الجريمة السبرانية مفهومها وسبل الوقاية منها

Cyber crime concept and ways to prevent it

علي قويدري [1] ، أمال العايش [2]

Ali kouidri [1], Amel laiche [2]

[1] جامعة عمار ثليجي الأغواط (الجزائر)، ali.kouidri@lagh-univ.dz

[2] جامعة عمار ثليجي الأغواط (الجزائر)، amel.amoula81@yahoo.com

تاريخ الاستلام: 2021/09/06 تاريخ القبول: 2021/10/03 تاريخ النشر: 2022/01/01

ملخص: تعتبر وسائل الإتصال الحديثة من أهم مميزات العصر الحالي عصر التكنولوجيا والرقمية، حيث سهلت على البشرية جمعاء كثير من المعاملات حيث قربت البعيد واختصرت الأوقات ويسرت التواصل بينهم، ولكن البعض استغل هذه التكنلووجيا لأغراض إجرامية أو ما يعرف بالجرائم الإلكترونية أو السبرانية. وتشهد التقنية والتكنولوجيا تطورات كثيرة واستحداث لأمور جديدة ،هذا الأمر ينذر بتطور أدوات وسبل الجريمة الإلكترونية بشكل أكثر تعقيدا أو أشد ضررا من قبل، الأمر الذي يلزم الدول لتطوير آليات مكافحة هذه الجرائم. وسنتطرق في هذه المقالة إلى مفهوم الجريمة السبيرانية ، والأسباب الإجتماعية والنفسية لارتكاب هذه الجرائم، وسبل مكافحتها والوقاية منها.

الكلمات المفتاحية: السبيرانية – الجريمة– الإلكترونية– الأنترنيت.

Abstract: Modern means of communication are considered one of the most important features of the current era, the era of technology and digital, as it facilitated many transactions for all of humanity, as it brought the distant and shortened the times and facilitated communication between them, but some took advantage of this technology for criminal purposes or what is known as electronic or cyber crimes. Technology and technology are witnessing many developments and the development of new things, and this portends the development of cybercrime tools and methods in a more complex or more harmful way than before, which obliges countries to develop mechanisms to combat these crimes. In this article, we will discuss the concept of cybercrime, the social and psychological reasons for perpetrating these crimes, and ways to combat and prevent them.

Keywords: cyber - crime - electronic - the Internet.

المؤلف المرسل: علي قويدري، **الإيميل:** ali.kouidri@lagh-univ.dz

1-مقدمة

تميز القرن 21 باستخدام المعلومات، وعلى مدى السنوات القليلة الماضية توسعت الإنترنت أضعافا مضاعفة .حاليا ، حوالي هناك 820 مليون شخص يستخدمون الإنترنت ، لقد وفرت السهولة النسبية لاستخدام الإنترنت، والحصول على الإنترنت على نحو متزايد أكثر للأنترنت بأسعار معقولة والحصول على أجهزة الكمبيوتر مع أجهزة المودم فائقة السرعة، كل ذلك مكن الناس من التواصل وتكوين الصداقات الجديدة، والتجارة ، والترفيه ، والتعلم، والقيام بأعمال تجارية، ودفع الفواتير عبر الإنترنت .وخلقت شبكة ويب العالمية ما يسمى العالم الافتراضي أو الفضاء الإلكتروني ، والذي يعرف بأنه" مكان لأجل غير مسمى حيث يتفاعل الأفراد والتجمعات. **(Britz, 2004)** .

إن المعلومات والبيانات مثلها مثل أية سلعة ذات قيمة مادية عالية عرضة للجريمة بما في ذلك الاحتيال والسرقة والتعدي والتخريب..ألخ .وتزداد جرائم المعلومات يومياً، وأصبحت محط حديث وسائل الإعلام والباحثين والعلماء. عندما سئل ويلي سوتن(Sutton) لماذا سطي على البنك أجاب" لأن المال ..موجود هناك"، والمال اليوم هو المعلومات، ولقد تعلم المجرمون اليوم مكان وجود المال ويمكنهم سرقة كميات بمخاطرة أقل .

ولقد تأزمت العلاقات بين الدول بسبب سرقة المعلومات أسرار عسكرية تتعلق بتقنيات متقدمة والأمثلة على ذلك بين الولايات المتحدة والصين، وكندا، والصين. لقد أصبحت الجريمة الإلكترونية وجرائم الحاسوب ونظمها، بلا حدود، وهي عالمية، التحقيق فيها والحكم عليها عملية معقدة .

وترتكب هذه الجرائم من قبل الأفراد أكثر مما ترتكب من قبل الأفراد أكثر مما ترتكب من قبل محترفي الحاسب وشبكات المعلومات .كما يمكن أن ترتكب من مراكز البحوث، ومن الأكاديميين، ومن مديرين يبحثون عن الثراء أو السلطة، أو من قبل مؤسسات تبحث عن معلومات عن منافسيها، أو من وسائل إعلام تبحث عن معلومات أو أخبار أو من قبل

حكومات تبحث عن معلومات تجارية، أو جريمة منظمة تبحث عن ملفات موثوقة **(البداينة، 1999)**.

وتعد الجريمة السيبرانية والأمن السبيراني من القضايا التي يمكن بالكاد الفصل فيها في بيئة موصلة بينيا، ومما يؤكد ذلك قرار الجمعية العامة للأمم المتحدة لعام 2010 شأن الأمن السيبراني الذي يتناول الجريمة السيبرانية باعتبارها أحد التحديات الكبرى.

وستناول في هذه المداخلة عن مفهوم الجريمة السيبرانية من خلال عدة تعريفات وما هي الأسباب التي تؤدي إلى مستعملي الأنترنيت والحواسيب لإرتكاب هذه الجرائم الإلكترونية، وما هي أفضل السبل والوقاية للحد من هذه الجرائم.

2-ما هي الجريمة الإلكترونية (السيبرانية)؟

لا يوجد إجماع على تعريف الجريمة الإلكترونية من حيث كيف تُعرف أو ما هي الجرائم التي تتضمنها الجريمة الإلكترونية .وكما يقول فان دير هلست و ونيف " هناك غياب لتعريف عام واطار نظري متسق في هذا الحقل من الجريمة ...وفي أغلب الأحيان تستخدم مصطلحات الافتراضية والحاسوب والإلكترونية والرقمية وكلها تعكس فجوات مهمة في التعريف **(Van der Hulst & Neve, 2008,)**

ويتراوح تعريف الجريمة الإلكترونية بين الجرائم التي ترتكب بواسطة الحاسوب إلى الجرائم التي ترتكب بأي نوع من المعدات الرقمية، وتعريف الجرائم الإلكترونية باختصار على أنها الجرائم التي ترتكب .باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال.**(PAC, 2008,)**.

تتكون الجريمة الإلكترونية أو الافتراضية (cyber crimes) من مقطعين هما الجريمة (crime)والإلكترونية (cyber).

ويستخدم مصطلح الإلكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات .

أما الجريمة فهي السلوكيات والأفعال الخارجة على القانون .والجرائم الإلكترونية هي "المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء

سمعة الضحية أو أذى مادي أو عقلي للضحية مباشر أو غير مباشر باستخدام شبكات الاتصالات مثل الإنترنت مثل غرف الدردشة، والبريد الإلكتروني والموبايل **(Halder & Taishankar,2011)**,

ويمكن تعريفها بأنها كل سلوك غير قانوني يتم باستخدام الأجهزة الإلكترونية، ينتج عنها حصول المجرم على فوائد مادية أو معنوية مع تحميل الضحية خسارة مقابلة وغالبا ما يكون هدف هذه الجرائم هو القرصنة من أجل سرقة أو إتلاف المعلومات.

ولقد عرفها ليوكفيلدت وفنسترا وستول (Leukfeldt, Veenstra & Stol,2013)كمصطلح عام لجميع أشكال الجريمة التي تلعب فيها تكنولوجيا المعلومات والاتصالات دورا أساسيا . وهنا تقع الكثير من الجرائم ضمن هذا التعريف.

لقد قدم ليوكفيلدت وآخرون((Leukfeldt et al,2012) قائمة بـ 28 جريمة بدءا من قرصنة الأنظمة الرقمية، وتثبيت برامج التجسس للاحتيال باستخدام الخدمات المصرفية عبر الإنترنت والمطاردة الافتراضية . **(Leukfeldt, Veenstra & Stol,2013)**

-التعريف الدولي للجريمة الإلكترونية (السيبرانية)

تعتمد "تعريفات" للجريمة الإلكترونية في الغالب على الغرض من استخدام المصطلح هناك عدد محدود من الأفعال ضد السرية والنزاهة وتوافر بيانات الكمبيوتر أو أنظمته تمثل جوهر الجريمة الإلكترونية أعمال متعلقة بالكمبيوتر لتحقيق مكاسب شخصية أو مالية أو ضرر، بما في ذلك أشكال الأفعال المتصلة بجريمة الهوية وجرائم محتويات الكمبيوتر لا تصلح بسهولة إلى الجهود للوصول إلى التعاريف القانونية للمصطلح الكلي.(**اسراء مرعي، 2016)**

-بعض تسميات الجرائم الإلكترونية:

-1جرائم الحاسوب والإنترنت

-2جرائم التقنية العالية

-3الجريمة الإلكترونية

-4الجريمة السايْبِريّة

-5جرائم أصحاب الياقات البيضاء

ويمكن مقارنة بعض نماذج الجريمة التقليدية مع الجريمة الإلكترونية لنرى كيف انتقلت الجريمة من الواقع المادي إلى الواقع الافتراضي

الجريمة التقليدية	الجريمة الإلكترونية
الاحتيال	الاحتيال على الشبكة، الاحتيال بالمزاد الإلكتروني....الخ
السطو	القرصنة على الإنترنت، الحرمان من الخدمة، الفيروسات
جرائم الأطفال الجنسية	استمالة الأطفال على النت، المواقع الإباحية
غسيل الأموال	أنظمة الدفع على الشبكة
السرقة	جرائم الهوية، وسرقة الملكية

(ACC ,2013)

3-أنواع الجرائم الإلكترونية (السيبرانية):

3-1-الجرائم ضد الافراد : وتسمى بجرائم الإنترنت الشخصية تتمثل في سرقة الهوية ومنها البريد الإلكتروني ،أو سرقة الاشتراك في موقع شبكة الإنترنت وانتحال شخصية أخرى بطريقة غير شرعية عبر الإنترنت بهدف الاستفادة من تلك الشخصية أو لإخفاء هوية المجرم لتسهيل عملية الإجرام.

3-2-الجرائم ضد الملكية : تتمثل في نقل برمجيات الضارة المضمنة في بعض البرامج التطبيقية والخدمية أو غيرها، بهدف تدمير الأجهزة أو البرامج المملوكة للشركات أو الأجهزة الحكومية أو البنوك أو حتى الممتلكات الشخصية.

3-3-الجرائم ضد الحكومات : مهاجمة المواقع الرسمية وأنظمة الشبكات الحكومية والتي تستخدم تلك التطبيقات على المستوى المحلي والدولي كالهجمات الإرهابية على شبكة الإنترنت ،وهي تتركز على تدمير البنى التحتية ومهاجمة شبكات الكمبيوتر وغالبا ما يكون هدفها سياسي.

4-أسباب ودوافع الجريمة الإلكترونية:

هناك عدد من الأسباب والدوافع التي يمكن حصرها كأسباب للجريمة الإلكترونية، منها ما يقع على مستوى عالمي، ومنها ما يقع على مستوى مجتمعي، ومنها ما يقع على مستوى فردي أو شخصي .كما أن أسباب الجريمة الإلكترونية تتفاوت وفق نوعها ونوع المستهدف ونوع الجاني ومستوى تنفيذه فردي، مجتمعي ، عالمي.

4-1-أسباب ودوافع الجريمة على المستوى الشخصي:

4-1-1 **البحث عن التقدير**(sake of recognition)

هناك بعض الجرائم الإلكترونية التي يرتكبها شباب طائش وصغار سن، وذلك من باب التحدي، وحب الظهور في الإعلام .وغالباً ما تتوقف هذه الفئة عن مثل هذه السلوكيات في عمر لاحق بعد سن العشرينيات.

4-1-2 الفرصة (Opportunity)

لقد وفرت التقنيات الحديثة والأنترنت فرصاً غير مسبوقة لانتشار الجريمة الإلكترونية ، أنّ الفرصة تنتج الجريمة. وتلعب البيئة وترتيباتها دوراً كبيرا في إنتاج الجريمة. والخروج على قواعد الاجتماعية .فوقت الإنحراف عن قواعد الامتثال ليلا ونهارا وفي أي مكان، وعدم وجود رقابة، كلها عوامل تزيد من فرصة ارتكاب الجريمة الإلكترونية .وقد تشكل المعلومات هدفاً سهل المنال، ويحقق المنفعة السريعة، وبالتالي يمكن سرقتها، أو سرقة محتوياتها .فهي فرصة مربحة، وقليلة المخاطر، واحتمالية الكشف للفاعل فيها ضئيلة . **(Laura Ani, 2011).**

4-1-3 ضبط الذات المنخفض:

تنطلق هذه الدراسة من النظرية العامة في السلوك الطائش، وتؤكد هذه النظرية أن احتمالية انخراط الأفراد في فعل إجرامي تحدث بسبب وجود الفرصة مع توفر سمة شخصية من سمات الضبط الذاتي المنخفض .وقد عرف كل من "جتفردستون وهيرشي" السلوك الطائش بأنّه :كل فعل يقوم على القوّة والخداع لتحقيق الرغبات الذاتية . وبناء على هذا التعريف الذي يستدل على طبيعة السلوك الطائش من خصائص الأشخاص، فإن السلوك الطائش يُعدّ مظهراً من مظاهر الضبط الذاتي المنخفض، وكما في نظرية الضبط الاجتماعي لهيرشي ، فالدوافع لارتكاب السلوك الطائش ليست متغيرة .وذلك لأن كل فرد قد يندفع لتحقيق مصالحه الشخصية بما في ذلك السلوك الطائش .فالسلوك الطائش يُعدّ عملاً سهلاً وقد يحقِق المصالح الخاصة بسرعة مثل (الرشوة،السرقة) ونحوهما من الأعمال الإجرامية التي تتحقق بسرعة وسهولة دون انتظارٍ أو بذل جهد، ولكن الاختلاف بين الأفراد يعود إلى مستوى ضبط الذات، ووجود الفرصة لارتكاب السلوك المنحرف.**(البداينة والرشيد والمهيزع، 2005).**

أظهرت الدراسات أيضا أن ضبط الذات المنخفض والاستعداد لتحمل المخاطر من أجل تحقيق مكاسب قصيرة الأجل، وهذا قد ينطبق على الأفعال التي يمكن إن تسهيل أو تتعزز بواسطة وسائط الاتصالات الإلكترونية والإنترنت. بالإضافة إلى ذلك، يتعرض الأفراد على الإنترنت لنماذج التعلم الإجرامي والأقران قد يكونون أكثر ميلا للإنخراط في الجريمة الإلكترونية. ونظرية التعلم الاجتماعي " نظرية قد يكون لها تطبيق خاص عندما يتعلق الأمر بالجرائم الإلكترونية ، فالمجرمين غالبا ما تحتاجون إلى تعلم تقنيات الكمبيوتر والإجراءات. فالنظرية العامة للجريمة ونظرية التعلم الاجتماعي، تريان إن الأفراد يتصرفون في البيئة الإفتراضية كما يتصرفون في العالم الحقيقي.**(ذياب البداينة، 2014).**

4-1-4 الضغوط العامة (General Strain)

ترجع نظرية الضغوط العامة الإنحراف وخرق القانون إلى دافع ناجم عن قوى البناء الاجتماعي أو استجاباته النفس اجتماعية للحوادث والظروف والتي تعمل كضغوطات أو مقلقات خاصة عندما لا تتاح للأفراد الفرصة لتحقيق أهدافهم المقبولة اجتماعياً وأن مصادر الضغوط لا تتوقف على الإحباط الذي يخبره الفرد عندما تُسد الطرق لتحقيق هدف ما، وإنما يشمل المشاعر السلبية التي تحدث في المواقف الاجتماعية المتنوعة كما قد تلعب العوامل الاجتماعية والاقتصادية أيضا دورا هاما في زيادة الجريمة الإلكترونية.

فالضغط على مؤسسات القطاع الخاص لخفض الإنفاق وخفض مستويات التوظيف يمكن أن يؤدي، على سبيل المثال، إلى تخفيضات في الأمن، وإلى فرص لاستغلال ثغرات وضعف تكنولوجيا المعلومات والاتصالات والشركات. مما يضطر لتوظيف المتعاقدين من الخارج أو المؤقتين، أو يصبح هناك موظفين ساخطين بسبب انخفاض الأجور والخوف من فقدان الوظيفة، والخطر يزداد من الأعمال الإجرامية والنفوذ من قبل منظمة إجرامية. **(UNODC, 2011)**

4-1-5 النشاط الروتيني:

ويمكن تفسير زيادة ضحاي الجريمة الإلكترونية من خلال التغيرات في أنشطة الناس الروتينية في الحياة اليومية. فمع ظهور شبكة الإنترنت فقد تغيرت طريقة الناس التي يتواصلون فيها أو يتفاعلون مع الآخرين في العلاقات الشخصية، والترفيه، والتجارة...الخ . أن التغيرات في أنشطة الناس الروتينية، من مثل استخدام النت وشبكات التفاعل الاجتماعي مثل الفيس بوك، والايميل والمواقع وغيرها قد خلقت فرصاً للجناة المتحفزين مع وجود أهداف قيمة وسهلة في الحيز الفضائي مع غياب الحراسة .يرى "كوهين و فيلسون" إلى أنه من المرجح أن تحدث الجريمة عندما تتلاقى ثلاثة عوامل هي :الجاني المتحفز والهدف المناسب وغياب الحراسة أنه لا بد من توافر هذه العوامل الثلاثة من أجل أن تحدث الجريمة، وعدم وجود واحد من هذه العوامل هو كافي لمنع حدوث ناجح لإكمال الاتصال المباشر في جريمة السلب ويعطي اهتمام إلى التقارب في الزمان والمكان، وإن هذا التلاقي يمكن أن يؤدي إلى زيادة كبيرة في معدلات الجريمة من دون أي تغيير في " الحالة الظرفية "التي تحفز

المجرمين، المبدأ الأساسي هو أن التغيرات الهيكلية في النشاط الروتيني تؤثر على التقارب في العناصر الثلاثة من الناحية النظرية، وبالتالي تؤثر على معدل الجريمة **(Meithe, Mark, and Scott, 1987)**.

4-2- أسباب ودوافع الجريمة السبيرانية على المستوى المجتمعي:

4-2-1 التحضر(Urbanization).

يعد التحضر أحد أسباب الجريمة الإلكترونية عامة، حيث الهجرة الكبيرة من الريف إلى المدينة وإلى المناطق الحضرية والمدن الكبيرة .وعادة ما يهاجر الشباب غير المتمكنين من مواجهة متطلبات الحياة الحضرية، باهضه التكاليف، والتي تتطلب مهارات عالية أحيانا . مما يجعل شرائح كبيرة من المهاجرين غير قادرين على تلبية متطلبات الحياة الحضرية، مما يجعلهم يعيشون في مدن الصفيح والأحياء الطرفية والهامشية .وكنتيجة يجد الناس أنفسهم في تنافس غير قادرين على مجاراته، مما يجعلهم يلتفتون إلى الاستثمار في الجريمة الإلكترونية حيث لا تتطلب راس مال كبير والتي تعرف" أولا الياهو"

وكما يرى ميك (Meke) فأن التحضر سبب رئيس للجرائم الإلكترونية في نيجيريا، وأن التحضر بدون الجريمة مستحيل، وكنتيجة فان الصفوة بينهم قد وجدوا إن الاستثمار في الجريمة الإلكترونية مربحة. (Meke, 2012)

4-2-2 البطالة(Unemployment).

ترتبط الجريمة الإلكترونية شأنها شأن الجريمة التقليدية بالبطالة والظروف الاقتصادية الصعبة .وتتركز البطالة بين قطاعات كبيرة الشباب .ولذا فان الشباب الذين يملكون المعرفة سيستثمرون ذلك في النشاط الإجرامي الإلكتروني.

4-2-3 الضغوط العامة(Strains).

تعد الضغوط العامة التي يتعرض لها المجتمع من فقر وبطالة وأمية وظروف اقتصادية صعبة عوامل ضاغطة على المجتمع عامة وخاصة على قطاع الشباب، مما يولد مشاعر سلبية عند شرائح كبيرة من الناس ضد الظروف وضد المجتمع مما يدفعهم إلى أساليب تأقلم

سلبية مع هذه الظروف منها الإتجار الإلكتروني بالبشر والجنس والجريمة الإلكترونية وغيرها.

4-2-4 البحث عن الثراء (Quest for Wealth)

يسعى الإنسان إلى المتعة ويتجنب الألم هكذا تقول النظرية العامة في الجريمة. لجتفردسون وهيرشي (Gottfredson and Hirschi ،1990) ، ويسعى الناس إلى الوسائل غير المقبولة اجتماعيا لتحقيق أهداف مقبولة اجتماعيا كما ترى نظرية الأنومي لميرتون. فالرغبة في الثراء يواجها صعوبات بالغة في تحقيقه بالطرق المقبولة اجتماعيا والقانونية، ولذا يلجأ بعض الناس إلى الجرائم الإلكترونية حيث المستهدف مجتمع أكبر وسهولة التنفيذ وسرعة المردود وقلة الخطورة.

4-2-5 ضعف إنفاذ القانون وتطبيقه في الجريمة الإلكترونية

هناك الكثير من الدول التي لم تطور تشريعاتها وأجهزة العدالة فيها لكي تتمكن من مجاراة التقدم في الجرائم الإلكترونية وأساليبها .وهذا لا يتوقف عند التشريعات وإنما يشمل الشرطة والتحقيق والقضاء، وكيفية التعامل مع الأدلة الرقمية على المستوى الوطني، كما هو الحالي على المستوى الدولي.

فمما يشعل الجريمة الإلكترونية غياب التشريعات الج ا زئية والجنائية وضعف الممارسات العدلية والشرطية والقضائية في محاكمة والتحقيق في الجرائم الإلكترونية .وغالباً ما تجد في دول كثيرة تواضع التقنيات المتوافرة وكذلك الخبراء القادرون على متابعة ورصد وملاحقة الجريمة الإلكترونية داخل المجتمع والعابرة منها للحدود الوطنية.**(البداينة، 2014)**

5-خصائص وسمات الجرائم الإلكترونية (السيبرانية):

-سهولة ارتكاب الجريمة بعيدا عن الرقابة الأمنية، فهي ترتكب عبر جهاز الكمبيوتر مما يسهل تنفيذها من قبل المجرم دون أن يراه أحد أو يكتشفه.

-صعوبة التحكم في تحديد حجم الضرر الناجم عنه قياسا بالجرائم الإلكترونية فالجرائم الالكترونية تتنوع بتنوع مرتكبيها وأهدافهم وبالتالي لا يمكن تحديد حجم الأضرار الناجمة عنها.

-مرتكبها من بين فئات متعددة تجعل من التنبؤ بالمشتبه بهم امرا صعبا أعمارهم تتراوح غالبا ما بين 18 إلى 48 سنة).

تنطوي على سلوكات غير مألوفة عن المجتمع.

-اعتبارها أقل عنفا في التنفيذ فهي تنفذ بأقل جهد ممكن مقارنة بالجرائم التقليدية ، لأن المجرم عند تنفيذه لمثل هذه الجرائم لا يبذل جهدا فهي تطبق على الأجهزة الإلكترونية وبعيدا عن أي رقابة مما يسهل القيام بها.

-جريمة عابرة للحدود لا تعترف بعنصر المكان والزمان فهي تتميز بالتباعد الجغرافي واختلاف التوقيتات بين الجاني والمجني عليه ،فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل بالإمكان ارتكابها عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى.

-سهولة إتلاف الأدلة من قبل الجناة، فالمعلومات المتداولة عبر الإنترنت على هيئة رموز مخزنة على وسائط تخزين ممغنطة وهي عبارة عن نبضات إلكترونية غير مرئية مما يجعل أمر طمس ومحو الدليل أمر سهل.

وتتعدد أنماط الجناة في الجريمة المعلوماتية ، فهناك الهاكارز " Hackers " أو المتسللون وهم عادةً مجرمون محترفون يستغلون خبراتهم وإمكانياتهم في مجال تقنية المعلومات للتسلل إلى مواقع معينة للحصول على معلومات سرية أو تخريب وإتلاف نظام معين وإلحاق الخسائر به بقصد الانتقام أو الابتزاز.

وهناك الكراكرز" " Crackers " المخترقون" سواء كان من الهواة أو المحترفين وعادةً ما يستخدم مجرمو هذا النمط قدراتهم الفنية في اختراق الأنظمة والأجهزة تحقيقاً لأهداف غير شرعية كالحصول على معلومات سرية أو للقيام بأعمال تخريبية. إلخ وهناك العابثون بالشفرات ومؤلفو الفيروسات " Malecions hackers " الخ.

وبينما قد يهدف المجرم المعلوماتي من جريمته إلى تحقيق مكاسب مادية معينة أو إثبات مهارته الفنية وقدرته على اختراق أجهزة الحاسب قد يرتكب مجرمو هذه الفئة جرائمهم بهدف التسلية أو الترفيه أو لمجرد الرغبة في الإضرار بالغير كالموظف الذي يتم فصله من وظيفته ويلجأ إلى الانتقام منها. **(إسراء مرعي، 2016)**

6-تصنيف مرتكبو الجرائم الإلكترونية:

6-1المثاليين المراهقين: وعادة ما يكونون غير مدربين أو مهرة ، وهم الشباب الذين تتراوح أعمارهم بين 13 و26 سنة

والذين يسعون إلى الإعتراف الاجتماعي. وهم يريدون أن يكونون في بؤرة الضوء في وسائل الإعلام. وتمتاز أفعالهم بأنها تسبب الخراب عالمياولكنها لا تذكر على المستوى الفردي. من "مثل الحرمان الكثير من خوادم هامة في التجارة الإلكترونية في شهر فبراير عام 2000 والتي سببت أضرارا عالية لهذه الشركات. " وفي معظم الأحيان يهاجم المثاليون أنظمة المعلومات بفيروسات طوروها؛ وضررهم الفعلي على كل فرد لا يكاد يذكر. وعادة ما يتوقفون في سن 26 عندما ينضجون ويفهمون نتائج أعمالهم.

6-2الجشع -المدفوع (المجرمون المهنيون):وهذا النوع من مجرمي الإنترنت خطير، وهذه الفئة عادة ما تكون عديمة الضمير وهم على استعداد لارتكاب أي ن وع من الجرائم، طالما أنها تجلب لهم المال .حيث بدؤوا في إنتاج المواد الإباحية وغالبا ما تسمى السيبرانية للمواد الإباحية والتي تشمل الإباحية القانونية وغير القانونية على شبكة الإنترنت .أنهم عادة ما يكونوا أذكياء جدا ومنظمون ويعرفون كيفية الهروب من وكالات إنفاذ القانون .ومجرمو الإنترنت هؤلاء يرتكبون الجرائم الخطيرة، وخاصة في جرائم إباحية الأطفال والقمار الإلكتروني وهذه تشكل تهديدا خطيرا للمجتمع.

6-3الإفتراض -الإرهابيون: هم مجموعة الأحدث والأكثر خطورة .والدافع الأساسي لهم ليس المال فقط ولكن أيضا لديهم قضية ما والتي يدافعون عنها .وعادة ما ينغمسون في إرسال رسائل التهديد وتدمير البيانات المخزنة في الغالب في نظم المعلومات الحكومية

لمجرد أن يسجلوا وجهة نظرهم .ويمكن مقارنة تهديد الإرهاب الإلكتروني بتهديدات السلاح النووي،
والبكتريولوجية أو الكيميائية .هذه المسألة المثبطة للهمم هي أنهم لا يعملون داخل حدود الدولة ؛ بل يمكن أن يعملوا من أي مكان في العالم، و هذا يجعل من الصعب اقتناصهم **(Alshalan, 2006)**

7-خصائص وسمات مرتكبو الجرائم:

-شخص ذو مهارات فنية عالية متخصص في الجرائم المعلوماتيةيستغل مداركه ومهارته في اختراق الشبكات وكسر كلمات المرور و الشفرات ويسبح في عالم الشبكات ،ليحصل على كل غالي وثمين من البيانات والمعلومات الموجودة في اجهزة الحواسيب من خلال الشبكات.
-شخص قادر على استخدام خبراته في الاختراق وتغيير المعلومات.
-شخص قادر على تقليد البرامج أو تحويل اموال.
-شخص محترف في التعامل مع شبكات الحاسبة.
-شخص غير عنيف لأن تلك الجريمة لا تلجا للعنف في ارتكابها.
-شخص يتمتع بذكاء اذ يمكنه التغلب على كثير من العقبات التي تواجهه اثناء ارتكابه الجريمة ،حيث يمتلك هذا المجرم من المهارات ما يؤهله للقيام بتعديل وتطوير في الانظمة الامنية حتى لا تستطيع ان تلاحقه وتتبع اعماله الاجرامية من خلال الشبكات أو داخل اجهزة الحواسب فالإجرام المعلوماتي هو اجرام ذكاء.
-شخص اجتماعي له القدرة على التكيف مع الاخرين. **(فرج يوسف، 2008)**

8-أهم طرق الجريمة الإلكترونية (السيبرانية):

وتشمل وليس حصرا على:

1 .**تخريب المعلومات وإساءة استخدامها:** ويشمل ذلك قواعد المعلومات، المكتبات، تمزيق الكتب، تحريف المعلومات، تحريف السجلات الرسمية .الخ.

2 .**سرقة المعلومات:** ويشمل بيع المعلومات كالبحوث أو الدراسات الهامة أو ذات العلاقة بالتطوير التقني، أو الصناعي، أو العسكري، أو تخريبها، أو تدميرها .الخ.

3 .**تزوير المعلومات:** ويشمل الدخول لقواعد في النظام التعليمي وتغيير المعلومات وتحريفها، مثل تغيير علامات الطلاب.

4 .**تزييف المعلومات:** وتشمل تغيير في المعلومات على وضع غير حقيقي مثل وضع سجلات شهادات لم تصدر عن النظام التعليمي وإصدارها.

5 .**انتهاك الخصوصية** :ويشمل نشر معلومات ذات طبيعة خاصة عن الأفراد، أو الدخول لحسابات الأفراد الإلكترونية ونشر معلومات عنهم، أو وضع معلومات تخص تاريخ الأفراد ونشرها.

6 .**التصنت** : وتشمل الدخول لقواعد المعلومات وسرقة المحادثات عبر الهاتف.

7 .**التجسس:** ويشمل إعتراض المعلومات ومحاولة معرفة ما يقوم به الأفراد.

8 .**التشهير:** ويشمل استخدام المعلومات الخاصة أو ذات الصلة بالإنحراف أو الجريمة ونشرها بشكل القصد منه اغتيال شخصية الأفراد أو الإساءة.

9 .**السرقة العلمية** :الكتب والبحوث العلمية الأكاديمية وخاصة ذات الطبيعة التجريبية والتطبيقية.

10 . **سرقة الإختراعات:** وخاصة في المجالات العلمية لاستخدامها أو بيعها.

11 . **الدخول غير القانوني للشبكات:** بقصد إساءة الاستخدام أو الحصول على منافع من خلال تخريب المعلومات أو التجسس أو سرقة المعلومات.

12 . **قرصنة البرمجيات:** ويشمل النسخ غير القانوني للبرمجيات واستخدامها أو بيعها مرة أخرى.

13 . **قرصنة البيانات والمعلومات:** ويشمل أعتراض البيانات وخطفها بقصد الاستفادة منها وبخاصة أرقام البطاقة الائتمانية وأرقام الحسابات وكلمات الدخول وكلمات السر.

14 . **خلاعة الأطفال** : وتشمل نشر صور خاصة للأطفال" الجنس السياحي "للأطفال خاصة، وللإناث على الشبكات Cyber) . (Sixبشكل عام، ونشر الجنس التخيلي.

15 . **القنابل البريدية** :وتشمل إرسال فيروسات لتدمير البيانات من خلال رسالة ملقومة إلكترونية.

16 . **إفشاء الأسرار:** وتشمل الحصول على معلومات خاصة جداً ونشرها على الشبكة.

17 .**الإحتيال المالي بالبطاقات:** وهذا ناتج عن استخدام غير شرعي لبطاقات التسوق أو المالية أو الهاتف.. الخ.

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

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

20 . **المطاردة والملاحقة:** والإبتزاز وتشمل ملاحقة الذكور للإناث أو العكس والتتبع بقصد فرض إقامة علاقة ما، وذلك من خلال استخدام البريد الإلكتروني وإرسال الرسائل.

21 . **الإرهاب الإلكتروني** :يشمل جميع المكونات السالفة الذكر في بيئة تقنية متغيرة والتي تؤثر على فرص الإرهاب ومصادره، هذه التغيرات تؤثر على تكتيكات الإرهاب وأسلحته وأهدافه ومن التكتيكات الإرهابية ما يعرف بالإرهاب الإلكتروني.**(بداينة، 2014)**

9-مكافحة الجرائم الإلكترونية (السيبرانية)

أولا : الجانب الأمني من الحماية

يتعلق هذا الجانب بكل ما هو فني و تقني لحماية شبكة الأنترنت والكمبيوتر وسوف نطرحه في ثلاث نقاط مسائل تتعلق بأمن المعلومات ومهددات أمن المعلومات وفي الأخير الإجراءات الأمنية.

9-1- مسائل تتعلق بأمن المعلومات

يتعلق أمن المعلومات بالمواضيع التالية:

-المسألة الإداريــة : يوجد في كل مؤسسة كمية هائلة من المعلومات تخزن الحاسوب ونظرا لأهميتها تحتاج إهتمام أمني.

–المسألة الماليــة : تتمثل في الكلفة المالية المصروفة قصد حماية النظم المعلوماتية والحاسوبية ذات القيمة الكبيرة.

–المسألة الوظيفية : يجب أن تكون المعلومات جاهزة لإستعمالها عند الحاجة و تكون صحيحة وسرية وكاملة.

–المسألة الخصوصية: يجب حماية النظم الذاتية الخاصة بالأشخاص وإلا سوف يساء إلى الحرية الفردية بإفشائها والتلاعب بها.

–مسألة تحديد مخاطر و حوادث الكمبوتر و الشبكة : هذه الحوادث قد تكون طبيعة أو مفتعلة وتطور تقنيات الحاسوب وإنشاء الإتصالات الحاسوبية يجعل تحديد المخاطر أكثر تعقيدا.

9-2- مهددات أمن المعلومات:

هي الحالة أو الظرف الذي يؤدي حتما إلى تعطيل الشبكة المعلوماتية وأنواع هذه المهددات:

– 1مهددات طبيعيـة : مثل الزلازل التي تؤدي إلى قطع الإتصالات بالشبكة.

– 2مهددات غير مقصودة من طرف الإنسان كسوء إستعمال كلمة السر.

– 3مهددات إنسانيـة: وهو ما يقوم به المتسللون الذين يخترقون المواقع.

إن الوقاية هي أمثل الأساليب نفعا في هذه الجرائم و من بينها:

–إستخدام جدار الحماية fire well وهو حاجز يوضع بين الشبكة الداخلي أنترنت و خادم شبكة الأنترنت ومن أهم مهامه فحص المعلومات الداخلة و الخارجة و السماح لها بالمرور في حالة مطابقتها للمواصفات وتقديم تقارير عن التحركات المشبوهة ولكنه يمكن أن يعطل بعض المعلومات ويحدث عطب.

–التشفير وهو تحويل المعلومة من نص واضح إلى آخر غير مفهوم و قد أستحسن هذا النوع من النظام لنجاعته في عدم كشف المعلومات على شبكة الأنترنت.

–التوقيع الرقمي و هي تقنية تفيد في إمكانية عدم تزوير الرسائل الإلكترونية .

–إستخدام أنظمة كشف الإختراقات و وضع حلول للثغرات الأمنية.

–وضع سياسة أمنية للشبكة وحشد كل الإمكانيات البشرية و المادية لتطبيقها.

–الإحتفاظ بنسخ إحتياطية لكل المعلومات الحساسة في أقراص إضافية ليست مرتبطة بالشبكة.

–تنصيب برامج لمنع ظهور الصور الخلاعية والإتصال بالمواقع الإرهابية.

–و يرى الدكتور عبد الفتاح مراد في كتابة التحقيق الجنائي الفني ضرورة إستخدام بعض البرامج التي صممت خصيصا للكشف والوقاية من الفيروس والبعد عن إستعمال كلمة السر البسيطة.

–عند فتح البريد الإلكتروني يجب معرفة من المرسل خشية أن يكون فيروس.**(البحر، 1999)**

ثانيا : الحلول التشريعية

تمثل هذه الحلول التشريعية في تدابير وقائية تتخدها الدولة و قوانين تسنها من أجل مكافحة هذه الجريمة و حماية المجتمع و لكن لصعوبة التعامل مع هذه الجرائم الجديدة في الوقت الراهن يتطلب الأمر بداية اللجوء إلى حلول قصيرة المدى ثم حلول طويلة المدى و هو إعادة النظر في معظم التشريعات لأن معظم الانترنت أصبح ظاهرة تمس جميع مجالات الحياة.

1- الحلول التشريعية قصيرة المدى

–إن هذه الحلول تتمثل في إصدار السلطة المختصة بعض المراسيم التنظيمية لمقاهي الأنترنت دون إحتكار المعلومة فيمكن في إجراءات إستعجالية فرض بعض الأمور على أصحاب مقاهي الأنترنت.

–وضع البرامج اللازمة لمنع الدخول إلى المواقع المخلة بالحياء و هذا من أهم الظواهر التي برزت في مجتمعنا في ظل غياب التربية السليمة مما يؤدي للإنحلال الخلقي لشبابنا وحتى المراهقين الذي أصبح من السهل عليهم دخول أي موقع يشاءون بالإضافة إلى المواقع الإباحية هناك المواقع الإرهابية و مواقع للعنف كتعليم القتل ، فلا بد من تدبير عاجل لأن الحرية في المعلومة لا تكمن في دخول هذه المواقع.

–وضع برامج للحماية من الفيروسات و هذا كله بمراسيم تنظيمية و يمكن للدولة أن تدعم هذه العملية بتخفيض أسعار هذه البرامج.

–التوعية القانونية والتعريف بمدى خطورة الجرائم الإلكترونية.

–إصدار مراسيم من أجل تنظيم تكوين محققين و رجال شرطة و قضاة على التقنية المعلوماتية والمعرفة الكافية لجرائم الانترنت.

–تعريض أشخاص أو مقاهي الأنترنت لغرامة مالية أو حتى إغلاق المقهى إذ تثبت أنه يسمح للمراهقين أو حتى الشباب بالدخول للمواقع السابقة ففي المواد الجنائية لا يمكننا ذكر أكثر من هذا إحتراما لمبدأ لاعقوبة إلا بنص قانوني.

أما من ناحية المواد المدنية و التجارية فإنه: – يمكن للمحاماة لعب دور مهم لتكييف بعض السلوكيات والمعلومات مع محاولة القضاة تكييف بعض المنازعات التجارية الإلكترونية قياسا على التجارة العادية لحين صدور التشريع المنظم للتجارة الإلكترونية.

–إعتماد حرية الإثبات في المجال التجاري.

–يجب على المشرع أن يوقع بعض المعاهدات لمكافحة الجريمة الإلكترونية.

–يجب على المشرع أن يوقع بعض الإتفاقيات التي تتبنى تعريف التوقيع الإلكتروني والعقد الإلكتروني ومسايرتها بسن قوانينها التنظيمية.

ثانيا : الحلول التشريعية طويلة المدي

–إن الطابع اللامادي و الإفتراضي لشبكة الأنترنت يستلزم تعديل العديد من التشريعات الحالية بالإضافة إلى إستحداث أخرى و هذا لايضطرنا بالضرورة إلى خلق شيء جديد بل يمكننا الإستفادة من الدول الأخرى التي سبقتنا في مجال التشريع لتجريم هذه السلوكيات ما دامت هذه التشريعات لا تخالف النظام العام والآداب العام و بما أنه لا يمكن معاقبة شخص من دون نص قانوني الركن الشرعي إذن لابد من سن نصوص قانونية تتناسب التطور الحالي.

ولكننا نلاحظ أنه رغم زيادة إنتشار الجرائم الإلكترونية و فعاليتها إلا أن المشرع لم يضع لحد الآن الإطار القانوني لأي من هذه الظواهر لذا على المشرع أن يعدل أو يصدر قوانين جديدة ففي نطاق الحماية الجنائية يتعين الإقرار بصلاحية المعلومات كمحل للحماية من أنشطة الإعتداء كافة فبدأ بالتشريعة العامة وهي القانون المدني فعلى المشرع أن يعدل فيه بسن تشريع جديد يتضمن الجرائم الإلكترونية ومن بينها العقد الإلكتروني والتوقيع الإلكتروني وغيرها من المفاهيم في العالم الإفتراضي الجديد.

–القانون التجاري لقد ظهر في عالمنا اليوم مفهوم جديد هو التجارة الإلكترونية و التسويق الإلكتروني والدفع عن طريق بطاقة الإئتمان وهي مجالات خصبة للإحتيال فلا بد على المشرع أن ينظمها.

–الإثبات وهذا في اعتقادنا من أهم الخطوات التي يجب أن يقوم بها المشرع وهذا بتبني الخبرة والمعاينة كأساليب للتحقيق وإثبات الجريمة الإلكترونية.

– تعديل قانون الإجراءات الجزائية وتعديل قانون حقوق المؤلف والحقوق المجاورة.

يمكن أن نلخص أساليب مكافحة الجرائم الإلكترونية فيما يلي:

–رسم سياسات دولية تفرض عقوبات صارمة على مرتكبي جرائم الإنترنت إذ يستلزم التدخل الحكومي والدولي نظراً للخطورة الجسيمة للأمر.

–الاعتماد على أساليب وتقنيات متطوّرة للتمكن من الكشف عن هوية مرتكب الجريمة والاستدلال عليه بأقل وقت ممكن.

–توعية الأفراد ونصحهم لماهية الجرائم الإلكترونية وكل ما يترتب عليها من مخاطر.

–الحرص على الحفاظ على سرية المعلومات الخاصة بالعناوين الإلكترونية كالحسابات البنكية، والبطاقات الائتمانيّة وغيرها.

–عدم الكشف عن كلمة السر نهائياً وتغييرها بشكل مستمر واختيار كلمات سر صعبة.

تجنب تخزين الصور الخاصة بالأفراد على مواقع التواصل الاجتماعي وأجهزة الحاسوب.

–تجنّب تحميل أي برنامج مجهول المصدر.

–استمرارية تحديث برامج الحماية الخاصة بأجهزة الحاسوب ومنها ، .MCafee, Norton

–تأسيس منظمة خاصة لمكافحة الجرائم الإلكترونية والحد منها.

–المسارعة في الإبلاغ للجهات الأمنية فور التعرض لجريمة إلكترونية.

–مواكبة التطورات المرتبطة بالجريمة الإلكترونية والحرص على تطوير وسائل مكافحتها.

–استخدام برمجيات آمنة ونظم تشغيل خالية من الثغرات.

–الحرص على استخدام كلمات سرية للوصول إلى البرامج الموجودة على جهاز الحاسوب.

–عدم ترك جهاز الحاسوب مفتوحاً.

–فصل اتصال جهاز الحاسوب بشبكة الإنترنت في حال عدم الاستخدام.

–أخذ الحيطة والحذر وعدم تصديق كل ما يصل من إعلانات والتأكد من مصداقيتها عن طريق محركات البحث الشهيرة.

–وضع الرقم السري 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 واللغات إلخ.

–يفضل تغيير كلمة المرور الخاصة بك بصفة دورية.

–لا تضع معلومات علي الانترنت لا تحب أن يراها الجميع من تعرفهم ولا تعرفهم وتذكر أنه بمجرد أن تضع معلومات علي الانترنت لن تتمكن أبدا من ارجاعها مرة أخرى حتى لو قمت بحذفها.

–معلوماتك الخاصة (اجعلها خاص) ان معلوماتك الخاصة مثل اسمك بالكامل ورقم هاتفك ورقم الهوية ورقم بطاقتك الائتمان وايضا عنوانك بالتفصيل هي معلومات خاصة لا يجب ان تتاح للجميع علي الانترنت لا شخص لا تعرفه فلا تفصح له عنها او تضعها علي اي موقع لا تثق به. **(إسراء مرعي، 2016)**

–خاتمة :

مع تقدم التكنولوجيا والتطور العلمي تطورت معها أيضا وسائل الجريمة وجلبت العديد من الأضرار والمخاطر على الإنسان والمجتمع والبيئة والكون ، ولا يكمن الخلل في التكنولوجيا ولا التطور العلمي إنما يكمن في الإنسان في حد ذاته فبصلاحه يصلح المجتمع والكون وبفساده يفسد المجتمع والكون مصداقا لقول الله تعالى: "**ظَهَرَ الْفَسَادُ فِي الْبَرِّ وَالْبَحْرِ بِمَا كَسَبَتْ أَيْدِي النَّاسِ لِيُذِيقَهُم بَعْضَ الَّذِي عَمِلُوا لَعَلَّهُمْ يَرْجِعُونَ**"(الروم: الآية 41)

فكان لزاما أن يؤهل الإنسان تأهيلا نفسيا وتربويا وأخلاقيا لإستخدام التكنولوجيا فيما يفيد الصالح العام، وهذا يستوجب نشر التوعية بجميع أنواعها النفسية والعلمية والقانونية وفي جميع المراحل التربوية سواء في المرحلة الإبتدائية والمتوسطة والثانوية والجامعية .

ويستحسن أيضا تنظيم ندوات ودورات علمية للتعريف بهذه الجرائم والتعريف بها عن طريق شرحها وتحليلها للناس وبيان وسائل وطرق الوقاية منها.

- المراجع

-البداينة، ذياب.(2014). ورقة علمية بعنوان.**الجرائم الإلكترونية المفهوم والأسباب**.ملتقى الجرائم المستحدثة في ظل المتغيرات والتحولات الدولية. كلية العلوم الإستراتيجية. عمان.

-أمير، فرج يوسف.(2008) . **الجرائم المعلوماتية على شبكة الإنترنت**. دار المطبوعات الجامعية: الإسكندرية.

-البداينة، ذياب؛ الرشيد، صالح؛ المهيزع، ناصر.(2050) . **فحص النظرية العامة للجريمة في المملكة العربية السعودية**. مجلة مؤته للبحوث الدراسات. المجلد20.العدد1. ١ص.ص 141-169.

-البداينه، ذياب .(1999) . **جرائم الحاسب والانترنت الظواهر الإجرامية المستحدثة وسبل مواجهتها** .في مركز الدراسات والبحوث. الرياض.ص ص 93-126.

-مرعي، إسراء.(2016). **الجرائم الإلكترونية " الأهداف – الأسباب – طرق الجريمة ومعالجتها**". المركز الديمقراطي العربي.https://democraticac.de/?p=35426

-البحر، عبد الرحمن (1999). **معوقات التحقيق في جرائم الأنترنت**." رسالة ماجستير غير منشورة" الرياض: أكاديمية نايف العربية للعلوم الأمنية.

-Alshalan, A. (2006). Cyber-crime and Victimization. Unpublished Ph.D Dissertation in Partial

Fulfillment of the Requirements for the Degree of Doctor of Philosophy in Sociology in Department of Sociology, Anthropology, and Social WorkMississippi State University

-Britz, Marjie. (2004). Computer Forensics and Cyber Crime: An Introduction. New Jersey:Pearson Prentice Hall.

-Halder, D., & Jaishankar, K. (2011): Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9.

-Leukfeldt, R. and Veenstra S., & Stol W.,(2013). High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands. International Journal of Cyber Criminology (IJCC) ISSN: 0974 – 2891 January – June 2013, Vol 7 (1): 1–17

-Laura Ani (2011): "Cyber Crime and National Security: The Role of the Penal and Procedural Law
-UNODC United Nations Office on Drugs and Crime (2013).Comprehensive Study on Cybercrime. United nations.
-Miethe, Terance; Stafford, Mark C.; and Long, J. Scott. 1987. " Social Differentiation in Criminal Victimization: A Test of Routine Activities/ Life style Theories". American Sociological Review, 52: 184-194.
-Meke Eze Stanley, N. (2012): An article "Urbanization and Cyber Crime in Nigeria: Causes and Consequences".
-Gottfredson, M. R. and Hirschi, T. (1990). A General Theory of Crime, California: Stanford University Press.