المجلة الدولية للإتصال الإجتماعي
جامعة عبد الحميد بن باديس- مستغانم
ISSN: 2437 – 1181
EISSN: 2710-8139

المجلد 10 / العدد: 01 (2023)، ص 443- ص 457

الأمن السيبراني و حماية خصوصية البيانات الرقمية في الجزائر في عصر التحول الرقمي و الذكاء الاصطناعي

التهديدات، التقنيات، التحديات، و آليات التصدي.

Cyber Security and Privacy of Digital Data in Algeria in the Era of Digital Transformation and Artificial Intelligence

Threats, Technologies, Challenges, and Mechanisms of response.

ليلى بن برغوث*

جامعة صالح بو بنيدر –قسنطينة 3- ، leila.benberghout@univ-costantine3.dz،

تاريخ الاستلام: 2022/10/12 تاريخ القبول: 2022/12/08 تاريخ النشر: 2023/03/31

DOI: 10.53284/2120-010-001-026

الملخص:

تهدف دراستنا هذه إلى كشف واقع الأمن السيبراني و خصوصية البيانات الرقمية الموجودة على قواعد البيانات و المواقع الالكترونية في الجزائر، و المكانة التي تعطيها لهما الدولة الجزائرية ضمن منظومتها الأمنية، و يتحقق ذلك من خلال التعرف على أنواع التهديدات السيبرانية التي تواجهها الجزائر ، و أهم التقنيات المستحدثة التي تستخدم في اختراق البيانات الرقمية و تنفيذ الهجمات و الحروب السيبرانية، و أيضا الوصول إلى التحديات و العقبات التي تقف أمام تنفيذ السياسة الأمنية الداخلية لدحض الجريمة الالكترونية عموما، و من ثم معرفة الإجراءات الاحترازية و آليات التصدي للهجمات السيبرانية التي تعمل عليها الجزائر، و وسائل المعالجة في حالة وقوع الهجمات.

كلمات مفتاحية: الأمن السيبراني،خصوصية البيانات الرقمية، الجريمة السيبرانية(الالكترونية)، التحول الرقمي، الذكاء الاصطناعي

Abstract:

Our study aims to reveal the reality of cyber security and the privacy of digital data found on databases and websites in Algeria. and the status accorded to them by the Algerian State within its security system, This is achieved by identifying the types of cyber threats that Algeria faces. And the most important new technologies used to penetrate digital data and carry out attacks and cyber warfare, Also, access to challenges and obstacles to the implementation of the internal security policy to refute cybercrime in general measures and mechanisms for dealing with Algeria's cyber attacks, and remedies in the event of attacks.

Keywords: Cyber Security, Privacy of Digital Data, Cybercrime (Electronic), Digital Transformation, Artificial Intelligence

* **المؤلف المرسل :**

1. مقدمة:

يسمى هذا العصر بعصر تكنولوجيا الاتصال، و عصر الرقمنة، و المعلوماتية، و عصر الوسائط المتعددة، و الذكاء الاصطناعي،و غيرها من التسميات الكثيرة الأخرى، و كلها تسميات تشير إليه من زاوية خاصة،و يرجع إطلاق التسميات إلى ما يتسم به من تقنيات مستحدثة، أدت بالضرورة إلى تهديد الأمن السيبراني و أمن المعلومات و خصوصية الأفراد و المجتمعات،و إلى الكم الهائل من التكنولوجيات العالية الدقة و التعقيد التي ظهرت فيه، و نظرا للانفجار المعلوماتي الذي حصل ، بفعل تسخير هذه التكنولوجيات للإنتاج اللامحدود من البيانات التي تحول بعد المعالجة إلى معلومات؛ حيث تعد الانترنيت البنية التحتية الأسرع نموا في عصرا الحالي، فالعديد من التكنولوجيات الحديثة التي أفرزتها الانترنيت غيرت البشرية للأفضل.

غير أن بسبب هذه التكنولوجيات الناشئة ، أصبحت المؤسسات بمختلف أنشطتها عاجزة عن حماية معلوماتها الخاصة على هذا الفضاء الافتراضي بطريقة فعالة، بما أن الجرائم الالكترونية تزداد بشكل كبير و مستمر، و بما أن أغلبية المعاملات التجارية و الشخصية على السواء، تجري باستخدام الوسائل المتاحة على الإنترنت، فقد بات من الضروري، أن تكون هناك خبرة أمنية سيبرانية لحماية المعاملات الرقمية. فالأمن السيبراني أصبح يثير جدلا كبيرا في ظل التكنولوجيات المتقدمة، مثل خدمات السحابة، والهواتف النقالة، والتجارة الإلكترونية، و مصارف الإنترنت، و الذكاء الاصطناعي، و العديد من الخدمات الأخرى التي تحتاج إليها جميع الوسائل و التكنولوجيات.

و تعد الجزائر من بين الدول التي تهتم بقضية الأمن السيبراني، خاصة و أنها تسير بخطى متسارعة نحو رقمنة قطاعاتها الحساسة، فقد أثارت قضية "بيغاسوس" بشكل خاص مخاوف أكبر بالنسبة لأجهزة الدولة الجزائرية، حول قضية تأمين و حماية البنية التحتية للمعلومات، و حمايتها من القرصنة و التجسس، و الاختراق، و أهمها منظومة الجيش الجزائري، التي بدأت تهتم بالدفاع السيبراني مؤخرا ، من خلال برامج، و استراتيجيات، و فعاليات، بغرض مناقشة سبل الحماية و الرد و التنبؤ، بالهجمات السيبرانية.

✓ الإشكالية:

يشكل موضوع الأمن السيبراني معضلة العصر، باعتباره السلاح الاستراتيجي الحالي، نظرا لما يفرزه الواقع التكنولوجي الذي يفرض نفسه على المجتمعات، و متطلباته، من تهديدات سيبرانية غير معروفة، و هجمات غير متوقعة، تثير تخوف الجميع، تساهم في زيادة حدة مخاطرها، كل من الرقمنة و الذكاء الاصطناعي. و بما أن الجزائر تتجه بشكل متسارع نحو رقمنة قطاعاتها، و هياكلها الحساسة، فقد بات من الضروري مناقشة، اهتمامها بقضية تأمين منظومتها الالكترونية ،و بنيتها المعلوماتية التحتية، و مدى قدرتها على توفير الأمن المناسب و الحماية الكافية لمستخدمي الفضاءات الالكترونية، و المنصات الرقمية الرسمية المستحدثة، في إطار تطبيق خدمات الحكومة الالكترونية، و خدمات الإدارة العمومية، و غيرها، و معرفة نوع التهديدات و المخاطر التي قد تقع على منظومة الأمن و مؤسسات الدولة و أفرادها، و الأمن السيبراني للجزائر، و التحديات التي توجهها

الجزائر في حالة محاولتها تطبيق سياسات الحماية المناسبة، و ردع و محاربة الجريمة الالكترونية العابرة للحدود و الإرهاب الالكتروني ، في ظل خصوصية الجريمة الالكترونية و الحروب السيبرانية، و بالحديث عن التحديات و التهديدات، لابد من معرفة مدى جاهزية الدولة الجزائرية و أنظمتها الدفاعية الالكترونية، المتمثلة في منظومة الجيش، و منظومة الاتصال، و مؤسسات التعليم العالي، و يمكن استخلاص ذلك من الاستراتيجيات و الآليات التي تنتهجها الدولة الجزائرية لتوفير الحماية بنيتها المعلوماتية الأساسية. و لتحقيق أهداف دراستنا كان لابد من طرح التساؤل الرئيسي التالي:

ما هو واقع الأمن السيبراني في الجزائر في ظل التحول الرقمي؟ و ما هو الحيز الذي يشغله ضمن الإستراتيجية الأمنية للوطن؟و ما هو مصير البيانات التي تستخدم ضمن الفضاء الرقمي، و هل خصوصية هذه البيانات محاطة بالحماية الكافية في الجزائر؟ و ما العلاقة التي تربط بين الأمن السيبراني و خصوصية البيانات الرقمية؟

و لمعرفة واقع الأمن السيبراني ؛ لابد من معرفة بعض القضايا الجزئية التي تعطينا تصورا لاستنباط الواقع الحقيقي للأمن الالكتروني (الرقمي)و يتجلى ذلك من خلال الأسئلة الآتية:

- ما هي أنواع التهديدات السيبرانية التي تواجهها الجزائر؟
- ما هي أهم التقنيات المستحدثة التي تستخدم في تنفيذ الهجمات السيبرانية، و ما هي التقنيات التي تساعد على تأمين المنظومة المعلوماتية؟
- ما هي الإجراءات الاحترازية لتفادي الهجمات السيبرانية و انتهاك البيانات في الفضاء الرقمي، و ما هي وسائل المعالجة في حالة وقوع الهجمات؟
- ما هي التحديات و العراقيل التي تواجهها الجزائر لتنفيذ السياسة الأمنية السيبرانية؟
- ما هي الآليات و الاستراتيجيات و الأجهزة المسؤولة عن التصدي للجريمة الالكترونية؟

✓ **أسباب اختيار الموضوع:**

ترجع أسباب اختيار الموضوع إلى نوعين، الأولى ذاتية: و تتمثل في الميل الشخصي إلى مثل هذه المواضيع الحديثة و الحساسة، و بحكم التخصص البحثي للباحث، لان الموضوع يصب ضمن الاهتمامات و الحقل البحثي للباحثة.و الثانية؛ هي أسباب موضوعية، و يتمحور ذلك حول طبيعة الموضوع الذي يفرض نفسه على الساحة البحثية في جميع المجالات، سواء التقنية، أو الاقتصادية، أو القانونية، أو الإعلامية، و غيرها.

✓ **أهداف البحث:**

الهدف من بحثنا الوصول إلى إجابات كافية على تسؤلاتنا المطروحة ،من خلال:

- التعرف على مخاطر التحول الرقمي و حوكمة المؤسسات و الهيئات الحساسة للدولة الجزائرية على أمنها الداخلي و منظومتها المعلوماتية.

- كشف طبيعة و حجم التهديدات التي تستهدف الجزائر و أمنها السيبراني الداخلي.
- تسليط الضوء على أنظمة و تقنيات الذكاء الاصطناعي، و معرفة مخاطر الظاهرة على البيانات الشخصية، و على الأمن السيبراني للدولة الجزائرية.
- معرفة التحديات التي تواجهها الجزائر أمام تنفيذها سياسات و آليات حماية البيانات و الأنظمة المعلوماتية، و الوقوف في وجه الهجمات السيبرانية التي تستهدفها.
- التعرف على أهم التقنيات الحديثة التي توظف في تنفيذ الهجمات السيبرانية.
- محاولة قياس الاستراتيجيات و الآليات الأمنية التي جندتها الجزائر في سبيل حماية بنيتها المعلوماتية التحتية من مخاطر الهجمات السيبرانية.

✓ أهمية البحث:

تكمن أهمية البحث، في أنه يسلط الضوء على موضوع راهن، يشغل العام و الخاص حاليا،و الرأي العام و نخبة المجتمع الدولي، و مخاطره المحتومة على الأفراد و الدول، و تتمثل هذه الظاهرة في التداعيات الأمنية لرقمنة هياكل الدولة و الحوكمة الالكترونية، و ترصد ما تشكله من مخاطر على أمن مؤسساتها و أفرادها؛ في ظل ما يسمى بحروب الجيل الخامس، التي تتلخص في توظيف أنظمة الذكاء الاصطناعي التي تطرح علامات الاستفهام، حول ما هو مصير الخصوصية و أمن المعلومات مع بروز الذكاء الاصطناعي.

✓ **المنهج المستخدم:**

إن طبيعة البحث تفرض علينا استخدام المنهج الوصفي التحليلي: الذي يقوم على وصف جوانب الظاهرة و الظروف المحيطة بها، و جمع المعلومات عنها، مع إيجاد وسائل مختلفة لتفسيرها،من خلال طرح الأسئلة و صياغة الفرضيات، لاستخراج النتائج، وفقا للشواهد و القرائن الموجودة. و هذا من خلال تحليلنا لتصريحات المسؤولين على القطاع و المختصين في مجال تكنولوجيا الاتصال و الأمن السيبراني في الجزائر.

2. تحديد المفاهيم:

1.2. مفهوم الأمن السيبراني Cyber security :

إن لفظة سيبار (Cyber) هي كلمة يونانية، مشتقة من كلمة (Kybernets) ، و تعني الشخص الذي يدير دفة السفينة (Steersman) ، و هناك من يرجع أصل اللفظة إلى منتصف القرن20، مع عالم الرياضيات الأمريكي " Narbert Wieners" ، الذي استخدمها للتعبير عن التحكم الآلي، حيث عرف السيبرنيتيقية على أنها "التحكم و التواصل عند الحيوان و الآلة"، كما ذكر في الكتاب ذاته أنها"علم نقل الرسائل بين الإنسان و الآلة أو بين الآلة و الآلة"، من هنا تبلورت السيبرانية و تم توظيفها للتعبير عن العمليات الآلية و العلاقات بين الأجهزة الالكترونية و الإنسان. (بن مرزوق، 2018، صفحة 35)

أما **الأمن السيبراني** فهو ممارسة الدفاع عن أجهزة الكومبيوتر، و الأجهزة المحمولة و الأنظمة الالكترونية،و الشبكات، و البيانات، من الهجمات الخبيثة، كما يرد بمعنى أمن الشبكات والأنظمة المعلوماتية، والبيانات، والمعلومات، والأجهزة المتصلة بالانترنيت، وعليه فهو المجال الذي يتعلق بإجراءات، ومعايير الحماية المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات،و منع الهجمات،أو على الأقل الحد من آثارها. (جبور الاشقر، 2017، صفحة 25) و قد عرفته وزارة الدفاع الأمريكي Pintagon أنه: كافة الإجراءات التنظيمية التي تأمن الحماية الكافية للمعلومات بجميع أنواعها و أشكالها ، سواء كانت الكترونية أو مادية، من مختلف المخاطر و الهجمات و الجرائم، و أفعال التخريب و التجسس و الحوادث، بينما أدرج الإعلان الأوروبي ، **الأمن السيبراني** بمعنى : "قدرة النظام المعلوماتي على مقاومة محاولات الاختراق أو الحوادث غير المتوقعة التي تستهدف البيانات". (الشمري، 2020، الصفحات 275-276)

و من بين من عرف الأمن السيبراني Edward Amors ،الذي قدم الأمن السيبراني بأنه: الوسائل التي من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، و منها الوسائل المستخدمة في مواجهة القرصنة و كشف الفيروسات. (Amoroso, 2007, p. 1) حيث جزم بالجدارة المطلقة لأجهزة الأمن السيبراني في ردع الجريمة المعلوماتية، إلا أن الوسائل المسخرة لحماية المعلوماتية و الأمن السيبراني ليس بالضرورة أنها تقوم دائما بردع الجرائم الالكترونية، و إنما قد تعمل على الحد منها و الحماية من وقوعها، و أيضا Kemmerer . A Richard الذي يرى أنه:"عبارة عن وسائل دفاعية من شأنها كشف و إحباط المحاولات التي يقوم بها القراصنة" .(Kemmerer, 2003, p. 3) و يبدو أنه قدم تعريفا مختصرا و لم يفصل في هوية القراصنة، و أنواع مرتكبي الهجمات السيبرانية.

2.2.خصوصية البيانات الرقمية Privacy of Digital Data:

يعود الفضل في صياغة مفهوم خصوصية المعلومات الالكترونية أو البيانات الرقمية، كمفهوم مستقل عن باقي مفاهيم الخصوصية إلى المؤلفين الأمريكيين **westin alan** و**milar** في مؤلفهما **الخصوصية و الحرية** ، و في كتاب **الاعتداء على الخصوصية** ، و يمكن القول أن مفهومي الخصوصية و الخصوصية المعلوماتية أو الرقمية مترادفان و ما يفرقهما هو فقط أن الخصوصية المعلوماتية برزت في ظل ظهور الانترنيت و تقنيات الاتصال الحديثة و الفضاءات الرقمية ، بينما الخصوصية عامة موجودة منذ القدم، انطلاقا من ضبط الحياة و السلوكيات الفردية في إطار الجماعة، و أحقية الآخرين عليه في احترام خصوصياتهم و لا يجوز لأي شخص التعدي عليها بآي شكل من الأشكال. و من هنا فالخصوصية المعلوماتية (الرقمية)هي حق الفرد في أن يضبط عملية جمع المعلومات الشخصية عنه، و عملية معاملتها آليا و حفظها و توزيعها و استخدامها في صنع القرار الخاص بالمؤثر فيه. (عدنان السيد، 2013، صفحة 433)

3.2. الجريمة السيبرانية Cyber crime:

الجريمة السيبرانية بمفهومها التقني؛ تعني الجريمة المعلوماتية تقنيا؛ ذلك النوع من النشاط الإجرامي الذي تستخدم فيه تقنيات الحاسوب الآلي، بطريقة مباشرة أو غير مباشرة، و الهدف من ذلك النشاط الإجرامي تنفيذ الفعل الإجرامي المقصود.

(حجازي، 2006، صفحة 20)بينما يتناولها مكتب تقييم التقنية في الولايات المتحدة الأمريكية بمعنى: "الجرائم التي تلعب فيها البيانات الحاسوبية و البرامج المعلوماتية دورا رئيسيا" (حامد، 2007، صفحة 24)، و قد ركز هذا الطرح على نوع الوسيلة التي ارتكبت بها الجريمة في تحديده لمفهومها.

و من جهتها ، عرفت رابطة كبار ضباط الشرطة الجريمة الالكترونية بأنها: تتضمن في ارتكابها ، أو تسهيل ارتكابها،استخدام الكومبيوتر أو الانترنيت و شبكات التكنولوجيا،و يبدو أن هذا التعريف قد ركز على وسيلة ارتكاب الجريمة ، بينما فصل في أنواع الوسائل التي تدخل ضمن ممارسة الجريمة السيبرانية فقط،

و من جهته يرى المعهد الاسترالي لعلم الإجرام، أن الجريمة الالكترونية هي تسمية عامة تطلق على ذلك النوع من الجرائم التي ترتكب باستخدام البيانات الالكترونية، أو أجهزة الاتصالات. (بارة، 2017، الصفحات 428-429)

و من هنا فالجريمة الالكترونية لا تعني الجرائم التي تستهدف البيانات الموجودة على أنظمة الحاسوب فقط، و إنما كل الأنشطة الإجرامية التي يستخدم فيها الحاسوب و الانترنيت و مختلف التقنيات المتطورة،بما في ذلك أنظمة الذكاء الاصطناعي التي توظف في حروب الجيل الخامس G5.

4.2. التحول الرقمي Digital Transformation :

و يعني التغيير الثقافي، والتنظيمي، والتشغيلي لمؤسسة، أو صناعة، أو نظام إيكولوجي، من خلال التكامل الذكي للتقنيات، و العمليات، والكفاءات الرقمية عبر جميع المستويات والوظائف بطريقة مرحلية و إستراتيجية.(i-scoop) فهو عملية تحويل المعلومات التناظرية إلى شكل رقمي، باستخدام محول تناظري إلى رقمي ، كما هو الحال في الماسح الضوئي للصور أو للتسجيلات الصوتية الرقمية، و مع تزايد استخدام الإنترنت منذ التسعينيات،زاد استخدام الرقمنة أيضًا،ومع ذلك، فإن التحول الرقمي أوسع من مجرد رقمنة العمليات الحالية .و يستلزم النظر في كيفية تغيير المنتجات والعمليات والمؤسسات ،من خلال استخدام التقنيات الرقمية الجديدة.(wikipedia) و يعني أيضا الاعتماد الاستراتيجي للتقنيات الرقمية، يتم استخدامه لتحسين العمليات الإنتاجية، و تقديم تجارب أفضل للعملاء و الموظفين، و إدارة مخاطر الأعمال، و التحكم في التكاليف. (artificial-solutions/digital-transformation)

5.2. الذكاء الاصطناعي Artificial Intelligence:

يعرف الذكاء الاصطناعي بأنه: "نظام كومبيوتر له القدرة على تقليد السلوك البشري، و الذكاء و الأداء و المهام." (Dan, 2018, p. 850)، و يرى البعض أن الذكاء الاصطناعي يشير إلى الآلات و الأجهزة التي تقوم بمهام تتطلب نوعا من الذكاء، لفهم العمليات المعرفية، مثل تمثيل المعرفة و التخطيط و التعلم و حل المشكلات و التكيف و التفاعل. من الناحية الرياضية، الذي بدوره سيؤدي إلى تفعيل هذه العمليات في نظام كومبيوتر، كما يمكن أن يشير إلى الأساليب المطلوبة لتحقيق ذلك، أي الخوارزميات و الهياكل الحسابية. (Dan, 2018, p. 850)

و يرد بمعنى بسيط: هو تقليد لسلوكيات الناس بطريقة ذكية، باستخدام الروبوتات، أو الآلات مع نظام مدمج من التفكير، بالطريقة المعرفية نفسها، التي يقوم بها البشر، و أداء مهام مثل حل المشكلات و اتخاذ القرارات و التعرف على الكلام و الترجمة. و غيرها. (nasrallah, 2021, p. 5) بحيث تصبح تقنياتها قادرة على التعلم و التعامل مع كميات ضخمة من البيانات، و تحويلها إلى أدوات فعالة، كما يمكنها توقع و اتخاذ قرارات بدلا عن البشر، بعد جمع و معالجة و تحليل كميات هائلة من البيانات ، بسرعة تفوق سرعة البشر بكثير. (بوبعاية، 2021) و يمكن الاستدلال على ذلك من خلال؛ التقدم الذي بلغته أنظمة الذكاء الاصطناعي، الذي وصل حد التعلم الآلي (ML) و التعلم العميق (DL)، و يرمزان إلى طريقة تعلم الخوارزميات التي يعمل بها الكومبيوتر لكيفية القيام بالأشياء، مثل تصنيف البيانات و التنبؤ بالقيم، و يتحقق ذلك عن طريق تحليل و معالجة البيانات الضخمة. (Authoriey, Accountants, 2017, p. 6)

3. التهديدات السيبرانية التي تواجهها الجزائر:

و قد أجمل "سمير بارة "أخطر التهديدات الالكترونية التي تواجهها الدول في أربع أنواع: تعطيل الخدمة، إتلاف المعلومات أو تعديلها، التجسس على الشبكات، تدمير الأصول و المعلومات. (بارة، 2017، الصفحات 428-429)

وفي ذات السياق كشف العميد "تيتوش نبيل يوسف" رئيس "دائرة الإشارة وأنظمة المعلومات والحرب الإلكترونية" في تصريح لمجلة "الجيش" التابعة لوزارة الدفاع الجزائرية، عن إحباط مصالحه مليون و242 ألف و801 محاولة هجوم إلكتروني ، وقرصنة سنة 2021 ومن "مختلف مناطق العالم" استهدفت مواقع إلكترونية جزائرية. (بورنان، حصيلة رسمية..الجزائر تحبط مليون هجمة الكترونية في 2021، 2022) و يرى البروفيسور و الخبير "سعدي سلامي" أن اخطر الهجمات التي تعاني منها الجزائر تتمثل في الهجمات المدعومة من الدول، التي تزيد من حجم الأضرار المحتملة ، و خاصة بعد فضيحة "بيغاسوس" و قضية التجسس الصهيوني المغربي على الجزائر. (www.akhbardzair.dz, 2022)

و في كلمة افتتاحية ألقاها قائد أركان الجيش الفريق "السعيد شنقريحة"، خلال افتتاح فعاليات ملتقى "**الأمن السيبراني و الدفاع السيبراني**: رهانات و تحديات على ضوء التحولات الجديدة متعددة الأبعاد "، الذي نظمته دائرة الاستعمال و التحضير لأركان الجيش الوطني ، بالنادي الوطني للجيش، كشف عن تصدي الجزائر للعديد من الهجمات السيبرانية، التي استهدفت مواقع حكومية، و أخرى تابعة لمؤسسات اقتصادية و حيوية و إستراتيجية، و أكد أن مواقع التواصل الاجتماعي ، أصبحت تعد ملاذا لشبكات إجرامية منظمة. (www.elmihwar.dz, 2022)

4. التقنيات المستخدمة في الأمن السيبراني للدول:

تتعدد التقنيات التي أصبحت توظف في مجال الهجمات السيبرانية، و من أهم الأسلحة السبيرانية؛ انترنيت الأشياء،و التزييف العميق، و تقنية البلوك تشين ،و الحوسبة السحابية و التعلم العميق، و التعلم الآلي... و غيرها.

و قد أفاد الخبير الأكاديمي "سعدي سلامي" ، في تصريح له لقناة "أخبار دزاير" الالكترونية، أن التقدم المتسارع الذي يشهده العالم ، في مجال الذكاء الاصطناعي، و التطور التكنولوجي، خلق تحديات كبيرة، على صعيد تحقيق الأمن السيبراني، و تعزيز الدفاعات السيبرانية للدول و المجتمعات،مؤكدا على مجموعة من التكنولوجيات الحديثة التي ترتبط خاصة بالذكاء الاصطناعي تتمثل في : (www.akhbardzair.dz, 2022)

1.4 التعلم العميق Deeplearning: و يتم عن طريق تعليم الحواسيب، باستخدام معالجة البيانات الضخمة عبر أنظمة الشبكات الاصطناعية المتعددة الطبقات، (www.Kaacenter.android.com, 2022)،و يشكل خطرا على أمن البنية التحتية للمعلومات التابعة للدول. كما يمكن استخدامه في المقابل لتأمين الشبكات و القواعد المعلوماتية.

2.4 اللسانيات الحاسوبية Computerized Linguistic :التي تسهل عملية جمع المعلومات بكل اللغات ،و عملية التعلم الآلي ، و التعلم العميق ، من خلال المحاكاة، مما يهدد الأمن المعلوماتي للدول، من خلال التعرف البصري على الحروف (بالانجليزية OCR)، و القواميس الالكترونية، التي تعد قواعد بيانات ضخمة ، و الترجمة الالكترونية، و تقنية التعرف الصوتي، التي و غيرها، التي تساعد في عملية استعادة المعلومات و المحاكاة. (مهديوي، 2016)

3.4 تأثيرات الذكاء الاصطناعي على الاقتصاد الرقمي Influence of al on EconomyNumerical Economy: من خلال جمع البيانات الضخمة، من قواعد البيانات، و مواقع الانترنيت، و مواقع التواصل الاجتماعي، باستخدام تقنيات الذكاء الاصطناعي، و جمع المعلومات الشخصية،و مقارنتها، و تكوين ملفات عن الأشخاص، و استهدافهم بالإعلانات التجارية،بالإضافة إلى الحوكمة الاقتصادية، و رقمنة الإدارات و المؤسسات، وغيرها.

4.4 الحوسبة السحابية Cloud Computin: و إنشاء كفضاء منفصل لتامين و حماية البيانات، من خلال إنشاء شبكات لا مركزية، و استخدامها بشكل مباشر و شفاف دون وسيط،و قد عمد الكثير إلى التوجه نحو استخدامها، خاصة في المعاملات المالية و أثبتت نجاعتها في حماية البيانات من الاختراق، إلا أن لها عيوب، و تتمثل في عدم معرفة هوية صاحب الحوسبة، و أيضا إمكانية تعرض البيانات إلى الضياع، أو الحذف و عدم إمكانية الدخول إليها أو استرجاعها.

5.4 الواقع المعزز Auguemented Reality: و يقصد به استخدام الآلة التي تعزز الوجود الإنساني، و تحاكي ذكاءه، و تعمل من خلال بياناته الخاصة.

6.4 الجيل الخامس G5: الذي اربط بالذكاء الاصطناعي.

7.4 شبكات الاستشعار اللاسلكية Wireless Sonsor Networks.

8.4 الجريمة الالكترونية Cybercriminality: العابرة للحدود و القارات.

9.4 المدن الذكية Smart cities

10.4 الحاسوب الكمومي Quantum computer: الذي يعمل بالكم الهائل من البيانات.

هذه الأنظمة التي تدخل في إطار الثورة الصناعية الرابعة Fourth Industrial Révolution في إطار عصر الذكاء الاصطناعي. (مهديوي، 2016)

11.4 بالإضافة إلى نوع آخر من التقنيات التي يعتبرها البعض حلا أمنا لحفظ البيانات و المعاملات المالية، إلا أن لها عيوب شأنها شأن المواقع على شبكة الانترنيت، و نحن هنا نتحدث عن **تقنية البلوك تشين. أو سلاسل الكتل.**

12.4 التزييف العميق Deepfake: وما يثيره من مخاوف بالنسبة للخداع بالفيديوهات المزيفة التي تحاكي الحركات و الأصوات و الصور الحقيقية.

5. التحديات التي توجهها الجزائر أمام تطبيق الأمن السيبراني:

ما يقع على العالم ككل من تحديات للأمن السيبراني يقع على الجزائر أيضا ، بالنظر إلى التحول إلى الرقمنة الجارية و الشاملة لكافة القطاعات الجزائرية، و قد لخص البعض التحديات المفروضة على الأمن السيبراني حاليا في سبعة تحديات أساسية: و تتمثل في هجمات المصيدة، و هجمات التغيرات الأمنية في التطبيقات و البرامج و أنظمة التشغيل، و هجمات انترنيت الأشياء،و هجمات الحوسبة السحابية، و هجمات الأجهزة القديمة الخارجة عن الدعم الفني، و هجمات الفيروسات، بالإضافة إلى أخطر الهجمات الراهنة، و هي هجمات الذكاء الاصطناعي؛ حيث باستخدامه، أصبحت الحرب الالكترونية سجال بين طرفين هما: الأطراف التي تطور وسائل المهاجمة، و الجهات التي تطور أنظمة الحماية و الصد(الردع). (محمدي، 2021) و من بين التحديات التي توجهها الجزائر في مجال تطبيق الأمن السيبراني:

- تزايد عدد المشتركين في شبكة الانترنيت و مواقع التواصل الاجتماعي في الجزائر ؛ الذي فاق 10 ملايين مشترك، مما يزيد من المخاطر المفروضة ؛مما ينعكس سلبا على عملية اكتشاف هوية مرتكبي الجرائم الالكترونية.
- انتشار تكنولوجيا الانترنيت فائقة التدفق و السرعة (ADSL/VSAT/SDSL)، الذي يفرض تحديا أمام سرعة متابعة الجناة و المتابعة، و التسلح بالأجهزة و البرامج الملائمة لها.
- الانترنيت اللاسلكي (WIFI/3G/4G/5G)أيضا يشكل عائقا في وجه محاربة الجريمة الالكترونية.
- عمليات التخفي أثناء استعمال شبكة الانترنيت(Proxy): الذي يصنف ضمن اكبر التحديات و العوائق التي تواجهها أجهزة محاربة الجريمة الالكترونية.
- نقص عامل التنسيق بين الدول و الحكومات، نظرا لخصوصية الجريمة السيبرانية، بما يمكن مرتكبيها من النفاذ إلى أنظمة المعلومات بسهولة،و سرية المعلومات التي لا يمكن كشف طبيعتها، و لا كشف البرامج التي تستخدم لحمايتها و تقاسمها مع الدول الأخرى.

- صعوبة تكييف القوانين الرادعة للجريمة المعلوماتية، و تفعيلها، و تطبيقها، بالموازاة مع التطور الحاصل في مجال التكنولوجيا و الهويات الافتراضية، و البرمجيات،و التقنيات التي تتجدد باستمرار ، و الاحترافية في التخفي، و الفيروسات القادرة على التخفي أيضا.

بالإضافة إلى عوامل أخرى يشترك فيها العديد من دول العالم الثالث و من بينهم الجزائر و هي:

- التجربة الفتية للجزائر في مجال تكنولوجيا الاتصال و المعلوماتية.
- استحواذ الدول المتقدمة على التكنولوجيا، و احتكارها للتقنيات الحديثة، مما يؤدي إلى عدم التمكن من التنبؤ بالتهديدات التي تواجهها. حيث نوه العميد "تيتوش نبيل" أن هناك "بعض الصعوبات"،والتي ربطها بتنفيذ العقود مع الشركاء الأجانب بفعل جائحة كورونا.

6. استراتيجيات و آليات تصدي الجزائر للتهديدات السيبرانية:

تولي الدولة الجزائرية الأولوية القصوى للأمن السيبراني ضمن الإستراتيجية الأمنية العامة للدولة، من حيث تسخير التدابير اللازمة ؛ التي من شأنها توفير أكبر درجة حماية لبنيتها المعلوماتية التحتية، و تحقيق أمنا سيبرانيا مناسبا للتحولات الرقمية الجارية و عملية عصرنة قطاعات الدولة ،التي تفرض تحديات كبيرة أمام تحقيق الأمن اللازم لمختلف أجهزة الدولة و مواطنيها، و يتأتى ذلك بمجموع الآليات و الاستراتيجيات التي سخرتها الدولة، و التي أقر بها العديد من الفاعلين و المسؤولين، خاصة مسؤولي الأمن السيبراني على مستوى جهاز الجيش الوطني الجزائري، و بعض الأشخاص المختصين في مجال الأمن و الجريمة الالكترونية. حيث ؛ كشف العميد تيتوش عن مجموعة من الآليات التي عملت الجزائر على تفعيلها و من بينها يذكر: (بورنان، https://al-ain.com/article/algeria-thwart-cyber-attacks-2012، 2022) تزود مخابر "دائرة الإشارة وأنظمة المعلومات والحرب الإلكترونية" والضباط العاملين بـ"أحدث الوسائل والأجهزة التعليمية المعتمدة في مجال التكوين، من بينها محاكيات متخصصة بمعايير دولية لاستعمال واستخدام وسائل الحرب الالكترونية.

- تعزيز المدرسة العليا للإشارة بأكاديمية "سيسكو" ،التي تقدم حاليا تكوينا عالي المستوى في تسيير و تأمين الشبكات."
- تجهيز الدائرة العسكرية بـ"وسائل وتجهيزات جد متطورة تستجيب للمعايير الدولية، مما يؤهلها اليوم إلى إنتاج كميات معتبرة من المعدات التي من شأنها تلبية بشكل فعال احتياجات المستخدمين.
- توفير ورشتين ميكانيكيتين مجهزتين بآلات تحكم رقمية عالية الدقة، تُستخدم لتصنيع الأجزاء وقطع الغيار الميكانيكية اللازمة في مجال التصليح والصيانة.
- ومن المرتقب – بحسب المسؤول ذاته – إبرام دائرة الحرب الإلكترونية بالجيش الجزائري عقود تطوير بالشراكة مع كبرى الشركات العالمية. في مجال تكنولوجيا الإعلام والاتصال.

- ومع نهاية 2021، تعززت قدرات الردع للجيش الجزائري بنوع آخر، بحسب ما ذكره موقع "مينا ديفينس" المختص في أخبار التسلح، إذ كشف عن حصول الجيش الجزائري على نظام حرب إلكتروني حديث، وصفه بـ"المتكامل في الحرب الإلكترونية"، استوردته الجزائر من الصين، من قبل شركتين صينيتين وهما "ELLNC" و."CEIC". و نبه إلى أن المعلومات المتوفرة حول هذا النظام الإلكتروني الدقيق "قليلة جدا"، لكنه لفت إلى عدم الخلط بينه وبين نظام التشويش المضاد للطائرات المعروف باسم."CHL-903" ،ومن بين الميزات المتوفرة في هذه المنظومة الإلكترونية الجديدة و"المعقدة" التي سردها المصدر "كشف رادارات العدو لمسافة 600 كليومتر، و تحديد المواقع وتصنيف تحركات العدو على هذه المسافات، وحماية الرادارات والأنظمة المضادة للطائرات من الصواريخ المضادة للإشعاع من خلال تغطية ترددات الرادار."وكذا "منع الاتصالات لمسافة 300 كيلومتر، ومنع العدو في الجو و ا لبحر و البر من استخدام أنظمة تحديد المواقع عبر الأقمار الصناعية لمسافة 300 كيلومتر."

أما بالنسبة لوزير الاتصال عمار بلحيمر، فقد أفاد في تصريح له لقناة الشروق اونلاين، أن سبل التصدي للتهديدات السيبرانية، التي تنتهجها الجزائر، تتمثل في: (بلحيمر، 2021)

- إنتاج محتوى وطني نوعي على المواقع الالكترونية الإعلامية و الأرضيات العلمية.
- تامين الشبكة تكريسا لسيادة الدولة على مجال الرقمنة.
- اشتراط التوطين الرقمي في نطاق DZ ، بالنسبة للمواقع الالكترونية الناشطة في إطار المرسوم التنفيذي المستحدث، و المتعلق بنشاط الإعلام عبر الانترنيت، و حق الرد و التصحيح.
- و بالنسبة لأدوات تأمين المواقع أشار الوزير إلى أن أبرزها، شهادة SSL أو شهادة المفتاح العمومي، التي هي عبارة عن بطاقة هوية رقمية، تسمح بالتحقق من هوية الشخص، أو المنظمة، أو الموقع الالكتروني.

كما أشار السيد عبد العزيز مجاهد، مدير المعهد الوطني للدراسات الاستراتيجية الشاملة، في حوار له على قناة النهار ، أن الإستراتيجية الجزائرية للأمن السيبراني تتمثل في إجراءات احترازية و أخرى للمعالجة، و تشمل التدابير الاحترازية كل فئات و مؤسسات الدولة، بداية من توعية المواطن، و مرورا بكل هياكل و مؤسسات الدولة و مؤسسة الجيش مسؤوليها. (النهار الجديد ennahar tv، 2021) و يتعلق ذلك بمجمل النشطات التي قامت بها الدولة الجزائرية في سبيل تعزيز الأمن السيبراني ، إلا أن هناك أجهزة عملياتية عمدت الدولة إلى إنشائها لغرض مواجهة الجريمة الالكترونية، و تتمثل في: (بارة، 2017، الصفحات 428-429)

- مركز الوقاية من جرائم الإعلام الآلي و الجرائم المعلوماتية للدرك الوطني.
- المعهد الوطني للأدلة الجنائية و علم الإجرام للدرك الوطني.
- المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني.

- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها.

بالإضافة إلى التظاهرات و الملتقيات و الأيام الدراسية ،التي نظمتها مؤسسات الدولة،مؤسسة الجيش حول الأمن السيبراني و التهديدات الأمنية، و الفعاليات التعاونية بين الدول الأعضاء.

و المراسيم الرئاسية الخاصة بالأمن السيبراني خير دليل على اهتمام الدولة بالموضوع،حيث وقع رئيس الجمهورية السيد عبد المجيد تبون خلال سنة 2020، على مرسوم يقضي بإرساء استرتيجية للأمن السيبراني، و إنشاء مجلس و وكالة للأمن السيبراني، و اعتماد نظام يقضة شامل بهدف التصدي للتهديدات الجديدة، و في أوت 2021، تم استحداث قطب جزائي جديد مكلف بمتابعة الجرائم السيبرانية و مكافحتها، و على مستوى الجيش الوطني، استحدثت مصلحة الدفاع السيبراني و مراقبة أمن الأنظمة في نوفمبر 2021. (مجلة الجيش، 2021، الصفحات 37-48)

كما اهتمت مؤسسة الجيش بمسألة الذكاء الاصطناعيAI و حروب الجيل الخامس G5، حيث سلطت جريدة الجيش الضوء على فعاليته في مجال الدفاع السيبراني، و التنبؤ بالهجمات و حجمها و أنواعها، بالإضافة إلى الوسائل و التقنيات التي تستخدم في حروب الجيل الخامس،مثل الذبابات الصغيرة التي تسير الصواريخ، و الروبوتات التي تقتحم ميادين المعارك، و غيرها، و أيضا تنويهها إلى المخاطر التي يفرضها هذه النوع من التقنيات الحديثة على منظومات الأمن الدولية. (مجلة الجيش، 2022)

و حسب البروفيسور "سعدي سلامي" عملت الجزائر مؤخرا ، ضمن برنامج رئيس الجمهورية من خلال السياسة الجديدة، الذي أعطى اهتماما بالغا لجانب الأمن السيبراني، خاصة بالنسبة للتكوين العالي، و ذلك من خلال: (مجلة الجيش، 2022، الصفحات 59-61)

1- إصدار مراسيم رئاسية تتضمن إنشاء مدارس عليا لتكوين إطارات في المجال.

2- إنشاء مركز عملياتي ذو محتوى وطني للأمن السيبراني في الجزائر، يقدم خدمات في مجال الهجمات السيبرانية ، للعديد من المؤسسات و الهيئات.

3- تحيين برامج التكوين و البحث العلمي، في مجال الالكترونيات و الإعلام الآلي ، بما يتلائم مع التكنولوجيات الحديثة، من أجل مواكبة الانتقال من الجيل الرابع إلى الجيل الخامس.

4- تركز الدولة الجزائرية في عملية تطبيق استراتيجيات و آليات التصدي للتهديدات السيبرانية، على أن ذلك من مهام و مسؤوليات جميع فئات و أجهزة الدولة الجزائرية، و ذلك من خلال استراتيجية وطنية شاملة للأمن السيبراني، تبدأ من المواطن؛ من خلال وعيه بالمخاطر الموجودة على الفضاء السيبراني،و تقيده الصارم بالإجراءات السليمة، عند استخدامه للوسائط التكنولوجية، ثم المختصين في مجال الأمن السيبراني، ثم المسؤولين على كافة المؤسسات الفاعلة في الدولة. (www.elmihwar.dz, 2021)

5- تحرص الدولة الجزائرية دائما، على التكيف مع التحولات السريعة للفضاء السيبراني.

6- توفر الدولة الجزائرية من خلال أجهزة الأمن و مكافحة الجريمة الالكترونية، على توفير الحلول ، سواء كانت استباقية، أو علاجية، لحماية الرصيد المعلوماتي.

7- اهتمام مؤسسة الجيش باستدعاء الفاعلين في القطاعات الحساسة للدولة، إلى كافة المحافل و المناسبات المخصصة للبحث في المجال الأمني السيبراني، بغرض الوصول إلى حلول عملية فعالة،و إشراك مسؤولي هذه القطاعات في تنفيذ استراتيجيات الأمن و حماية المعلومات، وهذا ما حدث خلال الملتقى الذي نظمته مؤسسة الجيش بعنوان الأمن السيبراني و الدفاع السيبراني ، كما أشرنا أنفا ؛ حيث حضره كل من وزراء الداخلية و الجماعات المحلية، و التهيئة العمرانية، و الاتصال، و التعليم العالي والبحث العلمي، و الرقمنة و الإحصائيات، و البريد و الاتصالات السلكية و اللاسلكية، و المدير العام للمعهد الوطني للدراسات الإستراتيجية الشاملة، و الأمين العام لوزارة الدفاع الوطني بالنيابة، بالإضافة إلى قادة القوات و الدرك الوطني، و منهم قائد الناحية العسكرية الأولى، و رؤساء دوائر و مدراء و رؤساء مصالح مركزية. (www.elmihwar.dz, 2022)

7. خاتمة:

لقد أبدت الجزائر اهتماما كبيرا بقضية الأمن السيبراني و حروب الجيل الرابع و الخامس، فأعدت إستراتيجية عامة من طرف رئاسة الجمهوري و الجيش للدفاع السيبراني ترتكز على سبعة مجالات تشرف عليها مصلحة الدفاع السيبراني و أمن الأنظمة؛ حيث تتخذ الجزائر إجراءات احترازية و أخرى علاجية، من بينها؛ تأمين الشبكة، و اشتراط التوطين في نطاق DZ، و إنتاج محتوى وطني نوعي على المواقع الالكترونية الإعلامية و العلمية، بالإضافة إلى التأكيد على شهادة المفتاح العمومي SSL، و إنشاء المنظومة الوطنية لأمن الأنظمة المعلوماتية في جانفي 2020،من خلال استحداث أجهزة و وحدات مهمتها الأساسية دحض الجريمة الالكترونية،و تأمين أنظمة المعلومات بالرغم من التحديات التي تواجهها الجزائر ، التي تتمثل في أن 85% من المواقع المشمولة بالدراسة لا تتوفر على شهادة SSL ، كما أن قوانين حماية الخصوصية تمنع من مراقبة المواقع الشخصية للأفراد ، و هذا يحول دون نجاح عملية تأمين أنظمة المعلومات، بالإضافة إلى الكم الهائل من المعلومات التي يصعب التحكم فيها. و تسارع التقنيات و تطويرها بشكل مستمر ، و تعد اعتباطية الاستخدام من اكبر العقبات ، و يرجع ذلك إلى عدم امتلاك الأفراد للاحترافية الكافية في مجال الانترنيت و تكنولوجيا الاتصال عموما.، و تتمثل أهم التقنيات المستحدثة التي تستخدم في تنفيذ الهجمات و الحروب السيبرانية؛ في تقنيات الذكاء الاصطناعي (AL)، كما تستخدم في تأمين المنظومة المعلوماتية. و تتمثل تقنيات الذكاء الاصطناعي في انترنيت الأشياء (LOT)، و تقنية البلوك تشين (Blockchain)،و الحوسبة السحابية (Cloud Computing)، و تقنيات الواقع الافتراضي و الواقع المعزز.و التعلم الآلي و العميق، و انترنيت الأشياء و اللسانيات الحاسوبية، و غيرها، و قد بدأت منظومة الأمن الجزائرية بالاهتمام بتقنيات الذكاء الاصطناعي و التنويه إلى أهميتها في الدفاع السيبراني، و استخدامها كآلية لردع الانتهاكات و الجرائم و التهديدات السيبرانية.

7. قائمة المراجع:

7. Amoroso, E. G. Cyber Security. (S. Press, Éd.2007).
8. *artificial-solutions/digital-transformation*. (s.d.). Consulté le 02 18, 2022, sur site web A: www.artificial-solutions.com/digital-transformation/
9. Authoriey, Accountants. (EBA/GL/2017/06)
10. Dan, B. (2018, 08 10). Artificial intelligence and cerebral palcy,Developmental medicine& child neurology.(*mac keith press , 60* (9)2018)
11. *i-scoop*. (s.d.). Consulté le 02 19, 2022, sur site web A I-SCOOP: https://www.i-scoop.eu/digital-transformation
12. Kemmerer, R. A. *Cyber security.* (Department of Computer Science: University of California Santa Barbara 2003).
13. nasrallah, N. M. *Using Artificial Intelligence(AI)in Banking Services* (introductory Booklet series issue .Vol. 24.2021).
14. *wikipedia*. (s.d.). Consulté le 02 18, 2022, sur site web A wikipedia: https://en.wikipedia.org/wiki/Digital_transformation/
15. *www.akhbardzair.dz*. (2022). Récupéré sur www.akhbardzair.dz/2021/08/30
16. *www.elmihwar.dz*. (2021). Consulté le 02 22, 2022, sur www.elmihwar.dz/2021/05/23
17. *www.elmihwar.dz*. (2022). Récupéré sur www.elmihwar.dz/2021/05/23
18. *www.Kaacenter.android.com*. (2022). Récupéré sur www.Kaacenter.android.com
19. الشمري، صلاح الدين .م .الأمن السيبراني كمرتكز جديد في الإستراتيجية العراقية .قضايا سياسية (السنة الثانية عشر،2020،62)
20. النهار الجديد ennahar tv. (2021). الأمن السيبراني و الحروب الالكترونية: اي استجابة لحماية الجزائر.
21. بارة، سمير .الأمن السيبراني (Cyber Security)في الجزائر:السياسات و المؤسسات .المجلة الجزائرية للأمن الإنساني (2، 2017)
22. عدنان السيد .سوزان ، انتهاك حرمة الحياة الخاصة عبر الانترنيت، مجلة جامعة دمشق للعلوم الاقتصادية ، (29، 3، 2013)
23. بلحيمر، عمار .(2021) .حرب سيبرانية صهيونية مغربية، حوار مع وزير الاتصال الناطق باسم الحكومة،) .م .ا .لاين , Intervieweur)
24. بن مرزوق، عنترة، م .البعد الالكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب .مجلة العلوم الإنسانية و الاجتماعية،((38)، جوان 2018).
25. بورنان، يوسف(2022). https://al-ain.com/article/algeria-thwart-cyber-attacks-2012. Consulté le 02 18, 2022, sur موقع العين الاخبارية- https://al-ain.com/article/algeria-thwart-cyber-attacks-2012 : 19:17 (2022, 01 05) .
26. جبور الاشقر، منى .السيبرانية هاجس العصر .(المركز العربي للبحوث القانونية و القضائية، بيروت، 2017).
27. حامد، علي .س .المعلوماتية و إجرام الانترنيت .(دار الفكر الجامعي، الاسكندرية 2007)

28.حجازي، بيومي .ع .مكافحة جرائم الكومبيوتر و الانترنيت في القانون العربي النموذجي (دار الفكر العرب، الاسكندرية 2006).

29.محمدي، صلاح الدين. (2021). http://www.elmohit.com. تاريخ الاسترداد 17 01, 2022، من موقع موسوعة المحيط: http://www.elmohit.com13:12

30.مجلة الجيش. (ديسمبر،2021). (701).

31.مجلة الجيش (2022) ، فيفري(703)

32. مهديوي، أحمد(2016) Consulté le 11:55 www.alukah.net/liturature/lan. (2016, 11 16). 02 24, 2022, sur 11:55 www.alukah.net/liturature/lan .

33.بوبعاية، نصيرة، الوافي شهرزاد. تحليل البيانات الضخمة باستخدام تقنيات الذكاء الاصطناعي في مهنة التدقيق، دراسة حالة شركة Price Waterhouse Coopers. (مجلة التكامل الاقتصادي ، 9 (3) سبتمبر, 2021)

34.بورنان، يونس. (2022) *حصيلة رسمية..الجزائر تحبط مليون هجمة الكترونية في 2021*. (العين الإخبارية، المحرر) تاريخ الاسترداد 17 03, 2022، من العين الاخبارية: https://al-ain.com