مجلة أبحاث إقتصادية معاصرة | ISSN 2572-0171 EISSN: 2716-8891 | المجلد 05،العـدد: 01 (2022)، ص 558- 577

الآثار الاقتصادية للجريمة الالكترونية

Economic impacts of cybercrime

بن جدو بن علية [1]*، درار عياش [2]

DERAR Ayeche BENDJEDOU Benalia

[1] جامعة بومرداس، الجزائر، b.bendjedou@univ-boumerdes.dz

[2] جامعة بومرداس، الجزائر، Ayeche_75@yahoo.fr

تاريخ الاستلام:2022-01-06 **تاريخ القبول:**2022-03-19 **تاريخ النشر:**2022-03-31

ملخص:

يهدف هذا البحث إلى التعرف على أهم المفاهيم المرتبطة بالجريمة الالكترونية أنواعها وخصائصها، وكذا التعرف على حجم الأضرار التي تكلفها الجرائم الالكترونية وآثارها على اقتصاديات الدول، حيث تشير الإحصائيات والتقارير المتخصصة إلى تزايد سنوي للخسائر المالية الناجمة عن اختراق البنوك والمؤسسات المالية والمصرفية.

توصل البحث إلى أن الجريمة الالكترونية تكلف الاقتصاد العالمي 0.8٪ كنسبة مئوية من الناتج المحلي الإجمالي العالمي. في النصف الأول من عام 2019، تم الإبلاغ عن أكثر من 3800 حالة اختراق للبيانات، مما أدى إلى تعرض أكثر من أربعة مليارات قاعدة بيانات لجرائم إلكترونية، كما تم تسجيل أكثر من 165000 موقع فريد للتصيد الاحتيالي في الربع الأول من عام 2020. خلال جائحة COVID-19، زادت هجمات برامج الفدية بشكل عام بنسبة 148٪ عن مستويات خط الأساس التي تم الإبلاغ عنها في فبراير 2020. وتقدر الخسائر السنوية للولايات المتحدة بما يتراوح بين 10 مليارات دولار و12 مليار دولار من الجرائم الإلكترونية التي تستهدف الملكية الفكرية وربما من 50 مليار دولار إلى 60 مليار دولار عالميًا.

الكلمات المفتاحية: الجريمة الالكترونية؛ الإرهاب السيبراني؛ الآثار الاقتصادية.

تصنيف JEL : O33 ؛ L96

Abstract:

The purpose of this research is to identify the most important concepts associated with cybercrime, their types and characteristics, and also to identify the extent of the damage caused by cybercrime and its effects on the economies of States.

Specialized statistics and reports indicate an annual increase in financial losses resulting from bank hacking. In the first half of 2019, more than 3800 data hacks were reported, this has resulted in more than four billion electronic crime databases. more than 165000 unique phishing sites were registered in the first quarter of 2020. During the covid 19 pandemic, ransom attacks are generally 148% higher than the baseline levels reported in February 2020. Annual United States losses are

*: المؤلف المرسل

estimated at between $10 billion and $12 billion in cybercrime, it targets intellectual property, probably from $50 billion to $60 billion globally.
Keywords: cybercrime, cyberterrorisme, economic Impacts.
JELClassification Codes : O33 ; L96

1.مقدمة:

رغم الايجابيات والمميزات التي قدمها التطور الهائل لتكنولوجيا المعلومات والاتصالات للبشرية والذي انعكس على شتى المجالات الحياتية، إلا أنها أفرزت بدورها مجموعة من العيوب أو السلبيات من بينها ما يعرف بالجرائم الالكترونية، حيث أدى الاستخدام الواسع للتكنولوجيا، وخاصة شبكة الانترنت، سواء فيما يتعلق بالتجارة الالكترونية والتسوق الالكتروني، أو في الجانب الاجتماعي بالولوج إلى مواقع التواصل الاجتماعي، أدى إلى تعرض المستخدمين لمجموعة من الانتهاكات التي قد تصل إلى حدود الجريمة. حيث تتعدد أشكال الجريمة الالكترونية وتصنيفاتها.

1.1. الإشكالية:

ومن هنا يمكن طرح الإشكالية الرئيسية التالية: ما هي الآثار الاقتصادية للجريمة الالكترونية؟ أو بصيغة أخرى ما مدى تأثير الخسائر المالية الناجمة عن الجريمة الالكترونية على الناتج المحلي الإجمالي لاقتصاديات الدول؟

2.1. أهداف البحث:

يهدف هذا البحث إلى التعرف على مفهوم وأنواع الجرائم الالكترونية، والتعرف على الآثار الاقتصادية لها.

3.1. منهج البحث:

ولمعالجة الإشكالية سالفة الذكر، تم إتباع المنهج الوصفي بالنسبة لعرض الأدبيات المتعلقة بالجريمة الالكترونية، بالاستعانة بمجموعة من المراجع والدراسات السابقة التي تناولت الموضوع، والمنهج التحليلي بالنسبة للمحور المتعلق بالجانب التطبيقي من خلال عرض وتحليل الإحصائيات المتعلقة بالموضوع.

4.1. متغيرات الدراسة:

تتمثل متغيرات البحث في الجريمة الالكترونية كمتغير مستقل وآثارها على الاقتصاد (نسبة الخسائر المالية من الناتج المحلي الإجمالي) كمتغير تابع.

5.1. المجال الزماني والمكاني للبحث:

واقتصرت فترة البحث على الإحصائيات الخاصة بنتائج ومخلفات الجريمة الالكترونية بين سنة 2012 وسنة 2020، على مستوى دول العالم. مع عرض آثار الجريمة الالكترونية من خلال مقارنة الخسائر المالية المترتبة عنها بالناتج المحلي الإجمالي لسنة 2017.

6.1. خطة البحث:

ولمعالجة الإشكالية تم تقسيم البحث إلى مبحثين رئيسيين: المبحث الأول تم فيه التطرق إلى الجانب النظري من خلال عرض أهم التعريفات للجريمة الالكترونية، تصنيفاتها، وخصائصها، أما المبحث الثاني فتم فيه عرض الجانب التطبيقي من خلال عرض وتحليل أهم الإحصائيات المتعلقة بالخسائر الناجمة عن الجريمة الالكترونية.

2. ماهية الجريمة الالكترونية

سنتناول في هذا المبحث أهم الجوانب النظرية لموضوع البحث، حيث سنتطرق إلى أهم التعريفات المقدمة للجريمة الالكترونية.

1.2. مفهوم الجريمة الالكترونية

يرتبط مصلح الجريمة بالسلوك العدواني لإلحاق الأذى بأطراف أخرى، ونظرا للانتشار الواسع لتكنولوجيا الإعلام والاتصال، فقد أدى استخدامها غير السليم إلى ظهور ما يعرف بالجريمة الالكترونية.

الجرائم الإلكترونية أو الجرائم السيبرانية هي الجرائم التي تُرتكب ضد الأفراد أو الجماعات مع الدافع الإجرامي المتمثل في الإضرار عمداً بسمعة الضحية، أو التسبب في ذلك بدنيًا أو الأذى النفسي ، والتسبب في فقدان المال أو المعلومات بشكل مباشر أو غير مباشر عن طريق استخدام الإنترنت والأجهزة الإلكترونية (Alansari, Aljazzaf, & Sarfraz, 2019, p. 10).

ويستخدم مصطلح الجريمة الإلكترونية لوصف أي نشاط غير قانوني باستخدام الكمبيوتر أو الحوسبة الأجهزة مثل الهواتف الذكية والأجهزة اللوحية والمساعد الرقمي الشخصي، لوحدها أو باستخدام شبكة الانترنت لتنفيذ الجريمة (Pande, 2017, p. 15).

ويستخدم مجرمو الإنترنت العديد من الأدوات غير القانونية باستخدام برامج أو أجهزة للتجسس ورصد وتسجيل كلمات السر أو كلمات المرور، وتمكين أنشطة التجسس من قرصنة وسرقة بيانات شخصية؛ رفض الخدمة الموزع (DDoS)، قرصنة نظام الكمبيوتر وجعله غير متاح للمستخدمين المصرح لهم، التوجيه الاحتيالي (pharming) بتوجيه وتحويل الاتصال من موقع ويب شرعي إلى موقع يتحكم فيه متسلل مجرم (Curtis, 2009, p. 2).

لقد تعددت التعريفات الخاصة بالجريمة الالكترونية إلا أنها تتفق على استخدام وسائل تكنولوجيا الإعلام والاتصال لإلحاق الضرر بالضحية، سواء كان ضرر مادي أو معنوي، وقد يكون الضحية فردا، مؤسسة أو دولة.

2.2. تصنيفات الجريمة الالكترونية

تتعدد الجرائم الالكترونية وتختلف أشكالها وأغراضها، وقد تم تصنيفها إلى: (Alansari, Aljazzaf, & Sarfraz, 2019, pp. 10 - 11)

1.2.2. جرائم الحاسوب: استخدام الوسائل والعمليات الإلكترونية مباشرة لاختراق نظام الأمن للحصول على البيانات والمعلومات بشكل غير قانوني.

2.2.2. جرائم التقنية والتكنولوجيا العالية: مجموعة واسعة من الأنشطة الإجرامية التي تخترق أجهزة الكمبيوتر بشكل غير قانوني في انتهاك لقوانين الدولة أو القوانين الفيدرالية، تتم هذه الجرائم عن طريق القرصنة، وغسيل الأموال، والبرمجيات الخبيثة (الفيروسات)، والسرقة الإلكترونية، وسرقة الهوية.

3.2.2. جرائم ذوي الياقات البيضاء: جريمة يرتكبها شخص ذو مكانة اجتماعية عالية أثناء عمله للحصول على المال.

4.2.2. الجرائم السيبرانية: نشاط إجرامي يتم باستخدام أجهزة الكمبيوتر والإنترنت، وذلك بالقيام بالتنزيل غير القانوني لملفات الموسيقى والألعاب، وسرقة ملايين الدولارات من الحسابات عبر الإنترنت، وأيضا الجرائم غير النقدية، مثل إنشاء فيروسات وتوزيعها على أجهزة كمبيوتر أخرى، أو نشر معلومات تجارية سرية على الإنترنت.

5.2.2. الإرهاب السيبراني: الهجوم المتعمد وذو الدوافع السياسية على المعلومات والبيانات وأنظمة وبرامج الكمبيوتر الكمبيوتر، مما يؤدي إلى العنف ضد أهداف مدنية، تشمل الأهداف المحتملة للإرهاب السيبراني القطاعات المصرفية والمنشآت العسكرية ومحطات الطاقة ومراكز مراقبة الحركة الجوية.

من خلال هذا يتبين أن هناك تصنيفات متعددة للجرائم الالكترونية، والتي تكون باستخدام الأجهزة الالكترونية، والتي قد تصل آثارها إلى المساس بالأمن القومي للدول أو ما يعرف بالإرهاب السيبراني.

3.2. أساليب ارتكاب الجريمة الالكترونية

تنطوي الجريمة الالكترونية على العديد من الأنشطة مثل التشهير، الاحتيال بواسطة بطاقات الائتمان، المطاردة السيبرانية عبر الإنترنت، الحصول على وصول غير مصرح به إلى أنظمة الكمبيوتر، تجاهل حقوق النشر وترخيص العلامة التجارية آمنة للحماية، تجاوز التشفير لعمل نسخ غير قانونية، قرصنة البرامج وسرقة برامج الهوية للقيام بأعمال إجرامية (P.S.Seemma, Nandhini, & Sowmiya, November 2018, p. 125). وتتمثل أنواع الجريمة الالكترونية فيما يلي:

1.3.2. الاختراق: عرف الاختراق بأنه الدخول غير المصرح به أو غير المشروع لنظام المعالجة الآلية للبيانات وذلك عن طريق انتهاك الإجراءات الأمنية، ويعرف الاختراق أيضا أنه عمليات غير شرعية تتم عن طريق فتحات موجودة في النظام يستطيع المخترق من خلالها الدخول إلى جهاز الضحية من أجل إتمام غرض معين يسعى إليه المخترق، فالاختراق بشكل عام هو القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاصة بالهدف، فالمخترق لديه القدرة على دخول أجهزة الآخرين عنوة دون رغبة منهم وحتى دون علم منهم بغض النظر عن الأضرار الجسيمة التي قد يحدثها سواء بأجهزتهم الشخصية أو نفسياتهم (رابحي، 2018/2017، صفحة 112). ومن أهم أساليب الاختراق ما يلي (رابحي، 2018/2017، الصفحات 113-118):

1.1.3.2. الاختراق عن طريق استعمال نظم التشغيل: لأن نظم التشغيل مليئة بالثغرات، فإنه يتم استغلالها في عمليات الاختراق، ولكن الأهم هو القيام بذلك عن طريق البروتوكولات التي يستخدمها النظام للتعامل مع شبكة الإنترنت أو الشبكات الداخلية بأنواعها، بعد تحديد رقم IP يحدد المخترق إمكانية

اختراق جهاز الضحية عن طريق مجموعة من الخطوات ورقم "اللآي بي" رقم ديناميكي متغير، فهو يتغير في كل مرة يدخل الشخص على شبكة الانترنت.

2.1.3.2. الاختراق باستخدام البرامج: لابد لقيام الاختراق بهذه الطريقة من وجود برنامجين، أحدهما بجهاز الضحية ويسمى بالبرنامج الخادم server لأنه بمثابة الخادم الذي يأتمر بأوامر المخترق وينفذ المهام الموكلة إليه داخل جهاز الضحية وثانيهما برنامج يوجد بجهاز المخترق ويسمى ببرنامج المستفيد العميل client، وأشهر مثال على هذه البرامج وأخطرها هو برنامج حصان طروادة ، فهو يتمتع بمجموعة من المميزات تجعل الأقدر على عملية الاختراق دون القدرة على كشفه وتتبعه والقضاء عليه.

3.1.3.2. التقاط كلمات السر وقرصنتها: إذا كانت أنشطة الاعتداء التي تتم باستعمال كلمة السر تتم غالبا فيما سبق عن طريق تخمين كلمات السر مستفيدة من ضعف الكلمات عموما وشيوع اختيار الأفراد لكلمات سهلة تتصل بمحيطهم الأسري أو محيط العمل أو حياتهم الشخصية، فإن الجديد استخدام برمجيات يمكنها تشمم أو التقاط كلمات السر خلال تجوالها في جزء من الشبكة أو أحد عناصرها ومراقبتها ومتابعتها لحركة الاتصال على الشبكة.

4.1.3.2. المسح والنسخ: هو أسلوب يستخدم فيه برنامج الماسح وهو برنامج احتمالات يقوم على فكرة تغيير التركيب أو تبديل احتمالات المعلومة، ويستخدم تحديثا بشأن احتمالات كلمة السر أو رقم هاتف الموزع أو نحو ذلك، وأبسط نمط فيه عندما تستخدم قائمة الاحتمالات لتغيير رقم الهاتف بمسح قائمة أرقام كبيرة للوصول إلى احدها الذي يستخدم موزع للاتصال بالإنترنت.

5.1.3.2. هجومات استغلال المزايا الإضافية: الأمر هنا يتصل بواحد من أهم استراتيجيات الحماية فالأصل أن مستخدم النظام – تحديد داخل المؤسسة يحدد له نطاق الاستخدام ونطاق الصلاحيات بالنسبة للنظام، ولكن في الواقع العملي يحدث أن مزايا الاستخدام يجري زيادتها دون تقدير لمخاطر ذلك أو دون علم من الشخص نفسه أنه يحظى بمزايا تتجاوز اختصاصه ورغباته.

6.1.3.2. استراق الأمواج و الهندسة الاجتماعية: يتم استراق الأمواج ذلك باستخدام لواقط تقنية لتجميع الموجات المنبعثة من النظم باختلاف أنواعه كالتقاط موجات شاشات الكمبيوتر الضوئية أو التقاط الموجات الصوتية من أجهزة الاتصال، أما عن الهندسة الاجتماعية فهي أسلوب من أساليب الاختراق التي تعتمد على العنصر البشري وليس لها أية أبعاد تقنية بحيث يستمل فيها أساليب الخداع والكذب للحصول على معلومات ذات طابع تقني.

7.1.3.2. التفتيش في مخلفات التقنية وانتحال شخصية الأفراد: التفتيش في مخلفات التقنية هو القيام بالبحث في مخلفات المؤسسة من القمامة والمواد المتروكة بحثا عن أي شيء يساعده على اختراق النظام، كالأوراق المدون عليها كلمات السر، أو مخرجات الكمبيوتر التي قد تتضمن معلومات مفيدة، أو الأقراص الصلبة المرمية بعد استبدالها، أو غير ذلك من المواد المكتوبة أو الأقراص أو الملاحظات أو أي أمر يستدل منه على أية معلومة تساهم في الاختراق،

بينما انتحال شخصية الأفراد هو قيام شخص باستخدام شخصية إنسان آخر للاستفادة من سمعته مثلا أو ماله وصلاحياته هذا الانتحال يمكنه القيام بذلك عن طريق المعلومات التي تتعلق بتلك الشخصية، كالاسم والعنوان ورقم الهوية مثلا ويستغلها استغلالا سيئا، والتي يحصل عليها من الإنترنت ويمكن أن تؤدي هذه الجريمة إلى استنزاف رصيد الضحية في البنك أو السحب من البطاقة الائتمانية أو الإساءة إلى سمعة الضحية وقد تكون وسيلة المجرم إلى ارتكاب جريمة النصب، مستفيدا من السمعة الطيبة لتلك الشخصية أو شركة قد استغرقت السنوات الطوال لبناء تلك السمعة.

8.1.3.2. انتحال شخصية المواقع: ويقوم الفاعل بهذه الجريمة من خلال وضع نفسه في موقع بيني بين البرنامج المستعرض Browser للحاسب الخاص بأحد مستخدمي الانترنت وبين الموقع Web ومن هذا الموقع البيني يستطيع حاسب المجرم أن يتصرف وكأنه صاحب الموقع الحقيقي، ويستطيع مراقبة أي معلومة متبادلة بين الضحية الذي يزور الموقع وبين الموقع نفسه كما يستطيع سرقة هذه المعلومات أو تغييره، ولكن القيام بهذه العملية حتى لو تم الاتصال بالموقع من خلال ما يسمى بنظم الاتصال الآمنة.

2.3.2. الفيروسات الالكترونية: فالفيروس هو عبارة عن برنامج يحتوي على مجموعة من الأوامر الخاصة بكيفية انتشاره داخل الملفات، ويتم كتابة هذا البرنامج باستخدام إحدى لغات البرمجة منخفضة المستوى ويحدث أثارا تخريبية وتختلف الآثار التي يخلفها الفيروس بحسب نوعه، وهي تتدرج من أقلها ضررا إلى أكبرها كما يلي (رابحي، 2018/2017، الصفحات 120-122):

- البطء الشديد في الحاسب بما يجعل التعامل معه مستحيلا؛
- عدم القدرة على تشغيل معظم التطبيقات، وظهور رسائل خطأ كلما تمت محاولة تشغيلها؛
- مسح الملفات التنفيذية كالبرامج سواء المثبتة داخل نظام التشغيل أو التي يحتفظ بها داخل الحاسب مما يسبب عدم القدرة على تشغيل هذه التطبيقات؛
- حذف ملفات FAT مما يعني حذف جميع المعطيات الموجودة داخل القرص الصلب، وهو الأمر الأكثر خطورة؛
- إصابة أحد أجزاء المكونات الصلبة، كما يحدث مع فيروس "تشير نوبل" الذي يصيب نظام الإدخال والإخراج الأساسية، مما يؤدي إلى توقف الحاسب بالكامل.

لقد واكب استخدام بطاقات الائتمان من خلال شبكة الإنترنت ظهور الكثير من المتسللين للسطو عليها، فبطاقات الائتمان تعد أموالاً إلكترونية والاستيلاء عليها يعد استيلاء على مال الغير، ومع انتشار التجارة الإلكترونية، عمدت العديد من شركات الأعمال إلى استخدام الإنترنت لإتاحة خدماتها على الشبكة، بهدف تسهيل العملية التجارية وتوسيع نطاقها وتطويرها، والجدير بالذكر أن الاستيلاء على بطاقات الائتمان ليس بالغ الصعوبة، فلصوص بطاقات الائتمان يستطيعون الآن سرقة مئات الآلاف من أرقام البطاقات في يوم واحد من خلال شبكة الإنترنت، ومن ثم بيع هذه المعلومات للآخرين (الإسكوا، 2012، صفحة 12).

ومن صور جرائم الأموال الإلكترونية استخدام بطاقات ائتمان انتهت صلاحيتها، أو بطاقات ملغاة من الجهة التي أصدرتها، أو استخدام بطاقات مسروقة أو مزوّرة، ومن صور جرائم التعدي على الأموال الإلكترونية أيضاً التعدي على أموال الغير بالوسائل الإلكترونية، مثل الدخول إلى مواقع البنوك، والدخول إلى حسابات العملاء، وإدخال بيانات أو مسح بيانات بغرض اختلاس الأموال أو نقلها أو إتلافها، ففي عام 2003 قامت الولايات المتحدة بالتحقيق في سرقة أرقام 8 ملايين بطاقة ائتمان من شركات تجارية في حادثة تعد الأخطر من نوعها، بالرغم من تكرار مثيلاتها في فترات لاحقة، وقد اعترفت الشركات التي تجري عمليات تحويل مالية لشركات فيزا وماستر كارد وأمريكان إكسبريس وديسكفر فاينانشال سيرفيسز بتعرضها لاختراق في نظام العمل من طرف خارجي غير مصرح له بالدخول على النظام (الإسكوا، 2012، صفحة 13).

من خلال هذا يتبين أن هناك أساليب متعددة للجرائم الالكترونية، باستخدام برامج فيروسية، واختراق الأجهزة الحاسوبية للآخرين، والتي تتعدد آثارها والتبعات التي قد تنجر عنها، والتي سنتطرق إليها في المبحث الثاني.

4.2. خصائص الجريمة الالكترونية

تعد الجريمة الالكترونية من الجرائم الحديثة بمجموعة فهي تتميز بمجموعة من السمات تميزها عن غيرها من الجرائم التقليدية، وذلك بالنظر إلى الوسائل التقنية المستخدمة كالحاسب الآلي والدراية الكافية من قبل الجاني بتقنية المعلومات حيث أصبحنا أمام ما يعرف بالمجرم الالكتروني، وتتمثل هذه الخصائص فيما يلي (بن سعيد، عثماني، و نوال، جويلية 2020، الصفحات 23-25):

1.4.2. طريقة التنفيذ وأسلوب الارتكاب: وهذا لكون الجريمة تتميز بالطابع التقني ولصعوبة الإثبات فيها نظرا لسهولة وسرعة فسخ ومحو الدليل في وقت سريع، حيث يتم التنفيذ بسرعة وتكفي ضغطة واحدة من الهاتف أو الحاسب الآلي أن تمر البيانات أو تنقلها أو تقوم بتحويل الحسابات وغيرها، وهذا كله يتم عن بعد أي دون وجود الفاعل في مسرح الجريمة، وبالتالي فهي تختلف عن الجرائم التقليدية التي في غالب الأحيان تتطلب العنف والمجهود البدني لارتكابها مثل الضرب والقتل والتحطيم والكسر...، عكس أسلوب تنفيذ الجريمة الالكترونية فهي تتم بذكاء وسرعة مع قدرة فنية وتقنية في التعامل مع الحاسب والانترنت.

2.4.2. صعوبة الإثبات والاكتشاف: إن الجرائم الواقعة على الانترنت جرائم مخفية، وتتميز عن غيرها من باقي الجرائم بعدم استخدام الجاني للعنف كما في الجرائم العادية، حيث يتم ارتكاب الجريمة الالكترونية بنقل معلومات أو تخريب معطيات من جهاز لآخر سواء كان حاسبا أو هاتفا أو من قبل إحدى الأجهزة الذكية التي تتصل بالانترنت وبالشبكة المعلوماتية، وبالتالي سهولة تدمير الدليل لعدم وجود خبرات في مجال المعلوماتية لأجهزة التحقيق سواء كانت الشرطة أو غيرها.

كما أنها صعبة الاكتشاف لأنها تنفذ بواسطة وسائل دقيقة ومتطورة فهي تتميز بكونها مستترة ومتخفية في غالب الأحيان ولا تترك أي دليل كتابي أو مادي واضح لتنفيذها بوسائط الكترونية تؤثر على الضحية أما في ماله أو شخصه إما بالسرقة أو التعديل أو الإتلاف أو التحطيم والسبب في عدم ترك أثر أو دليل خارجي وقدرته على محوه في أقل من ثانية.

3.4.2. عالمية الجريمة الالكترونية: بمعنى هي جرائم تتعدى الحدود الجغرافية للدول، فبظهور شبكة المعلومات وربط العالم بشبكة الاتصالات، أصبح نقل المعلومات عبر الدول بوسائل غير مرئية وغير ملموسة، وهذا من خلال الحاسب الآلي والانترنت في نقل وتبادل المعلومات وبالتالي تأثير العديد من الدول بالجرائم الالكترونية في وقت واحد، وهو ما يميز الجريمة الالكترونية عن الجرائم التقليدية، فغالبا ما تكون الجريمة الالكترونية في دولة والجاني في دولة أخرى، وهذا بفعل الانترنت التي تقضي على الحدود بين الدول، وهو ما يؤدي إلى المساس بثقافة الدولة المجني عليها، أو التأثير على دينها أو نظامها المعلوماتي والسياسي، وبالتالي يثير إشكال حول مجال الإجراءات والاختصاص في التحقيق والتفتيش في الجرائم العابرة للدول.

4.4.2. المجرم المعلوماتي: إن الإجرام التقليدي عادة ما يكون عن طريق العنف أو الإكراه أو الضرب، أما الإجرام الالكتروني فنجد أن المجرم الالكتروني يمتاز بدرجة من الذكاء لأنه يتعامل مع أجهزة متطورة وتقنية عالية في ميدان المعلوماتية والحاسب، وكذا الهواتف الذكية، وعليه فالمجرم الالكتروني يمتلك درجة من العلم والمعرفة وبالتالي مرتكبوا هذه الجرائم هم إما: مخترقون أو متطفلون وهو ما يطلق عليهم "هاكرز" (مجرمو الكمبيوتر المحترفون)، فئة صغار السن، وحبهم الاطلاع والاستكشاف، الحاذقون وهم من تحركهم الرغبة في الانتقام والثأر ويتميز المجرم المعلوماتي بمجموعة من السمات ويرمز إليها الأستاذ باركر "Parker" بكلمة S.K.R.A.M وهي تعني: المهارة Skill، المعرفة Knowledge، الوسيلة Ressources، السلطة Authority، الباعث Motives.

تختلف الجريمة الالكترونية عن الجريمة التقليدية، وهذا بتميزها بمجموعة من الخصائص التي تتصف بها، ابتداء بالوسائل المستعملة، بالإضافة إلى صعوبة الاكتشاف نظرا لصعوبة تحديد موقع منفذ الجريمة، وانتهاء بصفات المجرم الذي يقوم بالجريمة الالكترونية والذي يتصف بعض السلوكيات المختلفة عن المجرم التقليدي، وكذا الغرض من الجريمة الالكترونية، والذي قد يكون نفسي أكثر منه مادي.

3. عرض وتحليل أهم الإحصائيات الناتجة عن الجريمة الالكترونية

في عام 2014، قدّر مركز الاستراتيجية والدراسات الدولية CSIS أن الجريمة الإلكترونية كلفت العالم ما بين 345 مليار دولار و445 مليار دولار. كنسبة مئوية من الناتج المحلي الإجمالي العالمي، تكلف الجريمة الإلكترونية الاقتصاد العالمي 0.62٪ من الناتج المحلي الإجمالي في 2014. باستخدام نفس الأساليب، يعتقد CSIS الآن أن النطاق الآن بين 445 مليار دولار و600 مليار، وفي 2016 كلفت الجريمة السيبرانية الاقتصاد العالمي 0.8٪ كنسبة مئوية من الناتج المحلي الإجمالي العالمي (Lewis, 2018, p. 6).

جدول 1: الجريمة الالكترونية في العالم لسنة 2017

المنطقة	الناتج المحلي الإجمالي (تريليون دولار)	خسائر الجرائم الالكترونية (مليار دولار)	نسبة خسائر الجرائم الالكترونية (النسبة من الناتج المحلي الإجمالي)
أمريكا الشمالية	20.2	175 – 140	% 0.87 – 0.69
أوروبا ووسط آسيا	20.3	180 – 160	% 0.89 – 0.79
شرق آسيا	22.5	200 – 120	% 089 – 0.53
جنوب آسيا	2.9	15	% 0.52 – 0.24
أمريكا اللاتينية والكراييب	5.3	30 – 15	% 0.57 – 0.28
جنوب صحراء إفريقيا	1.5	3 – 1	% 0.20 – 0.07
شمال إفرقيا والشرق الأوسط	3.1	5 – 2	% 0.16 – 0.06
المجموع العالمي	75.8	608 – 445	% 0.8 – 0.59

Source: (Lewis, 2018, p. 7)

من خلال الجدول 1، يتبين أن خسائر الجرائم الالكترونية يتراوح بين 140 إلى 175 مليار دولار بالنسبة لقارة أمريكا الشمالية سنة 2017، والتي قد تصل نسبة خسائرها إلى 0.87 % من الناتج المحلي الإجمالي، بينما وصلت خسائر الجرائم الالكترونية إلى قيمة تتراوح بين 160 إلى 180 مليار دولار بالنسبة لأوروبا ووسط آسيا، والتي وصلت نسبة خسائرها إلى 0.89 % من الناتج المحلي الإجمالي، ويرجع ذلك إلى الانتشار الواسع لاستخدام تكنولوجيا المعلومات في اقتصاديات الدول المتقدمة، فيما وصلت خسائر الجرائم الالكترونية إلى قيمة تتراوح بين 1 إلى 3 مليار دولار بالنسبة لجنوب صحراء إفريقيا، بنسبة تتراوح بين 0.07 % إلى 0.2 % من الناتج المحلي الإجمالي، أما بالنسبة لشمال إفريقيا والشرق الأوسط فقد وصلت خسائر الجرائم الالكترونية إلى قيمة تتراوح بين 2 إلى 5 مليار دولار، وبنسبة تتراوح بين 0.06 % إلى 0.16 % من الناتج المحلي الإجمالي، ويرجع انخفاض النسبة إلى ضعف استخدام التكنولوجيا في هذه الدول.

ومن خلال نفس الجدول يتبين أن خسائر الجرائم الالكترونية تتراوح بين 445 إلى 608 مليار دولار سنة 2017 بالنسبة للعالم ككل، بنسبة تراوحت بين 0.59 % إلى 0.8 % من الناتج المحلي الإجمالي.

قارن مركز الاستراتيجية والدراسات الدولية CSIS مستوى خسائر الجرائم الالكترونية بمستوى تطور الأمن السيبراني، مؤشر الأمن السيبراني العالمي GCI هو مبادرة من قبل الاتحاد الدولي للاتصالات لقياس مدى التزام الدول بالأمن السيبراني في مختلف القطاعات، يقاس مستوى تطور الأمن السيبراني لكل بلد في خمس فئات: الإجراءات القانونية والتدابير التقنية والتدابير التنظيمية وبناء القدرات، والتعاون. تم تصنيف نتائج الاستطلاع إلى ثلاثة الفئات: البلدان التي تتميز اقتصاداتها بالرقمنة ولديها قدرات كبيرة

في مجال الأمن السيبراني، الدول التي تتم الرقمنة فيها بشكل متزايد ولكنها ما زالت تطور قدراتها في مجال الأمن السيبراني، والبلدان التي بدأت اقتصاداتها حديثا في التحول إلى الرقمنة وجهود تطوير الأمن السيبراني في بداياتها. يواجه تقدير تكلفة الجريمة السيبرانية العديد المشاكل، الأول هو نقص الإبلاغ من قبل ضحايا الجرائم الالكترونية وندرة جمع البيانات من قبل الحكومات، ثانيًا تكلفة تجنب المخاطر عبر الإنترنت، أين يختار الأشخاص العودة إلى الورق وتجنب المعاملات عبر الإنترنت بسبب مخاوفهم من الجرائم الإلكترونية التي يصعب تقديرها. ثالثا، تتمثل إحدى المشكلات الكبيرة في التكلفة الإجمالية المقدرة للبلدان، وليس الأفراد الشركات أو المستهلكين، على سبيل المثال، إذا كان لدى بلد ما 10 شركات وخسرت 100 دولار أمريكي خلال سنة بسبب الجريمة الإلكترونية، يبلغ متوسط التكلفة لكل شركة 10 دولارات، لكن في الواقع، التوزيع الحقيقي هو أن شركتين تخسران 50 دولارًا والثماني الآخرون يخسرون القليل أو لا يخسرون شيء (Lewis, 2018, pp. 7-9).

تصاعدت انتهاكات البيانات وعمليات القرصنة والاحتيال على الهوية بشكل متزايد، زادت خسائر الاحتيال في التجارة الإلكترونية بسرعة في أوائل العقد الأول من القرن الحادي والعشرين، خاصة بعد ظهور شبكات الروبوت، حيث بلغت ذروتها 181.7 مليون جنيه إسترليني في عام 2008 قبل أن تنخفض في عام 2011. وبلغ إجمالي الخسائر 217.4 مليون جنيه إسترليني في عام 2014، عندما شكلت 45٪ من إجمالي البطاقات الاحتيال و66٪ من إجمالي احتيال الشراء عن بعد. ارتفعت الخسائر التي لحقت بالقطاع المصرفي من الاحتيال المصرفي عبر الإنترنت في عام 2009 إلى 59.7 مليون جنيه إسترليني، وبلغت ذروتها إلى مستوى جديد في 2014/2013، عند 60.4 مليون جنيه إسترليني (Levi, October 2015, p. 4).

1.3. الآثار الاقتصادية الناجمة عن جرائم البرامج الفيروسية وبرامج التجسس Malware and spyware

تكلف برامج التجسس والبرامج الفيروسية (بما في ذلك الفيروسات والديدان وبرامج التجسس وأحصنة طروادة) المنظمات أكثر في عام 2019، بحيث تسهل البرامج الفيروسية مجموعة من الأنشطة الإجرامية، من برامج القرصنة وتسلل البيانات إلى تعطيل الشبكات، فقد شهدت الجرائم الالكترونية ظهور بائعين متخصصين ليسوا خبراء في تصميم البرامج الفيروسية فحسب، بل أيضًا في إعداد البنية التحتية اللازمة للهجوم، ويعرضون بيع هذه البرامج لمجرمي الإنترنت بمقابل مالي (Smith, Lostri, & Lewis, DECEMBER 2020, p. 24).

2.3. الآثار الاقتصادية الناجمة عن الجرائم اختراق وقرصنة البيانات Data breaches

في النصف الأول من عام 2019، تم الإبلاغ عن أكثر من 3800 حالة اختراق للبيانات، مما أدى إلى تعرض أكثر من أربعة مليارات قاعدة بيانات لجرائم إلكترونية، واختراق البيانات المتعلقة بصحة الأشخاص تعد واحدة من بين أهم الاختراقات، بحيث يمكن أن تكون هذه البيانات غالبًا واحدة من أكثر أشكال البيانات قيمة للمجرمين، في أوت 2020، كانت وزارة الصحة الأمريكية تحقق في أكثر من 550

حالة من حالات اختراق المعلومات الصحية الشخصية الناجمة عن السرقة أو القرصنة أو حوادث تكنولوجيا المعلومات أو الوصول غير المصرح به، تشمل هذه الحالات بيانات ما يقرب من 35 مليون فرد، غالبًا ما يكون اختراق البيانات نتيجة لجهات فاعلة خارجية، ولكن وجدت دراسة حديثة أن العديد منها ناتج عن هجمات من الداخل، ومن الأمثلة الحديثة على ذلك خرق عام 2019 لأكثر من 100 مليون قرص لمؤسسة كابيتال وان Capital One من قبل مهندس برمجيات يعمل في موقع أمازون Amazon Web Services. ويمكن أن يشكل العاملون داخل المؤسسات أيضًا تهديدًا على الملكية الفكرية الحساسة للشركات (IP)، ومن الأمثلة على ذلك حالة شركة Tesla في عام 2018، عندما أساء موظف استخدام وصوله لإجراء تغييرات على رمز الشفرة لنظام التشغيل التصنيعي لشركة Tesla، وقام بإرسال معلومات حول عمليات التصنيع في Tesla إلى جهة خارجية (Smith, Lostri, & Lewis, DECEMBER 2020, p. 24) .

3.3. الآثار الاقتصادية الناجمة عن جرائم التصيد Phishing

وفقًا لمجموعة عمل مكافحة التصيد الاحتيالي (APWG)، تم تسجيل أكثر من 165000 موقع فريد للتصيد الاحتيالي في الربع الأول من عام 2020. أصبح التصيد الاحتيالي أسهل في السنوات الأخيرة، حيث ظهرت عروض التصيد كخدمة في أسواق الجرائم الإلكترونية، بفضل هذه العروض، لم يعد مجرمو الإنترنت بحاجة إلى خبرة في تصميم البنية التحتية للتصيد الاحتيالي قبل إرسال حملاتهم، بدلاً من ذلك، يمكن للمجرمين ببساطة الشراء من البائعين الذين يعرضون مجموعاتهم الخاصة ويستضيفون، والتركيز على الضحايا (الذين تتوفر أيضًا تفاصيل الاتصال بهم بسهولة من نفس الأسواق). وجدت إحدى المجموعات البحثية أكثر من 5000 مجموعة من مجموعات التصيد الاحتيالي الجاهزة للاستخدام في النصف الأول من عام 2019 وحده (Smith, Lostri, & Lewis, DECEMBER 2020, p. 25).

4.3. الآثار الاقتصادية الناجمة عن الجرائم الالكترونية المالية Financial Cybercrime

تعتبر البنوك الهدف المفضل لمجرمي الإنترنت للمحترفين، تفرض الجرائم الإلكترونية تكلفة باهظة على الموارد المالية للمؤسسات المالية والمصرفية، جاء في أحد التقارير أن البنوك تنفق ثلاثة أضعاف على الأمن السيبراني مقارنة بالأمن غير المالي، يعتقد CSIS أن ثلاث دول – روسيا وكوريا الشمالية، وإيران – هي الأكثر نشاطًا في القرصنة المالية للمؤسسات، ولا تزال الصين هي الأكثر نشاطا في مجال التجسس، أهداف إيران ذات تأثير قسري، كما يتضح من هجوم حجب الخدمة الموزع الإيراني (DDoS) على البنوك الأمريكية الرائدة، يعتقد CSIS أنه بالنسبة للجرائم الإلكترونية، فإن أهم دولتين هما روسيا وكوريا الشمالية، إنهم يخترقون البنوك لكسب المال، حيث صرح نائب مدير وكالة الأمن القومي السابق علنًا، أن "الدول القومية تسرق البنوك"، وهم يفعلون ذلك باستعمال أجهزة الكمبيوتر وكان يشير إلى حملة

الجرائم الإلكترونية من 2015 إلى 2016 التي استهدفت العشرات من البنوك في شبكة SWIFT. كما تمت سرقة عشرات الملايين من الدولارات من البنوك في البلدان النامية (Lewis، 2018، صفحة 9).

تستمر الجرائم الإلكترونية في فرض تكاليف باهظة على المؤسسات المالية. اليوم، هناك خمسة مليارات من بيانات اعتماد المستخدم الفريدة (على سبيل المثال، مجموعات اسم المستخدم وكلمة المرور) المتاحة على الشبكة المظلمة لمجرمي الإنترنت. ينص تقرير جرائم الإنترنت لعام 2019 الصادر عن مكتب التحقيقات الفيدرالي على ما يلي: "يشتري بعض المجرمين بيانات الاعتماد في أسواق الشبكة المظلمة، حيث يبلغ متوسط تكلفة الحساب الواحد 15.43 دولارًا أمريكيًا. لكن أوراق الاعتماد المصرفية الأكثر رواجًا تباع بمتوسط 71 دولارًا ". كما تعرضت المؤسسات المالية للهجوم من قبل الدول القومية. في عام 2016، تمكن قراصنة كوريون شماليون من سرقة 81 مليون دولار من بنك بنغلاديش المركزي من خلال الاستفادة من أوراق الاعتماد المسروقة وتقديم طلبات تحويل أموال مزيفة إلى بنك الاحتياطي الفيدرالي في نيويورك. في الآونة الأخيرة، في عام 2018، تمكنت نفس المجموعة من المتسللين من سرقة 20 مليون دولار من بنك Bancomext المكسيكي. يمكن رؤية حجم التهديد الذي يواجه المؤسسات المالية بشكل أكثر وضوحًا في اعتقال زعيم عصابة جرائم إلكترونية عام 2018 قامت مجموعته بسرقة 1.2 مليار دولار من أكثر من 100 بنك على مدى خمس سنوات (Smith, Lostri, & Lewis, DECEMBER 2020, p. 25) .

5.3. الآثار الاقتصادية الناجمة عن الفيروسات (برامج الفدية) Ransomware

فيروسات الفدية هي أسرع الجرائم الإلكترونية انتشارًا، يشمل ضحايا برامج الفدية الشركات الكبرى والمؤسسات الصغيرة والمتوسطة والأفراد المستهلكين، في حين أن التكلفة التي يتحملها الفرد منخفضة، وعادة ما تكون حوالي 200 دولار في صورة فدية، فإن القدرة على إصابة آلاف الأهداف بتكلفة منخفضة ودون التعرض لخطر العقوبة تفسر سبب نمو هذه الفئة من الجرائم الإلكترونية بهذه السرعة، في حين أن العديد من الضحايا لا يدفعون فدية، ما يكفي لجعل هذا الأمر مربحًا، أفاد مكتب التحقيقات الفيدرالي بأنه تم دفع 209 ملايين دولار كفدية في الربع الأول من عام 2016، مقارنة بـ 24 مليون دولار فقط في مدفوعات الفدية في عام 2015 كله، ما دفع إلى مثل هذا النمو الهائل، بدأت برامج الفدية منذ سنوات بأقراص مرنة تم إرسالها عبر البريد، ودعوة الضحايا إلى إجراء مسح لتقييم مخاطر الإصابة بالإيدز، عندما تم إدخال القرص، أغلقت برامجه أجهزة الكمبيوتر الخاصة بهم وطالبوا بإرسال 189 دولارًا نقدًا إلى صندوق بريد في بنما. ومنذ ذلك الحين أصبح أكثر تعقيدا، حتى عام 2015، كانت حملات برامج الفدية تديرها مجموعات الجريمة المنظمة التي كتبت التعليمات البرمجية الخاصة بها. تشهد برامج الفدية تسويقا عبر الانترنت، مع توفر مجموعات أدوات برامج الفدية الجاهزة على الإنترنت مقابل بضعة دولارات وما يصل إلى 3000 دولار للعروض المتخصصة، يبلغ متوسط تكلفة شراء حزمة برامج الفدية 10 دولارات فقط، مما يسمح للعديد من المتسللين بتنفيذ هجمات للحصول على فدية، في الوقت الحالي، أكثر من

6000 موقع عبر الإنترنت تبيع منتجات وخدمات برامج الفدية، وتقدم أكثر من 45000 منتج مختلف (برامج فيروس) (Lewis, 2018, p. 11) .

على مدار العشرين عامًا الماضية، أصبحت الجرائم الإلكترونية أكثر تطور واحترافية، جرائم الإنترنت هي أسواق مزدهرة تقدم مجموعة من الأدوات والخدمات لمن يميلون إلى الجرائم، من منتجات مثل مجموعات الاستغلال والبرامج الفيروسية، الأدوات والمنصات الجديدة يمكن الوصول إليها أكثر من أي وقت مضى لأولئك الذين ليس لديهم مهارات تقنية متقدمة، مما يمكّن طوفانًا من الفاعلين الجدد من الانخراط في أنشطة الجرائم الإلكترونية، وفي الوقت نفسه، يمكن للمجرمين ذوي الخبرة التركيز على تطوير مجموعات مهارات أكثر تخصصا، واثقين في قدرتهم على العثور على الآخرين داخل النظام المزدهر للشبكة المظلمة والذين يمكنهم استكمال خدماتهم (Lewis, 2018, p. 12).

اعتبارًا من يونيو 2017، وجدت وكالة تطبيق القانون الأوروبية "يوروبول" أن شبكة Tor (شبكة الواب المظلمة أو المشفرة) تضم أكثر من 2.2 مليون مستخدم، يختلف الباحثون حول مقدار حركة المرور غير المشروعة على شبكة Tor، لكن إحدى الدراسات الحديثة قدرت أن ما يقرب من 57٪ من المواقع المظلمة تستضيف محتوى غير قانوني، في حين أن عدد المشاركين في هذه المجتمعات (شبكة الواب المظلمة أو المشفرة) هائل، قدر مكتب التحقيقات الفيدرالي أن سوق AlphaBay قد خدم أكثر من 200000 مستخدم وكان لديه 40.000 بائع قبل إزالته في يوليو 2017. في عام 2015، صرح نائب مدير وحدة الجرائم الإلكترونية الوطنية في المملكة المتحدة أن أجهزة إنفاذ القانون تعتقد أن الكثير من اقتصاد خدمات الجرائم الالكترونية CaaS قد تم إنشاؤه على عمل 100 إلى 200 شخص فقط، غالبًا ما يستفيد هؤلاء الأفراد بشكل كبير من مشاركتهم. وجدت إحدى المجموعات البحثية أن بعض المجرمين يمكن أن يكسبوا أكثر من 100000 دولار سنويًا فقط من بيع مجموعات برامج الفدية، أي أكثر من ضعف الراتب السنوي لمطور برمجيات في أوروبا الشرقية، حيث يعمل العديد من هؤلاء المجرمين (Lewis, 2018, pp. 12-13).

تظل برامج الفدية الجزء الأسرع نموًا في الجرائم الإلكترونية. خلال جائحة COVID-19، زادت هجمات برامج الفدية بشكل عام بنسبة 148٪ عن مستويات خط الأساس التي تم الإبلاغ عنها في فبراير 2020. أحد أكثر الاتجاهات المقلقة في برامج الفدية هو التحول نحو الأهداف في الصناعة التحويلية. بدأ باحثو الأمن في رؤية ظهور سلالات برامج الفدية التي تستهدف أنظمة التحكم الصناعية، وقد دفع ضحايا الصناعة بالفعل ملايين الفدية الذين وقعوا فريسة لها (Smith, Lostri, & Lewis, DECEMBER 2020, p. 25) .

6.3. الآثار الاقتصادية الناجمة عن الجرائم الكترونية متعلقة بانتهاك الملكية الفكرية Intellectual Property Theft

إن أهم مجال مكلف ماديا بالنسبة للجرائم الإلكترونية هو سرقة الملكية الفكرية والمعلومات السرية للأعمال، لقد فتح الاتصال بالإنترنت مساحة شاسعة للجرائم الإلكترونية، وتتجاوز سرقة بروتوكول الإنترنت المجالات التقليدية التي تهم الحكومات، مثل التقنيات العسكرية، تتمثل إحدى طرق قياس تكلفة سرقة الملكية الفكرية في البحث عن المنتجات المنافسة التي تحصل على حصة في السوق من أصحابها الشرعيين، إذا سرق المتسللون الملكية الفكرية، مثل تصميمات المنتجات، من مؤسسة صغيرة أو متوسطة الحجم، فقد تكون عملية قاتلة، تمثل سرقة الملكية الفكرية ربع تكلفة الجرائم الإلكترونية على الأقل، وعندما تنطوي على تكنولوجيا عسكرية، فإنها تخلق مخاطر على الأمن القومي أيضًا. غالبًا ما تكون هذه الخسائر غير مرئية للضحية (Lewis, 2018, p. 15).

تعتبر الصين مركز جرائم سرقة الملكية الفكرية، هناك إجماع عام على أن المتسللين الصينيين، المرتبطين غالبًا بجيش التحرير الشعبي (PLA)، كانوا يقودون حتى وقت قريب عمليات سرقة الملكية الفكرية. قبل عام 2015، كانت الصين مسؤولة عن نصف عمليات التجسس الإلكتروني ضد الولايات المتحدة التي تنطوي على سرقة الملكية الفكرية، وفقًا لمصادر حكومية أمريكية، ربما تسبب هذا في ضرر بقيمة 20 مليار دولار سنويًا، جاءت بقية التكلفة الإجمالية للجرائم الإلكترونية على الولايات المتحدة من الجرائم المالية وتكاليف الاسترداد وإنفاق الشركة الإضافي على الدفاعات، وهو ما يمثل ربما 100 مليار دولار في عام 2014، وفقًا لمسؤولين أمريكيين، في حين أن الأدلة، تشير إلى أن ثلاثة أرباع التجسس الصيني كان لأغراض تجارية، مما يشير إلى أن اتفاقية أوباما شي لعام 2015 بشأن التجسس الإلكتروني التجاري ربما تكون قد أنقذت الولايات المتحدة ما يصل إلى 15 مليار دولار سنويًا، في قمة 2015 Xi–Obama للرئيسين شي وأوباما رئيس الولايات المتحدة الامريكية ورئيس الصين، اتفق الزعيمان على أن "أي حكومة من الدولتين لن تقوم أو تدعم عن قصد سرقة الملكية الفكرية عبر الإنترنت، بما في ذلك الأسرار التجارية أو غيرها من المعلومات التجارية السرية، بقصد توفير مزايا تنافسية للشركات أو القطاعات التجارية، ليس من السهل قياس الخسائر الناجمة عن سرقة الملكية الفكرية، بالنسبة لتقرير 2018، بلغ تقدير قيمة جميع الملكية الفكرية في الولايات المتحدة بـ 12 تريليون دولار، مع زيادة سنوية تتراوح بين 700 مليار دولار و800 مليار دولار سنويا، تقدر الخسائر السنوية للولايات المتحدة بما يتراوح بين 10 مليارات دولار و12 مليار دولار من الجرائم الإلكترونية التي تستهدف الملكية الفكرية وربما من 50 مليار دولار إلى 60 مليار دولار عالميًا، تعتبر سرقة المعلومات التجارية السرية للاستفادة من المفاوضات التجارية أو الاستثمار جزءًا مهمًا من الخسائر الناجمة عن جرائم الإنترنت، ولكنها قد لا تعكس الخسارة العالمية الكاملة. قد تأتي التكلفة الخفية من استخدام القرصنة للتلاعب في أسعار الأسهم، ولكن لا يزال من الصعب اكتشاف هذا النوع من الجرائم الإلكترونية، يشبه هذا النوع من التلاعب التداول من الداخل، يقدر مركز أبحاث أسترالي الخسارة من جميع أنواع التلاعب بالسوق بحوالي 10 مليارات دولار في السنة (Lewis, 2018, pp. 16–17).

7.3. الآثار الاقتصادية الناجمة عن سرقة الهوية Identity Theft

تظهر الاستطلاعات بشكل روتيني سرقة الهوية كأحد أهم اهتمامات مستخدمي الإنترنت، وليس من المستغرب، بالنظر إلى حجم الانتهاكات التي تصنع الأخبار بشكل روتيني، لكن تقارير مكتب الإحصاءات والعدل (BJS) في عامي 2012 و2014 تشير إلى أن الخسائر الفعلية من سرقة الهوية لا تزال صغيرة، وجد تقرير BJS أن 16.6 مليون شخص قد تعرضوا لشكل من أشكال سرقة الهوية في عام 2012، مما أدى إلى خسائر بلغت حوالي 25 مليار دولار، يبلغ متوسط هذا المبلغ 1500 دولار لكل حادثة، فلماذا تثير سرقة الهوية مثل هذا القلق؟، وجدت وزارة العدل أنه كان أعلى نوع من جرائم الممتلكات في الولايات المتحدة، حيث تكلف 10 مليارات دولار أكثر من الخسائر المنسوبة إلى جميع جرائم الممتلكات الأخرى. ثانيًا، لم يكن لدى ثلثي الضحايا أي فكرة عن كيفية تعرضهم للاختراق ومتى تم اختراقه. تخلق سرقة الهوية شعوراً بالعجز. جريمة غير مرئية تؤثر على الملايين أمر يدعو للقلق. ليست كل سرقات الهوية مرتبطة بالإنترنت، ولكن الضحايا الحقيقيين هم البنوك وشركات بطاقات الائتمان التي تتحمل الجزء الأكبر من الخسائر. يشير تقرير CSIS الأخير، سرق المخترقون ما يقرب من ثلاثة مليارات من بيانات اعتماد الإنترنت وغيرها من معلومات تحديد الهوية الشخصية. من المحتمل أن يتضمن هذا تكرارات، لكن معدل النمو على مدى السنوات الخمس الماضية مذهل. يختلف سعر معلومات تحديد الهوية الشخصية المسروقة باختلاف العرض والطلب، من 50 دولارًا للسجلات الصحية في عام 2012 إلى بضعة سنتات. خرق وكالة التقارير الائتمانية Equifax، التي كشفت البيانات الشخصية لـ 143 مليون مستهلك أمريكي، في سبتمبر 2017 لا يزال انتهاك البيانات الأكثر دراماتيكية ياهو، مع فقدان مليار سجل فردي، كلف اختراق Equifax الشركة ما يقرب من 90 مليون دولار في الأشهر الأربعة الأولى بعد اكتشافه، تكبدت شركة Equifax رسومًا لمرة واحدة تتعلق بحادث الأمن السيبراني بقيمة 87.5 مليون دولار، وانخفض صافي دخلها بنسبة 27 ٪ في الربع الثالث (Lewis, 2018, pp. 17-18).

8.3. الآثار الاقتصادية الناجمة عن اختراق البريد الالكتروني لمنظمات الأعمال Business Email Compromise

تساعد سرقة الهوية مجرمي الإنترنت على إرسال رسائل بريد إلكتروني تنتحل شخصية الرئيس التنفيذي أو المدير المالي للشركة تطلب منهم إجراء تحويلات كبيرة. في أحد الأمثلة، تلقى موظف بمستوى أدنى كان يعمل لدى المدير المالي رسالة بريد إلكتروني من الرئيس التنفيذي خلال عطلة نهاية الأسبوع تفيد بأنه لا يمكنه الوصول إلى المدير المالي ويحتاج إلى تحويل الموظف 10 ملايين دولار على الفور إلى الحساب المصرفي الجديد للمورد. امتثل الموظف، وكان حساب "المورد" احتياليًا، وسرعان ما تم تحويل الأموال منه لتجنب التعقب. أصبحت هذه الممارسة منتشرة لدرجة أن مكتب التحقيقات الفيدرالي أطلق حملة توعية عامة لتحذير المديرين التنفيذيين. تمت سرقة أكثر من 5 مليارات دولار من خلال هذه الهجمات منذ عام 2015. أفاد مكتب التحقيقات الفيدرالي أن 22000 شركة في جميع أنحاء

العالم كانت ضحية لتسوية البريد الإلكتروني التجاري، يصعب على البنوك اكتشاف ومنع اختراق البريد الإلكتروني، نظرًا لأن المعاملة يتم تقديمها من قبل موظف شرعي ومعتمد من العميل. تحاول بعض البنوك توعية العملاء بالمخاطر، لكن الخسائر في تزايد مستمر، هناك أيضًا إحجام عن الإبلاغ عن الحوادث الناجحة، حيث تفضل الشركات استيعاب الخسائر وتحملها.

على الرغم من أن البنوك لا تزال هدفًا مفضلاً لمجرمي الإنترنت، فقد حدثت أيضًا زيادة في استخدام BEC، وهي فئة خاصة من سرقة الهوية. عادةً ما تستهدف هذه المخططات قسم الموارد البشرية في الشركة أو قسم الرواتب من خلال التظاهر كموظف يطلب تغيير معلومات الإيداع المباشر الخاصة به، بعد ذلك، يتم تحويل شيك راتب الموظف إلى حساب بطاقة مسبقة الدفع احتيالي. أشكال أخرى من تتضمن عمليات الاحتيال BEC حسابات البريد الإلكتروني للموردين والمحامين المخادعين وطلبات نموذج W-2 والطلبات الاحتيالية لبطاقات الهدايا، يسمح هذا لمجرمي الإنترنت بإرسال رسائل بريد إلكتروني تنتحل صفة أي موظف – من الموظفين الجدد إلى المدير التنفيذي (Smith, Lostri, & Lewis, DECEMBER 2020, p. 26) .

بشكل عام، تمثل عمليات الاحتيال BEC تحديات خاصة للبنوك، حيث قد يبدو أن طلب التحويل البنكي قد تم تقديمه من قبل عميل شرعي، ومع ذلك، قد يتم استغلال بيانات اعتماد هذا الشخص من قبل مجرمي الإنترنت لأغراض غير شرعية. في مايو 2020، أفادت شركة Virtual Financial، إحدى الشركات العالمية الرائدة في مجال الخدمات المالية وصنع السوق، بأنها وقعت ضحية لعملية احتيال بقيمة 6.9 مليون دولار أمريكي. وفقًا لوثائق المحكمة القانونية المقدمة من Virtu، تسلل المتسللون إلى حساب البريد الإلكتروني الخاص بالرئيس التنفيذي وأرسلوا عدة رسائل بريد إلكتروني تنتحل شخصية الرئيس التنفيذي إلى قسم المحاسبة. طلب المتسللون تحويلين برقيين إلى بنوك خارجية، أحدهما بمبلغ حوالي 3.6 مليون دولار والآخر بحوالي 7.2 مليون دولار. اعتقادًا بأن الطلبات مشروعة، امتثل قسم المحاسبة في Virtu للطلب فقط بعد أن أرسل قسم المحاسبة الأموال إلى الأموال، قام قسم التدقيق الداخلي في Virtu بوضع علامة على التحويلات على أنها احتيالية (Smith, Lostri, & Lewis, DECEMBER 2020, p. 26) .

9.3. الآثار الاقتصادية الناجمة عن الجرائم سرقة العملات المشفرة Crypto currency theft

لا تزال سرقة العملات المشفرة تمثل اتجاهًا رئيسيًا في جرائم الإنترنت، حيث سُرقت أكثر من 4 مليارات دولار من العملات المشفرة على مدار عام 2019 وحوالي 1.4 مليار دولار سُرقت في الأشهر الخمسة الأولى من عام 2020. غالبًا ما تحدث هذه السرقات من التبادلات والمحافظ حيث يحتفظ المستخدمون بعملاتهم المعدنية، باستخدام مجموعة من التكتيكات بما في ذلك التصيد والبرامج الفيروسية والسرقة من الداخل. هناك اتجاه ناشئ آخر وهو Cryptojacking، حيث يتم تثبيت البرامج الفيروسية على أجهزة كمبيوتر الضحايا لتعدين العملات المشفرة عن بُعد (Smith, Lostri, & Lewis, DECEMBER 2020, p. 26).

4. خاتمة

من خلال ما سبق، تم التعرف على أهم المفاهيم المرتبطة بالجريمة الالكترونية، وأنواعها وتصنيفاتها، حيث أدى استخدام تكنولوجيا الإعلام والاتصال بطرق غير شرعية، إلى ظهور ما يعرف بالجريمة الالكترونية، حيث تتعدد آثار الجريمة الالكترونية، من اختراق وانتهاك خصوصيات الآخرين (أفراد أو مؤسسات) إلى سرقة أو إتلاف معلومات، سرقة أموال، وهذا من خلال برامج فيروسية وحيل معلوماتية يوقع بها الضحية.

1.4. النتائج:

للجريمة الالكترونية آثار مادية وغير مادية قد تصل إلى المساس بالأمن القومي للدول، حيث يعاني الأفراد من انتهاك الخصوصية وسرقة المعلومات، التي قد تؤدي الابتزاز، تعطيل الحواسيب الشخصية، سرقة معلومات بطاقات الائتمان (سرقة أموال)، أما بالنسبة للمؤسسات فإن الخسائر المالية تكون أكبر بالإضافة إلى سرقات تتعلق بالملكية الفكرية والسطو على بحوث أو براءات اختراع تتعلق بالمنتجات. ومن أهم النتائج المتحصل عليها ما يلي:

- في 2016 كلفت الجريمة السيبرانية الاقتصاد العالمي 0.8٪ كنسبة مئوية من الناتج المحلي الإجمالي العالمي؛
- في النصف الأول من عام 2019، تم الإبلاغ عن أكثر من 3800 حالة اختراق للبيانات، مما أدى إلى تعرض أكثر من أربعة مليارات قاعدة بيانات لجرائم إلكترونية، واختراق البيانات المتعلقة بصحة الأشخاص تعد واحدة من بين أهم الاختراقات، بحيث يمكن أن تكون هذه البيانات غالبًا واحدة من أكثر أشكال البيانات قيمة للمجرمين، في أوت 2020، كانت وزارة الصحة الأمريكية تحقق في أكثر من 550 حالة من حالات اختراق المعلومات الصحية الشخصية الناجمة عن السرقة أو القرصنة أو حوادث تكنولوجيا المعلومات أو الوصول غير المصرح به، تشمل هذه الحالات بيانات ما يقرب من 35 مليون فرد؛
- تم تسجيل أكثر من 165000 موقع فريد للتصيد الاحتيالي في الربع الأول من عام 2020؛
- وجدت إحدى المجموعات البحثية أكثر من 5000 مجموعة من مجموعات التصيد الاحتيالي الجاهزة للاستخدام في النصف الأول من عام 2019 وحده؛
- تعتبر البنوك الهدف المفضل لمجرمي الإنترنت للمحترفين، تفرض الجرائم الإلكترونية تكلفة باهظة على الموارد المالية للمؤسسات المالية والمصرفية، جاء في أحد التقارير أن البنوك تنفق ثلاثة أضعاف على الأمن السيبراني مقارنة بالأمن غير المالي؛

- نص تقرير جرائم الإنترنت لعام 2019 الصادر عن مكتب التحقيقات الفيدرالي على أن بعض المجرمين يشتري بيانات الاعتماد في أسواق الشبكة المظلمة، حيث يبلغ متوسط تكلفة الحساب الواحد 15.43 دولارًا أمريكيًا. لكن أوراق الاعتماد المصرفية الأكثر رواجًا تباع بمتوسط 71 دولارًا؛
- أفاد مكتب التحقيقات الفيدرالي بأنه تم دفع 209 مليون دولار كفدية في الربع الأول من عام 2016، مقارنة بـ 24 مليون دولار كمدفوعات الفدية في عام 2015 كله؛
- خلال جائحة COVID-19، زادت هجمات برامج الفدية بشكل عام بنسبة 148٪ عن مستويات خط الأساس التي تم الإبلاغ عنها في فبراير 2020؛
- قبل عام 2015، كانت الصين مسؤولة عن نصف عمليات التجسس الإلكتروني ضد الولايات المتحدة التي تنطوي على سرقة الملكية الفكرية، وفقًا لمصادر حكومية أمريكية، ربما تسبب هذا في ضرر بقيمة 20 مليار دولار سنويًا، جاءت بقية التكلفة الإجمالية للجرائم الإلكترونية على الولايات المتحدة من الجرائم المالية وتكاليف الاسترداد وإنفاق الشركة الإضافي على الدفاعات، وهو ما يمثل ربما 100 مليار دولار في عام 2014؛
- تقدر الخسائر السنوية للولايات المتحدة بما يتراوح بين 10 مليارات دولار و12 مليار دولار من الجرائم الإلكترونية التي تستهدف الملكية الفكرية وربما من 50 مليار دولار إلى 60 مليار دولار عالميًا. ويقدر مركز أبحاث أسترالي الخسارة من جميع أنواع التلاعب بالسوق بحوالي 10 مليارات دولار في السنة؛
- تشير تقارير مكتب الإحصاءات والعدل (BJS) في عامي 2012 و2014 إلى أن الخسائر الفعلية من سرقة الهوية لا تزال صغيرة، وجد تقرير BJS أن 16.6 مليون شخص قد تعرضوا لشكل من أشكال سرقة الهوية في عام 2012، مما أدى إلى خسائر بلغت حوالي 25 مليار دولار، يبلغ متوسط هذا المبلغ 1500 دولار لكل حادثة؛
- يختلف سعر معلومات تحديد الهوية الشخصية المسروقة باختلاف العرض والطلب، من 50 دولارًا للسجلات الصحية في عام 2012 إلى بضعة سنتات؛
- أفاد مكتب التحقيقات الفيدرالي أن 22000 شركة في جميع أنحاء العالم كانت ضحية لتسوية البريد الإلكتروني التجاري، يصعب على البنوك اكتشاف ومنع اختراق البريد الإلكتروني، نظرًا لأن المعاملة يتم تقديمها من قبل موظف شرعي ومعتمد من العميل. تحاول بعض البنوك توعية العملاء بالمخاطر، لكن الخسائر في تزايد مستمر، هناك أيضًا إحجام عن الإبلاغ عن الحوادث الناجحة، حيث تفضل الشركات استيعاب الخسائر وتحملها؛
- لا تزال سرقة العملات المشفرة تمثل اتجاهًا رئيسيًا في جرائم الإنترنت، حيث سُرقت أكثر من 4 مليارات دولار من العملات المشفرة على مدار عام 2019 وحوالي 1.4 مليار دولار سُرقت في الأشهر الخمسة الأولى من عام 2020.

2.4. التوصيات:

لتفادي الآثار الوخيمة للجرائم الالكترونية وجب الاعتماد على مختلف الطرق الحمائية والدفاعية من خلال اقتناء وتثبيت البرامج المضادة للفيروسات الالكترونية، والاستعانة بخبراء المعلوماتية للتعرف على الثغرات الموجود بنظام الإعلام الآلي للمؤسسات، تكوين مستمر للمورد البشري على أحدث تقنيات تكنولوجيات الإعلام والاتصال، بالإضافة إلى ضرورة تطوير وسن التشريعات والقوانين التي تعاقب مختلف أشكال الجريمة الالكترونية.

3.4. آفاق البحث:

من خلال هذا البحث يمكن اقتراح العنوان التالي كتكملة لها: الأمن السيبراني ودوره في الحد من الجريمة الالكترونية.

5. قائمة المراجع:

- Glenn Curtis .(2009) .CYBERCRIME: AN ANNOTATED BIBLIOGRAPHY OF SELECT FOREIGN-LANGUAGE ACADEMIC .*Federal Research Division, Library of Congress, Washington*.
- James Lewis .(2018) .Economic Impact of Cybercrime-No Slowing Down . *McAfee*.
- Jeetendra Pande .(2017) .Introduction to Cyber Security .*Uttarakhand Open University*.
- M Alansari ،M Aljazzaf و، M Sarfraz .(2019) .On Cyber Crimes and Cyber Security .*Developments in Information Security and Cybernetic Wars, IGI Global ،Hershey, PA, USA* ، pp. 1-41.
- Michael Levi .(October 2015). The implications of economic cybercrime for policing .*City of London Corporation, Cardiff University*.
- P.S.Seemma ،S Nandhini و، M Sowmiya .(November 2018) Overview of Cyber Security .*International Journal of Advanced Research in Computer and Communication Engineering.7* ،
- Zhanna Malekos Smith ،Eugenia Lostri و، James A. Lewis .(DECEMBER 2020) .The Hidden Costs of Cybercrime .*McAfee, San Jose*.
- الإسكوا. (2012). نشرة تكنولوجيا المعلومات والاتصالات للتنمية في المنطقة العربية. *(18)* . اللجنة الاقتصادية والاجتماعية لغربي آسيا.

- خالد بن سعيد، عبد الرحمان عثماني، و مجدوب نوال. (جويلية 2020). الجريمة المعلوماتية وآثرها على التنمية الاقتصادية. *المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، برلين، ألمانيا* .
- عزيزة رابحي. (2018/2017). الأسرار المعلوماتية وحمايتها الجزائية. *أطروحة دكتوراه علوم في القانون الخاص* . جامعة أبوبكر بلقايد تلمسان.