مجلة طبنـــة للدراسات العلمية الأكاديمية ISSN 2661-7633 / EISSN 2716-8883

السنة: 2022 المجلد: 05 العدد: 02 ص.ص: 37-56

الأمن السيبراني والمضامين المفاهيمية المرتبطة به

Cybersecurity and its related conceptual implications

قطاف سليمان*[1]، مخبر البحث الحقوق والعلوم السياسية، جامعة الأغواط– (الجزائر)،
s.guettaf@lagh-univ.dz

بوقرين عبدالحليم[2]، جامعة الاغواط– (الجزائر)
Halim.ma@yahoo.fr

تاريخ إرسال المقال: 09-08-2022 تاريخ قبول المقال: 19-08-2022 .

الملخص: أصبح العالم اليوم نتيجة التطور التكنولوجي الحاصل، يعيش في قرية صغيرة، لكن بالرغم من الإيجابيات التي تقدمها هذه التكنولوجية الرقمية، الا انه هناك مخاطر تهدد هذه الحياة الإنسانية في شتى الميادين والمجالات، وأصبحت هذه المخاطر تؤرق الدول والمؤسسات وحتى الحياة الخاصة للأفراد، مما عجل بضرورة وحتمية الأمن السيبراني لتوفير الحماية السيبرانية، والبحث عن أليات لمواجهة التهديدات السيبرانية، وهذا على عاتق الامن السيبراني وتحديات التي يمثلها، وأصبحت التوعية بأهمية الامن السيبراني أكثر من ضرورة، لمكافحة الإجرام السيبراني لأجل تحقيق فعالية الامن السيبرانية، وتوفير الحماية من الابتزاز والاختراق للبيانات وحماية البنية التحتية للمعطيات سواء كانت دول أو أفراد.

الكلمات المفتاحية: الأمن السيبراني، الفضاء السيبراني، المخاطر السيبرانية.

Abstract: Today, as a result of technological development, the world has become living in a small village, but despite the positives offered by this digital technology, there are dangers that threaten this human life in various fields and fields, and these dangers have become afflicting countries, institutions and even the private lives of individuals, which hastened the necessity of And the imperative of cyber security to provide cyber protection, and to search for mechanisms to confront cyber threats, and this is the responsibility of cyber security and the challenges it poses, and awareness of the importance of cyber security has become more than a necessity, to combat cyber crime in order to achieve the effectiveness of cyber security, and provide protection from extortion and data breach and infrastructure protection For data, whether countries or individuals.

Key words : Cyber security, cyber space, cyber risks.

* قطاف سليمان

مقدمة:

يعد الأمن السيبراني ركيزة أساسية لسياسة الأمن، لذلك من غير المتصور أن الأنشطة خارج التحقيقات الأمنية ستنمو، من الناحيتين التقنية والقانونية. مع ظهور مجتمع المعلومات والفضاء السيبراني بالإضافة إلى الحكومة الإلكترونية وتطبيقاتها، كما أصبح الأمن السيبراني أحد مجالات الخدمات الرقمية وقيمة مضافة وركيزة للأنشطة الحكومية. مثل الصحة والتعليم عن بعد والتجارة الإلكترونية وما إلى ذلك. ومع ذلك، فإن الجوانب المتعددة للأمن السيبراني وعواقبه الخطيرة لا تقتصر على تعريض الأفراد والمؤسسات للخطر، بل تتجاوز تعريض أمن الدول والحكومات للخطر، مما يجعل مهمة المسؤولين عن الموضوع أكثر صعوبة. و مطلوب نهج معقد وصعب وشامل ومتكامل لمواجهة جميع التحديات التي يطرحها الفضاء السيبراني. لذلك من خلال استخدام المعرفة الأساسية لتكنولوجيا المعلومات والاتصالات فإن الإجراءات المضادة والحلول المقترحة فعالة في مجال التنمية لخدمة المجتمع البشري من حيث تحقيق الأمن وبناء الثقة في الفضاء السيبراني[1]. لذا، لابد من التوقف بداية، عند ماهية الامن بصفة عامة وعند ماهية الأمن السيبراني، لنستعرض بعدها أبعاد هذا الأمن السيبراني، وما يرتبط به من تحديات.

أولا– تحديد الموضوع: اصبح الأمن السيبراني ضرورة حتمية تحفظ الدول والمؤسسات والأفراد، وتجاهله يودي إلى خروقات سيبرانية وإنتهاك لخصوصية الافراد، لذا سنحاول من خلال هذه الورقة البحثية تحديد النقاط الأتية:

1– تعد المخاطر السيبرانية من الجرائم المستحدثة التي تمثل خطرا وتهديدا كبيرا على الفرد والمجتمع وكذلك على الأجهزة الأمنية للدولة؛

2– دراسة الامن السيبراني والتحديات التي يمثلها وما مدى فاعليته في مواجهة التهديدات السيبرانية؛

ثانياً– أهداف الموضوع: تتمثل أهداف هذا البحث فيما يلي:

1– التحسيس بالمخاطر السبرانية ودور الأمن السيبراني في مكافحتها؛

2– التعرف على أبعاد الأمن السيبراني في شتى الميادين المختلفة؛

3– مدى فعالية الامن السيبراني في كبح جماح الجريمة السيبرانية وخاصة التشريع الجزائري.

[1]– فيصل محمد عسيري، الأمن السيبراني وحماية المعلومات، ورقة بحثية متاحة على الرابط الإلكتروني التالي: https://www.kutub.info/library/book/21854 ، تاريخ التصفح 30 ماي2022على الساعة 21:24 h.

ثالثاً– إشكالية البحث: فكان بذلك محور الدراسة الحالية من خلال طرح إشكالية البحث التي تتمثل في التساؤل الجوهري التالي: ما هو الأمن السيبراني؟ وماهي أبعاده وأهميته والأهداف التي جاء من أجلها؟ لتوفير حماية فعالة للأمن السيبراني؟.

رابعاً– منهج البحث: اعتمدنا منهج البحث على المنهج الاستنباطي (التحليلي) والمنهج المقارن ببيان مفهوم الأمن السيبراني والتحديات التي يمثلها، وتناول الأبعاد والأهداف للأمن السيبراني.

خامساً– خطة البحث: للإجابة عن هذا الإشكالية المطروحة قسمت البحث إلى مبحثين: المبحث الأول يتحدث عن الإطار المفاهيمي للأمن السيبراني، أما الثاني عن الأمن السيبراني (المصطلحات المرتبطة به ،التحديات، الأهداف). على النحو التالي:

المبحث الأول: الإطار المفاهيمي للأمن السيبراني

المطلب الأول: مفهوم الأمن السيبراني

المطلب الثاني: نشأة الأمن السيبراني وأبعاده

المبحث الثاني: الأمن السيبراني (المصطلحات المرتبطة به ،التحديات، الأهداف)

المطلب الاول: المفاهيم المرتبطة بالأمن السيبراني

المطلب الثاني: التحديات التي يمثلها الأمن السيبراني وأهدافه

المبحث الأول: الإطار المفاهيمي للأمن السيبراني

يعتبر الامن السيبراني من ركائز السياسة الجنائية الأمنية، نظرا لأهميته في استقرار الأمن والمعاملات، وأصبحت الدول تخصص له إنفاقا كبير، لأجل درء الحرب السيبرانية المهددة للأمن الوطني والمساس بالبنية التحتية الحساسة للبيانات. اذن ما هو مفهوم الامن السيبراني وما هي ابعاده؟.

المطلب الأول: مفهوم الأمن السيبراني

شهد هذا القرن تطوراً هائلاً في وسائل الاتصال، مقابل فجوة بين مستخدمي الشبكة ، وظهور الاستخدام غير المشروع، مما أدى إلى ظهور جرائم عابرة للقارات، على عكس الجرائم التقليدية. وسميت بالجرائم المستحدثة أو الجرائم المعلوماتية أو الإلكترونية أو الجرائم السيبرانية وكانت هذه الجرائم تحديا لما يسمى بالأمن السيبراني

الفرع الأول: تعريف الأمن السيبراني

أولا: تعريف السيبرانية لغة: كلمة سايبر (CYBER) في المعاجم اللغوية يظهر انها يونانية الأصل وترجع الى مصطلح (KYBERNETES) بمعنى الشخص الذي يدير دفة السفينة وتعني القيادة او التحكم عن بعد). وكذلك ورد ذكر مصدر سايبر (CYBER) في قاموس (المورد) اذ يعرفها بانها علم الضبط ومصدرها(CYBERNETIEC) اي ضبط الاشياء عن بعد والسيطرة عليها . اذ جاء لفظها في القاموس بمعني تخيلي او افتراضي ودرج استخدامها لوصف الفضاء الذي يضم الشبكات المحوسبة ومنها اشتقت صفة السيبراني والسيبرانية (CYBERNETIC) وتعني علم التحكم الأوتوماتيكي، او علم الضبط أي ضبط الأشياء عن بعد والسيطرة عليها[1].

ثانيا– تعريف السيبرانية اصطلاحا: كلمة سيبرانية في مفهومها الحديث استعملت لأول مرة من قبل عالم الرياضيات الأمريكي « نوربرت وينر NORBERT INER» وهو أستاذ الرياضيات في معهد ماساشوستس التقني MIT الذي أعطاها مفهومها الإصطلاحي الحديث وكان ذلك عام 1948، ومن أجل وصف نظام التغذية الرجعيةFEEDBACK الإستفادة من مخرجات الأنظمة PUTS OUT في ضبط مدخلاتهاIN PUTS وفي التحكم فيها وإستقرار أدائها. ورأى «وينر» أنه يمكن تطبيق هذا النظام على نطاق واسع في مختلف المجالات ليس العملية فقط بل الإنسانية أيضا، وبالتالي فالمصدر الإصطلاحي الحديث لكلمة سيبرانية وهو «**علم القيادة والتحكم في الأحياء والآلات ودراسة آليات التواصل**»[2].

بالنسبة للغة العربية، من خلال نظرة خبرائها، وجدنا أن لديهم تحديات في اختيار مصطلح قريب من المصطلح باللغة الإنجليزية (CYBER) ، كما يتضح من حقيقة أن الترجمة العربية لعنوان اتفاقية مجلس أوروبا بشأن الجرائم السيبرانية حيث تمت ترجمته بشكل غير صحيح، لأن العنوان (CONVENTION ON CYBER CRIME) مترجم إلى اللغة العربية بـ (الاتفاقية المتعلقة بالجرائم السيبرانية)، وذلك لعدم وجود مصطلح مقابل في اللغة العربية[3].

[1]– أسعد طارش عبد الرضا، علي إبراهيم مشجل المعموري، الأمن الإنساني ودوره في إنتشار ظاهرة الإرهاب في العراق بعد عام 2003، مجلة دراسات دولية، العدد 80، يناير2020، ص153.

[2]– إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة مصداقية، كلية الحقوق والعلوم السياسية–جامعة العربي التبسي، تبسة، الجزائر، المجلد01، العدد01، 2019.

[3]– احمد عبيس نعمه الفتلاوي: الهجمات السيبرانية، دراسة قانونية تحليليه بشان تحديات تنظيمها المعاصر، الطبعة الأولى، منشورات زين الحقوقية، بيروت، 2018، ص12.

ثالث- تعريف الأمن السيبراني:" بأنه أمن الشبكات والأنظمة المعلوماتية، والبيانات، والمعلومات، والأجهزة المتصلة بالأنترنت". وعليه فهو المجال الذي يتعلق بإجراءات، ومقاييس، ومعايير الحماية المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات، أو للحد من آثارها في أقسى وأسوأ الأحوال. ويرتبط هذا الأمن، ارتباطا وثيقا، بأمن المعلومات، فالوصول إلى هذه الأخيرة، أو بثها أو الاطلاع عليها والمتاجرة بها، أو تشويهها واستغلالها، هو ما يقف، غالب الأحيان، وراء عمليات الاعتداء على الشبكات، وعلى الانترنت[1].

كما نذكر التعريف الذي جاء به الاتحاد الدولي للاتصالات الصادر في تقريره حول" **اتجاهات الإصلاح في الاتصالات للعام 2010-2011**"، **والذي يعتبر بمثابة أرضية إجماع لمختلف التوجهات الفكرية والمهنية "هو مجموعة من المهمات، مثل تجميع وسائل، وسياسات، واجراءات أمنية، ومبادئ توجيهية. ومقاربات الإدارة المخاطر، وتدريبات، وممارسات فضلي، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين"**[2].

كما عرفته المنظمة الدولية للتوحيد القياسي الأمن السيبراني أو أمن الفضاء الإلكتروني كما يلي: "**الحفاظ على سرية وسلامة وتوافر المعلومات في الفضاء السيبراني.**" وتم تعريف الفضاء السيبراني على أنه:" البيئة المعقدة الناتجة عن تفاعل الأشخاص والبرامج والخدمات على الإنترنت عن طريق تقنية الأجهزة والشبكات المتصلة به والتي لا وجود لها في أي منها شكل مادي"[3].

كما أعطى له المشرع الجزائري تعريفا في الفقرة الثالثة من المادة العاشرة من القانون رقـم: 18-04[4] بأنه:" **مجموع الأدوات والسياسات ومفاهيم الأمن والآليات الأمنية والمبادئ التوجيهية وطرق تسيير المخاطر والأعمال والتكوين والممارسات الجـــيدة والضمانات والتكنولوجيات التي يمكن استخدامها في حماية الاتصالات الإلكترونية ضـــد أي حـدث مـــن شأنه المساس بتوفير وسلامة البيانات المخزنة أو المعالجة أو المرسلة**". كما سعى المشرع في تعديله الأخير لقانون العقوبات للفصل

[1]- منى الأشقر جبور، السيبرانية هاجس العصر، دراسات وأبحاث، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، بيروت،2016, ص 26.

[2]- جمال بوازدية، الإستراتيجية الجزائرية في مواجهة السيبرانية" التحديات والأفاق المستقبلية"، مجلة العلوم القانونية والسياسية المجلد10،العدد01، أفريل2019، ص1267.

[3]- Syed, Rubab, Ahmed Awais Khaver, and Muhammad Yasin. "WHAT IS CYBER SECURITY?" Cyber Security: Where Does Pakistan Stand? Sustainable Development Policy Institute, 2019.p2 http://www.jstor.org/stable/resrep24376.5 .

[4]- أنظر المادة3/10 من القانون رقم 18-04 المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الصادر في الج.ر.ج العدد 27، بتاريخ 13 مايو 2018، ص 03.

الثالث من الباب الثاني من الكتاب الثالث من الأمر 156-66 إلى إضافة قسم سابع مكرر عنوانه: "**المساس بأنظمة المعالجة الآلية للمعطيات**"، بالقانون 04-15[1] ويشمل المواد من 394 مكرر إلى 394 مكرر 7. حيث جاء في هذا القسم بتسطير حماية فعالة لأنظمة المعالجة الآلية للمعطيات، وهو ما تركه ينص على بعض من الجرائم و ما يقابلها من عقوبات للحد من إرتكابها[2].

وقد عرف الجريمة السيبرانية في نص المادة 2 الفقرة-أ- من الفصل الأول من القانون 09-04[3] المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها تحت عنوان مصطلحات بأنهما "**جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية**"[4].

كما حظيت المعطيات ذات الطابع الشخصي بالحماية من قبل المشرع الجزائري فقد عرفها لنا من خلال المادة 03 من القانون 18-07[5] بأنها: " **كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه والمشار إليه أدناه (الشخص المعني بصفة مباشرة أو غير مباشرة، لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية**"[6].

من هذا المنظور ، يمكننا إعطاء تعريف شامل الأمن السيبراني بأنه هو مجموع القوانين والأدوات والنصوص والمفاهيم وآليات الأمن وأساليب إدارة المخاطر والممارسات الفنية المتعلقة بتكنولوجيا

[1]- انظر المواد من 394 مكرر إلى 394 مكرر 7 من القانون 184- القانون 04-15، المؤرخ في 10 نوفمبر 2004، الصادر في الج.ر.ج رقم: 71، المتضمن تعديل قانون العقوبات لسنة 2004، ص. ص: 11 و12.

[2]- بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتوراه علوم تخصص قانون عام، كلية الحقوق، جامعة الجزائر1 بن يوسف بن خدة ،2018، ص154.

[3]- أنظر المادة 02/أ من القانون رقم 09 - 04، المؤرخ في 14 شعبان عام 1430، الموافق 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المنشور بالج.ر.ج العدد 47 بتاريخ 16 غشت سنة 2009.

[4]- بلال بن جامع، الجرائم المعلوماتية على شبكة الانترنت دراسة حالة جامعة عبدالحميد مهري قسطنينة2، رسالة دكتوراه، معهد علم المكتبات والتوثيق، جامعة عبدالحميد مهري قسنطينة2، 2016-2017، ص116.

[5]- انظر المادة 03 من القانون 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الصادر في الج.ر.ج العدد34، في 10 يونيو 2018.

[6]- خلوف حسام، باطلي غنية، الآليات القانونية لحماية المعطيات ذات الطابع الشخصي، مجلة الدراسات القانونية والإقتصادية، المركز الجامعي بريكة، المجلد05، العدد01، 2022، ص1633.

المعلومات والاتصالات المستخدمة لحماية المصالح الدول والأشخاص. والأشخاص ، لذلك يظل الهدف النهائي هو قدرة هذه الأدوات على الدفاع ضد التهديدات المتعمدة من قرصنة المعلومات والبيانات أو سوء استخدام تكنولوجيا المعلومات والاتصالات[1]. بعد تعريفنا للأمن السيبراني نتطرق إلى أهمية الامن السيبراني في تحقيق الحماية السيبرانية وتوفيرها في الفرع الموالي.

الفرع الثاني: أهمية الأمن السيبراني

إن من أهم أسباب الحاجة إلى أمن السيبراني هو الدعوة إلى إطار تشريعي وقانوني وتنظيمي يتناسب مع التحديات التي يواجهها المجتمع أو المنظمات أو الأفراد وهي الحاجة إلى الاتصال بأنظمة الاتصال والإنترنت و عدم القدرة على عزل الأجهزة عن الشبكات المحلية وشبكات المنطقة الواسعة لأفرادها لتوفير المعلومات واعتماد المؤسسات المختلفة على توافر المعلومات مع زيادة التطور التكنولوجي وزيادة الشبكات، يزيد من متطلبات وتحديات هذه المؤسسات و صعوبة السيطرة على المخاطر أو تعقب المجرمين ومعاقبتهم ؛ بسبب استخدام الإنترنت، فليس لقرب الاتصال حدود جغرافية، حيث يتيح الفرصة لاختراق الحدود المكانية، بالإضافة إلى النمو المطرد في الاستخدام والتطبيقات الإلكترونية، وظهور التجارة الإلكترونية والتسوق عبر الإنترنت والحكومة الإلكترونية والإدارة الإلكترونية التي تتطلب بيئة معلومات آمنة.[2] وتتلخص فيما يأتي:

1- يتطلب اتصالاً بأنظمة الاتصال والإنترنت ولا يمكنه عزل الجهاز عن شبكة المحلية و الواسعة المطلوبة؛

2- اعتماد المؤسسات المختلفة على توافر المعلومات، مما يزيد مع زيادة التطور التكنولوجي والطلب على هذه المؤسسات.

3- صعوبات في مواجهة الأخطار ومكافحتها أو تعقب المجرمين ومعاقبتهم، بسبب عدم وجود حدود جغرافية عند استخدام الإنترنت والاتصالات الإلكترونية، حيث أنها تتيح الفرصة لاختراق الحدود المكانية.

4- يتطلب النمو المطرد للاستخدام والتطبيقات الإلكترونية وظهور التجارة الإلكترونية والتسوق عبر الإنترنت والحكومة الإلكترونية والإدارة الإلكترونية بيئة معلومات آمنة ؛

[1]- جمال بوازدية، مرجع سابق، ص1267.

[2]- أوس مجيد غالب العوادي، الامن المعلوماتي السيبراني، في حصاد البيان8، سلسلة إصدرات مركز البيان للدراسات و التخطيط، بغداد، 2016، ص6.

5- يشمل الأمن السيبراني تطوير إجراءات لمنع الاستخدام غير السلمي للفضاء السيبراني والتهديدات التي يشكلها للأمن العالمي والبنية التحتية للمعلومات. وهكذا أصبح الأمن الوطني جزءًا من الأمن الجماعي.

6- أصبحت قضية أمن الشبكات قضية دولية، سواء من حيث آليات واستراتيجيات الأمن، مما يتطلب استراتيجية مرنة تتكيف مع التغيرات المستمرة في مقابل المخاطر المتزايدة باستمرار[1]. وقد يتبادر إلينا كيف جاءت فكرت الأمن السيبراني؟ وماهي أبعاده؟ وهذا ما نتطرق إليه في المطلب الموالي.

المطلب الثاني: نشأة الأمن السيبراني وأبعاده

تعود نشأة وتطور فكرة الامن السيبراني إلى سنة 1934 ، وكانت الحروب التقليدية الميدانية آنذاك السبب الرئيسي في بروز الحرب السيبرانية إلى الواقع وهذا ما نراه في الفرع التالي.

الفرع الأول: إرهاصات الامن السيبراني وبداية الإهتمام المجتمع الدولي به

إذا نظرنا إلى الماضي في التاريخ، نجد أن النواة الأولى للفضاء السيبراني[2] ويمكن إرجاعها إلى اندلاع الحرب الأهلية الأمريكية في عام 1861. في ذلك الوقت تم استخدام التلغراف لأول مرة لإدارة الحرب. حيث أصبح التلغراف جزءًا مهمًا من نظام الحرب. وفي عام 1888 أظهر علماء ألمان أن الطاقة الكهربائية تولد ترددات في الفضاء كإشارات يمكن تبنيها ومراقبتها، وهو اكتشاف أثار الاهتمام حيث أصبح يعرف بترددات هيرتز التي طورها البريطانيون إلى نظام الراديو ، كان أول تطبيق عملي لهذه التقنية في عام 1904 أثناء الحرب الروسية اليابانية ، عندما قصفت سفينتين حربيتين يابانيتين (كاسوجا ونيسين) القاعدة البحرية الروسية في ميناء آرثر، وكان لديهم سفينة صغيرة تقوم بمعايرة النيران باستعمال راديو (اللاسلكي)[3].

---

[1]- أسعد طارش عبد الرضا، علي إبراهيم مشجل المعموري، مرجع سابق، ص 157-158 .

[2]- تذكر المراجع العلمية ان اول من وضع مصطلح السبرانية هو عالم الرياضيات (نوربرت وينر) في عام 1948 في نص (السبرانية أو التحكم والاتصال في الحيوان والالة) كتبة عن التحكم والاتصالات في الحيوانات والآلات باستعارة كلمة يونانية سبقه اليها الفرنسي آمبير في عام 1834 وهي وليدة منطق المنظومات ووحدة المعرفة واستخدمت في مصطلح علم التحكم الالي في مجال الاتصالات الالكترونية. **أنظر** احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل، كلية القانون، العدد04، السنة 08، 2016، ص614.

[3]- علي عبدالرحيم العبودي، هاجس الحروب السيبرانية وتداعياتها على الامن والسلم الدوليين، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، العدد 57، ص 93-94.

إن الحربان العالميتان اللتان شهدهما العالم في النصف الأول من القرن العشرين كانتا نقطة الانطلاق للتفكير في دور التكنولوجيا في إدارة الصراع وتحقيق النصر، لذلك سعت الدول المتحاربة إلى تطوير القدرات التكنولوجية المتمثلة في الاتصالات اللاسلكية (الرادار). وفي الثلاثينيات من القرن الماضي طورت الولايات المتحدة وبريطانيا وألمانيا بقوة أجهزة إرسال وأنتجت أجهزة استقبال ذات حساسية عالية وهوائيات اتجاهية دقيقة، مما مكن الرادارات من اكتشاف الطائرات على بعد حوالي (50) ميلاً. وفي النصف الأول من القرن العشرين، بسبب التنافس بين قطبي الاتحاد السوفيتي السابق والولايات المتحدة، حدث سباق في تطوير الأدوات الإلكترونية، نتج عن ذلك تطوير أنظمة الأسلحة واستخدامها الاتصالات الحديثة للأسلحة وتكنولوجيا أنظمة التحكم عن بعد[1].

في أوائل التسعينيات أصبح التركيز على المعلومات مصدرًا للميزة التنافسية، لذلك بدأت التطبيقات الأمنية في حماية كل ما يتعلق بجمع المعلومات وتخزينها ومعالجتها وتسليمها داخل المؤسسة من المنافسين الذين يحاولون الحصول عليها. إنه غير قانوني ويسمى (أمن المعلومات أو أمن نظام المعلومات) بالإضافة إلى الحماية المادية، ومع انتشار استخدام تكنولوجيا المعلومات والاتصالات، وتم توسيع مفهوم أمن الشبكات ليشمل حماية التجارة الإلكترونية، والحوكمة الإلكترونية إلى مفهوم أكثر شمولاً يشمل حماية المعاملات الإلكترونية بين الأطراف داخل الوكالة التجارية والإدارة، وكذالك الرهانات المختلفة على مستوى التهديدات السيبرانية وعلى المستوى الاستراتيجي، مثل الحرب السيبرانية والدفاع السيبراني، على المستوى القانوني، مثل المراقبة الإلكترونية وحماية الحياة الخاصة، وعلى المستوى الاقتصادي، مثل المنافسة والحاجة. للإبداع[2]. وللأمن السيبراني أبعاد متعدد ومختلفة.

الفرع الثاني: أبعاد الأمن السيبراني

إن الأمن السيبراني علاقته بمجالات مختلفة، والغاية هو تحقيق منظومة أمن مترابطة تسعى على تأمين الأمن الوطني للدولة من أي تهديدات سيبرانية محتملة، ويمكن توضيح ذلك كآلاتي:

1- البعد العسكري: نشأت الإنترنت بشكل أساسي في البيئة العسكرية ثم نُقل لاحقًا إلى المجتمع العلمي ممثلاً بالبحث في خدمة القدرات العسكرية وتطورها ، والتي جمعت من أجلها الأمثلة الموضحة. على سبيل المثال نذكر ما حدث في جورجيا وإستونيا وكوريا الجنوبية وإيران، كأمثلة على الهجمات والتسلل السيبراني، سواء بسبب النزاع المسلح الذي أعقب ذلك ، أو بسبب انقطاع الاتصال بالإنترنت في إستونيا

[1]- المرجع نفسه، ص 94.

[2]- اشرف محمد عبدة، البيئة الامنية للحكومة الإلكترونية (بين المخاطر ومتطلبات الامن والحماية) ، دار الكتب والدراسات العربية، لإسكندرية، 2018، ص117.

بين الدولة ومواطنيها، وتعطيل الدوائر الحكومية واختراق أنظمة المنشآت النووية في إيران ، والميزة للقوة السيبرانية تكمن في قدرتها على المرور عبر الفضاء السيبراني لترابط الشبكات العسكرية بالوحدات العسكرية لتسهيل تبادل وتدفق المعلومات، فضلاً عن اتخاذ القرارات العسكرية السريعة لتحقيق الأهداف. إن تسليحها بهذه التكنولوجيا، أو حمايتها من أي تسلل خارجي سيؤدي بالضرورة إلى هجوم سيبراني مضاد على الجيش، والذي من شأنه أن يضر بقاعدة البيانات[1].

2- البعد الاقتصادي: أصبح الفضاء السيبراني جاذبا لقطاعات المجتمع كافة، افرادا و جماعات وزاد الاعتماد بصورة أساسية على التكنولوجيا الرقمية في تخزين البيانات والمعلومات، بالإضافة لاستخدام الحاسب الآلي في تطوير الصناعات وتحريك الاقتصادات، وأصبحت المعاملات المالية والاقتصادية محوسبة، وباتت شبكات البنوك والبورصات وشركات الأسواق المالية مرتبطة ببعضها البعض بنظم و شبكات الكترونية، فأصبحت الإنترنت هي أساس المعاملات المالية والاقتصادية وباتت تشكل محورا رئيسيا للتطور الاقتصادي في القرن الحادي والعشرين، وهو ما أثار الحديث عن أهمية تحقيق الأمن السيبري في المجال الاقتصادي[2].

2- البعد السياسي: تسبب البعد السياسي للأمن السيبراني ، مثل التسريبات المختلفة للوثائق الحساسة ، في مشاكل في العلاقات بين الدول وجعل من الضروري للدول إعادة النظر في سياساتها الخارجية. والدور البارز للشبكات الاجتماعية في تحقيق الأهداف السياسية ، مثل تنظيم الأحداث الانتخابية أو المظاهرات الافتراضية وحركات الاحتجاج الإلكترونية بالإضافة إلى نشر رسائل سياسية على شبكات التواصل الاجتماعي[3].وتم الكشف عن العديد من الأنشطة الإرهابية في هذه المواقع[4]. مجالا لتجنيد أفرادها وجمع التمويل لعملياتها، واستخدامه كوسيط في الاتصال بين هذه الحركات، مما استجوب على الدول العمل على حماية أمنها الداخلي من التهديدات.

---

[1]- سمير بارة، الأمن السيبراني (Cyper Security) في الجزائر السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، المجلد02، العدد02، جويلية 2017، ص260.

[2]- عبدالفتاح بيومي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، مصر، المحلة الكبرى، البعة الأولى، دار الكتب القانونية، 2007، ص 198.

[3]- في بعض الدول مثل الولايات المتحدة. وسائل الإعلام لتحقيق أهدافها، على سبيل المثال، طور الجيش الأمريكي برنامجًا موقعًا إلكترونيًا لإطلاق حسابات شخصية على مواقع التواصل الاجتماعي بلغات مختلفة، بهدف نشر الرسائل الداعمة للرؤية الأمريكية على مواقع التواصل الاجتماعي. **أنظر** هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة الجرائم المعلوماتية (معلقا عليها)، دار النهضة العربية، الطبعة الأولى، القاهرة، 2007، ص 129.

[4]- المرجع نفسه، ص129.

3- البعد الاجتماعي: إن توعية جميع المشاركين في شبكات المعلومات الدولية بأهمية الفهم الصحيح للأمن، والخطوات الأساسية لتعزيز مستوى الأمن، إذا تمت صياغة هذه الخطوات بوضوح وتحديدها وتنفيذها بحكمة. ويتطلب مجتمع المعلومات المسؤول حملات إعلامية وتربية مدنية تغطي التحديات والمخاطر والتدابير الأمنية الوقائية والرادعة من أجل تثقيف جميع المواطنين. وينبغي التأكيد على الالتزامات الأمنية والمسؤولية الشخصية وتدابير الردع، وكذلك عواقب القانون الجنائي المحتملة لعدم الامتثال للالتزامات الأمنية. بشكل عام فهناك حاجة لتوفير التعليم والتدريب في مجال تكنولوجيا المعلومات والاتصالات، وليس فقط في تدابير الأمن والردع. كما يجب غرس ثقافة الأمن في ثقافة تكنولوجيا المعلومات، ومن الضروري تطوير مجموعة من الأخلاقيات الأمنية التي يتم قبولها واحترامها من قبل جميع العاملين في الفضاء السيبراني[1].

4- البعد القانوني: العلاقة بين القانون والتكنولوجيا علاقة تبادلية، حيث تواكب التطورات التكنولوجية المختلفة التشريعات القانونية، من خلال وضع أطر وتشريعات للسلوك القانوني وغير القانوني، ولكن بشكل عام هناك حاليًا نقص في القوانين الصارمة للجرائم السيبرانية. ربما بسبب عوامل مثل طبيعة هذه الجرائم نفسها، وصعوبة تحديد مرتكبي هذه الجرائم، ومرونة التعريفات المتعلقة بتكنولوجيا المعلومات، فإن الجريمة السيبرانية لا تعرف حدودًا وطنية، الأمر الذي يتطلب بدء تعاون دولي مشترك لمكافحتها[2].

بعد تعرضنا إلى مفهوم الامن السيبراني وإلى نشأته وأبعاده سنرى المضامين المفاهيمي المرتبطة به والتحديات التي يمثلها وهي أهدافه في الموالي.

المبحث الثاني: الأمن السيبراني (المصطلحات المرتبطة به ،التحديات، الأهداف)

للأمن السيبراني مفاهيم مرتبطة به، فهي تشترك معه من حيث التسمية ومن حيث الوظيفة لكن هناك اختلافات فكل منها تتميز عن غيرها في المعنى والمدلول، وبعضها تحديات للأمن السيبراني، ومنها يبتغي الامن السيبراني منها أهدافا يسعى لتحقيقها لتوفير الحماية السيبرانية.

المطلب الاول: المفاهيم المرتبطة بالأمن السيبراني

تتعدد المصطلحات والمفردات المرتبطة بالأمن السيبراني وهي كثيرة لكن سنتطرق إلى أهم هذه المصطلحات في الفرع الموالي.

[1]- حمدون توريه، دليل الأمن السيبراني في البلدان النامية، الاتحاد الدولي للاتصالات، 2007، ص 16-17.

[2]- إدريس عطية، مرجع سابق، ص106.

الفرع الاول: مصطلحات مرتبطة بالأمن السيبراني

1-**الفضاء السيبراني:** وعرفته الوكالة الفرنسية لأمن أنظمة الإعلام ANSSI، وهي وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي، بأنه: "**فضاء التواصل المشكّل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية**". وهو وسط بيئي تفاعلي مستجد، تشمل عناصر المعنوية والمادية، مركب من بعض المعدات الالكترونية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مستخدمين أو مستهلكين. كما أن هناك مَن عرّف الفضاء السيبراني بوصفه الذراع الرابعة للجيوش الحديثة.

2- **الجريمة السيبرانية:** "**مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة إلكترونية أو شبكة الإنترنت أو تبث عبرها محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها**". وهي الجريمة التي لها علاقة بالحاسب الالي، أي تصرف غير مشروع يرتكب باستعمال تكنولوجيات المعلومات والاتصالات[1].

وقد عرفت الجريمة السيبرانية بأنها: " **هي التي تتم بواسطة الكمبيوتر أو أحد وسائل التقنية الحديثة على كمبيوتر آخر، مع ضرورة توفر شبكة اتصال فيما بينهما** "

والبعض الآخر عرفها بأنها" **نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود**". ومنهم من عرفها بأنها هي السلوك غير المشروع أو المنافي للأخلاق أو غير المسموح به المرتبط بالشبكات المعلوماتية العالمية فهي جرائم العصر الرقمي التي تطا بالمال والمعرفة والثقة والسمعة، وهي كلها تنفذ عن طريق التقنية[2].

3- **الردع السيبراني:** يعرف على أنه: " **منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية** "، يقوم الردع السيبراني على ثلاث ركائز في مجال سياسة الدفاع متمثلة في مصداقية الدفاع؛ بتوافر نظم معلومات لنسخ إحتياطية، و الإستطاعة على الرد؛ و ذلك بخسران المهاجم بأضرار أكبر من المدافع، فالقدرة على الإنتقام لا تكفي وحدها.

4- **الهجمات السيبرانية** :هي" **فعل يقوض من قدرات وظائف شبكة الكمبيوتر، الغرض قومي أو**

[1]- فارس قرة، الأمن السيبراني – Cyber Security، الموسوعة السياسية، بدون تاريخ النشر، على الموقع: https://political-encyclopedia.org/dictionary/ تاريخ التصفح:03 جوان 2022، على الساعة 10:25سا.

[2]- زينب ياقوت، دور الاعلام الجزائري في التصدي للجريمة السيبرانية قناة النهار انموذجا، مجلة طبنـة للدراسات العلمية الأكاديمية المجلد 5, العدد 1, الصفحة 1362-1379، جوان 2022، ص1368.

سياسي، من خلال استغلال نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام[1].

5-**القوة السيبرانية:** عرفها جوزيف ناي على أنها "**مجموعة الموارد المتعلقة بالتحكم و السيطرة على أجهزة الحاسبات و المعلومات و الشبكات الإلكترونية، و البنية التحتية المعلوماتية و المهارات البشرية المدربة للتعامل مع هذه الوسائل** ". وتجدر الاشارة أن القوة السيبرانية أخذت دفعا مهما في اتجاهين؛ الأول، تدعيم القوة الناعمة للدول من خلال التأثير في توجهات الرأي العام، و الثاني، يندرج في زيادة النفقات من طرف الدول لسياسات الدفاع السيبراني.

6- **الصراع السيبراني:** مع انتشار الفضاء السيبراني وسهولة الدخول، اتسع نطاق النزاعات السيبرانية وازداد عدد المهاجمين. وهناك عاملان رئيسيان لتوسع النزاعات السيبرانية: أحدهما هو التغيير الأساسي في منظور الحرب؛ والنمط التحولات بين الناس. ثانيًا ، ظهور النزاعات على المستويين المحلي والدولي، وزيادة حدة النزاعات الداخلية وبؤر التوتر بعد الحرب الباردة، كما يوفر السياق الدولي للفضاء السيبراني بيئة مفتوحة للقوى المهمشة في السياسة الدولية.[2]

7-**أمن المعلومات:** يشمل الأمن الحفاظ على سرية المعلومات والبيانات التي يعلقها مستخدمو الإنترنت على مواقع التواصل الاجتماعي وجميع المنصات الإلكترونية، ويستمر في تشكيل حماية المعلومات والبيانات الشخصية من أي محاولة اختراق للنظام الإلكتروني أو التجسس الإلكتروني. وزادت حماية المعلومات من استخدامها مع تطور الإنترنت والتوسع في أساليبها وأنواعها. أمن المعلومات له أنواع أساسية من المعالجة وهي: نظام حماية نظام التشغيل و نظام حماية البرامج والتطبيقات و نظام الحماية البرامجية والإلكترونية والدخول و نظام حماية الخروج[3].

بعد تعريفنا للمفهومين الأمن السيبراني والأمن المعلومات يجب أن نبحث عن العلاقة بينهما.

---

[1]- رغدة البهي، الردع السيبراني: المفهوم و الإشكالات و المتطلبات ، مجلة العلوم السياسية و القانون ، المجلد 01، العدد 01 ، جانفي 2017، ص 53-52.

[2]- يوسف بوغرارة، مرجع سابق، ص 108.

[3]- سايبر وان، ما هو الفرق بين أمن المعلومات والأمن السيبراني؟،25-05-2021 ، https://cyberone.com/، تاريخ التصفح:04 جوان2022 على الساعة 21:32 سا.

الفرع الثاني: الفرق بين الأمن السيبراني والأمن المعلوماتي

التعريف الاصطلاحي للمعلومات: يمكن تعريفها انها: "**مجموعة من الرموز أو الحقائق أو المفاهيم او التعليمات التي تصلح لأن تكون محلا للتبادل والاتصال أو التفسير أو التأويل أو المعالجة، التي تتم بواسطة الأفراد أو الأنظمة الالكترونية**"[1].

العلاقة بين أمن المعلومات والأمن السيبراني هي علاقة جزئية، حيث يتضمن أمن المعلومات حماية المعلومات من الوصول غير المصرح به. وقد تكون المعلومات في شكل مستندات ورقية أو مخزنة على وسائط إلكترونية. ولكن لا يمكننا أبدًا أن نقول إن أمن المعلومات يشمل أمان الشبكة تمامًا، كما لا يمكننا القول أن أمان الشبكة يتضمن أمان المعلومات. ويشمل الأمن السيبراني أمن المعلومات المنقولة أو المخزنة أو المعالجة في أنظمة تكنولوجيا الاتصالات والمعلومات. هذا صحيح ، لكنه يشمل أيضًا الحفاظ على توافر وأمن الخدمات المقدمة عبر الفضاء السيبراني، مثل الطاقة الكهربائية ووسائل الاتصال، لذلك لا يصح القول إن أمن المعلومات يشمل الأمن السيبراني، وليس من الصحيح القول بذلك يشمل الأمن السيبراني أمن المعلومات، لأنه لا علاقة له بأمن المعلومات المكتوبة على المستندات الورقية، وذلك لأنه لا ينتمي إلى نطاق الفضاء السيبراني[2]. إذن العلاقة بين أمن المعلومات والأمن السيبراني هي التقاطع من حيث الإهتمام بأمن المعلومات الموجودة بالسايبر، ويختلفان فيما تبقى من الإهتمامات، وانتبه في نفس الوقت لا تستطيع استخدام أمن المعلومات والأمن السيبرانى كمصطلحين مترادفتين تماماً[3].

المطلب الثاني: التحديات التي يمثلها الأمن السيبراني وأهدافه

نظرا للمخاطر المتنوعة والمتطورة نتيجة تطور هذه الجرائم المستحدثة، فان الامن السيبراني تنظره تحديات، وهذه التحديات سنشرحها في الفرع الموالي.

الفرع الأول: التحديات التي يمثلها الأمن السيبراني

إن القضايا الاجتماعية والاقتصادية والسياسية والإنسانية، حيث يؤثر الأمن السيبراني على أمن الثروة الرقمية والثقافية للأشخاص والمنظمات والدول، بغض النظر عن الجانب الذي يحقق فيه الشخص

[1]– طارق ابراهيم الدسوقي عطية، الامن المعلوماتي (النظام القانوني للحماية المعلوماتية)، دار الجامعة الجديدة للنشر، طبعة 2009، ص38.

[2]– احمد عبد الكريم عبد الوهاب، محمود عبدالرحمن خلف، اشكالية المن السيبراني العراقي بين التهديدات السيبرانية والتقنين المقيد للحريات، مجلة دراسات السياسية، كلية العلوم السياسية، جامعة النهرين، العدد60، 2020، ص4.

[3]– مصطفى الطيب، الفرق بين أمن المعلومات و الأمن السيبراني، مدونة علوم، على الرابط التالي: https://www.oolom.com/6124/ تاريخ التصفح: 05 حوان2022، على الساعة 18:05 سا.

رؤيته، أو كيف تتغير أسمائهم. وبدلاً من ذلك، فإن التحديات التي ينطوي عليها الأمر معقدة، ويتطلب التصدي لها الإرادة السياسية اللازمة لتصميم وتنفيذ استراتيجيات لتطوير البنية التحتية والخدمات الرقمية، بما في ذلك استراتيجيات الأمن السيبراني المتماسكة والفعالة والقابلة للتحقيق. ويجب أن تكون استراتيجية الأمن السيبراني جزءًا من نهج متعدد التخصصات، مع حلول متاحة بسهولة على المستويات التعليمية والقانونية والفنية والإدارية. ويمكن للاستجابة القوية للجوانب البشرية والقانونية والاقتصادية لاحتياجات أمن البنية التحتية الرقمية أن تبني الثقة وتولد نموًا اقتصاديًا مرغوبًا يفيد المجتمع ككل. الفجوة الرقمية اقتصادية واجتماعية وتنطوي على أكثر من مجرد نهج أحادي البعد وتقني للأمن السيبراني[1]. فحدود الأمن السيبراني متعددة الأوجه منها الطبيعة المتطورة للإرهاب السيبراني. على الرغم من حجم وتوزيع الخطط الداخلية فقد تكون أكبر تهديد في بيئة إفتراضية، فأثر الإرهاب ونطاقه على الدول والأمم من خلال الشبكات الإجرامية، ولا يوجد فرق كبير بينهم نظرا لانتشار الجريمة السيبرانية والتجسس الالكتروني والإرهاب السيبراني، فلهم نفس القدرات في الهجوم السيبراني[2].

أن الهدف من الأمن السيبراني حماية أمن الدول والحكومات والمؤسسات والشركات العامة والخاصة، من كل تهديد يشكل خطر على أمنها ووجودها ويجعلها عرض للمخاطر السيبرانية، كما أن الأمن السيبراني ضرورة حتمية تهم الجميع حت الفرد في قضاء مصلحته، لذا وجب منا التصدي لهذه التهديدات سد الفراغ وغلق الطريق أمام المجرم السيبراني والجناة من الوصول إلى مبتغاهم والإفلات من العقاب. ومن أهدافه أيضا سنتطرق لها في الفرع الموالي.

الفرع الثاني: أهداف الأمن السيبراني

إن أهم هدف للأمن السيبراني هو حماية وتأمين المعطيات والبيانات وحماية الشبكات وأجهزة الكمبيوتر والبرمجيات من أي اختراق سيبراني والوصول غير المصرح به إلى البيانات، وأصبح الغرض من الأمن السيبراني له مهمة الدفاع والقدرة في صد أي هجوم سيبراني في الحرب السيبرانية، وذلك لحماية البنية التحتية من أجل سلامة المواطنين وممتلكاتهم الإلكترونية ونلخص ذلك فيما يلي:

1- تأمين البنى التحتية لأمن المعطيات والبيانات الخاصة بالافراد، لا بد من حماية فعالة لجميع ما يتعلق بمعلومات الأشخاص وحفظها حفظا امنا، والأجهزة ومواردنا وغيرها من ممتلكات إلكترونية من أي محاولة عبث أو اختراق أو تعديل لتحقيق الحماية اللازمة.

[1]- نبراس ابراهيم مسلم، الجرائم السيبرانية وأثرها على الامن السيبراني، مجدلة القادسية للقانون والعلوم السياسية، المجلد12، العدد 01، حزيران 2021، ص381.

[2]- Henry, Shawn, and Aaron F. Brantly. "Countering the Cyber Threat." The Cyber Defense Review 3, no. 1 (2018): 47–56, p49. http://www.jstor.org/stable/26427375 .

2- حماية شبكات المعلومات والاتصالات، التي تلعب دورًا مهمًا في تدفق البيانات بين المواطنين والدولة ومن جهة إلى أخرى ، والتي إذا تعرضت للخطر أو تم اختراقها أو اختراقها، يمكن أن تؤثر حتما على هذه الاتصالات وتعطلها، وتوقف تدفق البيانات. العمل وإيقاف الخدمة[1].

3- حماية شبكة المعلومات من أي هجوم من خلال معرفة أحدث التقنيات والحيل في هذا المجال وأهمها كشف الهدف من رسالة هذا العدو والتعرف على طبيعة هذا المهاجم وما هي طبيعة هذا المهاجم و ما يريده من أجل العمل على منع مثل هذه الاعتداءات بطرق علمية وتقنية.

4- تشفير المعاملات الإلكترونية بحيث لا يتمكن المتسللون من الوصول بسهولة إلى هذه البيانات والتطبيقات، لأن التشفير وسيلة حماية يصعب فك تشفيرها. هذه هي الأساسيات، أعتقد أن كل مواطن يجب أن يعرفها وأن يكون على دراية بها، لأنها مرتبطة بحياتنا وسلامتنا الشبكة ، فماذا يجب على المجتمع أن يفعل إذا عانى من مثل هذه الاعتداءات في هذه الخدمات الإلكترونية وتسبب في تعطيلها[2].

الخاتمة:

على ضوء ما تقدم فإن النتائج المتوصل إليها في دراستنا لموضوع الأمن السيبراني والمضامين المفاهيمي المرتبطة به، باختصار فإن النتائج التي توصلنا إليها حول موضوع الأمن السيبراني والآثار المفاهيمية المرتبطة به ، بشكل عام ، من الضروري التركيز على أهمية الأمن السيبراني ، خاصة أنه أحد التخصصات المتعلقة بحماية أجهزة الكمبيوتر والهواتف المحمولة وكذلك حماية ممارسة حماية البيانات من أي تجسس أو هجمات خارجية ، حيث قد يؤدي ذلك إلى انتهاك الخصوصية. ويعد فقدان المعلومات وابتزاز الموظفين من بين التحديات التي يفرضها الأمن السيبراني. لذلك فإن الأمن السيبراني مهم للغاية لأنه مصدر الأمن لجميع الوسائل التكنولوجية، ومن أهدافه إدراك أهميته ومساعدة الناس على فهم الأساليب الضرورية لحماية المعلومات التي يجب عليهم اتباعها. كما أصبح الأمن السيبراني ركيزة مهمة للأمن تحظى بتقدير كبير من قبل الدول والمنظمات، مع الحفاظ على السيادة الوطنية والأمن السياسي والاستقرار كأولوية قصوى، لأن المخاطر السيبرانية أصبحت تشكل تهديدًا على المستويين الدولي والوطني، **وبناءا على هذه النتائج فإننا نقترح مجموعة من المقترحات التالية:**

1- نشر على المستويين الدولي والوطني ثقافة الوعي بالأمن السيبراني؛

2- إنشاء وكالة وطنية للأمن السيبراني وحماية البنية التحتية للبيانات؛

[1]- جوهر الجموسي ، الافتراضي والثورة: مكانة الإنترنت في نشأة مجتمع مدني عربي، المركز العربي للأبحاث ودراسة السياسات ، بيروت ، 2019، ص120 .

[2]- فيصل محمد عسيري، مرجع سابق، ص6. التالي: https://www.kutub.info/library/book

3- الاستفادة من خبرات الدول المتقدمة في مكافحة هذه الجرائم والاستفادة منها مع النظر في اعتماد التعاون التشريعي والقضائي، مع الحفاظ على مبدأ السيادة الوطنية، لتحقيق مبادئ ومعاهدات الأمن السيبراني القائمة على الاتفاقيات المشتركة؛

4- اعتماد نظام دولي قائم على التعاون بين دول العالم التي تعمل معًا ضمن إطار سياسي موحد وإطار تشريعي وتنظيمي متماسك؛

5-تفعيل دور الإجراءات المستحدثة الوقائية من خلال مؤسسات التوعية للحد من الجريمة السيبرانية قبل وقوعها.

قائمة المصادر والمراجع:

أولا: النصوص القانونية:

1. القانون 04-15، المؤرخ في 10 نوفمبر 2004، الصادر في الج.ر.ج رقم: 71، المتضمن تعديل قانون العقوبات لسنة 2004، ص. ص: 11 و12، والذي أضيفت بموجبه المواد من 394 مكرر إلى 394 مكرر 07.
2. القانون رقم 09 - 04، المؤرخ في 14 شعبان عام 1430، الموافق 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المنشور بالج.ر.ج العدد 47 بتاريخ 16 غشت سنة 2009.
3. القانون رقم 18-04 المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الصادر في الج.ر.ج العدد 27، بتاريخ 13 مايو 2018، ص 03.
4. القانون 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الصادر في الج.ر.ج العدد34، في 10 يونيو 2018.

ثانيا: الكتب

5. احمد عبيس نعمه الفتلاوي: الهجمات السيبرانية، دراسة قانونية تحليليه بشان تحديات تنظيمها المعاصر، الطبعة الأولى، منشورات زين الحقوقية، بيروت، 2018.
6. اشرف محمد عبدة، البيئة الامنية للحكومة الإلكترونية(بين المخاطر ومتطلبات الامن والحماية) دار الكتب والدراسات العربية، لإسكندرية، 2018.

7. جوهر الجموسي، الافتراضي والثورة: مكانة الإنترنت في نشأة مجتمع مدني عربي، المركز العربي للأبحاث ودراسة السياسات، بيروت، 2019.
8. طارق ابراهيم الدسوقي عطية، الامن المعلوماتي (النظام القانوني للحماية المعلوماتية)، دار الجامعة الجديدة للنشر، طبعة 2009.
9. عبدالفتاح بيومي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، مصر، المحلة الكبرى، الطبعة الأولى، دار الكتب القانونية، 2007.
10. منى الأشقر جبور، السيبرانية هاجس العصر، دراسات وأبحاث، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، بيروت،2016.
11. هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة الجرائم المعلوماتية (معلقا عليها)، دار النهضة العربية، الطبعة الأولى، القاهرة، 2007.

ثالثا: الرسائل والمذكرات

12. بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتوراه علوم تخصص قانون عام، كلية الحقوق، جامعة الجزائر 1 بن يوسف بن خدة ،2018.
13. بلال بن جامع، الجرائم المعلوماتية على شبكة الانترنت دراسة حالة جامعة عبدالحميد مهري قسطنينة2، رسالة دكتوراه، معهد علم المكتبات والتوثيق، جامعة عبدالحميد مهري قسنطينة2، 2016-2017.

رابعا: المقالات

14. احمد عبد الكريم عبد الوهاب، محمود عبدالرحمن خلف، اشكالية المن السيبراني العراقي بين التهديدات السيبرانية والتقنين المقيد للحريات، مجلة دراسات السياسية، كلية العلوم السياسية، جامعة النهرين، العدد60، 2020.
15. احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل، كلية القانون، العدد04، السنة 08، 2016.
16. إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة مصداقية، كلية الحقوق والعلوم السياسية-جامعة العربي التبسي، تبسة، الجزائر، المجلد01، العدد01، 2019.
17. أسعد طارش عبد الرضا، علي إبراهيم مشجل المعموري، الأمن السيبراني ودوره في إنتشار ظاهرة الإرهاب في العراق بعد عام 2003، مجلة دراسات دولية، العدد 80، يناير 2020.

18. أوس مجيد غالب العوادي، الامن المعلوماتي السيبراني، في حصاد البيان8، سلسلة إصدرات مركز البيان للدراسات و التخطيط، بغداد، 2016.
19. جمال بوازدية، الإستراتيجية الجزائرية في مواجهة السيبرانية" التحديات والأفاق المستقبلية"، مجلة العلوم القانونية والسياسية ،المجلد10،العدد01، أفريل2019.
20. خلوف حسام، باطلي غنية، الآليات القانونية لحماية المعطيات ذات الطابع الشخصي، مجلة الدراسات القانونية والإقتصادية، المجلد05، العدد01، 2022.
21. رغدة البهي، الردع السيبراني: المفهوم و الإشكالات و المتطلبات ، مجلة العلوم السياسية و القانون، المجلد01، العدد01 ، جانفي 2017.
22. سمير بارة، الأمن السيبراني (Cyper Security) في الجزائر السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، المجلد02، العدد02، جويلية 2017.
23. علي عبدالرحيم العبودي، هاجس الحروب السيبرانية وتداعياتها على الامن والسلم الدوليين، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، العدد57، 2019.
24. نبراس ابراهيم مسلم، الجرائم السيبرانية وأثرها على الامن السيبراني، مجدلة القادسية للقانون والعلوم السياسية، العدد 01، المجلد 12 حزيران 2021.
25. زينب ياقوت، دور الاعلام الجزائري في التصدي للجريمة السيبرانية قناة النهار نموذجا، مجلة طبنـة للدراسات العلمية الأكاديمية المجلد05, العدد01, الصفحة 1362–1379، جوان 2022،

خامسا: أشغال الملتقيات

26. حمدون توريه، دليل الأمن السيبراني في البلدان النامية، الاتحاد الدولي للاتصالات، 2007.

سادسا: المواقع الإلكترونية

27. سايبر وان، ما هو الفرق بين أمن المعلومات والأمن السيبراني؟،25 ماي2021 متاح على الرابط التالي: https://cyberone.com، تاريخ التصفح:04 جوان2022 على الساعة 21:32 سا.
28. فارس قرة، الأمن السيبراني، الموسوعة السياسية، بدون تاريخ النشر، على الموقع: https://political-encyclopedia.org/dictionary ، تاريخ التصفح:03جوان2022، على الساعة10:25
29. فيصل عسيري، الأمن السيبراني وحماية المعلومات، ورقة بحثية متاحة على الرابط التالي: https://www.kutub.info/library/book/21854، تاريخ التصفح 30 ماي2022،على الساعة21:24 .
30. مصطفى الطيب، الفرق بين أمن المعلومات و الأمن السيبراني، مدونة علوم، على الرابط التالي: https://www.oolom.com/6124/تاريخ التصفح:05 جوان2022، على الساعة 18:05 سا.

قائمة المراجع باللغة الأجنبية:

31. Syed, Rubab, Ahmed Awais Khaver, and Muhammad Yasin. "WHAT IS CYBER SECURITY?" Cyber Security: Where Does Pakistan Stand? Sustainable Development Policy Institute, 2019. http://www.jstor.org/stable/resrep24376.5

32. Henry, Shawn, and Aaron F. Brantly. "Countering the Cyber Threat." The Cyber Defense Review 3, no. 1 (2018): 47–56,. http://www.jstor.org/stable/26427375 .