مقدمة 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 أيضًا التعرض للجرائم السيبرانية، إذ أصبح الفضاء السيبراني عرضة للانتهاكات من قبل مخترقي الشبكات سواء أكانوا دول أو غيرها مما يملكون هذه التقنيات المعلوماتية، فتوجهت الأنظار إلى الاهتمام وبشدة إلى الأمن السيبراني، [1] لذا أصبح أمن الفضاء السيبراني يدخل ضمن أولويات للعديد من الدول، ودفعت التهديدات المتزايدة الأمن 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 [1] لمواجهة تهديدات أمن الفضاء السيبراني، والعمل على استجابة القانون الدولي ملا 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 الأوروبي مبادرة للأمن السيبراني، فأصبحنا الآن أمام جرائم حقيقية متكاملة تتم عن طريق شبكات الإنترنت، 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، وتهديد 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. [1]

أهداف الدراسة: ـ2التعرف على الجهود المبذولة في مواجهة الجرائم السيبرانية. منهج الدراسة: كون هذه الدراسة تتناول الأمن السيبراني والجريمة السيبرانية والجهود الدولية في مكافحة الجرائم السيبرانية والصعوبات التي تواجهها 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 الأمن السيبراني والجريمة السيبرانية؟ ما هي الجهود المبذولة في مواجهة الجرائم السيبرانية؟ وما الصعوبات التي تواجه الجهود الدولية في القضاء على الجرائم السيبرانية؟ في هذا الفصل سوف نتطرق إلى تعريف الأمن السيبراني وأهدافه وإلى مفهوم الجريمة السيبرانية كما سنحاول إعطائها خصائص تتميز بها عن غيرها من الجرائم التقليدية، المطلب الأول: مفهوم الأمن السيبراني وأهدافه وأبعاده: 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 الأمن السيبراني وأهدافه أولًا: تعريف الأمن السيبراني: ويمكن أن نقارب هذا المفهوم من عدة زوايا: وهي مأخوذة من كلمة (سيبر) وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي، فالسيبرانية تعني (فضاء الإنترنت)، وكان يقصد بها قيادة ربان السفينة. 1948 ومن أجل وصف نظام التغذية الرجعية الاستفادة من مخرجات الأنظمة في ضبط مدخلاتها وفي التحكم فيها واستقرار أدائها [1] 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. [1] إن الأمن السيبراني عدة تعاريف لكنها تصب كلها في مفهوم واحد وهو توفير الحماية السيبرانية بهدف توافر واستمرارية عمل نظم المعلومات واتخاذ التدابير اللازمة لحماية الأفراد والدول من المخاطر السيبرانية، ونعرف ذلك من خلال الأهداف التي أنشأ لأجلها.

ثانيا: أهداف الأمن السيبراني: ومن أهم ما يدور في هذه التخصص والذي يقدمه هو: ـ تأمين البنى التحتية ألمن المعلومات والبيانات الخاصة بالمواطنين، وكذلك جميع أجهزتها ومواردنا الحياتية سواء من ممتلكات إلكترونية من أي محاولة عبث أو

اختراق أو تدمير وتوفير الحماية اللازمة. ـ 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. ـ 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. ـ تشفير التعاملات الإلكترونية بحيث لا يستطيع أي مخترق أو مهاجم أو عابث أن يدخل بسهوله لهذه البيانات والتطبيقات لأن التشفير أحد أساليب الحماية والتي يصعب فك رموزها ألنها تمس أمور حياتنا وتمس أمننا الإلكتروني.

[1] الفرع الثاني: أهمية الأمن السيبراني وابعاده أولًا: أبعاد الأمن السيبراني: ـ1البعد العسكري: لتنتقل فيما بعد إلى الأوساط العلمية والأكاديمية، تمثلت في أبحاث تخدم القدرات العسكرية وتطورها، والإنجازات العلمية التي تسهم في تفوق بلد على آخر، نذكر منها مثال ما حصل في جورجيا واستونيا وكوريا الجنوبية وإيران كمثال على بعض الهجمات والاختراقات التي ترجمت ماديا سواء باندلاع صراع مسلح الحق، كذلك الذي وقع بين روسيا وجورجيا أو بانقطاع الاتصال بالإنترنت في استونيا، بين الدولة والمواطنين، والتشويش على الإدارات الحكومية . الكهربائية، والمياه، والاتصالات السلكية واللاسلكية والخدمات الصحية، ومن ثم تدمير قواعد البيانات وما يلحقه من مخاطر. [1] ـ2البعد الاقتصادي: أصبح الفضاء الإلكتروني جاذبا لقطاعات المجتمع كافة، 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 محورًا رئيسيا للتطور الاقتصادي في القرن الحادي والعشرين، وهو ما أثار الحديث عن أهمية تحقيق الأمن السيبراني في المجال الاقتصادي. [1] ـ3 البعد الاجتماعي : تساهم شبكات التواصل الاجتماعي بشكل خاص في فتح المجال للأفراد للتعبير عن تطلعاتهم السياسية وطموحاتهم الاجتماعية بأشكالها المختلفة، [1] 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 الإلكترونية والحق في إنشاء التجمعات على الإنترنت والحق في حماية ملكية البرامج المعلوماتية. ـ5البعد السياسي: هناك أمثلة كثيرة تدفع نحو الاهتمام بالبعد السياس ي لألمن السيبراني، كالتسريبات المختلفة للوثائق الحساسة التي تؤدي إلى مشكلات كبيرة جدًا على المستوى الخارجي والدولي، تظاهرات افتراضية، حركات احتجاجية إلكترونية، كما يتم استغلال هذه المواقع من طرف العديد من الحكومات لتمرير سياساتها. 1] ثانيا: أهمية الأمن 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. 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، 1]، 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؟ وما هي أنواعها؟ نتعرف عليها 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، الفريق الثاني: نظرت إلى محل الجريمة باعتباره أساسًا لتعريف هذه النوعية من الجرائم، ومن ثم عرفت الجريمة المعلوماتية بأنها: "كل عمل غير قانوني أو كل سلوك غير مشروع يستخدم فيه الحاسب كأداة أو

موضوع للجريمة أو هيكل 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 المعلومات ي، 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 ال يتيح للعديد من الأفعال السيبرانية الإفلات من دائرة العقاب، ولعلنا نؤيد هذا التعريف نظرا لشموله لجميع أشكاله الجرائم السيبرانية. (العظيم. الفرع الثاني: أنواع الجريمة السيبرانية: تتنوع الممارسات التي تهدد الأمن السيبراني،