 مادة و06 فصول تؤكد في مجملها على احترام مبدأ محافظة على السرية الاتصالات إلا في استثناءات حددها المشروع.

س3 ماهي نظرة الدولة للقرصنة الالكترونية ؟

ان الدولة ترى القرصنة الالكترونية .

على أنها جريمة من الجرائم المنصوص عليها في المادة 394 من قانون العقوبات الذي يعتبرها مساسا بأنظمة المعالجة الآلية للمعطيات "كل دخول إلى نظام معلوماتي وتغيير معطياته أو سرقتها أو تخريبها"، حيث تعالج هذه الجرائم المرتبطة بالتطور التكنولوجي كيفية الجرائم على مستوى الشرطة القضائية التي تقوم بمعاينة هذا النوع من الجرائم والبحث عن المجرمين وتقديمهم أمام العدالة.

التحليل :

تبقى نظرة الدولة الجزائرية دائما نظرة سلبية كونها تؤمن بالقانون وهدفها حماية المواطن الجزائري من هذه الظاهرة حتى لا تتجاوز الخطوط الحمراء التي قد تؤدي الى تفاقم المشكل مما يستعصي حله مستقبلا وذلك بالاتخاذ عدة احتياطات تحمي المواطن الجزائري في اطار المنظومة القانونية لتحقيق الامن والاستقرار للمجتمع الجزائري الذي تبقى شعاره متطابقا مع نظام والمبدأ الاساسي للدولة الجزائرية .

س4 ماهي التدابير التي تقومونا بها عند وصول شكاوي متعلقة بالقرصنة؟

ولا يزال الإحجام عن تبليغ مصالح الشرطة عن الجرائم الالكترونية المرتكبة، عائقا يحول دون التعرف على المجرمين والضحايا الذين يتعرضون للقرصنة فضلا عما ينجز عن الجرائم الكلاسيكية المرتكبة عن طريق الوسائل التكنولوجيا الحديثة للإعلام والاتصال من مشاكل كالترهيب عن طريق رسائل التهديد والرسائل المخلة بالحياء واستعمال التكنولوجيات الحديثة للترويج للإرهاب.

وفي هذا الإطار أشار اخصائي في اللقاء الذي خص به "المساء" إلى أن مصالح الشرطة القضائية تقوم بحملات تحسيس للمواطنين وتوعيتهم من أجل رفع شكاوي عند تعرضهم للقرصنة أو التهديد وتمكين الشرطة من التحقيق في الميدان، مؤكدا على ضرورة وضع تدابير تنظيمية تخص تسيير مقاهي الانترنت وتجميد المواقع الإباحية المفتوحة التي تستعمل في غياب الرقابة الصارمة على هذه الأخيرة.

التحليل :

ان التدابير التي تسعى الدولة الجزائرية في اطار مكافحة هذه الظاهرة الى عدة استراتيجيات وخطط تفي غرضها لحماية الجهاز الحاسوب من القرصنة الالكترونية سواء على المستوى الداخلي أو على المستوى الخراجي بتوفير ما يطلق عليه بأمن المعلومات والتي تبقى من خصوصية الشعب الجزائري وذلك لوضع حد نهائي وتقليل من المخاطر التي يستهدف مرتكبوها الى زعزعة أمن البلاد واختراق الخصوصية اذ أن انشاء مركز وطني لمراقبة تدفق المعلومات يبقى مثال وخطوة تقوم بها الدولة الجزائرية كحل بدائي لهذه الظاهرة .

المحور الثالث : الاحتياطات الضرورية للحماية من القرصنة الالكترونية ؟

ان الحديث عن الاحتياطات الضروية يستدعي الى اللجوء الى خبير في تكنولوجيا الاعلام والاتصال باعتبارهم خبراء ومتخصصين في هذا المجال والتي تبقى عبارة عن خطوات ترتبط بالحاسوب والتي ارشدنا اليه .

س1 كيف تعرف ان جهازك مخترق ؟

ج1 دلنا على طريقتين ناجحتين لمعرفة اذا كان جهاز مخترق ام لا

- الطريقة الأولى

نفتح قائمة أبدأ

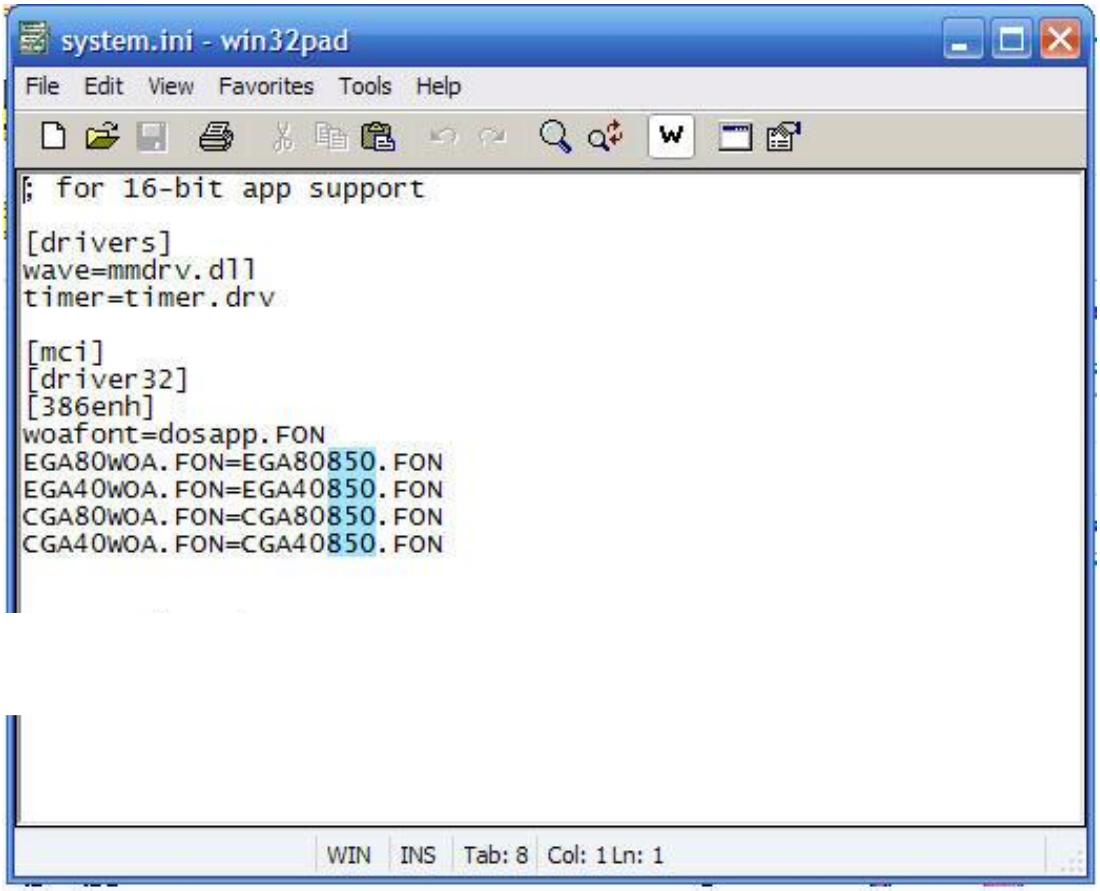
ثم نختارRun

ثم نكتب الامر التالى

system.ini

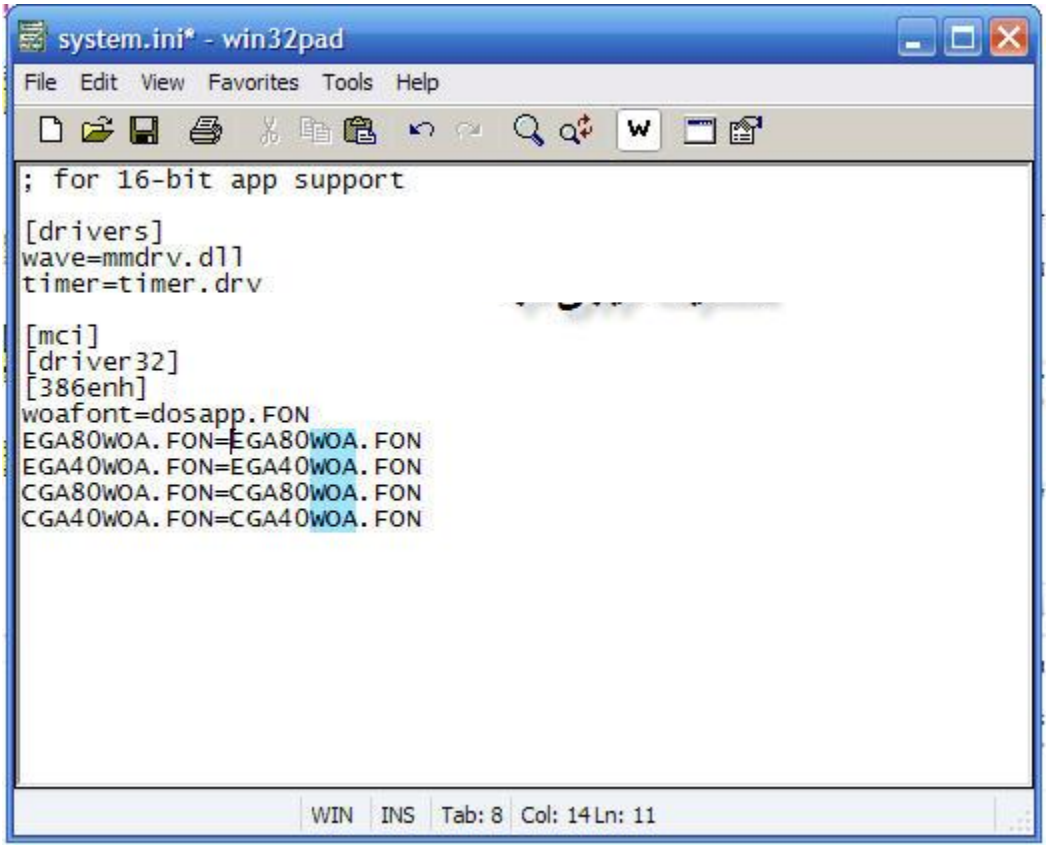
ثم نضغطok

بها بعض الاوامر كما بالصورةnote pad بعد ذلك سوف تظهر لنا مفكرة



اذا ظهر لك رقم 850 كما هو محدد بالصورة فان جهازك سليم 100 % وغير معرض للاختراق

أما اذا ظهر لك الرمزWOA



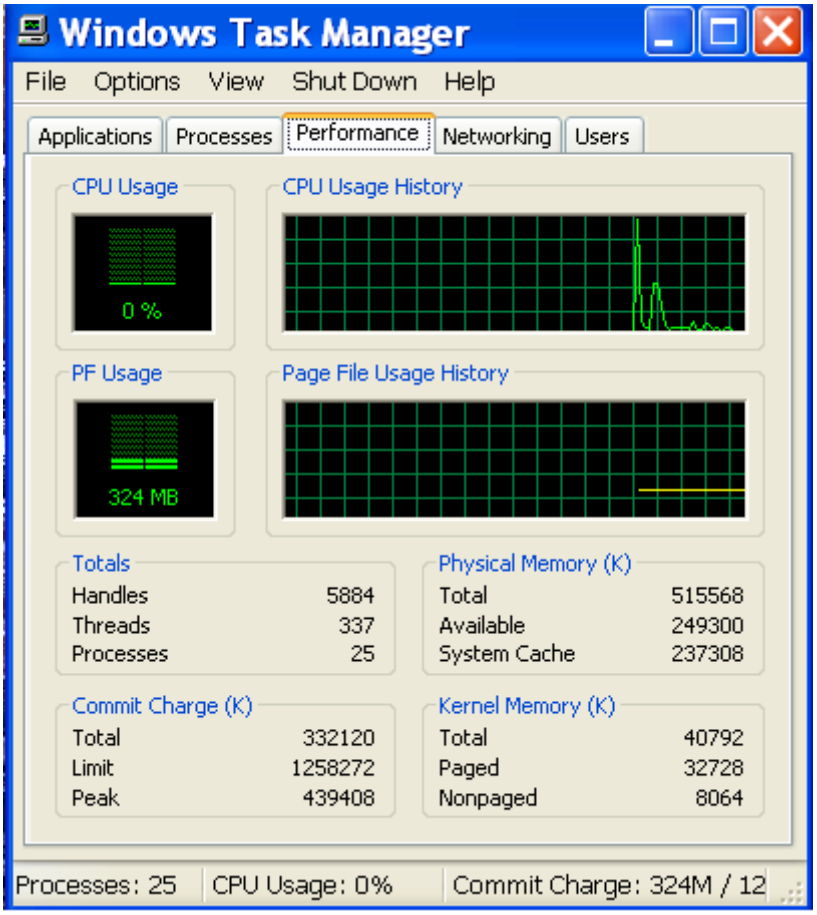
فهذا يعنى ان جهازك مخترق وبه ملفات تجسس وسهل جدا ان يتم إختراقة فى أى وقت

ويفضل أن تقوم بمحو الملفات الخاصة بأسرع وقت حتى لا يتم نقلها أو نقوم بعمل باسورد

- الطريقة الثانية

(Alt + ctrl + Delete) .. عند الضغط على الأزرار

سوف تفتح معك نافذة إدارة المهام



اذا وجدت الرسم البياني المشابة لمخطط القلب بالاعلى..

مرتفع ويمشي بخط مستقيم .. أعرف ان جهازك مهكر , ولتقم بعمل الفورمات فوراااا

س2 ما هي أهم السبل للحماية منها ؟

- ✓ شراء برامج أصلية، والمغلقة بغلاف الشركات المنتجة أو من الوكيل المعتمد أو من مورد ذات سمعة طيبة.
- ✓ لا يتم النسخ لأي برنامج على جهاز الحاسب الآلي إلا إذا كان القرص المحصل عليه البرنامج جيدا ومغلقا.
- ✓ لا يتم قبول أي قرص كهدية من شركة أو جهة مجهولة أو مورد غير معروف.
- ✓ يجب استخدام برامج مسح الفيروسات VIRUS SCAN، وذلك لتأكد من أن البرامج سليمة، وذلك قبل تحميل البرامج على القرص الصلب.
- ✓ إذا تم استخدام أحد الأقراص على جهاز حاسب إلى آخر، غير الحاسب المستعمل، فلا بد من التأكد من أن القرص لم يصب بفيروس من الحاسوب الآخر.

س3 ماهي احصائيات الجريمة الالكترونية في الجزائر ؟

تم تسجيل 12 قضية لجرائم معلوماتية طرحت على المحاكم، و20 شخص متابع منذ بداية السنة الجارية، ومع وضع88 شخص رهن الحجز مما يستدعي مناقشة كيفية محاربة هذه الجريمة نظرا لأخطارها على الأمن الوطني وسلامة الأشخاص وأوضح أن قضايا الدخول غير المشروع مع إتلاف المعطيات تشكل نسبة 34% والدخول غير المشروع 1.29، إدخال معطيات خلسة 21%، المتاجرة في المعطيات المتحصل عليها من دخول غير مشروع 2%، أما عن مرتكبي هذه الجرائم فيتراوح منهم ما بين 25 و 30 سنة بأعلى نسبة 68% ولهم معرفة بالمعلوماتية، كالطلبة والتنفيس وعلاقته بالضحية غالبا مهنية، في حين تكون الدوافع غالبا مادية بنسبة 65% لكن هناك دوافع أخرى كالانتقام أو الفضول أو التحدي وحسب ذات الإحصائيات يشير ذات المتحدث، فالضحية في الغالب تتمثل في إدارات عمومية ومؤسسات ذات طابع صناعي وتجاري بنسبة60%وشركات خاصة بنسبة 20% وباقي النسبة تمثلها شركات أجنبية وهيئات عمومية.

الاستنتاجات العامة :

4- تعتبر البرامج المجانية المنتشرة على الأنترنت وكذا الملحقات ذات الطابع التنفيذي مع البريد الالكتروني من أهم أسباب التي تعرض للقرصنة .

5- القرصنة الالكترونية تلحق أذي مادي ومعنوي سواء بالأفراد أو المؤسسات فهي ايذاء لسمعة ضحية ومساس به من خلال سرقة ملفاته الشخصية وقد تكون محاولات الكسب السريع وجني أرباح الطائلة دون تعب سبب في اخراق أنظمة المؤسسات والمساس بها ماديا .

6- القرصنة الالكترونية نشاط اجرامي يتمثل في استلاء على ملك الغير عن طريق اللهو أو السرقة دون اللجوء الى العنف أو الترهيب .

7- تتم أغلب عمليات الاختراق عن طريق زرع برامج معينة تحتوي على فيروسات أو ملفات تجسس في جهاز الضحية

8- الحصول على المعلومات الشخصية بغرض الانتقام أو الافتخار وكسب المال بسرعة من الدوافع التي تؤدي بالهاكر لممارسة القرصنة

9- تعتبر الانترنت بوابة اتصال بين الضحية والهاكرز والاتصال بها لمدة طويلة عامل يساهم في سهولة اختراق

10- تحميل برامج الحماية على الجهاز وتجنب المواقع المشبوهة وعدم فتح الرسائل المجهولة احتياطات وجب اتخاذها للحماية من الهاكرز

11- القراصنة هم مجموعة مبتدئين او لصوص جريمة المعلوماتية هوايتهم المساس بالافراد و المؤسسات سواء ماديا او معنويا.

12- شرعت عدة قوانين للحفاظ على أمن وسلامة المجتمعات والوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال

10- القرصنة حسب المشرع هي جريمة من الجرائم المنصوص عليها في المادة 394 من قانون العقوبات التي يعتبرها مساسا بأنظمة المعالجة الالية للمعطيات .

الخاتمة

خاتمة:

يوما بعد يوم تزداد مخاطر القرصنة الالكترونية وتتوسع دائرتها، حتى أصبحت الجزائر تحتل المراتب الأولى عالميا، وأصبحت القرصنة ترتكب كأنها روتين يومي يقوم به بعض الأشخاص، من نسخ غير مشروع، أو تطفل عبر الأنترنت، أو إرسال فيروسات

أو في فك للشفرات...إلى غير ذلك، مما يكلف خسائر مادية ومعنوية لضحاياهم.

ولكن ما يمكن ملاحظته مؤخرا أن الجزائر تفطنت مؤخرا إلى الضرورة الملحة للحد والوقوف في وجه الهاكرز، ووضع قوانين صارمة لردعهم ولو أن هذه القوانين التي هي في طور الإنجازجاءت متأخرة، ولعل من أهم أسباب تأخره، هو عدم وجود ثقافة التبليغ لدى أفراد المجتمع الجزائري الذي لم يتعود بعد على الإعتراف بوجودها أصلا.

وفي الأخير،يمكن أن نقول أن الخطوة التي قامت بها المنظومة القانونية الجزائرية في وضع قانون مكافحة الجرائم المعلوماتية ما هي إلا بداية لمواجهة جرائم تعد جديدة في قاموسها القانوني وخاصة وأن الجزائر في هذه المرحلة سنت عدة قوانين لردع القرصنة الالكترونية والحد من اتساع نطاقها .

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

I. المصادر :

1-القرآن الكريم: **سورة الاسراء الآية 24.**

II. قائمة المراجع باللغة العربية:

1-: المعاجم:

2- المعجم الوسيط، ج1، ط2، مجمع اللغة العربية، 1985

2: الكتب:

3- أنجرس موريس ، ترجمة: بوزيد صحراوي وأخرون، منهجية البحث العلمي في العلوم الإنسانية "تدريبات علمية د.ط ، "دار القصبة ، الجزائر، 2004

4- أيمن سيد درويش، المرجع الكامل لخدمات الأنترنت، ط1 ،سوريا، شعاع النشر والعلوم، 1998.

5- بن مرسلي أحمد ، مناهج البحث في علوم الإعلام و الاتصال، ط(3)، ديوان المطبوعات الجامعية، الجزائر

6- الجيلالي حسان بلقاسم سلاطنية ، أسس البحث العلمي، الكتاب الأول، د.ط ، ديوان المطبوعات الجامعية، الجزائر، 2007

7- حجازي عبد الفتاح بيومي ، التجارة الإلكترونية وحمايتها القانونية، د.ط، دار الفكر الجامعي، الاسكندرية 2006

8- حسن إسماعيل محمود ، مناهج البحث الإعلامي ، ط(1)، دار الفكر العربي، القاهرة، 2011

9- خشبة محمد سعيد ، مقدمة في التجهيز الإلكتروني، د.ط ،القاهرة، جامعة الأزهر

10- سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنيت، د.ط ، دار الفكر الجامعي، الإسكندرية، 2007

11- سميث كاتن و نورتن يون ، التجارة على الأنترنت،(ترجمة مركز التعريب و البرمجة) ط1، بيروت، الدار العربية للعلوم ، 1997

12- السيد أحمد مصطفى عمر ، البحث العلمي وإجراءاته ومناهجه، د.ط، مكتبة الفلاح، القاهرة، 2002

13 - شوا محمد سامي ، ثورة المعلومات وانعكاساتها على قانون العقوبات د.ط ، دار النهضة العربية، ،1994

14- عايد رجا الخلايلة، المسؤولة التقصيرية الالكترونية، المسؤولة الناشئة من إساءة استخدام الفرد الحاسوب والانترنت، ط1 ، دار الثقافة للنشر والتوزيع، ، الإصدار الأول، 2005

15- العريان محمد ، الجرائم المعلوماتية، كلية الحقوق، د.ط جامعة الاسكندرية ، 2004،

16- عظيمي أحمد ، منهجية كتابة المذكرات والأطروحات الدكتورة في علوم الإعلام والاتصال، د.ط، ديوان المطبوعات الجامعية، الجزائر، ،2009

17- عليان ربحي مصطفى ، عثمان غنيم، مناهج وأساليب البحث العلمي النظرية والتطبيق، د.ط ، دار الصفاء للنشر والتوزيع، عمان، 2009

18- ويمر روجرز و دومينيك جوزيف ، ترجمة: صالح أبو إصبع، فاروق منصور، مدخل إلى مناهج البحث الإعلامي ط(1)، مركز الدراسات الوحدة العربية، بيروت، 2013

3: الدوريات والمجالات:

19- هناء طالبي، وزارة العدل تعلن عن قرب الانتهاء من الهيئة الوطنية لمحاربة الجريمة المعلوماتية، (2010/05/06، العدد 1031

4: المذكرات والأطروحات "الماجستير"

20- بنت علي محمد القيسي نوال ، الجرائم الالكترونية دراسة عينة من ضحايا القرصنة مذكرة ماجيستر في العلوم الاجتماعية جامعة الامام محمد بن سعود الاسلامية ، السعودية 2011/2010

21- صغير يوسف الجريمة المرتكبة عبر الانترنت ، دراسة عينة من ضحايا القرصنة مذكرة ماجيستر في علوم الاعلام والاتصال ، تخصص الاعلام وتكنولوجيا الاتصال الحديثة ، جامعة مولود معمري ، تيزي وزو 2012/2011

22- عمر يوسفي، التكنولوجيا الرقمية وحقوق المؤلف والحقوق المجاورة، دراسة وصفية تحليلة، شهادة ماجستير، 2008

5: مواقع الأنترنت:

-23 ,www.echoroukonline.com

- 24http://3w.bladi.dz.com/articles/1883/1/la-securiteinformatique-en Algérie/page1html.le

-25http://www.dzmag.info/plus-dinfo/technologie/mafia-crew-purate-des-sites -Algeriens-impartents96.le

- 26www.el-massa.com/ar/centent/view

www.bladi-dz.com/articles- 27

ملاحق

لرصد جرائم المساس بأسرار الدولة وأسرار الحياة الشخصية والترويج للإباحية والإرهاب

كوماندو من 40 ضابطا لمطاردة هاكرز الأنترنت وجواسيس المعلوماتية

أطفال ضمن 20 قرصانا جزائريا موقوفا خلال 2009

سامر رياض

كشف مسؤولون بمديرية الشرطة القضائية للأمن الوطني في شاطوناف في لقاء مع "الشروق" عن شروع أول دفعة من 40 ضابطا في الشرطة القضائية تلقوا تكوينا خاصا وتربصات ميدانية متخصصة في مكافحة الجريمة المعلوماتية بداية من الأسبوع المقبل بعد انتهاء آخر دورة لهم، وسيوزعون على مستوى أمن الولايات بشكل تدرجي سيتم تغطية الـ48 ولاية من خلال دفعات أخرى قبل نهاية السنة الجارية.

أفاد محافظ الشرطة مصطفاوي بمديرية الشرطة القضائية في شاطوناف أن الدفعة الأولى المكونة من 40 ضابطا سينهون آخر تربص لهم ويباشرون مهامهم على مستوى مقرات أمن عدد من الولايات كمرحلة أولى إلى حين ضمان تغطية وطنية قبل نهاية السنة، وتتمثل مهام هؤلاء الضباط في قنص الجرائم المعلوماتية مهما كانت درجتها تطبيقا لقانون العقوبات الذي حدد نصوصا وعقوبات لمرتكبي جرائم ما يسمى باللغة القانونية "المساس بأنظمة المعالجة الآلية للمعطيات"

ومن بين المخالفات التي يعاقب عليها القانون وسيتولى هؤلاء الضباط رصد مرتكبيها والتحقيق حولهم وجمع أدلة الإدانة الدخول إلى نظام معلوماتي دون وجه حق، وعلى سبيل المثال اختراق البريد الإلكتروني الشخصي ومواقع الأنظمة المعلوماتية أو بنوك المعلومات للمؤسسات والهيئات العمومية والخاصة.

وإن كانت المخالفات المعروفة في الوقت الحالي تنحصر في خرق سرية أنظمة معلوماتية أو استباحة سرية معلومات شخصية أو مهنية من خلال الدخول إلى المواقع، غير أنها في المستقبل ستعرف منعرجا يضطر إلى فرض رقابة دقيقة لأية مخالفة مماثلة، ويتعلق الأمر بالتجارة الإلكترونية، حيث ستصبح المبادلات التجارية والمالية عن طريق الأنترنت، الأمر الذي يجعل من أموال ضخمة عرضة لقراصنة الأنترنت، ويجعل السطو عليها أمرا ممكنا في حال غياب آليات قمعية على النحو الذي تقرر البدء في العمل به.

وليست وحدها جرائم تخريب المعطيات أو تغيير الأنظمة واختراقها والتجسس على المعلومات وحدها المتعارف عليها، بل هناك جرائم تتعلق بالإشادة بالإرهاب من خلال المواقع الجماعات الإرهابية ومنتديات أنصارها، وعلى نفس النحو فيما يتعلق بالمواقع الإباحية والمروجين لها، فكلها أصبحت موضة الإجرام المعلوماتي التي ستكون في مقدمة اهتمامات الدفعات التي ستتخرج على مدار السنة، وهي الدفعات التي ستدشن بأول مجمعة تلقت تكوينا عاليا وتدربت على تقنيات التحقيق المعلوماتي بشكل يسهل من مهام الإطاحة بمحترفي جرائم الأنترنت.

وعن آلية كشف الجناة، حرص محافظ الشرطة مصطفاوي على التأكيد أنه استحدثت تجهيزات وتقنيات لتقفي آثار من أصبحوا يعرفون بـ"الهاكرز" والذين لا تخرج أهدافهم عن نزوة التحدي، باستثناء قلة منهم ممن يخترقون بدافع الفضول وإظهار الذات مثلما تكشفه رسائلهم الالكترونية فيما بينهم أو حسبما يتداولونه في منتدياتهم.

ومنذ الشروع في تطبيق قانون العقوبات الذي يجرم مخالفات الأنظمة المعلوماتية فقد تمت معالجة 20 قضية العام الماضي، تورط فيها شباب تتراوح أعمارهم بين 14 و25 سنة وليسوا من ذوي الاختصاص في الإعلام الآلي أو خريجي الجامعات، بل معظمهم موهوبون ويقضون أكبر وقت ممكن على النت للتمكن من حيل القرصنة والاختراق والتجسس المعلوماتي.

وتبقى الإجراءات الوقائية حسب محافظ الشرطة السيد مصطفاوي على مستوى المدارس والثانويات والأولياء الذين يوفرون الأنترنت لأولادهم من خلال توعيتهم بتفادي الانسياق وراء فضول الاختراق وتحدي التجسس المعلوماتي، مما قد يعرضهم لعقوبات قاسية في حالة تلبسهم بتهم الجريمة المعلوماتية.

نخبة أمنية لتتبع الجريمة الالكترونية

*الشروق اليومي، العدد 2831، بتاريخ الإثنين 25 جانفي2010.

الخميس 06 ماي 2010 / الموافق لـ 21 جمادى الأولى 1431 هـ / العدد 2925

99 بالمائة من مرتكبي الجرائم المعلوماتية تقنيون أو طلبة

3 آلاف هجمة شهريا للهاكرز على المواقع الإلكترونية في الجزائر

• تجربة "إختطاف" موقع الشروق وهيئات رسمية بينها الرئاسة والجمارك أعادت الحسابات

كشفت إحصائيات قدمها مركز البحوث القانونية والقضائية التابع لوزارة العدل أن عدد الهجمات اليومية على مختلف المواقع الإلكترونية في الجزائر وصل إلى 3000 هجمة في الشهر، مما يعني أن ظاهرة الجريمة المعلوماتية بدأت تعرف انتشارا بعد بداية استعمال تكنولوجيات الإعلام والاتصال الحديثة في جميع المجالات، وحسب إحصائيات المركز فإن عدد الجرائم المعلوماتية تطور من 12 قضية سنة 2005 تتضمن 20 متهما إلى 12 قضية تتضمن 51 متهما سنة 2006، وإلى غاية أفريل 2010 بلغ عدد الأشخاص المتابعين في الجرائم المعلوماتية 88 شخصا.

جميلة بلقاسم

■ الجرائم الالكترونية من الهواية الى المهنة

وأكدت نفس المصادر أن الجرائم المعلوماتية المنتشرة في الجزائر تتمثل في هجمات على مواقع إلكترونية جزائرية منها مواقع رسمية وخاصة، وقال مدير المركز أن عقوبة المتورطين في تدمير وتخريب المواقع الإلكترونية تصل إلى 3 سنوات سجنا في القانون الجزائري، غير أنها قد تكون أكثر إذا تعلق الأمر بمواقع رسمية تابعة للدولة أو مواقع تهدد الأمن الوطني للبلاد، كما سجل المركز حالات تتمثل في الدعاية الخادعة والإرهابية، وسرقة المعلومات عبر الانترنيت، من خلال التوغل في قاعدة المعطيات، والمساس بالحياة الخاصة، وسجل كذلك تدمير وتحويل مواقع هيئات وجرائد وطنية بينها موقع جريدة "الشروق"، وسجل أيضا استعمال الموقع الإلكتروني لبيع قطع أثرية بولاية عنابة، وعرض صور خليعة على الأنترنيت، واختراق منظومة البنك الجزائري والجمارك الوطنية من طرف شاب يتحكم في الإعلام الآلي من ولاية أم البواقي، كما تنتشر جرائم أخرى تتمثل في تفكيك شفرات القنوات التلفزيونية المشفرة بطريقة غير نظامية.

وتتمثل القضايا المسجلة في 13 قضية خاصة بالدخول غير المشروع مع إتلاف المعطيات أو تعديلها، و11 قضية تتعلق بالدخول غير المشروع، و8 قضايا إدخال معلومات خلسة، و3 قضايا حيازة معطيات متحصل عليها من دخول غير مشروع، وقضيتين تتعلقان بالمتاجرة في معلومات متحصل عليها من دخول غير مشروع ويمكن أن ترتكب بها جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وقضية واحدة خاصة بنشر صور للاستغلال الجنسي للأطفال، و99 بالمائة من مرتكبي هذه الجرائم هم تقنيون أو طلبة.

وقال المدير العام لمركز البحوث القانونية والقضائية جمال بوزرتيني في تصريحات للصحافة على هامش الملتقى الدولي حول محاربة الجريمة المعلوماتية أنه من حسن حظ الجزائر أنها ماتزال لا تعمل ببطاقات الدخول إلى الحسابات البنكية وماتزال لا تتوفر على الانترنت ذي التدفق العالي، غير أنه بعد 2013، حيث ستكون الانترنت ذات السرعة الفائقة متوفرة سيكون الأمر أخطر بكثير مما هو عليه ولا بد من اتخاذ الإحتياطات الضرورية.

وكشفت تقارير التي عرضها المركز في الملتقى أن الجزائر ليست في منأى عن الجريمة المعلوماتية، حيث يعتبر هذا الشكل الجديد من الإجرام العابر للحدود تهديدا حقيقيا للمؤسسات والشركات مما يستدعي ضرورة إنشاء جهاز للمحاربة والوقاية.

وحسب المدير العام للمركز فإن الجزائر قامت بتكييف الجهاز الأمني والقضائي بطريقة تمكنها من التحكم في محاكمة هذا النوع من الجرائم، حيث تم على مستوى أمن كل الدوائر عبر الوطن إنشاء فرقة متخصصة من الشرطة القضائية مهمتها التحقيق في الجرائم الإلكترونية، كما ينتظر أن يتم قريبا إصدار النص التنظيمي لقانون مكافحة الجريمة المعلوماتية الذي صادق عليه البرلمان بغرفتيه مؤخرا، في حين تم على مستوى جهاز العدالة تكوين قضاة متخصصين في الجرائم المعلوماتية في الولايات المتحدة الأمريكية، ومن المنتظر أن يتم قريبا تنصيب هيئة مختصة في مكافحة الجريمة الإلكترونية.

وكشفت إحصائيات مدير المركز أنه يوجد في الجزائر 4,5 مليون متصفح للأنترنت منهم 40 بالمائة يقضون 3 ساعات يوميا أمام الانترنت، وأن 74 بالمائة من مستعملي الانترنت هم رجال، و25 بالمائة نساء، وتعتبر الفئة العمرية التي يتراوح سنها بين 20 و29 سنة الأكثر تصفحا للأنترنت في الجزائر.

* جريدة الشروق اليومي، العدد 2925، بتاريخ 06 ماي2010.

بينها قضية استهداف موقع "الشروق أونلاين" وتخريبه من قبل مصريين

تحقيق في 800 اعتداء إلكتروني شنه "هاكرز"

فتحت الجهات القضائية المختصة تحقيقات معمقة في 800 قضية متعلقة بالجريمة الإلكترونية منذ دخول قانون مكافحة الجريمة الإلكترونية حيز التنفيذ السنة المنقضية، حيث تورط في هذه القضايا جزائريون وأجانب استهدفوا شبكات وبنوك المعلومات المركزية لمؤسسات جزائرية ومتعددة الجنسيات.

كشف، أمس، عبد العزيز دردوري رئيس مدير عام مؤسسة الأمن المعلوماتي وأمن شبكات الاتصال على هامش إلقائه محاضرة حول "الأمن المعلوماتي والجريمة الإلكترونية" بمركز الدراسات الإستراتيجية لجريدة "الشعب" بالجزائر العاصمة، عن فتح الجهات القضائية المختصة بالتنسيق مع خبراء المعلوماتية المعتمدين من قبل وزارة العدل تحقيقات معمقة في 800 قضية متعلقة بالهجمات الإلكترونية التي استهدفت شبكات وبنوك معلومات مؤسسات حساسة وكذا تخريب مواقع إلكترونية عن طريق القرصنة الرقمية.

وأوضح صاحب مؤسسة الأمن المعلوماتي وأمن شبكات الاتصال الجزائرية أن العدد الحقيقي للهجمات الإلكترونية التي تتعرض لها المواقع الجزائرية وشبكات وبنوك معلومات المؤسسات الجزائرية غير محدد بدقة لأن الكثير من ضحايا هذه الهجمات لا يصرحون بها أو حتى أنهم لا يتفطنون لعملية القرصنة الإلكترونية واختراق قواعد بياناتهم من قبل الغير، مضيفا أن الحكومة الجزائرية مطالبة بوضع تشريعات وقوانين كافية لحماية مستعملي الأنترنيت وأصحاب المواقع الإلكترونية وبنوك المعلومات وشبكات الاتصال من الاختراق والقرصنة، فضلا عن تكثيف دورات التوعية والتكوين لرفع مستوى الوعي والمعرفة الرقمية.

وذكر المتحدث أن الجريمة الإلكترونية والقرصنة الرقمية كبدت العالم خلال سنة 2008 خسائر مالية تجاوزت 100 مليار دولار، مشيرا إلى أن كل من الولايات المتحدة الأمريكية وروسيا والصين تعتبر الدول الأكثر خطورة في مجال تهديد أمن المعلومات، في حين تمثل كل من نيجريا وغانا وجنوب إفريقيا والكاميرون الدول الأخطر في الجريمة الإلكترونية على مستوى القارة الإفريقية ما يستدعي على الجزائر تعزيز أمنها المعلوماتي من خلال خطة حكومية تؤمن مختلف المؤسسات والهيئات خاصة في ظل تحضير الجزائر لإطلاق مشروع الحكومة والتجارة الإلكترونية.

كما أثارت قضية اختراق موقع "الشروق أونلاين" ومحاولة الاستيلاء عليه وتخريبه من قبل جهات مصرية نقاشا واسعا على هامش الندوة باعتبارها أكبر قضية مست الأمن المعلوماتي لمؤسسة جزائرية، حيث تعرض موقع "الشروق أونلاين" أكبر موقع إلكتروني جزائري من حيث عدد الزيارات والمشاهدة شهر مارس المنقضي إلى هجمة الكترونية مصرية تم فيها الاستيلاء على اسم النطاق ومرر القراصنة المصريون رسائل عبر الموقع قبل أن تسترجعه مؤسسة "الشروق" للإعلام والنشر بعد تكثيف الاتصالات مع المؤسسة الأمريكية المكلفة بإيواء الموقع ورفع شكوى للسلطات الجزائرية قصد التحقيق في حيثيات القضية.

● زين العابدين جبارة

* جريدة الشروق اليومي، العدد: 2945، بتاريخ الأربعاء 26 ماي2010.

"النهار" تنشر القصة الكاملة لأغرب قضية تعالجها العدالة الجزائرية

"هاكر" من باتنة يدوّخ أمريكا ومكتب تحقيقاتها الفيدرالي!

في أول قضية قرصنة إلكترونية تطرح على مستوى العدالة الجزائرية، نظرت نهار أمس محكمة الجنح لباتنة في ملف الهاكر "ع.ي" 21 سنة، الذي وجهت له تهمة البحث والتجميع والنشر والإتجار في معلومات إلكترونية بطريقة غير قانونية، وسط دهشة كل من كان في قاعة المحاكمة من متهمين، عناصر شرطة، محامين، مواطنين وحتى القاضي وممثل الحق العام.

سعيد حريقة

حيث ساد جو من الهدوء الكبير والإنتباه الشديد لتفاصيل المحاكمة من بدايتها إلى نهايتها دون كلل أو ملل كما جرت العادة، خاصة أثناء استجواب المتهم وطبيعة الأسئلة والأجوبة التي ورغم أن معظم من كان داخل القاعة لم يفهم فيها شيئا، إلا أن الإنتباه بقي سيد الموقف إلى النهاية، ذلك لأن أسئلة القاضي وممثل الحق العام كانت تتمحور حول أمور غير مألوفة لدى عامة المواطنين، والمألوفة منها كانوا يقرؤونها في الجرائد أو يسمعون عنها عبر أمواج الإذاعة وشاشات التلفزيون، باعتبار أنها كانت تتمحور حول مكتب التحقيقات الفيدرالي الأمريكي والأتراك والروس والإنجليز، وكبرى الشركات الأمريكية الخاصة بتطوير منظومات حماية المواقع الإلكترونية والقرصنة وبيع وشراء المعلومات عبر العالم الإفتراضي والأنترنت عن طريق المساومة والإبتزاز، وكان المتهم الذي بدت على وجهه ملامح التخلق والطيبة والسلوك السوي والذكاء الخارق، يجيب على جميع أسئلة القاضي بثقة وهدوء كبيرين، مفندا التهمة التي وجهت له، وموضحا أنه كان فقط يقوم ببيع أنظمة معلومات خاصة بحماية المواقع الإلكترونية، ويقوم بخدمات إشهارية لصالح أصحاب المواقع الإلكترونية الراغبة في ذلك، نظير تلقيه أموال مقابل هذه الخدمات، إلا أن القاضي كان يؤكد أن المتهم يقوم بالدخول إلى مواقع شركات أمريكية ويستولي على معلوماتها السرية، قبل أن يساومها من جديد بدفع أموال مقابل استرجاع تلك المعلومات، كما أكد القاضي أن المتهم يقوم ببيع تلك المعلومات لقراصنة من أستراليا، أوروبا الغربية، روسيا وتركيا، وهو ما أكدته الخبرة المنجزة من طرف الشرطة العلمية، والتي تلا تفاصيلها شرطي خبير قال إن المتهم وباستعمال بريده الإلكتروني العامل لاسم مستعار يعني بالعربية "القبعة البيضاء"، قام باقتحام موقع شركة "ساف نات وورك" الأمريكية المختصة في توفير الحماية لمختلف المواقع الإلكترونية، واستولى على معلومات سرية لزبائنها وساوم القائمين على الشركة بدفع مقابل مالي نظير استرجاع تلك المعلومات، وأن المتهم كان يقوم ببيع معلومات سرية خاصة بزبائن مواقع أخرى مقتحمة لقرصانين روسي وتركي وآخر جزائري مقيم في إنجلترا، مقابل مبالغ مالية ترسل إليه عن طريق حوالات بريدية عبر مؤسسة « وسترن

صورة تعبيرية

يونيون » العالمية، وحسب قاضي الجلسة فإن بداية كشف القضية كانت بعد شكوى شركة "سافت نات وورك" لمكتب التحقيقات الفيدرالي الأمريكي "أف بي آي"، تفيد بأن موقعها تعرض إلى قرصنة من قبل « هاكر » مجهول، تبين أنه جزائري بعد استعمال طرق علمية وتقنية متطورة، وهي الشكوى التي طلب من خلالها البوليس الدولي المساعدة من طرف الشرطة الجزائرية، هذه الأخيرة وفي إطار اتفاقيات تعاون دولية وباستعمال طرق تقنية كذلك واستغلالا للبريد الإلكتروني الذي كان يتعامل به القرصان، تم تحديد مكان هذا الأخير الذي حيّر أمريكا ودوّخ مكتب تحقيقاتها، وهو الشاب البانتي البالغ من العمر 21 سنة المدعو "ي.ع" القاطن في حي بوزوران وسط مدينة باتنة، والذي كان يقوم بكل تلك العمليات من غرفة مسكنه، قبل أن يلقى عليه القبض وتحجز في غرفته حوالات بريدية مختلفة وقرص مضغوط يحمل معلومات سرية خاصة بالشركة الأمريكية "ساف نات وورك"، وبحال بعد تحقيقات معمقة على أعلى المستويات على محكمة الجنح، التي أدانته نهار أمس عقب محاكمة فريدة من نوعها دامت ساعتين من الزمن بسنة حبسا نافذا وغرامة مالية مقدرة بخمسة ملايين سنتيم، بعد التماسات وكيل الجمهورية بتسليط عقوبة سنتين حبسا نافذا، وكان ممثل الحق العام الذي كان بدوره مندهشا لقوة تحكم المتهم، الذي لا يتعدى مستواه الدراسي السنة الثالثة ثانوي في الأنظمة المعلوماتية والإعلام الآلي، أشار إلى تواجد عدة مواقع شركات أمريكية إقتحمها الهاكر البانتي، ذكر منها ثلاثة مواقع فقط، وأنه عرض بيع 2000 معلومة بـ8 دولار مقابل المعلومة الواحدة، وذلك خلال أطوار الفخ المنصوب له من قبل الجهات المختصة، الأمر الذي نفاه المتهم تماما

وقال في شأنه إنه أراد فقط تصريف صاحب البريد الإلكتروني الذي عرض عليه فكرة شراء المعلومات المتواجدة بحوزته، وأضاف وكيل الجمهورية أن طبيعة هذه الجريمة التي تعالجها العدالة الجزائرية لأول مرة تعد سابقة من نوعها، وأن القانون الجزائري يجرم أفعالها وأن ما قام به المتهم يدخل في إطار التهمة الموجهة إليه، لذلك التمس إدانته بسنتين حبسا نافذا، هذا وكان دفاع المتهم المتكون من محاميين اثنين، قد ركّزا في مداخلتهما على انعدام أدلة التجريم من ركن مادي ونية في الجريمة، خاصة بعد رفض أحد المحاميين الخبرة التي أتت بها العدالة عن طريق الشرطي الخبير، حين قال إنه من الطبيعي أن تكون الخبرة ضد المتهم في هذه الحالة، مطالبا من رئيس الجلسة تسجيل إشهاد رفض من قبل القاضي، مضيفا أن موكله قد يكون أخطأ بالدخول إلى الشبكة العنكبوتية، لكنه لم يقم البتة بقرصنة مواقع أمريكية أو بيع معلوماتها السرية، كما تساءل الدفاع عن الأضرار التي ألحقت بالشركة التي تعرضت إلى القرصنة، ملتمسا من هيئة المحكمة براءة موكله المنحدر من عائلة جد محترمة، كل أفرادها إطارات في الدولة الجزائرية، مستشهدا في خصوص المتهم أنه غير مسبوق قضائيا ما يدل على أنه مواطن صالح، وأنه مجرد هاوي لإبحار في عالم الأنترنت لا غير، كما أضاف الدفاع أن شكوى المؤسسة الأمريكية لم تقتصر فقط على موكله وإنما تعدت عدة دول عبر العالم، دون الإشارة إلى ما إن كانت هذه الشكاوى وراء القبض على الهاكر التركي صديق الهاكر البانتني المتواجد حاليا رهن الحبس مثلما قال ممثل الحق العام في مرافعته، وبناء على كل ذلك ولانعدام أركان الجريمة - حسب الدفاع - التمس تبرئة ساحة الشاب من التهمة الموجهة إليه، وحسب مجريات المحاكمة فإن المتهم كان يقوم بقرصنة مواقع إلكترونية منذ سنة 2006 وتحصل مقابل ذلك على حوالي 100 مليون سنتيم، ولأن والد المعني يعد من رجال الأعمال المعروفين فقد ساد اعتقاد وسط الحضور - حسب البعض منهم - أن يكون المتهم قد سقط ضحية شبكة هاكر عالمية، استغلت مهارته في التحكم في الإعلام الآلي لتحقيق أغراض مشبوهة، منها جني أموال طائلة مقابل إعادة بيع المعلومات المباعة لهم بمبالغ رمزية لنفس المؤسسات التي تعرضت إلى القرصنة، وهي الفرضية التي رجّحها قاضي الجلسة وكذا ممثل الحق العام.

* جريدة النهار، العدد: 800 ، بتاريخ : الأربعاء 02 جوان2010.

Guerre à la piraterie

Le siège de l'APS a abrité hier, une conférence sur "la cyber sécurité : enjeux réels et stratégies en Algérie" animée par M. Abdelaziz Derdouri, directeur général de la SSRI.

La cyber sécurité est définie comme la protection des réseaux contre la menace des intrusions pirates grâce à des mesures de prévention pour juguler les risques et les préjudices dangereux pour la sécurité nationale.

Qu'arriverait-il, selon M. Derdouri, si les réseaux de distribution d'électricité, de transport, de défense, du commerce ne sont plus opérationnels ou fiables en raison d'attaques malveillantes ou criminelles ?

La cyber sécurité consiste en d'autres termes à protéger les systèmes informatiques des organismes vitaux contre les dégradations ou la destruction qui peuvent provoquer le ralentissement ou l'arrêt d'activité d'un pays.

L'évaluation de la menace s'effectue par exemple par l'intermédiaire des botnets (Robot Network) et Malwares (logiciel malveillant).

Très schématiquement un botnet est un ensemble de bots informatiques reliés entre eux. C'est un réseau de "machines-zombies" et toute machine connectée à internet est susceptible d'en être la cible. Quant au Malware, il peut être défini en tant que logiciel malveillant que l'on développe pour nuire à un système informatique. Il y a 4.000 à 6.000 botnets opérationnels aujourd'hui.

Botnets et Malwares sont devenus des affaires commerciales. Ils ne sont pas à l'abri de pratiques délictueuses. Le botnet, à titre d'exemple, relaie des spasms pour le commerce illégal, il peut affecter d'autres machines par diffusion de virus.

Même s'ils ne sont pas souvent déclarés, le conférencier avance le nombre de 3.000 incidents en 2009.

Il cite quelques pays dangereux d'où émanent les attaques. Les USA, la Chine, la Russie, la France, l'Iran...

S'agissant des risques pour l'année 2010, M. Abdelaziz Derdouri évoque l'augmentation du nombre d'attaques contre les points sensibles, le non-respect des consignes de sécurité, l'insuffisance des ressources. Quant aux menaces internes, il cite les cas d'accès aux sites sociaux, les pertes ou vols des équipements.

Les secteurs les plus attaqués demeurent l'information, les télécommunications, les institutions gouvernementales, les banques.

Il existe une cybernétique de la guerre. L'orateur parle de guerre psychologique. Une arme cybernétique coûte beaucoup moins cher qu'un avion de combat par exemple.

La guerre cybernétique, selon un responsable de l'OTAN, est un problème global, facilement déployable et très difficile à localiser.

A partir du moment où la cybercriminalité englobe toute les infractions susceptibles de se commettre sur un système informatique connecté à un réseau, se pose fatalement le problème de la sécurité des technologies de l'information et de la communication. La croissance exponentielle de tous ces matériels induit la nécessité de protéger les données et les ressources. M. Abdelaziz Derdouri énumère brièvement les dispositifs juridiques de la France et des USA. Il évoque l'Algérie qui a adopté une loi contre la cybercriminalité en 2009, qui vise à prévenir les infractions informatiques.

La cyber sécurité, à travers les enjeux qu'elle met en place et les stratégies qu'elle mobilise demeure indéniablement, un problème de sécurité nationale. L'orateur évoque pour ce qui concerne notre pays, des initiatives qui sont prises dans ce sens, mais il reste à faire pour développer notre propre logiciel.

De même que les choix technologiques rendent nécessaire une politique nationale des nouvelles technologies pour défendre nos entreprises et l'intérêt de notre pays d'une manière générale.

Mohamed Bouraïb

- journal el moudjahid, numéro : 13886, de 05mai2010.

تباع مقابل 5 آلاف دينار ويتم تحيينها عند الحاجة

بطاقة "أمنية" لمتابعة باقة "كنال بلوس" والجزيرة الرياضية

بطاقة "أمنية" لفك شفرات عدد من الباقات التلفزيونية، هي آخر ما جاد به "الهاكرز" الروس، حيث يتم اقتراحها حاليا بالمحلات المتخصصة مقابل سعر يتراوح بين 4500 و5 آلاف دينار، وتتيح البطاقة متابعة برامج كل قنوات باقة "كنال بلوس"، بما فيها قنوات "أم6" و"تي.أف.1"، بالإضافة إلى القنوات العشر لباقة الجزيرة الرياضية.

الجزائر: غدير فاروق

● دخل القراصنة عالم التسويق عبر اختيار اسم "أمنية" لآخر ما جاد به "الهاكرز"، والمتمثل في بطاقة تحقق أماني متابعة عدد الباقات الأكثر طلبا من قبل الجزائريين، في مقدمتها باقة "كنال ساتيليت" بقنواتها المائة وهذا على القمر الصناعي "أسترا". ومن ضمن هذا العدد من القنوات، توجد القنوات الفرنسية المعروفة لدى الجزائريين مثل "أم6" و"تي.اف.1"، فضلا عن باقي القنوات المتخصصة في بث الأفلام، البرامج الرياضية والأفلام الوثائقية الحديثة.

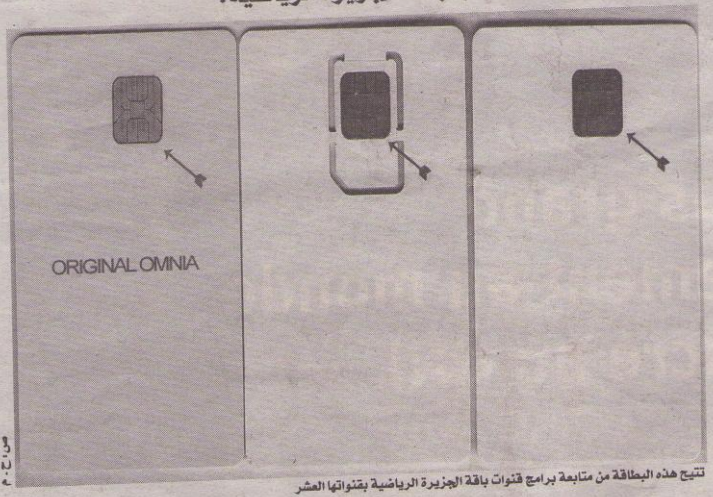
كما تتيح هذه البطاقة المنجزة من قبل زبدة "الهاكرز" الروسيين، من متابعة برامج قنوات باقة الجزيرة الرياضية بقنواتها العشر التي تبث لقاءات أحسن البطولات الأوروبية، وهذا على ثلاثة أقمار صناعية هي "عربسات"، "نايل سات" و"هوتبورد".

وقالت مصادرنا إن بطاقة أمنية، أحسن ما ابتدعه "الهاكرز" في السنوات الأخيرة، حيث تم إنجازها بمواصفات تقنية أذهلت المتخصصين، منذ ظهورها وشرع في تسويقها منذ فترة وجيزة، واقترحت في البداية مقابل 8 آلا دينار، ليتراجع السعر، كما يحدث لكل منتجات القرصنة، ليتراوح الآن بين 4500 و5 آلاف دينار.

وتقوم هذه البطاقة بفك شفرة أصعب نظام تشفير وهو نظام "فياكسس 3,0"، الذي عجزت كل أنظمة التحيين عن فك شفرته، وتستعين به أكثر الباقات طلبا من قبل الجزائريين مثل باقة "كنال بلوس" والجزيرة الرياضية. ومنذ طرحها للتداول، حاول مسؤولو الباقات المعنية كسر الشفرة التي أقامتها في نظام "فياكسس 3,0" غير أن محاولاتهم باءت بالفشل في مرتين متتاليتين، حيث استطاع "الهاكرز" طرح تحيين في كل مرة. وفي حال تحددت محاولات إفشال نظام كسر التشفير من قبل بطاقة أمنية من قبل الباقات المعنية، فيمكن تحيين البطاقة على مستوى المحلات المتخصصة، فيما يوجد جهاز استقبال واحد في السوق حاليا، يمكن تحيينه بدل تحيين البطاقة. للإشارة فإن هذه البطاقة قابلة للاستعمال على كل أجهزة الاستقبال المتوفرة.

وأضافت مصادرنا أن "الهاكرز" الروس يعملون الآن على تطوير برنامج تحيين يمكن، بعد تحيين البطاقة طبعا، من فك شفرات باقات أخرى، من ضمنها القنوات السويسرية التي كانت مفر الجزائريين لمتابعة لقاءات كأس العالم 2006 في ألمانيا.

غ. ف



تتيح هذه البطاقة من متابعة برامج قنوات باقة الجزيرة الرياضية بقنواتها العشر

- جريدة الخبر، العدد5932، بتاريخ: 11 مارس2010.

انتقاما لاختطاف موقع الشروق قبل أسابيع

قراصنة جزائريون يهاجمون 200 موقع مصري ويستهدفون نطاقاتها

نجح مجموعة من الهاكرز الجزائريين في تعطيل ما يقارب 200 موقع إلكتروني مصري على شبكة الأنترنيت دفعة واحدة حيث تبنى مجموعة من الشباب الجزائريين المتمكنين من التكنولوجيات الحديثة وخبايا عالم الإنترنت عملية الرد على القراصنة المصريين الذين هاجموا موقع الشروق أون لاين بمبادرة شخصية منهم ودون إيعاز من أحد.

ع.ب

وترك القراصنة الجزائريون رسائل واضحة للقراصنة المصريين تصدرت الصفحات الإلكترونية المصرية المخترقة مفادها "حملة تدمير 200 موقع إلكتروني مصري..هي حملة تحذير ووعيد من مغبة استهداف أي موقع إلكتروني جزائري .. هي رد على ما قام به بعض الهاركز المصريين عندما خولت لهم أنفسهم التجرأ على اختراق مواقع إلكترونية جزائرية والإستيلاء عليها خاصة موقع الشروق أون لاين".

كما تضمنت الرسالة عبارات تفضح نفاق بعض الهاكرز المصريين الذين اخترقوا مواقع إلكترونية جزائرية باسم الأخوة الجزائرية المصرية وإخماد نار الفتنة بين الشعبين ليقود ذات الهاكرز حملات دعائية لتشويه صورة الجزائر.

وتمكّن الهاكرز الجزائريون من اختراق مجموعة من الخوادم التي تأوي إسم نطاق "أو جي" المصري ما سهّل عملية الاستيلاء على كل المواقع المصرية المنتمية لهذا النطاق وأغلبها مواقع جامعية وإعلامية ما جعلها ضربة قوية للرد على الهاكرز المصريين، خاصة وأن النطاق "أو جي" هو النطاق الأكثر إيواء لأكبر المواقع المصرية، كما سجّل الهاكرز الجزائريون عملية اختراق المواقع المصرية على بوابة الهاكرز www.owned-m.com

وحاول مؤخرا مجموعة من القراصنة المصريين بتواطؤ ودعم من هيئات رسمية بالقاهرة استهداف بعض المواقع الإلكترونية لعدد من المؤسسات والهيئات الجزائرية كرد جبان من الجانب المصري بعد أن خسر جميع المواجهات في الميدان سواء الرياضية أو الإعلامية، ليشنوا حملة دعائية مضادة من خلال المنتديات الإلكترونية والمواقع الافتراضية على الشبكة العنكبوتية لتشويه صورة الجزائر وشتم رموزها وشهدائها مدعّمة بحملة جبانة أخرى تستهدف اختراق المواقع الإلكترونية الجزائرية والاستيلاء على عناوينها بطريقة غير شرعية واحتيالية.

واسترجعت مؤسسة الشروق منذ حوالي شهر موقعها الشروق أون لاين إثر استيلاء هاكرز مصري بعد معركة إلكترونية وإدارية ضارية تمكنت جريدة الشروق ومهندسين وتقنيين جزائريين من استعادة اسم النطاق الخاص بموقع الجريدة بعد عملية السطو والاختطاف التي تعرض لها الموقع على يد قراصنة مصريين بطريقة مخطط لها بدقة، وأثبتت التحريات أن أصحاب العملية تقف وراءهم جهات نافذة.

وكان القراصنة المصريون قد استهدفوا موقع الشروق أون لاين في العديد من المرات بعد أن أضحى يحتل مكانة متقدمة في مصر، حيث وصل ترتيبه أيام الحرب الإعلامية مع الاعلام المصري إلى المرتبة 60، متقدما حتى على أعتى الصحف المصرية وهو ما أغاض الاعلام المصري وجعله يكيد ويهاجم الشروق باستمرار، بل ويحمّلها مسؤولية الفتنة التي بدأها المصريون بالاعتداء على حافلة اللاعبين وأتبعوها بشتم الشهداء ورموز الدولة الجزائرية.

* جريدة الشروق اليومي، العدد 2911، بتاريخ: الأربعاء 21أفريل2010.