الأبعاد الإقتصادية للجريمة الإلكترونية

أ. صراع كريمة
جامعة وهران2
rimania1000@live.fr

أ.دقيش جمال
المركز الجامعي احمد زبانة غليزان
dekkiche.djamel@yahoo.fr

ملخص: لقد حاولنا من خلال هذه الورقة البحثية التطرق إلى الجريمة الإلكترونية من منظور إقتصادي و كيف يمكن للجريمة الإلكترونية أن يكون لها تأثير على الجانب الإقتصادي، خاصة نتيجة ما يمر به الاقتصاد العالمي نتيجة العولمة وتحرير التجارة الدولية و تحول الاقتصاد العالمي من مرحلة الاقتصاد التقليدي إلى مرحلة الاقتصاد الرقمي مما ادى إلى تصاعد خطورة الجريمة الإلكترونية واتساع حجمها ، لقد أصبحت تسبب هذه الجرائم تهديداً حقيقياً للأمن المجتمعي والاقتصاد من خلال عمليات الاحتيال والسرقة والقرصنة التي تتم من خلال الانترنت.

الكلمات المفتاحية: الجريمة الإلكترونية ،الانترنت، الجريمة الإلكترونية الإقتصادية، الهجوم الإلكتروني.

التصنيف JEL: L81

Abstract:

We have tried in this paper to address the electronic crime from an economic perspective and how can electronic crime that have an impact on the economic side, especially as a result of the world economy as a result of the globalization and liberalization of international trade, and the transformation of the world economy from the traditional economy to the stage of the digital economy, which led to the escalation of the seriousness of the crime, electronic commerce and the expansion of its size, causing these crimes has become a real threat to the community and economy through fraud, theft and piracy through the Internet.

KEY WORDS : cybercrime, internet, Electronic Economic Crime, Electronic attack.

Jel Classification codes:L81

مقدمة:

لفد أصبحت أجهزة الحاسوب من أهم وسائل الإتصال بين الأفراد و المؤسسات وقد ازداد التوجّه لاستخدام شبكات المعلومات الإلكترونيّة في الفترة الأخيرة بصفَتها أداة اتّصال دولية في مُختلف المجالات و نظرا لعديد المزايا التي تختص بها من سرعة إنتقال المعلومة و توفير الوقت و الجهد و إختصار المسافات و لكن لم يمنع الإنتشار الكبير لهذه الشبكات الإلكترونية ظهور العديد من المشاكل والمَخاطر، و التي قدّمت أصنافاً من الجرائم لم تكن مُتداولةً سابقاً، سُميّت بالجرائم الإلكترونية و هذا ما يدفعنا لطرح الإشكالية الأتية:

كيف يمكن أن يكون للجريمة الإلكترونية أثر على الإقتصاد؟

أهمية الدراسة:

تنبع أهمية أهمية البحث كون أن أ الجرائم الإلكترونية أصبحت تهدد أمن وسلامة الأفراد والمؤسسات, ومع تزايد المعلومات واستخدام شبكة الإنترنت في تبادلها الالكترونية وغيرها من الأنشطة سوف تتزايد صور الاعتداءات والتهديدات، وظهور العديد من أنماط القضايا المُختلفة، وهو الأمر الذي تطلب ضرورة التصدي لهذه الطائفة من الجرائم بالشكل الذي يُحقق فاعلية في تصدي لها.

أهداف الدراسة:

1-التطرق إلى مفهوم الجريمة الإلكترونية و خصائصها و أهم الطرق المستخدمة في الجريمة الإلكترونية.

2- إبرازالأثار الإقتصادية و الخسائر المالية التي تسببها الجريمة الإلكترونية

وللإجابة على هذه الأسئلة إرتأينا أن نقسم هذه الورقة البحثية إلى ثلاث محاور:

المحور الأول تطرقنا فيه إلى مفهوم الجريمة الإلكترونية خصائصها من هم مرتكبو الجريمة الإلكترونية.

المحور الثاني تطرقنا فيه إلى الجريمة الإلكترونية الإقتصادية و تأثيرها على الإقتصاد .

المحور الثالث تطرقنا إلى المجهودات الدولية الساعية للحد من تأثيرات الجريمة الإلكترونية و أهم أساليب مكافحتها.

أولا.مفهوم الجريمة الإلكترونية:

قبل التطرق لمفهوم الجريمة الإلكترونية لابد للتطرق لمفهوم كلمة الجريمة بإعتبار ان الجريمة الإلكترونية تتكون من مقطعين الجريمة و كلمة الإلكترونية.

فقد عرفت الجريمة بصفة عامة على أنها كل فعل غير مشروع صادر عن إرادة آثمة يقرر لها القانون عقوبة أو تدبير احترازيا.

بينما عندما نضيف كلمة الإلكترونية فنقصد أنها فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية" كما تعرف بأنها "كل أشكال السلوك غير المشروع الذي يرتكب باستخدام

الحاسوب" وكذلك تعرف بأنها "الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسا.[1]

كما عرفت الجريمة الالكترونية على أنها نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي.كما يعرفها البعض الآخر: بأنها تصرف غير مشروع يؤثر في الأجهزة و المعلومات الموجودة عليها[2].

الجرائم الناشئة عن الاستخدام الغير المشروع لشبكة الانترنيت على المعلومة بشكل رئيسي، وهذا الذي أدى إلى إطلاق مصطلح الجريمة المعلوماتية على هذا النوع من الجرائم.[3]

و قد عرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية عرفها من خلال تعريف الحاسب الآلي بأنها " الجرائم التي تقوم فيها بيانات الحاسب الآلي والبرامج المعلوماتية بدور رئيسي " ، كما عرفت أيضا بأنها " نشاط جنائي يمثل اعتداءً على برامج وبيانات الحاسب الإلكتروني "[4]

ومما سبق نستخلص أن الجريمة الإلكترونية هي كل فعل إجرامي ناشئ عن إستخدام أجهزة الكمبيوتر و شبكة المعلوماتية بطريقة غير شرعية.

الجريمة الإلكترونية لها مسميات عدة منها:

-1جرائم الحاسوب والإنترنت

-2جرائم التقنية العالية

-3الجريمة الإلكترونية

-4الجريمة السايْبِريّة

-5جرائم أصحاب الياقات البيضاء

1.التطورالتاريخي لجرائم الأنترنت:

مرت جرائم الأنترنت بتطور تاريخي تبعا لتطور التقنية واستخداماتها، ولهذا مرت بثلاث مراحل.

-المرحلة الأولى :مع بداية استخدام الحواسيب في فترة الستينات لم تظهر جرائم الكمبيوتر سوى في شكل مقالات صحفية و كانت موضوع تساؤل هل جرائم الكمبيوتر جرائم بالمعنى القانوني أم انها مجرد سلوكيات غير أخلاقية في مجال المعلوماتية و خلال فترة السبيعينات تزايد الإهتمام بموضوع جرائم الكمبيوتر خاصة مع إتساع إستخدام الحواسيب الشخصية ، وبدأ الحديث عنها بوصفها ظاهرة إجرامية لا مجرد سلوكيات مرفوضة.

-المرحلة الثانية: في الثمانينات، ظهرت عمليات اقتحام نظام الكمبييوتر عن بعد وأنشطة نشر وزرع الفيروسات الالكترونية التي تقوم بعملية تدميرية للملفات أو البرامج و إنتشر مصطلح

"الهاكرز " و هو الشخص القادر على إقتحام النظم ،ةو تحولت رغبة المحترفين تجاوز امن المعلومات وإظهار تفوقهم التقني إلى أداة إجرام خاصة بعد إرتكاب أفعال تستهدف الاستيلاء على المال أو التجسس أو الاستيلاء على البيانات السرية والاقتصادية الاجتماعية والسياسية والعسكرية

-المرحلة الثالثة: حيث شهدت التسعينات تناميا هائلا في شبكة الإنترنت و ما صاحبته من تسهيل لعمليات دخول الأنظمة واقتحام شبكة المعلومات أدى إلى توسع انماط و نطاق الجرائم الالكترونية فإنتشرت جرائم نشر الفيروسات عبر المواقع الالكترونية لما تسهله من انتقالها إلى ملايين المستخدمين و جرائم تتعلق بتعطيل نظام التقني للعديد من مواقع الانترنت خاصة المواقع التسويقية الذي يتسبب انقطاعها عن الخدمة لساعات في خسائر مالية بالملايين للشركات[5]

.2مرتكبو الجريمة الإلكترونية:

أنواع الجناة في جرائم الانترنت كما يُطلق عليهم إسم القراصنة،و يمكن حصر هؤلاء في ثلاثة فئات :

أ -الهاكرز : أو القراصنة و تعتبر القرصنة من أخطر الجرائم المعلوماتية فقد تكون القرصنة ذات غراض تخريبية او تكن ذات اغراض ترفيهية فضولية . أكثر القراصنة من الفئات الشبابية و يتميزون بهوس التعمق بالكمبيوتر و الانترنت.

ب -الكراكرز :وهم القراصنة المحترفون، ويعد هذا النوع من أكثر أنواع مرتكبي الجرائم الإلكترونية خطورة، ويكون القراصنة من هذه الطائفة ذوي مكانة اجتماعية عادية أو متخصصين في العلوم الإلكترونية.

ت -الطائفة الحاقدة :تستهدف غالباً هذه الطائفة المنظمات والمنشآت وأرباب العمل، ويكون الهدف من ارتكابها للجريمة بحق هذه الأطراف عادة بغية الانتقام والحصول على المنفعة المادية أو السياسية،وقد يكون تطرف أو جاسوس أو مخترق الأنظمة.[6]

3.تطور المفهوم التقليدي للجريمة إلى المفهوم الإلكتروني:

إن تطور مفهوم الجريمة من الشكل التقليدي إلى الشكل الإلكتروني كان نتيجة تغير الدوافع و الظروف الإجتماعية التي مر بها الإنسان و لعل أهم هذه التطورات هي التقدم العلمي الكبير في مجال التكنولوجيات الإتصال فقد أصبحت الانترنت شبكة إتصال دولية ألغت الحواجز و الفواصل بين الدول و أصبح النشاط الإنساني مرتكزا بشكل أكبر على شبكة الانترنت مما جعلها

وسيلة مثالية لتنفيذ العديد من الأفعال غير المشروعة و إمتداد شكل الجريمة من الواقع المادي إلى الجريمة في العالم الإفتراضي كما يبين الجدول الاتي:

الجدول 01:تطور الجريمة من الشكل التقليدي إلى الشكل الإلكتروني

الجريمة التقليدية	الجريمة الإلكترونية
الإحتيال	الإحتيال على الشبكة ،على المزاد الإلكتروني..
السطو	القرصنة ،الحرمان من الخدمة ،نشر الفيروسات
جرائم الأطفال الجنسية	إستمالة الأطفال على النت، المواقع الإباحية
غسيل الأموال	أنظمة الدفع على الشبكة
السرقة	جرائم الهوية، سرقة الملكية.

المصدر:ذياب موسى المديانة،**الجرائم الإلكترونية المفهوم و الأسباب**،الملتقى العلمي الجرائم المستحدثة في ظل التغيرات و التحولات الإقليمية و الدولية، الأردن ،2-2014/09/4

4.خصائص الجرائم الإلكترونية:

-عا لمية الجريمة "جرائم عابرة للقارات"

بمعنى انها لا تعترف بالحدود الجغرافية للدول وحتى بين القارات، و بفضل شبكة الانترنت أصبح مجتمع المعلومات مجتمع منفتح لا يخضع لحرس الحدود[7] و أصبحت الجريمة المرتبكة على الانترنت تعتبر جريمة لا حدود و ظهرت مشاكل حول تحديد القانون الواجب تطبيقه و تحديد الدولة صاحبة الإختصاص القضائي.

-جرائم بدون عنف: أطلقت على الجرائم التي تحدث عبر الانترنت بأنها الجرائم الناعمة إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي في ارتكابها كالقتل، السرقة ،وغيرها ، فالجرائم الالكترونية لا تتطلب أدنى مجهود عضلي ممكن ، بل تعتمد على المجهود الذهني المحكم، والتفكير العلمي المدروس القائم عن معرفة تقنية ممتازة بالحاسب الآلي، والتعامل السليم بالشبكة، على أساس أن الجاني في الجرائم الالكترونية هو إنسان متوافق مع المجتمع ولكنه يقترف هذا النوع من الجرائم بدافع اللهو أو لمجرد إظهار تفوقه على آلة الكمبيوتر أو على البرامج التي يشتغل بها، وأكيد لتحقيق مصلحة ما[8]

-**صعوبة إثباتها:** بحيث يتميز الجاني المجرم المعلوماتي بالذكاء و الإحترافية لذلك يصعب تتبع أثره إضافة إلى عدم و جود دليل مادي كالبصمة كما يستطيع أن يمحي أثره عن طريق إستخدام برامج أو كلمات سرية و رموز و يلجأ إلى التشفير لمنع أي دليل يقود إلى إدانته ،[9] كما أن المجني عليهم وهم غالبا مؤسسات عامة أو خاصة يحجمون عن الإبلاغ عنها تجنبا للإساءة إلى السمعة وهز الثقة، فضلا عن إمكانية تدمير الدليل في مدة زمنية قياسية و تعد جرائم صعبة الإثبات لكونها:

-جريمة لا تترك أثرا بعد ارتكابها

-صعوبة الاحتفاظ الفني بآثارها أن وجدت

-أنها تحتاج لخبرة فنية يصعب على المحقق التقليدي التعامل معها.

-أنها تعتمد على الخداع في ارتكابها و التضليل في التعرف على مرتكبيها.

-أنها تعتمد على قمة الذكاء في ارتكابها.[10]

5.أهم طرق الجريمة الإلكترونية

وتشمل وليس حصرا على:

-سرقة و تخريب و تزوير المعلومات واساءة استخدامها ويشمل ذلك قواعد المعلومات المكتبات تمزيق الكتب تحريف المعلومات و الدراسات الهامة الخاصة بالتطوير التقني و الصناعي او العسكري...

-انتهاك الخصوصية من خلال سرقة حسابات الأفراد و نشر معلومات سرية عنهم بهدف إفشاء أسرارهم.

– التصنت وتشمل الدخول لقواعد المعلومات وسرقة المحادثات عبر الهاتف.

– التجسس ويشمل اعتراض المعلومات ومحاولة معرفة ما يقوم به الأفراد.

-التشهير ويشمل استخدام المعلومات الخاصة أو ذات الصلة بالانحراف أو الجريمة ونشرها بشكل القصد منه اغتيال شخصية الأفراد أو الإساءة.

-السرقة العلمية الكتب والبحوث العلمية الأكاديمية وخاصة ذات الطبيعة التجريبية والتطبيقية.

– سرقة الاختراعات وخاصة في المجالات العلمية لاستخدامها أو بيعها..

– قرصنة البرمجيات ويشمل النسخ غير القانوني للبرمجيات واستخدامها أو بيعها مرة أخرى.

– قرصنة البيانات والمعلومات ويشمل اعتراض البيانات وخطفها بقصد الاستفادة منها وبخاصة أرقام البطاقة الائتمانية وأرقام الحسابات وكلمات الدخول وكلمات السر.

-خلاعة الأطفال وتشمل نشر صور خاصة للأطفال "الجنس السياحي" للأطفال خاصة وللإناث على الشبكات بشكل عام ونشر الجنس التخيلي.

– إرسال فيروسات على شكل رسائل إلكترونية بهدف تدمير البيانات .

-الإحتياال المالي بالبطاقات وهذا ناتج عن استخدام غير شرعي لبطاقات التسوق أو المالية أوالهاتف الخ.

– سرقة الأرقام والمتاجرة بها وخاصة أرقام الهواتف السرية واستخدامها في الاتصالات الدولية أو أرقام بطاقات الائتمان.

– التحرش الجنسي ويقصد به المضايقة من الذكور للإناث أو العكس من خلال المراسلة أو المهاتفة، أو المحادثة أو الملامسة.

– المطاردة والملاحقة والابتزاز وتشمل ملاحقة الذكور للإناث أو العكس والتتبع بقصد فرض إقامة علاقة ما وذلك من خلال استخدام البريد الإلكتروني وارسال الرسائل.

– الإرهاب الإلكتروني. يشمل جميع المكونات السالفة الذكر في بيئة تقنية متغيرة والتي تؤثر على فرص الإرهاب ومصادرة هذه التغيرات تؤثر على تكتيكات الإرهاب وأسلحته وأهدافه ومن التكتيكات الإرهابية ما يعرف بالإرهاب الإلكتروني.[11]

ثانيا: الجريمة الإلكترونية الإقتصادية:

لقد نتج عن الثورة التكنولوجية ظهور نوع جديد من المعاملات يسمى المعاملات الإلكترونية تختلف عن المعاملات التقليدية التى نعرفها من حيث البيئة التي تتم فيها هذه المعاملات فقد سمحت المعلوماتية و الانترنت في تداول الانشطة التجارية عبر الشبكة مما أ تاح للانشطة الإجرامية بتحقيق عوائد ماليةعن طريق وسائل غير مشروعة ناتجه عن عمليات التزوير و الإحتيال و نذكر اهم الجرائم الإلكترونية التي تقع على الأموال عبر الانترنت كالاتي:[12]

-التحويل الإلكتروني غير المشروع للأموال و السطو على بطاقات الإئتمان:

تتم عملية التحويل الإلكتروني للأموال بشكل غير مشروع من خلال التحايل و ذلك بالحصول على رقم كلمة السر من جهاز كمبيوتر المحتال عليه او عن طريق إنتحال شخصية وهمية و إيهام المحتال عليه بوجود مشروع مربح و بالتالي يتم تحويل إلكتروني للاموال لصالح المحتال كما يمكن أن يتم الإحتيال بإستعمال بطاقات الإئتمان و هي بطاقات بنكية للدفع او السحب الإلكتروني تصدرها هيئات عالمية كماستر كارد و فيزا كارد تسمح هذه البطاقات بعمليات البيع و الشراء عبر الانترنت تحمل أرقاما خاصة بكل عميل و مع التطور التقني و تطور البرمجيات أصبح بالإمكان الإستيلاء على هذه الأرقام و الحصول على الاموال منها

-**القمار و غسيل الاموال عبر الانترنت** :لقد اتاحت الانترنت إمكانية تواجد أندية أقمار إفتراضية عن طريق تواجدها عبر مواقع الأنترنت الأمر الذي ساعد المجرمين في أنشطتهم الإجرامية عن طريق غسيل اموالهم وخاصة مع ما تتوفر عليه الأنترنت من سرعة و امكانية تخطي الحواجز الحدودية مما يساعد المجرمين في تخطي القوانين التي تعيق انشطتهم غير المشروعة مما يسهل عملية غسيل الاموال الامر الذي يصعب في تقفي أثارها.

-**السطو على اموال البنوك**: عن طريق سرقة معلومات الشخصية للمستخدمين و الإستخدام غير الشرعي لمعلوماتهم للسطو على اموال البنوك بطريقة متخفية أو عن طريق قرصنة حسابات البنوك و المصارف المالية و تحويل الأاموال من حساب إلى حساب أخر

1.الإبعاد الإقتصادية الجريمة الإلكترونية :

إن الجرائم والهجمات الالكترونية من أخطر التهديدات التي تواجه معظم دول العالم، ولاشك مع ظهور العولمة و إستخدام الشبكة المعلوماتية في النشاطات الإقتصادية و التي أصبحت تدار إلكترونيا ومع إمكانية تحويل الإلكتروني للأموال بسرعة هائلة عبر شبكة الانترنت بين جميع الدول دون تحديد هوية المرسل وعدم وجود قيود و ضوابط جمركية لتدفق رؤوس الاموال و الأفراد أدى إلى ظهور أشكال و أنماط جديد للإجرام و بذلك إمتدت الجريمة الإلكترونية إلى المنظمات و القطاعات الإقتصادية و المالية التي أصبحت تكبد ها خسائر مالية كبيرة مما يؤثر سلبا على الإقتصاد .

إن الجرائم الالكترونية التي قد يتعرض لها الأفراد و الشركات و البنوك و حتى الدولة من طرف أشخاص أو منظمات محترفة هدفها الرئيسي الربح و التأثير المادي عليها و زعزعة أمن و الإستقرار

الإقتصادي للدول و في الأتي نذكر أهم الجرائم الإلكترونية التي تتعرض لها القطاعات الإقتصادية والتي تؤثر عليها سلبا في الجانب المادي.

1.1الجرائم الإلكترونية التي يتعرض لها الفرد:

لفد سمحت الانترنت للأفراد بالتواصل مع العالم الخارجي بحيث أصبح بإمكانه إجراء معاملات الشراء أو البيع وإدارة أعماله إلكترونيا

الجرائم الالكترونية التي قد يتعرض لها الفرد والتي تؤثر على الجانب المادي لديه:

- سرقة الهوية الشخصية
- سرقة بطاقة الائتمان الخاصة به
- الابتزاز والتهديد
- عمليات احتيال
- تحويل أو نقل حسابه المصرفي
- نقل ملكية الأسهم
- زيادة الفواتير بتحويل فواتير المجرم للضحية.

2.1الجرائم الالكترونية التي تتعرض لها الشركات :

- الإطلاع على معلومات سرية لصفقة أو مناقصة أو أمور تسويقية خاصة والاستفادة منها
- العبث بمخازن المعلومات الخاصة بالشركة بحذفها أو تعديلها أو تعطيل الوصول إليها
- سرقة الأموال وتحويل حسابات مصرفية الخاصة بالشركة
- الغش في المعاملات الالكترونية كالتغيير في المبيعات
- عمليات الاحتيال
- التهديد والابتزاز
- اختراق الموقع الإلكتروني الخاص بالشركة

3.1الجرائم الالكترونية التي تتعرض لها البنوك :

- السطو الإلكتروني
- العبث بمخازن المعلومات الخاصة بالبنك بحذفها أو تعديلها أو تعطيل الوصول إليها
- تعطيل النظام

•نقل ملكية الأسهم
•اختراق الموقع الإلكتروني الخاص بالبنك

4.1الجرائم الالكترونية التي تتعرض لها المنظمات والمؤسسات:

•الإطلاع على معلومات سرية والاستفادة منها
•العبث بمخازن المعلومات الخاصة بالمنظمة أو المؤسسة بحذفها أو تعديلها أو تعطيل الوصول إليها
•سرقة الأموال وتحويل حسابات مصرفية الخاصة بالمنظمة أو المؤسس
•عمليات الاحتيال
•الابتزاز و التهديد
•اختراق الموقع الإلكتروني الخاص بالمنظمة أو المؤسسة

5.1.الجرائم الالكترونية التي قد تتعرض لها الجهات والأجهزة الحكومية :

•الوصول إلى المعلومات سرية و الإطلاع عليها أو حذفها أو تعديلها بما يحقق هدف المجرم
•دعم الإرهاب والأفكار المتطرفة ونشر الإشاعات
•تعطيل وتخريب الخوادم الموفرة للمعلومات
•تعطيل أنظمة قطاعات حكومية و حيوية
•تعطيل الانترنت بالكامل
•سرقة الأموال

2.الخسائر المالية للجريمة الإلكترونية :

إن تحول الاقتصاد العالمي من مرحلة الاقتصاد التقليدي إلى مرحلة الاقتصاد الرقمي و تحول التعاملات التجارية و المالية إلى شكل إلكتروني زاد من خطورة الجريمة الإلكترونية و التي أصبحت في تصاعد مستمر ومن المتوقع أن يتزايد حجم الخسائر التي يتكبدها العالم بسبب الجريمة الإلكترونية في العقود القليلة المقبلة، نتيجة تزايد عدد الشركات التي تعتمد على الإنترنت في ممارسة نشاطها.

فبحسب أخر الإحصائيات فإن الاقتصاد العالمي يتضرر جراء الجريمة الإلكترونية تريليون دولار سنوياً، غير أن الخطورة الحقيقية لا تنبع من ضخامة حجم الخسائر فقط، وإنما من القبول المتزايد لخسائر الجريمة الإلكترونية باعتبارها ضريبة لا مفر منها لممارسة الأعمال في مختلف أنحاء العالم.

وتشير التقديرات إلى أن الاقتصاد العالمي المستند إلى الإنترنت يولد سنوياً نحو ثلاثة تريليونات دولار، وهذا الرقم مرشح للنمو بقوة في العقود المقبلة، وتطال الجريمة الإلكترونية نسبة تتراوح بين 15 و20 في المئة من حجم الاقتصاد العالمي المستند إلى الإنترنت[13]

.

ويتوقع ان تتجاوز التكلفة الإجمالية للتهديدات والجرائم الإلكترونية على مستوى العالم، ستتجاوز 6 تريليونات دولار في عام 2021. بهذا الاطار تكون معدل الجريمة قد سجلت ارتفاعا بنحو ثلاثة تريليونات دولار في عام 2015.[14]

و بحسب المنتدى الاقتصادي العالمي فإن ممارسات التزوير والقرصنة قد كلفت حوالي 1.77 تريليونات دولار في سنة 2015 ما يمثل قرابة 10 .% من التجارة العالمية.[15]

وبحسب تقرير .Grant Thornton يعتبر قطاع الخدمات المالية الأكثر عرضة للهجمات بنسبة 46%، يليه قطاع الرعاية الصحية بنسبة 24% من ثم قطاع الطاقة بنسبة 23.%

وتعد منطقة الشرق الأوسط، من بين الأكثر تضررا في العالم، من الهجمات الإلكترونية، بحسب تقرير أصدرته PWC وأظهر أن 56% من شركات المنطقة التي تعرضت لهجوم إلكتروني خسرت 500 ألف دولار.[16]

وتتضح خطورة الجريمة الإلكترونية على الاقتصاد العالمي، عبر مقارنة الخسائر التي يتكبدها الاقتصاد العالمي من الجريمة الإلكترونية بحجم الخسائر التي يتكبدها الاقتصاد العالمي من مصادر التهديد الأخرى.

ففي الوقت الذي يخسر فيه الاقتصاد العالمي 0.8 في المئة من إجمالي الناتج المحلي العالمي نتيجة الجريمة الإلكترونية، فإن النسبة تقل عن 0.2 في المئة نتيجة القرصنة البحرية، أى إن الجريمة الإلكترونية تكبد الاقتصاد العالمي أربعة أمثال الخسائر التي تكبدها الاقتصاد العالمي نتيجة القرصنة البحرية.

وتتساوى الخسائر التي يتكبدها الاقتصاد العالمي نتيجة الجريمة الإلكترونية مع حجم الخسائر التي يتكبدها الاقتصاد العالمي من السلع المغشوشة، كما تتساوى أيضاً مع حجم الخسائر التي يتكبدها الاقتصاد العالمي نتيجة تجارة المخدرات.

وبحسب تقرير أعدته شركة مكافي المتخصصة في حماية أمن البيانات، فإن الجريمة الإلكترونية تجارة مربحة منخفضة التكلفة قليلة المخاطر تدر أرباحاً طائلة، تزيد على إجمالي الدخل القومي للكثير من الدول.

ولا تقتصر خسائر الجريمة الإلكترونية فقط على الخسائر المباشرة، وإنما تشمل أيضاً الخسائر غير المباشرة مثل حقوق الملكية الفكرية، وسرقة الأصول المالية والمعلومات التجارية الحساسة، وتكلفة استعادة البيانات وتكلفة الفرص البديلة وبطبيعة الحال لا يمكن تجاهل تأثير الجريمة الإلكترونية على الاقتصاد الوطني، وعلى أداء الشركات وعلى حركة التجارة العالمية، وعلى القدرة التنافسية والابتكار.

1.2أحدث هجوم إلكتروني عالمي "فيروس الفدية":

تتعرض حكومات العالم لموجة جديدة من التهديدات الإلكترونية ولعل أخرها هو الهجوم الإلكتروني الذي تم من طرف مجموعة من القراصنة تطلق على نفسها "شادو بروكرز" ،و التي أطلقت فيروس إسمه فيروس الفدية .

فيروس الفدية هو عبارة عن برمجيات خبيثة أسميت ب "wannacry" أصابت أكثر من 300,000 جهاز حاسب في نحو 150 دول منذ ماي 2017 [17] استهدفت آلاف المؤسسات والأفراد وطالت الهجمات مستشفيات بريطانية ومجموعة رينو الفرنسية لصناعة السيارات والنظام المصرفي الروسي ومجموعة "فيديكس" الأميركية وجامعات في اليونان وايطاليا، وغيرها من الأهداف في جميع القارات[18]

و فيروس الفدية هجوم الإلكتروني يبدأ بوصول رسالة أو رابط من شخص مجهول يطلب تحميل الملف على أنه ملف مهم أو شخصي. وفور تحميل الملف في الكمبيوتر أو الهاتف الذكي تبدأ عملية تشفير_البيانات ويصبح بعدها صاحب الجهاز غير قادر على الوصول إليها.

يقوم برنامج الفدية بإقفال ملفات المستخدمين المستهدفين و يمنعهم من فتح نظام تشغيل جهازهم و يقوم بتشفير جميع البيانات داخل الجهاز ويرغم القراصنة على دفع مبلغ من المال

يتراوح بين 300 و600 دولار على هيئة بيتكوينز[19] مقابل إعادة فتحها و في غضون ثلاثة أيام المبلغ سيزداد إلى الضعف، أما إذا لم يتم الدفع بعد سبعة أيام فسيتم محو الملفات..

ثالثا: المجهودات الدولية الرامية للتصدي لجريمة الإلكترونية:

مع تزايد خطورة الجريمة الإلكترونية على المستوى العالمي إنصبت الجهود الدولية و الإقليمية من اجل خلق أليات قانونية للحماية من أخطارها و برزت في هذا المجال العديد من المنظمات الدولية و الإقليمية، فعلى الصعيد الدولي عقد مؤتمر القمة العالمي المعني بمجتمع المعلومات، الذي عقد في جنيف في2003 من ثم في تونس في عام 2005، و قد خلصت نتائج هذا المؤتمر أهمية تطوير مجتمع المعلومات في جميع البلدان وقد سلطت الضوء الوثائق المتضمنة إعلان مبادئ جنيف، وخطة عمل جنيف والتزام تونس ، وجدول أعمال تونس لمجتمع المعلومات، على أهمية وتعزيز الثقة والأمن في مجتمع المعلومات، ووضع الأطر اللازمة لتحقيق تلك الأهداف .وقد اعتمدت ما مجموعه 174 دولة هذه الوثائق الختامية.

بالإضافة إلى إتفاقية مجلس أوروبا بشأن الجريمة الإلكترونية (المعروفة أيضا باسم اتفاقية بودابست)، والتي عقدت في 2001 و دخلت حيز النفاذ في 2004، هي معاهدة إقليمية رئيسية ترمي إلى تحديد الجريمة الإلكترونية وتحديد التشريعات الخاصة بها ، وبناء القدرات للتحقيق في أشكالها، وتعزيز التعاون في هذا المجال .

وعلاوة على ذلك، لمواءمة تشريعات الجرائم الإلكترونية في كمنولث الأمم، قات مجموعة من الخبراء

بإعداد قانون نموذجي في عام 2002 مستوحى من اتفاقية بودابست المعروفة باسم قانون الجرائم المتصلة بالحواسيب .وعلاوة على ذلك، اعتمد الاتحاد الأوروبي في عام 2003 إطارا قانونيا بشأن نظام المعلوما ت التي دخلت حيز التنفيذ في عام 2005.[20]

وكذا مجهودات الامم المتحدة لمكافحة الجريمة الإلكترونية فقد عقدت الكثير من الإتفاقيات و المؤتمرات في سبيل مكافحة كل أشكال الجريمة و الجريمة المستحدثة فقد عقدت إتفاقية خاصة سنة 2000 لمكافحة إساءة إستخدام تكنولوجيا المعلومات لأغراض إجرامية و عقب ذلك عقدت مؤتمرا بالبرازيل أفريل 2010 بحيث تناولت أعماله تحليل الظاهرة إحصائيات المتعلقة بالجريمة الإلكترونية إجراءات التحقيق،الأدلة الإلكترونية ،المساعدة التقنية الدولية،خدمات الانترنت، التعاون الدولي للتصدي للجريمة الإلكترونية .بالإضافة إلى أعمال اللجنة الإقتصادية و الإجتماعية لغربي اسيا التابعة للمجلس الإقتصادي و الإجتماعي تحت غطاء منظمة الأمم

المتحدة سنة 2008 [21]ومن ثم افريل 2015 و قد جاءت جهود الإسكوا(ESCWA)[22] الرامية إلى تطوير التشريعات الإلكترونية ومواءمتها وكذا إنشاء مجتمع المعرفة في المنطقة العربية،مع التركيز على الاطر التنظيمية و الإجرامية لمكافحة الجريمة الإلكترونية و ضمان السلامة الإلكترونية.

وبالإضافة إلى أعمال منظمة التعاون الإقتصادي و التنمية و التي تعقد سنويا مجموعة من المؤتمرات لمواكبة مستويات التطور الإجتماعي و الإقتصادي في العالم و قد بدأ إهتمام هذه المنظمة بالجرائم المرتكبة عبر الأنترنت مندر1978 و في عام 1983 أصدرت المنظمة تقريرا حول الجرائم المرتبطة بالحاسوب حيث تضمن التقرير مجموعة من أفعال سوء إستخدام الكمبيوتر و التي يجب على الدول أن تجرمها و تفرض عقوبات قانونية على مرتكبيها [23] وفي سنة 1992 وضعت المنظمة تقريرا يضم توصيات إرشادية خاصة بامن المعلومات و ذلك بفرض إجراءات عقابية على الأفعال الاتية:

-التلاعب بالبيانات بمعاجتها أليا أو محوها

--قرصنة البرامج

- الدخول غير المشروع للبيانات

-التجسس المعلوماتي يندرج تحته الحصول أو الإقتناء أو الإستعمال غير المشرع للمعطيات.

-التخريب المعلوماتي و يندرج تحته الإستخدام غير المشرع أو سرقة وقت الحاسب .

-إعتراض إستخدام المعطيات او نقلها.[24]

اما بالنسبة للإتحاد الدولي للاتصالات فقد وضع مخططا لتعزيز الأمن السيبراني العالمي يتكوّن من سبعة أهداف رئيسة، والأهداف السبعة هي:

- وضع استراتيجيات لتطوير نموذج التشريعات السيبرانية يكون قابلاً للتطبيق محليًا وعالميًا بالتوازي مع التدابير القانونية الوطنية والدولية المعتمدة.

- وضع استراتيجيات لتهيئة الأرضية الوطنية والإقليمية المناسبة لوضع الهيكليات التنظيمية والسياسات المتعلّقة بجرائم الانترنت.

- وضع استراتيجية لتحديد الحد الأدنى المقبول عالميًا في موضوع معايير الأمن ونظم تطبيقات البرامج والأنظمة.

- وضع استراتيجيات لوضع آلية عالمية للمراقبة والإنذار والرد المبكر مع ضمان قيام التنسيق عبر الحدود.

- وضع استراتيجيات لإنشاء نظام هوية رقمي عالمي وتطبيقه، وتحديد الهيكليات التنظيمية اللازمة لضمان الاعتراف بالوثائق الرقمية للأفراد عبر الحدود الجغرافية.
- تطوير استراتيجية عالمية لتسهيل بناء القدرات البشرية والمؤسسية لتعزيز المعرفة والدراية في مختلف القطاعات وفي جميع المجالات المعلوماتية.
- تقديم المشورة بشأن إمكانية اعتماد إطار استراتيجي عالمي لأصحاب المصلحة من أجل التعاون الدولي والحوار والتعاون والتنسيق في جميع المجالات التي سبق ذكرها.[25]

أما على المستوى العربي فقد أسفرت الجهود العربية عن ميلاد اتفاقية عربية لمكافحة جرائم تقنية المعلومات، و هذا كنتيجة للاجتماع المشترك لمجلس وزراء الداخلية و العدل العرب والمنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة و ذلك في ديسمبر 2010 و هذا بهدف تعزيز التعاون بين الدول العربية في مجال مكافحة جرائم تقنية إلى تعزيز القدرة على إنفاذ سياسات التقنية المعلوماتية والأمن المعلوماتي لضمان فاعلية تطبيق الخطط المنبثقة عن تلك السياسات لدى كل المؤسسات والهيئات والمنظمات والمنشآت في القطاعين العام والخاص بما يحقق أمناً جدياً وشاملاً للمعلومات، وبما يتوافق مع معايير الحد الأدنى لأمن المعلومات ومتطلباته وأدواته التقنية والإدارية والقانونية.[26]

1. أساليب مكافحة الجريمة الإلكترونية:

-فرض عقوبات صارمة على مرتكبي جرائم الانترنت و تأسيس منظمات خاصة لمكافحة الجريمة و الحد منها.

-تشريع قوانين دولية من أجل محاكمة مرتكبي جرائم الأنترنت في أي دولة وذلك نظرا للطبيعة الدولية للجريمة الإلكترونية و ذلك بتعزيز التعاون و التنيسق مع المؤسسات الدولية للتصدي لكافة أشكال الجريمة الإلكترونية عبر العالم.

-إستخدام أحدث التقنيات و العمل على تطويرها من أجل كشف هوية مرتكبي الجريمة بأسرع وقت ممكن.

-توعية الأفراد و المؤسسات بشكل دائم بخطوره الجرائم الألكترونية و ذلك بنشر خطورتها و أضرارها عبر وسائل الإعلام أو عبر تنظيم ملتقيات و أيام دراسية .

-الحفاظ على كلمة السر و تغييرها بشكل مستمر مع المحافظة على سرية المعلومات الشخصية و ذلك بعدم نشر ها في مواقع غير موثوقة.

-وضع رقم سري بشكل مطابق للمواصفات الجيدة التي تصعّب من عملية القرصنة عليه من هذه المواصفات بأن يحتوي على أكثر من ثمانية أحرف أن يكون متنوع الحروف والرموز

-عدم تحميل برامج مجهولة المصدر مع إستمرارية تحديث البرامج الأمن الخاصة بأجهزة الحاسوب.

-إستخدام برمجيات أمنة و خالية من الثغرات .

-الإبلاغ الفوري في حالة تعرض لجريمة إلكترونية .

-أخذ الحيطة والحذر وعدم تصديق كل ما يصل من إعلانات والتأكد من مصداقيتها عن طريق محركات البحث الشهيرة[27]

خاتمة:

بسبب التطور المضطرد والمتسارع في تكنولوجيا المعلومات، غدت الإنترنت ملعب جديد لإستحدات أشكال جديدة من الجرائم لم تكن معروفة قبلا و التي شكلت تهديدات جديدة تقع على مجمل الأنشطة الإقتصادية التي تتم في بيئة إفتراضية كظهور الاحتيال على الدفع الإلكتروني وغسل الأموال ;و التحويل غير المشروع للاموال إلكترونيا ، ، إن خطورة تزايد أعداد الجرائم الإلكترونية وتطور أساليبها وأنواعها و تأثيراتها سواء أكان من الناحية الاجتماعية أو الاقتصادية فقد أصبحت الجرائم المعلوماتية تتسبب في خسائر مالية مما يؤثر سلبا على الإقتصاد المحلي أو العالمي لذاك فإن التصدي لجرائم تقنية المعلومات باعتبارها من الجرائم العابرة للحدود الوطنية في كثير من أدوارها، يتطلب تعاوناً استراتيجياً مشتركاً على كل الأصعدة الوطنية والدولية ومن اهم النتائج التي يمكن إستخلاصها انه يجب على الحد و الوقاية من الجرائم الإلكترونية عن طريق:

-فرض قوانين و عقوبات صارمة على الجناة المدانين في الجرائم الإلكترونية.

-تعزيز التعاون الدولي و الإقليمي من أجل التصدي و متابعة الجرائم الإلكترونية بين مختلف دول العالم.

-رصد و متابعة المواقع المشبوهة من خلال أقسام و فرق متخصصة في أشكال الجرائم الإلكتونية و العمل على تدريبهم و تأهيلهم بأحدث الوسائل و التقنيات.

-وضع خطط و إستراتيجيات شاملة و مترابطة مبنية على دراسات و أبحاث ميدانية في مجال مكافحة كل اشكال الجريمة الإلكترونية.

-توعية المؤسسات و الافراد و الشركات بمدى الاخطار التي تسببها جرائم الالكترونية و التحذير منها

-تطوير برمجيات الامن بشكل دوري و مستمر و سد الثغرات و تأمين جميع وسائل التحويل الإلكتروني و البطاقات الإئتمانية و برامج و أجهزة البنوك و المؤسسات الإقتصادية و المالية.

المراجع والهوامش:

1. أسامة أبو الحجاج ،**دليلك الشخصي الى الأنترنت** ،دار النهضة المصرية،القاهرة، 1998. ص11
2. أمير فرج يوسف ، **الجرائم المعلوماتية على شبكة الأنترنت** ، دار المطبوعات الجامعية الأسكندرية ، 2009.
3. دردور نسيم: **الجرائم المعلوماتية على ضوء القانون الجزائري والمقارن** –رسالة لنيل شهادة الماجستير – كلية الحقوق – جامعة منتوري قسنطينة- 2012 –2013، ص 05.
4. عبد الفتاح بيومي حجازي ، **الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت** ، بدون ناشر ، طبعة مزيدة ومنقحة ، 2009 ، ص7-8 .
5. عبد الفتاح مراد، **دور الكمبيوتر في مجال ارتكاب الجرائم الإلكترونية**، دار الكتب والوثائق المصرية،2005 ،ص 43
6. نفس المرجع السابق،ص65
7. نهلا عبد القادر عبد المومن، **الجرائم المعلوماتية**، دار الثقافة للنشر و التوزيع، ط1،عمان،2008،ص50
8. هشام محمد رستم، **الجرائم المعلوماتية**، أصول التحقيق الجنائي الفني مجلة الأمن والقانون، دبي العدد(2)،1999 ، ص،24.
9. محمد عبد الرحيم سلطان العلماء،**جرائم الانترنت و الإحتساب عليها**، مؤتمر القانون و الكمبيوتر و النترنت ،جامعة الإمارت العربية المتحدة،1-3 ماي 2000،المجلد 3،ط2004،3،ص877.
10. بد الفتاح مراد، **شرح جرائم الكمبيوتر والأنترنت**، دار الكتب والوثائق المصرية، ص2 4
11. ذياب موسى المديانة،**الجرائم الإلكترونية المفهوم و الأسباب**،الملتقى العلمي الجرائم المستحدثة في ظل التغيرات و التحولات الإقليمية و الدولية، الأردن ،2-2014/09/4
12. صغير يوسف،**الجريمة المرتكبة عبر الانترنت**،مذكره ماجيستر في القانون الدولي للاعمال ،جامعة تيزي وزو2013 ص 45-47

مليار دولار خسائر الاقتصاد العالمي من 870 http://www.alhadath.ps/article/34. **13**
الجريمة المنظمة126/ 2016-03-05consulte le 28/05/2017

14 .خالد ممدوح العزي،**جرائم المالية الإلكترونية /الجرائم المصرفية نموذجا**،أعمال أعمال مؤتمر الجرائم الإلكترونية المنعقد في طرابلس/ لبنان، يومي 24-25|03|2017، ص 137

15 .جورج فهيم ،الجريمة الإلكترونية تكبد الاقتصاد العالمي تريليون دولار سنوياً . دبي 16 - نوفمبر, 2015 http://site.alroeya.ae/2015/11/16/292547 consulte le 25/05/2017

16..ليان عوده، لجرائم الإلكترونية أبرز مخاطر الثورة الصناعية الرابعة 18 يناير على الموقع http://www.alarabiya.net/ar/aswaq/world-economic-forum/2017/01/18 2017 consulté le 25/05/2017

17.http://www.alarabiya.net/ar/technology/2017/05/20 consulté le 24/05/2017

18. http://rawabetcenter.com Consulte le 24/05/2017.

19.عملة الكترونية تمكن مقارنتها بالعملات الأخرى مثل الدولار أو اليورو، مع وجود عدة فوارق أساسية، من أبرزها أن هذه العملة تتداول عبر الإنترنت فقط من دون وجود فيزيائي لها، وتختلف عن العملات التقليدية بعدم وجود هيئة تنظيمية مركزية تقف خلفها، ولكن يمكن استخدامها كأي عملة أخرى للشراء عبر الإنترنت، أو تحويلها إلى العملات التقليدية.

20 .اللجنة الإقتصادية و الإجتماعية لغربي أسيا،ورشة عمل السياسات بشأن السلامة السيبرانية ومكافحة الجريمة السيبرانية في المنطقة العربية،15 افريل 2015 ،نيويورك، E/ESCWA/TDD/2015/1

21.اللجنة الإقتصادية و الإجتماعية لغربي أسيا ،ورشة عمل حول التشريعات السيبرانية و تطبيقها في منطقة الإسكوا ،بيروت 15-16 ديسمبر 2008،المجلس الإقتصادي و الإجتماعي التابع للأمم المتحدة رقم E/ESCWA/ICTD/2009/1

22. The United Nations Economic and Social Commission for West Asia

23.غازي عبد الرحمن هيان الرشيد،**الحماية القانونية من جرائم المعلوماتية (الحاسب و الانترنت)**، أطروحة لنيل درجة الدكتوراة في القانون ،الجامعة الإسلامية لبنان،كلية الحقوق ،2004،ص179-180

24.دليل البلدان النامية ،فهم الجريمة السيبريانية،شعبة تطبيقات تكنولوجيا المعلومات و الإتصالات و الأمن السيبرياني،دائرة السياسات و الإستراتيجيات ،قطاع تنمية الإتصالات الصادر عن الإتحاد الدولي للإتصالات ،أفريل 2009،ص94.

25. Schjolberg and Hubbard, «**Harmonizing National Legal Approaches on Cybercrime**», 2005, page 5. available at: http://www.itu.int

26 .قداري إيمان، **مكافحة الجرائم المعلوماتية في القانون الدولي**،مذكره ماجيستر،جامعة سيدي بلعباس،كلية الحقوق، 2014،ص1.

27.إسراء جبريل رشاد مرعي، الجرائم الإلكترونية " الأهداف – الأسباب – طرق الجريمة ومعالجتها http://democraticac.de/?p=35426 consulte 29/05/2017