مجلــة

جامعة

الملك خالد

للعلوم الإنسانية

دورية علمية نصف سنوية ، محكمة

المجلد ٧، العـدد ٢

ربيع الثاني ١٤٤٢ هـ ديسمبر ٢٠٢٠م

مجلة جامعة الملك خالد

للعلوم الإنسانية

المـجـلد السابع ـ العدد الثاني ربيـع الثاني١٤٤٢ هـ ديـسمبر ٢٠٢٠

مجلة علمية، نصف سنوية، مُحكمة

المراسلات:

توجه جميع المراسلات إلى رئيس هيئة التحرير على العنوان التالي:
مجلة جامعة الملك خالد للعلوم الإنسانية

الرمزالبريدي: ٦١٤١٣ صندوق البريد ٩١٠٠، المملكة العربية السعودية

البريد الإلكتروني: humanities@kku.edu.sa

إخلاء مسؤوليـة

المواد العلمية المنشورة في المجلة تعبر عن آراء أصحابها ولا تنسب إلى الرعاة أو الناشر أو المحرر أو هيئة تحرير مجلة جامعة الملك خالد للعلوم الإنسانية.

رقم إيداع ١٤٣٥/٣٠٧٦ بتاريخ ١٤٣٥/٣/١٢هـ
الرقم الدولي المعياري (ردمد) ٦٧٢٧-١٦٥٨

أعضاء هيئة التحرير

م	الاسم	الصفة
١	أ.د. عبد العزيز إبراهيم يوسف فقيه	رئيس التحرير
٢	أ.د. يحيي عبد الله الشريف	عضو هيئة التحرير
٣	أ.د. مربع بن سعد آل هباش	عضو هيئة التحرير
٤	أ.د. عوض بن عبد الله القرني	عضو هيئة التحرير
٥	أ.د. أحمد بن يحي آل فايع	عضو هيئة التحرير
٦	أ.د. عبد اللطيف بن إبراهيم الحديثي	عضو هيئة التحرير
٧	أ.د. حسين بن محمد آل عبيد	عضو هيئة التحرير
٨	د. سلطانة بنت محمد الشهراني	عضو هيئة التحرير
٩	د. إسماعيل خليل الرفاعي	عضو هيئة التحرير ومدير التحرير
١٠	أ. تركي بن علي آل حميد	سكرتير المجلة

أعضاء الهيئة الاستشارية

م	الاسم	الجهة
١	أ. د. إبراهيم الجبري	جامعة الملك فهد للبترول والمعادن
٢	أ. د. أحمد عبد العزيز الحليبي	جامعة الملك فيصل
٣	أ. د. أمين بلمكي	جامعة بكر بلقايد
٤	أ. د. حسام بن عبدالمحسن العنقري	جامعة الملك سعود
٥	أ. د. خوزيه راباسا	جامعة هارفارد
٦	أ. د. دوج آرنولد	جامعة إسيكس
٧	أ. د. سعد البازعي	جامعة الملك سعود
٨	د. محمد أمين مخيمر	جامعة بني سويف
٩	أ. د. صالح بن سعيد الزهراني	جامعة أم القرى
١٠	أ. د. صالح زياد الغامدي	جامعة الملك سعود
١١	أ. د. صالح معيض	جامعة الملك سعود
١٢	أ. د. فواز عبد الحق	جامعة اليرموك
١٣	أ. د. محمد عباس	جامعة الملك خالد
١٤	أ. د. محمد مرسي الحارثي	جامعة أم القرى
١٥	أ. د. منى بيكر	جامعة مانشستر
١٦	أ. د. جلن استكويل	جامعة ويسيدا اليابان

مجلة جامعة الملك خالد للعلوم الإنسانية

مجلة جامعة الملك خالد للعلوم الإنسانية دورية علمية متخصصة في العلوم الإنسانية، محكمة في آلية قبول البحوث القابلة للنشر بها، وتهدف إلى نشر الإنتاج العلمي للباحثين في تخصصات العلوم الإنسانية، وتعنى بالبحوث الأصيلة التي لم يسبق نشرها باللغتين العربية والإنجليزية والتي تتسم بالمصداقية وإتباع المنهجية العلمية السليمة.

أهداف المجلة

١. الإسهام في إبراز دور الحضارة الإسلامية في إثراء العلوم الإنسانية.
٢. نشر البحوث العلمية المحكمة في مجال العلوم الإنسانية بفروعها المختلفة.
٣. الإضافة إلى مركوم المعرفة في الدراسات الإنسانية.
٤. إبراز جهود الباحثين في الدراسات والبحوث العلمية ذات الصلة بموضوعات الإنسانيات.

شروط النشر

١. يجب أن يتصف البحث بالأصالة والابتكار والجدة واتباع المنهجية العلمية الملائمة وصحة اللغة وسلامة الأسلوب.
٢. أن لا يكون قد سبق نشره أو قدم للنشر في مكان آخر، ويتعد الباحث كتابةً أن لا يكون البحث قد سبق نشره أو قد قدم للنشر مزامنة مع تقديمه للنشر في مجلتنا إلى مجلة أخرى حتى يتم اتخاذ القرار المناسب في هذا الشأن.
٣. ألا يكون البحث جزءاً من كتاب منشور أو مستلاً من رسالة علمية.
٤. أن لا يزيد عدد صفحات البحث عن ٤٠ صفحة.
٥. تخضع جميع البحوث المقدمة للنشر في المجلة للتحكيم بعد اجتيازها مرحلة الجرد الداخلي.
٦. لا يجوز نشر البحث أو أجزاء منه في مكان آخر بعد إقرار نشره في مجلة جامعة الملك خالد للعلوم الإنسانية إلا بعد الحصول على إذن كتابي بذلك من رئيس التحرير.
٧. موافقة المؤلف على نقل حقوق النشر كافة إلى المجلة، وإذا رغبت المجلة في إعادة نشر البحث فإن عليها أن تحصل على موافقة مكتوبة من صاحبه.
٨. يمنح المؤلف نسخة واحدة من العدد المنشور فيه بحثه، وجميع أصول البحث التي تصل إلى المجلة لا تردّ سواء نشرت أم لم تنشر.

متطلبات النشر وتعليماته

١. تصنف المواد التي تقبلها المجلة للنشر وفق ما يأتي:

البحث أو الدراسة: من عمل المؤلف في مجال تخصصه، ويجب أن يكون أصيلاً، وأن يضيف جديداً للمعرفة.

المقالة: وتتناول العرض النقدي والتحليلي للبحوث والكتب ونحوها التي سبق نشرها في ميدان معين من ميادين الدراسات الإنسانية.

منبر الرأي: رسائل القراء إلى المحرر والردود والملحوظات التي ترد إلى المجلة.

٢. بالنسبة للبحوث والدراسات، تنشر المجلة البحوث الآتية فقط:

أولا: البحوث الميدانية (الامبريقية): يورد الباحث مقدمة يبين فيها طبيعة البحث ومبرراته ومدى الحاجة إليه، ثم يحدد مشكلة البحث، ثم يعرض طريقة البحث وأدواته، وكيفية تحليل بياناته، ثم يعرض نتائج البحث ومناقشتها والتوصيات المنبثقة عنها، وأخيراً يثبت قائمة المراجع.

ثانياً: البحوث النوعية التحليلية: يورد الباحث مقدمة يمهد فيها لمشكلة البحث وأسئلته مبيناً فيها أهميته وقيمته في الإضفاء إلى العلوم والمعارف وإغنائها بالجديد، ثم يقسم العرض بعد ذلك إلى أقسام متسلسلة ومترابطة على درجة من الاستقلال فيما بينها، بحيث يعرض في كل منها فكرة مستقلة ضمن إطار الموضوع الكلي ترتبط بما سبقها وتمهد لما يليها، ثم يختم الموضوع بخلاصة شاملة وتوجيهات، وأخيرا يثبت قائمة بالمراجع.

٣. أن يحتوي البحث على: عنوان البحث باللغتين العربية والانجليزية وملخص باللغتين العربية والإنجليزية في صفحة واحدة بحدود (١٥٠) كلمة لكل ملخص، وأن يتضمن البحث كلمات دالة على التخصص الدقيق للبحث باللغتين وسيرة ذاتية مختصرة للباحث أو الباحثين.

٤. تقدم البحوث مطبوعة بخط (Simplified Arabic) حجم (١٤) للنصوص في المتن، ويكتب البحث على وجه واحد، مع ترك مسافة ١.٥ بين السطور.

٥. إن سياسة المجلة تستوجب (بقدر الإمكان) أن يتكون البحث من الأجزاء التالية (للبحوث الامبريقية - الميدانية): مقدمة الدراسة، مشكلة الدراسة، وأهدافها وأسئلتها/ أو فرضياتها، أهمية الدراسة، محددات الدراسة، التعريفات بالمصطلحات، إجراءات الدراسة، وتتضمن: المجتمع والعينة، أداة الدراسة، صدق وثبات الأداة، المنهج المتبع في الدراسة، ثم عرض النتائج، ومناقشتها، وأخيراً الاستنتاجات والتوصيات.

٦. يراعى في أسلوب توثيق المراجع داخل النص وفق نظام جمعية علم النفس الأمريكية (APA).

معلومات الاتصـــال

ينبغي توجيه جميع المراسلات إلى رئيس تحرير مجلة جامعة الملك خالد للعلوم الإنسانية على العنوان التالي:

مجلة جامعة الملك خالد للعلوم الإنسانية

الرمز البريدي ٦١٤١٣

صندوق البريد ٩١٠٠

البريد الإلكتروني: humanities@kku.edu.sa

المحتويات

مجلة جامعة الملك خالد للعلوم الإنسانية
المجلد ٧ العدد ٢
٢٠٢٠

King Khalid University Journal of Humanities, Volume 7 , Issue 2, 2020
https://hj.kku.edu.sa

الدور القانوني للأمن السيبراني في مكافحة الجريمة

د. هدى بنت أحمد البراك(*)

جامعة المجمعة

الملخص

عالم اليوم أضحى بكل أساليبه، وأنماطه وتفاصيله مرتبطاً ارتباطاً وثيقا بالشبكة العنكبوتية، وبأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية وارتبطت فيه أغلب الأنشطة الحياتية الأساسية. يواجه العالم أخطر المشاكل التي تتمثل في الجرائم السيبرانية حيث أثرت هذه المشاكل على حياة ونشاط الإنسان لذا تنبهت الدول إليها ودعت المنظمات الدولية إلى عقد العديد من المؤتمرات وإبرام اتفاقيات من أجل مكافحة هذه الجرائم والحد منها، لذلك تعتمد مشكلة الدراسة على تسليط الضوء على الأمن السيبراني والبعد الأمني والمعلوماتي والاقتصادي بالفضاء السيبراني ودوره القانوني في مكافحة الجرائم السيبرانية وأثر الهجمات على مستوى العالم والتركيز على السعودية ومعرفة الدور القانوني لهيئة الأمن السيبراني في مكافحة الجرائم الالكترونية، وتكمن أهمية الدراسة في ضرورة التعاون الدولي لمكافحة الجرائم الالكترونية نظرياً وعملياً، حيث يعتبر من المواضيع التي ترتبط بشكل مباشر بمصالح الفرد وأمن الدولة، وتعتمد هذه الدراسة على المنهج الوصفي حيث تم الاعتماد على جمع المعلومات حول موضوع الدراسة خلال فترة زمنية معينة للوصول إلى النتائج المطلوبة.-

الكلمات المفتاحية: **السيبرانية، الأمن السيبراني، الموصولية والجريمة السيبرانية، الهيئة الوطنية للأمن السيبراني، الاتحاد السعودي للأمن السيبراني والبرمجة.**

(*) د. هدى بنت أحمد البراك، أستاذ القانون المشارك، قسم القانون كلية العلوم والدراسات والإنسانية، جامعة المجمعة.

مجلة جامعة الملك خالد للعلوم الإنسانية
المجلد ٧ العدد ٢
٢٠٢٠

King Khalid University Journal of Humanities, Volume 7 , Issue 2, 2020
https://hj.kku.edu.sa

The legal role of cybersecurity in combating crime

Dr. Huda Ahmed Albarrak (*)

Majmaah University

Abstract

Today's world has become, with all its methods, patterns and details, closely linked to the World Wide Web, IT systems and operational technology systems, and most basic life activities have been associated with it. The world is facing the most serious problems that are represented in cybercrime, as these problems have affected human life and activity, so countries have alerted them and international organizations have emerged to hold many conferences and conclude agreements to combat and reduce these crimes, so the problem of the study depends on highlighting cybersecurity and the dimension The security, information, and economic space in cyberspace and its legal role in combating cybercrimes. The necessity of international cooperation to combat cybercrime theoretically and practically, as it is considered one of the topics that are directly related to the interests of the individual and state security, and this study relies on the descriptive approach where it was relied on collecting information on the subject of the study during a specific time period to reach the required results.

Keywords: cyber security, cyber security, connectivity and cybercrime, the National Cyber Security Authority, the Saudi Cyber Security Federation and Programming

(*) Dr. Huda A. Albarrak, Associote professor of law, Law department, College of sciences and humanities, Majmaah University

المقدمة

لقد أدت نهاية الحرب الباردة إلى بروز العديد من التحديات والتهديدات التي لم يشهدها المجتمع الدولي من قبل، والتي تُعرف بالتهديدات العابرة للحدود التي لا تعترف لا بالحدود أو السيادة الوطنية أو فكرة الدولة القومية، الأمر الذي أدى الى تحولات في حقل الدراسات الأمنية والاستراتيجية وكذلك على مستوى الممارسة السياسية. ومع انفجار الثورة المعلوماتية ودخول العصر الرقمي خاصة في القرن الحادي والعشرون ما نتج عنه من تداعيات عديدة بسبب ظهور تهديدات وجرائم سيبرانية أصبحت تشكّل تحدياً كبيراً للأمن القومي وكذلك الدولي، لدرجة أن العديد من الباحثين اعتبر الفضاء السيبراني بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء، هو ما استدعى ضرورة وجود ضمانات وفي ظل التوجه الدولي نحو الحكومة الإلكترونية وعقب إصدار أمر من خادم الحرمين الشريفين يقضي بإنشاء هيئة باسم" الهيئة الوطنية للأمن السيبراني"، ترتبط بخادم الحرمين الشريفين والموافقة على تنظيمها، وتم إنشاؤها بأمر ملكي رقم ٦٨٠١ تاريخ ١٤٣٩/٢/١١ هـ، أصبحت قضية الأمن المعلوماتي السيبراني من التحديات الكبرى على الصعيدين الإقليمي والعالمي لا سميا مع تزايد التهديدات الأمنية الإلكترونية، والمملكة العربية السعودية سعت جاهدة لحماية منظوماتها المعلوماتية من خلال العديد من الأجهزة الأمن وعلى الرغم من الإيجابيات التي حملتها الإنترنت، إلا أنها حملت معها العديد من التهديدات والمخاطر التي لم تفرق بين الأشخاص والمؤسسات والدول، ناهيك عن التهديدات التي قد تطال أمن واستقرار الدولة، إذ لا ينكر أحد الدور المتعاظم لشبكة الإنترنت في الثورات العربية.

لذا فقد أصبح الأمن المعلوماتي السيبراني ركناً أساسياً ضمن المنظومة الأمنية المعاصرة، نظرًا للاستغلال المتنامي للشبكات الالكترونية لأهداف إجرامية والتي تؤثر سلبًا على سلامة البنى التحتية للمعلومات الوطنية الحساسة.

مشكلة الدراسة :

يعتبر انتشار التكنلوجيا تحدياً جديداً يواجه المجتمع، حيث بالرغم من إيجابياتها إلا أنها تسبب تهديداً خطيراً على سلامة المعلومات الشخصية الهامة للفرد، مما قد يسبب القلق لأصحاب المواقع الكبيرة عن كيفية حماية مواقعهم من خطر القرصنة وانتهاك الخصوصية، لذا كان لا بد من تسليط الضوء على الأمن السيبراني ودوره القانوني في مكافحة الجرائم الالكترونية، وهذا ما سيتم توضيحه في هذا البحث بإذن الله.

أهمية الدراسة:

تكمن أهمية هذه الدراسة في ضرورة التعاون الدولي لمكافحة الجرائم الالكترونية نظرياً وعملياً، حيث يعتبر من المواضيع التي ترتبط بشكل مباشر بمصالح الفرد ومصلحة أمن الدولة بشكل خاص.

تساؤلات الدراسة:

تتضمن كل دراسة عدة تساؤلات هامة يتم الإجابة عليها من خلالها، والتساؤل الرئيسي هنا هو:

ما هو الدور القانوني لهيئة الأمن السيبراني في مكافحة الجرائم الالكترونية؟

وهناك عدة تساؤلات فرعية أهمها:

١. ما المقصود بالسيبرانية والتعريفات المرتبطة بها؟
٢. ما هي التحديات والعوائق التي تواجه الأمن السيبراني في مكافحة الجرائم الالكترونية؟
٣. هل تم الاتفاق دولياً وإقليماً على تشريع للمكافحة الجريمة السيبرانية؟
٤. ما هو الهدف من إنشاء الهيئة الوطنية للأمن السيبراني؟
٥. ما هي أثر الهجمات السيبرانية على العالم والمملكة؟

منهج الدراسة:

تعتمد هذه الدراسة على المنهج الوصفي حيث تم الاعتماد على جمع المعلومات حول موضوع الدراسة خلال فترة زمنية معينة للوصول إلى النتائج المطلوبة.

تقسيم الدراسة :

المبحث الأول :حقيقة الأمن السيبراني .

المطلب الأول :ماهية السيبرانية.

المطلب الثاني :أهمية الأمن السيبراني وأبعاده.

المبحث الثاني :الدور القانوني في مكافحة الجريمة السيبرانية.

المطلب الأول :الدور القانوني للهيئات الدولية في مكافحة الجريمة السيبرانية.

المطلب الثاني :الدور القانوني في مكافحة الجريمة السيبرانية ببعض الدول العربية.

المبحث الأول

حقيقة الأمن السيبر اني

إن البحث في موضوع الأمن السيبراني يستلزم بالضرورة تحديد مختلف المفاهيم والمصطلحات الدالة عليه، ثم التطرق إلى التفرقة بين الأمن السيبراني وأمن المعلومات، حيث يعتبر الخطوة الأولى لتوضيح أهمية الأمن السيبراني، مروراً بالموصلية للجريمة السيبرانية والبعد الأمني والمعلوماتي والاقتصادي بالفضاء السيبراني انتهاءً بأثر الهجمات السيبرانية على العالم وبشكل خاص على المملكة.

المطلب الأول

ماهية السيبر انية

أولاً :الفضاء السيبر اني:

الفضاء السيبراني الوعاء الحاضن للسيبرانية وهو: "مجال عالمي داخل البيئة المعلوماتية يتكون من شبكة مستقلة من البنى التحتية لأنظمة المعلومات، ويتضمن ذلك الإنترنت وشبكات الاتصالات وأنظمة الحاسب والمعالجات المدمجة"(١).

في تعريف آخر: "استخدام الفضاء السيبراني للدفاع أو الهجوم على المعلومات وشبكات الحاسب الآلي وحرمان العدو من تنفيذ نفس المقدرات (٢).

تتفق جميع الدراسات العلمية على أن هذا الفضاء(٣)هو بيئة افتراضية تعتمد في بنيتها على التكنولوجية الحديثة في التعامل والتواصل بين العديد من الفواعل سواء كانوا أشخاص أو هيئات حكومية وغير حكومية من خلال شبكة إلكترونية (الحاسوب) لها استقلاليتها عن وسائل الاتصال، بمعنى أخر أن كل المعلومات والمعاملات المتداولة بقدر ما تسهل عملية الاندماج بين كل أجهزة الاتصالات والقمار الصناعية، والفضاء الإلكتروني، بقدر ما تفتح المجال لعمليات الاختراق (٤).

(١) المستشار :صالح بن علي بن عبدالرحمن الربيعة , الأمن الرقمي وحماية المستخدم من مخاطر الانترنت , هيئة الاتصالات وتقنية المعلومات)ص:8).

(٢) المرجع السابق.

(3) Le terme cybernétique (en anglais cybernetics), formé à partir du mot grec κυβερνήτης (kubernêtês) « pilote, gouverneur », Voir à ce sujet. Le site internet Wikipedia.

(٤) عادل عبد الصاد، " الفضاء الإلكتروني والرأي العام: تغير المجتمع والدوات والتأثير" ، المركز العربي لبحاث الفضاء الإلكترونى: قضايا استراتيجية،2013 ، العدد.2459.

ومن بين العلماء الذي يعتبره الباحثون بمثابة الأب الروحي والمؤسس لهذا الفضاء، عالم الرياضيات الأمريكي الاستاذ (NORBERT WIENER'S) الذي استطاع وضع تعريف دقيق لهذا الفضاء، " علم التحكم والتواصل عند الحيوان والآلة، لنقل الرسائل بين النسان والآلة، أو بين الآلة والآلة كما يعتبره علم القيادة أو التحكم في كل منهما[١] .وعرفته الوكالة الفرنسية لأمن أنظمة الإعلام (ANSSI)، وهي وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي، بأنه : "فضاء التواصل المشكّل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية" [٢].

فهو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكوّن من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين كما أن هناك مَن عرّف الفضاء السيبراني بوصفه الذراع الرابعة للجيوش الحديثة.

ثانياً :تعريف السيبرانية والأمن السيبراني

مع انفجار الثورة المعلوماتية ودخول العصر الرقمي خاصة في القرن العشرين وما نتج عنه من تداعيات عديدة بسبب ظهور تهديدات وجرائم سيبرانية أصبحت تشكّل تحدياً كبيراً للأمن القومي وكذلك الدولي، لدرجة أن العديد من الباحثين اعتبر الفضاء السيبراني بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء، وهو ما استدعى ضرورة وجود ضمانات أمنية ضمن هذه البيئة الرقمية، تبلورت بشكل أساسي في ظهور الأمن السيبراني cyber security كبُعد جديد ضمن أجندة حقل الدراسات الأمنية، وقد اكتسب اهتمامات العديد من الباحثين في هذا المجال.

ومن هنا تبرز الحاجة إلى ضرورة فهم ماهية الأمن السيبراني كمتغير جديد في العلاقات الدولية إضافةً إلى التعريفات المرتبطة به.

هناك عدة مفاهيم مرتبطة بالأمن السيبراني ارتباطاً لا يمكن تجزئته، سنستعرض بتعريفنا لبعض المصطلحات

مصطلح السيبرانية: والآن هو واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي، وتشير المقاربة

(1) Dans son livre « Cybernetics or control and communication in the Animal and the machine » .publié en 1947, il a proposé ce concept pour promouvoir une vision unifiée des domaines naissants de l'automatique, de l'électronique et de la théorie mathématique de l'information.

(٢) راجع:

Ebert Hannes and Maurer Tim . " Cyber Security" oxfordbibliographies , LAST MODIFIED: 11 JANUARY ,2017.

الإيتيمولوجية لكلمة "cyber " إلى أنها لفظة يونانية الأصل مشتقة من كلمة "kybernetes" بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازاً للمتحكم "governor" [١].

اصطلاحاً :هناك العديد من التعاريف التي قُدمت لمفهوم الأمن السيبراني، حيث يُعرّف بأنه" :مجموعة من الإجراءات المتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة"[٢].

عُرّف الأمن السيبراني بأنه" :مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر، وتدريبات وممارسات فضلى وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين"[٣].

وقدمت وزارة الدفاع الأمريكية "البنتاغون "تعريفاً دقيقاً لمصطلح الأمن السيبراني، فاعتبرته" :جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية، من مختلف الجرائم :الهجمات، التخريب، التجسس والحوادث"[٤]. في حين اعتبر الإعلانُ الأوروبي الأمنَ السيبراني أنه يعني" :قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات ."

يمكن القول إن الأمن السيبراني هو مجموعة الآليات والإجراءات والوسائل والأطر التي تهدف إلى حماية البرمجيات وأجهزة الكمبيوتر)الفضاء السيبراني بصفة عامة(، من مختلف لهجمات والاختراقات التهديدات السيبرانية التي قد تهدد الأمن القومي للدول.

(١) الفتلاوي أحمد عبيس نعمة" الهجمات السيبرانية :" مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر ."مجلة المحقق الحلي للعلوم القانونية والسياسية.

(٢) ايفانز فراهام، بوبلهام جيفري .قاموس بتغوين للعلاقات الدولية .ت :مركز الخليج للأبحاث الإمارات العربية المتحدة :مركز الخليج للأبحاث 2004.

(3) Lehto Mali Maithaanmak Pekka Cyber Scurity: Analytics, Techirvology and Automation, Switzerland: Springer International Publishing 2015.

(4) ValerianoBrandon and C. Maluess Ryan," international relations theory and Cyber Security threats conflicts and ethics in an Emerrent Domain in an emergen.

المطلب الثاني

أهمية الأمن السيبر اني و ابعاده

أولاً :أهمية الأمن السيبر اني

في عالمنا المترابط بواسطة الشبكة، يستفيد الجميع من برامج الدفاع السيبراني .فمثلاً على المستوى الفردي يمكن أن يؤدي هجوم الأمن السيبراني إلى سرقة الهوية أو محاولات الابتزاز أو فقدان البيانات المهمة مثل الصور العائلي كما تعتمد المجتمعات على البنية التحتية الحيوية مثل محطات الطاقة والمستشفيات وشركات الخدمات المالية لذا فإن تأمين هذه المنظمات وغيرها أمر ضروري للحفاظ على عمل مجتمعنا بطريقة آمنة وطبيعية.

إن أهمية الأمن السيبراني، يقوم في تامين المعلومات الحساسة البالغة لأهمية الدول الأفراد على حد سواء المعرضة للخطر والاختراق والاستيلاء كي تحافظ على الأمن الوطني وحفظ وحماية السرية والخصوصية للبيانات الشخصية للمواطنين .وتكمن الأخيرة كقضية ناشئة في حقل العلاقات الدولية من خلال حداثة هذا المجال، السياق العام لظهور الأمن السيبراني هذا المجال، فهناك تاريخ طويل من التخمينات حول دور التكنولوجيا الرقمية في الدراسات الأمنية .يستفيد الجميع أيضًا من عمل الباحثين في مجال الأمن السيبراني، فمثلاً يضم فريق تالوس ٢٥٠ باحثاً يحققون في التهديدات الجديدة والناشئة واستراتيجيات الهجوم السيبراني .فهم يكشفون عن نقاط الضعف الجديدة، ويثقفون الجمهور بشأن أهمية الأمن السيبراني، ويعملون على تقوية أدوات المصادر المفتوحة .مما يجعل العمل على الإنترنت أكثر أمانًا للجميع[1].

إن أهمية الأمن السيبراني يقوم في تامين المعلومات الحساسة البالغة لأهمية الدول الأفراد على حد سواء المعرضة للخطر والاختراق والاستيلاء كي تحافظ على الأمن الوطني وحفظ وحماية السرية والخصوصية للبيانات الشخصية للمواطنين.

ويظهر الدور القانوني للأمن السيبراني في ضمانه لاستمرارية توافر المعلومات في النظام المعلوماتي وأخذ جميع الاحتياطات لحماية المستهلكين من الأخطار المحتملة التي تعزز حماية وسرية البيانات الشخصية لهم .التصدي لأي محاولة ولوج غير مسموح به لأهداف غير سليمة إلى الأنظمة التشغيلية والسعي لتعزيز حماية مكوناتها من أجهزة وبرمجيات وما تقدمه من خدمات وما تحتويه من بيانات.

(1) www.cisco.com.

حماية مصالح المملكة العربية السعودية وأمنها الوطني والبنى التحتية الحساسة فيها، والتأسيس لصناعة وطنية في مجال الأمن السيبراني تحقق للمملكة الريادة في هذا المجال .كما يهدف الأمن السيبراني إلى مراعاة الأهمية الحيوية المتزايدة لتخصصها وتعزيز حماية الشبكات وأنظمة تقنية المعلومات بحيث تكون المرجع الوطني للمملكة في شؤون تخصصها.

ثانياً :الفرق بين الدور القانوني للأمن المعلوماتي والأمن السيبراني(١).

أمن المعلومات والأمن السيبراني مصطلحان متشابهان لكنهما ليسا متطابقين، فأمن المعلومات بالتعريف أعم وأشمل من الأمن السيبراني، ولكن هنا نخصص بالتركيز على مجال الأمن السيبراني كمجال من مجالات العلم، فمثلاً عمل الحاسوب وعلم التشفير بدايةً اشتقا من علم الرياضيات ثم بعد مرور الزمن حلقت هذه المجالات في فضاء العلم لتتوسع وتنتشر وتخرج خارج الإطار العلمي لمجال الأب .وهو الأمر ذاته لمجال الأمن السيبراني وأمن المعلومات . فمفهوم الأمن السيبراني أوسع من أمن المعلومات فإن تأمين البيانات والمعلومات التي تتداول عبر الشبكات الداخلية والخارجية والتي يتم تخزينها في خوادم داخل أو خارج المنظمات من الاختراقات، وهذا هو أحد أهم الأسباب وراء الأمر الملكي بإنشاء الهيئة الوطنية للأمن السيبراني.

ثالثاً :الموصولية والجريمة السيبرانية

كان عدد الموصولين بالإنترنت في عام 2011، لا يقل عن 2.3بليون نسمة، أي ما يعادل أكثر من ثلث مجموع سكان العالم .ويعيش أكثر من 60في المائة من جميع مستخدمي الإنترنت في البلدان النامية، ولا يتجاوز عمر 45 في المائة من مجموع مستخدمي الإنترنت ال 25عاماً، وبحلول عام 2017، من المتوقع أن تناهز نسبة المشتركين في خدمات الإنترنت النقالة ذات النطاق العريض 70في المائة من المجموع الكلي لسكان العالم(٢).

وبحلول عام ٢٠٢٠م، سيفوق عدد الأجهزة المتصلة بالشبكة)الأشياء المتصلة بالإنترنت (عدد الناس بنسبة ستة إلى واحد، مما سيؤدي إلى تغيير المفاهيم الحالية للإنترنت .ففي عالم الغد المتسم بالموصولية البالغة، سيصعب تصدّر وقوع جريمة حاسوبية وربما أي جريدة أخرى لا تنطوي على أدلة إلكترونية تتعلق بالموصولية بواسطة

(١) ورقة عمل للمستشار القانوني صالح الربيعة بعنوان الأمن الرقمي وحماية المستخدم من مخاطر الإنترنتhttp://cutt.us/ftcVd .

(٢) الجريمة السيبرانية والإيقاع الإجرامي التقليدي بالضحايا، دراسة شاملة عن الجريمة السيبرانية ، مكتب الأمم المتحدة المعني بالمخدرات والجريمة, مسودة شباط / فبراير ،٢٠١٣م، (ص.xxi).

بروتوكول الإنترنت(IP) [١] .

وتتوقف "تعاريف "الجريمة السيبرانية، في المقام الأول، على الغرض من استخدام المصطلح .فالجريمة سيبرانية الأساسية تتمثل في عدد محدود من الأعمال التي تمس بسرية البيانات أو النظم الحاسوبية وسلامتها توافرها .أمّا الأعمال المنفذة بواسطة الحواسيب والرامية إلى تحقيق مكاسب شخصية أو مالية أو إحداث اضرار، بما في ذلك أشكال الجريمة المتصلة بالهوية وبمحتوى الحواسيب)والتي تندرج كلها ضمن نطاق أوسع من معنى مصطلح "الجريمة السيبرانية("، فلا يمكن تطويعها بسهولة لتنضوي ضمن تعاريف قانونية لمصطلح جامع[٢].

ويلزم تعريف الأعمال الأساسية التي تشكّل جريمة سيبرانية، وإن كان "تعريف "الجريمة السيبرانية لا يتسم بنفس القدر من الأهمية فيما يخص الأغراض الأخرى، كتحديد نطاق صلاحيات الهيئات المختصة بالتحريات التعاون الدولي، حيث يفضل التركيز على الأدلة الإلكترونية فيما يخص أي جريمة، بدلا من التركيز على تركيبة واسعة واصطناعية لـ"الجريمة السيبرانية"[٣] .

رابعاً :البعد الأمني والمعلوماتي والاقتصادي بالفضاء السيبراني

ولقد ظهرت في الأفق عدة أبعاد بالفضاء السيبراني:

- البعد الأول هو البعد الأمني، وخير مثال علي ذلك هو مركز تكامل استخبارات التهديد السيبراني (CTIIC)بالولايات المتحدة الأمريكية الذي يعمل على التنسيق بين مختلف أجهزة الأمن الأمريكية الأخرى، مثل :مكتب التحقيقات الفيدرالي، وكالة الاستخبارات المركزية، ووكالة الأمن القومي .وكذلك المثال العربي علي ذلك وهو الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية[٤].
- البعد الثاني فهو يتعلق بأمن المعلومات فنجد أن العديد من الدول تقوم بتخصيص قيمة كبيرة من ميزانيتها لأجل مجابهة الهجمات السيبراني وتحديث وتطوير أنظمة الأمان لديها .
- البعد الثالث الاقتصادي فينقسم اقتصاد الإنترنت إلى مجالين رئيسيين، المجال الأول يتعلق بصناعة تكنولوجيا

(١) الجريمة السيبرانية والإيقاع الإجرامي التقليدي بالضحايا، المرجع السابق ص.25.
(٢) المرجع السابق.
(٣) المرجع السابق.
(٤) محمود عزت، الفضاء السيبراني وتحديات الأمن المعلوماتي العربي، المجلة العربية العدد ٤٩٨، أبريل 2018،(ص35 ،.36).

المعلومات والاتصالات (ICT)، ويشمل تطوير أجهزة وبرمجيات وانتاجها وخدمات أخري، أما المجال الثاني فهو مجال التجارة الإلكترونية من خلال فتح سوق حر علي شبكة الإنترنت .

لذلك يستوجب بالدول العربية أن تطوّر من نفسها حتى تستطيع مواكبة هذا الزخم التكنولوجي، بالأخص في مجال الأمن السيبراني، وسنقوم في الورقة البحثية باستعراض مشكلات التطور السيبراني وآثاره على المنطقة العربية بشكل عام والمملكة العربية السعودية بشكل خاص والجهود التي تم بذلها في ذلك الصدد .ومن هنا تأتي ضرورة توضيح ما يترتب على تلك الهجمات السيبرانية من آثار سلبية على العالم ومنها نسلط الضوء على المملكة العربية السعودية.

خامساً :أثر الهجمات السيبرانية على العالم

كشفت أرقام وبيانات عالمية، تزايد الجرائم السيبرانية في مختلف أنحاء العالم، مع التوسع المتزايد لاستخدام الانترنت والأجهزة الذكية، وأظهرت دراسة لموقع "أرقام ديجتال "أن عدد ضحايا الهجمات والجرائم الالكترونية، يبلغ 555مليون مستخدم سنوياً، وأكثر من 1.5مليون ضحية يومياً، في حين تقع ضحية كل ثانية لهذه الهجمات، وأكثر أنواع الجرائم سرقة هويات وعددها 224مليون سرقة، وأظهرت الدراسة أن مواقع التواصل الاجتماعي هي الأكثر اختراقاً، إذ بينت أن أكثر من 600ألف حساب فيسبوك يتم اختراقها يوميا وبينت الدراسة أن الكلفة السنوية المخصصة للأمن المعلوماتي قدرت بـ 100مليار دولار، بعدما كانت في حدود 63,1مليار دولار سنة 2011، ومن المتوقع أن تتجاوز 120مليار دولار بحلول سنة ٢١٧م[١] .

وحسب تقرير نشرته شركة مشاريع الأمن السيبراني (CYBERSECURITY VENTURES) بعنوان: (2017-2021) Cyber Security Economy predictions)، فإن العالم سينفق ما قيمته تريليون دولار خلال الفترة التي تمتد من 2017الى غاية ٢٠٢١ على منتجات وخدمات الأمن السيبراني لمكافحة الجريمة الالكترونية و في هذا الإطار فقد سجل فتح حوالى مليون وظيفة خاصة بالأمن السيبراني خلال سنة 2016، و من المتوقع أن يكون هناك عجز بحوالي 1,5 مليون وظيفة خلال عام ٢٠١٩م[٢].

(١) احصائيات صادمة وغريبة عن جرائم الأمن المعلوماتي، دراسة مقدمة من طرف موقع أرقام ديجيتال بتاريخ 25/10/2015 متوفرة على موقع: http://digital.argaam.com/article/detail/112326، 11/2/2017 :.

(2) cyber security economy predictions 2017-2021,cybersecurity ventures2016..

أثر الهجمات السيبرانية على المملكة العربية السعودية

كشف موقع «جوبال ريسك إنسايتس» أن المملكة العربية السعودية هي البلد الأكثر استهدافا بالهجمات الإلكترونية في الشرق الأوسط، وأن إيران أكثر من يستهدفها إلكترونياً، وينوه التقرير إلى أن الهجمات الإلكترونية على المملكة وصلت عام ٢٠١٥ إلى ١٦٠ ألف محاولة هجوم يومياً، ويشير نفس التقرير إلى أن الإمكانيات الرقمية والالكترونية الكبيرة للسعودية تجعلها هدفاً مميزاً للهجمات الالكترونية حيث تمتلك المملكة أكبر عدد من المشتركين في خدمة الإنترنت في العالم العربي. (١)

وتسببت الهجمات الإلكترونية ضررًا كبيرًا على البنية التحتية، وفي السعودية تضمنت أبرز الحوادث الرئيسية في هجمات استهدفت في البداية شركة أرامكو السعودية المملوكة للدولة في عام 2012وعطلت نشاط الشركة لمدة شهر في ما يشار إليه بأكبر اختراق في التاريخ ,وقد تسببت هذه البرمجيات الخبيثة في حدوث خلل مرة أخرى في نوفمبر ٢٠١٦م، ويناير ٢١٠٧م. (٢)

كذلك أوضح تقرير Over Security Advisory Councilوالصادر في 2016، أن الهجوم علي شركة أرامكو السعودية قد كلفها تغيير 50000قرص صلب لأجهزتها الحاسوبية، ولم تستطع استخدام الأنترنت لمدة خمسة أشهر تقريباً، وهذا يعتبر زمناً قياسياً في الإصلاح، خاصة إذا ما أخذنا بعين الاعتبار إمكانات أرامكو المالية والتقنية .كذلك هاجم Mamba Ransomwareالمملكة العربية السعودية في يوليو 2017، وتم استهداف شبكات الشركات داخل المملكة العربية السعودية .ظهرت Mamba Ransomwareفي عام 2016 في الولايات المتحدة الأمريكية وكانت واحدة من الفيروسات الأولى التي لا تشفر الملفات، ولكن الأقراص الصلبة بأكملها، ويستخدم أداة شرعية Disk Cryptor لتشفير لقرص أكمله(٣).

(١) محمد خالد، السعودية الأكثر تعرضا للهجمات الإلكترونية في الشرق الأوسط، مقال منشور على موقع الخليج الجديد , http://thenewkhalij.org/ar/node/43159.

(2) Arab News (2016), 'Cybercrime hit 6.5m in Kingdom last year', 11 August 2016, www.arabnews.com/node/967966/saudi-arabia.

(3) Ivanov Anton, Orkhan Mamedov. The Return of Mamba Ransomware Secure list - Information about Viruses, Hackers and Spam. N.p., 09 Aug. 2017. Web. 13 Sept. 2017. https://securelist.com/thereturn-ofmamba-ransomware/79403.

المبحث الثاني

الدور القانوني في مكافحة الجريمة السيبرانية

بدأت المؤسسات التشريعية ومختلف الهيئات والمنظمات على جميع الأصعدة الدولية الإقليمية الوطنية، تهتم بحماية استخدام الحاسوب وتجريم السلوكيات التي تستهدفه، حيث قامت بوضع العديد من الاتفاقيات الدولية والقوانين للتصدي لهذه الظاهرة الإجرامية، وسنتطرق إلى الدور القانوني المبذول في مكافحة الجريمة السيبرانية في دول العالم والوطن العربي ثم المملكة.

سنت عدد من الدول الأوربية قوانين خاصة بجرائم الانترنت والحاسوب مثل بريطانيا وهولندا وفرنسا والدنمارك والمجر وبولندا واليابان وكندا، كما اهتمت البلدان الغربية بإنشاء أقسام خاصة بمكافحة جرائم الإنترنت، بل إنها خطت خطوة إلى الأمام وذلك بإنشاء مراكز لاستقبال ضحايا تلك الجرائم(١). أما على مستوى الدول العربية فقد قامت الدول العربية بالتوقيع على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وذلك بتاريخ ٢٠١٠/١٢/٢١م، كما أدت هذه الاتفاقية كذلك لميلاد قوانين عديدة لمكافحة ما يسمى بالجرائم الإلكترونية في السعودية والأردن وقطر والإمارات والعراق وسلطنة عمان .وصارت الاتفاقية سارية المفعول بعد تصديق الرئيس المصري عليها سنة 2015 ليكتمل نصاب الدول السبع المطلوبة لسريانها(٢).

وبناءً على ما تقدم سيتم التطرق في هذا المبحث إلى الدور القانوني الدولي والإقليمي لمكافحة الجريمة السيبرانية، مروراً إلى آليات مكافحة الجريمة السيبرانية بدولة الامارات العربية ومصر والمملكة العربية السعودية .

المطلب الأول

الدور القانوني للهيئات الدولية في مكافحة الجريمة السيبرانية

في إطار الجهد الدولي المبذول وجدت العديد من الهيئات والمنظمات والمجالس الدولية التي لها دور ملحوظ في ابرام الاتفاقيات محاولة ترسيخ التعاون الدولي لمواجهة الجرائم السيبرانية وحماية مستخدمي الأنترنت، وهذا ما أكدته الاتفاقيات الدولية والإقليمية ومختلف التشريعات .مع ارتفاع الخسائر الناتجة عن الإجرام السيبراني وتزايد

(١) سمير سعدون مصطفي، محمود خضر سلمان، حسن كريم عبد الرحمن، الجريمة الالكترونية عبر الانترنيت اثرها وسبل مواجهتها، مجلة التقني، المجلد ٢، الإصدار ٩، ٢٠١١، (ص.49).

(٢) عزة مغازي، قانون الجريمة الإلكترونية التورنت يحملك إلى طرة، مقال منشور على موقع المنصة بتاريخ ٤ / ٢ / ٢٠١٦م.

حجم الأضرار الناتجة عنه، والتي تتخطى في أغلب الأحيان حدود الدول لتصل اعتداءاتها لأجهزة الحواسيب المملوكة للأفراد أو المؤسسات المالية أو الحكومات[١]، ورغم تميز الجرائم السيبرانية بالبعد الدولي كونها جرائم عابرة للحدود، الا انها لا تعتبر من بين الجرائم التي تختص المحكمة الجنائية الدولية بالنظر فيها[٢]. إن الجريمة السيبرانية يعاقب عليها من خلال التشريعات الوطنية، والسلوك الإجرامي المكون لها يتم على المستوى الداخلي، فهي جرائم داخلية لكن قد يترتب عنها ضرر على المستوى الدولي، لذا اهتمت الهيئات والمنظمات الدولية بمواجهة هذه الجرائم، وعلى رأسها هيئة الأمم المتحدة والجمعية الدولية لقانون العقوبات، وكذلك المجلس الأوربي.

أولاً :مواجهة المنظمات الدولية للجريمة السيبر انية

في سبيل محاولة التصدي للجرائم السيبرانية تبذل كل من الأمم المتحدة والجمعية الدولية لقانون العقوبات، جهوداً لا يستهان بها، تأكيدا على ضرورة تعزيز العمل المشترك بين جميع الدول.

أ. القرار الصادر عن الأمم المتحدة بشأن جرائم الكمبيوتر - هافانا: ١٩٩٠م، بعد انعقاد مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين في مدينة ميلانو الإيطالية عام ١٩٨٦م، والذي تمت من خلاله الإشارة إلى مشكلة الجريمة السيبرانية، حيث انبثقت عنه مجموعة من التوجهات من بينها تكليف لجنة الخبراء العشرين لدى منظمة الأمم المتحدة، بدراسة موضوع حماية نظم المعلومات والاعتداء على الحاسب الآلي، والتي بدورها أقرت جملة من التوصيات والمقترحات والمبادئ، التي تبناها المؤتمر الثامن لمكافحة الجريمة ومعاملة المجرمين المنعقد في أوت ١٩٩٠م، بالعاصمة الكوبية هافانا[٣] تتلخص توصيات مؤتمر هافانا أساساً في التأكيد على ضرورة وضع إطار قانوني دولي بتظافر جهود جميع الدول الأعضاء، من أجل التعاون على الحد من انتشار وتعاظم آثار هذه الظاهرة الإجرامية المستحدثة[٤]، وذلك بأن تقوم كل دولة عضو بتكثيف جهودها لمكافحة إساءة استخدام الكمبيوتر[٥]، وأشار القرار أنه على الدول الأعضاء وفي سبيل مواجهة الإجرام السيبراني اتخاذ مجموعة من الإجراءات تتلخص في:

- تحديث القوانين وأغراضها الجنائية، من أجل ضمان تطبيق الجزاءات والقوانين الراهنة بشأن جهات

(١) علي جبار الحسيناوي, جرائم الحاسوب والأنترنت، داراليازوري العلمية للنشر والتوزيع، عمان، (ص74)

(٢) عبد اللطيف معتوق، المرجع السابق، (ص2) .

(٣) علي جبار الحسيناوي، المرجع السابق، ص.147 .

(٤) محمود أحمد عباينة، جرائم الحاسوب وأبعادها الدولية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان،2009 ، (ص:١٥٥)

(٥) يوسف صغير، المرجع السابق، (ص: ٩٣).

التحقيق وقبول الأدلة في الإجراءات القضائية على نحو ملائم، وادخال تغييرات مناسبة إذا دعت الضرورة إلى ذلك، مع تحسين تدابير أمن الحاسب الآلي ومراعاة حماية الخصوصية واحترام حقوق الإنسان وحرياته الأساسية.

- وضع أحكام واجراءات تتعلق بالتحقيق والأدلة للتصدي لمثل هذا الشكل الجديد والمعقد من أشكال النشاط الإجرامي، ومصادرة أو رد الأصول الناجمة عن ارتكاب جرائم ذات صلة بالحاسوب.
- اعتماد تدابير لزيادة وعي الجماهير والعاملين في الأجهزة القضائية وأجهزة التنفيذ، بالمشكلة وبأهمية مكافحة الجرائم ذات الصلة بالحاسب الآلي.
- اعتماد تدابير مناسبة التدريب القضاة والمسؤولين عن منع الجريمة الاقتصادية والجرائم المتعلقة بالحاسب الآلي والتحري والادعاء فيها.
- الاهتمام بوضع قواعد خاصة بالآداب المتبعة في استخدام جهاز الحاسب الآلي، واعتماد سياسات تعالج المشكلات المتعلقة بضحايا جرائم الحاسب الآلي[١].

ب. القرارات الصادرة عن المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات بشأن جرائم الكمبيوتر -ريودي جانيرو 1994 : أوصى المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات الذي انعقد في ريودي جانيرو بالبرازيل في 04 أكتوبر 1994، والذي تم من خلاله مناقشة جرائم الحاسب الآلي بأن تتضمن قائمة الحد الأدنى من الأفعال المشكلة لجرائم الحاسب الآلي والمتعين تجريمها والتي يمكن ذكرها على النحو التالي[٢]:

- الاحتيال أو الغش المرتبط بالكمبيوتر، تزوير الكمبيوتر أو التزوير المعلوماتية.
- الإضرار بالبيانات والبرامج وتشمل المحو والإتلاف والتعطيل للمعطيات، تخريب وإتلاف الكمبيوتر.
- الدخول غير المصرح به : وهو الولوج إلى نظام ما عن طريق انتهاك إجراءات الأمن.
- الاعتراض غير المصرح به :وهو الاعتراض عن طريق وسائل فنية للاتصال توجه لنظام الكمبيوتر أو عدة نظم أو شبكة اتصالات[٣].

(١) عبد الله عبد الكريم عبد الله، المرجع السابق، (ص: ١٠٨-١١٠).

(٢) نسيم كروز، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة ماجستير، جامعة منتوري قسنطيقة، كلية الحقوق والعلوم السياسية، قسم الحقوق،2013-2012 ، (ص: ٨٤) .

(٣) عبد اللطيف معتوق، المرجع السابق، (ص: ١٠٠) .

وقد وضع القرار الصادر عن المؤتمر بعض القواعد الإجرائية لمكافحة الجرائم السيبرانية، كوجوب تحديد السلطات المؤهلة للتفتيش وضبط الأدلة في البيئة المعلوماتية، والسماح لها باعتراض المراسلات، وكذا ضرورة توفير قدر من التعاون بين الضحايا والشهود ومستخدمي هذه التكنولوجيا لإتاحة استخدام المعلومات في المتابعة القضائية، كما أكد القرار على ضرورة الأخذ بعين الاعتبار كل الوسائل المتعلقة بانتهاك حرمة الحياة الخاصة والتجسس والمخاطر والخسائر الاقتصادية أثناء عملية التفتيش وضبط الأدلة[١]. زيادة على هذه الجهود المبذولة، تلعب الوكالات والمنظمات العالمية العاملة تحت لواء الأمم المتحدة دورا في هذا المجال، ومن ذلك المنظمة العالمية للملكية الفكرية WIPO[٢]، فبعد تزايد الحاجة إلى إيجاد نصوص قانونية خاصة لحماية البرامج، شكلت المنظمة مجموعة عمل تضم عددا من الخبراء لحماية برامج الحاسب الآلي، وعبرت الاجتماعات المتكررة والتي كان آخرها عام 1985بالتعاون ما بين الويبر واليونيسكو في جنيف، ساد رأي لدى أغلب الدول الصناعية ودول العالم الثالث، وهو خضوع برامج الحاسب الآلي لقوانين حماية المؤلف، ومنذ ذلك العام وحتى الآن، علت معظم الدول تشريعاتها الخاصة بحق المؤلف وأضافت برامج الحاسب الآلي إلى المصنفات الأدبية المحمية وفقاً للقانون[٣].

ثانياً: مواجهة الإجرام السيبراني على المستوى الإقليمي

أ. **اتفاقية بودابست لمكافحة جرائم المعلوماتية والأنترنت -بودابست :2001** لعب المجلس الأوربي دورا هاما في مكافحة الجرائم السيبرانية، وصدرت عنه العديد من التوصيات لحماية تدفق المعلومات، ففي سنة 1981وقع المجلس الأوربي اتفاقية تتعلق بحماية الأشخاص لمواجهة المعالجة الإلكترونية للبيانات ذات الصبغة الشخصية، وفي أبريل 2000تقدمت اللجنة الأوربية بمشروع اتفاقية حول مشكلات جرائم المعلوماتية والحاسب الآلي والتي تمت المصادقة عليها سنة 2001ببودابست عاصمة المجر[٤]. تتكون الاتفاقية من مقدمة وأربعة فصول، حيث تم استعراض أهداف الاتفاقية ومرجعياتها السابقة، وبعض التدابير التشريعية الإقليمية والدولية المتعلقة

(١) المرجع نفسه.

(٢) نسيم دردور، المرجع السابق، (ص: ٨٤-٨٥).

(٣) محمود أحمد عبابنة، المرجع السابق، (ص:١٦٢).

(٤) هشام عبد الكريم، " التميز العنصري وصول الإستخدامات الجديدة للأنترنت، مداخلة مقدمة ضمن فعاليات الملتقى الدولى الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة برج بوعريريج، الموسوم بعنوان :الإجرام السيبراني المفاهيم والتحديات، يومي ١١و١٢ / ٤ / ٢٠١٧م، (ص: ٨).

بجرائم المعلوماتية، كما ثمّنت المقدمة التعاون الدولي في هذا المجال[١]. حيث تضمّن الفصل الأول من الاتفاقية تعريف المصطلحات من خلال نص المادة الأولى، أما الفصل الثاني جاء تحت عنوان الإجراءات المتعين اتخاذها على المستوى الوطني وتضمّن ثلاثة أقسام، يضم القسم الأول منها المواد من ٢ إلى ١٣ ويعالج النصوص الموضوعية الجرائم المعلوماتية[٢]، حيث نص على خمس مجموعات:

- المجموعة الأولى :وتتضمن الجرائم التي تستهدف أمن المعلومات وسريتها، وسلامة معطيات المنظومة المعلوماتية وإساءة استخدام الأجهزة .
- المجموعة الثانية :الجرائم المرتبطة بالكمبيوتر وهي التزوير والاحتيال المرتبطين به.
- المجموعة الثالثة : وتتضمن الجرائم المرتبطة بالمحتوى، وتنطوي تحتها صورة واحدة وهي جرائم دعارة الأطفال وتشمل تجريم أي نشاط متعلق بهذا الموضوع.
- المجموعة الرابعة :وهي الجرائم المرتبطة بحقوق المؤلف والملكية الفكرية.
- المجموعة الخامسة :تحوي المساهمة والشروع والمسؤولية الجزائية للأشخاص المعنوية[٣].

ب. **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات** :بتاريخ ٢١ /ديسمبر/ ٢٠١٠م، وافق مجلس وزراء الداخلية والعدل العرب في اجتماعهم المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة، على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، تحتوي هذه الاتفاقية على ٤٣ مادة، وجاء في المادة الأولى منها "تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات لدرء أخطار هذه الجرائم، حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها "، ونجد في الفصل الثاني تفصيلا للأفعال التي تعد مجرمة، أما الفصل الثالث منها فقد تم التعرض من خلاله إلى نطاق تطبيق الأحكام الإجرائية، وفي الفصل الرابع تُصل على التعاون القانوني والقضائي، أما الفصل الخامس فتضمن أحكاما ختامية[٤].

ت. **القمة الخليجية** :أقرت القمة الخليجية الأمريكية ست مبادرات أمنية، تمثلت في التدريب وإجراء مناورات عسكرية مشتركة فيما بينها وتبادل المعلومات الاستخبارية، بالإضافة إلى نظام إنذار مبكر ضد الصواريخ

(١) عبد الله عبد الكريم عبد الله، المرجع السابق، فصل ١٢٤-١٢٥.
(٢) عبد اللطيف معتوق، المرجع السابق، ص.101 .
(٣) مخروس قصار غايب، " الجريمة المعلوماتية" ، مجلة هيئة التعليم التقني الأكاديمية، المجلد24 ، العراق،2011 ، (ص: ٢٠-٢١).
(٤) فاروق خلف، المرجع السابق، (ص: ٨).

الباليستية، وإجراء مناورات عسكرية أمريكية خليجية تبدأ في شهر مارس من العام القادم ٢٠١٩م، والتعاون البحري وإقرار مبادرات لتعزيز الأمن السيبراني .تتعدد طرق الاختراق للشبكة المعلوماتية التي توفرها وتعرف باسم (Programs)ولا دخل للأجهزة والمعدات المعروفة باسم (Hardware)إلا إذا كان يتضمن حماية خاصة .إن معظم الأفراد والمؤسسات بكل أنواعها يرغبون في الحفاظ على خصوصية المعلومات الحساسة، لكن البعض لا يدرك بأن تلك المعلومات التي يراها بسيطة هي ذات أهمية كبرى لدى المخترق.

لهذا وضعت القوانين لحماية المعلومات ولكن هذه القوانين تختلف من دولة إلى أخرى حسب منظوماتها التشريعية والقانونية كما أن بعض الدول لم تضع قوانين تعاقب على ذلك، ولكن يوجد هناك تعاملات إلكترونية وتعهدات دولية بين الدول توفر الحماية وتفرض العقوبة .فاليوم نعيش حربًا سيبرانية تتمثل في اختراق أجهزة الحاسب مما يكلف الدول مبالغ باهظة وقد يؤدي إلى تعطيل الجهاز، فقد أصبحت الحرب السيبرانية لها القدرة على تدمير بعض الأسلحة وإسقاط بعض الطائرات وإحداث الشلل في الاتصالات، ولأن الإنترنت مربوط بالأقمار الاصطناعية فإن الولايات المتحدة الأمريكية لديها القدرة على تعطيل الأجهزة والتحكم في كثير من دول العالم .فتوفير الولايات المتحدة للحماية يساعد دول الخليج على تحقيق الأمن السيبراني، ويوفر لها التقنية اللازمة للوقاية من الحروب السيبرانية في السلم والحرب.

المطلب الثاني

الدور القانوني في مكافحة الجريمة السيبرانية ببعض الدول العربية

أولا :دولة الامارات العربية المتحدة

تعد دولة الإمارات العربية المتحدة من الدول العربية القليلة والرائدة في تعزيز الدور القانوني في مكافحة الجريمة السيبرانية، وقد تناول القانون الاتحادي رقم ٢ لسنة ٢٠٠٦ المتعلق بمكافحة جرائم المعلوماتية، مجموعة من الجرائم، كجريمة اختراق المواقع والأنظمة الإلكترونية، أين تم التمييز بين الأنظمة المعلوماتية وبين الاختراق، وترتب نتيجة متعلقة بالإلغاء أو الحذف أو تدمير المعلومات، إذ جعل العقوبة في الحالة الثانية أشد وتُقدر بالحبس لمدة لا تقل عن ٦ أشهر مع غرامة مالية، وفي حالة اختراق النظم المعلوماتية يترتب عن ذلك انتهاك للمعلومات الشخصية، وتكون العقوبة في الحبس لمدة لا تقل عن سنة وغرامة مالية مقدرة بعشرة آلاف درهم[١].

(١) عبد اللطيف معتوق، المرجع السابق، (ص: ٩٥-٩٦).

لكن هذا القانون تعرض للنقد في حلقة نقاشية نظمها معهد التدريب والدراسات القضائية بالإمارات العربية المتحدة، حيث أن المشاركين من قضاة ووكلاء نيابة أكدوا في ختام النقاش أن مواد هذا القانون تتعارض فيما بينها، ودعوا لإيجاد محاكم مختصة للبت في جرائم تقنية المعلومات وعقد المزيد من برامج التدريب والتظافر لتوعية الشباب بالقانون(١).

ثانيا :دولة مصر

لقد وضع المؤتمر التأسيسي الأول لجمعيات قانون الأنترنت الذي عقد بالقاهرة في ٢٧/ سبتمبر/٢٠٠٤م اللبنة الأولى لإنشاء جمعيات ومنظمات للعمل التطوعي في مجال قانون الأنترنت، ثم تم عقد المؤتمر الدولي الأول لقانون الأنترنت بمدينة الغردقة في أوت ٢٠٠٥ وبدأ الاهتمام في مصر بمكافحة الجرائم المعلوماتية(٢) ثم تأسست الجمعية المصرية لمكافحة جرائم المعلوماتية في نفس السنة، وهي منظمة غير حكومية تعمل على نشر الوعي وإعداد الدراسات والمؤتمرات حول هذه الجرائم(٣)، وتعتبر حركة التشريع في مجال مكافحة الجريمة السيبرانية في مصر، ضعيفة مقارنة بدولة الإمارات العربية المتحدة، إلا أن تطبيق بعض النصوص التقليدية المتعلقة بالتزوير والاحتيال والسرقة والمساس باعتبار الأشخاص، لا يزال مستمرا في القانون المصري(٤) ويعتبر قانون التوقيع الإلكتروني الصادر سنة ٢٠٠٤م، أول قانون يصدر بشأن الأفعال المتعلقة بالنظم المعلوماتية في مصر، حيث جرم أفعالا بموجب المادة ٢٣ منه، تتعلق بالحصول على توقيع أو وسيط أو محرر إلكتروني بدون وجه حق، أو اعتراضه أو تعطيله عن أداء وظيفته وقد عُرّف الوسيط الإلكتروني في الفقرة الرابعة من المادة الأولى من قانون التوقيع الإلكتروني المصري بأنه "أداة أو أدوات أو أنظمة إنشاء التوقيع الإلكتروني، فهو عبارة عن نظام معلوماتي يساعد على إنشاء التوقيع الإلكتروني واصدار المحررات الإلكترونية(٥).

من خلال ما سبق عرضه يتضح أن مختلف الاتفاقيات الدولية والإقليمية وكذا التشريعات الوطنية قد أولت اهتماماً كبيراً بالدور القانوني في مكافحة الجريمة السيبرانية، وذلك بهدف تحقيق مجموعة من الأهداف المتمحورة

(١) عبد الله عبد الكريم عبد الله، المرجع السابق، (ص: ٧٩).
(٢) عبد الفتاح بيمو حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، الطبعة الأولى، دار الفكر الجامعي الإسكندرية، ٢٠٠٦م، (ص: ٥٥٦).
(٣) عبد الله عبد الكريم عبد الله، المرجع السابق، (ص: ٩٣).
(٤) عبد اللطيف معتوق، المرجع السابق، (ص: ٩٧).
(٥) على عدنان الفيل، الإجرام الإلكتروني، الطبعة الأولى، منشورات تزين الحقوقية، بيروت، ٢٠١١م، (ص: ٢٣١-٢٤٢) .

أساساً حول توفير الحماية اللازمة لمستخدمي الانترنت وللنظم المعلوماتية حيث سعت هذه الاتفاقية إلى بناء سياسة جنائية مشتركة من أجل مكافحة الجرائم المعلوماتية في جميع أنحاء العالم من خلال تنسيق وانسجام التشريعات الوطنية ببعضها البعض، و تعزيز قدرات القضاء وكذا تحسين التعاون الدولي في هذا الإطار، إضافة إلى تحديد عقوبات للجرائم السيبرانية في إطار القوانين الداخلية.

ثالثاً : المملكة العربية السعودية

إدراكاً من المملكة بأهمية الأمن السيبراني، فقد بادرت بإحداث هيئة وطنية للأمن السيبراني، وتعزيز وحماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، مراعية في ذلك الأهمية الحيوية المتزايدة للأمن السيبراني في حياة المجتمعات، ومستهدفة التأسيس لصناعة وطنية في مجال الأمن السيبراني تحقق للمملكة الريادة في هذا المجال انطلاقاً مما تضمنته رؤية المملكة العربية السعودية2030 ، ويضمن توافر واستمرارية عمل نظم المعلومات، وتأمين حماية وسرية وخصوصية البيانات الشخصية، وحماية المواطنين من المخاطر في الفضاء السيبراني، وتفعيل الحكومة الالكترونية.

إن المملكة العربية السعودية لديها أيضاً قانون للجرائم الإلكترونية صادر بموجب مرسوم ملكي في عام ٢٠٠٧م وهو يهدف إلى مكافحة الجرائم الإلكترونية عن طريق تحديد الجرائم وتحديد العقوبات لحماية أمن المعلومات، وحماية الحقوق المتعلقة بالاستخدام المشروع لأجهزة الكمبيوتر وشبكات المعلومات، وحماية المصلحة العامة[١]. بالإضافة إلى ذلك، يمكن لوزارة الداخلية السعودية ولجنة تكنولوجيا المعلومات معاقبة مرتكبي الجرائم الإلكترونية بشدة مثل سرقة الهوية والتشهير والقرصنة الإلكترونية وسرقة البريد الإلكتروني وغير ذلك من الأعمال غير القانونية . وقال ترولز أورتينغ يورغنسن، رئيس مركز الأمن السيبراني في المنتدى الاقتصادي العالمي، إن السعودية تتحول من مستهلك للمعرفة إلى مُصدّر لها، مشيرا إلى أن المركز الذي يرأسه يعمل مع جهات حكومية ومن القطاع الخاص في المملكة على مواجهة التهديدات السيبرانية اختصاصات الهيئة الوطنية للأمن السيبراني[٢]. وكان الاتحاد الدولي للاتصالات التابع للأمم المتحدة قد قام باستحداث مؤشر عالمي للأمن السيبراني (GCI)، يتم قياسه بشكل دوري كل عامين بناء على خمس ركائز رئيسية؛)القانونية والتعاونية والتقنية والتنظيمية وبناء القدرات (لتحديد مدى النضج

(1) M.A. Saeed, "Cyber Security and Data Privacy Law in Saudi Arabia, Financier Worldwide, April 2015, http://www.financierworldwide.com/cyber-security-and-data-privacy-law-insaudi- arabia/#.V2buhed950s.

(2) https://bit.ly/2G4kyla.

في الدول الأعضاء في مجال الأمن السيبراني وفقًا لمعايير محددة، ويهدف الاتحاد العالمي من وضع هذا المؤشر إلى رفع مستوى الأمن السيبراني وتعزيز تبادل الخبرات ومشاركة التجارب فيما بين دول العالم.

واحتلت المملكة العربية السعودية المرتبة الأولى بين الدول العربية التي حصلت على أعلى الدرجات في عمود بناء القدرات .تُظهر المملكة العربية السعودية التزاماً قوياً ببناء القدرات من خلال العديد من المبادرات، بما في ذلك برنامج حاضنة التكنولوجيا(BADIR)، والشبكة العربية للبحوث والابتكار والاتحاد السعودي للأمن الإلكتروني والبرمجة، كما طورت المملكة العربية السعودية دعامة تعاون قوية(١).

بناءً على ما سبق تكون المملكة العربية السعودية قد أحرزت مركز متقدم في المؤشر العالمي للأمن السيبراني الصادر عن الاتحاد الدولي للاتصالات التابع للأمم المتحدة وجاءت الأولى عربياً، فيما تبوأت المرتبة ١٣ بين ١٧٥ دولة.

أولاً :الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية

تعتبر منظمة وطنية تحت مظلة اللجنة الأولمبية السعودية، تسعى لبناء قدرات محلية واحترافية في مجال الأمن السيبراني والبرمجة بناءً على أفضل الممارسات والمعايير العالمية للوصول بالمملكة العربية السعودية إلى مصاف الدول المتقدمة في صناعة المعرفة التقنية الحديثة، زيادة على أنه سلاح استراتيجي في يد الحكومة والفرد، لا سيما أن الحرب السيبرانية أصبحت جزءًا لا يتجزأ من التكتيكات الحديثة للحروب بين الدول .لذا تُعد لضمان وجود واستمرارية مجتمع المعلومات للأمة وحماية فضاء الإنترنت والمعلومات الخاصة به، والأصول والبنية التحتية الحيوية.

عالم اليوم أضحى بكل أساليبه، وأنماطه وتفاصيله مرتبطًا ارتباطا وثيقاً بالشبكات العالمية المتجددة، وبأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية؛ بل أصبح قرية كونية صغيرة يتفاعل الجميع فيها ويتواصلون ويتشاركون في المعلومات والأفكار، وارتبطت فيه أغلب الأنشطة الحياتية الأساسية بانسيابية المعلومات وأمانها وتكامل أنظمتها .ويتهيأ العالم مع هذا التقدم لاستقبال ثورة صناعية رابعة تقوم على تقنيات تتسم بالنمو المتسارع في قدرات المعالجة الحاسوبية وقدرات التخزين الهائلة للبيانات وتبادلها، والاستعداد للتعامل مع منتجات ومعطيات الذكاء الاصطناعي والروبوتات والأجهزة ذاتية التحكم، وكل ذلك يتطلب المواكبة الذكية، وتنمية القدرات النوعية المختلفة، والتكييف وفق متطلبات الأمن السيبراني.

وانطلاقاً من إدراك المملكة العربية السعودية لهذه المتغيرات وتفاعلها مع مستجدات العصر وتطوراته، وترجمة

(1) International Telecommunication Union, Global Cybersecurity Index.2018. p27.

لنهج خادم الحرمين الشريفين الملك سلمان بن عبد العزيز وسمو ولي العهد حفظهم الله في قيادة بلادنا لتكون نموذجاً ناجحاً ورائداً في العالم على كافة الأصعدة، ولرؤية المملكة 2030 التي جعلت التحول نحو العالم الرقمي وتنمية البنية التحتية الرقمية ضمن مستهدفاتها، واستشعارا لأهمية البيانات والأنظمة التقنية والبنى التحتية الحساسة وارتباطها بالمصالح الوطنية، وأهمية حمايتها من أي تهديدات أو مخاطر يشهدها الفضاء السيبراني يأتي تأسيس الهيئة الوطنية للأمن السيبراني وارتباطها بالملك -حفظه الله -وذلك وفق الأمر الملكي الكريم بالموافقة على تنظيمها بتاريخ ١١ / ٢ / ١٤٣٩هـ. لتكون الهيئة هي الجهة المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه، وتهدف إلى تعزيزه؛ حمايةً للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية .ولا يخلي ذلك أي جهة عامة وخاصة أو غيرها من مسؤوليتها تجاه أمنها السيبراني بما لا يتعارض مع اختصاصات ومهمات الهيئة الواردة في تنظيمها(١).

للهيئة اختصاصات عدة أهمها(٢):

- استقطاب الكوادر الوطنية :تضع الهيئة على رأس أولوياتها استقطاب الكوادر الوطنية المؤهلة والطموحة وتأهيلها وتمكينها، وبناء الشراكات مع الجهات العامة والخاصة.
- حماية الأمن الوطني للملكة :وتهتم بحماية مصالح المملكة الحيوية وأمنها الوطني، والبنية التحتية الحساسة فيها، وضم أعضاء مجلس إدارة الهيئة الوطنية للأمن السيبراني، رئيس أمن الدولة، ورئيس الاستخبارات العامة، ونائب وزير الداخلية، ومساعد وزير الدفاع.
- تحفيز الابتكار والاستثمار :كما تساعد على تحفيز الابتكار والاستثمار في مجال الأمن السيبراني للإسهام في تحقيق نهضة تقنية تخدم مستقبل الاقتصاد الوطني للمملكة، وأيضًا تأسيس صناعة وطنية في مجال الأمن السيبراني تحقق للمملكة الريادة في هذا المجال انطلاقًا، ما تضمنته رؤية السعودية 2030
- تعزيز أنظمة التقنيات التشغيلية :ومن اختصاصها أيضًا مراعاة الأهمية الحيوية المتزايدة للأمن السيبراني في حياة المجتمعات، وتعزيز أنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات.

(١) الهيئة الوطنية للأمن السيبراني National Cybersecurity Authority ، الضوابط الأساسية للأمن السيبراني ، Essential Cybersecurity Controls, (ECC- ١:٢٠١٨) ،إشارة المشاركة ، تصنيف الوثيقة: غير مصنف ، راجع الرابط التالي: https://nca.gov.sa/pages/about.html.

(٢) الهيئة الوطنية للأمن السيبراني National Cybersecurity Authority ، الضوابط الأساسية للأمن السيبراني ، Essential Cybersecurity Controls, (ECC- ١:٢٠١٨) ،إشارة المشاركة ، تصنيف الوثيقة: غير مصنف.

كل هذه التغيرات تستدعي وجود نشاط قانوني ينسجم مع التطورات الحاصلة، سواء على مستوى الحقوق أو مستوى البيئات والعمليات .كما قامت الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية، بتطوير الضوابط الأساسية للأمن السيبراني، بعد دراسة عدة معايير وأطر وضوابط للأمن السيبراني قامت بإعدادها سابقاً عدة جهات ومنظمات محلية ودولية، ودراسة متطلبات التشريعات والتنظيمات والقرارات الوطنية ذات العلاقة، وبعد التطلع على أفضل الممارسات والتجارب في مجال الأمن السيبراني والاستفادة منها، وتحليل ما تم رصده من حوادث وهجمات سيبرانية على مستوى الجهات الحكومية وغيرها من الجهات الحساسة؛ وتُطبق هذه الضوابط على الجهات الحكومية في المملكة العربية السعودية وتشمل الوزارات والهيئات والمؤسسات وغيرها والجهات والشركات التابعة لها، وجهات القطاع الخاص التي تمتلك بنى تحتية وطنية حساسة (Critical National Infrastructures)، أو تقوم بتشغيلها أو استضافتها، كما تُشجع الهيئة الجهات الخرى في المملكة وبشدة على الاستفادة من هذه الضوابط لتطبيق أفضل للممارسات فيما يتعلق بتحسين الأمن السيبراني وتطويره داخل الجهة(١).

أطلقت الهيئة الوطنية للأمن السيبراني عدة مبادرات لمواجهة النقص في الكوادر الوطنية في هذا المجال، إذ أطلقت مؤخراً مبادرة الابتعاث في الأمن السيبراني بالشراكة مع وزارة التعليم من خلال برنامج خادم الحرمين الشريفين للابتعاث الخارجي، حيث تم الاتفاق على زيادة أعداد مقاعد الابتعاث للعام الأول من 200إلى 540مقعداً، لتلبية حاجة بناء القدرات الوطنية في مجال الأمن السيبراني ولسد الاحتياج الذي يتطلبه سوق العمل الحكومي والخاص بهدف حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، لحماية الفضاء السيبراني للمملكة؛ وتأتي هذه المبادرة تنفيذًا لما ورد في تنظيم الهيئة الوطنية للأمن السيبراني المتضمن اختصاصها ببناء القدرات الوطنية المتخصصة في مجالات الأمن السيبراني، والمشاركة في إعداد البرامج التعليمية والتدريبية الخاصة بها(٢).

ثانياً :دور الجهات الحكومية والخاصة وغيرها تجاه الأمن السيبراني(٣):

إن تعزيز الأمن السيبراني للمملكة يتطلب تعاون كافة الجهات للعمل في منظومة وطنية متكاملة قادرة على مواجهة المخاطر السيبرانية وتقليل أثرها .ولذلك فإن الهيئة الوطنية للأمن السيبراني تعتبر كل جهة، عامة كانت أو

(١) الهيئة الوطنية للأمن السيبراني، الضوابط الأساسية للأمن السيبراني .(ص: ٧-٩).

(٢) الأمن السيبراني,السعودي, يبدأ بتدريب-800-مواطن,https:// www .today/alarabiya.net/ar/saudi, خلال ٢٤ / ١١ / ٢٠١٨م.

(٣) الهيئة الوطنية للأمن السيبراني National Cybersecurity Authority ، الضوابط الأساسية للأمن السيبراني ، Cybersecurity Essential Controls, (ECC- ١: ٢٠١٨) ،إشارة المشاركة ، تصنيف الوثيقة: غير مصنف ، راجع الرابط التالي: https://nca.gov.sa/pages/about.html.

خاصة، شريكا أساسياً لتحقيق الأهداف التي أنشئت من أجلها الهيئة .

وقد أكد تنظيم الهيئة على أنها الجهة المختصة في المملكة بالأمن السيبراني، وأن ذلك لا يخلي أي جهة عامة أو خاصة أو غيرها من مسؤوليتها تجاه أمنها السيبراني بما لا يتعارض مع اختصاصات ومهمات الهيئة الواردة في تنظيمها.

كما أكد الأمر السامي الكريم بتاريخ 10/11/1339هـ "بأن على جميع الجهات الحكومية رفع مستوى أمنها السيبراني لحماية شبكاتها وأنظمتها وبياناتها الإلكترونية، والالتزام بما تصدره الهيئة الوطنية للأمن السيبراني من سياسات وأطر ومعايير وضوابط وإرشادات بهذا الشأن ."وبحسب تنظيم الهيئة تلتزم كافة الجهات ذات العلاقة بما يأتي:

١. تمكين الهيئة من مباشرة اختصاصاتها، وتنفيذ مهماتها بشكل كامل.
٢. إبلاغ الهيئة بشكل فوري بأي خطر أو تهديد أو اختراق لأمنها السيبراني واقع أو محتمل.
٣. تنفيذ السياسات وآليات الحوكمة والأطر، وتطبيق المعايير والضوابط التي تقرها الهيئة.
٤. التعاون التام مع الهيئة عند قيامها بأي أعمال تحرٍ أو تدقيق أو تقييم للأمن للسيبراني.
٥. تزويد الهيئة بالوثائق والمعلومات والبيانات والتقارير اللازمة للقيام باختصاصاتها ومهماتها، وتمكينها من فحص الأجهزة والشبكات والنظم والبرمجيات الخاصة بتلك الجهات.

دور الاتحاد السعودي للأمن السيبراني والبرمجة :وعلى ذلك يتمثل دور الاتحاد السعودي للأمن السيبراني والبرمجة في:

- تعزيز حماية الشبكات.
- تعزيز حماية أنظمة تقنية المعلومات.
- تعزيز حماية أنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، ومراعاة الأهمية الحيوية المتزايدة لتخصصها.
- التأسيس لصناعة وطنية في مجال الأمن السيبراني تحقق للمملكة الريادة في هذا المجال.
- أن تكون المرجع الوطني للمملكة في شؤون تخصصها.
- حماية مصالح المملكة الحيوية وأمنها الوطني، والبنى التحتية الحساسة فيها.

يترتب على نشاط كل من الفرد والمؤسسة والحكومة في الفضاء السيبراني نتائج قانونية وموجبات تتطلب اهتمامًا

خاصًا لحل النزاعات التي يمكن أن تنشأ عنها وهو ما يُلزم مواكبة التحولات التي رافقت ظهور مجتمع المعلومات، فظهرت عدة حقوق أخرى كحق النفاذ إلى الشبكة العالمية للمعلومات، والحق في إنشاء المدونات الإلكترونية وإنشاء التجمعات على الإنترنت، كما ظهرت موجبات جديدة ذات انعكاس اقتصادي مثل: موجب الاحتفاء ببيانات الاتصالات، وموجب الإبلاغ عن مخالفات وجرائم خاصة بالمحتوى.

مكافحة الجرائم الالكترونية(١):

الحماية في شقها الأمني:

هذا الجانب متعلق بكل شيء يختص بحماية شبكة الإنترنت والكمبيوتر سواء من ناحية فنية أو تقنية، سنتطرق إلى ثلاث نقاط تتعلق بأمن ومهددات المعلومات والإجراءات الأمنية.

أولاً : مسائل تتعلق بأمن المعلومات يتعلق أمن المعلومات بالمواضيع التالية :

- المسألة الإدارية :جميع المؤسسات تمتلك كمية كبيرة من المعلومات الهامة التي يتم حفظها في جهاز الحاسب وتحتاج إلى الحماية الأمنية .
- المسألة المالية : تتشكل في التكلفة المادية التي يتم صرفها مقابل حماية النظم المعلوماتية ذات الأهمية الكبيرة .
- المسألة الوظيفية :تتمثل في المقدرة على توفير المعلومات دائما بالشكل الصحيح والسري الكامل في حال الحاجة إليها .
- المسألة الخصوصية :تتمثل بواجبها نحو حماية النظام الذاتي الخاص بالفرد أو التلاعب بها .
- مسألة تحديد مخاطر وحوادث الكمبيوتر والشبكة :قد تحدث هذه الحوادث بشكل طبيعي أو مقصود وبالنظر إلى مدى تطور التقنية الحاسوبية يصبح تحديد المخاطر أكثر تعقيدًا.

ثانياً :مهددات أمن المعلومات: هي حالة تؤدي إلى توقف وتعطل الشبكة المعلوماتية مما يصعب أو يمنع الوصول إلى المعلومات . وأنواع هذه المهددات:

- مهددات طبيعية : مثل الزلازل التي تؤدي إلى قطع الاتصالات بالشبكة.
- مهددات غير مقصودة :تحدث بسبب الأشخاص كإساءة استخدام الفرد لكملة المرور.

(١) دراسة بحثية بعنوان" الجرائم الالكترونية "للباحثة إسراء مرعي.

- مهددات إنسانية : هي تسلل المخترقون للمواقع الأمنية.

إن الثغرات الأمنية يمكن كشفها من طرف المخترق خاصةً في الحواسب الشخصية، أما بالنسبة لخطوط الاتصال فهي معرضة للمراقبة بالإشعاعات أو التصنت والتجسس، بحيث يتم استخدام الاتصال بالشبكة العنكبوتية (الإنترنت) عن طريق الألياف البصرية والأقمار الصناعية كما يمكن اعتراض طريق وصول الأسلاك لسرقة المعلومات عن طريق الشبكة .

الشق الأمني :قد قدمت شركة FireEye المتخصصة في مجال التصدي للهجمات الالكترونية المتقدمة إجراءات مهمة لتفادي مخاطر تزايد الهجمات الالكترونية التي تستهدف دول الخليج العربي، بعدما كشفت عن جملة من التصورات والرؤى التحليلية بشأن مشهد الهجمات الالكترونية في مناطق أوروبا والشرق الأوسط وأفريقيا، وعلى وجه الخصوص في دول مجلس التعاون الخليجي، وتمثلت هذه الإجراءات فيما يلي:[(١)]

١. التوقع الدائم بأن تكون تلك الشركات مستهدفة.
٢. أنه من الممكن تخطي حدود الضوابط الأمنية المتوفرة لديها.
٣. التأكد دائما من أن ليس هناك أي كيان تجاري بمنأى عن الهجمات.
٤. وضع إطار عمل خاص بالمخاطر ذات الصلة بالأنترنت.
٥. الحصول على منصة استخبارات التهديدات الأنسب لتحسين قدرات الكشف عن الهجمات المحتملة.
٦. إنشاء خدمة الاستجابة للحوادث الطارئة وإدارتها، والتي من شأنها تمكين الشركات من اكتشافها والتفاعل مع هجمات APT بالسرعة الممكنة.
٧. تسخير التكنولوجيا المناسبة القادرة على تحديد واكتشاف هذه التهديدات الجديدة.
٨. وضع خطة استجابة واضحة والعمل على تحضيرها استعدادا للتعامل مع أي حالة اختراق.

وإن مواجهة مخاطر الجرائم المعلوماتية تعتمد بشكل كبير على تبني إستراتيجية أمنية مجتمعية متكاملة، والتي تعمل فيها أجهزة مكافحة الجريمة الرسمية في الدولة جنباً إلى جنب مع أفراد المجتمع ومؤسسات القطاع الخاص، هو ما يمكن من خلاله مكافحة الأنشطة الإجرامية في الفضاء الإليكتروني والتقليل من مخاطرها والحد من انتشارها،

(١) إجراءات لتفادي مخاطر تزايد الهمجات الالكترونية التي تستهدف دول الخليج العربي، مقال منشور على موقع جريدة مكة، تاريخ النشر ٢٠١٦/٦/١م، على الرابط http://makkahnewspaper.com/article/١٤٧٨٧١.

وهذه الرؤية تتسق مع نتائج الدراسات التي أجريت في بلدان مختلفة من العالم حول التعامل مع جرائم الإنترنت، والتي أوضحت أهمية مشاركة العديد من المصادر والمؤسسات الخاصة في تحمل جزءًا من المسؤولية فيما يتعلق بمكافحة هذه الجرائم والسيطرة عليها وتلك المصادر تتمثل في: (١)

١. مزودو خدمة الإنترنت الذين يملكون القدرة على تحديد ما يعرف ب (IP) (Internet Protocol) للمشتركين، ما يتيح إمكانية مراقبة الأنشطة الخطرة على الإنترنت وتقييد اشتراك المستخدمين المنخرطين في تلك الأنشطة.

٢. المواطن العادي بدوره كذلك يمكن أن يساهم من خلال تحمل مسؤولية حماية نفسه من الوقوع ضحية لجرائم الإنترنت باقتنائه برمجيات الحماية من الفيروسات.

٣. المصارف التجارية وشركات البطاقات الائتمانية عليها أيضاً مسؤولية كبيرة في حماية عملائها من خلال تطبيق إجراءات وقائية ضد الاحتيال، وكذلك تنصيب برمجيات مراقبة خاصة على خوادمها لتعقب النشاطات غير المعتادة على حسابات العملاء ووضع أنظمة لتنبيه العميل على كل عملية تتم على حسابه.

٤. المحققين الخاصين الذين يعملون بالتنسيق مع أجهزة العدالة الجنائية يمكن أن يلعبوا دوراً مهماً في مكافحة جرائم الإنترنت.

الخاتمة

إن التطرق الجديد للأمن السيبراني في الفترة الحالية توجب علينا التوقف والتمعن في هذا المفهوم لاسيما في ظل التطور السريع في التكنلوجيا ومجال الإعلام الآلي الذي تحولت فيه الخدمات من الشكل الورقي التقليدي إلى الإلكتروني السريع، وعلى الرغم من إيجابياته إلا أنه وجب توفير الأمن لنجاح هذه الخدمات بالشكل المطلوب.

والمملكة العربية السعودية كغيرها من الدول اتجهت نحو إنشاء هيئة متخصصة لحماية العالم الإلكتروني المعلوماتي وعلى الرغم من ذلك إلا أن عدد الجرائم المرتكبة يوحي بحجم الأخطار التي قد تحصل مستقبلًا وهو ما يجعل الأمن السيبراني أمام تحدي جديد وقوي لتحقيق الأمن حاليًا ومستقبلًا.

(١) عبدالله بن فازع القرني، مواجهة جرائم الإنترنت :نحو إستراتيجية أمنية – مجتمعية متكاملة، مقال منشور على موقع جريدة الرياض بتاريخ ٢٠١٤/٢/٢١م، على الرابط::http://www.alriyadh.com/912032 .

التوصيات

١. إصدار قوانين خاصة مستقلة لمكافحة الجرائم السيبرانية.

٢. نشر الثقافة المجتمعية في كيفية استخدام التكنلوجيا بالصورة التي تجنب مخاطر القرصنة Hacking والاختراق Cracking وغيرها من الجرائم الإلكترونية.

٣. توجيه المدارس عامةً والجامعات خصوصاً للبحث والدراسة في الجرائم المعلوماتية ومحاولة إنشاء دبلومات متخصصة في مكافحة تلك الجرائم.

٤. حث جامعة الدول العربية لإصدار قانون نموذجي موحد لمكافحة الجرائم الإلكترونية.

٥. تأمين انسجام الأنظمة القانونية المكافحة للجرائم السيبرانية بما يمنع نشوء جنات رقمية.

٦. يجب إقرار الأمن القومي بتحقيق الأمن السيبراني كجزء هام من مهامه القومية.

٧. إنشاء آلية ونظام واضح وفعّال مسؤول عن مراكز للسلامة المعلوماتية وطوارئ الاتصال.

٨. تدريب وتأهيل وحدات عسكرية أمنية خاصة يمكنها مراقبة البنى التحتية للاتصالات بحيث تقوم بتحديد المخاطر المحتملة وإزالتها.

قائمة المراجع:

المراجع العربية

الفتلاوي أحمد عبيس نعمة "الهجمات السيبرانية :"مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر ."مجلة المحقق الحلي للعلوم القانونية والسياسية.

ايفانز فراهام، بويلهام جيفري .قاموس بتغوين للعلاقات الدولية .ت :مركز الخليج للأبحاث الإمارات العربية المتحدة : مركز الخليج للأبحاث .2004

جبور على الأشقر السيبرانية هاجس العصر، بيروت :جامعة الدول العربية -المركز العربي للبحوث القانونية والقضائية، .2016

المستشار :صالح بن علي بن عبدالرحمن الربيعة، الأمن الرقمي وحماية المستخدم من مخاطر الانترنت، هيئة الاتصالات وتقنية المعلومات .

كتاب رامي متولي القاضي، مكافحة الجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠١١م.

أسامة أحمد المناعسة، جلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، الطبعة الأولى، دار الثقافة للنشر

والتوزيع، ٢٠١٠م.

جلال ثروت، قانون العقوبات، القسم العام، الدار الجامعية، بيروت، غير متضمن سنة النشر.1996

عبد القادر جرادة، مبادئ قانون العقوبات الفلسطيني، الجريمة والمجرم، المجلد الأول، مكتبة أفاق، غزة، ٢٠١٠م.

عادل عبد الصاد، "الفضاء الإلكتروني والرأي العام :تغير المجتمع والأدوات والتأثير "، المركز العربي لبحاث الفضاء الإلكتروني :قضايا استراتيجية، 2013، العدد.2459

علي جبار الحسيناوي ,جرائم الحاسوب والأنترنت، داراليازوري العلمية للنشر والتوزيع، عمان، .2009

أيسر أنور على، أمال عبد الرحيم عثمان، أصول علمي الأجرام والعقاب، الجزء الأول في علم الأجرام، غير متضمن دار النشر، 1996م.

الجريمة السيبرانية والإيقاع الإجرامي التقليدي بالضحايا، دراسة شاملة عن الجريمة السيبرانية ، مكتب الأمم المتحدة المعني بالمخدرات والجريمة, مسودة شباط / فبراير ،٢٠١٣م .

محمود عزت، الفضاء السيبراني وتحديات الأمن المعلوماتي العربي، المجلة العربية العدد 498، أبريل .2018

حسن بن علي العجمي، الثورة الصناعية الرابعة وتغييرات الحياة الإنسانية، المجلة العربية العدد 498، إبريل .2018

سمير سعدون مصطفي، محمود خضر سلمان، حسن كريم عبد الرحمن، الجريمة الالكترونية عبر الانترنيت أثرها وسبل مواجهتها، مجلة التقني، المجلد ٢، الإصدار ٩، ٢٠١١.

الهيئة الوطنية للأمن السيبراني National Cybersecurity Authority ، الضوابط الأساسية للأمن السيبراني ، Essential Cybersecurity Controls, (ECC- ١ : ٢٠١٨) ،إشارة المشاركة ، تصنيف الوثيقة: غير مصنف .

المراجع الأجنبية:

Ivanov Anton, Orkhan Mamedov. The Return of Mamba Ransomware Secure list - Information about Viruses, Hackers and Spam. N.p., 09 Aug. 2017. Web. 13 Sept. 2017.

https://securelist.com/thereturn-ofmamba-ransomware/79403

: Ebert Hannes and Maurer Tim . " Cyber Security" oxfordbibliographies LAST MODIFIED: 11 JANUARY ,2017.

Lehto Mali Maithaanmak Pekka Cyber Scurity: Analytics, Techirvology and Automation, Switzerland : Springer International Publishing 2015

ValerianoBrandon and C. Maluess Ryan," international relations theory and Cyber Security threats conflicts and ethics in an Emerrent Domain in an emergen

https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-ar.pdf, International Telecommunication --union-- (ITU)

M.A. Saeed, "Cyber Security and Data Privacy Law in Saudi Arabia, Financier Worldwide, April 2015,

.2018p27,,International Telecommunication Union, Global Cybersecurity Index

Arab News (2016), 'Cybercrime hit 6.5m in Kingdom last year', 11-

August 2016, /967966/saudi-arabia

قوانين:

نظام مكافحة جرائم المعلوماتية السعودي رقم م17/، لسنة 1428هـ.

القانون الأمريكي رقم ١٢١٣ لسنة 1986م الخاص بمواجهة جرائم الكمبيوتر.

مقالات ودراسات:

دراسة بحثية بعنوان "الجرائم الالكترونية "للباحثة إسراء مرعي.

عزة مغازي، قانون الجريمة الإلكترونية التورنت يحملك إلى طرة، مقال منشور على موقع المنصة بتاريخ ٢٠١٦/٢/٤م على الرابط التالي : ttps://almanassa.com/ar/storyh/١٠١٩.

إجراءات لتفادي مخاطر تزايد الهجمات الالكترونية التي تستهدف دول الخليج العربي، مقال منشور على موقع جريدة مكة، تاريخ النشر ٢٠١٦/٠٦/٠١ على الرابط: /http://makkahnewspaper.com/article/١٤٧٨٧

عبدالله بن فازع القرني، مواجهة جرائم الإنترنت :نحو إستراتيجية أمنية - مجتمعية متكاملة، مقال منشور على موقع جريدة الرياض.

احصائيات صادمة وغريبة عن جرائم الأمن المعلوماتي، دراسة مقدمة من طرف موقع أرقام ديجيتال بتاريخ 25/10/2015متوفرة على موقع: 11/2/2017 : http://digital.argaam.com/article/detail/112326

cyber security economy predictions 2017-2021,cybersecurity ventures2016

ورقة عمل للمستشار القانوني صالح الربيعة بعنوان الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت http://cutt.us/ftcVd