

الأمن الجماعي الرقمي كآلية لمواجهة التهديدات السيبرانية: نحو بناء أمن سيبراني إفريقي

Collective digital security as a tool to face cyber threats: Toward an African cyber security

كيم سمير¹

¹ جامعة الشهيد الشيخ العربي التبسي تبسة، s.kime@univ-tebessa.dz

تاريخ الاستلام: 2024/08/04

تاريخ القبول: 2024/09/16

تاريخ النشر: 2024/10/15

ملخص:

تعد التهديدات السيبرانية من أبرز التحديات الجديدة للأمن الوطني والإقليمي والعالمي، وهو ما يتطلب آليات متنوعة للمواجهة، ومن أبرز هذه الآليات آلية الدفاع السيبراني الإقليمي. على ضوء ذلك فإن دول شمال إفريقيا وعلى رأسها الجزائر وفي ظل تنامي التهديدات السيبرانية يجب العمل على تطوير آليات تعاون إقليمي من أجل بناء أمن جماعي رقمي، ويشكل الفضاء الإفريقي مجالا حيويا لتجسيد هذا التعاون. توصلت الدراسة إلى أن تحقيق الأمن الجماعي الرقمي يتطلب العمل على توحيد التشريعات والسياسات العمومية من أجل أمن سيبراني إفريقي يتماشى مع سرعة الربط بالقارة الإفريقية، وكذا التزام الدول بإعتماد نظم جديدة من خلال قوانين تكون في المستوى لمواجهة الخطر الذي يمثلته التهديد الرقمي. كلمات مفتاحية: الأمن الرقمي الجماعي، الدفاع السيبراني الإقليمي، الأمن السيبراني الإفريقي.

Abstract:

Cyber threats are one of the most important new challenges to national, regional and global security, which require a variety mechanisms. The most prominent of these mechanisms is the regional cyber defense mechanism. For this reason the north African countries, led by Algeria under the growing of cyber threats must develop regional cooperation mechanisms for the building of digital collective security, and the African space is vital for the realization of this cooperation.

This study result that the realization of the regional digital security requires the consolidation of legislations and public policies for African cyber security, in

line with the speed of connectivity to the African continent, also the commitment of countries to adopt new systems of during laws at the level to counter the threat posed by the digital threats.

Keywords: Collective Digital security; Regional cyper defense; African cyper security.

المؤلف المرسل: كيم سيمير، s.kime@univ-tebessa.dz

مقدمة:

تشهد البيئة الأمنية في القرن الواحد والعشرين تطورات عديدة مست مختلف المستويات المتعلقة ببنية وطبيعة التهديدات الأمنية، حيث تتميز التهديدات الأمنية الجديدة بالتعقيد والتشابك، بالنظر لطبيعتها الهلامية، إضافة لتعدد الفواعل والحركات السببية المرتبطة بهذه التهديدات، حيث أصبح إنتشار هذه التهديدات يتجاوز المستوى الوطني ليصل إلى المستويين الإقليمي والدولي.

على ضوء ما تقدم تشكل التهديدات السيبرانية اليوم أحد الأنماط الجديدة للتهديدات الأمنية، التي أصبحت أحد وسائل الحروب الجديدة، حيث إنتقل مجال التهديدات من الفضاء الواقعي العملي إلى الفضاء السيبراني، وهو ما يتطلب من الدول إيجاد إستراتيجيات متنوعة لمواجهة التهديدات السيبرانية تتجاوز الإستراتيجيات الوطنية لتصل إلى البحث عن إستراتيجيات جماعية إقليمية.

في هذا السياق تشكل إستراتيجية الأمن الجماعي الرقمي أحد أهم الإستراتيجيات الفعالة لمواجهة التهديدات السيبرانية التي يجب على دول شمال إفريقيا وعلى رأسها الجزائر تبنيها من أجل مواجهة مختلف التهديدات المتعلقة بالفضاء السيبراني على المستويين الوطني والإقليمي ببعديه المغاربي والإفريقي.

تهدف هذه الورقة البحثية إلى تحليل مختلف الآليات التي تمكن الجزائر والدول المغاربية من تطوير أمن جماعي رقمي في الفضاء السيبراني الإفريقي بهدف مواجهة مختلف التهديدات السيبرانية، عبر العمل على إيجاد تنسيق وتعاون مشترك على المستوى الإقليمي، إضافة إلى تعزيز التعاون الإفريقي عبر التنسيق المؤسسي في إطار المنظمات الإقليمية المختلفة.

لتحقيق هذا الهدف تسعى هذه الورقة البحثية إلى معالجة الإشكالية التالية: كيف يمكن أن تساهم إستراتيجية الأمن الجماعي الرقمي في مواجهة التهديدات السيبرانية في الفضاء السيبراني الإفريقي؟

تندرج تحت هذه الإشكالية الأسئلة الفرعية التالية:

- ما المقصود بالأمن الجماعي الرقمي؟
 - ماهي الآليات المعتمدة للتعاون في إطار الفضاء السيبراني الإفريقي؟
 - ماهي أبرز التحديات المرتبطة بمأسسة فضاء سيبراني إفريقي موحد؟
- لمعالجة هذه الإشكالية والإجابة على مختلف الأسئلة الفرعية سيتم اختبار الفرضيات التالية:
- تؤدي الطبيعة المتشابكة والمعقدة للتهديدات السيبرانية إلى محدودية الإستراتيجيات القطرية في مواجهتها.
 - يؤدي العمل على التنسيق والتعاون المشترك بين الدول الإفريقية في المجال السيبراني إلى مأسسة فضاء سيبراني إفريقي موحد.
 - على ضوء ما تقدم سيتم من خلال هذه الورقة البحثية اعتماد المحاور التالية:
 - أولاً: الأمن الجماعي الرقمي مقارنة مفاهيمية.
 - ثانياً: آليات التعاون السيبراني في الفضاء السيبراني الإفريقي.
 - ثالثاً: تحديات مأسسة أمن سيبراني إفريقي.

أولاً: الأمن الجماعي الرقمي مقارنة مفاهيمية

إن ضبط مفهوم الأمن الجماعي الرقمي يتطلب الإحاطة بمجموعة من المفاهيم المرتبطة به وأبرزها مفهوم الأمن السيبراني، الردع السيبراني.

1. مفهوم الأمن السيبراني:

حسب التقرير الصادر عن الاتحاد الدولي للاتصالات، ، حول "إتجاهات الإصلاح في الاتصالات للعام 2010-2011"، فإن الأمن السيبراني هو مجموعة: " من المهمات، مثل تجميع وسائل، وسياسات، واجراءات أمنية، و مبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات، وممارسات فضلى، وتقنيات، يمكن إستخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين ".⁽¹⁾

كما يعرف الباحث إدوارد أمورسو **Edward Amoroso** الأمن السيبراني بأنه: " وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل

الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها وتوفير الاتصالات المشفرة... الخ".⁽²⁾

و يعرف الكاتبان **Martti Lehto , Pekka Neittamaki** الأمن السيبراني بشكل موجز على أنه: "عبارة على مجموعة من الإجراءات التي إتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها ويتضمن تنفيذ التدابير المضادة المطلوبة".⁽³⁾

في حين تعرف الباحثة منى الأشقر جبور الأمن السيبراني بأنه: "النشاط الذي يؤمن حماية الموارد البشرية، والمالية، المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار، التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع الى ما كان عليه، بأسرع وقت ممكن، بحيث لا تتوقف عجلة الانتاج، وبحيث، لا تتحول الأضرار الى خسائر دائمة".⁽⁴⁾

2. مفهوم الردع السيبراني:

يعرف الردع السيبراني على أنه "منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية".

ويرتكز الردع السيبراني على ثلاثة ركائز هي عماد إستراتيجية الدفاع السيبراني، تتمثل في: مصداقية الدفاع، والقدرة على الانتقام، والرغبة في الانتقام، ويمكن توضيح ذلك من خلال مايلي:⁽⁵⁾

– **الركيزة الأولى مصداقية الدفاع:** يتطلب الدفاع عن أنظمة المعلومات، وردع أي محاولة لاختراقها من بين متطلبات أخرى، توافر أنظمة نسخ احتياطية **Backup Systems**، مما يعني أن أي هجوم ناجح عليها، لن يسفر عن التدمير التام لها أو فقدان الكلي لما تحويه من معلومات؛ ورغم تزايد تكلفة هذا الحل إلا إنه الحل العملي الأكثر فعالية.

– **الركيزة الثانية القدرة على الانتقام:** لا بد أن يتكبد المهاجم ضرراً يفوق ما وقع على المدافع من أضرار، ولكن هذا يتطلب القدرة على الانتقام وتنفيذ هجمة سيبرانية أو أكثر ضد المهاجم الأصلي، بعد التعرف عليه وهو صعب التحقق.

– **الركيزة الثالثة الرغبة في الانتقام:** فعلى المدافع أو من تعرض للهجوم أن يعلن عن رغبته في الانتقام من المهاجم، ذلك أن امتلاك القدرة على الانتقام لا تكفي بمفردها لردعه.

3. الأطر النظرية المفسرة للأمن السيبراني:

ثمة مجموعة من الأطر التفسيرية والمرتبطة في آن واحد لظاهرة "الحروب السيبرانية"، مما يعكس معضلة تشابك تفاعلات الفضاء الإلكتروني. ففيما يرتبط الأمن السيبراني، سواء للدول أو العالم، ارتباطا وثيقا بهذه الحروب، فإن سعي الدول لحيازة القوة السيبرانية، علاوة على تغير طبيعة الصراعات الدولية، يشكلان بدوريهما مدخلا تفسيريا لنشوب الأنشطة العدائية الإلكترونية، ويمكن تفصيل ذلك على النحو الآتي: (6)

-الإطار الأول الأمن السيبراني:

تزايدت العلاقة بين الأمن والتكنولوجيا، خاصة مع إمكانية تعرض المصالح الاستراتيجية للدول إلى أخطار وتهديدات، الأمر الذي حول الفضاء الإلكتروني لوسيط ومصدر لأدوات جديدة للصراع الدولي. و فرضت تلك التطورات إعادة التفكير في مفهوم "الأمن القومي للدولة"، والذي يعني بحماية قيم المجتمع الأساسية، وإبعاد مصادر التهديد عنها، وغياب الخوف من خطر تعرض هذه القيم للهجوم .

بيد أن طبيعة ذلك الفضاء، كساحة عالمية عابرة لحدود الدول، جعل الأمن السيبراني يمتد من داخل الدولة إلى النظام الدولي ليشكل نوعا من الأمن الجماعي العالمي، خاصة مع وجود مخاطر تهدد جميع الفاعلين في مجتمع المعلومات العالمي.

لذا أصبحت هناك مصلحة قطرية، وكذلك دولية، في الحفاظ على أمن الفضاء الإلكتروني، على أساس أن الأخير صار جزءا من الأمن العالمي. ودعم ذلك الطبيعة المتغيرة للتفاعلات الإلكترونية، خاصة مع تطور القدرات البشرية على إنتاج تقنيات جديدة، فضلا عن تصاعد مخاطر التهديدات الإلكترونية على البنية التحتية الكونية للمعلومات .

كما أن تراجع سيادة الدولة مع تصاعد دور الفاعلين من غير الدول في العلاقات الدولية (مثل الشركات التكنولوجية العابرة للحدود، وشبكات الجريمة، والقرصنة الإلكترونية، والجماعات الإرهابية وغيرها) فرض تحديات عديدة في الحفاظ على الأمن السيبراني العالمي. و دفع ذلك إلى بروز اتجاهات متعددة لتحقيق ذلك الأمن عبر التنسيق بين أصحاب المصلحة من الحكومات، والمجتمع المدني، والشركات التكنولوجية، ووسائل الإعلام، وغيرها .

– الإطار الثاني القوة السيبرانية:

لعب الفضاء الإلكتروني دورا أساسيا في تعظيم القوة، أو الاستحواذ على عناصرها الأساسية في العلاقات الدولية، حيث أصبح التفوق في ذلك المجال عنصرا حيويا في تنفيذ عمليات ذات فاعلية في الأرض، والبحر، والجو، والفضاء، واعتماد القدرة القتالية في الفضاء الإلكتروني على نظم التحكم والسيطرة التكنولوجية.

وأدى ذلك الأمر إلى تغيير في مفهوم القوة الوطنية للدولة، فبات بالإمكان تعريفها بأنها "مجموعة الوسائل، والطاقت، والإمكانات المادية وغير المادية، المنظورة وغير المنظورة التي بحوزة الدولة، ويستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة، وتؤثر في سلوك الوحدات السياسية الأخرى.

ثانيا: آليات التعاون السيبراني في الفضاء السيبراني الإفريقي

يشكل الفضاء السيبراني الإفريقي أحد الفضاءات الحيوية المهمة لدول شمال إفريقيا وعلى رأسها الجزائر من أجل إيجاد آليات تعاون إقليمية في المجال السيبراني، على ضوء ذلك سيتم من خلال هذا المحور تحليل مختلف الجهود الإقليمية في مجال التعاون السيبراني على مستوى الفضاء السيبراني الإفريقي، وذلك على النحو التالي:

1. إتفاقية الاتحاد الإفريقي لأمن الفضاء السيبراني كمرجعية لمأسسة الفضاء السيبراني الإفريقي:

رغم الإنتشار الواسع للتهديدات السيبرانية وخصوصية الدول الإفريقية، إلا أن الجهود المؤسسية الفعلية لمواجهة التهديدات السيبرانية من خلال الاتحاد الإفريقي من أجل تطوير مبادرات تنظيمية ملموسة في إطار الأمن السيبراني لم تبدأ إلا مع سنة 2008، وبعد إنخفاض تغلغل تكنولوجيا المعلومات و الاتصالات في إفريقيا، وكذا قلة توفر التقنيات اللاسلكية على نطاق واسع عاملا رئيسيا قد يعيق مبادرات التعاون الإقليمي في المجال السيبراني، وهو ما دفع الاتحاد الإفريقي إلى بدء أولى الخطوات في مجال تعزيز الأمن السيبراني التي تم تبنيها من خلال مسودة تقرير الاتحاد الإفريقي حول دراسة إمكانية تنسيق الاتصالات والبيانات والسياسات التكنولوجية وتنظيمها سنة 2008. التقرير أكد على الحاجة إلى وضع سياسة إقليمية منسقة على المستوى الإفريقي وإطار تنظيمي بشأن الأمن السيبراني.⁽⁷⁾

في سنة 2011 قادت جهود الاتحاد الإفريقي واللجنة الاقتصادية لإفريقيا إلى وضع مسودة لتطوير إطار للأمن السيبراني سميت مسودة إتفاقية إنشاء إطار قانوني موثوق للأمن السيبراني في إفريقيا، وقد تم اعتماد هذه الإتفاقية في سنة 2012 من طرف فريق الخبراء المعني بالأمن السيبراني، وأعقب ذلك موافقة

الإتحاد الإفريقي من خلال الدورة العادية الثانية والعشرين للمجلس التنفيذي للإتحاد الإفريقي في جانفي 2013 على عرض الاتفاقية للمصادقة القانونية من قبل مؤتمر وزراء العدل في الإتحاد الإفريقي في أكتوبر 2013. وفي 27 جوان 2014 وبعد تأجيلات عديدة نتيجة لمشكلات تقنية وقانونية إعتد رؤساء ودول وحكومات الإتحاد الإفريقي نسخة منقحة من مشروع الاتفاقية خلال الدورة الثالثة والعشرين للجمعية العامة للإتحاد الإفريقي في مالابو عاصمة غينيا الإستوائية ، والتي أصبحت تعرف بإسم إتفاقية الإتحاد الإفريقي للأمن السيبراني وحماية البيانات ذات الطابع الشخصي.⁽⁸⁾

تهدف إتفاقية الإتحاد الإفريقي للأمن السيبراني وحماية البيانات ذات الطابع الشخصي إلى تحقيق الأهداف، ومن بينها تحقيق ومواءمة قوانين الدول الإفريقية بشأن التجارة الإلكترونية، حماية البيانات، حوكمة الأمن السيبراني، مكافحة الجرائم السيبرانية، كما حددت الإتفاقية أهداف مجتمع المعلومات في إفريقيا وتسعى لتعزيز القوانين الحالية لتكنولوجيا المعلومات و الإتصالات للدول الأعضاء وتعزيز الإقتصاد الإقليمي من خلال إحترام قواعد حوكمة الأمن السيبراني ومكافحة الجرائم السيبرانية.⁽⁹⁾

وقد تضمنت ديباجة هذه الإتفاقية مفهوم للأمن السيبراني الإفريقي بإعتباره عمل الدول الإفريقية على تنظيم المجال التكنولوجي على وجه الخصوص من خلال رؤية تعكس توقعات العديد من الجهات الفاعلة مع المصالح المتباينة في الكثير من الأحيان، عبر التأسيس لفضاء سيبراني آمن للتعاملات الإلكترونية، حماية البيانات الشخصية، مكافحة الجرائم السيبرانية.⁽¹⁰⁾

وقد تضمنت الإتفاقية مجموعة من الإلتزامات والآليات المفروضة على الدول الأعضاء التقيد بها من أجل حماية وضمان أمن سيبراني إفريقي، وتتمثل هذه الآليات فيمايلي:⁽¹¹⁾

- تأسيس إطار وطني للأمن السيبراني.
- تعزيز ثقافة الأمن السيبراني.
- تأسيس بنى وقواعد وطنية لتعزيز حوكمة الأمن السيبراني.
- حماية البنية التحتية للمعلومات.
- مأسسة الإجراءات والتدابير الجزائية اللازمة لمكافحة الجرائم السيبرانية.
- تعزيز التعاون الدولي في مجال مواءمة التشريعات المتعلقة بالأمن السيبراني.

أن العمل على تطبيق إتفاقية الاتحاد الإفريقي للأمن السيبراني يحقق العديد من المكاسب أهمها:

- زيادة الوعي بالأمن السيبراني لدى الدول الأعضاء.
- تعزيز الأنظمة الوطنية للأمن السيبراني.
- فرض مجموعة من الالتزامات على الدول الأعضاء ذات الطابع الإيجابي فيما يخص حماية أمنها السيبراني.
- إمكانية فرض عقوبات من طرف الاتحاد الإفريقي على الدول الأعضاء غير الملتزمة بقواعد الإتفاقية.

2. مقومات التعاون السيبراني في الفضاء السيبراني الإفريقي:

تم إطلاق العديد من المبادرات وتنفيذها لتحسين الفضاء السيبراني الإفريقي، وأهم هذه المبادرات تحسين الجودة التنظيمية للفضاء السيبراني، ويمكن رصد أهم الجوانب المؤسسة لتعاون سيبراني إفريقي من خلال مايلي:

- تعزيز الأمن السيبراني عبر حملات التوعية حول أمن البيانات والمعلومات، حماية البيانات الشخصية للمواطنين:

يتم هذا الأمر عبر تقييم الاستعدادات الحالية للدول الإفريقية في مجال الأمن السيبراني، من أجل المضي قدما في الاستقرار الاقتصادي وتحقيق أهداف التنمية المستدامة لإفريقيا. إضافة إلى تعزيز القدرات المحلية والوطنية وتعزيز الأطر والسياسات واللوائح التنفيذية في مجال الأمن السيبراني التي تم إعتمادها في إتفاقية الاتحاد الإفريقي للأمن السيبراني وتنفيذها على العديد من المستويات أمر بالغ الأهمية لبناء وزيادة تعبئة الموارد للتوعية من الأخطار المرتبطة بالفضاء السيبراني وتعبئة المواطنين وتطوير قدراتهم ومهاراتهم على أساس متين لمواجهة التهديدات السيبرانية.

إضافة إلى ذلك تعزيز وتطوير قدرة الفضاء السيبراني على الصمود وتوظيف الخبراء في المجال السيبراني خبرتهم في إطار الوقاية والحماية والتخفيف والرد ضد جميع أنواع الهجمات الإلكترونية والمخاطر التي تؤثر على السلامة والرفاهية والأمن الإقتصادي للدول الإفريقية.⁽¹²⁾

- إلزام مختلف الفواعل المحليين والوطنيين بالتجسيد الفعلي لمختلف المبادرات التعاونية في المجال السيبراني:

من خلال العمل على تقييم السياق التقني والتنظيمي للفضاء السيبراني للدول الإفريقية، وذلك على العديد من المستويات منها المتطلبات التقنية والتنظيمية، البنى المحلية والوطنية، اللوائح والتدابير القانونية، التعاون التقني على المستوى الدولي، المساعدات والتبادلات، بناء القدرات وتعزيز الكفاءات، هي متطلبات ذات أهمية كبيرة في مجال تعزيز وحماية الأمن السيبراني عبر تحليل وتقييم نقاط الضعف في المجال السيبراني في الوقت المناسب، وكذا إستخدام تقنيات الإنذار المبكر وتعزيز التأهب و الإستجابة لمختلف المخاطر السيبرانية.⁽¹³⁾

في هذا السياق يشير التقرير الخاصة بمجلس الاتحاد الإفريقي نوفمبر 2016 حول الأمن السيبراني أن 11 دولة إفريقية لديها أحكام وقوانين محددة للتعامل مع جرائم الإنترنت والأدلة الإلكترونية وهي: بوتسوانا، الكاميرون، كوت ديفوار، غانا، موريتانيا، وموريشيوس ونيجيريا والسينغال وتنزانيا وأوغندا وزامبيا. وهناك 12 دولة أخرى إتخذت على الأقل بعض التدابير التشريعية في مجال الأمن السيبراني.⁽¹⁴⁾

في نفس السياق يقترح مجموعة من الخبراء الأفارقة مجموعة من القواعد والآليات التي تعزز التعاون بين الدول الإفريقية في المجال السيبراني وهي:⁽¹⁵⁾

- تحسين الإطار الحالي للأمن السيبراني من أجل كفاية وفعالية التعاون الدولي، وتعزيز المساعدات المتبادلة بين الدول الإفريقية.
- إذا تم الإتفاق على أن التهديدات السيبرانية تؤثر على الدول الإفريقية، فإن مصادر هذه التهديدات قد تكون خارج القارة الإفريقية، وهو ما يستدعي الحاجة إلى تعاون دولي واسع بين كل الدول.
- إنشاء فرق إقليمية للإستجابة لحالات الطوارئ المتعلقة بالتهديدات السيبرانية، لتسهيل جهود الأمن السيبراني، والرد على الجرائم السيبرانية على المستوى الإقليمي، إضافة إلى تسهيل التعاون في مجال الأمن السيبراني بين المراكز الوطنية المختلفة المختصة في الأمن السيبراني.
- تعزيز مشاركة القطاع الخاص في مجال الأمن السيبراني الإفريقي.
- تشجيع اعتماد وتنفيذ التدابير المتعلقة بتعزيز الأمن السيبراني في مجال الخدمات الإلكترونية ، ومكافحة الجرائم السيبرانية و إنتهاكات حقوق الإنسان في الفضاء السيبراني.

- تقديم المشورة للحكومات الإفريقية بشأن التدابير الرامية إلى تعزيز الأمن السيبراني ومكافحة الجرائم الإلكترونية.
- تحليل السلوكيات الإجرامية لمستخدمي الفضاء السيبراني الإفريقي وتحويل المعلومات المرتبطة بشأنها إلى المراكز الوطنية المتخصصة.
- إنشاء وكالة سيبرانية إقليمية محاكاة للوكالة الأوروبية لأمن المعلومات.
- يجب أن توفر المقاربة العالمية المنسقة في المجال السيبراني للبلدان الإفريقية فهما واضحا للمخاطر المستقبلية ومواطن الضعف في التكنولوجيا الذكية والإنترنت، ودعم البلدان لإيجاد بيئة إلكترونية آمنة ومرنة من خلال توفير المساعدة من أجل تطوير المنظومة الوطنية للأمن السيبراني لمنع ومكافحة جميع الأنشطة الخبيثة التي تتم عبر الإنترنت.
- ضرورة عمل البلدان الإفريقية على أن المخاطر السيبرانية أصبحت تهديدات ذات طابع عالمي، وهي تساعد على زيادة خطر التهديدات التقليدية مثل الإرهاب، وهو ما يستدعي تكييف المنظومة الأمنية للدول مع التحديات الأمنية للعصر الرقمي.

3. نحو بناء جيش سيبراني إفريقي:

- تشكل مسألة بناء الجيوش السيبرانية تجربة حديثة يمكن للدول الإفريقية إعتماها من أجل فضاء سيبراني إفريقي آمن وموحد، والمهمة التي سيقوم بها الجيش السيبراني للدول الإفريقية ستكون حماية السيادة السيبرانية للدول الإفريقية، وبالأخص حماية الجيش، الحكومة، قواعد البيانات المدنية، وستكون مهام الجيش السيبراني الإفريقي كمايلي: ⁽¹⁶⁾
- إيجاد سياسة وإستراتيجية وعقيدة وحوكمة للجيش السيبراني.
 - تأسيس قيادة سيبرانية مركزية للقدرات السيبرانية.
 - تعزيز وبناء القدرات الهجومية والدفاعية في المجال السيبراني.
 - تنفيذ وتحليل جميع عمليات التشفير في الفضاء السيبراني.

- تعزيز كفاءة وقدرات القيادة السيبرانية المركزية، التخطيط، التنسيق، وتنفيذ العمليات السيبرانية.
- الربط بين دور الفاعلين في إطار المجموعات الخاصة بالأمن السيبراني.
- تجميع المعلومات الاستخباراتية وتحليل في الميدان السيبراني.
- توظيف المحاربين في المجال السيبراني.
- تدريب وتعزيز قدرات المحاربين في المجال السيبراني.
- التعاون مع المختصين الخارجيين في مجال الأمن السيبراني.

على ضوء ما تقدم فإن الجيش السيبراني الإفريقي يجب أن يكون تحت قيادة إستراتيجية عسكرية، من أجل التكامل مع باقي العناصر والمكونات المشكلة للجيش السيبراني من أجل ضمان تسيير إستراتيجي للجيش السيبراني، وسيكون الدفاع السيبراني استثمارا كبيرا للدول الإفريقية بالنظر للحاجة إلى تطوير التكنولوجيات الدفاعية والهجومية ضد الهجمات السيبرانية.

كما أن تأسيس جيش سيبراني إفريقي سيكون له العديد من المزايا الإستراتيجية، ومنها أن الجيش السيبراني سيكون بمثابة آلية إرشادية للقوات العسكرية للتمكن والتحكم أكثر في الفضاء المعلوماتي، حيث سيتم تعزيز قدرات الدفاع والحماية للممتلكات التكنولوجية، والفضاء السيبراني للدولة، ويجعل من الممكن التصدي للعدوان والهجمات السيبرانية من طرف الدول المعادية. والميزة الإستراتيجية ستكون الحفاظ على السيادة الوطنية السيبرانية والقدرة على المحافظة عليها ضد الهجمات السيبرانية. كما سوف تدعم النهوض بالإقتصاد الوطني للدول بالنظر لأمن الفضاء السيبراني.⁽¹⁷⁾

ثالثا: تحديات مؤسسة أمن سيبراني إفريقي

تواجه الدول الإفريقية العديد من التحديات في إطار مؤسسة أمن سيبراني إفريقي موحد، في هذا

الإطار يمكن رصد أهم التحديات من خلال عدة مستويات:

1. التحديات المرتبطة بتنمية التجارة الإلكترونية في إفريقيا:

- أقرت إتفاقية الإتحاد الإفريقي للأمن السيبراني لسنة 2014، في ديباجتها أن هناك العديد من التحديات الأمنية التي تعيق تنمية التجارة الإلكترونية في إفريقيا وهي:⁽¹⁸⁾
- أوجه القصور المؤثرة في تنظيم الاعتراف القانوني بالاتصالات البينية والتوقيع الإلكتروني.
 - عدم وجود قواعد قانونية محددة تحمي المستهلكين وحقوق الملكية الفكرية والبيانات ذات الطابع الشخصي وأنظمة المعلومات.
 - عدم وجود تشريعات متعلقة بالخدمات الإلكترونية والعمل عن بعد.
 - إشكالية تطبيق التقنيات التكنولوجية على الأعمال التجارية والإدارية.
 - الأدلة الموثوق بها الناجمة عن التقنيات الرقمية.
 - القواعد المطبقة على أجهزة وخدمات التشفير.
 - الرقابة على الإعلانات عبر الإنترنت.
 - عدم وجود تشريعات مالية وجمركية ملائمة للتجارة الإلكترونية.

2. التحديات المرتبطة بالمنظومات الوطنية للأمن السيبراني:

والتي يمكن رصدتها من خلال مايلي:⁽¹⁹⁾

- انخفاض مستوى التحكم في القواعد الأمنية اللازمة لمنع ومراقبة المخاطر التكنولوجية والمعلوماتية.
- نقص الدراية الفنية في مجال الأمن السيبراني، وعدم القدرة على الرصد والدفاع عن الشبكات الوطنية، وهو ما جعل البلدان الإفريقية معرضة للتجسس الإلكتروني، وكذا هجمات شبكات الإرهاب الإلكتروني.
- عدم القدرة على تطوير الأطر القانونية اللازمة لمنظومة الأمن السيبراني الوطني لمواجهة مختلف الجرائم السيبرانية، في هذا السياق وفي إطار مسح أجرته اللجنة الاقتصادية للإتحاد الإفريقي حول 21 دولة من

الدول الإفريقية وجدت ضعف التدابير التشريعية المقترحة لأجل حماية النظم المعلوماتية ومكافحة الجريمة الإلكترونية في كل من القطاعين العام والخاص.

- إن التحديات المرتبطة بالأمن السيبراني تتجاوز المخاطر المرتبطة بالأمن الوطني ، ومع ذلك نجد أن القليل من المبادرات المتعلقة بالأمن السيبراني يتم تنفيذها، ورغم أن الاتحاد الدولي للاتصالات رحب بإنهاء الكثير من المشاكل المرتبطة بالفضاء السيبراني في إفريقيا، إلا أن الكثير من التحديات الملحة تحتاج معالجة أكثر شمولاً.

- الحاجة إلى إعادة بناء مجتمع المعلومات يحترم القيم الحقوق والحريات، ويضمن المساواة في الوصول إلى المعلومات، مع تشجيع إنشاء معرفة أصيلة تؤسس لبناء الثقة في استخدام تكنولوجيا المعلومات و الاتصالات.

- المستوى المحدود للوعي من مخاطر القضايا المتعلقة بأمن المعلومات والبيانات من قبل الفاعلين في المجال السيبراني مثل منظمات الاتصالات وتكنولوجيا المعلومات، الوكالات القانونية، القضاء، المتخصصين في المعلومات والتكنولوجيا والمستخدمين.

3. التحديات المرتبطة بحوكمة الفضاء السيبراني الإفريقي:

تواجه عملية حوكمة الفضاء السيبراني الإفريقي مجموعة من التحديات تتمثل أهمها فيما يلي:⁽²⁰⁾

- التحدي الأول يتمثل في ضعف أداء الحكومات الإفريقية في مجال النشاط والمشاركة في التعاون الدولي في تسيير الأمن السيبراني، وفي سياق التعاون الدولي على المستوى الإقليمي فقد عقد المنتدى الإفريقي لحوكمة الإنترنت ثلاث دورات فقط لحد الآن، كما أن عدد الدول المشاركة يجب أن يتضاعف مع مرور الوقت، وبالتفصيل فإن المشاركين 195 في الدورة الثانية للمنتدى الإفريقي لحوكمة الإنترنت كانوا من الحكومات، القطاع الخاص، المجتمع المدني، المنظمات الإقليمية لـ 29 دولة فقط مقارنة بالعدد الإجمالي للدول الإفريقية المقدرة بـ 54 دولة.

- التحدي الثاني مرتبط بالتأثر الكبير لمؤسسات الحوكمة الإفريقية وتبعيتها للدول الغربية، وهو ما يجعلها تقبل بجميع مفاهيمها، المخاطر المعلوماتية، النظم المعلوماتية، وهو ما يؤدي إلى نتيجة إلى أن القارة الإفريقية سوف تستعمر مجددا في مجالها السيبراني، ولن تكون مستقلة وليست لها قوة اتخاذ القرارات في قضايا حوكمة الفضاء السيبراني.

- التحدي الثالث يرتبط ضعف قدرات إدارة الفضاء السيبراني على المستوى الإفريقي، ويتجسد ذلك من خلال ضعف القدرات الفنية والمالية، قصور المستخدمين والوكالات المتخصصة في مكافحة الجرائم السيبرانية للدول الإفريقية، وهو ما يضع الكثير من الحواجز لتنفيذ التدابير والوسائل المتعلقة بالأمن السيبراني، إضافة إلى غياب وكالة متخصصة في مجال الأمن السيبراني.

- التحدي الرابع المتعلقة بمأسسة حوكمة الفضاء السيبراني الإفريقي، أن الإتحاد الإفريقي لم يقيم بتأسيس أي قوة ترافق الدول الأعضاء، وكالة رسمية وغير رسمية، ولذا على الدول الإفريقية الاستفادة من تجربة الإتحاد الأوروبي الذي أسس نظام لإدارة الفضاء السيبراني الأوروبي، وبالمقابل فإن مستوى التكامل في إفريقيا ضعيف، والعلاقة بين الإتحاد الإفريقي والدول الأعضاء ليست وطيدة، إضافة إلى أن الإتحاد الإفريقي من الصعب أن يلعب دور المنسق والجامع لنشاطات الدول الإفريقية في مجال الأمن السيبراني، إضافة إلى ضعف المنظمات غير الحكومية الإفريقية التي أغلبها مدعمة ماليا من طرف الدول الغربية.

خاتمة:

لقد تم من خلال هذه الورقة البحثية تحليل دور آلية الأمن الجماعي الرقمي في الحد من التهديدات السيبراني، عبر تقديم مجموعة من التصورات المتعلقة ببناء فضاء سيبراني إفريقي، حيث تم تقديم التأصيل المفاهيمي عبر تحديد مفهوم الأمن السيبراني والردع السيبراني، كما تم ضبط الأطر النظرية المفسرة للأمن السيبراني، وقد تم تحليل آليات التعاون السيبراني في الفضاء السيبراني الإفريقي من خلال تحليل مختلف جوانب إتفاقية الإتحاد الإفريقي لأمن الفضاء الرقمي، كما تم تحديد المقومات التي تدعم التعاون السيبراني الإفريقي، وأخيرا تم تحديد مختلف التحديات التي تواجه مأسسة أمن سيبراني إفريقي.

على ضوء ما تقدم يمكن الخروج بالنتائج التالية:

- تعتبر آلية التعاون الجماعي السيبراني خيارا إستراتيجيا للدول المغاربية وعلى رأسها الجزائر من أجل بناء فضاء سيبراني آمن.
 - يشكل الفضاء السيبراني الإفريقي مجالا حيويا لتعزيز التعاون السيبراني بين الدول المغاربية في مجال حماية الأمن السيبراني.
 - تشكل إتفاقية الإتحاد الإفريقي لأمن الفضاء الإلكتروني مرجعية مؤسسية مهمة لدعم التعاون السيبراني الإفريقي.
 - يرتبط نجاح التعاون السيبراني الإفريقي بضرورة إلتزام الدول بتنفيذ مختلف المبادرات الإقليمية المتعلقة بأمن الفضاء السيبراني.
 - إن مؤسسة أمن سيبراني إفريقي تواجه العديد من التحديات التقنية والفنية والمالية ، وهو ما يحتم على الدول الإفريقية العمل على تجاوز هذه التحديات من أجل فضاء سيبراني إفريقي موحد.
- الهوامش:

¹: منى الأشقر جبور، " الأمن السيبراني: التحديات ومستلزمات المواجهة". شوهدي في: 02-08-2024، أنظر:

https://carjj.org/sites/default/.../wrq_ml_lmrkz_-_d._mn_lshqr.docx

²: مُجد مختار، " هل يمكن أن تتجنب الدول مخاطر الهجمات الإلكترونية"، دورية اتجاهات الأحداث ، العدد 6، (جانفي 2015)، ص 35

³: Martti Lehto , Pekka Neittaanmäki , Cyber Security: Analytics, Technology and Automation (Switzerland : Springer International Publishing , 2015), P25.

⁴: جبور، مرجع سابق.

⁵: رغدة البهي، " الردع السيبراني: المفهوم والإشكاليات"، مجلة العلوم السياسية والقانون ، العدد 01 (2017). ص 52.

⁶: عادل عبد الصادق، " أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي"، مجلة السياسة الدولية، العدد 208 (2017)، ص32.

⁷: Uchenna Jerome Orji , " The African Union convention on cyper security : a regional response towards cyper stability ? ", Masaryk University Journal of Law and Technology, Number 02.(2018) , p 96.

⁸ : Uchenna Jerome Orji, " Multilateral legal responses to cyber security in Africa: Any hope for effective International cooperation? ", see on 03-08-2024 , look : <https://ccdcoe.org/uploads/2018/10/Art-08-Multilateral-Legal-Responses-to-Cyber-Security-in-Africa-Any-Hope-for-Effective-International-Cooperation.pdf> .

⁹ : Ibidem .

¹⁰ : Xiao Yingying , Yuan Zhengqing , " A primary exploration on cyber security governance in Africa", Jouranal of West Asia and Africa , Number 03.(2016), p 08.

¹¹: Uchenna, (The African Union), op-cit , p113.

¹² : Ernest Tambo, Kazienga Adama , " Promoting cyber security awareness and resilience approaches, capabilities and actions plans against cyber crimes and frauds in Africa", International Journal of Cyber-Security and Digital Forensics , Number 03. (2017), p 132.

¹³ : Ibid, p 133.

¹⁴ : Nir Kshetri , " Cyber crime and Cybersecurity in Africa ", Journal of Global Information Technology Management, Number 02. (2019), p78.

¹⁵ : African Telecommunications Union, "Enhancing Cyber Security in Africa: New challenges for regional Organizations ? ", see on : 02-08-2024 , look : https://www.itu.int/en/ITU-T/Workshops-and-Seminars/cybersecurity/Documents/PPT/S3P2_Meriem_Slimani.pdf .

¹⁶ : M Aschmann, J Jansen Van Vuuren , L Leenen , " Towards the establishment of an African Cyber- Army ", Journal of information warfare, Number 03.(2015) , p 25.

¹⁷ : Ibid, p 26.

¹⁸ : منظمة الاتحاد الإفريقي، " إتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي". معتمدة في 27 جوان 2014.

¹⁹ : United Nations economic commission for Africa , " Tackling the challenges of cybersecurity in Africa " see on 03-08-2024 , look : https://www.uneca.org/sites/default/files/PublicationFiles/ntis_policy_brief_1.pdf,

²⁰ : Xiao Yingying, Yuan Zhengqing , op-cit. p23.