المخاطر السبيرانية وأمن الشبكات الإلكترونية
التحديات و المواجهة
Cyber Risks and Network Security
Challenges and Responses

الدكتور: بوعبسة محمد- أستاذ مساعد قسم ب – كلية الحقوق – جامعة عين تموشنت
الايمايل: mohamed.bouabca@univ-temouchent.edu.dz

الدكتور:بن صابر بلقاسم- مخبر حقوق الإنسان و الحريات العامة- كلية الحقوق و العلوم السياسية جامعة عبد الحميد بن باديس- مستغانم
الايمايل: belkacembensaber@gmail.com

الملخص

أصبحت المجتمعات الحديثة مجتمعات رقمية تعتمد على تكنولوجيا الاتصال والمعلومات المرتبطة بالشبكة العنكبوتية العالمية، إلا أن هذا الاعتماد صاحبه جملة من المخاطر الناجمة والمحتملة التي تهدد وبشكل أساسي الشبكة وأمن المعلومات، إذ أضحت الشبكات الإلكترونية بفعل سوء الاستغلال هدفا لأغراض إجرامية توثر سلبا على سلامة البنية التحتية للمعلومات الحساسة؛ لاسيما المعلومات الشخصية للمواطنين و الحكومية التي تمس أمن الدول.

لذلك بات الأمن السبيراني يشكل أولويـة؛ وجزءًا لا يتجزأ من أي سياسة أمنية وطنية لمواجهة المخاطر والتهديدات التي يتوجب على الدول التصدي لها في الحقبة الراهنة.

Summary

Modern societies have become digital societies that rely on communication and information technology linked to the World Wide Web. However, this reliance has been accompanied by a number of emerging and potential risks that mainly threaten the network and information security, as electronic networks have become the target of misuse for criminal purposes that negatively affect the integrity of sensitive information infrastructure, especially the personal information of citizens and governmental information that affects the security of states.

Therefore, cybersecurity has become a priority and an integral part of any national security policy to confront the risks and threats that countries must address in the current era.

مقدمـــة:

يعتبر الأمن السيبراني (**cyber security**) من الأولويات الملحة في ظل التحديات والمتغيرات التي تواجهها دول العالم في العصر الرقمي الحالي، ويذهب المهتمين بهذا الشأن أنه ثمة قلق كبير من تنامي الهجمات الإلكترونية، وفي سياق ذلك يشير التقرير العالمي للمخاطِر GRR 2016 " أن هذه المخاطر أصبحت ملموسة وعلى نحو متزايد،وهي بحاجة لمعالجتها ومواجهتها من خلال التعاون العميق بين الدول".[1]

وعليه، فالإشكال الذي يمكن طرحه من خلال هذه الورقة هو كالأتي:

ما مفهوم الأمن السيبراني وما هو الدور الذي يلعبه في حماية أمن أنظمة المعلومات والاتصالات أمام تصاعد مخاطره وتنامي تهديداته؟ وبعبارة أخرى؛ماذا بإمكان مجتمع تقنيات المعلومات القيام به لمواجهة التهديدات والمخاطر السيبرانية التي تعوق تطوير مجتمع رقمي فعال؟

للإجابة على هذه الإشكالية قسمت الدراسة إلى محورين رئيسيين، **المحور الأول** تطرقت فيه إلى أساسيات الأمن السيبراني: المفهوم والأبعاد، أما **المحور الثاني** خصصته للمخاطروالتهديدات التي تحيق بالبيئة السيبرانية وطرق مواجهتها، وفي الخاتمة عرضت النتائج والتوصيات.

المحور الأول: أساسيات الأمن السيبراني :المفهوم و الأبعاد

أولا: مفهوم الأمن السيبراني

1- تعريف الأمن السيبراني:

كلمة **"أمن سيبراني"** هي تعريب لكلمة (**Cyber Security**) فكلمة **Cyber** هي بادئة مرتبطة في الأساس بأجهزة الكومبيوتر والمحمول، أي بتكنولوجيات المعلومات والاتصالات.[2]

ويعني المصطلح عند خبراء الأمن المعلوماتي: الحماية من اختراق شبكات المعلومات، وبالذات تلك التي تحتوي معلومات سرية، والحماية من هجمات التعطيل والهجمات الإلكترونية لِلْهَاكَرْز، ومن الجريمة الإلكترونية، ومن تهديدات فيروسات "سوفت وير" وكذلك الحماية من ترددات المكالمات.

ويعرف التقرير الصادر عن الإتحاد الدولي للاتصالات حول **"اتجاهات الإصلاح في الاتصالات للعام 2010-2011"** الأمن السيبراني بأنه:(مجموع الأدوات والسياسات ومفاهيم وضوابط الأمن والمبادئ التوجيهية لإدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وآليات الضمان والتكنولوجيات التي يمكن استخدامها في حماية البيئة المعلوماتية وأصول المؤسسات والمستعملين.

وتشمل أصول المؤسسات والمستعملين أجهزة الحوسبة المرتبطة بالشبكة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات ومجموع المعلومات والمنقولة و/ أو المحفوظة في البيئة السيبرانية).[3]

من خلال هذا التعريف، يتبين أن مجال الأمن السيبراني يتعلق بإجراءات ومقاييس ومعايير الحماية التي يتعين اتخاذها لمواجهة المخاطر والتهديدات ومنع الاعتداءات على أمن الشبكات والأنظمة المعلوماتية والمعلومات والأجهزة المتصلة بالانترنت.

فالخطر يتناول أمن الشبكات وأمن الانترنت من زاويتين: الأولى،تتعلق بالبنية التحتية وما تتضمنه من نقاط دخول وخروج وتخزين واعتراض للمعلومات، والثانية، تتعلق بعمليات التخريب والتدمير والتعطيل الذي يطالها ويطال الأموال والأشخاص.[4]

وبناء عليه، فإن الأمن السيبراني (أمن تكنولوجيا المعلومات وأمن الاتصالات) يمس أمن الثروة الرقمية والثقافية لأفراد والمنظمات والدول[5] .

2-العناصر الأساسية للأمن السيبراني:

يقوم الأمن السيبراني على جملة من العناصر التي تسهم في الوفاء بمعايير الأمن الأساسية، ويمكن إيجازها كما يلي:

أ-التوافر (Availability): ونعني به ضمان بقاء المعلومات وامتلاك القدرة على الوصول إليها وإمكانية استخدامها بصورتها الحالية.

وأهم الأخطار التي تهدد توافر المعلومات تتمثل في رفض الخدمة الناجم عن تعطيل خدمات نظم الحاسب و شبكاته بصورة تحول دون الوصول إلى المعلومات، فقدان القدرة على معالجة البيانات وتخريبها أو اختلاطها بمعلومات أخرى على نحو يؤدي إلى تلوثها، أوإطالة استخدامها أوسوء تفسيرها أو قلبها.[6]

ب-الصحة والسلامة: ونعني به ضمان عدم تعرض المعلومات للتعديل أثناء تخزينها أو نقلها ووقايتها من التلاعب والتدمير والإتلاف، ويمكن توفير حماية سلامة المعلومات واستقامة البيانات بواسطة آليات أمن مثل: مراقبة صارمة على النفاذ، تشفير البيانات[7]، الحماية من الفيروسات[8] والديدان[9] والبرامج الخبيثة.[10]

ج - السرية (Confidentiality): ونعني بها الحفاظ والتكتم على سرية المعلومات وتدفقات المعلومات والخدمات أو الإجراءات التي تجري في الفضاء السبيراني، وهي تضمن حماية الموارد من الإفشاء غير المرخص به، ويمكن تنفيذ السرية عن طريق مراقبة النفاذ والتشفير.

ثانيا: أبعاد الأمن السيبراني

يرتبط الأمن السيبراني ارتباطا وثيقا بسلامة مصادر الثروة الرقمية في العصر الحالي، والتي نعني بها البيانات، والمعلومات، والقدرة على الاتصال والتواصل، وهو بذلك يتعدى في أبعاده مختلف المجالات الاجتماعية والاقتصادية والسياسية والعسكرية والقانونية.

1- البعد الاجتماعي:

لاشك أن ما تقدمه الانترنت من إمكانات و قدرات في مختلف المجالات العلمية والاقتصادية و الثقافية والخدماتية دوراً كبيراً في أن يعبر المواطن عن تطلعاته، فضلا عما توفر له من اطمئنان في حياته اليومية[11]، والاستفادة من تقنيات المعلومات والاتصال، بل يتعدى ذلك إلى ترسيخ القيم الجوهرية في المجتمع كقيم الانتماء والمعتقدات والعادات والتقاليد عبر المدونات والشبكات الاجتماعية بشكل خاص التي تهتم بنشر الوعي في هذه المسائل. لكن المخاطر السيبرية تطال المجتمع ككل، فالمحتويات غير المشروعة أو غير المرغوب فيها تمثل تهديداً له، كالمواد الإباحية والدعارة، ونشر الفكر المتطرف، وتجنيد الشباب في القضايا التي تمس أمن الدول والمجتمع الدولي[12]، بالإضافة إلى ذلك جعل المواطنين أكثر انكشافا على الثقافات الأخرى، ومن ثم تُعَرَض القوميات والهويات لعمليات اختـراق خارجي تؤثر على الأفكار والتوجهات، مما يجعلها سبباً في تهديد السلم

الاجتماعي[13]، لذلك ينبغي التعامل بحذر وذكاء مع البيئة السيبرانية عن طريق ثقافة أمنية تغرس داخل ثقافة تكنولوجيات المعلومات لتحقيق الأمن السيبراني في بعده الاجتماعي.[14]

2- البعد الاقتصادي:

أصبحت التكنولوجيا الرقمية تستخدم في تحريك اقتصاديات الدول من خلال جعل المعاملات المالية وشبكات البنوك والبورصات العالمية وشركات الأسواق المالية محوسبة بنظم وشبكات إلكترونية، الأمر الذي أدى إلى الأخذ بأهمية الأمن السيبراني في مجال الاقتصاد الرقمي أو ما يصطلح عليه "بعالم المال الإلكتروني" الذي تتنافس فيه الشركات على إصدار تطبيقات تسمح بآليات دفع آمنة و حفظ المال في

المحفظة الإلكترونية، لكن ذلك أوجد صعوبات للحد من بعض الجرائم الاقتصادية و المالية الخطيرة العابرة للحدود كجرائم تبييض الأموال التي تمثل تهديداً لنمو الاقتصاد الرقمي ما لم تقم الدول بإرساء معايير الأمن السيبراني و تطويرها للتقليل من هذه الجرائم.

3- البعد السياسي:

هناك عدة اعتبارات تدفع الاهتمام بالأمن السيبراني في بعده السياسي، لعل أهمها هو حق الدول في حماية كيانها ونظامها السياسي، في وقت تؤثر التقنيات التكنولوجية في موازين القوى داخل المجتمع، بحيث أصبح المواطن فاعل سياسي في اللعبة السياسية من خلال تنظيم حملات انتخابية أو شن تظاهرات افتراضية أو حركات احتجاجية إلكترونية،[15]وفي المقابل لا يتوانى السياسيون الاستفادة مما تقدمه هذه التقنيات كشبكات التواصل الاجتماعي في الوصول إلى أكبر شريحة ممكنة من المواطنين و الترويج لبرامجهم السياسية.[16]

لكن في المقابل،نجد أن الحركات الإرهابية تستغل المواقع الإلكترونية لتحقيق أهدافها في تجنيد أفرادها، مما جعل الدول تعمل على حماية أمنها الداخلي، فضلا عن التسريبات الحساسة للوثائق الدبلوماسية السرية عبر موقع وكيليكس التي سببت مشكلات في العلاقات بين الدول، مما حتم على هذه الأخيرة أن تراجع سياستها الخارجية في ظل هذه التسريبات.[17]

4-البعد القانوني:

إنّ تدابير الأمن المتخذة من جانب الدول تميل إلى توفير حماية البيئة الرقمية،لكنها تظل عاجزة عن منع النشاط الإجرامي عبر الانترنت، ولعل ذلك مرّده إلى طبيعة الجريمة الإلكترونية ذاتها وصعوبة تحديد هوية مرتكبيها، ومرونة التعريفات المرتبطة بتكنولوجيات المعلومات، الأمر الذي يجعل النظام القانوني التقليدي لمكافحتها غير فعال في سياق الانترنت.

إنّ معاييرالأمن السيبراني تلزم وضع إطار قانوني مصمم يناسب استخدام التكنولوجيا الجديدة، وتحليل القرائن و التعرف على مقترفي الأعمال الإجرامية[18] والممارسات غير القانونية في الفضاء السيبراني، وهذا يستدعي بالضرورة إعداد البنية التنظيمية والتشريعية وبناء قدرات هيئات المكافحة والحكم.[19]

5-البعد العسكري:

تطور مفهوم الأمن القومي اتجاه التهديدات الجديدة التي فرضتها البيئة السيبرانية، وتغيرت الحروب التقليدية و أصبحت الجيوش العسكرية في كافة دول العالم تهتم بحرب المعلومات التي يتوقع حدوثها في الفضاء الإلكتروني، وظهرت مناورات للتدريب على هذا النوع الجديد الذي أصطلح عليه "بالحرب السيبرانية"[20] وكيف يمكن مواجهته والاستعداد له،[21]

فإن لم تكن الشبكة الإلكترونية المستخدمة مؤمنة بشكل جيد من أي اختراق خارجي، فقد يتسبب ذلك في شن هجمات إلكترونية مضادة على شبكات القوات المسلحة وأجهزة الاستخبارات،[22] ومن تم تدمير قواعد البيانات العسكرية، أوقطع أنظمة الاتصال بين الوحدات العسكرية وتعطيل شبكات الكومبيوتر، وقد يتم شل أنظمة الدفاع الجوي أو التوجيه الإلكتروني للعدو، وفقدان السيطرة على وحدات القيادة والتحكم أوالاتصال بالأقمار الصناعية.[23]

المحور الثاني: مخاطر الأمن السيبراني و مواجهتها

يجمع الخبراء المختصون أن مخاطر تكنولوجيا المعلومات والاتصالات آخذة في الازدياد، بحيث أن الظاهرة باتت جد مقلقة بفعل الاختراقات والاعتداءات "مجهولة الهوية"، ناهيك عن الممارسات والأعمال الإجرامية التي تقع على شبكة الإنترنت،[24] لذلك كان لزاما على الدول أن ترفع من حالة

التأهب والتصدي بشكل مستمر لمواجهة طبيعة هذه الأخطار والتهديدات والتعقيدات التي أفرزها الفضاء السيبراني العالمي.

من هذا المنطلق،سنخصص المحور الثاني من هذه الورقة تصنيف المخاطر السيبرانية، تم اقتراح بعض الحلول لمواجهتها والتقليل من حجم خسائرها.

أولا: تصنيف المخاطر السيبرانية

يمكن تصنيف المخاطر التي تهدد الأمن السيبراني إلى ثلاثة أقسام رئيسية و هي:

1-المخاطر التي تستهدف خرق الحماية المادية للمعلومات و الاتصالات:

يقصد بها الأنشطة التي تستهدف المعلومات والبرمجيات وتتمثل في:

أ-إتلاف المعلومات أو تعديلها: حيث يلجأ المهاجم إلى اختراق النظام المعلوماتي للحاسوب عن طريق القيام بعملية التلاعب بالمعلومات متعمدا تشويهها، فالمعلومات تظل موجودة من دون تدمير، لكنها تكون مضللة، أو يلجأ إلى إتلافها أو محوها، وهذا بمسح كلي أو جزئي للملفات المخزنة بالحاسوب.

وهذا التهديد هو الأسهل بالنسبة للمخترقين الذين يطلق عليهم باسم القراصنة أو الهاكرز[25]، لأنه لا يعتمد على بيانات سرية أو معلومات حول المستخدمين[26] .

ب-هجمات البرمجيات: تشمل التصيّد[27] والسرقة واختلاس المعلومة، والتعرض لسرية الاتصالات التي تطال البريد الإلكتروني، ونقل الملفات، والدخول إلى الأنظمة للإطلاع على المعلومات دون إذن، واستخدام البرامج الخبيثة، كالفيروسات وأحصنة طروادة والدودة الإلكترونية والقنابل المنطقية،[28] والميكروبات فائقة الصغر والاختناق المروري الإلكتروني، ويجمع بين هذه الأنواع باعتبارها برمجيات ضارة تستخدم لتدمير الأصول والمعلومات و البيانات الموجودة على الشبكات وقواعد الشبكات، وإن كان بعضها يستخدم في الأغراض العسكرية.[29]

2-المخاطر المتعلقة بخرق الحماية للأشخاص و الحكومات:

تعتبر المخاطر التي تستهدف الأشخاص (الأفراد) و الحكومات من التهديدات الحرجة لدى جهات الأمن المعلوماتي.

أ-المخاطر التي تستهدف الأشخاص: ولها صور عديدة أبرزها: سرقة الهوية،انتحال صفة،الاعتداء على الخصوصية الابتزاز، الإزعاج والتحرش، التهديد،التحريض على الانتحار والقتل على الانترنت، السرقة،الغش،الخداع،الاتجار بالبشر،استغلال القاصرين للدعارة وإفسادهم بأنشطة جنسية عبر الوسائل الإلكترونية،والاعتداء على الملكية الفكرية.[30]

ب-المخاطر التي تستهدف الحكومات: تتمثل في عدد من الاعتداءات نذكر أهمها:

- التسلل إلى أنظمة البيانات الحكومية و اختراق الأجهزة و المواقع الإلكترونية الرسمية بهدف تعطيل الأعمال الحكومية، وتنفيذ القانون والعبث بالأدلة القضائيـــة والتأثير فيها، وبث البيانات من مصادر مجهولة وتهديد السلامة العامة.[31]
- الحرب السيبرانية من خـلال التجسس على الشبكـات لاختراق أمن وأسرار الدولـة

والحصول على معلومات حساسة في غاية السرية قد تشمل خططا عسكرية دفاعية أوهجومية، أومعلومات سياسية وإستخباراتية، ويحصل التجسس عن طريق الدخول للمواقع الحكومية و العسكرية المرتبطة بشبكات المعلومات دون أن يصاحب ذلك تدمير أوتخريب للبيانات والمعلومات.[32]

والأسلحة الأساسية في الحرب السيبرانية الفيروسات التي تؤدي إلى تعطيل عمل الشبكات الإلكترونية والخوادم الرئيسية **(servers)** كفيروس **(stuxnet)** الذي استطاعت وكالتا الاستخبارات الأمريكية والإسرائيلية تصميمه لاختراق و تعطيل المفاعل النووي الإيراني، وبالفعل كان الهجوم دقيقا إلى درجة

تحديد عدد أجهزة الطرد المركزي وتعطيلها بمهارة فائقة، حيث عمل على تغيير الضغط وجعل سرعة الدورات داخل الأجهزة متفاوتة مما أدى إلى انهيارها، ورأى الخبراء أن نجاح هذا الهجوم جعل العالم ينتقل إلى مرحلة توظيف الهجمات السيبرانية في تحقيق أضرار مادية متعمدة للحكومات والدول، ويفتح الباب أمام الكثير من التكهنات بأن مثل هذه الأسلحة المتطورة يمكن أن تصبح أمرا شائعاً في المستقبل.[33]

3-المخاطر المتعلقة بالإرهاب[34] الإلكتروني:

ظهر مصطلح"الإرهاب الإلكتروني" بظهور الفضاء السيبراني، ويمكن تعريفه بأنه: "الأعمال التي توظف فيها التقنيات الرقمية بغرض إرعاب الآخرين وبث الخوف فيهم"، كما يمكن تعريفه أيضا بأنه: (الاعتداءات التي توجه ضد أنظمة المعلومات بدوافع سياسية أو دينية)،[35] وهذا النوع من الإرهاب يتم ممارسته باستعمال التكنولوجيات الاتصال الرقمية الحديثة المتمثلة في الأجهزة الحاسوبية والمعلوماتية والقيام بأعمال التدمير والتلاعب والتعطيل وتغيير البيانات المتاحة على شبكة أو أنظمة المعلومات المتعلقة بإدارة مصالح الدولة الحيوية بنية إلحاق الأذى لأسباب ودوافع إيديولوجية أو سياسية أو اجتماعية أو دينية، ومن خصائصه مقارنة مع الإرهاب التقليدي، سرعة التنفيذ وعدم اعتماد عملياته على موارد بشرية مرتفعة التكلفة والعدد، ويمكن للفاعل أن ينفذ ما يريد عن بعد كالقيام بتحويل مالي أوسرقة معلومات حساسة أوتخريب. ويصنف الإرهاب الإلكتروني ضمن الجرائم الناعمة التي لا تتطلب استخدام الأدوات والعنف، فنقل البيانات أو سرقتها أو تدميرها لا يتطلب أي عنف أو مواجهة، ويوجه إلى كل منظمة أو مؤسسة في الدولة متصلة بالحاسوب الآلي سواء كانت عسكرية أومدينة بنية الإضرار بالمعلومات المتداولة والبرمجيات والاتصالات لتحقيق أهداف محددة أو لخدمة عمليات إرهابية كبرى.[36]

لقد سمحت ثورة الانترنت للجماعات الإرهابية بإخفاء عملياتها بطرق جديدة أكثر تعقيداً، فالوجود الإرهابي على الشبكة العالمية يستفيد من تقنيات الإخفاء و المجهولية، ومن خبرات السيبرانيين في تغيير عناوين الانترنت عبر ما يسمى بالانترنت المظلم،[37]حيث تنتشر أخطر أنواع الجرائم وهذا ما يساعد في ظهور مواقع إرهابية تؤدي مهمة محددة لمدة قصيرة، ثم تعود إلى الاختفاء، وهو ما صّعب القضاء عليها.[38]

ثانيا: مواجهة المخاطر السيبرانية

في الحقيقة لا يوجد حل فريد أو علاج شامل لقضايا الأمن السيبراني، على الرغم من زيادة الوعي بالتهديدات والمخاطر المحدقة،لكن عادة ما تتخذ التدابير و الإجراءات الأمنية بعد اختراق البيانات وتعطيل الأنظمة، لذلك يمكن استعراض بعض الحلول لمواجهة هذه المخاطر كما يلي:

1- **استخدام تقنيات الوقاية من الهجمات السيبرية:** وأهمها:

أ- استعمال ما يعرف ببرامج مكافحة الفيروسات **(Antivirus Programs)** بإصدارتها المتعددة، وينصح باستعمال برامج الحماية الجديدة التي تعرف بأدوات الإزالة، وهي تسمى بأسماء الفيروسات المنتشرة حاليا في الانترنت.

ب- استعمال أدوات التخزين الاحتياطي للبيانات والمعلومات، وذلك بتزويد جهاز الحاسوب بوحدات التخزين، ويتم ذلك في شكل أشرطة أو أقراص مضغوطة كما يوجد في برمجيات الاستعراض مثل خيارات خاصة للملفات و المجلدات التي تتطلب تخزينا احتياطيا لها.

ج- التأكد من سلامة الرسائل الإلكترونية والمرفقات والصور وغيرها عن طريق ما يعرف ببرامج التصفية **(Filters)**، وهي برامج خاصة بالبريد الإلكتروني تستخدم في تحديد خيارات المواقع والعناوين أفرادًا ومؤسسات ممن لا يرغب المستخدم في الاستقبال منهم لعدم ثقته فيهم.

د- توجد برامج وقاية هامة تقوم بصدّ محاولات الاختراق أو الهجوم مثل:جدران الحماية المعروفة باسم جدار النار **(Firewall)** التي تزود الشبكات بحماية جيدة عن طريق التأكد من شرعية كل شخص يود زيارة الشبكة المحمية، ومزودات بروكسي **(Proxy servers)** التي تحتفظ بصفحات الشبكة للويب على القرص الصلب[39]، والبرامج النشطة **(Activex)** ضمن المستعرض **(Internet Explorer)**، وأيضا برتوكولات معينة مثل:"أس أس تي" **(SST)**، و"أس أس أل" **(SSL)**، وينصح باستعمالها لضمان أكبر قدر ممكن من الأمن المعلوماتي.

هـ- إتباع الطرق السلمية عند استخدام الحاسوب، كالانتباه إلى الرسائل المشبوهة والمرفقات المغرية، والأسماء والعناوين الغريبة،والمنظمات غير الرسمية، مع ضرورة التعامل بتقنيات التشفير **(Ciphering)** بين المستخدمين.[40]

2- معالجة المسائل المتعلقة بحوكمة الانترنت:

يقصد بحوكمة الانترنت (إدارة الانترنت) تطوير وتطبيق الحكومات و القطـاع الخاص والمجتمع المدني، كل حسب دوره، للمبادئ والمعايير والقواعد المشتركة، وإجراءات اتخاذ القرارات ووضع البرامج التي تحدد شكل تطور الانترنت واستعمالها.[41]

وهناك شقين اثنين يتعلقان بحوكمة الانترنت: الشق التقني والشق القانوني، إلاّ أنهما يطرحان تحديات على المستوى العالمي، تبدأ بكيفية التنسيق بين الهيئات والحكومات المختلفة، لتصل إلى اعتماد مقاييس ومعايير تقنية موحدة، ونصوص تنظيمية وتشريعية تستجيب للمسائل القانونية المستجدة في الفضاء السيبراني نذكر منها: تحويل أسماء النطاقات إلى عناوين رقمية،[42]استثمار خدمات الاتصالات،المسؤولية عن الأعمال التجارية والأعمال غير الشرعية على الانترنت،مكافحة الجريمة،التجارة الإلكترونية،حماية مستخدمي الانترنت و حماية المستهلك...

ويعد الشق الأول هو الأهم في مسألة حوكمة الانترنت كونه الأساس الذي يقوم عليه الفضاء السيبراني وطريقة عمله، فضلا على أن هذا الشق يساهم في تقرير ما يمكن اعتماده من مناهج متابعة ومراقبة تقنية ضرورية في التنظيم القانوني،لاسيما من خلال وضع قواعد المراقبة و الملاحقة و التنفيذ سعيا إلى حماية أمن الانترنت وصولاً إلى حماية الفضاء السيبراني، وهذا يستلزم اللجوء إلى نظام إشراك أكبر عدد من الأطراف المعنية نظراً لاتساع نطاق مهمة تشغيل الانترنت و تأمين الموارد الأساسية لها من قدرات مادية ومؤهلات بشرية، وهي المقاربة الأجدى على مستوى إدارة وحوكمة الانترنت التي تختلف عن المقاربة التقليدية في مقاربة الأمن.[43]

لقد حددت القمة العالمية لمجتمع المعلومات و إدارة منتدى الانترنت المسائل التي لابد أن تدخل في صلب النقاش والمعالجة ذات الصلة بنظام الحكومة كالتالي:

- البنية التحتية، وإدارة الموارد الحرجة للانترنت.
-استخدام الانترنت،البريد غير المرغوب فيه، أمن الشبكات،الجريمة السيبرانية.
-المسائل القانونية التي يمكنها أن تؤثر على استخدام الانترنت مثل:الملكية الفكرية والتجارة الدولية.
- الجوانب المتعلقة بالتنمية و التطوير، كبناء القدرات في الدول النامية.[44]

3- تعقب ومتابعة الجرائم السيبرانية:

تمثل الجريمة السيبرانية تحديا كبيراً للأجهزة القانونية و القضائية في كل الدول المتقدمة والنامية، ذلك أن عملية التشريع تستغرق وقتا طويلا تحول دون مكافحتها بسرعة،فضلا على أن التعامل بالأدلة الرقمية يتطلب إجراءات محددة للحفاظ على سلامة المعلومات وتجنب تعديلها أو حذفها، أو التعدي على حقوق مستخدمي الانترنت الأبرياء،يضاف إلى ذلك صعوبة كشف الأجهزة و البرامج التي يستخدمها

المشتبه بهم، وكشف هوية مستخدمي الانترنت عن طريق تحليل الرسائل الإلكترونية واستعادة الملفات المحذوفة و تحديد الأدلة ذات الصلة بالجرائم و فك التشفير،[45]لذلك يجمع خبراء الأمن السيبراني على ضرورة وضع ومتابعة التحديث التشريعي الشامل للتعامل مع الجرائم السيبرانية وتقنين إجراءات الملاحقة و التحقيق و جمع الأدلة و المحاكمة و إقرار العقوبات الرادعة لمجرمي تقنيات المعلومات تتماشى مع طبيعة هذه الجرائم،[46]مع ضرورة تأهيل أجهزة الأمن ورجال الضبط والتحقيق الجنائي بالمعارف التقنية بتدريس الأساليب الفنية المستخدمة في ارتكاب الجريمة، وكيفية إثباتها ومعانيها والتحفظ عليها وفحصها تقنيا، والتعاون مع الخبراء المتخصصين في المعلوماتية، و إخضاع القضاة لدورات تدريبية مستمرة لمعالجة هذا النوع من القضايا التي تحتاج إلى خبرات عالية في قبول الأدلة الناشئة عنها و تقديرها، والفصل بجدارة في مثل هذه الجرائم المستحدثة التي تقع في الفضاء السيبراني.[47] فضلا عن تعزيز التعاون القضائي المشترك في مجال الملاحقة الدولية بإقرار مبدأ الاختصاص العالمي نظراً لطبيعة هذه الجرائم العابرة للأوطان، وتسليم المطلوبين وتبادل المساعدة القانونية والاعتراف بالأحكام الأجنبية، والتنسيق مع الهيئات الدولية ذات الصلة كمنظمة الشرطة الجنائية الدولية **(INTERPOL).**

4- إقرار نظام عالمي للمكافحة:

على الرغم من التدابير الوطنية التي تتخذ، تظل التهديدات والمخاطر مشكلة دولية، ومرد ذلك أن الأمن السيبراني عالمي وبعيد الأثر شأنه شأن الانترنت، فضلا عن التطور والتعقيد المستمرين لهذه التهديدات وجوانب الضعف في البرمجيات والنمو الهائل في الأجهزة المتنقلة والاتجاهات الجديدة مثل:الحوسبة السحابية،[48] فالتهديدات السيبرانية عالمية لذلك يجب أن تكون حلولها عالمية أيضا، و من الضروري جداً أن تتوصل جميع الدول إلى تفاهم مشترك بشأن الأمن السيبراني لتوفير الحماية من محاولات النفاذ غير المشروعة والتلاعب في موارد المعلومات المهمة و الحساسة و تدميرها،[49]ويظل إقرار نظام عالمي أفضل الطرق لمكافحة هذه التهديدات في شكل اتفاق دولي على معايير ومقاييس وقواعد قانونية تضمن سلامة الممتلكات و الأشخاص و المجتمعات واستقرار العلاقات بين الدول، وهذا يقتضي الاهتمام وتعزيز التنسيق والتعاون الدولي الذي يرعي جميع المسائل ذات الصلة بالمخاطر والتهديدات بما فيها الحرب السيبرانية، ونسجل هنا دور الأمم المتحدة التي تقود جهوداً عبر إقرارها تنظيم القمة العالمية لمجتمع المعلومات وإنشائها مجموعات عمل لمكافحة الجريمة السيبرانية، واتخاذها العديد من القرارات التي تدعم الأمن والسلامة في الفضاء السيبراني كالقرارين: الأول رقم 55/63 الصادر في 4 ديسمبر2000 والثاني رقم 56/12 الصادر في 2001/12/19 بشأن **"مكافحة استخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات"**، حيث يدعوان هذين القرارين الدول الأعضاء،عند وضع التشريعات الوطنية لمكافحة إساءة استخدام تكنولوجيا المعلومات، أن تأخذ بالاعتبار عمل لجنة منع الجريمة والعدالة الجنائية، وأيضا القرار رقم 57/239 المؤرخ في 2002/12/20 بشأن ثقافة عالمية للأمن السيبراني.

كما لا يخفى دور الإتحاد الدولي للاتصالات كمنبر إستراتيجي يضم 192 دولة و 700 شركة من القطاع الخاص و المؤسسات الأكاديمية، حيث يعمل على مساعدة الدول في الاتفاق على مبادئ مشتركة تفيد الحكومات و الصناعات التي تعتمد على تكنولوجيا المعلومات و البنية التحتية للاتصالات، فضلا عن وضعه مخطط لتعزيز إطار الأمن السيبراني العالمي.[50]

الخاتمـــة: من خلال هذه الدراسة نخلص إلى النتائج والتوصيات الآتية:

النتائـــج:

1- لم يعد الأمن السيبراني قضية يتولاها فنيون وتكنوقراط داخل المنشآت والمؤسسات كل على حدى بشكل مجزأ، بل أصبح من المسائل التي يتولاها سياسيون و إستراتيجيون و صناع قرار يترجمونه في سياسات وطنية تعمل ضمن إطار منظومة الأمن الوطني الشامل وتضبط العلاقة بين أمن المعلومات والأمن الوطني و توجهها الوجهة السليمة.

2- إن التصدي للمخاطر والتهديدات السيبرية المعقدة، يتطلب إرادة سياسية تضطلع بوضع وتنفيذ إستراتيجية لتنمية البنى الأساسية و الخدمات الرقمية قابلة للتنفيذ، بشكل فعال ومتماسك، فضلا عن ضرورة توفير مستوى كاف من أمن الشبكات والمعلومات والاتصالات بما في ذلك الموارد والكوادر البشرية المؤهلة.

3-إنّ تقنية الأمن المستخدمة لا تزال معقدة وغير عملية و لا تتماشى جيداً مع احتياجات المستخدمين، فالعديد من أسماء التعريف و كلمات المرور المعقدة هو أمر مزعج للغاية ويكون السبب في الكثير من القضايا الأمنية، كما أن نشر المعلومات الشخصية على المواقع العامة أحد العوامل المساهمة في سرقة الهوية والانتحال والخداع والابتزاز وما إلى ذلك.

4- فضلا عن تهديد الإرهاب الإلكتروني للنظم المعلوماتية والعالم السيبراني الذي ترمز إليه الشبكة العالمية للمعلومات (الانترنت)، فإنه يظل كذلك تهديداً حقيقيا يعرض حياة الناس وسلامتهم للخطر، لذلك يتعين على الدول تكثيف التعاون وتوحيد جهودها لاحتواء مخاطره.

5- تقوم أنظمة كشف التسلل بالكشف عن المشكلات التي وقعت بالأمس و ليس المشكلات التي من المتوقع أن تحدث في المستقبل، لذلك تحتاج النماذج والمعايير والتقنيات الأمنية إلى تطوير مستمر تثبت فعاليتها ومرونتها لتبديد هذه المخاوف.

6-إن قوات الشرطة الوطنية في الحد من الجرائم الإلكترونية العالمية تسير ببطء شديد لاتضاهي أبداً القدرات التقنية التي يتميز بها المجرمون السيبرانيون، بل إنّ الجرائم السيبرية أصبحت قضية أكبر من قضايا المخدرات غير المشروعة، لذلك تدعو الحاجة إلى تطوير مفهوم الاختصاص العالمي لتعزيز و تنسيق التعاون القضائي بين الدول في مجال مكافحة هذه الجرائم العابرة للحدود.

التوصيات:

1- إقامة إستراتيجية وطنية من قبل الدول لتعريف الناس على الحكومة الإلكترونية، وتسهيل الخدمات الحكومية بشفافية و إتقان.

2- نشر الوعي بمخاطر وتهديدات الأمن السبيراني لفئات المجتمع من طلاب المدارس والجامعات والموظفين وصناع القرار في القطاعين العام والخاص، والتنسيق مع الجهات و الهيئات الرسمية لتسويق أمن المعلومات للإدارات و الدوائر الحكومية.

3- دمج موضوع الأمن السيبراني في برامج التعليم للمؤسسات الأكاديمية باعتباره مكوناً أساسياً لعلوم تكنولوجيا المعلومات والاتصالات، وهذا لتوفير أيدي عاملة مجهزة على نحو جيد للمساهمة بدورها في المجتمع الرقمي.

4- التعاون بإنشاء قواعد للمعلومات الخاصة بالمعايير والمقاييس والنماذج المعتمدة في مجال أمن المعلومات والأنظمة، وأمن الأشخاص الطبيعيين والمعنويين.

5- الاضطلاع والعمل المستمر على تقييم ووضع مختلف مؤشرات تقدم الأطر التشريعية والتنظيمية ومدى كفايتها لمواجهة جرائم و تهديدات الأمن السبيرية.

الهوامـــش:

[1] http://nasaforum.com/forum// blogs. ، تاريخ الاطلاع : 2024/03/04.

[2] http://www.dotmsr.com/details/10- ، تاريخ الاطلاع : 2024/03/06.

[3] https:// www. Itu.int/net/itunews/issues/2010/09/pdf/21009_20-ar.pdf ، تاريخ الإطلاع: 2024/03/06.

[4] منى الأشقر جبور،السيبرانية هاجس العصر، المركز العربي للبحوث القانونية و القضائية،جامعة الدول العربية ،ص 25.

[5] الإتحاد الدولي للاتصالات، دليل الأمن السيبراني للبلدان النامية،جنيف سويسرا،2006 ، ص 7.

[6] عمر بن محمد العتيبي،الأمن المعلوماتي في المواقع الالكترونية ومدى توافقه مع المعايير المحلية و الدولية، أطروحة دكتوراه في العلوم الأمنية، كلية الدراسات العليا،جامعة نايف العربية للعلوم الأمنية،الرياض، 2010، ص 17.

[7] يساعد التشفير على حماية سرية المعلومات أثناء الإرسال أو التخزين بتحويلها إلى شكل غير مفهوم لأي شخص لا يمتلك وسائل فك هذا التشفير.(أنظر: الإتحاد الدولي للاتصالات، مرجع سابق، ص 23).

[8] مصطلح "فيروس" يستخدم لتسمية أي برنامج حاسوبي ضار فيحدث العدوى، والتدمير و يكون قادراً على التكاثر وإكثار نفسه، وفي عام 2005 كان هنالك ما يربو عن 50 ألف فيروس جديد منتشراً بأجهزة الحاسوب في العالم؛ فقد أصاب مثلا الفيروس (HTML-NETSKY .P) حسب تقديرات المركز العالمي لمتابعة الفيروسات 855244 جهازاً حول العالم منذ 2004، وكانت التكلفة للشركات التي انتقلت إليها العدوى ما يقارب حوالي 42 مليون دولار أمريكي.(أنظر : الإتحاد الدولي للاتصالات ،مرجع سابق، ص 38).

[9] الديدان: هي بياتات من شفرة حاسوبية تسافر عبر النت دون مساعدة خارجية وهي تعمل على الإضرار بخدمات النظام أو تساعد على التحكم في النظام المصاب بالعدوى عن بعد.(أنظر: الإتحاد الدولي للاتصالات،المرجع نفسه، ص 38).

[10] تكون البرامج الخبيثة المعروفة باسم أحصنة طروادة غاليا مخبأة داخل البرامج العادية أو الملفات المساعدة تم تتسلل إلى النظم، حيث تحاول السيطرة أو تتلاعب بالبيانات أو البرامج أو تدمرها وتتسبب في انهيارات، كما تقوم بالتطفل وأشكال النشاطات الخبيثة الأخرى، أو أنها تنام ريثما تتاح لها الفرصة للهجوم مستقبلا.(أنظر :الإتحاد الدولي للاتصالات،المرجع نفسه،ص 38).

[11] في عام 2011 كان عدد الموصولين بالانترنت لا يقل عن 2,3 بليون نسمة أي ما يعادل أكثر من ثلث مجموع سكان العالم،ويعيش أكثر من 60% من جميع مستخدمي الانترنت 25 في الدول النامية، ولا يتعدى عمر 45 % من مجموع مستخدمي الانترنت 25 عاما، و بحلول سنة 2017 سيكون المتوقع أن تفوق نسبة المشتركين بخدمة الانترنت النقالة ذات النطاق العريض 80% من مجموع سكان العالم، و بحلول عام 2020 سيفوق عدد الأجهزة المتصلة بالشبكة العالمية عدد الناس بنسبة 6 إلى 1، مما سيؤدي إلى تغيير في المفاهيم الحالية للانترنت.(أنظر: تقرير لفريق الخبراء الحكومي المعني بإجراء دراسة شاملة عن الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء و المجتمع الدولي و القطاع الخاص للتصدي لها، 25 -28 شباط/فبراير 2013، لجنة منع الجريمة و العدالة الجنائية،مكتب الأمم المتحدة المعني بالمخدرات والجريمة،فيينا،ص2 . الوثيقة:UNODC CCPCJ/EG.4/2013/2 المؤرخة في 2013/01/23 – النسخة العربية).

[12] منى الأشقر جبور،*الأمن السيبراني: التحديات ومستلزمات المواجهة*، اللقاء السنوي الأول للمختصين في أمن و سلامة الفضاء السيبراني 27- 28 أغسطس (آب) 2012 بيروت، مركز البحوث القانونية و القضائية، جامعة الدول العربية، ص 16.

[13] محمد مختار، مرجع سابق، ص 6-7.

[14] الإتحاد الدولي للاتصالات، مرجع سابق،ص 17.

[15] في العديد من الدول تم إسقاط أنظمة سياسية حاكمة بفعل استخدام شبكات التواصل الاجتماعي كمصر مثلا في عهد الرئيس المخلوع (حسني مبارك) في إطار ما سمي بثورات الربيع العربي.

[16] كاستخدام الرئيس الأمريكي الأسبق (باراك أوباما) الشبكات الاجتماعية بشكل مكثف خلال حملاته الانتخابية للوصول إلى البيت الأبيض.

[17] محمد مختار،مرجع سابق،ص 7.

[18] الإتحاد الدولي للاتصالات،مرجع سابق،ص 17- 18.

[19] منى الأشقر جبور، السيبرانية هاجس العصر،مرجع سابق،ص 31.

[20] مصطلح "الحرب السيبرانية" (cyber warfare) يستند إلى أيديولوجية أمنية أو عسكرية تضع منهاجاً لتحقيق أهداف على الصعيد الأمني أو العسكري تجاه العدو المفترض.(أنظر: أحمد عبيس نعمة الفتلاوي،الهجمات السيبرانية:مفهومها و المسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر،مجلة المحقق الجلي، كلية القانون، جامعة بابل، 2015 -2016 ،ص 6).

[21] نسرين الشحات الصباحي علي،"*الأبعاد العسكرية للقوة السيبرانية على الأمن القومي للدول دراسة حالة- إسرائيل منذ عام 2010 -"* المركز العربي للدراسات الإستراتيجية والسياسية والاقتصادية، متاح على الرابط التالي: http:// demacraticac.de/ ?p=30962 ، تاريخ الإطلاع: 2017/02/27.

[22] نذكر في هذا الصدد ما تعرضت له أنظمة الاتصال الإلكترونية التابعة لوزارة الدفاع الأمريكي (Pantagan) ووكالة الفضاء الأمريكية (NASA) ووكالة الطاقة الأمريكية لهجمات سيبرانية بين سنوات 1998-2000، وأدى ذلك إلى الاستيلاء على الآلاف من الملفات بالغة الحساسية التي تصنف في خانة السرية، وقد اتهمت الولايات المتحدة الأمريكية روسيا الاتحادية،وأنكرت هذه الأخيرة الهجوم.(راجع: عبيس نعمة الفتلاوي، مرجع سابق، ص12).

[23] محمد مختار،مرجع سابق،ص 6.

[24] أورد التقرير السادس حول جرائم الكومبيوتر ودراسة أمن المعلومات المسحية لعام 2001 المعد من قبل معهد أمن المعلومات بالتعاون مع مكتب التحقيقات الفيدرالية في الولايات المتحدة الأمريكية (2001/CSI/FBI Computer crime and Security) نتائج الدراسة الشاملة التي أجريت بمشاركة (538) مؤسسة أمريكية تضم وكالات حكومية وبنوك ومؤسسات مالية وصحية وجامعات وأظهرت النتائج بوجه عام تنامي خطر جرائم الكومبيوتر وارتفاع حجم الخسائر الناجمة عنها بالرغم من زيادة الوعي بمسائل أمن المعلومات، بحيث تبين أن 85% من المشاركين في الدراسة وتحديداً المؤسسات الحكومية تعرضت لاختراقات إلكترونية وأن 64% لحقت بهم خسائر مادية جراء هذه الاعتداءات، وأن 35% تمكنوا من حساب مقدار خسائرهم المادية التي بلغت حوالي 378 مليون دولار في حين كانت الخسائر لعام 2000 في حدود 265 مليون دولار، وأن معدل الخسارة السنوية للأعوام الثلاثة السابقة لعام 2000 وصلت إلى 120 مليون دولار، وتمثلت أخطر مصادر الخسارة المالية في سرقة المعلومات المتعلقة بالأموال والممتلكات بحوالي 151 مليون والاحتيال المالي بـ 53 مليون، كما كشفت الدراسة أيضا أن 70% من الاعتداءات حصلت من نقطة الاتصال الخارجي عبر الانترنت مقابل 30% حصلت من نقطة تتعلق بداخل النظام نفسه، في حين كانت نسبة الاختراق عبر اتصال الانترنت 59% عام 2000، وأن 365 من المشاركين بالدراسة أبلغوا جهات الإنقاذ والقانون حول هذه الاختراقات بنسبة زيادة 11% من عام 2000، حيث كانت نسبة المبلغين 25% عام 2000 في حين كانت 16% عام 1996 . أما حول مصدر و طبيعة الاعتداءات فإن 40% من الاعتداءات تمت خارج المؤسسات مقابل 25% في عام 2000، وأن 38% من الاعتداءات بهجمات تعطيل الخدمة مقابل 27% عام 2000، وأن نسبة الموظفين الذين ارتكبوا أفعال إساءة استخدام اشتراك الانترنت لمنافع شخصية بلغت 91% تتوزع بين الاستخدام السيئ للبريد الإلكتروني وتنزيل مواد إباحية من الشبكة، في حين كانت هذه النسبة 79% عام 2000، وأن 94% من المشاركين تعرضوا لهجوم الفيروسات مقابل 85% عام 2000.(للمزيد أكثر أنظر: جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات- رؤية جديدة للجريمة الحديثة- ط:01، دار البداية،عمان،2007،ص 116 – 121).

[25] مصطلح "الهاكرز" مرادف في الغالب لهجمات التحدي، فالهاكرز هم فئة متطفلون يغلب عليهم صغر السن وقلة الخبرة يخترقون أمن النظم والشبكات بدافع التحدي وإثبات المقدرة دون محاولة القيام بأية عمليات تخريب كبيرة (اختراقات أمنية)، إلاّ أن هناك نوع آخر من الهاكرز الذين يكون دافعهم الأساسي هو التخريب، حيث ينصب اهتمامهم على سرقة المعلومات متسببين في إحداث أنواع متعددة من الدمار (محو محركات الأقراص الصلبة)،وفي بعض الأحيان يتسببون في تدمير نظم بأكملها.(أنظر:جعفر حسن جاسم الطائي، المرجع نفسه، ص 157 – 161).

[26] محمد مختار،مرجع سابق، ص 5.

[27] التصيّد: هو عبارة عن هجمة سيبرانية تحاول الحصول على معلومات سرية بطرق احتيالية، مثل أسماء المستخدمين و كلمات السر وتفاصيل بطاقات الائتمان وغير ذلك من خلال استدراج المستخدم برسالة تبدو قادمة من مؤسسة مشروعة، وهو ما قد يتسبب في أضرار فادحة (أنظر: http://ar.unesco.org/glossaries/igg ، تاريخ الإطلاع: 2017/02/24).

[28] القنبلة المنطقية عبارة عن برنامج أو جزء من برنامج ينفذ في لحظة محددة أو كل فترة زمنية منتظمة، و يتم وضعه في شبكة المعلومات بهدف تحديد ظروف أو حالة فحوى النظام بغرض تسهيل تنفيذ عمل غير مشروع.(أنظر: جعفر حسين جاسم الطائي، مرجع سابق،ص 186).

[29] عمر بن محمد العتيبي،مرجع سابق، ص 88.

[30] منى الأشقر جبور، السيبرانية هاجس العصر، مرجع سابق، ص 53 – 54.

[31] جعفر حسن جاسم الطائي،مرجع سابق،137.

[32] محمد مختار، مرجع سابق، ص 6.

[33] محمد محمود السيد،عرض لكتاب: كيف سيواجه العالم تحديات الأمن السيبراني؟ لمؤلفيه بيتر سبنجر والآن فريدمان، مجلة السياسة الدولية الأهرام،متاح على الرابط التالي: www.siyassa.org.eg/Newsq/4925.aspx ، تاريخ الإطلاع: 2024/03/22..

[34] مفهوم الإرهاب مفهوم نسبي متطور يختلف من مكان إلى آخر و من فرد إلى آخر و من عقيدة أو فكر إلى آخر، ومن الصعب الإقرار بوجود مفهوم واحد للإرهاب يمكن أن يقبل به الجميع.(أنظر: عادل نايف ترابة، رؤية قانونية للإرهاب في المجتمع الدولي، مجلة المؤتمر، العدد 18،المركز العالمي لدراسات وأبحاث الكتاب الأخضر طرابلس،2003 ،ص 17).

[35] منى الأشقر جبور، السيبرانية هاجس العصر، مرجع سابق، ص 85.

[36] عمر بن محمد العتيبي،مرجع سابق، ص 89-90.

[37] الانترنت المظلم هو جزء من الانترنت الخفي، لايمكن الوصول إليه باستخدام المتصفحات العادية أو محركات البحث المعروفة مثل: غوغل، ياهو، فاير فوكس، بل عن طريق متصفحات خاصة مثل تور (TOR)، فريبتو (Freepto) وفرينت (Freenet) وغيرها، والميزة الأساسية لها هو إخفاء الأثر الذي يمكن أن يتركه المتجول عبر الانترنت، ومنع تعقبه و مراقبته مما يتيح له حماية هويته ومعلوماته،إنشاء مواقع على الانترنت دون كشف هويته أو مكان وجوده، تجاوز أنظمة الحجب المعتمدة في بعض الدول، تكوين شبكات تبادل معلومات آمنة وإرسال معلومات سرية، ويتم ذلك عبر تقنية تشفير البيانات وعلى شبكة من آلاف الخوادم الموزعة حول العالم التي تستقبل طلبات الدخول إلى المواقع، وتقوم بترميزها قبل إرسالها بما يؤمن إخفاء هوية المتصفح و سرية التصفح والحركة.(أنظر: منى الأشقر جبور، السيبرانية هاجس العصر، مرجع سابق، ص 87 -88).

[38] منى الأشقر جبور، مرجع نفسه، ص 87-88.

[39] جعفر حسن جاسم الطائي،مرجع سابق، ص 246-247.

[40] عمر بن محمد العتيبي، مرجع سابق، ص 51-54.

[41] Ar.uneco.org/glossaries/igg، تاريخ الاطلاع: 2024/03/22..

[42] تعتبر أسماء نطاقات الانترنت كبطاقة الهوية في تعريفها عن الموقع وعن الشخص الذي ينشئه، ويتولى إدارة العناوين وتوزيعها هيئة متخصصة هي هيئة الانترنت للأسماء و الأرقام المخصصة (آيكان).

[43] منى الأشقر جبور،السيبرانية هاجس العصر، مرجع سابق، ص 16 -15.

[44] منى الأشقر جبور،السيبرانية هاجس العصر، مرجع نفسه، ص 18.

[45] http:// www.Lebarmy.gov.Lb/ar/content، تاريخ الاطلاع : 2024/03/22.

[46] صغير يوسف،الجريمة المرتكبة عبر الانترنت، رسالة ماجيستر في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية،جامعة مولود معمري- تيزي وزو،2013، ص 19-20.

[47] جعفر حسن جاسم الطائي،مرجع سابق، ص 262 -264 .

[48] "الحوسبة السحابية" مصطلح يشير إلى المصادر والأنظمة الحاسوبية المتوافرة تحت الطلب عبر الشبكة والتي تستطيع توفير عدد من الخدمات الحاسوبية المتكاملة دون التقيد بالموارد المحلية بهدف التيسير على المستخدم.(أنظر الرابط التالي :

www.qscience.com/doi/pdf/10.5339/qproc.2015.gsla.8)، تاريخ الاطلاع :22 /2024/03..

[49] الإتحاد الدولي للاتصالات،"*بناء الثقة و الأمن في استعمال تكنولوجيا المعلومات و الاتصالات*"، مجلة أخبار الإتحاد،العدد 10، ديسمبر 2010، ص 46.

[50] جورج لبكي،"*المعاهدات الدولية للإنترنت:حقائق و تحديات*"،مجلة الدفاع الوطني اللبناني،العدد 83، كانون الثاني،2013، (ar/content/83-d)،الموقع الرسمي للجيش اللبناني: https:// www.Lebarmy.gov.lb/ar/content، تاريخ الاطلاع : 2024/03/22.