التداعيات السياسية والاقتصادية لمهددات الأمن السيبراني في نيجيريا

د. شيماء محي الدين محمود

أستاذ العلوم السياسية المساعد بكلية الدراسات الأفريقية العليا– جامعة القاهرة

د. سمر حسن الباجوري[1]

أستاذ الاقتصاد المساعد بكلية الدراسات الأفريقية العليا– جامعة القاهرة

ملخص:

لقد أدى التوسع الكبير في استخدام الإنترنت وتطبيقاته المختلفة إلى ظهور تهديدات أمنية مثيرة للقلق خلفت آثاراً سياسية واقتصادية واجتماعية بالغة الخطورة. وبصفة عامة، انتشرت الهجمات والجرائم السيبرانية بشكل يسترعي الانتباه، لاسيما في دول القارة الأفريقية، التي تعاني من ضعف البنية التحتية التكنولوجية واختراق الأمن السيبراني على نحو متكرر وفي الكثير من الأجهزة والمصالح الكبرى سواء حكومية أو غير حكومية. ولقد اتسع نطاق الجرائم السيبرانية لتشمل سرقة الهوية والمواد الإباحية والقرصنة ورسائل البريد الإلكتروني الاحتيالية والتصيد الاحتيالي، وغير ذلك من جرائم باتت تنتشر وتكبد حكومات الدول الأفريقية خسائر ذات بال، وذلك من خلال وجود خروقات متكررة للبيانات الإلكترونية للوكالات الحكومية، والتي غالبًا ما تنفذها الجماعات الإرهابية بهدف زعزعة استقرار الأنظمة السياسية. وقد سلطت العديد من الحوادث في العقد الماضي الضوء على مهددات وتحديات الأمن السيبراني التي تواجه الدول الأفريقية، فمازالت أنظمة الأمن السيبراني في العديد من الدول الأفريقية غير كافية، حيث كشف تقرير الأمن السيبراني لعام ٢٠٢٣ أن تدابير الأمن السيبراني في أفريقيا في كل من القطاعين العام والخاص أقل من المتوسط، مما يجعل أفريقيا واحدة من أكثر المناطق التي تواجه تهديدات لأمنها السيبراني في جميع أنحاء العالم. وفي هذا

---

[1] د. شيماء محي الدين محمود، أستاذ العلوم السياسية المساعد بكلية الدراسات الأفريقية العليا، جامعة القاهرة.

د. سمر حسن الباجوري، أستاذ الاقتصاد المساعد بكلية الدراسات الأفريقية العليا، جامعة القاهرة.

(ISSN: 2536 - 9555)

الإطار، تعد نيجيريا حالة جديرة بالدراسة، حيث ارتفعت الجرائم السيبرانية على مدى العقد الماضي بشكل غير مسبوق. ومن هذا المنطلق، تهدف هذه الورقة إلى دراسة وتحليل التداعيات السياسية والاقتصادية لمهددات الأمن السيبراني في نيجيريا. ولقد خلصت الدراسة إلى أن الجرائم والهجمات السيبرانية أثرت بشكل كبير على الاقتصاد النيجيري على المستويين الكلي والجزئي كما أثرت على مناخ الاستثمار وبيئة الأعمال النيجيرية بشكل عام، فضلاً عن تداعيات تلك الهجمات على فاعلية مؤسسات الدولة وأجهزة الأمن في نيجيريا، إلى الحد الذي انعكس على سمعة ومصداقية الدولة على نطاق واسع.

الكلمات المفتاحية: الأمن السيبراني– الجرائم السيبرانية– نيجيريا– مؤشر الأمن السيبراني– القدرة التنافسية.

The Political and Economic Implications of cybersecurity threats in Nigeria

Abstract:

Over the years, the rapid expansion of the internet and the widespread use of various applications have brought about increasingly concerning security threats. Cybercrimes, which include spamming, identity theft, pornography, hacking, fraudulent emails, piracy, and phishing, occur daily and pose a significant global issue, particularly in Africa, where the impacts are severe. In several African countries, especially Nigeria, there are frequent breaches of electronic data from government agencies, often carried out by terrorist groups aiming to destabilize political regimes. Numerous incidents in the past decade have highlighted the cybersecurity risks facing African States. cybersecurity systems in many African countries remain insufficient. The 2023 Cybersecurity Report reveals that cybersecurity measures in both the public and private sectors are below average, making Africa one of the most vulnerable regions worldwide. Nigeria is a key case study where cybercrime has surged over the past decade. This paper examines the political and economic repercussions of cybersecurity threats in Nigeria. The analysis emphasizes the

impact of cybercrimes and attacks on the Nigerian economy at both the macro and micro levels, in addition to the repercussions of these attacks on the effectiveness of state institutions and security agencies in Nigeria, to the extent that it has been reflected in the reputation and credibility of the state on a large scale.

Key words: Cybersecurity- cybercrime- Nigeria- cyber security index- competitiveness.

مقدمة

لقد أدى التطور التكنولوجي والاستخدام المكثف للإنترنت إلى تمهيد الطريق لتحديات أمنية جديدة، مثل الهجمات والجرائم السيبرانية، والتي تنطوي على استخدام التكنولوجيا الرقمية لارتكاب أنشطة غير قانونية، مثل القرصنة وسرقة الهوية والاحتيال عبر الإنترنت وتوزيع البرامج الضارة، وذلك بهدف سرقة معلومات حساسة أو التسبب في تلف أنظمة الكمبيوتر والشبكات العامة والخاصة بالشركات أو الأفراد. ولقد شهدت السنوات الماضية نموًا متطوراً وغير مسبوقاً في عدد الأفراد الذين يستخدمون الإنترنت في أنشطة غير قانونية، حيث يلجأ الجناة إلى أساليب متقدمة مثل استخدام أنظمة الكمبيوتر لارتكاب الاحتيال والإرهاب وغيرها من الأنشطة الإجرامية دون مغادرة أراضيهم الجغرافية الحالية. وجدير بالذكر أن هذا المستوى من التطور والارتفاع المستمر في هذه الممارسات أثار حالة من القلق والرعب بين الأفراد والمنظمات والحكومات على مستوى العالم، وذلك نظراً لما له من تداعيات بالغة الخطورة على الأفراد والجماعات. وبالإضافة إلى ذلك، يشكل الارتفاع المستمر في الجرائم السيبرانية تهديدًا هائلاً للبنية التحتية للدول القومية بشكل يسترعي الانتباه.

وبالرغم من أهمية الإنترنت وما يوفره من فرص للتفاعل الاجتماعي والاقتصادي في أفريقيا، إلا أن استخدامه ينطوي على مخاطر كبيرة خاصة مع كثافة الجرائم السيبرانية وغيرها من مهددات الأمن السيبراني. وتعتبر نيجيريا من أكثر الدول التي تعاني من اختراق أمنها السيبراني لدرجة باتت تهدد استقرارها السياسي والاقتصادي، الأمر الذي يستوجب اهتماماً فورياً ومكثفاً لمعالجة القصور في البنية التحتية الرقمية في نيجيريا،

(ISSN: 2536 - 9555)

ذلك القصور الذي جعلها هدفاً رئيسيًا لمجرمي الإنترنت الذين يستغلون هذه النقاط الضعيفة لارتكاب جرائم مثل سرقة الهوية والاحتيال والتجسس الإلكتروني وغير ذلك من جرائم. وعليه، تتبلور الإشكالية الرئيسية لهذه الدراسة في الإجابة عن تساؤل مفاده: ما أبرز التداعيات السياسية والاقتصادية لمهددات الأمن السيبراني في نيجيريا؟

وفي هذا الإطار، تهدف هذه الورقة إلى دراسة وتحليل تداعيات التهديدات السيبرانية في نيجيريا، سواء كانت سياسية أو اقتصادية، حيث تقدم إطاراً تحليليا لما تسفر عنه تلك التهديدات من آثار كارثية ألقت بظلالها على فرص الاستثمار في الدولة وكذا على مصداقيتها داخلياً وخارجياً، الأمر الذي يجعل من دراسة هذه الآثار وتلك التداعيات أمراً من الأهمية بمكان، وذلك بغرض الوقوف على حدود تأثير تلك الجرائم على الأفراد والحكومات وإلقاء الضوء على نقاط القصور التي يتعين تطويرها وتعزيزها من أجل التخفيف من وطأة تلك الجرائم والحد من آثارها.

ولعل لاختيار حالة نيجيريا ما يبرره، حيث تعتبر نيجيريا الدولة الأفريقية الأكبر من حيث عدد السكان، كما تتميز بتنوع ثقافي واجتماعي يكسبها حالة من الثراء، فضلاً عن كونها دولة بها وفرة بالموارد الطبيعية، الأمر الذي يجعلها قوة إقليمية هامة في إقليم غرب أفريقيا ومحط أنظار الكثير من الدول داخل المنطقة وخارجها. ومن ناحية أخرى، فقد ساهمت جملة من العوامل من بينها الفقر والبطالة ووجود فجوات قانونية وتنظيمية وضعف هيئات وأجهزة تنفيذ القانون وغياب التنسيق بينها وغير ذلك من عوامل ساهمت في انتشار الجرائم والهجمات السيبرانية في نيجيريا، لدرجة أنها باتت تهدد اقتصاد الدولة كما تهدد البنية الأساسية الحيوية لها، فضلاً عن تهديد أمن الأفراد والشركات الكبرى النشطة في نيجيريا، الأمر الذي دفعها إلى سن قوانين وتبني سياسات مثل وثيقة سياسة الأمن السيبراني الشاملة المعتمدة في عام ٢٠١٥، والتي تتضمن إجراءات محددة تستهدف مساعدة الحكومة لإنشاء بيئة رقمية أكثر أمانًا. وبالإضافة إلى ذلك، تم إنشاء الوكالة الوطنية لتطوير تكنولوجيا المعلومات (NITDA) في عام ٢٠١٥ لتنظيم وتطوير قطاع تكنولوجيا المعلومات في البلاد. ورغم ذلك، تشير التقارير الدولية والإحصاءات إلى أن حجم الجرائم السيبرانية في نيجيريا مازالت في تزايد. ولعل هذا ما

يثير القلق، فوفقاً لتقرير صادر عام ٢٠٢٢، تخسر نيجيريا ما يعادل ٢٠٠ مليار نيرة سنويًا بسبب الجرائم السيبرانية، وإذا استمرت هذه الجرائم دون رادع، فمن المتوقع أن تخسر نيجيريا حوالي ٦ تريليون دولار بحلول عام ٢٠٣٠. وعليه فقد أصبح من الواضح أن الفضاء السيبراني في نيجيريا يشهد الكثير من الممارسات التي تهدد أمنها السيبراني وتسبب ضررًا ماليًا وسياسياً بالغاً للدولة.

وتنقسم الدراسة إلى أربعة أقسام رئيسية، يقدم الأول منها إطاراً مفاهيميا لأبرز المفاهيم ذات الصلة بالأمن السيبراني ومهدداته، وكذا عرضاً لأهم الأدبيات ذات الصلة بموضوع الدراسة. أما القسم الثاني، فيعرض حالة الأمن السيبراني في نيجيريا، بالإشارة إلى أهم المؤشرات العالمية ذات الصلة بالأمن السيبراني والجرائم السيبرانية. ويركز القسم الثالث من الدراسة على أبرز التداعيات الاقتصادية لمهددات الأمن السيبراني في نيجيريا، بينما يتناول القسم الرابع من الدراسة أهم التداعيات السياسية الناجمة عن انتشار التهديدات والجرائم السيبرانية في نيجيريا. وتقدم خاتمة الدراسة عرضا لأبرز النتائج التي تم التوصل إليها من خلال الدراسة.

أولاً: الإطار المفاهيمي والنظري للدراسة:

أ. مفهوم الأمن السيبراني والمفاهيم ذات الصلة:

١. الأمن السيبراني Cybersecurity

اكتسب مفهوم الأمن السيبراني اهتماماً دولياً واسع النطاق في مختلف المجالات البحثية، وذلك لما ينطوي عليه من أهمية ولما قد يسفر عنه اختراقه أو تهديده من آثار كارثية على الأفراد والمجتمعات. ولتوضيح معنى الأمن السيبراني، يمكن تفكيك المصطلح لكلمتي "الأمن" و"السيبراني". فمفهوم "الأمن" يتسم بدرجة عالية من الغموض وعدم التحديد، وقد يتسع أو يضيق نطاقه طبقاً للغرض منه. وبصفة عامة يتعلق الأمن بالعملية المرتبطة بتخفيف أي نوع من التهديدات التي يتعرض لها الأفراد وقيمهم الثمينة. ولهذا السبب يؤكد بوزان أن الأمن يتعلق بالحرية من التهديد وقدرة الدول على الحفاظ على هويتها المستقلة وسلامتها الوظيفية ضد قوى التغيير التي تراها معادية في حين أن هدفها النهائي هو البقاء. ومن خلال ما سبق، يمكن القول أن الأمن يتعلق

(ISSN: 2536 - 9555)

بالشعور بالأمان من الأذى والخوف والقلق والقمع والخطر والفقر، كما يتعلق بحماية القيم الأساسية والدفاع عنها والحفاظ عليها ضد أي تهديد، والتحرر من كافة الأفعال والممارسات التي من شأنها أن تقوض التماسك الداخلي، والوجود المؤسسي للدولة وقدرتها على الحفاظ على مؤسساتها الحيوية لتعزيز قيمها الأساسية وأهدافها الاجتماعية والسياسية والاقتصادية، فضلاً عن تلبية التطلعات المشروعة للشعب[٢]. أما كلمة "سيبراني"، فهي مشتقة من "السيبرناطيقا" Cybernatics، التي تشير إلى علم الاتصالات الذي يتعامل مع دراسة أنظمة التحكم الآلي وكذلك أنظمة الاتصالات الميكانيكية الكهربائية. وبالتالي فإن كلمة "سيبراني" تستخدم لوصف التفاعلات التي تتعلق بأجهزة الكمبيوتر أو الشبكات أو تنطوي عليها[٣].

ولقد تعددت اجتهادات الباحثين في محاولة تعريف "الأمن السيبراني"، واختلفوا في ذلك بين فريق يستخدم المفهوم في نطاق ضيق، ليقتصر على بعض الجوانب التقنية والعملياتية فحسب، وفريق أخر رأى أن الأمن السيبراني يعد من المفاهيم المعقدة متعددة الأبعاد التي ينبغي أن تتسع لتشمل أكثر من مجرد أبعاد فنية. وفي هذا الإطار، يعرف البعض الأمن السيبراني– الذي يطلق عليه أحياناً الأمن الإلكتروني أو أمن المعلومات الإلكتروني– باعتباره "ممارسة الدفاع عن أجهزة الكمبيوتر والأجهزة المحمولة والأنظمة الإلكترونية والشبكات والبيانات من الهجمات الضارة". وهناك من يعرفه بأنه "حماية الأنظمة المتصلة بالإنترنت، بما في ذلك الأجهزة والبرامج والبيانات، من الهجمات الإلكترونية"[٤]. وهناك اتجاه ثالث يرى أن الأمن السيبراني ما هو إلا "تقنيات لحماية

---

(2) Muyiwa B. Afolabi: "concept of security"., in Kunle Ajayi (ed), **Readings in Intelligence and Security Studies**, (Ekiti: Intelligence and Security Studies Programme, 2015), pp. 1- 2.

(3) Umaru Ibrahim: **The Impact of Cybercrime on The Nigerian Economy and Banking System**, available at: https://demo.ndic.gov.ng/wp-content/uploads/2020/08/NDIC-Quarterly-Vol-34-No-12-2019-Article-The-Impact-Of-Cybercrime-On-The-Nigerian-Economy-And-Banking-System.pdf/ accessed on 28/ 07/ 2024.

(4) Margaret Rouse: **Definition of cybersecurity,** available at: https://searchsecurity.techtarget.com/definition/cybersecurity/ accessed on 17/ 08/ 2024.

أجهزة الكمبيوتر والشبكات والبرامج والبيانات من الوصول غير المصرح به أو الهجمات التي تهدف إلى الاستغلال"[٥]. وفي تعريف آخر، يشار إلى الأمن السيبراني بأنه "أمن الشبكات وأنظمة الترابط، مثل الأجهزة والبرامج والبيانات، ضد التهديدات الإلكترونية لتقليل تأثير المهاجمين المحتملين في تعطيل العمليات العادية" وبهذا المعنى فإن الأمن السيبراني يمكن أن يمارسه كل من المنظمات والأفراد[٦]. وهنا يلاحظ أن هذه التعريفات سالفة الذكر تتبنى منظورًا اجتماعيًا تقنيًا محدودًا للأمن السيبراني.

وفى محاولة للتوصل إلى تعريف أكثر دقة وشمولاً لمفهوم الأمن السيبراني، يمكن الاعتماد على التعريف الذي تبناه خبراء الاتحاد الدولي للاتصالات، ووفقاً لهذا الاتجاه من الباحثين والمتخصصين، يعرف الأمن السيبراني باعتباره:

"مجموعة من الأدوات والسياسات والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات والتطمينات والتقنيات التي يمكن استخدامها لحماية البيئة والتنظيم السيبراني، وكذلك أصول الشركات والمستخدمين"[٧].

بهذا المعنى، يتسع المفهوم ليتضمن عدة عناصر من بينها الموارد والإجراءات ومبادئ الأمن وبروتوكولات السلامة واللوائح واستراتيجيات إدارة المخاطر والأنشطة والتدريب وأفضل الممارسات والامتثال والتكنولوجيا. وتتكون "الأصول" المعنية من أجهزة الحوسبة المتصلة والموظفين والمعدات والبرامج والمرافق وشبكات الاتصالات وجميع

---

(5) The Economic Times: **Definition of" cyber security",** available at: https://economictimes.indiatimes.com/definition/cyber-security/ accessed on 1/ 07/ 2024.

(6) Yakubu Ajiji Makeri: "Cyber Security Issues in Nigeria and Challenges"., in **International Journal of Advanced Research in Computer Science and Software Engineering**, (New Delhi: Advanced Research International Publcation House, volume 7, issue 4, April 2017), pp. 316- 317.

(7) ITU High Level Experts Group: **ITU Global Cyber-Security Agenda (GCA) High Level Experts Group [HLEG]** (Geneva: Global Strategic Report, 2008), p. 27.

لمزيد حول هذا المفهوم أنظر:

U. J. Orji: **Cybersecurity Law and Regulation**, (Nijmegen: Wolf Legal Publishers, 2012), pp. 10–16

(ISSN: 2536 - 9555)

البيانات المتبادلة والمعالجة في البيئة السيبرانية[٨]. بعبارة أخرى، ينطوي الأمن السيبراني على جمع وتنسيق الموارد المختلفة، مثل الموظفين والبنية الأساسية، وإنشاء الهياكل والعمليات لتأمين الشبكات وأنظمة الكمبيوتر التي تعمل عبر الإنترنت ضد التهديدات التي قد تعرض سلامتها للخطر وتنتهك حقوق الملكية، الأمر الذي يؤدي إلى حدوث خسائر بدرجات متفاوتة[٩].

وبالنظر إلى هذا التعريف السالف بيانه، يلاحظ أنه يعكس الطبيعة المعقد للأمن السيبراني، كما أنه يعترف بالتفاعلات الاجتماعية والتقنية بين البشر والأنظمة وكذلك التفاعلات بين الشبكات، وينظر في استراتيجيات حماية الأنظمة من مجموعة واسعة من التهديدات. وعليه فإن القائمين على صنع سياسات الأمن السيبراني يجب أن يكونوا قادرين على تحديد التهديدات الأمنية وكذا تحديد الأهداف أو الأطراف المعرضة للتهديد ومستوى الأمن المطلوب بدرجة عالية من التحديد.

وبهذا المعنى، فإن تدابير وعمليات إدارة الأمن السيبراني لابد أن تشمل الجوانب الفنية والتنظيمية والسياسية والقانونية. وتتناول الجوانب الفنية لإدارة الأمن السيبراني تطوير وتنفيذ تدابير الحماية التقنية لأنظمة الكمبيوتر والبنية التحتية للشبكات، في حين تتناول الجوانب التنظيمية تطوير القدرات المؤسسية لتعزيز الأمن السيبراني، مثل إنشاء منظمات إنفاذ القانون، وكذلك تطوير القدرات المؤسسية بما في ذلك إنشاء فرق الاستجابة لحالات الطوارئ الحاسوبية (CERTs) لتقديم الخدمات الحيوية مثل الوقاية والإنذار المبكر، واكتشاف وإدارة حوادث الأمن السيبراني. أما الجوانب السياسية والقانونية لإدارة الأمن السيبراني، فهى تتناول السياسات والتدابير القانونية التي تهدف إلى تعزيز الأمن السيبراني. وعادة ما تعتبر التدابير القانونية أكثر الجوانب ارتباطاً بالتحكم في الجرائم الإلكترونية، حيث تشمل هذه التدابير وضع قوانين تحظر الأعمال

(8) Pallavi Murghai Goel: "A Literature Review of Cyber Security"., in **International Journal of Research and Analytical Reviews**, (Gujarat: Atman Publishing Academy, Vol. 6, Issue 2, April 2019), p. 136.

(9) Francisco Schiliro: **Towards a Contemporary Definition of Cybersecurity**, 2022, available at: https://doi.org/10.48550/arXiv.2302.02274/ accessed on 1/ 08/ 2024.

التي تنتهك أمن أو سلامة أو إتاحة بيانات الكمبيوتر أو الأنظمة أو الشبكات والهجمات ضد البنية التحتية الحيوية للمعلومات، كما تشمل أيضا كافة التدابير القانونية ذات الصلة بتسهيل التعاون عبر الحدود في مجال الأمن السيبراني، بما في ذلك منع الأفعال المحظورة والتحقيق فيها وملاحقتها[١٠].

٢. الفضاء السيبراني cyber space

يشير الفضاء السيبراني إلى مجال تفاعلي يتكون من شبكات رقمية تستخدم لتخزين المعلومات وتعديلها وتوصيلها، ويشمل الإنترنت بالإضافة إلى أنظمة المعلومات الأخرى. بعبارة أخرى، يمكن تعريف الفضاء السيبراني باعتباره مجال عالمي داخل البيئة المعلوماتية، يتكون من شبكة مستقلة من البنى التحتية لأنظمة المعلومات، ويتضمن ذلك الإنترنت وشبكات الاتصالات وأنظمة الحاسب والمعالجات المدمجة. وعادة ما يستخدم الفضاء السيبراني للدفاع أو الهجوم على المعلومات وشبكات الحاسب الآلي لحرمان العدو من تنفيذ ذات الأهداف[١١].

ب. مهددات الأمن السيبراني:

١. الجرائم السيبرانية cybercrime

يرتبط مفهوم الأمن السيبراني بمفهوم "الجرائم السيبرانية" Cybercrime، التي اتسع نطاقها خلال العقد الماضي بشكل يسترعى الانتباه، وكثيراً ما يطلق عليها أيضا مصطلح "جرائم الإنترنت". وبصفة عامة، تشير "الجريمة" إلى الأفعال أو التقاعس عن العمل بسبب الإهمال الذي يضر بالصالح العام أو الأخلاق، وهو أمر محظور قانونًا. وتعتبر الجريمة السيبرانية ظاهرة عالمية تحدث في الفضاء السيبراني أي في عالم أجهزة الكمبيوتر وعلى الإنترنت. وتتضمن الجريمة السيبرانية استخدام تطبيقات متخصصة في

(10) Uchenna Jerome Orji: "The African Union Convention on Cybersecurity: A Regional Response towards Cyber Stability?"., **Masaryk University Journal of Law and Technology,** (Brno: Institute of Law and Technology, vol. 12, no. 2, Fall 2018), pp. 92- 93

(11) Moses Owiny: **The politics of Cyber Security policy making in Africa: The Case Study of Uganda**, available at: https://thecfma.org/wp-content/uploads/2019/10/Securitization-and-the-logic-of-Cyber-Security-policy-making-in-Africa.pdf/ accessed on 26/ 08/ 2024.

(ISSN: 2536 - 9555)

أجهزة الكمبيوتر مع الإنترنت من قبل أفراد مهرة تقنيًا لارتكاب جريمة. وقد تهدد عواقب مثل هذه الجرائم بنية الأمن والصحة المالية للدولة. ولذا، يمكن تفسير الجريمة السيبرانية ببساطة على أنها الأفعال الإجرامية التي يتم ارتكابها أو تسهيلها بمساعدة نظام كمبيوتر ومن خلال استخدام الإنترنت(١٢).

وبهذا المعنى، تنطوي الجرائم السيبرانية على أنشطة غير مشروعة تتم بواسطة بعض الجهات الفاعلة أو المجموعات التي تستهدف اختراق الأنظمة الإلكترونية للدول والشركات والأنظمة العامة والخاصة لتحقيق مكاسب مالية أو للتسبب في حدوث خلل. ولقد وصفت الأمم المتحدة هذه الجرائم السيبرانية بأنها تلك التي تنطوي على سلوك غير قانوني يستهدف أمن أنظمة الكمبيوتر والبيانات التي تتم معالجتها. وتأخذ مثل هذه الجرائم أو الهجمات أشكالا مختلفة تشمل: حقن البرامج الضارة، مثل الفيروسات أو برامج التجسس في الفضاء السيبراني بقصد التخريب؛ أو التصيد الاحتيالي، وهو طلب للبيانات من مصدر شبه موثوق بهدف خداع المستخدمين لتقديم معلومات حساسة، أو النقر فوق رابط ضار؛ أو القرصنة، والتي تنطوي على معرفة كلمة مرور سرية خاصة بالنظام الأساسي وذلك للوصول إلى النظام(١٣).

وهنا تجدر الإشارة إلى أن الهجمات سالفة الذكر تحدث من خلال تبادل المعلومات دون اتصال جسدي بين المهاجم والضحية. وفي بعض الحالات، يمكن أن تؤدي الاتصالات عبر الإنترنت إلى ضرر مادي فعلي، وذلك عندما تستهدف هذه الهجمات أنظمة الدولة أو المؤسسات، حيث تنطوي على إمكانية إلحاق الضرر بالمجتمع بطرق جديدة وحاسمة، كما يمكن لهذا النوع من الهجمات، على سبيل المثال، إفساد الأنظمة الانتخابية أو عرقلة القطارات الآلية أو إسقاط الشبكات الكهربائية أو التسبب فى انهيار أنظمة التحكم في حركة المرور أو تفجير مصافي النفط أو التسبب فى خروج الطائرات

(12) Susan W. Brenner: "Cybercrime, Cyberterrorism and Cyberwarfare"., in **International Review of Penal Law** (Indiana: Marchal et Billard, Vol. 77, no. 3, 2006), pp. 454- 455.

(13) **Ibid,** pp. 456- 457.

عن السيطرة. وتعتبر الدول النامية من أكثر الدول تعرضاً لهذه الهجمات، خاصة فى ظل افتقارها إلى التكنولوجيا والمهارات اللازمة لدرء مثل هذه الهجمات(١٤).

٢. الإرهاب السيبراني cyber Terrorism

يشير الإرهاب السيبراني إلى "عمل هادف، تحركه بواعث وأهداف شخصية أو سياسية، يهدف إلى تعكير صفو أو تدمير استقرار المصالح التنظيمية أو الوطنية، من خلال استخدام الأجهزة الإلكترونية التي تستهدف أنظمة المعلومات أو برامج الكمبيوتر أو غيرها من الوسائل الإلكترونية للاتصال والنقل والتخزين". وعليه، ينطوي الإرهاب السيبراني على استخدام الفضاء السيبراني لإحداث هجمات إرهابية (لأغراض الإرهاب)(١٥). وبالتالي، فإن الإرهاب السيبراني يلخص استخدام تقنيات الكمبيوتر والشبكات للترويج للميول المتطرفة أو العدوانية، والتي عادة ما تكون ذات دوافع سياسية أو دينية أو اجتماعية والتي تترك أثراً قوياً أو حتى وحشياً. "يمكن أن يتسبب تفجير قنبلة في إحداث تأثير هائل ولكن صنعها وتسليمها يكلف الكثير. يمكن أن يكون تنفيذ هجوم إرهابي سيبراني مدمراً بنفس القدر (أو أكثر من ذلك) ولكنه لا يكلف شيئًا جزئيًا لتنفيذه"(١٦).

٣. الحروب السيبرانية Cyberwarfare

تقوم الحرب السيبرانية على استخدام الدول القومية للفضاء السيبراني لتحقيق نفس الغايات العامة التي تسعى إليها من خلال استخدام القوة العسكرية التقليدية، أي لتحقيق مزايا معينة على دولة قومية منافسة أو لمنع دولة قومية منافسة من تحقيق مزايا أكثر منها. وجدير بالذكر أن السمة المميزة للحرب هي أنها صراع بين الدول القومية، ولذا فهي نشاط بشري، يقوم به أفراد، لكن هؤلاء الأفراد يتصرفون لصالح دولة قومية معينة.

(14) Ken Obura: **Cyberspace is the latest conflict frontier in Afrika,** 22nd June 2018, available at: https://www.iafrikan.com/2018/06/22/is-cyberspace-the-latest-conflict-frontier-on-the-african-continent/ Accessed on: 26/ 08/ 2024.

(15) N. Veerasamy: "A High-level Conceptual Framework of Cyber-terrorism", **Journal of Information Warfare**, (Virginia: Peregrine Technical Solutions LLC, Vol. 8, No. 1, 2009), pp. 43- 44.

(16) Andrew M. Colarik: **Cyber Terrorism: Political and Economic Implications**, (Pennsylvania: Idea Group Pub., 2006), p. X.

(ISSN: 2536 - 9555)

وبهذا المعنى فإن الحرب السيبرانية صراع قائم على الإنترنت ينطوي على اختراق أنظمة الكمبيوتر وشبكات الدول الأخرى. يمتلك هؤلاء المهاجمون الموارد والخبرات اللازمة لشن هجمات هائلة على الإنترنت ضد دول أخرى لإحداث ضرر أو تعطيل الخدمات. وفي هذا الإطار، يمكن لدولة أن تغزو البنية التحتية للدولة الأخرى باستمرار، وتسرق أسرار الدفاع، فضلاً عن جمع المعلومات حول التكنولوجيا لتضييق الفجوات في صناعاتها العسكرية. وتتضمن الحروب السيبرانية عمليات التجسس الصناعي والعسكري، وهي عمليات من الخطورة بمكان، حيث يمكن للبيانات الحساسة المخترقة أن تعطي المهاجمين القدرة على ابتزاز الأفراد داخل الحكومة. وقد تسمح المعلومات للمهاجم بالتظاهر بأنه مستخدم مصرح له بالوصول إلى معلومات أو معدات حساسة. وهناك تقارير تفيد بأن جمهورية الصين الشعبية ("PRC") تشن حروبا سيبرانية تهدف إلى شل البنية التحتية لتايوان و"شل" حكومة واقتصاد الدولة، حيث تستهدف شبكات المرافق العامة والاتصالات والنقل و"الأمن التشغيلي" في تايوان. وهنا تجدر الإشارة إلى أنه إذا لم تستطع الحكومة الدفاع عن نفسها ضد الهجمات السيبرانية، فقد يفقد المواطنون الثقة في قدرة الحكومة على حمايتهم(١٧).

ج. الدراسات السابقة:

تناولت العديد من الأدبيات التداعيات الاقتصادية والسياسية للهجمات السيبرانية وخاصة في ظل التطورات التكنولوجية المتعاقبة، والتي أججت من مخاطر هذه الهجمات وأدت إلى اتساع نطاق تأثيراتها. فعلى سبيل المثال، أشارت دراسة (Schia and Gjesvik, 2018) إلى أن للأمن السيبراني العديد من التأثيرات الاقتصادية والاجتماعية حيث يمكن للتقنيات الرقمية تعزيز الحرية وتوفير مساحات للتعبير عن الرأي والفكر، كما أن له دور هام في تعزيز التنمية الاقتصادية والمجتمعية. إلا أن الدراسة أكدت على أن تعزيز الأمن السيبراني على المستوى الدولي لا يكون قوياً إلا بقدر أضعف حلقاته، لذلك أكدت الورقة على ضرورة بناء آلية للتعاون الدولي تهدف إلى

(17) Susan W. Brenner: **op.cit.**, pp. 465- 467.

تحسين آليات الأمن السيبراني في الدول النامية[١٨]. أما دراسة (Kelley, 2022) والتي هدفت إلى تحليل تطور عدد وطبيعة الجرائم السيبرانية حول العالم وكيفية مواجهتها، فقد أكدت على دور التدريب والتعليم للأفراد والمؤسسات في الحد من هذه الهجمات واحتواء تأثيراتها وتقليل خسائرها الاقتصادية[١٩]. كذلك فقد أشارت دراسة (Yadav & Gour, 2014) إلى أن التهديدات والجرائم السيبرانية أصبحت شاغل عالمي يؤثر على الاقتصادات النامية والمتقدمة، وأن التكلفة الاقتصادية للتهديدات السيبرانية إذا لم يتم مواجهتها قد ترتفع بصورة مطردة مع التقدم التكنولوجي السريع وتوسيع تطبيقاته في القطاعات الاقتصادية المختلفة[٢٠]. ولعل هذا ما ذهبت إليه دراسة (Hua & Bapna, 2012)، حيث أكدت على الآثار أو التداعيات الاقتصادية السلبية للتهيدات السيبرانية، الأمر الذي يستوجب ضرورة توجيه حجم أكبر من الاستثمارات إلى مجالات حماية البيانات[٢١].

أما الدراسات التي تناولت الجرائم السيبرانية والأمن السيبراني في نيجيريا، فمنها على سبيل المثال دراسة (Saidu, etal., 2021) والتي تناولت تحليل تحديات وآفاق الأمن السيبراني في نيجيريا وذلك للفترة (٢٠٠٩-٢٠١٩) وذلك من خلال تحليل البيانات من مصادر أولية (الاستبانات) ومصادر ثانوية (التقارير الدولية والمحلية). وقد خلصت

(18) Lars Gjesvik and Niels Nagelhus Schia: **Managing a Digital Revolution-Cybersecurity Capacity Building in Myanmar**, 2018, at:https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2563201/Managing%2ba%2bdigital%2brevolution.pdf?sequence=1&isAllowed=y

(19) Patrick Kelley: **Evolution of Cyber Attacks and Their Economic Impacts**, 2022, at:https://doi.org/10.36227/techrxiv.21670718.v1

(20) Hetram yadav and Shashant Gour: "Cyber Attacks: An Impact on Economy to an Organization", **International Journal of Information & Computation Technology,** Vol 4, No. 9, at: https://www.ripublication.com/irph/ijict_spl/ijictv4n9spl_11.pdf

(21) Jian Huaa and Sanjay Bapna: "The Economic Impact of Cyber Terrorism", **Journal of Strategic Information Systems**, at: https://www.researchgate.net/publication/261860155_The_economic_impact_of_cyber_terrorism

(ISSN: 2536 - 9555)

الدراسة إلى مجموعة من الاستنتاجات من أهمها: زيادة حجم تهديدات الأمن السيبراني في نيجيريا خلال فترة الدراسة والحاجة إلى الاستثمار المستمر في البحث والبنى التحتية التقنية والتي يمكن من خلال تعزيزها الحد من مخاطر التهديدات السيرانية[٢٢].

وقد ركزت دراسة (Idowu, Oluwafemi Amos, 2021) على تحديات السيطرة على الجرائم الإلكترونية في نيجيريا، واعتمدت هذه الدراسة على عدد من الاستبيانات الموجهة للفئات المختلفة في نيجيريا، واستخلصت الدراسة مجوعة من النتائج من أهمها وجود علاقة معنوية بين معدل الجرائم الإلكترونية والبطالة والفساد. وكذلك فقد أكدت الدراسة على ضرورة تعزيز الإطار القانوني والتشريعي لمواجهة مثل هذه الجرائم وضرورة إشراك القطاع الخاص في سياسات الحد منها[٢٣].

وعن التكلفة الاقتصادية للجرائم السيبرانية، أشارت دراسة (Sesan, etal, 2023) باستخدام تحليل الاستبيانات، إلى أن هذه التكاليف لا تقتصر فقط على التكاليف غير الملموسة مثل غياب الفرص الاقتصادية أو التأثير على حجم الاستثمار أو خسائر الأموال، وإنما تتعدى ذلك إلى التأثير على مسار رقمنة الاقتصاد النيجيري مع انخفاض الثقة في الآليات الرقمية في التعامل نتيجة تزايد التهيدات السيبرانية خاصة الآليات المترتبطة بالقطاعات المالية والمصرفية مثل التحويلات الإلكترونية أو النقود الرقمية وغيرها[٢٤]. وهو نفس ما ذهبت إليه دراسة (Jackson & Ene, 2016)، فقد اشارت إلى أن التطورات التكنولوجية وانتشار استخدام الإنترنت في نيجيريا أدى إلى زيادة معدلات الجرائم السيبرانية بصورة كبيرة لتصبح نيجيريا واحدة من أهم الدول التي تشكل مصدراً لهذه الجرائم مما يشكل صورة ذهنية سيئة عن الدولة ويؤثر على الاستثمارات

(22) I. R. Saidu, etal.: The Challenges of Security Threats in Nigeria Cyberspace, **FUDMA Journal of Sciences**, vol.5, No.1, March 2021. At: https://doi.org/10.33003/fjs-2021-0501-554

(23) Idow, Oluwafemi Amos, "Cybercrimes and Challenges of Cyber-Security in Nigeria", **International Journal of Sociology and Development**, Vol. 3, No.1, at: https://www.academia.edu/50170416/Cybercrimes_and_Challenges_of_Cyber_Security_in_Nigeria

(24) Gbenga Sesan, etal,: **Economic Cost of Cybercrime in Nigeria**, University of Toron, 2023, at: http://www.opennetafrica.org/?wpfb_dl=7

الأجنبية ويقلل الثقة في الاقتصاد الرقمي. ولعل هذا ما يتطلب وضع أطر قانونية أكثر صرامة في مواجهة هذا النوع من الجرائم، كما يتطلب توفير فرص العمل للشباب وزيادة حملات التوعية بالتهديدات السيبرانية ومخاطرها وتداعياتها[٢٥].

ثانياً: حالة الأمن السيبراني في نيجيريا:

شهدت القارة الإفريقية في السنوات الأخيرة تنامياً في معدلات التهديدات والهجمات السيبرانية، خاصة التي تستهدف البنية التحتية الحيوية في دولها، حيث مثل القطاع المصرفي هدفاً رئيسياً للنسبة الأكبر من هذه الهجمات. وكذلك فقد شهدت إفريقيا في عام ٢٠٢٣ موجة حادة من الهجمات السيبرانية منها على سبيل المثال الهجمة ضد أنظمة الاتحاد الإفريقي وأنظمة بيانات الحكومة الكينية والبنية التحتية للانتخابات النيجيرية.

ولقد دفعت هذه الوتيرة المتزايدة في التهديدات السيبرانية مجلس السلم والأمن التابع للاتحاد الإفريقي إلى وضع قضية الأمن السيبراني على قمة أولوياته في قمة الاتحاد الافريقي لعام ٢٠٢٣. وفي هذا الاجتماع تم توجيه مفوضية الاتحاد الأفريقي للإسراع في وضع استراتيجية قارية للأمن السيبراني، كما تم اعتماد سياسة قارية لحماية الأطفال على شبكة الإنترنت، وتم الاتفاق على موقف إفريقي مشترك بشأن تطبيق القانون الدولي في الفضاء الإلكتروني[٢٦].

ولم تكن نيجيريا بأي حال من الأحوال بمنأى عن ذلك، فعلى سبيل المثال تعرضت قاعدة بيانات **Directorate of Secret Services (DSS)** في عام ٢٠١٢ إلى هجوم من قبل جماعة بوكو حرام رداً على محاولات الحكومة الفيدرالية النيجيرية

---

(25) T.C.B Jackson & Robert W. Ene: "Cybercrime and the Challenges of Socio-Economic Development in Nigeria, **Journal of Researches in National Development,** Vol12, No.2, at: https://www.researchgate.net/publication/313361300_CYBERCRIME_AND_THE_CHALLENGES_OF_SOCIO-ECONOMIC_DEVELOPMENT_IN_NIGERIA

(٢٦) **تحديات الأمن السيبراني في إفريقيا: بناء جسور التكنولوجيا وتحقيق الاستدامة الرقمية**، فبراير ٢٠٢٤، في: https://gate.ahram.org.eg/News/4731124.aspx

(ISSN: 2536 - 9555)

لمواجهتهم. كذلك كان هناك محاولة لاختراق اللجنة الوطنية المستقلة للانتخابات (INEC) أثناء انتخابات عام ٢٠١٥[٢٧].

ويمكن تحليل وضع الأمن السيبراني في نيجيريا بصورة أكثر وضوحاً من خلال المؤشرات الدولية للأمن السيبراني وهي: المؤشر العالمي للأمن السيبراني **(GCI) Global Cybersecurity Index**، ومؤشر الجرائم السيبرانية العالمي **World Cybercrime Index**.

أ. مؤشر الأمن السيبراني:

تم وضع هذا المؤشر من قبل الاتحاد الدولي للاتصالات International Telecommunication Unit (ITU)، وهو منظمة دولية تختص بقضايا تكنولوجيا المعلومات والاتصالات. ويتم في هذا المؤشر تقييم الإطار العام للأمن السيبراني في الدولة من خلال خمسة أبعاد أساسية تقيم مدى جاهزية الدولة للتعامل مع قضية الأمن السيبراني، تشمل الجوانب القانونية والتكنولوجية والتشريعية والقدرات البشرية والمؤسسية في الدولة والتعاون بين القطاعين العام والخاص في تحقيق الأمن السيبراني. وتتراوح قيمة المؤشر بين الصفر والمائة، إذ يشير الرقم ١٠٠ إلى أن الدولة آمنة سيبرانياً[٢٨]. ويتم تقسيم الدول وفقاً لقيمة المؤشر إلى خمسة فئات (Tiers) على النحو التالي:

---

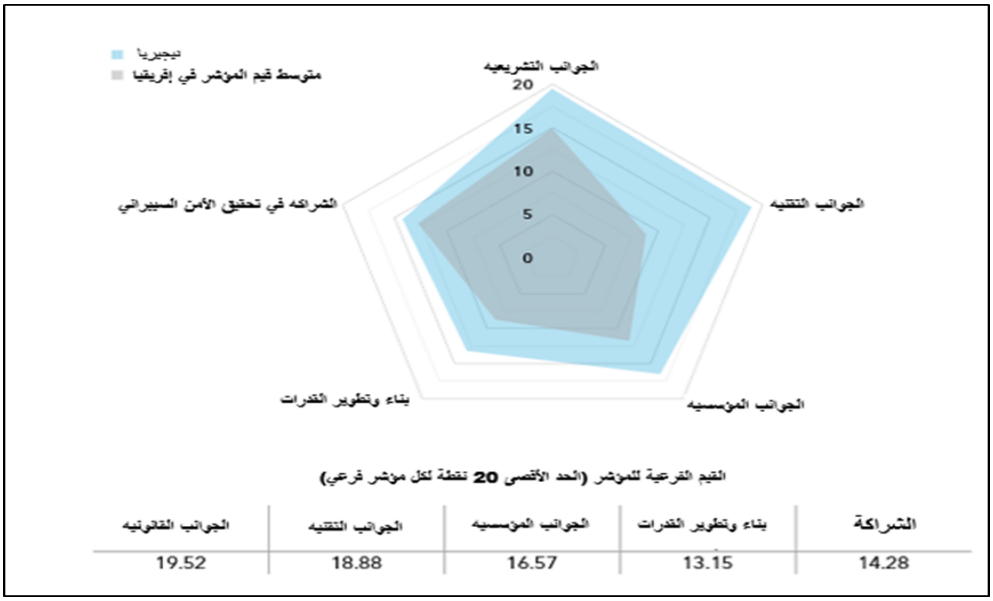
[٢٧] فاروق أبوضيف: التهديدات السيبرانية التي تواجه القارة الإفريقية، **قراءات إفريقية**، يوليو ٢٠٢٤، في:
https://qiraatafrican.com/21857/%D8%A7%D9%84%D8%AA%D9%87%D8%AF%D9%8A%D8%AF%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D8%A7%D9%84%D8%AA%D9%8A-%D8%AA%D9%88%D8%A7%D8%AC%D9%87-%D8%A7%D9%84%D9%82%D8%A7/

[٢٨] لمزيد من التفاصيل عن منهجية المؤشر يمكن الاطلاع على:
برنامج الأمن السيبراني: **الاصدار الخامس للرقم القياسي العالمي للأمن السيبراني: نموذج مرجعي (المنهجية)**، ٢٠٢٤، في:
https://web.archive.org/web/20240118014737/https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/513560_2A.pdf

قيمة المؤشر	الفئة
٠-٢٠	في مرحلة البناء Building
٢٠-٥٥	في طور التقدم في مجال الأمن السيبراني Evolving
٥٥-٨٥	أنشأت نظام للأمن السيبراني Establishing
٨٥-٩٥	متقدمة في مجال الأمن السيبراني Advancing
٩٥-١٠٠	آمنة سيبرانياً Role-modelling

ومن بين ١٩٤ دولة شملها المؤشر، لا يقع في الفئة الأولى (٩٥-١٠٠) إلا ٤٦ دولة فقط، بينما تقع ١٠٥ دولة ما بين الفئتين الثانية والثالثة. وتصنف نيجيريا من ضمن دول الفئة الثالثة. وبالنظر إلى المكونات الفرعية للمؤشر في نيجيريا (شكل رقم ١) يتبين أن الأبعاد أو الجوانب التقنية والمؤسسية هي التي تحتاج إلى مزيد من التحسين في نيجيريا، إلا أنها وبالرغم من ذلك فإن مستوى الأمن السيبراني لديها أعلى من المتوسط الإفريقي في كل أبعاد المؤشر.

شكل رقم (١) مؤشر الأمن السيبراني العالمي في نيجيريا ٢٠٢٤م



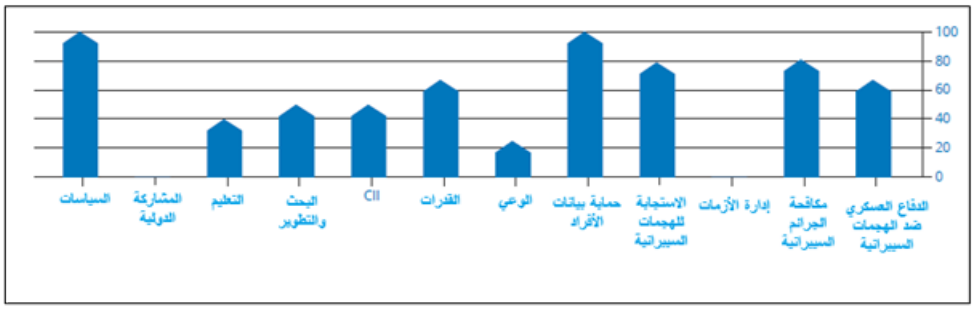
Source: ITU: **Global Cybersecurity Index 2024**, at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

(ISSN: 2536 - 9555)

وفي نفس السياق، هناك أيضاً **مؤشر الأمن السيبراني الوطني** National Cybersecurity Index (NCI) الذي تصدره e-Governance Academy Foundation (eGA)، والذي يقيم جاهزية الدول في منع التهديدات أو تدبير الحوادث السيبرانية، وذلك من خلال تقييم نسب استيفاء المعايير المختلفة أو المتطلبات المختلفة للقدرات المحلية المتعلقة بالأمن السيبراني سواء القدرات المؤسسية، أو السياسية، أو العسكرية، أو قضايا الوعي أو غيرها من الجوانب المرتبطة بالأمن السيبراني، والتي يتم بشكل عام تصنيفها تحت ثلاث مجموعات رئيسية هي: الاستجابة لمخاطر التهديد السيبرانيResponsive Cybersecurity Indicators، المنع أو الحد من التهديدات Preventive Cybersecurity Indicators، واستراتيجيات التعامل مع قضية الأمن السيبرانيStrategic Cybersecurity Indicators[٢٩].

ويأتي ترتيب نيجيريا في هذا المؤشر (٣٠) وقد استطاعات نيجيريا استيفاء نسب معتبرة في عدد من المؤشرات الفرعية لهذا المؤشر، منها على سبيل المثال تقييم استجابة الحكومة لمخاطر الأمن السيبراني ووجود استراتيجية وطنية مختصة بالأمن السيبراني وإطار قانوني لمكافحته، بينما كانت القيم منخفضة في مؤشرات مثل الوعي بقضايا الأمن السيبرانية والمشاركة في الجهود الدولية وكفاءة إدارة الأزمات المتعلقة بتهديدات الأمن السيبراني، والتعليم وتنمية القدرات، وذلك كما يتبين من الشكل رقم (٢).

شكل رقم (٢): أبعاد مؤشر الأمن السيبراني الوطني في نيجيريا لعام ٢٠٢٤



Source: NCSI: **National Cybersecurity Index: Nigeria**, at: https://ncsi.ega.ee/country/ng/

(29) NCSI: **National Cybersecurity Index: Methodology,** at: https://ncsi.ega.ee/methodology/

ب. مؤشر الجرائم السيبرانية:

يستخدم هذا المؤشر في تحديد بؤر الجرائم السيبرانية حول العالم من خلال ترتيب الدول وفقاً لعدد الجرائم السيبرانية التي حدثت داخلها سواء كان مصدرها من الداخل أو الخارج. وقد صدرت النسخة الأولى لهذا المؤشر في إبريل عام ٢٠٢٤ في مقال بعنوان: "Mapping the Global Geography of Cybercrime with the World Cybercrime Index". ويعتمد المؤشر على قياس تأثير أو مخاطر خمسة أنواع رئيسية من الجرائم السيبرانية وهي: الاحتيال في تقديم الخدمات أو المنتجات الإلكترونية؛ الابتزاز؛ سرقة البيانات أو الهوية؛ عمليات الاحتيال؛ سرقة وغسيل الأموال. ويتم بعدها تحديد الدول التي تعتبر مصدراً لكل نوع من أنواع الجرائم ومدى تأثير هذه الجرائم أو التهديدات(٣٠).

وفي هذا المؤشر جاءت نيجيريا في المرتبة الخامسة من ضمن أكثر عشر دول من حيث الجرائم السيبرانية، تلك الدول التي تعد مصدراً للجرائم السيبرانية على مستوى العالم، وكانت قيمة المؤشر ٢١.٨. ومن الجدير بالذكر أنه وبالرغم من المهارات التقنية المنخفضة لهذه الهجمات مقارنة بالدول الأخرى، إلا أن تأثيرها كان مماثلاً للهجمات القادمة من دول مثل روسيا أو الصين أو الولايات المتحدة الأمريكية، والتي تسبقها مباشرة في الترتيب، وذلك كما يتبين من الجدول رقم (١).

(٣٠) لمزيد من التفاصيل عن منهجية المؤشر انظر:

Bruce M, Lusthaus J, Kashyap R, Phair N, Varese F, **Mapping the global geography of cybercrime with the World Cybercrime Index,** April 2024, at:
https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0297312#sec003

(ISSN: 2536 - 9555)

جدول رقم (١)

مؤشر الجرائم السيبرانية في أعلى ١٠ دول لعام ٢٠٢٤

الترتيب	الدولة	تقييم التأثير	المهارات الاحترافية	المهارات التقنية	مؤشر الجرائم الإليكترونية
١	روسيا	٨.٩٦	٨.٨١	٨.٧٣	٥٨.٣٩
٢	أوكرانيا	٨.٣٧	٨.٢٩	٨.٢٤	٣٦.٤٤
٣	الصين	٨.٢٢	٨.٢٢	٧.٧٠	٧.٨١
٤	الولايات المتحدة الأمريكية	٧.٩٩	٧.٢١	٧.٢١	٢٥.٠١
٥	نيجيريا	٨.٢٥	٦.٤٩	٥.٨٠	٢١.٢٨
٦	رومانيا	٧.١٢	٧.٠٤	٧.١٥	١٤.٨٣
٧	كوريا الشمالية	٧.٩١	٧.٢٣	٧.٣٨	١٠.٦١
٨	المملكة المتحدة	٧.٨٦	٧.٢١	٦.٧٥	٩.٠١
٩	البرازيل	٦.٩٠	٦.٣٥	٦.٣٢	٨.٩٣
١٠	الهند	٧.٩٠	٦.٦٠	٦.٦٥	٦.١٣

Source: Bruce M, Lusthaus J, Kashyap R, Phair N, Varese F, **Mapping the global geography of cybercrime with the World Cybercrime Index,** April 2024, at: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0297312#sec003

وعلى المستوى التشريعي والمؤسسي، أصدرت نيجيريا في عام ٢٠٠٣ "مبادرة الأمن السيبراني الوطنية" National Cybersecurity Initiative والتي كان هدفها الأساسي صياغة إطار تشريعي ومؤسسي لتحقيق الأمن السيبراني وحماية البنى التحتية والمعلوماتية في نيجيريا. وفي إطار هذه المبادرة تم إنشاء مجموعة عمل لمكافحة الجرائم السيبرانية في عام ٢٠٠٤ والتي كان من أهم مخرجاتها إعداد مسودة قانون أمان الحاسبات والبنية التحتية الحرجة للمعلومات Computer Security and Critical Information Infrastructure Bill والذي يعد أول تشريع قانوني في مجال الأمن السيبراني في نيجيريا. وقد أعقب ذلك مجموعة أخرى من الإجراءات التشريعية

والمؤسسية، منها: إنشاء هيئة الأمن السيبراني وحماية البيانات عام ٢٠٠٨، ومسودة قانون مكافحة الاحتيال الإلكتروني في عام ٢٠٠٨. كما تم إصدار قانون الأمن السيبراني في عام ٢٠١١ –والذي دخل حيز التنفيذ في عام ٢٠١٥. وفي عام ٢٠١٤، أصدرت الحكومة النيجيرية وثيقة سياسات الأمن السيبراني والاستراتيجية القومية للأمن السيبراني National Cybersecurity Policy and Strategy (NCPS) والتي تم إصدار نسختها الثانية في عام ٢٠٢١[٣١].

ثالثاً: التداعيات الاقتصادية لمهددات الأمن السيبراني في نيجيريا:

للتهديدات السيبرانية العديد من التداعيات الاقتصادية التي لا تقتصر فقط على التكلفة الاقتصادية التي تواجهها القطاعات الاقتصادية المختلفة وإنما تمتد إلى رفع تكلفة الانتاج في هذه القطاعات لتصبح أكثر قدرة على مواجهة مثل هذه التهديدات كإجراءات احترازية. هذا بجانب الخسائر المالية المباشرة لهذه التهديدات والجرائم (سرقة أموال أو مقابل ابتزاز أفراد ومؤسسات). هذا بالطبع بالإضافة إلى التكلفة غير المباشرة والتي قد يتحملها الاقتصاد القومي والتي تتمثل في انخفاض حجم الاستثمارات وانخفاض القدرة التنافسية و التأثير على معدلات النمو الاقتصادي، هذا بجانب التأثير على تخصيص الموارد حين تقوم الحكومات بتوجيه قدر أكبر من مواردها إلى البنى التحتية التكنولوجية اللازمة لمواجهة هذه التهديدات. وفي هذا السياق أشار تقرير إليانز لمخاطر الأعمال لعام ٢٠٢٤ Allianz Risk Barometer أن التهديدات السيبرانية تشكل الخطر الأكبر للأعمال في عام ٢٠٢٤ بحيث سبقت حتى المخاطر الاقتصادية العالمية الأخيرة مثل اضطرابات سلاسل الإمداد أو حتى الكوارث الطبيعية[٣٢].

وعلى الرغم من صعوبة تقدير التكلفة الاقتصادية الإجمالية للتهديدات والهجمات السيبرانية على المستوى الكلي، إلا أن بعض التقديرات تشير إلى أن هذه التكلفة عالمياً

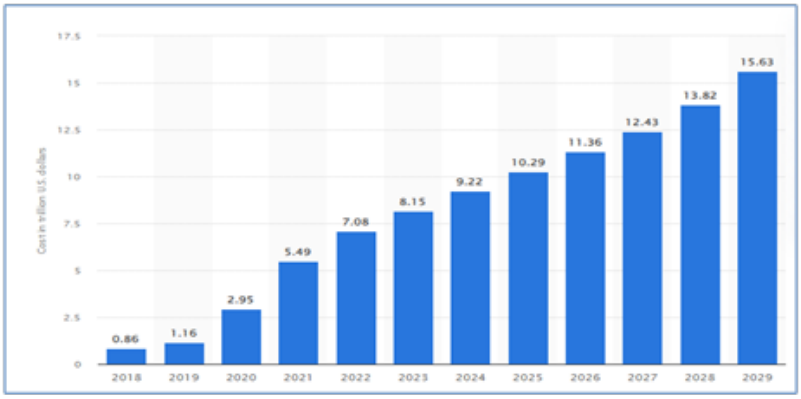
(31) IISS: **Cyber Capabilities and National Power Report**, Volume 2, 2023, at: https://www.iiss.org/research-paper/2023/09/cyber-capabilities-national-power-volume-2/

(32) **Allianz Risk Barometer 2024**, at: https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2024-Appendix.pdf

(ISSN: 2536 - 9555)

قد بلغت حوالي ٩.٢٢ تريليون دولار في عام ٢٠٢٤ ومن المتوقع أن تستمر في التزايد مع زيادة دمج التكنولوجيا في القطاعات الاقتصادية المختلفة لتقدر في عام ٢٠٢٩ بحوالي ١٥.٦٣ تريليون دولار وذلك كما يتبين من الشكل رقم (٣).

شكل رقم (٣)
اجمالي تكلفة الهجمات السيبرانية العالمية
(تريليون دولار)



Source: Statista: **Estimated cost of cybercrime worldwide 2018-2029**, at: https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

وقد قدرت التكلفة الاقتصادية للجرائم السيبرانية في إفريقيا في عام ٢٠٢١ بحوالي ٤ مليار دولار، وهو ما يشكل قرابة ١٠% من إجمالي الناتج المحلي للقارة الإفريقية. وقد ارتفعت وتيرة الجرائم والهجمات السيبرانية من ذلك الحين بمعدل زيادة متسارعة بلغ متوسطه حوالي ٢٣% في الفترة من عام ٢٠٢١ إلى عام ٢٠٢٤ وهو معدل الزيادة الأكبر عالمياً[٣٣].

وفي نيجيريا، وبالرغم من وجود إطار تشريعي وقانوني لمواجهة الجرائم والتهديدات السيبرانية، إلا أن نيجيريا لا تزال واحدة من أكبر الدول التي تعاني من الجرائم السيبرانية

(33) INTERPOL: **Interpol African Cyberthreats Assessment Report 2024: Outlook by African Cybercrime Operations Desk**, 3rd edition, at: https://www.interpol.int/en/content/download/21048/file/24COM005030AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf

بل وتعتبر إلى حد كبير كما سبقت الإشارة مصدراً لهذه التهديدات. وفي عام ٢٠٢٣ قدرت لجنة الاتصالات النيجيرية Nigerian Communications Commission (NCC) الخسائر الاقتصادية للجرائم السيبرانية في نيجيريا بحوالي ٥٠٠ مليار دولار سنوياً. كذلك فقد سجلت لجنة الجرائم الاقتصادية والمالية التابعة لوكالة مكافحة الفساد Economic and Financial Crimes Commission (EFCC) زيادة مطردة في عدد الجرائم السيبرانية لأكثر من ثلاثة أضعاف في الفترة من عام ٢٠٢٠ إلى عام ٢٠٢٣[٣٤]. وبشكل عام يمكن إجمال التداعيات الاقتصادي للجرائم والتهديدات السيبرانية في نيجيريا في مجموعتين رئيسيتين، تضم الأولى التأثيرات على المستوى الجزئي، بينما تضم الثانية التأثيرات الاقتصادية الكلية:

أ- تأثير الجرائم والتهديدات السيبرانية على المستوى الجزئي:

تؤثر المعدلات المرتفعة للجرائم والتهديدات السيبرانية في نيجيريا على الأنشطة الاقتصادية ومؤسسات الأعمال المختلفة في نيجيريا. فمن جهة قد تؤدي هذه الجرائم إلى انخفاض القدرة التنافسية لمنظمات الأعمال نتيجة ما تتكبده من خسائر جراء هذه الهجمات وما تنطوي عليه من سرقة لمعلوماتها وخططها الانتاجية المستقبلية. ومن جهة أخرى تعاني هذه الشركات من ارتفاع التكاليف الخاصة بتعزيز الأمن السيبراني بهذه الشركات لمواجهة والحد من هذه الهجمات[٣٥].

وفي هذا السياق تجدر الإشارة إلى أنه وفقاً لتقرير مخاطر الأعمال لعام ٢٠٢٤، جاءت التهديدات السيبرانية في المرتبة الأولى في مخاطر الأعمال بنسبة ٣٦%، وهي نفس النسبة الخاصة بمخاطر مثل الاختلالات الاقتصادية كالتضخم، وتغير القوانين

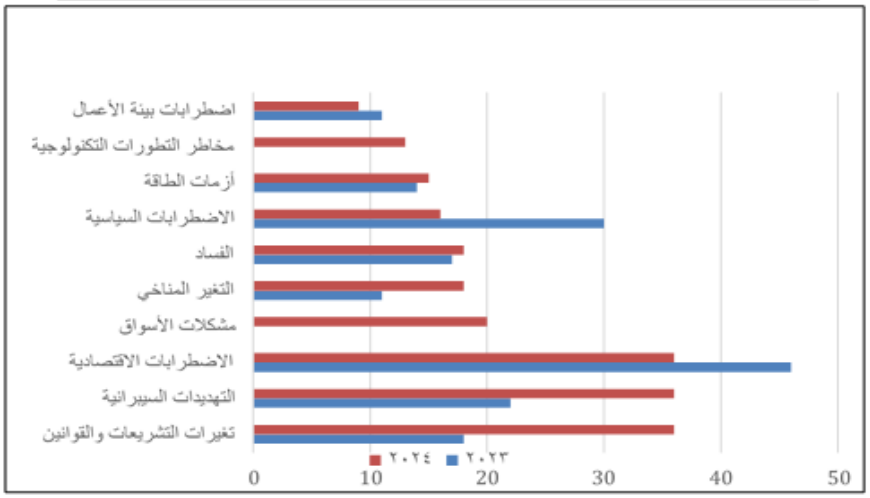
(34) Forbes: Cybercrime and The Challenge of Static Legislations in Nigeria, April 2024, at: https://www.forbes.com/councils/forbestechcouncil/2024/04/29/cybercrime-and-the-challenge-of-static-legislations-in-nigeria/#:~:text=An%20Increasingly%20Common%20Crime&text=The%20Nigeria%20Communications%20Commission%20(NCC,million%20per%20annum%20to%20cybercrime.

(35) Umaru Ibrahim: **op.cit.**

(ISSN: 2536 - 9555)

والتشريعات الاقتصادية، وذلك بعد أن كانت في المرتبة الثالثة في عام ٢٠٢٣، على النحو المبين في الشكل رقم (٤).

شكل رقم (٤)
مخاطر الأعمال في نيجيريا لعامي ٢٠٢٣ و٢٠٢٤ وفقاً لتقرير إليانز باروميتر



Source: **Allianz Risk Barometer 2024**, at: https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2024-Appendix.pdf

ب- تأثير الجرائم والتهديات السيبرانية على الستوى الكلي:

تُعتبر الجرائم السيبرانية عاملاً مثيرًا للقلق للعديد من المستثمرين الأجانب والمحليين، حيث يدرك المستثمرون أنه في بيئة يغلب عليها الاحتيال والجرائم الإلكترونية، تزداد تكلفة التأمين ضد المخاطر، مما يجعلها بيئة غير جذابة للاقتصاد الوطني. علاوة على ذلك، فإن الشركات المحلية التي تتعرض لهجمات إلكترونية تواجه صعوبة في التعافي، مما يؤدي إلى فقدان الوظائف وتقليص النشاط الاقتصادي. وتشير الدراسات إلى أن محاولات الجرائم السيبرانية تؤثر كذلك على الناتج المحلي الإجمالي الوطني، حيث تضعف قدرتها على النمو وتعزز من معدلات الفقر. وفي نيجيريا التي تعتبر في السنوات الأخيرة من بؤر الجرائم السيبرانية فإن التأثيرات على بيئة الاستثمار تكون واضحة خاصة في القطاعات الاقتصادية غير البترولية.

كذلك تؤثر الجرائم السيبرانية على موثوقية الجهاز المصرفي في نيجيريا في ظل الرقمنة والتوسع في استخدام التكنولوجيا. فعلى سبيل المثال، ارتفعت عمليات الاحتيال الإلكتروني في القطاع المصرفي بحوالي ٣٠٠% في عام ٢٠٢٣ بحيث وصلت خسائر البنوك الناتجة عنها إلى حوالي ١٠ مليار نيرة نيجيرية[٣٦].

رابعًا: التداعيات السياسية لمهددات الأمن السيبراني في نيجيريا

أسفرت الجرائم السيبرانية وغيرها من مهددات الأمن السيبراني في نيجيريا عن تداعيات بالغة الخطورة. والمتأمل لتلك التداعيات يدرك أنها متعددة الأبعاد، كما أنها تمتد إلى ما هو أبعد من المجال الرقمي لتهدد السياق الاجتماعي والاقتصادي والجيوسياسي الأوسع نطاقاً. وفيما يلي بعض أبرز التداعيات السياسية التي تم رصدها كنتيجة لمهددات الأمن السيبراني في نيجيريا:

أ- زعزعة الثقة وتهديد سمعة الدولة ومواطنيها داخلياً وخارجياً

يعتبر تهديد سمعة الدولة عالمياً أحد أبرز التأثيرات السلبية الرئيسية للجرائم السيبرانية في نيجيريا، فمع الانتشار الكبير للجرائم والهجمات السيبرانية في نيجيريا، أدى ذلك إلى تشوه صورة الدولة في الداخل والخارج، ففي الداخل، تراجعت ثقة المواطنين في قدرات الدولة التشريعية والتنفيذية على حماية حياتهم وممتلكاتهم، الأمر الذي أسفر عن عزوف عدد كبير من المواطنين عن التعامل عبر الإنترنت، حيث أصبح الفضاء السيبراني مصدر خوف وقلق لدى قطاع كبير من المواطنين في نيجيريا. ولعل هذا ما يشكل عقبة كبيرة أمام تطور عملية التحول الرقمي في نيجيريا، ويعيق الاستراتيجيات والمبادرات الوطنية في هذا الإطار، في ظل الزيادة المطردة للجرائم السيبرانية عاماً بعد عام[٣٧]. ولا يقتصر هذا التآكل في الثقة على الداخل النيجيري فحسب، بل يمتد إلى

(36) Daily Trust: **Banks Lost N10bn to Cyber Fraud in 2023**, 19 April 2024, at: https://dailytrust.com/banks-lost-n10bn-to-cyber-fraud-in-2023/

(37) Folashade B. Okeshola and Abimbola K. Adeta: "The Nature Causes and Consequences of Cybercrime in Tertiary Institutions in Zaria- Kaduna State, Nigeria"., in **American International Journal of Contemporary**

(ISSN: 2536 - 9555)

العلاقات الدولية والشراكات والتعاون، حيث تساهم الجرائم السيبرانية في تهديد سمعة الدولة أيضا إقليمياً ودولياً، ذلك أنه إذا تم التشكيك في جدارة الدولة بالثقة على الساحة العالمية بسبب الجرائم السيبرانية السائدة، فإن ذلك قد يخلف عواقب دبلوماسية وجيوسياسية وخيمة ربما تلقي بظلالها على تفاعلات الدولة وكذا على فرصها وفرص مواطنيها في المستقبل، فمن ناحية، أدى اختراق الأمن السيبراني في نيجيريا إلى بث حالة من الشك والريبة وبخاصة لدى عدد كبير من المستثمرين الذين أصبحوا أكثر حذراً وأقل استعداداً للاستثمار في الدولة(٣٨). ومن ناحية أخرى، أدى تصنيف نيجيريا بوصفها ملاذاً للجرائم السيبرانية ومرتكبيها إلى إثارة حالة من الارتياب والخوف من التعامل مع مواطني هذه الدولة بشكل عام، ولعل هذا ما يواجهه المواطنون النيجيريون بالفعل في الوقت الحالي، حيث أصبح المواطن النيجيري يجد صعوبات بالغة في القيام بأي تفاعل اجتماعي عبر الإنترنت فقط لأنه مواطن نيجيري، ولذا فقد بات يواجه تحدياً كبيراً يتمثل في محاولة تبرير موقفه وإثبات أنه ليس محتالاً محتملاً أو مرتبطاً بإحدى الجماعات أو الشبكات التي ترتكب الجرائم السيبرانية والتي باتت منتشرة لدرجة يصعب رصدها أو السيطرة عليها من قبل الأجهزة والسلطات الرسمية النيجيرية(٣٩).

ب- انتشار الوعي بسبل ارتكاب الجرائم السيبرانية وتشجيع الشباب على ارتكابها

لقد أدى الانتشار الواسع لوسائل التواصل الاجتماعي إلى نشر الوعي بالجرائم السيبرانية بين الشباب في نيجيريا. وقد أدى هذا إلى تحفيز قطاع كبير من الشباب من أجل السعي للمشاركة في تلك الجرائم. ولقد وصل الأمر إلى حد دفع بعض الشباب إلى الانسحاب من المدرسة للانضمام إلى صفوف المجرمين السيبرانيين، الذي يحفزه تدفق الشباب من الريف إلى المدينة الحضرية حيث من المرجح أن يتم تأسيسهم، وكثيراً ما

Research (New York: The Brooklyn Research and Publishing Institute, Vol. 3, No 9, September 2013), pp. 111- 112.

(38) Alex Omojo Okoru and Ochuko Oluku: "Cybercrime, Crime Security and National Development in Nigeria"., in **FUOYE Journal of Criminology and Security Studies**, (Oye: Federal University Oye-Ekiti, Vol. 3, No. 2, 2024), pp. 97- 98.

(39) **Ibid,** p. 98.

يسافرون خارج نيجيريا إلى دول أخرى للاختباء وتنفيذ أنشطتهم دون أن يتركوا أثراً سهلاً[٤٠]. وهنا تجدر الإشارة إلى أن انتشار مقاهي الإنترنت يعد من أبرز العوامل المحفزة لانتشار الجرائم السيبرانية لاسيما بين الشباب في نيجيريا، حيث توفر تلك المقاهي بيئة خصبة لمجرمي الإنترنت، الذين يستخدمونها كقاعدة لارتكاب أنشطتهم غير المشروعة. علاوة على ذلك، لا تخضع المقاهي الإلكترونية في نيجيريا للتنظيم الجيد في كثير من الأحيان، وغالبًا ما لا توجد تدابير كافية للتحقق من هويات المستخدمين أو مراقبة أنشطتهم. وقد جعل هذا الافتقار إلى الرقابة والتنظيم من السهل على مجرمي الإنترنت القيام بأنشطة غير مشروعة غير مكتشفة، كما ساعد على انتشار الجرائم السيبرانية على نطاق واسع[٤١].

ج- الترويج للطائفية والإرهاب وزيادة أحداث العنف الطائفي

يعتبر العنف الطائفي أحد التداعيات الرئيسية للجرائم السيبرانية، حيث رصدت عدة دراسات أنه قد تم استخدام وتوظيف وسائل التواصل الاجتماعي لنشر خطاب الكراهية، فضلاً عن نشر عدد من المحتويات المثيرة للانقسام، والتي غالبًا ما تؤدي إلى التوتر بين مختلف الجماعات الإثنية الموجودة في نيجيريا. ولعل خير مثال على ذلك الصراع المستمر والتاريخي السائد بين المزارعين والرعاة في نيجيريا، حيث تم استخدام وسائل التواصل الاجتماعي لتصوير الصراع على أنه حرب عرقية دينية. وبالإضافة إلى ذلك، تم استخدام الفضاء السيبراني للتحريض على العنف، حيث بدأ مجرمو الإنترنت في ارتكاب أعمال إرهابية عبر شبكات الكمبيوتر. وفي هذا السياق، أصبح الإرهاب السيبراني والتجسس الإلكتروني وتمويل التمرد والتجنيد تدريجيًا هو القاعدة. ولعل من أبرز وأخطر تداعيات الجرائم السيبرانية في نيجيريا ما يتعبق باستخدام الفضاء السيبراني

(40) Juliet Jenebu Obajobi, Francis Ojima Akoji, & Chubado Umaru: "Impact of Cybercrime on National Development: A Review on Nigeria"., in **Lapai Journal of Humanities**, (Lapai: The Department of History and International Studies, Ibrahim Badamasi Babangida University, Vol. 13 No. 1, June 2022), p. 61.

(41) Yakubu Ajiji Makeri: **op.cit.,** p. 319.

(ISSN: 2536 - 9555)

لطلب الأموال وزيادة عضوية المنظمات الإرهابية وتغذية بعض التوجهات الإيديولوجية وتعزيز التطرف(٤٢). وجدير بالذكر أن جماعة بوكو حرام الإرهابية بدأت في اكتساب حضور سيبراني واسع النطاق في نيجيريا خلال السنوات الماضية. وفي ٣٠ أغسطس عام ٢٠١٣، اخترقت جماعة بوكو حرام خوادم وزارة أمن الدولة، وسربت تفاصيل أكثر من ٦٠ مسئولاً بما في ذلك عناوينهم وأسماء أفراد أسرهم. ولعل هذا ما يشكل تهديدًا كبيرًا لحياة المسئولين وأفراد أسرهم، وبالطبع يشكل ضغطًا على الأمن القومي للدولة ككل(٤٣).

د- تهديد الأمن القومي للدولة وانتشار المعلومات المضللة

يعتبر مفهوم الأمن القومي من المفاهيم المعقدة متعددة الأبعاد التي اتسع نطاقها خلال السنوات الأخيرة بشكل أكبر من ذي قبل، وهناك اجتهادات وإسهامات عدة من جانب الباحثين في توضيح مفهوم الأمن القومي ومؤشراته. ويعرف البعض الأمن القومي باعتباره:

"حماية الدولة وأراضيها وشعبها من الاعتداء المادي من قبل قوة خارجية، فضلاً عن حماية المصالح الاقتصادية والسياسية والعسكرية والاجتماعية والثقافية والقيمة للدولة المهمة من الهجمات الصادرة عن مصادر أجنبية أو محلية والتي قد تقوض أو تآكل أو تقضي على هذه المصالح، وبالتالي تهدد بقاء الدولة. يمكن السعي إلى مثل هذه الحماية بوسائل عسكرية أو غير عسكرية"(٤٤).

(42) Juliet Jenebu Obajobi, **op.cit.**, pp. 60- 61.

(43) Tope Shola Akinyetun: "Poverty, Cybercrime and National Security in Nigeria"., in **Journal of Contemporary Sociological Issues**, (East Java: the University of Jember, Volume 1, Issue 2, 2021), p. 15.

(44) Daniel S. Papp and David S. Alberts: "National Security in the Information Age: Setting the Stage" in David S. Alberts and Daniel S. Papp (eds): **Volume II. Information Age Anthology: National Security Implications of the Information Age**, (Washington, DC: office of the assistant secretary of defense, command and control research program (CCRP), 2000), p. 10.

وبهذا المعنى، فقد أصبح انتشار الجرائم السيبرانية وما تنطوي عليه من تعقيد يشكل تهديداً وتحدياً كبيراً للبنية الأساسية للأمن القومي للدولة بشكل عام ولنيجيريا بصفة خاصة، حيث أدى التقدم السريع للتكنولوجيا وتوسع المشهد الرقمي في نيجيريا إلى خلق سبل جديدة لمجرمي الإنترنت، الذين أصبحوا أكثر تطوراً وتنظيماً لاستغلال عدم الكشف عن الهوية الذي توفره شبكة الإنترنت وثغرات نظام الأمان النيجيري لإجراء أنشطة وهجمات ممنهجة تستهدف اختراق بيانات جهات فاعلة في الدولة. وبالتالي، فإن المخاطر المتزايدة لاختراق البيانات في السنوات الأخيرة لها آثار كبيرة على الأفراد والمنظمات والهيئات الحكومية(٤٥). ولقد أصبحت شبكات وأنظمة الكمبيوتر التي تدعم البنية التحتية الحيوية، بما في ذلك شبكات الطاقة وشبكات الاتصالات والتمويل، أهدافًا رئيسية لمجرمي الإنترنت. كما أنه مع تحويل الحكومة وحتى الشركات الخاصة لعملياتها إلى منصات رقمية، تصاعدت عمليات سرقة وتدمير البيانات الحساسة، مما عرض عمليات الحكومة للخطر، وهو ما له عواقب متعددة الأبعاد على الأمن القومي للدولة(٤٦). بالإضافة إلى ذلك، يمكن أن يؤدي الاستخدام غير المشروع للمعلومات المسروقة من قبل مجرمي الإنترنت إلى الاستغلال المالي، حيث قد يبتزون الضحايا– سواء كانوا أفراد أو شركات كبرى– للحصول على الأموال أو يبيعون البيانات السرية في السوق السوداء(٤٧).

(45) Omolola Tobiloba Adisa: **"The impact of cybercrime and cybersecurity on Nigeria's national security"**., Master Thesis, (Prague: Faculty of Social Science, Charles University, 2023), pp. 23- 25.

(46) Peter Grabosky: "Organized Cybercrime and National Security"., in Russell G. Smith, Ray Chak-Chung Cheung and Laurie Yiu-Chung Lau (eds), **Cybercrime Risks and Responses** (London: Palgrave Macmillan, 2015), pp.74- 75, available at: https://doi.org/10.1057/9781137474162_5/ accessed on 12/ 08/ 2024.

(47) Simon Handler and Liv Rowley: **The 5×5—Cybercrime and national security**, available at: https://www.atlanticcouncil.org/commentary/the-5x5-cybercrime-and-national-security/#:~:text=%E2%80%9CCybercrime%20impacts%20national%20security/ accessed on 3/ 08/ 2024.

(ISSN: 2536 - 9555)

واستناداً إلى ما تقدم، يمكن القول إن الوصول غير المصرح به والاختراق المتعمد والممنهج للبيانات الحساسة باتا من أبرز العوامل التي تهدد الأمن القومي النيجيري بصورة مثيرة للقلق، فعندما يستهدف الخصوم المؤسسات الأساسية مثل وكالات الاستخبارات أو المؤسسات العسكرية، هناك خطر كبير يتمثل في إمكانية وقوع البيانات السرية في أيدي جماعات معادية سواء في الداخل أو في الخارج، وقد تكشف مثل هذه الخروقات عن استراتيجيات الدفاع النيجيرية، مما يمنح القوات المعادية رؤى لا تقدر بثمن حول استعدادات أجهزة الدولة وآليات الاستجابة. وعلاوة على ذلك، يمكن أن تؤدي التدخلات السيبرانية في عمليات جمع المعلومات الاستخباراتية وتحليلها ونشرها إلى حدوث حالة من الاضطراب من شأنها عرقلة العمليات الاستخباراتية الجارية، الأمر الذي يمهد الطريق لانتشار المعلومات المضللة، ويجعل عملية اتخاذ القرار مسألة من الصعوبة بمكان، حتى على أعلى مستويات الحكومة. وهنا تجدر الإشارة إلى أن آثار الجرائم السيبرانية على الأمن القومي تتجاوز فكرة اختراق البيانات لتكسب مرتكبي هذه الجرائم اليد العليا من الناحية الاستراتيجية، وذلك من خلال الاطلاع على المعلومات السرية النيجيرية، الأمر الذي يمكن هؤلاء الخصوم من تقويض المكانة الجيوسياسية للدولة ونفوذها في مجالات مختلفة، من المفاوضات الدبلوماسية إلى إقامة شراكات دولية وفرض النفوذ على المنصات العالمية وغير ذلك من آثار سلبية[٤٨].

خاتمة

أوضحت الدراسة أن الجرائم والهجمات السيبرانية تشكل تهديدًا كبيرًا سواء بالنسبة للاقتصاد النيجيري أو حتى للسلام والأمن الوطنيين. وقد أظهرت الدراسة أن إساءة استخدام التكنولوجيا أثرت بالفعل على اقتصاد الدولة على المستويين الكلي والجزئي، حيث أدت إلى انخفاض القدرة التنافسية لمنظمات الأعمال نتيجة ما تتكبده من خسائر جراء هذه الهجمات، كما أدت إلى هروب المستثمرين وتقليص النشاط الاقتصادي

(48) Omolola Tobiloba Adisa: **op.cit.,** pp. 62- 63.

وارتفاع تكلفة التأمين ضد المخاطر، فضلاً عن التداعيات السياسية بالغة الخطورة، والتي تتعلق بالإضرار بسمعة الدولة والنيل من صورتها ومصداقيتها الدولية، وما لذلك من تداعيات ذات صلة بعرقلة خطط واستراتيجيات التحول الرقمي وغير ذلك من آثار كارثية. وبالرغم من أن نيجيريا تبنت عدة تشريعات واستراتيجية لحماية أمنها السيبراني ومكافحة مهددات الأمن السيبراني فيها، إلا أن المتأمل لحجم الجرائم والهجمات السيبرانية خلال السنوات الأخيرة يدرك دونما عناء أنها في تزايد كل عام، الأمر الذي يؤكد على أن ثمة ضعف وقصور في الإطار القانوني المتصل بالجرائم السيبرانية، وكذا في القدرة على إنفاذ قوانين مكافحة هذه الجرائم، الأمر الذي جعلها تبدو بمثابة بؤرة للأفراد والجماعات التي تمارس الجرائم السيبرانية، والملفت أن نشاط هذه المجموعات بات يتزايد وتمكنت من توظيف الفضاء السيبراني في الترويج لأنشطتها وتشجيع عدد كبير من الشباب على ممارسة هذه الجرائم بهدف الإثراء الذاتي غير المشروع، وبث الفرقة بين مختلف الجماعات المشكلة لشعب الدولة، مستغلة في ذلك عجز الأجهزة الرسمية عن ملاحقة ومعاقبة مرتكبي تلك الجرائم. ومن هذا المنطلق، فإن تنظيم الاستخدام المسيء للإنترنت ووسائل التواصل الاجتماعي وملاحقة مرتكبي الجرائم السيبرانية ومعاقبتهم يعد أولى خطوات مكافحة هذا النوع من الجرائم والحد من آثارها وتداعياتها السياسية والاقتصادية السلبية في نيجيريا.

وختاماً يمكن القول إن العواقب الحالية والمحتملة لمهددات الأمن السيبراني في نيجيريا تعد بعيدة المدى، فضلاً عن كونها مترابطة. ذلك أن التأثير الاقتصادي وفقدان الثقة في المنصات الرقمية والمساس بالمعلومات والاستخبارات ليست ظواهر منعزلة عن بعضها البعض، وإنما ترسم مجتمعة صورة لدولة تتصارع مع التهديدات الرقمية التي لديها القدرة على تقويض استقرارها الاقتصادي وثقتها الاجتماعية وسلامة أمنها القومي. إن معالجة هذه العواقب تتطلب جهداً شاملاً ومنسقاً، كما تتطلب مواءمة الاستراتيجيات الاقتصادية والتكنولوجية والاجتماعية والأمنية، وذلك بغية الحد من آثار التهديدات السيبرانية على النحو الذي يحقق الأمن السيبراني المنشود.

(ISSN: 2536 - 9555)

قائمة المراجع

أولاً: المراجع العربية

١. برنامج الأمن السيبراني: **الاصدار الخامس للرقم القياسي العالمي للأمن السيبراني: نموذج مرجعي (المنهجية)**، ٢٠٢٤، في:
https://web.archive.org/web/20240118014737/https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/513560_2A.pdf

٢. **تحديات الأمن السيبراني في إفريقيا: بناء جسور التكنولوجيا وتحقيق الاستدامة الرقمية**، فبراير ٢٠٢٤، ٩/ ٠٩/ ٢٠٢٤، في:
https://gate.ahram.org.eg/News/4731124.aspx

٣. فاروق أبوضيف: **التهديدات السيبرانية التي تواجه القارة الإفريقية، قراءات إفريقية**، يوليو ٢٠٢٤، ٩/ ٠٩/ ٢٠٢٤، في:
https://qiraatafrican.com/21857/%D8%A7%D9%84%D8%AA%D9%87%D8%AF%D9%8A%D8%AF%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D8%A7%D9%84%D8%AA%D9%8A-%D8%AA%D9%88%D8%A7%D8%AC%D9%87-%D8%A7%D9%84%D9%82%D8%A7/

ثانياً: المراجع الأجنبية

A) Books:

1. Ajayi, Kunle (ed), **Readings in Intelligence and Security Studies**, (Ekiti: Intelligence and Security Studies Programme, 2015).
2. Alberts, David S. and Daniel S. Papp (eds): **Volume II. Information Age Anthology: National Security Implications of the Information Age**, (Washington, DC: office of the assistant secretary of defense, command and control research program (CCRP), 2000).
3. Colarik, Andrew M.: **Cyber Terrorism: Political and Economic Implications**, (Pennsylvania: Idea Group Pub., 2006).

B) Articles:

1. Akinyetun, Tope Shola: "Poverty, Cybercrime and National Security in Nigeria"., in **Journal of Contemporary Sociological Issues**, (East Java: The University of Jember, Volume 1, Issue 2, 2021).

2. Brenner, Susan W.: "Cybercrime, Cyberterrorism and Cyberwarfare"., in **International Review of Penal Law** (Indiana: Marchal et Billard, Vol. 77, no. 3, 2006).
3. Bruce M, Lusthaus J, Kashyap R, Phair N, Varese F, "Mapping the global geography of cybercrime with the World Cybercrime Index"**, PLoS,** Vol 19, No.4, April 2024, at: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0297312#sec003
4. Goel, Pallavi Murghai: "A Literature Review of Cyber Security"., in **International Journal of Research and Analytical Reviews**, (Gujarat: Atman Publishing Academy, Vol. 6, Issue 2, April 2019), p. 136.
5. Makeri, Yakubu Ajiji: "Cyber Security Issues in Nigeria and Challenges"., in **International Journal of Advanced Research in Computer Science and Software Engineering**, (New Delhi: Advanced Research International Publcation House, volume 7, issue 4, April 2017).
6. Obajobi, Juliet Jenebu, Francis Ojima Akoji, & Chubado Umaru: "Impact of Cybercrime on National Development: A Review on Nigeria"., in **Lapai Journal of Humanities**, (Lapai: The Department of History and International Studies, Ibrahim Badamasi Babangida University, Vol. 13 No. 1, June 2022).
7. Okeshola, Folashade B. and Abimbola K. Adeta: "The Nature Causes and Consequences of Cybercrime in Tertiary Institutions in Zaria- Kaduna State, Nigeria"., in **American International Journal of Contemporary Research** (New York: The Brooklyn Research and Publishing Institute, Vol. 3, No 9, September 2013).
8. Okoru, Alex Omojo and Ochuko Oluku: "Cybercrime, Crime Security and National Development in Nigeria"., in **FUOYE Journal of Criminology and Security Studies**, (Oye: Federal University Oye-Ekiti, Vol. 3, No. 2, 2024).
9. Orji, Uchenna Jerome: "The African Union Convention on Cybersecurity: A Regional Response towards Cyber Stability?"., **Masaryk University Journal of Law and Technology,** (Brno: Institute of Law and Technology, vol. 12, no. 2, Fall 2018).
10. Veerasamy, N.: "A High-level Conceptual Framework of Cyber-terrorism", **Journal of Information Warfare**, (Virginia: Peregrine Technical Solutions LLC, Vol. 8, No. 1, 2009).

(ISSN: 2536 - 9555)

C) Thesis:

1. Adisa, Omolola Tobiloba: **"The impact of cybercrime and cybersecurity on Nigeria's national security"**., Master Thesis, (Prague: Faculty of Social Science, Charles University, 2023)

D) Reports

1. Allianz Trade: **Allianz Risk Barometer 2024**, at:https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2024-Appendix.pdf
2. ITU High Level Experts Group: **ITU Global Cyber-Security Agenda (GCA) High Level Experts Group [HLEG]** (Geneva: Global Strategic Report, 2008).
3. IISS: **Cyber Capabilities and National Power Report**, Volume 2, 2023, at:https://www.iiss.org/research-paper/2023/09/cyber-capabilities-national-power-volume-2/
4. INTERPOL: **Interpol African Cyberthreats Assessment Report 2024: Outlook by African Cybercrime Operations Desk**, 3rd edition, at:https://www.interpol.int/en/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf
5. NCSI: **National Cybersecurity Index: Nigeria**, at:https://ncsi.ega.ee/country/ng/

E) Internet Sources:

1. Daily Trust: **Banks Lost N10bn to Cyber Fraud in 2023**, 19 April 2024, at: https://dailytrust.com/banks-lost-n10bn-to-cyber-fraud-in-2023/
2. Forbes: **Cybercrime and The Challenge of Static Legislations in Nigeria**, April 2024, accessed on: 04/10/2024, at: https://www.forbes.com/councils/forbestechcouncil/2024/04/29/cybercrime-and-the-challenge-of-static-legislations-in-nigeria/#:~:text=An%20Increasingly%20Common%20Crime&text=The%20Nigeria%20Communications%20Commission%20(NCC,million%20per%20annum%20to%20cybercrime.
3. Grabosky, Peter: "Organized Cybercrime and National Security"., in Russell G. Smith, Ray Chak-Chung Cheung and Laurie Yiu-Chung Lau (eds), **Cybercrime Risks and Responses** (London:

Palgrave Macmillan, 2015), available at: https://doi.org/10.1057/9781137474162_5/

4. Handler, Simon and Liv Rowley: **The 5×5—Cybercrime and national security**, available at: https://www.atlanticcouncil.org/commentary/the-5x5-cybercrime-and-national-security/#:~:text=%E2%80%9CCybercrime%20impacts%20national%20security/ https://dailytrust.com/banks-lost-n10bn-to-cyber-fraud-in-2023/ https://ncsi.ega.ee/methodology/
5. Hua, Jian, & Bapna, Sanjay, "The Economic Impact of Cyber Terrorism", **Journal of Strategic Information Systems**, at: https://www.researchgate.net/publication/261860155_The_economic_impact_of_cyber_terrorism
6. Ibrahim, Umaru: **The Impact of Cybercrime on The Nigerian Economy and Banking System**, available at: https://demo.ndic.gov.ng/wp-content/uploads/2020/08/NDIC-Quarterly-Vol-34-No-12-2019-Article-The-Impact-Of-Cybercrime-On-The-Nigerian-Economy-And-Banking-System.pdf/ accessed on 28/ 07/ 2024.
7. Idowu, Oluwafemi Amos, Cybercrimes and Challenges of Cyber-Security in Nigeria, **International Journal of Sociology and Development**, Vol3, No.1, at: https://www.academia.edu/50170416/Cybercrimes_and_Challenges_of_Cyber_Security_in_Nigeria
8. Jackson, T.C.B & Ene, Robert W., "Cybercrime and the Challenges of Socio-Economic Development in Nigeria, **Journal of Researches in National Development,** Vol12, No.2, at: https://www.researchgate.net/publication/313361300_CYBERCRIME_AND_THE_CHALLENGES_OF_SOCIO-ECONOMIC_DEVELOPMENT_IN_NIGERIA
9. Kelley, Patrick, **Evolution of Cyber Attacks and Their Economic Impacts**, 2022, at: https://doi.org/10.36227/techrxiv.21670718.v1
10. NCSI: **National Cybersecurity Index: Methodology,** at: https://ncsi.ega.ee/methodology/
11. Obura, Ken: **Cyberspace is the latest conflict frontier in Afrika,** 22nd June 2018, available at:

(ISSN: 2536 - 9555)

https://www.iafrikan.com/2018/06/22/is-cyberspace-the-latest-conflict-frontier-on-the-african-continent/

12. Owiny, Moses: **The politics of Cyber Security policy making in Africa: The Case Study of Uganda**, available at: https://thecfma.org/wp-content/uploads/2019/10/Securitization-and-the-logic-of-Cyber-Security-policy-making-in-Africa.pdf/
13. Rouse, Margaret: **Definition of cybersecurity,** available at: https://searchsecurity.techtarget.com/definition/cybersecurity/
14. Saidu, I. R., etal., The Challenges of Security Threats in Nigeria Cyberspace, **FUDMA Journal of Sciences**, vol.5, No.1, March 2021. At: https://doi.org/10.33003/fjs-2021-0501-554
15. Schia, N.N., and Gjesvik, L., **Managing a Digital Revolution-Cybersecurity Capacity Building in Myanmar**, 2018, at: https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2563201/Managing%2ba%2bdigital%2brevolution.pdf?sequence=1&isAllowed=y
16. Schiliro, Francisco: **Towards a Contemporary Definition of Cybersecurity**, 2022, available at: https://doi.org/10.48550/arXiv.2302.02274/
17. Sesan, Gbenga, etal,: **Economic Cost of Cybercrime in Nigeria**, University of Toron, 2023, at: http://www.opennetafrica.org/?wpfb_dl=7
18. Statista: **Estimated cost of cybercrime worldwide 2018-2029**, at: https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide
19. The Economic Times: **Definition of" cyber security"** available at: https://economictimes.indiatimes.com/definition/cyber-security/
20. Yadav, Hetram and Gour, Shashant, "Cyber Attacks: An Impact on Economy to an Organization", **International Journal of Information & Computation Technology,** Vol 4, No. 9, at: https://www.ripublication.com/irph/ijict_spl/ijictv4n9spl_11.pdf