Int. J. Media. Mas. Com. Vol. 05, No. 02, 76-110 (2023)
DOI: 10.46988/IJMMC.05.02.2023.04
ISSN: 2536-0035
ISBN: 2535-9797
Arab Impact Factor (1.04) (2021).

International Journal of Media and Mass Communication المجلة الدولية للإعلام والاتصال الجماهيري

Information crimes as one of the obstacles to institutional communication on the Gulf Cooperation Council

Dr. Ayman Sayed Mohamed Mostafa Alasaglani

Assistant Professor at Faculty of Law at Alasala University - KSA

Received: 23 Feb. 2023 *Revised: 15 April. 2023* *Accepted: 03 June. 2023* *Published: 01 July 2023*

Abstract:
The global nature of the digital space combined with weak identification of users, insufficient attribution of actions, the complexity of internationally deployed services, the global development of social networking sites, and emerging international crime markets all raise serious concerns about the rise in cybercrime and thus the sustainability of a stable society as a basis for personal development and economic prosperity, and the weak societal infrastructure for technology Information, communications, and the unlimited collection and storage of data threaten personal freedom and international stability. Citizens' trust in society and government to protect their security, safety, and prosperity is eroded by the risks and uncertainties arising from technological developments, with the heavy economic losses that this entails. This study aims to understand cybercrimes and the statement of the resulting crimes. Therefore, urge urgently to find a strategy to address these problems based on a coherent analysis of technological, societal, economic, and political trends and consequences.

Keywords: Cybercrimes, Institutional Communication, Networking

الجرائم المعلوماتية كأحد عوائق الاتصال المؤسسي بدول مجلس التعاون الخليجي

د. أيمن سيد محمد مصطفى العسقلاني

أستاذ مساعد القانون الدولي بكلية الحقوق، جامعة الأصالة الدمام المملكة العربية السعودية

الملخص:

إن الطابع العالمي للفضاء الرقمي مقترناً بضعف تعيين هوية المستعملين وعدم كفاية إسناد الأفعال وتعقّد الخدمات المنتشرة دولياً والتطوير العالمي لمواقع الشبكات الاجتماعية وأسواق الجريمة الدولية الناشئة كلها تُثير القلق الجدي من ارتفاع الجريمة السيبرانية وبالتالي استدامة المجتمع المستقر كأساس للتنمية الشخصية والرخاء الاقتصادي، وضعف البنية التحتية المجتمعية لتكنولوجيا المعلومات والاتصالات وجمع وتخزين البيانات بدون حدود يهددان الحرية الشخصية والاستقرار الدولي، وثقة المواطنين في المجتمع والحكومة لحماية أمنهم وسلامتهم ورخائهم تتعرض للتآكل بفعل الأخطار والشكوك الناشئة عن التطورات التقنية مع ما ينطوي عليه ذلك من خسائر اقتصادية باهظة. وتهدف هذه الدراسة إلى معرفة الجرائم السيبرانية وبيان الجرائم الناجمة عنها.

ولذلك فإننا نحّث على سبيل الاستعجال على إيجاد إستراتيجية للتصدي لهذه المشاكل استناداً إلى تحليل متماسك للاتجاهات والعواقب التكنولوجية، والمجتمعية، والاقتصادية، والسياسية.

الكلمات المفتاحية: الجرائم السيبرانية، الاتصال المؤسسي، الشبكة العنكبوتية

المقدمة

تعد الجرائم السيبرانية من أبرز وأخطر التحديات التي تواجه كافة مجتمعات العالم في مجالات استخدامات تقنية المعلومات سواء على المواطن أو الدولة أو مؤسسات القطاع الخاص، وأصبحت تكنولوجيا المعلومات والاتصالات جزءاً لا يتجزأ من الحياة اليومية لكثير من الأشخاص في أنحاء العالم. والاتصالات الرقمية والشبكات والأنظمة تقدم موارد حيوية وتمثل بنية تحتية لا غنى عنها في كل جوانب المجتمع العالمي، وهي ضرورات لا يمكن لكثير من سكان العالم الازدهار أو حتى البقاء بدونها.

ومع تزايد الاعتماد على تكنولوجيا المعلومات في مجالات الاتصال المؤسسي وبخاصة في دول مجلس التعاون الخليجي تزايد أيضاً التعرض للهجمات على البنية التحتية الحرجة من خلال الفضاء السيبراني، ورغم أن المعالم الدقيقة لأي "حرب سيبرانية" لا تزال غير محددة فإن الهجمات الكبيرة ضد البنية التحتية للمعلومات وخدمات الإنترنت في العقد الأخير تُعطي صورة ما عن الشكل والنطاق المحتملين للنزاع في الفضاء السيبراني.

ولذلك ليس غريبا أن يصف المفكر الإنجليزي أنتوني جيدنز ANTONY GIDDENS العالم الذي نعيش فيه بأنه عالم متقلب Runway world لا يمكن الإمساك بعصمته أو إخضاعه للسيطرة، وقد يعطي ذلك تفسيرا مقنعا لما نراه اليوم

من النمو المتزايد والمطرد للجرائم السيبرانية (C. Antony, 1999)

وتعد دول مجلس التعاون الخليجي من الدول التي اعتمدت على التقنيات الحديثة في مجال الاتصال المؤسسي الأمر الذي استلزم التصدي لهذه الظاهرة الإجرامية، وهذا بالطبع ليس مستغربا فقد أصبحت صاحبة السبق والريادة في المجال الأمني الأمر الذي أهلها أن تكون من الدول الأكثر أمنا في العالم وصاحبة أعلى معدل عالمي في مواجهة الجرائم السيبرالية. (الحمادي، 2006)

مشكلة الدراسة

تكمن مشكلة البحث في تنامي ظاهرة الجرائم السيبرانية وتفاقمها وتعدد أنواعها وازدياد حجم الخسائر الناجمة عنها والتي قد يصعب حصرها في كافة المجالات الحيوية والعامة وعلى الأفراد أو القطاع العام والخاص، بل وأصبحت هذه الظاهرة الخطيرة من مهددات الأمن القومي مع تنامي استخدام الشبكة السيبرانية من قبل الجماعات الإرهابية نظرا لما تتميز به هذه الشبكة وسهولة استخدامها وانتشارها الواسع، وبالطبع فإن آثار هذه الجريمة في منطقة الخليج العربي تتزايد خطورتها نظرا لأهمية وقوة الاقتصاد لدول الخليج العربي وما حباها به المولى عز وجل من ثروات وموقع إستراتيجي، وازداد الأمر تعقيدا في تنامي الاعتماد على تقنيات الانترنت في الاتصال المؤسسي بين دول مجلس التعاون الخليجي الأمر الذي أوجب وضع إستراتيجية لمواجهة هذه الظاهرة.

أهمية الدراسة

تكتسب الدراسة أهميتها من الخطورة المتزايدة للجرائم السيبرانية وعظم الآثار والخسائر الناجمة عنها وخطورة الجرائم السيبرانية على البنى التحتية المعلوماتية والتي أصبحت عصب الحياة فيفي الاتصال المؤسسي في المجتمع الخليجي اقتصاديا واجتماعيا وأمنيا، مما يحتم معه ضرورة أن يكون لمجلس التعاون لدول الخليج العربي دورا فعالا في التصدي لهذه الجرائم، ومن خلال البحث والتحليل فقد رأينا اقتراح إستراتيجية لتفعيل دور مجلس التعاون لدول مجلس الخليج العربي في المواجهة.

أهداف الدراسة

تتمثل الأهداف التي تسعى الدراسة إلى تحقيقها في الآتي: –

- التعريف بمفهوم الجرائم السيبرانية وخصائصها وتصنيفاتها
- بيان الآثار الخطيرة التي تنجم عن الجرائم السيبرانية.
- بيان التحديات والعراقيل التي تواجه مكافحة الجرائم السيبرانية والتي تحول دون مواجهة هذه الجرائم بالكفاءة المطلوبة.
- إبراز دور مجلس التعاون لدول الخليج العربي في مواجهة هذه الظاهرة الخطيرة والحد من آثارها.
- الإستراتيجية المقترحة لتفعيل المواجهة وأهم المحاور التي ترتكز عليها.

فروض الدراسة

- انتشار ظاهرة الجرائم السيبرانية نظرا لطبيعتها كجريمة عابرة للحدود.

- طبيعة دول مجلس التعاون لدول الخليج العربي ووضعها الاقتصادي باعتبارها بيئة جاذبة للاستثمار الأمر الذي يجعلها بيئة خصبة لنمو هذه الجرائم.
- الصعوبات والتحديات التي تواجهها الأجهزة المعنية بمواجهة الجرائم السيبرانية والتي تعيقها عن ممارسة دورها.
- تأكيد أهمية التعاون الدولي والتنسيق في التصدي لهذه الظاهرة الإجرامية ودور مجلس التعاون في دعم وتعزيز ذلك.
- أهمية إعداد إستراتيجية موحدة لمواجهة الجرائم السيبرانية في دول مجلس التعاون لدول الخليج العربي.

تساؤلات الدراسة

تقدم الدراسة محاولة للإجابة على التساؤلات الآتية: –

- ماهية الجرائم السيبرانية، وخصائصها وتصنيفاتها؟
- ما هي الآثار الناجمة عن الجرائم السيبرانية والخسائر الناجمة عن تفشيها؟
- ما هي العراقيل والعقبات التي تحول دون المواجهة الفعالة لهذه الظاهرة؟
- كيفية وسبل تخطي هذه العقبات؟
- ما هو الدور الذي يقوم به مجلس التعاون لدول الخليج العربي في مواجهة هذه الظاهرة؟
- ما هي الإستراتيجية المقترحة للمواجهة وتفعيلها؟

الدراسات السابقة

تعتمد الدراسة البحثية على أحدث الدراسات السابقة والتي تعرضت للجريمة السيبرانية والآثار الناجمة عنها من خلال أحدث الدراسات التي أجرتها المراكز المتخصصة هي هذا الشأن وتم إدراج هذه الدراسات والمراجع في قائمة المراجع التي تم تسطيرها في نهاية الدراسة.

وإن كانت هناك مشكلة أساسية تتمثل في قلة الدراسات العربية وندرتها ومع ذلك فقد تم بذل أقصى الجهد من أجل البحث والتنقيب.

منهج البحث

يتمثل المنهج الرئيسي في هذه الدراسة المنهج الوصفي التحليلي الذي يقوم على وصف الظاهرة وتحليلها من أجل الخروج بتوصيات ونتائج من خلال إستراتيجية مقترحة في هذا الصدد، حتى تعم الفائدة المرجوة من البحث العلمي.

تقسيم الدراسة

تم تقسيم الدراسة لتكون على النحو التالي: –

المبحث الأول: مفهوم الجريمة السيبرانية وخصائصها وتصنيفاتها وينقسم إلى:

- المطلب الأول: – مفهوم الجريمة السيبرانية
- المطلب الثاني: – خصائص الجريمة السيبرانية وأركانها

- المطلب الثالث: – تصنيفات الجريمة السيبرانية

المبحث الثاني: – الناجمة عن الجرائم السيبرانية ودور مجلس التعاون الخليجي في المواجهة والإستراتيجية المقترحة في هذا الشأن وينقسم إلى: –

- المطلب الأول: – الأخطار الناجمة عن الجرائم السيبرانية في دول مجلس التعاون الخليجي.
- المطلب الثاني: – دور مجلس التعاون الخليجي في مواجهة الجرائم السيبرانية.
- المطلب الثالث: – الإستراتيجية المقترحة لتفعيل المواجهة

المبحث الأول

مفهوم الجريمة السيبرانية وخصائصها وتصنيفاتها

يعتبر موضوع الجريمة السيبرانية في حد ذاته موضوع الساعة، وتزداد أهمية هذا الموضوع أمام الطابع الدولي العلمي لشبكة الإنترنت، والتي تعد سلاح ذو حدين يحمل بين جنبيه الظلمة والنور، ويعكس وجهي الخير والشر في الإنسان، فهو وسيلة للربط والاتصال والتقارب ولتبادل المعلومات والمنافع بين بني البشر، إلا أنه يمكن أن يكون أداة تزوير وارتكاب الجرائم والتعدي على حقوق الآخرين، ومن هنا ظهرت الحاجة الماسة إلى الحد من هذا الجانب المظلم لها. (الجدير بالذكر انه في عام 1984م أصدر الكونجرس الأمريكي قانون مكافحة الجرائم الماسة بالمعالجة والوصول والدخول غير المرخص للحواسيب، واستخدام الحاسوب، وقد أشار الكونجرس وقدم في مواد هذه القانون بيان واضح للأنشطة المحظورة).

وترجع أهمية هذا الموضوع البالغة لارتباطه بمجال حساس وهو المعلومة وتأمينها من الأخطار لاسيما كونها عصب الحياة في عصرنا الحالي والاهتمام بها في مختلف المستويات الفردية والحكومية، أو من قبل المنظمات الإقليمية والدولية، أو في شتى المجالات الاقتصادية والسياسية والاجتماعية والإدارية، وغيرها من المجالات والقطاعات، ففي ظل تنامي معدلات الجريمة الإليكترونية وانتشارها إما بالتعدي على المعلومات بالحذف، أو التعديل، أو الدخول غير المشروع، أو الاختراق، أو الحجب، أو التعطيل. (Katrina, 2004)

كما أن خصائص الإبحار على الشبكة السيبرانية وإتاحتها بمجرد أن تكون متصلا بالإنترنت ساهمت في الانتشار الواسع، أضف إلى ذلك الخصائص الأخرى التي تجعل من الصعوبة متابعة هذه الجرائم العابرة للحدود وتقفي أثر مرتكبيها مما يستدعي تكاتف الجهود وتفعيل آليات الحماية القانونية لردع مرتكبيها (Grabosky,2013) والحد منها. وقد رأينا تقسيم دراستنا لهذا المبحث لتكون على النحو التالي:

- المطلب الأول: – مفهوم الجريمة السيبرانية
- المطلب الثاني: – خصائص الجريمة السيبرانية وأركانها
- المطلب الثالث: – تصنيفات الجريمة السيبرانية

المطلب الأول

مفهوم الجريمة السيبرانية

أدت الحداثة التي تتميز بها الجريمة المرتكبة عبر الإنترنت، واختلاف الأنظمة القانونية والثقافية بين الدول إلى عدم الاتفاق على وضع تعريف موحد لهذه الظاهرة الإجرامية، وذلك خشية حصرها في مجال ضيق (عريان،2004، صفحة 13)، فهي نشاط إجرامي للحاسب الآلي دورا في ارتكابه (J. O'hearn, 1998,p1148)، ومن الصعب في الغالب معاقبة مرتكبيها إلا بعد جهود مضنية وعمليات تتبع معقدة (Young Pi, 2011)، ومن هنا رأى البعض أن تعريف هذه الجريمة ليس بالأمر الهين (Mc Quade, 2008,p16)

وقد تعددت الاتجاهات في تعريف الجريمة السيبرانية وذلك على النحو التالي: -

الاتجاه الأول: تعريفها على أساس وسيلة ارتكاب الجريمة: -

يرتكز تعريف الجريمة السيبرانية أو السيبرالية على أساس الحاسب كوسيلة لارتكابها ,فيعرفها مكتب التقنية في الولايات المتحدة الأمريكية بأنها "الجرائم التي يلعب فيها البيانات الكمبيوترية دورا رئيسا (الكعبي، 2011، صفحة33)، كما عرفت أيضا "نشاط إجرامي يستخدم فيه التقنية الإلكترونية "الحاسب الآلي" وشبكة الإنترنت بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف" (عبد الله، 2007، صفحة 15).. وقد أطلق عليها البعض الجريمة التخيليةvirtual crime وعرفها "أية جريمة يكون فيها للشبكة السيبرانية دور في أسلوب ارتكابها(الجنيهي، 2005، صفحة 13) ، أو التوقيع على أحد وثائقها بأية طريقة كانت" (Eoglan casey, 2000,p 259)

كما عرفها الفقيه الألماني تاديمان "شكل من أشكال السلوك غير المشروع، (مزغيش، 2013) أو الضار بالمجتمع الذي يرتكب بواسطة الحاسب الآلي" (حجازي، 2006، صفحة 22)، وعرفها كيسي أنها " كل نشاط إجرامي يؤدي فيه الحاسب الآلي دورا لإتمامه على أن يكون هذا الدور على قدر من الأهمية " (قوره، 2004، صفحة 26)، وعرفت كذلك "أنها تشمل سرقة خدمات الحاسوب، الدخول غير المشروع في نظم الحاسب المحمية، قرصنة البرامج، تعديل أو سرقة المعلومات المخزنة إلكترونيا، الابتزاز بواسطة الحاسوب، دخول غير مصرح به على سجلات البنوك، إصدار بطاقات ائتمان. أو وكالات العملاء، الاتجار في كلمات السر المسروقة، وبث الفيروسات والأوامر الهدامة ,L. Mendle) 1988, p13)وعرفت "أنها تلك الجرائم الناتجة عن استخدام السيبرانية ، والتقنية الحديثة المتعلقة بالكمبيوتر والإنترنت في أعمال وأنشطة إجرامية بهدف تحقيق عوائد مالية ضخمة يعاد ضخها في الاقتصاد الدولي عبر شبكة الإنترنت باستخدام النقود الإليكترونية، أو بطاقات السحب التي تحمل أرقام سرية بالشراء عبر الإنترنت باستخدام النقود، أو تداول الأسهم (شوا،1993، صفحة 2) ، وممارسة الأنشطة التجارية عبر هذه الشبكة (المصري،2011، صفحة 7)

عرفها البروفيسور St. Viswanathan " أي إجراء قانوني يكون فيه الحاسوب أداة، أو موضوعا في الجريمة (St. Viswanathan, 2001, p81)، أو أي جريمة تهدف إلى التأثير على وظيفة الحاسوب، أي حادث مرتبط بتكنولوجيا الحاسوب يعاني منه الضحية، أو قد يعاني من خسارة ويكون مرتكب الجريمة حقق مكاسب (Moafa, 2014)

ثانيا: التعريف على أساس شخصي

يركز أنصار هذا الاتجاه في تعريفه للجريمة الإليكترونية على الفاعل لهذه الجرائم، وأن يكون ملما بتقنية المعلومات،

(عبابنة، 2005، صفحة 16) ومن هذه التعريفات تعريف وزارة العدل في الولايات المتحدة الأمريكية " أية جريمة لفاعلها معرفة فنية بتقنية الحاسبات تمكنه من ارتكابها (الخن، 2018)

وعرفها الأستاذ (David Thompson) " أي جريمة يكون متطلب لارتكابها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب (Thompson, 2016)، وعرفتها منظمة التعاون الاقتصادي والتنمية OECD

(Organization for Economic Cooperation and Development)" كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية، أو المعنوية يكون ناتجا بطريقة مباشرة، أو غير مباشرة عن تدخل التقنية السيبرانية (عفيفي، 2003، صفحة 32) ، وقد قوبل هذا الاتجاه بالعديد من الانتقادات حيث أن مجرد توافر المعرفة التقنية لا يكفي في ضوء عدم توافر العناصر الأخرى لتصنيف الجريمة من ضمن الجرائم السيبرانية.

ثالثا: تعريف الجريمة السيبرانية على أساس موضوع الجريمة

يذهب أنصار هذا الاتجاه إلى التركيز على الجانب الموضوعي باعتبار أن هذه الجريمة ليست من الجرائم التي يستخدم فيها الحاسب الآلي فحسب، بل تقع عليه (الملط، 2006، ص86-85)، أو في داخل نطاقه (حجازي،2006، صفحة 26)، ويوسع البعض في تعريفه لهذه الجريمة فيرى الخبير الأمريكي باركر" كل فعل إجرامي معتمدا أيا كانت صلته بالسيبرانية (فكري، 2005، صفحات 22-25)، تنشأ عنه خسارة تلحق بالمجني عليه بفعل أو مكسب يحققه الفاعل. (الشوابكه، 2004، صفحة 15).

وقد وضع مؤتمر الأمم المتحدة لمنع الجريمة ومعاقبة المجرمين تعريفا جامعا لجرائم الحاسب الآلي وشبكاته حيث عرف الجريمة السيبرانية أنها " أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي، أو شبكة حاسوبية، أو داخل نظام حاسوب، ويشمل تلك الجرائم من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة إجرامية. (الطائي، 2007، صفحة 110).

عرفها K. Jaishanker " الجرائم المرتكبة ضد الأفراد، أو المجموعات، أو بدافع إجرامي يضر عمدا بسمعة الضحية، أو يسبب ضرر جسدي أو معنوي، أو خسارة للضحية بشكل مباشر أو غير مباشر باستخدام شبكات الاتصالات الحديثة من الإنترنت (غرف الدردشة- البريد الإليكتروني .... الخ) ((Chaubey, 2012

ونرى أن الجريمة السيبرانية هي كل فعل عمدي، وكل سلوك غير مشروع، أو غير أخلاقي، أو غير مسموح صادر عن إرادة جنائية، ويقوم به شخص ما له دراية ومعرفة بتكنولوجيا المعلومات المختلفة، وتوجه ضد المصلحة العامة والخاصة.

المطلب الثاني

خصائص الجريمة السيبرانية وأركانها

أبرزت ثورة الاتصالات والمعلومات وسائل جديدة للنشر يجعل وسائل جديدة للبشرية تجعل الحياة أفضل من ذي قبل، غير إنها فتحت الباب على مصراعيه لظهور صور من السلوك الإجرامي لم يكن من المتصور وقوعها في الماضي، والتي تخرج عن دائرة التجريم والعقاب القائمة، لأن المشرع لم يتصور حدوثها أصلا (عوض، 1993، صفحة 36)،

حيث سمحت من جهة ظهور صور إجرامية جديدة مثل سرقة المعلومات والأسرار المودعة في قواعد المعلومات، كما وأنها أدت إلى تطور الأنشطة الإجرامية التقليدية وجعلتها أكثر تطورا من جهة أخرى.

وللجريمة السيبرانية خصائص تتفرد بها، ولا تتوافر في أي من أفعال الجرائم التقليدية وذلك على النحو التالي: –

أولا: خصائص الجريمة السيبرانية

1- الحاسب باعتباره أداة للجريمة

فتتميز هذه الجرائم بأن الحاسب يكون أداة في ارتكابها، فلا يمكن تسميتها بالجريمة السيبرانية بدون استعمال الحاسوب لأنه وسيلة الإجرام فيها، وأداة تنفيذها أيا كان نوعها.

2- استخدامها عبر الإنترنت

حيث تعد الشبكة العنكبوتية في معظمها هي حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم (الحسيني)

3- جريمة لا حدود لها

حيث ألغت شبكة الإنترنت أي حدود جغرافية، وجعلت من العالم قرية صغيرة(Alshalan, 2006) ، فما يحدث في الطرف الشمالي للقارة يراه من في الطرف الجنوبي لها في نفس الوقت وكذلك التواصل بين الأفراد، وعليه فإن الجريمة المرتكبة عبر الإنترنت تتخطى حدود الدولة وتتعدى آثارها السلبية للبلدان الأخرى في العالم (البداينة، 1998، صفحات 9-25)

4- أنها لا تترك أثر لها بعد ارتكابها(العجلوني،2006)، (همام، 2002) ولذلك يصعب اكتشافها (العجمي، 2014، صفحة 21)

5- صعوبة الاحتفاظ الفني بآثارها هذا إن وجدت أصلا لسهولة إخفاء معالمها

6- تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها

7- سهولة ارتكابها

8- يسهل البعد الزمني (اختلاف التوقيت بين الدول) والمكاني دورا هاما في تشتيت جهود التحري والتنسيق الدولي لتعقب هذه الجرائم.

9- الغموض حيث يصعب إثباتها والتحقيق فيها عكس الجرائم التقليدية

10- عدم الإبلاغ عنها غالبا، إما لعدم اكتشاف الضحية، أو خوفا من الفضيحة والتشهير.

11- خطورة الجرائم السيبرانية لمساسها بالإنسان في حياته، والمؤسسات في اقتصادها، والبلاد في أمنها القومي والسياسي والاقتصادي، مما يضفي عليها أبعاد خطيرة غير مسبوقة على حجم الأضرار والخسائر على مختلف القطاعات (سليم، 2014، صفحة96)

12- سمات مرتكبها حيث يتميز مرتكبيها بالسمات الآتية (الصغير، 1992، صفحة 8)

المهارة – المعرفة – الوسيلة حيث تتميز الوسيلة بالبساطة وسهولة الحصول عليها – السلطة مثل الشفرة الخاصة بالدخول على النظام، (السعيد، 2002، صفحة 3) سلطة استخدام الحاسب – الباعث حيث يكون الباعث مختلف أقوى هذه البواعث الرغبة في قهر النظام ونشوة الانتصار وتخطي الحواجز الخاصة بالحماية. (الحديثي، 1992، صفحة 11) (ابراهيم، 2009، صفحة 78).

ثانيا أركان الجريمة السيبرانية: –

تقوم أي جريمة على ثلاثة أركان أولا: – الركن المادي وتعني ماديات الجريمة التي تبرز إلى العالم الخارجي، الركن المعنوي وهو إرادة حدوث الفعل سواء عمدي أو خطأ، الركن الشرعي وتعني قاعدة التجريم والعقاب (الجبور،2012، صفحة 59)

1. الركن المادي: –

الركن المادي هو كل العناصر الواقعية التي تتطلبها النص الجنائي العام للجريمة لأن المشرع لا يجرم مجرد التفكير، أو على الدافع، أو النزاعات النفسية الخالصة (عبيد، 1979)، فالمشرع لا يستطيع الغوص في أعماق نفوس البشر وتفتيش تفكيرهم المجرد ليعاقبهم عليه دون أن يتخذ هذا التفكير وتلك العوامل المادية مظهرا ماديا، فلابد من فعل أو امتناع يمكن إثباته.

والركن المادي يختلف حسب تصنيف الذي يقع على الفعل، وصعوبة الجريمة السيبرانية تأتي من أنها عبارة عن معلومات تتدفق في الكابلات المتصلة بالحواسيب فلا يمكن الإمساك بها ماديا (معاشي، 2011، صفحة 280)، كما وأنه لا يمكن حصر الجرائم السيبرانية تحت تكييف وأحد، فقد تشكل الواقعة التي تحمل وصف الجريمة السيبرانية جريمة قذف، أو تهديد، أو تحريض وبشكل مطابق لما يجري في قانون العقوبات وينطبق قواعده عليها متى وقعت على الجهاز الحاسب (سلامة، 2011، صفحة 8)، إلا أن هناك أنواعا من السلوك تطلب التمييز بينها وبين سابقتها التقليدية وهذا الأمر يدعو إلي ضرورة التدخل التشريعي.

فهناك الكثير من أنواع السلوك جاءت نتيجة وسائل تقنية متقدمة لا يمكن أن ينطبق عليها نصوص قانون العقوبات، بل أن تطبيق القواعد عليها يعد خروجا على مبدأ الشرعية الذي يتعين على القضاء الالتزام به هذا من جانب، ومن جانب آخر لا يمكن التعويل على التفسير الواسع للنصوص لأن من شان ذلك توسيع دائرة التجريم، مما يلزم تدخل تشريعي لتلافي هذا العوار، وحرصا على مبدأ المشروعية.

مما سبق تبين أن الجرائم السيبرانية كثير منها محكوم بالقواعد العامة التي تحكم سائر الجرائم ،وإن كان هناك ثمة ما يخرج عن نطاق هذه القواعد يلتزم معه التدخل التشريعي لمعالجتها (من السلوك المستحدث الذي يرتكب بواسطة الكمبيوتر السرقة السيبرانية التي لا يتشابه أحكامها مع أحكام السرقة العادية، حيث أنها تتم دون انتقال المنقول لحيازة فاعله، بمعني أن المجرم المعلوماتي قد يدخل إلى ذاكرة كمبيوتر ويطلع على ما فيها من محتويات واخذ نسخه منها، أو الاحتفاظ بها في ذاكرته ، فهل يعد ذلك سرقة بالمفهوم التقليدي أم تجسس، ومن الجرائم المستحدثة اختراق الشبكات، وأجهزة الكمبيوتر التابعة للغير سواء شخص طبيعي أو معنوي يمثل تطفل غير مشروع، أو خرق للسرية والحياة الخاصة، وبث الأفكار غير المشروعة عبر شبكات الإنترنت أيا كانت دينية، سياسية، أخلاقية، وكذلك تعطيل شبكات الإنترنت، الدخول على الشبكات وتعطيلها بطريق الفيروسات، وتدمير كل أو جزء أو تحريف المعلومات أو العبث بها وتغييرها واعتراضها) (مرهج، 2002، صفحة 159)

2. الركن المعنوي: –

إن الجريمة ليست كيانا ماديا خالص قوامه الفعل وما يترتب عليه، بل هي فوق ذلك كيان نفسي، ويتمثل في الركن المعنوي في القصد الجنائي، وهو اتجاه إرادة الجاني الإجرامية مع علمه بأن ما هو مقدم عليه يوقعه في الإثم الجنائي

(أنفوش، 2016، صفحة5) ويعرف الركن المعنوي "أنها العلاقة التي تربط ماديات الجريمة وشخصية الجاني مرتكبها، وهذه العلاقة هي محل الأذناب في معنى استحقاق العقاب، ومن ثم يوجه إليها لوم القانون وعقابه ".

(حسني،1971، صفحة 90)

وهناك بعض التشريعات التي تقسم الجريمة على أساس الركن المعنوي " جريمة عمدية – وغير عمدية " في الأولي تتجه إرادة الفاعل لارتكاب الفعل ولإحداث النتيجة معا، وفي الأخرى لم يقصد الفاعل سوي ارتكاب الفعل دون إرادة تحقيق النتيجة، وهو ما سنطبقه على الجريمة السيبرانية على النحو التالي: –

أ. الجريمة السيبرانية كجريمة عمدية: –

كانت النظرة القديمة للمجرم تنصب على أنه من أحط أنواع البشر، وأن السمات الإجرامية لا تتوافر إلا من ذوي المستوى البيئي المتواضع، بيد أن هذه النظرة تغيرت مع المجرم المعلوماتي، وكذلك مع ظهور أنماط جديدة من الجرائم مثل غسيل الأموال والاتجار بالأعضاء البشرية، فهؤلاء لديهم من العلم والثقافة ما يؤهلهم لارتكاب مثل هذه الأنواع من الجرائم، بل إن الأمر وصل إلى توجيه أصابع الاتهام نحو المتعلمين ووصل الأمر إلى الاستعانة بعلماء من اجل ارتكاب الجريمة. (الداود، 1999، صفحة 8)، والجريمة السيبرانية حسب المتصور لا تقع إلا بصورة عمدية، حيث إنه لابد أن يسبقها تفكير وتدبر وتدبير للحصول على المعلومات واختراق الحاسوب والإنترنت من أجل تحقيق المنفعة، أو الهدف المرسوم للجاني وكل جرائم السيبرانية يتطلب إرادة تحقيق نتائجه فهي عمدية إذن.

ب. الجريمة السيبرانية كجريمة غير عمدية: –

تكون الجريمة غير عمدية متى وقعت النتيجة بسبب خطأ الفاعل سواء أكان إهمالا، أو رعونة، أو عدم انتباه ،أو عدم احتياط، أو عدم مراعاة للقوانين والأنظمة والأوامر، وبصفة عامة تكون الجريمة غير عمدية إذا أراد الفاعل السلوك ولم تتجه إرادته للنتيجة الإجرامية، ومن الممكن تصور حدوث الجرائم السيبرانية وفق هذه الصورة، فمن يعتمد على مهارته في تلافي متاعب مشاكل الفيروسات وأدى ذلك إلى لتدمير أجهزة الدائرة التي يعمل فيها نتيجة إفراطه في استخدام جهاز الكمبيوتر العائد للدائرة بعملياته الشخصية، وتكون مسؤوليته هنا غير عمدية، وكذلك من يستخدم أقراص مرنة أو usb ولم يتأكد من خلوها من الفيروسات ويتسبب في نقل فيروسات لهذه الأجهزة وتدميرها، وغيرها من الحالات.

3. الركن الشرعي: –

يقصد بالركن الشرعي للجريمة وجود نص تشريعي يوضح العقوبة المترتبة عليه وقت وقوع الفعل (أحمد، 2005، صفحة 5)، فمبدأ الشرعية يمنع المسائلة الجنائية ما لم يتوافر نص تشريعي "لا جريمة ولا عقوبة إلا بنص"، فمتى انتفى النص التشريعي انتفت الجريمة وامتنعت المسئولية، وتحقق القصور في مكافحة هذه الجرائم (عرب، 2001، صفحة 43) تمثل المشروعية حجر الزاوية للنظام الجنائي بأسره، فمنه تتفرع وحوله تدور كافة المبادئ التي تحكم القواعد الجنائية موضوعية كانت أو إجرائية. (وزير، 2009، صفحة 33)

والسؤال محل البحث في هذا الشق هل النصوص القانونية القائمة كفيلة لمعالجة هذه الظاهرة التي من بينها الاستخدام غير المشروع لشبكة الإنترنت؟ (الحنيص، 2011، صفحة 191)، وتبين من الواقع أنه في بعض الأحوال توجد ثمة أفعال جديدة ترتبط باستعمال الكمبيوتر لا تكفي النصوص الحالية القائمة لمكافحتها منها الاعتداء على حرمة الحياة

الخاصة حيث أن تجميع معلومات عن الأفراد وتسجيلها في الكمبيوتر لا تخضع للتجريم وفقا للقواعد العامة، كما أن التداخل في نظام الحاسب الآلي وتغيير البيانات صورة جديدة لا يعرفها قانون العقوبات قبل ظهور الحاسب الآلي وشبكة الإنترنت، مما يؤكد وجود قصور القواعد التقليدية في القانون الجنائي على مكافحة هذا النوع المستحدث من الجرائم (غنام، 2003، صفحات 626-625)

من هنا تبدو الحاجة الماسة إلى تدخل المشرع لمواجهة جرائم الإنترنت باعتبارها من المستحدثات التي عجزت مواد القوانين العقابية التقليدية في مواجهتها (رمضان، 2007، صفحة 17)، لذلك سعت دول العالم المتقدمة إلى سن التشريعات لمواجهة هذه الظاهرة (قشقوش، 1992، 102). (في فرنسا صدر القانون رقم 19 لسنة 1988م تحت عنوان " الجرائم في المواد السيبرانية" ، وادمج في الفصل الثاني من قانون العقوبات وخصصت له المواد من 432-282-9/462 ، تم تعديله في عام1992م ، وفي عام2000م صدر القانون رقم 230 بشأن الإثبات المتعلق بالتوقيع الإليكتروني ، وفى الولايات المتحدة الأمريكية وضع قانون خاص بحماية الحاسوب والشبكات 1976م ، وعرفت دول أخرى هذا النوع من القوانين مثل ألمانيا عام 1986م ، النمسا والنرويج واليابان عام 1987م ، واليونان 1988م ، وسويسرا1994م، واسبانيا والدانمرك وكندا وفنلندا 1995م) (المطردي، 2001، صفحات 6-7) (وعلى مستوى الدول العربية فقد صدر عن مجلس وزراء العدل العرب بجامعة الدول العربية قانون عربي استرشادي لمكافحة جرائم التقنية انظمه المعلومات مكون من 27 مادة للاسترشاد به عند سن القوانين غير أننا لم نر له أثرا فعليا علي أغلب التشريعات الجنائية في الدول العربية وبصفة خاصة مصر، فلا يوجد بها حتى الآن تشريع جنائي خاص بالجريمة الالكترونية يقدم الحلول الناجعة لكافة المشكلات القانونية الناجمة عنها على الرغم من وجود بعض النصوص القانونية التي تحتويها قوانين تنظم موضوعات مختلفة تناولت بعض صور التجريم الالكتروني، منها قانون الأحوال المدنية المصري رقم 143 لسنة 1994، قانون حماية الملكية الفكرية رقم 82 لسنة 2002 ، قانون تنظيم الاتصالات 10 لسنة 2003، وقانون التوقيع الالكتروني 15 لسنة 2004، وقانون الطفل المعدل في 2008، إلا أن هذه القوانين لم تغط كافة صور التجريم الالكتروني راجع :- - قرار مجلس وزراء العدل العرب الدورة التاسعة القرار رقم 495-د19- 2003/10/8م ، ومجلس وزراء الداخلية العرب الدورة الحادية والعشرون القرار 417-د2004/21م)

ويتبقى التساؤل هل التوسع في تفسير النصوص القائمة لتطبيقها على جرائم الإنترنت يبقى هو الحل لتلافي هذه الفجوة؟

قد يبدو ذلك الحل أمام الدول التي لم تشرع قوانين لتجريم مختلف الجرائم الناتجة عن الاستخدام غير المشروع لشبكة الإنترنت سوى تطبيق القوانين القائمة بموادها التقليدية على هذه الوقائع خوفا من إفلات الجناة من قبضة العدالة.
ولكن تطبيق هذه النصوص التقليدية بمفهومها الواسع والخاصة ببعض الجرائم مثل السرقة وتطبيقها على بعض الوقائع التي تحدث على الانترنت من شأنه المساس بمبدأ الشرعية الجنائية **(Nullum crimen, nulla poena sine lege)** وهو من المبادئ الدستورية (حرص المشرع الدستوري المصري على النص عليه في المادة 95 من الدستور المصري الحالي الصادر في عام 2014)،(طنطاوي، 2007، صفحة 21) إذا ترك الأمر بيد القضاء لتفسير النصوص القائمة على نحو أوسع من الذي وضعت لأجله، من شأنه المساس بمبدأ الشرعية الجنائية (الكعبي، 2011، صفحة 53) (وهو ما يعد أحد أوجه النقض التي وجهت لمبدأ الشرعية الجنائية حيث قيل أن هذا المبدأ يقف عقبة في سبيل تطور المجتمع ورقيه لأن المشرع عندما يضع نصوص التجريم والعقاب فإنما يضعها لكي تحمى المصالح والحقوق التي تكون قائمة وقت التشريع وإذا كانت هذه المصالح بحكم طبيعتها قابلة للتطور قد يكون هذا التطور عن أفعال تمثل خطرا عليها، مما

يؤدي إلي عدم خضوع الكثير من الأفعال الضارة بمصالح المجتمع للعقاب لعدم وجود نص يجرمها ويعاقب عليها؛ ولعل ذلك ما يجعل المشرع يستخدم عند وضعه لنصوص التجريم والعقاب عبارات ذات أفكار قانونية عامة بحيث يمكن عن طريق تفسيرها التفسير السليم تحقيق التوازن بين المحافظة علي مبدأ الشرعية وبين الحاجة إلي تمكين القاضي من حماية المجتمع إزاء الأفعال الضارة التي تهدد مصالحه)

المطلب الثالث

تصنيفات الجريمة السيبرانية

TAXONOMIES OF CYBERCRIME

تعد ظاهرة الجرائم السيبرانية باعتبارها من الجرائم المستحدثة جرائم تنصب على معطيات الحاسوب (بيانات – معلومات – برامج) تطال الحق في المعلومات، ويستخدم لاقترافها وسائل تقنية تقتضي باستخدام الحاسب، ولا تعد الجرائم التي تنصب على الكيانات المادية مما يدخل في نطاق الجرائم التقليدية، ولا تندرج ضمن الجرائم المستجدة لجرائم الحاسوب.

وتصنف الجرائم السيبرانية إلى ثلاث فئات: – (Poonia, 2014)

1– الجرائم ضد الأفراد 2– الجرائم ضد الممتلكات 3– الجرائم ضد الحكومة (القاضي، 2011، صفحة 31)

وقد قسمت Sarah Oatis الجرائم السيبرانية إلي: –

1– الجريمة الافتراضية Virtual crime

2– الجريمة الهجينة Hybrid Crime

3– الجريمة التقليدية المعززة Augmentable Traditional crime

وقد قسمتها اتفاقية مجلس أوربا المعنية بالجرائم السيبرالية2001م إلى (احمد، 2002، صفحة 67): –

1– جرائم ضد سرية البيانات الحاسوبية وسلامتها

2– الجرائم المتعلقة بالحاسوب

– الجرائم المتعلقة بالمحتوي

الأنواع المختلفة للجرائم السيبرانية: –

(1) – الوصول غير المصرح به والقرصنة جريمة انتهاك الحق في الخصوصية والتي تحدث عندما يتم اعتراض المراسلات الالكترونية والاتصالات الالكترونية الخاصة بالغير. وهذه الجريمة تتعلق بكافة أشكال النقل الالكتروني للبيانات سواء عن طريق التليفون، أو الفاكس، أو البريد الالكتروني، أو غير ذلك من الوسائل التقنية الحديثة.

(2) اختراق الشبكة العنكبوتية HIJACKING WEB وهي السيطرة بالقوة على المواقع الإليكترونية للآخرين مما يفقد مالك الموقع السيطرة عليه

(3) دعارة الأطفال PORNOGRAPHY حيث يتم استخدام الإنترنت بشكل كبير كوسيلة للاعتداء الجنسي على الأطفال (عيسى،2000)، ويقع الأطفال ضحية للجريمة السيبرالية لسهولة الوصول إليهم على الشبكة وإثارتهم جنسيا والتحرش بهم ومحاولة مقابلتهم لممارسة الجنس معهم (التواب، 1995)، وأحيانا يستخدموا أطفال في نفس مراحلهم

السنية للتواصل معهم واستدراجهم (عبد، 2006)، وإقناعهم بأن ما يفعلونه شيء طبيعي.(Ford,2006, p 22)

(3) المطاردة الإليكترونية CYBER STALKING لملاحقة الالكترونية شبيهة بالملاحقة في الواقع، في تكرار التحرش بالضحية. التحرش الذي يحدث في العالم الافتراضي، لكن ممكن يرتبط بملاحقة حقيقية. منها مثلا نشر اتهامات كاذبة وافتراءات على الانترنت، سلوك مهدد، مراقبة المواقع الاجتماعية وعناوين الآي بي، الهجوم بفيروسات على الحواسيب والأجهزة الالكترونية، انتحال شخصية، النشر الخبيث لأشياء في حق الضحية (مثل أشياء إباحية)، وتشجيع الآخرين على الانضمام للتحرش، يمكن للملاحق نشر أرقام هواتف الضحية في المواقع التي تقدم الخدمات الجنسية، أو الاشتراك بالحساب الإليكترونية للضحية بعدد لا محدود من المواقع الإباحية وغيرها من طرق الملاحقة (النجار، 2009، صفحة 66).

(4) الحرمان من الاستفادة من الخدماتDENIAL OF SERVICE ATTACK يقوم المجرم بملىء صندوق البريد للضحية عن طريق رسائل FLOOD مما يعطل الموقع ويفقده فاعليته. (أنواع الجرائم الإليكترونية: –الإدارة العامة لمكافحة الفساد البحرين على الوقع http://www.acees.gov.bh/cyber-crime/types-of-cybercrim)

(5) قرصنة البرامج SOFTWARE PIRACY وذلك عن طريق النسخ غير القانوني للنسخ الأصلية لهذه البرامج وتوزيعها تجاريا، وانتهاك حقوق النشر والطبع والعلامات التجارية، وسرقة الكود الخاص بالحواسيب وانتهاك براءة الاختراعات المحمية بموجب قوانين العلامات التجارية (رشدي،2004، صفحة 31)

(6) – هجمات سلامي SLAMI ATTACK وتستخدم في الجرائم المالية كأن يقوم موظف البنك بإدراج في خوادم البنك برنامج يخصم مبالغ صغيرة جدا لا تلاحظ من حسابات العملاء في حسابه أو أي حساب آخر يقوم بإنشائه.

(7) هجمات الفيروسات VIRUS ATTACK فيروس الحاسوب هو برنامج خارجي صنع عمداً بغرض تغيير خصائص الملفات التي يصيبها لتقوم بتنفيذ بعض الأوامر إما بالإزالة، أو التعديل، أو التخريب وما شابهها من عمليات أي إن فيروسات الكومبيوتر هي برامج تتم كتابتها بواسطة مبرمجين محترفين بغرض إلحاق الضرر بكومبيوتر آخر، أو السيطرة عليه أو سرقة بيانات مهمة، وتتم كتابتها بطريقة معينة .

(8) الخداع أو الاحتيال PHISHING عن طريق إرسال رسائل بريد اليكتروني تدعي فيها فئة على غير الحقيقة إنشاء منشاة قانونية لخداع المستخدمين وإخضاعهم لإعطاء بياناتهم الخاصة التي يستخدمها الضحية بسرية مثل كلمات المرور– بطاقة الائتمان –رقم الضمان الاجتماعي– أرقام الحسابات المصرفية عن طريق المطالبة بتحديث البيانات بمواقع وهمية تستخدم فقط لسرقة معلومات المستخدمSALE OF ILLEGAL ARTICLES.، وأحيانا يتم استخدام المواقع في تجارة المواد غير المشروعة. (الجبوري،2014، صفحات 10–18).

(9) لعب القمار على الإنترنت ONLINE GAMBLING حيث توجم ملايين من المواقع من الخارج تقدم القمار على الإنترنت، ويعتقد أنها مواقع لغسل الأموال، ومعاملات الحوالة (المطيري، 2004)

(10) خداع انتحال الشخصية EMAIL SPOOFING منها تزوير البريد الإليكتروني وتتم من خلال السكربت المشهور MAILER ويتم تغيير عناوين أو أجزاء أخرى من الربد الإليكتروني من مصدر مختلف، ويقوم بإرسال بريد لشخص آخر يبدو أنه أرسل من شخص ما محاكاة للبريد الأصلي للحصول على كلمات المرور أو رقم بطاقات

الائتمان (منشاوي،1423هـ)

(11) التشهير الإليكتروني CYBER DEFAMTION ويقوم المجرم فيها بنشر مواد تشهيرية لشخص ما على مواقع الويب أو يرسل رسائل بريدية للعديد من الأشخاص بغرض التشهير بهذا الشخص ويسمى التشهير الإليكتروني (الشهري، 2017)

(12) التزوير FORGERY يتم استخدام الحاسوب والطابعات، وأجهزة الماسح الضوئي في تزوير وتزييف العملات والأوراق النقدية والطوابع البريدية وغيرها باستخدام هذه الأجهزة (حفصي،2014)

(13) سرقة المعلومات المتضمنة في محتوى اليكتروني THEFT OF INFORMATION CINTAINED IN ELECTRONIC FORM وتشمل سرقة المعلومات المخزنة في الأقراص الصلبة للحواسيب ووسائط التخزين .... وغيرها

(14) تفجير البريد الإليكتروني E-MAIL BOMBING وذلك عن طريق إرسال عدد ضخم من الرسائل إلى البريد الإليكتروني مما يؤدي إلى إتلافه.

(15) سرقة وقت الإنترنت INTERNET TIME THEFT يشير وقت الإنترنت إلى الاستخدام من قبل شخص غير مصرح له عدد من ساعات الإنترنت المدفوعة من قبل شخص آخر. (يونس، 2004)

(16) سرقة نظام الحاسوب THEFT COMPUTER SYSTEM تشمل سرقة الحاسوب، أو أية أجزاء منه.

(17) الإضرار المادي لنظام الكمبيوتر PHYSICALLY DAMAGING A COMPUTER SYSTEM تلحق هذه الجرائم أضرار مادية بجهاز الحاسوب وملحقاته.

(18) انتهاك الخصوصية والسرية BREACH OF PRIVACY AND CONFIDENTIALLITY الخصوصية هو حق الأفراد أو المجموعات أو المؤسسات أن يحددوا لأنفسهم، متى وكيف أو إلى أي مدى يمكن للمعلومات الخاصة بهم أن تصل للآخرين (قايد، 1988، صفحة 48)، والسرية تعني عدم الكشف عن المعلومات غير المصرح بها وغير المرغوب فيها وتسريبها مما يلحق بهم أضرار مادية ومعنوية (الأستاذ، 2013 صفحة 433)

(19) تراجع البيانات DATA DIDDLING وتتضمن تغيير البيانات قبل أو أثناء إدخالها على الحاسوب سواء عن طريق مدخل هذه البيانات، أو عن طريق البرامج والفيروسات، وتصميم برامج قاعدة البيانات أو التطبيقات، أو أي شخص يتضمن عملية إدخال أو تخزين البيانات، وتشمل التغيير التلقائي للمعلومات المالية قبل المعالجة.

(20) التجارة الإليكترونية والاستثمار الاحتيالي E-COMMERCE INVESTMENT FRAUD حيث يستخدم مزاعم كاذبة، أو مزورة لطلب استثمارات، أو قروض، أو شراء واستخدام، أو الاتجار في الأوراق المالية المزورة أو المزيفة والتعاقد على بيع البضائع عبر الإنترنت ولا يتم تسليمها (صراع، 2013)

(21) الإرهاب الإليكتروني CYBER TERRORISM ويشمل هجمات المنشآت العسكرية (Johnson,2004,p290-293)، (الشحات، 2002، صفحات 32-55) ومحطات توليد الكهرباء والسكة الحديدية ... وغيرها (مصطفى، 2017)

المبحث الثاني

الأخطار الناجمة عن الجرائم السيبرانية ودور مجلس التعاون الخليجي في المواجهة والإستراتيجية المقترحة في هذا الشأن

تعد تكنولوجيا المعلومات وقود الثورة الصناعية الثالثة، وأن المعلومات في حد ذاتها هي المادة الخام للإنتاج الذي يعتمد المجتمع على إنتاجها وإيجادها والاستفادة منها (الجندي، 2018)، هذا الوجه المشرق لتقنية المعلومات جاء خاليا من الجانب المظلم الذي يتمثل في الجرائم السيبرانية الذي استغل هذه التقنيات المتطورة لتحقيق مصالح ومآرب متنوعة ومتعددة (أحمد، 2003، صفحة 12؛ العريان، 2011، صفحة 23)

تعد أهم التحديات الإستراتيجية للمخاطر السيبرانية في المجتمع الخليجي، هو ضعف الإطار التنظيمي والقانوني وصعوبة تحذير المستخدمين في الوقت المناسب من المخاطر والحوادث السيبرانية المرتقبة لكون معظم المستخدمين لا يتابعون تطوراتها، بجانب انخفاض الوعي حول المخاطر السيبرانية (الحنيلي، 2017)، بجانب الزيادة الرهيبة في استخدام الإنترنت في المجتمع الخليجي وفق أخر الإحصائيات في هذا الشأن[1].

وشهد العالم تفاقم في مؤشرات الجرائم السيبرانية فاقت آثارها الاقتصادية آثار الجريمة التقليدية (Smith, 2008)، حيث بلغت الخسائر الناجمة عن الجرائم السيبرانية في القطاع المصرفي على سبيل المثال على الصعيد العالمي قرابة 114 مليار دولار أمريكي كل عام بسبب جرائم الإنترنت، وأن كلفة مكافحة جرائم الإنترنت تعدت ضعف هذا المبلغ حيث قدرت وفق أحد الإحصائيات قرابة 247 مليار دولار أمريكي، وقد تستغرق حل مشكلة تأثير الهجمات السيبرانية في القطاع المصرفي عشرة أيام كاملة مما يزيد من التكلفة (Parhiban, 2014)، ومما يستدعي القلق في هذا الشأن هو غياب خدمة تعريف وتجميع اتجاهات الجرائم السيبرانية (حوتيه وآخرون، 2015، صفحة 14)، ووضع نموذج موحد لها (Zirgutis, 2017)

ولعل هذا الأمر جعلنا ندق ناقوس الخطر نظرا للخسائر المادية والمعنوية الفادحة للجرائم السيبرانية والتي لا يمكن حصر كلفتها لا، وبخاصة نظرا لأهمية اقتصاديات دول مجلس التعاون الخليجي ليس على المستوى الإقليمي فحسب، بل وعلى المستوى العالمي، خاصة وأن أي اهتزاز فيها سيؤثر بالطبع على الاقتصاد العالمي بأكمله، ولذلك فقد رأينا تقسيم دراستنا لهذا المبحث وذلك على النحو التالي: –

المطلب الأول: – الأخطار الناجمة عن الجرائم السيبرانية في دول مجلس التعاون الخليجي.

المطلب الثاني: – دور مجلس التعاون الخليجي في مواجهة الجرائم السيبرانية.

المطلب الثالث: – الإستراتيجية المقترحة لتفعيل المواجهة.

[1] - أشارت أحدث الإحصائيات بخصوص مستخدمي الإنترنت عام 2018م في العالم يزيد على الأربعة مليار شخص (4,521)، وعلى صعيد المجتمع الخليجي بلغ مستخدمي الانترنت في قطر 2,640,360 بنسبة99%، وفي الكويت 4,100,000 بنسبة 98% والبحرين 1,499,193 بنسبة 89%، وأشارت إحصائية أخرى عدد المستخدمين في السعودية أكثر من 17 مليون59,2% من عدد السكان، والإمارات العربية 8,8 مليون بنسبة 93,4 من عدد السكان، وسلطنة عمان 2،5 مليون بنسبة 65,8 % من عدد السكان للمزيد يرجى مراجعة: -
- 2018 Digital in 2018 : World 'internet users pass 4 Billion mark.
- Number of internet user (2014) live stats.

المطلب الأول

الأخطار الناجمة عن الجرائم السيبرانية في دول مجلس التعاون الخليجي

تشهد اقتصاديات دول مجلس التعاون الخليجي ازدهارا اقتصاديا متصاعد مما جعل المنطقة هدفا جاذبا للجريمة السيبرانية (Menon, 2010) ، ومما زاد الأمر صعوبة وساعد في تفاقم آثار هذه الجريمة النمو المتسارع بشكل غير مسبوق في استخدام الشبكة المعلوماتية في دول مجلس التعاون الخليجي، لذلك ظلت قضية الحفاظ على أمن منطقة الخليج العربي تحتل رأس الأولويات الإستراتيجية ليس فقط لدول مجلس التعاون الخليجي فحسب بل ولجميع القوى والأطراف الإقليمية الدولية المعنية بأمن واستقرار هذه المنطقة الحيوية من العالم نظرا لما تملكه من ثروات وموقع إستراتيجي يتحكم في أهم الممرات المائية واعتبارها من الأسواق الجاذبة والواعدة للاستثمار (الهمري، 2010)

حيث شهدت المملكة العربية السعودية نمو بنسبة3000% في استخدام الإنترنت ففي الفترة من 2000–2009 أصبح23% من مستخدمي شبكة الإنترنت ضحايا للجرائم السيبرانية بحلول منصف عام2009م ، حيث أشار تقرير Trend Micro في أول تسعة أشهر من عام 2009م حيث سجلت 796.000 حالة هجوم سيبراني بلغت نسبتها 64% من إجمالي الحالات التي شهدها دول مجلس التعاون الخليجي، وفي دولة الإمارات العربية المتحدة في عام2011 أشار نفس التقرير عام 2011م أن76% من مستخدمي الإنترنت وقعوا ضحايا لمجرمين سيبرانين مخلفة خسائر قاربت المليار دولار(2.3 مليار درهم) ، وقد تم تسجيل248.000 هجوم سيبراني عام 2009م بنسبة 20% من إجمالي الهجمات التي تعرض لها مجلس التعاون الخليجي (Ajbaili M., 2009) ، بجانب 95000 هجوم في الكويت و60000 في مملكة البحرين و37000في سلطنة عمان.

وقد كانت دولة الإمارات العربية الشقيقة كعهدنا بها في الحقبة الأخيرة كقبلة وقدوة في المجال الأمني (مطر، 2013) وهذا ما يعنينا بالطبع بجانب التقدم الاقتصادي والتقني المذهل في شتى المجلات حيث قامت بتقوية أمنها الإليكتروني (تميم،2017، صفحة 2) مما أهلها لاحتلال المرتبة الأولي بين دول مجلس التعاون الخليجي والرابع عالميا في مجال الأمن الإليكتروني وفقا لتقرير صادر عن المعهد الدولي للتنمية الإدارية. (حسين، 2016)

وتتعدد الآثار الناجمة عن الجرائم السيبرانية: – (عقادة، 2003، صفحة 47)

على مستوى الفرد (سرقة الهوية – سرقة بطاقات الائتمان – الابتزاز والتهديد – عمليات الاحتيال– تحويل ونقل الحساب المصرفي – نقل ملكية الأسهم – زيادة الفواتير....)

وعلى مستوى البنوك والمؤسسات (السطو الإليكتروني – التلاعب بالبيانات الخاصة بالبنوك – سرقة الأموال– تحويل الحسابات المصرفية – الغش في المعلومات الإليكترونية– الاختراق والنفاذ غير المشروع...)

الانترنت العميق (صالح، 2018، صفحة 390) والذي يزدهر فيه الجانب المظلم من الإنترنت (Dark net) والذي أصبح ملاذا للمنظمات الإرهابية، والجريمة المنظمة وأصبح تهديدا لأمن الدول، وأصبحت العملات الافتراضية اللامركزية التي لا يمكن تعقبها أداة للتعامل، وتباع جميع الممنوعات في هذه الأسواق(Daniel, 2015)

وعلى مستوى المجتمع (بث الأفكار الهدامة والدعوات المنحرفة المخالفة للقيم والعادات والقانون– عرض المواد الإباحية والفاضحة الخادشة للحياء العام – التشهير والمضايقة وبث الشائعات– الاستغلال الجنسي للأطفال – انتهاك الحقوق

الخاصة والعامة) .

وعلى المستوى الحكومي (سرقة الأموال – تعطيل المرافق العامة – الإرهاب الإليكتروني ,Ngafesson) 1999,p120)

(Roshan N. 2008) وانتهاك سيادة الدولة وتجاوز حدودها الإقليمية حيث أن هذه الجرائم لا تقيم اعتبار للحدود الجغرافية للدول (الباب، 2003، صفحة 4) والتهديد للأمن من خلال زيادة فرص ارتكاب الجريمة (نمرابوسكي، 2006)

وقد تناول تقرير DETICA قياس تكاليف الجرائم السيبرانية أربعة تكاليف للجرائم السيبرانية

1- التكاليف المترتبة مثل (برامج الفيروسات والتأمين)
2- التكاليف الناجمة عن الجرائم السيبرانية مثل الخسائر المباشرة وغير المباشرة مثل ضعف القدرة التنافسية للملكية الفكرية)
3- تكاليف الآثار الجرائم السيبرانية مثل تعويض الضحايا والغرامات التي تدفعها الهيئات التنظيمية.
4- التكاليف غير المباشرة مثل الأذى الذي يلحق بالسمعة – وفقدان الثقة في المعاملات من قبل الأفراد وانخفاض عائدات القطاع العام ونمو الاقتصاد السري)

المطلب الثاني

دور مجلس التعاون الخليجي في مواجهة الجرائم السيبرانية

بعد أن استعرضنا الأخطار الناجمة عن الجرائم السيبرانية وآثارها الخطيرة على دول مجلس التعاون الخليجي، وضرورة التدخل العاجل والسريع وبشكل فعال لمواجهة هذه الظاهرة الخطيرة، والحد من آثارها ومكافحتها نظرا لأن شبكة الإنترنت أصبحت المجال الرئيسي والمحوري في شتى مناحي الحياة، هذا الأمر استدعى تدخل مجس التعاون لدول الخليج العربي (الكريطي، 2009) لمواجهة هذه الظاهرة وهو ما سنتناوله في هذا الجزء من الدراسة لمحاولة الخروج منها بإستراتيجية مقترحة للمواجهة الفعالة.

ولكن قبل التطرق غلى هذا الأمر رأينا أنه يجب التعرض: –

لأهم التحديات والعقبات التي تعترض سبل المواجهة الفعالة لهذه الظاهرة ومدى فاعلية تدخل مجلس التعاون الخليجي ونجاحه في تخطي هذه العقبات ومواجهة هذه التحديات لمواجهة هذه الظاهرة

أولا: – عدم الاتفاق على تعريف موحد للجرائم السيبرانية: –

استعرضنا في الجزء الأول من الدراسة التعرض لمفهوم الجرائم السيبرانية وتبين لنا عدم الاتفاق على تعريف موحد لهذه الجرائم، ويرجع ذلك بالطبع لاختلاف العادات والتقاليد بين الدول، وكذلك الطبيعة المتطورة لهذه الجرائم (ابراهيم، 2008، صفحات 40-41) الأمر الذي يمثل حجر عثرة في سبيل المواجهة الفعالة لهذه الظاهرة

ثانيا: –اختلاف التشريعات بين الدول: –

تتميز الجريمة السيبرانية على النحو الذي تم استعراضه بأنها جريمة عابرة للحدود وأن يمكن أن ترتكب في دولة وتطول

آثارها وخسائرها العديد من الدول (عبد الله، 2007، صفحة 18) ،(علاوي2007)، ومما لا شك فيه أن اختلاف التشريعات قد تجعل فعل مجرم في دولة غير مجرم في غيرها الأمر الذي قد يحبط من جهود الملاحقة القضائية لمرتكبي هذه الجرائم وتعد من أهم العقبات التي تحول دون المواجهة الفعالة (عباوي، 2017، صفحة 280)،(الشكري، 2008، صفحة 111) لذلك يتحتم على الدول وضع نموذج موحد لجميع الأفعال المجرمة المكونة للجريمة السيبرانية. (بوخبزة، 2012، صفحة 273)

ثالثا: – قصور التشريعات العربية في مواجهة الجريمة السيبرانية: –

وكانت دولة الإمارات العربية المتحدة من الدول ذات السبق في دق ناقوس الخطر فيما يخص اكتشاف هذا القصور والدعوى والعمل على قدم وساق لسد هذا الفراغ التشريعي. (وفي هذا الصدد وخلال المؤتمر الذي نظمته أكاديمية اتصالات إمارة دبي، حيث تم عمل محاكاة لجلسة محاكمة لأحد قراصنة الإنترنت المشهورين(فليكس ليندر26 عام) الذي استعانت به أحد الشركات لاختراق شبكة المعلومات الخاصة بشركة منافسة واستطاع من خلال ذلك الاختراق الحصول على ملف اليكتروني لأحد العروض الذي كانت تلك الشركة ستتقدم به في مناقصة لأحد المشروعات الضخمة وحصول الشركة المنافسة على هذا الملف وتقديم عطاء أقل مما مكنها من الفوز بهذا المشروع الضخم الذي بلغت قيمته 20 مليون دولار، وجرت المحاكمة بحضور قضاة من دولة الإمارات وقضاه أمريكي، وتمت إدانته وفقا للقانون الأمريكي وبراءة القاضي الإماراتي بسبب عدم تجريم الفعل في دولة الإمارات) (حجازي، 2005، صفحة 9)

رابعا: – عدم وجود قانون إجراءات ينظم التحقيق والتحري في هذه الجرائم: –

على الرغم من أن التشريعات الخليجية تتضمن أغلبها التعريفات للمصطلحات المستخدمة والتجريم الموضوعي، إلا أن العقبة الرئيسية التي تحول دون فاعلية هذه التشريعات عدم وجود قانون إجراءات ينظم التحري والتحقيق في هذه الجرائم، حيث أن غالبية دول الخليج العربي تعتمد على القواعد الإجرائية العامة التي(George, 2013) لا تأخذ في اعتبارها خصوصية الجرائم السيبرانية (Hakmeh J.C,2017)، وفي ظل غياب مثل هذه الأحكام فإن قدرة الدول على التحقيق والملاحقة القضائية والفصل في الجرائم السيبرانية وتسيير التعاون في التحقيقات عبر الدول مهددة بالفشل بدونها (Alwast, 2015) (Aljneibi , K,2014) و (هروال، 2007)

خامسا: – التوفيق بين حقوق الإنسان والمواجهة: –

وما يعنينا في هذا المجال هي حريات التعبير وحرية المعلومات والنشاط السياسي وحرية التجمع وتكوين الجمعيات، حيث أن كل دول مجلس التعاون الخليجي عدا سلطنة عمان أعضاء في الميثاق العربي لحقوق الإنسان (الميثاق، 2004)، ويبدو أن هناك مشكلة في التوفيق بين حماية الأخلاق العامة والنظام العام والصحة العامة والأمن القومي والحق في الخصوصية[2] والحق في الخصوصية من أهم الحقوق والقيم للإنسان فقد أكد علماء الاجتماع وعلم النفس أن للإنسان حاجة ضرورية للخصوصية فهي من صميم قيم الديمقراطية (Kang J.,1998).، وهى التزام في جميع

[2] ولا تعد مشكلة الخصوصية المعلوماتية مجرد مشكلة سياسية داخلية ، ويرجع ذلك للسهولة التي يتم بها نقل المعلومة خارج حدود بلد المنشأ ، وكذلك فقد حرص صكان دوليان هامان التأكيد على ذلك وهما اتفاقية مجلس أوربا 1981 بشان حماية الأفراد فيما يتعلق بالمعالجة التلقائية للمعلومات الشخصية ، اتفاقية مجلس أوربا ومنظمة التعاون والتنمية في الميدان الاقتصادية OCED والتي عدن بمثابة مبادئ توجيهية تحكم حماية الخصوصية وتدفق البيانات عبر الحدود ، وفي عام 1995م أصدر الإتحاد الأوربي توجيه حماية البيانات من أجل موازنة قوانين الدول الأعضاء في توفير مستويات متسقة من الحماية للمواطنين مع ضمان التدفق الحر للبيانات الشخصية في مواد 25،26 والتي حرصت على أن البيانات الشخصية ينبغي أن تتدفق فقط إل دول خارج الإتحاد الأوربي للدول التي تضمن مستوى كاف من الحماية

تشريعات دول مجلس التعاون وبين حرية التعبير، مما دعا بعض المنظمات ذات التوجهات الغير منضبطة إلى إدانة بعض دول المجلس (H.R.W, 2012)

سادسا: – عدم الوعي من رجال إنفاذ القانون (شرطة– نيابة– قضاه – محامون)

بأهمية المعلومات المتحصلة من المصادر الإليكترونية (Makkaik,2004) وطريقة التعامل مع الأدلة وتحصيلها والحفاظ عليها (Paul,2008,p 13-14) وقلة وضعف المختبرات العلمية التي تتعامل مع الجريمة السيبرانية وعدم كفايتها وضعف الكوادر اللازمة للتعامل العلمي معها (الهاجري، 2011)(Howell ,2005)، وقلة الدورات التدريبية (Kelman,2002) (Bohm,2004)

سابعا: – ضعف الوعي القومي لدى المواطن العادي بخطورة الجرائم السيبرانية وطرق الحماية منها والإحجام عن الإبلاغ عن هذه الجرائم سواء على مستوى الأفراد، أو المؤسسات وكلا له ما يبرر له ذلك.

ثامنا: – ضعف التنسيق والتعاون coordination and cooperation حيث إن هذه الجريمة جريمة ذات طبيعة عالمية عابرة للحدود فلابد من التعاون الدولي دون النظر إلى الاعتبارات السياسية (وفي هذا الصدد فقد كان مجلس التعاون لدول الخليج العربي حريصا على تفعيل آليات التعاون الدولي والإقليمي للحد من تفشي ظاهرة الجريمة السيبرانية وهو ما سيتم تفصيله لاحقا إيمان من المجلس بالدور الهام والفعل لآليات التعاون والتنسيق.)

تاسعا: – سهولة إخفاء معالم الجريمة وصعوبة الحصول على الأدلة لسهولة تدميرها والتخلص منها ووجود كم كبير من المعلومات يتعين فحصها

جهود مجلس التعاون الخليجي في مكافحة الجريمة السيبرانية: –

أولا: – المؤتمرات التي عقدتها دول مجلس التعاون الخليجي لمواجهة الجرائم السيبرانية: – كان لدول مجلس التعاون الخليجي دورا ملموسا في عقد العديد من المؤتمرات لمواجهة الجريمة السيبرانية لعل من أهمها: –

- **مؤتمر أبو ظبي لمكافحة الجرائم الإلكترونية في دول مجلس التعاون الخليجي 18–6–2007**نظمه معهد التدريب والدراسات القضائية بالتعاون مع شركة مايكروسوفت على أهمية تجنب المخاطر التي تشكلها الجرائم الإلكترونية وأهمية الحلول الإجرائية والموضوعية للحد منها .
- **مؤتمر أبو ظبي العالمي للأمن السيبراني التهديدات الوطنية المشتركة –** الحماية والتعليم بالاشتراك وتمويل من معهد نيويورك للتكنولوجيا والكلية العالمية للتكنولوجيا أبو ظبي[3].
- **مؤتمر الأمن السيبراني مسقط 23**–24 مارس 2014م لمناقشة أهمية الأمن السيبراني نظرا للاستخدام المتزايد لتكنولوجيا المعلومات والاتصال[4]

[3] - Global cyber security conference in Abu Dhabi : National and cooperate threats and protection &education , March 25,2014.

[4] - للمزيد من التفاصيل أنظر أوراق عمل ووثائق المؤتمر الإقليمي للأمن السيبراني مسقط 20-21 أبريل .2014 على الموقع http//www.cybersecuritysummit.com

- **مؤتمر الأمن السيبراني الدوحة103 ديسمبر2014 والذي نظمته** شركة تانجينت لينك البريطانية تحت رعاية شركة معلوماتية القطرية أهمية مراقبة التهديدات وضرورة تبني نهج استباقي لإدارة أهداف الأمن السيبراني لمؤسسات القطاعين العام والخاص، وحماية مصالح حاملي الأسهم في بيئة رقمية.
- **المؤتمر الدولي الأول حول مكافحة جرائم الإنترنت** الرياض السعودية لرفع مستوى مكافحة جرائم الإنترنت باستخدام التقنيات الحديثة والاستفادة من التجارب الدولية في هذا الشأن عام 2015م

اجتماع الخبراء الإقليمي لدول الخليج العربي لحماية الشباب من مخاطر الجريمة السيبرانية الكويت 20-21 مارس 2017م

هذا بجانب العديد من المؤتمرات التي يتبين منها حرص دول مجلس التعاون الخليجي لعقد العديد من المؤتمرات والتي لا يتسع المجال لذكرها جميعا لضيق المساحة المخصصة لهذه الدراسة واكتفينا بالإشارة لبعض منها على سبيل الاستدلال دون الاستفاضة.

ثانيا: – المراكز الوطنية الخليجية لحماية الأمن السيبراني (نزوي،2016): – فرق الاستجابة لطوارئ الحاسب الآلي لحماية الأمن السيبراني ومواجهة الجريمة الإليكترونية (Computer Emergency Response Team (CERTs: –

- مركز الاستجابة لطوارئ الحاسب الآلي في دولة الإمارات والمنشأ بواسطة هيئة الاتصالات الإماراتية عام 2007م.
- المركز الوطني الإرشادي لأمن المعلومات والمنشأ بمعرفة هيئة الاتصالات وتقنية المعلومات السعودية.
- المركز الوطني للاستجابة لطوارئ الحاسب الآلي الكويت وتم الإعلان عن تأسيسه في 19 مايو 2012 إلا أن الجهاز المركزي لتكنولوجيا المعلومات أعلن عن بدء أعمال المركز الوطني للاستجابة لطوارئ الحاسبات في ندوة نظمها في مقره للجهات الحكومية للتعريف بأعمال المركز ومهامه. عام2015.
- المركز الوطني للسلامة المعلوماتية بسلطنة عمان وتم من خلاله إنشاء مركز الاستجابة لطوارئ الحاسب الآلي في أبريل 2010م.
- فريق الاستجابة لطوارئ الحاسب الآلي القطري والمنشأ بواسطة المجلس الأعلى لهيئة تقنية المعلومات والاتصالات القطرية ديسمبر 2005م.

ثالثا: –مشروع الربط الشبكي بين برامج الحكومات الإليكترونية بدول مجلس التعاون الخليجي

يهدف هذا المشروع غلى ربط برامج الحكومات الإليكترونية بدول المجلس بشبكة معلومات أمنة وذات موثوقية وأداء عاليين، ويسهل التبادل الأمن لبيانات الخدمات الإليكترونية وذلك بين الأجهزة الحكومية ذات العلاقة بدول الخليج، كما يهدف هذا المشروع إلى توفير الشبكة والأدوات اللازمة لتقديم خدمات إلكترونية أكثر كفاءة، وتكون وسيلة أمنة لتبادل بيانات الخدمات الإليكترونية. (الجريدة الرسمية لمجلس التعاون لدول الخليج العربي، العدد السابع عشر، السنة الخامسة، 15 يناير 2017م.)

كما يهدف المشروع إلى توفير تبادل آمن للبيانات والمعلومات الإليكترونية بين برامج الحكومات الإليكترونية بين دول مجلس التعاون من خلال توفير أعلى معايير أمن وسلامة المعلومات لضمان مستوى عالي لسرية المعلومات، وتم الاتفاق أن يكون التواصل من خلال المراكز الرئيسية لبرامج الخدمات الإليكترونية بدول المجلس فقط ولضمان أمن

الشبكة من أي اختراقات.

مراحل تنفيذ المشروع: – تم تقسيم مراحل تنفيذ المشروع إلى أربعة مراحل وأكد المشروع على أهمية أمن البيانات واعتبار ذلك أمر جوهري في غاية الأهمية، وقد تم اعتماد أكثر من أسلوب وأداة لضمان أمن وسرية وسلامة البيانات المرسلة والمستقبلة بين دول المجلي على النحو التالي: –

- تقنية الشبكة الافتراضية MPLS VPN وتعمل على تسهيل ربط المواقع التابعة لمجلس التعاون الخليجي، وتتكون من أقراص موحدة وخاصة.
- الجدران النارية FIREWALLS حيث ترتبط مراكز الخدمات الإليكترونية لدول مجلس التعاون بالشبكة عن طريق جدر نارية لمنع أية اختراقات ومراقبة العمليات التي تمر بالشبكة.
- أسلوب تشفير الربط PSEC VPN حيث تم اعتماد أمن بروتوكول الاتصال المشفر لضمان سرية وسلامة البيانات المرسلة والمستقبلة على السواء بين الدول المتصلة بالشبكة عن طريق ثلاثة بروتوكولات الأول رأس المصادقة Authentication header(AH) في توقيع الرسائل والبيانات والثاني استخدام Encapsulating security payload تغليف الحمولة الأمنية في التشفير والتوقيع معاEncryption and signing لضمان مصداقية المرسل Source authentication، والتشفير للبيانات Data encryption الثالث internet key exchange تبادل مفاتيح الإنترنت لضمان الكيفية وعملية توزيع ومشاركة المفاتيح بين مستخدمي IPSEC مجموعة البروتوكولات، كما تعمل الشبكة على التدقيق الخارجي لأمن المعلومات External security auditing وذلك بتطبيق الحلول الأمنية لضمان سلامة وسرية الاتصال بين الدول الأعضاء وتقييم مدى تطبيق المعايير القياسية العالمية في مجال أمن المعلومات بالشبكة.

المطلب الثالث

الإستراتيجية المقترحة لتفعيل المواجهة

بعد أن استعرضنا الجريمة السيبرانية من خلال تعريفها والتعرض لأهم خصائصها وتصنيفاتها، والآثار التي قد تنجم عنها، ودور مجلس التعاون الخليجي في مواجهة هذه الظاهرة تبقى لنا من خلال الاستعراض السابق ضرورة تبني إستراتيجية موحدة مقترحة من جانبنا وذلك بعد التعرض لأهم التحديات والعقبات التي تواجهه مكافحة تفشي هذه الظاهرة الإجرامية الخطيرة وذلك بغية التغلب على هذه العقبات، ومن أجل مواجهة فعالة وناجزه، وتتكون هذه الإستراتيجية من عدة محاور وذلك على النحو التالي: –

أولا: – المحور التشريعي: –legislation axis ينقسم هذا المحور لعدة اتجاهات: –

الاتجاه الأول: – تشريع موحد لمكافحة الجريمة السيبرانية: –

نقصد المحور التشريعي إنشاء تشريع موحد يتم إقراره في جميع دول مجلس التعاون الخليجي يتضمن تعريف موحد للجريمة السيبرانية يتم الاتفاق علي بين جميع دول مجلس التعاون حيث أنه من العقبات الرئيسية التي تحد من المواجهة الفعالة لهذه الظاهرة اختلاف التشريعات وتنازعها، حيث أن ظهور الجرائم السيبرانية خلق تحديات كثيرة في مواجهة النظام القانوني القائم (عكور،2014) ويجب حل جميع الإشكاليات الخاصة بالأفعال المجرمة وحل مشكلات تنازع

الاختصاصات والملاحقة القضائية ومراعاة مبدأ التناسب والضرورة في التوازن بين الحقوق والحريات وفاعلية المواجهة ، وغيرها من الإشكاليات على أن يتوافق هذا التشريع الموحد مع المعايير العالمية والتشريعات الناجحة في التجارب الدولية الرائدة ، مع المراجعة الدورية للتشريع لسد أي ثغرات ناجمة عن تطبيق القانون أو بسبب الطبيعة المتطورة لهذه الجريمة وظهور أنماط متطورة لها،(حسين، 2002، صفحة 38) وكذا بحث مسئولية مزودي الخدمة Internet Service Provider(I.S.P) وهي المشكلة التي مازالت محل خلاف وتتعدد فيها الاتجاهات الفقهية والتشريعية (رمضان، 2007، صفحات 57-69)

الاتجاه الثاني:- سن تشريع إجراءات خاص بهذه الجرائم:-Code of cyber Criminal Proceedings :-

تبين لنا من خلال الاستعراض السابق أن المشكلة الرئيسية ليست في وجود تشريعات لمواجهة الإجرام السيبراني حيث أنها متواجدة بالفعل ،(عوض، 1971، صفحة 657) ولكن وجود هذه القوانين بدون إجراءات جنائية تراعي طبيعة هذه الجريمة وطبيعة الأدلة السيبرانية (سلامة، 1977) (والتي لا تتناسب معها القواعد الإجرائية التقليدية التي لا تراعي الطبيعة المتفردة لها يتناول إجراءات استخلاص الأدلة وكيفية التعامل معها، تشريع يواجه التحديات التي تواجه جميع القائمين على التعامل مع الجرائم السيبرانية سواء قضاة أو محامين أو النيابة المختصة (Paul,2008)، هذا الأمر مجاله متسع للغاية ولكن لا نستطيع الإبحار فيه لاتساعه وضيق المساحة.

الاتجاه الثالث: - تبني سياسة عقابية جديدة: -

تعد الجرائم السيبرانية من جرائم ذو الياقات البيضاء White collar crimes والتي يتميز مرتكبيها بسمات خاصة تجعله يختلف بشكل كامل عن الصورة الذهنية المعروفة للمجرم التقليدي حيث يتميز مرتكبيها بالمهارة – المعرفة – الوسيلة حيث تتميز الوسيلة بالبساطة وسهولة الحصول عليها – السلطة مثل الشفرة الخاصة بالدخول على النظام (السعيد، 2002)، سلطة استخدام الحاسب – الباعث حيث يكون الباعث مختلف اقوي هذه البواعث الرغبة في قهر النظام ونشوة الانتصار (ابراهيم، 2009، ص 78) وتخطي الحواجز الخاصة بالحماية.(الحديثي، 1992، صفحة 11)

وهذا ما دعانا إلى أن ننادي بضرورة أن تتبني هذه الإستراتيجية سياسة عقابية غير تقليدية تراعي الطبيعة التقنية لهذه الجريمة مثل: -

- **تطبيق برامج إصلاح وتأهيل** Reform **and rehabilitation خاصة** بالمحكومين في هذا النوع من الجرائم، بحيث تهدف هذه البرامج إلى إعادة تأهيل المجرمين ومحاولة الاستفادة منهم وتجنيدهم لحساب الدولة
- **التوسع في العقوبات الافتراضية Virtual penalties الغير سالبة للحرية في** بعض أنماط الجرائم السيبرانية بما يتناسب مع الطبيعة التقنية لهذه الجريمة ونقترح في هذا الصدد إيجاد وسيلة تقنية **تمكن من سلب الحرية الرقمية** بما يكفل منع مرتكبي بعض أنماط الجرائم السيبرانية من الدخول على شبكة الإنترنت، سواء عن طريف أنشاء هوية سيبرانية لكل مواطن لا يمكنه الدخول والنفاذ إلى الشبكة السيبرانية بدونها وبالتالي يمكن عقابه بسلب حريته الرقمية بما يكفل الردع الذي يتناسب مع السمات الشخصية لمرتكبي هذه الجرائم، أو بأي وسيلة أخرى تحقق الهدف المنشود.

هذا بجانب العقوبات التقليدية الأخرى والعقوبات التبعية في بعض الأنماط الأخرى الخطيرة التي تستلزم تشديد العقوبة والحزم الشديد لتحقيق الردع الكافي لكل من تسول له نفسه اقترافها.

ثانيا المحور الهيكلي The structural Axis: –

نقترح في هذا المحور إنشاء كيان معني بحماية الأمن السيبراني في دول مجلس التعاون الخليجي واقترحنا لهذا الكيان مسمى مؤسسة الخليج للأمن السيبراني

GULF INSTITUTION FOR CYBER SECURITY (G.I.C.S) على أن تكون هذه المؤسسة ذات طبيعة إقليمية تعمل تحت مظلة مجلس التعاون الخليجي تعنى بحماية الأمن السيبراني

أهداف المؤسسة: –

- توحيد التشريعات المعنية بحماية الأمن السيبراني والجرائم السيبرانية، والإجراءات الجنائية داخل دول مجلس التعاون الخليجي مواكبا للتطورات في مجال الأمن السيبراني
- تدبير التمويل اللازم لمواجهة الجرائم السيبرانية وحماية الأمن السيبراني، حيث يعد التمويل والتكلفة المالية Financial Costالعالية من العقبات الرئيسية التي تجهض أية فعاليات لمواجهة هذه الجريمة بالشكل المطلوب والذي يحقق الهدف المنشود.
- اتخاذ كافة التدابير اللازمة لحماية البنى التحتية السيبرانية بداخل دول مجلس التعاون.
- تعزيز ورفع قدرة المعامل والمختبرات الفنية اللازمة لحماية الأمن السيبراني، وكشف وتحصيل والمحافظة على الأدلة اللازمة لكشف الجرائم بما يضمن التوصل لمرتكبيها ومعاقبتهم وردعهم.
- إعداد وتدريب الكوادر اللازمة لرجال إنفاذ القانون (نيابة – قضاة – محامين– خبراء أدلة) بهدف أعداد كوادر مؤهلة للتعامل مع الجرائم السيبرانية لمنع الإفلات من العقاب، ولتحقيق أعلى معدلات في ضبط ومكافحة هذه الجرائم.
- خلق مناخ جيد للاستثمار وبيئة تحفيزية للمستثمرين عن طريق إيجاد بني تحتية سيبرانية، وحماية للمعلوماتية وبرامج الإنترنت والمعلوماتية التي تعتمد عليها الشركات الاستثمارية
- التنسيق مع مختلف التحالفات الإقليمية والدولية والمنظمات والمؤسسات المعنية بمكافحة الجرائم السيبرانية، وحماية الأمن السيبراني، وصياغة الاتفاقيات الثنائية الإقليمية أو الدولية المعنية بذلك الأمر.
- تفعيل سبل التعاون الإقليمي والدولي سواء بين الدول والمؤسسات الدولية والشرطية لمكافحة هذه الظاهرة بما يضمن الملاحقة القضائية والمحاكمة وتسليم مرتكبي هذه الجرائم واستثناء هذه الجرائم من أية موانع تمنع التسليم لخطورتها
- إنشاء وكالة الخليج لحماية البنى التحتية Gulf Agency For Information Infrastructure Protection(G.A.I.I.P) على أن يكون هذا الكيان الجهاز التنفيذي لهذه المؤسسة يتكون من أعضاء من دول مجلس التعاون الخليجي وتتكون من جمعية ومجلس وسكرتارية يديرها أمين عام لتنفيذ الأهداف السابق الإشارة إليها، وتقترح التوصيات والاقتراحات والتعديلات والتشريعات وغيرها مما يمكن من تنفيذ أهداف المؤسسة، والنظر في التدابير التي تقترحها المؤسسة لمنع أية دولة من دول مجلس التعاون الخليجي أن يتم استخدامها كملاذ آمن لانتهاك الأمن السيبراني وتعريضه للخطر وتهديد البنى التحتية السيبرانية لدول المجلس.

- تنسيق التعاون مع الأجهزة الشرطية المعنية الإقليمية والدولية (شرطة الخليج – يور وبول– الانتربول ... وغيرها) وغيرها من أجل التحقيق، والضبط، وتفعيل الملاحقة، والتسليم.
- تقديم المساعدة للدول المتضررة من الجرائم السيبرانية عن طريق إنشاء فرق طوارئ من الكوادر الفنية ذات المستوى التقني العالي للتدخل السريع لمواجهة أية انتهاكات أو اعتداءات على البنى التحتية لدول المجلس.
- تشكيل شبكة مشتركة بين دول المجلس للربط بين حكومات دول مجلس التعاون الخليجي لحماية الأمن السيبراني وربطها بالشبكات الدولية ذات الصلة بنفس الموضوع.
- إعداد البرامج التدريبية لرجال إنفاذ القانون في الجرائم السيبرانية لرفع الكفاءة، وكذا البرامج التوعوية والمناهج الدراسية لرفع الوعي لدى مواطني دول مجلس التعاون الخليجي.
- دعم وتعزيز المختبرات الفنية ذات الكفاءة التقنية العالية والمدعمة بأحدث التقنيات الفاعلة في مجال المواجهة، ورفع كفاءة الفنيين والتقنيين العاملين بها.
- بناء القدرات في مجال تقنية المعلومات لرصد وتحليل التهديدات الأمنية المحتملة للجريمة التقنية وآثارها.
- توفير برامج حماية المعلومات التقنية وخاصة المعلومات ذات الحساسية والبنى التحتية لها Critical Information Infrastructure
- تقديم التقارير الدورية عن حالة البنى التحتية السيبرانية.

ثالثا محور التدريب والتعليم: –Training and Education Axis: –

يعد محور التدريب والتعليم من أهم المحاور التي ترتكز عليها هذه الإستراتيجية فقانون بدون كوادر بشرية لا قيمة له وهو والعدم سواء، ومعامل ومختبرات بدون هذه الكوادر تصبح عديمة الفائدة وتفقد الهدف المرجو منها وتعد إهدارا للمال العام، كما أنه انطلاقا من مبدأ الوقاية خير من العلاج فإن دور التوعوي والتعليمي لرفع مستوى الوعي بشأن مخاطر الجرائم السيبرانية لا شك أنه الطريق السليم الذي يحد من هذه الجرائم ويحمي المجتمع من خطر الوقوع في براثن هذه الجريمة ويوفر مبالغ طائلة تنفق لمواجهة هذه الجرائم. ونقترح أن يتم تفعيل هذا الأمر من خلال الآتي: –

- إعداد البرامج التدريبية التي تواكب أحدث المستجدات في مجال الأمن السيبراني والجرائم السيبرانية، وحماية البنى التحتية المعلوماتية وأمن الشبكات ورفع والتحصل والحفاظ على الأدلة السيبرانية لرجال إنفاذ القانون.
- إعداد البرامج التوعوية في مجال التوعية من مخاطر الجرائم السيبرانية وطرق تحققها، وأهم الإجراءات الوقاية منها، وطرق الأمن السيبراني، والاستخدام الآمن لشبكة الإنترنت، فغياب الوعي التقني بكيفية التعامل الآمن مع التقنيات الحديثة يمكن أن يؤدي إلى الوقوع في خطأ ارتكاب الجريمة وليس مجرد التعرض لها (البحيري، 2011، صفحة 18)
- إعداد البرامج والمناهج الدراسية الخاصة بالجرائم والأدلة السيبرانية، وبخاصة في كليات القانون وتكنولوجيا المعلومات والاتصالات، والمناهج المبسطة التي تتناسب مع مختلف المراحل التعليمية المختلفة.
- بناء القدرات(Capacity Building) في مجال تقنية المعلومات لرصد وتحليل التهديدات الأمنية المحتملة للجريمة الإليكترونية وآثارها.
- إنشاء مراكز علمية متطورة لدراسة أحدث المستجدات والتطورات في مجال الجرائم السيبرانية، ومستجدات دعم وتعزيز الأمن السيبراني.

- تشجيع البحث العلمي والتطوير في مجال الأمن السيبراني والجرائم السيبرانية، ورصد انتهاكاتها وضبط أدلتها ومرتكبيها.
- عقد المؤتمرات الدولية والإقليمية والمحلية والمشاركة في المؤتمرات الخارجية في الدول المتقدمة بعد انتقاء وفرز أفضل العناصر والكوادر البشرية في مجال الأمن السيبراني الجرائم السيبرانية.
- إنشاء مراكز بحثية على شاكلة مراكز دراسة العلوم الجنائية تعنى بدراسة العلم الجنائي السيبراني تحت مسمى مراكز أبحاث الأمن السيبراني الدفاعي .Cyber Defense Research Centers لدراسة الظواهر الإجرامية فما يخص انتهاكات الشبكة السيبرانية ودوافع ارتكابها
- دراسة أثر البطالة على ارتكاب هذه الجريمة ودورها في ارتفاع نسبة ارتكاب الجريمة والعمل على حل هذه المشكلة الخطيرة لدى الشباب التي هي آفة خطيرة وعامل مشترك في ارتفاع معدلات ارتكاب جميع الجرائم سواء التقليدية أو المستحدثة على السواء فالمواجهة يجب أن يشترك فيها جميع مؤسسات الدول وألا تقتصر المواجهة على الجانب الأمني فقط.
- تنمية البرامج الدينية المتصلة بالجرائم السيبرانية وإظهار دور القيم الدينية المناهضة لجرائم السيبرانية والتي لو التزم بها الشباب وتقوية الوازع الديني لقلت نسب ارتكاب الجريمة السيبرانية باعتبار أن هذه الجرائم تتنافى مع صحيح الدين.
- وضع أطر وقواعد وتأسيس العلم الجنائي السيبراني على أن يتضمن الجرائم السيبرانية وتعريفها وأركانها والإجراءات الجنائية الخاصة بالأدلة الرقمية ومشروعيتها الطرق الكفيلة بترسيخ حجيتها القضائية وغيرها مما يستجد من قواعد على أن يتميز هذه العلم بالمرونة المستمرة بالطرق التي تكفل المراجعة المستمرة الدورية له نظرا لما تتسم ب هذه الجرائم من طبيعة تقنية متطورة، وألا يتسم بالجمود وعدم القابلية للتطوير.
- إعداد برامج وإستراتيجيات لإدارة الأزمات على أسس علمية في مهددات الأمن السيبراني.
- إنشاء مفوضية خاصة بتعليم الأمن السيبراني وطرق الوقاية من الجرائم السيبرانية.
- تنظيم معسكرات صيفية للطلاب تركز برامجها على الأمن السيبراني، وتنظيم فعاليات ترويجية لمفهوم الأمن السيبراني في الجامعات.
- تنظيم مسابقات الدفاع السيبراني cyber defense بين الجامعات لتحفيز الطلاب في دول مجلس التعاون الخليجي على المشاركة وتنمية الإبداع في مجال مواجهة الجرائم السيبرانية وطرق الوقاية منها على اعتبار أن الشباب هم أغلب المستهدفين بهذه الجرائم وفي نفس الوقت اغلب مرتكبيها.

رابعا محور التنسيق التعاون الدولي– International Coordination and cooperation Axis:

تبين لنا من خلال استعراض أهم خصائص الجرائم السيبرانية أنها جرائم ذات طابع دولي عابرة للحدود فمن الممكن أن ترتكب في دولة وتتعدى آثارها العديد من الدول، فهي جريمة تختفي معها وتتضاءل الحدود الجغرافية وتتلاشى فيها اعتبارات السيادة الوطنية، وعلية فإن الجهود الوطنية لمواجهة هذه الظاهرة مهما بلغت درجة كمالها تصبح هي والعدم سواء بدون هذا المحور الهام ومن أجل تفعيل هذا المحور نقترح الآتي: – (حجازي، 2011، ص102)

- إنشاء تحالف إقليمي لدول مجلس التعاون الخليجي تحت مظلة مجلس التعاون الخليجي ويرتبط بشراكة مع منظمة التحالف الدولي لحماية الأمن السيبراني[5] لحماية الأمن السيبراني والجرائم السيبرانية.
- تعزيز جهود التعاون الدولي بعقد المؤتمرات الدولية والإقليمية لمواجهة الجرائم السيبرانية، والمشاركة فيها خارج نطاق مجلس التعاون الخليجي.
- دراسة مقترح انضمام مجلس التعاون الخليجي لاتفاقية مجلس أوربا للجرائم السيبرانية (المفتوحة) بوصفها أول وأهم مبادرة عالمية في هذا المجال
- التوسع في الاتفاقيات الدولية الثنائية والمتعددة الإقليمية أو الدولية للحد من الجرائم السيبرانية وضبط مرتكبيها ومحاكمتهم وذلك لتقليل والحد من ظاهرة الإفلات من العقاب وللحد من والتقليل من الملاذ الآمن لمرتكبي هذه الجرائم.
- تنظيم التنسيق والتعاون القضائي لحل الإشكاليات الخاصة بتنازع القوانين والاختصاص والملاحقة القضائية والتحقيق وتسليم المجرمين.
- التوسع في اتفاقيات الخاصة بتسليم مرتكبي هذه الجرائم للحد من دعوى السيادة الوطنية والاعتبارات السياسية التي تحول دون تسليم مرتكبي هذه الجرائم فبدون المحاسبة تصبح جميع هذه الجهود عدما بلا قيمة ولا تساوي قيمتها المداد الذي سطرت به
- إنشاء جهاز شرطي خاص بمكافحة هذه الجرائم مكون من خبراء من جميع دول مجلس التعاون له اختصاص مكاني يشمل جميع دول مجلس التعاون الخليجي ومزود بالكوادر البشرية المدربة والمؤهلة للتعامل مع هذه الجرائم وفرق التدخل السريع لمواجهة أيه انتهاكات وتعديات على البنى التحتية السيبرانية
- إنشاء محكمة جزائية خاصة موحدة لدول مجلس التعاون الخليجي لمحاكمة مرتكبي الجرائم السيبرانية.

الخاتمة

حققت البشرية فوائد عظيمه ونقلة نوعية تاريخية نتيجة للثورة التكنولوجية الهائلة في جمال تقنية المعلومات والاتصالات وتطبيقات الحاسب الآلي وشبكة الإنترنت، حيت أصبح الاعتماد على هذه التقنيات أحد أبرز أساسيات الحياة المعاصرة في كافة المجالات الاقتصادية والاجتماعية والسياسية والأمنية والدفاع، بما تشمله من تفاصيل، وعلى مستوى الأفراد. وحقق استخدام هذه التقنيات نهضة كبرى غير مسبوقة وازدهارا علميا واقتصاديا، وصناعيا، وطبيا، وهندسيا.. إلخ.

ومن هنا تبدو أهمية مواجهة الجرائم السيبرانية حيث أصبح استخدام الإنترنت عصب الحياة العصرية في شتى المجالات سواء على مستوى الأفراد أو المؤسسات بمختلف أنواعها ، ونظرا لما تمثل بيئة المجتمع الخليجي وتشهده من نهضة اقتصادية غير مسبوقة وما تملكه من ثروات جعلها قبلة المستثمرين من شتى بقاع العالم بجانب موقعها الإستراتيجية وتحكمها في العديد من الممرات الإستراتيجية، الأمر الذي خلق منها بيئة خصبة لنمو وتنامي الجريمة السيبرانية بما تمثله وتفرزه من آثار خطيرة على المجتمع الخليجي في شتى مجالات الحياة، ومن هنا أضحى تدخل مجلس التعاون لدول مجلس الخليج العربي أمرا واجبا وألا يقف مكتوف الأيدي والتصدي الفوري لهذه الظاهرة الخطيرة.

وقد قسمنا دراستنا البحثية من أجل وصولها لمبتغاها إلى شقين، في الشق الأول تناولها تعريف مفردات الدراسة من

[5] - منظمة التحالف الدولي لحماية الأمن السيبراني منظمة عالمية تأسست في بريطانيا نوفمبر 2011م، لتوجيه التمويل والخبرات والمساعدة لوحدات إنفاذ قانون الجرائم السيبرانية وتضم شركات وطنية وأخرى كثيرة متعددة الجنسيات.

خلال التعرض لتعريف الجرائم السيبرانية، وأهم السمات التي تتصف بها وكذا أهم تصنيفاتها.

وفي الشق الثاني تناولنا أهم الآثار الخطيرة التي تنجم عن الجرائم السيبرانية، ثم تعرضنا إلى دور مجلس التعاون لدول الخليج العربي في مواجهة هذه الظاهرة الخطيرة من خلال التعرض لأهم العقبات والتحديات التي قد تفشل أو تعرقل وتعد حجر عثرة في طريق جهود المكافحة ثم تناول دور مجلس التعاون لدول الخليج العربي، وأخيرا ما تم إفرازه من ثغرات نتجت من التطبيق، والتي دعتنا إلى اقتراح إستراتيجية لتفعيل المواجهة والتي حاولنا فيها جاهدين سد الثغرات والفجوات التي نتجت من الواقع العملي في التطبيق

وفي نهاية البحث أقول لكم أنني بشر فمن الممكن أن أخطئ ومن الممكن أن أصيب، ولكنني أتمنى من الله عز وجل أن تغفروا لي أخطائي إذا أخطأت وأن يتسع صدر كل من يقرأ هذا البحث للقراءة دون الشعور بالملل، والحمد لله سبحانه وتعالى الذي وفقنا وهدانا إلى كتابة هذا البحث.

نتائج الدراسة

- إن خصوصيات الإنترنت والسمات التي يتميز بها تجعل منه أدوات مثالية بالنسبة للمجرمين والمنظمات الإجرامية، فاستخدام الإنترنت المظلم يسمح لهؤلاء بالانخراط في أعمال إجرامية سرية صعبة الكشف والزجر، ويسمح لهم بالنشاط على نطاق واسع يشمل جميع دول العالم، كما أن سهولة استعمال برمجيات إخفاء الهوية وصعوبة الكشف عن هذه الجرائم تبرز التحدي الذي تواجهه السلطات.
- أن أنشطة هؤلاء المجرمين عابرة للحدود، فإن مكافحة الإنترنت المظلم لا يمكن أن تتم إلا بصفة عالمية، وتستوجب تعزيز وسائل التعاون القضائي الدولي وتطوير التعاون بين أجهزة الشرطة في مختلف دول العالم . إن تجريم الأفعال وحده لا يكفي لضمان زجر فعال للجرائم التي ترتكب على الإنترنت المظلم، إذ يجب تبني وتعزيز وتطوير وسائل التقصي المناسبة لهذا الفضاء، وذلك في ظل قصور وسائل التحري التقليدية .وتتمثل وسائل التحري المناسبة للعالم الافتراضي في الاختراق، التقصي تحت اسم مستعار واعتراض المعطيات عن بعد.
- إن رفع هذه التحديات الجديدة النابعة عن التطور التكنولوجي يفرض على الباحثين والأكاديميين في مختلف المجالات وعلى السلطات المكلفة بإنفاذ القانون أن يدرسوا هذه الظواهر وأن يقوموا بصياغة إطار قانوني وتنظيمي يسمح ببسط سلطة القانون.
- الحاجة الضرورية إلى تحديث التشريعات المعنية بمعالجة الجرائم السيبرانية وسن التشريعات التي تتناسب مع طبيعتها.
- قلة الكوادر البشرية العالمة ببواطن وأسرار الجرائم التقنية وطبيعتها وتقنياتها الأمر الذي يعد حجر عثرة وتحديا هائلا يعترض المواجهة الفاعلة لهذه الجرائم.
- ضعف المختبرات المعنية بالتعامل مع الأدلة السيبرانية وقلة إمكانياتها الأمر الذي يجعلها غير مؤهلة للتعامل مع هذا الأنواع من الجرائم.

- أهمية الدور الذي يقوم به مجلس التعاون لدول الخليج العربي في مواجهة هذه الظاهرة
- أهمية التعاون الدولي لمواجهة هذه الظاهرة من خلال عقد الاتفاقيات الدولية وبروتوكولات التعاون، وكذا الملاحقة القضائية وتسليم مرتكبي هذه الجرائم.
- التكلفة العالية التي تتطلبها مواجهة هذه الجرائم الأمر الذي يستدعي تدبير مصادر تمويل مستمرة لتغطية هذه التكلفة.

أهم التوصيات

- ضرورة تجفيف منابع تمويل الجرائم السيبرانية، ومكافحة ومراقبة الوسائل المستحدثة في عملية التمويل ومنها بالطبع العملات الافتراضية والتي يصعب مراقبتها وتتبعها بالوسائل التقليدية ومن هنا أصبحت الحاجة ملحه للغاية للبحث عن وسائل تقنية وغير تقليدية لمواجهة هذه الوسيلة شديدة الخطورة–
- ضرورة المراجعة المستمرة للتشريعات المعنية بمواجهة الجرائم السيبرانية والتي يجب أن تواكب الطبيعة التقنية المستمرة لهذه الجرائم ألا تتسم بالجمود وضرورة إيجاد آلية تمكنها من القابلية المستمرة للتطوير والتعديل لمواجهة ما يستحدث من جرائم.
- أن القواعد الإجرائية التقليدية لا تتناسب مطلقا مع الطبيعة التقنية للجرائم السيبرانية الأمر الذي استدعى ضرورة سن قانون إجراءات يتناسب مع الطبيعة التقنية لهذه الجريمة.
- ضرورة توفير وتدريب الكوادر البشرية من رجال إنفاذ القانون على التعامل مع الجرائم السيبرانية والتعامل مع تقنياتها واستخراج الدليل من أوعيتها والحفاظ علية ومراعاة مشروعيته أمام القضاء حتى يمكن الحد من ظاهرة إفلات مرتكبي هذه الجرائم من العقاب.
- عقد المؤتمرات الدولية وتدعيم مراكز البحث العلمي المعنية برصد ومكافحة الجرائم السيبرانية.
- توفير البرامج التدريبية المتطورة والتي تواكب أحدث التطورات المستحدثة في مجال الجرائم السيبرانية لرجال إنفاذ القانون على مختلف مستوياتهم بما يمكن من رفع كفاءتهم في هذا المجال.
- دعم وتطوير المختبرات العلمية المعنية بالتعامل مع الأدلة السيبرانية ورفع كفاءتها بما يمكنها من التعامل الفعال مع الجرائم السيبرانية للحد من ظاهرة إفلات مرتكبي هذه الجرائم من العقاب.
- إنشاء جهاز شرطي خاص بمكافحة هذه الجرائم مكون من خبراء من جميع دول مجلس التعاون له اختصاص مكاني يشمل جميع دول مجلس التعاون الخليجي ومزود بالكوادر البشرية المدربة والمؤهلة للتعامل مع هذه الجرائم وفرق التدخل السريع لمواجهة أيه انتهاكات وتعديات على البنى التحتية السيبرانية
- إنشاء محكمة جزائية خاصة موحدة لدول مجلس التعاون الخليجي لمحاكمة مرتكبي الجرائم السيبرانية.
- وضع أطر وقواعد وتأسيس العلم الجنائي السيبراني على أن يتضمن الجرائم السيبرانية وتعريفها وأركانها والإجراءات الجنائية الخاصة بالأدلة الرقمية ومشروعيتها الطرق الكفيلة بترسيخ حجيتها القضائية وغيرها مما

يستجد من قواعد على أن يتميز هذه العلم بالمرونة المستمرة بالطرق التي تكفل المراجعة المستمرة الدورية له نظرا لما تتسم ب هذه الجرائم من طبيعة تقنية متطورة، وألا يتسم بالجمود وعدم القابلية للتطوير.

- إعداد برامج وإستراتيجيات لإدارة الأزمات على أسس علمية في مهددات الأمن السيبراني.
- إنشاء مفوضية خاصة بتعليم الأمن السيبراني وطرق الوقاية من الجرائم السيبرانية.
- تنظيم معسكرات صيفية للطلاب تركز برامجها على الأمن السيبراني، وتنظيم فعاليات ترويجية لمفهوم الأمن السيبراني في الجامعات.
- تنظيم مسابقات الدفاع السيبراني cyber defense بين الجامعات لتحفيز الطلاب في دول مجلس التعاون الخليجي على المشاركة وتنمية الإبداع في مجال مواجهة الجرائم السيبرانية وطرق الوقاية منها على اعتبار أن الشباب هم أغلب المستهدفين بهذه الجرائم وفي نفس الوقت اغلب مرتكبيها.
- إعداد البرامج التوعوية في مجال التوعية من مخاطر الجرائم السيبرانية وطرق تحققها، وأهم الإجراءات الوقاية منها، وطرق الأمن السيبراني، والاستخدام الآمن لشبكة الإنترنت.
- إيجاد سياسة عقابية غير تقليدية تتناسب مع طبيعة هذه الجرائم والسمات التي يتفرد بها مرتكبو هذه الجرائم.
- ضرورة تبني إستراتيجية جديدة للتعامل مع هذه الظاهرة وهو الأمر الذي حاولنا ونأمل أن نكون وضعنا ولو لبنة واحدة في صرحها العظيم

المصادر والمراجع

إبراهيم حامد طنطاوي، د. علي محمود حمودة، شرح الأحكام العامة لقانون العقوبات الجزء الأول النظرية العامة للجريمة، دار النهضة العربية، القاهرة، 2007م.

أحمد حسام طه همام: - الحماية الجنائية لتكنولوجيا الاتصالات " دراسة مقارنة "، دار النهضة العربية، القاهرة، 2002م.

أحمد خالد العجلوني: - التعاقد عن طريق الإنترنت "دراسة مقارنة "، الدار العالمية الدولية للنشر والتوزيع، عمان ،2006م.

احمد خليفة الملط: - الجرائم السيبرانية، دار الفكر الجامعي، الإسكندرية ،2006م.

أحمد عبد الكريم سلامة: - الإنترنت والقانون الدولي الخاص " فراق أم تلاق "، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الإستراتيجية، مركز تقنية المعلومات، الإمارات ،1-3 مايو 2000م.

أسامة عبد الله قايد: الحماية الجنائية للحياة الخاصة وبنوك المعلومات- مصر جامعة القاهرة 1988 ص48 .

أوراق عمل ووثائق المؤتمر الإقليمي للأمن السيبراني مسقط 20-21 أبريل .2014 على الموقع .http//www.cybersecuritysummit.com

إيمان عبد الكاظم جبار الكريطي: العملة الخليجية الموحدة الفرص والتحديات، مجلة الغري للعلوم الاقتصادية والإدارية، المجلد 4 العدد 13 , 200.

أيمن سيد محمد مصطفى: - الإرهاب الالكتروني " دراسة حول صيغة مقترحة لاتفاقية دولية لمكافحة الإرهاب الاليكتروني " مقدم إلى المؤتمر الدولي لجامعة عين شمس بعنوان القانون والتكنولوجيا، 9-11 ديسمبر2017م. جوهر بنت عبد العزيز آل سعود الجرائم الإليكترونية ومكافحتها " الحاسب الآلي أداة تخزين ووسيلة اكتشافها على الموقع -http//www. Al .jazera.com/dig/imag2705

أيمن عبد الله فكري: - جرائم نظم المعلومات، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2005-2006م.

بيتر نمرابوسكي، جرائم الحاسب الآلي، الأبعاد العالمية، دولة الإمارات العربية المتحدة، أبو ظبي، مركز البحوث والدراسات الأمنية، شرطة أبو ظبي، ورقة عمل قدمت بندوة نوفمبر6-7 2006 م، - شبكات الإنترنت وتأثيراتها الاجتماعية والأمنية، الطبعة الثانيه.

الجريدة الرسمية لمجلس التعاون لدول الخليج العربي، العدد السابع عشر، السنة الخامسة، 15 يناير 2017م.

الجريمة الإليكترونية في المجتمع الخليجي وكيفية مواجهتها، مجمع البحوث والدراسات، أكاديمية السلطان قابوس لعلوم الشرطة، نزوي، سلطنة عمان ،2016 م.

جعفر حسن جاسم الطائي: - جرائم تكنولوجيا المعلومات، رؤية جديدة للجريمة السيبرانية، دار البداية عمان، 2007م.

جميل عبد الباقي الصغير: - القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، ط1، دار النهضة العربية، القاهرة ،1992م.

حاتم عبد الرحمن منصور الشحات: - الإجرام المعلوماتي، دار النهضة العربية، القاهرة ،2002م.

حامد ممدوح إبراهيم، أمن الجريمة الإليكترونية، مطبوعات الدار الجامعية، الإسكندرية 2008م.

خالد ممدوح إبراهيم: -الجرائم السيبرانية، دار الفكر الجامعي، الإسكندرية، ط1 ،2009م.

خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط1 ،2009م.

خليل يوسف الجندي، المواجهة التشريعية للجريمة المعلوماتية على المستوى الدولي والوطني، مجلة كلية القانون للعلوم القانونية والسياسية المجلد السابع، جامعة دهوك، العدد26 ،2018م،

ذياب البدينة: - هندرة الثقافة الأمنية والتحصين الاجتماعي ضد الجريمة، مجلة الفكر الشرطي، المجلد 7، العدد2.

رءوف عبيد: - مبادئ القسم العام من التشريع العقابي، دار الفكر العربي، 1979م.

ربيع أنور فتح الباب، النظم السياسية السلطة الدولة الحكومة صورها أساليبها، دار نصر للطباعة الحديثة، القاهرة 2003م.

رشا خليل عبد: - جرائم الاستغلال الجنسي للأطفال عبر الإنترنت، مجلة الفتح، العدد السابع والعشرون ،2006م.

سامر سلمان عبد الجبوري: - جريمة الاحتيال الإليكتروني، رسالة ماجستير، كلية الحقوق، جامعة النهرين، 2014م.

سامي البحيري، صراع في العالم الرقمي " الجرائم الإليكترونية تمثل هاجسا كبيرا لأجهزة الأمن، مجلة الثقافة الاجتماعية الأمنية العدد562، اكتوبر2011م.

سامي الشوا: - الغش المعلوماتي كظاهرة إجرامية مستحدثة، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة 25-28أكتوبر 1993م.

سعاد أنفوش: - الركن المعنوي في الجريمة، رسالة ماجستير، كلية الحقوق، جامعة عبد الرحمن ميرة، بجاية، الجزائر ،2016-2017م.

سعد الهاجري، المؤتمر الدولي لجرائم الإنترنت، الإمارات العربية المتحدة ،14ديسمبر2011م.

سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية، رسالة ماجستير، كلية الحقوق، جامعة محمد خيضر بسكرة ،2013-2014م، الجزائر.

سميرة معاشي: - ماهية الجريمة السيبرانية، بحث منشور في المنتدى القانوني، العدد السابع، جامعة محمد خيضر، بسكرة، الجزائر، 2011م.
سوزان عدنان الأستاذ: - انتهاك حرمة الحياة الخاصة على الإنترنت، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، العدد الثالث ،2013م.

سوميه عكور: - الجرائم المعلوماتية وطرق مواجهتها " قراءة في المشهد القانوني والأمني، ورقة علمية مقدمة للملتقى العلمي " الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، 2-4/9/2014 م، عمان الأردن.
صقر بن هلال المطيري: - جريمة غسل الأموال، دراسة حول مفهومها ومعوقات التحقيق فيها وإشكاليات تنسيق الجهود الدولية لمواجهتها، رسالة ماجستير، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية ،2004م.
ضاحي خلفان تميم، الجريمة، دبي-2017م.
طارق الخن، جرائم المعلوماتية، منشورات الجامعة الافتراضية، سوريا ،2018م.
طوني ميشال عيسى، التنظيم القانوني لشبكة الإنترنت، دراسة مقارنة في ضوء القوانين الوضعية والاتفاقيات الدولية رسالة دكتوراه مقدمة إلى مجلس كلية الحقوق والعلوم السياسية والإدارية الجامعة اللبنانية ،2000م.
عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، كلية القانون، جامعة الكوفة، مركز دراسات الكوفة العدد السابع، 2008م.
عائشة بوخبزة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، رسالة ماجستير، كلية الحقوق، جامعة وهران، الجزائر ،2012م ،2013م.
عباس الحسيني مقال بعنوان جرائم الكمبيوتر والإنترنت، منشور على الموقع الإليكتروني الفريق العربي للأمن والحماية السيبرانية www.atsdp.com.
عباس حفصي: -جرائم التزوير الإليكترونية "دراسة مقارنة "، رسالة دكتوراه، كلية العلوم الإنسانية والعلوم الإسلامية، جامعة وهران، الجزائر ،2014-2015م.
عبد الجبار الحنيص: - الاستخدام غير المشروع لنظام الحاسوب من وجهة نظر القانون الجزائي " دراسة مقارنة"، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد27، العدد الأول، 2011م.
عبد الحفيظ عبدا لرحيم محبوب: التبادل التجاري للإنتاج الصناعي بين دول مجلس التعاون الخليجي في ظل التكتلات الإقليمية والعالمية، رسائل جغرافية، الكويت- الرسالة261 (2002).

عبد العزيز الهمري، التحولات السياسية في النظام الدولي الجديد وأثرها على أمن دول مجلس التعاون الخليجي في الفترة من1990م-2010م، كلية الآداب والعلوم السياسية، جامعة الشرق الأوسط ،2009م-2010م.

عبد العظيم مرسي وزير: شرح قانون العقوبات، دار النهضة العربية، القاهرة، 2009م.
عبد الفتاح بيومي حجازي: - مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، 2006م.

عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت – دراسة متعمقة في جرائم الحاسب الآلي، دار الكتب القانونية، القاهرة، 2002م
عبد الله دغش العجمي: -المشكلات العملية والقانونية للجرائم الإليكترونية " دراسة مقارنة"، رسالة ماجستير في القانون العام جامعة الشرق الأوسط، 2014م.
عبد الله عبد الكريم عبد الله: - جرائم السيبرانية والإنترنت "الجرائم الإليكترونية "، منشورات الحلبي الحقوقية، بيروت، ط1، 2007م.
عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت) الجرائم الالكترونية (دراسة مقارنة، منشورات الحلبي الحقوقية لبنان 2007م.

عبد المحسن الداود: - التحديات الثقافية العلمية للأمن العربي، ورقة عمل مقدمة إلى المؤتمر العربي العلمي عن التعليم والأمن، أكاديمية نايف العربية للعلوم الأمنية، 4-6 أكتوبر 1999م.
عبد المحسن بدوي محمد أحمد: - إستراتيجيات ونظريات معالجة قضايا الجريمة والانحراف في وسائل الإعلام الجماهيرية، الندوة العلمية حول الإعلام والأمن، مركز الدراسات والبحوث، قسم الندوات واللقاءات العلمية، أكاديمية نايف العربية للعلوم الأمنية ،11-13 /5/ 2005م.
عبير على محمد النجار: -جرائم الحاسب الآلي في الفقه الإسلامي، رسالة ماجستير، كلية الشريعة والقانون، الجامعة الإسلامية بغزة، 2009م.

عفيفي كامل عفيفي: - جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، بيروت 2003م.
عمر حوتية، رحاب فايز أحمد سيد، تجربة دولة الإمارات في التصدي للجرائم المعلوماتية الواقعة على التجارة الإليكترونية، المجلة الأردنية للمكتبات، المجلد50، العدد4، ديسمبر2015م.
عمر محمد أبو بكر بن يونس: - الجرائم الناشئة عن استخدم الإنترنت، رسالة دكتوراه في القانون الجنائي ' كلية الحقوق، جامعة عين شمس ،2004 م.
غنام محمد غنام: - عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، الإمارات العربية المتحدة، كلية الشريعة والقانون، 1-3مايو 2003م، المجلد الثاني.
فخري عبد الرازق الحديثي: - شرح قانون العقوبات القسم العام، مطابع الأوفست، الرمادي، بغداد 1992م.
فهد بن محمد الشهري: -جريمة التشهير الإليكتروني " دراسة مقارنة "، رسالة ماجستير، المعهد العالي للقضاء، جامعة الإمام محمد بن سعود، السعودية.
كامل السعيد: - دراسات جنائية متعمقة في الفقه والقانون والقضاء المقارن، ط1، عمان 2002 م.
كريمة صراع: -واقع وآفاق التجارة الإليكترونية في الجزائر، رسالة ماجستير، كلية العلوم الاقتصادية وعلوم التسيير والعلوم التجارية، جامعة وهران، الجزائر2013-2014م
اللواء خميس مطر، نائب القائد العام لشرطة دبي " الجرائم الإليكترونية الاقتصادية جريدة الاتحاد الإماراتية 23 فبراير 2013م.
مأمون سلامة، الإجراءات الجنائية في التشريع المصري، دار الفكر العربي، القاهرة 1977م.
مبارك سعيد الحنيلي مدير الشرطة الخليجية بمدير الإدارات المختصة بمكافحة الجرائم الإليكترونية، جريدة الإتحاد الإماراتية 24 مارس2017م.
محمد أحمد محمد الحمادي، تشريعات مكافحة جرائم تقنية المعلومات في دولة الإمارات العربية وأحكام القضاء، ورقة عمل ندوة شبكات الإنترنت 6-7 نوفمبر 2006م، مركز الدراسات الأمنية، أبو ظبي، الإمارات.
محمد الجبور: - الوسيط في قانون العقوبات- القسم العام، دار وائل، عمان، الأردن، ط1، 2012م.
محمد السعيد رشدي، الإنترنت والجوانب القانونية لنظم المعلومات، دار النهضة العربية، القاهرة، 2004م.
محمد أمين أحمد الشوابكه: - جرائم الحاسوب والإنترنت " الجريمة السيبرانية"، مكتبة دار الثقافة، عمان، 2004م.
محمد حجازي، جرائم الحاسبات والإنترنت الجرائم المعلوماتية، المركز المصري للملكية الفكرية، مارس2005م.
محمد حماد مرهج: - التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة عمان، 2002م.
محمد عبد الظاهر حسين، المسئولية القانونية في مجال شبكات الإنترنت، دار النهضة العربية، القاهرة ،2002م.
محمد عبد الله منشاوي: - جرائم الإنترنت من منظور شرعي وقانوني: -مكة المكرمة 1-11-1423هـ.
محمد عبيد الكعبي: - الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، بدون سنة نشر ورقم طبعة، ص 33، رامي متولي القاضي، مكافحة الجرائم المعلوماتية، دار النهضة العربية، ط1 ،2011م.
محمد علاوي، دور الأمن المعلوماتي في الحد من الجريمة المعلوماتية، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر.
محمد على عريان: - الجرائم السيبرانية، دار الجامعة الجديدة، الإسكندرية، 2004م.

محمد محيي الدين عوض: - قانون الإجراءات الجنائية في السودان معلقا عليه، المطبعة العالمية، القاهرة ،1971م.
محمد محيي الدين عوض: - مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات والكمبيوتر، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة25-28 أكتوبر 1995م، حول مشكلات المسئولية الجنائية في مجال الإضرار بالبيئة والجرائم الواقعة في مجال التكنولوجيا المعلومات، دار النهضة العربية، القاهرة 1993م.
محمود أحمد عبابنة: - جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الأردن، 2005م.
محمود نجيب حسني: - النظرية العامة للقصد الجنائي، دار النهضة العربية، ط2 ،1971م.
مدحت رمضان: - جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية ن القاهرة، 2007م.مزيود سليم: - الجرائم السيبرانية في الجزائر وآليات مكافحتها، المجلة الجزائرية للاقتصاد والمالية، العدد 1، أبريل 2014م.
معوض عبد التواب، الموسوعة الشاملة في الجرائم المخلة بالآداب العامة وجرائم هتك الأعراض، دار المطبوعات ا لجامعية، الإسكندرية ،1995م.
مفتاح بو بكر المطردي: - الجريمة الإليكترونية، ورقه عمل مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، السودان 23-25 أيلول ،2001م.
منير ممدوح الجنيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية ،2005م.

مولود بو عقادة، الجرائم الاقتصادية والمالية وسبل محاربتها دوليا ووطنيا، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة خميس مليانه، الجزائر 2003-2004م.
نائلة عادل فريد قوره: - جرائم الحاسب الاقتصادية " دراسة نظرية تطبيقية"، دار النهضة العربية، القاهرة، 2004م.

نجاة عباوي، الإشكاليات القانونية في تجريم الاعتداء على أنظمة المعلومات، مجلة دفاتر السياسة والقانون، العدد 16، يناير 2017م ص280.
نعيم مغبغب: مخاطر السيبرانية والإنترنت (المخاطر على الحياة الخاصة وحمايتها) دراسة في القانون المقارن، لبنان، منشورات الحلبي الحقوقية.
نيفين حسين، جهود دولة الإمارات العربية المتحدة في مجالات الابتكار واقتصاد المعرفة، وزارة الاقتصاد، وزارة الاقتصاد، مبادرات الربع الثاني2016م.
هدى حامد قشقوش: - حماية الحاسب الاليكتروني، في التشريع المقارن، دار النهضة العربية، القاهرة 1992م
هشام فريد رستم: - قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الجديدة، أسيوط 1994م.
هلال عبد الله أحمد: الجوانب الموضوعية والإجرائية لجرائم السيبرانية على ضوء اتفاقية بودابست الموقعة 23 نوفمبر 2001، دار النهضة العربية، 2002م.
هلالي عبد اللاه أحمد، الجوانب الإجرائية لجرائم المعلوماتية، ط1، دار النهضة العربية، القاهرة ،2003م، ص12، محمد على العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2011م.
وليد بن صالح، الإنترنت المظلم والعملات الافتراضية التحديات الجديدة للقانون الجنائي، مجلة كلية القانون الكويتية العالمية، الجزء الثاني، اكتوبر2018م.
يوسف المصري: - الجرائم السيبرانية الرقمية للحاسوب والإنترنت، دار العدالة، مصر، ط1، 2011م.
يونس عرب: - قراءة في الاتجاهات التشريعية للجرائم الإليكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان، ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإليكترونية، مسقط، 2-4 أبريل 2001م.

A.R Raghavan, Latha Parhiban, the effect of cybercrime on a bank's finances, international journal of current research and Academic Review, Vol.2, No.2, Feb. 2014.

Ajbaili, M. (2009). Saudi & UAE at High Risk to Cyber-crime: Report. Retrieved from http://www.alarabiya.net/articles/2009/11/15/91411.html.

Ajeel Singh Poonia, Cybercrime challenges and its classification, international journal of emerging trends of technology in computer science, Vol.3, Issue6, Nov., Dec. 2014

Algenib , K. , The current electronic evidence in the United Arab Emirates :Current limitations and proposal for reform , University of Bangor thesis for PhD(2014) .

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 Work Mississippi State University.

Alwast , A thesis at the university of Bahrain confirms the importance of electronic evidence as a definitive proof in the criminal field, 6 , July, 2015.

Baum Katrina , Identity theft , 2004 , First estimate from the national crime victimization survey , Washington U.S Department of justice, 2006.

Beryl Howell , Read world problems of virtual crime , Yale journal of law and technology , Vol.7 , No.1.

Brittany Crompton, David Thompson, Manuel Reyes, Cyber security Awareness Shrewsbury Public schools , Clark Digital Commons, School of Professional Studies , Clark University, 2016.

Capron J.A Johnson, Computer tools for information age, Pearson education, Inc., upper Saddle River, New Jersey ,2004.

Chissik and Alistair Kelman , E-commerce law and practice 3ed. Sweet and Maxwell, 2002

Craig Ball, Cross-examination on the computer forensic experts(2004).

Cybercrime , Law and Practice , retrieved fromwww.img.kerala.gov.in/docs/download/cyber%20crimes pdf

Digital in 2018 : World 'internet users pass 4 Billion mark.

Eoglan casey , Digital evidence and computer crime , New York , Academic press,2000.

Fahad Abdullah Moafa , Based legislation A comparative research between the UK and KSA , International journal of advanced computer research ,vol.4,No.2,15 June2014.

George Paul , Foundation of digital evidence , Chicago American Bar Association 2008.

George Paul , Foundations of digital evidence, Chicago American Bar Association ,2008.

Giddens C. Antony , Runway world : How globalization reshaping our lives, London profile books,1999.

Global cyber security conference in Abu Dhabi : National and cooperate threats and protection &education , March 25,2014.

Grabosky , Cybercrime in oxford handbook of organized crime by L.Paoli , Oxford university press , 2013.

Gulf daily news , cybercrime alert(2009) http//www.gulf-daily-news.com/newsdetails-aspx?storyid=26246.

H.R.W. 2012, UAE cybercrime decree attacks free speech, 28, Vol.2012.

Hakmeh J.C, Building stronger international legal framework on cybercrime, Chatham house expert comment, 6June 2017.

Helping law: Legal solutions worldwide received from http//www.helpinglaw.com/employment.gov/employment-criminal-and-labour/cybercrime-int-india.html.

Joyce Hakmeh , Cybercrime legislation in the GCC countries fit for purpose? , International security department , July2018.

Kang J., Information privacy in cyber space transaction , Stanford law review,1998.

Katherine T. Smith , Case studies of cybercrimes and its impact on marketing activity and shareholder value.

Krachman, Stan , J. Smith , Perpetration and prevention of cybercrimes internet Auditing , Vol.23, NO.2(March – April)20083-12.

Laura Barouiene, Vytautas Zirgutis, Cyber security facets, counter factual impact evaluation of measure (process as it) in enterprises of its sector, JSC, Vol.6, N0.3 March 2017.

Madison Ngafesson , Cybercrimes classification : Motivational model" , College of business administration , University of Texas,1999 p.120, also Roshan N.. What is cybercrime , Asian school of cyber law, 2008.

Masson and Nicholas Bohm ,Banking and fraud " a written submission to the house of treasury committee on January17th. , Jan.2011.

Mathus M. Hoscheidt , Elisa Feber Eichen , Legal and political measures to address cybercrime/UFRGSMUN/UFRGS/ISDN2318-3195(V.2.201).

Mc Quade , Encyclopedia of cybercrime , Green wood press , London , 2008.

Menon, V.C, GCC cybercrime has double warns security expert, retrieved from http//www.bezpeka.com/en/news/2010/08/09/gcc-cybercrime-has-doublewarns-security-expert.html.

Nigel Jones, Esther George, Electronic evidence guide" a basic guide for police officer, prosecution, and judge ,2013, version 1, Council of Europe.

Number of internet user (2014) live stats.

OECD (Organization for Economic Cooperation and Development) (2002), OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, Recommendation of the Council adopted 25 July 2002, OECD, Paris.

R.K. Chaubey, An introduction to cybercrime and cyber law, Kamal law house, 2012.

Ronald L. Mendle , Investigating computer crime ; A primer for security manager , New York Charles Thomas ,1988.

Rudesill Dakota ,Caverlee James and Sui Daniel , The deep web and the dark net " a look inside the internet massive black box , Ohio state public law , working paper, No.314,OCT.2015.

Sarah Gorden, Richard Ford, On the definition and classification of cybercrimes, Springer-Verlag, France ,2006.

St. Viswanathan , The Indian cybercrime law with cyber , Glassary, 2001.

Symantec cybercrime Report (2014).

The Cost of Cyber Crime, A DETICA REPORT IN PARTNERSHIP WITH THE OFFICE OF CYBER SECURITY AND INFORMATION ASSURANCE IN THE CABINET OFFICE.

Timothy J.O'hearn,, Crime and technology ,(new rules in a new world) , information & communication technology law, Vol.7(2) 1998.

Toni Makkaik , Media release on" effective investigation of high tech crime , Institution of criminology , December 2004.

Understanding Cybercrime: A Guide for Developing Countries, at 72, International Telecommunication Union, April 2009, www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf (hereinafter "Understanding").

Young Pi ,New China criminal legislation against cybercrimes , 2011, in http//www.coe.int/dghl/cooperate/economiccrime/cybercrime/document/countryprofiiles/cyber-cp-china-pi-young document.