University of Benghazi
Faculty of Education Al marj
Global Libyan Journal

جامعة بنغازي
كلية التربية المرج
المجلة الليبية العالمية

العدد الثاني والثلاثون – 30/ نوفمبر (2017)

نظرة عامة عن الجريمة الإلكترونية في الفضاء السيبراني

أ. يوسف إسماعيل يوسف مانيطه

(محاضر مساعد بقسم الحاسوب ، جامعة بنغازي ، كلية الآداب والعلوم سلوق)

نظرة عامة عن الجريمة الإلكترونية في الفضاء السيبراني

Abstract

The tremendous development of information technology over the past two decades The so-called cyberspace, a more comprehensive term than the Internet, was born today, providing opportunities for all people to access the information they want in all areas from and to anywhere in the world.

Due to the increase in the number of Internet users around the world, and the greater the use of technology, the greater the crime of the Internet.

Cybercrime is committed by members of young age groups with good education.

Cybercrime indicates that illegal acts are carried out by computer either as a tool or a target or both, and cybersecurity refers to a computer-based mechanism to protect equipment, information and services from unauthorized and unauthorized access.

The rules and regulations governing cyberspace indicate that there are cells of cybercrime around the world and cybercrime cases are increasing and the perpetrators are more difficult to prosecute.

Changes in technology used in cyberspace and cyberspace are very rapid and there is no strong legal legislation that makes cyber activities legal.

Introduction

Every human being is affected by information technology, the Internet is being used to improve his life, and because of the increased use of technology, cybercrime has increased and has covered all forms of crime related to computer networks.

Cybercrime is on the rise and criminals are conducting several attacks around the world, highly educated criminals and experts with a deep knowledge of information technology. There are many cybercrime such as password piracy, transferring money from a victim account to other accounts and other crimes. Some rules and regulations governing cyberspace which the legislator must include in rules for dealing with cybercrime, and the severe punishment of criminals who violate laws, these laws apply to all violators both at home and abroad and Wei This request global cooperation. [2]

Internet crime has a negative impact on individuals and institutions as well as States and caused many losses, for example: physical, security, social and with the increasing use of computers and information systems, the pace of electronic financial transactions among individuals and institutions around the world has increased; It was necessary to highlight the negative effects of electronic transactions and how to address them, represented in the protection of computer equipment and resources and information is not authorized access or disclosure.

Knowledge of legislation on cybercrime and cybercrime is an urgent need for people who deal with computer networks and the Internet to have a secure world without fear of illegal acts in cyberspace. [1]

الخلاصة

التطور الهائل الذي طرأ على تكنولوجيا المعلومات خلال العقدين السابقين ولد ما يسمى اليوم الفضاء السيبراني وهو مصطلح أشمل من الإنترنت حيث وفر فرصا لجميع الناس للوصول إلى معلومات التي يريدونها في جميع المجالات من وإلى أي مكان في العالم .

نظرا لزيادة عدد مستخدمي الانترنت عبر العالم ، وكلما زاد استخدام التكنولوجيا تزايد معها جرائم الإنترنت.

ترتكب الجرائم عبر الفضاء السيبراني من قبل أفراد ذوي فئات عمرية شبابية ، يتمتعون بتعليم جيد .

وتشير الجريمة السيبرانية إلى أن الأفعال غير المشروعة تتم بواسطة الحاسوب إما أداة أو هدفا أو كليهما ، كما يشير الأمن السيبراني إلى الآلية التي تعتمد على الحاسوب لحماية المعدات والمعلومات والخدمات من الوصول غير القانوني وغير المصرح به .

تشير القواعد والأنظمة التي تحكم الفضاء السيبراني إلى أن هناك خلايا للجرائم السيبرانية في جميع أنحاء العالم و قضايا الجريمة السيبرانية في تزايد مستمر وتزداد صعوبة ملاحقة مرتكبيها .

التغيرات التي تطرأ على التكنولوجيا المستخدمة في الإنترنت والفضاء السيبراني سريعة جدا ولا توجد تشريعات قانونية محكمة تجعل الأنشطة السيبرانية قانونية.

المقدمة

يتأثر كل إنسان بتكنولوجيا المعلومات ، ويتم استخدام الإنترنت لتحسين حياته ، ونظرا لزيادة استخدام التكنولوجيا ، ازدادت معها الجريمة الإلكترونية وأصبحت تغطي جميع أشكال الجريمة المتصلة بشبكات الحاسوب.

الجريمة السيبرانية في تزايد والمجرمين يجرون عدة هجمات في جميع أنحاء العالم ، المجرمون ذوو تعليم عالي وخبراء لديهم معرفة عميقة بتكنولوجيا المعلومات ، وهناك العديد من الجرائم السيبرانية مثل قرصنة كلمة المرور ، نقل الأموال من حساب ضحية إلى حسابات أخرى وغيرها من الجرائم ، ولمعالجتها هناك حاجة لتنفيذ بعض القواعد واللوائح التي تحكم الفضاء السيبراني والتي يجب على المشرع تضمينها في قواعد للتعامل مع الجرائم السيبرانية ، وإنزال العقوبة الشديدة على المجرمين الذين ينتهكون القوانين ، وهذه القوانين تطبق على جميع المنتهكين سواء في الداخل أو في الخارج ويتطلب هذا الأمر تعاونا عالميا. [2]

جرائم الأنترنت لها آثار سلبية على الأفراد والمؤسسات وكذلك الدول وسببت كثيرا من الخسائر منها على سبيل المثال: مادية ، أمنية ، اجتماعية ومع تزايد استعمال أجهزة الحاسوب ونظم المعلومات ، ازدادت معها وتيرة التداولات المالية الإلكترونية بين

الأفراد وكذلك المؤسسات في جميع أنحاء العالم ; عليه كان لابد من تسليط الضوء على الآثار السلبية للتداولات الإلكترونية وكيفية معالجتها ، ممثلة في حماية معدات الحواسيب ومواردها والمعلومات غير المصرح الوصول إليها أو إفشائها.

معرفة التشريعات المتعلقة بالجرائم الإلكترونية والجرائم في الفضاء السيبراني حاجة ملحة للأشخاص الذين يتعاملون مع شبكات الحاسوب والأنترنت لنحصل على عالم آمن بدون وجود خوف من الأعمال غير المشروعة في الفضاء السيبراني . [1]

1. أنواع الجريمة السيبرانية :

1.1 القرصنة

يستخدم فيها المجرم مجموعة متنوعة من البرامج للدخول إلى حاسوب الضحية عن بعد وبدون علمه ، وتقتضي هذه الجريمة أن يتم اختراق جهاز حاسوب الضحية للوصول إلى بياناته الشخصية أو بيانات مهمة موجودة على جهازه . [1]

1.2 السرقة

تحدث هذه الجريمة عندما ينتهك شخص ما حقوق الطبع والنشر بتنزيل ملفات ومنها مثلا: ملفات الكتب الإلكترونية ، الموسيقى ، الأفلام ، الألعاب، والبرامج من مواقع شركات المبيعات على شبكة المعلومات الدولية دون إذن مسبق منها . [3]

1.3 المطاردة السيبرانية

هو أحد أنواع التحرش عبر الإنترنت يستخدم فيه المجرم وابلا من رسائل إلكترونية عبر البريد الإلكتروني أو بالدخول إلى غرف الدردشة الموجود بها الضحية ويقوم بمضايقته. [3]

1.4 هجوم الحرمان من الخدمة

يتم في هذا النوع من الهجمات استهداف صندوق البريد الإلكتروني للضحية بعدد كبير من رسائل البريد المزعجة التي تحرمه من الخدمات المتوفرة ، وتجعل موارد الشبكة غير متاحة لاستخدامها. [7]

1.5 ناشروا الفيروسات

أفراد يقومون بنشر بعض البرامج الخبيثة التي تُعلق نفسها على غيرها من البرمجيات.

البرامج الخبيثة مثل: الفيروس ، الدودة، حصان طروادة ، القنبلة الموقوتة ، القنابل المنطقية ، تتسبب تلف الملفات والبيانات الموجودة في جهاز الضحية ، أو التحكم بجهازه وانتحال شخصيته والانتقال إلى أجهزة أخرى وإدارة أعمال غير مشروعة باسمه[7] .

1.6 قرصنة البرمجيات

هي عملية يتم فيها سرقة البرمجيات من خلال النسخ غير القانوني للبرامج الأصلية للشركات والمؤسسات وإعادة توزيعها.

يمكن القيام بذلك عن طريق نسخ المستخدم النهائي ، أو تحميل القرص الثابت ، أو تنزيل غير القانوني من الإنترنت. [1]

2. أنواع القراصنة :

مجرمو الإنترنت هم أفراد ذوي تحصيل علمي عال مثل : طلاب الدراسات العليا في علوم الحاسوب ونظم المعلومات ، المهندسين ، الذين يحاولون الوصول إلى أنظمة معلومات أخرى بطرق غير شرعية ، و يمكن تصنيفهم على حسب سلوكهم المتبع في الاختراق إلى : [9]

2.1 الهواه

أشخاص يفتقرون إلى الخبرة الفنية العالية ، ولديهم فقط القدرة على اختراق الأنظمة ضعيفة الحماية ولا يستطيعون التسبب في أي أضرار جسيمة للضحايا . [1]

2.2 المحتالون

هم الأشخاص الذين يرسلون رسائل بريد إلكترونية وهمية للضحايا مثل : رسائل خصم مالية ، جوائز اليانصيب الاحتيالية ، ومن خلال الإحصائيات تسبب هؤلاء المحتالون سرقة أموال أعداد كبيرة من الضحايا خلال السنوات السابقة .[1].

2.3 مجموعات الهاكر

يعملون في الخفاء ويخترقون أجهزة الحاسوب دون أي أسباب إجرامية ، يتم تكليفهم من قبل المنظمات والوكالات الحكومية لاختبار الثغرات الأمنية ونقاط ضعف الأنظمة الإلكترونية. [1]

2.4 الصيادون

هم أشخاص يحتالون غالبا على الضحية بتوجيهه إلى موقع إلكتروني شبيه بالموقع الأصلي الذي يرغب الضحية في الدخول إليه بغية الحصول على أرقام بطاقة الائتمان ، وكلمات السر أو غيرها من البيانات الشخصية ، وعادة يستخدمون البريد الإلكتروني في الخداع أو الرسائل الفورية. [1]

2.5 المجموعات السياسية ، التجارية

مجموعات تدار من قبل مؤسسات لحكومات ليست لها اهتمام بالمكاسب المالية ، تقوم بتطوير برمجيات خبيثة لأغراض سياسية أو تجارية ، مثل : الوصول إلى معلومات تخص خصوما سياسيين في بلد ما ، أو مثل : الهجمات التي شنت على الحواسيب الموجودة في مراكز السيطرة على المرافق النووية الإيرانية. [1]

2.6 المطلعون

يعتبر هؤلاء المهاجمون أشدهم خطرا على المؤسسات لأنهم متواجدون داخلها ، ولديهم معرفة بجميع تفاصيل المنظمة ولهم قدرة على اختراق أمنها وإفساد أنظمتها. [1]

2.7 القراصنة ذوي القبعات البيضاء

مهمتهم هي تأمين أنظمة المعلومات و كشف نقاط الضعف في أنظمة الحماية بالمؤسسات المستهدفة وهم غالبا يعملون في شركات أمن المعلومات. [1]

2.8 القراصنة ذوي القبعات السوداء

أشخاص يضرون بأمن نظم الحاسوب بالمؤسسات المستهدفة ويدخلون إليها بدون أذن مسبق بنية تدمير البيانات أو سرقتها أو تزويرها أو استغلال النظم لتحقيق مكاسب مالية خاصة . [1]

2.9 القراصنة ذوي القبعات الرمادية

يشار إليهم بأنهم محترفون يعملون أحيانا بطرق قانونية ليس لهم نية خبيثة أو مكاسب شخصية وهم هجين بين القبعات البيضاء والسوداء ، وعادة ما يستخدمون هذه الطرق خلال تجاربهم في مجال عملهم . [1]

3. آثار الجريمة السيبرانية على المجتمع :

إن جرائم الأنترنت لها آثار سلبية على الأفراد والمؤسسات وكذلك الدول وسببت كثيرا من الخسائر سواء مادية أو أمنية أو اجتماعية وغيرها ومع تزايد استعمال أجهزة الحاسوب ونظم المعلومات في جميع المؤسسات ودخول التداول الإلكتروني لأموال بها حتى مع الأفراد وتنوع أثارها السلبية لذى تم تصنيف هذه الآثار إلى عدة أصناف :

3.1 الجريمة الإلكترونية ضد الحكومة

يعملون في مثل هذه الجرائم على اختراق قواعد بيانات الحكومة لاستخدام معلومات حساسة كأن يخترقون أنظمة معلومات وزارة الداخلية مثلا ويطلق على هذا السلوك "الإرهاب السيبراني" ، وتستخدم الجريمة السيبرانية لتقويض فعالية الحكومة وبالتالي تقليل إيمان المواطنين بأعمالها وتوجيه الرأي العام ضدها. [10]

3.2 الجريمة السيبرانية ضد الممتلكات

تشمل البرامج الضارة عبر مواقع الأنترنت أو البريد الإلكتروني أو مواقع الدردشات التي من خلالها تمكنهم مثلا من سرقة معلومات من حاسوب الضحية ، أو سرقة النطاق الترددي بغية الوصول غير المصرح للإنترنت . [10]

3.3 الجريمة الإلكترونية ضد الأعمال

تحدث عندما يخترق المجرمون مثلا : أنظمة الحاسوب ويحصلون على بيانات سرية للمؤسسة تشمل أرقام الحسابات المصرفية ويقومون بانتحال صفة مسئول المؤسسة للاستلاء على أموالها ونقلها إلى حساباتهم مما يجعل المؤسسة مفلسة . [10]

3.4 الجريمة الإلكترونية ضد الأفراد

يقوم المجرم باستدراج الضحية إلى موقع على الأنترنت شبيه بالموقع الذي يريد الدخول إليه ويشعره بالأمان ويتحصل بعد ذلك على معلوماته الشخصية مثل بطاقة الائتمان المصرفي. [10]

4. التشريعات الدولية للفضاء السيبراني :

القانون السيبراني أو قانون الإنترنت هو المصطلح الذي يعنى بالمسائل القانونية المتعلقة باستخدام الإنترنت" .

قانون الحاسوب" هو مصطلح يميل إلى ربط مسائل تشمل الإنترنت وقوانين براءات الاختراع وحق المؤلف الخاصة بجوانب تكنولوجيا الحاسوب والبرمجيات ، ويشمل الوصول إلى الإنترنت واستخدامه ، والخصوصية ، وحرية التعبير. الهدف من هذه القوانين هو تقديم الاعتراف القانوني والسجلات الإلكترونية والمعاملات التي تتم عن طريق تبادل البيانات الرقمية وتعالج مسائل تتعلق بالأمن ، وحقوق الأفراد والمؤسسات نتيجة هذه التداولات وهي أمور بالغة الأهمية لإنجاح المعاملات الإلكترونية وهي معتمدة في دول كثيرة منها عالميا مثلا : الولايات المتحدة ، فرنسا ، الهند ، وعربيا مثلا : الإمارات العربية المتحدة ، الأردن ، مصر ، الجزائر وقد أعطت هذه القوانين تعريفا له مفهوم التوقيعات الرقمية الآمنة.

هذه القوانين قد تكون غامضة لغالبية الأفراد والمؤسسات المستخدمة لتكنولوجيا المعلومات والأنترنت الأمر الذي يجعلهم يجهلون كيفية التعامل مع الجرائم السيبرانية .[10]

يجب على الحكومات أن تشجع البحث في مجال الجريمة السيبرانية ليتمكن الأفراد من الحصول على المعرفة الكاملة حول الجرائم الإلكترونية بحيث لا يقعوا بسهولة في فخاخ مجرمي الإنترنت.

يتعين على الأفراد إبلاغ الهيئات المعنية بمكافحة الجرائم الإلكترونية وتقديم المعلومات التي تفيد تلك الجهات من إنفاذ القوانين الكفيلة بردع وملاحقة مجرمي الإنترنت في الداخل والخارج.

4. الأمن السيبراني :

يشير الأمن السيبراني إلى التقنيات والعمليات المعدة لحماية أجهزة الحاسوب والشبكات والبيانات الخاص بالمؤسسات من الأشخاص غير المصرح لهم للوصول إلى تلك الأجهزة والبيانات ، ومعالجة مواطن الضعف والهجمات التي تتعرض لها تلك المؤسسات عبر الإنترنت من قبل مجرمي الإنترنت.

ISO27001 هو أحد المعايير الدولية الخاصة بالأمن السيبراني الذي يوفر نموذجا لإنشاء، وتشغيل، ورصد، ومراجعة، والحفاظ على أمن المعلومات ، وتحسين نظام إدارة أمن المعلومات .

الاتحاد الدولي للاتصالات هو أحد أهم المؤسسات الدولية التي يقع على عاتقها بناء الثقة والأمن في استخدام المعلومات وتكنولوجيا الاتصالات وخصوصا بعد القمة العالمية لمجتمع المعلومات ومؤتمر المندوبين المفوضين للاتحاد لعام 2010. [6]

5. الوقاية من الجريمة السيبرانية :

تأكد من تركيب برامج مضادة للفيروسات وبرامج مضادة لعمليات التسلل وبرامج الجدار الناري ، أن تكوين كلمات مرور قوية لأنظمتك وقواعد بياناتك ، وفي مواقع التواصل الاجتماعي ، والشبكات ، و صناديق البريد الإلكتروني وما إلى ذلك. لا تستجيب لرسائل البريد الإلكتروني من مصادر غير معروفة وخصوصا في حالة طلبهم منك الولوج إلى مواقعهم على شبكة المعلومات الدولية وطلب تفاصيل عن بطاقة الائتمان والمعلومات الشخصية وما إلى ذلك.

6. معايير الأمن السيبراني :

ISO_IEC 27001 6.1

هو أفضل المعايير الدولية الخاصة بنظم إدارة أمن المعلومات (**ISMS**) وهو مجموعة من العناصر المترابطة التي تستخدمها المؤسسات في إدارة ومراقبة مخاطر أمن المعلومات تتمثل في الحماية ، المحافظة على سرية وسلامة وتوافر المعلومات . [4]

ISO/IEC 27032 6.2

معيار دولي خاص بالأمن السيبراني . يشمل المبادئ التوجيهية بوضع الأطر العامة لحماية نظم المعلومات خارج حدود المؤسسة وأيضا ضد الجرائم السيبرانية التي تنشأ من الخارج في الفضاء السيبراني . [6]

ISO/IEC 27031 6.3

معيار دولي خاص بتكنولوجيا المعلومات والاتصالات لاستمرارية الأعمال وهذا المعيار يعمل كجسر لضمان استمرارية الأعمال العامة بعد التصدي لأحداث الاختراق ، مما يجعل الفضاء السيبراني أكثر مرونة . [5]

ISO/IEC 22301 6.4

معيار دولي خاص بأنظمة استمرارية إدارة الأعمال التجارية ، هذا المعيار لا يركز فقط على الخروج من الكوارث ، ولكن أيضا الحفاظ على إمكانية الوصول لأنظمة أمن المعلومات، وهو أمر بالغ الأهمية عند استمرار عمل نظم المعلومات. [8]

7. الخلاصة

تزداد تكنولوجية المعلومات يوما بعد يوم ويزداد معها استخدم فضاء الإنترنت في جميع أنحاء العالم ، مما يمكن المجرمين من استخدام هذه الوسائط لاختراق الأنظمة الإلكترونية باستخدام خبراتهم للوصول إلى خصوصيات الأفراد والمؤسسات مما يعرض أمنها للخطر والابتزاز وسرقة الأموال و المعلومات .

إن الجريمة السيبرانية تتمثل في الأفعال غير القانونية باستخدام الحاسوب كأداة أو هدف أو كليهما .

الجريمة السيبرانية خطر يتعين التصدي له بفعالية ، من خلال تثقيف الأفراد عن الفضاء السيبراني ، ومختلف أشكال الجرائم السيبرانية والتدابير الوقائية الكفيلة بتقليل خطر الوقوع في فخاخ الجريمة الإلكترونية .

قانون تكنولوجيا المعلومات هو التعبير عن جميع القوانين والبروتكولات القائمة من قبل المؤسسات والحكومات عبر العالم الكفيلة بحماية مستخدمي نظم المعلومات من الاختراق ومعاقبة كل من تسول له نفسه انتهاك خصوصيات الأفراد والمؤسسات .

يجب على المشرع في جميع البلدان سن القوانين الخاصة بالجرائم السبرانية والانضمام إلى المعاهدات والقوانين الدولية المبرمة لمكافحة الجرائم الإلكترونية ، وتثقيف الأفراد والمؤسسات الذين يعملون بأنظمة الحاسوب ، وتكنولوجيا المعلومات والاتصالات بدور القانون السيبراني في حمايتهم.

المراجع :

[1] **Allen Harper and others** (2011) , Gray Hat Hacking The Ethical Hacker's Handbook , Third Edition , McGraw-Hill Companies, New York , Pages 3-47,413-421

[2] En.wikipedia.org/wiki/Cyber_security_standards. Last visit date 01/08/2017.

[3] Hassan A. B., Lass D. F. and Makinde J. (2012). Cybercrime in Nigeria: Causes, Effects and the
Way out. ARPN Journal of Science and Technology. 2(7) , pages 626-628 , 631.

[4] Information security management , ISO_IEC 27001 available on https://www.iso.org . Last visit date 12/08/2017.

[5] Information technology , Security techniques , ISO_IEC 27031 2011 available on https://www.iso.org . Last visit date 15/08/2017.

[6] Information technology - Security techniques , ISO_IEC 27032 2012 available on https://www.iso.org . Last visit date 15/08/2017.

[7] Skinner, W.F. & Fream, A.M. (1997). A social learning theory analysis of computer crime among college students. Journal of Research in Crime and Delinquency, 34, 499-508.

[8] Societal security , Business continuity management systems Requirements , ISO 22301 2012 available on https://www.iso.org . Last visit date 15/08/2017.

[9] Young, R., Zhang, L., & Prybutok, V. R. (2007). Hacking into the minds of hackers. Information Systems Management, 24, pages 271-278

[10] Walden, I. (2004). Harmonising Computer Crime Laws in Europe. European Journal of Crime, Criminal Law and Criminal Justice, 12(4), pages 325-332.3