مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية

Confronting cyber crimes in the light of international conventions

ط. د/ قطاف سليمان

مخبر البحث في الحقوق والعلوم السياسية-جامعة عمار ثليجي الأغواط، الجزائر

s.guettaf@lagh-univ.dz

أ.د: بوقرين عبدالحليم

كلية الحقوق والعلوم السياسية - جامعة عمار ثليجي الأغواط، الجزائر

Halim.ma@yahoo.fr

تاريخ الاستلام: 2022/01/02 تاريخ القبول للنشر: 2022/05/03

****

ملخص:

باتت الجرائم السيبرانية نوع جديد من أنماط الجريمة وما تتميز به من خاصية عابرة للحدود الإقليمية للدول مما أدى إلى توجه المجتمع الدولي للتعاون من أجل التصدي لتلك الجرائم ، إذا ما تركت على الأمن القومي للدول في جميع النواحي، لذلك سعت الدول إلى اتخاذ إجراءات مشتركة للتصدي لتلك الجرائم، وذلك من خلال إبرام اتفاقيات ومواثيق دولية لمواجهة تلك الجرائم والعمل على محاربتها خاصة جهود الأمم المتحدة، منها اتفاقية بودابست لمكافحة الجرائم السيبرانية، واتفاقية جامعة الدول العربية وكذلك الاتفاقيات الثنائية والمتعددة لتسليم المجرمين، والتي تعد من أهم أساليب مكافحة تلك الجرائم نظرا لما تتمتع به تلك الجريمة من خاصية اللاحدودية.

الكلمات المفتاحية: الجريمة السيبرانية، الاتفاقيات الدولية، التعاون الدولي، الأمن السيبراني

Abstract:

Has become cybercrime a new type of crime patterns and the characteristics of the transient characteristic of the regional borders of the countries which led to the orientation of the international community to cooperate in order to address those crimes, if left on the national security of States in all respects, so sought states to take joint action to address those crimes, through the conclusion of the charters of

international conventions that to confront the crimes and work on the special United Nations efforts to combat it, including the Budapest Convention against cybercrime, and the Convention on the League of Arab States, as well as bilateral and multilateral agreements for extradition, which is one of the most important combat methods of crime because of its This crime is a characteristic of infinity.

Keywords :cyber crime, international agreements, international cooperation, cyber

مقدّمة:

لقد أحدثت تكنولوجيا المعلومات والاتصالات ثورة شاملة في جميع نواحي الحياة، وزادت هيمنة تكنولوجيا المعلومات والاتصالات على نسق الحياة العام، وصاحب ظهور الحاسب الآلي والتوسع في استخدام شبكة الإنترنت في مجالات الحياة المختلفة ظهور بعض الآثار السلبية والمخاطر المترتبة على هذا التوسع الكبير، إذ كلما زاد الاعتماد على هذه التقنيات في التنمية زادت المخاطر الخاصة بحماية المعلومات، ومع تزايد الاعتماد العالمي على تكنولوجيا المعلومات والاتصالات تزايد أيضا التعرض للجرائم السيبرانية، إذ أصبح الفضاء السيبراني عرضة للانتهاكات من قبل مخترقي الشبكات سواء أكانوا دولا أو غيرها مما يملكون هذه التقنيات المعلوماتية، فتوجهت الأنظار إلى لاهتمام وبشدة إلى الأمن السيبراني، وأصبح الحفاظ عليها حفاظا على الأمن القومي للدول (أميرة عبدالعظيم ، 2020، صفحة 370).

لذا أصبح أمن الفضاء السيبراني يدخل ضمن أولويات للعديد من الدول، ودفعت التهديدات المتزايدة لأمن الفضاء السيبراني العديد من الدول للعمل على بذل جهود مضنية في استحداث قوانين لمكافحة الجريمة السيبرانية، لذا قامت العديد من الدول باعتماد استراتيجيات من شأنها دعم الجانب العسكري في الفضاء السيبراني ليس فقط ضد الهجمات التي قد يقوم بها الأفراد والقراصنة بل أيضا ضد احتمال استخدام الدول لمثل هذا المجال الجديد في الصراع، ولذلك بات من الضروري توحيد الجهود الدولية لوضع الأطر القانونية والتنظيمية والإجرائية لمواجهة المخاطر السيبرانية، وآثارها على المستوى الدولي (أميرة عبدالعظيم ، 2020، صفحة 372) لمواجهة تهديدات أمن الفضاء السيبراني، والعمل على استجابة القانون الدولي لما يحدث من تهديدات في الفضاء السيبراني، وتعزيز أشكال التعاون الدولي في سبيل مكافحتها من أجل حفظ أمن الفضاء السيبراني.

وقد أطلقت العديد من المبادرات التي تقوم بها المنظمات الدولية لدعم الأمن السيبراني مثل الاتحاد الدولي للاتصالات الذي أطلق مبادرة للأمن السيبراني وحلف شمال الأطلنطي الذي أنشا وحدة للدفاع السيبراني، وأطلق الاتحاد الأوربي مبادرة للأمن السيبراني، فأصبحنا الآن أمام جرائم حقيقية متكاملة تتم عن طريق شبكات الانترنت، وأجهزة الحاسوب من التخطيط والترويج لعمليات إرهابية، والنصب والاحتيال لسرقة الأموال، والتجسس وكذلك القرصنة باعتبارها الجريمة الأكثر شيوعا، وأصبحت الجريمة السيبرانية تكلف الاقتصاد العالمي خسائر فادحة ويتعرض الفضاء السيبراني إلى 1000 هجوم كل دقيقة، و تهديد أمن المطارات والمصانع الكيمائية ومحطات الطاقة النووية فيه وغيرها من المؤسسات التي تسير بنظام الحاسوب ولا تطبق إجراءات أمنية بشكل كاف وعلى هذا فيمكن اعتبار تحدي الأمن السيبراني أعلى تحديات الأمن الدولي في الوقت الراهن، فقد أسقطت تكنولوجيا المعلومات والاتصالات مفهوم الحدود الجغرافية بين الدول. (أميرة عبدالعظيم ، 2020، صفحة 375) .

أهداف الدراسة:

1-التعريف بمفهوم الامن السيبراني والجريمة السيبرانية.

2-التعرف على الجهود المبذولة في مواجهة الجرائم السيبرانية.

3-بيان الصعوبات التي تواجه الجهود الدولية في القضاء على الجرائم السيبرانية.

منهج الدراسة:

كون هذا الدراسة تتناول الأمن السيبراني والجريمة السيبرانية والجهود الدولية في مكافحة الجرائم السيبرانية والصعوبات التي تواجها فإن المنهج العلمي المتبع فيها سيكون المنهج الوصفي التحليلي المقارن إذ سأتعرض لدراسة الجريمة السيبرانية من مفهوم القانون الدولي وللجهود الدولية والإقليمية لمكافحة جرائم السيبرانية،

إشكالية الدراسة:

ما الامن السيبراني والجريمة السيبرانية؟ ما هي الجهود المبذولة في مواجهة الجرائم السيبرانية؟ وما الصعوبات التي تواجه الجهود الدولية في القضاء على الجرائم السيبرانية؟

المبحث الأول: ماهية الامن السيبراني والجريمة السيبرانية

في هذا المبحث سوف نتطرق الى تعريف الأمن السيبراني وأهدافه وإلى مفهوم الجريمة السيبرانية كما سنحاول إعطائها خصائص تتميز بها عن غيرها من الجرائم التقليدية، كما نتطرق إلى أنواعها وصورها وذلك في المطالب الثلاث الأتية:

المطلب الأول: مفهوم الامن السيبراني وأهدافه وابعاده

يعد الأمن السيبراني من المواضيع المستحدثة والتي غيرت رؤية المجتمع الدولي لمفهوم الأمن بصفة عامة لهذا نحاول إعطاء مفهوم الأمن السيبراني أهدافه وأهميته في الفرعين التاليين:

الفرع الأول: مفهوم الامن السيبراني وأهدافه

أولا: تعريف الأمن السيبراني:

ويمكن أن نقارب هذا المفهوم من عدة زوايا:

السيبرانية لغة:

وهي مأخوذة من كلمة (سيبر) وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي، فالسيبرانية تعني (فضاء الأنترنت)، وهي كلمة مشتقة من الكلمة اليونانية التي وردت بداية في مؤلفات الخيال العلمي، وكان يقصد بها قيادة ربان السفينة

السيبرانية اصطلاحا: كلمة سيبرانية في مفهومها الحديث استعملت لأول مرة من قبل عالم الرياضيات الأمريكي «نوربرت وينر» وهو أستاذ الرياضيات في معهد ماساشوستس التقني MIT الذي أعطاها مفهومها الإصطلاحي الحديث وكان ذلك عام 1948، ومن أجل وصف نظام التغذية الرجعية الاستفادة من مخرجات الأنظمة في ضبط مدخلاتها وفي التحكم فيها واستقرار أدائها (إدريس ، 2019، صفحة 103)

فالأمن السيبراني هو عبارة عن مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير 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 الفضاء السيبراني (ياسمين بلعسل و عمروش، 2021، صفحة 164)

إن للأمن السيبراني عدة تعاريف لكنها تصب كلها في مفهوم واحد وهو توفير الحماية السيبرانية بهدف توافر وإستمرارية عمل نظم المعلومات وإتخاذ التدابير الازمة لحماية الافراد والدول من المخاطر السيبرانية، ونعرف ذلك من خلال الأهداف التي أنشأ لأجلها.

ثانيا: أهداف الأمن السيبراني

يهدف الأمن السيبراني إلى تعزيز الحماية الأنظمة الإلكترونية وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية وجميع مكوناتها المحيطة بالمجتمع من أجهزة وبرمجيات ومعدات وجميع ما يؤثر على تقدم هذه الخدمات، ومن أهم ما يدور في هذه التخصص والذي يقدمه هو:

- تأمين البنى التحتية لأمن المعلومات والبيانات الخاصة بالمواطنين، إذ لا بد من حماية قوية لجميع ما يتعلق ببيانات المواطنين وحفظها في مكان آمن، وكذلك جميع أجهزتها ومواردنا الحياتية سواء من ممتلكات إلكترونية من أي محاولة عبث أو اختراق أو تدمير وتوفير الحماية اللازمة؛
- حماية شبكة المعلومات والاتصالات والتي تلعب دورا كبيرا في تدفق خط سير تدفق البيانات بين المواطنين والدولة ومن طرف إلى طرف آخر، والتي إذا تعرضت إلى تخريب أو تدمير أو اختراق حتما قد يؤثر ويقطع هذه الاتصالات ويتوقف سير العمل وتتوقف الخدمات؛
- حماية شبكة المعلومات من أي هجوم وذلك بمعرفة آخر التقنيات والتكتيكات الموجود في هذا المجال ومن أهمها كشف أهداف رسائل هذا العدو والتعرف على طبيعة هذا المهاجم وذلك وماذا يريد من خلال معرفة تكنيكاته المستخدمة والأساليب المختلفة لكي يتم العمل على إيقاف هذا الهجوم بأسلوب علمي وتقني محكم يمنع هذا الهجوم
- تشفير التعاملات الإلكترونية بحيث لا يستطيع أي مخترق أو مهاجم أو عابث أن يدخل بسهوله لهذه البيانات والتطبيقات لأن التشقير أحد أساليب الحماية والتي يصعب فك رموزها لأنها تمس أمور حياتنا وتمس أمننا الإلكتروني. (عسيري، 2002)

الفرع الثاني: أهمية الامن السيبراني وابعاده

أولا: أبعاد الأمن السيبراني:

1-البعد العسكري:

لقد كانت بدايات الانترنت في بيئة عسكرية، بشكل أساسي، لتنتقل فيما بعد إلى الأوساط العلمية والأكاديمية، تمثلت في أبحاث تخدم القدرات العسكرية وتطورها، والانجازات العلمية التي تسهم في تفوق بلد على آخر، حيث كان التنافس على أشده بين الاتحاد السوفياتي والولايات المتحدة الأميركية في مجال الوصول إلى الفضاء الخارجي وتطوير الأسلحة النووية،

وتتراكم الأمثلة الموضحة لذلك، نذكر منها مثلا ما حصل في جورجيا واستونيا وكوريا الجنوبية وإيران كمثال على بعض الهجمات والاختراقات التي ترجمت ماديا سواء باندلاع صراع مسلح لاحق، كذلك الذي وقع بين روسيا وجورجيا أو بانقطاع الاتصال بالأنترنت في استونيا، بين الدولة والمواطنين، والتشويش على الإدارات الحكومية. الكهربائية، والمياه، والاتصالات السلكية واللاسلكية والخدمات الصحية، والنقل والانترنت وتكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الإلكتروني سيؤدي بالضرورة إلى شن هجمات إلكترونية مضادة على شبكات القوات العسكرية، ومن ثم تدمير قواعد البيانات وما يلحقه من مخاطر (بارة، 2017، صفحة 260)

2-البعد الاقتصادي:

أصبح الفضاء الإلكتروني جاذبا لقطاعات المجتمع كافة، افرادا وجماعات وزاد الاعتماد بصورة أساسية على التكنولوجيا الرقمية في تخزين البيانات والمعلومات، بالإضافة لاستخدام الحاسب الآلي في تطوير الصناعات وتحريك الاقتصادات، وأصبحت المعاملات المالية والاقتصادية محوسبة، وباتت شبكات البنوك والبورصات وشركات الأسواق المالية مرتبطة ببعضها البعض بنظم وشبكات الكترونية، فأصبحت الإنترنت هي أساس المعاملات المالية والاقتصادية وباتت تشكل محورا رئيسيا للتطور الاقتصادي في القرن الحادي والعشرين، وهو ما أثار الحديث عن أهمية تحقيق الأمن السيبري في المجال الاقتصادي (حجازي، 2007)

3-البعد الاجتماعي:

تساهم شبكات التواصل الاجتماعي بشكل خاص في فتح المجال للأفراد للتعبير عن تطلعاتهم السياسية وطموحاتهم الإجتماعية بأشكالها المختلفة، كذلك تشكل مشاركة جميع شرائح المجتمع ومكوناته وسيلة لتطوير المجتمع مما يتيح الفرصة للاطلاع على الأفكار والمعلومات وبما تكونه من حاجة لدى المجتمع في الحفاظ على استقرار الفضاء الإلكتروني والمجتمع الذي يرتكز إليه، كما أن انفتاح مجتمع ما على المجتمعات الأخرى يؤسس لتبادل خبرات وأفكار وتكوين آفاق التعاون والتكامل (إدريس ، 2019، صفحة 105)

4-البعد القانوني:

يترتب على النشاط الفردي والمؤسساتي والحكومي في الفضاء السيبراني نتائج قانونية وموجبات تستدعي اهتماما خاص لحل النزاعات التي يمكن أن تنشأ عنها، وهو ما يستدعي مواكبة التحولات التي رافقت ظهور مجتمع المعلومات، فظهرت حقوق أخرى كحق النفاذ إلى

الشبكة العالمية للمعلومات وتوسعت بعض المفاهيم لتشمل أساليب الممارسة الجديدة باستخدام تقنيات المعلومات والاتصالات، كالحق في إنشاء المدونات الالكترونية والحق في إنشاء التجمعات على الانترنت والحق في حماية ملكية البرامج المعلوماتية.

5-البعد السياسي

هناك أمثلة كثيرة تدفع نحو الاهتمام بالبعد السياسي للأمن السيبراني، كالتسريبات المختلفة للوثائق الحساسة التي تؤدي إلى مشكلات عويصة جدا على المستوى الخارجي والدولي، كما أنه لا ينكر أحد الدور المتعاظم الشبكات التواصل الاجتماعي على المستوى السياسي حملات انتخابية، تظاهرات افتراضية، حركات احتجاجية إلكترونية، كما يتم استغلال هذه المواقع من طرف العديد من الحكومات لتمرير سياساتها (بارة، 2017، صفحة 263)

ثانيا: أهمية الامن السيبراني:

تكمن أهمية الأمن السيبراني في توفير وضع أمني جيد لأجهزة الكمبيوتر والخوادم والشبكات والأجهزة المحمولة والبيانات المخزنة على هذه الأجهزة من المهاجمين ذوي النوايا الخبيثة، يمكن تصميم الهجمات الإلكترونية للوصول إلى البيانات الحساسة للمؤسسة أو المستخدم أو حذفها أو ابتزازها.

الجميع الآن في حاجة إلى وجود الأمن السيبراني في المؤسسات والشركات والمصانع والجهات الحكومية وحتى المنازل، وقد أصبح ضرورة ملحة بعد ظهور الثورة الصناعية الرابعة أو ما يعرف بثورة البيانات، لأن فضاء الإنترنت أصبح يعج بالمعاملات والتعاملات الإلكترونية والتي تحتاج إلى تشفير وتأمين تلك التعاملات. (أمنة ، 2021) ،كما سبق وأن ذكرنا أن من أهداف الأمن السيبراني هو مكافحة المخاطر السيبرانية ومن بين وأهم المخاطر التي هي في صلب الفضاء السيبراني هي الجريمة السيبرانية، إذن ماهي الجريمة السيبرانية ,أنواعها...إلخ؟ في هذا المطلب.

المطلب الثاني: تعريف الجريمة السيبرانية وانواعها

للجريمة السيبرانية مسميات كثيرة فالبعض يطلق عيها اسم جرائم الحاسب الآلي والبعض الأخر الجرائم المستحدثة أو جرائم الكمبيوتر أو الجرائم الإلكترونية، ونظرا لطبيعتها الخاصة التي تتميز بها فهي أوسع وأشمل من المسميات السابقة وسوف نحاول تفريقها ومعرفة أنواعها على النحو التالي:

الفرع الأول: تعريف الجريمة السيبرانية:

يمكن تعريف الجريمة السيبرانية بأنها: "**كل فعل أو امتناع عن فعل باستعمال نظام معلوماتي معين للإضرار بمصلحة أو حق يحميه القانون من الآلي أو بمساعدته أو أن يكون أداة رئيسية في ارتكابه، أو له دورا هاما إيجابيا في هذا الارتكاب**"

الطائفة الثانية: نظرت إلى محل الجريمة باعتباره أساسا لتعريف هذه النوعية من الجرائم، وبتالي عرفت الجريمة المعلوماتية بأنها كل سلوك أو نشاط غير مشروع يتعلق بنسخ أو تغيير أو حذف البيانات أو المعلومات المخزنة داخل النظام أو الوصول إليها أو تلك التي يتم تحويلها عن طريقه أو هي كل سلوك أو نشاط غير مشروع موجه إلى المعالجة الآلية للبيانات أو نقلها.

الطائفة الثالثة: حاولت الجمع بين الوسيلة التي يتم بها ارتكاب الجريمة ومحل أو موضوع هذه الجريمة، ومن ثم عرفت الجريمة المعلوماتية بأنها: "كل عمل غير قانوني أو كل سلوك غير مشروع يستخدم فيه الحاسب كأداة أو موضوع للجريمة أو هي كل فعل جنائي يكون الحاسب أداة أو موضوع للنشاط غير المشروع، أو هي كل فعل أو امتناع عن فعل من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجة بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية، أو التقنية المتقدمة لنظم التطورات.

وقد ذهب مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فيينا عام 2000 إلى تعريف الجريمة السيبرانية بأنها: "**أي جريمة يمكن ارتكابها على نظام حاسوبي أو شبكة حاسوبية، وتشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية**".

ولعلنا نلاحظ أن هذا التعريف قد حاول الإحاطة بجميع الأشكال الإجرامية للجريمة السيبرانية، سواء تلك التي تقع بواسطة النظام المعلوماتي، أو داخل هذا النظام على المعطيات والبرامج والمعلومات، كما يشمل التعريف جميع الجرائم التي يمكن أن تقع في بيئة سيبرانية، فلم يحصر الجريمة المعلوماتية في مجال محدد حتى لا يتيح للعديد من الأفعال السيبرانية الإفلات من دائرة العقاب، ولعلنا نؤيد هذا التعريف نظرا لشموله لجميع أشكاله الجرائم السيبرانية. (أميرة عبدالعظيم ، 2020، الصفحات 391-393)

الفرع الثاني: أنواع الجريمة السيبرانية:

تتنوع الممارسات التي تهدد الأمن السيبراني، يتنوع أهدافها، كما ويتنوع الجهات، التي تعتمدها ويمكن ايراد بعضها على الشكل الآتي:

1-التعرض لسرية الاتصالات، التي تطال البريد الإلكتروني والدردشة ونقل الملفات والدخول إلى الأنظمة للاطلاع على المعلومات دون اذن، ويشابه هذا التنصت على المخابرات الهاتفية والاطلاع على البريد الشخصي ودخول المنازل لتفتيشها، ما يتطلب عادة وبحسب القواعد القانونية اذنا مسبقا من قبل السلطات المختصة في البلاد التي تقوم على احترام القاعدة القانونية، وتعتبر هذه الأعمال في غير تلك الحالة سواء قام بها الأفراد أو قامت بها السلطات العامة جرائم اعتداء على الحريات والحقوق الشخصية.

2-التلاعب بالمعلومات الموجودة في نظام معين وتشويهها أو اتلافها سواء عبر الاقتحام البدوي أو عبر ارسال برامج وفيروسات متخصصة بذلك، ففي هذا اعتداء على الملكية وعلى حقوق التمتع والتصرف بها يضاف إلى ذلك التعرض لسلامة عمل المواقع الشخصية منها والتجارية عندما تتوفر نية الأضرار بغض النظر عن تحقق الضرر المرجو أم لا، الجرائم العادية التي تستخدم الانترنت في تنفيذها، كالسرقة والغش والخداع والتغرير بالقاصرين وتسهيل الدعارة والترويج لنشاطات مخالفة للقانون والاعتداء على الملكية الفكرية، فكل هذه جرائم تعاقب عليها القوانين الوضعية ويميل إلى القول هنا انها لا تتطلب بالضرورة إقرار نصوص جديدة بل تعديل ما هو موجود، ليتناسب مع العناصر المادية الجديدة التي يدخلها الفضاء السيبيري، من خلال طبيعته الخاصة.

3-الجرائم التي تندرج في إطار الجريمة المنظمة والتي تهدد أمن الأفراد والدول على السواء في الفضاء السيبيري وفي الفضاء التقليدي، وتأتي في هذا الإطار جرائم تبييض الأموال والإرهاب (منى الأشقر ، 2016)

المطلب الثالث: خصائص الجريمة السيبرانية وصورها

بعد ما تعريف الجريمة السيبرانية وانواعها سنتطرق إلى خصائصها وصورها في الفرعيين التاليين:

الفرع الأول: خصائص الجريمة السيبرانية

إن الجريمة السيبرانية تتميز بعدة خصائص منها:

أولا: جرائم ترتكب بواسطة الأجهزة الالكترونية كالحاسب الالي والهواتف الخلوية:

وهما الأداتان التي تمكن المجرم من دخول الإنترنت لتنفيذ جريمته.

ثانيا: جرائم خفية: فليس من السهولة اكتشافها لضعف القدرة الفنية للضحية وذلك مقارنة بالمجرم ولربما أيضا لمهارات المجرم الفنية والعلمية المتقدمة لقدرته على إخفائها أو لخوف الضحية من الإبلاغ عن الجريمة تجنبا للإساءة إلى السمعة.

ثالثا: جرائم سريعة التنفيذ: فسرعة ارتكاب الجريمة قد تكون خلال جزء من الثانية وقد لا تتطلب الإعداد قبل التنفيذ.

رابعا: جرائم عن بعد: فيمكن للجاني تنفيذ جريمته وهو في دولة بعيدة كل البعد عن المجني عليه.

خامسا: جرائم عابرة للحدود: فهي لا تعرف الحدود الجغرافية للدول، لارتباط العالم بشبكة واحدة وهذا قد يسبب إشكاليات لدى الاختصاص القضائي من حيث التحقيق والمحاكمة، وذلك تبعا لتعقيد الإجراءات التي تحكمها الاتفاقيات والمعاهدات والعلاقات الدولية، والتنازع فيما بينهما على أي القانون الواجب التطبيق (روان بنت عطية الله، 2020، صفحة 11)

سادسا: جرائم صعبة الإثبات: وتكمن صعوبة إثباتها إلى أن متابعتها واكتشافها عن طريق الصدفة ومن الصعوبة حصرها في مكان معين حيث أنها لا تترك أثرا واضحا للعيان أو تشاهد بالعين المجردة فما هي إلا أرقام تدور في السجلات والمواقع الالكترونية، كما أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف عنها وتعود الصعوبة لعدة أسباب منها إنها كجريمة لا تترك أثرا بعد ارتكابها صعوبة الاحتفاظ الفني بآثارها إن وجدت تحتاج لخبرة فنية يصعب على المحقق التقليدي التعامل معها تعتمد على الخداع في ارتكابها، والتضبيب في التعريف على مرتكبيها.

سابعا: جرائم ناعمة: فهي جرائم لا تمارس بالعنف ولا تحتاج إلى أدني مجهود عضلي بعكس بعض الجرائم التقليدية.

ومن هنا نلاحظ بأن المجرم السيبراني يتميز بمهارات عالية، فهو يعتمد على قدراته العقلية بالذكاء والدهاء ومعرفة الطرق السيبرانية لإتلاف البرامج واختراق الحواجز الأمنية، ولعل الدافع للمجرمين السيبرانيين قد يكون بدافع المال بلجوئهم إلى الطرق الغير مشروعة وذلك بسبب ما يعانوه من البطالة، وقد يكون بدوافع عقائدية وسياسية أو للتجسس وانتهاك الخصوصية. (روان بنت عطية الله، 2020، صفحة 12)

بعد معرفة أنواعها وخصائصها جلي بنا أن نعرف صور ها.

الفرع الثاني: صور الجريمة السيبرانية

تتعدد أشكال الجرائم السيبرانية وتختلف من حيث الطبيعة والمصادر والأهداف كالتجسس وسرقة المعلومات وشن الحروب وبالتالي بات العديد من الفواعل الدوليين يلجئون إلى آليات إلكترونية لتحقيقها، وعلى الرغم من تعدد صور وأشكال الهجمات الإلكترونية، غير أنه من الممكن تقسيمها إلى المجموعات رئيسية التالية:

1-خطر الكوارث الطبيعية أو (العرضية للكابلات البحرية):

تعد الكبلات Submarine Cableجزء هاما لتوفير خدمة الاتصالات بين دول العالم في مجال الأنترنت وشبكات الكمبيوتر وغيرها، فمنذ عام 2005 أصبحت الكابلات البحرية مأهولة على مجال الاتساع والانتشار، أما على نطاق التقدم والتطور تحولت إلى تقنيات أخف وزنا وأصغر حجما، كما تعرضت تلك الكابلات إلى عدد من المشكلات التي تؤثر سبا على أعمال البنى التحتية بالضرر، حيث لا تقع في مياه المحيط العميق.

2-التجسس السيبراني Cyber Espionage:

يعد أحد أنواع التجسس التقليدي، باستخدام وسائل التكنولوجيا الفائقة، ومعظم الهجمات السيبرانية المتطورة التي تقع ضمن هذه الفئة، حيث يتم الحصول على معلومات سرية بطرق غير مشروعة بهدف الحصول على أفضلية اقتصادية، أو استراتيجية أو عسكرية. فالتجسس السيبراني هو ذلك التجسس الذي يعتمد على إستخدام التقنيات الإلكترونية في الحصول على معلومات، ويختلف التجسس السيبراني من حيث النوع، فهناك التجسس عن طريق الأفراد، ومن خلال الشبكات السلكية أو التجسس من خلال الأقمار الصناعية. (إدريس ، 2019، صفحة 109)

3-الإرهاب السيبرانيCyber Terrorism:

المقصود بالإرهاب المعلومات أو الإرهاب السيبراني هو ذلك الاستخدام للموارد المعلوماتية، المتمثلة في الإعلام وأجهزة الحاسوب وشبكة الأنترنت والفضائيات من أجل أغراض التخويف أو الإرغام لأغراض سياسية، أو الاقناع الفكري والتثقيف السلبي والعدواني، ويرتبط الإرهاب المعلوماتي إلى حد كبير بالمستوى المتقدم للغاية والذي باتت تكنولوجيا المعلومات والإعلام تؤديه في جميع مجالات الحياة في العالم، ويمكن أن يتسبب الإرهاب المعلوماتي في إلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات أو قطع شبكات الاتصالية بين الوحدات والقيادة المركزية وتعطيل أنظمة الدفاع الجوي وغيرها.

4-الحروب السيبرانية Cyber Warfare

تشمل الحروب السيبرانية الناجحة على أكثر من «مشغلي» حروب إلكترونية، وتعتمد على فريق من المختصين في المعارك الإلكتروني، حيث كل منهم يتميز بمسؤولياته ومهاراته الخاصة لترسيخ القدرة على القتال والتحكم بها وإبرازه ضمن الفضاء السيبراني، ويقوم مشغلو «الحروب السيبرانية» بالتخطيط للنشاطات الهجومية والدفاعية وإدارتها وتنفيذها عبر الفضاء السيبراني (إدريس ، 2019، صفحة 110)

المبحث الثاني: الجهود الدولية والإقليمية في مواجهة الجريمة السيبرانية

إن هناك العديد من الهيئات والمنظمات والمجالس الدولية التي تلعب دورا ملحوظا في إطار إبرام الاتفاقيات في محاولة منها لترسيخ وجوب التعاون الدولي لمواجهة الجرائم السيبرانية، وعلى رأس هذه المنظمات هيئة الأمم المتحدة، والمجلس الأوروبي وبعض الهيئات الأخرى، وعليه فإن هذا الموضوع ستتم معالجته عبر مطالب ثلاثة يخصص الأول منها لدور الأمم المتحدة ومنظمة التعاون الاقتصادي والتنمية، ويخصص الثاني للجهود الإقليمية كاتفاقية بودابست والاتفاقية العربية، ويخصص الثالث لعرض الصعوبات التي تواجه الجهود الدولية وكيفية القضاء عليها.

المطلب الاول: الجهود الدولية في مكافحة الجريمة السيبرانية

سنتطرق في هذا المطلب إلى جهود الأمم المتحدة وبعض المنظمات الدولية كمنظمة التعاون الاقتصادي والتنمية والإتحاد الدولي للاتصالات.

الفرع الأول: جهود الأمم المتحدة في مجال مكافحة الجريمة السيبرانية

اتخذ المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة توصية بأن تأخذ المنظمة الدولية على عاتقها دورا رئيسيا في رسم سياسة منع الجريمة وتحقيق العدالة الجنائية دولية، وفعلا تحقق ذلك بموافقة الجمعية العامة للأمم المتحدة في العام 1950م على هذه التوصية التي بموجبها تم إنشاء اللجنة الاستشارية الخبراء منع الجريمة ومعاملة المجرمين التي يقع على عاتقها مهمة مكافحة الجريمة وتقديم المشورة للأمين العام وإيجاد البرامج ووضع الخطط ورسم سياسات لتدابير دولية في مجال منع الجريمة ومعاملة المجرمين.

وبعد انعقاد مؤتمر الأمم المتحدة لمنع الجريمة ومعاملة المجرمين في كيوتو باليابان عام 1970م، تم استبدال اللجنة الاستشارية بلجنة منع الجريمة ومكافحتها بناء على توصية للمجلس الاقتصادي والاجتماعي عام 1971م. حيث تهدف مؤتمرات الأمم المتحدة المعنية بمنع الجريمة ومعاملة المجرمين التي تعقد كل خمس سنوات إلى تعزيز تبادل المعرفة والخبرات بين

الأخصائيين من مختلف الدول وإلى تدعيم التعاون الدولي والإقليمي في مكافحة الجريمة، وهي بذلك تشكل محفلا رئيسيا للتعاون الدولي والذي يعنينا في هذه الدراسة هو جهود الأمم المتحدة من خلال مؤتمراتها الخاصة بمنع الجريمة ومعاملة المجرمين المتعلقة بالجرائم التقنية أو جرائم الحاسب الآلي وهنا تشير إلى أن مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين الذي تم انعقاده في مدينة ميلانو بإيطاليا في العام 1985م (عبابنة، 2009، صفحة 156)، انبثقت عنه مجموعة من القواعد التوجيهية والتي اكتملت صياغتها في احات الإقليمية التحضيرية للمؤتمر الثامن الذي أجاز هذه المبادئ والذي عقد في هافانا بكوبا في العام 1990م.

كما أكد المؤتمر على وجوب تطبيق التطورات الجديدة في مجال العلم والتكنولوجيا في كل مكان لصالح الجمهور وبالتالي لمنع الجريمة على نحو فعال، كما أكد على أن التكنولوجيا بما أنها قد تولد أشكالا جديدة من جريمة فإنه ينبغي اتخاذ تدابير ملائمة ضد حالات إساءة الاستعمال الممثلة لهذه التكنولوجيا وأشاروا إلى مسألة الخصوصية التي يمكن أن تخترق عن الاطلاع على البيانات الشخصية المخزنة داخل نظم الحاسبات الآلية، والتي تشكل انتهاكا لحقوق الإنسان واعتداء على حرمة الحياة الخاصة وأكد على وجوب اعتماد ضمانات ملائمة لصون السرية، وإقرار نظم تكفل وصول الأفراد إلى هذه البيانات التصحيح الأخطاء فيها، كذلك المؤتمر عبر قواعده التوجيهية على ضرورة تشجيع التشريعات الحديثة التي تجرم وتتناول جرائم الحاسب الآلي باعتبارها نمطا من أنماط ال المنظمة كغسيل الأموال والاحتيال المنظم وفتح حسابات وتشغيلها بأسماء وهمية. (عبابنة، 2009، صفحة 157) ،ويمكن إجمال توصيات مؤتمر هافانا للعام 1990م وذلك طبقا للمبادئ التالية:

1. تحديث القوانين الجنائية الوطنية بما في ذلك التدابير المؤسسية؛
2. تحسين أمن الحاسب الآلي والتدابير المنيعة؛
3. اعتماد اجراءات تدريب كافية للموظفين والوكالات المسؤولة عن مع الجريمة الاقتصادية والجرائم المتعلقة بالحاسب الآلي والتحري والادعاء فيها؛
4. تلقين آداب الحاسب الآلي كجزء من مفردات مقررات الاتصالات والمعلومات واعتماد سياسات تعالج المشكلات المتعلقة بالمجني عليهم في تلك الجرائم؛
5. زيادة التعاون الدولي من أجل مكافحة هذه الجرائم.

كذلك فقد عقد المؤتمر التاسع لمنع الجريمة ومعاملة المجرمين برعاية الأمم المتحدة في القاهرة وذلك في العام 1990م، والذي أكدت توصياته ايضا على وجوب حماية الإنسان في

حياته الخاصية وفي ملكيته الفكرية من تزايد مخاطر التكنولوجيا ووجوب التنسيق والتعاون بين أفراد المجتمع الدولي لاتخاذ الإجراءات المناسبة للحد منها. (عبابنة، 2009، صفحة 158)

ربما تكون أفضل استراتيجية طويلة الأجل لمكافحة الجريمة السيبرانية هي من خلال الاتفاقات الدولية التعاون في تقديم مرتكبي جرائم الكمبيوتر إلى العدالة. نظرًا للانتشار العالمي للإنترنت، ويمكن أن تنشأ الجريمة الإلكترونية نفسها في أي مكان في العالم وتستهدف أي دولة بها مستخدمو الإنترنت، تتمثل المشكلة المتكررة في مزيج من الاختصاصات القضائية التي تتجاوزها الجرائم الإلكترونية، وتتم معظم الجهود في مكافحة الجرائم السيبرانية من خلال تدابير أمنية تقنية، مثل مكافحة الفيروسات وتصفية البريد العشوائي والتشفير هذا يمنع الهجمات الإلكترونية من النجاح حيث تكون هذه الإجراءات الأمنية كافية، لكنها لا تمنع مجرمي الإنترنت من العثور على أهداف مناسبة في مكان آخر، ويحتمل أن يكون أفضل وسيلة يتم القضاء على هجمات مجرمي الإنترنت تمامًا عن طريق حبس الجاني (Alex , 2015)

الفرع الثاني: جهود المنظمات الدولية في مجال مكافحة الجريمة السيبرانية

قد اتخذت مبادرات من قبل العديد من المنظمات كالاتحاد الدولي للاتصالات (ITU)، الإنتربول/يوروبول منظمة التعاون الاقتصادي والتنمية (OECD)، مؤسسة الإنترنت للأسماء والأرقام المخصصة (ICANN) والمنظمة الدولية لتوحيد المقاييس (ISO)، واللجنة الكهرو تقنية الدولية (IEC) وفرق عمل هندسة الإنترنت ومنظمة التعاون الاقتصادي للمحيط الهادئ وآسيا (APEC) ومنظمة الدول الأميركية (OAS) ورابطة دول جنوب شرق آسيا (ASEAN) وجامعة الدول العربية، والاتحاد الأفريقي، وسنأخذ في دراستنا منظمتين على سبيل المثال:

أولا: منظمة التعاون الاقتصادي والتنمية (OECD)

تهدف هذه المنظمة إلى تحقيق أعلى مستويات النمو الاقتصادي وتناغم التطور الاقتصادي مع التنمية الاجتماعية، بدأت هذه المنظمة الاهتمام بالجريمة السيبرانية منذ عام1978،حيث وضعت مجموعة من الأدلة وقواعد إرشادية تتصل بتقنية المعلومات، ويعد الدليل المتعلق بحماية الخصوصية وقواعد نقل البيانات من أول الأدلة التي تم تبنيها من قبل مجلس المنظمة في عام 1980 مع التوصية للأعضاء بالالتزام فأصدرت سنة 1983 تقريراً بعنوان الجرائم المرتبطة بالحاسوب وتحليل السياسة القانونية الجنائية، حيث استعرض التقرير السياسة الجنائية القائمة والمقترحات الخاصة في عدد من الدول الأعضاء، وتضمن التقرير

الحد الأدنى من لأفعال سوء استخدام الحاسوب والتي على الدول تجريمها وتشمل هذه الأفعال (مشوش، 2019، صفحة 709):

- الاستخدام أو الدخول إلى نظام ومصادر الحاسب على نحو غير مصرح به؛
- الإفشاء غير مصرح به للمعلومات المعالجة آلياً والنسخ والإتلاف أو التخريب ما يحتويه من بيانات وبرامج والإعاقة غير المشروعة للوصول لمصادر الحاسب من منع أو تعطيل استخدام الحاسب أو برامجه أو البيانات المخزنة داخله.

وفي عام 1992 وضعت المنظمة توصيات وإرشادات خاصة بأنظمة المعلومات وأوصت بضرورة أن تعطي التشريعات الجنائية للدول الأعضاء مبادئ عامة تتمثل في:

1-حدود التجميع: يتعين فرض قيود على تجميع البيانات؛

2-نوعية البيانات: حيث تنص على أن تتعلق البيانات بالغاية والغرض الذي سوف تستخدم من أجله؛

3-تعيين الغرض: بحيث يكون الغرض الذي تستخدم فيه البيانات الشخصية محصورة ومحددة سلفا؛

4-حدود الاستخدام: يقتضي الالتزام بعدم إفشاء البيانات الشخصية ونشرها لغير المصرح لهم بذلك؛

5-الوقاية الأمنية: ضرورة اتخاذ تدابير وإجراءات أمنية ملائمة وحازمة في إحاطة البيانات؛

6-**المشاركة الفردية**: حق الأشخاص المعنية في الوصول والتعرف على البيانات التي تخصهم فضلاً عن رقابة مدى صحتها؛

7-**المسائلة والمحاسبة**: التي تقتضي محاسبة الأشخاص والجهات المرخص لهم الوصول والاطلاع على البيانات والتعامل معها في حالة تجاوز أي من الإجراءات التي تكفل حماية البيانات ذات الصفة الخاصة. (مشوش، 2019، صفحة 710).

ثانيا: الاتحاد الدولي للاتصالات (ITU)

اعتمد المؤتمر العالمي لتنمية الاتصالات لعام 2006 القرار رقم (45) الذي دعا فيه مدير مكتب تنمية الاتصالات إلى تنظيم اجتماع بشأن الأمن المعلوماتي ومكافحة الرسائل الاقتحامية، وتقديم تقرير يتضمن نتائج الاجتماع إلى مؤتمر المندوبين المفوضين العام 2006، وقد تم تبني مجموعة من التوصيات في مجال الأمن المعلوماتي والرسائل الاقتحامية، كما أطلق الأمين العام للاتحاد في أيار 2007، جدول أعمال الأمن المعلوماتي العالمي لوضع إطار لمواجهة

التحديات المتزايدة لأمن الإنترنت، ولإيجاد حلول لتعزيز الثقة والأمن في مجتمع المعلومات، وفي أكتوبر 2007 أنشئ فريق من الخبراء رفيع المستوى (HLEG) ضم أكثر من مائة خبير قدموا التقارير والتوصيات في حزيران 2008 حيث نشرت الإستراتيجية العالمية في 2008/11/12 وقد اشتملت الإستراتيجية على المجالات التالية: التدابير القانونية والتدابير التقنية والإجرائية، والهياكل التنظيمية وبناء القدرات، والتعاون الدولي (النوايسة، 2017)

المطلب الثاني: الجهود الإقليمية في مكافحة الجريمة السيبرانية

الاتفاقيات والمعاهدات الدولية هي واحدة من أهمها أشكال التعاون الدولي بشكل عام وفي مجال المكافحة الجرائم الناتجة عن الجرائم لإلكترونية على وجه الخصوص بين المعاهدات والاتفاقيات التي تعمل على التعاون الدولي في مجال المكافحة الجرائم الإلكترونية، ومعاهدة بودابست لمكافحة جرائم الإنترنت واتفاقية الجامعة العربية لمكافحة الجريمة السيبرانية وتوصيات المجلس الأوروبي بشأن المشاكل الجنائية الإجراءات المتعلقة تكنولوجيا المعلومات، ونوضحها في التالية:

الفرع الأول: توصيات المجلس الأوروبي

أدى التطور السريع في مجال الحاسبات وتقنية الإنترنت وشعور الدول الأوروبية بأهمية إعادة النظر في الإجراءات الجنائية مما عجل إلى إصدار المجلس الأوروبي التوصية رقم: 13/95 بتاريخ :1995/09/11 بخصوص مشاكل الإجراءات الجنائية المتعلقة بالتكنولوجيا وتكنولوجيا المعلومات، وعقوبات وطنية لتتناسب مع التنمية في هذا المجال (AL_khafagy, 2020)، ومن بين أهم الأمور المذكورة في التوصية لأوروبية المجلس هم:

- أن توضح القوانين إجراءات تفتيش أجهزة الكمبيوتر وضبط المعلومات التي تحويها ومراقبة المعلومات أثناء انتقالها؛
- أن تسمح الإجراءات الجزائية الوطنية لجهات التفتيش ضبط برامج الكمبيوتر والمعلومات الموجودة بالأجهزة وفقا لذات الشروط الخاصة بإجراءات التفتيش العادية، ويتعين إخطار الشخص القائم على الأجهزة بأن النظام كان محلا للتفتيش مع بيان المعلومات التي تم ضبطها؛
- أن يسمح أثناء عملية التفتيش للجهات القائمة بالتنفيذ ومع احترام الضمانات المقررة بمد التفتيش إلى أنظمة الكمبيوتر الأخرى في دائرة اختصاصهم والتي

تكون متصلة بالنظام محل التفتيش وضبط ما بها من معلومات، بشرط ان يكون هذا الإجراء ضروريا؛

- أن يوضح قانون الإجراءات الجزائية أن الإجراءات الخاصة بالوثائق التقليدية تنطبق في شأن المعلومات الموجودة بأجهزة الكمبيوتر؛
- تطبق إجراءات المراقبة والتسجيل في مجال التحقيق الجنائي في حالة الضرورة في مجال تكنولوجيا المعلومات ويتعين توفير السرية والاحترام للمعلومات التي يفرض القانون لها حماية خاصة؛
- يجب إلزام العاملين بالمؤسسات الحكومية والخاصة التي توفر خدمات الاتصال بالتعاون مع سلطة التحقيق لإجراء المراقبة والتسجيل؛
- يتعين تعديل القوانين الإجرائية بإصدار أوامر لمن يحوز معلومات سواء أكانت برامج أم قواعد أم بيانات، تتعلق بأجهزة الكمبيوتر بتسليمها للكشف عن الحقيقة؛
- يتعين إعطاء سلطات التحقيق سلطة توجيه أوامر لمن يكون لديه معلومات خاصة للدخول على نظام من أنظمة المعلومات أو الدخول على ما يحويه من معلومات باتخاذ اللازم للسماح لرجال التحقيق بالاطلاع عليها؛ (الزهراني، 2020، صفحة 752)
- يجب تطوير وتوحيد أنظمة التعامل مع الأدلة الإلكترونية، وحتى يتم الاعتراف بها بين الدول المختلفة ويتعين أيضا تطبيق النصوص الإجرائية الخاصة بالأدلة التقليدية على الأدلة الإلكترونية؛
- يجب تشكيل وحدات خاصة لمكافحة جرائم الكمبيوتر وإعداد برامج خاصة التأهيل العاملين في مجال العدالة الجنائية لتطوير معلوماتهم في مجال تكنولوجيا المعلومات؛
- قد تتطلب إجراءات التحقيق من الإجراءات إلى أنظمة كمبيوتر أخرى قد تكون موجودة خارج الدولة وتفترض التدخل السريع، وحتى لا يمثل هذا الأمر اعتداء على سيادة الدولة والقانون الدولي، يجب وضع قاعدة قانونية صريحة تسمح بمثل هذا الإجراء، ولذلك كانت الحاجة إلى عمل اتفاقيات تنظم وقت وكيفية اتخاذ مثل هذه الإجراءات؛

- يجب أن تكون هناك إجراءات سريعة ومناسبة ونظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهة أجنبية لجمع ادله معينة ويتعين عندئذ أن تسمح السلطة الأخيرة بإجراءات التفتيش والضبط (الزهراني، 2020، صفحة 753).

الفرع الثاني: اتفاقية بودابست لمكافحة جرائم السيبرانية 2001:

شهدت العاصمة الماجرية بودابست، في أواخر عام 2001 أولى المعاهدات الدولية التي تكافح جرائم الانترنت. ومواكبة للتطور فقد أبرم المجلس الأوروبي اتفاقية ببوداست في:8/11/2001 ووضعت للمصادقة في:23/11/2001، والتي تضمنت التعريف بأهدافها ووضعت قائمة للجرائم التي يجب على الدول المصادقة عليها أن تحرمها في قوانينها الداخلية، وتعد الأولى في مجال مكافحة جرائم الانترنت وشملت العديد من جرائم الانترنت منها: الإرهاب، تزوير بطاقات الائتمان، دعارة الأطفال وتعمد الاتفاقية إلى تنسيق القوانين الجديدة في دول عديدة، وجاءت نتيجة مشاورات طويلة بين الحكومات واجهزة الشرطة وقطاع الكمبيوتر وصاغ نصها عدد من الخبراء في مجلس أوروبا بمساعدة عدة دول منها الولايات المتحدة (درار، 2017، صفحة 273)

كما تعد الاتفاقية الوحيدة المتعددة الأطراف المعنية بمكافحة الجرائم التي تتم باستخدام أو ضد الكمبيوتر وباستخدام شبكة الانترنت، وهي تمثل ركيزة أساسية منذ دخولها حيز النفاذ، في الأول من جويلية لعام 2004 اعلى مستوى الدول أعضاء مجلس الاتحاد الأوروبي وكما سبق الإشارة، فلقد وقعت عليها العديد من الدول من غير أعضاء مجلس اوروبا مثل كندا واليابان وجنوب إفريقيا، كما صادقت عليها الولايات المتحدة الأمريكية، كما أن هذه الاتفاقية بمثابة دعوة موجهة إلى دول العالم للتفاعل مع الانترنت جاءت نتيجة محاولات عديدة منذ ثمانيات القرن العشرين حتى ظهرت بشكلها النهائي في2001/11/23 م في بودابست وقعت عليها ثلاثون دولة أوروبية بما في ذلك الدول الأربعة من غير الأعضاء في المجلس الأوروبي المشاركة في إعداد هذه الاتفاقية وفي كندا واليابان وجنوب أفريقيا والولايات المتحدة الأمريكية، وقد تضمنت هذه الاتفاقية الأقسام التالية: (درار، 2017، صفحة 274)

القسم الأول: تحديد المصطلحات؛

القسم الثاني: الخطوات الواجب اتخاذها في إطار التشريع الوطني؛

القسم الثالث: التعاون الدولي؛

القسم الرابع: الشروط النهائية حول الانضمام إلى الاتفاقية.

كما حددت الجرائم التي يجب أن تتضمنها التشريعات الوطنية، للدول الأعضاء وذلك على النحو التالي:

- الجرائم المتعلقة بأمن الشبكات الدخول والمراقبة غير المشروعة والعدوان على الثقة في البيانات أو على النظام والإساءة إليه؛
- الجرائم المعلوماتية كما هو الشأن في الاختلاق والانتحال والنصب والاحتيال المعلوماتي... الخ؛
- جرائم الأخلاق مثل إنتاج أو بث أو حيازة ما يتعلق بدعارة الأطفال؛
- جرائم العدوان على حقوق الملكية الأدبية والفكرية كاستنساخ المصنفات المشمولة الي بالحماية؛
- المسؤولية الجنائية للأشخاص المعنوية، وكذلك الاهتمام بالإجراءات الجنائية لاسيما في مرحلة التحقيق والملاحقة القضائية مثل التحفظ على الأدلة والتفتيش والضبط وما إلى ذلك وقد حملت هذه الاتفاقية الطابع التوجيهي للخطوات، التي يلزم اتخاذها في إطار التشريع الوطني في كل دولة فيما يتعلق بالأحكام الموضوعية والإجرائية كما أشرنا أعلاه. وألزمت الدول الأعضاء بمراعاة حقوق الإنسان وحرياته الأساسية، التي تضمنتها الاتفاقيات الدولية والتشريعات الوطنية على حد سواء والالتزام بعدم انتهاكها، مع إمكانية الدول الأخرى غير الأعضاء في الاتفاقية الاستعانة بهذه الاتفاقية، عند إعداد التشريعات الوطنية باعتبارها مصدر تاريخي في مجال مكافحة الجريمة على الانترنت.

كما تضمنت الاتفاقية جانب آخر من التعاون انصب هذه المرة حول تدريب أعوان الأمن لإكسابهم خبرات عملية كما ورد في التوصية الصادرة عن اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجرائم السيبرانية، وتعد الولايات المتحدة الأمريكية، من الدول المتطورة تقنيا في مجال مكافحة الجرائم المعلوماتية والشبكات، وهي تساعد على تدريب أجهزة الشرطة و قضاة الدول الأخرى، بتمكينها من تعزيز قدراتها على ضبط مشاكل هذه الجرائم، قبل أن تفلت منها زمام الأمور فقد أوجدت وزارة العدل الأمريكية مكتب للمساعدة و التدريب لتطوير أجهزة

الادعاء العام في الدول الأخرى، و يعمل إلى جانبه البرنامج الدولي للمساعدة و التدريب (ICITAP) لتوفير المساعدات لأجهزة الشرطة بالدول النامية (درار، 2017، صفحة 278)

الفرع الثالث: إتفاقية الجامعة العربية لمكافحة الجريمة السيبرانية

صدر عن جامعة الدول العربية قانونا استرشاديا لمكافحة جرائم تقنية الفضاء السيبراني سعت الدول العربية لتقنين وتجريم الأعمال الغير مشروعة المرتكبة من خلال استخدام الفضاء السيبراني بالتوقيع على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010/12/21 لتعزيز التعاون بين الدول العربية لمكافحة الجرائم السيبرانية والحفاظ على أمنها وسلامة مجتمعاتها.

ودعا المجلس، الدول العربية المصدقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى موافاة الأمانة الفنية للمجلس باتخاذه من إجراءات المواءمة تشريعاتها مع أحكام الاتفاقية وتجريم الصور المستحدثة من الجرائم الإلكترونية لمنع الإرهابيين من استخدام الإنترنت وتعزيز التعاون مع المنظمات الدولية والإقليمية المعنية بمواجهة كافة أشكال جرائم الإرهاب الإلكترونية.

كما دعا المجلس، الدول العربية إلى التعاون لمنع الإرهابيين من استغلال تكنولوجيا المعلومات والاتصالات والإنترنت للتحريض على دعم أعمالهم الإرهابية وتمويل أنشطتهم والتخطيط والإعداد لها، وأكد المجلس على أهمية تعزيز التعاون مع المنظمات والوكالات الدولية المتخصصة للحصول على المساعدات المطلوبة في بناء القدرات اللازمة لمواجهة خطر استخدام الإرهابيين لأسلحة الدمار الشامل أو مكوناتها، ودعم أمن المطارات والموانئ والحدود. (أميرة عبدالعظيم ، 2020، صفحة 499) بالرغم من كل هذه الجهود الدولية سواء على مستوى الأمم المتحدة والمنظمات الدولية وعلى المستوى الإقليمي وخاصة إتفاقية بودابست التي تعتبر بمثابة دعوة للدول لإعادة النظر في تشريعاتها الداخلية والدعوة إلى التعاون الدولي لأجل مكافحة الجرائم السيبرانية التي لا تعرف الحدود الجغرافية. إلا هناك صعوبات تواجه هذه الجهود، سنتطرف إلى هذه الصعوبات وكيفية القضاء عليها في هذا المطلب.

المطلب الثالث: الصعوبات التي تواجه الجهود الدولية كيفية القضاء عليها

رغم الجهود التي تبذلها المنظمات والهيئات الدولية في مكافحة الجرائم السيبرانية إلا هناك عوائق وصعوبات تقف في كعارض في نفاذ هذه الاتفاقيات الدولية والإقليمية سوف نتطرق لها في هذا المطلب ونتناول كيفية القضاء عليها.

الفرع الأول: الصعوبات التي تواجه الجهود الدولية

نادى البعض بضرورة انشآ وحدات خاصة بمكافحة الجريمة المعلوماتية أسوة بجهات البحث الجنائي الوطنية والدولية(الانتربول)، وذلك لإثبات الجريمة عند وقوعها وتحديد أدلتها وفاعليها مما يعني إيجاد صيغة ملائمة للتعاون الدولي لمكافحة جرائم الاعتداء على المعلومات الخاصة وتبادل الخبرات والمعلومات حول هذا النوع من الجرائم ومرتكبيها وسبل مكافحتها، ورغم المناداة بضرورة التعاون الدولي في مكافحة الجريمة المعلوماتية، إلا أن هناك عوائق تحول دون ذلك بل وتجعل من هذا التعاون صعبا، ويمكن إيجاز ذلك في الأسباب التالية:

أولا: عدم وجود نموذج واحد متفق عليه فيما يتعلق بالنشاط الإجرامي، بسبب أن الأنظمة القانونية في بلدان العالم لم تتفق على صور محددة يندرج ضمنها ما يسمى: بإساءة استخدام نظم المعلومات الواجب إتباعها، كما انه لا يوجد تعريف محدد للنشاط المفروض أن يتفق على تجريمه وهذا راجع إلى قصور التشريع ذاته في كافة بلدان العالم وعدم مسايرته لسرعة التقدم المعلوماتي ومن ثم الجريمة المعلوماتية.

وما تجدر الإشارة إليه أن العديد من الدول العربية لم تصدر قانونا يتعلق بالجريمة المعلوماتية سواء ارتكبت عن طريق الكمبيوتر أو عن طريق الانترنت، ولا يزال الخلاف قائما حول أفضلية تعديل التشريعات العقابية لكي تستوعب نماذج الجريمة المعلوماتية أم أنه تعدل قوانين حماية الملكية الفكرية كي تستوعب هذه الأنشطة من السلوك ويتم تجريمها، أم من الأفضل إصدار تشريعات جديدة خاصة بالجريمة المعلوماتية، حتى أن الأمر لا يتوقف هنا بل يتعداه، حيث أن عدم اتفاق الأنظمة القانونية المختلفة على صورة موحدة للسلوك الإجرامي في الجريمة المعلوماتية يغري قراصنة الحاسب الآلي على تنظيم أنفسهم وارتكاب جرائمهم دون التقيد بالحدود الجغرافية الأمر الذي يؤكد حتمية التعاون الدولي لمكافحة هذه الجريمة.

ثانيا: عدم وجود معاهدات ثنائية أو جماعية بين الدول على نحو يسمح بالتعاون المثمر في مجال هذه الجرام وحتى في حالة وجودها فان هذه المعاهدات تبقى قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم وبرامج الحاسب الآلي وشبكة الانترنت، ومن ثم تطور الجريمة المعلوماتية بذات السرعة على نحو يؤدي إلى إرباك المشرع وسلطات امن الدول، ويظهر الأثر السلبي في التعاون الدولي وهو ما حاولت الأمم المتحدة الاهتمام به وكذلك بعض البلدان الأوروبية (شرابسة، 2009، صفحة 250)

ثالثا: عدم وجود تنسيق فيما يتعلق بالإجراءات الجنائية المتبعة المتعلقة بالجريمة المعلوماتية بين الدول المختلفة خاصة فيما يتعلق بالتحقيق والحصول على الأدلة لا سيما وأن الحصول على دليل في مثل هذه الجرائم خارج نطاق حدود الدولة عن طريق الضبط أو التفتيش في نظام معلوماتي معين أمر في غاية الصعوبة فضلا عن صعوبة الحصول على الدليل ذاته.

رابعا: إشكالية الاختصاص في الجرائم الالكترونية كونها تعد من المشكلات التي تعرقل الحصول على الدليل فيها خاصة وأنها من أكثر الجرائم التي تثير مسألة الاختصاص على المستوى المحلي والدول بسبب التداخل والترابط بين شبكات المعلومات، لأن الجريمة قد تقع في مكان معين وتنتج آثارها في مكان آخر.

وما يلاحظ أن جل التشريعات الجنائية المطبقة حاليا في معظم دول العالم ترتكز على الصفة الإقليمية فيما يتعلق بتطبيق قواعد الإجراءات الجنائية عن طريق السلطات غير الوطنية لذلك لا مناص من الاتفاقيات الثنائية والجماعية بين الدول لتسهيل تحقيق جرائم المعلوماتية و رغم إبرام بعض الاتفاقيات إلا أنها لم تف بالغرض في حل مشكلات الاختصاص وتبادل الأدلة الجنائية وتسليم المجرمين، لذلك تبقى الحاجة جد ماسة إلى تشريعات جنائية أكثر مرونة حتى تواكب سرعة التقدم لتكنولوجي و عصر المعلوماتية إن إجراءات التحقيق في بيئة تكنولوجيا المعلومات وفقا لما جاء في توصية المجلس الأوروبي رقم (13/95)تقتضي التدخل السريع لمد الإجراءات إلى أنظمة كمبيوتر قد تكون موجودة خارج الدولة، وحتى لا يمثل هذا الأمر اعتداء على سيادة دولة معينة أو على أحكام القانون الدولي يجب وضع قاعدة قانونية صريحة تسمح بهذا الإجراء (شرابسة، 2009، صفحة 251)

الفرع الثاني: كيفية القضاء على الصعوبات التي تواجه الجهود الدولية في مكافحة جرائم السبرانية

أولا: حل العقبة المتعلقة بالمساعدات القضائية الدولية:

1-تبادل المعلومات: وهو يشمل تقديم المعلومات والبيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية وهي بصدد النظر في جريمة ما، عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم.

2- نقل الإجراءات: ويقصد به قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ إجراءات جنائية وهي بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى ما توافرت شروط معينة.

ثانيا: حل عقبة عدم وجود نموذج موحد للنشاط الإجرامي:

يتم حل هذه العقبة بتوحيد النظم القانونية. وتخفف من غلو الفوارق بين الأنظمة العقابية الداخلة، وذلك من خلال في تحديث التشريعات المحلية المعنية بالجرائم المعلوماتية وإبرام اتفاقيات خاصة يراعي فيها هذا النوع من الجرائم.

ثالثا: حل عقبة تنوع واختلاف النظم القانونية الإجرائية.

بالنسبة لمعوقة الخاصة بتنوع واختلاف النظم القانونية الإجرائية نجد أن الصكوك الدولية الصادرة عن الأمم المتحدة غالبا ما تشجع الأطراف فيها على السماح باستخدام بعض تقنيات التحقيق الخاصة الشيء الذي يخفف من غلو واختلافي النظم القانونية والإجرائية، ويفتح المجال أمام تعاون دولي فعال، فمثلا المادة20 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية تشير في هذا الصدد إلى التسليم المراقبة والمراقبة الإلكترونية وغيرها من أشكال المراقبة والعمليات المستترة (نصيرات وائل ، 2015، صفحة 134)

التي تعتبر من أهم التقنيات المستخدمة في التصدي للجماعات الإجرامية المنظمة المحنكة بسب الأخطار والصعوبات الكامنة وراء محاولة الوصول إلى النطاق المكاني لذلك الطرف الأخر، والتي ينوي الطرف طالب المساعدة أن يقدم طلبا للمساعدة بشأنها بغرض القيام بالتفتيش أو الكشف عن البيانات المشار إليها، كما أشارت المادة 31 إلى المساعدة المتعلقة بالدخول إلى البيانات المحفوظة، حيث أجازت لأي طرف أن يطلب من أي طرف آخر أن يقوم بالتفتيش أو أن يدخل بأي طريقة مشابكة وأن يضبط أو يحصل بطريقة مماثل وأن يكشف عن البيانات المحفوظة بواسطة شبكة المعلومات أيضا نصت المادة 33 على تعاون الدول الأطراف فيما بينها لجمع البيانات في الوقت الحقيقي عن التجارة غير المشروعة، ونلاحظ مما سبق أن الاتفاقية الأوربية الإجرام المعلوماتي أوجدت بعض الحلول التي من شأنها التغلب على مشكلة اختلاف النظم الإجرائية أمام التعاون الدولي لمواجهة الجرائم المتعلقة بشبكة الإنترنت.

رابعا: حل عقبة عدم وجود قنوات اتصال.

للحد من ظاهرة عدم وجود قنوات اتصال بين جهات إنفاذ القانون فنلاحظ أنه غالبا ما تشجع الصكوك الدولية الدول إلى التعاون فيما بينها و تدعوها إلى إنشاء قنوات اتصال بين سلطاتها المختصة ووكالاتها ودوائرها المتخصصة بغية التيسير في الحصول علي هذه المعلومات وتبادلها، ومن الأمثلة على هذه الصكوك الدولية اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة

عبر الوطنية والاتفاقية الأوربية التي أوجبت على الدول الأطراف فيها ضرورة تحديد نقطة اتصال تعمل لمدة 24 (نصيرات وائل ، 2015، صفحة 135)

خاتمة:

إن الجريمة السيبرانية باعتبارها من الجرائم المعلوماتية المعاصرة، التي واكبت عصر التقدم التكنولوجي خصوصا بعد ظهور شبكة المعلومات الدولية "انترنت"، بسبب التقدم العلمي الحاصل ساعد على انتشار و تنوع هذا السلوك الإجرامي و الذي أصبح يهدد الإنسان في مختلف المجالات لا سيما الاقتصادية والاجتماعية والثقافية، والأخلاقية وحتى المعتقدات الدينية لذلك وأمام الانتشار الواسع لهذا النمط الإجرامي الجد متطور والذي تستخدم فيه أحدث التقنيات التكنولوجية العالية والمتطورة وسرعة وحيلة وبداهة مرتكبيها التي تجعلهم دائما يفلتون من العقاب في ظل غياب الدليل المادي للجريمة إضافة إلى غياب منظومة تشريعية وطنية تحدد الفعل، تجرمه، ثم تحدد العقوبة المناسبة لمرتكبه انعكس ذلك سلبا على المستوى الدولي، فعلى الرغم من وجود العديد من الاتفاقيات الدولية المتعلقة بالجريمة الالكترونية التي سبق التطرق إليها إلا أنها تبقى غير كافية في غياب تظافر للجهود الدولية والتي تسعى في مجملها إلى اتخاذ التدابير اللازمة للحد من هذه الجرائم بالنظر إلى الطبيعة الخاصة لها كونها من الجرائم الدولية العابرة للحدود .

ويمكن التوصل إلى مجموعة من الاقتراحات التالية:

- العمل على إبرام اتفاقيات دولية ثنائية ومتعددة الأطراف لاحتواء الجريمة والتخفيف منها؛
- دعم وتطوير نظم التعاون الدولي في مجال مكافحة الإجرام السيبراني؛
- يجب على جميع الدول أن تسعى إلى تعديل قوانينها الداخلية وجعلها تواكب التطور العلمي والتكنولوجي؛
- ضرورة تفعيل نظم الحماية والدفاع الفعال لمنظومة المعلومات، والسيطرة والتحكم في تكنولوجيات الإعلام والإتصال.

قائمة المراجع:

عبدالإله النوايسة. (2017). جرائم تكنولوجيا المعلومات-شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية. الأردن: دار وائل للنشر والتوزيع، المجلد الأولى ،عمان.

محمود أحمد عبابنة. (2009). جرائم الحاسوب وأبعادها الدولية. الأردن: دار الثقافة للنشر والتوزيع،الإصدار الثاني، المجلد الأولى، عمان.

الصحفي روان بنت عطية الله. (2020). الجرائم السيبرانية. المجلة الإلكترونية الشاملة متعددة لإختصاصات، العدد24، 1-53.

أم يوسف أمنة. (17 01, 2021). فوائد الأمن السيبراني. تاريخ الاسترداد 10 11, 2021، من جريدة الطاسيلي: https://altassili.com

عسيري ,ف .(2002) .الامن السيبراني وحماية المعلومات-تقنية المعلومات .المملكة العربية السعودية.

بنت نبي ياسمين بلعسل ، و الحسين عمروش. (2021). التهديدات الإلكترونية والأمن السيبراني في الوطن العربي. مجلة نوميروس الاكاديمية، المجلد02، العدد02.

جبور منى الأشقر. (2016). السيبرانية هاجس العصر. جامعة الدول العربية، بيروت، لبنان: المجلد 1،المركز العربي للبحوث القانونية والقضائية.

سمير بارة. (2017). الامن السيبراني في الجزائر السياسات والمؤسسات. المجلة الجزائرية للآمن الإنساني، العدد04، 255-280.

شيخه حسين الزهراني. (2020). التعاون الدولي في مواجهة الهجوم السيبراني. مجلة جامعة الشارقة للعلوم القانونية، المجلد17، العدد01.

عبدالفتاح حجازي. (2007). مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت. مصر: دار الكتب القانونية، المحلة الكبرى،الطبعة الأولى.

عطية إدريس. (2019). مكانة الأمن السيبراني في منظومة الامن الوطني الجزائري. مجلة مصداقية، المجلد01، العدد01، 100-121.

ليندا شرابسة. (2009). السياسة الدولية و الإقليمية في مجال مكافحة الجريمة الالكترونية. مجلة دراسات وأبحاث، المجلد01، العدد01 241-253

محمد عبد الجواد أميرة عبدالعظيم. (2020). المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام. مجلة الشريعة والقانون، الجزء03، العدد35، 361-541.

محمد عبدالرحمان نصيرات وائل. (2015). الجهود الدولية في مكافحة الجرائم المعلوماتية والصعوبات التي تواجها. المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية-ICACC. جامعة الإمام محمد بن سعود الإسلامية المملكة العربية السعودية.

مراد مشوش. (2019). الجهود الدولية لمكافحة الاجرام السيبراني. مجلَّة الواحات للبحوث والدراسات، المجلد12، العدد703،01-726.

نسيمة درار. (2017). الامن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني دراسة مقارنة. أطروحة دكتوراه. جامعة أبي بكر بلقايد تلمسان-الجزائر، كلية الحقوق والعلوم السياسية.

Alex, K. (2015). Routine Activity Theory and the Determinants of High Cybercrime Countries. Social Science Computer Review.
AL_khafagy, B. (2020). NTERNATIONAL EFFORTS TO COMBAT CYBERCRIME. palarch's journal of archeology of egypt.