مقال بعنــوان:

الحوكمة الرقمية كآلية للحد من مخاطر الجريمة السيبرانية.

إعـداد:

الأستاذ: ميدون عباس

جامعة– باتنة1 – الجزائر–

Email: abbes-h@hotmail.fr

الأستاذ: شرقي عمار

جامعة– الجزائر 1

مقدمة:

شهدت الحياة اليومية تطورات وتغيرات عالمية متسارعة شكلت تحديا كبيرا في مجال تكنولوجيا المعلومات والاتصال، بشكل أصبحت فيه هذه الأخيرة هي الأساس الذي يعتمد عليه في شتى المجالات، كما واكب هذه النهضة السريعة توجه عالمي نحو الاستفادة من الفوائد الناجمة عن استخدام التكنولوجيا الرقمية لتحقيق النمو الاقتصادي وزيادة الإنتاجية والكفاءة وتحسين الخدمات وبأقل التكاليف.

وفي السياق ذاته ومع تزايد الاعتماد على مختلف التكنولوجيا الحديثة والاتصال من خلال الاستخدام المتنامي للتطبيقات المتصلة بالانترنت والوسائط الالكترونية والرقمية الجديدة ، مما أدى إلى ظهور أنماط جديدة من الجرائم جاءت عن الاستغلال السيئ للتكنولوجيا، ترتب عنه خلق ظاهرة إجرامية جديدة لم تكن تعرف من قبل، والتي تعرف بالجريمة السيبرانية ، وقد تشعبت أنواعها فمنها مايتصل بالاعتداء على ذات النظام الالكتروني، ومنها مايتعلق بالاعتداء على أمن المعلومات وأخرى ترتبط بعمليات الاحتيال والتزوير الالكتروني...

وبات من الضرورة بمكان إتباع سياسات واستراتيجيات تسهم في الحد من هذه الجرائم وكذلك إشراك المجتمع ومؤسساته العامة والخاصة بذلك، ولهذا فان هناك الكثير من المخاطر المرتبطة بتكنولوجيا المعلومات، لذا أصبح من الضروري استخدام أنظمة امن لأجل الحماية من هذه الجرائم.

الأمر الذي فرض على دول المجتمعات المتقدمة والنامية على البحث عن آليات فعالة للوقاية من هذا النوع من الجرائم من خلال البحث عن مقاربات جديدة يمكن لها أن تواكب هذا التطورات والمتغيرات الجديدة، وإنشاء اطر عمل ووكالات قانونية لحماية البيانات وتقديم المشورة للشركات والمؤسسات ، بالإضافة إلى توفير قنوات رسمية تضمن إعداد كوادر من المهندسين والفنيين المهرة التي تكفل تطبيق استراتيجيات الحوكمة الرقمية بكافة القطاعات ومختلف المجالات مع الحفاظ على أمن وسرية البيانات.

وتعد الجزائر من الدول أولت الاهتمام بتعزيز الأمن السيبراني ومحاربة الجريمة السيبرانية في ظل التحولات الرقمية والثورة المعلوماتية المعاصرة، وذلك قصد فك شفرات وعقد هذا النوع من الجرائم وتفادي الأضرار والخسائر التي يمكن أن تنجر عنها.

وفي ضوء ماسبق يتضح أهمية استخدام الحوكمة الرقمية كآلية وأسلوب للحد من هذا النوع من الجرائم بالاعتماد على مجموعة من الإجراءات والتدابير التي تعمل على الكشف المبكر عنها وإمكانية احتوائها والكشف عن مصادرها قبل وقوعها.

من هذا المنطلق تطرح الورقة البحثية الإشكالية التالية :

إلى أي مدى يمكن أن تساهم الحوكمة الرقمية كآلية فعالة لمواجهة الجريمة السيبرانية ؟

أولا : الإطار النظري والمفاهيمي للحوكمة الرقمية.

1- مفهوم الحوكمة الرقمية: قبل التطرق لمفهوم الحوكمة الرقمية لابد من التطرق إلى توضيح مفهوم الحوكمة والذي يعتبر مفهوما مستجدا على الساحة العلمية.

- يمكن تعريف الحوكمة على أنها الأدوات والعلاقات والأساليب المتعلقة بالحكم لتشمل مجموعة العلاقات القائمة بين الحكومة والمواطنين سواء كافرا داو كجزء من مؤسسات سياسية واجتماعية واقتصادية.[1]

- كما تعرف مؤسسة التمويل الدولية الحوكمة بأنها: النظام الذي يتم من خلاله إدارة الشركات والتحكم في أعمالها، أما منظمة التعاون الاقتصادي والتنمية بأنها: مجموعة من العلاقات التي تربط بين القائمين على إدارة الشركة ومجلس الإدارة وحملة الأسهم وغيرهم من أصحاب المصالح. [2]

- وهناك من يعرفها على أنها: مجموعة القواعد والقوانين التي تضبط عمل المنظمات وتحقيق الرقابة الفعالة على إدارتها وتنظيم العلاقة بينها وبين أصحاب المصالح المختلفة وتهدف إلى تحقيق الشفافية والعدالة ومكافحة الفساد. [3]

في ضوء ما تقدم من التعريفات السابقة يمكن فهم الحوكمة الرقمية بأنها امتداد للحوكمة وهي أداة لتطبيق هذه الممارسات بوسائل الكترونية، أي استخدام التكنولوجيا الحديثة وذلك من اجل إضفاء مزيد من الفعالية والسرعة والشفافية على أداء أنشطة الإدارة الحكومية ونشر المعلومات للعموم وللمؤسسات الأخرى.

بينما تعرف الحوكمة الرقمية حسب منظمة اليونيسكو على أنها: استخدام تكنولوجيا المعلومات والاتصال في القطاع العام، بغرض تحسين تقديم الخدمات وتشجيع مشاركة المواطنين في صنع القرار وجعل الحكومة أكثر خضوعا للمساءلة والشفافية والفعالية[4].

ويعرفها Backus بأنها تطبيق للوسائل الالكترونية في التفاعل بين الحكومة والمواطنين والحكومة والمنظمات وكذلك في مختلف العمليات الحكومية الداخلية لتحسين الديمقراطية والحكومة ومختلف الأعمال الأخرى.

في حين يعرف Heeks الحوكمة الرقمية بأنها : عبارة عن استخدام تكنولوجيا المعلومات والاتصالات من اجل دعم الحوكمة الرشيدة[5].

وعليه يمكن القول أن الحوكمة الرقمية هي استغلال التقنيات الحديثة وتكنولوجيا المعلومات والاتصال لتحقيق أهداف ومبادئ الحوكمة، وذلك بتحويل المحتوى المعلوماتي بالمؤسسات إلى محتوى رقمي، يدعم البنية الأساسية لتكنولوجيا المعلومات.

2- **مبررات التحول نحو الحوكمة الرقمية:** إن من أهم مبررات التحول نحو الحوكمة الرقمية نلخصها فيما يلي: [6]

- الضغوط المتزايدة الملقاة على عاتق الحكومة حول ضرورة تلبية حاجات المواطنين ورغباتهم بكل كفاءة وفاعلية خصوصا مع ازدياد أعداد السكان وارتفاع مستويات المعيشة.
- التعقيدات المتزايدة الملقاة التي تواجه المتعاملين مع القطاعات الحكومية الخدمية المختلفة وفي مقدمتها البيروقراطية والروتين والبطء في تقديم الخدمة.
- التقدم التكنولوجي والثورة المعلوماتية المتسارعة والرغبة والإصرار على تطبيقها لتحسين مستويات الأداء الحكومي.
- تعزيز دور المواطن في المشاركة في عملية الرقابة والمساءلة واتخاذ القرار.
- تقليل كلفة الإجراءات الحكومية .
- الشفافية في الإجراءات.
- تحسين نوعية الخدمات المقدمة وجودتها من خلال الحوكمة الرقمية.

3- **أهمية وأهداف الحوكمة الرقمية:** تكمن أهمية وأهداف الحوكمة الرقمية في :

4-1 -**أهمية الحوكمة الرقمية:** تكمن أهمية الحوكمة الرقمية في النقاط التالية[7]:

- وجود قوانين واطر تحكم تصميم وإطلاق الخدمات الالكترونية.
- وحدة المعايير المتبعة في بناء أنظمة الكترو-حكومية في المؤسسات الحكومية .

- الحد من إخلال الإدارات والمؤسسات بالمخططات التوجيهية العامة الصادرة عن الهيئة المكلفة بإدارة الحوكمة الرقمية.
-القدرة على تقديم خدمات ذات جودة عالية وقياس مدى إقبال الجمهور المستهدف عليها.
- تحقيق أعلى مستويات الفعالية والشفافية والمساءلة بفضل تكامل وتجانس الخدمات الحكومية المقدمة من طرف كل جهة.
- تسهيل عملية الرقابة والإشراف على أداء المؤسسات عبر تحديد اطر الرقابة الداخلية.
- يؤدي انتهاج أسلوب الحوكمة الرقمية إلى توفير الجهد، الوقت والمال لكل الجهات المتعاملة.
- خلق مجتمع متطور يواكب عصر الرقمنة ويتعامل مع مختلف المعطيات التقنية الجديدة.

4-2- **أهداف الحوكمة الرقمية:** تهدف الحوكمة الرقمية إلى تحقيق مجموعة من الأهداف نوجزها فيمايلي[8]:

- تسعى الحوكمة من خلال اعتمادها على التكنولوجيا إلى تسهيل وتدعيم ديناميكية العمل الداخلي للمؤسسات من خلال تشجيع تفاعلاتها، وتحسين سيرورة اتخاذ القرارات ومشاركة المواطنين.
- تؤدي الى الرشادة في تسيير الخدمات العمومية لفائدة مختلف الأعوان
- العمومية الخاصة والمواطنين.
- توفير أحسن للمعلومات وتقديم أجود الخدمات.
- تحقيق الشفافية بهدف التقليل والحد من الفساد.
- تعزيز المصداقية والمسؤوليات السياسية .
- تعزيز الممارسات الديمقراطية من خلال المشاركة والتشاور مع تبادل المعلومات مع المواطنين والمؤسسات والإدارات الحكومية.
- تسليم أسرع وأكثر كفاءة للخدمات العامة.

4-متطلبات تحقيق الحوكمة الرقمية: إن الانتقال إلى الحوكمة الرقمية هو عملية معقدة ومتدرجة تأخذ وقتا طويلا، ويتطلب إنجاح هذه العملية تحقيق مجموعة من الشروط يمكن إيجازها فيما يلي[9]:

- **الدعم الإداري:** تشكل قناعة واهتمام ومساندة الإدارة العليا لتطبيق تكنولوجيا المعلومات في المؤسسات كافة احد العوامل المهمة والمساعدة في تحقيق نجاح تطبيق الحوكمة الرقمية.

- **البنية التحتية للاتصالات وموارد تكنولوجيا المعلومات:** يتطلب نجاح تطبيق الحوكمة الرقمية توفير تكنولوجيا المعلومات الداعمة له، والتي بدورها تتطلب توفير البنى التحتية وتوافر الموازنات المالية للدولة.

- **التشريعات:** لإنجاح الحوكمة الرقمية فان الأمر يتطلب الاعتراف بعملياتها تشريعا وتحديد متطلبات تطبيقها، والسماح بأطر التعاون بين المؤسسات والتركيز على الخصوصية والأمن المعلوماتي.

- **الموارد البشرية:** مع تنامي تحول الحكومات نحو تقديم خدماتها الكترونيا نمت الحاجة إلى الموارد البشرية المتخصصة في جانب تكنولوجيا المعلومات، مما وضع القطاع العام أمام تحديات تنافسية مع القطاع في الحصول على هذه الموارد.

- **الأمن والخصوصية:** يعرف الأمن على انه مجموعة من الإجراءات والسياسات والمقاييس الفنية التي تستخدم لمنع الأفراد غير المسموح لهم بالدخول إلى الشبكة والعبث بمحتوياتها،اوسرقة وتدبير المعلومات الموجودة على نظامها،أما الخصوصية فهي المحافظة على سرية المعلومات الخاصة بالأفراد والتي يتم تخزينها في نظم الحوكمة الرقمية وعدم السماح بالاطلاع عليها من قبل الأفراد الآخرين.

ثانيا- الأطر المعرفية للجريمة السيبرانية:

1- مفهوم الجريمة السيبرانية: تعتبر الجريمة السيبرانية من بين الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطورها ، فقد اصطلح على تسميتها بداية ب إساءة استخدام الكمبيوتر مرورا بإصطلاح احتيال الكمبيوتر، فالجريمة المعلوماتية بعدها جرائم الكمبيوتر، وجرائم التقنية العالية إلى جرائم الهاركز، فجرائم الانترنت وأخيرا الجرائم السيبرانية.

ويقصد بالجريمة السيبرانية جميع الأنشطة التي تؤدي بغرض إجرامي في الفضاء السيبراني، وتستهدف هذه الأنشطة ثلاث فئات: الأشخاص، والمنظمات التجارية وغير التجارية، والحكومات.[10]

وتعرف أيضا بأنها كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل.

في حين عرفت هيئة الأمم المتحدة الجريمة السيبرانية: أنها جميع السلوكات الغير قانونية التي تستخدم عمليات الكترونية تستهدف امن النظام المعلوماتي والمعطيات التي يعالجها.[11]

وقد عرف المشرع الجزائري الجريمة السيبرانية وأطلق عليها تسمية الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وعرفها بموجب المادة02 من القانون رقم 09-04 على أنها:" جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات."

2- أسباب الجرائم السيبرانية: تتمثل أهم أسباب الجرائم السيبرانية فيما يلي:

- **دوافع مادية:** تعد الرغبة في تحقيق الثراء من العوامل الرئيسية لارتكاب الجريمة السيبرانية، فقد تدفع حاجة البعض إلى تحقيق الثراء السريع عن طريق إتاحة الاطلاع على معلومات معينة أساسية ذات أهمية خاصة لمن يطلبها.
- **دوافع انتقامية:** يعد دافع الانتقام من اخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب الجريمة لأنه غالبا مايصدر من شخص يملك معلومات كبيرة عن مؤسسة أو الشركة التي يعمل بها، ويقوم بدافع الانتقام إما نتيجة فصله من العمل أو تخطيه من الحوافز والترقيات ،أو زرع فيروسات في أجهزة العمل أو سرقة صور شخصية بنية التحرش أو التهديد.
- **دوافع شخصية:** غالبا مايكون الدافع لدى مرتكبي الجرائم السيبرانية هي الرغبة في إثبات الذات و الانتصار على تقنية المعلومات، وتحقيق صورة البطل والذكي الذي يستحق الإعجاب لا صورة المجرم الذي يستوجب محاكمته، وهم فئة غير خطيرة لان دافعهم هو الفضول بالدرجة الأولى وليس الربح ولا يملكون أية نوايا سيئة.
- **الرغبة في التعلم:** بهدف الحصول على معلومات وسبر أغوار هذه التقنية المتسارعة التطور، ويفضل هؤلاء البقاء مجهولين اكبر وقت ممكن حتى يتمكنوا من الاستمرار

في التواجد داخل الأنظمة وتعلم أكثر كيفية اختراق المواقع الممنوعة والتقنيات الأمنية الحاسوبية.

- **دوافع سياسية:** وتتمثل في الرغبة في الدفاع عن الآراء والإيديولوجيات مما نتج عنه نشاط إرهابي الكتروني وأفعال إجرامية ضد المعارضين .
- **دافع التهديد والمنافسة:** ينتشر هذا الدفع نتيجة الوقوع تحت تهديد وضغط من الغير في مجالات الأعمال التجارية والخاصة بالتجسس والمنافسة لمحاولة اكتشاف أسرار المنافسين. [12]

3- خصائص الجريمة السيبرانية: تمتاز الجريمة السيبرانية بمجموعة من الخصائص نذكر منها مايلي: [13]

- **جرائم ترتكب بواسطة الأجهزة الالكترونية كالحاسب الآلي والهواتف الخلوية:** وهما الأداتان التي تمكن المجرم من دخول الانترنت لتنفيذ الجريمة.
- **الجرائم السيبرانية هي جرائم عابرة للحدود:** إن الجريمة المعلوماتية هي شكل من أشكال الجرائم العابرة للحدود، فمسح الجريمة لم يعد محليا بل أصبح عالميا، اذ أن العامل لايتواجد ماديا على مسرح الجريمة، فالفاعل يستطيع القيام بجريمته بالدخول إلى ذاكرة الحاسوب الموجود في بلد آخر، وهذا الفعل ليلقى شخصا ثالثا موجود في بلد آخر.
- **صعوبة اكتشاف واثبات الجرائم السيبرانية:** تتميز هذه الجرائم بصعوبة الاكتشاف والإثبات وذلك لعدم ترك الجاني آثار تدل على إجرامه، فالجريمة تتم عن طريق إدخال رموز وأرقام دقيقة يصعب اكتشافها وإثباتها، لهذا عادة مايتم اكتشافها بالصدفة وغالبا مايصعب معاقبة المجرم، وذلك لعدم وجود أدلة قائمة في حقه.
- **جرائم سريعة التنفيذ:** فسرعة ارتكاب الجريمة قد تكون خلال جزء من الثانية، وقد لاتتطلب الإعداد قبل التنفيذ.
- **جرائم ناعمة:** فهي جرائم لاتمارس بالعنف ،ولا تحتاج إلى أدنى مجهود عضلي بعكس بعض الجرائم التقليدية.

4- طبيعة وأشكال الجرائم السيبرانية : تصنف الجرائم السيبرانية إلى قسمين:القسم الأول يستهدف الحواسيب وشبكات المعلومات كالفيروسات، والقسم الأخر يستهدف مستخدمي الانترنت ورواد الفضاء السيبراني، ويشمل ذلك الأفراد والمؤسسات الاقتصادية، والوزارات

الحكومية ومنها التنمر الالكتروني، التصيد والهندسة الاجتماعية وغيرها من الأشكال وهي كمايلي:[14]

– **الفيروسات:** هي برامج حاسوبية خبيثة تنتقل بين الحواسيب بعدة طرق، وتتكاثر بالاعتماد على ملفات أخرى، وهناك عدة أنواع للفيروسات منها مايبدأ عمله بوقت او حادثة معينة، ومنها مايكون مكونا بأجزاء متعددة، ومنها ما تتغير صفاته بشكل دوري، ومنها مايكون متخفيا حتى عن برامج مكافحة الفيروسات، وهي تلحق أضرارا كبيرة ببيئة المعلومات وقد تصل إلى تدمير جميع الملفات الموجودة على وسائط التخزين، او استبدال المعلومات بأخرى لا معنى لها.

– **التنمر الالكتروني:** يعد التمر الالكتروني من أكثر أشكال الجرائم السيبرانية انتشارا خاصة بين طلبة المدارس في جميع المراحل التعليمية، ويتخذ أشكالا متعددة منها: الإساءة والتهديد بالإيذاء، الذم والقدح والتحقير، إرسال الصور والفيديوهات غير الأخلاقية، سرقة الحسابات الشخصية والتطفل عليه، بث خطاب الكراهية، التشهير والتخويف والابتزاز...

– **الهندسة الاجتماعية:** شاع هذا الشكل من الجرائم السيبرانية مؤخرا بسبب الانتشار الواسع والمتسارع لشبكات التواصل الاجتماعي، وتهدف الهندسة الاجتماعية إلى التركيز على اختراق العقول بدلا من التركيز على أجهزة الحواسيب وشبكات المعلومات.

– **تشويه السمعة:** ويعني تشويه سمعة شخص في الفضاء السيبراني من خلال نشر معلومات غير صحيحة بهدف الإساءة إليه والحط من شأنه، ويتضمن تشويه السمعة نشر صور للشخص المستهدف عبر مواقع التواصل الاجتماعي اوعبر البريد الالكتروني بعد تعديلها بواسطة برامج التصميم الرقمي لخدمة أهداف المهاجم.

– **القرصنة:** هي عملية الدخول إلى الأنظمة المعلوماتية من أصحاب الخبرة، وهو عادة مبرمجون غير مسموح لهم بالدخول إلى تلك الأنظمة بهدف كسر الحواجز الأمنية المحيطة بها.

– **التصيد:** يعتبر من أسهل الجرائم السيبرانية لمجرمي الفضاء السيبراني، ولا يتطلب الأمر منهم سوى إنشاء موقع انترنت وإرسال رسائل عبر البريد الالكتروني، لتبدو وكأنها مرسلة من

شركات معروفة لدى الضحايا، وبهذه الطريقة يمكنهم الحصول على بعض تفاصيل حساباته البنكية ، أرقام بطاقة الائتمان أو بعض التفاصيل الشخصية.

– **الاستمالة أو التعزيز:** ويعني هذا النوع من الجرائم السيبرانية محاولة احد الأشخاص البالغين المهتمين بالاستغلال الجنسي للأطفال إقامة علاقة صداقة مع طفل أو مراهق دون الثامنة عشرة من عمره، ويتظاهر المهاجم في بداية الاتصال بصغر سنه ومشاركته نفس الاهتمامات مع الطفل الذي يتواصل معه، لتتطور العلاقة بينهما إلى أن يحوز ثقة الطفل ليدفعه إلى إرسال صور جنسية، كما قد يتطور الأمر إلى إقامة لقاءات جنسية مباشرة بين الطرفين.

ثالثا– انعكاسات تطبيق الحوكمة الرقمية على مخاطر الجريمة السيبرانية: يتمثل دور الحوكمة الرقمية في الحد من مخاطر الهجمات السيبرانية من خلال المحاور التالية:

– **المحور الأول:** ترتكز الحوكمة الرقمية على ثلاث دعائم تتمثل الدعامة الأولى في :الأبعاد الأساسية لتطبيق التحول الرقمي والتي تشمل الهيكلة المالية والإدارية لأنشطة وعمليات وإدارات المؤسسة، وهندسة العمليات التشغيلية للكشف عن العمليات التي تضيف قيمة واستبعاد العمليات التي لاتضيف قيمة، وتحديد شكل وجودة المخرجات النهائية، وصياغة واعتماد مقومات التغذية العكسية، بينما تتناول الدعامة الثانية متطلبات ومقومات نجاح الحوكمة الرقمية من حيث(هيمنة فكر الإدارة الرقمية الفعالة، وتوافر الموازنة المالية الكافية والملائمة، واختيار أفضل الممارسات الرقمية، وبناء واعتماد مؤشرات تقييم الأداء الرقمي)، وأخيرا تشمل الدعامة الثالثة محاور الأمن والخصوصية من حيث(ضمان سرية البيانات والمعلومات، صياغة وتبني معايير السلامة والدقة الرقمية، سهولة تداول البيانات والمعلومات عبر المنصات الرقمية والحكومية.)

– **المحور الثاني:** يتناول انعكاسات تطبيق الحوكمة الرقمية على نجاح استراتيجيات التحول الرقمي وذلك من خلال تعزيز استخدام التكنولوجيا والتقنيات المستحدثة مثل(نظم الذكاء الاصطناعي، تحليل البيانات الضخمة، تقنيات الحوسبة...) وكذلك التغيرات في خلق القيمة المضافة للأنشطة والعمليات والأفراد، التغيرات الهيكلية والبنى التحتية الالكترونية ، وأخيرا الجوانب المالية المعززة من حيث توافر السيولة اللازمة لتطبيق استراتيجيات التحول الرقمي

وتجهيز البنى التحتية الالكترونية وتدريب الأفراد وشراء الأجهزة والبرامج وتدشين المنصات الرقمية.

– **المحور الثالث:** يسهم نجاح الحوكمة الرقمية في تحقيق العديد من المزايا المتمثلة خاصة في سرعة تقديم المنتجات والخدمات والانخفاض النسبي في التكاليف، و ضمان جودة العمليات والخدمات المقدمة للمواطنين، وإحكام عمليات الرقابة والمساءلة للعاملين والمسؤولين من قبل الجهات الرقابية والإشرافية، فضلا عن تعزيز مستويات الإفصاح والشفافية من خلال تقديم ملائمة وآنية عبر المنصات الرقمية لمتخذي القرار.

– **المحور الرابع:** يشمل هذا المحور ضوابط ومعايير تعزيز الأمن السيبراني، حيث أن نجاح تطبيق الحوكمة الرقمية يتوقف على المعايير والضوابط التي تتبناها المؤسسات وتعمل على تنفيذها بشكل سليم وأهمها: معايير إدارة امن الشبكات، وإدارة الأصول المادية والمعنوية، وآليات حماية الأنظمة وأجهزة معالجة المعلومات، ومنهجية إدارة سجلات الأحداث ومراقبة مخاطر الهجمات السيبرانية، ونماذج حماية وتشفير البيانات والمعلومات، الأمر الذي يضمن جودة العمليات والمنتجات والخدمات الحكومية والحد من هجمات الجريمة السيبرانية.

الخاتمة:

إن مواجهة انعكاسات الجريمة السيبرانية تعد من أصعب التحديات التي تتطلب تظافر الجهود خاصة وان استخدام هذه التكنولوجيا في تزايد مستمر في إدارة مختلف الشؤون الأمنية والاقتصادية والعسكرية، مما يتطلب التعاون بين الدول في مجال الأمن المعلوماتي ومواجهة مخاطر الجريمة السيبرانية.

وعلى هذا الأساس أصبحت الجزائر كغيرها من البلدان النامية، مضطرة إلى الدخول في الحوكمة الرقمية القائمة على التكنولوجيا في مختلف المجالات والميادين، وعليه بات من الواجب أن توفر الشروط الضرورية لضمان الاستخدام الآمن والسليم لتكنولوجيا المعلومات والاتصال، قصد تجنب مخاطر وتهديدات الجريمة السيبرانية التي يمكن أن تؤثر على مختلف الأبعاد الاقتصادية والاجتماعية، السياسية ،الثقافية ،الدينية وحتى الفردية.

ومن أهم التوصيات التي يمكن أن نقدمها للتقليل من آثار الجريمة السيبرانية في النقاط التالية:

- ضرورة وضع قواعد إجرائية سريعة تتناسب مع سرعة الجريمة السيبرانية لكي يسهل تقديم الأدلة ومعرفة مرتكبيها وإثباتها.
- العمل على إدارة مخاطر الهجمات السيبرانية على نحو ممنهج يهدف إلى حماية الأصول المعلوماتية والتقنية، وفقا للسياسات والإجراءات التنظيمية والمتطلبات التشريعية.
- ضرورة قيام إدارة المؤسسات بتعظيم الاستفادة من الحوكمة الرقمية في بناء قواعد بيانات ومنصات رقمية، تسهم في معالجة وتحليل البيانات وإدارتها بشكل جيد كضمانة للحد من مخاطر الهجمات السيبرانية.
- زيادة الاستثمار في البنية التحتية الالكترونية من خلال تكريس الإمكانات المالية والبشرية للتصدي لهذه الظاهرة.
- تكثيف الدورات التدريبية والتكوينية والاستفادة من تجارب وخبرات الدول المتقدمة لمحاربة مختلف مظاهر الجريمة السيبرانية.

قائمة المراجع والمصادر:

1- سليمة بن حسين، الحوكمة دراسة في المفهوم، مجلة العلوم القانونية والسياسية، جامعة الشهيد حمة لخضر الوادي،الجزائر،العدد10،2015 ،ص183.

2- زينب يحياوي، الحوكمة الالكترونية مدخل نحو جودة الخدمة العمومية،مجلة التميز الفكري للعلوم الاجتماعية والإنسانية، جامعة الطارف، الجزائر،العدد08،2021، ص64.

3- سعاد مقدم، متطلبات تفعيل الحوكمة الالكترونية في التنظيمات الإدارية الحديثة المفاهيم والية التطبيق،مجلة التميز الفكري للعلوم الاجتماعية والإنسانية،جامعة الطارف،الجزائر،العدد08،2021،ص32.

4- رانية تناح، صافية بومصباح، جاهزية الإدارات المحلية لاعتماد الحوكمة الالكترونية دراسة ميدانية في مقر ولاية برج بوعريريج، مجلة أبحاث ودراسات التنمية، العدد04،2016، ص58.

5- Heeks Rbuilding, e-governance for Development Aframe work -5 for National and Donor Action i- Government Working Paper Series, N12,2001,P02.

6- مقدم سعاد، مرجع سابق، ص ص34-35.

7- رانية تناح، صافية بومصباح، مرجع سابق، ص58.

8- ياسي الهام، الثقافة كمفتاح لنجاح الحوكمة الالكترونية ، مجلة المنهل الاقتصادي ، المجلد03،العدد 02،2020، ص334.

9- تلي مريم، الحوكمة الالكترونية كآلية لتحسين جودة الخدمة الصحية- مع الإشارة إلى تجربة الجزائر، مجلة الحوكمة المسؤولية الاجتماعية والتنمية المستدامة، المجلد03، العدد02،2021، ص ص60-61.

10- Singh,Brijendra. & Singh Hemant Kumar,web data mining research:a Survey paper presented at Computational Intellingence and.Computing Research.(ICCIC) India, Coimtatore,2010,p1.

11- Romain Beas,la lute Contre la Cyber criminalite au regard de laction des etats , doctorat de droit prive,et Sciences

Criminelles,Universite de lorraine,Faculte de droit,Paris,2016,P25-26.

12- سليمة ذياب، بلال بوترعة، الجريمة الالكترونية: الأسس والمفاهيم، مجلة تطوير العلوم الاجتماعية، العدد13، 2020، ص ص14-15.

13- روان بنت عطية الله الصحفي، الجرائم السيبرانية، المجلة الالكترونية الشاملة متعددة التخصصات، العدد2020،24، ص11.

14- Tiwari,S,Bhalla A, & Rawat, Cyber-Crime and -14 Security,Interntional journal of advanced research in .computer Science and Software engineening,2016,P47.