و اقع الامن السيبراني في الجزائر
THE reality of cybersecurity in Algeria

عدائكة أسماء*[1]، بوعسلة بشرى [2]

[1]جامعة الشهيد حامة لخضر ، (الوادي)، adaika-asma@univ-eloued.dz

[2]المدرسة العليا لعلوم التسيير ، (عنابة)، bouasla.bouchra@essg-annaba.dz

ملخص:

في الوقت الراهن يعتبر العالم كقرية صغيرة نظرا لاعتماده على الأدوات و الخدمات المستندة إلى الانترنت و الأجهزة الذكية ، بحيث أصبح من الضروري في وقتنا الحالي الانتباه إلى قضية الامن المعلوماتي السيبراني وكيفية حماية قاعدة البيانات والمعلومات، و الجزائر كغيرها من الدول و في ظل التوجه الدولي نحو الإدارة الالكترونية سعت في حماية منظومتها المعلوماتية من خلال الأجهزة والخليا الأمنية .

تهدف دراستنا إلى التعرف عن واقع الامن السيبراني في الجزائر و التعرف على التهديدات و عوائق تحقيق الامن السيبراني في ظل التحديات الانية و المستقبلية .

الكلمات المفتاحية : الامن السيبراني ، الامن المعلوماتي ، الجريمة الالكترونية ،.....

Abstract:

Currently the world is considered a small village due to its reliance on Internet- based tools and smart devices, it has become necessary to pay attention to the issue of cyber security and how to protect the database and information, Algeria, like other countries, and in line of the international trend towards electronic management, has sought to protect its information system through security devices and measure**.**

This study aims to understand the state of cyber security in Algeria and to identify the threats and obstacles to achieving cyber security in light of current and future challenges**.**

Keywords: Cyber security, information security, electronic crime

1 – مقدمة :

شهد القرن الأخير ثورة هائلة في تكنولوجيا الإعلام والاتصال، حتى أن بعض الخبراء صنفوا المجال السيبراني كميدان خامس للنزاعات بعد الأرض، البحر، الجو، والفضاء. يعود ذلك إلى الانتشار السريع لهذه التقنية، التي أصبحت أساساً في مختلف مجالات الحياة. مع التحول نحو الخدمات الإلكترونية التي قلصت الجهد والوقت والتكلفة، وساهمت في تلبية الاحتياجات بمرونة، جاءت الإنترنت بمخاطرها، متمثلة في جرائم إلكترونية تهدد الأشخاص والمؤسسات والدول، وأثرت بشكل كبير على استقرار الدول.

تخصص الأمن السيبراني في الجزائر يشهد نموًا متسارعًا بفضل التطورات المحلية والعالمية في هذا المجال، ويُتوقع أن يكون هذا التخصص أحد أهم الخيارات المستقبلية للشباب الجزائري. إذا كنت مهتمًا بحماية البيانات والنظم والشبكات، فإن هذا التخصص قد يكون الخيار المثالي لك

في ظل تزايد الهجمات السيبرانية على مستوى العالم، بدأت الجزائر في اتخاذ خطوات حثيثة لتعزيز أمنها السيبراني، تمثل هذه الخطوات جزءًا من استراتيجية وطنية تهدف إلى بناء بنية تحتية قوية للأمن السيبراني. ومن بين هذه الخطوات البارزة، افتتاح مدرسة جديدة متخصصة في الأمن السيبراني تهدف إلى تلبية الحاجة المتزايدة للخبراء في هذا المجال وتقديم برامج تعليمية متقدمة تغطي أحدث التقنيات وأساليب الحماية وهذا التطور يعكس التزام الجزائر بتعزيز قدراتها في مواجهة التهديدات السيبرانية، من خلال الدراسة التي قمنا بها نطرح التساؤلات التالية :

- هل تمتلك الجزائر إستراتيجية لتحقيق أمنها السيبراني ؟
- ماهي أهم المعوقات و التحديات التي تواجه الجزائر لتحقيق أمنها السيبراني ؟

I. الاطار العام للدراسة

تنفّذ المؤسسات استراتيجيات الأمن السيبراني من خلال العمل مع متخصّصين في الأمن السيبراني. يقيّم هؤلاء المتخصصون المخاطر الأمنية لأنظمة الحوسبة الحالية، والشبكات، ومخازن البيانات، والتطبيقات، والأجهزة المتصلة الأخرى. بعد ذلك، ينشئ متخصصو الأمن السيبراني إطار عمل شامل للأمن السيبراني وينفّذون تدابير وقائية في المؤسسة .

لضمان نجاح برنامج الأمن السيبراني، يجب إعلام الموظفين في سياقه بأفضل الممارسات الأمنية واستخدام تقنيات الدفاع السيبراني الآلية في البنية الأساسية الحالية لتكنولوجيا المعلومات. تعمل هذه العناصر معًا لإنشاء طبقات متعددة من الحماية ضد التهديدات المحتملة على جميع نقاط الوصول إلى البيانات. فهي تحدّد

المخاطر، وتحمي الهويات والبنية الأساسية والبيانات، وترصد أوجه الخلل والأحداث، وتستجيب وتحلل السبب الجذري، وتتعافى بعد وقوع الحدث.

1. **تحديد المفاهيم:**

1.1. **الامن المعلوماتي information security**: هو الامن الذي يهتم بالمحافظة على سرية المعلومات البيانات التي يرفقها مستخدم الانترنت على مواقع التواصل الاجتماعي وكافة المنصات الالكترونية ومتابعة في تشكيل أنظمة إلكترونية تحمي المعلومات و البيانات الشخصية من أي اختراق أو تجسس الكتروني [1]

- **أهدافها**: يمكن حصر الأمن المعلوماتي:

-التأكد باستمرار من أن المعلومات المتوفرة وبعيدة عن أي تهديد قد يعرضها للتلف أو التعديل أو السرقة ،

-التأكد من سرية المعلومات و الهدف منها أن تكون المعلومات المتوفرة للتأكد من سلامتها من أي خطأ قد يطرأ عليها

-التأكد من صحة المعلومات بهدف مراجعة المعلومات المتوفرة للتأكد من سلامتها من أي خطأ قد يطرأ عليها ،

-قواعد ومخاطر و أساليب مواجهة مخاطر الامن السيبراني.

- **قواعد الامن المعلوماتي** : تتمثل في

- سرية المعلومات و سلامتها ،
- سلامة المعلومات أو المحتوى.

2.1 .**الامن السيبراني Cyber security**: هو حماية الأنظمة و الشبكات و الأجهزة من الهجوم الالكتروني و الرقمي أي أن الامن السيبراني يتشكل من مجموعات معلومات وعمليات رقمية تهدف إلى الوصول إلى البيانات و المستندات الرقمية وتشكيل سد الكتروني يحميها من محاولت اختراق أو تجسس[2].

ويظهر هذا النوع أكثر في المجال العلمي و الصناعي الذي يتهدف فيه المؤسسات إلى إفشال منافسيها لكي تحضى بتفوق على المؤسسة المنافسة ورقم تنوع استخدام هذا النوع من الامن إلا انه قد اثبت أن هذا النوع تحديدا من أنواع الإلكتروني يحتاج إلى خبرة مضاعفة و إلى المام إلكتروني من كل الجهات

[1] دحان عزام ناصر القريطي ، الامن السيبراني و حماية المعلومات ،الإسكندرية ،دار الفكر الجامعي ، الطبعة الأولى 2021 ص 7.

[2] عبد الوهاب لطفي الراوي ، إستراتيجية تحقيق الامن المعلوماتي بين آلية معالجة التغرات و التشفير و مسؤولية حماية البيانات عبر الانترنت في ظل حوكمة تكنولوجيا المعلومات و الاتصالات ، الإسكندرية ، دار الفكر الجامعي ، الطبعة الأولى ،2022.

يعتمد الامن السيبراني إضافة إلى دور المختصين و المهندسين الالكترونيين على وعي المستخدم نفسه و ذلك لان العديد من الجهات ترفق توعية وثقافة إلكترونية تساهم في تقليل نسبة تعرض الشخص لمحاولات ابتزاز أو وقوع في شبكة الجرائم الالكترونية ، وكلما جدد المستخدم مخزون المعلومات لديه صار اكثر حصانة وبعدا عن الوقوع في مشكلات الكترونية.

الامن السيبراني يعتمد على 3 نقاط أساسية و هي:

- أجهزة الكمبيوتر و الأجهزة الذكية
- الشبكات
- السحابة الالكترونية

الجدول : توضيح الفرق بين امن المعلوماتية و الامن السيبيراني

وهذا بالضبط ما يفتح لنا مجال المقارنة بين أمن المعلوماتية و الامن السيبراني والمتمثل فيمايلي:

الامن المعلوماتي	الامن السيبراني
يهتم بحماية البيانات المرفقة أصلا على المنصات الالكترونية	يهتم في أن لاتخترق هذا المعلومات ولا تستخدم أصلا من قبل الجهة التي تحفظها أي أنه يطبق على المستخدم شروط خصوصية التي تحددها الشركة
يؤكد الحفاظ على المعلومات المتعلقة بالتطبيق	يمنع عمليات الوصول غير الشرعي لهذه المعلومات من قبل جهات غريبة تحاول ذلك حتى و إن أرفقت البيانات على حستبك الشخصي بهدف حمايتك من عمليات الابتزاز
يقوم بحفظ كافة بياناتك عندما توافق على شروط استخدام التطبيق الالكتروني	يمنع التطبيق ذاته من التجسس عليك أو ابتزازك و تتبعك من خلال اهتماماتك و متابعاتك على منصات التطبيق
أمن المعلومات من الممكن أن يكون عرضة للاختراق عند استخدام أنظمة تجسس واختراق و فيروسات	الامن السيبراني يشكل نظاما إلكتروني يحمي الأجهزة نفسها من استقبال أي نوع من أنواع الفيروسات و يتم تبليغ المستخد بها ليقوم بالخطوات المناسبة لحماية بياناته من إمكانية السرقة
من الممكن أن يحمي الصور والبيانات عن الأشخاص المصنفين عامة على مواقع التواصل الاجتماعي لدى المتسخدم	إمكانية تتبع المخترق الالكتروني و عرفة هويته الشخصية و تجميع المعلومات عنه فيما يضمن بناء لائحة اتهام كاملة للمخترق معترف بها قانونيا
يمكنه تبليغك بمحاولة اختراق إلكتروني لاحدى منصاتك أو مخازن البيانات التي بحوزتك	يك تحديد بيانات و هويات الأشخاص المخترقين الشرعيين و غير الشرعيين و الوصول إليهم

المصدر: سامح عبد المطلب عامر، علاء الدين ، **الاتصال الإداري الفعال:الفلسفة – التطوير** ،ص489.

3.1.بعض المفاهيم المتعلقة بالأمن السيبراني Some concepts related to cyber security:

من هنا نحاول التعرف على بعض التعاريف المرتبطة بالأمن السيبراني

- الدفاع السيبراني:

هو عملية تطبيق الإجراءات الأمنية من أجل حماية من الهجمات السيبرانية و التعامل معها بما تستهدف البنية التحتية لنظم الاتصالات و السيطرة

- الردع السبيراني

منع الاعمال الضارة ضد الأصول الوطنية في الفضاء الأصول التي تدعم العمليات الفضائية

- الجريمة السيبرانية

هو أي عمل ليست له في القانون أو أعراف قطاع الاعمال جزاء يضر بالاشخاص و الاموال أو يوجه ضد أو يستخدم التقنية المتقدمة العلية لنظم المعلومات

4.1. أهمية الأمن السيبرانيThe importance of SYBERSECURITY

يمكن تلخيص أهمية الامن السيبراني في نقاط التالية[3]:

- توفير الحماية الفائقة لخصوصية المعلومات و الابقاء على سريتها وذلك بعدم السماح لغير المخولين بالوصول إليها و استخدامها؛
- استكشاف نقاط الضعف و الثغرات في الانظمة و معالجتها الحفاظ على المعلومات و سلامتها و تجانسها وذلك بكف الايادي من العبث بها؛
- حماية الأجهزة والشبكات ككل من الاختراقات لتكون الدرع واقيا للبيانات و المعلومات؛
- تحقيق وفرة البيانات و جاهزيتها عند الحاجة إليها ،بإضافة لتوفير بيئة عمل آمنة جدا خلال العمل عبر الشبكة العنكبوتية؛
- توفير بيئة عمل آمنة جدا خلال العمل عبر الشبكة العنكبوتية.

الاستراتيجية الجزائرية لتحقيق الامن السيبراني:

قدم بلفر سبع أهداف وطنية تطلع بها الدولة تطلع بها أي دولة ومنها الجزائر لحماية أمنها السيبراني ،وهي:

[3] سامح عبد المطلب عامر ،علاء الدين محمد عوض ، الاتصال الإداري الفعال (الفلسفة ، التطوير ، المهارات، التقويم)،دار الفكر ،الطبعة الأولى ،2023،ص484.

- مسح و مراقبة المجموعات المحلية من خلال قيام الدولة ،من منطلق حماية أمنها القومي بالمراقبة الالكترونية لرصد و اكتشاف و جمع المعلومات الاستخبارية عن التهديدات المحلية و الجهات الفاعلة داخل حدودها؛
- تقوية و تعزيز الدفاعات السيبيرانية؛
- التحكم في بيئة المعلومات و معالجتها؛
- جمع المعلومات الاستخبارية من دول أخرى لحماية الامن القومي؛
- تحقيق مكاسب تجارية أو تعزيز نمو الصناعة المحلية ،فيمكن الدولة من خلال نشاطها السيبراني تنمية صناعة التكنولوجية المحلية الخاصة بدولة ما أو استخدام الوسائل التكنولوجية لتطوير الصناعات المحلية الأخرى؛
- تدمير أو تعطيل البنية التحتية للخصم كإستخدام دولة ما تقنيات و تكتيكات و إجراءات إلكترونية مدمرة؛
- تحديد القواعد و المعايير التقنية الالكترونية الدولية.

II. الإطار القانوني لتحقيق للأمن السيبراني في الجزائر Legal framework for achieving cyber security in Algeria:

تركزت الجهود الجزائرية لتحقيق الامن السيبراني أساسا في مجال الإجراءات القانونية دون غيرها من التدابير الأخرى، ويتضح ذلك من خلال صدور القانون رقم 09-04 المؤرخ في 05 أوت ،2009 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والتي تم فيه تحديد الحالات التي تسمح باللجوء إلى مراقبة الاتصالات الإلكترونية بناءا على ما ورد في المادة 4 التي نصت على ما يلي :

-للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة؛

-في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

كما نصت المادة 13 على إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وهذا ما تم من خلال صدور المرسوم الرئاسي رقم 15- 261 المؤرخ في 08 أكتوبر سنة 2015، والذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها . كما أنشأت الجزائر هيئات

أخرى تضطلع بأدوار جد هامة فى مواجهة مختلف الجرائم الالكترونية منها:

- مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني .
- المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني.
- المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني .29

وفي إطار إعداد الإستراتيجية الوطنية لأمن أنظمة المعلومات في الجزائر، تم إنشاء المجلس الوطني لأمن أنظمة المعلومات في الجزائر في مرسوم رئاسي رقم 05-20 بتاريخ 24 جمادى الأولى 1441 الموافق لـ 20 جانفي 2020 يحمل عنوان "جهاز وطني لأمن أنظمة المعلومات". [4]

ويأتي اهتمام الجزائر بإنشاء مثل هذه المؤسسات إلى تزايد معدلات الجرائم الالكترونية التي أصبحت تشكل تهديدا كبيرا على الأمن الوطني، فقد ارتفع معدل الجرائم الالكترونية في الجزائر بشكل كبير خلال السنوات الأخيرة حسب بعض التقارير الأمنية، يتعلق أبرزها بانتهاك الحريات

الشخصية، والتهديد عبر الانترنت، ونشر صور فاضحة الابتزاز ، والقرصنة الالكترونية وغيرها.

لحد الآن لا توجد مؤسسة مستقلة تتولى مهمة التأمين الالكتروني، فأغلب الجهود في هذا المجال تابعة لهيئات أمنية – مؤسسات الدفاع الوطني – كالدرك الوطني أو الجيش الشعبي الوطني، ورغم اعتباره إضافة يتوجب تثمينها كونها يضم بعداً جديداً في السياسة الدفاعية القومية الجزائرية، غير أن حصره في هذه المؤسسات قد يؤثر على جدوى تطوير سياسات كلية لمواجهة

التهديدات الالكترونية وعلى جهود مكافحة الجرائم السيبرانية المتعددة ، ويقلل من تحقيق أكبر قدر من الاستفادة من الفرص والإمكانات التي يوفرها الفضاء الالكتروني، والتي تبقى مقتصرة على الاستخدامات العسكرية والأمنية (كتلك التابعة للدرك الوطني ومديرية الأمن الوطني).

III. .الرؤية الجزائرية لقضايا للأمن السيبراني

قبل التطرق إلى الرؤية الجزائرية ينبغي توضيح أهم صور التهديدات والهجمات الالكترونية التي يمكن أن تتعرض لها الجزائر أغيرها من الدول في مجال الفضاء السيبراني[5]

3.1. التجسس الالكتروني : القيام باختراق شبكة أو جهاز إلكتروني بهدف سرقة المعلومات.

3.2. الجرائم الالكترونية : القيام بهجومات الكترونية بهدف تحقيق مكاسب مالية

[4]مهدي رضا، الجرائم السيبرانية و آليات مكافحتها في التشريع الجزائري ، مجلة إيليز للبحوث و الدراسات، المجلد 06/العدد: 02/2021 ،ص 111،ص125.

[5]بن مرزوق عنتر ، حرشاوي محي الدين ، الامن السيبراني كبعد جديد في السياسة الجزائرية ،مجلة دفاتر السياسية و القانون،العدد 17، جامعة قاصدي مرباح ،65،2017.

3.3. الإرهاب الالكتروني :يشير إلى الاعتداءات و التهديدات الموجهة إلى أجهزة الحاسب الالي و الشبكات الالكترونية و المعلومات الموجودة عليها

3.4. الحرب الالكترونية : وهي الحرب التي تتم إدارتها في مجال الفضاء الالكتروني و التي تكون الفواعل الرئيسية فيها هي الدولة.

تعتمد الجزائر لحماية امنها الالكتروني على استراتيجية تحلل المخاطر التي تتعرض لها الدولة و تحدد الخطوات و البرامج و المبادرات اللازمة لمواجهة هذه المخاطر عبر مايلي :

- ضرورة منح أهمية للفضاء الالكتروني و المعلوماتي لتعزيز الأمن و الدفاع الوطني ؛

-محاولة لجمع بين الاستباقية و الوقاية لضمان جاهزية أكبر في حالات خطر الاختراق أو تجسس أو التخريب ؛

-تثمين العنصر البشري من حيث تدريب أشخاص المكلفين بحماية الأنظمة الأمنية الالكترونية ؛

-رسم سياسة واضحة من أجل إعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية التي تعمل على تأمين المصالح الحكومية و المؤسسات التابعة للدولة ؛

-إعداد تقارير لتحليل المخاطر الأمنية الالكترونية و تحديد إستراتيجيات التعامل مع الكوارث ، و القيام بمراجعات و تقييمات مستمرة للسياسات الأمنية الالكترونية لبيان أوجه القصور فيها وتطويرها .

IV. استراتيجيات و اليات تصدي الجزائر للتهديدات السيبرانية:

يمكن القول أن زيادة معدلات التهديدات يرتبط بطبيعة هيكل النظام الدولي كبيئة محفزة لزيادة الهجمات السيبرانية منها فيروس كرونا حيث ساهم انتشار هذا الأخير عالميا في زيادة سرعة تحديث كثير من المجتمعات تكنولوجيا وزيادة الاعتمادية على التكنولوجيا في هذا الصدد[6].

انطلاق من التخوف من تلك التهديدات و الهجمات ، يأتي تحقيق الامن القومي في مقدمة مصالح الدول كافة،بغض النظر عن مكانتها على الساحة الدولية أو حج مكانتها.

ففي ظل عالم تتطور فيه التهديدات الأمنية و تتغير بسرعة فائقة ،لم يعد تبنى الدول الاستراتيجيات مرنة تستطيع مواكبة هذه التطورات مجرد خيار أمامها ، وإنما أصبح ضرورة حتمية تفرضها مقتضيات العصر الحديث.

لهذا تحتاج الدول إلى تطوير إستراتيجيات دفاعية جديدة ، مختلفة اختلافا كليا ونوعيا عن استراتيجيات مواجهة التهديدات التقلدية

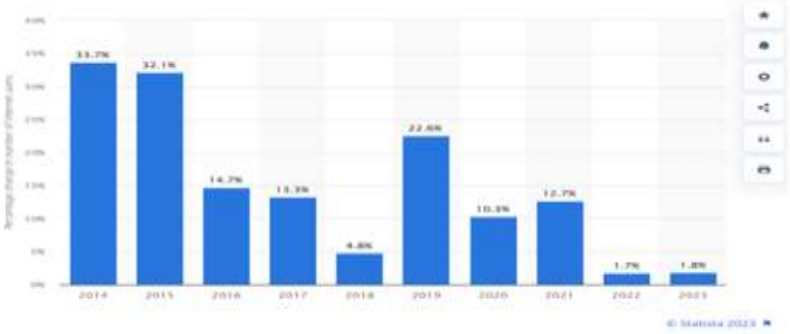
1. واقع الامن السيبراني في الجزائر :

[6]ليلي بن برغوت ، الامن السيبراني و حماية خصوصية البيانات الرقمية في الجزائر في عصر التحول الرقمي و الذكاء الاصطناعي ، مجلة الدولية لاتصال الاجتماعي جامعة عبد الحميد بن باديس ، مستغانم ، المجلة 10/ العدد 01 2023 ص 52.

تشير آخر الاحصائيات إلى أن هناك 32.09 مليون مستخدم للإنترنت في الجزائر مع بداية عام 2023، حيث بلغت نسبة انتشار الإنترنت 70.9% ، كما يستخدم حوالي 23.95 مليون مستخدم وسائل التواصل الاجتماعي في يناير 2023، أي ما يعادل 52.9 % من إجمالي السكان.

هذا وبلغ معدل انتشار الإنترنت في الجزائر 70.9% من إجمالي السكان مع بداية عام 2023. ويشير تحليل كيبيوس إلى أن عدد مستخدمي الإنترنت في الجزائر زاد بـ 553 ألفا (+1.8%(بين عامي 2022 و 2023 . .23 . ومن الجدير بالذكر أن حصة السكان من الوصول إلى الإنترنت تزايدت باستمرار خلال السنوات الماضية ويشير المخطط البياني التالي إلى ارتفاع نسبة عدد مستخدمي الانترنت من 2014 إلى غاية 2023، حيث يظهر أن أعلى معدل نمو كان في عام 2015 بنسبة 32.1 24%

ومن المتوقع حسب Statista أن ترتفع حصة السكان الذين لديهم إمكانية الوصول إلى الإنترنت في الجزائر بشكل مستمر بين عامي 2024 و 2028 بإجمالي 15.3 نقطة مئوية. [7]



'aifaddin Galal, Percentage change in the number of internet users in Algeria from '014 to 2023 Jun 29, 2023.

أما فيما يخص سرعة الاتصال بالانترنت في الجزائر عام 2023، تشير البيانات التي نشرتها شركة Ookla إلى أن متوسط سرعة الاتصال بالإنترنت عبر الهاتف المحمول عبر الشبكات الخلوية: 13.40 ميجابت في الثانية، في حين أن متوسط سرعة الاتصال بالإنترنت الثابت: 11.01 ميجابت في الثانية.

حسب مؤشر الأمن السيبراني الذي يصدره الاتحاد الدولي للاتصلات(ITU)

[7] J.Denhard,internet usage reach in algeria 2013-2028,Aug14,2023
http://www.statista.com/1137904/inernet-pentration-forecast-inalgeria

ITU-Global Cybersecurity Index 2020 Measuring commitment to cybersecurity، التابع للأمم المتحدة، فإن الجزائر تحتل المرتبة 104 عالميا من مجموع 182 بلد ، 93 من 160 أمة

حسب تصنيف الأمم (NCSI) ، والمرتبة 23 أفريقيا، و12 عربيا من مجموع 22 بلد عربي، ويأتي تصنيف البلدان الأفريقية، التي تحقق أفضل أداء فيما يتعلق بالأمن السيبراني كما يلي:

موريشيوس مؤشر رقم 96.89/100 | الأولى على المستوى الأفريقي.

تنزانيا مؤشر رقم 90.58/100 | الثانية على المستوى الأفريقي .

غانا مؤشر رقم 86.69/100 | الثالثة على المستوى الأفريقي .

نيجيريا مؤشر رقم 84.76/100| الرابعة على المستوى الأفريقي.

ويأتي تصنيف بلدان المغرب العربي ضمن شروط الأمن السيبراني كالآتي:

تونس : مؤشر رقم 86.23/100 | الخامس على منطقة المينا.

المغرب : مؤشر رقم 82.41/100 | السابع المستوى على منطقة المينا .

الجزائر : مؤشر رقم 33.93/100 | الثالث والعشرين على منطقة المينا.

ليبيا : مؤشر رقم 28.78/100 | السادس والعشرين على منطقة المينا .

موريتانيا : مؤشر رقم 18.94/100 | الثاني والثلاثين على منطقة المينا. [8]

وحسب نفس القرير فإن مؤشر الأمن السبراني للجزائر تحصل على 33.95 نقطة من مجموع 100 نقطة، حسب المجالات التالية: الإجراءات القانونية 12.46 نقطة من مجموع 20 نقطة ويمكن اعتبارها نتيجة مرضية، الإجراءات التقنية 2.73 نقطة ومن هنا تظهر هشاشة الأمن السيبراني في هذا المجال ، الإجراءات التنظيمية 1.44 نقطة وهو أضعف تنقيط، رغم المحاولات والمجهودات المبذولة في ميدان وضع هياكل إدارية وتنظيمية لإدارة الأمن السيبراني ، أما مجال تنمية القدرات فتحصل على 10.07 ويمكن قراءتها على أنها تنقيط متوسط إلى إيجابية وأخيرا مجال إجراءات التعاون فكان تنقيطه 7.25 وهو تنقيط دون المتوسط[9]

2. **المجهودات الجزئرية لتحقيق الامن السيبراني :**

[8] . Cybresécurité :l'algerie classé 23e en afrique ;8septembre 2021
http ://vinybusiness.com/algerie-23e-afrique-cybersecurite /

[9] زمورة جمال، بن عيسى ليلى ، أهمية حوكمة الامن سيبراني لضمان تحول رقمي آمن للخدمات العمومية في الجزائر ، مجلة البحوث الاقتصادية المتقدمة ، المجلد 07: العدد 02 / 2022 ص 415-429.

2.1عوائق تحقيق الامن السيبراني في ظل التحديات الانية و المستقبلية:

يمكن ان نذكر أهمها:

- تزايد عدد مستخدمي الشبكة مما ساهم في تزايد المخاطر لتتحول عملية إكتشاف هوية مرتبكي الجرائم الالكترونية إلى تحدي بسبب صعوبة البحث و التحري ضمن هذا العدد الهائل ؛
- تسهم التكنولوجيا المتطور ة في سرعة إنجاز الجريمة ،وهذا يضع الجهات الأمنية المختصة أمام سرعة سرعة مباشرة التحقيقات ومتابعة الجناة بالاجهزة المتطورة و البرامج الحديثة ؛
- التطور التكنولوجي و ظهور الانترنت :4G / 3G / wifi بسبب التقنيات أصبح القيام بالجريمة الالكترونية لا يستدعي الجلوس أمام الحاسوب مما يجعل الجهات الأمنية ترفع التحدي و الاستعداد بأحدث التقنيات لمواجهة التصدي لهذه التطورات؛
- تفعيل القوانين على أرض الواقع و تطبيقها بصرامة إذ من بين أكبر الإشكاليات التي تسهم في انتشار الجريمة الالكترونية هو الإفلات من العقاب و التأخر في تفعيل القوانين وهو ما يمنح المجرم فرص التكرار جرائمه لذلك من ضروري تأكيد على تطبيق القانون .

3.2. معوقات التي تواجه الأمن السيبيراني في الجزائر:

يمكن تلخيصها في العوامل الداخلية و الخارخية ،تتمثل :

- العوامل الخارجية:
  - شدة تعقيد البيئة الالكترونية؛
  - الازدياد المطرد في عدد مستخدمي الانترنت مما يسهل عمليات الاختراق ويصعب مهمة الدفاع؛
  - غياب الدليل وصعوبة اثباته خاصة في ظل سهولة إتلاف وتدمير الدليل المادي. إشكالية تحديد هوية المهاجم، في ظل توفر تقنيات تعرقل الوصول إليه.
- العوامل الداخلية:
  - قلة التجربة الجزائرية وخبرتها في المجال الالكتروني (خاصة الأجهزة الأمنية والقضائية) والراجع إلى انخفاض في القوة الالكترونية التي تعتبر أحد ركائز استراتيجية تحقيق الأمن السيبراني؛
  - نقص اعتمادها على الفضاء الالكتروني – بما فيه تكنولوجيا المعلومات والاتصالات والانترنت — في إدارة شئونها القومية إدارة بناها التحتية؛
  - انخفاض الميزانية الموجه لها، خاصة تلك الموجهة لأبحاث تطوير الأمن السيبراني نسبة إلى الناتج القومي الإجمالي؛
  - غياب الأطر التشريعية اللازمة لمكافحة الجرائم السيبرانية.

الخاتمةconclusion :

من خلال دراستنا لهذا الموضوع توصلنا لجملة من الاستنتاجات و التوصيات المتمثلة فيما يلي :

لقد توصلت الدراسة إلى جملة من الاستنتاجات نوردها كما يلي:

-إن الأمن السيبراني أضحى يمثل أهم صور الأمن المتحكمة في أنماط التفاعل بين الفواعل الدولية سواء التعاونية أو الصراعية ؛

-إن قضايا الأمن السيبراني وتهديداته باتت في صلب أي استراتيجية أمنية ناجعة.

-إن اهتمام الجزائر بالأمن السيبراني لا يعني قدرتها على تطوير استراتيجيات أمنية الكترونية حقيقية، بقدر ما يعني اضطرارها لمجابهة التهديدات الالكترونية التي غدت ظاهرة بوضوح بشكل يحتم عليها مواجهة التحديات والتهديدات الحالية والمستقبلية.

التوصيات

-الحاجة إلى تقييم التجربة الجزائرية عبر طرح تساؤلات حول أسباب تدني مستوى الأمن السيبراني للجزائر مقارنة بدول جارة لا تملك نصف امكانياتها.

-تطوير استراتيجيات أمنية الكترونية حقيقية، عبر انشاء مؤسسات مستقلة للتأمين الالكتروني وعدم حصرها في الأجهزة الأمنية للدولة.

-ضرورة الانفاق على تكنولوجيا المعلومات والاقتناع بكونها مهمة أهمية الانفاق العسكري كونها عنصر مضاعف لقوة الدولة.

المراجع :

1. الكتب:

- دحان عزام ناصر القريطي ، الامن السيبراني و حماية المعلومات ،الإسكندرية ،دار الفكر الجامعي ، الطبعة الأولى 2021 .
- عبد الوهاب لطفي الراوي ، إستراتيجية تحقيق الامن المعلوماتي بين آلية معالجة التغرات و التشفير و مسؤولية حماية البيانات عبر الانترنت في ظل حوكمة تكنولوجيا المعلومات و الاتصالات ، الإسكندرية ، دار الفكر الجامعي ، الطبعة الأولى ،2022.
- سامح عبد المطلب عامر ،علاء الدين محمد عوض ، الاتصال الإداري الفعال (الفلسفة ، التطوير ، المهارات، التقويم)،دار الفكر ،الطبعة الأولى ،2023.

2. المقالات:

- زمورة جمال، بن عيسى ليلى ، أهمية حوكمة الامن سيبراني لضمان تحول رقمي آمن للخدمات العمومية في الجزائر ، مجلة البحوث الاقتصادية المتقدمة ، المجلد 07: العدد 02 / 2022 .
- ليلي بن برغوت ، الامن السيبراني و حماية خصوصية البيانات الرقمية في الجزائر في عصر التحول الرقمي و الذكاء الاصطناعي ، مجلة الدولية لاتصال الاجتماعي جامعة عبد الحميد بن باديس ، مستغانم ، المجلة 10/ العدد 01 2023 .
- بن مرزوق عنتر ، حرشاوي محي الدين ، الامن السيبراني كبعد جديد في السياسة الجزائرية ،مجلة دفاتر السياسية و القانون،العدد 17، جامعة قاصدي مرباح ،2017.
- مهدي رضا، الجرائم السيبرانية و آليات مكافحتها في التشريع الجزائري ، مجلة إيليز للبحوث و الدراسات، المجلد 06/العدد: 2021/02.

3. المواقع :

- Cybresécurité :l'algerie classé 23e en afrique ;8septembre 2021 http ://vinybusiness.com/algerie-23e-afrique-cybersecurite
- J.Denhard,internet usage reach in algeria 2013-2028,Aug14,2023 http://www.statista.com/1137904/inernet-pentration-forecast-inalgeria