جامعـــة الشهيـــد حمـة لخضر - الـــوادي
كليـة الحقـوق والعلـــوم السيـاسيـــة
قســـــم العلوم السياسية

آثار الذكاء الاصطناعي على الامن السيبراني
دراسة حالة الجزائري

مذكرة تخرج تدخل ضمن متطلبات نيل شهادة الماستر ل.م.د في العلوم السياسية
تخصص سياسة عامة

إعداد الطالبين:

- **عبد الباسط عيساوي**
- **سفيان زيتون**

تحت إشراف الدكتورة:

مجيدي يحيى

لجنة المناقشة

الاسم واللقب	الجامعة	الصفة
معمري حفيظة	جامعة الشهيد حمه لخضر - الوادي	رئيسا
مجيدي يحيى	جامعة الشهيد حمه لخضر - الوادي	مشرفا ومقررا
ركابي صدام	جامعة الشهيد حمه لخضر - الوادي	مناقشا

السنة الجامعية: 2024/2023

شكر وعرفان

بعد الحمد لله وشكره جلّ وعلا

نتقدم بجزيل الشكر وعظيم الامتنان إلى أستاذنا الفاضل المؤطر الذي تفضّل بالإشراف على هذا العمل، حيث قدّم لنا كل النصح والإرشاد طيلة فترة الإعداد فله منّا كل الشكر والتقدير.

كما نتقدم بجزيل الشكر لأعضاء لجنة المناقشة على قبولهم ومراجعة هذا العمل وتصويبه.

الإهداء

إلى الذين صدقوا ما عاهدوا الله عليه إخوة الطريق ورفاق الدرب

إلى الباحثين عن حقيقة العلم والدعوة إليه عقيدة وفكرا ومنهجا في الحياة

إلى آبائنا وأمهاتنا الذين كانوا سببا في وجودنا حيث ربّونا صغارا حتى صرنا كبارا

إلى أبنائنا قرّة العيون وفلذات الأكباد ليفقهوا طريق العلم من بعدنا

و مواصلة مسيرتنا

إلى الذين ناصروا قضية الوعي والالتزام وكانوا حرّاس القضية وحماة الأقصى

الشريف

إلى هؤلاء جميعا نهدي ثمرة جهدنا المتواضعة متمنين أن تكون أحسن

إضافة للاستقرار الأمني في البلاد

المقدمة

في ظل التوجه الدولي نحو الحكومة الإلكترونية أصبحت قضية الأمن المعلوماتي السيبراني من التحديات الكبرى على الصعيدين الإقليمي والعالمي، لا سيما مع تزايد التهديدات الأمنية الإلكترونية، والجزائر كغيرها من الدول سعت منذ انتهاجها للإدارة الإلكترونية حماية منظومتها المعلوماتية من خلال العديد من الأجهزة والخلايا الأمنية. لقد أصبح الأمن المعلوماتي السيبراني ركن أساسي ضمن المنظومة الأمنية المعاصرة، والتي يجب على الدفاع الوطني من خلال أجهزته كالدرك الوطني الجزائري باعتباره مسؤول أمني داخلي تحقيقه في ظل تنامي الجريمة الرقمية، وكذا نظر اللاستغلال المتنامي للشبكات الالكترونية لأهداف إجرامية، والتي تؤثر سلباً على سلامة البنى التحتية للمعلومات الوطنية الحساسة لا سيما على المعلومات الشخصية.

ومع ذلك، على الرغم من أن الذكاء الاصطناعي يحمل فرصًا هائلة، إلا أنه يأتي أيضًا مصحوبًا بتهديدات لا يمكن التنبؤ بها. وبينما يعتبر مصدرا للتطور والابتكار، ووسيلة لتسريع وتيرة التطور التكنولوجي، فإنه يثير أيضا العديد من الأسئلة. وهذا ينذر بعواقب وتحديات اجتماعية وقانونية وأخلاقية جديدة، تتطلب تطوير إطار قانوني شامل لحماية الأفراد والمجتمعات وتنظيم استخدام التقنيات الذكية، مع الحفاظ على التوازن بين التطور التكنولوجي والقانون والأخلاق مسؤولية.

وفي عصر يتسم بـ"الأمن السيبراني"، تظهر المخاطر و"التهديدات السيبرانية" الواحدة تلو الأخرى، وتضاعفت أشكال الهجمات السيبرانية، وتعارضت المصالح والأهداف المعلوماتية مع بعضها البعض، واشتداد سباق التسلح الإلكتروني. الجزائر، مثل بقية دول العالم، تواجه الآن تحديات على المستوى المؤسسي، الحكومي وغير الحكومي، والمجتمع المدني والأفراد، خاصة في مختلف القطاعات، بما في ذلك قطاع الإعلام والاتصال، قطاع المال والأعمال، قطاع التجارة. الخ، لأن الدولة الجزائرية لا بد من إنشاء وكالة وطنية متخصصة في مجال مكافحة "المخاطر السيبرانية"، ويمكن من خلالها تقديم الاستجابات والمساعدة للمؤسسات والأفراد

والقطاعين العام والخاص. من مكافحة حوادث القرصنة والتجسس والقرصنة والحد منها، إلى زيادة الوعي والفهم للتهديدات التي يشكلها التطور الهائل للاتصالات والاتصال عبر "الفضاء السيبراني"، فإن النظام الأمني الجزائري لا يعاني من نقص في القضايا السيبرانية وتحول إلى تطوير استراتيجيات أمنية شاملة لضمان "الأمن السيبراني"، وبما أن أمن المعلومات يعتبر أمناً وطنياً كلياً وشاملاً، فإن قطاع الأمن الجزائري يدرك أن التغيرات السريعة في التكنولوجيا تؤدي إلى تهديدات أقل احتمالاً للنشوء، ولذلك فمن الضروري العمل على ضمان أمن شبكات المعلومات والإنترنت من خلال اتخاذ خطوات مهمة والاعتماد على مجموعة واسعة من الوسائل القانونية والفنية لمواجهة الاستخدام غير القانوني للإنترنت من أجل حماية أنظمة المعلومات ووسائل الاتصال، وبالتالي حماية الدولة والمواطنين والمؤسسات من مخاطر "التهديدات السيبرانية".

نظرًا لأن أمن المعلومات يُعتبر جزءًا من الأمن الوطني الشامل، فإن الأجهزة الأمنية الجزائرية تدرك أن التطورات السريعة في التكنولوجيا تخلق تهديدات معقدة. لذلك من الضروري العمل على تأمين المعلومات وشبكات الإنترنت من خلال اتخاذ خطوات هامة تعتمد على مجموعة واسعة من الوسائل القانونية والتقنية لمواجهة الاستخدام غير المشروع للإنترنت. يهدف هذا الجهد إلى حماية نظم المعلومات ووسائل الاتصالات، وبالتالي حماية الوطن والمواطنين والمؤسسات من مخاطر "التهديدات السيبرانية".

في هذا السياق، نستعرض المجالات المكانية والزمانية للدراسة المتعلقة بالتهديدات السيبرانية، يتحدد المجال المكاني للدراسة من خلال عنوان الموضوع الذي يركز على الدولة الجزائرية. أما المجال الزماني، فيقتصر على الفترة التي تمتد من بداية إنشاء الهيئات والمؤسسات الأمنية المتخصصة في مكافحة التهديدات السيبرانية، بدءًا من عام 2009 وحتى عام 2024.

- **مشكلة الدراسة:**

الإشكالية الرئيسية:

يقتضي استمرار منظومة الأمن الوطني الجزائري والمحافظة على كيانها، ضرورة التكيف مع التغيرات التي تواجهها سواء في البيئة الداخلية أو الخارجية، وتحديد التهديدات السيبرانية التي يواجهها الوطن والمواطن والقطاعات العامة والخاصة، انطلاقا من أهمية الفعل داخل المنظومة بصورة عقلانية لنشاط يقوم به مجموعة من المختصين الفاعلين باستراتيجية واعية لتحقيق أهداف مشتركة وواضحة، ومن هنا يطرح الإشكال الذي يفرض نفسه في هذه الدراسة : **ما مدى قوة الدولة الجزائرية من استخدام التطورات في مجال الذكاء الاصطناعي لتعزيز أمنها السيبراني؟**

وتندرج ضمن السؤال البحثي المركزي الأسئلة الفرعية التالية:

- ✓ما هو دور الذكاء الاصطناعي واهميته في حل المشكلات؟
- ✓ما المقصود بالأمن السيبراني ؟ وما هي أبعاده ؟
- ✓ما هي مجالات استخدام الذكاء الاصطناعي في الأمن السيبراني؟
- ✓ما هي التحديات التي اعتمدتها منظومة الأمن الوطني للتهديدات السيبرانية؟

- **فرضيات الدراسة**

– تساهم تكنولوجيا المعلومات والاتصالات في تحقيق مزايا تعاونية في المجال السيبراني للمؤسسات الأمنية الجزائرية في ظل اعتمادها على أسلوب التسيير.

– تجد الأجهزة الأمنية نفسها مجبرة على اختيار البديل الإستراتيجي المناسب، في إطار مواجهة التحديات السيبرانية في الجزائر.

– كلما كانت الخطط الإستراتيجية محكمة، كلما تحققت الأهداف الأمنية السيبرانية.

أهمية الدراسة

1- **الأهمية العلمية** : يكتسي موضوع الدراسة أهمية علمية انطلاقا من المتغيرات المراد تحليلها، حيث باتت إشكالية" **الأمن السيبراني** "تحظى بوتيرة اهتمام متزايد واجتهادات من طرف الباحثين والأكاديميين، بهدف فهم وتبسيط هذا المفهوم الجديد" **الأمن السيبراني** "وقدرة التفسير لمختلف الحركيات المرتبطة بعاملي التحدي والتهديد من جهة ومدى ضبطه في إطار علمي يمكن الباحث من استيعاب هذه التحولات من خلال معرفة أسبابها وعمق تأثيرها على واقع البني الأساسية(الدول).

2- **الأهمية العملية** :أما عمليا فتقع الأهمية على مدى إدراك مختلف تجلياتها، ومدى تعميق هذا الواقع الراهن ومعرفة العلاقة الترابطية بين الأمن الوطني والتهديدات السيبرانية (تأثير وتأثر)، ما بات يحتم على الأجهزة الأمنية العملياتية المختصة ضرورة تبني إستراتيجيات وسياسات قطرية تهدف إلى التمكن من مكافحة هذه

التهديدات والتحديات الإلكترونية وضمان" **أمان سيبراني** "شامل.

- **أهداف الدراسة:**

✓إبراز وتوضيح المفاهيم الجديدة في الفضاء السيبراني.

✓توضيح العلاقة بين الأمن السيبراني والأمن القومي علاقة التأثير والتأثر.

✓إبراز إسهامات وجهود الدول وخاصة الجزائر في مواجهة التهديدات السيبرانية.

- **أسباب إختيار الموضوع:**

هناك مجموعة من الأسباب أدت إلى اختيار موضوع الدراسة، منها ما هو ذاتي ومنها ما هو موضوعي.

الأسباب الذاتية:

- الرغبة الذاتية في تناول مثل هذا الموضوع لأنه يتوافق مع الميولات الشخصية للطالب في دراسة مواضع ذات طابع قانوني واقتصادي في نفس الوقت.
- توافق موضوع الدراسة مع الخبرة المكتسبة من طبيعة عمل الطالب.

الأسباب الموضوعية:

- التعرف على المزيد من التشريعات والقوانين الضابطة لإستخدام التكنولوجيا بصفة عامة، والأمن السيبراني بصفة خاصة لما لها من أهمية على المستوى العملي.

- الرغبة والتشجيع البحث والتطوير في مجال الأمن السيبراني لتطوير حلول مبتكرة لمواجهة التهديدات الجديدة والناشئة.

- **المنهج المتبع :**

يعتمد هذا من الدراسات في الغالب على المنهج الوصفي الذي سوف يوظف في تحديد مفاهيم مهمة في موضوع الدراسة كتوصيل البيئة الأمنية السيبرانية في الجزائر وتحليل مختلف الفواعل والديناميكيات المرتبطة بالموضوع من تفسير وتحليل التحولات الأمنية في الجزائر وفهم تجلياتها وأبعادها على واقع ومسار منظومة الأمن الوطني الجزائري، وكذلك

1-**المنهج تحليل المحتوى** الذي سوف يساعد في تفسير المواد القانونية التي لها علاقة مباشرة بموضوع الدراسة. و**منهج دراسة الحالة** الذي سوف يساعد في تحديد خصوصية من خلال اعتماد الجزائر كنموذج، لنوضح من خلاله مدى تأثير التهديدات السيبرانية على الأمن القومي الجزائري ورصد التحديات الأمنية التي تحول دون ذلك .

2-الدراسات السابقة

تبلور موضوع الدراسة انطلاقا من مجموعة الأبحاث السابقة التي تعتبر منطلقا مهما في خوض هذه التجربة البحثية، وفي هذا الصدد يمكن الإشارة إلى مجموعة منها:

الدراسة الأولى :كتاب لـ" **منى الأشقر جبور**"بعنوان: "السيبرانية هاجس العصر"، حيث تندرج الدراسة في إطار جهود جامعة الدول العربية، التي أخذت على عاتقها منذ سن وات مهمة نشر الوعي، على مستوى مراكز القرار العربي، بأهمية الأمن السيبراني، والحاجة إلى التعاون لتحقيقه، كما تندرج الدراسة أيضا في إطار الاهتمام الدولي المتصاعد" **بالأمن السيبراني** "بدءا

من الممارسات الحكومية، مرورا بالعلاقات بين الدول، وصولا إلى جهود المنظمات الدولية والإقليمية، منها الأمم المتحدة، الإتحاد الأوروبي، دول الكومنولث، جامعة الدول العربية.

الدراسة الثانية:" **أحمد عبيس الفتلاوي**" الهجمات السيبرانية :مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، حيث دف هذه الدراسة إلى المرتبة المتقدمة التي يحتلها موضوع" الهجمات السيبرانية "في الجهد القانوني، وبالذات عند المؤسسات المتخصصة لتحليل أحكام القانون الدولي العام والجهود الدولية ذات الصلة بتنظيم استخدامها بالخطر أو التقييد.

الدراسة الثالثة :الدراسة التي قام بها كل من " :**عنترة مرزوق** " و"**محي الدين حرشاوي** "حول : "الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية"، وتهدف هذه الدراسة إلى الجهود الجزائرية في مجال تحقيق الأمن السيبراني، والتي تعتبر أن الإرهاب الإلكتروني كأحد أخطر التهديدات المحتملة على الأمن الوطني الجزائري في ظل الثورة التكنولوجية الحديثة.

الدراسة الرابعة :كتاب ل"**إيمان بن سالم** "بعنوان:" جريمة التجنيد الإلكتروني للإرهاب وفقا لقانون العقوبات الجزائري"، حيث يهدف الكتاب إلى محاولة الإحاطة بالشكل المستحدث للإرهاب المتمثل في التجنيد الالكتروني ورفع الستار عن أهم العوامل والاستراتيجيات المتبعة من أجل إنجاح عملية التجنيد، وتوضيح الرؤية وتسيير سبل الحد من الظاهرة.

- **تقسيمات الدراسة:**

لتحقيق الأهداف المرجوة ونظرا لاتساع الموضوع وتشعب فروعه وقصد إعطاء القدر الكافي من الاهتمام والتركيز، تم الاعتماد على منهجية تقسيم الدراسة إلى ثلاث فصول مقسمة إلى مبحثين ويحتوي مضمون كل مبحث على ثلاث مطالب وفق ترتيب الفصول كما يلي:

حيث تناولنا في الفصل الاول الجانب النظري الذي يعالج مفاهيم الدراسة بدأ بالذكاء الاصطناعي الذي أصبح يلعب دورا هاما، نظرا لأهميته في حل المشكلات، ثم تطرقنا إلى الأمن السيبراني وأبعاده وأهميته، أما بالنسبة للفصل الثاني فيتعلق باستخدامات الذكاء

الاصطناعي في الأمن السيبراني والتحديات الأمنية نظرا للتهديدات السيبرانية والجرائم الالكترونية والجوسسة في الفضاء السيبراني .

الفصل الثالث :يحتوي هذا الفصل على دراسة تحليلية لاستخدامات الإنترنت في الجزائر باعتماد إستراتيجيات من قبل الدولة لتحقيق الأمن السيبراني مما أدى إلى بناء حزمة إلكترونية، حيث عرفت الجزائر مجموعة من التهديدات السيبرانية حيث كرّست تحديات أمنية غاية في الأهمية والنجاح.

الفصل الأول:

التأصيل النظري والمفاهيمي للدراسة

مرت البشرية بكثير من الثورات الصناعية، تأتي في مقدمتها الثورة الصناعية الأولى في القرن السابع عشر الميلادي، حيث تم الانتقال من الإنتاج اليدوي في الصناعات إلى الإنتاج باستخدام طاقة البخار، وتدرج التطور إلى استخدام الطاقة الكهربائية مرورًا بثورة المعلومات والاتصالات إلى أن وصلنا الآن إلى الثورة الصناعية الرابعة، التي تعتمد على البيانات الضخمة وتقنيات الذكاء الاصطناعي وأدواته في مجالات عدة حديثة من أبرزها: الروبوتات، وإنترنت الأشياء، والمدن والمنشآت الذكية، والطباعة ثلاثية الأبعاد، والهندسة الوراثية، والمجالات الأمنية والعسكرية وغيرها من المجالات، ويعد الذكاء الاصطناعي (Artificial Intelligence) من أسرع المجالات نموًّا، وله آثار إيجابية مهمة في كثير من المجالات من أبرزها: المجالات المختلفة للأمن بمفهومه الشامل والعمليات العسكرية. وقد اهتمت الدول بتطوير تطبيقات الذكاء الاصطناعي واستخداماتها في المجالات الأمنية والعسكرية (مثل: جمع المعلومات الاستخبارية وتحليلها، والخدمات اللوجستية، والعمليات الإلكترونية، والقيادة والسيطرة، والحرب الإلكترونية وغيرها)، وهذا التطوير تطلب بعض القرارات المتعلقة بالميزانية والقوانين والتشريعات، التي تدعم اتخاذ القرارات الأمنية، وتعزز اعتماد ودعم استخدام تطبيقات الذكاء الاصطناعي في المجالات الأمنية والعسكرية. ونستعرض في هذه الورقة ماهية الذكاء الاصطناعي، وأبرز الفرص والتحديات لاستخدام تطبيقاته في القطاعات الأمنية والعسكرية وأهم مجالات استخدامها في هذه القطاعات.

المبحث الأول: ماهية الذكاء الاصطناعي

الذكاء الاصطناعي (Artificial Intelligence)، أو ما يُعرف اختصارًا بـ(AI) مفهوم شاع دكره وتطور عبر السنين ليصبح واقعا من أبرز التقنيات في القرن الحادي والعشرين؛ إذ يتمثل الهدف الرئيسي منه محاكاة القدرات الذهنية البشرية، مثلا التفكير والتحليل والتعلم، من خلال الأنظمة الحاسوبية.

المطلب الأول: المفهوم والتطور التاريخي للذكاء الاصطناعي

أولا: مفهوم الذكاء الاصطناعي

ظهر مصطلح الذكاء الاصطناعي لأول مرة في ورقة بحثية عام 1956 اقترح فيها المؤلف أنه يمكن إحراز تقدم كبير إذا تمكنت الآلات من "حل المشاكل التي لا يمكن حلها الآن إلا من قبل البشر". وكان يعتقد أن ذلك ممكنًا "إذا أمضت مجموعة مختارة من العلماء صيفًا في العمل معًا". وعلى الرغم من إحراز تقدم محلي في بعض الأحيان، إلا أنه ثبت أن ذلك كان مفرطاً في التفاؤل، انتهى الأمر بالقول:

يعد الذكاء الاصطناعي بأكثر مما يستطيع تحقيقه، وقد توصل معظم العلماء إلى استنتاج مفاده أنهم يتجنبون مصطلح "الذكاء الاصطناعي"، وفضَّلوا الحديث عن "النظم الخبيرة" أو "الشبكات العصبية". ولم يُرَد الاعتبار لعبارة "الذكاء الاصطناعي"، ولم يستعِد العلماء الحماسة له، إلا في عام 2012، مع ظهور ما يسمى تحدي شبكة الصور[1].

يُعرف الذكاء الاصطناعي بأنه فرع من فروع علوم الحاسوب متخصص في تطوير أنظمة قادرة على التعلم واتخاذ القرارات والتنبؤ في مجالات محددة[2].

في أبسط أشكاله، يأخذ الذكاء الاصطناعي البيانات ويطبق بعض القواعد الرياضية (أو الخوارزميات) على البيانات لاتخاذ القرارات أو التنبؤ بالنتائج. على سبيل المثال، البيانات

[1] – فهد الحازمي وفكتور سحاب، يناير/كانون الثاني– فبراير/شباط 2017، " **الذكاء الاصطناعي: تقنياته، تطوره ووعودها**"، مجلة القافلة، العدد 1، المجلد 66، ص37.

[2] – سميث، ماثيو، 2018،" **الذكاء الاصطناعي وتنمية الإنسان**" نحو جدول أبحاث،.

المقدمة هي صور لكلمات أو حروف أو أرقام مكتوبة بخط اليد. الخوارزمية عبارة عن برنامج كمبيوتر يكتبه الإنسان ويحتوي على قواعد مثل الشكل العام والمسافات بين كل حرف وآخر. وهذا يسمح للكمبيوتر بتحليل الصور الممسوحة ضوئيًا للنصوص المكتوبة بخط اليد وتطبيق القواعد للتنبؤ بالحروف والأرقام والكلمات الواردة فيها. وبالمناسبة، تم استخدام هذا النوع من الذكاء الاصطناعي من قبل خدمة البريد الأمريكية منذ عام 1997 لقراءة عناوين الرسائل آلياً[1].

كما تعُد قوة الحوسبة كدلك أمرًا حيويًا في دعم عمليات الذكاء الاصطناعي (AI) والبيانات الضخمة والحوسبة السحابية التي تدعم كل شيء بدءًا من خدمات نقل الركاب إلى العمليات التجارية اليومية وروبوتات الدردشة كأنظمة الذكاء الاصطناعي "المولدة ChatGPT والتي يُمكنها إنشاء محتوى لا يمكن تمييزه عن الإنتاج البشري. ويُعد الذكاء الاصطناعي أحد أهم المحركات الرئيسة للثورة الصناعية الرابعة التي نعيش في ظلها اليوم إلى جانب التحول الرقمي وإنترنت الأشياء.

ثانيا: تاريخ وتطور الذكاء الاصطناعي

في منتصف القرن العشرين بدأت الجهود والاصرار من العلماء لاستكشاف نهج جديد لبناء آلات ذكية، بالاعتماد على الاكتشافات الحديثة في هدا المجال.

الفرع الأول :بروز **الفكرة** .

تعود الاكتشافات الأولى إلى أوائل الخمسينيات. فقد اعتمدت مجموعة من العلماء نهجاً جديداً لابتكار آلات ذكية نتيجة للاكتشافات الحديثة في علم الأعصاب، وذلك باستخدام نظرية رياضية جديدة للمعلومات واللجوء إلى اختراع أجهزة تعتمد على جوهر المنطق الرياضي .

ان أول حدث سجل في مجال الذكاء الاصطناعي هو نشر بحث علمي بعنوان " Computing intelligence and Machinery للعالم الرياضي البريطاني" Turing Alan حيث اخترع اختبار إذا اجتازه الجهاز يصنف بأنه ذكي, وهذا الاختبار عبارة عن أسئلة تسأل من قبل

[1] – برنارد وارد، 2022، "**تطبيقات الذكاء الاصطناعي: كيف استخدمت 50 شركة ناجحة الذكاء الاصطناعي والتعلم الآلي لحل المشكلات**"، تر: عائشة يكن، العبيكان للنشر والتوزيع، الرياض، ،ص23.

شخص يعرف بالحكم" judge "، وتوجه إلى شخص آخر، والى حاسب آلي في آن واحد فإذا لم يتمكن الحكم من التميز بين الشخص والحاسب، فإن الحاسب يجتاز اختبار الذكاء ويصنف بأنه ذكي ولكن هذه لم تكن سوى فكرة بدائية عن هذا العلم [1] .

الفرع الثاني: مراحل تطور الذكاء الاصطناعي

مرت تقسيم الفترات الزمنية لتطور الذكاء الصناعي إلى ثلاث مراحل

المرحلة الأولى: بدأت هذه المرحلة في عام 1950، بعد نهاية الحرب العالمية الثانية مباشرة، مع عمل العالم شانون على ألعاب الشطرنج، وانتهت مع العالم فيغن في عام 1963. هذه المرحلة، التي تميزت باستخدام الحواسيب لإيجاد حلول للألعاب وحل الألغاز، استندت على الفكرة الأساسية لتطوير أساليب البحث في التمثيلات المكانية للحالات وتطورت إلى النمذجة الحاسوبية والنمذجة الحاسوبية القائمة على ثلاثة عناصر:

- تمثيل الحالة البدائية للموضوع قيد البحث (مثل لوحة الشطرنج عند بدء اللعب) .
- اختيار شروط إدراك الوصول إلى النهاية (الوصول إلى التغلب على الخصم) .
- مجموعة القواعد التي تحكم حركة اللاعب بتحريك قطع الشطرنج على اللوحة .

المرحلة الثانية: والتي يطلق عليها المرحلة الشاعرية، والتي بدأت في منتصف الستينات إلى منتصف السبعينات, حيث قام العالم (منسكى) بعمل الإطارات لتمثيل المعلومات، ووضع العالم (ونجراد) نظام لفهم اللغة الانجليزية مثل القصص والمحادثات، وقام العالم (ونستون) بتلخيص كل ما تم تطويره في (معهد الماسيشوستس للتكنولوجيا)، والتي تحتوي على بعض الأبحاث عن معالجة اللغات الطبيعية والرؤية بالحاسب والروبوتات (الإنسان الآلي) والمعالجة الشكلية أو الرمزية.

المرحلة الثالثة: وتسمى المرحلة الحديثة، والتي بدأت في منتصف السبعينيات من القرن العشرين، وتتميز بظهور تقنيات مختلفة للعديد من التطبيقات، وفعلياً نقل جزء كبير من الذكاء

[1] – عقيلة أفندي، 2007، "**إدارة المعرفة التمييز في المؤسسة المعاصرة**"، رسالة ماجستير، جامعة سعد دحلب، البليدة، ص25.

البشري إلى برامج الحاسوب، وتعتبر هذه الفترة العصر الذهبي لازدهار هذا العلم وظهرت العديد من ظهرت العديد من أنظمة الذكاء الاصطناعي الحديثة.

المرحلة المستقبلية : على الرغم من التطورات والتقدم الذي شهده الذكاء الاصطناعي، إلا أن بعض المراقبين يرون أن علم الذكاء الاصطناعي لا يزال في بداياته. ومن المتوقع أن تتطور أساليب وتقنيات الذكاء الاصطناعي بشكل كبير في المستقبل، مع وجود العديد من التطبيقات في الحياة العامة واستخدامها على نطاق واسع من قبل العديد من المستخدمين، وقد تمتد هذه الفترة بين عامي 2015 و 2025[1]

ومع تطور الذكاء الاصطناعي نذكر المجالات التي تم استخدامه فيها[2] :

المجال الهندسي من حيث القدرة على وضع وفحص خطوات التصميم وأسلوب تنفيذه .

في المجال الطبي من حيث التشخيص للحالات المرضية ووصف الدواء لهم .

في القطاع العسكري، اتخاذ القرارات في القتال وتحليل المنشآت ورسم الخطط والإشراف على تنفيذها في القطاع العسكري، القيام بواجبات المعلمين، تقديم المشورة في قطاع التعليم .

وفي المجالات الأخرى المتعددة وفي المصانع مراقبة عمليات الإنتاج والإحلال محل العمال في الظروف السيئة الصعبة، وفي التجارة والأعمال كتحليل حالة السوق والتنبؤ ودراسة الأسعار، وغيرها من المجالات.

[1] – شرقاوي محمد علي، 1996، "**الذكاء الاصطناعي والشبكات العصبية والمكتب العصري الحديث**"، مكتبة الأسكندرية، مصر، ص 28.

[2] – السيد نصر الدين السيد، 2006، "**كيف يفكّر الحاسوب (دليل القارئ الذكي لأسرار الذكاء الاصطناعي**"، دار العين للنشر، القاهرة، مصر، ص ص : 10-11.

المطلب الثاني: خصائص وأنواع الذكاء الاصطناعي

يقوم الذكاء الاصطناعي Intelligence Artificial" " على أساس صنع آلات ذكية تتصرف كما يتصرف الإنسان، ويستخدم أسلوب مقارن للأسلوب البشري في حل المشكلات، بالإضافة إلى أنه يتعامل مع الفرضيات بشكل متزامن وبدقة وسرعة عالية .

أولا: خصائص الذكاء الاصطناعي

للذكاء الاصطناعي عدد من الخصائص التي أدت إلى جذب اهتمام الباحثين نذكر منها:

- ✓ هو علم تطبيقي وليس نظري، يسعى لتسهيل نمط الحياة عمليا، وتقديم حلول لمشكلات عن طريق الآلة .
- ✓ توفير وترشيد النفقات، ويقلل من التكاليف
- ✓ . سيمكن الآلة من حل المشاكل التي تواجهها بطرق مختلفة لاستخدامها في الإنتاج والتحليل.
- ✓ القدرة على الاستجابة السريعة للمواقف، والفهم من التجارب والخبرات. [1]
- ✓ القدرة على اكتساب المعرفة وتطبيقها .
- ✓ استخدام التجربة والخطأ لاستكشاف الأمور المختلفة .
- ✓ القدرة على التصور والإبداع وفهم الأمور المرئية وإدراكها والقدرة على تقديم المعلومات لاستناد القرارات الإدارية .[2]
- ✓ استخدام الذكاء في حل المشاكل المعروضة مع غياب المعلومات الكاملة .
- ✓ التعامل مع المعلومات غير تامة والغامضة .[3]

---

[1] أمينة عثمانية، 2019، "**المفاهيم الأساسية للذكاء الاصطناعي**"، مقال منشور في المؤلف الجماعي بعنوان تطبيقات الذكاء الاصطناعي كتوجه حديث لتعزيز تنافسية منظمات الأعمال، مجلد 01، العدد 01 ،المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، عنابة، الجزائر،، ص 11 .

[2] – النجار فايز جمعة، 2010، "**نظم المعلومات الإدارية –منظور إداري**"، الطبعة 03 ،دار الحامد للنشر والتوزيع، الأردن، ص ص:169 170 .

[3] –عبد الحميد بسيوني، 1998 ،"**مقدمة الذكاء الاصطناعي للكمبيوتر ومقدمة البرولوج**"، الطبعة 01، دار النشر للجامعات، مصر، ص 11 .

ثانيا: أنواع الذكاء الاصطناعي

اعتمادًا على قدراتها، يمكن تصنيف الذكاء الاصطناعي على نطاق واسع إلى ثلاثة أنواع، تتراوح بين ردود الفعل البسيطة والإدراك والتفاعل الذاتي، على النحو التالي:

1- ذكاء الاصطناعي الضيق: AI Weak or AI Narrow هو أبسط أشكال الذكاء الاصطناعي، حيث تتم برمجته للقيام بوظائف معينة داخل بيئته، ويعتبر تصرفه بمنزلة ردة فعل على موقف معين، ولا يمكن له العمل إلا في ظروف البيئة الخاصة به .[1]

2- الذكاء الاصطناعي العام: General AI or Strong AI هذا الذكاء متقدم جداً ولا يعتبر فقط محاكاة للعالم الحقيقي، بل هو ذكاء يتفاعل مع مكونات العالم الفردي ويطمح إلى البناء في المستقبل، ويقارن بين المعدات والبرمجيات الموجودة ويجمع المعلومات ويحللها ويستخلص الخبرات من المواقف المكتسبة ويتميز بقدرته على التراكم وهو مؤهل لاتخاذ قرارات مستقلة وذكية، مثل روبوتات الدردشة الفورية.

3- الذكاء الاصطناعي الخارق: Super AI يعرفه البروفيسور Bostrom Nick :بأنه قدرة تفوق أداء أفضل العقول البشرية في كافة المجالات، وتشمل الإبداع العلمي، الحكمة العامة والمهارات الاجتماعية، وتمتد مجالاته من الكمبيوتر الأذكى من العقل البشري، نجد هذا النوع من الذكاء هو أكثر الأنواع إثارة وهو الذي يمكن أن يشكل الخطورة الأكبر على البشرية[2]، فالذكاء الاصطناعي الخارق نموذج لازال تحت التجربة ويسعى لمحاكاة الإنسان، ويمكن هنا التمييز بين نمطين أساسيين، الأول: أحدهما يحاول فهم الأفكار والمشاعر البشرية التي تؤثر على السلوك البشري ولديه قدرات محدودة على التفاعل الاجتماعي: والآخر هو نموذج نظري

[1] – توربان إفرام، 2000، "**نظم دعم القرارات ونظم الخبرة**"، تعريب سرور علي إبراهيم سرور، الطبعة 01 ،دار المريخ للنشر، السعودية، ص 87 .

[2] – Bostrom, Nick, Op Cit, 05/03/2022 à 18 :00.

للعقل يمكنه التعبير عن الحالات الداخلية للذات، والتنبؤ بمشاعر ومواقف الآخرين والتفاعل معهم، ومن المتوقع أن يصبح الجيل القادم من آلات الذكاء الخارق.[1]

ما هو الفرق بين الذكاء الاصطناعي الضيق والعام؟

يمكن توضيح الفرق بين الذكاء الاصطناعي الضيق والعام فيما يلي:

الذكاء الاصطناعي الضيق

- يُستخدم للعمل ضمن مجموعة من الوظائف المحددة مسبقًا التي يتم تعليم البرمجة إكمالها أو حلها.
- لا يحقق الوعي الذاتي.
- لا يمكنه نقل المعرفة إلى مجالات أو مهام أخرى.

الذكاء الاصطناعي العام

- يُستخدم لإنجاز أي نوع من المهام التي يمكن أن يتخيلها عقله.
- يتم تطويره ليكون ذكيًا حقًا ومدركًا لذاته تمامًا.
- يستخدم نقل المعرفة لمعالجة المشكلات والمجالات الجديدة.

ما هي الأنواع الأربعة للذكاء الاصطناعي وفقًا للوظيفة؟

هناك أربعة أنواع رئيسية من الذكاء الاصطناعي وفقًا للوظيفة، وهي على النحو التالي:

1- الآلات التفاعلية Reactive Machines

تشير الآلات التفاعلية إلى الأجهزة التي تتفاعل مع بعض المدخلات والمخرجات، وتستجيب لمختلف الأوامر، وذلك دون استخدام الذاكرة الوظيفية، وهو أبسط أنواع الذكاء الاصطناعي. وتُعد الآلات التفاعلية هي الأكثر شيوعًا في تصميم الألعاب، إذ تُستخدم في إنشاء الخصوم، فيرد الخصم على الهجمات أو الحركات دون أن يدرك الهدف العام للعبة.

[1] – عبد الوهاب شادي، وآخرون، 2018، "**فرص وتهديدات الذكاء الاصطناعي في السنوات العشر القادمة**"، تقرير المستقبل، العدد27 ،مركز المستقبل للأبحاث والدراسات المستقبلية، متاح على الرابط:

http://www.academia.edu/ consulté le 06/04/2024/à 15 :22.

كما تستخدم روبوتات الدردشة الذكاء الاصطناعي التفاعلي في الرد على الرسائل بالمعلومات الصحيحة وهي الروبوتات المُستخدمة في خدمة العملاء، ولذلك فهو أداة تسويق مهمة تعزز من إنتاجية المسوقين، إضافة إلى دور هذا النوع من الذكاء الاصطناعي في تحليل سلوك العملاء وأداء الحملات واتجاهات السوق، ويستخدم المسوقون تلك المعلومات في تحسين حملاتهم التسويقية.

2- الذاكرة المحدودة Limited Memory

يستخدم الذكاء الاصطناعي للذاكرة المحدودة كمية محدودة من البيانات أو التعليقات للتعلم ولعمل تنبؤات أفضل، ولكن باستخدام ذاكرة محدودة لا تحفظ الذكريات لفترات طويلة.

ولا بد من تزويد خوارزميات الذاكرة المحدودة بمعلومات دقيقة ومُحدثة وذات صلة، لأن عملها على بيانات قديمة قد يؤدي إلى ارتكاب أخطاء أو تقديم تنبؤات غير دقيقة.

ويُعد ChatGPT أبرز مثال لهذا النوع من الذكاء الاصطناعي، إذ يحتوي على حد 4000 رمز، ولا يتذكر أي شيء من محادثة حالية بعد هذا الحد.

ويُستخدم الذكاء الاصطناعي للذاكرة المحدودة في التسويق، إذ يعمل على تحليل كميات كبيرة من البيانات، وبناء عليها يتخذ المسوقون قرارات مستنيرة بشأن استراتيجياتهم التسويقية، ووفقًا لتلك البيانات يقدم هذا النوع العديد من التنبؤات والتوصيات.

3- نظرية العقل Theory of Mind

يشير مصطلح نظرية العقل إلى قدرة آلة الذكاء الاصطناعي على نسب الحالات العقلية إلى الكيانات الأخرى، وهو أحد أنواع الذكاء الاصطناعي الذي لا يزال قيد التطوير.

وتعمل نظرية العقل على إنشاء آلات لديها القدرة على تحليل الصوت والصورة وأنواع أخرى من البيانات، بهدف التعرف على المشاعر البشرية ومحاكاتها ومراقبتها والاستجابة لها بشكل مناسب، فيكون الذكاء الاصطناعي قادرًا على فهم البشر واكتشاف حالتهم العاطفية.

وعلى سبيل المثال، إذا كان أحد العملاء ساخطًا وغير راضيًا عن خدمة ما؛ فإن الذكاء الاصطناعي العاطفي يستطيع فهمه ومن ثم الاستجابة له بلباقة أكبر.

4- الوعي الذاتي Self Aware

الوعي الذاتي أو الذكاء الاصطناعي الواعي، هو المرحلة التالية في تطور نظرية العقل، إذ تكون الآلات لديها القدرة على فهم المشاعر الإنسانية، ويكون لتلك الآلات أيضًا مشاعر ومعتقدات واحتياجات، وهذا النوع لم يتحقق بعد، فهو موجود من الناحية الافتراضية.

المطلب الثالث: أهمية الذكاء الاصطناعي في حل المشكلات وأبعاده

أولا: أهمية الذكاء الاصطناعي

لا يزال يُنظر إلى الذكاء الاصطناعي (AI) على أنه خيال علمي لن يتحقق أبدًا.

تزداد أهمية الذكاء الاصطناعي مع تطور الاقتصاد وسوق العمل في الثورة الصناعية الرابعة.[1]:

- تمكين الإنسان من استخدام اللغة الإنسانية في التعامل مع الآلات بدلًا من لغات البرمجة الحاسوبية، وهو ما يجعل الآلات في متناول الجميع بمن فيهم ذوو الإعاقة، بعدما كان التعامل مع الآلات المتقدمة مقتصرًا على المتخصصين.

- يلعبون دورًا مهمًا في العديد من المجالات الحساسة، مثل المساعدة في تشخيص المرض ووصف الأدوية وإجراء العمليات الجراحية وعلاج الأمراض الخطيرة. الاستشارات القانونية والمهنية، والتعليم التفاعلي مثل التدريب على الطيران والقيادة والأمن والدفاع.

- وتبرز أهميتها في المجالات التي تُتخذ فيها القرارات. فكونها مستقلة ودقيقة وموضوعية، فإن عملية اتخاذ قراراتها خالية من الخطأ أو التحيز أو العنصرية أو التحيز أو التدخل الخارجي أو الشخصي.

يسهم الذكاء الاصطناعي إسهامًا إيجابيًا في العديد من المجالات والقطاعات، حيث يساهم في زيادة الإنتاج، سواء في الإنتاج المادي أو الخدمات، وكذلك في الوقاية من الجرائم الإلكترونية وتطوير الخدمات التعليمية والطبية التي تساعد على منع الجرائم الإلكترونية.

[1] - ابتسام ناصر هويمل وخولة عبد الله المفيز، 2022، "**الذكاء الاصطناعي: مستقبل إدارة الموارد البشرية**"، العبيكان للنشر والتوزيع، الرياض، ص 59-58.

وتشمل هذه المجالات الوقاية من الجرائم السيبرانية، وتطوير الخدمات التعليمية والصحية، لا سيما في الاستجابة للجائحة التي تحققت خلال جائحة كوفيد-19، بالإضافة إلى بناء وتطوير المدن الرقمية والحكومات الرقمية.

تستخدم وكالات الأمم المتحدة الذكاء الاصطناعي. فعلى سبيل المثال، يقوم مشروع خريطة الجوع التابع لبرنامج الأغذية العالمي بجمع البيانات لتحديد مناطق الجوع. كما يعمل البرنامج على تطوير شاحنات تعمل عن بُعد لتوصيل المساعدات الطارئة في مناطق الخطر. من المتوقع أن ينمو سوق التعليم إلى 4 مليارات دولار أمريكي[1] وبحلول عام 2023، سيصل معدل النمو السنوي المركب المقدر إلى 74% بسبب حجم سوق الذكاء الاصطناعي في التعليم

يمكن أن يساهم الذكاء الاصطناعي والروبوتات والأتمتة الذكية الأخرى بما يصل إلى 15 تريليون دولار أمريكي في الناتج المحلي الإجمالي العالمي بحلول عام 2030، مع تحقيق فوائد اقتصادية كبيرة، وفقًا لتحليل شركة برايس ووترهاوس كوبرز. (PricewaterhouseCoopers). ستولد هذه الثروة الجديدة أيضًا الطلب على العديد من الوظائف، ولكن هناك أيضًا مخاوف من أنها قد تحل محل العديد من الوظائف الحالية[2].

لكن التقدم لا يحدث على الحدود النظرية لهذا المجال فحسب؛ فالأدوات التي تستخدم التعلم الآلي هي خاليا أنظمة الغد فائقة الذكاء، والعديد منها موجود بالفعل في السوق، وأخذ استخدامها ينمو بسرعة في قطاعات مثل التمويل والرعاية الصحية والتصنيع.

يمكّن الذكاء الاصطناعي من العمليات وتطوير منتجات وخدمات جديدة، وتحسين الجودة والكفاءة يمكن للذكاء الاصطناعي أن يؤثر على جميع قطاعات الاقتصاد تقريبًا وجميع جوانب التجارة، بما في ذلك التجارة في الخدمات.

وسيكون للذكاء الاصطناعي التأثير الأكبر على الأمور الأكثر روتينية في الوظائف القائمة على المعلومات وفي وظائف الأعمال المتعلقة بتقديم القروض أو معالجة الحسابات أو تحليل

[1] – للاستزادة، انظر: https://shorturl.at/clCPV (تاريخ الدخول: 7 يوليو/تموز 2023)

[2] –Price WaterhouseCoopers (PWC),The macroeconomic impact of artificial .intelligence,UK,London, February 2018, p. 3

الاختبارات الطبية، من بين أمور أخرى. وفي الوقت نفسه، يمكن للذكاء الاصطناعي أن يدعم التجارة على نطاق أوسع من خلال تحسين تيسير التجارة وترقيتها. وكال التطبيقين يساعدان المزيد من الشركات للانخراط في التجارة، لاسيما الشركات المتوسطة والصغيرة والمتناهية الصغر، حيث ينخفض الوقت والتكلفة وتوفير فرص التصدير. وسيكون الذكاء الاصطناعي في قلب تسهيل التجارة الرقمية؛ حيث يُتيح استخدام تكنولوجيا الاتصالات الحديثة في تبسيط حركة السلع عبر الحدود، وتقدر منظمة التجارة العالمية أن الإجراءات الجمركية غير الفعالة تمثل نحو 6 % من إجمالي التباين في تكاليف التجارة[1].

ثانيا: أبعاد الذكاء الاصطناعي

يتم استخدام الذكاء الاصطناعي في مجموعة متنوعة من المجالات، بما في ذلك القطاع الطبي والأسواق المالية والمصرفية والعسكرية والسيارات ذاتية القيادة والمنازل الذكية والألعاب الذكية والاستراتيجية. يتطور هذا المجال بوتيرة أسرع مما توقعه العلماء والخبراء، كما يتضح من التطور اليومي للبرامج الخاصة بالهواتف الذكية والأجهزة اللوحية وأجهزة الكمبيوتر.

نقسم الذكاء الاصطناعي في عالمنا هذا إلى أربعة أنواع أساسية، تشبه إلى حدّ كبير هرم ماسلو للاحتياجات الأساسية، حيث أنّ أبسط أنواع الذكاء الاصطناعي تستطيع القيام بالوظائف الأساسية فقط، في حين أنّ الأنواع الأكثر تقدّمًا هي بمثابة كيان واعٍ تمامًا بذاته وبما يدور من حوله، ويشبه إلى حدّ كبير الوعي البشري. هذه الأنواع الأربعة هي كما يلي:

- ✓الآلات التفاعلية .Reactive Machines ويمثل أوّل مراحل الذكاء الاصطناعي، ومن الأمثلة عليها الأجهزة البسيطة التي تتعرّف على الوجه ولعبة الشطرنج على الالواح الذكية.
- ✓الذاكرة المحدودة .Limited Memory وهذا النوع من الذكاء الاصطناعي، نجد يستخدم في السيارات ذاتية القيادة، والتي تخزّن مختلف البيانات المتعلّقة بحالة الطرق والسيارات

[1] – World Economic Forum ،Mapping TradeTech: Trade in the Fourth.Industrial Revolution, Insight Report ،December, 2020, p.18

الأخرى في الطريق وغيرها من العوامل، وتتخذُ بناءً على هذه البيانات قرارات بشأن الطريق الذي ستسلكه أو ردّة الفعل المعيّنة التي ستقوم بها.

✓ نظرية العقل .Theory of Mind لا يزال هذا النوع سوى فكرة نظرية، أو مشروعٍ لا يزال العمل جاريًا على تطويره. يمكننا القول أنّ نظرية العقل هي المرحلة المقبلة من أنظمة الذكاء الاصطناعي التي يعمل العلماء حاليًا على ابتكارها وتطويرها. وفي هذا النوع ستتمكّن الآلة (بفضل تقنية الذكاء الاصطناعي) من فهم الكيانات التي تتفاعل معها، ومعرفة احتياجاتها ومشاعرها ومبادئها، بل وحتى عملية التفكير التي تقوم بها.

الوعي الذاتي Self Aware يعتبر هذا النوع ذات بعدا مجهول قد يتمكّن البشر أخيرًا من تطوير ذكاء اصطناعي واعٍ بذاته. إنها مثل شيء خارج من فيلم خيال علمي. قد يثير هذا النوع من الذكاء الاصطناعي الكثير من الآمال، ولكنه يثير أيضًا الكثير من المخاوف. وذلك لأن البشر سيضطرون إلى التفاوض مع آلات من صنعهم، وستفسح نتائج هذه المفاوضات المجال للكثير من الافتراضات والتوقعات والخيالات.

المبحث الثاني :ماهية الأمن السيبراني

الأمن السيبراني هو حماية أجهزة الكمبيوتر والشبكات والتطبيقات البرمجية والأنظمة والبيانات الهامة من التهديدات الرقمية المحتملة. تتحمل المؤسسات مسؤولية حماية البيانات للحفاظ على ثقة العملاء والامتثال للمتطلبات التنظيمية. توظف المؤسسات تدابير وأدوات الأمن السيبراني لحماية البيانات الحساسة من الوصول غير المصرح به ولمنع انقطاع الأعمال بسبب نشاط غير مرغوب فيه على الشبكة. تعتمد المؤسسات الأمن السيبراني من خلال تبسيط الدفاع الرقمي بين الأشخاص والعمليات والتكنولوجيا.

المطلب الأول :مفهوم الأمن

إن الأمن ليس من المفاهيم المتفق عليها بصورة عامة ومن الصعب إعطاء تعريف محدد لما تعنيه كلمة "الأمن" شأنها في ذلك شأن كثير من الكلمات المتداولة التي تفتقر إلى تعريف محدد لها يمكن تقديره بشكل قاطع [1].

يعتبر مصطلح الأمن من أكثر المصطلحات استخداماً في مجال العلوم السياسية، وخاصة في مجال العلاقات الدولية، وبشكل أكثر تحديداً فيما يسمى بأدبيات الدراسات الأمنية. فالأمن حاضر دائما في الاهتمامات اليومية والعامة لجميع الأفراد، حيث يشمل جميع جوانب الحياة الإنسانية، ويمكن اعتبار الأمن من أهم المحددات التي تحكم سلوك الأفراد والجماعات وحتى الوحدات السياسية على حد سواء. وقد أدى البحث المستمر عن الأمن إلى تكوين التجمعات والمجتمعات البشرية، ويمكن اعتبار عملية البحث عن الأمن خاصية غريزية، كما أن الحيوانات أيضًا تميل إلى العيش في جماعات مع بني جنسها من أجل الحصول على الأمن.

تتسم دراسة مفهوم الأمن باختلاف وتباين كبيرين في المفاهيم بين الباحثين والمهتمين به، وذلك تبعاً للمنهج المتبع في تحليل المصطلح وشخصية الباحث ونفسيته المتداخلة مع البيئة الجغرافية والسياسية والاجتماعية.

---

[1]– سليمان عبد الله الحربي، صيف 2008، "**مفهوم الأمن: مستوياته وصيغه وتهديداته (دراسة نظرية في المفاهيم والأطر**"، المجلة العربية للعلوم السياسية، عدد 19، ص.9.

ومن ذلك، يعد مفهوم الأمن أحد المفاهيم التي تتشعب دلالتها، حيث يتسع هذا المفهوم ليشمل مضامين متعددة تتداخل مع شتي أنظمة الحياة، ليشمل الإصلاح الاجتماعي، والارتباط بالقضاء والعدل، والتربية والإرشاد كما أن لفظ الأمن هو من الألفاظ ذات الدلالات الواضحة البينة، إذ تعرف حقيقته عند النطق به .ومن أهم المراجع التي يمكن الاعتماد عليها في تحديد مفهوم الأمن، القرآن الكريم وما تضمن من آيات تحمل هذا المعنى العميق:

قال الله تعالي: ﴿**وضرب الله مثلا قرية كانت آمنة مطمئنة يأتيها رزقها رغدا من كل مكان فكفرت بأنعم الله فأذاقها الله لباس الجوع والخوف بما كانوا يصنعون**[1]﴾

وقوله تعالى: ﴿**الذين أمنوا ولم يلبسوا إيمانهم بظلم أولئك لهم الأمن وهم مهتدون**[2]﴾

وقوله عز وجل: ﴿**وليبدلنهم من بعد خوفهم أمنا**﴾"[3]. "

الأمن لغة: مصدره أمن، الأمان والأمانة بمعني: وقد أمنت فأنا آمن، وأمنت غيري من الأمن والأمان ضد الخوف [4] وهو بذلك اطمئنان النفس وزوال الخوف ومنه الإيمان والأمانة، المعني الذي ورد في التنزيل العزيز بقوله تعالى:" وآمنهم من خوف" [5]، ومنه قوله تعالى:﴿ **وهذا البلد الأمين** ﴾[6] أي الآمن، وهو من الأمن، وعليه فإن مفهوم الأمن قديم جدا، فعندما عدنا إلى النص القرآني وجدنا مادة أمن ذكرت مئات المرات بنسبة تواتر وتوارد مرتفعة جدا والسبب في ذلك راجع إلى أنها المادة التي اشتق منها الإيمان[7] .

---

[1] سورة النحل، الآية 112

[2] – سورة الأنعام، الآية 82

[3] – سورة النور، الآية 55

[4] – الفيروز أبادي،2005، "**القاموس المحيط**"، ط8، مؤسسة الرسالة للطباعة والنشر والتوزيع، لبنان ،ص. 1176.

[5] – سورة قريش، الآية 4

[6] – سورة التين، الآية 3

[7] – صفية نزاري،2010،" **الأمن الثقافي لمنطقة المغرب العربي في ظل تنامي العولمة: دراسة مقارنة لحالات: الجزائر، تونس والمغرب**"، مذكرة مقدمة لنيل شهادة الماجستير في العلوم السياسية، تخصص علاقات مغاربية ومتوسطية في التعاون والأمن، قسم العلوم السياسية، جامعة باتنة، ص36

1- **الأمن اصطلاحا:** أما فيما يتعلق بالجوانب الاصطلاحية لمفهوم الأمن، فعلى الرغم من الأهمية القصوى للمفهوم وانتشار استخدامه على نطاق واسع، إلا أنه من الصعب حصر الأمن في مفهوم واحد. حيث تتسم دراسة مفهوم الأمن باختلافات وتوسعات كبيرة، كما أن المهتمين بالأمن يهتمون بالأمن من حيث المفهوم. ويعود استخدام مصطلح الأمن إلى نهاية الحرب العالمية الثانية في الأدبيات التي تسعى إلى تحقيق الأمن وتجنب الحرب. أما في الموسوعة البريطانية فيشير الأخير إلى الأمن من حيث المفهوم: وقد أدى ذلك إلى إنشاء وزارات الأمن القومي في معظم الدول والاهتمام بحالة الأمن.

ويعرف" هنري كيسنجر" الأمن على أنه: "وفيما يلي عدد من التعريفات التي وضعها باحثو العلاقات الدولية من خلال معظم النظريات التي تم تناول الأمن من خلالها. ويسعى المفكرون من خلال هذه التعاريف إلى توضيح المعاني التي ارتبط بها مصطلح الأمن لدى الباحثين بمتغيرات التهديد وانعدام الأمن، على الرغم من الاختلافات حول مضمونه ومصادره. لذا فانه لا يمكن تصور الأمن دون اللاأمنinsecurity والعكس صحيح [1]، ونجد في الدراسات العربية العلامة "ابن خلدون" يرى أن هذا المصطلح يعادل القوة لأنها سر وجود الدولة وسبب استمرارها واستقرارها فإن وجدت القوة وجدت الدولة، وإن غابت القوة زالت الدولة من الوجود، وتتجسد القوة بالملك والجيش من جهة والمال من جهة أخرى، ويلخص ابن خلدون الأمن بأنه الأمن من الهزيمة دون ذلك لابد من مضاعفة الحذر، القوة، الاقتدار، التحشد، الدفاع والحماية [2]، أما في الأدبيات الغربية نجد أن مصطلح الأمن تعددت دلالاته ومعانيه ففي كتاب "الأمير" يرى نيكولاميكيافيلي machiavel Niccole أن الأمن مرهون بالقضاء على المنافسين، لأن القاعدة العامة بالنسبة إليه تقول "من يسمح لأي كان بأن يصبح قويا يدمر ذاته"، ويربط والترليبمان lipman walter بين الأمن والحفاظ على المصلحة، فيقول الأمة الآمنة هي التي لا يتحتم

[1]- أحمد إيدابير، 2011 ،"**التعددية الاثنية والأمن المجتمعي : دراسة حالة مالي**"، مذكرة مقدمة لنيل شهادة الماجستير في العلوم السياسية والعلاقات الدولية تخصص الدراسات الأمنية والاستراتيجية، قسم العلوم السياسية والعلاقات الدولية، جامعة الجزائر3، ص60 .

[2]- عبد الرحمان ابن خلدون،2004، "**المقدمة**"، ط1، دار الفكر، بيروت، ص141

عليها التضحية بمصالحها المشروعة لتجنب حرب ما، وفي الوقت نفسه تكون قادرة، إذا ظهر في وجهها أي تحد، على حماية مصالحها الحيوية باللجوء إلى الحرب [1]، أما علماء السياسة فقد عرفوا الأمن في الإطار الفكري تبعا للنظرية التي يتم من خلالها النظر للمصطلح وهي ثلاثة: النظرية الواقعية، النظرية الليبرالية ونظرية الاستقرار المهيمن.

المطلب الثاني :مفهوم الأمن السيبراني

1- **السيبرانية لغة** :يعود منشأ كلمة" السيبراني "إلى اللغة اليونانية، وبالذات كلمة "كبيرنتيك"وتحمل هذه الكلمة معنى يدمج بين المقصودين :التوجيه (steering) والحوكمة (gouvermance)، حيث استخدم" نوربرت فينر(Norbert Wiener) فمصطلح" السيبرانية" لأول مرة عام1948 ، من أجل وصف نظام التغذية الراجعة(Feedbak)

الذي يعمل على الإستفادة من مخرجات الأنظمة في ظبط مدخلاتها والتحكم فيها، واستقرار أدائها ورأى" فينر "أنه يمكن تطبيق هذا النظام على نطاق واسع.[2]

ووفقاً لقاموس الأمن السيبراني، يشير مصطلح "سيبراني" إلى الهجمات عبر الفضاء الإلكتروني التي تهدف إلى السيطرة على المواقع أو الهياكل المحمية إلكترونياً أو تدميرها، ولكن بالرجوع إلى خبراء اللغة العربية باستثناء الترجمة العربية، فإنهم يجدون أنفسهم يواجهون صعوبات في اختيار مصطلح أقرب إلى المصطلح الإنجليزي "سيبراني".

العنوان (convention on cybercrime) إلى اللغة العربية(الإتفاقية المتعلقة بالجريمة، الإلكترونية، ويعود السبب في عدم وجود مصطلح مناظر في اللغة العربية).[3]

2- **السيبرانية اصطلاحا** :وهو يعني نظاماً إلكترونياً مركزياً يربط بين الحواسيب والأنظمة الآلية وينسق بين جميع الآلات والمعدات التي تستخدمها المدينة والدولة والعالم بشكل شامل، من

---

[1]- حمد سعيد الموعد، 1999، "**أمن الممرات المائية العربية**"، إتحاد كتاب العرب، دمشق، ص9.

[2]- سعد علي الحاج علي بكري، أوت2017 ،" **الأمن السيبراني ومعضلة حمايته ..عولمة التعليم العالي ..الرقمي**"، جريدة العرب الاقتصادية الدولية، العدد24، ص 24 .

[3]- أحمد عبيس نعمة الفتلاوي، 20 جانفي2018 ، "**الهجمات السيبرانية :مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر**"، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الرابع، السنة الثامنة،2016 ، ص214

أجل تحقيق أعلى درجات الرفاهية للبشرية جمعاء، وليس كنظام إداري عصبي إلكتروني يمتد إلى جميع مجالات البنية الاجتماعية. يمكن اعتباره

الأمن السيبراني هو مجموعة الوسائل التقنية والإدارية، والتي يتم استخدامها لمنع الاستخدام غير مصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات الشخصية ولحماية المواطن من مخاطر الفضاء السيبراني[1] .

يمكن تعريف الأمن السيبراني على أنه أمن الشبكات المتصلة بالإنترنت ونظم المعلومات والبيانات والمعلومات والأجهزة المتصلة بالإنترنت. وعلى هذا النحو، فهو مجال يُعنى بالإجراءات والتدابير ومعايير الحماية التي يجب اتخاذها أو الالتزام بها في مواجهة تهديد ما أو للتقليل من تأثيره في أشد وأسوأ السيناريوهات. ويرتبط هذا الأمن ارتباطاً وثيقاً بأمن المعلومات، حيث أن الوصول إلى المعلومات ونقلها وعرضها وتداولها وتشويهها واستغلالها غالباً ما يكون وراء الهجمات على الشبكات والإنترنت.

كما أن الأمن السيبراني ذلك النشاط الذي يؤمن حماية الموارد البشرية والمالية، المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار، التي تترتب في حال تحقيق المخاطر والتهديدات.

كما يتيح الفرصة لإعادة الوضع إلى ما كان عليه، بأسرع وقت ممكن، بحيث لا تتوقف عجلة الإنتاج، ولا تتحول الأضرار إلى خسائر دائمة[2].

إذا،" **الأمن السيبراني**" سيما أن التهديدات السيبرانية أصبحت جزءا لا يتجزأ من التكتيكات الحديثة للمخاطر والهجمات السيبرانية بين الدول.

---

[1]– ليال بيطار،20 جانفي 2018،" **ماذا يعني الأمن السيبراني؟**"، الوقيت:17 ،http//anbaaoline.com

[2]– منى الأشقر جبور،2013، "**السيبرانية هاجس العصر**"، المركز العربي للبحوث القانونية والقضائية، بيروت، ص29

المطلب الثالث: أبعاد الأمن السيبراني

1- الأبعاد العسكرية :

تطورت بدايات الإنترنت في بيئة عسكرية، بشكل أساسي، لتضاف إليه فيما بعد البيئة الأكاديمية، تتمثل في أبحاث تخدم تطوير القدرات العسكرية، والإنجازات العلمية التي تحافظ على تفوق بلد آخر، فتتمثل خطورة الهجمات السيبرانية، والتجسس والسرقة والاختراق التي ترجمت ماديا، سواء باندلاع صراع مسلح لاحق، كالذي وقع بين روسيا وجورجيا، أو بانقطاع الاتصال بالانترنت في أستونيا، بين الدولة والمواطنين والتشويش على الإدارات الحكومية، كما واجه خبراء أمريكيين خطابا مفتوحا إلى الرئيس "جورج بوش) Bush. W George) "في أيلول 2007 محذرين إياه، من خطر الهجمات السيبرانية على البنية التحتية الأمريكية، التي تضم إلى الدفاع، إمدادات الطاقة الكهربائية، والمياه والاتصالات السلكية واللاسلكية، والخدمات الصحية والنقل والانترنت[1].

2-الأبعاد الاقتصادية :

إن الغرض من أمن المعلومات ليس كسب المال، بل حماية الموارد الاقتصادية وتجنب ضياعها أو فقدانها. إن تحديد الفوائد المستمدة من المعلومات ليس بالأمر السهل، كما أن تقدير تكلفة الأمن المتمثلة في السمات المرصودة وتكلفة المنتجات الأمنية والتدريب وبناء مراكز التحكم وغيرها من الأمور ذات الصلة أمر صعب للغاية. إن حساب تكلفة أمن المعلومات والخسائر الناجمة عن الأخطاء والأفعال الضارة أمر صعب للغاية، حيث يتم تحديد هذه التكاليف حسب احتياجات المنظمة. ويرجع ذلك إلى أنه لا يمكن تحديد التكاليف من حيث الأصول التي يتم العمل عليها والتي تحتاج إلى حماية، والأضرار الناجمة عن عدم كفاية الأمن والتعرض المحتمل للهجمات والاختراقات.[2]

[1] – منى الأشقر جبور، مايو2012، "**الأمن السيبراني: التحديات ومستلزمات المواجهة**"، المركز العربي للبحوث القانونية والقضائية،ص16

[2] – أوس مجيد غالب العوادي،2016 ،"**الأمن المعلوماتي السيبراني**"، مركز البيان للدراسات والتخطيط، بيروت، ص06.

3- الأبعاد الاجتماعية :

يشير تقرير مؤسسة Sosial Are we إلى نحو 5.2 مليار نسمة، أي ما يعادل 35 %من سكان العالم يستخدمونه، ولا شك في أن هناك دورا للانترنت في تعبير المواطن عن تطلعاته في المجالات المختلفة، سواء سياسية أو علمية أو اقتصادية أو ثقافية، ....الخ، وبعض من الموارد المنشورة والمفيدة وتؤثر بالإيجاب على أخلاقيات المجتمع، والبعض الآخر يمثل تهديدا له، كالإرهاب ونشر الفكر المتطرف، ومحاولة تجنيد الشباب، والترويج للاتجار بالممنوعات ... الخ. بالإضافة إلى جعل المواطنين أكثر انكشاف على الثقافات الأخرى، ومن ثم تعرض القوميات والهويات لعمليات اختراق خارجي قد تؤثر على الأفكار والتوجهات والعادات، خاصة أنها قد تخرج عن النسق العام للدولة، وتسبب في تهديد السلم الاجتماعي، وعليه فلا بد من العمل على توعية المواطنين بتلك النوعية من المخاطر لتحقيق الأمن السيبيري في بعده المجتمعي[1].

4- الأبعاد السياسية :

وتتمثل في مسؤولية الدولة وسيادة الدول

- مسؤولية الدولة تتحمل الدولة مسؤولية رئيسية في توفير الأمن السيبراني. وينبغي أن تتجاوز أنشطة الدولة تعزيز وتشجيع البحث والتطوير في مجال الأمن إلى تعزيز ثقافة أمنية على المستوى الاستراتيجي وضمان الوعي بأفضل الممارسات في مجالات الإدارة الوقائية، والإبلاغ، وتبادل المعلومات، وتبادل المعلومات، والإنذار، والأمن، وإدارة المخاطر وفيما يلي بعض القضايا الرئيسية التي يجب معالجتها.
- **سيادة الدول:** يتعارض الاتجاه نحو التبسيط والكفاءة في مجال الأمن مع تعقيد الاحتياجات والبيئات، مما يجعل الاستعانة بمصادر خارجية لأمن الأنظمة والمعلومات لموردين متخصصين أكثر جاذبية. يخلق هذا الاتجاه درجة عالية من التبعية ويمثل خطراً أمنياً كبيراً.

[1] – محمد مختار، يناير2015،"**هل يمكن أن تتجنب الدول مخاطر الهجمات الالكترونية؟**"، اتجاهات الأحداث، العدد 06، ص 06.

يجب أن تكون الدول حذرة من الاعتماد على كيانات خارجية خارجة عن سيطرتها في الإدارة الاستراتيجية والتكتيكية والتشغيلية للأمن. للحكومات دور تلعبه في التقليل من مخاطر ضعف التكنولوجيا والحلول الأمنية.[1]

5- الأبعاد القانونية :

أعلن المستشار القانوني للجنة الدولية للصليب الأحمر"لوران جيسل"(Gisil Laura)أن المادة 36من البروتوكول لعام 1977، يلزم الدول الأطراف بأن تكون الأسلحة الجديدة متوافقة مع أحكام القانون الدولي، إلا أن عدم تنظيم استخدام الفضاء السيبراني لا يعني تركه لمشيئة المتعاديين، فهناك أحكام عامة تفرضها قواعد الأخلاق، ومبادئ الإنسانية، وهناك أيضا نصوص مدونة بشأن الهجمات الجوية، تلائم طبيعة التهديدات السيبرانية، ويمكن أن تطبق عليها، حيث كشفت تسريبات أن الحكومة الأمريكية تنفق 3.4 بمليار دولار سنويا، على العمليات السيبرانية سنة 2011، وتم إعلان أكثر من 130 دولة حول العالم عن تخصيص أقسام قانونية خاصة بالتهديدات السيبرانية[2].

[1] – حمدون توريه،2006 "**الأمن السيبراني في البلدان النامية**"، الاتحاد الدولي للاتصالات، ص 15.

[2] – طارق المجذوب، تموز 2014،"**ساحة خفية لحرب "ناعمة" قادمة!**"، منشورات الدفاع الوطني اللبناني، العدد 89 ،ص 58.

خلاصة الفصل:

الذكاء الاصطناعي هو فرع من فروع علوم الحاسوب يهتم بإنشاء أنظمة لها القدرة على التعلم والتكيف والتفكير والتفاعل مع بيئتها بطرق مشابهة لقدرات البشر، ويستخدم الذكاء الاصطناعي في العديد من التطبيقات، بما في ذلك الروبوتات والتعرف على الصور والتعرف على الكلام والتعلم الآلي والتعلم العميق. وهو أحد أكثر التخصصات تقدماً في عصرنا الحالي.

الفصل الثاني :

الذكاء الاصطناعي بين التطور التقني والتحدي الأمني

دخلت وسائل الاتصال الإلكتروني في ساحة الصراعات البشرية لتحدث ثورة معلوماتية ضخمة في جل القطاعات، الأمنية والعسكرية والسياسية وهذا التحول كبّر في مجال السياسات بين الدول وعلاقاتهم؛ بحيث تطورت خلافاتهم ونزعاتهم من تقليدية إلى نزاعات كانت فيها التهديدات السيبرانية سلاحا حاسما وليدة اليوم والمستقبل في آن واحد.

فإن استخدام الأجهزة الاتصالية والإلكترونية في التهديدات السيبرانية بمثابة هاجس وتحدي للدول التي وجب عليها أن تكون متيقظة في هذا المجال وواقعا ملموسا في نتائجه على الدول.

المبحث الأول: التحديات الأمنية في مواجهة التهديدات السيبرانية

لقد أصبح الفضاء الإلكتروني ساحة المعركة الدولية الخامسة بعد البر والبحر والجو والفضاء[1] يمكن للهجمات التي تستهدف البنية التحتية السيبرانية أن تكون مدمرة لاقتصاد بلد ما، أو مدمرة بشدة لجميع القطاعات القابلة للاختراق إلكترونياً، العسكرية والمدنية على حد سواء.

المطلب الأول: أنماط وعوامل تنامي التهديدات السيبرانية

أولا: أنماط التهديدات السيبرانية

وعلى الرغم من تنوع طبيعتها ومصادرها وأهدافها، مثل التجسس وسرقة المعلومات والحرب، فإن التهديدات السيبرانية تتخذ أشكالاً عديدة وتعتمد العديد من الجهات الدولية الفاعلة على الآليات السيبرانية.

يمكن أن تتخذ الهجمات السيبرانية أشكالاً متعددة، ولكنها تصنف بشكل أساسي في المجموعات التالية:

1- خطر الكوارث الطبيعية أو (العرضية للكابلات البحرية):

تلعب الكابلات البحرية دورًا هامًا في توفير خدمات الاتصالات بين الدول في مجالات مثل الإنترنت وشبكات الحاسوب منذ عام 2005، حيث تلعب الكابلات البحرية دورًا هامًا في توفير خدمات الاتصالات بين الدول في مجالات مثل الإنترنت وشبكات الحاسوب منذ عام 2005، ولكن على نطاق الانتشار والانتشار، فقد حدث تحول نحو التقنيات الأخف والأصغر حجمًا وهذه الكابلات غير موجودة في المياه العميقة وبالتالي فهي معرضة لعدد من المشاكل التي تؤثر على البنية التحتية. فقد شهدت دول الشرق الأوسط انقطاعاً مفاجئاً للإنترنت بنسبة 80%؛ وفي يونيو 2005، حدثت 50% من حالات انقطاع الكابلات في المحيط الأطلسي،

[1]- باسكال بونيفاس، الجيوبوليتيك، 2020، "**مقاربة لفهم العالم في 48 مقالا**"، تر: إياد عيسى، منشورات الهيئة العامة السورية للكتاب، وزارة الثقافة، دمشق، ص 81 .

وفي 27 ديسمبر 2006، تسبب زلزال في جنوب شرق آسيا في فقدان الاتصال بشبكة الإنترنت[1].

2-التجسس الإلكتروني (Cyber Espionage)

وهو نوع من أنواع التجسس التقليدي عالي التقنية، وأكثر الهجمات الإلكترونية تعقيدًا التي تحصل على معلومات حساسة بطريقة غير مشروعة من أجل الحصول على ميزة اقتصادية أو استراتيجية أو عسكرية. التجسس الإلكتروني هو نوع من التجسس الذي يستخدم التكنولوجيا الإلكترونية للحصول على المعلومات، وهناك أنواع مختلفة من التجسس الإلكتروني، منها التجسس الفردي والتجسس باستخدام الشبكات السلكية والتجسس باستخدام الأقمار الصناعية.

3- **الجريمة السيبرانية(Cyber Crime)**

الجريمة السيبرانية هي أي نوع من أنواع الحواسيب الآلية، بما في ذلك الحواسيب الشخصية وشبكات الحواسيب والإنترنت ووسائل التواصل الاجتماعي، تُستخدم لتسهيل ارتكاب أفعال إجرامية أو غير قانونية، أو لتخزين البيانات أو البرامج المنقولة أو التدخل فيها أو تغييرها, أي فعل أو إغفال معد أو مخطط له يحدث على الشبكة نفسها عن طريق القرصنة بقصد المحو أو الجريمة السيبرانية أو الجريمة الافتراضية التي تتكون من جزأين: "إجرامي" و"سيبراني". ويستخدم مصطلح "السيبراني" لوصف فكرة كونه جزءًا من عصر الحاسوب والمعلومات، بينما يشير مصطلح الجريمة إلى أي عمل أو سلوك خارج عن القانون. والجريمة السيبرانية هي جريمة ترتكب ضد فرد أو مجموعة من الأفراد الذين لديهم دافع إجرامي لاستخدام الإنترنت أو شبكات الاتصالات الأخرى لإلحاق ضرر جسدي أو معنوي بالضحية بشكل مباشر أو غير مباشر والإضرار بسمعة الضحية) غرف الدردشة والبريد الإلكتروني والهواتف المحمولة (الجرائم المتعلقة بالهوية)، والأفعال المتصلة بالحاسوب لأغراض شخصية أو تحقيق مكاسب أو

[1]- عادل عبد الصادق،2012، "**الفضاء الالكتروني وتهديدات جديدة للأمن القومي**"، المركز العربي للأبحاث الالكترونية، ص 13

أضرار مالية، والأفعال المتعلقة بمحتوى الحاسوب، كلها مشمولة ضمن المعنى الواسع لمصطلح "الجريمة السيبرانية"، بما في ذلك ".[1]

تشير الجريمة السيبرانية أو الجريمة المعلوماتية إلى أي إغفال متعمد أو فعل ناشئ عن فعل غير قانوني يتمثل في نسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة على جهاز كمبيوتر بغرض الاعتداء على الأموال أو الممتلكات أو الخصوصية المادية أو المعنوية.[2] .فالجريمة السيبرانية لها مسميات كثيرة هي :الجريمة المعلوماتية، جرائم الفضاء الافتراضي، جرائم الكمبيوتر والانترنت جرائم مجتمع المعلومات وجرائم مجتمع المعرفة وجرائم مجتمع ما بعد المعلومات، وعلى اختلاف التسميات وتعدد مداخل الدراسات والتعاريف تتفق كلها على عنصر وحيد رئيسي لمفهوم الجريمة السيبرانية وهو الحاسب الآلي كأداة لكنه أيضا قد يكون معتدى عليه أو بيئة الجريمة.[3]

الجريمة السيبرانية أو الجريمة الإلكترونية هي الاستخدام غير المصرح به للحاسب الآلي والأجهزة المماثلة بوسائل غير مشروعة لتحقيق أهداف متعددة ومتنوعة، وتشمل جميع جرائم الحاسب الآلي المعروفة والموثقة أدواراً أخرى تؤثر فيها الحواسيب وهي "الأهداف، البيئات، الأدوات, الشفرات البرمجية". وبالتالي فإن جريمة الحاسب الآلي هي نشاط إلكتروني يتسبب في إلحاق الضرر المادي والمعنوي بالآخرين من خلال استخدام حاسوب الجاني ضد حاسوب الضحية. وبالتالي فإن الجريمة الحاسوبية هي نشاط إلكتروني يتسبب في إلحاق ضرر مادي ومعنوي بالآخرين من خلال استخدام حاسوب الجاني ضد حاسوب الضحية، حيث يمكن أن يكون الحاسوب بيئة الجريمة، بما في ذلك تدمير البيانات وتخريب مكونات الحاسوب والبرمجيات. وهذا يندرج تحت هذه الفئة. وتشمل الجريمة السيبرانية الاستخدام غير المصرح به

---

[1]– ذياب موسى البداينة، 2014،"**الجرائم الالكترونية :المفهوم والأسباب، ملتقى علمي حول :الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية**"، كلية العلوم الاستراتيجية، عمان، المملكة الأردنية الهاشمية، ص05.

[2]– سليم مزيود، 2015،"**الجرائم المعلوماتية واقعها في الجزائر وآليات مكافحتها**"، جامعة المدية، الجزائر، ص96

[3]– خديجة قصعة، جمال بن مرزوق، جانفي 2010 ، "**تفعيل آليات الحماية القانونية للحد من إنتشار الجريمة الإلكترونية في العالم والجزائر**"، مجلة تاريخ العلوم، العدد السادس، ص247

أو غير المشروع لشبكات الحاسوب، والهجوم على نظم المعلومات والبيانات المعالجة، والهجوم على الحياة الخاصة والشخصية والبيانات الشخصية، ونشر فيروسات الحاسوب، وغسل الأموال، والاحتيال، والاحتيال، وتنظيم الشبكات الإرهابية. وتشمل الجرائم السيبرانية نوعين من الجرائم التي ترتبط مباشرة بتكنولوجيا المعلومات كأداة لارتكاب هذا النوع من الجرائم. ويشمل ذلك الجرائم التي تُرتكب في العالم المادي والجرائم التي تُرتكب اليوم في العالم الافتراضي للإنترنت.[1] .

فالجريمة المرتكبة عبر الانترنت هي نشاط إجرامي يستخدم فيه التقنية الإلكترونية بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف، وهي نوع من الجرائم التي تتطلب الموضوع إلمام خاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقق فيها ومقاضاة فاعليها.كما أن أي تصرف غير مشروع من أجل العمليات الإلكترونية تمس بأمن الأنظمة المعلوماتية والمواضع التي تعالجها فالجريمة التي يستخدم فيها الحاسب الآلي كوسيلة أو أداة لارتكابها ويمثل إغراء بذلك، أو جريمة يكون الحاسب نفسه ضحيتها[2] .

ثانيا: عوامل تنامي التهديدات السيبرانية

لا يزال المهاجمون السيبرانيون يتمتعون بأفضلية على المدافعين بسبب التأثيرات المفاجئة التي لا يمكن أن تقلل من تأثيرها أي أساليب أمنية أو دفاعية سلبية أو إيجابية، كما أن هؤلاء المهاجمين لديهم القدرة على تغطية آثارهم.[3]

وفي الواقع لقد ساعدت عدة عوامل على تنامي التهديدات السيبرانية لمصالح الدول، ومن ثم إمكانية بروز حروب سيبرانية، من هذه العوامل ما يلي:

---

[1]– حنان براهمي،**2015**،" **جريمة تزوير الوثيقة الرسمية الإدارية، ذات الطبيعة المعلوماتية**"، أطروحة دكتوراه علوم، كلية الحقوق والعلوم السياسية، تخصص قانون جنائي، جامعة محمد خيضر، بسكرة، ص3

[2]– يوسف صغير،2014، "**الجريمة المرتكبة عبر الانترنت**"، رسالة ماجستير، كلية الحقوق، تخصص :قانون دولي للأعمال، جامعة مولود معمري، تيزي وزو، ص5 .

[3]– جوزيف هينروتين وآخرون، جوان 2019، "**حرب واستراتيجية :نهوج ومفاهيم** ،الجزء الثاني، تر: أيمن منير، المجلس الوطني للثقافة والفنون والآداب، الصفاة، الكويت، ص 71 .

1- تزايد ارتباط العالم بالفضاء الإلكتروني (السيبراني)، الأمر الذي اتسع معه خطر تعرض البنية التحتية الكونية للمعلومات لهجمات إلكترونية في الفضاء السيبراني

2- تراجع دور الدولة في ظل العولمة وانسحابها من بعض القطاعات الاستراتيجية مع تصاعد أدوار الشركات متعددة الجنسيات، خاصة العاملة في مجال التكنولوجيا كفاعل مؤثر في الفضاء السيبراني.

3- تزايد اعتماد الدول على الأنظمة الإلكترونية في جميع منشآتها الحيوية، الأمر الذي جعل من الممكن الإضرار بمصالحها من خلال الهجمات الإلكترونية في حالات العداء.

4- الحرب السيبرانية أقل تكلفة من الحرب التقليدية، حيث يمكن شن الهجمات في أي وقت والوقت اللازم لتنفيذها محدود.

5- لقد أصبحت الحرب الإلكترونية إحدى الأدوات المستخدمة للتأثير على المعلومات المستخدمة في مختلف مستويات ومراحل الحرب الإلكترونية والصراع، سواء على المستوى الاستراتيجي أو التكتيكي العملياتي، بهدف التأثير السلبي على هذه المعلومات وأنظمتها العملياتية.

6- توظيف الفضاء السيبراني في تعظيم قوة الدول، من خلال إيجاد ميزة أو تفوق أو تأثير في البيئات المختلفة، وبالتالي ظهر ما يسمى الاستراتيجية السيبرانية للدول.

7- إن مخاطر الأنشطة العدائية التي تقوم بها الجهات الفاعلة الحكومية وغير الحكومية في الحرب السيبرانية واسعة النطاق. فقد تشن هذه الجهات هجمات سيبرانية من خلال هياكلها الدفاعية والأمنية الخاصة بها، أو قد تجند قراصنة وموالين لشن هجمات ضد الدول المعادية دون روابط رسمية.[1]

[1]- علي زياد العلي، مرجع سابق، ص ص.79 – 78

المطلب الثاني: الجرائم الالكترونية والجوسسة في الفضاء السيبراني

تتعرض دول مختلفة حول العالم للقرصنة الإلكترونية والتجسس في الفضاء الإلكتروني، والحصول على معلومات استخباراتية عسكرية ومدنية، بل وتنفيذ عمليات تدمير البيانات وتدمير المنشآت. وقد خلقت الاختلافات الوطنية في مجال الحماية وأنظمة الدفاع الإلكتروني، وقدرات الدول الرئيسية في مجال السيطرة على الفضاء الإلكتروني وإدارته، ومحاولات الدول السيطرة على الفضاء الإلكتروني وإدارته دون استثناء، تحديات أمنية وتعرضها لتحديات متنوعة منها:

1- استهداف البنية التحتية للدول: أصبحت البنى التحتية الوطنية، المدنية والعسكرية على حد سواء، هدفاً للهجمات السيبرانية[1] مثل هذه الهجمات تشل أنظمة الدول، وتفسد أنظمة التشغيل، وتؤثر على تدفق المعلومات وتعطل عمل البنية التحتية الحيوية.[2] .

2- السيطرة على الأنظمة العسكرية وتعطيلها وإتلافها: ويرجع ذلك إلى إطلاق هجمات إلكترونية من قبل قراصنة محترفين وعسكريين إلكترونيين وعملاء إلكترونيين يهدفون إلى السيطرة على أنظمة القيادة والتحكم عن بعد، مما يؤدي إلى إبعاد بعض أنظمة الأسلحة عن سلسلة القيادة المركزية وإعادة توجيهها ضد أطراف داخلية ودول صديقة. كما يمكنهم أيضاً السيطرة على المركبات الجوية غير المأهولة والغواصات النووية في أعماق البحار والأقمار الصناعية العسكرية في الفضاء الخارجي، مما يخرج هذه الأسلحة والمعدات عن سيطرة الدولة التي تنتمي إليها. وتزداد خطورة مثل هذه الهجمات مع تطور التكنولوجيا واستحداث أنظمة لوجستية وأنظمة قيادة وسيطرة.[3]

كما تعمل الهجمات السيبرانية على تعطيل الأنظمة الإلكترونية في المنشآت العسكرية الحيوية؛ وتعطيل أو إتلاف شبكات الدفاع عن بعد العسكرية؛ واختراق الشبكات المدنية ذات

---

[1]- إيهاب خليفة، جويلية/ أوت 2017، "**تنامي التهديدات السيبرانية للمؤسسات العسكرية**"، مجلة اتجاهات الأحداث، ع 22، ص. 56.

[2]- أميرة عبد العظيم محمد عبد الجواد، مرجع سابق، ص ص: 431 – 432

[3]- إيهاب خليفة،" **تنامي التهديدات السيبرانية للمؤسسات العسكرية**"، **مرجع سابق**، ص57 .

الصلة بالجيش أو تعطيلها أو تدميرها؛ والتدخل في سلامة البيانات العسكرية الداخلية للدول الأخرى ومحاولة تعطيل أنظمتها أو التدخل فيها.[1]

3- **سرقة المعلومات والبيانات العسكرية أو التلاعب بها:** وفي هذه الحالة، فإن الهجوم الإلكتروني هو محاولة اختراق شبكة مؤسسة عسكرية وسرقة أو سرقة أو تزوير أو تدمير خرائط أنظمة الأسلحة أو مخططات المعدات العسكرية إلكترونياً.

4- **جمع معلومات اقتصادية استخباراتية** :ويتحقق ذلك من خلال اختراق قواعد البيانات المالية والمصرفية والشركات لجمع المعلومات التي يمكن أن تؤثر على الأمن القومي للدول، أو من خلال التجسس على المسؤولين الماليين ووزراء المالية ورؤساء الشركات الكبرى.

أدى الهجوم إلى مزيد من النقاش حول طبيعة التهديدات السيبرانية والحاجة إلى تحسين الأمن السيبراني[2] يرتبط هذا النوع من التجسس بصناعات التكنولوجيا مثل البرمجيات والتكنولوجيا الحيوية وتكنولوجيا الفضاء والاتصالات والموارد والطاقة.[3]

---

[1]- أميرة عبد العظيم محمد عبد الجواد، **مرجع سابق**، ص ص: 373. -374 .

[2]- علاء الدين فرحات،03 ديسمبر 2019 ،" **الفضاء السيبراني :تشكيل ساحة المعركة في القرن الحادي والعشرين**"، **مجلة العلوم القانونية والسياسية**، م10 ، ع، ص93 .

[3]- أميرة عبد العظيم محمد عبد الجواد، **مرجع سابق**، ص ص:418 - 419 .

المبحث الثاني: استخدامات الذكاء الاصطناعي في الأمن السيبراني

يُعد الأمن السيبراني أحد التحديات الرئيسية في العصر الرقمي الحديث. وقد أدى ظهور التهديدات السيبرانية المتقدمة إلى ضرورة توفير حلول فعالة لحماية البيانات والأنظمة الهامة. وهنا يأتي دور الذكاء الاصطناعي لتعزيز الأمن السيبراني ومكافحة التهديدات الإلكترونية.

إن التطورات الحديثة في مجال الذكاء الاصطناعي هي المفتاح لتحقيق أمن أفضل في العالم الرقمي؛ حيث يمكن للذكاء الاصطناعي أن يوفر حلولاً ذكية للكشف عن الهجمات الإلكترونية واكتشافها، وحماية البيانات الحساسة، واكتشاف الثغرات الأمنية، وتحليل سلوك المستخدم للكشف عن الاحتيال. يمكن أن يوفر.

المطلب الأول: مفهوم التهديد السيبراني

التهديدات التي تواجهها نظم المعلومات وإمكانية اختراقها بأبعادها المختلفة. وذلك لأن أي اختراق محتمل لهذه الأنظمة يشكل تهديدات أمنية خطيرة، مثل تلك التي تؤثر على حركة الطيران والمعاملات من خلال آليات التجارة الإلكترونية والمصارف والمؤسسات والمنظمات الأخرى التي تستخدم هذه العمليات[1] الأسلاب الآلية الحديثة في المعاملات. هذا إضافة إلى إمكانية اختراق منظمات الاتصال والتحكم في إدارة فالتهديدات السيبرانية هي استغلال الحاسبات وتكنولوجيا المعلومات في تخريب وتدمير البنية المعلوماتية للخصوم، بل وتعطيل شبكات الدفاع الجوي واختراق أنظمة المعلومات للبريد الإلكتروني لمكاتب رؤساء الدول والتجسس عليهم وفق خطة ممنهجة،[2] وهذا ما تقوم به الولايات المتحدة وأجهزة مخابراتها لزعزعة استقرار البلاد وتقسيمها وتدميرها من الداخل باستخدام بعض مواطنيها وجماعاتها الداخلية للتعدي على إدارة البلاد ونشر الفوضى دون تدخل عسكري يكلف أموالاً وأرواحاً.

[1] – محمد سعد أبو عامود،2013 ،"**المفهوم العام للأمن المعلوماتي**"، جامعة حلوان، مصر ،،ص07

[2] – CERT-UK. Common Cyber Attaks Reducing The Impact.the Informatio Cecurity Arm ofGCHQ. 2015. P 05

فالتهديدات السيبرانية أو الهجمات السيبرانية هي التي تهدد أمن المجتمع وأمن الاقتصاد الوطني والجانب الأمني والعسكري للدول،كما أن للتهديدات السيبرانية أهداف مسطرة، حيث تمس كلا من الجانب المعنوي والجانب المادي وعلى جميع الأصعدة[1]، لكن ما يتوجب على الدول المعرضة لتلك التهديدات وضع خطط إستراتيجية من أجل مكافحتها والتخلص منها.

المطلب الثاني: الثغرات الأمنية الشائعة التي تم اكتشافها بواسطة أدوات الفحص[2]

في البيئة الرقمية اليوم، حيث تتطور التهديدات السيبرانية باستمرار وتصبح أكثر تطوراً، من الضروري أن تبقى المؤسسات متقدمة بخطوة على نقاط الضعف المحتملة. إحدى الطرق الفعالة لتحديد الثغرات الأمنية في الأنظمة هي من خلال فحص الثغرات الأمنية.

يسمح استخدام أدوات الفحص للمؤسسات باكتشاف نقاط الضعف الشائعة بشكل استباقي واتخاذ إجراءات للتخفيف من المخاطر المحتملة.

يسلط هذا القسم الضوء على بعض الثغرات الأمنية الأكثر شيوعًا التي يمكن اكتشافها بواسطة أدوات الفحص، ويؤكد على أهمية فحص الثغرات الأمنية. (IDRB أفضل ممارسات كشف التسلل والاستجابة له) .

1- إدارة البرامج والتصحيحات القديمة:

واحدة من أكثر الثغرات الأمنية شيوعاً التي يمكن لأدوات الفحص تحديدها هي البرامج القديمة وإدارة التصحيحات الأمنية. لا تقوم العديد من المؤسسات بتحديث برامجها بأحدث التصحيحات الأمنية، مما يجعلها عرضة للثغرات الأمنية المعروفة. يمكن لأدوات الفحص أن تكتشف إصدارات البرامج القديمة والتصحيحات البرمجية المفقودة وتوفر رؤى مهمة لمساعدة المؤسسات على تحديد أولويات إدارة التصحيحات البرمجية. على سبيل المثال، يمكن لأدوات

[1] – أحمد السيد النجار، محمد عبد الهادي علام، يوليو2015، "**حروب المعلومات من يواجهها؟**"، مجلة الأهرام، العدد 139 مصر،ص 26.

[2] -Vulnerability scanning The Importance of Vulnerability Scanning in IDRB

فحص الثغرات الأمنية تحديد الإصدارات القديمة من أنظمة التشغيل وخوادم الويب، مما يسلط الضوء على الحاجة إلى التصحيح الفوري لمعالجة الثغرات الأمنية المعروفة.

2- كلمات المرور والمصادقة الضعيفة:

لا تزال كلمات المرور الضعيفة وآليات المصادقة غير الكافية تشكل نقطة ضعف كبيرة للمؤسسات. يمكن لأدوات الفحص تقييم قوة كلمات المرور، وتحديد كلمات المرور الافتراضية أو التي يمكن تخمينها بسهولة، ووضع علامة على الحسابات التي لا تحتوي على سياسات كلمات مرور مطبقة. ومن خلال الكشف عن نقاط الضعف هذه، يمكن للمؤسسات فرض سياسات أقوى لكلمات المرور، أو تنفيذ مصادقة متعددة العوامل، أو إجراء تدريب للموظفين لرفع مستوى الوعي حول أهمية ممارسات المصادقة القوية. على سبيل المثال، قد تسلط أداة فحص الثغرات الأمنية الضوء على حسابات المستخدمين التي تحتوي على كلمات مرور ضعيفة مثل "password123"، مما يدفع المؤسسة إلى فرض متطلبات كلمة مرور أقوى.

3- إعدادات الأمان التي تم تكوينها بشكل خاطئ:

يمكن أن تؤدي إعدادات الأمان التي تمت تهيئتها بشكل خاطئ إلى تعريض أنظمة المؤسسة وبياناتها لتهديدات محتملة دون قصد. يمكن لأدوات فحص الثغرات الأمنية أن تكتشف التهيئة الخاطئة في جدران الحماية وأجهزة التوجيه والتحكم في الوصول وإعدادات الأمان الأخرى. يمكن لهذه الأدوات تحديد المنافذ المفتوحة والخدمات غير المرغوب فيها وبروتوكولات التشفير الضعيفة التي قد تجعل النظام عرضة للوصول غير المصرح به أو اختراق البيانات. على سبيل المثال، يمكن لأدوات فحص الثغرات الأمنية تحديد جدران الحماية التي تسمح بالاتصالات الواردة من أي عنوان. IP، مما يشير إلى وجود خطأ في التكوين يحتاج إلى اهتمام فوري.

4- التصحيحات الأمنية المفقودة:

يعد الحفاظ على تحديث التصحيحات الأمنية المطبقة أمرًا ضروريًا لحماية الأنظمة من الثغرات الأمنية المعروفة. ومع ذلك، غالباً ما تواجه المؤسسات صعوبة في تحديد وتطبيق

التصحيحات الأمنية اللازمة في الوقت المناسب. يمكن لأدوات فحص الثغرات الأمنية البحث تلقائياً عن التصحيحات الأمنية المفقودة في أنظمة التشغيل وتطبيقات البرامج والمكونات الخارجية. من خلال الحصول على رؤية شاملة للتصحيحات المفقودة، يمكن للمؤسسات تحديد أولويات إدارة التصحيحات وتقليل فرصة المهاجمين المحتملين لاستغلال الثغرات المعروفة.

إصدارات البرامج الضعيفة:

يمكن لأدوات الفحص أيضاً اكتشاف إصدارات البرامج الضعيفة المعرضة للهجمات والثغرات المعروفة. يمكن لهذه الأدوات أن تقارن إصدارات البرامج المثبتة مع قواعد بيانات الثغرات الأمنية لتحديد البرامج التي قد تحتوي على ثغرات أمنية معروفة. على سبيل المثال، يمكن لأدوات فحص الثغرات الأمنية تحديد خوادم الويب التي تشغل إصدارات قديمة من Apache. يحتوي هذا الأباتشي على ثغرة أمنية معروفة يمكن استغلالها للوصول غير المصرح به. من خلال تحديد إصدار البرنامج الضعيف، يمكن للمؤسسة اتخاذ إجراءات فورية لتحديث أو استبدال البرنامج المتأثر، مما يقلل من خطر الاستغلال.

تلعب أدوات فحص الثغرات الأمنية دوراً رئيسياً في تحديد الثغرات الأمنية الشائعة التي يمكن أن تشكل تهديداً خطيراً للوضع الأمني للمؤسسة. ومن خلال الكشف عن البرمجيات القديمة وكلمات المرور الضعيفة والتهيئة الخاطئة والتصحيحات المفقودة وإصدارات البرامج الضعيفة، توفر هذه الأدوات رؤى قيمة تمكّن المؤسسات من معالجة الثغرات الأمنية بشكل استباقي وتعزيز الأمن العام. من خلال إجراء فحوصات منتظمة للثغرات الأمنية، يمكن للمؤسسات البقاء في طليعة التهديدات المحتملة وتقليل مخاطر الهجمات الناجحة وضمان الدفاع القوي ضد التهديدات الإلكترونية المتطورة.

خلاصة الفصل :

مما سبق يمكن القول إن المجال السيبراني قد دخل في المحددات الجديدة للقوة وأبعادها، ليس فقط من حيث طبيعتها وأنماط استخدامها، بل من حيث طبيعة الفاعلين فيها، مما يؤثر على قدرات الدولة وعلاقاتها الخارجية، ويضيف خصائص جديدة للقوة. وقد اتسعت هذه القوة لتشمل جميع الوسائل والطاقات والإمكانات المادية وغير المادية المرئية وغير المرئية التي تمتلكها الدولة ويستخدمها صانعو القرار في العمل الفعال لتحقيق مصالح الدولة، ومع تزايد انتقال المحتوى الاستخباراتي والعسكري والأمني والسياسي والمعلوماتي والأمن القومي سيتكثف ويؤثر على سلوك الوحدات السياسية الأخرى، وقد أدى توسع القطاعات الاقتصادية والاجتماعية والفكرية والخدمية والعلمية والبحثية في الفضاء الإلكتروني، ولا سيما تسارع تطبيق الحكومة الإلكترونية والمدن الذكية في العديد من البلدان، ونمو نطاق وعدد مستخدمي الإنترنت في جميع أنحاء العالم، إلى تعريض قواعد البيانات الوطنية للعالم الخارجي. بالإضافة إلى ذلك، أدت الحملات الدعائية وحملات التضليل ونشر الشائعات والدعوات التحريضية ودعم المعارضة والأقليات إلى تآكل السيادة الوطنية، مما يشكك في قدرة الدول على الحفاظ على أمنها.

الفصل الثالث :

الأمن السيبراني الجزائري في العصر الرقمي بين التطورات التكنولوجية وحماية المعلومات

لقد أفرزت التحولات الأمنية خاصة بعد الحرب الباردة إلى يومنا هذا أثرا كبيرا على الأمني الوطني لجميع الدول، وكانت الدولة الجزائرية واحدة من تلك الدول، حيث عرفت الجزائر ومنذ استقلالها مجموعة من التهديدات الأمنية أثرت على أمنها واستقرارها، مما جعلها تعمل على تطوير عقيد ا الأمنية لمكافحة تلك التهديدات من خلال وضع مجموعة من السياسات الاستراتيجيات من أجل التفاعل مع تلك التهديدات،

لكن الجزائر وكغيرها من الدول تواجه تحديات نتيجة لتأثير تلك التهديدات الأمنية على جميع الأصعدة لأمنية والسياسية، والتساؤل حول هذا الفصل :ما هو تأثير التحولات الأمنية على الأمن الوطني الجزائري؟

المبحث الأول :استراتيجيات الدولة الجزائرية لتحقيق الأمن السيبراني

يعد الأمن السيبراني أحد التحديات الأمنية المعاصرة التي باتت تشكل تحدياً للعديد من الجهات الفاعلة وخاصة الدول، وأصبح بعداً مفاهيمياً ينبغي دراسته من قبل الأكاديميين ومجتمعات المعرفة لخلق صيغ معرفية تسهل على صناع القرار إيجاد حلول واتفاقيات على المستوى الإمبراطوري، تعتبر الجزائر من أوائل الدول التي انضمت إلى ركب الحكومة الإلكترونية والعالم السيبراني، مما أدى إلى تبني الدولة الجزائرية إصلاحات واستراتيجيات أمنية لتحقيق الأمن السيبراني في الفضاء الإلكتروني.

المطلب الأول: الأليات القانونية والتشريعية

1-التدابير القانونية :

تطرق المشرّع الجزائري على غرار الدول الأخرى مثل فرنسا لتجريم أفعال المساس بأنظمة الحاسب الآلي إلا وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل، مما دفع بالمشرّع إلى تعديل قانون العقوبات بموجب القانون رقم 04-15 المتمم للأمر رقم 66 - 156 المتضمن قانون العقوبات، والذي أفرد القسم "السابع مكرر" منه تحت عنوان "المساس بأنظمة المعاجلة الآلية للمعطيات " من المادة 394 مكرر إلى 394 مكرر 7، ونص على عدة جرائم، أما في عام حيث 2006 أدخل المشرّع الجزائري تعديل آخر على قانون العقوبات بموجب القانون رقم 06-23 [1]مسّ ذلك التعديل القسم السابع مكرر الخاص بالجرائم الماسة بأنظمة المعاجلة الآلية للمعطيات، وقد تمّ تشديد العقوبة المقررة لهذه الأفعال فقط دون المساس بالنصوص التجريمية الواردة في هذا القسم من قانون 04-15 ،وربما يرجع سبب هذا التعديل إلى ازدياد الوعي بخطورة هذا النوع المستحدث من الإجرام باعتباره يؤثر على الاقتصاد الوطني بالدرجة الأولى وشيوع ارتكابه، كما أدخل

[1] - محمد أحمد سليمان عيسى، 2016، "**التعاون الدولي لمواجهة الجرائم الإلكترونية**"، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد 02، كلية العلوم والدراسات الإنسانية بالغاط، المملكة العربية السعودية.

المشرّع الجزائري بالقانون رقم 16-02[1] المعدّل والمتمّم لقانون العقوبات مادتين وهما 87 مكرر 11 ،و394 مكرر 8 فاستعمل في الأولى عبارة (تكنولوجيات الإعلام والاتصال)، وفي الثانية عبارة(مقدم خدمات الانترنت)[2].

2-التدابير التقنية والإجرائية:

قد أدرك المشرّع الجزائري جيدا بأن المواجهة الفعالة للإجرام الإلكتروني تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية، إنما لابد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية وتحفظية، والتي من شأنها تفادى وقوع الجريمة الإلكترونية أو على الأقل الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها، وهو ما استدركه المشرّع بتضمين القانون رقم 06-22[3] المعدل لقانون الإجراءات الإجراءات الجزائية تدابير إجرائية مستحدثة تتعلق بالتحقيق في الجرائم الإلكترونية تتمثل في مراقبة الاتصالات الإلكترونية وتسجيلها والترسب. ويقصد باعتراض المراسلات اعتراض أو تسجيل أو نسخ المراسلات التي تكون في شكل بيانات قابلة للإنتاج والتوزيع، التخزين الاستقبال والعرض التي تمت عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة عنها. ولقد أشار المشرّع الجزائري إلى ظروف وكيفية اللجوء هذا الإجراء في المادة 65 مكرر 5 من قانون الإجراءات الجزائية بموجب هذه المادة فإن المشرّع الجزائري يسمح لسلطات التحقيق والاستدلال إذا استدعت ضرورة التحري الجريمة المتلبس بها أو التحقيق في الجريمة الالكترونية، اللجوء الى إجراء اعتراض المراسلات السلكية واللاسلكية وتسجيل المحادثات والأصوات والتقاط

[1] – محمد السعيد زناتي، ديسمبر 2017" **الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية**"، مجلة إيليزا للبحوث والدراسات، المجلد02 ،العدد01 ،المركز الجامعي إيليزي، الجزائر،

[2] – مراد مشوش، 2020" **الجريمة المعلوماتية في ظل قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال**"، مجلة القانون المجلد09 ،العدد01.

[3] – أبو المعالي محمد عيسى، المنعقد في الفترة من 28 إلى 29 أكتوبر 2009" **الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجريمة حول المعلوماتية**"، ورقة بحثية مقدمة في إطار المؤتمر العلمي المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، ليبيا.

الصور والاستعانة بكل الترتيبات التقنية اللازمة لذلك لأجل الوصول إلى الكشف عن ملابسات الجريمة وإثباتها دون أن يتقيدوا بقواعد التفتيش والضبط المألوفة[1].

ومع هذا فإن المشرّع الجزائري لم يطلق حق اللجوء إلى هذا الإجراء، بل أحاطه بمجموعة من الضمانات القانونية التي تحدّ من تعسّف سلطات الاستدلال والتحري وتصون الحقوق والحريات العامة والحياة الخاصة للأفراد.

المطلب الثاني: الأليات الأمنية والتقنية

أولا: تطوير الإنترنت في الجزائر.

سعت الجزائر بشبكة الإنترنت في مارس 1994 من خلال مركز البحث العلمي والتكنولوجي للمعلوماتية الذي أنشأته وزارة التعليم العالي والبحث العلمي في أبريل 1986، وسعت للاستفادة من خدمات الإنترنت والتقنيات المتعلقة بالأمن، [2] وقد قدر(Cerist) عدد الهيئات المشتركة في الإنترنت سنة 1996 ؛ أي بعد سنتين من دخول الإنترنت إلى الجزائر بحوالي 130هيئة .كما قدر في سنة 1999 عدد الهيئات المشتركة في الشبكة ب 800 هيئة، منها 100في القطاع الجامعي و 50في القطاع الصحي و 500 في القطاع الاقتصادي و 150في قطاعات أخرى .وفي نفس السنة أي 1999 كان لمركز البحث في الإعلام العلمي والتقني حوالي 3500 مشترك.[3] وعام 2001 قامت وزارة البريد والموصلات بعد إنشاء مؤسسة"الجزائر تيليكوم "(Algérie-Telecom) بتعاقد مع شركتين عالميتين هما: "لوستن

---

[1] – أسمهان بوضياف، 2018 "**الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر**"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد03 ،العدد03 ،ص364.

[2] – زهرة خلوط، 2014،"**التسويق الابتكاري وأثره على بناء ولاء الزبائن**"، **دراسة حالة :مؤسسة اتصالات الجزائر**"، رسالة ماجستير، جامعة امحمد بوقرة، بومرداس، كلية العلوم الاقتصادية تجارة وعلوم التسيير، 2014/2013.

[3] – نعيمة برنيس،2010" **الوظيفة الإعلامية لشبكة الأنترنت في عصر ثورة المعلومات**"، رسالة ماجستير، جامعة منثوري قسنطينة، كلية العلوم الإنسانية والاجتماعية، فرع:صحافة مكتوبة وسمعى بصري، 2010/2009، ص101 .

تكنولوجي(Losent- "Technologie) و"أريسكون" (Ericson) السويدية لإنشاء قواعد خاصة، ستمكن من الحصول على بث يتجاوز 30 ميغابت/ثا.

وقد تعرضت الإنترنت في الجزائر إلى مجموعة من العوائق تتلخص في إرتفاع أسعار الهاتف الثابت وكذا بطء في الشبكة سنة. 2003[1] كما كشفت إحدى الإحصائيات أن مجموع مستخدمي الإنترنت بلغ نحو ثلاث ملايين بحلول2006 ، إذ بلغ مع نهاية 2006 المرتبطين بالإنترنت عن طريق (ADSL) 300000 إلى أن اتجه إلى الوضع نحو تبني سياسة توفير جهاز كمبيوتر لكل عائلة جزائرية بحلول2010[2] .

أما حسب الإحصائيات الأخيرة فقد بلغ عدد مستخدمي الأنترنت لسنة2012 ، حوالي 5 مليون و 230000 مستخدم بنسبة تبلغ 14.% [3].

ثانيا :مشروع الجزائر الإلكتروني2013

استراتيجية الجزائر الإلكترونية، المعروفة باسم مشروع الجزائر الإلكترونية 2013. يندرج هذا المشروع في إطار المبادرات والمشاريع التنموية التي تتبناها الحكومة الجزائرية لتحقيق التنمية المستدامة في مختلف مناحي الحياة، ويندرج في إطار بروز مجتمع علمي ومعرفي للجزائريين، وإدخال نظام إلكتروني شامل ومتطور ونشر التكنولوجيات الحديثة من خلال ترقية الأنظمة المعلوماتية في قطاع الاتصالات السلكية واللاسلكية، حيث تم إطلاق مشروع الجزائر الإلكترونية من طرف وزارة البريد والتكنولوجيا والاتصالات السلكية واللاسلكية بالتشاور مع الهيئات العمومية والإدارية والمتعاملين الاقتصاديين العموميين والخواص والجامعات ومراكز البحث والجمعيات.

---

[1]– باديس لونيس،2008، "**جمهور الطلبة الجزائريين والأنترنت، دراسة في إستخدامات إشباعات طلبة جامعة منتوري قسنطينة**"، رسالة ماجستير، جامعة منتوري، قسنطينة، كلية العلوم الإنسانية والعلوم الإجتماعية، قسم علوم الإعلام والاتصال2008/2007، ص 62 .

[2]– خيرة روابحي،2010، "**ثقافة الأنترنت :دراسة ميدانية لاستعلامات الشبكة بمدينة تيهيرت**"، رسالة ماجستير، جامعة وهران، كلية العلوم الإنسانية والحضارة الإسلامية، قسم علم المكتبات والعلوم الوثائقية،2009 /2010، ص 78.

[3]– كريمة صراع،2014، "**واقع وآفاق التجارة الإلكترونية في الجزائر**"، رسالة ماجستير، جامعة وهران، كلية العلوم الاقتصادية وعلوم التسيير، تخصص استراتيجية، (2014/2013)، ص 139 .

المهنية التي تنشط في مجال العلوم والتكنولوجيات الإعلام والاتصال[1] .

وقد تم اعتماد الخطة من خلال تقييم حالة قطاع تكنولوجيا المعلومات والاتصالات باستخدام عدة مؤشرات: مؤشر الجدوى ومؤشر الوصول الرقمي ومؤشر الاستعداد الرقمي, مؤشر نشر تكنولوجيا المعلومات والاتصالات[2] إن تبني الجزائر لمشروع الجزائر الإلكترونية يعكس اهتمام الحكومة الجزائرية بضرورة تحديث القطاع الحكومي المستمد من الاحتياجات الاجتماعية والاقتصادية والسياسية والتكنولوجية التي تمس معظم الدول المتقدمة. فالمعركة الرقمية وتعزيز رأس المال البشري ضروريان لمواجهة التحديات التي تفرضها التنمية الاقتصادية والاجتماعية، وهما عاملان أساسيان في تهيئة البلاد لمواجهة تحديات العولمة ومخاطر التهديدات المعلوماتية بمختلف أشكالها، حيث تستند استراتيجيات مشروع الجزائر الإلكترونية على التحول العميق والسريع الذي يشهده العالم مع الأخذ بعين الاعتبار ظهور مجتمع العلم والمعرفة.[3] .

ثالثا :مركز الوقاية من جرائم الإعلام الآلي لدرك الوطني:

1- مركز الوقاية من جرائم الإعلام الآلي لدرك الوطني:

تأسس المركز في عام 2008 في بيل مراد ريس، ويهدف المركز إلى ضمان أمن نظم المعلومات من أجل السلامة العامة. ويقوم المركز بتحليل بيانات وبيانات الجرائم الإلكترونية لتحديد مرتكبيها، سواء كانوا أفراداً أو عصابات أو غيرهم.[4] .

ويهدف المركز إلى دعم تعاون السلطات الأمنية الأخرى في مكافحة الجرائم الإلكترونية. ويعمل المركز على تطوير سبل مكافحة هذه الجرائم، كما يعمل المركز من خلال التعاون مع

---

[1]– عادل غزال، مارس 2014، "**مشاريع الحكومة الإلكترونية من الاستراتيجية إلى التطليق، مشروع الجزائر :الحكومة الإلكترونية 2013 أنموذجا**"، مجلة المكتبات والمعلومات، العدد 34 ، ص64 .

[2]– إلياس شاهد، الحاج عرابة، عبد النعيم دفرو،2016،" **تقييم تجربة تطبيق الحكومة الإلكترونية في الجزائر**"، المجلة الجزائرية للدراسات المحاسبية والمالية، العدد الثالث، ص13 .

[3]– عبد القادر عبان، 2015، "**تحديات الإدارة الإلكترونية في الجزائر، دراسة سوسيولوجية ببلدية الكاليتوس العاصمة**"، أطروحة دكتوراه (ل م د) ،جامعة محمد خيضر، بسكرة، كلية العلوم الإنسانية والاجتماعية، تخصص إدارة وعمل، ص91 .

[4]– سمير بارة،2014،"**الدفاع الوطني والسياسات الوطنية للأمن السيبراني (Cyber Security) في الجزائر :الدور والتحديات**"، جامعة قاصدي مرباح، ورقلة، ص445 .

وزارة العدل على تطوير التشريعات المنظمة لمجال استغلال المعلومات وإنشاء مختبر خاص بعلم الجريمة لتحسين مستوى التعامل مع الجريمة بشكل عام والجريمة الإلكترونية بشكل خاص. وتسعى الجزائر إلى الاستفادة من تجارب الدول الأخرى في مجال تأمين الأنظمة المعلوماتية وحمايتها من الجريمة، ومن أهم عناصرها:

الوقاية: ويشمل ذلك حملات توعية وتثقيف بالتعاون مع وزارة التضامن الوطني والأسرة، والمشاركة في المنتديات والمحاضرات والأيام الدراسية والمنتديات الدولية والمنتديات الصحفية والبرامج التلفزيونية والإذاعية وغيرها من تدابير النشر والدعاية.

المكافحة : نشر الوعي بين الجزائريين من خلال استخدام شبكات التواصل والإنترنت من خلال نشر تعليقات تدافع عن الجزائر ومقاطع فيديو تربطهم بالجناة لتحديد السلوكيات المشبوهة والتهديدات بالاعتداءات، وتسهيل التحقيقات التي تقوم بها قوات الدرك واعتقال المشتبه فيهم جنائياً والجناة في الوقت المناسب[1] .

2- المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني:

يعتبر المعهد أحد المشاريع المنجزة في إطار تطوير سلك الدرك الوطني" **ببوشاوي**"، حيث تم إنشاءه بموجب 04 المؤرخ في 26 جوان2004 ، ودخل حيز الخدمة ابتداء من الفاتح جانفي / مرسوم رئاسي 133/ 2009 ، أما الفترة الممتدة بين2004 و 2009كرست لتكوين المورد البشري واقتناء المعدات العلمية والتقنية الضرورية، ويقوم المعهد بالعديد من المهام التي من شأ ا تلبية الطلبات الواردة من السلطة القضائية، ضباط الشرطة القضائية والسلطات المؤهلة، قانونيا خاصة أثناء معالجة القضايا المعقدة[2] .

---

[1]- سهام بو عموشة، 24 ماي،2017 ، "**الفضاء السيبراني يتميز بانفتاح شبكة المعلوماتية وانعدام الحواجز الجغرافية**"، جريدة الشعب، العدد17345 ، ص06 .

[2]- نسيمة سحواذ، "**الطموح لتوسيع دائرة الاعتماد المتبادل بإدراج طرق تحليلية لفائدة مخابر أخرى**"، في مارس // http Dikanews.com13:63/2018: 02

-مصلحة الإعلام الآلي:

قسمت مصلحة الإعلام الآلي إلى الأدلة الجنائية وعلم الجريمة التابع للدرك، وهو قسم تابع لمعهد الأدلة الجنائية وعلم الجريمة التابع للدرك، يقوم بمراقبة وإدارة وتتبع عمليات القرصنة والاختراق، والكشف عن المعلومات المسروقة وتفكيك برامج الكمبيوتر [1] :

- العمل لاستكمال إقامة منظومة اتصال آلية على شكل شبكة تربط مختلف وحدات وهياكل الدرك الوطني تسمح بالاتصال الآلي للمعلومات أفقيا وعموديا مما يسهل على المحققين التحري عن الجرائم وتعقب المجرمين بفعالية.
- العمل على تنظيم هياكل ووحدات مكلفة بممارسة الشرطة القضائية على نحو يعزز تخصص الوحدات أو على الأقل إنشاء فرق متخصصة في المخدرات والتزوير وجرائم الإعلام الآلي، وغيرها من الجرائم المعقدة التي تنفذها شبكات منظمة والتي تصنف على أنها إجرام منظم[2] .

3 -المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني:

تم إنشاء فرقة العمل المركزية لمكافحة الجريمة الإلكترونية سنة 2011 بعد أن استجاب جهاز الأمن الجزائري للمطالب المتعلقة بأمن المعلومات ومكافحة التهديدات الأمنية الناجمة عن الجريمة الإلكترونية. وكانت فرقة العمل هذه تكييفاً للتشكيل الأمني التابع للمديرية العامة للعدل والشرطة، وكانت أول فصيلة أساسية لتشكيل أمني خاص لمكافحة الجريمة الإلكترونية على مستوى المديرية العامة للأمن الوطني[3].

أخيرا طورت المديرية العامة للأمن العام جبهة أمنية فعالة لمكافحة الجرائم الجديدة ذات الصلة الوثيقة بعلوم المعلومات والإنترنت، من خلال الاجتهاد في الأساليب التي تؤدي إلى

---

[1]- بارة سمير، مرجع سابق، ص43

[2]- أحمد غاي، "**تكييف الشرطة القضائية مع متطلبات إصلاح العدالة، تقييم وآفاق**"، في :03مارس 2018/14:13 w.w.w.mjustice .dg

[3]- عبد القادر سعيدي، "**المصلحة المركزية الالكترونية في مواجهة مجرمي العالم الافتلاضي**"، في: 03مارس 2018 17:42/ www.essalamonline.com

تفاقم هذه الظاهرة العابرة للحدود الوطنية، والتي باتت تعرف بـ"الجريمة الإلكترونية"، والتعامل مع هذه الآفة التي أخذت طابعا أكثر خطورة مع مرور السنوات. ومن أجل التمكن من القيام بذلك، شدد على أهمية أن تكون جميع إدارات الشرطة مستعدة وجاهزة كل في مجال اختصاصها.

ومن أجل الحد من هذا النوع من الجرائم، دعت المديرية العامة لأمن الولاية دائما إلى وضع خطط عمل ميدانية لتعزيز يقظة الشرطة والمصالح المختصة في مجال مكافحة الجريمة المعلوماتية، وذلك بفضل وسائل وآليات تسيير تكنولوجيا المعلومات والاتصالات[1] .

1- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

نصت على إنشاء هذه الهيئة المادة 13 من القانون04/09 المؤرخ في أوت المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها من خلال : "تنشأ هيئة وطنية وتنظيمها وكيفيات سيرها عن طريق التنظيم "أما مهامها فقد أوردت المادة 14من نفس القانون وتتمثل في:

أ **الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال** :وتشمل التدابير الوقائية رفع مستوى الوعي لدى مستخدمي تكنولوجيا المعلومات والاتصالات بخطورة الجرائم التي قد يقعون ضحايا لها أثناء تصفح واستخدام تكنولوجيا المعلومات والاتصالات، وأهمها: التجسس على الاتصالات ورسائل البريد الإلكتروني؛ والتلاعب بحسابات العملاء؛ والشركات الكبرى والمؤسسات والهيئات الحكومية ويشمل ذلك اختراق الأجهزة.

ب **مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال** :بحسب نص المادة 14 من القانون 04/09هناك نوعان من المكافحة تقوم بهما هذه الهيئة:

[1]– رضية مناد، " **تطوير قدرات الشرطة في مواجهة الجريمة الالكترونية، أمن واستراتيجية**"، 03 مارس www.dgayerinfo.com.21:19/2018

أ مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية المادة 14 فقرة(ب) من القانون09 /04.

ب ولتبادل المعلومات مع الدول الأجنبية من أجل جمع كل البيانات المفيدة لتحديد ومكافحة مرتكبي الجرائم المتعلقة بتكنولوجيا المعلومات والاتصالات، يقترح المشروع في هذا الفصل إنشاء وكالة وطنية متخصصة تتولى المهام التالية تنشيط وتنسيق الوقاية من الجريمة المعلوماتية ومساعدة السلطات القضائية والشرطة القضائية في التحقيق في الجرائم المعلوماتية وجمع المعلومات من نظيراتها الأجنبية لمكافحة هذه الجريمة الخطيرة.[1]

إستراتيجيات المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني

1- سعت المديرية العامة للأمن الوطني لوضع خطط عمل ميداني للرفع من يقظة جهاز والمصالح المختصة في متابعة الجريمة المعلوماتية، وهذا بفضل وسائل وآليات التحكم في تكنولوجيا الإعلام والاتصال لمكافحة هذا الشكل من الجرائم

2- وهي فرصة لتبادل الخبرات والأفكار مع الخبراء في الجزائر على وجه الخصوص، من أجل تحليل هذه الظاهرة على نطاق واسع[2] .

3- برمجت المديرية العامة للأمن الوطني عدة دورات تكنولوجية حول موضوع" الوقاية السيبرانية "من خلال توفير دورات تكنولوجية تقنية عالية المستوى في المجال لمكافحة الجريمة الالكترونية ومسايرة فرق المحققين من الشرطة لإحداث التكنولوجيا والتحكم فيها والاطلاع عليها على الأساليب المعتمدة دوليا في الوقاية والمكافحة لهاته الجرائم الإلكترونية الهدامة.

[1]- الجريدة الرسمية،27يونيو 2009، "**القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال وطرق مكافحتها**"، الفترة التشريعية السادسة، السنة الثالثة، الدورة الرابعة، رقم122 ، ص 04 .

[2]- مناد ارضية، مرجع سابق

4- وضع خطة استراتيجية في مجال الوقاية والتعرض لهذه الجرائم الناشئة عن إساءة استخدام شبكات الإنترنت، خاصة من قبل الشباب والأطفال، وذلك من خلال الدعوة إلى العمل الإيجابي للقضاء على الأخطار المحتملة وحماية الأفراد والمجتمع من هذا النوع من الجرائم.[1] .

المبحث الثاني: الذكاء الإصطناعي والتحديات الأمنية في الجزائر

تواجه الجزائر تحديًا كبيرًا في توفير القدرات المهنية في مجال الذكاء الاصطناعي هناك نقص في المهنيين والمتخصصين الذين يتمتعون بالمهارات اللازمة لتطوير وتنفيذ مشاريع الذكاء الاصطناعي عالية الجودة، كما أن البنية التحتية التقنية ضعيفة: تعتمد تطبيقات الذكاء الاصطناعي على بنية تحتية تقنية قوية، بما في ذلك الشبكات عالية السرعة والأجهزة المتقدمة. ومع ذلك، تواجه الجزائر تحديًا يتمثل في عدم كفاية تطوير البنية التحتية والاستثمار بما يتماشى مع متطلبات تكنولوجيا الذكاء الاصطناعي.

المطلب الأول: التهديدات السيبرانية في الجزائر

يشهد الوضع الأمني في الجزائر، كما هو الحال في الدول الأخرى، العديد من التهديدات التي تفرضها الثورة التكنولوجية الحديثة. خاصة بعد انتشار وسائل التواصل الاجتماعي وكثرة المواقع الإلكترونية التي تنشر أفكارا تزعزع وتهدد استقرار ووحدة البلاد وتدعو إلى نشر الفوضى والعنف والتطرف والكراهية والفرقة. الأمر الذي دفع الدولة الجزائرية إلى البحث عن سبل مكافحة مثل هذه الجرائم من أجل تحقيق الأمن السيبراني من خلال الأجهزة الأمنية المختصة بمكافحة الجرائم الإلكترونية. والأمثلة التالية توضح بشكل أفضل تجربة الجزائر في مكافحة مثل هذه الجرائم:

أولا: خطر الإرهاب السيبراني على الأمن الوطني الجزائري

يعتبر الإرهاب الإلكتروني من أهم التهديدات التي تستهدف أمن جميع الدول بما فيها الدولة الجزائرية. وهذا ما أكده اللواء مناد نوبة القائد العام للدرك الجزائري في كلمة ألقاها في افتتاح ندوة دولية حول "الأمن السيبراني" في مايو 2017، حيث قال فيها "إن الإرهاب الإلكتروني من

[1]- صالح ميهوبي،18جويلية 2017،" **جرائم الانترنت تنخر المجتمع الجزائري**"، جريدة البلاد، العدد5369 ، ص07.

أخطر الجرائم التي تستهدف الشعب الجزائري من خلال تشجيعه لكل أشكال العنف والإرهاب والتطرف. وبتشجيعه على كل أشكال العنف والإرهاب والتطرف، أصبح من أخطر الجرائم التي تستهدف الشعب الجزائري". لذلك دعا إلى إطلاق خلية أمنية متخصصة للعمل على تعزيز إجراءات الرقابة لحماية المواطنين الجزائريين، خاصة فئة الشباب من هذه الجريمة الإلكترونية التي تشكل خطورة كبيرة على استقرار البلاد. وشدد على ضرورة أن تكون الدولة الجزائرية "مسلحة إلكترونيا" بكل الوسائل التكنولوجية والفعالة لمكافحة العنف والفكر المتطرف وكل أشكال الجريمة المنظمة والجريمة الدولية.[1]

كما تمكنت الجزائر ممثلة أساسا في أجهز ا الأمنية التابعة للدرك الوطني والأمن الوطني وبالتعاون مع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال من معالجة أكثر من 1000 جريمة إلكترونية منها % 30 على مواقع التواصل الاجتماعي، هذا وقد سجلت مديرية الشرطة القضائية بالمديرية العامة للأمن الوطني خلال السداسي الأول عام 2016وجود 11 قضية متعلقة بالإرهاب الإلكتروني أغلبها خاصة بتهديدات إرهابية باسم "تنظيم داعش الإرهابي "لتسفر جهود البحث والتحري والتنسيق بين مختلف القطاعات المختصة توقيف 58 شخص متورط في قضايا إرهاب إلكتروني تمت إحالتهم على القضاء.

تمكن الجيش الإلكتروني الجزائري من إلقاء القبض على أكثر من 160 جزائريًا على صلة مباشرة بتنظيم داعش في العراق وسوريا وليبيا. كما استعملت منظومات تكنولوجية متطورة واستلمت منشورات إرهابية تدعو للالتحاق بمنتديات إرهابية ومعلومات عن اتصالات وطنية ودولية نتيجة للرسائل المتبادلة واستخدام المواقع الإلكترونية ومنصات التواصل الاجتماعي،

[1]– عنترة بن مرزوق، محي الدين حرشاوي،"**الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية**"، كلية الحقوق والعلوم السياسية، المركز الجامعي آفلو، ص68

خاصة فيسبوك وتويتر. وقد تمكنا من فك شفرة أكثر من 30 خلية تحاول تجنيد الشباب في التنظيمات الإرهابية من خلال [1] .

ثانيا :مخاطر الألعاب الإلكترونية على أطفال الجزائر

قام مرصد حقوق الطفل بالتعاون مع الهيئات أمنية مختصة بدراسة حول" جرائم الإنترنت والأطفال في الجزائر "وشملت عينة الدراسة 975 طفلا منهم 548 ذكرا و 427 أنثى ينتمون إلى 10 بلديات مختلفة على المستوى الجزائر العاصمة، حيث طرح عليهم 16 سؤالا لمعرفة مدى علاقتهم بالتقنيات الجديدة لوسائل الإعلام والاتصال.

فقد بينت إجابات المستجوبين أن 23.89 % من الآباء مقابل 13.79 % من الأمهات الأطفال يعانون من الأمية، في حين أن 43.69 % من الآباء مقابل 49.02 % من الأمهات يملكون مستوى تعليميا يتأرجح بين الابتدائي والثانوي، في حين 32.82 %من الآباء مقابل 18,76% من الأمهات لديهم مستوى جامعي .كما كشفت الاستجوابات أن 56,26%من عائلات الأطفال الباحثون يملكون جهاز كمبيوتر واحد، فيما يملك 8 %منهم أكثر من جهاز كمبيوتر، إضافة إلى ثلث الأسر مربوطة بشكل الإنترنت.

أظهرت نتائج الاستطلاع أن 72.25% من الأطفال لديهم إمكانية الوصول المجاني إلى الإنترنت في المنزل، وقال 68.75% من الأطفال أن والديهم يسمحون لهم باستخدام الإنترنت. ومن المهم أيضًا الإشارة إلى أن 30.5% من الأطفال الذين شملهم الاستطلاع قد تلقوا هدايا أو مزايا من جهة مجهولة، و48% من الأطفال الذين شملهم الاستطلاع سمعوا عن جرائم الإنترنت، ويعتقد 25.80% من الأطفال أنه من الضروري حماية الأطفال من مخاطر الإنترنت أظهرت النتائج أن 25.80% من الأطفال يعتقدون أنه من الضروري حماية الأطفال من مخاطر الإنترنت.

[1]– آمال صويلح،2017، "**الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام خطوة هامة نحو مكافحة الارهاب الالكتروني بالجزائر**"، الملتقى الدولي حول" الاجرام السيباني"، المفاهيم والتحديات يومي:11– 12 أفريل– 2017 ، جامعة 8ماي1945 ، قالمة الجزائر، ص 09.

واستنادا إلى هذه المعطيات، خلص فريق البحث إلى أن الجزائريين منفتحون على تكنولوجيات المعلومات والاتصالات الجديدة، وأن الكثير من الأسر تثق كثيرا في الإنترنت، وهو ما ينعكس في سماحهم لأطفالهم باستخدام الإنترنت دون رقابة. وخلصت الدراسة إلى أن نسبة عالية من الأطفال يتعرضون للإنترنت ومخاطره، وأن هناك نقصا في المتابعة الأسرية مع الأطفال ووعي الأسرة بمخاطر الإنترنت. وهذا يؤكد على ضرورة تفعيل دور الأسرة والمجتمع ككل من أجل اتخاذ الإجراءات الوقائية اللازمة.

وبالرغم من تناول الدراسة مؤشرات للمستوى التعليمي والوضع الاقتصادي للأولياء، إلا أنه تبين مدى ارتباط ذلك بالوعي بمخاطر الإنترنت أو وجود الرقابة الأسرية على الأطفال[1] .

ثالثا :مخاطر مواقع التواصل الاجتماعي الهدامة

1- مخاطر التواصل الاجتماعي على الأمن الوطني الجزائري:

تعتبر مواقع التواصل الاجتماعي وبالأخص "الفايسبوك" من أخطر مواقع التواصل على الأمن القومي الجزائري، حيث احتل المرتبة الأولى بنسبة 50.45 بالمائة، يليه موقع "يوتيوب" في المرتبة الثانية بنسبة 30.63 بالمائة ثم موقع "تويتر" في المرتبة الثالثة بنسبة 18.92 بالمائة. وهذا يدل على أن "فيسبوك" مصدر خطير للمعلومات بالنسبة للأمن الوطني. فالفيسبوك يؤثر على أجهزة الدولة الرسمية ويفقدها مصداقيتها لأنه يتداول أخباراً ومعلومات تختلق الشائعات والأخبار الكاذبة. وبالفعل، لا يوجد لدى جهاز المخابرات العامة فريق متخصص لمتابعة الأنشطة التخريبية الإرهابية الإلكترونية، لذلك فإن الخطوة التالية هي أن يقوم الجهاز بمتابعة ورصد المعلومات المتعلقة بأنشطة الجماعات الإرهابية مع تطور التكنولوجيا.[2] .

---

[1]– مسعودة بايوسف، ديسمبر2016 ، "**الطفل والانترنت المنزلي، مجالات الاستخدام والاشباعات المحققة**"، مجلة العلوم الإنسانية والاجتماعية، العدد27 ، ص4 .

[2]– حكيم غريب،الثلاثاء11أفريل 2017، " **مخاطر مواقع التواصل الاجتماعي على الأمن المجتمعي :الرهانات والاستراتيجيات**"، ندوة علمية دولية حول" :عولمة الاعلام السياسي وتحديات الأمن القومي للدول النامية، ص08 .

2- الإشاعات وآثارها على الاستقرار الأمني والسياسي للدولة الجزائرية:

وهذا ما يدل على أن الدولة الجزائرية ليست بمنأى عن ظواهر تشويه السمعة التي تعصف بالمجتمع وتؤثر على استقراره وديمومة أمنه واستقراره السياسي والاجتماعي. يعمل موقع التواصل الاجتماعي "فيسبوك" على بناء الثقة والاستقرار في المجتمع الجزائري وإيجاد وعاء للأفكار الخاطئة والتضليل والمعارضة الهدامة التي لا تسعى إلى زعزعة الثقة في المسؤولين. إن المعضلة الحقيقية التي تقف كتحدٍ للدولة هي صعوبة السيطرة على هذه الصفحات، وهو ما يطرح إشكالية نطاق وحدود قدرة الدولة الجزائرية: هل المنظومة القانونية الرادعة للأفراد أم قدرة الدولة التقنية[1] .

المبحث الثالث: نماذج التحديات الأمنية

تميل معظم الدول والحكومات إلى تبني استراتيجيات وسياسات لتحقيق أقصى قدر من الأمن من التهديدات والتحديات من أجل تحقيق الأمن السيبراني، والجزائر كغيرها من الدول مهتمة بتبني نموذج الحكومة الذكية في سياق مجتمع المعلومات الجزائري، وهذه المخاطر السيبرانية، وتعمل على إنشاء وكالة أمنية متخصصة لمواجهة هذه المخاطر. إذن، ما هي المخاطر السيبرانية التي تعاني منها الجزائر وما هي الاستراتيجيات الأمنية المعتمدة؟

المطلب الأول: تسريبات بكالوريا2016

أكدت مصالح الأمن الوطني أن بكالوريا 2016 انتهت على وقع توتر كبير عقب تسرب مواضيع الامتحان على شبكات التواصل الاجتماعي، تم على إثره تحديد هوية 31 شخصا متورطا في هذه القضية.

ونفى الديوان الوطني للامتحانات والمسابقات إلغاء الامتحانات بعد المعلومات التي تم نشرها على شبكات التواصل الاجتماعي (فيسبوك). فيسبوك (كما استجوبت السلطات الأمنية امرأة

[1]– شرف الدين بن إرث،الثلاثاء 11 أفريل2017، " **إشاعات وآثارها على الاستقرار الأمني والسياسي للدولة، حقائق من صفحات التواصل الاجتماعي، صفحات الفيسبوك الجزائرية**"، ندوة علمية دولية حول" :عولمة الاعلام السياسي وتحديات الأمن القومي للدول النامية"، ص06 .

يعتقد أنها المتورطة الرئيسية في تسريب موضوع امتحانات التاريخ والجغرافيا ووضعتها تحت الرقابة القضائية. وأكد وزير العدل حافظ الأختام الطيب لوح أن النيابة العامة في عدة ولايات كلفت الشرطة القضائية والدرك بالتحقيق في أسباب تسريب مواضيع البكالوريا.

وتوضح الخدمة أنه تم تحديد صفحات التبادل المتورطة). وقد أسفرت التحقيقات المتعمقة والتدابير المضادة التي قام بها مركز منع الجرائم الإلكترونية والتصدي لها التابع للدرك عن استخدام أكثر من 15 حسابًا على فيسبوك ومصادرة 150 حسابًا (بعضها كان مقره في الخارج)[1] .

المطلب الثاني :لعبة الحوت الأزرق المميتة

بدأت لعبة "الحوت الأزرق" في روسيا عام 2013، لكنها انتشرت منذ ذلك الحين وهي لعبة قاتلة تستهدف الأطفال والمراهقين. تتحكم اللعبة في الأطفال عبر 50 مرحلة، وتأمرهم بتنفيذ مهمات خطيرة، وفي المرحلة الأخيرة تأمرهم بالانتحار، وقد يكون الأطفال الجزائريون من بين ضحايا هذه اللعبة القاتلة.

حذرت السلطات الأمنية الجزائرية وخبراء في علم الاجتماع من مخاطر استخدام الأطفال والقصر للإنترنت في الجزائر، في ظل انتشار ظاهرة "الحوت الأزرق". وذكر الخبراء في ملتقى جهوي حضره رؤساء السلطات الأمنية في ولايات الشرق الجزائري أن الظاهرة تندرج في إطار الجريمة الإلكترونية، وأنه سيتم عرض الوثائق القانونية المتعلقة بالجريمة الإلكترونية وسبل مكافحتها، وتنظيم قافلة تحسيسية توعوية.

تشارك فيها مديرية النشاط الاجتماعي، مديرية التربية والتكوين المهني ومصالح الأمن، لتفعيل الجانب الوقائي من مخاطر الإنترنت[2] .

---

[1]– غنية توات،19جوان2016، "**القرار الأخير بشأن مصير الامتحان يعود للحكومة، يومية إخبارية وطنية**"، جريدة الفجر، العدد4778، ص 05 .

[2]– علجية عيش،ديسمبر2017،" **الحوت الأزرق من الجرائم الالكترونية التي يعاقب عليها القانون**"، جريدة الأحرار، العدد325، ص 04 .

كما أعلنت وزارة العدل أن الإدارة العامة للوقاية من جرائم المعلوماتية والاتصالات بالولاية وبالتعاون مع النيابة العامة المختصة قد باشرت التحقيق في هذه اللعبة القاتلة التي تدفع الأطفال إلى الانتحار. وفي هذا الصدد، أطلقت المديرية العامة لأمن الدولة ووزارة التربية والتعليم بالولاية حملة توعية عبر المؤسسات التعليمية لتوعية التلاميذ وأولياء أمورهم بمخاطر الألعاب الإلكترونية، وذلك استجابة لتزايد عدد ضحايا ما يسمى بلعبة "الحوت الأزرق" على الإنترنت.[1] .

وأكدت وزيرة البريد وتكنولوجيا الاتصالات الجزائرية " هدى أيمان فرعون " أنه من الجانب التقني، لا تملك تماما، لأنه لا يوجد موقع ألعاب يمكن حجبه، وإنما تطبيقات يتم تحميلها مثل هذه اللعبة.ونقلت تقارير محلية عن مديرية الشرطة القضائية الجزائرية حول مخاطر الألعاب الالكترونية والاستخدام السيء للإنترنت على الأطفال بأنه يستحيل حجب هذه الألعاب الإلكترونية والسبب يعود إلى "التطور التكنولوجي" الذي يسمح بفتح الآلاف الصفحات في ثانية واحدة[2] .

[1]– الإذاعة الجزائرية،" **فتح تحقيق قضائي في" انتحار "بعض الأطفال بسبب لعبة الحوت الأزرق**"، 01 أفريل 2018/10:00 www.Radioalgerie.dg

[2]– عثمان لحياني،" **السلطات الجزائرية : تحجب" الحوت الأزرق "مستحيل ... وهذا بديلها**"، في 01 :أفريل 2018/10:22 www.altahrironlen.com

خلاصة الفصل الثالث:

إن للجزائر تجربة فريدة من نوعها في ظل التطورات التكنولوجية والمعلوماتية، في إنشاء أجهزة أمنية مخصصة لمواجهة التهديدات السيبرانية الوشيكة. وتعمل هذه الأجهزة على استكمال إنشاء نظام اتصال آلي على شكل شبكات تربط بين مختلف الوحدات والمؤسسات لنقل المعلومات أفقيا وعموديا.

الخاتمة.

الخاتمة:

نستخلص من هذه الدراسة التي تناولنا فيها موضوع استخدامات التكنولوجيا الذكاء الاصطناعي وعلاقته بالأمن السيبراني في الجزائر، والتي حاولنا فيه الإجابة على الإشكالية التي تتضمّن جهود الدولة الجزائرية في استخدامات الذكاء الاصطناعي لتعزيز أمنها السيبراني، حيث يمكننا القول بأن الذكاء الإصطناعي يمثل تقدما هائلا في مجال التكنولوجيا وله العديد من الفوائد والتطبيقات المحتملة، ومع ذلك يجب إستخدامه بشكل مسؤول وفقا للقوانين و الأخلاقيات، وأن يتم التركيز على حماية الخصوصية وتجنب التأثيرات السلبية المحتملة لإستخدام هذه التكنولوجيا الجديدة وجعلها ألية فعالة لتحقيق الأمن السيبراني وفضاء الرقمي أكثر أمانا.

لقد خلصنا من خلال هذه الدراسة الى جملة من النتائج نوردها فيما يلي:

- ✓ تطوير برامج تدريبية وتوعية للموظفين والمستخدمين بشأن مخاطر الأمن السيبراني وكيفية التعامل معها بشكل فعال.
- ✓ تشجيع الوصول الى البيانات بشكل أكبر للباحثين دون المساس بالخصوصية الشخصية للمستخدمين بإعتماد تقنيات الذكاء الإصطناعي.
- ✓ تعزيز التشريعات والسياسات القائمة لحماية البيانات الحساسة والتصدي للاختراقات السيبرانية.
- ✓ الترويج لنماذج جديدة عن التعليم الرقمي، وتطوير القوى العاملة في مجال الذكاء الإصطناعي.
- ✓ إنشاء فرق متخصصة في استجابة الطوارئ السيبرانية للتعامل مع الهجمات بشكل فوري وفعال.
- ✓ تعزيز التعاون بين القطاع العام والقطاع الخاص لتبادل المعلومات والخبرات حول التهديدات السيبرانية.
- ✓ تعزيز البنية التحتية السيبرانية وتحديث التقنيات والأنظمة الأمنية لتقليل الفجوات وزيادة القدرة على استكشاف ومواجهة الهجمات.

- ✓ تعزيز التعاون الدولي لتبادل المعلومات والخبرات في مجال الأمن السيبراني والتصدي للتهديدات العابرة للحدود.
- ✓ تشجيع البحث والتطوير في مجال الأمن السيبراني لتطوير حلول مبتكرة لمواجهة التهديدات الجديدة والناشئة.
- ✓ هذه المقترحات يمكن أن تكون نقطة انطلاق قوية لتعزيز الأمن السيبراني في الجزائر ومواجهة التحديات الحديثة في هذا المجال.
- ✓ فرض عقوبات على سوء إستخدام الذكاء الإصطناعي وتعزيز الأمن السيبراني، لأن تطبيقات الذكاء الإصطناعي مهمة جدا في الحفاظ على خصوصيات رواد ومستخدمي مختلف المنصات في البيئة لرقمية الحديثة.

قائمة المصادر والمراجع

قائمة المصادر عبد الباسط

- **القرآن الكريم**
- **المعاجم العربية:**

- الفيروز أبادي،2005، "القاموس المحيط"، ط8، مؤسسة الرسالة للطباعة والنشر والتوزيع، لبنان.

- **المصادر:**

- عبد الرحمان ابن خلدون، 2004، "المقدمة"، ط1 ،بيروت: دار الفكر،.

- **المراجع:**

1. أوس مجيد غالب العوادي،2016 ،"الأمن المعلوماتي السيبراني"، مركز البيان للدراسات والتخطيط،بيروت – آمال صويلح،2017، "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام خطوة هامة نحو مكافحة الارهاب الالكتروني بالجزائر"، الملتقى الدولي حول "الاجرام السيباني"، المفاهيم والتحديدات يومي:11- 12 أفريل- 2017 ، جامعة 8 ماي 1945، قالمة الجزائر

2. ابتسام ناصر هويمل وخولة عبد الله المفيز، 2022، "الذكاء الاصطناعي: مستقبل إدارة الموارد البشرية"، العبيكان للنشر والتوزيع، الرياض

3. أبو المعالي محمد عيسى، المنعقد في الفترة من 28 إلى 29 أكتوبر 2009" الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجريمة حول المعلوماتية"، ورقة بحثية مقدمة في إطار المؤتمر العلمي المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، ليبيا.

4. باسكال بونيفاس، الجيوبوليتيك، 2020، "مقاربة لفهم العالم في 48 مقالا"، تر: إياد عيسى، منشورات الهيئة العامة السورية للكتاب، وزارة الثقافة، دمشق.

5. برنارد وارد، 2022، "تطبيقات الذكاء الاصطناعي: كيف استخدمت 50 شركة ناجحة الذكاء الاصطناعي والتعلم الآلي لحل المشكلات"، تر: عائشة يكن، العبيكان للنشر والتوزيع، الرياض.

6. توربان إفرام، 2000، "نظم دعم القرارات ونظم الخبرة"، تعريب سرور علي إبراهيم سرور، الطبعة 01 ،دار المريخ للنشر، السعودية.

7. جوزيف هينروتين وآخرون، جوان 2019، "حرب واستراتيجية :نهوج ومفاهيم" ،الجزء الثاني، تر: أيمن منير، المجلس الوطني للثقافة والفنون والآداب، الصفاة، الكويت.

8. حسن بن أحمد الشهري، 2010،"الأنظمة الالكترونية الرقمية المطورة لحفظ وحماية سرية المعلومات من التجسس"، مركز النور للأبحاث الإلكترونية.

9. حكيم غريب،الثلاثاء11أفريل 2017، " مخاطر مواقع التواصل الاجتماعي على الأمن المجتمعي :الرهانات والاستراتيجيات"، ندوة علمية دولية حول" :عولمة الاعلام السياسي وتحديات الأمن القومي للدول النامية.

10. حمد سعيد الموعد، 1999، "أمن الممرات المائية العربية"، إتحاد كتاب العرب، دمشق.

11. حمدون توريه،2006 "الأمن السيبراني في البلدان النامية"، الاتحاد الدولي للاتصالات.

12. ذياب موسى البداينة، 2014،"الجرائم الالكترونية :المفهوم والأسباب، ملتقى علمي حول : الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية"، كلية العلوم الاستراتيجية، عمان، المملكة الأردنية الهاشمية.

13. سميث، ماثيو، 2018،" الذكاء الاصطناعي وتنمية الإنسان" نحو جدول أبحاث.

14. سليم مزيود، 2015،"الجرائم المعلوماتية واقعها في الجزائر وآليات مكافحتها"، جامعة المدية، الجزائر.

15. سمير بارة،2014،"الدفاع الوطني والسياسات الوطنية للأمن السيبراني (Cyber Security) في الجزائر :الدور والتحديات"، جامعة قاصدي مرباح، ورقلة.

16. السيد نصر الدين السيد، 2006، "كيف يفكّر الحاسوب (دليل القارئ الذكي لأسرار الذكاء الاصطناعي"، دار العين للنشر، القاهرة، مصر.

17. شرف الدين بن إرث،الثلاثاء 11 أفريل2017، " إشاعات وآثارها على الاستقرار الأمني والسياسي للدولة، حقائق من صفحات التواصل الاجتماعي، صفحات الفيسبوك الجزائرية"، ندوة علمية دولية حول" :عولمة الاعلام السياسي وتحديات الأمن القومي للدول النامية.

18. شرقاوي محمد علي، 1996، "الذكاء الاصطناعي والشبكات العصبية والمكتب العصري الحديث"، مكتبة الأسكندرية، مصر.

19. صلاح نيوف،" مدخل للفكر الاستراتيجي"، المركز الأكاديمي المفتوح للعلوم السياسية الدنمارك.

20. عبد الحميد بسيوني، 1998 ،"مقدمة الذكاء الاصطناعي للكمبيوتر ومقدمة البرولوج"، الطبعة 01 ،دار النشر للجامعات، مصر.

21. محمد مختار، يناير2015،"هل يمكن أن تتجنب الدول مخاطر الهجمات الالكترونية؟"، اتجاهات الأحداث، العدد 06.

22. محمد سعد أبو عامود،2013 ،"المفهوم العام للأمن المعلوماتي"، جامعة حلوان، مصر.

23. منى الأشقر جبور،2013، "السيبرانية هاجس العصر"، المركز العربي للبحوث القانونية والقضائية، بيروت.

24. منى الأشقر جبور، مايو2012، "الأمن السيبراني: التحديات ومستلزمات المواجهة"، المركز العربي للبحوث القانونية والقضائية.

25. النجار فايز جمعة، 2010، "نظم المعلومات الإدارية –منظور إداري"، الطبعة 03 ،دار الحامد للنشر والتوزيع، الأردن.

- **المذكرات:**

26. أحمد إيدابير، 2011 ،"**التعددية الاثنية والأمن المجتمعي : دراسة حالة مالي**"، مذكرة مقدمة لنيل شهادة الماجستير في العلوم السياسية والعلاقات الدولية تخصص الدراسات الأمنية والاستراتيجية، قسم العلوم السياسية والعلاقات الدولية، جامعة الجزائر3.

27. أحمد براهيم، 2010،" الدولة العالمية والنظام الدولي الجديد"، أطروحة دكتوراه، (جامعة السانيا، وهران، كلية العلوم الاجتماعية.

28. أحمد مسعود مريم،2013، "آليات مكافحة جرائم تكنولوجيا الاعلام والاتصال في ضوء القانون رقم 04/09""، رسالة ماجستير، جامعة قاصدي مرباح، ورقلة، كلية الحقوق والعلوم السياسية، قسم الحقوق،2013/2012.

29. إدريس عطية، 2011،"الإرهاب في إفريقيا :دراسة في الظاهرة وآليات مواجهتها"، رسالة ماجستير، كلية الحقوق والعلوم السياسية، والعلاقات الدولية، تخصص :دراسات إفريقية جامعة الجزائر3.

30. باديس لونيس،2008، "جمهور الطلبة الجزائريين والأنترنت، دراسة في إستخدامات إشباعات طلبة جامعة منتوري قسنطينة"، رسالة ماجستير، جامعة منتوري، قسنطينة، كلية العلوم الإنسانية والعلوم الإجتماعية، قسم علوم الإعلام والاتصال2008/2007.

31. براهمي، 2015، "جريمة تزوير الوثيقة الرسمية الإدارية، ذات الطبيعة المعلوماتية"، أطروحة دكتوراه علوم، كلية الحقوق والعلوم السياسية، تخصص قانون جنائي جامعة محمد خيضر، بسكرة.

32. خيرة روابحي،2010، "ثقافة الأنترنت :دراسة ميدانية لاستعلامات الشبكة بمدينة تيهيرت"، رسالة ماجستير،جامعة وهران، كلية العلوم الإنسانية والحضارة الإسلامية، قسم علم المكتبات والعلوم الوثائقية،2009 /2010.

33. زهرة خلوط، 2014،"التسويق الابتكاري وأثره على بناء ولاء الزبائن"، دراسة حالة :مؤسسة اتصالات الجزائر"، رسالة ماجستير، جامعة امحمد بوقرة، بومرداس، كلية العلوم الاقتصادية تجارة وعلوم التسيير،2014/2013.

34. عباس حفصي،2015، "جرائم التزوير الالكتروني، دراسة مقارنة"، أطروحة دكتوراه،، أحمد بن بلة، كلية العلوم الإسلامية، تخصص شريعة وقانون، جامعة وهران1 .

35. عبد القادر عبان، 2015، "تحديات الإدارة الإلكترونية في الجزائر، دراسة سوسيولوجية ببلدية الكاليتوس العاصمة"، أطروحة دكتوراه (ل م د) ، كلية العلوم الإنسانية والاجتماعية، تخصص إدارة وعمل، جامعة محمد خيضر، بسكرة.

36. عقيلة أفندي، 2007، "إدارة المعرفة التمييز في المؤسسة المعاصرة"، رسالة ماجستير ،جامعة سعد دحلب، البليدة.

37. عنترة بن مرزوق، محي الدين حرشاوي،"الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية"، كلية الحقوق والعلوم السياسية، المركز الجامعي آفلو.

38. صفية نزاري،2010،" الأمن الثقافي لمنطقة المغرب العربي في ظل تنامي العولمة: دراسة مقارنة لحالات: الجزائر، تونس والمغرب"،مذكرة مقدمة لنيل شهادة الماجستير في العلوم السياسية، تخصص علاقات مغاربية ومتوسطية في التعاون والأمن، قسم العلوم السياسية، جامعة باتنة.

39. كريمة صراع،2014، "واقع وآفاق التجارة الإلكترونية في الجزائر"، رسالة ماجستير، كلية العلوم الاقتصادية وعلوم التسيير، تخصص استراتيجية، جامعة وهران، (2014/2013).

40. محمد أحمد سليمان عيسى، 2016، "التعاون الدولي لمواجهة الجرائم الإلكترونية"، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد 02، كلية العلوم والدراسات الإنسانية بالغاط، المملكة العربية السعودية.

41. نسيمة طويل، 2010،" الاستراتيجية الأمنية الأمريكية في منطقة شمال شرق آسيا :دراسة لمرحلة ما بعد الحرب الباردة"، أطروحة دكتوراه علوم، كلية العلوم السياسية :تخصص علاقات دولية، جامعة الحاج لخضر، باتنة، (2009 /2010) .

42. نعيمة برنيس،2010" الوظيفة الإعلامية لشبكة الأنترنت في عصر ثورة المعلومات"، رسالة ماجستير، جامعة منثوري قسنطينة، كلية العلوم الإنسانية والاجتماعية، فرع:صحافة مكتوبة وسمعى بصري، 2010/2009 .

43. يوسف صغير،2014، "الجريمة المرتكبة عبر الانترنت"، رسالة ماجستير، كلية الحقوق، تخصص :قانون دولي للأعمال، جامعة مولود معمري، تيزي وزو.

- **المراجع الأجنبية:**

44. Bostrom, Nick, 1973, Is a Swedish, born philosopher at. the University ,of Oxford known for his Work on existential risk, the anthropic principal, human enhancement ethics, super intelligence risks, and the reversal test , https:// bit.Iy/3vb Yejk, in 05/03/2022 à 18 :00.

45. Price WaterhouseCoopers (PWC), 2018,The macroeconomic impact of artificial. intelligence,UK,London, February.

46. The macroeconomic impact of artificial intelligence,op.cit.,

47. Mckinsey Global Institute,2017, Artificial Intelligence:Implications for China ..

48. Impact of Generative AI,2023, The Future of Work in Japan, Social science.research institute of the International University of Japan June.

49. World Economic Forum ،2020,Mapping TradeTech: Trade in the Fourth.Industrial Revolution, Insight Report ،December,.

50. CERT-UK. 2015,Common Cyber Attaks Reducing The Impact.the Informatio Cecurity Arm ofGCHQ.

- **الجرائد والمجلات:**

51. أسمهان بوضياف، 2018 ،"الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد03 ،العدد03.

52. أحمد السيد النجار، محمد عبد الهادي علام، يوليو2015، "حروب المعلومات ..من يواجهها؟"، مجلة الأهرام، العدد 139.

53. أحمد عبيس نعمة الفتلاوي،2016" الهجمات السيبرانية :مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر"، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الرابع، السنة الثامنة.

54. الجريدة الرسمية، 27 يونيو2009 "القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وطرق مكافحتها"، الفترة التشريعية السادسة، السنة الثالثة، الدورة الرابعة، رقم122 .

55. إلياس شاهد، الحاج عرابة، عبد النعيم دفرو،2016، "تقييم تجربة تطبيق الحكومة الإلكترونية في الجزائر"، المجلة الجزائرية للدراسات المحاسبية والمالية، العدد الثالث.

56. أمينة عثمانية،2019، "المفاهيم الأساسية للذكاء الاصطناعي"، مقال منشور في المؤلف الجماعي بعنوان تطبيقات الذكاء الاصطناعي كتوجه حديث لتعزيز تنافسية منظمات الأعمال، مجلد 01 ،العدد 01 ،المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، عنابة الجزائر.

57. إيهاب خليفة، جويلية/ أوت 2017، "تنامي التهديدات السيبرانية للمؤسسات العسكرية"، مجلة اتجاهات الأحداث، ع 22.

58. جريدة العرب،3 أغسطس/آب 2023 /https://alarab.news/sites/default

59. خديجة قصعة، جمال بن مرزوق،جانفي2010، "تفعيل آليات الحماية القانونية للحد من إنتشار الجريمة الإلكترونية في العالم والجزائر"، مجلة تاريخ العلوم، العدد السادس.

60. سعد علي الحاج علي بكري، أوت2017 ، "الأمن السيبراني ومعضلة حمايته ..عولمة التعليم العالي ..الرقمي"، جريدة العرب الاقتصادية الدولية، العدد24.

61. سليمان عبد الله الحربي، صيف 2008، "مفهوم الأمن: مستوياته وصيغه وتهديداته(دراسة نظرية في المفاهيم والأطر)"، المجلة العربية للعلوم السياسية، عدد 19.

62. سهام بو عموشة، 24ماي2017 ، "الفضاء السيبراني يتميز بانفتاح شبكة المعلوماتية وانعدام الحواجز الجغرافية"، جريدة الشعب، العدد17345 .

63. طارق المجذوب، تموز 2014، "ساحة "خفية" لحرب "ناعمة" قادمة!"، منشورات الدفاع الوطني اللبناني، العدد 89.

64. صالح ميهوبي، 18جويلية 2017 ، "جرائم الانترنت تنخر المجتمع الجزائري"، جريدة البلاد، العدد5369 .

65. عادل غزال، مارس2014،"مشاريع الحكومة الإلكترونية من الاستراتيجية إلى التطليق، مشروع الجزائر :الحكومة الإلكترونية 2013 أنموذجا"، مجلة المكتبات والمعلومات، العدد 34.

66. علاء الدين فرحات، 2019 ، "الفضاء السيبراني :تشكيل ساحة المعركة في القرن الحادي والعشرين"، مجلة العلوم القانونية والسياسية، م 10 ع03ديسمبر2019.

67. علجية عيش، ديسمبر2017 ، "الحوت الأزرق من الجرائم الالكترونية التي يعاقب عليها القانون"، جريدة الأحرار، العدد325.

68. غنية توات، 19جوان 2016 ، "القرار الأخير بشأن مصير الامتحان يعود للحكومة، يومية إخبارية وطنية"، جريدة الفجر، العدد4778 .

69. محمد السعيد زناتي،2017، "الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية"، مجلة إيليزا للبحوث والدراسات، المركز الجامعي إيليزي، الجزائر، المجلد02 ،العدد01 ديسمبر2017.

70. مراد مشوش،2020، "الجريمة المعلوماتية في ظل قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال"، مجلة القانون المجلد09 ،العدد01.

71. مسعودة بايوسف، ديسمبر 2016،"الطفل والانترنت المنزلي، مجالات الاستخدام والاشباعات المحققة"، مجلة العلوم الإنسانية والاجتماعية، العدد27.

72. فهد الحازمي وفكتور سحاب، يناير/كانون الثاني– فبراير/شباط، 2017، "الذكاء الاصطناعي: تقنياته، تطوره ووعودها"، مجلة القافلة،المجلد 66، العدد 1.

- **المواقع الالكترونية:**

73.الإذاعة الجزائرية،" فتح تحقيق قضائي في" انتحار "بعض الأطفال بسبب لعبة الحوت.

74.تولاي آسر20جانفي2018،" ما هي السيبرانية؟ وما دورها في صناعة القرار"؟

http//Zeitgeistarrabia.com

75. رضية مناد،03مارس2018، " تطوير قدرات الشرطة في مواجهة الجريمة الالكترونية، أمن واستراتيجية. www.dgayerinfo.com.21:19

76.عثمان لحياني،01أفريل2018،" السلطات الجزائرية : تحجب" الحوت الأزرق "مستحيل ... وهذا بديلها". www.altahrironlen.com10:22

77. عبد القادر سعيدي،03مارس2018، "المصلحة المركزية الالكترونية في مواجهة مجرمي العالم الافتلاضي". www.essalamonline.com 17:42

78. عبد الوهاب شادي، وآخرون،2022/04/06، فرص وتهديدات الذكاء الاصطناعي في السنوات العشر القادمة، تقرير المستقبل، العدد27 ،مركز المستقبل للأبحاث والدراسات المستقبلية ،متاح على الرابط.22: 15 http://www.academia.edu/ consulté

79. نانسي البنا،20جانفي2018،" الأمن السيبراني ..بيئة تكنولوجية أكثر أمنا ". http//boutiqueceena.eg

80. "الحوت الأزرق"، 01 أفريل2018 10:00/ www.Radioalgerie.dg

81. https://shorturl.at/clCPV 7 يوليو/تموز 2023

82. 26 أغسطس/ أب 2023 https://rb.gy/wz9jg

83. https://shorturl.at/clCPV 7 يوليو/تموز 2023

فهرس المحتويات

الفصل الثالث الأمن السيبراني الجزائري بين التطورات التكنولوجية وحماية المعلومات	
المبحث الأول :استراتيجيات الدولة الجزائرية لتحقيق الأمن السيبراني	45
المطلب الأول: الأليات القانونية والتشريعية	45
التدابير القانونية	45
التدابير التقنية والإجرائية	46
المطلب الثاني: الأليات الأمنية والتقنية	47
أولا: تطوير الإنترنت في الجزائر	47
ثانيا :مشروع الجزائر الإلكتروني2013	48
ثالثا :مركز الوقاية من جرائم الإعلام الآلي لدرك الوطني	49
مركز الوقاية من جرائم الإعلام الآلي لدرك الوطني	49
المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني	50
المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني	51
الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها	53
المبحث الثاني: الذكاء الإصطناعي والتحديات الأمنية في الجزائر	54
المطلب الأول: التهديدات السيبرانية في الجزائر	54
أولا: خطر الإرهاب السيبراني على الأمن الوطني الجزائري	54
ثانيا :مخاطر الألعاب الإلكترونية على أطفال الجزائر	55
ثالثا :مخاطر مواقع التواصل الاجتماعي الهدامة	57
مخاطر التواصل الاجتماعي على الأمن الوطني الجزائري	57
الإشاعات وآثارها على الاستقرار الأمني والسياسي للدولة الجزائرية	57
المبحث الثالث: نماذج التحديات الأمنية	59
المطلب الأول: تسريبات بكالوريا2016	59
المطلب الثاني :لعبة الحوت الأزرق المميتة	59

الملخّص:

تحاول هذه الدراسة البحث في موضوع استخدامات الذكاء الاصطناعي وعلاقته بالأمن السيبراني، حيث تطرقنا في الفصل الأول الذي يعالج فيه مفاهيم الدراسة بدأ بالذكاء الاصطناعي وأهميته في حل المشكلات، ثم عرّجنا إلى الأمن السيبراني وأبعاده وأهميته وأما في الفصل الثاني ذكرنا فيه استخدامات الذكاء الاصطناعي في الأمن السيبراني والتحديات الأمنية، ويحتوي الفصل الثالث على دراسة تحليلية لاستخدامات الإنترنت في الجزائر باعتماد إستراتيجيات من قبل الدولة لتحقيق الأمن السيبراني حيث كرّست الدولة الجزائرية تحديات أمنية غاية في الأهمية والنجاح.

الكلمات المفتاحية:

الذكاء الاصطناعي – الأمن السيبراني – تكنولوجيات المعلومات

Abstract:

This study attempts to research the topic of the uses of artificial intelligence and its relationship to cyber security, as we discussed in the first chapter, which deals with the concepts of the study. We started with artificial intelligence and its importance in solving problems, then we went to cyber security, its dimensions and importance, and in the second chapter we mentioned the uses Artificial intelligence in cyber security and security challenges. The third chapter contains an analytical study of the uses of the Internet in Algeria, adopting strategies by the state to achieve cyber security, as the Algerian state has devoted itself to extremely important and successful security challenges.

key words:
Artificial intelligence – cyber security - information technologies