Journal of University Studies for inclusive Research
Vol.6, Issue 10 (2021), 1856–1873
USRIJ Pvt. Ltd.,

جهود المملكة العربية السعودية في مكافحة جرائم الأمن السيبراني و الحماية منها

المهندس : سعد ناصر ال عزام

القانون

الجامعة السعودية الالكترونية \ المملكة العربية السعودية

snazzam.199@gmail.com

الملخص :

هدفت هذه الدراسة الى التعرف على تعد الجرائم الإلكترونية من أهم الجرائم الإلكترونية الضارة على جميع المستويات في الدولة ، حيث يمكن أن تؤدي إلى ضياع حقوق الملكية الفكرية والمعلومات التجارية التنافسية وغيرها من المجالات التي تتعرض لهجمات إلكترونية.

الأمن السيبراني هو مجموعة من الوسائل التقنية والتكنولوجية التي يمكن من خلالها حماية الشبكات والأجهزة والبرامج والبيانات من الهجمات السيبرانية الضارة والوصول غير المصرح به إلى المعلومات والبيانات المهمة سواء للأفراد أو الحكومات.

تُعرف الهيئة السعودية للاتصالات والمعلومات بأنها من أهم الهيئات في المملكة العربية السعودية التي تعنى بالجرائم الإلكترونية. تُعرَّف الجرائم الإلكترونية على أنها سلوك غير قانوني أو غير أخلاقي أو غير مصرح به يتعلق بشبكات المعلومات العالمية. إنها جرائم العصر الرقمي التي تمس الثقة والمال والمعرفة والسمعة وكلها تنتقل عبر الإنترنت والتقنيات الحديثة، تعد جريمة السب والسب والاعتداء على أموال البنوك والاحتيال من أبرز الجرائم الإلكترونية في القانون السعودي.

من أهداف المملكة العربية السعودية لرؤية 2030 تطوير البنية التحتية الرقمية في المملكة العربية السعودية من خلال إبراز الشراكات بين القطاعين العام والخاص كوسيلة لتطوير قطاع الاتصالات وتكنولوجيا المعلومات في المملكة. لذلك اتخذت المملكة العربية السعودية عددًا من الخطوات في مجال الأمن السيبراني ، من أهمها إنشاء هيئة وطنية يتم من خلالها مكافحة الجرائم الإلكترونية ومكافحتها في المملكة العربية السعودية.

الكلمات الدالة : الجرائم السيبرانية ، الهجمات الإلكترونية ، تقنية المعلومات ، نظم المعلومات.

USRIJ Journal of University Studies for Inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة

The Efforts Of The Kingdom Of Saudi Arabia In Fighting Cyber Security Crimes And Protecting Them

Abstract

Cybercrime is one of the most important harmful cybercrimes at all levels in the country, as it can lead to the loss of intellectual property rights, competitive commercial information, and other areas that are subject to cyber-attacks.

Cyber security is a set of technical and technological means through which networks, devices, programs and data can be protected from harmful cyber-attacks and unauthorized access to information and important data whether for individuals or governments.

The Saudi Communications and Information Authority is known as one of the most important bodies in the Kingdom of Saudi Arabia that is concerned with cybercrime. Cybercrime is defined as unlawful, unethical or unauthorized behavior related to global information networks. They are crimes of the digital age that affect trust and money, knowledge, and reputation and all of which are channeled through the Internet and modern technologies.

The crime of insulting and cursing, attacking bank funds, and fraud are among the most prominent cybercrimes in the Saudi law.

One of the objectives of the Kingdom of Saudi Arabia for 2030 vision is to develop the digital infrastructure in the Kingdom of Saudi Arabia by highlighting the partnerships between the public and private sectors as a means to develop the telecommunications and information technology sector in the Kingdom. Therefore, the Kingdom of Saudi Arabia has taken a number of steps in the field of cyber security, the most important of which, is the establishment of the national authority through which cybercrimes are fought and combated in the Kingdom of Saudi Arabia .

Keywords: Cybercrime , Cyber-attacks , Information technology , Information systems

مقدمة الدراسة:

إن فكرة التقدم التكنولوجي التي يشهدها المجتمع في العصر الحديث قد ساهمت بصورة كبيرة في تغيير ملامح المجتمعات البشرية بشكل ملموس ، و تعرضت العديد من جوانب المجتمع و مجالاته إلى تغييرات بالجملة نتيجة التطورات التكنلوجية الرهيبة التي أحدثاها وسائل الاتصال التكنولوجي الحديث فعلى سبيل المثال حلت الرسائل الإلكترونية محل الرسائل المكتوبة بخط إلبد ، و تحولت المجالس الأسرية التي تجمع العائلات إلى غرف دردشة على مجموعات وسائل التواصل الاجتماعي من خلال الفيس بوك ، و الواتس أب ، و لم يعد هناك ضرورة من أجل سفر الأصدقاء لرؤية بعضهم البعض ، خاصة أن ثورة الاتصالات و المعلومات التي يشهدها العصر الحالي فرضت ظهور ما يسمي " الفضاء السيبراني أو الإلكتروني " الذي يتضمن عدداً لا نهائي من المجموعات و المجتمعات الافتراضية ، بداية من غرفة الدردشة و مجموعات الفيس بوك و الواتس أب و المجموعات البريدية إلى اتساع مساحات الإنترنت في حياة مجتمعنا إلبومي ، و لم يعد عالم الإنترنت فقط عالم افتراضي بل اصبح **عالم واقعي موازي لحياتنا إلبومية** [1].

و بالرغم من الإيجابيات العديدة التي يقدمها عالم الإنترنت للبشرية للأفراد و المجتمعات و الدول إلا أنه في نفس يطرح علينا عالم الإنترنت مجموعة من المخاطر و الافخاخ ، ففي كل زاوية في عالم الإنترنت توجد مخاطر عديدة من ابتزاز و قرصنة و سرقات و سطو عل الحسابات البنكية ، و هجوم على المعلومات و سرقتها أو تدميرها أو تغييرها ، و غيرها من بصور الانحرافات و الجرائم التي تمارس من خلال الإنترنت ، و أصبح هناك حديث طويل على أن الفضاء السيبراني أصبح فضاء غير أمن بمعنى أن الإنترنت اصبح سهل لجماعات كثيرة منتجة للجرائم و الانحرافات الواقعية ، حيث أثبتت عدد من التقارير أن حوإلى نصف مليون شخص قد تعرض للهجوم عبر الفضاء الإلكتروني ، و أن هناك الألف الجرائم و الانحرافات التي يمارسها بعض المستخدمين كل دقيقة ضد ضحايا من الأفراد و الجماعات و الشركات و الدول [2].

و يعتبر الأمن الركيزة الأساسية للمجتمع ، بحيث لا يمكن تصور نمو أي نشاط إلا من خلال تحقق الأمن سواء كان على المستوى التقني أو القانوني ، خاصة بعد بروز الفضاء السيبراني حيث تحول الأمن مع بروز مجتمع المعلومات و الفضاء السيبراني إلى واحد من أهم قطاعات الخدمات في المجتمع التي تشكل قيمة مضافة و دعامة أساسية لأنشطة الحكومات و الأفراد على حد سواء ، حيث أصبحت الجريمة السيبرانية لا تقف فقط عند حدود الإساءة للأفراد بل تعدت إلى تعريض سلامة الدول و الحكومات للخطر ، الأمر الذي زاد من تعقيد و صعوبة فكرة " الأمن السيبراني " و أصبح من الضروري الوصول إلى حلول مقترحة يمكن من خلالها وضع حدود لفكرة الجريمة السيبرانية و خطورتها على المجتمع [3].

---

[1]) خالد كاظم أبو دوح ، الأمن السيبراني للدول و الأفراد ، المجلة العربية ، العدد 398 ، الرياض ، ، 2018، ص 1.

[2]) خالد كاظم أبو دوح ، الأمن السيبراني للدول و الأفراد ، مرجع سابق ، ص 2.

[3]) سماح عبد الصبور ، الصراع السيبراني ، مجلة السياسة الدولية ، مؤسسة الأهرام ، 2017 ، ص 17.

و المملكة العربية السعودية تحتل المركز التاسع عالمياً في عدد الهجمات الإلكترونية التي تتعرض لها ، حتي أصبح الأمر مقلق بشكل كبير للمتخصصين في مجال الأمن الإلكتروني في المملكة العربية السعودية ، و من أبرز الحوادث التي تعرضت لها المملكة العربية السعودية تلك الهجمات التي تعرضت لها شركة أرامكو السعودية المملوكة للدولة في عام 2012 م و عطلت نشاط الشركة لمدة شهر ، و أشير إلى هذه الهجوم بأنه أكبر اختراق إلكتروني في التاريخ ، و تسببت هذه البرمجيات الخبيثة التي استخدمت في الهجوم إلى حدوث خلل مرة أخرى في نظام الشركة في نوفمبر عام 2016 و يناير عام 2017 م ، و ذلك بذلك المملكة العربية السعودية العديد من الجهود في مجال مكافحة جرائم الأمن السيبراني من حيث سن نظام الجرائم المعلوماتية ، و سن نظام التعاملات الإلكترونية ، و إنشاء الهيئة السعودية للأمن السيبراني ، و غيرها من الاتفاقيات الدولية التي انضمت إليها المملكة العربية السعودية [1]، و ذللك سوف نحاول من خلال هذه الدراسة إلقاء الضوء على جهود المملكة العربية السعودية في مكافحة جرائم الأمن السيبراني و الحماية منها.

مشكلة الدراسة و تساؤلاتها:

تعد الجرائم السيبرانية من أهم الجرائم الإلكترونية الضارة على كافة المستويات في الدولة ، حيث يمكن أن تؤدي إلى فقدان حقوق الملكة الفكرية ، و المعلومات التجارية التنافسية ، و غيرها من المجالات التي تكون محل للهجمات السيبرانية ، و المملكة العربية السعودية ليست بعيدة عن كل الهجمات السيبرانية ، حيث تعرضت المملكة العربية السعودية للعديد من الهجمات السيبرانية الخطيرة التي أثرت علىها في مختلف المجالات ، الأمر الذي فرض علىها ضرورة بذل جهود إضافية من اجل مكافحة هذه الجرائم من خلال سن العديد من التشريعات التي يمكن من خلالها وضع أسس للأمن السيبراني في المملكة العربية السعودية ، بالإضافة إلى إنشاء هيئة قومية تهدف بصورة أساسية إلى وضع القواعد القانونية التي يمكن من خلالها مواجهة الجرائم السيبرانية ، و لذلك يمكن القول أن مشكلة الدراسة تتمثل في محاولة الإجابة عن السؤال الرئيسي التإلى:

ما هي جهود المملكة العربية السعودية في مكافحة جرائم الأمن السيبراني؟

و يتفرع من السؤال الرئيسي السابق عدد من التساؤلات الفرعية التإلية:

- ما هو الأمن السيبراني ؟
- ما هي مجالات تطبيق الأمن السيبراني؟
- ما هو مفهوم الجرائم السيبرانية ؟
- ما هي الجرائم السيبرانية في النظام السعودي؟
- ما هي الأنظمة التي وضعتها المملكة العربية السعودية من أجل مكافحة الجرائم السيبرانية ؟
- ما هو دور هيئة الأمن السيبراني السعودية في مكافحة جرائم الأمن السيبراني؟

[1]) عبد الرحمن عاطف أبو زيد ، الأمن السيبراني في الوطن العربي ، المركز العربي للبحوث و الدراسات ، العدد 48 ، 2019 ، ص 56.

أهداف الدراسة: تهدف الدراسة إلى تحقيق الاتي:

- التعرف على مفهوم الأمن السيبراني .
- التعرف على مجالات تطبيق الأمن السيبراني.
- إلقاء الضوء على مفهوم الجرائم السيبرانية .
- إلقاء الضوء على الجرائم السيبرانية في النظام السعودي.
- الوقوف على الأنظمة التي وضعتها المملكة العربية السعودية من أجل مكافحة الجرائم السيبرانية .
- إبراز دور هيئة الأمن السيبراني السعودية في مكافحة جرائم الأمن السيبراني.

أهمية الدراسة:

تتنبع أهمية هذه الدراسة في محاولة لإثراء الدراسات والبحوث التي أجريت في مجال جهود المملكة العربية السعودية في مكافحة جرائم الأمن السيبراني ، والتي تعد قليلة نوع ما في الوطن العربي، ويمكن تحديد جوانب أهمية الدراسة من المساهمة والإضافة المتوقعة منها ، كما يلي:

أولاً: الأهمية النظرية:

1- تتمثل أهمية العلمية للدراسة في أن هذا الموضوع يلقي الضوء على موضوع جديد فرضه ضرورة مواجهة المملكة العربية السعودية للهجات الإلكترونية ، ولذلك يسعى الباحث أن تكون هذه الدراسة الباب الواسع أمام الدارسين والباحثين للخوض في أغمار جهود المملكة العربية السعودية لمكافحة جرائم الأمن السيبراني.

2- سيتم إثراء هذه الدراسة بالعديد من الدراسات التي تحدثت عن الموضوع بشكل تفصيلي، والاستفادة من الجهات البحثية العلمية في الدراسات الأكاديمية، خصوصاً في مجال دور المملكة العربية السعودية في مكافحة جرائم الأمن السيبراني ، و لذلك يرغب الباحث في أن تكون هذه الدراسة مرجعاً مهماً للباحثين والدراسين.

ثانياً: الأهمية التطبيقية:

1- يأمل الباحث في أن تسهم نتائج الدراسة في زيادة الاهتمام بمجال الجرائم السيبرانية في النظام السعودي ، والوقوف على دور الأنظمة السعودية في مكافحة الجريمة السيبرانية.

2- تكمن أهمية الدراسة في التعرف على جهود المملكة العربية السعودية في مكافحة الجرائم السيبرانية.

مصطلحات الدراسة:

الأمن السيبراني.

" مجموعة من الوسائل التقنية و الإدارية و التكنولوجية التي يمكن من خلالها حماية الشبكات و الأجهزة و البرامج و البيانات من الهجمات الضارة و الوصول الغير مصرح به للمعلومات و بيانات هامة سواء بالنسبة للأفراد أو الحكومات ، و لذلك يعتبر الأمن السيبراني عبارة عن تدابير هدفها التقليل من مخاطر الهجمات السيبرانية [1].

1- الجرائم السيبرانية.

" أنشطة غير مرخصة من قبل القانون ، اعدت بشكل أساسي إلى تعطيل نظم المعلومات أو الاتصالات أو الشبكات و البنية التحتية المادية أو الافتراضية التي تتحكم في أجهزة الكمبيوتر و أنظمة المعلومات ، أي أن هذه الهجمات السيبرانية تركز على إضعاف السرية و النزاهة و التوافر التي تقدمها هذه الشبكات الإلكترونية للمستخدمين ، و من أمثلتها سرقة البيانات الشخصية للأفراد ، و انتهاك نزاهة بيانات معلومات المصارف و البنوك[2].

المبحث الأول: ماهية الأمن السيبراني.

سوف نتناول في هذا المبحث ماهية الأمن السيبراني من خلال مطلبين ، نوضح في المطلب الأول مفهوم الأمن السيبراني ، و نتناول في المطلب الثاني مجال تطبيق الأمن السيبراني .

المطلب الأول: مفهوم الأمن السيبراني.

أصبح الأمن السيبراني من القضايا الهامة على المستوى الدولي ، و صنفت العديد من الدول مسائل الدفاع السيبراني و الأمن السيبراني كأولوية للدفاع الوطني ، و أعلنت أكثر من 130 دولة حول العالم عن تخصيص أقسام و سيناريوهات خاصة للحرب السيبرانية التي قدد تتعرض لها دولها ، و تضاعفت الجهود لمواجهة الجرائم الإلكترونية و الاحتيال الإلكترونية و غيرها من الجرائم السيبرانية ، و أصبحت سياسات الأمن السيبراني الوطني تعتمد على خمس ركائز أساسية و هي[3] :

- تطوير استراتيجية الأمن السيبراني لحماية البنية التحتية للمعلومات.
- إنشار تعاون وطني بين الحكومة و مجتمع المعلومات و الاتصالات من أجل وضع حائط دفاع قوي ضد الهجمات الإلكترونية.
- ردع الجريمة السيبرانية.
- خلق قدرات وطنية قادرة على إدارة حوادث الحاسب الإلى
- تحفيز ثقافة وطنية للأمن السيبراني.
- نشر ثقافة الأمن السيبراني على مستوى واسع بين المواطنين و الجماعات و الشركات.

---

[1]) سماح عبد الصبور ، الصراع السيبراني ، مرجع سابق ، ص 18.

[2]) علم الدين بانقا، مخاطر الهجمات الإلكترونية و أثارها الاقتصادية ، المعهد العربي للتخطيط " دراسات تنموية " ، العدد 63 ، 2009 ، ص 14.

[3]) خالد كاظم أبو دوج ، الأمن السيبراني للدول و الأفراد ، مرجع سابق ، ص 3.

و لذلك قامت المملكة العربية السعودية باتخاذ عدد من الخطوات التاريخية من أجل حماية المجتمع السعودي من الهجمات السيبرانية، و صدر أمر ملكي بإنشاء هيئة تسمى " الهيئة الوطنية للأمن السيبراني " ترتبط بمقام خادم الحرمين الشريفين ، و تقوم الهيئة بالاتي[1]:

- حماية مصالح المملكة العربية السعودية الحيوية من الهجمات السيبرانية .
- كما تسعى الهيئة بشكل أساسي إلى تعزيز الأمن السيبراني في المملكة العربية السعودية و حماية أمنها الوطني و البنى التحتية الحساسة فيها .
- تعمل الهيئة على سن الأنظمة و التشريعات التي يمكن من خلالها مواجهة الهجمات السيبرانية.
- توحيد الممارسات في سبيل ضمان تطبيق الأنظمة الحرجة للاتصالات و تقنية المعلومات .
- الحفاظ على سرية و خصوصية و جاهزية تكامل البيانات و المعلومات في المملكة العربية السعودية.

الأمن السيبراني هو مجموعة من الوسائل التقنية و يمكن القول أن مصطلح الأمن السيبراني ظهر في أواخر هذا العصر من الكلمة اللاتينية " Cyber" و معناها " الفضاء المعلوماتي " و هو تعبير شامل لجميع الخدمات التي يمكن من خلالها حفظ البيانات و المعلومات و البرمجيات و غيرها من الأمور التي تتم من خلال شبكة الإنترنت من أي هجمات إلكترونية قد تتعرض لها من خلال شبكات الحاسب و الاتصالات و الإنترنت، هناك العديد من التعريفات قد وردت بشأن الأمن السيبراني و من أهمها الاتي:

- الإدارية و التكنولوجية التي يمكن من خلالها حماية الشبكات و الأجهزة و البرامج و البيانات من الهجمات الضارة و الوصول الغير مصرح به للمعلومات و بيانات هامة سواء بالنسبة للأفراد أو الحكومات ، و لذلك يعتبر الأمن السيبراني عبارة عن تدابير هدفها التقليل من مخاطر الهجمات السيبرانية [2].
- يعرف الأمن السيبراني بالنسبة للأفراد بأنه شكل من أشكال التأمين الأساسية التي يقوم بها الفرد حفاظاً على معلوماته الشخصية ، فمثلما يحرص الفرد على تأمين الأبواب و النوافذ في منزله قبل البدء في رحلة سفر إلى الخارج ، فأنه يتخذ أيضاً كافة الإجراءات و التدابير الشخصية التي ترفع من أمنه السيبراني على شبكة الإنترنت و ذلك من خلال:

- حرص مستخدم الإنترنت على استخدام المتصفحات الإلكترونية الأكثر أماناً.
- وضع مستخدم الإنترنت كلمات مرور قوية لحمايه بياناته الشخصية، و يقوم بتغييرها بشكل مستمر كل ثلاثة أشهر، فضلاً عن دوره في عدم مشاركتها مع أي شخص أخر.
- حرص مستخدم الإنترنت على التحديث المستمر لبرامج التصفح من خلال مواقع موثقة.
- اعتماد مستخدم الإنترنت على إعدادات خصوصية قوية التي تقلل بقدر المستطاع من نشر المعلومات الشخصية.
- حرص مستخدم الإنترنت على القيم الأخلاقية عبر الفضاء السيبراني ، و عدم التعامل معه على انه مجال متحرر خالي من الأطر الأخلاقية[3].

---

[1]) هيئة تحرير المجلة الدبلوماسية ، الأمن السيبراني ، مجلة الدبلوماسي ، معهد الأمير سعود الفيصل للدراسات الدبلوماسية ، العدد 90 ، 2018 ، ص 10.

[2]) ، سماح عبد الصبور ، الصراع السيبراني ، مرجع سابق ، ص 18.

[3]) خالد كاظم أبو دوح ، الأمن السيبراني للدول و الأفراد ، مرجع سابق ، ص 4.

- يعرف الأمن السيبراني بأنه مجموعة من الأطر القانونية و التنظيمية ، و كافة آليات حماية الوسائل التقنية و التكنولوجية التي تهدف إلى حماية الفضاء السيبراني للدولة ، مع التركيز على ضمان توافر أنظمة المعلومات ، و تدعيم الخصوصية ، و حماية سرية المعلومات الشخصية ، و غيرها من الإجراءات التي يمكن من خلالها حماية المواطنين و المستهلكين من مخاطر الفضاء السيبراني [1].

يتضح من هذه التعريفات أن الأمن السيبراني بهدف إلى تحقيق الاتي[2]:

(أ) تأمين البني التحتية لأمن المعلومات و البيانات الخاصة بالمواطنين ، و ذلك من خلال وضع حماية قوية للبيانات و المعلومات المتعلقة بالمواطنين و حفظها في مكان أمن ، بالإضافة إلى ضرورة وضع الأجهزة الإلكترونية الضرورية بعيداً عن أي مجال من مجالات العبث أو الاختراق أو التدمير لتوفير الحماية اللازمة لهم.

(ب) حماية شبكة المعلومات و الاتصالات التي تلعب دور كبير في تدفق خط سير البيانات و المعلومات من الدولة إلى المواطنين و العكس من المواطنين إلى الدولة ، حيث أنه إذا تعرض هذه الشبكة لأي نوع من أنواع الضرر فأنه سوف تؤثر بصرة كبيرة على قطع الاتصالات و توقف سير العمل و توقف الخدمات بين المواطنين و الدولة .

(ت) حماية شبكات المعلومات و الاتصالات من أي هجوم قد تتعرض له سواء تقني أو تكتكي ، و في حالة التعرض للهجوم يكون هدف الأمن السيبراني التعرف على طبيعة المهاجم و محاولة وضع حد للهجوم الذي يقوم به من خلال أساليب علمية و تقنية تقف أمام الهجمات التي قد تتعرض لها شبكات المعلومات و البيانات في المستقبل.

(ث) من أهم أهداف الأمن السيبراني تشفير كافة التعاملات الإلكترونية التي تتم بواسطة المواطنين و الدولة ، لأن التشفير من أهم أساليب الحماية التي يتم من خلالها منع العبث بسهولة في البيانات و التطبيقات الإلكترونية .

المطلب الثاني: مجال الأمن السيبراني.

إن الأمن السيبراني يرتبط بالعديد من المجالات في المجتمع التي تحتاج إلا نوع من الحماية ضد الهجمات الإلكترونية سواء كانت اقتصادية أو سياسية أو عسكرية أو غيرها ، و يمكن القول أن أهم مجالات الأمن السيبراني تتمثل في الاتي:

(1) المجال العسكري: يعد المجال العسكري من أهم المجالات التي تحظى بحماية الأمن السيبراني ، و يرجع ذلك إلى أن أغلب القوات العسكرية في الوقت الحالي أصبحت تعتمد على الفضاء الإلكتروني في تبادل المعلومات ، و إعطاء الأوامر العسكرية ، فضلاً عن اعتماد الأجهزة العسكرية على شبكات الإنترنت في إصابة الأهداف عن بعد و تدميرها ، و هذه المزايا العديد التي تقدمها شبكات الإنترنت للأجهزة العسكرية في مختلف المجتمعات قد تتحول إلى نقطة ضعف إذا لم تتمكن تلك الشبكات الإلكترونية التي تعتمد عليها مؤمنة بشكل واضح من أي اختراق خارجي قد يتسبب في شن هجمات إلكترونية ضدها مما يؤدي إلى تدمير قواعد البيانات العسكرية ، و تعطيل شبكات الحاسب الآلي التي تربط بين مقر القوات العسكرية و الجنود في أرض الواقع ، كما يمكن من خلال هذه الهجمات السيبرانية شل أنظمة الدفاع العسكري للمجتمع و جعلها غير قادرة على القيام بوظائفها ،

[1]) خالد كاظم أبو دوح ، الأمن السيبراني للدول و الأفراد ، مرجع سابق ، ص 3.

[2]) جوهر الجموسي، الافتراضي و الثورة ، المركز العربي للأبحاث و الدراسات السياسية ، بيروت ، 2016 ، ص 120.

و لذلك من الضروري أن يشمل الأمن السيبراني المجال العسكري بكافة أجهزته الأمنية و الاستخباراتية و العسكرية من الأمثلة العربية الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية الذي يعمل على حماية المملكة من كافة الهجمات السيبرانية التي قد تتعرض لها [1] .

(2) المجال الاقتصادي: من أهم المجالات التي ترتبط بالأمن السيبراني، و ينقسم هذا المجال إلى بعدين رئيسين و هم [2]:

- البعد الأول يتعلق بصناعة تكنولوجيا المعلومات و الاتصالات " ICT" و ذلك من خلال تطوير أجهزة و برمجيات و إنتاجها و خدمات أخرى في مجال التكنولوجيا.
- البعد الثاني يتعلق بمجال التجارة الإلكترونية و ذلك من خلال الأسواق العديدة التي يشهدها العصر الحالي على شبكات الإنترنت.

فالعالم في العصر الحديث أصبح يعتمد في تعاملاته الاقتصادية على المعاملات المالية الإلكترونية، و باتت شبكات البنوك و البورصة و الأسواق الإلكترونية مرتبطة ببعضها البعض من خلال شبكات إلكترونية ، و لذلك أصبحت هذه الشبكات الإلكترونية هي الأساس للتطور الاقتصادي في نظام المعاملات المالية و الاقتصادية في مختلف دول العالم في القرن الحادي و العشرين ، و لذلك لابد أن يشمل الأمن السيبراني هذا المجال الاقتصادي لحمايته من أي هجمات سيبرانية قد تؤدي إلى تدمير اقتصاديات العديد من الدول [3].

(3) المجال السياسي: من الناحية السياسية تبذل العديد من الدول المزيد من الجهد من أجل حماية الوثائق السياسية الحساسة التي قد يشكل اختراقها أو الحصول عليها من خلال شبكات الإنترنت مشاكل كبيرة بين الدول و بعضها البعض ، كما أن كل الدول في العالم في الوقت الحالي تعتمد على شبكات الإنترنت في حملاتها الانتخابية و عرض بيانتها الشخصية للمواطنين من خلالها ، بالإضافة إلى ما سبق فإن شبكات الإنترنت تعد بيئة خصبة للاحتجاجات الإلكترونية ضد سياسات العديد من الدول ، و من أمثلة ذلك قيام الجيش الأمريكي بعمل حسابات وهمية بأسماء وهمية على شبكات التواصل الاجتماعي من أجل تقديم الدعم لرؤية الولايات المتحددة الأمريكية على مواقع التواصل الاجتماعي ، و يجب أن نشير أيضا إلى أن حماية المجال السياسي من الهجمات السيبرانية أمر مهم لمواجهة العمليات الإرهابية التي تشهدها العديد من المجتمعات في الوقت الحالي ضد الأنظمة السياسية التي تحكمها ، و لذلك كان لابد من توفير الأمن السيبراني لكافة المعلومات السياسية التي قد يستفيد منها العدو في المستقبل[4].

---

[1]) محمد الأمين البشري ، التحقيق في جرائم الحاسب الإلى ، بحث مقدم إلى مؤتمر القانون و الكمبيوتر و الإنترنت المنعقد في الفترة من 3/1 مايو / بكلية الشرية و القانون بدولة الإمارات ، 2000 ، ص 39.

[2]) عبد الرحمن عاطف أبو زيد ، الأمن السيبراني في الوطن العربي ، مرجع سابق ، ص 55.

[3]) عبد الفتاح بيومي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الإنترنت ، دار الكتب القانونية ، القاهرة ، 2007 ، ص 198.

[4]) هلالي أحمد ، اتفاقية بودابيست لمكافحة الجرائم المعلوماتية ، دار النهضة العربية ، القاهرة ، 2007 ، ص 129.

(4) المجال القانوني: هناك علاقة قوية بين التطور التكنولوجي الذي يشهده المجتمع في العصر الحديث و بين وضع القوانين المختلفة التي يمكن من خلالها مواكبة الجرائم المختلفة التي تشهدها مختلفة المجتمعات ، خاصة أن الهجمات السيبرانية في العديد من المجتمعات تفتقر إلى أطر قانونية تحكمها مثل صعوبة تحديد طبيعة الجريمة الإلكترونية ، و صعوبة تحديد هوية مرتكبي الجرائم الإلكترونية ، فضلاً أن الجرائم السيبرانية تفتقد للعديد من الحدود و التعاون بين الدول لمنعها ، و لذلك لابد من وضع القوانين الصارمة التي يمكن من خلالها وقف هذا الامتداد للجرائم السيبرانية[1].

(5) المجال الاجتماعي: من الطبيعي أن يرتبط الأمن السيبراني بالمجال الاجتماعي في المجتمعات ، فهناك حوالى 35 % من سكان العالم يستخدمون الإنترنت ، و العديد منهم يستخدم الإنترنت في التعبير عن تطلعاته في مختلف مجالات المجتمع السياسية أو الاقتصادية أو العالمية أو الثقافية ، و لذلك لابد من أن يوفر المجتمع الأمن السيبراني الذي يمكن من خلاله حماية أفكار الأفراد داخل المجتمع في مختلف المجالات ، فضلاً أن شبكة الإنترنت تتضمن العديد من الأمور التي تسبب الأضرار للمجتمع كأفكار الإرهاب ، و المواد الإباحية ، و الترويج للاتجار في الممنوعات ، و لذلك لابد من توفير المجتمع كافة سبل حماية أفكار أبناء المجتمع من هذه الأخطار.

المبحث الثاني: الجرائم السيبرانية

سوف نوضح في هذا المبحث الجرائم السيبرانية من خلال ثلاثة مطالب ، نوضح في المطلب الأول مفهوم الجريمة السيبرانية ، و نتناول في المطلب الثاني أنواع الجرائم السيبرانية ، و أخيراً نلقي الضوء في المطلب الثالث على الجرائم السيبرانية في النظام السعودي.

المطلب الأول: مفهوم الجريمة السيبرانية

- تعرف الجريمة السيبرانية بأنها أنشطة غير مرخصة من قبل القانون ، اعدت بشكل أساسي لتعطيل نظم المعلومات أو الاتصالات أو الشبكات و البنية التحتية المادية أو الافتراضية التي تتحكم في أجهزة الكمبيوتر و أنظمة المعلومات ، أي أن هذه الهجمات السيبرانية تركز على إضعاف السرية و النزاهة و التوافر التي تقدمها هذه الشبكات الإلكترونية للمستخدمين ، و من أمثلتها سرقة البيانات الشخصية للأفراد ، و انتهاك نزاهة بيانات معلومات المصارف و البنوك[2].
- تعرف الجريمة السيبرانية بأنها استخدام وسائل الاتصال و التكنولوجيا الحديثة في ممارسات غير مشروعة للقوانين تستهدف التحايل على أنظمة معالجة البيانات و المعلومات ، و ذلك من أجل كشف البيانات الحساسة لدى الدولة أو الأفراد أو الشركات و التأثير على سلامتها أو حتى إتلافها [3].
- تعرف الجريمة السيبرانية بأنها مجموعة من العمليات الغير القانونية التي تستهدف بصورة مباشرة الدخول بطريقة غير مشروعة إلى أجهزة الغير و شبكاتهم الإلكترونية ، و ذلك بقصد المساس بسرية محتوي هذه الشبكات و تعطيل قدراتها و كفاءتها للقيام بأعمالها ، أي أن الجريمة السيبرانية تعني الوصول بطريقة غير مشروعة إلى بيانات و معلومات من خلال ثغرات في نظام الحماية الخاص بالهدف [4].

---

[1]) هلالى أحمد ، اتفاقية بودابيست لمكافحة الجرائم المعلوماتية ، مرجع سابق ، ص 135.

[2]) علم الدين بانقا ، مخاطر الهجمات الإلكترونية و أثارها الاقتصادية ، المعهد العربي للتخطيط " دراسات تنموية " ، العدد 63 ، 2009 ، ص 14.

[3]) ليتيم فتحيه ، الأمن المعلوماتي للحكومة الإلكترونية و إرهاب القرصنة ، مرجع سابق ، ص 242.

[4]) زكريا محمود جميل ، ورقة في الجريمة المعلوماتية و أساليب التامين ، المؤتمر الدولي للأمن المعلومات الإلكترونية ، سلطنة عمان ، 2005 ، ص 147.

- تعرف هيئة الاتصالات و المعلومات السعودية الجرائم السيبرانية بأنها سلوك غير مشروع أو منافي للأخلاق أو غير مسموح به مرتبط بالشبكات المعلوماتية العالمية ، فهي جرائم العصر الرقمي التي تطال الثقة ، و المال ، و المعرفة ، و السمعة ، و هي كلها تنفذ من خلال شبكات الإنترنت و التقنيات الحديثة .[1]

و يتضح من هذه التعريفات أن الجرائم السيبرانية لها خصائص تتميز بها و لا تتوافر في الجرائم التقليدية ، و تتمثل هذه الخصائص في الاتي[2]:

- أنها جرائم ذات بعدي عالمي لا حدود جغرافية لها، ولذلك تعدد وسائلها و يبتكر المجرمين كل يوم وسائل حديثة لمواكبة عصر التطور التكنولوجي. وأنها جرائم صعبة الاكتشاف، حيث لا تترك أثر واضح يمكن من خلاله تعاقبها و الوصول إلى مرتكبها، فضلاً أن الضحية لا تكتشف وقوعها إلا بعد فترة من ارتكابها. جرائم سريعة الوقوع يصعب أن تترك أثر يسهل تعقبه ، و لذلك يغيب الدليل في العديد من الجرائم السيبرانية و يصعب إثباتها ، و يرجع ذلك إلى التقدم التكنولوجي الكبير في الوسائل التي يستخدمها مرتكبي هذه الجرائم. ويتمتع المجرم في هذه الجرائم بتقنية عالية و خبرة فائقة في مجال الاتصالات و الشبكة العنكبوتية ، و استخدام الكمبيوتر و التكنولوجيا المعاصرة. ترتبط هذه الجرائم بصورة كبيرة بالشبكات العنكبوتية ، حيث تعد شبكات الإنترنت هي المصدر الأساسي للمعلومات و البيانات التي تستهدفها الجرائم السيبرانية .

المطلب الثاني : أنوع الهجمات السيبرانية

هناك العديد من النماذج للجرائم و الهجمات السيبرانية و منها الاتي:

(أ) **تدمير الشركات المنافسة**: تمارس العديد من الشركات في السوق العالمية العديد من الهجمات السيبرانية على الشركات المنافسة ، و غالباً ما تكون هذه الهجمات من أجل سرقة الملكية الفكرية للشركات المستهدفة ، حيث تعتبر جريمة سرقة الملكية الفكرية من أعلى الجرائم السيبرانية تكلفة ، و ذلك بسبب عدم تمكن الشركة المخترقة من اكتشاف الاختراق إلا بعد عدة سنوات ، الأمر الذي يتيح للمجرم من استخدام ملكيتها الفكرية لفترة طويلة و إلحاق أضرار بها ، و من أمثلة هذه الجريمة السيبرانية نموذج سرقة الملكية الفكرية و المعلومات الخاصة لشركة " SOLAR WORLD AG" الألمانية بواسطة الشركات المنافسة الصينية ، حيث أعلنت السلطات الفيدرالية الأمريكية في مايو 2014 م الملاحقة القضائية لخمسة أشخاص صينين بتهمة التجسس و سرقة الأسرار التجارية و الاحتيال و القرصنة على 6 شركات أمريكية و من بيتهم هذه الشركة ، حيث تمت سرقة آلاف الإيميلات و الملفات الخاصة بالمدراء التنفيذيين خلال 13 هجوم سيبراني خبيث لمدة 8 سنوات دون أن تشعر هذه الشركات[3].

(ب) **تدمير المواقع الإلكترونية**: من الجرائم السيبرانية تدمير المواقع الإلكترونية من خلال ضخ مئات الألاف من الرسائل الإلكترونية من جهاز الحاسوب للشخص المعتدي إلى الموقع المراد تدميره ، و هناك العديد من الأسباب التي تسهل عملية تدمير الموقع منها ضعف الكلمات السرية المستخدمة ، حيث أن العديد من مستخدمي شبكات الإنترنت يستخدمون كلمات مرور ضعيفة يسهل مسرها و تخمينها من قبل المخترق ، و أيضاً من أسباب سهولة اختراق المواقع عدم وضع البرامج التي يمكن من خلالها حماية المواقع من الاختراق و التدمير ، فضلاً عن عدم قيام العديد من المستخدمين بالتحديثات المستمرة لبرامج الحماية [4].

---

[1]) صالح بن على الربيعة ، الأمن الرقمي و حماية المستخدم من مخاطر الإنترنت ، هيئة الاتصالات و تقنية المعلومات ، 2017 ، ص 9.

[2]) حسن طاهر داوود ، جرائم نظم المعلومات ، أكاديمية نايف العربية للعوم الأمنية ، الرياض ، 2000 ، ص 180.

[3]) علم الدين بانقا ، مخاطر الهجمات الإلكترونية و أثارها الاقتصادية ، مرجع سابق ، ص 19.

[4]) ليتيم فتحيه، الأمن المعلوماتي للحكومة الإلكترونية و إرهاب القرصنة ، مرجع سابق ، ص 246.

المطلب الثالث: الجرائم السيبرانية في النظام السعودي

نصت المادة الثالثة من نظام مكافحة الجرائم المعلوماتي السعودي على أشكال الجرائم السيبراني بالقول يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

1- التصنت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي دون مسوغ نظام صحيح أو التقاطه أو اعتراضه.

2- الدخول غير المشروع لتهديد شخص أو ابتزازه، لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعا.

3- الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.

4- المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها.

5- التشهير بالآخرين، وإلحاق الضرر بهم، عبر وسائل تقنيات المعلومات المختلفة.

و يتضح من هذا النص أن أهم الجرائم السيبرانية في النظام السعودي تتمثل في الاتي[1]:

(أ) جريمة السب و الشتم عبر الإنترنت: و يقصد بالشتم هو كل قبيح اعتاد الناس على قبحه و سوؤه ، و لذلك نجد العديد من المستخدمين لشبكات الإنترنت ما يستسهل سب الأخرين و يرجع ذلك إلى أن اغلب من يرتكب ذلك يختفي وراء أسباب وهميه فيأمن من العقاب ، فضلاً أن المتعاملين من خلال شبكة الأنترنت لا تحدهم حدود جغرافية معينة و لذلك يصعب تعقبهم قضائياً.

(ب) إفشاء الإسرار: حيث يمكن من خلال الحاسب الآلي الاعتداء على خصوصيات الأفراد و إفشاء أسرارهم ، و ذلك من خلال استخدام بيانات حقيقة بدون ترخيص .

(ت) الابتزاز و التهديد: و يتم ذلك من خلال تهديد المجني عليه بنشر أخباره أو صوره أو معلومات غير صحيحة عنه ، و يكون هذا التهديد مصاحب بطلب مبلغ مالي حتى لا ينشرها سواء كان المقابل مالي أو علاقة غير مشروعة.

(ث) جريمة التصنت: و ذلك من خلال استخدام برنامج في جهاز الشخص المعتدي عليه يمكن من خلاله الاطلاع و الاستماع إلى جميع المحادثات و المراسلات الصادرة من الشخص المعتدي عليه.

(ج) جريمة إساءة استخدام الهواتف النقالة: هذا النوع من الجرائم له العديد من الأثار الاجتماعية و النفسية على مستوى الأفراد نظراً لما يدخله في نفوس الأفراد من خوف .

(ح) التشهير بالأشخاص: أصبحت هذه الجريمة من ابرز الجرائم السيبرانية بل أنه يوجد مواقع تم تصميمها من أجل التشهير بالأشخاص و التسميع بهم ، و يتم ذلك من خلال البريد الإلكتروني أو شبكة الويب العالمية أو غرف المحادثات أي أن الشخص يقوم بالتشهير و إلحاق الضرر الأخرين من خلال وسائل المعلومات التقنية المختلفة.

(خ) الاحتيال المعلوماتي: تقع هذه الجريمة من خلال إساءة استعمال الحاسبات الآلية للتلاعب في نظام المعالجة الإلكترونية للبيانات و المعلومات للحصول على غير حق على أموال أو خدمات .

[1]) صالح بن على الربيعة ، الأمن الرقمي و حماية المستخدم من مخاطر الإنترنت ، مرجع سابق ، ص 50.

(د) جريمة السطو على البنوك: و يتم ذلك من خلال استخدام الجاني الحاسب الآلي للدخول على شبكة الأنترنت و الوصول بطريقة غير مشروعة إلى البنوك و المصارف و المؤسسات المالية ، و يقوم بتحويل الأموال من حسابات تلك البنوك الخاصة بالعملاء إلى حسابات أخرى و ذلك من خلال إدخال بيانات غير حقيقة أو تعديل و مسح بيانات موجودة بقصد اختلاس الأموال أو نقلها أو إتلافها.

(ذ) التحريض على الجريمة المعلوماتية : نصت المادة رقم (9) من نظام المعلومات و الاتصالات السعودي بانه يعاقب كل من حرض غيره أو ساعده أو اتفق معه على ارتكاب أي من الجرائم المنصوص عليها في هذا النظام إذا وقعت الجريمة بناء على هذا التحريض أو المساعدة أو الاتفاق ، بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها .

المبحث الثالث: جهود المملكة العربية السعودية في مكافحة الجرائم السيبرانية

سوف نتناول في هذا المبحث الجهود التي بذلت من المملكة العربية السعودية من اجل القضاء على الجرائم السيبرانية من خلال اربع مطالب ، نوضح في المطلب الأول سن نظام الجرائم المعلوماتية ، و نتناول في المطلب الثاني سن نظام التعاملات الإلكتروني ، و نتناول في المطلب الثالث إنشاء الهيئة السعودية للأمن السيبراني ، و أخيرا نوضح في المطلب الرابع الاتفاقيات الدولية التي انضمت إليها المملكة العربية السعودية.

المطلب الأول: سن نظام الجرائم المعلوماتية

تؤثر الجرائم المعلوماتية بصورة كبيرة على الدول إذا لم تتم مكافحتها بشكل فعال ، و يرجع ذلك إلى أن استفحال و انتشار هذا النوع من الجرائم دون ضوابط أو إجراءات سيؤثر بصورة سلبية على الدول خاصة في ظل توسع مستخدمي شبكة الإنترنت و أجهزة الحاسوب و الوسائل التكنولوجية لحديثة ، و في إطار الحد من خطورة هذه الجريمة سارعت العديد من الدلو العربية لوضع تشريعات خاصة بمكافحة الجريمة المعلوماتية و منها المملكة العربية السعودية التي أصدرت نظام مكافحة الجرائم المعلوماتية الصادر بالمرسوم الملكي رقم (17) بتاريخ 1428/3/18 هجرياً [1].

و نصت المادة الثانية من هذا النظام على الهدف من سنه بالقول (يهدف هذا النظام إلى الحد من وقوع الجرائم المعلوماتية ، و ذلك بتحديد هذه الجرائم و العقوبات المقرر لكل منها ، و بما يؤدي إلى ما يأتي:

- المساعدة على تحقيق الأمن المعلوماتي.
- حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الألية و الشبكات المعلوماتية.
- حمية المصلحة العامة ، و الأخلاق ، و الآداب العامة.
- حماية الاقتصاد الوطني.[2]

[1]) لورنس سعيد الحوامدة، الجرائم المعلوماتية ، بحث مقدم إلى جامعة طيبة ، كلية الحقوق ، المملكة العربية السعودية ، 2017، ص 26.

[2]) المادة رقم (2) من نظام الجرائم المعلوماتي السعودي.

المطلب الثاني: سن نظام التعاملات الإلكتروني

إن عصر المعلومات و التكنولوجيا فرض ضرورة حدوث تطورات في المعاملات التجارية ، و كان من أهم تلك التطورات ظهور العقود الإلكترونية في كافة فروع الحياة و منها التصرفات التجارية ، و تحتاج العقود الإلكترونية لتحقيق غايتها درجة كبيرة من الدقة و الوضوح من خلال وضع مجموعة من النظم و القواعد لتحكم التعاملات الإلكترونية ، و لذلك قامت المملكة العربية السعودية بوضع نظام التعاملات الإلكترونية السعودية رقم (18) الصادر في تاريخ 1428/3/8 هجرياً [1].

و أوضح هذا النظام أن التعاملات الإلكترونية هي أي تبادل أو تراسل أو تعاقد أو أي إجراء يبرم أو ينفذ بشكل كلي أو جزئي بوسيلة إلكترونية ، و أوضحت المادة الثانية من هذا النظام أنه يهدف إلى ضبط التعاملات و التوقيعات إلكترونية و تنظيمها ، و توفير إطار نظامي لها بما يؤدي إلى تحقيق ما يلي:

- إرساء قواعد نظامية موحدة لاستخدام التعاملات و التوقيعات الإلكترونية ، و تسهيل تطبيقها في القطاعين العام و الخاص بواسطة سجلات إلكترونية تعول عليها.
- إضفاء الثقة في صحة التعاملات و التوقيعات و السجلات الإلكترونية و سلامتها.
- تيسير استخدام التعاملات و التوقيعات الإلكترونية على الصعيدين المحلي و الدولي للاستفادة منها في جميع المجالات كالإجراءات الحكومية ، و التجارة ، و الطب ، و التعليم، و الدفع المالي الإلكتروني.
- إزالة العوائق أمام استخدام التعاملات و التوقيعات الإلكترونية.
- منع إساءة استخدام و الاحتيال في التعاملات و التوقيعات الإلكترونية[2].

المطلب الثالث: إنشاء الهيئة السعودية للأمن السيبراني

من أهدف رؤية المملكة العربية السعودية 2030 هي تطوير البنية التحتية الرقمية في المملكة العربية السعودية من خلال تسليط الضوء على الشركات ما بين القطاعين العام و الخاص كوسيلة لتطوير قطاع الاتصالات و تقنية المعلومات في المملكة ، و يعد الأمن السيبراني مكون أساسي من مكونات أي تحول رقمي و يرجع ذلك إلى أن حماية البيانات و البينة التحتية سيكون مصدر قلق كبير للحكومة و العامة و القطاع الخاص بسبب الهجمات السيبرانية التي تتعرض لها المملكة العربية السعودية ، الأمر الذي فرض ضرورة التعامل مع مثل هذه الهجمات من خلال إنشاء هيئة سعودية للأمن السيبراني [3].

و لذلك صدر امر ملكي بأنشاء هيئة تسمى " الهيئة الوطنية للأمن السيبراني " ترتبط بمقام خادم الحرمين الشريفين ، و تقوم الهيئة بالاتي و تقوم الهيئة بالاتي[4]:

- حماية مصالح المملكة العربية السعودية الحيوية من الهجمات السيبرانية .
- كما تسعى الهيئة بشكل أساسي إلى تعزيز الأمن السيبراني في المملكة العربية السعودية و حماية أمنها الوطني و البنى التحتية الحساسة فيها .
- تعمل الهيئة على سن الأنظمة و التشريعات التي يمكن من خلالها مواجهة الهجمات السيبرانية.
- توحيد الممارسات في سبيل ضمان تطبيق الأنظمة الحرجة للاتصالات و تقنية المعلومات .

---

[1]) محمد فواز مطابقة ، العقود الإلكترونية و البيئة الإلكترونية في النظام السعودي ، مكتبة جامعة خازان ، المملكة العربية السعودية ، ص 837.

[2]) المادة رقم (2) من نظام التعاملات الإلكترونية السعودي.

[3]) فؤاد الصلاحي ، الأمن السيبراني ، مجلة الدوحة ، وزارة الإعلام ، 2015 ، ص 129.

[4]) هيئة تحرير المجلة الدبلوماسية ، لأمن السيراني ، مجلة الدبلوماسي ، معهد الأمير سعود الفيصل للدراسات الدبلوماسية ، العدد 90 ، 2018 ، ص 10.

- الحفاظ على سرية و خصوصية و جاهزية تكامل البيانات و المعلومات في المملكة العربية السعودية.
- تحقيق التكامل بين أجهزة الدولة المعنية بذلك المجال مثل (المركز الوطني للأمن الإلكتروني في وزارة الداخلية ، و مركز التميز في جامعة الملك سعود ، و مركز الأمن السيبراني في مدينة الملك عبد العزيز للعلوم التقنية).

و يأتي في مقدمة أهداف و مهما الهيئة الوطنية للأمن السيبراني ما يلي:

- إعداد استراتيجية وطنية للأمن السيبراني.
- حماية البنية التحتية لأمن المعلومات في المملكة العربية السعودية.
- حفظ التعاملات الإلكترونية من الاختراق و سلامتها و سريتها.
- حماية و تأمين شبكة المعلومات الوطنية من أي هجوم إلكتروني سواء داخل المملكة العربية السعودية أو خارجها.
- استقطاب الكوادر الوطنية المؤهلة و الطموحة و تأهيلها و تمكينها.
- بناء الشراكات مع الجهات العامة و الخاصة و تحفيز الابتكار و الاستثمار في مجال الأمن السيبراني للإسهام في تحقيق نهضة تقنية تخدم مستقبل اقتصاد المملكة العربية السعودية [1].

و تم إنشاء كلية في تخصص الأمن السيبراني في المملكة العربية السعودية تختص بالأمن السيبراني و البرمجة و الذكاء الاصطناعي ، و يكمن الهدف من إنشاء هذه الكلية في تمكين الشباب و تحفيزهم في صناعة طاقات احترافية بإبداعات تقنية ذات قيمة عالية و ابتكارية في مختلف المجالات ، و تسعى الكلية إلى بناء و تأهيل قدرات وطنية شابه محترفة بأحدث الوسائل التقنية من أجل تحقيق رؤية المملكة العربية السعودية 2030م.

المطلب الرابع: الاتفاقيات الدولية التي انضمت إليها المملكة العربية السعودية

(1) الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: ء حيث صدر عن جامعة الدول العربية التي تعتبر المملكة العربي السعودية عضواً فيها اتفاقية حديثة تعتهم بمكافحة الجرائم المعلوماتية سميت " الاتفاقية العربية لمكافحة الجرائم المعلوماتية " ، حيث وافق على الاتفاقية مجلس وزراء الداخلية العرب بتاريخ 2010/12/21 م ، و دخلت الاتفاقية حيز التنفيذ بتاريخ 2010/2/7م بعد مصادقة الدول الأطراف عليها ، و صادقت عليها المملكة العربية السعودية في تاريخ 2010/12/21م ، و تعد هذه الاتفاقية نقطة نحول في التعاون العربي لمكافحة الجرائم السيبرانية ، حيث نصت الاتفاقية على التعاون العربي في مكافحة الجرائم المعلوماتية في العديد من المجالات منها (التعاون القضائي ، تبادل المعلومات ، تبادل الحبرات ، الاختصاص القضائي ، تسليم المجرمين ، المساعدة القضائية) و غيرها من الموضوعات ذات الصلة [2] ، و أوضحت المادة الثالثة من الاتفاقية مجالات تطبيقها بالقول (تنطبق الاتفاقية على جرائم تقنية المعلومات بهدف منعها و التحقيق فيها و ملاحقة مرتكبيها ، و ذلك في الحالات الأتية:

- ارتكبت في أكثر من دولة.
- ارتكبت في دولة و تم الإعداد أو التخطيط لها أو توجيهها أو الإشراف عليها في دولة أو دول أخرى.
- ارتكبت في دولة و ضلعت في ارتكابها جماعة إجرامية منظمة تمارس أنشطة في أكثر من دولة.
- ارتكبت في دولة و كانت لها أثار شديدة في دولة أو دول أخرى.

---

[1]) هيئة تحرير المجلة الدبلوماسية ، لأمن السيراني ، مرجع سابق ، ص 11.

[2]) لورنس سعيد الحوامدة ، الجرائم المعلوماتية ، مرجع سابق ، ص 29.

(2) اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية و الصادرة من الأمم المتحددة لعام 2000م : من أبرز اتفاقيات مكافحة الجرائم المنظمة عبر الوطنية و منها الجرائم السيبرانية ، و قد صادقت المملكة العربية السعودية على الاتفاقية عام 2005 م ، و صادقت على البروتوكولات الثلاثة المكملة للاتفاقية و ذلك في إطار تنفيذ ولايات برنامج الأمم المتحددة لمنع الجرائم و العدالة الجنائية ، و تهدف الاتفاقية إلى الاتي[1]:

- تشجع الاتفاقية بقوة الدول الأطراف على تيسير التعاون في العمل بين السلطات المركزية بسبل من بينها إقامة الشبكات الإقليمية أو استخدام الوسائط الافتراضية مثل تقنيات التداول عن طريق الفيديو، و تشدد على الأهمية الخاصة للتعاون في العمل بين السلطات المركزية من أجل استعراض تنفيذ الطلبات ومناقشة معوقات التعاون واستبانة حلول للتغلب على تلك التحديات.
- تحث الاتفاقية الدول الأطراف على أن تقوم بالتعاون مع مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة وغيره من الجهات، بتعزيز التدريب والمساعدة التقنية من أجل تسهيل التعاون الدولي في إطار الاتفاقية، ويشجِّع في هذا الصدد الدول الأطراف على إعطاء أولوية للجهود الرامية إلى تدعيم المعارف والقدرات لدى السلطات المركزية وسائر المؤسسات ذات الصلة، بما يشمل الجهود الرامية إلى المحافظة على سرية طلبات التعاون الدولي ومحتوياتها، إذا طلب منها ذلك.

- تشجع الاتفاقية الدول الأطراف على الاستفادة التامة على خير وجه من التكنولوجيات المتاحة لتيسير التعاون بين السلطات المركزية، بما يشمل الاستعانة بموارد الاتصال الحاسوبي المباشر المستحدثة على المستوى الوطني والأدوات المناسبة التي استحدثها مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة، مثل بوابة إدارة المعارف المعروفة باسم بوابة الموارد الإلكترونية والقوانين المتعلقة بالجريمة وأداة كتابة طلبات المساعدة القانونية المتبادلة، وإقامة شبكات افتراضية بين السلطات المركزية واستكشاف مدى إمكانية إقامة اتصالات إلكترونية آمنة.

[1]) لورنس سعيد الحوامدة ، الجرائم المعلوماتية ، مرجع سابق ، ص 29.

الخاتمة:

أولاً: أهم النتائج:

1- أن الأمن السيبراني هو مجموعة من الوسائل التقنية و التكنولوجية التي يمكن من خلالها حماية الشبكات و الأجهزة و البرامج و البيانات من الهجمات السيبرانية الضارة و الوصول الغير مصرح به للمعلومات و بيانات هامة سواء بالنسبة للأفراد أو الحكومات.

2- تعرف هيئة الاتصالات و المعلومات السعودية من أهم الهيئات في المملكة العربية السعودية التي تهتم بالجرائم الإلكترونية، و تعرف الجرائم السيبرانية بأنها سلوك غير مشروع أو منافي للأخلاق أو غير مسموح به المرتبط بالشبكات المعلوماتية العالمية ، فهي جرائم العصر الرقمي التي تطال الثقة ، و المال ، و المعرفة ، و السمعة ، و هي كلها تنفذ من خلال شبكات الإنترنت و التقنيات الحديثة.

3- جريمة السب و الشتم ، و الاعتداء على أموال البنوك ، و الاحتيال من أبرز الجرائم السيبرانية في النظام السعودي.

4- من أهدف رؤية المملكة العربية السعودية 2030 هي تطوير البنية التحتية الرقمية في المملكة العربية السعودية من خلال تسليط الضوء على الشراكات ما بين القطاعين العام و الخاص كوسيلة لتطوير قطاع الاتصالات و تقنية المعلومات في المملكة ، و لذلك اتبعت المملكة العربية السعودية عدد من الخطوات في مجال الأمن السيبراني من أهمها إنشاء الهيئة الوطنية التي يتم من خلالها مكافحة الجرائم السيبرانية في المملكة العربية السعودية.

ثانياً: أهم التوصيات:

- ضرورة إبرام العديد من الاتفاقيات الدولية في مجال مكافحة الجرائم السيبرانية.
- ضرورة إنشاء مركز دولي مقرهُ الأمم المتحددة يساهم في مكافحة الجرائم المعلوماتية على المستوى الدولي.

المراجع:

1. أبو دوح، خالد كاظم (2018م) الأمن السيبراني للدول و الأفراد، المجلة العربية، العدد 398، الرياض .
2. أبو زيد، عبد الرحمن عاطف (2019م) الأمن السيبراني في الوطن العربي، مجلة البحوث والدراسات، العدد 48، المركز العربي للبحوث و الدراسات .
3. أحمد، هلالي (2007م) اتفاقية بودابيست لمكافحة الجرائم المعلوماتية، دار النهضة العربية، القاهرة .
4. بانقا، علم الدين (2009م) مخاطر الهجمات الإلكترونية و أثارها الاقتصادية، " مجلة دراسات تنموية "، العدد 63. المعهد العربي للتخطيط.
5. البشري، محمد الأمين (2000م) التحقيق في جرائم الحاسب الإلى، بحث مقدم إلى مؤتمر القانون و الكمبيوتر و الإنترنت المنعقد في الفترة من 3/1 مايو / بكلية الشرية و القانون بدولة الإمارات.
6. بيومي، عبد الفتاح (2007م) مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الإنترنت، دار الكتب القانونية، القاهرة .
7. الجموسي، جوهر (2016م)، الافتراضي و الثورة، المركز العربي للأبحاث و الدراسات السياسية، بيروت .
8. جميل، كريا محمود (2005م) ورقة في الجريمة المعلوماتية و أساليب التامين، المؤتمر الدولي للأمن المعلومات الإلكترونية، سلطنة عمان.
9. الحوامدة، لورنس سعيد (2017م) الجرائم المعلوماتية، بحث مقدم إلى جامعة طيبة، كلية الحقوق، المملكة العربية السعودية.
10. داوود، حسن طاهر (2000م) جرائم نظم المعلومات، أكاديمية نايف العربية للعوم الأمنية، الرياض
11. الربيعة، صالح بن على (2017م) الأمن الرقمي و حماية المستخدم من مخاطر الإنترنت، هيئة الاتصالات و تقنية المعلومات، المملكة العربية السعودية.
12. الصلاحي، فؤاد (2015م) الأمن السيبراني، مجلة الدوحة، وزارة الإعلام.
13. عبدالصبور، سماح (2017م) الصراع السيبراني، مجلة السياسة الدولية، مؤسسة الأهرام، القاهرة.
14. ليتيم، فتحيه (2014م) الأمن المعلوماتي للحكومة الإلكترونية و إرهاب القرصنة، مجلة الفكر، العدد (12) . جامعة عنابة، الجزائر.
15. مطابقة، محمد فواز (2018م) العقود الإلكترونية و البيئة الإلكترونية في النظام السعودي، مكتبة جامعة خازان، المملكة العربية السعودية
16. هيئة تحرير المجلة الدبلوماسية (2018م) الأمن السيبراني، مجلة الدبلوماسي، العدد 90، معهد الأمير سعود الفيصل للدراسات الدبلوماسية .