سبل مكافحة الجرائم السبرانيه العابره للحدود

دراسه مقارنه

علي إبراهيم يوسف الخضيري*

DOI:10.15849/ZJJLS.240330.43

*قسم القانون ، جامعة صفاقس، تونس .

للمراسلة : ali_khdairi@hotmail.com

الملخص

تناولت هذه الدراسة أحد أهم المواضيع التي تتعلق بدراسة الجرائم السيبرانية التي تعد من أكثر الجرائم خطورة على الأمن القومي للدول، وتتجلى خطوره هذه الجريمه في انه يمكن لمرتكي الجرائم السيبرانية وضحاياهم أن يتواجدوا في مناطق مختلفة، ويمكن أن تمتد آثار الجريمة عبر المجتمعات إلى جميع أنحاء العالم، وازدادت خطورة الأمن السيبراني بعد ما أسقطت تكنولوجيا المعلومات والاتصالات مفهوم الحدود الجغرافية، السياسية، والثقافية بين الدول، ووضعت السيادة الوطنية على المحك؛ الأمر الذي جعل هناك علاقة طردية بين التهديدات السيبرانية والأمن القومي، حيث كلما زادت التهديدات السيبرانية، كلما اثر ذلك سلبا على الأمن القومي للدولة، وانعكاسه على الامن الوطني ولما تسببه تلك الجرائم من خطورة تهدد المجتمع كله في اقتصاده وسيادته وأمنه، وغيرها العديد من التأثيرات السلبية التي تهدد أمن المجتمع وسلامته، وكذلك تاثير الجريمه السيبرانيه العالمي والدولي وأخطر تلك الجرائم الإرهاب السيبراني الذي لايعرف حدود ولا جغرافيا,الأمر الذي يحتم على المجتمع الدولي والمحلي ان يتخذ العديد من الإجراءات والتدابير للحد من تلك الجريمة من خلال بذل جهود بكافه السبل لمكافحتها والحد منها قبل وقوعها بالاضافه نشر الوعي بين الدول والمجتمعات بخطوره هذه الجريمه.

الكلمات الدالة: الامن السيبراني,الجرائم الالكترونيه، الجهود الدوليه والوطنيه، التحقيق الجنائي.

Ways to combat cross-border cybercrimes

A comparative study

Ali Ibrahim Yousef Al-Khdiri*

[*]**Department of law, University of Sfax,Tunisia**

*** Crossponding author:ali_khdairi@hotmail.com**

Abstract

This study addressed one of the most important topics related to the study of cybercrimes, which are considered one of the most dangerous crimes to the national security of countries. The seriousness of this crime is evident in the fact that the perpetrators of cybercrimes and their victims can be present in different regions, and the effects of the crime can extend across societies to all parts of the world. The danger of cybersecurity increased after information and communications technology eliminated the concept of geographical, political, and cultural borders between countries, and put national sovereignty at stake. Which made there a direct relationship Between cyber threats and national security, where the more cyber threats increase, the more this negatively affects the national security of the state, and its impact on national security, and because these crimes cause a seriousness that threatens the entire society in its economy, sovereignty, and security, and many other negative effects that threaten the security and safety of society, As well as the global and international impact of cybercrime, and the most dangerous of these crimes is cyberterrorism, which knows no borders or geography, which requires the international and local community to take many actions and measures to reduce this crime by making efforts in all ways to combat and reduce it before it occurs, in addition to spreading awareness among countries and communities. The seriousness of this crime.

Keywords: cybersecurity, cybercrime, international and national efforts, criminal investigation

المقدمة

في عصر التكنولوجيا أصبحت مسائل الدفاع السيبراني هي أحد أولويات الدفاع الوطني، حيث أصبح لأمن المعلومات أهمية كبرى في الدفاع على الدولة من أي هجوم الكتروني قد تتعرض الأنظمة التشغيلية لها من أي قرصنة إلكترونية، وقد أعلنت 130 دولة حول العالم عن قيامها بتخصيص بعض الأقسام للأمن السيبراني، هذا بالإضافة إلى بعض الطرق الأخرى التي تفرضها الدول كعقاب للجرائم الإلكترونية , وتعتبر الجرائم السيبرانية من أكثر الجرائم خطورة على الأمن القومي للدول، وهي من الجرائم التي تباينت تسميتها عبر المراحل الزمنية نظرا لتطورها، فكان يعبر عنها بداية بمصطلح إساءة استخدام الكمبيوتر او الحاسب الالي، مرورا باصطلاح احتيال الكمبيوتر، والجريمة المعلوماتية او الالكترونيه، فاصطلاح جرائم الكمبيوتر، والجريمة المرتبطة بالكمبيوتر، وجرائم التقنية العالية، إلى جرائم الهاكرز، فجرائم الإنترنت، إلى آخر المصطلحات الجرائم السيبرانية.

وتتجلى خطوره هذه الجريمه في مختلف نواحي الحياه ابتدا من المنشات الحيويه وتعطيل الحياه العامه أو إشاعة الأخبار الكاذبة وسرقة الملفات الهامه الخاصة بالوسسات وبالأفراد ونشرها على الإنترنت ووسائل الاتصالات وتتسبب أيضا بالتفكك الأسري والخلافات بين الأفراد بسبب التشهير وغيرها العديد من التأثيرات السلبية التي تهدد أمن المجتمع وسلامته، وكذلك تاثيرالجريمه السيبرانيه العالمي والدولي وأخطر تلك الجرائم الإرهاب السيبراني الذي لايعرف حدود ولا جغرافيا، الأمر الذي يحتم على المجتمع الدولي والمحلي ان يتخذ العديد من الإجراءات والتدابير للحد من تلك الجريمة من خلال بذل جهود دوليه ووطنيه لمكافحتها لذا سنعرض هذا البحث في محبثين:

المبحث الاول: ماهيه الجرائم السبرانيه.

المبحث الثاني: اجراءات مكافحة الجرائم السبرانيه .

مشكلة الدراسة:

تكمن مشكلة الدراسة في مامدى كفايه الحمايه الدوليه والوطنيه القانونيه التي تضمن مكافحه الجرائم السبيرانيه من خلال دراسه مقارنه بين التشريعات العربيه وبالاخص المشرع الاردني والتشريعات العالميه وهذه مشكلة تنبثق عنها مجموعة من التساؤلات والطروحات والتي جاءت هذه الدراسة لتتصدى لها من خلال:

عناصر مشكلة الدراسة (أسئلة الدراسة):

1. ما المقصود بالجرائم السبيرانيه؟
2. هل يوجد مبادئ تعاون دولي او جهود واضخه لمكافحه هذه الجريمه؟
3. ماهو مدى التاثير الدولي والوطني لهذه الجريمه؟ .

أهمية الدراسة:

تتجلى أهمية الدراسة من خلال تقديم دراسه مقارنه ومعالجة تحليلية وعلى وجه الخصوص سعيا إلى رسم إطار قانوني يضمن مكافحه الجرائم السبيرانيه والحد من مخاطرها.

محددات الدراسة: تتمثل محددات الدراسة على النحو الآتي:

المحدد المكاني: هذه الدراسة ستكون في المملكة الأردنية الهاشمية مع دراسه بالتشريع المقارن العربي والعالمي كاطار عام وذلك نظرا لحداثه الموضوع.

المحدد الموضوعي: دراسة على الواقع العملي للجريمه السيبرانيه وفق مانصت عليه التشريعات وبالاخص الأردني .

المحدد الزماني: لا يمكن حصر الدراسة بمحدد زماني لكن يمكن الحديث عن تطور التشريعات بخصوصها.

منهجية الدراسة:

تقوم هذه الدراسة بالأساس على المنهجين والتحليلي والمقارن بشكل رئيس والمنهج الوصفي أيضاً كلما كأن ذلك ممكناً وضرورياً ذلك أن تناول مفهوم الدفوع الممكن إثارتها أمام المدعي العام أثناء السير بإجراءات التحقيق يستلزم إتباع المنهج الوصفي من خلال وصف النصوص المتعلق بالمشكلة ومن أجل الوصول إلى إطار قانوني أو لنظرية عامة بشأن هذه مكافحه الجريمه السيبرانيه وذلك يستلزم بطبيعة الحال تناول النصوص الناظمة لهذا الموضوع بشيء من الدراسة والتحليل وبيان رأي الفقه، وتمحيص النصوص القانونية وتحليلها والعمل على التوفيق والمقاربة فيما بينها والاستعانة في كل ذلك برأي الفقه القانوني المقارن وما توصل إليه اجتهاد القضاء الأردني حول هذا الموضوع مع التعريج قدر ما أمكن للتشريعات المقارنة وأحكام القضاء المقارن.

خطه الدراسة:

تتناول هذه الدراسة موضوع بحثنا احيث تم تقسيمه الى مبحثين:

المبحث الاول: ماهيه الجرائم السبرانيه.

المطلب الاول: مفهوم الجرائم السبرانيه.

المطلب الثاني: خصائص الجرائم السبرانيه.

المبحث الثاني: اجراءات مكافحة الجرائم السبرانيه.

المطلب الاول: الجهود الدولية لمكافحة الجرائم السبرانيه .

المطلب الثاني: الجهود الوطنيه لمكافحة الجرائم السبرانيه.

المبحث الاول: ماهيه الجرائم السبرانيه

المطلب الاول: مفهوم الجرائم السبرانيه.

كلمه cyber عرفها قاموس اكســـفورد بأنها صـــفة لاي جريمة مرتبطة بثقافة الحواســـيب أو تقنية المعلومات أو الواقع الافتراضي.

فالجريمة السيبرانية تعد من الجرائم التي تباينت تسميتها عبر المراحل الزمنية لتطويرها فكانت بداية جريمة إساءة اســـتخدام الكمبيوتر، ثم جريمة احتيال الكمبيوتر، والجريمة الالكترونيه المعلوماتية، وجريمة التقنية العالية، جرائم الهاكرز، إلى الجرائم السيبرانية.

وهناك تعريفات كثيرة للجريمة الســيبرانية منها: هي التي تتم بواســطة الكمبيوتر أو أحد وســائل التقنية الحديثة بســرقة أو تدمير أو تعطيل معلومات متواجدة في كمبيوتر او جهاز تقني أخر مع ضرورة توافر شبكة إتصال فيما بينهما.

وكذلك تعرف الجريمة السيبرانية: بانها التي تتم بواسطة الكمبيوتر أو أحد وسائل التقنية الحديثة بسرقة أو تدمير أو تعطيل معلومات متواجدة في كمبيوتر أو جهاز تقني أخر مع ضرورة توافر شبكة اتصال فيما بينهما.

ويمكن اعتبار العديد من الأعمال جريمة عبر الإنترنت بما في ذلك الوصول غير المصرح به عير الإنترنت إلى معلومات شخص آخر، أو بيانات بطاقة الائتمان، أو دعم المنظمات الإرهابية أو التشهير بشخص ما.

والبعض يقصد بسلوك الجريمة السيبرانيه: هو الدخول الغير المشروع لأجهزة وأنظمة الحاسب الألي، أو لنظام معلوماتي، أو شـبكة معلومات، أو موقع إلكتروني من خلال اختراق وسـائل وإجراءات الحماية بشـكل جزئي أو كلي لأي غرض كان بدون تفويض في ذلك أو بالتجاوز التفويض الممنوح.

ولعل ظهور مفهوم الإرهاب السيبراني كصور جديدة من صور الجرائم الدوليه تلك الجريمة التي يعاني منها العالم بأسره، في ظل طهور ثورة المعلومات، ادى الى بذل الجهود لمكافحتها فلم يعد يحتاج الإرهابي ذو الخبرة الاحترافية، سوى جهاز إلكتروني (حاسـب آلي أو أيباد أو تلفون أو نحو ذلك) متصـل بشـبكة الإنترنت للقيام بأعمال إرهابية، وهو جالس في أي مكان أمن سـوى في بيته أو في مقهى إنترنت أو بيت أحد أقاربه أو أصـدقائه، وذلك من خلال بعض النقرات البسـيطة على لوحة المفاتيح، أو باستخدام الفارة، وأن يترك دليلا الكتروني في الجهاز الذي استخدمه، وهذا الدليل الإلكتروني سهل التخلص منه من خلال حذفه نهائيا بمجرد نقرة لا تستغرق ثواني.

ويشـــار الى مفهوم الإرهاب الســـيبراني بأنه: تعبير يشـــمل مزج مصـــطلح التبديد بنظام المعالجات التهديد بنظام الكتروني اوالآلي للمعلومات او باستخدام تقنية اتصـالات حديثة ,يعرف بأنه: العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الإلكترونية[1].

في الاردن فقد صـدر قانون الأمن السـيبراني الاردني لسـنة (2019) بالاضـافه ما صـدر سـابقا من قانون انظمه

[1] سلمان، عبدالستار شاكر، جرائم الامن السيبراني واثر الجهود الدوليه في مكافحتها، ط1، هاتريك للنشر والتوزيع، 2023، ص15.

المعلومات لسنه (2010) وقانون الجرائم الالكترونيه لسنه (2015) والذي تم الغائها بموجب قانون الجرائم الالكترونيه رقم (17) لسنه (2023) حيث نص المشرع على تعريف الفضاء السيبراني: بانه بيئة تتكون من تفاعل الأشخاص والبيانات والمعلومات ونظام المعلومات والبرامج على الشبكات المعلوماتية وانظمة الاتصالات والبنى التحتية المرتبطة بها كما عرف الأمن السيبراني : الإجراءات المتخذة لحماية الأنظمة والشبكات المعلوماتية والبنى التحتية الحرجة من حوادث الأمن السيبراني والقدرة على استعادة عملها واستمراريتها سواء أكان الوصول إليها بدون تص ريح أو سوء استخدام أو نتيجة الاخفاق في اتباع الإجراءات الأمنية أو التعرض للخداع الذي يؤدي لذلك [1].

وفي التشريعات العربيه قد عرف المشرع المصري في المادة (14) من قانون مكافحة جرائم تقنية المعلومات بأنه "كل دخول يحدث عمدا أو بالخطأ غير عمدي والبقاء بدون وجه حق على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه.

وقد سلك المشرع الكويتي في المادة الثانية من قانون مكافحة جرائم تقنية المعلومات ذات المسلك الذي سلكه المشرع المصري من حيث تجريم الأفعال إلا أنه إختلف من حيث العقوبة حيث ضاعف المشرع الكويتي في العقوبة المقررة لجريمة الهكترة إذا ما إقترن تلك الجريمة بإتلاف أو محو أو تغير أو نسح أو ... الخ.

كذلك المشرع الإماراتي سلك نفس المسلك بل ذهب إلى أبعد من ذلك وتدرج ضمن هذه الأفعال، فعل البقاء في هذه الأنظمة أو الشبكات بصورة غير مشروعة حتى وإن كان الدخول قد تم بطريقة مشروعة. مع العلم أن الأمن السيبراني هو عبارة عن مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام لغير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في القضاء السيبراني، ويعمل الأمن السيبراني على حماية الأمن في الدولة وذلك لما يقدمه من حماية معلوماتية للأفراد والهيئات والمنظمات الموجودة في الدولة أيضاً [2].

المطلب الثاني: خصائص الجرائم السبرانيه.

تتميز الجرائم التقنية او السيبرانيه بخصائص تختلف إلى حد ما عن الجريمة العادية والمجرم السيبراني يستخدم تقنية الاختراق لتنفيذ جريمته وذلك من خلال التحايل على الأنظمة المعلوماتية، فيكون الاختراق بالقدرة على وصول هدف معين عن طريق ثغرات في نظام الحماية الخاصة، وتتم عن طريق برنامجين الأول الخادم وهو بجهاز الضحية إذ ينفذ المهام الموكلة إليه، والثاني يوجد بجهاز المخترق ويسمى بالبرنامج المستفيد واهم خصائص الجريمه السيبرانيه هي انها عابر للحدود وانها سهله الارتكاب صعبه الاثبات وسنبحث ذلك في فرعين:

الفرع الاول : ان الجريمه السيبرانية لا تعرف حدود دولية:

حيث انه من اخطر خصائص الجرائم السيبرانية أنها جرائم لا تعترف بأي خصوصية أو سيادة للدول فهي تقع

---

[1] قانون الأمن السيبراني الاردني رقم 17 لسنه 2023 الماده 2

[2] العودي، جلال فضل، الارهاب السيبراني، عدن، 2022.

بين أكثر من دولة ولا تعترف بالحدود الجغرافية مثلها مثل جرائم غسـيل الأموال والمخدرات وغيرها ففي عصـر الحاسـوب والإنترنت أمكن ربط أعداد هائلة من الحواسـيب عبر العالم، وعند وقوع جريمة إلكترونية غالبا يكون الجاني في بلد والمجني عليه في بلد آخر كما قد يكون الضـرر في بلد ثالث وان كثير من دول العالم بما فيها الدول الكبرى لم تسـتطع التصـدي للجرائم السـيبرانية وتعرضـت لاختراقات إلكترونية فعلى سـبيل المثال لا الحصـرالولايات المتحدة الأمريكية في عام (2021) في عهد الولايه الرئاسـيه الاخيره تعرضـت أهم المؤسـسـات الأميركيه، وهو البيت الأبيض ووزاره الخارجية والتجارة والخزانة والأمن الداخلي، ووكالات فدرالية أخرى لهجمات إلكترونية، تعد واحدة من أكبر الاختراقات واشدها تعقيدا في السنوات الخمس الأخيرة [1].

وعلى إثر هذه الهجمات أصـدر مكتب التحقيقات الفيدرالية، ووكلة الأمن السـيبراني، ومكتب الاسـتخبارات الأمريكية، بيانا مشتركا أكـدوا فيه أن العمل مستمر لتقيـيم حجم الضرر الذي لحق بشبكات الحكومة الفدرالية , وفي بداية شـهر يوليو (2022) أعلنت وزارة الخارجية الأمريكية عن اسـتعدادها لدفع ما يصـل إلى 10 ملايين دولار للحصـول على معلومات حول الهجمات المحتملة على النظام الانتخابي الأمريكي خلال الانتخابات المقبلة، وأشـارت الوزارة إلى أنها "تقدم السـلطات مكافأة مالية لأي شـخص يقدم معلومات من شـأنها أن تسـمح بتحديد هوية ومكان أي شـخص أو كيان أجنبي شـارك عن قصـد أو يشـارك فى هجمات القرصـنة على البيت الأبيض وأوضـحت أن "التدخل الأجنبي في الانتخابات يشـمل سـلوك معينا من قبل الأجانب ، والذي يشـير إلى "أفعال أو محاولات خفية أو احتيالية أو مضـللة غير قانونية يتم القيام بها بقصـد محدد للتأثير على الناخبين أو تقويض ثقة الجمهور في العمليات أو المؤسـسـات الانتخابية أو التأثير أو تقوض الثقة أو تغيير نتيجة التصـويت العام". وتابعت: "قد يشـمل الأمر تزوير الأصـوات والتطفل على قواعد البيانات أو تأثيرا معينا، أو معلومات مضـللة، أو حملات أو هجمات إلكترونية خبيثة" ,من جهته، قال مدير المخابرات الوطنية الأمريكية أفريل هاينز خلال منتدى بواشنطن ، إن "الولايات المتحدة بدأت في تسجيل المزيد من محاولات المتسللين للتأثير على العملية الانتخابية في البلاد" [2].

وكذلك في بريطانيا: أعلنت وزارة الدفاع البريطانية، بتاريخ 3 يوليو 2022 عن فتح تحقيق بعد اختراق حسابات الجيش البريطاني على موقعي تويتر ويوتيوب وقالت الوزارة على تويتر "نحن على علم بخرق لحسابات الجيش على تويتر ويوتيوب والتحقيق جار" أضافت يأخذ الجيش أمن المعلومات على محمل الجد ونحن بصدد معالجة المشكلة حتى يكتمل تحقيقهم، سيكون من غير المناسب تقديم مزيد من التعليقات.

اما **حلف شـمال** الاطلسـي ففي يوم الأربعاء الموافق 29 يونيو 2022 قالت شـركة البرمجيات الأمريكية مايكروسـوفت، إن قراصـنة روس بدأوا في شـن هجمات إلكترونية واسـعة النطاق على حلفاء أوكرانيا الغربيين وحذرت شـركة البرمجيات من أن القراصـنة يسـتهدفون أجهزة الكمبيوتر الحكومية في الدول الأعضـاء في حلف شمال الأطلسـي (ناتو) عل وجه الخصـوص، مضـيفة أنه رغم أن الهدف الرئيسـي لهم هو الولايات المتحدة، فإن خبراء مايكروسـوفت إكتشـفوا هجمات إلكترونية ضـد نحو 128 منظمة في 42 دولة مختلفة خارج أوكرانيا,

[1] مهمل، أسامة، الاجرام السيبراني، رسالة ماجستير، جامعه محمد بوضياف، 2018.

[2] الحمد، مسره خالد، الدليل الرقمي ومعايير جودته في الاثبات الجنائي، ط1، مركز التجارب الأكاديمي، عمان– الاردن، 2014، ص 25.

واوضحت الشركة أن القراصنة الروس نجحوا في اختراق 29 من الشبكات التي حاولوا مهاجمتها، مضيفة أنه في ربع الهجمات الناجحة عل الأقل تم الاستيلاء على البيانات ,وفي الوقت ذاته، أكدت مايكروسوفت أن روسيا هاجمت البنية التحتية لتكنولوجيا المعلومات في أوكرانيا بكل من الهجمات الإلكترونية والصواريخ منذ بداية الحرب، ومع ذلك، قالت إن أنظمة الكمبيوتر في البلاد أثبتت أنها مرنة للغاية في مواجهة مثل تلك الهجمات، وأن الفضل في ذلك يرجع إلى حد كبير إلى التدابير الاحترازية [1].

ورغم قوة هذا الدول وتقدمها الا انها تعرضت لقرصنة الالكترونية، ولم تستطع أن تحمي أهم مؤسساتها من الاختراقات الكترونيه وهذا يوكد ضروره إنشاء هيئة وطنية للأمن السيبراني، في نفس الوقت سرعة اصدار قانون مكافحة جرائم تقنية المعلومات والجرائم السيبرانيه في جميع دول العالم .

وهناك أربع طرق رئيسة تهدد الأمن السيبراني تتمثل في الآتي:

الأولى: هجوم الحرمان من الخدمة حيث يتم إطلاق خدمة كبيرة من الطلبات على خوادم الضحية بصورة تفوق قدرة الخادم، أو الجهاز على معالجتها والاستجابة لها، مما يؤدي إلى توقيفه بصورة جزئية أو كلية، أو إبطاء عمله ، وهذا ما يسبب ضررا للمستخدم النهائي، وهو هجوم يهدف إلى تعطيل قدرة الهدف على تقديم الخدمات المعتادة، وذلك عن طريق تعطيل جهاز الحاسب الآلي للخدمة، وهذه الطريقة تستخدم بطبيعة الحال ضد مواقع الإنترنت أو البنوك، أو المؤسسات من أجل التأثير عليها أو لدفع فدية مالية.

أما الطريقة الثانية، فهي إتلاف المعلومات أو تعديلها، ويقصد بهذه الطريقة الوصول إلى معلومات الضحية عبر شبكة الإنترنت أو الشبكات الخاصة، والقيام بعملية تعديل البيانات المهمة دون أن يكتشف الضحية ذلك، فالبيانات تبقى موجودة لكنها مضللة قد تؤدي إلى نتائج كارثية، خاصة إذا كانت خططا عسكرية أو خرائط سرية.

والطريقة الثالثة، هي التجسس على الشبكات، ويقصد بها الوصول غير المصرح، والتجسس على شبكات الضحية دون تدمير او تغيير في البيانات، والهدف منه الحصول على معلومات قد تتعلق بالأمن القومي للبلاد.

الطريقة الرابعة، هي تدمير المعلومات، في هذا الطريقة يتم مسح وتدمير كامل لأصول المعلومات، والبيانات الموجودة على الشبكات، ويصطلح عليه "تهديد لسلامة المحتوى، ويعني تغيير في البيانات، سواء بالحذف أو التدمير من قبل أشخاص غير مخولين[2].

الفرع الثاني: جرائم سهله الارتكاب صعبة الإثبات:

يستخدم فيها الجاني وسائل فنية معقدة وسريعة في كثير من الأحيان قد لا تستغرق أكثر من بصع ثواني، بالإضافة إلى سهولة محو الدليل والتلاعب فيه والأهم عدم تقبل القضاء في الكثير من الدول للأدلة التقنية المعلوماتية التي تتكون من دوائر وحقول مغناطيسية ونبضات كهربائية غير ملموسة بالحواس الطبيعية للإنسان[3].

---

[1] الحسيني، عمار عباس، التصوير المرئي والتسجيل الصوتي وحجتهما في الاثبات الجنائي، ط1، المركز العربي للنشر والتوزيع، القاهرة، 2017، ص 69.

[2] العودي، جلال فضل، الارهاب السيبراني، مكتب النائب العام، عدن، 2022، ص 50.

[3] المايل، عبدالسلام، والشريجي، عادل، الجريمه الالكترونيه في الفضاء الالكتروني، مجله افاق للبحوث والدراسات المركز الامعي ايلزي،

وتعد الجرائم السيبرانيه مغرية للمرتكبين حيث إن سرعة تنفيذها (كبسة زر) وإمكانية القيام بها عن بعد دون اشتراط التواجد في مسرح الجريمة تجعلها مغرية بما لا يقبل الشك انخفاض تكلفة الآليات الإلكترونية مقارنة بالأدوات التي تستخدم بالاجرام التقليدي فالجريمه السيبرانيه يحتاج المجرم جهاز إلكتروني وخط إنترنت، اما الارهاب التقليدي يحتاج تدريب ادوات.... إلخ وكذلك غياب السيطرة والرقابة على الشبكة المعلوماتية من أهم أسباب انتشار الجريمه السيبرانيه وقد يكون ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق، وهذا بطبيعة الحال يوفر للإرهابيين طريقا لتحقيق أهدافهم بسهولة مع التاكيد على غياب الحدود الجغرافية في الفضاء الإلكتروني يعد فرصة مناسبة للمجرمين ومن اهم صور ذلك هي اختراق الهواتف الخلويه واسعه الانتشار حيث ان هناك علامات أو إشارة تبين أن هاتفك الشخصي مخترق منها زيادة فاتورة الإنترنت يجب أن تعرف تقريبا مقدار بيانات الإنترنت التي تستخدما كل شهر. وفي حال زادت فاتورة الخدمة بشكل كبير فأنت بحاجة إلى معرفة سبب حدوث ذلك بالضبط حيث من الممكن أن يكون هناك تطبيقات تستهلك بيانات الإنترنت في هاتفك وكذلك يجب الانتباه الى الإعلانات غير المرغوب فيها بهاتفك ومن الضروري أن تعرف ما هو موجود ضمن هاتفك وخاصة التطبيقات التي تعمل في الخلفية، حيث إن ظهور تطبيقات لم تقم بتثبيتها سابقا يعني أنها غالبا تحتوي على برامج ضارة ويجب الحذرمن إرسال الرسائل العشوائية إذا وجدت أن هاتفك يتلقى الكثير من رسائل البريد العشوائية أو ورود مكالمات هاتفية من أرقام غريبة وغير مألوفة فهذا يعني أن هناك خطأ ما ومثال ذلك إذا ذكر لك أحد أفراد العائلة أو الأصدقاء أنك ترسل لهم رسائل نصية أو رسائل بريد إلكتروني غريبة، فإن هذا يعني أن هاتفك غالبا قد تعرض للاختراق وأن هاتفك المصاب يحاول تثبيت برامج ضارة عبر هواتف أصدقائك أو أفراد أسرتك كما يجب ملاحظه إذا بدأ الهاتف فجأة في فقد طاقته وهذا يحدث عندما يكون هناك أحد التطبيقات يعمل بداخل هاتفك وان ملاحظه عندما يسخن هاتفك سرعة، حتى لولم تكن تجري أي مكالمات أو حتى تستخدمه من الأساس ويعتبر هذا دليلا آخر على أن هناك تطبيقا يعمل في الخلفية دون درايه منك وكذلك إذا عمل هاتفك من تلقاء نفسه؛ يفتح ويغلق وحده، أو يبدأ فتح تطبيقات واذا أتت مكالمات مجهولة المصدر وبالخصوص اذا تكررت تلك المكلمات وإذا كانت هناك أصوات تشبه الصدى تسمعها خلال المكالمات ولم تكن موجودة من قبل [1].

وان من ابرز خصائص الجريمه السيبرانيه: انها جرائم سهلة الارتكاب فهي جرائم ناعمة (CRIME SOFT) وأطلق عليها البعض اسم جرائم الياقات البيضاء. وعند توفر التقنية اللازمة للجاني يصبح ارتكاب الجريمة من السهولة بمكان ولا تحتاج الى وقت ولا جهد، تلك المشكلة جعلت العديد من الخبراء، يقوم بوضع إجراءات وقواعد هامة لحفظ البيانات والمعلومات الشخصية من الاختراق الإلكتروني منها:

1. عدم الوثوق في أية رســائل إلكترونية غير اعتيادية مثل تلك التي تطلب تحويل مبالغ مالية أو التي تبشــر بالفوز بجائزة معينة.
2. إنشاء كلمات سر قوية ومعقدة لا يسهل الوصول إليها، وعدم توحيد كلمة السر لأكثر من جهاز أو حساب، بحيث لو أخترق أحد أجهزتك، لا يستطيع الهكر اختراق بقية أجهزتك الإلكترونية.
3. عدم الاتصــال بشـبكات الإنترنت المفتوحة في المطارات أو الأماكن العامة بدون وجود برنامج واق ضـدها،

طرابلس، العدد4، 2019.

[1] الجرائم الالكترونيه– محمود القرعان – دار وائل للنشر ط1 عمان الاردن– 2017 ص19.).

وكذلك ضـرورة تفعيل التطبيقات المضـادة للفيروسـات، وإجراء التحديثات الجديدة بشـكل مسـقر؛ لأنها في الغالب تكون لسد ثغرة معينة قد يستغلها بعض المخترقين.

4. عدم التعامل مع مواقع غير معتمدة خاصـة، في مسـألة جوزات الفنادق أو الطيران، وضـرورة الاعتماد على المواقع الرسمية للحجوزات.
5. لا تثق بأحد حتى لو كان من الأشخاص الذين تثق بهم فعند إرسال معلومات مهمة على البريد الإلكتروني أو على الشـبكات الاجتماعية لهذا الشـخص مثل كلمة مرور إحدى حسـاباتك، فممكن أن يتعرض هذا الشخص لعملية اختراق وبالتالي الوصول إلى حسابك.
6. تغيير كلمة المرور من حين لآخر؛ كي تساعدك على إبقاء حسابك بحالة أمنية مستقرة دائما."
7. عدم مشـاركة البيانات البنكية مع أي شـخص آخر، والتواصـل مع البنك في حال حدوث أي تعامل على الحساب بدون علم صاحب الحساب.
8. قم بمسـح بياناتك من على الأجهزة القديمة التي سـتتخلص منها، عن طريق اسـتخدام الطرق الحديثة التي تقوم بمسح البيانات نهائيا، من المعروف أن مسح البيانات والملفات من الأجهزة بالطرق التقليدية لا يضمن التخلص النهائي منها، وذلك لوجود الكثير من الطرق والبرمجيات التي تسـاعد على اسـترجاعها حتى بعد مرور الكثير من الوقت بعد حذفها.
9. أحرص على استخدام خيار شبكة الضيوف، يرغب الأصدقاء والعائلة دائما في استخدما شبكة الواي فاي الخاصة بك عند زيارتك، فبدلا من اسـتخدام الشـبكة الخاصـة بك التي ترتبط بها جميع أجهزتك، يمكنك تخصـيص شـبكة خاصة لهم في جهاز التوجيه، والتي تعرف باسم شبكة الضيوف، تتيح لك هذه الميزة مشاركة اتصالك بالإنترنت مع ضيوفك في حين إبقائهم خارج شبكتك الأساسية، مما يمنعهم من رؤية الملفات والخدمات المشتركة، لذلك قم بإعداد شبكة الضيوف الخاصة بك باستخدام أسم شبكة مختلف وكلمة مرور مختلفة وقوية.
10. حفظ إضـافي للبيانات up back، حتى يكون هناك نسـخة إضـافية لجميع الملفات الموجودة في الهاتف الذي في حال التعرض لهجوم سـيبراني، حتى لا يتعرض صـاحب الجهاز للابتزاز من قبل المخترق لاستعادة البيانات[1].

المبحث الثاني: اجراءات مكافحة الجرائم السبرانيه

انتشرت في الآونة الأخيرة في العالم جريمة الاختراق الإلكتروني، لم يسلم أي فرد أو شركة أو دولة.

المطلب الأول: الجهود الدولية لمكافحة الجرائم السبرانيه

هناك علاقة وثيقة بين مواجهة التهديدات السيبرانية والقضاء عليها وبين إصدار التشريعات القانونية الوطنية اللازمة لوضع ضوابط للتحكم في الأمن السيبراني وسنعرض ذلك في فرعين:

الاول: الجهود العالميه لمكافحه الجريمه السيبرانيه .

[1] العودي، جلال فضل، مقالات في الارهاب السيبراني، عدن، 2022، ص57.

الثاني: الجهود العربيه لمكافحه الجريمه السيبرانيه .

الفرع الاول: الجهود العالميه لمكافحه الجريمه السيبرانيه:

ان أول من تنبه بالإرهاب الســـيبراني ومخاطره، هي الولايات المتحده الأمريكيه في عام 1996، حيث قامت بتشــكيل لجنة حماية منشــآت البنية التحتية الحســاســة وكان أول اســتنتاج لهذه الهيئة هو أن مصــادر الطاقة الكهربائية والاتصـالات إضـافة إلى شـبكات الكمبيوتر ضـرورية بشـكل قاطع لنجاة الولايات المتحدة، وبما أن هذه المنشــآت تعتمد بشــكل كبير على المعلومات الرقمية، فإنها ســتكون الهدف الأول لأية هجمات إرهابية تســتهدف أمن الولايات المتحدة، وفي أعقاب ذلك، قامت كافة الوكالات الحكومية في الولايات المتحدة إنشـــاء هيئاتها ومراكزها الخاصــة، للتعامل مع احتمالات الإرهاب الإلكتروني فقامت وكالة الاســتخبارات المركزية بإنشــاء مركز حروب المعلوماتية، ووظفت الفا من خبراء أمن المعلومات، وقوة ضــاربة عل مدى ٢٤ ســاعة لمواجهة الإرهاب الإلكتروني وقامت القوات الجوية الأمريكية باتخاذ خطوات مماثلة، ومثلها المباحث الفدرالية، كما قامت الدول التابعة لحلف الأطلسي، باتخاذ إجراءات مماثلة [1].

وإذا كانت أكبر دولة في العالم وهي الولايات المتحدة الأمريكية تتعرض لقرصنة وهجمات إلكترونية، جعلت اللاداره لديهم، أن تولي الأمن السيبراني أولوية قصوى، فقد أصدرت العديد من التشريعات المتعلقة بمجال تقنية وتكنولوجيا المعلومات، وكان من بينها القانون رقم 474 – 99— 100 وهو قانون تشريعي عام شمل القانون التشريعي رقم 1213 لسنة (1986) م والمعدل للقانون 1030 u , s , 18s الخاص بموجب جرائم الحاسوب.

ومن ضمن الدول العالميه التي أصدرت تشريعات لمكافحة الجرائم التقنية الدول منها دولة السويد حيث أصدرت عام 1976م اول قانون لها في مجال مكافحة تقنية المعلومات، وهو قانون البيانات السويدي، والذي أهتم بمعالجة قضايا الدخول غير المشروع للبيانات الحاسوبية، أو تزويرها، أو تحويلها، أو الحصول غير المشروع عليها، وهي بذلك تعتبر أول دولة تقوم فعليا بإصدار تشريعات تتعلق بجرائم التقنية، لا سيما التزوير المعلوماتي. وكذلك دولة الدنمارك والتي لحقت السويد في هذا التطور الحاصل في مجال تقنية المعلومات بإصدارها أول قانون لها يتعلق بمكافحة جرائم الحاسب الآلي والإنترنت عام 1985 م، وكان من أهم نصوص هذا القانون ما تضمن منها فقرات خاصة بتحديد العقوبات والأفعال المجرمة التي تعد انتهاكا للحاسب الآلي كالتزوير المعلوماتي وفي بريطانيا قامت باصدار قانون مكافحة التزوير والتزييف عام 1986، وعرف أداة التزوير بأنها عبارة عن وسائط التخزين الحاسوبية المتنوعة، أو أي أداة أخرى يتم التسجيل عليا، سواء بالطرق التقليدية أو الإلكترونية أو بأي طريقة أخرى وايضا ألمانيا أصدرت عام 1986 قانون خاص لمكافحة التزوير المعلوماتي والذي بموجبه تكون لحقت عجلت التطور التشريعي الحاصل في مجال تقنية المعلومات ويجب الاشاره الى فرنسا التي أصدرت القانون الفرنسي رقم (19) لسنة (1988) الخاص بالتصدي للتزوير المعلوماتي.

ولا بد من الاشاره اتفاقية بودابست ، حيث اجتمع المجلس الأوروبي عام 2001 في العاصمة المجرية بودابست في 23 نوفمبر 2001، للتشاور حول هذه الظاهرة الإجرامية المستحدثة والاتفاقية الأوروبية الدولية لمكافحة

[1] سلمان، عبدالستار شاكر، جرائم الامن السيبراني واثر الجهود الدوليه في مكافحتها، ط1، هاتريك للنشر والتوزيع، 2023، ص 39.

الإجرام السيبيري (الإجرام عبر الإنترنت)، ووقعت عليها 30 دولة، ثم انظم إليها العديد من الدول من خارج المجلس الأوروبي، وكان من أبرز هذه الدول الولايات المتحدة الأمريكية، التي صادقت عليها في 22 سبتمبر 2006 م، ودخلت حيز النفاذ في الأول من يناير 2007م، واشتملت على عدة جوانب من جرائم الإنترنت، بينها الإرهاب وعمليات تزور بطاقات الائتمان ودعارة الأطفال[1].

الفرع الثاني :الجهود العربيه لمكافحه الجريمه السيبرانيه:

في التشريعات **العربيه** كما اشارنا سالفا فقد عاقب المشرع المصري على جريمة الاختراق في الفقرة الثانية من المادة (14) من قانون مكافحة جرائم تقنية المعلومات على أنه " إذا نتج عن الدخول إتلاف، أو محو، او تغيير، أو نسخ، أو إعادة نشر البيانات، أو المعلومات الموجودة على تلك الموقع، أو الحساب الخاص، أو النظام المعلوماتي تكون العقوبة الحبس لمدة لا تقل عن سنتين وغرامة لا تقل عن مائة ألف جنيه ولا يتجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين .

وقد سلك المشرع الكويتي في المادة الثانية من قانون مكافحة جرائم تقنية المعلومات ذات المسلك الذي سلكه المشرع المصري من حيث تجريم الأفعال إلا أنه إختلف من حيث العقوبة حيث ضاعف المشرع الكويتي في العقوبة المقررة لجريمة الهكترة إذا ما إقترن تلك الجريمة بإتلاف أو محو أو تغير أو نسح أو ... الخ.

كذلك المشرع الإماراتي سلك نفس المسلك بل ذهب إلى أبعد من ذلك وتدرج ضمن هذه الأفعال، فعل البقاء في هذه الأنظمة أو الشبكات بصورة غير مشروعة حتى وإن كان الدخول قد تم بطريقة مشروعة.

أما المشرع السعودي في الفقرة (2، 3) من المادة الثالثة من نظام مكافحة جرائم تقنية المعلومات على أنه "يعاقب بالحبس مدة لا تزيد على سنة وبغرامة لا تزيد خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أي من الجرائم المعلوماتية:

- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الالي – دون مسوع نظامي صحيح أو التقاطه أو اعتراضه.
- الدخول غير المشروع لتهديد شخص أو ابتزازه، لحمله على القيام بفعل أو الإمتناع عنه، ولوكان القيام بهذا الفعل أو الإمتناع عنه مشروعا.
- الدخول غير المشروع إلى موقع إلكتروني، أو الدخول الى موقع إلكتروني لتغيير تصاميم هذا الموقع أو إتلافه أو تعديله أو شغل عنوانه.
- المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها.
- التشهير بالآخرين، وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة. مع العلم أن هناك هيئة

[1] جمال، براهيمي، التحقيق الجنائي في الجرائم الالكترونيه، أطروحة دكتوراه، جامعه مولود معمري، الجزائر، 2018، ص 185.

الوطنية للأمن السيبراني في المملكة العربيه السعوديه التي تم إنشاؤها في شهر نوفمبر عام 2017 م، تعمل تحت إشراف خادم الحرمين الشريفين في المملكه لديهم[1].

وكما اشرنا في الاردن فقد صدر قانون الأمن السيبراني الاردني لسنة (2019) بالاضافه ما صدر سابقا من قانون انظمه المعلومات لسنه (2010) وقانون الجرائم الالكترونيه لسنه (2015) والذي تم الغائها بموجب قانون الجرائم الالكترونيه رقم(17) لسنه (2023).

المطلب الثاني: الجهود الوطنيه لمكافحة الجرائم السبرانيه:

كشفت الجريمة السيبرانيه عالما جديدا لا يعترف بالحدود الجغرافية والسياسية للدول ولا بسيادتها، حيث فقدت الحدود الجغرافية كل آثر لها في بيئة إلكترونية متشعبة العلاقات، الأمر الذي خلق صعوبات وإشكالات قانونية لا تقتصر على ضبط هذه الجرائم وإثباتها فحسب، وإنما أثارت أيضا تحديات اكثر تعقيدا مرتبطة بتحديد جهة الاختصاص وبالتبعية القانون الواجب التطبيق على هذا الصنف من الجرائم وفي الاردن فقد صدر قانون الأمن السيبراني الاردني لسنة (2019) بالاضافه ما صدر سابقا من قانون انظمه المعلومات لسنه (2010) وقانون الجرائم الالكترونيه لسنه (2015) وهذين القانونين تم الغائها بموجب قانون الجرائم الالكترونيه رقم(17) لسنه (2023) الساري المفعول بحكم ان هذه الجريمه لم تعد خطرا على الأفراد، بل على أمن واستقرار الدول؛ الأمر جعل المجتمع الدولي يتخذ العديد من الإجراءات والتدابير للحد من تلك الجريمة الخطيرة، ومن تلك الإجراءات سن قوانين عقابية لتصدي لظاهرة الإجرام المعلوماتي الذي يتطلب من الدول تسخير حلول أخرى غير الحلول الأمنية للتصدي لتلك الظاهرة من خلال التركيز غلى دور المجتمع والراي العام ودور الاسره والموسسات التعليميه وسنعرض ذلك في فرعين:

الفرع الاول: دور المجتمع في مكافحة الجرائم السيبرانيه

أثارت هذه الجريمة بعض التحديات القانونية والعملية أمام الأجهزة المعنية بالبحث عن الجرائم وضبطها وخصوصا فيما يخص مباشرة إجراءات البحث والتحري التقليدية في بيئة افتراضية لا مكان فيها للأدلة المادية، مما أظهر مدى الحاجة إلى تطور آليات البحث بما يتلاءم وخصوصيات هذه الجرائم، وجعل مسألة ملاءمة الإجراءات الجنائية في البحث والتحري مع خصوصية الجريمة الإلكترونية تستأثر باهتمام المشرعين في مختلف الدول. وتختلف كل دولة عن غيرها في طريقة مكافحة الجريمة السيبرانية، فكثير من دول العالم أنشئت مراكز للأمن السيبراني لمكافحة الاختراق الإلكتروني وما ينجم عنه من أضرار سلبية على نظم المعلومات سوى عن طريق الاتلاف او التدمير او الابتزاز او أي اختراق الكتروني كما تقوم مراكز الامن السيبراني على حماية الموسسات السياسية والاقتصادية والحيويه من أي اختراق الكتروني، وبالرغم من ذلك ان مراكز الامن السيبراني تظل عاجزة بالقيام بجميع مهامها التي أنشأت من اجله ولا يستطيع أي مركز امن سيبراني في العالم لحماية جميع افراد المجتمع من خطر الإجرام السيبراني الامر[2].

---

[1] جرائم الانترنت وعقوبتها وفق نظام مكافحه الجرائم المعلوماتيه، السعوديه 20، الرياض، ط1، دار الكتاب الجامعي، 2017، ص70.

[2] سلمان، عبدالستار شاكر، جرائم الامن السيبراني واثر الجهود الدوليه في مكافحتها، ط1، هاتريك للنشر والتوزيع، 2023، ص 79.

وكثير من الحوادث والجرائم أدت إلى غضب كافة الشرائح الاجتماعية في المجتمع الاردني، وتحولت من قضية شخصية إلى قضية رأي عام، وتفاعل الألاف على منصات التواصل الاجتماعي مطالبين القضاء باتخاذ تدابير رادعة وحازمة ضد الجناة، حتى يكونوا عبرة لكل من تحدث نفسه بالقيام بتلك الأعمال القذرة.

وهناك شريحة من المجتمع سعت بإنشاء مواقع إلكترونية لمحاربة من يقوم بالاخلال بالامن السيبراني او اي شكل من اشسكال الجرائم الالكترونيه كبث الاشاعات او اثاره النعراعات او جريمة الابتزاز الإلكتروني.

ومن ابرز الحلول او المعالجات لمكافحة الإجرام السيبراني تسخير الجانب الاكاديمي في التصدي لتلك الظاهرة الخطيرة سوى بطريقة غير مباشرة عن طريق تحصين طلبة الجامعات من خطورة واضرار الجريمه او بالسماح لاساتذة الجامعة باستخدام وسائل الاعلام المرئية والسمعية والمقروءة وهناك العديد من الوسائل التي بحوزة الاكاديميين لتصدي لجريمة الامن السيبراني كما أن هناك شريحة قانونيه وأكاديمية طالبت جهات الاختصاص بسرعة إصدار قانون مكافحة الجرائم السيبرانيه والالكترونيه، ولسد الفراغ التشريعي ومعالجه النقص، والحد من انتشار الجرائم الإلكترونية سيما وان هناك عدد كبير لا يستطيعون اللجوء للأجهزة الأمنية بسبب الخوف من المجتمع اوالأهل أو لأسباب تتعلق بطبيعة المجتمع التقليدي والمحافظ.

فكانت الحاجة لإنشاء هيئة وطنية للأمن السيبراني يكون من أبرز أهدافها أن تعمل على حماية الشبكات وأنظمة تقنية المعلومات وأن تعمل على نشر التوعية بأهمية الأمن السيبراني بين منتسبي القوات المسلحة والأمن والأجهزة الاستخبارية وجميع المرافق الحكومية والخاصة وتعمل على تعزيز دور الأمن السيبراني في حماية مصالح الدولة والحفاظ على امنها القومي وحماية المرافق العامة وبصفة خاصة، وزارة الدفاع ووزارة الداخلية والأجهزة الاستخبارية والاتصالات ومعظم المواقع الحيويه وهو مت نص عليه فعلا الأمن السيبراني الاردني رقم (16) لسنة (2019) وسد النقص التشريعي من خلال **الجرائم** الالكترونيه رقم (17) لسنه (2023).

الفرع الثاني: دور ألاسره في مكافحة الجريمة السبيرانيه

انتشرت في الآونة الأخيرة في المجتمع عده جرائم تخص الامن السيبراني منها الارهاب السيبراني والاختراق وادخول الى مواقع موسسات الدوله الحيويه ومن وابرزها جريمة الابتزاز الإلكتروني، بعضها ظهرت على السطح وكشف امرها، والكثير منها لم تظهر بسبب طبيعة المجتمع الشرقي والخوف من العار ومثال ذلك لجوء بعض الذي تعرضن لجريمة الابتزاز الالكتروني للانتحار, والأخطر والأهم ذلك من وجهة نظرنا أن هناك دور سلبي للاسره، ولم يقوموا بالمسؤولية الملقاة على عاتقهم حيث يجب عليهم تشجيع الأبناء وخاصة الفتيات على إبلاغ أولياء الأمور مباشرة باي شخص حصل على معلومات خاصة بهن، فالمجرم في البداية سيطلب طلب سهل ثم يدرج في طلبه فعلى الاسره حث ابنائهم على عدم التفاوض أو دفع أي مال للمبتز لأن ذلك لن يجعله يتوقف عن ابتزازهم واذا كان بالإمكان التعرف على أي تفاصيل عن المبتز مثل الهوية، والحساب ونوع هاتفه، وأي دليل يدعم جريمة الابتزاز) في حال كان الابتزاز الإلكتروني نتيجة عملية اختراق فاستعن بأحد المختصين لتوثيق عملية الاختراق، ثم أقطع الاتصال بالإنترنت على الجهاز، لكن إذا لم تكن بسبب الاختراق، فحينها يفضل فحص الجهاز من الفيروسات فمن الأفضل سرعة استشارة من هو قريب إليك وخاصا أحد والديك حتى يحاولان إيجاد حل للمشكلة قبل أن تتفاقم ويصبح حلها معقدا وان لا يتردد الاسره بان تطلب المساعدة من وحده الجرائم الالكنرونيه او احدى وزارت الاتصالات

أوالداخليه او من المختصين بمجال الحفاظ على الامن العام.

التوصيات والنتائج

توصل الباحث من خلال هذا البحث إلى مجموعة من النتاتج والتوصيات أهمها:

اولا: **النتائج:**

- الجرائم السيبرانية جرائم في غايه الخطوره أنها جرائم لا تعترف بأي خصوصية أو سيادة للدول فهي تقع بين أكثر من دولة ولا تعترف بالحدود الجغرافية وعابره للحدود.
- على جميع دول العالم بذل الجهود لمكافحته الجريمه السيبرانيه بكافه الطرق والاشكال وسبل التعاون الدولي بالاضافه الى الدور الوطني والمجتمعي والاسري وبذلك يحد من اضرار ومخاطر هذه الجريمه.
- تتجلى صوره الجريمه السيبرانيه بجريمه الارهاب السيبراني كصور جديدة من صور الجرائم الدوليه تلك الجريمة التي يعاني منها العالم بأسره، في ظل ظهور ثورة المعلومات ويجب الحذر من شكل هذه الجريمه.

التوصيات :

- على جميع الدول أن تعمل على حماية الشبكات وأنظمة تقنية المعلومات وإنشاء هيئة وطنية للأمن السيبراني في كل دوله، يكون من أبرز أهدافها مكافحه هذه الجريمه قبل وقوعها.
- بذل الجهود الدوليه والوطنيه والعمل على نشر التوعية بأهمية الأمن السيبراني بين كافه شرائح المجتمع وخاصه الطلاب بالاضافه الى منتسبي القوات المسلحة والأمن والأجهزة الاستخبارية وجميع المرافق الحكومية والخاصة.
- الحرص على تعزيز دور الأمن السيبراني في حماية مصالح الدولة والحفاظ على أمنها القومي وحماية المرافق العامة والحيويه.
- السعي لانشاء منظمه دوليه او هيئه عالميه على غرار منظمه الصحه العالميه وماشابه والسرعة أعداد مشروع قانون مكافحة الجرائم السيبرانيه وايضا المتعلقه بتقنية المعلومات، للحد من الجرائم السيبرانيةقبل وقوعها.
- عقد مؤتمرات دوليه للحث على بذل الجهد في مكافحة الإرهاب السيبراني مكافحة الابتزاز السياسي الإلكتروني وحماية العلاقات الدوليه الاجتماعية والسياسية.

قائمه المراجع:

- آل جار الله، عبدالعزيز بن غرام الله، جرائم الانترنت وعقوبتها وفق نظام مكافحه الجرائم المعلوماتيه، السعوديه 20، ط1، دار الكتاب الجامعي، الرياض، 2017.
- جمال، براهيمي، التحقيق الجنائي في الجرائم الالكترونيه، أطروحة دكتوراه، جامعه مولود معمري، الجزائر، 2018.

- الحسيني، عمار عباس، التصوير المرئي والتسجيل الصوتي وحجتهما في الاثبات الجنائي، الطبعة الاولى، المركز العربي للنشر والتوزيع، القاهرة، مصر، 2017.
- الحمد، مسره خالد، الدليل الرقمي ومعايير جودته في الاثبات الجنائي، الطبعة الاولى، مركز الكاتب الاكاديمي، عمان، الاردن، 2014.
- سلمان، عتد الستار شاكر، جرائم لامن السيبراني واثر الجهود الدوليه في مكافحتها، ط1، هاتريك للنشر والتوزيع، 2023.
- العودي، جلال فضل، الارهاب السيبراني، مكتب النائب العام، التوجيه المعنوي الامن العام اليمن، عدن، 2022.
- العودي، جلال فضل، مقالات في الجرائم السيبرانيه، تعرض لموقع اخباري روسيا اليوم، عدن، 2022.
- القرعان، محمود، الجرائم الالكترونيه، ط1، دار وائل للنشر، عمان– الأردن، 2017.
- المايل، عبد السلام والشريجي، عادل، الجريمه الالكترونيه في الفضاء الالكتروني، مجله افاق للبحوث والدراسات، المركز الامعي ايلزي، طرابلس، 2019.
- مهمل، أسامة، الاجرام السيبراني، رساله ماجستير كليه الحقوق والعلوم السياسيه، جامعه محمد بوضياف، الجزائر، 2018.

القوانين :

- قانون الأمن السيبراني الاردني رقم 16 لسنة (2019
- قانون الجرائم الالكترونيه رقم(17) لسنه 2023
- قانون أصول المحاكمات الجزائية الأردني رقم 9 لسنة 1961

