دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي

عقيد دكتـــــور
خالد ظاهر عبدالله جابر السهيل المطيري
أستاذ مساعد بأكاديمية سعد العبدالله للعلوم الأمنية بالكويت
دكتوراه في القانون الجنائي

دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي

خالد ظاهر عبدالله جابر السهيل المطيري
قسم المقررات القانونية، أكاديمية سعد العبدالله للعلوم الأمنية، دولة الكويت.
البريد الإلكتروني : Kh_alsohel@hotmail.com

ملخص البحث:

هدف الدراسة : تهدف إلى إلقاء الضوء على أبرز النماذج الإجرامية التي تواجه دول مجلس التعاون والوقوف على مدى قدرة التشريعات الجزائية بها على مواجهة هذه الجرائم والحد منها ، ومدى الحاجة إلى سن تشريعات جديدة.

مشكلة الدراسة : تتلخص في كون الجرائم السيبرانية المستحدثة تمثل تحديًا تشريعيًا وقضائيًا لأي مجتمع بسبب المخاطر الناتجة عنها ، فالتهديدات لم تعد تعتمد علي قوة السلاح فقط، بل ظهرت وسائل إجرامية حديثة تعتمد علي التقنيات الجديدة وعابرة للحدود .

منهج الدراسة : اعتمدت على المنهج التحليلي النقدى الذي يسعى إلى وصف ، وتحليل ، وتشخيص ،الموضوع من مختلف جوانبه وأبعاده ، بهدف التوصل إلى نظرة عن تعريف الأمن السيبراني والبيانات والمعلومات ، والوقوف على مدى كفاية التشريعات ومدى فاعليتها على أرض الواقع وتقديم المعالجة ، وكذلك المنهج المقارن لبيان أوجه الاتفاق والاختلاف بين تلك التشريعات وتقتصر معالجة الموضوع علي نطاق دول مجلس التعاون ، وهو ما يقتضي ، تفهم التحديات التي تواجه هذه الدول .

بيانات الدراسة : الدراسة مقسمة إلى ثلاثة مباحث ، ونخصص أولها : مفهوم الأمن السيبراني ، وثانيها: أبرز النماذج الإجرامية التي تواجه دول مجلس التعاون ، وثالثها : الحماية التشريعية من الجريمة السيبرانية بدول مجلس التعاون .

النتائج: انتهى البحث إلى عدة نتائج أبرزها : يجب على كل دولة من دول مجلس التعاون انشاء مركز وطني للأمن السيبراني يعكف على دراسة التهديدات السيبرانية وأسبابها ووضع الخطط لمكافحتها وتحديد سبل الاستجابة الوطنية وإنشاء مركز خليجي للأمن السيبراني ينسق بين المراكز الوطنية .

الكلمات المفتاحية : الأمن السيبراني، الجرائم السيبرانية، فريق الاستجابة لطوارئ الحاسبات، بروتوكول الإنترنت.

The role of penal legislation in protecting cyber security in the Gulf Cooperation Council countries

Khaled dhaher abdullah almutairi
Department of law, Saad Al-Abdullah Academy for Security Sciences, Kuwait.
E-mail: Kh_alsohel@hotmail.com

Abstract:

Objective of the study:
The study aims to shed light on the most prominent criminal models facing the countries of the Gulf Cooperation Council and to determine the extent of the ability of their penal legislation (regulations) to confront and limit these crimes, and the need to enact new legislations.

Statement of the problem
The statement of the problem is summarized in the fact that the newly created cyber-crimes constitute a legislative and judicial challenge for any society because of the risks resulting therefrom. Threats no longer depend on the power of arms only, but modern criminal means have appeared that depend on new and cross-border technologies.

Methodology of the Study:
The study relied on the critical analytical approach that seeks to describe, analyze, and diagnose the subject of the study from its various aspects and dimensions, with the aim of getting to a view of the definition of cybersecurity, data and information. To further determine the adequacy of legislation along with its effectiveness on the ground and providing treatment. As well as the comparative approach to show the aspects of agreement and differences amongst these legislations. The addressing of this subject is limited to the scope of the GCC countries, which requires, in the first place, an understanding of the challenges facing these countries.

Study data:
The study is divided into three sections, the first of which is: the concept of cyber security, the second: the most prominent criminal models facing the GCC countries, and the third: legislative protection from cyber-crime in the GCC countries.

Results:
The research concluded with several results, most notably: Each of the GCC countries should establish a national center for cyber security to study cyber threats and their causes, develop plans to combat them, determine ways of national response. In addition, to establish a Gulf center for cyber security that coordinates between the national centers. Meanwhile, cyber security goes through two stages: the first: prevention of risks, and the second stage: treatment of the cyber-attack after penetration.

Recommendations:
Among the most prominent recommendations: The Gulf Cooperation Council must work to establish a cyber-intelligence authority to exchange intelligence information between the GCC countries and improve access to cyber threats. An electronic platform must be created to receive reports of cyber-crimes, keeping pace with programs and applications for securing cyberspace on an ongoing basis.

Keywords: Intrusion Detection System, The Internet of Things – IOT, Internet Protocol – IP, Computer Emergency Response Team.

المقدمة

سبب إختيار الموضوع :

لا شك أن الجرائم السيبرانية - خصوصا تلك المرتكبة ضد الحياة الخاصة للأفراد واختراق المؤسسات المالية كالبنوك والشركات المالية - تشكل أحد العناصر الرئيسية ، التي تثير قلق المجتمع الداخلي والدولي و تهدد أمنه وسلامته ، لكونها تمثل اعتداء صارخًا علي أحد المصالح الأساسية التي يكفل لها القانون الجنائي والدولي حماية خاصة . من هذا المنطلق كان لزامًا علي الدول أن تسعى - من خلال مؤسساتها المعنية - لمواجهة تلك الأنشطة الإجرامية .

ومع التطورات المتلاحقة للتكنولوجيا أضحى الأختلاف بين الجريمة السيبرانية والجريمة التقليدية يزداد انطماسًا بشكل عام . فمع التزايد المستمر للعولمة [1] و انتشار الأجهزة

---

(١) "العولمة Globalization : هو مصطلح إنجليزي تم ترجمته إلي اللغة العربية ، وتعني جعل الشي عالميًا من حيث النطاق أو التطبيق أو بمعني أخر الظاهرة التي تشير إلي مرحلة من مراحل التطور التاريخي للمجتمعات الإنسانية (الاقتصادية والاجتماعية والثقافية والسياسية) فهذه الظاهرة – تسعي إلي تذويب الحدود بين المجتمعات ، بحيث تصبح جميع الأنشطة الإنسانية مفتوحة علي بعضها البعض والمساواة بينها ، والحقيقة أن هذه الظاهرة لم يكن لها تعريف جامع وشامل ، ولكن كانت هناك محاولات عديدة لتعريفها ولم تختلف صياغتها عن المضمون الذي جاءت به تلك الظاهرة ، فقد عرفها البعض بأنها الظاهرة التي من خلالها تصبح الشعوب متصلة ببعضها في كافة الأوجه الثقافية والاقتصادية والاجتماعية والسياسية ،والأخر يرى أنها حركة تهدف إلي تعميم أو تطبيق أمر ما على العالم أجمع .. "راجع :
Bhagwati ،Jagdihln. Defence of Globalization. New Yourk: Oxford University Press ،٢٠٠٤ ،p28.

وراجع حول ذلك أيضا :

د/ محمد سامي الشوا ، ثورة المعلومات وانعكاساتها علي قانون العقوبات ، دار النهضة العربية ، ٢٠٠٣ ، القاهرة ، ص ١٧ . وراجع أيضًا : أحمد وهدان ،الانعكاسات الأمنية للعولمة دراسة في أثر العولمة على الجريمة المنظمة ، المجلة الجنائية القومية ، المجلد الرابع والأربعون ، العددان الأول والثانى ، مارس / يوليو ، عام ٢٠٠١ م .

الإلكترونية ووسائل التواصل الإجتماعي أدى إلى التطور السريع في وسائل ارتكاب الجرائم ، ودول مجلس التعاون الخليجي ليست بمنأى عن هذا التطور ، فسارعت إلى إصدار التشريعات الخاصة بمكافحة جرائم تقنية المعلومات.

"الشبكة في أبسط مستوياتها هي" اتصال جهازين أو أكثر بطريقةٍ ما باستخدام الأجهزة والبرمجيات لتمكين الأجهزة من الاتصال ، و يمكن لأجهزة مثل أجهزة الكمبيوتر والطابعات وأجهزة التوجيه والمحوِّلات والأجهزة اللاسلكية ونقاط الوصول وأجهزة الكمبيوتر المحمولة والطابعات والمساعدات الرقمية الشخصية أن تكون العقد علي الشبكات . والعقدة هي مكوِّنٌ للشبكة تقوم بتنفيذ وظائف مُرتبِطة بالشبكة ويتم التعامل معها ككيان واحد" .

DAVID (E . LEARNER .) ، ELECTRONIC CRIME SCENE INVESTIGATION ،PUBLISHED IN NOVA SCIENCE ،LNC ،NEW YORK ، ٢٠٠٩ ،P. 106

وعرفت أيضًا الشبكة أنها هي: "ترابط بين نظامي كمبيوتر أو أكثر، ويمكن أن تكون الوصلات أرضية (على سبيل المثال: الأسلاك أو الكابلات) أو لاسلكية (مثل: الراديو أو الأشعة تحت الحمراء أو القمر الصناعي) أو كليهما، ويمكن أن تكون الشبكة محدودة جغرافيًا في منطقة صغيرة (شبكات المنطقة المحلية) أو أن تمتد على مساحة شاسعة (شبكات المنطقة الواسعة)، وهذه الشبكات بدورها يمكن أن تكون مترابطة فيما بينها. ويُعتبَر الإنترنت شبكة عالمية تتكوَّن من العديد من الشبكات المترابطة تستخدم جميعها نفس البروتوكولات، وتُوْجَد أنواع أخرى من الشبكات سواءً كانت متصلة بالإنترنت أم لا، القادرة على تحويل بيانات الكمبيوتر بين أنظمة الحاسوب. ويمكن أن تكون أنظمة الكمبيوتر متصلة بالشبكة كنقاط نهاية أو كوسيلة للمساعدة في التواصل على الشبكة. الأمر الأساس هو أن تبادل البيانات يتم عبر الشبكة " راجع : التقرير التفسيري لإتفاقية بودابست ، ص ٥ .

وعُرِّفَت الشبكة المعلوماتية على أنها : " ارتباط بين أكثر من نظام معلوماتي للحصول على المعلومات وتبادلها" .

راجع: المادة الثانية فقرة (٦) من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠م.

وعلي الرغم من أن هناك تشريعات جنائية قد واجهت الاعتداءات على أمن الفضاء السيبراني والشبكة المعلوماتية [١]، إلا أن مسرح الأحداث الدولية قد شهد العديد من النشاطات الإجرامية التي تتجاوز أثارها حدود الدولة الواحدة لتمتد إلي عدة دول ، مكتسبة بذلك طابعًا عالميًا ، مما يجعل منها جريمة ضد النظام العام الدولى ، وأمن وسلام الشعوب ، وحقوق وحريات الأفراد .

هدف الدراسة وأهميتها :

تهدف الدراسة إلى إلقاء الضوء على التحديات السيبرانية التي تواجه دول مجلس التعاون لدول الخليج العربية نظراً لأن الجرائم السيبرانية تعتبر جرائم ذات طبيعة خاصة . والوقوف على مدى قدرة التشريعات الجزائية بدول المجلس على مواجهة هذه الجرائم وكيفية التصدي لها ، والحد منها أم أن الأمر يستلزم سن تشريعات جديدة لمواجهتها وصولاً إلى الحماية الكافية وتحقيق الأمن السيبراني .

---

(١) انظر : المادة الأولي فقرة (ب) من أتفاقية بودابست الأوربية رقم ١٨٥ المتعلقة بمكافحة الجرائم الإلكترونية لعام ٢٠٠١ .

وقد أشارت المذكرة التفسيرية إلي أن تعريف بيانات الكمبيوتر الوارد في المادة الأولي مأخوذ من المنظمة الدولية للمواصفات. ويتضمن هذا التعريف مصطلحات "مناسب للمعالجة"، بمعنى أنه يتم وضع البيانات في شكل يسمح بمعالجتها مباشرة من خلال نظام الكمبيوتر وتوخِّيًا لتوضيح أن البيانات الواردة في هذه الاتفاقية يجب أن تُفهَم على أنها بيانات في شكل إلكتروني أو أي شكل آخر قابل للمعالجة التلقائية، وتم إدخال مفهوم "بيانات الكمبيوتر"، وأوضحت أنه يمكن أن تكون بيانات الكمبيوتر التي تتم معالجتها تلقائيًا موضوع إحدى الجرائم الجنائية المحدَّدة في اتفاقية بودابست ، وكذلك موضوع تطبيق أحد تدابير التحقيق المحدَّدة في هذه الاتفاقية .

راجع : المذكرة التفسيرية لإتفاقية بودابست ، المعتمدة من لجنة وزراء مجلس أوربا في ٨ نوفمبر / تشرين الثاني عام ٢٠٠١ م ، ص ٦ . وجدير بالذكر أنه قد عرف القانون الكويتى رقم ٦٣ لسنة ٢٠١٥ الشبكة المعلوماتية بأنه هو " ارتباط بين أكثر من منظومة اتصالات لتقنية المعلومات للحصول على المعلومات وتبادلها " .

كما تهدف إلى التركيز على آليات مواجهة هذه الجرائم سواء على الصعيد الداخلى أو الدولي من خلال الإشارة إلى بعض القوانين الجزائية والاتفاقيات الدولية المتعلقة بمكافحة الجرائم السيبرانية

مشكلة الدراسة :

تتلخص مشكلة الدراسة في أن الجرائم السيبرانية المستحدثة تمثل تحديًا أمنيًا وتشريعيًا وقضائيًا لأي مجتمع بسبب المخاطر الناتجة عن هذه الجريمة ، فالتهديدات لم تعد تعتمد علي قوة السلاح فقط ، بل ظهرت وسائل إجرامية حديثة تعتمد علي التقنيات الجديدة ، فالمعطيات القديمة لم تستمر علي حالها ، إذ ما لبث العالم أن تحول إلي قرية صغيرة بفعل سهولة الاتصالات التي قادتها ثورة التكنولوجيا المعلوماتية الحديثة ، مما يتطلب الوقوف على كيفية مواجهة هذه الجرائم .

تساؤلات الدراسة :

لمعالجة المشكلات المتعلقة بالأمن السيبراني الذي يعمل على مكافحة الجرائم السيبرانية التي تواجه دول مجلس التعاون نطرح بعض التساؤلات المتعلقة بالدراسة وهي كالأتي :

أولاً : ماذا يعني مفهوم الأمن السيبراني ؟

ثانياً : ماذا يعني مفهوم البيانات والمعلومات ؟

ثالثاً : ما هي الأهداف المرتبطة باستراتيجية الأمن السيبراني ؟

رابعاً : ما هي التحديات السيبرانية المستقبلية التي تواجه دول مجلس التعاون الخليجي ؟

خامساً : ما هي القطاعات المتضررة من تهديدات الجريمة السيبرانية ؟

سادساً : ما هي دوافع الإرهاب السيبراني ؟

سابعاً : ما هي السبل لمواجهة التحديات السيبرانية ؟

منهج الدراسة :

اعتمدت الدراسة على المنهج التحليلي النقدى الذي يسعى إلى وصف ، وتحليل ، وتشخيص ،موضوع الدراسة من مختلف جوانبها ، وأبعادها ، بهدف التوصل إلى نظرة عن

تعريف الأمن السيبراني والبيانات والمعلومات ، والوقوف على مدى كفاية التشريعات ومدى فاعليتها على أرض الواقع ، وكذلك المنهج المقارن لبيان أوجه الاتفاق والاختلاف بين تلك التشريعات ، وتقديم المعالجة الجزائية المناسبة . ، وتقتصرمعالجة الموضوع علي نطاق دول مجلس التعاون ، وهو ما يقتضي بالدرجة الأولى تفهم التحديات التي تواجه هذه الدول .

المصطلحات المستخدمة في الدراسة واختصاراتها :

EU	الاتحاد الأوربي
CERT	فريق مواجهة الطوارئ الحاسوبية
ECHR	فريق الاستجابة لحوادث أمن الفضاء الإلكتروني
EUROPOL	مكتب الشرطة الأوروبي
ICT	تكنولوجيا المعلومات والاتصالات
INTERPOL	المنظمة الدولية للشرطة الجنائية
IP	بروتوكول الإنترنت
ISP	مقدمو خدمات الإنترنت
IT	تكنولوجيا المعلومات
ITU	الاتحاد الدولي للاتصالات
OP-CRC-SC	البروتوكول الاختياري لاتفاقية حقوق الطفل بشأن بيع الأطفال واستغلال الأطفال في البغاء والمواد الإباحية
UNODC	مكتب الأمم المتحدة المعني بالمخدرات والجريمة
URL	الاسم التقني لعنوان الموقع الالكتروني على الإنترنت

GCI	المؤشر العالمي لقياس الأمن السيبراني للدول
Lot	إنترنت الأشياء
CITRA	الهيئة العامة للاتصالات وتقنية المعلومات بالكويت

خطة الدراسة :

الدراسة مقسمة إلى ثلاثة مباحث ، وذلك على نحو ما سيلي بيانه .

المبحث الأول : الأحكام العامة لمفهوم الأمن السيبراني

مع تطور العصر التكنولوجي وتنامي الجهود نحو تطوير الاقتصاد المبني على المعرفة ، أضحت تكنولوجيا المعلومات والاتصالات أداة رئيسية في توليد المعرفة ، وحفظها ، ومعالجتها ، وتبادلها ، وتساهم في تحقيق التنمية المستدامة ، وإتاحة فرص عمل جديدة للشباب ، وتحفيز النمو الاقتصادي . وقد شهد هذا المجال ازدياداً كبيراً في أعداد مستخدمي الإنترنت وفي انتشار الأجهزة النقالة الذكية ، وفي النفاذ إلى خدمات الحزمة العريضة النقالة ، إلا أن هذا الانفتاح الذي يتسم به الفضاء السيبراني جعل من مستخدميه عرضة للتعديات ، وضحايا للأنشطة الإجرامية التي يرتكبها المجرمون و مخترقو الشبكات[1]. وسوف نتناول هذا المبحث في المطالب الآتية :

المطلب الأول : التطور التاريخي للإنترنت والأمن السيبراني وتعريفه

نقسم هذا المطلب إلى ثلاثة فروع على النحو التالي :

الفرع الأول : التطور التاريخي للإنترنت والأمن السيبراني

تجرع العالم في القرن العشرين ويلات حربين عالميتين : الأولى ما بين عام ١٩١٤ - ١٩١٨م، والثانية ما بين ١٩٣٩ – ١٩٤٥م ، ومع تطور المد الشيوعي والتقدم التكنولوجي للاتحاد السوفيتي بعد الحرب العالمية الثانية بدأت الولايات المتحدة الأمريكية في تكوين حُلفاء جدد لها؛ وذلك لترسيخ وجودها لمواجهة المد الشيوعي للاتحاد السوفيتي ، وقامت الولايات المتحدة بكسب حلفاء عسكريين إلى جانب اهتمامها بالعلوم والتكنولوجيا لوقف هذا المد .

---

(١) تقرير اللجنة الاقتصادية والإجتماعية لغربي أسيا (الإسكوا) ، التابع للأمم المتحدة ، بعنوان ورشة عمل حول تحفيز الأمان في الفضاء السيبراني في المنطقة العربية ، مسقط ٨-٩ كانون الأول / ديسمبر عام ٢٠١٤ ، وثيقة رقم :

E/ESCWA/TDD/2015/WG.1/Report .

ثم بدأت حرب من نوع آخر حيث انتقلت ساحة المعركة إلى الفضاء الالكتروني عندما أطلق الإتحاد السوفيتي القمر الصناعي سبوتنيك عام ١٩٥٧م مما أدى إلى إطلاق ناقوس الخطر في الولايات المتحدة الأمريكية بسبب الفجوة في العلوم،واتجهت نحو زيادة الاستثمارات الحكومية في العلوم والتكنولوجيا[١] .

ويرجع إنشاء الإنترنت في بادئ الأمر في الستينات من القرن الماضي نتاجًا لمشروع حكومي أمريكي سمي بالآربانت (ARPA NET) [٢] ؛ وكان ذلك بهدف تأمين شبكة اتصال خاصة لا يمكن إتلافها أو تدميرها في حال حدوث عمليات تخريب أو نشوب حرب مفاجئة، وعهدت وزارة الدفاع بهذه المهمة إلى وكالة مشاريع الأبحاث المُتقدمة القادرة على مقاومة الكوارث والاستمرار في العمل في حالة حدوث هجوم، وكانت هذه الشبكة تربط أربعة حاسبات آلية ضخمة فيما بينها لغرض التجربة [٣]

و في ١٩ ديسمبر عام ١٩٦٨ م تبنت الجمعية العامة للأمم المتحدة في اجتماعها توصيات المؤتمر الأول لحقوق الإنسان المنعقد في طهران عام ١٩٦٨ والخاص بالآتي[٤]:

---

(1) Janet (ABBATE.) , INVENTING THE INTERNET , PUBLISHED BY THE MIT PRESS CAMBRIDGE ،LONDON ، ١٩٩٩، P . 8

(٢) محمد أمين أحمد الشوابكة ، الجرائم المرتكبة عبر الإنترنت ، رسالة قدمت لنيل درجة الماجستير في القانون إلي معهد البحوث العربية للتربية والثقافة والعلوم ، جامعة الدول العربية ، القاهرة ،عام ٢٠٠٢ م، ص ١٥ .

(٣) حسين بن سعيد بن سيف الغافري ، السياسة الجنائية في مواجهة جرائم الإنترنت "دراسة مقارنة " ، رسالة قدمت لنيلِ درجة الدكتوراه في القانون من جامعة عين شمس ، عام ٢٠٠٧ م، ص ١٢ .

لمزيد من التفصيل حول نشأة شبكة الإنترنت راجع : نهلا عبدالقادر المومني ، الجرائم المعلوماتية ، دار الثقافة ، الطبعة الثانية ، عام ٢٠١٠ م، ص ٣٧ وما بعدها .

(٤) د/ أسامة عبدالله قايد ، الحماية الجنائية للحياة الخاصة وبنوك المعلومات دراسة مقارنة في القانون الفرنسي والأمريكي والمصري وفقًا لآخر التعديلات التشريعية ، دار النهضة العربية ،بدون رقم طبعة ، القاهرة ، عام ٢٠١٥ م، ص ١٢٨.

(١) دراسة أثر التقدم التكنولوجي على حقوق الإنسان .

(٢) ضرورة احترام الحياة الخاصة في مواجهة التقدم التكنولوجي .

(٣) حماية حقوق الأفراد وحرياتهم من خطر التعدي عليها .

أما فيما يتعلق بتبادل المعلومات بين الحاسبات بعضها البعض فقد طالبت وكالة الأبحاث المتقدمة التابعة لوزارة الدفاع الأمريكيةعام ١٩٦٩ ببرتوكول للاتصالات مستقل عن أنظمة الاتصالات الأخرى لمشيدي هذه الأنظمة عن طريق حزم المعلومات ، وفي عام ١٩٧٠ تم ربط أربع جامعات أمريكية بشبكة واحدة [١].

وفي نهاية عام ١٩٧٠م تم استخدام أول برتوكول وهو (X25) لربط الحاسبات الآلية التي تعمل بلغات مختلفة ببعضها البعض ، وبذات العام استخدم مصطلح الاختراق للمرة الأولى وكان التركيز على البرمجية الاستثنائية التي يمتلكها المتسلل. [٢] وفي نهاية عام ١٩٧٢م ابتكر الباحثان BOB KAHN وVINTON CERF برتوكول (IP / TCP) الذي تم اعتماده رسميًا ؛ ليِحل محل البرتوكول السابق [٣] ، وفي عام ١٩٧٧م أبدت منظمة التعاون الإقتصادي والتنمية اهتمامها بالمشكلات التي أثارتها نظم المعلومات في الحياة الاقتصادية، وبدأ الاهتمام أيضًا بحماية الخصوصية من التهديد المعلوماتي، وأنتج هذا الاهتمام عدة قواعد لحماية البيانات الشخصية [٤]

---

(١) عبدالحليم بركات أحمد غزال ، الحماية الجنائية الموضوعية لتعاملات الشبكة الدولية للمعلومات ، رسالة قدمت لنيل درجة الدكتوراه في القانون ، جامعة المنصورة ، عام ٢٠١٤م ، ص ١٠ .

(٢) نشرة تكنولوجيا المعلومات والاتصالات للتنمية في المنظقة العربية ،الإسكوا التابعة للأمم المتحدة ، العدد ١٨ ، عام ٢٠١٢ ، ص ١٥ .

(٣) حسين بن سعيد بن سيف الغافري ، المرجع السابق ، ص ١٣ .

(٤) أيمن عبدالله فكري ، جرائم نظم المعلومات – دراسة مقارنة – ، رسالة قُدِّمَت لنيل درجة الدكتوراه في القانون من جامعة المنصورة ، عام ٢٠٠٦م ، ص ٩١ وما بعدها .

وفي عام ١٩٨٣ ، رأت وزارة الدفاع الأمريكية فصل الشق العسكري (milnet) عن الشبكة ، وقامت الهيئة القومية للعلوم بإنشاء شبكة NSFNET لتوصيل خمسة حاسبات تعمل بسرعة فائقة لتحل محل الأنظمة السابقة ؛ وذلك لخدمة مركز البحوث الأمريكية [١].

وفي أواخر الثمانينات من القرن العشرين تم اختراع شبكة الويب العالمية في جنيف بسويسرا في مختبرات CERN ، وتعني مركز الدراسات والبحوث النووية، وهي منشأة عالمية للفيزياء التجريبية والنظرية ، ويرجع الفضل في ذلك لشاب يبلغ من العمر أربعة وثلاثين عامًا يُدعى TIM BERNERSLEE ؛ وذلك بسبب صعوبة عثورِه على المواد البحثية الخاصة به، فصمم لغة جديدة تسمى HTML ، وهي لغة ترميز النص التشعبي مصممة لمساعدة أجهزة الكمبيوتر على التّحدث مع غيرها ومشاركة البيانات بشكل أفضل [٢].

ويمكننا القول أن لغة (HTML) هي اختصار لجملة Hyper Text Markup Language، وتستخدم هذه اللغة في التنقل بين صفحات الويب العالمية بشرط توصيلها بشبكة الإنترنت ، فهي تسمح بالتجوال داخل المُتصفحات الموصولة "بالشبكة "[٣]، ومن

---

(١) د/ مدحت رمضان ، جرائم الاعتداء على الأشخاص والإنترنت ، دار النهضة العربية ، بدون رقم طبعة ، القاهرة ، عام ٢٠٠٠ ، ص ٣ .

(2) :DR. JACQUES) VALLEE. (،THE HEART OF THE INTERNET : AN INSIDER'S VIEW OF THE ON-LINE REVOLUTION ، PUBLISHED BY HAMPTON ROADS ،٢٠٠٣ ،P. 107 .

(٣) "الشبكة في أبسط مستوياتها هي" اتصال جهازين أو أكثر بطريقةٍ ما باستخدام الأجهزة والبرمجيات لتمكين الأجهزة من الاتصال ، و يمكن لأجهزة مثل أجهزة الكمبيوتر والطابعات وأجهزة التوجيه والمحوِّلات والأجهزة اللاسلكية ونقاط الوصول وأجهزة الكمبيوتر المحمولة والطابعات والمساعدات الرقمية الشخصية أن تكون العقد علي الشبكات. والعقدة هي مكوِّنٌ للشبكة تقوم بتنفيذ وظائف مُرتبِطة بالشبكة ويتم التعامل معها ككيان واحد" .

DAVID (E . LEARNER .) ،ELECTRONIC CRIME SCENE INVESTIGATION ،PUBLISHED BY NOVA SCIENCE ،LNC ،NEW YORK ،٢٠٠٩ ،P. 106

أشهر برامج المتصفحات هي INTERNET EX PLORER وبرنامج CHROME وبرنامج OPERA وبرنامج mozilla firefox .

وفي عام ١٩٩٤م أوصى المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات في البرازيل والخاص بجرائم الحاسب الآلي والإنترنت بضرورة إدخال الدول بعض التعديلات على قوانينها الجنائية الداخلية [١] .

وفي عام ١٩٩٨ م أُبرمت مذكرة تفاهم (mou: understanding of memorandum) بين منظمة ICANN والدائرة التجارية (doc: commerce of Department) ؛ وذلك بهدف نقل أسماء الدومين المعروف باسم .com إلى المجال التجاري [٢] .

وتتولى جهة أخرى تعرف بالمختصر (IANA) إدارة طائفتين للدومين وهما : الطائفة الأولى لدومين الدارج (GTLD) والطائفة الثانية لدومين متمثل في رقم كودي لكل دولة،

وعرفت أيضًا الشبكة أنها هي: "ترابط بين نظامي كمبيوتر أو أكثر، ويمكن أن تكون الوصلات أرضية (على سبيل المثال: الأسلاك أو الكابلات) أو لاسلكية (مثل: الراديو أو الأشعة تحت الحمراء أو القمر الصناعي) أو كليهما، ويمكن أن تكون الشبكة محدودة جغرافيًا في منطقة صغيرة (شبكات المنطقة المحلية) أو أن تمتد على مساحة شاسعة (شبكات المنطقة الواسعة)، وهذه الشبكات بدورها يمكن أن تكون مترابطة فيما بينها. ويُعتبَر الإنترنت شبكة عالمية تتكوَّن من العديد من الشبكات المترابطة تستخدم جميعها نفس البروتوكولات، وتوجد أنواع أخرى من الشبكات سواءً كانت متصلة بالإنترنت أم لا، القادرة على تحويل بيانات الكمبيوتر بين أنظمة الحاسوب. ويمكن أن تكون أنظمة الكمبيوتر متصلة بالشبكة كنقاط نهاية أو كوسيلة للمساعدة في التواصل على الشبكة. الأمر الأساس هو أن تبادل البيانات يتم عبر الشبكة " . راجع : التقرير التفسيري لإتفاقية بودابست لمكافحة الجرائم الالكترونية ، المجر ، ص ٥ .

(١) د / رامي متولي القاضي ، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية ، دار النهضة العربية ، الطبعة الأولي ، عام ٢٠١١ م، ص ١١ .

(٢) د / محمد حسام محمود لطفي ، حقوق الملكية الفكرية المفاهيم الأساسية – دراسة لأحكام القانون رقم ٨٢ لسنة ٢٠٠٢ في ضوء أراء الفقه وأحكام القضاء المقارن –، دار النهضة العربية ، الطبعة الثانية ، القاهرة ، عام ٢٠١٢ م ، ص ١١٧ .

ففي مجال الطائفة الأولي نجد أن ثلاثة أسماء متاحة للجميع وهو COM الخاصة بمجال التجارة ، وNET الخاصة بمجال الشبكات المعلوماتية و ORGالخاصة بمجال المنظمات وأربعة أسماء غير متاحة للجمهور مُقيَّد التسجيل بها وهي GOV والخاصة بالمجال الحكومي وmil الخاصة بالمجال العسكري و edu الخاصة بالمعاهد التعليمية التي تمنح مُـؤَهِّلات لسنوات دراسية أربع سنوات والجامعات وint المقصورة على المنظمات الحكومية، وفي ١٦ من نوفمبر/ تشرين ثان عام ٢٠٠٠م أُضِيفت خمسة مجالات أخرى إلى المجالات السابقة يُتاَح للجمهور القيد بها [١] .

ويعد الإنترنت "غير مملوك لأحد وغير مسيطرعليه من أحد؛ لكونه ملكية تعاونية للبشرية بقدر إسهامهم فيه" [٢].

وإدراكًا بعمق التغيرات التي أحدثتها تكنولوجيا المعلومات والعولمة الخاصة بالكمبيوتر وبمخاطر استخدام الشبكات في ارتكاب جرائم سيبرانية ، وأهمية التعاون الدولي بين الدول والقطاع الخاص اعتمد الاتحاد الأوربي عام ٢٠٠١ ،اتفاقية دولية خاصة بمكافحة الجرائم الالكترونية [٣].

وفي شهر مايو من عام ٢٠٠٥ ، قام الاتحاد الأوروبي بالتوسع في خطة العمل بشأن شبكة إنترنت أكثر أمانًا (safer internet plus) عن الفترة من عام ٢٠٠٥ -٢٠٠٨م؛ وذلك لتعزيز الإستخدام الآمن لشبكة الإنترنت وما يقترن بها من تكنولوجيا حديثة لاسيما المواد غير القانونية .[٤]

---

(١) د/ محمد حسام محمود لطفي ، المرجع السابق ، ص ١١١ وما بعدها .

(٢) علي عواد شحاته ، نحو نظرية عامة لمكافحة جرائم الحاسب الآلي ، رسالة قدمت لنيل درجة الدكتوراه في الحقوق من جامعة القاهرة ، عام ٢٠١٧ م ، ص ٢٧ . وللمزيد راجع في ذلك أيضاً : محمد حسين موسي عبدالناصر ، المواجهة الجنائية لجرائم الاعتداء علي حقوق الملكية الأدبية والفنية عبر الانترنت ، رسالة قدمت لنيل درجة الدكتوراه في الحقوق من جامعة أسيوط ، عام ٢٠١٦ م، ص ١٥ .

(٣) اتفاقية بودابست الأوربية رقم ١٨٥ المتعلقة بمكافحة الجرائم الإلكترونية لعام ٢٠٠١م .

(4) yaman (akdeniz) , internet child pornography and the law : national and international responses , published by ashgate . uk . 2008 .p 33 .

وفي تقرير صادر عن الاتحاد الدولي للاتصالات (ITU) عام ٢٠١٨م أشار إلى أن هناك أكثر من نصف سكان العالم موصولون بالإنترنت ، ففي البلدان المتقدمة هناك أربعة أفراد من بين كل خمسة أفراد موصولون بالإنترنت .[١]

إن التطور التكنولوجي الخاص بتوفر الإنترنت وانتشاره عبر الأجهزة المتنقلة – أو النقالة – ، وذلك توازيا مع توافر حزمة الإنترنت العريضة قليلة التكلفة عبر تلك الأجهزة؛ أدى إلى تزايد عدد المستخدمين للإنترنت، وأيضا زيادة الاعتماد على هذا النوع من التكنولوجيا في التنمية الاجتماعية والاقتصادية، غير أن ما يميز شبكة الإنترنت والفضاء السيبراني – بشكل عام – هو الانفتاح، وهذه الميزة جعلتها عرضة للنشاط الإجرامي وتعدياته، الأمر الذي جعل مستخدمي الفضاء السيبراني يتعرضون للانتهاكات من قبل مخترقي الشبكات . وهذا ما دعى إلى ضرورة وضع أطر إجرائية لمواجهة تلك المخاطر السيبرانية، ونشر الوعي الخاص بخطورة هذه التعديات على مستوى الأفراد والمؤسسات، وآثارها السلبية على أعمالهم.[٢]

ومن الخطوات الجيدة التي اتخذت في شأن الأمن السيبراني هو استحداث الاتحاد الدولي للاتصالات التابع للأمم المتحدة مؤشر عالمي للأمن السيبراني (GCI) وهو اختصار ل GLOBAL CYBER SECURITY INDEX وذلك لتحديد مدي تطور الدول في مجال الأمن السيبراني .

---

(١) تقرير الاتحاد الدولي للاتصالات لقياس مجتمع المعلومات خلال الندوة العالمية السادسة عشرة لمؤشرات الاتصالات وتكنولوجيا المعلومات (WTIS) ، في الفترة من ١٠ إلي ١٢ ديسمبر عام ٢٠١٨ م، جنيف ، سويسرا ، ص٢ ، ومنشور بموقع الاتحاد الدولي للاتصالات https://itu.int في ٢٠/ ٢/ ٢٠١٩ م .

(٢) موقع الاسكوا التابع للأمم المتحدة (https://www.unescwa.org) .

وفي عام ٢٠١٨ حصلت المملكة العربية السعودية على المركز الأول عربياً في مؤشر الأمن السيبراني للاتحاد الدولي وحصلت على المركز الثالث عشر دولياً ، وتقدمت بثلاثة وثلاثون مرتبة عن المؤشر العالمي للأمن السيبراني عام ٢٠١٦ . (١)

ويتضح مما سبق : أن الأمن السيبراني تطور بتطور الإنترنت والتكنولوجيا وصولاً إلى ما يسمى بإنترنت الأشياء(٢) ، والتي تستخدم بروتوكول الإنترنت كمنصة تفاهم بين الأجهزة والشبكة . فعندما كانت الولايات المتحدة والاتحاد السوفيتي يسعيان لكسب تقدم علمي لكل منهما على حساب الأخر كان يتم تطوير الشبكات وتعزيز الأمن المناسب لها للتصدي لأي محاولة إختراق سيبراني ، وسعت المنظمات والمجالس الدولية أيضاً لوضع اتفاقيات دولية ناشدت فيها الدول على إصدار قوانين داخلية لتعزيز الأمن السيبراني لمكافحة الجريمة السيبرانية ومن أبرزها كما أوضحنا سلفًا اتفاقية الاتحاد الأوربي عام ٢٠٠١ واتفاقيات الأمم المتحدة المتعلقة بهذا الشأن .

ويمكننا أيضاً إبراز التطور التاريخي لبعض الجرائم المرتكبة بواسطة مجرمين سيبرانيين من خلال الجدول الآتي(٣) :

---

(١) صحيفة الشرق الأوسط الإلكترونية (https://aawsat.com)، المنشورة في ٢٩/ ٣/ ٢٠١٩ .

(٢) إنترنت الأشياء : هي شبكة عملاقة يتم من خلالها إتصال ملايين من الأجهزة والسيارات بشبكة الإنترنت ليتم من خلاله تمرير البيانات ، ومن أمثلة ذلك أنه يمكن استخدام إنترنت الأشياء في إدارة قطاع الطاقة ويتم من خلاله التحكم في العداد الذكي . ومن أبرز الأمثلة أيضاً قامت اسرائيل عام ٢٠١٠ بتعطيل المفاعل النووي لدولة إيران عن طريق فيروس باسم stux net ، وقام الهاكرز باختراق شبكة الكهرباء في أوكرانيا وأظلمت الدولة لعدة ساعات .

(3)Babak Akhgar , Andrew Staniforth, Francesca Bosco , Cyber Crime and Cyber Terrorism Investigator's HandbooK , BY : ELSEVIER , USE ,2014 , P 20 ,21 .

م	الأعوام	الجرائم السيبرانية
١	١٩٧٠	بدءًا من عام ١٩٧٠ وعلى مدار ثلاث سنوات، تلاعب عدد كبير من الصرافين في فرع park avenue لبنك union dime savings في نيويورك في معلومات الحسابات المتعلقة بالعملاء ومنذ ذلك الحين ظهرت الجرائم الالكترونية المتعلقة بالتزوير والاحتيال .
٢	١٩٧١	طور توماس " فيروس creeper " الذي أصاب الأنظمة في Arpanet وكانت تجربته غير مجرمة في ذلك الوقت .
٣	١٩٧٧	سرق شخص خلال عطلة الأسبوع المئات من شرائط الكمبيوتر الأصلية ونسخها الاحتياطية من مركز الكمبيوتر والتخزين الاحتياطي لشركة صناعة كيميائية تسمى lcl . وحاول ابتزاز أصحاب الشركة وطلب مبالغ مالية .
٤	١٩٨٨	أطلق روبرت موريس ، أول دودة كمبيوتر على الإنترنت أصابت آلاف الأنظمة ، وأدين بموجب قانون الاحتيال وإساءة استخدام الكمبيوتر وحكم عليه بثلاث سنوات وغرامة قدرها ١٠٠٠٠ دولار أمريكي
٥	١٩٨٩	"استغل البعض مرض نقص المناعة المكتسبة (الإيدز) وتم توزيع عدد كبير من النسخ الخاصة بأحد البرامج الذي يهدف في ظاهره إلى بعض النصائح عن المرض ، إلا أنه في حقيقته يحتوي على فيروس (حصان طرواده) ومجرد تشغيله يتعطل جهاز الحاسب الالي ثم تظهر عبارة بعد ذلك على الشاشة

		بطلب مبلغ مالي حتى يمكنه إرسال مضاد الفيروس وكان المتهم أمريكي وأرسل البرنامج من المملكة المتحدة "[1] .
٦	١٩٩٤	أجرى قراصنة روس ٤٠ عملية تحويل بلغت قيمتها الإجمالة أكثر من ١٠ ملايين دولار أمريكي من city bank إلى حسابات بنكية في فنلندا وروسيا وألمانيا وهولندا والولايات المتحدة وإسرائيل وسويسرا . وتم استرداد جميع الأموال باستثناء ٤٠٠ ألف دولار .
٧	١٩٩٧	أنشات EDT أداة لإنشاء نسخة إلكترونية من الاعتصامات على الإنترنت وفي ١٠ أبريل عام ١٩٩٨ ، تم استخدام أداة floodnet الخاصة بهم من قبل المتظاهرين في العديد من الدول ومنها المكسيك والولايات المتحدة الأمريكية
٨	١٩٩٨	تم التلاعب عن بعد من مخترقين بنظام محطة طاقة تعمل بالفحم ووضعها في وضع الطوارئ وأزال برنامج scada .
٩	٢٠٠٥	تم اختراق نظام تكييف الهواء الخاص بمركز كمبيوتر لأحد البنوك الأوربية ، وارتفعت درجة الحرارة وتسبب ذلك في إغلاق جميع خدمات نظام الكومبيوتر
١٠	٢٠٠٦	بدأت شبكة روسية تدعى RBN كنقطة مركزية لجرائم البريد الإلكتروني والتصيد الاحتيالي وأحصنة طروادة
١١	٢٠١٠	في هذا العام ظهرت الدودة الحاسوبية STUX NET وتم استهداف أنظمة التحكم في محطة تخصيب اليورانيوم في

(١) أحمد خليفة الملط ، الجرائم المعلوماتية ،دراسة مقارنة ، دار الفكر الجامعي بالاسكندرية ، الطبعة الثانية ، عام ٢٠٠٦ م ، ص ١٦

		إيـران. كـان تأثيرهـا هـو أنهـا قامـت بـشكل سري بـالتحكم الإلكتروني في سرعة أجهزة الطرد المركـزي الفائقـة ممـا أدى إلى اختراقها
١٢	٢٠١١	تـم إخـتراق صـفحات الويـب لوكالـة الاسـتخبارات البريطانيـة وتم استبدال المحتوى إلى وصفات لصنع الكعك .
١٣	٢٠١٢	حـدث هجـوم عـلى شركـة أرامكـو المتخصـصة في مجـال البترول في المملكة العربية السعودية وكـان واحـداً مـن أشرس الهجمات السيبرانية الأكثر ضرراً على الأعمال التجارية [١]
١٤	٢٠١٣	أوائـل عـام ٢٠١٣ اتهمـت النيابـة العامـة في أمريكـا الـشمالية ثلاثة رجـال أوروبيـين بإنتـاج وتوزيـع فيـروس حاسـوبي ألحـق الضرر بأكثر مـن مليـون جهـاز حاسـوب عـلى مـستوى العـالم، وتمكنـوا مـن الوصـول إلى معلومـات بـشأن حـسابات بنكيـة شخصية، واستولوا على ٢١ مليـون دولار أمريكـي عـلى الأقـل والفيروس كان يسمى (gozi) [٢].
١٥	٢٠١٩	شـنت إيـران حملـة للتجـسس الـسيبراني اسـتهدفت شـبكات حساسة في الكويـت وخـلال النـصف الأول عـام ٢٠٢٠ بلغـت الهجـمات الالكترونيـة نحـو ١٣٠٥ هجمـة مرتبطـة بفـيروس (covid 19) [٣].

(١) موقع باللغة العربية ، https://www.bahrainedb.com/ .

(٢) موقع باللغة الإنجليزية ، https://www.fbi.gov/ .

(٣) تصريح ألينا رومانوسكي ، السفيرة الأمريكية لدى دولة الكويت ، منشور في جريـدة الـراي الكويتيـة – العدد الصادر بتاريخ ٩/ ٣/ ٢٠٢١ .

١٦	٢٠٢٠	تم اختراق شبكات ١٨٠٠ مؤسسة أمريكية ، تضررت منها ٥٠ شركة ضرر شديد ، وارتكبت الجريمة أيضاً على وزارتي الأمن الداخلي والدفاع . [١]

يتبين من هذا الجدول أن القراصنة قد استغلوا نقاط ضعف تكنولوجيا المعلومات والاتصالات والسلوك البشري وارتكبوا جرائم سيبرانية جسيمة تهدد أمن واستقرار الدول والأفراد .

(١) موقع ال BBC بالعربي ، WWW.BBC.COM ، منشور في ٢١ ديسمبر عام ٢٠٢٠ .

الفرع الثاني : تعريف الأمن السيبراني

لا شك أن وجود الجرائم السيبرانية يفرض على الدول التزام بتحقيق الأمن السيبراني وقبل تعريف الأمن السيبراني لابد من التطرق إلى تعريف كلمة الأمن أولاً ونعرضها على النحوالآتي:

أولاً : تعريف الأمن :

الأمن لغة : كما جاء في معجم المعاني الجامع أنه من الفعل أمِنَ : أي إطمأن ولم يخف وهو الطمأنينة وعدم الخوف والثقة وعدم الخيانة .

الأمن إصطلاحاً : عرفه البعض بأنه "القدرة التي تتمكن بها الدولة من إطلاق مصادر قوتها الداخلية والخارجية والاقتصادية والعسكرية في شتى المناحى لمواجهة مصادر الخطر في الداخل والخارج في حالتي السلم والحرب . مع إستمرار الإنطلاق المؤمن لتلك القوى في الحاضر والمستقبل" . (١)

وبالنسبة للتعريف الإجرائي للأمن : فيعرفه البعض بأنه "شعور الإنسان بالطمأنينة على نفسه وما يتصل به من عرض ومال ومسكن وملبس وطعام . وإذا ما تم إضافة لفظ الأمن إلى أى مجال من المجالات إنحصر معنى الأمن فيما أضيف إليه" .(٢)

ثانياً : الأمن السيبراني :

عرف بعض الفقهاء الأمن السيبراني أنه " أمن الشبكات والأنظمة المعلوماتية والبيانات والمعلومات والأجهزة المتصلة بالإنترنت ، وهو المجال الذي يتعلق بإجراءات ومقاييس

---

(١) مشارإليه : عبدالرحمن بجاد شارع العتيبي ، دور الأمن السيبراني في تعزيز الأمن السيبراني ، رسالة قدمت لنيل درجة الماجستير في العلوم الإستراتيجية ، جامعة نايف العربية للعلوم الأمنية ، كلية العلوم الإستراتيجية قسم الأمن الإنساني ، السعودية ، عام ٢٠١٧ ، ص ٦ .

(٢) عبدالرحمن بجاد شارع العتيبي ، المرجع السابق ، ص ٧ .

ومعايير الحماية المفروض اتخاذها ، أو الالتزام بها ، لمواجهة التهديدات ، ومنع التعديات ، أو للحد من اثارها في أقسى وأسوأ الاحوال " [١]

وعرفه آخرون بأنه التقنيات والإجراءات التي تهدف إلى حماية أجهزة الكمبيوتر والشبكات والبيانات من الدخول غير القانوني ونقاط الضعف والهجمات المنقولة عبر الإنترنت من قبل الجانحين السيبرانيين [٢].

وقد عرفه آخرون بأنه " عبارة عن مجموع الوسائل التقنية والإدارية التي يتم القيام بها لمنع الاستخدام غير المشروع ، وسوء الاستغلال للمعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها . بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات الشخصية ولحماية المواطنين من المخاطر في الفضاء السيبراني " [٣]

وقد عرفه فريق العمل المشترك المعني بتعليم الأمن السيبراني في جامعة جورج واشنطن أنه نظام قائم على الحوسبة يشمل التكنولوجيا والأشخاص والمعلومات والعمليات المؤكدة ، ويشمل إنشاء وتشغيل وتحليل واختبار أنظمة الكمبيوتر الآمنة . إنها دورة دراسة متعددة

---

(١) مشار إليه : عبدالله يحي سعيد الزهراني ، استراتيجيات الأمن السيبراني في ضوء التقنيات والتحديات الحديثة ،دراسة مقارنة ، رسالة قدمت لنيل درجة الماجستير في العلوم الإستراتيجية ، جامعة نايف العربية للعوم الأمنية ، كلية العلوم الإستراتيجية قسم الدراسات الاستراتيجية ، السعودية ، عام ٢٠٢٠ ، ص ١١ .

(2)K. K. Panigrahi , Information Security and Cyber Law , published by tutorials point ,2015 ,p.1.

(٣) عبدالرحمن بجاد شارع العتيبي ، دور الأمن السيبراني في تحقيق رؤية ٢٠٣٠ ، المرجع السابق ، ص ١٣.

التخصصات ، بما في ذلك الجوانب القانونية والسياسية والعوامل البشرية والأخلاق وإدارة المخاطر "[١] .

"وقد ذهب الكاتبان Neittaanmäki Pekka,Lehto Martti في كتابهما المعنون Cyber Security: Analytics, Technology and Automation ، إلى أن الأمن السيبراني هو: "عبارة عن مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة". وعرفه إدوارد أمورسو Amoroso Edward بأنه: "وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة"[٢] .

وفي عام ٢٠١٠ صدر تقرير من الاتحاد الدولي للاتصالات (itu) عرف من خلاله 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 وموجدات المؤسسات والمستخدمين " [٣] .

---

(١) عبدالرحمن بجاد شارع العتيبي ، دور الأمن السيبراني في تحقيق رؤية ٢٠٣٠ ، رسالة قدمت لنيل درجة الدكتوراه في الفلسفة في الدراسات الاستراتيجية ، جامعة نايف للعلوم الأمنية ، كلية العلوم الإستراتيجية قسم الدراسات الاستراتيجية ، السعودية ، عام ٢٠٢٠ ، ص ١٢.

(٢) موقع : https://political-encyclopedia.org/

(٣) تقرير صادر عن الاتحاد الدولي للاتصالات ، التابع للأمم المتحدة ، عام ٢٠١٠ . وراجع أيضاً :

Ramjee Prasad • Vandana Rohokale , Cyber Security: The Lifeline of Information and Communication Technology , 2019 , india , publisded by springer , p. 3 .

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". [١].

ومن الجدير بالذكر أن الأمن السيبراني له مفهوم أوسع من أمن المعلومات، فأمن المعلومات يهتم بأمن المعلومات الفيزيائية . أما الأمن السيبراني يهتم بأمن كل ما هو موجود على السايبر .

ولكي نعرف الأمن السيبراني بشكل أوضح لابد من التطرق لبعض التعريفات المرتبطة به ونوضحها في الجدول الآتي [٢]:

المصطلح	التعريف
هجوم Attack	أي نوع من أنواع الأنشطة الخبيثة التي تسعى إلى الوصول بشكل غير مشروع إلى المعلومات أو جمع موارد النظم المعلوماتية، أو تعطيلها أو منعها أو تحطيمها أو تدميرها.
الحماية من التهديدات المتقدمة المستمرة Advanced Persistent Threat (APT) Protection	الحماية من التهديدات المتقدمة التي تقوم باستخدام أساليب خفية، هادفة إلى الدخول غير المشروع على الأنظمة والشبكات التقنية، ومحاولة البقاء فيها لأطول فترة ممكنة، وذلك بواسطة تفادي منظومات الكشف والحماية.
النسخ الإحتياطية Backup	"الملفات والأجهزة والبيانات والإجراءات المتاحة للاستخدام في حالة الأعطال أو

(١) موقع : https://political-encyclopedia.org/ ، المرجع السابق .

(٢) الهيئة الوطنية للأمن السيبراني السعودي ، الضوابط الأساسية للأمن السيبراني ، نسخة إصدار رقم (١) ، عام ٢٠١٨ .

	الفقدان، أو إذا حذف الأصل منها أو توقف عن الخدمة".
توافر Availability	"ضمان الوصول إلى المعلومات والبيانات والأنظمة والتطبيقات واستخدامها في الوقت المناسب."
صلاحية المستخدم Authorization	الخاصية التي من خلالها يتم تحديد والتأكد من حقوق/ تراخيص المستخدم التي تتيح له الوصول إلى الموارد والأصول المعلوماتية والتقنية للجهة، والسماح له وفقًا لما تم تحديده مسبقًا في حقوق/ تراخيص المستخدم.
الدائرة التلفزيونية المغلقة CCTV	"يستخدم التليفزيون ذو الدائرة المغلقة، والمعروف أيضًا باسم المراقبة بالفيديو، كاميرات الفيديو لإرسال إشارة إلى مكان محدد على مجموعة محدودة من الشاشات. وغالبًا ما يطلق هذا المصطلح على تلك التقنية المستخدمة للمراقبة في المناطق التي قد تحتاج إلى مراقبة حيث يشكل الأمن المادي مطلبًا هامًا فيها"
الحوسبة السحابية Cloud Computing	"نموذج لتمكين الوصول عند الطلب إلى مجموعة مشتركة من موارد تقنية المعلومات مثل (: الشبكات والخوادم والتخزين والتطبيقات والخدمات) التي يمكن توفيرها بسرعة وإطلاقها بالحد الأدنى من الجهد الإداري التشغيلي

	والتدخل/ التفاعل لإعداد الخدمة من مزودي الخدمة. وتسمح الحوسبة السحابية للمستخدمين بالوصول إلى الخدمات القائمة على التقنية من خلال شبكة الحوسبة السحابية دون الحاجة لوجود معرفة لديهم أو تحكم في البنية التحتية التقنية التي تدعمهم. ويتألف نموذج الحوسبة السحابية من خمس خصائص أساسية هى خدمة ذاتية حسب الطلب، ووصول إلى الشبكة بشكل واسع، ومجمع الموارد، ومرونة سريعة، والخدمة المقاسة. "
انتهاك أمني Compromise	الإفصاح عن معلومات لأشخاص غير مصرح بتسريبها أو الحصول على تلك المعلومات، أو انتهاك السياسة الأمنية السيبرانية للجهة بالإفصاح عنها، أو تغيير أو تخريب أو فقد شيء بقصدٍ أو بغير بقصد. ويُقصد بالانتهاك الأمني: الإفصاح عن الحصول على بيانات حساسة أو تسريبها أو تغييرها أو تبديلها أو استخدامها بدون تصريح (بما في ذلك مفاتيح تشفير النصوص وغيرها من المعايير الأمنية السيبرانية الحرجة).
السرية Confidentiality	"الاحتفاظ بقيود مصرح بها على الوصول إلى المعلومات والإفصاح عنها بما في ذلك وسائل حماية معلومات الخصوصية والملكية الشخصية"

الأمن من خلال التصميم Security-by-Design	"منهجية لتطوير الأنظمة والتطبيقات وتصميم الشبكات التي تسعى إلى جعلها خالية من نقاط الضعف والثغرات الأمنية السيبرانية، والمقدرة على صد الهجوم السيبراني قدر الإمكان من خلال عدة تدابير على سبيل المثال: الاختبار المستمر، وحماية المصادقة والتمسك بأفضل ممارسات البرمجة والتصميم، وغيرها"
جدار الحماية لتطبيقات الويب Web Application Firewal	"نظام حماية يوضع قبل تطبيقات الويب لتقليل المخاطر الناجمة عن محاولات الهجوم الموجهة على تطبيقات الويب".

ومن خلال التعريفات سالفة البيان وحتى لا يختلط على الباحثين التفرقة بين الأمن السيبراني وأمن المعلومات فيجب أن يشمل تعريف الأمن السيبراني، الأمن الإلكتروني والأمن الرقمي ، ويمكن تعريف الأمن السيبراني بأنه (كل الإجراءات التي تتخذ لحماية الاتصالات والشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ، ومكوناتها من برمجيات وأجهزة ، وما تقدمه من خدمات ، وما تحتويه من بيانات ، سواء كانت حماية سابقة وقائية بواسطة وضع أنظمة حماية من المخاطر المحتملة أو حماية لاحقة من أي هجوم سيبراني أو اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع ويشمل أيضاً المحافظة على البنى التحتية الحساسة للدولة من هجمات الروبوتات وغيرها وسواء ارتكبت الجريمة السيبرانية عن طريق الجهات الحكومية أو غير الحكومية) وينظم الإجراءات الخاصة بالأمن السيبراني وفقاً للقوانين واللوائح الوطنية للدولة .

ومن الجدير بالذكر أن الأمن السيبراني هو مصطلح يستخدم لوصف قدرات بلد أو منظمة أو شركة في الحماية من الهجمات الفيروسية . وهناك العديد من الأدوات التي تم استخدامها كما سبق أن أوضحنا، لتقييم وضع الأمن السيبراني. -مثال على هذه الأداة – هو مؤشر الأمن

السيبراني العالمي (g c l)التابع للاتحاد الدولي للاتصالات. وهي أداة لبناء القدرات تقيم التزام البلدان بالأمن السيبراني وتحدد قدراته لديها ومجالات التحسين. ويمكن تقييم وضع الأمن السيبراني للبلدان بناءً على تطورها في الركائز الخمس (القانونية والتقنية والتنظيمية وبناء القدرات والتعاون) ، ومن هذا المنطلق لابد من التطرق لتوضيح التفرقة بين المعلومات والبيانات ، المشمولين بحماية الأمن السيبراني .

الفرع الثالث: تعريف المعلومات والبيانات

أولاً : تعريف المعلومات :

(أ) : لغةً : كما جاء في معجم المعاني الجامع أنها مشتقة من الفعل علم : أي أحاط بالشئ وهى جمع معلومة وتعني أخبار وتحقيقات أو كل ما يؤدي إلى كشف الحقائق وإيضاح الأمور وإتخاذ القرارات ، وإصطلاحًا :" المعنى المستنتج من البيانات حسب ما جرى عليه العرف والخبرة" [١] .

(ب) : ومن جانب الفقه عرف أحد الفقهاء المعلومات أنها : " مجموعة رموز يستخلص منها معنى مُعين في مجال محدد وتتمتع بالتحديد والابتكار والسرية والاستئثار "[٢] .

ويرى البعض الأخر أنها " عامل من عوامل اتخاذ القرارات وعُنصر من عناصر الملاءمة [٣] .

ويرى أحد الفقهاء أنها " مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح أن تكون محلاً للتغيير أو للتأويل " interpretation " ، أو للمعالجة " processing " ، سواء بواسطة الأفراد أو الأنظمة الإلكترونية ، وهى تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها ، أو نقلها بوسائل وأشكال مختلفة " . [٤]

---

(١) د / هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الألات الحديثة ، عام ١٩٩٤ ،بدون رقم طبعة القاهرة ، ص ٢٦ .

(٢) د / أحمد خليفة الملط ، الجرائم المعلوماتية ،دراسة مقارنة ، مرجع سابق ، ص ٧٤ .

(٣) د / أحمد حسام طه تمام ، الجرائم الناشئة عن استخدام الحاسب الآلي ، دراسة مقارنة ، دار النهضة العربية ، القاهرة ، عام ٢٠٠٠ ، ص ٤١ .

(٤) د / عمرو إبراهيم الوقاد ، الحماية الجنائية للمعلوماتية ، دار النهضة العربية ، القاهرة ، بدون رقم طبعة ، عام ١٩٩٩ ، ص ٩٣ .

ويرى البعض أن المعلومات هى : المعنى الذي يستخلص من هذه البيانات [١] ، ويدلل البعض على هذه التفرقة بين البيانات والمعلومات بالمثال التالي : إن عبارة " le soleil prille " باللغة الفرنسية - على سبيل المثال - تعني أن الشمس مشرقة ، وهي لا تعدو أن تكون بياناً للشمس ،[٢] ولا يمكن أن تتحول إلي معلومة إلى أحد الأشخاص إلا بتوافر شرطين ، الأول : أن يطلع عليها بالفعل والثانى : أن يكون هذا الشخص مطلع وعلى علم باللغة الفرنسية ؛ حتى يستطيع أن يتفهمها وحتى يتحقق هذان الشرطان تظل البيانات مجموعة من الحروف ، ولا يمكن أن تتحول المعلومة إلا بتوافرهما [٣] .

ويمكننا القول أن المعلومات المشمولة بحماية الأمن السيبراني هي المعلومات التي يتم نقلها عبر شبكات المعلومات وغيرها من أجهزة التكنولوجيا الحديثة.وينبغي أن يتوافر في المعلومات عنصران أساسيان هما التحديد والابتكار من ناحية ، ومن ناحية أخرى السرية والاستئثار لأن المعلومة غير السرية تقبل التداول ولابد من التحديد لأن الحق ينبغي أن يرد على محل محدد ، وكذلك الاستئثار ضروري لأن الشئ الذي لا يمكن حيازته والانفراد به لا يعتبر حقاً [٤] .

ثانيا : تعريف البيانات :

عرفها أحد الفقهاء أنها : كيان مادي محسوس ، ويتمثل في نبضات إلكترونية أو إشارات ممغنطة ، ويمكن تخزينها لوسائط أوعية معينة ونقلها واستغلالها وإعادة إنتاجها ، وبالإضافة إلى

---

(١) د/ حمام عبداللطيف عبدالشافي حنفي معوض ، الحماية الجنائية للبرامج والبيانات المعالجة إلكترونيًا ، دراسة مقارنة ، رسالة قدمت لنيل درجة الدكتوراه حقوق القاهرة ، عام ٢٠١٧ ، ص ٢٠ .

(٢) د / نائلة عادل محمد قورة ، جرائم الحاسب الألي الاقتصادية ،دراسة نظرية وتطبيقية ، دار نشر الحلبي ، عام ٢٠٠٥ ، الطبعة الأولى ، ص ٩٤

(٣) د / عمرو إبراهيم الوقاد ، الحماية الجنائية للجرائم المعلوماتية ، مرجع سابق ، ص٩٤ .

(٤) جزار منصورية – الجريمة المعلوماتية ، رسالة للحصول على شهادة الماجستير في الحقوق والعلوم السياسية ، جامعة عبدالحميد بن باديس ، الجزائر ، عام ٢٠١٦ / ٢٠١٧ ، ص ٧ .

إمكانية تقديرها أو قياسها ؛ إذًا هي ليست شيئًا معنويًا كالحقوق والأفكار [١] .

وعرفها كذلك أحد الفقهاء بأنها : " الفعل المفهوم أو التعليمات المتمثلة في شكل اصطلاحي مهيأة للاتصال والتفسير أو للمعالجة بواسطة وسائل انسانية أو آلية " [٢].

وقد وضعت اتفاقية بودابست لمكافحة الجرائم المعلوماتية تعريفًا للبيانات المعلوماتية وهي " أية عمليات عرض للحقائق أو المعلومات أو المفاهيم في قالب مناسب لعملية معالجة داخل منظومة الكمبيوتر ، بما في ذلك برنامج مناسب لجعل منظومة كمبيوتر تؤدي وظائفها ". [٣]

ويرى رأي أخر من الفقه أنه يجب التفرقة بين مصطلحين وهما البيانات والمعلومات – لأن البعض يستخدمهما كمترادفين – رغم أن لكل منهما مدلوله المختلف فالمقصود بالبيانات Data أو DONNEES هي: المدخلات للحاسب الإلكتروني INPUTS التي تمثل الخامات التي يتم تشغيلها .

أما المعلومات INFORMATIONS فهي : المخرجات OUT PUTS الناتجة من معالجة البيانات التي تم إدخالها وهذا ما يؤكده التعريف اللغوي لكل من البيانات والمعلومات، فيعرف القاموس البيانات بأنها: حقائق أو أشياء معروفة يقينًا ، ويمكن منها الوصول إلي نتائج معينة . أما المعلومات هى تقديم أخبار أو معرفة ، بمعنى أى شي يضيف إلى الشخص معرفة جديدة . وبالرغم من هذا الفرق بين البيانات والمعلومات لا يمكن وضع حد فاصل دقيق بين ما يعتبر بيانات (مدخلات) وما يعتبر (مخرجات) فالتداخل قائم بينهما ، وما يعد معلومات في بعض المراحل يعد بيانات في مراحل أخرى إذا أجري عليه معالجة [٤] .

---

(١) د/ حمام عبداللطيف عبدالشافي حنفي معوض ، مرجع سابق ، ص ٢٠ .

(٢) د/ حاتم عبدالرحمن منصور الشحات ، الإجرام المعلوماتي ، الطبعة الأولي ،عام ٢٠٠٢ ، دارالنهضة العربية ، القاهرة ، ص ٢٨ .

(٣) اتفاقية بودابست لمكافحة الجرائم المعلوماتية ، الفقرة (ب) من المادة الأولى من القسم الأول من الاتفاقية، ص ٤ .

(٤) د/ أسامة عبدالله قايد ، الحماية الجنائية للحياة الخاصة وبنوك المعلومات ، دراسة مقارنة في القانون الفرنسي والأمريكي والمصري وفقًا لأخر التعديلات التشريعية ، المرجع السابق ، ص ٧٧ – ٧٨ .

المطلب الثاني : الأهداف المرتبطة باستراتيجية الأمن السيبراني :

التعريف الاصطلاحي للاستراتيجية :

عرفها البعض أنها " مجموعة من الإجراءات أو الأنشطة ، التي تقود وتوجه استخدام الموارد لتحقيق الرؤية والأهداف ، وتحقيق الميزة التنافسية المستدامة " [١]

وإجرائياً تعرف أنها : " الخطط المستقبلية التي تضعها الدولة والمؤسسات لحماية معلوماتها من التهديدات الخارجية [٢].

وتعتمد استراتيجيات دول مجلس التعاون المتعلقة بالأمن السيبراني لمواجهة الجرائم السيبرانية على عدة محاور وهى : محور التكامل ، محور التنظيم ، محور التوكيد ، محور الدفاع ، محور التعاون بين دول المجلس ، ومحور البناء.

ونجمل الأهداف المرتبطة بالأمن السيبراني في الجدول الأتي :

١ : الهدف الاستراتيجي للأمن السيبراني هو حماية الفضاء السيبراني	يهدف الأمن السيبراني بشكل عام إلى مواجهة الجرائم السيبرانية ومخاطرها، ويهدف إلى تعزيز الثقة في البنى التحتية للاتصالات والمعلومات وتطبيقاتها وخدماتها في جميع المجالات والقطاعات، والعمل على تأمينها من خطر الاختراق، وذلك تحقيقًا لبيئة رقمية تتصف بالأمان، وتكون موثوقةً لدى دول مجلس التعاون الخليجي.
٢ : حوكمة متكاملة للأمن السيبراني على مستوى دول مجلس التعاون	ويكون ذلك عن طريق تحقيق قدر كبير من التنسيق، وتبني توجه شامل للأمن السيبراني بين

(١) عبدالله يحيى سعيد الزهراني ، المرجع السابق ، ص ١٠ .

(٢) عبدالله يحيى سعيد الزهراني ، مرجع سابق ، ص ١١.

	دول مجلس التعاون الخليجي، وذلك ضمانا لإسهام خطط هذه الدول في تنفيذ التشريعات الوطنية والدولية المعنية بذلك الشأن، ويجب أن يعتمد رئيس الجهة – حكومية كانت أو خاصة- استراتيجية للأمن السيبراني ، ويتطلب منه القيام بإنشاء إدارة مستقلة تتعلق بالأمن السيبراني، تتحدَّدُ فيها مسئولياتُ كل مشارك في عملية الأمن السيبراني، ويتم فيها اتباع الأساليب الحديثة في تقييم المخاطر الأمنية، وكذلك يتم التأكد من كون البرامج المستخدمة في تحقيق الأمن السيبراني متوافقةً مع قوانين دول مجلس التعاون أم لا، لاسيما الدولة التي يقع فيها الاختراق الأمني .
٣: إدارة فعالة للمخاطر السيبرانية على مستوى دول مجلس التعاون .	تهدف إلى إدارة المخاطر المحتملة على مستوى دول المجلس، وكذلك تهدف إلى أن تضع لها أفضل الحلول، وأن تختار أفضل الخيارات لحل هذه المشاكل الأمنية، وذلك سعيا لحماية الجهات داخل هذه الدول عن طريق وضع بعض الضوابط المتعلقة بمنع الوصول غير المصرح له للمخترقين، وكذلك

	وضع أولوية لحماية الأجهزة ونظم المعلومات والبريد الإلكتروني والشبكات والأجهزة المحمولة.
٤: تعزيز الشراكات والتعاون في مجال الأمن السيبراني	يتطلب الأمن السيبراني تعزيزًا للتعاون بين دول المجلس وبين مؤسسات القطاع الخاص المعنية بالأمن السيبراني، سواء على مستوى دول الخليج أو على المستوى العالمي، ويكون ذلك – أيضا -بمشاركة مؤسسات المجتمع المدني.
٥: من أهم الأهداف : تطوير صناعة الأمن السيبراني على مستوى دول مجلس التعاون لدول الخليج العربية ، وبناء القدرات البشرية .	يجب وضع الخطط الخاصة بتنمية صناعة التكنولوجيا، وذلك بوصفها من أهم الصناعات العالمية الحالية، والتي تتعلق بالأمن السيبراني، مع الاستمرار في تدعيم القدرات البشرية، من خلال تدعيم الكوادر الخاصة بذلك، وإلحاقهم بالبرامج التعليمية والتدريبية الملائمة .

وبعد أن أوضحنا الأهداف المرتبطة باستراتيجية الأمن السيبراني نقسم هذا المطلب إلى فرعين .

الفرع الأول : خصائص وسمات الأمن السيبراني .

يتميز الأمن السيبراني بعدة سمات ومن أهمها :

١ : الأمن السيبراني ليس مسار عمل لمرة واحدة ؛ إنما هو عملية مستمرة ويحتوي على آليات دفاع مبتكرة لكونه يواجه التهديدات التي تقع على الأنظمة والشبكات وغيرها .

٢: يعمل على خلق نظام بيئي سيبراني آمن وإنشاء نظام موثوق به .

٣: يقوم بعملية وقائية رقابية مسبقة بهدف البحث عن المخاطر والعمل على حلها وسد الثغرات .

٤: يعمل على الدفاع اللاحق والذي يتمثل في قاعدة إرجاع الوضع إلى ما كان عليه .

٥: يوفر خاصية التنبيه إلى وجود خطأ أو إساءة استخدام الشبكات التي تعرض البيانات والمعلومات إلى الخطر من داخل المؤسسات .وأيضاً تغطية المخاطر الخارجية ومراقبة التهديدات .

الفرع الثاني : أبعاد وتطورات الأمن السيبراني

إذا وضعنا في الاعتبار طبيعة المخاطر والتهديدات وأبعاد الأمن السيبراني ، يمكن ترتيب المشكلات التي تواجهها دول مجلس التعاون لدول الخليج العربية ، من أهمها : عدم اكتمال التشريعات الداخلية المتعلقة بالأمن السيبراني ، ضعف التعاون بين دول المجلس ، سواء على المستوى الداخلى للدول أو على المستوى الخارجي ، وللأمن السيبراني أبعادغالباً ما تكون متعلقة بالأمن القومي وتعد هذه الأبعاد مختلفة ونجمل أهمها في الأتي :

أولاً : الأبعاد العسكرية :

بدأت دراستنا بالتطور التاريخي للإنترنت وما تبعه من تطور أساليب الأمن السيبراني ، وأوضحنا أنه قد نشأ في بيئة عسكرية ، ثم انتقل بعد ذلك إلى المجال العلمي الذي يخدم أيضاً تطوير القدرات العسكرية التي تحافظ على تفوق الدولة على الدول الأخرى .

ويلعب الأمن السيبراني دوراً هاماً في عملية تبادل المؤسسات العسكرية المعلومات الهامة بشكل إلكتروني إفتراضي بدون اختراق هذا التواصل ، مما ينعكس ذلك إيجابياً على تحقيق الأهداف العسكرية لدول مجلس التعاون كافة .

ثانياً : الأبعاد السياسية

يشكل الأمن السيبراني دوراً هاماً في الحياة السياسية ، حيث تعاظم هذا الدور في ظل إعتماد المواطنين على مواقع التواصل الأجتماعي في حياتهم اليومية والتقنيات الحديثة ، فالأمن السيبراني له دور في الحملات الإنتخابات البرلمانية ، والاحتجاجات الإلكترونية وغيرها .

ثالثاً : الأبعاد الاقتصادية والإجتماعية :

البعد الاقتصادي يتعلق بمجالين رئيسيين ، الأول : صناعة تكنولوجيا المعلومات والاتصالات ، ويشمل تطوير الأجهزة والبرمجيات وانتاجها ، والثاني : التجارة الإلكترونية من خلال فتح سوق حر على شبكة الإنترنت [1] ومن أشهر الأمثلة تقديم خدمات المحفظة الإلكترونية .

ويمكن أيضاً أن تنمو سوق الأمن السيبراني على مستوى دول مجلس التعاون وذلك بالإعتماد على شراء منتجات وخدمات الأمن السيبراني من تقنيات متعلقة بحماية الأجهزة والكشف عن التهديدات السيبرانية .

ويتعلق البعد الإجتماعي بكثرة تواصل الأفراد بين بعضهم البعض عن طريق المدونات والبريد الإلكتروني ومواقع التواصل الإجتماعي ،والذي يشكل ما يمكن تسميته الجمهور

---

(١) عرف بعض الباحثين الأمن القومي أنه : قدرة الدولة على تأمين استمرار أساس قوتها الداخلية أو الخارجية ، والعسكرية ، والاقتصادية في مختلف مناحي الحياة لمواجهة الأخطار التي تهددها من الداخل والخارج ، وفي حالة الحرب والسلم على حد سواء . راجع : علاء عبدالحفيظ محمد عبدالجواد ، العلاقة بين الأمن القومي والدبمقراطية . رسالة قدمت لنيل درجة دكتوراه الفلسفة في العلوم السياسية ، كلية الاقتصاد والعلوم السياسية ، القاهرة ، عام ٢٠٠٩ ، ص ٤٣ .

العابر للحدود والأوطان أو جمهور العالم الافتراضي ، وبالتالي لابد من تأمين هذه الشبكات والمواقع . ولكن على النقيض قد يعرض أخلاق المجتمعات للخطر ويسبب تهديد السلم الاجتماعي لدول مجلس التعاون .

ويرتبط البعد الإجتماعي أيضاً بالمجالات العلمية، والثقافية، والخدمية، حيث تسمح بالوصول الى مناطق بعيدة، والى فئات محددة، ككبار السن، والمرضى، وغيرهم من ذوي الاحتياجات الخاصة.

بالإضافة إلى الدور الذي يمكن أن يؤديه، في تبادل المعلومات، في أوقات الازمات الإنسانية والكوارث، ولا تقف الابعاد الاجتماعية عند حدود توفير اطمئنان المواطن إلى حياته اليومية، والاستفادة من طاقات تقنيات المعلومات والاتصالات، في تطوير نشاطاته المختلفة، بل تتعداها، إلى صيانة القيم الجوهرية في المجتمع: كالانتماء، والمعتقدات . [1]

رابعاً : الأبعاد القانونية :

ترتب على ثورة المعلومات والاتصالات والتكنولوجيا بصفة عامة أنماط حديثة من السلوك الذي يشكل أفعالاً مخالفة يترتب عليها المسئولية الجنائية والمدنية [2] ،ونتج عن ذلك أيضاً فرض أطر تشريعية حديثة للجرائم المرتكبة ضد الفضاء السيبراني لتواكب هذه التطورات المتسارعة في التكنولوجيا ، وتفعيل أسس التعاون الدولي المشترك لمكافحة الجريمة السيبرانية . ومن أبرز الممارسات القانونية في نطاق الأمن السيبراني هو ضمان بعض

---

(١) عبدالرحمن عاطف أبوزيد ، بحث في الأمن السيبراني في الوطن العربي ، دراسة حالة المملكة العربية السعودية ، المركز العربي للبحوث والدراسات ، العدد ٤٨ ، عام ٢٠١٩ ، ص ٥٥ .

ولمزيد من التفصيل حول دور الإنترنت في المعاملات التجارية والمصرفية ، أ . د / هدي حامد قشقوش ، بحث الجرائم المعلوماتية ، منشور بمركز بحوث الشرطة بإكاديمية مبارك للأمن ، العدد العشرون – يوليو ٢٠٠١ة- ربيع ثان ١٤٢٢ ، ص ٢١٧ .

(٢) د: منى الأشقر جبور ، بحث بعنوان : الأمن السيبراني: التحديات ومستلزمات المواجهة ، اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني بيروت ٢٧ – ٢٨ أغسطس (آب) ٢٠١٢ ، المركز العربي للبحوث القانونية والقضائية / جامعة الدول العربية ، ص ١٦ .

الحقوق في هذا المجال ومن أهمها : حق النفاذ إلى الشبكة المعلوماتية ، وشملت الأشكال الجديدة المتعلقة باستخدام تقنية المعلومات والاتصالات ، كالحق في إنشاء المدونات الإلكترونية ، والحق في ملكية البرامج الثقافية [١] .

(١) الدكتور المستشار / عبدالفتاح بيومي حجازي ، الجريمة في عصر العولمة ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، عام ٢٠١٠ ، ص ٦١ .

المبحث الثاني :
نماذج إجرامية تمثل تحديات سيبرانية تواجه دول مجلس التعاون الخليجي

هناك عدة تحديات تواجه دول مجلس التعاون في الحفاظ على هويتها الرقمية وحماية أمنها المعلوماتي وسنحاول إلقاء الضوء على هذه التحديات في السطور التالية :

المطلب الأول : أبرز النماذج الإجرامية التي تواجه دول مجلس التعاون

أضحى تأمين الفضاء الإلكتروني أحد التحديات الرئيسية في بداية القرن الحادي والعشرين،نتيجة التقدم التكنولوجي والمرشح إلى مزيد من التطور والولوج في أنشطة لا تخطر على بال إنسان ، وتزايد التهديدات التي أصبحت تمس الأمن القومي للدول وعليه نقسم هذا المطلب إلى فرعين :

الفرع الأول :
أبرز التحديات المستقبلية التي تواجه الأمن الوطني لدول مجلس التعاون .

التحدي الأول للأمن السيبراني : طبيعة التهديدات

طبيعة التهديد من بين التحديات الأكثر خطورة في القرن الحادي والعشرين ، فالتهديدات السائدة والمحتملة في مجال الأمن السيبراني . تنبع من مصادر عديدة ، فتأخذ شكل أنشطة تخريبية تستهدف الأفراد والشركات والبنى التحتية الوطنية للدول. وتتسبب آثار هذه التهديدات في مخاطر كبيرة متعلقة بالأتي :

١ : السلامة العامة .

٢: أمن الدول ، واستقرار المجتمع الدولي المترابط عالمياً .

ويمكن إخفاء الاستخدام الضار لتكنولوجيا المعلومات بسهولة ، ومن الصعب تحديد أصل أو هوية المجرم، حتى الدافع وراء الجريمة ليس بالمهمة السهل اكتشافها. ويمكن لممثلي التهديد العمل بحرية كبيرة من أي مكان تقريبًا. ويمكن أن تكون دوافع الاختراق : إظهار البراعة التقنية ببساطة ، سرقة أموال ، معلومات ، إلخ، و يشكل المجرمون والإرهابيون

، وأحيانًا الدولة نفسها مصدر هذه التهديدات فيستخدم المجرمون والمتسللون أنواعًا مختلفة من الأدوات والأساليب الضارة إلى جانب اتخاذ الأنشطة الإجرامية أشكالًا جديدة كل يوم [١] .

التحدي الثاني : سهولة محو الدليل أو تدميره :

يجد الأمن السيبراني صعوبة غالباً بسبب سهولة محو الجاني الدليل أو تدميره في فترة زمنية وجيزة ، بالإضافة إلى سهولة تنصله من هذا العمل الإجرامي ، فمن أهم التحديات التي تواجه الأمن السيبراني وتعوق عملية الإثبات في مجال الجرائم السيبرانية الحديثة التستر والخفاء في أغلب حالات هذه الجرائم ، لدرجة أن المجني عليه قد لا يعلم بوجود جريمة سيبرانية وقعت عليه ، فضلاً عن قدرة الجاني في حجب السلوك المكون لجريمته ، وطمس معالمها عن طريق التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية [٢] .

التحدي الثالث : إنتشار كوفيد ١٩

إن وكيلة الأمين العام للأمم المتحدة والممثل السامي لشؤون نزع السلاح السيدة إيزومي ناكاميتسو حذرت من ازدياد الجرائم السيبرانية بشكل كبير تزامنا مع تفشي وباء كورونا. وأكدت أن انتشار الوباء حاليا وزيادة الاعتماد الرقمي أدى إلى زيادة نسبة الجريمة السيبرانية بنحو ٦٠٠ في المئة في رسائل البريد الإلكتروني الخبيثة، وأشارت إلى أنه في كل ٣٩ ثانية يقع هجوم إلكتروني. وعلى ذلك طالبت دول العالم بمزيد من الابتكار التكنولوجي والتعاون عبر الشبكة الإلكترونية، لا سيما وقد وُجِدت تقارير عن هجمات يتم شنها استهدافا لأنظمة الرعاية الصحية، ومرافق البحوث الطبية في دول عديدة حول العالم[٣] ، وقد أدى انتشار وباء كورونا إلى سرعة تحول دول مجلس التعاون إلى الخدمات الإلكترونية .

---

(1)K. K. Panigrahi , Information Security and Cyber Law , op.cit. , p. 2 .

(٢) عذاري سعود عبدالمحسن ، الضبط والتفتيش في جرائم الحاسب الآلي ، رسالة قدمت لنيل درجة الدكتوراه في الحقوق ، قسم القانون الجنائي ، جامعة القاهرة ، عام ٢٠١٦ ، ص ٥٣ .

(٣) مقال بموقع https://www.independentarabia.com/ ، نشر بتاريخ ١٨ من شهر يونيو ، عام ٢٠٢٠ ، بعنوان أين العرب من الأمن السيبراني .

وقد ازداد عدد الحملات السيبرانية الواقعة من المخترقين حول موضوع كوفيد ١٩ أضعافًا في مختلف دول العالم، وقامت هذه الحملات باستغلال حاجة المواطنين إلى متابعة أحدث الأخبار والمعلومات الخاصة بكيفية العلاج من الفيروس المنتشر، وبناءً على ذلك؛ كانت منظمة الصحة العالمية هي أبرز الضحايا من الهجمات السيبرانية ، فالمهاجمون كانوا يحاولون الوصول إلى حسابات موظفي المنظمة بغية الحصول على بيانات ومعلومات حول لقاحات فيروس كورونا ، وقد أوضحت الهيئة الوطنية بالمملكة العربية السعودية أنه في الفترة ما بين ٩ إلى ٢٣ من شهر مارس تم إنشاء أكثر من ٣١٥٠٠٠ موقع متعلق بموضوع كوفيد ١٩ ، من بينها ٩ من أصل ١٠ روابط خبيثة أو مرتبطة بعمليات الاحتيال أو الخداع [١] .

التحدي الرابع : الأخطاء البشرية للموظفين بالشركات :

يتمثل الخطأ البشري المؤثر على الأمن السيبراني في صورتين وهما :

الأولى : عدم تدريب الموظفين .

هناك كثير من الصور الشائعة للمتسللين الذين يبحثون عن نقاط ضعف في أنظمة الأمن، ويقومون بتجاوزها بواسطة مهارات في تكنولوجيا المعلومات، إلا أن الأمر لم يقتصر على ذلك فحسب؛ بل من الممكن أن تكون هناك أسباب أخرى تؤدي إلى السماح للمخترقين بالوصول إلى أنظمة الأمان واختراقها بسهولة ، وهم أولئك الأشخاص الذين يهملون في تنفيذ سياسات الشركات المتعلقة بالأمن ، وهذا يرجع إلى أسباب عديدة، من أهمها : استخدام كلمة مرور ضعيفة، أو استخدام كلمة مرور لكافة المصادقات، سواء كانت الشخصية أوالتجارية.[٢]

الثانية : إحجام الموظفين وأصحاب الشركات عن الإبلاغ بالإعتداء السيبراني .

---

(١) النشرة الربعية للأمن السيبراني الصادرة عن مركز الدراسات الاستراتيجية التابعة للهيئة الوطنية للأمن السيبراني ، الربع الأول ،المملكة العربية السعودية ، عام ٢٠٢٠ ، ص ٣ وما بعدها .

(٢) موقع https://www.a7la-home.com/ ، مقال منشور عام ٢٠٢٠ .

من أهم التحديات التي تواجه الأمن السيبراني في دول مجلس التعاون وغيرها هو إحجام المجني عليهم عن الإبلاغ . وخطورة ذلك لا تقتصر على صعوبة قدرة جهات التحقيق على إثبات (الجرائم السيبرانية) بل تعدت إلى التأثير على الوقوف على إحصاء دقيق لتلك النوعية من هذه الجرائم ، وتم التعبير عن ذلك بالرقم المظلم [١] .

ويرجع إحجام المجني عليهم عن الإبلاغ إلى الرغبة في تجنب الأضرار المترتبة على العلانية خوفاً من التأثير على سمعة الشركة وخوفاً من أن تهتز صورتها أمام العملاء مع الإكتفاء بإتخاذ إجراءات إدارية داخلية في هذا الصدد [٢] .

التحدي الخامس : عدم وجود نظام موحد لدول مجلس التعاون .

لا يوجد حتى الان نظاماً موحداً لدول مجلس التعاون حول الأمن السيبراني على غرار الاتحاد الأوربي . وذلك لتدعيم التعاون الاقليمي بين دول المجلس ودرء خطورة الجرائم السيبرانية المستحدثة ، فقد وضع الاتحاد الأوربي في عام ٢٠١٦ م ، نظاماً يسمى توجيه الاتحاد الأوربي حول أمن الشبكات والمعلومات ، ويعد ذلك أول تشريع ينظم الأمن السيبراني ، وشمل هذا النظام مجموعة من الضوابط الأمنية المتعلقة بحماية الأمن السيبراني ، وقد طلب من الشركات التي تعمل في البنية التحتية ومشغلي الخدمات الأساسية ، ومقدمي خدمات البيانات ، ضمان مستوى أعلى من الأمن يتناسب مع المخاطر ، مع مراعاة أمن النظم والمرافق ، والتعامل مع الحوادث ، وإدارة استمرارية العمل ، والرصد والتدقيق والاختبار بما يتوافق مع القواعد الدولية [٣] .

---

(١) د. سعيد عبداللطيف ، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت ، دار النهضة العربية ، عام ١٩٩١ ، الطبعة الأولى ، ص ٥٩ .

(٢) عذاري سعود عبدالمحسن ، مرجع سابق ، ص ٤٩ وما بعدها .

(٣) د/ حازم حسن أحمد الجمل ، بحث في الحماية الجنائية للأمن السيبراني في ضوء رؤية المملكة ٢٠٣٠ ، مجلة البحوث الأمنية ، جامعة الملك فهد الأمنية ، مركز البحوث والدراسات ، مجلد ٣٠ ، عدد ٧٧ ، شهر أغسطس ، عام ٢٠٢٠ ،ص٢٦٣.

ويمكننا القول أنه مع تطور الدور الرقمي وتنامي المساعي لبناء مجتمع جديد يرتكز على المعلومات والمعرفة فلابد من تحديث الأطر التشريعية لتتلاءم مع المتطلبات المستجدة المتعلقة بالجرائم السيبرانية والفضاء السيبراني وكيفية حمايته ، وبالرغم من الجهود الواعدة التي تبذلها دول مجلس التعاون الإ أنه لم يصدر وثيقة أو نظام عن المجلس يمثل استراتيجية موحدة للأمن السيبراني لمواجهة المخاطر السيبرانية التي تطال أي دولة من دول مجلس التعاون .

التحدي السادس : التطبيقات الضارة

إن من أهم التحديات التي تواجه الأمن السيبراني لدول مجلس التعاون التطبيقات الضارة، تلك التي ينجذب الناس إليها باعتبارها من التطبيقات الجديدة على أجهزتهم المحمولة. وأثناء تثبيت أي تطبيق على الجهاز المحمول ، تنبثق نافذة في كل مرة فيها طلب الإذن لبعض الأشياء، مثل الوسائط والموقع والكاميرا على أجهزتنا. هذه التطبيقات من الممكن أن تكون خطرة، لأننا نمنحها الإذن دون أن نتحقق من معرفتها فعلياً ، وبهذا يصبح الجهاز عرضة لهذه الأنواع من التطبيقات الضارة. ونتيجة لذلك ؛ قد يحدث فقدان للبيانات أو تلفٌ في تخزينها . [١]

التحدي السابع : كثرة برامج التجسس والثغرات الأمنية .

بغض النظر عن نظام التشغيل الذي يمتلكه المستخدمون على هواتفهم المحمولة ، فإن أجهزتهم هي أهداف للتهديد عن طريق الروابط الخبيثة التي يبحث عنها المتسللين وقد واجهت الشركات الكبرى مثل Apple أيضًا ثغرات أمنية في أجهزتها المحمولة مما أبقى الأجهزة متاحة لهجمات برامج التجسس. في الآونة الأخيرة ، وتم العثور على برنامج تجسس Pegasus يتجسس على أجهزة Apple لتتبع المستخدمين والحصول على المعلومات. ثم أصدرت Apple تصحيحًا مع تحديثات لحماية المستخدمين من مثل هذا النوع من الثغرات الأمنية.[٢]

---

(١) Ramjee Prasad • Vandana Rohokale , op.cit., p.221

(٢) .Ramjee Prasad • Vandana Rohokale , op.cit., p.222

التحدي الثامن : استخدام المخترقين شبكات wifi .

يتم الاعتماد على شبكات ال wifi في كثير من الأماكن مثل المدارس والمصانع والشركات والمنازل والمطارات والسكك الحديد والمقاهي . ويعد إنتشار شبكات wifi العامة أكثر ملاءمة في الوقت الحالي ، ولكنها في ذات الوقت غير موثوق بها لأنه يتم استخدامها بواسطة المتسللين ، وتصبح البيانات عرضة للخطر من خلال هذه الشبكات ويتم تسريب المعلومات إلى المتسلل .

التحدي التاسع : التطبيقات غير النشطة .

تكون التطبيقات غير النشطة على أجهزة المحمول والتي لا يستخدمها المستخدمون مطلقاً سبب من أسباب اختراق البيانات والمعلومات المتعلقة بالأشخاص والشركات ، فتعد هذه التطبيقات غير النشطة المصدر الرئيسي لخرق الأمن والخصوصية . وتطلب بعض هذه التطبيقات النقر فوق الإعلانات ليتم الوصول إلى كافة المعلومات .

ويمكننا القول أنه ينبغي أن تحث دول مجلس التعاون الشركات التي تعمل في مجال المحمول على زيادة تفعيل وضع بند يتيح حذف هذه التطبيقات في حال مرور فترة من الزمن على عدم إستخدامها .

التحدي العاشر : البريد الإلكتروني العشوائي .

البريد الإلكتروني هو عبارة عن رسالة عادية لكن بطريقة إليكترونية يكتبها شخص بطريقة عادية على جهاز الحاسب الالي الخاص به ، وذلك بعد أن يقوم بفتح الصفحة الخاصة ببريده الإليكتروني ، والتي تعد لها رقم سري مسبقاً واسم للمستخدم ، ولا يمكن لغيره استخدام هذا البريد .[1] وقد يقوم بعض المخترقين بإرسال رسالة عبر بريد إليكتروني فيتم الضغط علي رابطها من قبل الضحية ويتم اختراقه والتسلل إلى بيانته .

---

(١) الدكتور المستشار / عبدالفتاح بيومي حجازي ، المرجع السابق ، ص ٢٠ .

التحدي الحادي عشر : نقص المعرفة الفنية للمحللين الأمنيين .

نظراً لعدد الانتهاكات الأمنية في المنظمات الذي يستمر في الازدياد ، يمكن أن يكون ذلك مؤشراً على نقص المعرفة الفنية للمحللين الأمنيين ...،[١] : ويظهر صدى ذلك في اتخاذ القرار أثناء العمليات الأمنية ، وعلى الرغم من أن مهام المحللين الأمنيين تختلف من منظمة إلى أخرى ، لكن هناك عدة وظائف تقوم بوصف بوضوح عمليات عمل هؤلاء المحللين من أهمها :

١ : مراقبة الهجمات والاقتحامات والأنشطة غير العادية أو غير المصرح بها أو غير القانونية .

٢ : تحديد نقاط الضعف المحتملة ، سعياً إلى تحديد أنماط التهديدات الناشئة فعلى سبيل المثال عمل محاكاة للانتهاكات الأمنية .

٣ : القيام بتقارير لكل من الموظفين التقنيين وغير التقنيين وأصحاب المصلحة والمساعدة في عمليات التدقيق الداخلية والخارجية المتعلقة بأمن المعلومات .

٤ : مراقبة ومتابعة أنشطة التزييف ، والقيام بالصيانة ، وتقديم التدريبات الخاصة بالتوعية بالأمن السيبراني .

التحدي الثاني عشر : نمو إختراق إنترنت الأشياء (LOT).

يعد نمو اختراق إنترنت الأشياء من التحديات الحالية والمستقبلية التي أولى الفقهاء والباحثين لها أهمية خاصة ، وقد وضع بعض الباحثين عدة طرق للحفاظ على أمان إنترنت الأشياء وعدم إختراقها ومن أهمها :

١ : يجب أن تأخذ عمليات النشر المتعلقة بأنظمة أمان إنترنت الأشياء بعين الاعتبار بسبب وجود كيانات متنافسة في هذا الشأن .

---

(١) Andrew W. M'manga , Designing for Cyber Security Risk-based Decision Making , A dissertation submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy , Department of Computing and Informatics Bournemouth University January 2020 , P.1.

٢: يجب أن تظل أنظمة أمان إنترنت الأشياء آمنة في ظل وجود خصم قوي يقوم بالتهديد ومعاملة الجميع على أنهم مهاجمين محتملين .

٣: يجب ألا تتطلب أنظمة أمان إنترنت الأشياء مزيداً من الموارد سواء كانت حسابية أو شبكات ، أكثر مما هو متاح على منصات الاستشعار الحديثة . (١)

ووفقًا لـ IoT Analytics ، سيكون هناك حوالي ١١.٦ مليار جهاز إنترنت الأشياء في عام ٢٠٢١. وأجهزة إنترنت الأشياء هي أجهزة حوسبية ورقمية وميكانيكية يمكنها نقل البيانات بشكل مستقل خلال الشبكة. ومن أمثلة أجهزة إنترنت الأشياء أجهزة الكمبيوتر المكتبية ، وأجهزة الكمبيوتر المحمولة ، والهواتف المحمولة ، وأجهزة الأمان الذكية ، وما إلى ذلك ، إن الاعتماد على أجهزة إنترنت الأشياء يتزايد بمعدل غير مسبوق ،وحماية أجهزة إنترنت الأشياء يمثل تحدياً كبيراً في مجال الأمن السيبراني ، حيث إن الوصول إلى هذه الأجهزة من الممكن أن يفتح الأبواب أمام المزيد من الهجمات الضارة (٢).

---

(1) Justin King-Lacroix , Securing the Internet of Things: decentralised security for wireless networks of embedded systems , A thesis submitted for the degree of Doctor of Philosophy, University of Oxford, 2016, p42.

١. "Realistic deployments of IoT security systems will necessarily have to take into account the possibility of interactions between competing entities. The architecture of such security systems must therefore be decentralised, to ensure that no single entity controls the security infrastructure".

"R.2 IoT security systems must remain secure in the fact of a strong adversary – the threat model in Section 4.1 suggests treating all nodes as potential DolevYao [32] attackers".

"R.3 IoT security systems must not require more resources (whether computational, performance, or networking) than are available on modern sensor platforms."

(2) https://www.jigsawacademy.com/

التحدي الثالث عشر : إنتشار برامج الفدية بدول مجلس التعاون .

أضحت هجمات برامج الفدية منتشرة في السنوات القليلة الماضية وتشكل أحد أبرز تحديات الأمن السيبراني في دول مجلس التعاون . وتتضمن هجمات برامج الفدية اختراق بيانات المستخدم ومنعهم من الوصول إليها حتى يتم دفع فدية. وتؤثر هذه الهجمات على المستخدمين الفرديين ولكن تأثيرها أكبر على الشركات التي لا يمكنها الوصول إلى البيانات لتشغيل عملياتها اليومية. ومع ذلك ، مع معظم هجمات برامج الفدية ، لا يفصح المهاجمون عن البيانات حتى بعد إجراء الدفع، ويقومون بمحاولة ابتزاز المزيد من الأموال.

التحدي الرابع عشر : تطور تقنيات التعلم الآلي والذكاء الاصطناعي .

بينما أثبتت تقنيات التعلم الآلي والذكاء الاصطناعي أنها مفيدة للغاية للتطور الهائل في مختلف القطاعات ، إلا أن بها نقاط ضعف أيضًا. ويمكن استغلال هذه النقاط من قبل الأفراد المتسللين لتنفيذ هجمات إلكترونية وتشكيل تهديدات للشركات. وتعد هجمات التعلم الآلي والذكاء الاصطناعي مصدر قلق كبير . وقد يكون من الصعب للغاية التعامل مع هجوم متطور بسبب نقص خبرة القائمين على الأمن السيبراني .[١]

التحدي الخامس عشر : المخاطر المتزايدة للسحابة .

تقوم الشركات بنقل بياناتها الهامة من مراكز البيانات القديمة إلى السحابة ، وذلك بسبب المرونة والتكاليف التي ينطوي عليها نقل هذه البيانات. ويحتاج نقل البيانات إلى السحابة إلى الإلتزام بتدابير الأمان المطبقة وإلا ستكون هناك فرص للوقوع في فخ الاختراق . ويقوم مقدمو الخدمات السحابية فقط بتأمين نظامهم الأساسي ، وتأمين البنية التحتية للشركات من السرقة والحذف . وهناك العديد من الحلول للأمان السحابي مثل جدران الحماية والمصادقة متعددة العوامل والشبكات الافتراضية الخاصة .[٢]

---

(١) موقع باللغة الإنجليزية ، المرجع السابق ، https://www.jigsawacademy.com/ .

(٢) موقع باللغة الإنجليزية ، https://www.teceze.com/cybersecurity-challenges-in-2020-and-how-to-tackle-them/

التحدي السادس عشر : الهجمات ضد تقنية BLOCKCHAIN .

تقنية blockchain هي التقنية الأكثر استخداماً من قبل الشركات والمستخدمين . وذلك لمنع هجوم DDOS والتهديدات الأخرى التي تهدد إنترنت الأشياء ، فهي تعتمد على عمليات تتطور بإستمرار وليس لمرة واحدة .

فمع التقنيات الكبيرة التي يستخدمها المتسللون تحتاج تقنية BLOCKCHAIN ، إلى التطور والنمو بشكل كبير . (١) فبعض المتسللين يمكن أن يستخدموا هذه التقنية لاختراق بيانات الضحايا أو يمكن العمل على اختراق هذه التقنية والتسلل من خلالها .

التحدي السابع عشر : عدم تكافؤ التجريم .

يمثل التعاون الإقليمي فيما بين دول مجلس التعاون للتحقيق في أعمال الجريمة السيبرانية تحدياً فيما يتعلق بعدم تكافؤ التجريم . فتخضع طلبات التعاون الإقليمي والدولي لعدة متطلبات إجرائية وموضوعية حيث يتعين رضا الدولة متلقية الطلب ، وأن يكون الفعل المكون للجريمة السيبرانية مُجرم بالدولتين الطالبة ومتلقية الطلب .

التحدي الثامن عشر : غالباً ما ترتكب الجريمة السيبرانية بشكل منظم .

تعتبر السمات التقليدية للجريمة المنظمة مثل استخدام العنف والاستيلاء على الأراضي من الصعب الأخذ بها في توصيف النشاط الإجرامي السيبراني . إلى جانب أنه لاتبدو المسائل المتعلقة بالموروث الإداري للجماعات المنظمة والتي تقوم على الثقة والتنفيذ ، وعلى التسلسل الهرمي والمعياري ، من الأمور اليسيرة أن تتوسط بيئة مثل بيئة المنتديات وغرف الدردشة ، وبالرغم من ذلك ما يستطيع الأفراد فعله يمكن للمنظمات فعله وربما يكون بشكل أفضل . وقد أوضحت بعض الدراسات ، والتي أجرت استعراض لعينة من ٥٠٠ جريمة

---

(١) Ramjee Prasad • Vandana Rohokale , op.cit., p.269.

سيبرانية مسجلة لدى أجهزة الشرطة ، وأتضح أن ما يزيد عن ٨٠ ٪ في المائة منها تستخدم بعض من أشكال الإجرام المنظم .[١]

التحدي التاسع عشر : المحافظة على حقوق الإنسان .

يجب على الدول أثناء مباشرة إجراءات الأمن السيبراني للتصدي للهجمات الإلكترونية أن تراعي التزاماتها الدولية والإقليمية والدستورية بشأن حقوق الإنسان وألا تنتهك هذه الحقوق بداعي المحافظة على أمن المعلومات .

التحدي العشرون : العملات المشفرة :

انتشرت في الآونة الأخيرة العملات المشفرة مثل بتكوين وغيرها. وإتجه عدد كبير من المواطنيين في دول الخليج إلى الاستثمار فيها ، وبدأ المجرمون في شن هجمات برمجية خبيثة من نوع clonhive omine، المتعلقة بالتنقيب عن العملات المشفرة حيث يقوم المخترق بارسال ملفات خبيثة في وحدة معالجة الرسومات (gpu) تضر الخوادم أو أجهزة الحاسوب أو المحولات (routers) ومن ثم يتحصل على المعلومات التي تمكنه من التنقيب عن العملات الافتراضية .

وكذلك يلجأ المخترقون للابتزاز باستخدام خدمات البريد الالكتروني لشركة مثل proton mail .com المشفرة مستغلين عدم تعاون هذه الشركة مع وحدات إنفاذ القانون في الدول ، ويمكن التصدي لهذا التحدي عن طريق استخدام أحدث البرامج التي توصي بها الشركات المزودة للخدمة وحظر خدمات شركة بروتون .

التحدي الواحد والعشرون : التهديد والابتزاز الجنسي :

يحدث عن طريق سرقة حسابات الاشخاص على مواقع التواصل الاجتماعي وسرقة صورهم الخاصة وابتزازهم ومطالبتهم بمبالغ نقدية ،ويقوم المخترق في هذه الحالة بالدخول إلى حساب سهل ضعيف الحماية ثم ينتقل منه لآخر متواجد لدى هذا الحساب ، ثم يقوم

---

(١) دراسة شاملة عن الجريمة المنظمة ، صادرة عن مكتب الأمم المتحدة المعني بالمخدرات والجريمة ، في فبراير ، عام ٢٠١٣ ، ص ٦٥ .

بارسال روابط وهمية يتحصل من خلالها على الارقام السرية ووسائل الحماية ،أو عن طريق إرسال روابط ذاتية التفعيل تجبر الشخص على الخروج من حسابه ليفسح المجال للمخترق بتفعيل خاصية التحقق الثنائي المرتبطة بالرمز التعريفي وهو في الغالب مرتبط بالحاسب الآلي وليس الحساب، ولو تمكن المخترق من التوصل لتغيير كلمة السر يتمكن عندئذ من الدخول للحساب بسهولة .

ويمكن معالجة ذلك بتوعية الأفراد من عدم فتح الروابط الوهمية وتفعيل خاصيتي التحقق الثنائي والرمز المتغير .

التحدي الثاني والعشرون : سرقة الأصول الافتراضية :

حيث يقوم المخترق بايهام شخص برغبته في شراء اسم مستخدم في أحد التطبيقات الافتراضية وعند اتمام الشراء يختفي المجرم ولا يمكن إعادة تعيين كلمة السر .

التحدي الثالث والعشرون : الإيهام بالجوائز:

حيث يستخدم الجناة في هذه الحالة وسائل التواصل التي تتيح الاتصال الدولي عبر الانترنت والاتصال على الاشخاص من أرقام تخص البنوك المحلية وشعارها، والايهام بالفوز بجائزة وأن قواعد الجائزة تقتضي ايداع رسوم أولاً بغرض الاستيلاء عليها ،وهو ما يمكن أن يطلق عليه الاحتيال الهاتفي .

التحدي الرابع والعشرون : الاستغلال الجنسي للأطفال :

ويقوم الجناة باستخدام الالعاب الالكترونية مثل لعبة pubg أو fortnite ومن خلال التواصل مع الأطفال عن طريق هذه الالعاب وإغراءهم بمنحهم رصيد مالي وهمي يستخدمه في هذه الالعاب في مقابل أن يطلب من الأطفال تصوير ذويهم سواء أمهاتهم أو أخواتهم خلسة أو مطالبة الطفل بتصوير مقاطع مخلة بالآداب نظير هذا الرصيد الوهمي وفي سبيل إقناعهم بذلك قد يرسل له مقاطع مماثلة من أطفال آخرين لتحفيزهم على الاستجابة .

والسبيل في القضاء على هذا التحدي هو التوعية لأولياء الامور والأطفال وحظر الدخول على هذه الالعاب بالتنسيق مع مزودي الخدمة .

التحدي الخامس والعشرون : جرائم الملكية الفكرية :

وذلك عن طريق وضع علامات تجارية على منتجات غير حقيقية بغرض الاستفادة من جودة العلامة التجارية والحصول على ربح غير مستحق .

الفرع الثاني : القطاعات المتضررة من تهديدات الجريمة السيبرانية

تـزداد الجريمـة الـسيبرانية وتتـسارع بـشكل كبـير ، وتظهـر لهـا – أيـضاً- أشـكال جديـدة باستمرار، ويصبح مرتكبو الجرائم السيبرية أكثر مرونة، فيقومون باستغلال أدوات التكنولوجيا الحديثة بشكل فائق السرعة، ويخططون لاعتداءاتهم بدقة مستخدمين أساليب جديدة [١].

أولاً قطاع الرعاية الصحية :

إن فيروس كورونا المنتشر في جميع أنحاء العـالم ومرضـه المعـروف باسـم COVID-19 قد أحدث تأثيرًا كبيرًا على كل شيء تقريبًا . ونحن نشهد جميعًا الآن أزمة صحية عامة عالمية كبرى غير مسبوقة وغير متوقعة ، كما أن هذا الوباء تسبب أيضًا في حدوث اضطرابات اجتماعية ضخمة ، وساهم في تعطيل الصناعات كلها تقريبًا ، وأثرعلى حياة وعمل الجميع في كل بلد ، حيث تم إغلاق الشركات والمؤسسات التعليمية ، واضطر العديد من الموظفين إلى العمل من منازلهم ، وتعطلت سلاسل التوريد ، وطلب من المواطنين عزل أنفسهم ،وتم حظر معظم رحلات السفر والاجتماعات الشخصية ، والمؤتمرات ، ويمكن أن تستمرالاضطرابات لأشهر ، ويُتوقع أن يستمر التأثير الاقتصادي والتجاري والاجتماعي لسنوات ، [٢]وفي سبيل

---

(١) موقع الإنتربول الرسمي ، https://www.interpol.int/ar/4/6 .

(2) THE RAPID AND worldwide spread of the coronavirus and its illness known as COVID-19 has made huge impact on almost everything has taken us all by surprise. We all are now experiencing a major unprecedented and unexpected global public health crisis. This pandemic has also triggered huge social upheavals, disrupted almost every industry, and impacted the life and work of everyone in almost every country. Businesses and educational institutions are closed, many employees are forced to work from their homes, supply chains have been disturbed, people are being required to self-isolate, and most travel, in-person meetings, and conventions have been banned. These disruptions could continue for months, and the resulting economic, business, and social impact will last for years.
Tim Weil ,San Murugesan , IT Risk and Resilience— Cybersecurity Response to COVID-19 , journal , it Professional ,Published by the IEEE Computer Society, may2020 , p 4 .

استغلال ذلك عدل المخترقون اتجاهاتهم نحو قطاعات معينة ،وولوا نظرهم تجاه القطاع الصحي .

وقد ركزت التهديدات والهجمات السيبرانية جهودها نحو قطاع الرعاية الصحية وبشكل خاص تجاه حملات كوفيد – ١٩ . فشكلت العديد من الهجمات التي تستهدف قطاع الرعاية الصحية مصدر قلق للعالم أجمع . نظراً لأن هذا القطاع يشهد عالمياً ضغطاً تشغيلياً كبيراً في محاولة احتواء حالات الطوارئ الصحية . فمنذ بداية الأزمة ازدادت الحملات الإجرامية من المهاجمين الذين يتظاهرون أنهم ينتمون إلى منظمة الصحة العالمية بهدف الحصول على الأموال وقد أصدرت منظمة الصحة العالمية بياناً تحذر فيه من حملات الهندسة الاجتماعية ، وقد تكرر الإعتداء على قطاع الرعاية الصحية أيضاً عندما تم الاعتداء على المركز الأمريكي للسيطرة على الأمراض والوقاية منها . وتمثل الهجمات في قطاع الرعاية الصحية عالمياً في الربع الأول من عام ٢٠٢٠ بنسبة ١٣.٣٧ ٪ .[1] فضلاً عن تلك التي تستهدف الحصول على معلومات عن اللقاح وغيرها ، كذلك فأن هذا الوباء سرع من التحول للخدمات الإلكترونية وقابلها محاولات اختراق عديدة للحصول على خدمات غير مشروعة .

ثانياً : قطاع الطاقة :

يعد قطاع الطاقة من أبرز القطاعات المتضررة من الجرائم السيبرانية المرتكبة ضد دول مجلس التعاون ، فيضم قطاع الطاقة نظم وشبكات ومحطات التحكم في إنتاج وتوزيع الكهرباء والبترول والغاز ومحطات الطاقة النووية وغيرها .

ومن أبرز الجرائم المرتكبة ضد قطاع الطاقة الاعتداء السيبراني على شركة أرامكو السعودية الذي تسبب في إختراق المعلومات الحساسة والسرية للشركة وتسبب في خسائر مالية لها .

---

(١) النشرة الربعية للأمن السيبراني ، الصادرة عن الهيئة الوطنية للأمن السيبراني ، المرجع السابق ، ص ٣، ٤ .

وفي المنتدى الدولي للأمن السيبراني أضاف كبير الموظفين الإداريين بشركة أرامكو أنهم يتبعون إجراءات مشددة لتعزيز الأمن السيبراني، وأنهم تعلموا من درس الاختراق الكبير الذي وقع على الشركة قبل ثمانية أعوام. وأنهم قاموا بإتخاذ عدة إجراءات منها : تطبيق أنظمة المراقبة والتحكم باستخدام الذكاء الاصطناعي، والشراكات مع الجهات الرائدة في مجال الأمن السيبراني، والتدريب والتطوير المستمر للموظفين وأكد على أنه ليس هناك أهم من الاستثمار في تطوير الكفاءات البشرية القادرة على التعامل مع هذا النوع من التهديدات الخطيرة.[١]

وفي صورة أخرى لاختراق الأمن السيبراني لقطاع الطاقة فقد يتضح لنا أن الطاقة المتجددة تعتمد على أنظمة التحكم الصناعية المتطورة وشبكات التوزيع. ونظرًا لعدم توفر مصادر الطاقة المتجددة مثل الرياح والطاقة الشمسية على مدار الساعة، فإنه يتطلب أيضًا حلول لتخزين الطاقة. وتعدهذه الأنظمة جميعها عرضة للهجمات السيبرانية . ولكي يتم إثبات هذه الحقيقة، قام أحد الباحثين في جامعة تلسا الأمريكية عام ٢٠١٨م باختراق وإيقاف أحد توربينات الرياح غير الخاضعة للرقابة في وقت قليل للغاية، وذلك عن طريق الوصول إلى الخادم غير الآمن. حيث قام بتوصيل جهاز الكمبيوتر المحمول عبر خادم تلك التوربينة ليتمكن من الوصول على الفور إلى عنوان الـ IP الذي يمثل كل التوربينات في تلك الشبكة.[٢]

ثالثاً : القطاع المالي .

مع زيادة اعتماد الخدمات المالية ، والمصرفية -بصفة خاصة - على التكنولوجيا أدى إلى أرتفاع نسبة المخاطر والهجمات السيبرانية على المؤسسات المالية . ففي مجال البنوك _ على سبيل المثال _ لم تعد الإجراءات الرقابية المصرفية التقليدية ذات أهمية ، فقد تم

---

(١) الموقع الرسمي لشركة أرامكو ، https://www.aramco.com/ar/news-media/news/2020/sa-calls-for-boosting-the-vital-role-of-cybersecurity .

(٢) عبدالرحمن بن صالح الشريدة ، مقال بصحيفة مال : https://www.maaal.com/archives/20190417/121725 ، في ١٧أبريل من عام ٢٠١٩ .

الاستعانة ببعض الخبراء والشركات في مجال التكنولوجيا لتفعيل وسائل الحماية الحديثة ، والقطاع المصرفي أصبح أكثر القطاعات المالية استهدافاً من قبل القراصنة ،وقد كثر في الآونة الأخيرة في دول الخليج ورود اتصالات من أرقام وأسماء لمصارف وطنية من خارج البلاد وتحاول الحصول من العملاء على بيانات عن حساباتهم أو بطاقتهم الإئتمانية وإساءة استخدامها بعد ذلك [١]، ومكافحة الجرائم الالكترونية تعد أهمية قصوى للقطاع المصرفي في هذه الأيام .

رابعاً: الخدمات التي تقدمها حكومات دول مجلس التعاون عبر المواقع الإلكترونية .

تعد الحكومة الإلكترونية إحدى الطرق الحديثة التي تتبعها حكومات (دول مجلس التعاون) لاستخدام التقنية الحديثة في تحسين كفاءة المؤسسات والأجهزة الحكومية واستغلال موارد الدولة بالشكل الأمثل ، ولتزويد المواطنين بآليات أفضل وأيسر للوصول إلى الخدمات داخل مؤسسات الدولة وتتيح هذه المواقع للمواطنين المشاركة بأرائهم ومقترحاتهم . وتعرف الحكومة الإلكترونية أنها " استخدام تكنولوجيا الإتصالات والمعلومات لتحقيق الإصلاح من خلال تسريع عملية الشفافية وتقريب المسافات ، وإزالة العوائق ، وإعطاء الفرصة للمواطنين للمشاركة في كافة مراحل العملية السياسية والقرارات المتعلقة بها والتي تؤثر على نواحي حياتهم المختلفة " [٢] .

---

(١) تجدر الإشارة أن المصارف الكويتية طلبت من شركات الاتصالات حظر الأرقام المشابهة لأرقامها والتي ترد من خارج دولة الكويت مع تحذير العملاء من مثل هذه الاتصالات .

(٢) اللواء الدكتور / أشرف السعيد أحمد ، تكنولوجيا المعلومات في المجال الأمني ، مطابع الشرطة للطباعة والنشر والتوزيع ، الطبعة الثانية ، عام ٢٠١٥ ، ص ١١٢ .

وفي إطار جهود دولة قطر لخدمة مواطنيها ، أصدرت استراتيجية الحكومة الإلكترونية عام ٢٠٢٠ ، معتمدة على عدة أهداف أهمها رفع كفاءة العمليات الإدارية الحكومية والارتقاء بمستوى الخدمات [١] .

وقد يترتب على تقديم الحكومة الرقمية أو الإلكترونية لخدماتها اختراق أمني يتم من خلاله الاستيلاء على المعلومات والبيانات المتعلقة بالعملاء أو المواطنين ، ولم يتعلق الأمر في هذه الحالة بسوء السمعة التي تتعرض لها المواقع الحكومية فحسب ، بل يتعدى أثار هذا الإختراق إلى فقدان البيانات وسوء استخدام المعلومات أو الحصول عليها بطريقة غير مشروعة .

(١) د/ حصة الجابر ، وزيرة الاتصالات وتكنولوجيا المعلومات القطرية ، الكلمة الافتتاحية لاستراتيجية الحكومة الإلكترونية لدولة قطر ، الملخص التنفيذي ، عام ٢٠٢٠ ، الصادرة عن وزارة الاتصالات وتكنولوجيا المعلومات القطرية .

المطلب الثاني : نماذج من الإرهاب السيبراني وأبعاده وطرق تطوره [١].

بداية ، لا يوجد صك عالمي ليكون أساساً لتعاون الدول لمكافحة الإرهاب عبر الإنترنت الذي يقوم به أشخاص ضالعون في ارتكاب تصرفات غير قانونية تجرمها القوانين الداخلية ، وفي ظل عدم وجود صك خاص فتستمر السلطات الوطنية لدول مجلس التعاون في تجريم هذه الأفعال وفقاً للمعاهدات أو الترتيبات الدولية أو الإقليمية التي وضعت لتيسر التعاون الدولي علي التحقيق في جرائم الإرهاب أو الجريمة المنظمة العابرة للحدود الوطنية بشكل عام والملاحقة القضائية بشأنها . ومن الواضح أن عدم وجود صك لمكافحة الإرهاب يتناول خصيصاً المسائل السيبرانية يعرقل إلى حد كبير التعاون بشأن التحقيق في قضايا الإرهاب الذي يستخدم فيها الإنترنت ، وهناك أيضاً صكوك عديدة يمكن أن تكون أساساً قانونياً للتعاون الدولي في قضايا الإرهاب المنطوية على عنصر من عناصر استخدام الإنترنت، ويمكن أن تدعمها الدول بمعاهدات ثنائية أو متعددة الأطراف [٢].

وبناء على ما سبق ، يمكن تقسيم هذا المطلب إلى فرعين :

---

(١) عنى قادة دول مجلس التعاون بظاهرة الإرهاب بصفة عامة مبكراً ، ففي الدورة الثامنة للمجلس الأعلى لدول مجلس التعاون المنعقدة في الرياض بالمملكة العربية السعودية في عام ١٩٨٧ تم إقرار الاستراتيجية الأمنية الشاملة ، ثم صدر في تشرين الأول / أكتوبر ، عام ٢٠٠١ عن دول مجلس التعاون إعلان مسقط لمكافحة الإرهاب ، وفي عام ٢٠٠٤ وقع وزراء داخلية دول مجلس التعاون على الاتفاقية الدولية لمكافحة الإرهاب في الكويت ، وذلك في إطار عمل مشترك لاحتواء ظاهرة الإرهاب وتنسيق الجهود للاستناد إلى قاعدة معلوماتية أمنية مشتركة . راجع في ذلك : دراسة مكتب الأمم المتحدة المعني بالمخدرات والجريمة ، فيينا ، بموضوع تشريعات مكافحة الإرهاب في دول الخليج العربية واليمن ، عام ٢٠٠٩ ، ص ١٥ .

(٢) استخدام الإنترنت في أغراض إرهابية ، مكتب الأمم المتحدة المعني بالمخدرات والجريمة بالتعاون مع فرقة العمل التابعة للأمم المتحدة المعنية بتنفيذ تدابير مكافحة الإرهاب ، نيويورك ،عام ٢٠١٣ ، ص ٧٤ وما بعدها .

الفرع الأول : نماذج من الإرهاب السيبراني

قبل إيضاح نماذج من الإرهاب السيبراني لابد من التطرق أولاً لتعريف الإرهاب السيبراني ، فقد عرف البعض الإرهاب بصفة عامة أنه : استخدام طرق عنيفة كوسيلة الهدف منها نشر الرعب للاجبارعلى اتخاذ موقف معين أو الامتناع عن موقف معين . ومن هذا التعريف يتضح أن ملامح جريمة الإرهاب تختلف عن غيرها من الجرائم حيث أنها وسيلة وليست غاية ، والوسائل المستخدمة عديدة ومتنوعة ، وتتميز بطابع العنف وتخلق حالة من الفزع والخوف ، وغالباً ما يكون الدافع من وراء جرائم الإرهاب المشاكل السياسية أو أن هناك فريقان مختلفان . (١)

أما الإرهاب السيبراني فقد عرفه البعض أنه " العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق باستخدام الموارد المعلوماتية والوسائل الإلكترونية بشتى صنوف العدوان وصور الإفساد " (٢)

وعرفه أخر أنه " الهجوم القائم على مهاجمة الحاسوب، وأن التهديد به يهدف إلى الترويع أو إجبار الحكومات أو المجتمعات لتحقيق أهداف سياسية أو دينية أو عقائدية، وينبغي أن يكون الهجوم مدمرًا وتخريبيًّا لتوليد الخوف بحيث يكون مشابهًا للأفعال المادية للإرهاب" (٣)

---

(١) د. أحمد محمد رفعت ، الإرهاب الدولي ، دار النهضة العربية ، عام ٢٠٠٦ ، بدون رقم طبعة ، ص ٢٢٦ وما بعدها.

(٢) بيان مجمع البحوث الإسلامية بالأزهر الشريف ، بشأن ظاهرة الإرهاب ، القاهرة ، في ١٥/ ٨/ ١٤٢٢ هـ _ ١/ ١١/ ٢٠٠١ م ، ومشار إليه في : د. خالد سامي السيد ، الأمن القومي الإلكتروني وجرائم المعلومات ، دار النهضة العربية ، الطبعة الأولى ، عام ٢٠٢١ ، ص ٤٩ .

(3) DENNING ,DOROTHY, E., (Aug 2000)" Cyber terrorism" , Global Dialogue ,p1.

ومشار إليه في : رانيا سليمان ، فاتن فايز ، نهى الدسوقي ، مقال بعنوان سياسات مكافحة الإرهاب الإلكتروني ، مصر والسعودية نموذجاً ، منشور بتاريخ ٢ فبراير ، عام ٢٠٢٠ على الموقع الإلكتروني :
http://www.acrseg.org/41483

ويمكننا القول أن هذا التعريف به قصور لكونه لم يتطرق للشبكات الإلكترونية وتقنية المعلومات بصفة عامة كمحل للجريمة الإرهابية الإلكترونية وذكر فقط مهاجمة الحاسوب.

ويوجد ندرة في المراجع التي تطرقت لمفهوم الإرهاب السيبراني، ويمكن تعريف جرائم الإرهاب السيبراني بأنها تلك التي ترتكبها الجماعات الإرهابية بواسطة الوسائل التقنية الحديثة سواء كان الهدف سياسياً أو اجتماعياً أوعسكرياً أو دينياً أو عقائدياً وذلك إما لنشر دعايتهم للوصول إلى التجنيد ودفع الأشخاص تجاه التطرف أو التحريض على الأعمال الإرهابية ، وإما لتمويل الأعمال الإرهابية، وإما استخدام الشبكات الإلكترونية بوصفها ساحة تدريب ، وإما للتخطيط لعمل إرهابي وغالباً ما تكون هذه الأعمال الإرهابية عابرة للحدود الوطنية ، وإما لحمل الطرف الآخر على التصرف على نحو معين في أمر ما .

ومن هذا المنطلق ، نبرز نماذج من الإرهاب السيبراني ومن أهمها :

١: استهداف النظم العسكرية :

يعد هذا النوع من التهديدات من أخطر نماذج الإرهاب ومن أبرز السيناريوهات المحتملة التي تواجه المجتمع وتبدأ في مراحلها الأولى باختراق المنظومة الأمنية المتعلقة بالأسلحة الاستراتيجية ونظم الدفاع الجوي والصواريخ النووية وقد تقوم الجماعات الإرهابية بفك الشفرات السرية للتحكم في تشغيل منصات إطلاق الصواريخ الاستراتيجية مما يؤدى إلى خسائر فادحة [1] ، ويقلل من قدرات الدولة العسكرية وحماية أراضيها ومنشآتها الحيوية ومواطنيها .

٢: التحريض على ارتكاب أعمال عنف .

ومن أبرز نماذج الإرهاب السيبراني هو تحريض الجماعات الإرهابية على ارتكاب أعمال إرهابية تتعلق بالعنف .

ومن أبرز القضايا في هذا الشأن : قضية الولايات المتحدة الأمريكية ضد إيمرسون وينفيلد بيغولي. فقد تم أتهام طالب أمريكي في الثانية والعشرين من عمره ، بالضلوع في نشر

(١) د. خالد سامي السيد ، المرجع السابق ، ص ٥٤ وما بعدها .

معلومات على شبكة الإنترنت متعلقة بصنع القنابل والتحريض على ارتكاب أعمال عنف وجرائم أخرى . وكان إيمرسون يعرف باسم مستعار " أسد الله الشيشاني " ، له دور نشط في المنتدى الجهادي المعروف دولياً والمسمى باللغة الإنجليزية " شبكة أنصار المجاهدين " وقد شارك في إدارته وعبر عن وجهة نظره المتطرفة ، وقام بتشجيع الزائرين على ارتكاب أعمال إرهابية ضد الولايات المتحدة الأمريكية ، ونشر أشرطة تحتوي على فيديوهات تبث كيفية تعلم صنع المتفجرات ، وقد وجهت إليه المحكمة المحلية الأمريكية للدائرة الشرقية بولاية فرجينيا في ١٤يوليه عام ٢٠١١ عدة تهم منها النشر على المنتدى الإلكتروني عبارات تدعو إلى الإرهاب . (١)

الفرع الثاني : دوافع وأبعاد الإرهاب السيبراني وطرق تطوره .

هناك العديد من التطورات في تكنولوجيا المعلومات ، بما في ذلك نقل البيانات ، والاتصالات الأسرع ، وإمكانية التفاعلات الثقافية بين مختلف الأشخاص. وقد خلق هذا التطور تصورات تهديد جديدة للدول ، لأنها غير قادرة على إعاقة نقل المعلومات والأدوات الأخرى المرتبطة بتكنولوجيا الكمبيوتر... وأصبح الفضاء الإلكتروني أداة للإرهابيين لمهاجمة الدول والمنظمات الدولية ... ويتصف الإرهابيين الإلكترونيين بأنهم أفراد يكرهون أو يرهبون منظمة أو حكومة عن طريق شن هجمات إلكترونية ضد شبكة أو أجهزة كمبيوتر فردية – بما في ذلك المعلومات المخزنة بغرض تعزيز أهدافهم الاجتماعية أو السياسية. (٢)

---

(١) مكتب الأمم المتحدة المعنى بالمخدرات والجريمة ، استخدام الإنترنت في أغراض إرهابية ، المرجع السابق ، ص ٤٠.

(2)Mehmet Emin Erendor , AN ANALYSIS OF THREAT PERCEPTIONS: COMBATING CYBER TERRORISM: THE POLICIES OF NATO AND TURKEY, EVALUATED USING GAME THEORY IN THE CONTEXT OF INTERNATIONAL LAW , Thesis for the Degree of Doctor of Philosophy , UNIVERSITY OF SOUTHAMPTON FACULTY OF BUSINESS AND LAW , January 2017 , P. 114 .

أولاً : دوافع وأبعاد الإرهاب السيبراني :

غالباً ما يرغب المتسللون الإرهابيون في تحقيق هدف معين من عملياتهم . وعادة ما تتأثر هذه الأهداف بانحياز سياسي معين ، فعلى سبيل المثال تستخدم بعض الدول مثل هؤلاء الإرهابين لاختراق المعلومات الحكومية لدولة معارضة لتحقيق مكاسب سياسية أو من أجل عرقلة قرارات سياسية أو اجتماعية لتلك الدولة . والوجه الجديد للإرهاب خطير لأنه لا حدود له ، بسبب استخدامه للفضاء السيبراني ،وقدرتهم على ارسال فيروسات إلى أنظمة الكمبيوتر وشل المواقع العسكرية والسياسية والاقتصادية لدولة واحدة ، أو حتى لقارة . ويعد الإرهاب السيبراني أكثر فعالية من أنواع الإرهاب الأخرى ، ليس فقط لتكلفته الزهيدة ، ولكن أيضًا لأنه يكون من الصعب على الدول والمنظمات الدولية تعقب الإرهابيين الإلكترونيين. ، فإن الإرهاب السيبراني ، يستهدف أجهزة الكمبيوتر وشبكات الكمبيوتر الخاصة بالحكومات والأفراد والمرافق العامة و شركات الطيران الخاصة وما إلى ذلك .... ويضمن الإرهابيون نقاط ضعف يستغلونها ، لذلك هناك خطر واضح من الهجمات على المرافق الحكومية والعامة على حد سواء ، مما يخلق الخوف ، والذي يمكن أن يحقق نجاحًا أكثر من الأنواع الأخرى من الإرهاب [1].

ومن هنا يمكن أن يكون هناك عدة دوافع للإرهاب السيبراني ،سواء سياسية ، اجتماعية ، دينية وعقائدية ، اقتصادية .

ومن نافلة القول أنه غالباً ما يكون دافع الإرهاب السيبراني هو دافع متعلق بالسياسة .

ثانياً : أبعاد الإرهاب السيبراني

الأبعاد المتعلقة بالإرهاب السيبراني هي تلك المتعلقة بالجرائم السيبرانية الأخرى والتي سبق أن ذكرناها سلفاً وهي الأبعاد الاجتماعية والسياسية والقانونية والاقتصادية والعسكرية ، وذلك نظراً لما تسببه هذه الجرائم من دمار وخسائر فادحة .

---

(1) Mehmet Emin Erendor , op.cit .P. 114 -115.

وعلى سبيل المثال فقد تم رصد حدثين في دولة الكويت بتاريخ ١٧/ ١٢/ ٢٠٢٠ يحوزان أسلحة ويخططان للاعتداء على أحد المساجد وتبين أنه تم تجنيدهما عن طريق المواقع الالكترونية .

ثالثاً : تطور الإرهاب السيبراني :

يتمثل الهدف الأساسي للإرهاب التقليدي في تقويض قدرة المدنيين على الصمود من خلال غرس الشعور بالخوف والضعف لديهم مما يقوض لديهم الثقة في قدرة الحكومة ووكالات إنفاذ القانون على حمايتهم ضد الهجمات المستقبلية. فهل التداعيات النفسية للإرهاب التقليدي والإرهاب الإلكتروني متطابقة ؟ وهل يؤثر تهديد الإرهاب التقليدي أو الإلكتروني على الثقة في الحكومة ودعم السياسات الأمنية الصارمة بنفس الطريقة ؟ ... فيمكن الإجابة أن الإرهاب السيبراني يؤدي إلى تفاقم القلق والتوتر ويزيد من حدة الضعف كردود فعل مشابهة لما يفعله الإرهاب التقليدي . [1] ولكن تطور الإرهاب السيبراني في استخدامه للأدوات التي يرتكب بها الجريمة ومن أهم هذه الأدوات التكنولوجيا وذلك على التفصيل الأتي :

أ: بروتوكول الاتصال الصوتي عبر الإنترنت والبريد الإلكتروني :

تزايد على مدار العقد الماضي ، الإقبال على التطبيقات التي تتيح (للإرهابيين الإلكترونيين) الاتصال فيما بينهم باستخدام بروتوكول الاتصال عبر الإنترنت أو الدردشة بالفيديو ، أو الدردشة بالرسائل النصية ، كما ازداد تطورها ، فتتيح هذه التطبيقات خصائص متقدمة لتبادل المعلومات والملفات ، ويقوم هذا البروتوكول بتحويل الصوت التناظري إلى شكل رقمي مضغوط بما يتيح نقل حزم معلومات رقمية عبر الإنترنت باستخدام وصلات ذات نطاق ترددي ضيق نسبياً ، عن طريق بعض البرامج المستخدمة مثل سكايب وفونيدج والبريد الإلكتروني أيضاً يمكن أن يستغل في تبادل الرسائل غير المشروعة بين الإرهابيين بوصفها وسيلة سرية

---

(1) Herbert Lin and Amy Zegart , Bytes, Bombs, and Spies The Strategic Dimensions of Offensive Cyber Operations , Publisher : Brookings Institution Press , Washington , 2019 , 235-236 .

للإتصال [١]، ويستفاد من هذه الخاصية في التحقيقات لأن البريد يحتفظ بترويسة مختصرة عن بعض المعلومات ويمكننا القول أن هذه البروتوكولات قد تكون مجدية في التحقيقات في الجرائم الإرهابية التي ترتكب عبر الإنترنت ، فيمكن لسلطات إنفاذ القانون طلب معلومات عن الإرهابيين الإلكترونيين من مقدمي خدمات بروتوكول الإتصال عبر الإنترنت ، ويمكن أن تكون هذه المرحلة هي مرحلة تالية لمرحلة جمع المعلومات ومرحلة البحث عن معلومات إضافية متاحة عبر خدمات الإنترنت مثل مواقع التواصل الإجتماعي و محركات البحث .

ب: تقنيات تشفير البيانات وإخفاء الهوية والتكنولوجيا اللاسلكية .

تشفير البيانات يعني الحماية من إفشاء معلومات رقمية عن طريق تحويلها إلى نص مشفر ، باستخدام خوارزمية رياضية ومفتاح تشفير ، بحيث لا يفهمها إلا متلقيها والمرسلة إليه ، وغالباً ما تكون أدوات التشفير عبارة عن معدات أو برمجيات حاسوبية أو جهازاً أو أكثر من وسيلة . كما يمكن إخفاء الهوية أو الأنشطة الشبكية عبر تقنيات متقدمة ، بما في ذلك طمس عنوان بروتوكول الإنترنت المرسل بانتحال عنوان بروتوكول الإنترنت الخاص بنظام أخر ، أو إعادة توجيه حركة المعلومات على الإنترنت إلى عنوان مطموس . ويمكن أن تستخدم الجماعات الإرهابية الشبكات اللاسلكية التي تعتمد على الاتصال بالإنترنت من إشارة لاسلكية دون أن يكون التسجيل ضرورياً [٢].

---

(١) مكتب الأمم المتحدة المعني بالمخدرات والجريمة ، استخدام الإنترنت في الأغراض الإرهابية ، المرجع السابق ، ص ٥٤ .

(٢) مكتب الأمم المتحدة المعني بالمخدرات والجريمة ، استخدام الإنترنت في الأغراض الإرهابية ، المرجع السابق ، ص ٥٧ وما بعدها .

المبحث الثالث :
الحماية التشريعية من الجريمة السيبرانية بدول مجلس التعاون

يشهد المجتمع الخليجي تطوراً متسارعًا في تكنولوجيا المعلومات والاتصالات . كما يشهد التزايد في التطبيقات والخدمات التي تعتمد الفضاء الإلكتروني أساساً لها . ولأن تكنولوجيا المعلومات تعد الخطوة الأولى لبناء مجتمع المعرفة والقوام الاساسي في نموه وتطوره لذا تطلعت العديد من دول المجلس إلى إصدار القوانين التي تجرم الأشكال الجديدة والمستجدة للجريمة وعملت على إصدار العديد من الاستراتيجيات المتعلقة بالأمن السيبراني ومعالجة المشكلات القانونية الناتجة عن استخدام تكنولوجيا المعلومات والاتصالات وتطبيقاتها المختلفة المتعلقة بالحياة الاقتصادية والاجتماعية ، وعليه نقسم هذا المبحث إلى مطلبين على النحو التالي :

المطلب الأول : التشريعات الوطنية التي واجهت الجرائم السيبرانية

للحد من الأخطار الكبيرة والمتعددة التي تنطوي عليها الجريمة السيبرانية ، ولكونها عابرة للحدود ، استحدثت التشريعات الجنائية الوطنية نصوصاً خاصة للعقاب على هذه الأنشطة الإجرامية . ويمكننا القول أن نطاق التجريم يختلف من تشريع لآخر ،.ونقسم هذا المطلب إلى ستة فروع .

الفرع الأول : تشريع دولة الكويت

نظراً لتعدد جوانب مشكلة الجرائم السيبرانية ، وتماشياً مع الاتجاه الحديث الذي أقرته أغلب التشريعات المقارنة فيما يتعلق بوضع سياسة جنائية خاصة لمواجهة المخاطر المتزايدة التي تنطوي عليها الجرائم المتعلقة بالتكنولوجيا والاتصالات ، قام المشرع الكويتي بإصدارالقانون رقم ٢٠ لسنة ٢٠١٤ بشأن المعاملات الإلكترونية ، كما أصدر القانون رقم ٣٧ لسنة ٢٠١٤ المتعلق بإنشاء هيئة تنظيم الاتصالات وتقنية المعلومات ، وتلاه القانون رقم ٩٨ لسنة ٢٠١٥ المتعلق بتعديل أحكام القانون رقم ٣٧ لسنة ٢٠١٤ وجاء من أهم نصوصه في المادة الأولى " تعقب مصدر أي موجات راديوية للتحقق من ترخيص ذلك المصدر دون

المساس بسرية الرسائل ... "[١] ، وبموجب قرار رئيس مجلس الوزراء رقم ٩٩٣ لسنة ٢٠١٥ صدرت اللائحة التنفيذية للقانون رقم ٣٧ لسنة ٢٠١٤ ، والتي أولت لرئيس الهيئة عدة أعمال من اختصاصات أهمها :

١: إصدار لوائح تنظيم قطاعي الاتصالات وتقنية المعلومات .

٢: اقتراح مشروعات القوانين ومواكبة التطور السريع في قطاعي الاتصالات وتقنية المعلومات . .

ويتكون قطاع تقنية المعلومات في دولة الكويت من عدة إدارات وهي إدارة تطوير تقنية المعلومات، وإدارة أمن المعلومات والاستجابة والطوارئ ، وإدارة تشغيل المشاريع الوطنية ، وإدارة حوكمة القطاع العام . ومن أهم إختصاصات إدارة أمن المعلومات والاستجابة والطوارئ الآتي [٢]:

أولاً : إعداد الاستراتيجية الوطنية للأمن السيبراني .

ثانياً : تعزيز الوعي الوطني لدى المواطنين والمؤسسات والقطاع العام بالأمن السيبراني .

ثالثاً : إنشاء مركز الأمن الوطني السيبراني NCSC كمظلة لمراكز عمليات الأمن السيبراني SOC لحماية المصالح الوطنية من الهجمات السيبرانية المحتملة.

رابعاً : تطوير كفاءة المتخصصين في مجال الأمن السيبراني ومكافحة الجرائم السيبرانية وفقاً للمعايير الدولية.

وأُدخلت الجريمة السيبرانية إلى التشريع الكويتي بموجب القانون رقم ٦٣ لسنة ٢٠١٥ ، المتعلق بمكافحة جرائم تقنية المعلومات ،ويعد هذا القانون هو أول الخطوات التي اتخذتها

---

(١) استبدلت المادة رقم ٣ بند (م) من القانون رقم ٣٧ لسنة ٢٠١٤ ، بموجب القاتون رقم ٩٨ لسنة ٢٠١٥ المتعلق بإنشاء هيئة تنظيم الاتصالات وتقنية المعلومات .، الصادر في ١٦ أغسطس عام ٢٠١٥ .

(٢) الموقع الرسمي للهيئة العامة للاتصالات وتقنية المعلومات : (citra)

https://citra.gov.kw/sites/ar/Pages/Sectors/CompetenciesInformationTechnologySector.asx

دولة الكويت نحو تجريم الأنشطة الإجرامية غير المشروعة التي ترتكب بواسطة تقنية المعلومات والاتصالات، وبموجب هذا القانون تم تجريم عدة أفعال وهي : الدخول غير المشروع إلى نظام الحاسب أو نظامه أو إلى نظام المعالجة الإلكترونية للبيانات أو إلى نظام كومبيوتر مؤتمت أو إلى شبكة معلوماتية ، والدخول غير المشروع إلى موقع أو نظام معلوماتي ، وجريمة تزوير مستند أو سجل أو توقيع إلكتروني ، وجريمة التهديد والإبتزاز والاستيلاء على الأموال والجرائم الماسة بالأداب العامة والجرائم الواقعة على الأطفال، وجرائم الاتجار بالبشر وجرائم المخدرات المرتكبة بواسطة تقنية المعلومات،وغيرها من الجرائم . (١)

ونظراً لأهمية تعزيز ثقافة الأمن السيبراني ولحماية البنى التحتية لدولة الكويت واتاحة سبل التعاون بين مختلف الجهات المحلية والدولية في مجال الأمن السيبراني ، أصدرت دولة الكويت الاستراتيجية الوطنية للأمن السيبراني، ٢٠١٧ - ٢٠٢٠ ، كنتيجة حتمية للتحديات والتهديدات التي تواجهها . (٢)

وقد أصدرت الهيئة العامة للاتصالات وتقنية المعلومات عدة لوائح متعلقة بمكافحة الجريمة السيبرانية ومن أهمها اللائحة الوطنية لخدمة الواي فاي (wifi) ، والتي ألزمت مقدمي الخدمة بعدة التزامات ومنها :

١ : الالتزام بتوفير أحدث البرامج والأجهزة اللازمة لحماية الشبكات والبيانات ومراقبتها ، وذلك وفقاً لمعايير الهيئة العامة للاتصالات وتقنية المعلومات .

---

(١) الجريدة الرسمية بالكويت (الكويت اليوم) ، العدد ١٢٤٤ ، في ١٢ يوليو عام ٢٠١٥ ، المادة الثالثة وما بعدها .

(٢) للمزيد من التفاصيل حول الاستراتيجية الوطنية المتعلقة بالأمن السيبراني ٢٠١٧-٢٠٢٠ ، الموقع الرسمي للهيئة العامة للاتصالات وتقنية المعلومات ، https://citra.gov.kw/sites/ar/LegalReferences/Cyber%20Security.pdf

٢: يحق للهيئة العامة للاتصالات وتقنية المعلومات مراقبة ومتابعة المرخص لهم الخدمة التجارية لبيان مستوى سرية وأمن المعلومات ومدى تطبيقه للمواصفات والمعايير المتعلقة بالأمن السيبراني .

وأخيراً استحدثت الكويت وزارة لشئون الاتصالات وتكنولوجيا المعلومات [١] وعهد إليها تطوير البنية التحتية الالكترونية وتعزيز الأمن السيبراني والارتقاء بالخدمات الحكومية الالكترونية والذكية وتنمية قطاع الاتصالات .

ويمكننا القول أن دولة الكويت حاولت تلبية المتطلبات الدولية بشأن إصدار القوانين واللوائح المتعلقة بمكافحة الجرائم السيبرانية [٢]، وقامت بتفعيل بعض المبادرات المتعلقة بتطوير وتأهيل الكوادر الوطنية بمجالات الأمن السيبراني، وبعض المبادرات الهامة أثناء فترة إنتشار كورونا ومنها مبادرة Cisco Umbrella المتعلقة بتأمين العمل عن بعد ، إلا أنه لابد من وضع استراتيجية متكاملة متعلقة بالأمن السيبراني تغطي كافة النواحي التقنية والإجرائية والقانونية وتغطي التعاون الكامل بين دول مجلس التعاون .

---

(١) أُنشأت الوزارة بالمرسوم الأميري رقم ١٨/ ٢٠٢١ ، الصادر في ٢/ ٣/ ٢٠٢١ بتشكيل الوزارة ، والمنشور بالجريدة الرسمية – الكويت اليوم ، العدد ١٥٢٥ ، السنة السابعة والستون – بتاريخ ٧/ ٣/ ٢٠٢١ .

(٢) في ٢٦/ ١٠/ ٢٠٢٠ ، قضت محكمة الجنايات في الكويت بمعاقبة أحد المخترقين بالحبس لمدة سبع سنوات مع الشغل والنفاذ لاختراقه حساب وكالة الأنباء الكويتية (كونا) وإذاعته خبراً غير صحيح عن القوات الأمريكية في الكويت .

الفرع الثاني : تشريع دولة الإمارات

أجرت دولة الإمارات العربية المتحدة منذ عام ٢٠٠٦ ، إصلاحات أساسية على تشريعاتها الموضوعية والإجرائية والتنفيذية المتعلقة بالسياسات من أجل مكافحة الجريمة السيبرانية بفعالية .

وأصدر المشرع الإماراتي القانون رقم ١ لسنة ٢٠٠٦ المتعلق بالمعاملات والتجارة الإلكترونية (١)،وصدر القانون الاتحادي رقم ٢ لسنة ٢٠٠٦ بشأن مكافحة جرائم تقنية المعلومات ، وتلا ذلك القرار الوزاري رقم ١ لسنة ٢٠٠٨ ، المتعلق بإصدار لائحة مزودي خدمات التصديق (٢) ،وفي ضوء تحديث دولة الإمارات لتشريعاتها صدر المرسوم بقانون اتحادي رقم ٣ لسنة ٢٠١٢ المتعلق بإنشاء الهيئة الوطنية للأمن الإلكتروني وتختص بعدة اختصاصات من أهمها (٣):

أ: مكافحة جرائم الحاسب الآلي والشبكة المعلوماتية وتقنية المعلومات على اختلاف أنواعها.

ب: تلقي الشكاوى والمقترحات المتعلقة بالأمن الإلكتروني في الدولة.

ج: إقتراح التشريعات المتعلقة بالأمن الإلكتروني.

د: نشر الوعي بأهمية الأمن الإلكتروني بالتنسيق مع الجهات المعنية.

وصدر المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ ، المتعلق بمكافحة جرائم تقنية المعلومات ، وبموجب المادة ٥٠ منه تم إلغاء القانون رقم ٢ لسنة ٢٠٠٦ ، وتم تجريم عدة أفعال إجرامية تشكل جرائم سيبرانية ومن أهمها :

---

(١) الجريدة الرسمية بالإمارات ، العدد رقم ٤٤٢ ، المنشور في ٣١/ ١/ ٢٠٠٦ .

(٢) البوابة الرسمية لحكومة دولة الإمارات ، https://u.ae/ar-ae/resources/laws.

(٣) الجريدة الرسمية بالإمارات العدد ٥٤٠ ، بتاريخ ٢٦/ ٨/ ٢٠١٢ ، المادة ٥ ، من مرسوم بقانون اتحادي رقم ٣ لسنة ٢٠١٢ ، المتعلق بإنشاء الهيئة الوطنية للأمن الإلكتروني ، وتم تعديل هذا المرسوم بموجب مرسوم بقانون اتحادي رقم ٩ لسنة ٢٠١٥ .

١: دخول موقع الكتروني أو نظام معلومات الكتروني أو شبكة معلومات أو وسيلة تقنية معلومات بدون تصريح وبصورة غير مشروعة .

٢: دخول موقع إلكتروني بغير تصريح بقصد تغيير تصميمه أو إتلافه أو تعديله أو الغائه .

٣: الادخال عمداً وبدون تصريح برنامج معلوماتي إلى الشبكة المعلوماتية أو نظام المعلومات الإلكتروني أو إحدى وسائل تقنية المعلومات وإغراق البريد الالكتروني بالرسائل بقصد التعطيل أو الإيقاف أو الإتلاف .

٤: استخدام الشبكة المعلوماتية أو نظام المعلومات الإلكتروني أو وسائل تقنية المعلومات بهدف الحصول على أرقام أو بيانات بطاقة ائتمانية أو إلكترونية أو حسابات مصرفية .

٥: حيازة مواد إباحية للاحداث عمداً باستخدام إحدى وسائل تقنية المعلومات .

٦: وبموجب القانون رقم ١٢ لسنة ٢٠١٦ المتعلق بتعديل المرسوم بقانون رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات ، نص على فرض عقوبة السجن المؤقت والغرامة على كل من تحايل على العنوان البروتوكولي للشبكة المعلوماتية باستخدام عنوان وهمي أو عنوان عائد للغير أو بأي وسيلة أخرى بقصد ارتكاب جريمة أو الحيلولة دون اكتشافها [١] .

ولتحقيق التوازن بين عملية نشر وتبادل البيانات ، والحفاظ على سريتها وخصوصيتها ، وغيرها من الاهداف ، أصدر المشرع الإماراتي القانون رقم ٢٦ لسنة ٢٠١٥ ، المتعلق بتنظيم ونشر البيانات في إمارة دبي ، وفي ضوء حماية بيانات المتعاملين نصت المادة ١٣ من ذلك القانون على إلتزام مزدوي البيانات بإتخاذ كافة الإجراءات اللازمة للحفاظ على سرية وخصوصية بيانات المتعاملين التي تتمتع بالحماية القانونية خلال عملية النشر وتبادل البيانات [٢] .

---

(١) الجريدة الرسمية ، ملحق العدد ٥٩٧ ، منشور بتاريخ ٢٣/ ٥/ ٢٠١٦ ، المادة الأولى من القانون رقم ١٢ لسنة ٢٠١٦ .

(٢) الجريدة الرسمية بالإمارات ، العدد ٣٩٣ ، السنة ٤٩ ، منشور بتاريخ ٢٧ ديسمبر عام ٢٠١٥ ، المادة ١٣ من القانون رقم ٢٦ لسنة ٢٠١٥ .

وتلبية لمتطلبات المرحلة الراهنة والتي تشهد تزايداً في عدد حوادث الأمن السيبراني عالمياً ، والتي تسببت في تضاعف الخسائر بشكل كبير والتي أثرت على الإقتصاد العالمي ، أصدرت هيئة تنظيم الإتصالات بدولة الإمارات الاستراتيجية الوطنية للأمن السيبراني عام ٢٠١٩ ، والتي عملت على تعزيز المنظومة المتكاملة للأمن السيبراني من خلال تنفيذ ٦٠ مبادرة ضمن ٥ محاور، حيث حددت الاستراتيجية القوانين والأنظمة المتعلقة بالأمن السيبراني، لمعالجة جميع أنواع الجرائم السيبرانية، وحماية التكنولوجيا الحالية والناشئة، والعمل على حماية الشركات الصغيرة والمتوسطة، وذلك من خلال تطوير معايير الأمن السيبراني الأساسية للشركات الصغيرة والمتوسطة، و إلزام موردي الجهات الحكومية بحيازة شهادة تطبيق الأمن السيبراني، وتطوير بوابة موحدة للشركات الصغيرة والمتوسطة لتمكينها من تنفيذ المعايير القانونية . [1]

وتماشياً مع التطور التكنولوجي الذي يشهده العالم ، والتحول الذكي الذي تشهده إمارة دبي ، وعملت إمارة دبي على صياغة استراتيجية للأمن السيبراني ، لتوفير الحماية الكاملة ضد مخاطر الهجمات السيبرانية . وعملت على ترسيخ أطر التعاون الدولي مع القطاعات الداخلية والخارجية من خلال تأسيس شركات محلية وعالمية .

ومن الجهود التي قامت بها حكومة دولة الإمارات في تعزيز الأمن الرقمي والسلامة السيبرانية هي منصة الإبلاغ عن الجرائم السيبرانية ، مثل الابتزاز الإلكتروني، والاختراقات التقنية، والاحتيالات المالية وغيرها من الجرائم التي ترتكب عبر شبكة الإنترنت، وشبكات التواصل الاجتماعي ، ويمكن أن يتم الإبلاغ أيضاً عبر التطبيق الذكي "مجتمعي آمن" الذي أنشأته النيابة العامة بدولة الإمارات [2] .

---

(١) الموقع الرسمي لهيئة تنظيم الإتصالات (tra) بالإمارت، https://www.tra.gov.ae/ar/media-hub/press-releases/2019/6/24/tra-launches-the-uae-national-cybersecurity-strategy.aspx

(٢) البوابة الرسمية لحكومة دولة الإمارات العربية المتحدة ، المرجع السابق .

الفرع الثالث : تشريع المملكة العربية السعودية

نظراً للزيادة المطردة في الجرائم السيبرانية لدى المملكة العربية السعودية ، والتي أثارت عدد من التحديات الجديدة لأجهزة إنفاذ القانون [١] ، من حيث طبيعتها ونطاقها وأدلتها وأنشطتها ، أصدرت المملكة العربية السعودية نظاماً يواجه به الجرائم السيبرانية بموجب المرسوم الملكي رقم م / ١٧ بتاريخ ٨/ ٣/ ١٤٢٨ هـ ، بناء على قرار مجلس الوزراء رقم ٧٩ ، بتاريخ ٧/ ٣/ ١٤٢٨ ، ونصت المادة الثانية من النظام على وجود عدة أهداف للحد من الجرائم المعلوماتية وهي [٢] :

١ : المساعدة على تحقيق الأمن المعلوماتي

٢ : حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الالية والشبكات المعلوماتية .

---

(١) أعد تقرير الأمم المتحدة بموجب القرار رقم ٧٣/ ١٨٧ ،المتعلق بمكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية ، وفي ذلك القرار طلبت الأمم المتحدة من الدول الأعضاء إعداد رأي بشأن التحديات التي تواجه الأجهزة المعنية أثناء إنفاذ القانون ، وقد وضعت المملكة العربية السعودية عدة تحديات أثناء مواجهة الجريمة السيبرانية ومن أهمها :

أ: ضعف تعاون شركات المنصات الرقمية مع السلطات القانونية وسلطات إنفاذ القانون حول العالم .

ب: غياب الهوية الرقمية في العالم الإفتراضي ، واستخدام هويات وهمية ، وتباين التشريعات والقوانين للدول الأعضاء بالأمم المتحدة ، والافتقار بين التنسيق والتعاون والمساعدة بين الدول بشأن مكافحة الجرائم السيبرانية .

ت: عدم كفاية الضوابط المتعلقة بتقديم الخدمات الإلكترونية .

ث: الافتقار إلى نظم المعلومات التي تكشف العمليات المشبوهة ، وضعف القدرات البشرية والتقنية .

جـ: ضعف الوعي بالاستخدام الامن والأمثل لتكنولوجيا المعلومات والاتصالات .

راجع في ذلك : تقرير الأمم المتحدة رقم A/74/130 ، بتاريخ ٢٠١٨/ ٧/ ٣٠ ، ص ٧٩ وما بعدها .

(٢) د. إيمان بنت محمد علي عادل عزام ، بحث محكم بعنوان : العقوبة في نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية ، دراسة تأصيلية مقارنة ، مجلة العدل ، مجلة فصلية علمية محكمة ، العدد ٨٢ ، شهر رجب ١٤٣٩ هـ ، ص ٨٨ .

٣: حماية المصلحة العامة ، والأخلاق ، والأداب العامة .

٤: حماية الاقتصاد الوطني .

وقد قامت المملكة العربية السعودية ، عام ٢٠١٨ ، بإصدار الضوابط الأساسية المتعلقة بالأمن السيبراني ، والتي أوضحت معاني المصطلحات التقنية وعملت على الحد من الجرائم السيبرانية ،الا أن هذه الضوابط قد شابها قصور من ناحية زيادة تدعيم التعاون بين دول مجلس التعاون والدول الأخرى سواء على المستوى القضائي أو الشرطي .

وفي شهر يونيو من عام ٢٠٢٠ ، أصدرت المملكة الإطار التنظيمي للأمن السيبراني لمقدمي الخدمة في قطاع الاتصالات وتقنية المعلومات والبريد ، ولهذا الإطار عدة أهداف من أهمها : توفير متطلبات لتحسين إدارة مخاطر الأمن السيبراني ، وتمكين ممارسات الأمن السيبراني إلى مقدمي الخدمة في قطاع الاتصالات وتقنية المعلومات ، وضمان سرية الخدمات المقدمة للعملاء . (١)

(١) الموقع الرسمي لهيئة الاتصالات وتقنية المعلومات السعودية :
https://www.citc.gov.sa/ar/RulesandSystems/CyberSecurity/Documents/CRF-ar.pdf

الفرع الرابع : تشريع سلطنة عمان .

في ضوء إهتمام سلطنة عمان بتجريم الأنشطة الإجرامية للجريمة السيبرانية ، صدر المرسوم السلطاني رقم ١٢ لسنة ٢٠١١ ، المتعلق بإصدار قانون مكافحة جرائم تقنية المعلومات ، والذي جرم عدة أنشطة إجرامية منها : التعدي على سلامة وسرية وتوافر البيانات والمعلومات الإلكترونية والنظم المعلوماتية ، إساءة استخدام وسائل تقنية المعلومات ، التزوير والاحتيال المعلوماتي ، وجرائم المحتوى المتعلقة بالأطفال ، والجرائم المرتكبة من العناصر الإرهابية عبر الإنترنت ، وجرائم التعدي على البطاقة الإئتمانية .[١]

وقد عملت سلطنة عمان على إصدار العديد من الضوابط والأطر ، ومن أهمها ضوابط محتوى المواقع الإلكترونية ، وأطر الحوكمة في وزارة التقنية والاتصالات ، ودليل سياسات مواقع الويب وأمانها ، ودليل إرشادات تصنيف البيانات ونظم أمن المعلومات ، وسياسة التواصل الاجتماعي ، وضوابط محتوى المواقع الإلكترونية ، وضوابط النفاذ الرقمي ، وإطار إدارة مخاطر تقنية المعلومات ، ودليل إرشادات حوكمة الأمن السيبراني ، وإطار حوكمة الحوسبة السحابية ، والدليل الإرشادي الخاص بالضوابط الاساسية لأمن المعلومات ، واستراتيجية عمان الرقمية[٢] .

وتحت شعار "التحكم في مخاطر الأمن الإلكتروني المصاحبة للعمل عن بعد"؛ نظمت وزارة النقل والاتصالات وتقنية المعلومات ممثلة في المركز الوطني للسلامة المعلوماتية

---

(١) الجريدة الرسمية ، العدد ٩٢٩ ، المرسوم السلطاني رقم ١٢ لسنة ٢٠١١ ، المتعلق بقانون مكافحة جرائم تقنية المعلومات .

(٢) الموقع الرسمي للخدمات الحكومية العمانية ، https://omanuna.oman.om/ .

"التمرين الافتراضي للأمن السيبراني الثامن للدول العربية وللدول الأعضاء بمنظمة التعاون الإسلامي وذلك بمشاركة ٢٥ دولة [١]

الفرع الخامس : تشريع دولة قطر

أصدرت قطر القانون رقم ١٤ لسنة ٢٠١٤ ، المتعلق بمكافحة الجرائم الإلكترونية ، الذي يشكل خطوة متقدمة نحو تعزيز التشريعات والإجراءات الوطنية لمكافحة الجرائم السيبرانية . وتناول القانون عدة أفعال بالتجريم ومنها : التعدي على نظم وبرامج وشبكات المعلومات ، وجرائم الاحتيال والتزوير الإلكترونيين ، وجرائم إنتهاك حقوق الملكية الفكرية ، ونص أيضاً على السماح بالتعاون الدولي ، بما في ذلك المساعدة القانونية المتبادلة وتسليم المجرمين .

وأدركت دولة قطر أن هناك حاجة ملحة إلى تعزيز التدابير القانونية على الصعيدين الوطني والدولي من أجل التصدي للجريمة السيبرانية ، وأنه من الضروري إتخاذ إجراءات فعالة نحو تجريم الجرائم الإرهابية المرتكبة بواسطة وسائل تقنية المعلومات ، وذلك من أجل صون السلام والاستقرار وتهيئة بيئة منفتحة ومستقرة وسليمة لتكنولوجيا المعلومات والاتصالات [٢]

كما أصدرت الاستراتيجية الوطنية للأمن السيبراني عام ٢٠١٤ ، ونظراً لإستضافة قطر لكأس العالم ٢٠٢٢ ، فقد دعت مؤخرًا إلى إنشاء منصة دولية موحدة من خلال الإنتربول "لتعزيز التواصل والتعاون في مجال الأمن السيبراني للأحداث الرياضية".

ويظهر هذا التطور الأخير أن قطر تدرك ضرورة المشاركة الدولية في جهود الأمن السيبراني حول العالم . [٣]

---

(١) الموقع الرسمي للمركز الوطني للسلامة الوطنية : https://www.cert.gov.om/media_news_details_arabic.aspx?news=103 ، بتاريخ ٢٢/ ١٢/ ٢٠٢٠ .

(٢) راجع في ذلك : تقرير الأمم المتحدة رقم A/74/130 ، المرجع السابق ، ص ٧٤ وما بعدها .

(٣) الموقع الرسمي لمنتدي الخليج العربي ، https://gulfif.org/the-new-battlefront-cyber-security-across-the-gcc/ ، في ٢٩/ ١٠/ ٢٠١٨ .

الفرع السادس : تشريع مملكة البحرين

أصدر المشرع البحريني القانون رقم ٦٠ لسنة ٢٠١٤ ،المتعلق بمكافحة جرائم تقنية المعلومات ، وقد جرم هذا القانون الجرائم الواقعة على أنظمة وبيانات تقنية المعلومات والجرائم ذات الصلة بوسائل تقنية المعلومات ، والجرائم ذات الصلة بالمحتوى وبصفة خاصة الواقعة على الأطفال . [١]

وبموجب القانون رقم ٢ لسنة ٢٠١٧ ، تم تصديق مملكة البحرين على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ، وأصدر المشرع القانون رقم ٣٠ لسنة ٢٠١٨ بشأن حماية البيانات الشخصية [٢] ، والمرسوم بقانون رقم ٥٦ لسنة ٢٠١٨ بشأن تزويد خدمات الحوسبة السحابية لأطراف أجنبية [٣]، وأخيراً صدر التشريع رقم ٢٠ لسنة ٢٠٢٠ المتعلق باعتماد الخطة الوطنية للترددات [٤].

وفي إطار مواجهة مملكة البحرين للجريمة السيبرانية ، أصدرت اللائحة التنظيمية لإدارة مخاطر البنية التحتية الأساسية للاتصالات ، وأعتمدت الاستراتيجية الوطنية للأمن السيبراني ، ويمكن القول أن تلك الاستراتيجية جاءت فقيرة ولابد من تعديلها وإضافة العديد من سبل التعاون والإجراءات ووسائل التقنية الحديثة المستخدمة في تدعيم الأمن السيبراني لمواجهة الأنشطة غير المشروعة المرتكبة عبر وسائل تقنية المعلومات .

ومن خلال مؤشر الاتحاد الدولي للاتصالات نرتب دول مجلس التعاون لدول الخليج العربية التي أولت إهتمام بالأمن السيبراني وعقد مقارنة بين عامي ٢٠١٧، ٢٠١٨ من حيث

---

(١) الجريدة الرسمية بالبحرين ، العدد ٣١٧٨ ، ٩/ ١٠/ ٢٠١٤ ، قانون رقم ٦٠ لسنة ٢٠١٤ ، المتعلق بمكافحة جرائم تقنية المعلومات .

(٢) الجريدة الرسمية بالبحرين ، العدد ٣٣٧٥ ، في ١٩ يوليو من عام ٢٠١٨ ، قانون رقم ٣٠ لسنة ٢٠١٨ .

(٣) الجريدة الرسمية بالبحرين، العدد ٣٣٩٥ ، في ٢٩ نوفمبر ٢٠١٨ ، قانون رقم ٥٦ لسنة ٢٠١٨.

(٤) الجريدة الرسمية بالبحرين ، العدد ٣٤٨١ ، في ٢٣ يوليو عام ٢٠٢٠ ، قانون رقم ٢٠ لسنة ٢٠٢٠ .

ارتفاع مؤشر الأمن السيبراني من النواحي الإجرائية والقانونية والتقنية وبناء القدرات والتعاون ، ونوضحها في الجدول الآتي :

عام	الكويت	الإمارات	السعودية	عمان	قطر	البحرين
٢٠١٧	١٣٨ عالمياً ١٧ عربياً	٤٧ عالمياً ٦ عربياً	٤٦ عالمياً ٥ عربياً	٤ عالمياً ١ عربياً	٢٥ عالمياً ٣ عربياً	٦٤ عالمياً ٨ عربياً
٢٠١٨	٦٧ عالمياً ٦ عربياً	٣٣ عالمياً ٥ عربياً	١٣ عالمياً ١ عربياً	١٦ عالمياً ٢ عربياً	١٧ عالمياً ٣ عربياً	٦٨ عالمياً ٧ عربياً

المطلب الثاني :
الاتفاقيات الدولية والعربية التي نادت بتعاون الدول لمواجهة الجرائم السيبرانية .

تعد المعاهدات الدولية والاتفاقيات الاقليمية من أهم صور التعاون بصفة عامة ، وفي مجال مكافحة الجرائم الناتجة عن الهجمات السيبرانية بصفة خاصة ، ومن بين الاتفاقيات الدولية التي تعمل على دعم التعاون الدولي في مجال مكافحة الجرائم السيبرانية ، اتفاقية بودابست لمكافحة الجرائم السيبرانية ، ومن الاتفاقيات الإقليمية ، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ، ونبينهما فيما يلي :

الفرع الأول : اتفاقية بودابست لمكافحة الجرائم السيبرانية

أبرم مجلس أوروبا اتفاقية مكافحة الجرائم السيبرانية في مدينة بودابست عام ٢٠٠١ ، إيماناً من دول المجلس بالتغيرات العميقة التي أحدثتها التطورات الرقمية والتقارب والعولمة المستمرة للشبكات المعلوماتية ، وتتكون الاتفاقية من ثماني وأربعون مادة [١] تتعلق بتجريم بعض أشكال الجريمة السيبرانية ووضع قواعد التعاون الدولي بين الدول .

وتعد اتفاقية بودابست الأساس القانوني التقني والإجرائي الأول للتعاون الدولي بين دول العالم بصفة عامة لمواجهة الجرائم السيبرانية وتحقيق الأمن السيبراني .

ونظراً للطابع غير المستقر لأدلة الإثبات الإلكترونية والتي فرضت تحديات أمام التعاون الدولي ، منها صعوبة وصول أجهزة إنفاذ القانون إلى البيانات ، مثل نقاط الاتصال المتاحة على مدار الساعة فيما يتعلق بالتحريات عن الجرائم السيبرانية ، والوصول غير المحدود إلى البيانات الحاسوبية المخزنة ، والطلبات العاجلة للمساعدة المتبادلة ، فبموجب اتفاقية

---

(١) د. هلالي عبداللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقاً عليها ، دار النهضة العربية ، القاهرة ، الطبعة الثامنة ، عام ٢٠١١ ، ص ٧ وما بعدها .

بودابست ، تتولى نقاط اتصال على مدار الساعة طوال أيام الأسبوع لتسهيل ما سلف ذكره ، إذا كانت تسمح قوانين الدول بذلك [١].

وبالرغم من أن اتفاقية بودابست تعد من الصكوك الدولية التي تعتمد الكثير من الدول عليها في تعزيز التعاون الدولي إلا أننا بحاجة إلى اتفاقية دولية إضافية تبرز حماية البيانات وغيرها من الضمانات التي تحقق سيادة القانون ، و تعزيز آلية الكشف السريع عن البيانات في حالة الطوارئ ، وتطوير النظام الحالي للإفصاح الطوعي عن البيانات من قبل مقدمي الخدمة ، وتدعيم الفعالية المحدودة للأدلة الإلكترونية المتطايرة .

وإلى جانب الدول الأعضاء في مجلس أوروبا الذين قاموا بالتصديق والتوقيع على هذه الاتفاقية يوجد نحو ٣١ دولة من غير الأعضاء قاموا بالتوقيع والتصديق عليها حتى ٢٩/ ١/ ٢٠٢١وأول هذه الدول هي الولايات المتحدة الأمريكية [٢]

ومن الجدير بالذكر أن دول مجلس التعاون لم تقم بطلب الإنضمام إلى اتفاقية مجلس أوروبا المتعلقة بمكافحة الجريمة السيبرانية على الرغم من توقيع وتصديق العديد من الدول العربية الأخرى والدول الأفريقية ودول بقارة أسيا كما هو موضح بالجدول سالف الذكر وذلك وفقاً للمادة رقم٣٧، ٣٨، ٤٨ من الاتفاقية .

---

(١) ورقة معلومات أساسية بعنوان جمع وتبادل الأدلة الإثباتية الإلكترونية ، الأمم المتحدة ، مؤتمر الأطراف لمكافحة الجريمة المنظمة عبر الوطنية ، وثيقة رقم CTOC/COP/WG.3/2015/2 ، في ١٨ / ٨ / ٢٠١٥ .

(٢) الموقع الرسمي لاتفاقية بودابست المتعلقة بمكافحة الجرائم السيبرانية ، https://www.coe.int/ .

الفرع الثاني : اتفاقية جامعة الدول العربية

في سبيل تعزيز التعاون بين الدول العربية فيما بينها وتبني سياسة جنائية مشتركة لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ، تم إبرام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي تعد الأساس القانوني للتعاون بين الدول العربية في مجال مكافحة الجرائم السيبرانية .

وقد حثت الاتفاقية العربية على التعاون الدولي بين الدول الأعضاء سواء على المستوى القانوني أو على المستوى القضائي ونبين ذلك من عدة أوجه :

أولاً : من حيث الاختصاص : ألزمت الاتفاقية الدول الأعضاء بمد اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من الاتفاقية إذا ارتكبت في إقليم الدولة الطرف أو على متن سفينة أو متن طائرة مسجلة تحت قوانين الدولة الطرف أو إذا ارتكبت من أحد مواطني الدولة ، وإذا ادعت أكثر من دولة بالاختصاص القضائي فيقدم طلب الدولة التي أخلت الجريمة السيبرانية بأمنها. (١)

ثانياً : من حيث تسليم المجرمين : نصت الاتفاقية على عدة شروط لتسليم المجرمين المرتكبين للجرائم السيبرانية المنصوص عليها في الباب الثاني من أهمها أن تكون الجريمة السيبرانية معاقب عليها في الدولة الطرف بعقوبة لا تقل عن سنة أو بعقوبة أشد إلا إذا وجد اتفاق بين دولتين أو معاهدة أخرى تنظم المسألة فيطبق الاتفاق أو المعاهدة الأخرى .

ثالثاً : بالنسبة للمساعدة المتبادلة : حثت الاتفاقية الدول الأعضاء على المساعدة المتبادلة فيما بينها بشأن التحقيقات أو الإجراءات المتعلقة بجرائم تقنية المعلومات وجمع الأدلة الإلكترونية عن الجرائم .

---

(١) المادة الثلاثون ، الفصل الرابع ، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ، الموقعة في القاهرة .

وأن يتم تقديم طلب المساعدة من الدولة الطرف بواسطة الكتابة وفي حالة الاستعجال يتم تقديمه بواسطة البريد الإلكتروني المشفر أو الفاكس مع الحفاظ على عنصر السرية .[1]

وقد وقعت دول مجلس التعاون على هذه الاتفاقية بتاريخ ٢١/ ١٢/ ٢٠١٠ عدا سلطنة عمان حيث وقعت بتاريخ ١٥/ ٢/ ٢٠١٢ ، ويمكننا القول أن جامعة الدول العربية سعت نحو إبراز دور التعاون بين الدول الأعضاء في هذه الاتفاقية ، على الرغم من وجود بعض المسائل الفنية والتقنية التي كان لابد من الاعتماد عليها في هذا التعاون ولم تبرزها تلك الاتفاقية .

(١) المادة الثانية والثلاثون ،والمادة السادسة والثلاثون الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ، المرجع السابق .

الخاتمة

أصبحت تكنولوجيا المعلومات والاتصالات بنية تحتية عالمية لكل من الحكومات والشركات . وبالتالي ، أصبح الأمن السيبراني أولوية لدول مجلس التعاون لدول الخليج العربية . ويلعب الأمن السيبراني دورًا هامًا في محاولة منع الجرائم السيبرانية ،وبشكل خاص في حماية سرية وسلامة وحماية البيانات السرية وحماية البنية التحتية الحيوية وأنظمة الكمبيوتر الحكومية من الهجمات السيبرانية وانتهاك البيانات الحساسة التي تؤثر على السلامة العامة والأمن القومي ، وفي ضوء تنفيذ تدابير الأمن السيبراني يجب احترام سيادة القانون وخصوصية البيانات وحرية التعبير وحقوق الإنسان .

بالإضافة إلى ذلك ، تحولت بيئة التهديد للكيانات المكلفة بحماية البنية التحتية الحيوية والمعلومات الحساسة بقدر لم يعد من الممكن افتراض أنه يمكن حماية النظام بشكل كاف ضد الهجمات المستهدفة .

فلا يوجد شيء اسمه الأمن المطلق ، ولكن يجب على الأفراد والشركات والحكومات بذل قصارى جهدهم لجعل الهجمات الإجرامية صعبة قدر الإمكان والاستعداد لها، فهي لاشك الحرب القادمة، لذلك من الأهمية ألا يستثمر جميع أصحاب المصلحة في الحماية المباشرة لتكنولوجيا المعلومات والاتصالات (أنظمة وتكنولوجيا المعلومات والاتصالات) فحسب ، بل يجب أن يستثمروا قدراتهم في الكشف عن التهديدات. ومن المهم بنفس القدر وجود الأطر القانونية والتنظيمية اللازمة لتمكين وتسهيل التعاون وتبادل المعلومات بين السلطات الوطنية والقطاع الخاص كما أوضحت اتفاقية بودابست الأوربية والاتفاقية العربية لمكافحة جرائم تقنية المعلومات ، وقد سعت دول مجلس التعاون لدول الخليج العربية لإصدار العديد من الاستراتيجيات المتعلقة بالأمن السيبراني لمكافحة الجرائم السيبرانية بشكل أحادي ، وعملت على التوعية من آثارها وبفضل ذلك تقدمت في التصنيف العالمي للأمن السيبراني .

النتائج

١: تطور الأمن السيبراني بالتوازي مع تطور أساليب وأشكال الجريمة السيبرانية ، مما فتح سبل جديدة لتعزيز التدابير لمواجهة المخاطر والعمل على تدعيم البنية التحتية للدول والقطاع الخاص .

٢: الأمن السيبراني يمر بمرحلتين : المرحلة الأولى : الوقاية من المخاطر ، والمرحلة الثانية: علاج الهجوم السيبراني بعد الاختراق .

٣: من أبرز القطاعات التي تضررت منها المملكة العربية السعودية في السنوات الأخيرة هو قطاع الطاقة ، كما أن القطاع المالي (وخاصة المصارف) أضحى مستهدفاً من الهجمات السيبرانية في دول المجلس .

٤: تزايد ضحايا الجريمة السيبرانية في ظل إنتشار كوفيد-١٩ ، وكان القطاع الصحي دولياً من أكثر القطاعات المتضررة من الهجمات السيبرانية المرتبطة بهذه الجائحة .

٥: جائحة كورونا سرعت من التحول إلى الخدمات عبر الإنترنت وهو ما يؤدي إلى تزايد المخاوف من الهجمات السيبرانية .

٦: يعد إنتشار إنترنت الأشياء من أهم التحديات السيبرانية في العصر الحديث فقد أدى إلى زيادة المخاطر السيبرانية نظراً لأن الإعتماد عليه قد يوفر وسيلة يمكن من خلالها شن الهجمات السيبرانية .

٧: الإرهاب الإلكتروني في الغالب يكون عابراً للحدود ، وغالباً ما يكون نتيجة الخلافات السياسية بين الدول والجماعات .

٨: الإرهاب التقليدي يرتكب عن طريق أعمال العنف كالقتل وخلافه أما الإرهاب الإلكتروني فيرتكب بأبسط الأدوات التكنولوجية التي تعتمد على وسائل تقنية المعلومات الحديثة .

٩: سعت دول مجلس التعاون نحو إصدار عدة تشريعات لتجريم الأنشطة الإجرامية المختلفة للجريمة السيبرانية .

١٠: أصدرت دول مجلس التعاون استراتيجيات أحادية متعلقة بالأمن السيبراني ، وإن كان بعضها يحتاج لمراجعة قانونية وتقنية لمواجهة المخاطر السيبرانية كافة .

التوصيات

١: يجب أن يتلاءم تعريف الأمن السيبراني مع فكرة عالمية المعلومات والاتصالات بحيث يكون التعريف مقبولاً على أن يراعي في هذا التعريف التطور المتزايد للتكنولوجيا .

٢: يجب أن تنص تشريعات دول مجلس التعاون علي تعريف موحد للأمن السيبراني ويكون متفق عليه ومقبولاً من الدول كافة ، حتي يتسنى لدول المجلس مواجهة الجريمة السيبرانية المتطورة

٣: يجب على كل دولة من دول مجلس التعاون انشاء مركز وطني للأمن السيبراني يعكف على دراسة التهديدات السيبرانية وأسبابها ووضع الخطط لمكافحتها وتحديد سبل الاستجابة الوطنية وإنشاء مركز خليجي للأمن السيبراني ينسق بين المراكز الوطنية .

٤: نظراً للتحديات التي تواجه الأمن السيبراني في مواجهة الجرائم السيبرانية فلابد من تطوير التطبيقات والبرامج والعمل على الإستعانة بالتقنيات الحديثة في تأمين الفضاء السيبراني .

٥: يجب العمل على إنشاء مجلس التعاون لدول الخليج هيئة الإستخبارات السيبرانية لتبادل المعلومات الاستخباراتية بين دول المجلس وتحسين الإطلاع على التهديدات السيبرانية .

٦: ضرورة عمل دورات تدريبية وتثقيفية للعاملين بمجال الأمن السيبراني وثقل معارف رجال إنفاذ القانون بتعليمات الأمن السيبراني والجريمة السيبرانية بشكل عام .

٧: يجب أن تتعاون الهيئات العامة لتنظيم قطاع الاتصالات بدول مجلس التعاون، وبين وزارات التربية على إعداد محتوى علمي يتعلق بالأمن السيبراني والتوعية من مخاطر الجريمة السيبرانية .

٨: ينبغي على دول مجلس التعاون أن تشرك بشكل مكثف القطاع الخاص في مواجهة الجرائم السيبرانية لحماية البنية التحتية الحيوية للمعلومات والفضاء السيبراني .

٩: يجب إنشاء منصة إلكترونية باللغتين العربية والأجنبية ، بدول المجلس تتلقى بلاغات المواطنين والمقيمين عن الجرائم السيبرانية كافة الواقعة عليهم ، وأن تسمح للشركات الوطنية والأجنبية بالإبلاغ عن الجرائم السيبرانية عبر تطبيق محدد وسهل .

١٠: نظراً لتخوف الشركات على مركزها المالي وسمعتها، وإحجامها عن الإبلاغ بوقوع هجوم سيبراني. فيجب أن يشترط أثناء إعطاء رخصة للشركات لمزاولة الأعمال التجارية أو الصناعية أو غيرها أن تقوم الشركة بالإبلاغ عن الجرائم السيبرانية ،وإلا يتم إلغاء هذه الرخصة مع ضمان الحفاظ على سرية هذا الابلاغ والحفاظ على مصالح تلك الشركات .

١١: يجب أثناء منح الرخص للشركات أن تلتزم بتدابير الأمن السيبراني وأن تقوم بتعيين إدارة لإدارة المخاطر والأمن السيبراني .

١٢: يجب أن تلتزم سلطات إنفاذ القانون بدول مجلس التعاون أثناء البحث عن الأدلة الإلكترونية بمبادئ حقوق الإنسان وعدم التعدي على خصوصية البيانات إلا بإذن قضائي .

١٣: يجب على دول المجلس أن تصدر تشريعًا يجرم الأنشطة الإجرامية التي ترتكبها الجماعات الإرهابية عبر الإنترنت .

١٤: يجب أن تعدل دولة البحرين الاستراتيجية المتعلقة بالأمن السيبراني لتواكب المستجدات المتعلقة بالأمن السيبراني وتطور التكنولوجيا .

١٥: في سبيل مواجهة دول المجلس للجرائم السيبرانية لابد من التعاون مع جهات مثل منظمة الشرطة الجنائية الدولية (الإنتربول) ووكالة تطبيق القانون (اليوروبول) ، ووكالات الأمن السيبراني في مختلف الدول والمنظمات العالمية والإقليمية .

١٦: يجب إصدار استراتيجية إقليمية من مجلس التعاون تتعلق بالأمن السيبراني لتنظيم التعاون بين دول المجلس لمواجهة الجريمة السيبرانية بفعالية وتبادل المعلومات المتعلقة بمرتكبيها .

المراجع

أولاً : المؤلفات المتخصصة :

- د/ محمد سامي الشوا : ثورة المعلومات وانعكاساتها علي قانون العقوبات ، دار النهضة العربية ، ٢٠٠٣ ، القاهرة .
- نهلا عبدالقادر المومني ، الجرائم المعلوماتية ، دار الثقافة ، الطبعة الثانية ، عام ٢٠١٠ م.
- د/ أسامة عبدالله قايد ، الحماية الجنائية للحياة الخاصة وبنوك المعلومات دراسة مقارنة في القانون الفرنسي والأمريكي والمصري وفقًا لآخر التعديلات التشريعية ، دار النهضة العربية ،بدون رقم طبعة ، القاهرة ، عام ٢٠١٥ م .
- د/ مدحت رمضان ، جرائم الاعتداء على الأشخاص والإنترنت دار النهضة العربية ، بدون رقم طبعة ، القاهرة ، عام ٢٠٠٠ .
- د / رامي متولي القاضي ، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية ، دار النهضة العربية ، الطبعة الأولي ، عام ٢٠١١ م .
- د / محمد حسام محمود لطفي ، حقوق الملكية الفكرية المفاهيم الأساسية – دراسة لأحكام القانون رقم ٨٢ لسنة ٢٠٠٢ في ضوء أراء الفقه وأحكام القضاء المقارن –، دار النهضة العربية ، الطبعة الثانية ، القاهرة ، عام ٢٠١٢ م .
- د / هشام محمد فريد رستم ، قانون العقوبات و مخاطر تقنية المعلومات ، مكتبة الألات الحديثة ، عام ١٩٩٤ ،بدون رقم طبعة القاهرة .
- د / أحمد خليفة الملط ، الجرائم المعلوماتية ،دراسة مقارنة، دار الفكر الجامعي بالاسكندرية ، الطبعة الثانية ، عام ٢٠٠٦ م.
- د / أحمد حسام طه تمام ، الجرائم الناشئة عن استخدام الحاسب الألي دار النهضة العربية ، القاهرة ، عام ٢٠٠٠ .
- د / عمرو إبراهيم الوقاد ، الحماية الجنائية للمعلوماتية ، القاهرة ، بدون رقم طبعة ، عام ١٩٩٩ .

- د / نائلة عادل محمد قورة ، جرائم الحاسب الألي الاقتصادية ،دراسة نظرية وتطبيقية ، دار نشر الحلبي ، عام ٢٠٠٥ ، الطبعة الأولى .

- د / حاتم عبدالرحمن منصور الشحات ، الإجرام المعلوماتي ، الطبعة الأولي ،عام ٢٠٠٢ ، دارالنهضة العربية ، القاهرة .

- الدكتور المستشار / عبدالفتاح بيومي حجازي ، الجريمة في عصر العولمة الطبعة الأولى ، دار النهضة العربية ، القاهرة ، عام ٢٠١٠.

- د./ سعيد عبداللطيف ، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت ، دار النهضة العربية ، عام ١٩٩١ ، الطبعة الأولى .

- اللواء الدكتور / أشرف السعيد أحمد ، تكنولوجيا المعلومات في المجال الأمني ، مطابع الشرطة للطباعة والنشر والتوزيع ، الطبعة الثانية ، عام ٢٠١٥.

- د/ أحمد محمد رفعت ، الإرهاب الدولي، دار النهضة العربية ، عام ٢٠٠٦ .

- د/ خالد سامي السيد ، الأمن القومي الإلكتروني وجرائم المعلومات دار النهضة العربية ، الطبعة الأولى ، عام ٢٠٢١.

- د. هلالي عبداللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقاً عليها ، دار النهضة العربية ، القاهرة ، الطبعة الثامنة ، عام ٢٠١١.

ثانياً : رسائل الدكتوراه :

- د/ حسين بن سعيد بن سيف الغافري ، السياسة الجنائية في مواجهة جرائم الإنترنت "دراسة مقارنة "، رسالة قدمت لنيلِ درجة الدكتوراه في القانون من جامعة عين شمس ، عام ٢٠٠٧ .

- د/ عبدالحليم بركات أحمد غزال ، الحماية الجنائية الموضوعية لتعاملات الشبكة الدولية للمعلومات ، رسالة قدمت لنيل درجة الدكتوراه في القانون ، جامعة المنصورة ، عام ٢٠١٤ .

- د/ أيمن عبدالله فكري ، جرائم نظم المعلومات – دراسة مقارنة – ، رسالة قُدِّمَت لنيل درجة الدكتوراه في القانون من جامعة المنصورة ،عام ٢٠٠٦ .

- د/ علي عواد شحاته ، نحو نظرية عامة لمكافحة جرائم الحاسب الآلي ، رسالة قدمت لنيل درجة الدكتوراه في الحقوق من جامعة القاهرة ، عام ٢٠١٧ .

- د/ محمد حسين موسي عبدالناصر ، المواجهة الجنائية لجرائم الاعتداء علي حقوق الملكية الأدبية والفنية عبر الانترنت ، رسالة قدمت لنيل درجة الدكتوراه في الحقوق من جامعة أسيوط ، عام ٢٠١٦.

- د/ عبدالرحمن بجاد شارع العتيبي ، دور الأمن السيبراني في تحقيق رؤية ٢٠٣٠ ، رسالة قدمت لنيل درجة الدكتوراه في الفلسفة في الدراسات الاستراتيجية ، جامعة نايف للعلوم الأمنية ، كلية العلوم الإستراتيجية قسم الدراسات الاستراتيجية ، السعودية، عام ٢٠٢٠ .

- د/ حمام عبداللطيف عبدالشافي حنفي معوض ، الحماية الجنائية للبرامج والبيانات المعالجة إلكترونيًا ، دراسة مقارنة ، رسالة قدمت لنيل درجة الدكتوراه حقوق القاهرة ، عام ٢٠١٧ .

- د/ علاء عبدالحفيظ محمد عبدالجواد ، العلاقة بين الأمن القومي والدبقراطية . رسالة قدمت لنيل درجة دكتوراه الفلسفة في العلوم السياسية ، كلية الاقتصاد والعلوم السياسية ، القاهرة ، ٢٠٠٩.

- د/ عذاري سعود عبدالمحسن ، الضبط والتفتيش في حرائم الحاسب الالي ، رسالة قدمت لنيل درجة الدكتوراه في الحقوق ، قسم القانون الجنائي ، جامعة القاهرة ، عام ٢٠١٦.

ثالثاً : رسائل الماجستير :

- محمد أمين أحمد الشوابكة ، الجرائم المرتكبة عبر الإنترنت ، رسالة قدمت لنيل درجة الماجستير في القانون إلي معهد البحوث العربية للتربية والثقافة والعلوم ، جامعة الدول العربية ، القاهرة ، عام ٢٠٠٢ .

- عبدالرحمن بجاد شارع العتيبي ، دور الأمن السيبراني في تعزيز الأمن السيبراني ، رسالة قدمت لنيل درجة الماجستير في العلوم الإستراتيجية ، جامعة نايف للعوم الأمنية ، كلية العلوم الإستراتيجية قسم الأمن الإنساني ، السعودية ، عام ٢٠١٧ .

- عبدالله يحي سعيد الزهراني ، استراتيجيات الأمن السيبراني في ضوء التقنيات والتحديات الحديثة ،دراسة مقارنة ، رسالة قدمت لنيل درجة الماجستير في العلوم الإستراتيجية ، جامعة نايف للعوم الأمنية ، كلية العلوم الإستراتيجية قسم الدراسات الاستراتيجية ، السعودية ، عام ٢٠٢٠.

- جزار منصورية – الجريمة المعلوماتية ، رسالة للحصول على شهادة الماجستير في الحقوق والعلوم السياسية ، جامعة عبدالحميد بن باديس ، الجزائير ، عام ٢٠١٦ / ٢٠١٧ ، ص ٧ .

رابعاً : الأبحاث العلمية والتقارير والنشرات :

- أحمد وهدان ،الانعكاسات الأمنية للعولمة دراسة في أثر العولمة على الجريمة المنظمة ، المجلة الجنائية القومية ، المجلد الرابع والأربعون ، العددان الأول والثانى ، مارس / يوليو ، عام ٢٠٠١ م .

- تقرير اللجنة الاقتصادية والأجتماعية لغربي أسيا (الإسكوا) ، التابع للأمم المتحدة ، بعنوان ورشة عمل حول تحفيز الأمان في الفضاء السيبراني في المنظقة العربية ، مسقط ٨-٩ كانون الأول / ديسمبر عام ٢٠١٤ .

- نشرة تكنولوجيا المعلومات والاتصالات للتنمية في المنظقة العربية ،الإسكوا التابعة للأمم المتحدة ، العدد ١٨ ، عام ٢٠١٢ .

- تقرير الاتحاد الدولي للاتصالات لقياس مجتمع المعلومات خلال الندوة العالمية السادسة عشرة لمؤشرات الاتصالات وتكنولوجيا المعلومات (WTIS) ، في الفترة من ١٠ إلي ١٢ ديسمبر عام ٢٠١٨ م، جنيف ، سويسرا ، ص٢ ، ومنشور بموقع الاتحاد الدولي للاتصالات https://itu.int في ٢٠/ ٢/ ٢٠١٩ .

- تقرير صادر عن الاتحاد الدولي للاتصالات ، التابع للأمم المتحدة ، عام ٢٠١٠ .
- عبدالرحمن عاطف أبوزيد ، بحث في الأمن السيبراني في الوطن العربي ، دراسة حالة المملكة العربية السعودية ، المركز العربي للبحوث والدراسات ، العدد ٤٨ ، عام ٢٠١٩ ،
- أ . د / هدى حامد قشقوش ، بحث الجرائم المعلوماتية ، منشور بمركز بحوث الشرطة بإكاديمية مبارك للأمن ، العدد العشرون – يوليو ٢٠٠١ة- ربيع ثان ١٤٢٢ .
- منى الأشقر جبور ، بحث بعنوان : الأمن السيبراني: التحديات ومستلزمات المواجهة ، اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني بيروت ٢٧ – ٢٨ أغسطس (آب) ٢٠١٢ ، المركز العربي للبحوث القانونية والقضائية / جامعة الدول العربي .
- النشرة الربعية للأمن السيبراني الصادرة عن مركز الدرسات الاستراتيجية التابعة للهيئة الوطنية للأمن السيبراني ،المملكة العربية السعودية الربع الأول ، عام ٢٠٢٠ .
- د/ حازم حسن أحمد الجمل ، بحث في الحماية الجنائية للأمن السيبراني في ضوء رؤية المملكة ٢٠٣٠ ، مجلة البحوث الأمنية ، جامعة الملك فهد الأمنية ، مركز البحوث والدراسات ، مجلد ٣٠ ، عدد ٧٧ ، شهر أغسطس ، عام ٢٠٢٠ .
- دراسة شاملة عن الجريمة المنظمة ، صادرة عن مكتب الأمم المتحدة المعني بالمخدرات والجريمة ، في فبراير ، عام ٢٠١٣ .
- د/ حصة الجابر ، وزيرة الاتصالات وتكنولوجيا المعلومات القطرية ، الكلمة الافتتاحية لاستراتيجية الحكومة الإلكترونية لدولة قطر ، الملخص التنفيذي ، عام ٢٠٢٠ ، الصادرة عن وزارة الاتصالات وتكنولوجيا المعلومات بدولة قطر .
- دراسة مكتب الأمم المتحدة المعني بالمخدرات والجريمة ، فيينا ، بموضوع تشريعات مكافحة الإرهاب في دول الخليج العربية واليمن ، عام ٢٠٠٩ .
- استخدام الإنترنت في أغراض إرهابية ، مكتب الأمم المتحدة المعني بالمخدرات والجريمة بلتعاون مع فرقة العمل التابعة للأمم المتحدة المعنية بتنفيذ تدابير مكافحة الإرهاب ، نيويورك .

- تقرير الأمم المتحدة رقم A/74/130 ، بتاريخ ٢٠١٨/ ٧/ ٣٠ .
- د. إيمان بنت محمد علي عادل عزام ، بحث محكم بعنوان : العقوبة في نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية ، دراسة تأصيلية مقارنة ، مجلة العدل ، مجلة فصلية علمية محكمة ، العدد ٨٢ ، شهر رجب ١٤٣٩ هـ .
- ورقة معلومات أساسية بعنوان جمع وتبادل الأدلة الإثباتية الإلكترونية ، الأمم المتحدة ، مؤتمر الأطراف لمكافحة الجريمة المنظمة عبر الوطنية .

خامساً : الجرائد الرسمية :

- الجريدة الرسمية بالكويت (الكويت اليوم) ، العدد ١٢٤٤ ، في ١٢ يوليو عام ٢٠١٥ .
- الجريدة الرسمية بالإمارات ، العدد رقم ٤٤٢ ، المنشور في ٣١/ ١/ ٢٠٠٦ .
- الجريدة الرسمية بالإمارات العدد ٥٤٠ ، بتاريخ ٢٦/ ٨/ ٢٠١٢ .
- الجريدة الرسمية بالإمارات ، ملحق العدد ٥٩٧ ، منشور بتاريخ ٢٣/ ٥/ ٢٠١٦
- الجريدة الرسمية بالإمارات، ملحق العدد ٥٩٧ ، منشور بتاريخ ٢٣/ ٥/ ٢٠١٦
- الجريدة الرسمية بالإمارات، العدد ٣٩٣ ، السنة ٤٩ ، منشور بتاريخ ٢٧ ديسمبر عام ٢٠١٥
- الجريدة الرسمية بسلطنة عمان ، العدد ٩٢٩ ، المرسوم السلطاني رقم ١٢ لسنة ٢٠١١ .
- الجريدة الرسمية بالبحرين ، العدد ٣١٧٨ ، ٩/ ١٠/ ٢٠١٤ .
- الجريدة الرسمية بالبحرين ، العدد ٣٣٧٥ ، في ١٩ يوليو من عام ٢٠١٨.
- الجريدة الرسمية بالبحرين ، العدد ٣٣٩٥ ، في ٢٩ نوفمبر ٢٠١٨ .
- الجريدة الرسمية بالبحرين ، العدد ٣٤٨١ ، في ٢٣ يوليو عام ٢٠٢٠ .

سادساً / المواقع الإلكترونية :

- موقع الاسكوا التابع للأمم المتحدة (https://www.unescwa.org) .
- موقع باللغة العربية ، https://www.bahrainedb.com/ .
- صحيفة الشرق الأوسط الإلكترونية (https://aawsat.com)

- موقع باللغة الإنجليزية ، https://www.fbi.gov/ .
- موقع ال BBC بالعربي ، WWW.BBC.COM .
- موقع : https://political-encyclopedia.org/ .
- مقال بموقع https://www.independentarabia.com/ .
- موقع https://www.a7la-home.com/ ، مقال منشور عام ٢٠٢٠ .
- موقع https://www.jigsawacademy.com/ .
- موقع باللغة الإنجليزية ، المرجع السابق ، https://www.jigsawacademy.com/
- موقع باللغة الإنجليزية ، https://www.teceze.com/cybersecurity-challenges-in-2020-and-how-to-tackle-them/ .
- موقع الإنتربول الرسمي ، https://www.interpol.int/ar/4/6 .
- الموقع الرسمي لشركة أرامكو ، https://www.aramco.com/ar/news-media/news/2020/sa-calls-for-boosting-the-vital-role-of-cybersecurity
- موقع : http://www.acrseg.org/41483 .
- الموقع الرسمي للهيئة العامة للاتصالات وتقنية المعلومات (citra):
https://citra.gov.kw/sites/ar/Pages/Sectors/CompetenciesInformationTechnologySector.aspx .
- الموقع الرسمي للهيئة العامة للاتصالات وتقنية المعلومات :
https://citra.gov.kw/sites/ar/LegalReferences/Cyber%20Security.pdf
- البوابة الرسمية لحكومة دولة الإمارات ، https://u.ae/ar-ae/resources/laws .
- الموقع الرسمي لهيئة تنظيم الإتصالات (tra) بالإمارت،
https://www.tra.gov.ae/ar/media-hub/press-releases/2019/6/24/tra-launches-the-uae-national-cybersecurity-strategy.aspx .

- الموقع الرسمي لهيئة الاتصالات وتقنية المعلومات السعودية : ،

- https://www.citc.gov.sa/ar/RulesandSystems/CyberSecurity/Documents/CRF-ar.pdf .

- الموقع الرسمي للخدمات الحكومية العمانية ،

https://omanuna.oman.om / .

- الموقع الرسمي للمركز الوطني للسلامة الوطنية :

https://www.cert.gov.om/media_news_details_arabic.aspx?news=103 .

- الموقع الرسمي لمنتدي الخليج العربي ،

https://gulfif.org/the-new-battlefront-cyber-security-across-the-gcc / .

- الموقع الرسمي لاتفاقية بودابست المتعلقة بمكافحة الجرائم السيبرانية ،

https://www.coe.int / .

سابعاً : المراجع الأجنبية :

- Bhagwati ،Jagdihln. Defence of Globalization. New Yourk: Oxford University Press٢٠٠٤ ،
- DAVID (E . LEARNER .) ،ELECTRONIC CRIME SCENE INVESTIGATION ،PUBLISHED IN NOVA SCIENCE ،LNC ، NEW YORK ٢٠٠٩ ،.
- Janet (ABBATE.) , INVENTING THE INTERNET , PUBLISHED BY THE MIT PRESS CAMBRIDGE ،LONDON ١٩٩٩ ، .
- DR. JACQUES) VALLEE. (،THE HEART OF THE INTERNET : AN INSIDER,S VIEW OF THE ON-LINE REVOLUTION ، PUBLISHED BY HAMPTON ROADS ٢٠٠٣ ، .
- DAVID (E . LEARNER .) ،ELECTRONIC CRIME SCENE INVESTIGATION ،PUBLISHED BY NOVA SCIENCE ،LNC ، NEW YORK ٢٠٠٩ ، .
- yaman (akdeniz) , internet child pornography and the law : national and international responses , published by ashgate . uk . 2008 .

- Babak Akhgar , Andrew Staniforth, Francesca Bosco , Cyber Crime and Cyber Terrorism Investigator's HandbooK , BY : ELSEVIER , USE ,2014 .
- K. K. Panigrahi , Information Security and Cyber Law , published by tutorials point ,2015 .
- Ramjee Prasad • Vandana Rohokale , Cyber Security: The Lifeline of Information and Communication Technology , 2019 , india , publisded by springer
- Andrew W. M'manga , Designing for Cyber Security Risk-based Decision Making , A dissertation submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy , Department of Computing and Informatics Bournemouth University January 2020 .
- Justin King-Lacroix , Securing the Internet of Things: decentralised security for wireless networks of embedded systems , A thesis submitted for the degree of Doctor of Philosophy , University of Oxford , 2016 .
- Tim Weil ,San Murugesan , IT وRisk and Resilience— Cybersecurity Response to COVID-19 , journal , it Professional ,Published by the IEEE Computer Society, may2020 .
- DENNING ,DOROTHY, E., (Aug 2000)" Cyber terrorism" , Global Dialogue .
- Mehmet Emin Erendor , AN ANALYSIS OF THREAT PERCEPTIONS: COMBATING CYBER TERRORISM: THE POLICIES OF NATO AND TURKEY, EVALUATED USING GAME THEORY IN THE CONTEXT OF INTERNATIONAL LAW , Thesis for the Degree of Doctor of Philosophy , UNIVERSITY OF SOUTHAMPTON FACULTY OF BUSINESS AND LAW , January 2017 .
- Herbert Lin and Amy Zegart , Bytes, Bombs, and Spies The Strategic Dimensions of Offensive Cyber Operations , Publisher : Brookings Institution Press , Washington , 2019 .

فهـــــرس الموضوعـــــات