مجلة العلوم القانونية و الاجتماعية

Journal of legal and social studies

Issn: 2507-7333

Eissn: 2676-1742

جريمة إستهداف الأنظمة المعلوماتية للبنوك و المصارف وعلاقته بتمويل الإرهاب

The crime of targeting the information systems of banks and its relationship to financing terrorism

نشلة مصطفى [1]*، رابحي لخضر [2]

[1] جامعة عمار ثليجي الأغواط ، (الجزائر)، mu.nechla@lagh-univ.dz،

مخبر الحقوق و العلوم السياسية

[2] جامعة عمار ثليجي الأغواط ،(الجزائر)، rabhi.lakhdar03@gmail.com ،

مخبر الحقوق و العلوم السياسية

تاريخ ارسال المقال: 2023/03/06	تاريخ القبول: 2023/05/01	تاريخ النشر: 2023/06/01

* المؤلف المرسل

الملخص:

في ظل ما تقدمه التكنولوجيا الحديثة من خدمات سهلت بفضلها الحياة اليومية للبشر ، وقد إستفادت المصالح الحيوية في دول العالم من هاته الثورة الرقمية ومن بين هذه المصالح المؤسسات المالية كالبنوك والمصارف والتي سارعت لمواكبة هذا التطور بغية عصرنة هذا القطاع من جهة ومن أجل مضاعفة عائدتها ومداخيلها من جهة أخرى ، غير أن هذه المؤسسات المالية وجدت نفسها أمام تحدي يتمثل في مواجهة الهجمات السيبرانية التي تتعرض له أنظمتها المعلوماتية من طرف القراصنة والهاكرز المحترفين ، وقد شكلت هاته الأفعال جرائم سارعت بعض الدول لتخصيص نصوص قانونية تجرمها وتتابع مرتكبيها كما هو الحال في القانون السعودي والمصري بينما اكتفت بعض الدول بالمعاقبة على الجريمة الإلكترونية بشكل عام ، وقد خرجت جريمة إستهداف الأنظمة الألية للبنوك والمصارف في بعض الأحيان من نطاق الجرائم العادية للتحول لجرائم إرهابية أو لها علاقة بتمويل الإرهاب ، كما تنوعت أشكال تلك الهجمات السيبرانية الإرهابية فمنها المباشر كسرقة البنك من خلال القيام بتحويلات داخلية وخارجية وبدرجة أخف إبتزاز البنك ببعض المعطيات التي تم قرصنتها أو غير المباشر عن طريق إستغلال موظفي البنوك من خلال قرصنة هواتفهم أو حواسيبهم الشخصية لإجبارهم على تسهيل عمليات السرقة ، ولمواجهة هاته الهجمات إقترح صندوق النقد الدولي عدة طرق وإستراتجيات لتعزيز الأمن السيبراني نذكر منها على سبيل المثال التحديد الكمي للمخاطر السيبرانية وتعزيز أنظمة الأمن السيبراني كما دعى الصندوق لتكثيف التعاون و التنسيق بين المؤسسات المالية حول العالم لمواجهة هذا النوع من الجرائم .

الكلمات المفتاحية: النظام المعلوماتي ؛ البنوك ؛ الأمن السيبراني ؛ تمويل الإرهاب ؛ القرصنة ؛ السرقة الإلكترونية ؛ الهجوم السيبراني

Abstract :

In light of the services provided by modern technology, thanks to which the daily life of human beings is facilitated, vital interests in the countries of the world have benefited from this digital revolution. Others, however, these financial institutions found themselves facing a challenge represented in the face of cyber-attacks against their information systems by hackers and professional hackers. Some countries have punished cybercrime in general, and the crime of targeting the automated systems of banks and banks has sometimes gone out of the scope of ordinary crimes to turn into terrorist crimes or related to the financing of terrorism, and the forms of these terrorist cyber attacks varied, including direct bank robbery through internal and external transfers. And to a lesser degree, the bank's extortion of some data that was hacked or indirectly through the exploitation of

its employees Banks through hacking their phones or personal computers to force them to facilitate theft operations, and to counter these attacks, the International Monetary Fund has proposed several ways and strategies to enhance cybersecurity, including, for example, the quantification of cyber risks and the strengthening of cybersecurity systems. The Fund also called for intensifying cooperation and coordination between financial institutions. around the world to confront this type of crime.

Keywords: information systems ؛ hackers؛ cybersecurity ؛bank ؛cyber attacks

مقدّمة:

مع توسع دائرة إستخدام الأجهزة الرقمية وتأثيرها على حياة البشر حيث لم تصبح هاته الأجهزة مستخدمة فقط لغرض التصفح والمطالعة و التواصل الإجتماعي بل إمتد أثرها لتصبح ركيزة أساسية للتجارة العالمية ووسيلة للشراء و البيع وإجراء المعاملات المالية بشتى أنواعها وقد كانت الدول والمؤسسات المالية وخاصة البنوك و المصارف سباقة لتوفير تلك الخدمات إلكترونيا لتسهيلها على متعامليها وتجنيبهم عناء التنقل لمقرات تلك المؤسسات للقيام بتلك المعاملات النقدية ، و في المقابل أصبحت الأنظمة المعلوماتية المسيرة والمنظمة لتلك المعاملات هدفا للهاكرز والقراصنة الرقميين وتمكنوا من الولوج لها والقيام بعدة جرائم في مقدمتها جريمة السرقة الإلكترونية وتحويل تلك الأموال لحسابات مجهولة .

وأصبحت تثار إشكاليات عديدة لدى الباحثين والمختصين في هذا المجال نذكر من بينها :

ماهو الإطار القانوني لجريمة إستهداف الأنظمة المعلوماتية للبنوك و المصارف ؟

وما علاقة هذه الجريمة بتمويل الإرهاب ؟ وكيف يمكن مواجهتها والحد من خطورتها ؟

الفرضيات المعتمدة :

الجرائم الحديثة في إستهداف المؤسسات المالية وعلى رأسها البنوك و المصارف.

ترابط جريمة القرصنة الإلكترونية للبنوك أحيانا مع تمويل التنظيمات الإرهابية.

أهداف المقال :

إعطاء الباحثين و المختصين في مجال المعاملات المالية رؤية قانونية لجرائم المساس بالأنظمة المعلوماتية للبنوك.

إثبات العلاقة التي تكون في بعض الحالات بين تمويل الإرهاب وجرائم السرقة الإلكترونية في شقها المؤسساتي.

إبراز الوسائل المتاحة لتعزيز الأمن السيبراني للبنوك و المصارف .

للإجابة على الإشكاليات المذكورة سابقا ستكون إجابتنا مقسمة لثلاث محاور :

المحور الأول : الإطار القانوني لجريمة استهداف الأنظمة المعلوماتية للمصارف و البنوك

المحور الثاني : العلاقة بين جريمة إستهداف الأنظمة الإلكترونية البنكية وتمويل الإرهاب

المحور الثالث : وسائل تعزيز الأمن السيبراني للبنوك

المحور الأول : الإطار القانوني لجريمة استهداف الأنظمة المعلوماتية للمصارف و البنوك

قبل الشروع في الكلام عن جريمة إستهداف الأنظمة الإلكترونية للبنوك ينبغي التطرق لماهية هاته الأنظمة وماهي أسباب الإنتقال من التعاملات المالية التقليدية إلى التعاملات المالية الإلكترونية .

أولا : دوافع الإنتقال من التعاملات المالية التقليدية إلى التعاملات المالية الإلكترونية:

بفضل تطور الشبكات العنكبوتية. والنجاح الهائل في مجال الاتصالات التي نعيش في رحابه. دفع الشركات المالية والتجارية الكبيرة والمصارف والبنوك الانتقال السريع نحو استخدام الفضاء الالكتروني لكي يكون العامل الرئيسي في دفع التجارة المالية والاقتصادية الى مستوى الحياة الجديدة .

ويعتبر العمل المصرفي الالكتروني من الأمور التي أفرزها التطور التكنولوجي الهائل في مجال الاتصالات، حيث تم استحداث وسائل دفع جديدة تكون ملائمة لطبيعة ومتطلبات التجارة الإلكترونية، وأصبح بإمكان العميل الاستفادة من الخدمات المصرفية كسداد فواتير السلع والخدمات عن طريق الاتصال الهاتفي والالكتروني.

إن قيام البنوك بتسوية أنشطتها وخدماتها المالية عبر الانترنت يعود عليها بفوائد الكثيرة والتي من أهمها :

– تخفيض النفقات التي يتحملها البنك لأجراء بعض المعاملات البنكية المختلفة بدون الحاجة للانتقال الى البنك ، وهذا ما يؤدي إلى توفير تكلفة إنشاء فروع جديدة للبنك في المناطق البعيدة لان تكلفة انشاء موقع للبنك عبر الانترنت لا تقارن بتكلفة إنشاء فرع جديد له ، بما يحتاجه من مباني واجهزة وعمالة مدربة ومستندات وصيانة. فممارسة البنك عبر موقعه عبر الانترنت ، تسويق خدماته البنكية وبعض المعاملات البنكية تساعده على امتلاك ميزة تنافسية وتدعيم علاقته مع عملائه مما يؤدي الى زيادة ارتباطهم به والارتقاء الى مستوى المعاملات التجارية.

– تعزيز راس المال الفكري وتطوير تكنولوجيا المعلومات.

– إن العمليات المصرفية الالكترونية تؤدي لتيسير التعامل بين البنوك وجعله متواصلا على مدار الوقت.

– اختصار المسافات الجغرافية ورفع الحواجز التقليدية.

– قيام علاقات مباشرة بين البائع والمشتري.

– توفير المزيد من فرص العمل والاستثمار. (1) .

ثانيا: التعريف بجريمة المساس بالأنظمة الألية للبنوك :

لقد قابل ثورة الإنفتاح على التكنولوجيات الاعلام و الإتصال ظهور جرائم جديدة في هذا المجال والتي منها الجرائم الماسة بالأنظمة الإلكترونية للمصارف و البنوك بغية تعطيلها أو التشويش عليها من أجل سرقة حسابات العملاء ، ويمكننا إستنباط بعض التعريفات لهاته الجريمة من خلال بعض التشريعات الداخلية التي تصدت لهذا النشاط الإجرامي الإلكتروني ضد المؤسسات المالية البنكية فقد نصت مثلا المادة الرابعة من المرسوم الملكي الخاص بنظام مكافحة الجرائم المعلوماتية للمملكة العربية السعودية أنه : يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

1. الاستيلاء لنفسه أو لغيره على مال منقول أو على سند ، أو توقيع هذا السند ، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة.
2. الوصول – دون مسوغ نظامي صحيح – إلى بيانات بنكية ، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات ، أو معلومات، أو أموال، أو ما تتيحه من خدمات.(2)

كما نص القانون المصري رقم 175 لسنة 2018 الخاص بجرائم تقنية المعلومات في الفصل الثاني الخاص بالجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات جرائم الإحتيال والإعتداء على بطاقات البنوك والخدمات وأدوات الدفع الإلكتروني في المادة 23 أنه : يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن 30 الف جنيه ولا تتجاوز 50,000 جنيه او بإحدى هاتين العقوبتين كل من استخدم الشبكة المعلوماتية أو احدى وسائل تقنية المعلومات في الوصول بدون بدون وجه حق إلى أرقام أو بيانات بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الالكتروني .

فإن قصد من ذلك استخدامها في الحصول على أموال الغير أو ما تتيحه من خدمات يعاقب بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن 50 الف جنيه ولا تتجاوز 100,000 جنيه أو بإحدي هاتين العقوبتين وتكون العقوبة الحبس مدة لا تقل عن سنة وبغرامة لا تقل عن 100,000 جنيه ولا تتجاوز 200 الف جنيه او احدى هاتين العقوبتين اذا توصل من ذلك الى الاستيلاء لنفسه او لغيره على تلك الخدمات أو مال الغير . (3)

كما أكد الدكتور عبدالرحمن بن عبدالله الحميدي المدير العام ورئيس مجلس إدارة صندوق النقد العربي في افتتاح ورشة العمل حول مواجهة التهديدات الإلكترونية في الخدمات المالية في الدول العربية :

أن الخدمات والمؤسسات المالية والمصرفية هي الأكثر استهدافاً للهجمات الإلكترونية، حيث نمت الهجمات الإلكترونية بأكثر من ثلاثة أضعاف بالمقارنة مع العقد الماضي، وذلك مع تزايد الاهتمام بالخدمات المالية الرقمية وما تتيحه من فرص، حيث تعرضت الصناعة المالية للهجمات الإلكترونية الأكثر تكراراً في السنوات الخمس الماضية 2016-2020، بنسبة تقدر بنحو 26 في المائة من إجمالي الهجمات، وهي النسبة الأعلى بين القطاعات الاقتصادية. كما أن الهجمات الإلكترونية على أي كيان مهما كان حجمه، ذات تداعيات سريعة وتنعكس على النظام المالي وتُلقي بظلالها على الاقتصاد ككل. يتزامن ذلك مع زيادة وتطور أدوات وأساليب القرصنة، مما جعلها أشد تأثيراً من ذي قبل في ظل توسع الخدمات المالية الرقمية وانتشارها، ذلك نتيجة تزايد الترابط المالي والتقني بين النظم المالية المحلية والدولية.(4)

ولقيام المسؤولية الجنائية عن هاته الجريمة ينبغي التعرف على أركانها :

أولا الركن الشرعي : الملاحظ لأغلب التشريعات الداخلية وفي الوقت الحاضر يجد أن الدول قد تبنت تجريم هذا النوع من الجرائم في قوانينها وقد ذكرنا سابقا بعض المواد المجرمة للمساس بالشبكة المعلوماتية للمؤسسات المالية في القانون السعودي و المصري على سبيل المثال ، وبالمقابل حتى الدول التي لم تذكر تحديدا إستهداف الأنظمة الألية للبنوك والمصارف قد وضعت تشريعات وقوانين تواجه من خلالها الجريمة الإلكترونية بكافة أبعادها .

ثانيا الركن المادي : لقيام المسؤولية الجنائية على جريمة إستهداف الأنظمة الإلكترونية للبنوك يجب وجود سلوك إجرامي متمثل في قيام الجاني بدخول الغير مصرح أو التجسس أو تخريب أو تشويش أو سرقة بإستخدام أي وسيلة من الوسائل الإلكترونية ضد الأنظمة الألية للبنوك و المصارف وأحدثت على إثر ذلك هاته الأفعال نتيجة إجرامية كسرقة الأموال والتلاعب في الأرصدة أو سرقة معلومات الزبائن ... ، ثم قامت العلاقة السببية بين ذلك السلوك الإجرامي والنتيجة الإجرامية ويكون بذلك إكتمل الركن المادي لهاذا النوع من الجرائم .

ثالثا الركن المعنوي : وهو إتجاه إرادة المجرم بدون إكراه أو إرغام إلى القيام بجريمة المساس بأنظمة الإلكترونية للمؤسسات المالية وقد تثار إشكالات في هذا الركن في حالة كان لموظف البنك علاقة بالجريمة سواء بالإيجاب أو بالسلب ومعرفة هل تم إبتزازه أو إكراهه لتسهيل جريمة الإختراق على المجرمين وكذا في حالة قيام الموظف بموجب عمله بأحداث ضرر غير عمدي أدى لإتلاف معلومات أو حذفها عن غير قصد .

رابعا : الركن الخاص بهاته الجريمة وهي العنصر الإلكتروني حيث أن هاته الجريمة ليست جريمة تقليدية وبتالي لتكيفيها يجب أن تكون الوسيلة المستخدمة فيها إما هاتف ذكي أو جهاز حاسوب أو أي وسيلة أخرى معلوماتية أما الشرط الأخر أن يكون النظام الألي للمؤسسة المالية هو المستهدف .

ثالثا : أمثلة عن الهجمات السيبرانية التي إستهدفت الأنظمة الرقمية لبعض المؤسسات المالية في العالم

لقد شهد المجتمع الدولي عدة سوابق إجرامية تعرضت من خلالها المؤسسات المالية وبالتحديد البنوك و المصارف في بعض الدول لهجمات سيبرانية :

فقد ذكرت الصحيفة المالية الروسية "كوميرسانت" أن الهاكرز نجحوا في تحويل 58 مليون روبل من حسابات المصرف الروسي "بير بانك "، لدى البنك المركزي الروسي إلى بطاقات مصرفية ، و في حوادث مشابهة داخل روسيا ذكرت جريدة "الفايننشيال تايمز"، أن "قراصنة الإنترنت في روسيا نفذوا عمليات سطو إلكتروني على 240 مصرفاً روسياً في العام 2017 وسرقوا حوالى 17 مليون دولار منها خلال هذه العمليات."

وأكد المصرف الروسي حدوث الهجمة الإلكترونية، التي تعد الأولى خلال العام الجاري. وقالت رئيسة مجلس إدارة مصرف "بير بانك"، أولغا كولوسوفا، إنه يصعب تقدير حجم الخسائر بدقة، لأنه تمت استعادة جزء من الأموال المسروقة، لكن الجزء الأكبر قد سرق.

وعن كيفية وقوع العملية، أشارت المسؤولة إلى أن القراصنة قاموا بتحويل الأموال المسروقة إلى بطاقات مصرفية شخصية صادرة عن 22 بنكاً تندرج ضمن قائمة أفضل 50 مصرفاً في روسيا، ومن ثم جرى سحب الأموال عبر ماكينات الصرافة الآلية في ليلة الاختراق نفسها.(5)

وفي مصر ورد بلاغ إلى الأجهزة الأمنية من إحدى شركات تحويل الأموال، بورود تحويل مالي من أحد رعايا إحدى الدول العربية قيمته 6 آلاف دولار أمريكي لشخص يحمل جنسية دولة إفريقية مقيم داخل مصر، ومع تشكيل فريق بحث، أكدت المعلومات صحة الواقعة، وأن وراء ارتكابها تشكيل عصابي مكون من 4 أشخاص جميعهم يحملون

جنسية دولة إفريقية، تخصصوا في الاحتيال على مستخدمي شبكة الإنترنت والاستيلاء على أموالهم بطرق احتيالية مختلفة.

وبعد استصدار إذن من النيابة العامة، تمكن ضباط الإدارة من ضبطهم، وعثر بمحل سكنهم على عدد من الحوالات المالية تفيد استلامهم مبالغ مالية محولة من ضحاياهم بعدد من الدول بلغت قيمتها 500 ألف دولار أمريكي، و10 بطاقات دفع إلكتروني بأسماء المتهمين منسوبة لعدد من البنوك الأفريقية يتم إيداع المبالغ المالية متحصلات نشاطهم في حساباتهم .

كما عثر على 7 هواتف محمولة وعدد من شرائح الهواتف المحمولة لشركات مصرية وأجنبية يستخدمها المتهمون في جرائمهم، وكمية من المشتريات والمقتنيات عالية القيمة وباهظة الثمن، و6 أجهزة كمبيوتر "لاب توب"، من حصيلة نشاطهم، وأموال اجنبية ومصرية، وبفحص الأجهزة المضبوطة تبين أنها تحتوي على برامج قرصنة للاستيلاء على البريد الإلكتروني، ورسائل إلكترونية إحتيالية مرسلة للآلاف من مستخدمي شبكة الإنترنت، وعدد من صور لجوازات سفر ورخص قيادة مزورة، وبرامج تخفي على شبكة الإنترنت لصعوبة تعقبهم وضبطهم، وكمية كبيرة من الملفات يحتوى كل منها على عدد هائل من عناوين البريد الإلكتروني الخاص بضحاياهم.

وبحسب "التحقيقات" أن الأجهزة الأمنية تمكنت من القبض على المتهم وزوجته الشريكة معه في ارتكاب الوقائع ، حيث اعترفا باشتراكهما مع المتهم "أ" في ارتكاب وقائع نصب مع شخص أخر أفريقي الجنسية ويدعى "أ. أ"، والمقيم بدولة أفريقية، والذى يقوم بتنفيذ التحويلات بعد اختراق البريد الإلكتروني للشركات المستهدفة، وإرسالها لها عبر "الواتس آب" ليقوم هو وزوجته بعد ذلك بإرسالها للمتهم "أ"، لكي يقوم بصرفها من البنوك باستخدام صاحب الحساب البنكى .(6)

وأعلن البنك المركزي التونسي، أن نظام سلامته المعلوماتية كشف تعرضه لهجمة سيبرانية تسببت في توقف خدمات موقعه الرسمي ، وقال البنك المركزي في بلاغ إن نظام السلامة المعلوماتية للبنك تمكن من الكشف عن هجمة سيبرانية، تمت السيطرة عليها بفضل تظافر جهود مصالح كل من البنك المركزي والوكالة الوطنية للسلامة المعلوماتية.

وأكد أن جميع المعطيات المتعلقة بالنظام المعلوماتي للبنك المركزي لم تخترق وظلت سليمة، بالرغم من تسجيل المؤسسة بعض الاضطرابات على مستوى عدد من أنشطتها ومن بينها الموقع الإلكتروني الرسمي.

ولم يكشف البنك المركزي عن مصدر الهجمة، في حين قالت مصادر مصرفية لـ"العربي الجديد" إن توقف الخدمات شمل أيضا منظومة التحويل ما بين المصارف وشركات الوساطة بالبورصة. وأكد أن منظومات التحويل بين البنوك تعطلت أيضا فيما تواصلت التحويلات العادية ومختلف العمليات البنكية التي تؤمن الخدمات الأساسية للعملاء.

وفي فبراير 2021، تمت محاولة قرصنة إلكترونية للأنظمة المعلوماتية لأكبر بنك تجاري خاص في تونس، حيث تناقلت وسائل إعلام محلية حينها أنباء عن هجوم قراصنة على أنظمة البنك العربي الدولي ومطالبتهم بفدية قدرها 60 مليون يورو مقابل عدم المساس بقاعدة البيانات البنكية، غير أن إدارة البنك أنكرت حينها تعرّض

أنظمتها للقرصنة، مؤكدة أن الأمر لا يتعدى خللا فنيا، وأنه جرى ضمان استمراريّة كل الخدمات البنكيّة في أفضل الظروف.(7)

ومن خلال تبعات الحرب الروسية الأوكرانية التي مازالت مستمرة إلى غاية كتابة هذا المقال أعلن مصرف "سبيربنك" الروسي أنه تمكن من إحباط هجوم سيبراني واسع النطاق استهدف بطاقات العملاء والزبائن من قبل مطور تطبيقات أوكراني، حاول شطب الأرصدة من قاعدة بيانات العملاء .

وقال ستانيسلاف كوزنتسوف نائب رئيس مجلس إدارة المصرف إن الهجوم السيبراني استهدف العديد من المواطنين الروس الذين لديهم بطاقات مصرفية صادرة عن البنك، بعد بدء العملية الخاصة العسكرية الروسية. وأن المصرف تمكن من إحباط عمليات سحب للأموال من بطاقات عملائه واسعة النطاق بلغ عددها عشرات الآلاف في الدقيقة. مؤكدا أن المتابعة والتحقيقات أظهرت أن الهجوم شنته شركة أوكرانية تعمل على تطوير تطبيقات الهاتف المحمول.

وأوضح أن هذه الشركة، التي لديها نحو 50 تطبيقا رسميا مختلفا، قامت بجمع وتخزين بيانات البطاقات المصرفية لعملائها، مخالفة شروط أنظمة الدفع الدولية.(8)

المحور الثاني : العلاقة بين جريمة إستهداف الأنظمة الإلكترونية البنكية وتمويل الإرهاب

لمعرفة العلاقة بين المساس بالأنظمة الألية البنكية وتمويل الإرهاب سنركز على ثلاث نقاط في هذا المحور :

- أولا : التمييز بين أسباب الدافعة للإستهداف الأنظمة الإلكترونية البنكية
- ثانيا : طرق تمويل الإرهاب عبر جريمة إستهداف الأنظمة الرقمية للبنوك والمصارف
- ثالثا : مثال عن المباحثات بين البنوك العربية والأمريكية للحد من إستغلال المصارف في عمليات تمويل الإرهاب

أولا التمييز بين أسباب إستهداف الأنظمة الإلكترونية البنكية :

تتنوع أسباب ودوافع إرتكاب جريمة المساس بالأنظمة الإلكترونية للبنوك والمصارف لهذا يجب التمييز بينها لمعرفة ما يكون الغرض منه تمويل الإرهاب تحديدا وما يكون في إطار الجريمة العادية ، قالت الأستاذة أمل المرشدي في مقالها مفهوم الجرائم الإلكترونية و أثرها على البنوك: إن ارتكاب هذه الجريمة يتم في الغالب لأسباب شخصية أو سياسية أو اقتصادية وتقوم النفوس المريضة و الإجرامية بالتعدي على البنوك أو غيرها، للحصول على بعض المعلومات بقصد نشرها أو كشفها لجهات معينة أو للجمهور وذلك لأسباب سياسية بقصد إحراج الحكومة مثلا أو بغرض الابتزاز و طلب المال من البنوك أو الشركات أو غيرهم. وهناك من يتعدى بغرض تقديم المعلومات للبنوك أو لجهات أخرى منافسة أي بغرض الجاسوسية أو بغرض الإرهاب الاقتصادي أو السياسي...الخ .(9)

وإذا أردنا حصر هاته الأسباب و الدوافع نجدها لا تخرج عن أربعة عناصر هي :

- الإستهداف لأجل أغراض سياسية
- الإستهداف لأجل أغراض تجارية

- الإستهداف لأجل أغراض فردية كالسرقة والإبتزاز
- الإستهداف لأجل أغراض إرهابية

وأهمية التمييز بين أسباب إستهداف الأنظمة الإلكترونية البنكية تساهم أساسا في مساعدة صناع النصوص القانونية في حصر الحالات التي تدخل ضمن نطاق الجرائم العادية أو الجرائم الإرهابية وتصنيفها كجنح أو جنايات مما يسهل على الجهات القضائية والأمنية التعامل مع هكذا الجرائم على أرض الواقع .

ثانيا : طرق تمويل الإرهاب عن طريق إستهداف الأنظمة الرقمية للبنوك والمصارف

تتنوع والأساليب التي تنتهجها الجماعات الإرهابية للإستهداف الأنظمة الألية للبنوك والتي يكون الغرض منها تمويل التنظيمات الإرهابية بطريقة مباشرة أو غير مباشرة وتشكل كل واحدة منها جريمة مستقلة :

أولا : جريمة إختراق النظام الإلكتروني للبنوك و المصارف والقيام بتحويلات مالية داخلية وخارجية الهدف منها دعم التنظيم الإرهابي ماليا وتعتبر هذه الجريمة أخطر أنواع الإستهداف حيث تمكن الجماعات الإرهابية من الحصول على الأموال والعملات الصعبة بطريقة مباشرة .

ثانيا : في حال عدم القدرة على القيام بتحويلات مالية تلجأ التنظيمات الإرهابية لجريمة إبتزاز البنك وتهديده بالتشهير مستغلين القدر الذي تحصلوا عليه من معلومات من خلال عملية الإختراق للنظام الرقمي للبنك ومطالبة البنك أو المصرف مقابل عدم نشر تلك المعلومات عن البنك وعملائه.

ثالثا : جريمة تعطيل النظام الأمني الإلكتروني للبنك وهذا يكون عادة الهدف منه تسهيل عمليات السطو المسلح على البنك.

رابعا : جريمة إختراق الهواتف والحواسيب الشخصية لموظفي وعمال البنك وإبتزازهم بالمعلومات والصور والفيديوهات المحصل عليها لضغط عليهم من أجل القيام بعمليات مالية مشبوهة بموجب وظيفتهم في البنك الهدف منها تمويل التنظيمات الإرهابية .

خامسا وأخيرا : مع ما تقدمه البنوك الإلكترونية من خدمات تسهل حركة الأموال من بلد لبلد ومن قارة لقارة بضغطة زر واحدة قد تستغل تلك الخدمات من طرف التنظيمات الإرهابية في تحويل الأموال فيما بينها أو بينها وبين الممولين لها وهذا يكون عادة عن طريق تبيض تلك الأموال تحت غطاء أنشطة تجارية وهمية .

ثالثا : مثال عن المباحثات بين البنوك العربية والأمريكية للحد من إستغلال المصارف في عمليات تمويل الإرهاب في تقرير لمؤسسة إتحاد المصارف العربية بعنوان : "مكافحة تمويل الإرهاب والفساد والعلاقة مع البنوك المراسلة" والذي كان حول مؤتمر الحوار المصرفي العربي – الأميركي حول البنوك المراسلة PSD 2017 في مقر البنك المركزي الفدرالي الأميركي، نيويورك، بالولايات المتحدة الأميركية، وهو يُعتبر أكبر تجمع مصرفي عربي – أميركي يُنظمه إتحاد المصارف العربية، وذلك يوم الاثنين 16 تشرين الأول/ أكتوبر 2017، حيث حضره 500 شخصية مصرفية، بالتعاون مع جمعية المصرفيين العرب في شمال أميركا ABANA .

وجمع المؤتمر الذي يحمل عنوان «مكافحة الإرهاب وتمكين العلاقات مع المصارف المراسلة»، عدداً كبيراً من المصرفيين العرب ومن الولايات المتحدة الأميركية مع قادة ومسؤولين من السلطات الرقابية والتنظيمية والتشريعية

الأميركية، لبحث المواضيع الراهنة حول التطورات الرقابية في ما يتعلق بالعقوبات وعلاقة البنوك المراسلة .
كما شمل البحث الإتفاقية الأخيرة لمكافحة الإرهاب، وتحديد دور المصارف تحت مظلة هذه الإتفاقية، التي وُقعت مؤخراً خلال أعمال القمة العربية الإسلامية – الأميركية، إضافة إلى عوامل قانونية تتعلق بالمعوقات القائمة أمام تبادل المعلومات، والحاجة إلى التخفيف من حدة المخاطر والتصدي للتهديد الصادر عن تمويل الإرهاب مما يُشكل ضغوطات كبيرة على المصارف. (10)

تعريف هامشي لمعنى البنوك المرسلة حيث يعرفها الأستاذ وصل الله سالم أنها : شبكة من البنوك والمؤسسات المالية الأجنبية التي يستخدمها أو يتعامل معها البنك المحلي لتقديم خدمات تحويل الأموال وتمويل التجارة الخارجية والاعتمادات المستندية وغيرها من الخدمات المالية الاخرى لصالح عملائه المحليين أو أنشطة البنك الاستثمارية الدولية.

المحور الثالث : وسائل تعزيز الأمن السيبراني للبنوك

لقد أبدى صندوق النقد الدولي رأيه حول الهجمات السبرانية التي تستهدف المؤسسات المالية حول العالم حيث أكد : أن كثير من النظم المالية الوطنية ليس مستعدة بعد للتعامل مع تلك الهجمات، كما أن التنسيق الدولي لا يزال ضعيفا. وفي بحث جديد لخبراء الصندوق*، اقترح ست استراتيجيات أساسية من شأنها تقوية الأمن السيبراني بدرجة كبيرة وتحسين الاستقرار المالي على مستوى العالم نذكر منها :

أولا : إعداد الخرائط السيبرانية والتحديد الكمي للمخاطر

يمكن الخروج بفهم أفضل لأوجه الاعتماد المتبادل في النظام المالي العالمي عن طريق إعداد خرائط لأهم الروابط التشغيلية والتكنولوجية المتبادلة والبنية التحتية ذات الأهمية الحرجة. ذلك أن إدماج المخاطر السيبرانية بصورة أفضل في تحليل الاستقرار المالي من شأنه تحسين القدرة على فهم المخاطر على مستوى النظام وتخفيف حدتها.
وسيساعد التحديد الكمي للأثر المحتمل على تركيز الاستجابة وتشجيع الالتزام بهذه القضية على نحو أقوى. ولا يزال العمل في هذا المجال وليدا – وهو ما يرجع في جانب منه إلى نقص البيانات المتعلقة بأثر الأحداث السيبرانية والتحديات التي تعترض عملية النمذجة – إلا أنه يتعين تسريع وتيرته بما يتوافق مع أهميته المتنامية.

ثانيا : تقارب القواعد التنظيمية

ستؤدي زيادة الاتساق الدولي في مجال التنظيم والرقابة إلى تخفيض تكاليف الامتثال وبناء منبر لتعاون أقوى عبر الحدود. وقد بدأت جهود تعزيز التنسيق وزيادة التقارب من جانب جهات دولية، مثل مجلس الاستقرار المالي ولجنة المدفوعات والبنى التحتية للأسواق المالية ولجنة بازل. وينبغي للسلطات الوطنية أن تعمل معا من أجل التنفيذ.

ثالثا : القدرة على الاستجابة

في ظل شيوع الهجمات السيبرانية بشكل متزايد، يجب أن يكون النظام المالي قادرا على استئناف عملياته بسرعة حتى في مواجهة هجمة ناجحة، بحيث يحمي الاستقرار. ولا يزال ما يسمى باستراتيجيات الاستجابة ومعاودة النشاط في طور النشأة، ولا سيما في البلدان منخفضة الدخل، ومن ثم تحتاج إلى دعم في تطويرها. ومن الضروري وضع ترتيبات دولية لدعم الاستجابة ومعاودة النشاط في المؤسسات والخدمات العابرة للحدود.

رابعا : الرغبة في العمل المشترك

من شأن زيادة تبادل المعلومات بشأن التهديدات والهجمات والاستجابات عبر القطاعين العام والخاص أن تعزز القدرة على الردع والاستجابة بشكل فعال. غير أن هناك حواجز كبيرة باقية، وغالبا ما تكون ناشئة عن شواغل الأمن الوطني وقوانين حماية البيانات. وعلى الأجهزة الرقابية والبنوك المركزية أن تضع بروتوكولات وممارسات لتبادل المعلومات من شأنها العمل بفعالية في ظل هذه القيود. ومن الممكن تخفيض الحواجز القائمة من خلال نموذج متفق عليه عالميا لتبادل المعلومات، وزيادة استخدام منصات المعلومات المشتركة، وتوسيع الشبكات التي تحظى بالثقة.

خامسا : ردع أقوى

ينبغي أن تصبح الهجمات السيبرانية أكثر تكلفة وخطرا من خلال إجراءات فعالة لمصادرة عائدات الجريمة ومقاضاة المجرمين. ومن شأن تعزيز الجهود الدولية لمنع المهاجمين وتعطيلهم وردعهم أن يقلص المخاطر من منبعها. ويتطلب هذا تعاونا وثيقا بين أجهزة إنفاذ القانون والسلطات الوطنية المسؤولة عن البنية التحتية الحيوية أو عن الأمن، عبر البلدان والهيئات المعنية. ولما كان القراصنة لا يعترفون بالحدود، فإن مواجهة الجريمة العالمية تتطلب إنفاذا عالميا للقوانين المتفق عليها.

سادسا : تنمية القدرات

ستؤدي مساعدة الاقتصادات النامية والصاعدة على بناء القدرات في مجال الأمن السيبراني إلى تعزيز الاستقرار المالي ودعم الشمول المالي. والبلدان منخفضة الدخل معرضة بشكل كبير للمخاطر السيبرانية. وقد أبرزت أزمة جائحة كوفيد-19 الدور الحاسم الذي يقوم به الربط الإلكتروني في العالم النامي. وستظل الاستفادة من التكنولوجيا بشكل يحفظ الأمن والسلامة قضية محورية في التنمية ومعها الحاجة إلى ضمان معالجة المخاطر السيبرانية. وعلى غرار أي فيروس، فإن تكاثر التهديدات السيبرانية في أي بلد يجعل بقية العالم أقل أمانا. وستتطلب معالجة كل هذه الثغرات جهدا تعاونيا من الأجهزة المعنية بوضع المعايير، والهيئات التنظيمية الوطنية، وأجهزة الرقابة، واتحادات الصناعات، والقطاع الخاص، وجهات إنفاذ القوانين، والمنظمات الدولية وغيرها من مقدمي خدمات تنمية القدرات والجهات المانحة. ويركز الصندوق جهوده على مساعدة البلدان منخفضة الدخل، من خلال تقديم خدمات تنمية القدرات لأجهزة الرقابة المالية، وإبراز قضايا هذه البلدان ومنظوراتها للأجهزة الدولية وفي سياق المناقشات المعنية بالسياسات التي لا تحظى فيها هذه البلدان بالتمثيل الكافي. (11)

وأكد خالد ممدوح العزي في مقاله أنه : " لمواجهة هذه التحديات لم يكن أمام المصارف سوى العمل الجاد لتقبل هذه المخاطر، مما يستوجب عليها مسؤوليات كبيرة لمواجهتها من خلال تبني إدارة مخاطر شاملة لتحديد هوية هذه المخاطر، والحد منها من خلال الوسائل الرقابية ووضع السياسات العملية المناسبة لمواجهتها وهو ما تبنته التوصية الأوروبية الصادرة عام1988 لمسؤولية البنك على أساس تحمل المخاطر . حيث تنص المادة 71 / من التوصية الأوروبية 88 /11/ 1 بشان العلاقة بين مصدري النقود الالكترونية والمستهلكين على أن البنك مسؤول أمام

المستهلك على نتائج عدم التنفيذ أو التنفيذ الخاطئ للعمليات المحددة في المادة الأولى من هذه الاتفاقية خاصة إذا تم تنفيذ هذه العمليات من خلال جهاز الكتروني لا يقوم البنك برقابته بشكل مباشر أو بشكل منفرد(12)

خاتمة :

لقد توسع نطاق الجريمة الإلكترونية عما كانت عليه من قبل ولم تعد تقصر فقط على جرائم متفرقة نادرة هنا وهناك و يقوم بها فقط الهاكرز بل إتسع نطاقها تزامنا مع توسع إستخدام التكنولوجيا الحديثة التي شملت جميع مناحي الحياة خاصة في الجانب المالي و الإقتصادي والذي أصبح يعتمد في جل الخدمات التي يقدمها على الأنظمة الرقمية مما جعلها عرضة للهجمات السيبرانية للأغراض كثيرة من بينها عمليات سرقة الأموال والتي قد تستخدم في عمليات تمويل الإرهاب ، ومما سبق يمكن نستخلص النتائج التالية :

- إتساع نطاق الجريمة الإلكترونية ودخولها مرحلة الجريمة المنظمة .
- نقص وقصور الجانب التشريعي في مواجهة الهجمات السيبرانية ضد البنوك والمصارف في بعض الدول .
- تركيز البنوك على توفير الخدمات الرقمية لتحقيق الأرباح مع إهمال جانب الأمن السيبراني
- تعدد دوافع وأسباب إستهداف المؤسسات المالية والتي قد تكون تجارية أو فردية كالسرقة أو سياسية أو حتى إرهابية .
- ظهور علاقة وطيدة بين السرقة الإلكترونية للبنوك وبين تمويل الإرهاب .
- نقص التأطير والتكوين في جانب الأمن السيبراني لدى موظفي البنوك .
- عدم إنتشار الوعي بأخطار السرقة الإكترونية لدى الزبائن و المتعاملين مع البنوك من خلال قرصنة هواتفهم من أجل الحصول على الأرقام السرية للحسابات البنكية .

ومن خلال هذه الدراسة نقترح ما يلي :

- سن نصوص قانونية خاصة بالجرائم الإلكترونية الماسة بالأنظمة الألية للبنوك والمصارف
- إلزام المؤسسات المالية بإقتناء أحدث الأنظمة الأمنية السيبرانية الحديثة لمواجهة الهجمات الإلكترونية .
- رفع كفاءة وجاهزية موظفي البنوك وخاصة في الجانب الأمن المعلوماتي سواء في هواتفهم وحواسيبهم الشخصية أو الأجهزة الإكترونية الخاصة بالبنك .
- تكثيف التعاون وتبادل الخبرات بين البنوك سواء الوطنية أو الإقليمية أو الدولية في مجال الأمن السيبراني .
- إختبار الأنظمة الأمنية الإلكترونية من حين لأخر لتكون في تمام الجاهزية لصد أي هجوم سيبراني على البنك أو المصرف .

الهوامش :

1- مداخلة خالد ممدوح العزي بعنوان : الجرائم المالية الإلكترونية الجرائم المصرفية أنموذجا | مؤتمر الجرائم الإلكترونية المنعقد في طرابلس/ لبنان، يومي 24-25|03|2017، على موقع مركز جيل للبحث العلمي تاريخ الإطلاع 2022/05/28 على الرابط : https://jilrc.com/archives/6192

2- المرسوم الملكي رقم م/17 بتاريخ 8 / 3 / 1428 الخاص بنظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية.

3- قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 المؤرخ في 2018 المادة 23 الجريدة الرسمية العدد 23 مكرر ج.

4- كلمة الدكتور عبدالرحمن بن عبدالله الحميدي المدير العام رئيس مجلس إدارة صندوق النقد العربي في افتتاح ورشة العمل حول مواجهة التهديدات الإلكترونية في الخدمات المالية في الدول العربية منشورة على موقع صندوق النقد العربي بتاريخ 2021/12/08 تاريخ الإطلاع 2022/05/30 على الرابط :

https://www.amf.org.ae/ar/news/08-12-2021/maly-aldktwr-bdalrhmn-bn-bdallh-alhmydy-almdyr-alam-ryys-mjls-adart-sndwq-alnqd-0

5- مقال صحفي على موقع العربي الجديد بعنوان : "هاكرز" يسطون على بنك روسي ويسرقون 58 مليون روبل" تاريخ النشر بتاريخ 06 يوليو 2018 تاريخ الإطلاع 2022/05/28 على الرابط :

https://www.alaraby.co.uk/"هاكرز"-يسطون-على-بنك-روسي-ويسرقون-58-مليون-روبل

6- مقال علاء رضوان على جريدة البوم السابع المصرية بعنوان : (تفاصيل 8 ساعات تحقيقات مع "العصابة الدولية" للنصب الإلكترونى.. المتهمون الأربعة يحملون جنسية دولة أفريقية.. والاتهامات تتضمن القرصنة الإلكترونية على حسابات البنوك والشركات.. والعمليات تمت عبر رسائل "الواتس آب) تاريخ النشر الجمعة، 30 يوليو 2021 05:30 م تاريخ الإطلاع 2022/05/28 على رابط :

https://www.youm7.com/story/2021/7/30/5407062/تفاصيل-8-ساعات-تحقيقات-مع-العصابة-الدولية-للنصب-الإلكترونى-المتهمون

7- مقال إيمان الحامدي على موقع العربي الجديد بعنوان : "هجوم إلكتروني يعطل موقع البنك المركزي التونسي" تاريخ النشر 24مارس 2022 تاريخ الإطلاع 2022/06/02 على الرابط :

https://www.alaraby.co.uk/economy/التونسي/هجوم-إلكتروني-يعطل-خدمات-موقع-البنك-المركزي-

8- مقال على موقع روسيا اليوم بعنوان : " مصرف "سبيربنك" الروسي يحبط هجوما سيبرانيا أوكرانيا استهدف أرصدة عملائه" تاريخ النشر 18.04.2022 تاريخ الإطلاع 2022/06/01 على الرابط :

https://arabic.rt.com/russia/1345322-سبير-بنك-يبطل-هجوما-واسع-النطاق-من-قبل-مطور-تطبيقات-أوكراني-استهدف-بطاقات-بنكية

9- مقال الأستاذة أمل المرشدي: " مفهوم الجرائم الإلكترونية و أثرها على البنوك " على موقع المحاماة نت تاريخ النشر 3مارس، 2017 تاريخ الإطلاع 2022/06/05 على الرابط :

https://www.mohamah.net/law/مقال-قانوني-هام-يوضح-مفهوم-الجرائم-الإ

10-تقرير مؤسسة إتحاد المصارف العربية بعنوان : "مكافحة تمويل الإرهاب والفساد والعلاقة مع البنوك المراسلة" العدد 440 بدون تاريخ نشر تاريخ الإطلاع 2022/05/28 على الرابط :

https://uabonline.org/ar/مكافحة-تمويل-الإرهاب-والفساد-والعلاق

11-جنيفر إليوت ونايجل جنكينسون خبراء صندوق النقد الدولي دراسة بعنوان : " المخاطر السيبرانية ... التهديد الجديد للاستقرار المالي " ، تاريخ النشر 7ديسمبر 2020 الموقع الإلكتروني الرسمي لصندوق النقد الدولي تاريخ الإطلاع 2022/06/11 :

https://www.imf.org/ar/News/Articles/2020/12/07/blog-cyber-risk-is-the-new-threat-to-financial-stability

12-خالد ممدوح العزي : الجرائم المالية الإلكترونية الجرائم المصرفية أنموذجا | مداخلة في مؤتمر الجرائم الإلكترونية المنعقد في طرابلس/ لبنان، يومي 24-25|03|2017، على موقع مركز جيل للبحث العلمي تاريخ الإطلاع 2022/05/28 على الرابط : https://jilrc.com/archives/6192

قائمة المراجع :

1- مداخلة خالد ممدوح العزي بعنوان : الجرائم المالية الإلكترونية الجرائم المصرفية أنموذجا | مؤتمر الجرائم الإلكترونية المنعقد في طرابلس/ لبنان، يومي 24-25|03|2017، على موقع مركز جيل للبحث العلمي على الرابط : https://jilrc.com/archives/6192

2- المرسوم الملكي رقم م/17 بتاريخ 8 / 3 / 1428 الخاص بنظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية.

3- قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 المؤرخ في 2018 المادة 23 الجريدة الرسمية العدد 23 مكرر ج.

4- كلمة الدكتور عبدالرحمن بن عبدالله الحميدي المدير العام رئيس مجلس إدارة صندوق النقد العربي في افتتاح ورشة العمل حول مواجهة التهديدات الإلكترونية في الخدمات المالية في الدول العربية منشورة على موقع صندوق النقد العربي بتاريخ 2021/12/08 على الرابط :
https://www.amf.org.ae/ar/news/08-12-2021/maly-aldktwr-bdalrhmn-bn-bdallh-alhmydy-almdyr-alam-ryys-mjls-adart-sndwq-alnqd-0

5- مقال صحفي على موقع العربي الجديد بعنوان : "هاكرز" يسطون على بنك روسي ويسرقون 58 مليون روبل" تاريخ النشر بتاريخ 06 يوليو 2018 على الرابط :
https://www.alaraby.co.uk/هاكرز"-يسطون-على-بنك-روسي-ويسرقون-58-مليون-روبل"

6- مقال علاء رضوان على جريدة اليوم السابع المصرية بعنوان : (تفاصيل 8 ساعات تحقيقات مع "العصابة الدولية" للنصب الإلكترونى.. المتهمون الأربعة يحملون جنسية دولة أفريقية.. والاتهامات تتضمن القرصنة الإلكترونية على حسابات البنوك والشركات.. والعمليات تمت عبر رسائل "الواتس آب) تاريخ النشر الجمعة، 30 يوليو 2021 05:30 م على رابط :
https://www.youm7.com/story/2021/7/30/5407062/تفاصيل-8-ساعات-تحقيقات-مع-العصابة-الدولية-للنصب-الإلكترونى-المتهمون

7- مقال إيمان الحامدي على موقع العربي الجديد بعنوان : "هجوم إلكتروني يعطل موقع البنك المركزي التونسي" تاريخ النشر 24مارس 2022 على الرابط :
https://www.alaraby.co.uk/economy/التونسي

/هجوم-إلكتروني-يعطل-خدمات-موقع-البنك-المركزي-

8- مقال على موقع روسيا اليوم بعنوان : " مصرف "سبيربنك" الروسي يحبط هجوما سيبرانيا أوكرانيا استهدف أرصدة عملائه" تاريخ النشر 18.04.2022 على الرابط :

https://arabic.rt.com/russia/1345322-سبير-بنك-يبطل-هجوما-واسع-النطاق-من-قبل-مطور-تطبيقات-أوكراني-استهدف-بطاقات-بنكية

9- مقال الأستاذة أمل المرشدي: " مفهوم الجرائم الإلكترونية و أثرها على البنوك " على موقع المحاماة نت تاريخ النشر 3مارس، 2017 على الرابط :

https://www.mohamah.net/law/مقال-قانوني-هام-يوضح-مفهوم-الجرائم-الإ

10- تقرير مؤسسة إتحاد المصارف العربية بعنوان : "مكافحة تمويل الإرهاب والفساد والعلاقة مع البنوك المراسلة" العدد 440 بدون تاريخ نشر على الرابط :

https://uabonline.org/ar/مكافحة-تمويل-الإرهاب-والفساد-والعلاق

11- جنيفر إليوت ونايجل جنكينسون خبراء صندوق النقد الدولي دراسة بعنوان : " المخاطر السيبرانية ... التهديد الجديد للاستقرار المالي " ، تاريخ النشر 7ديسمبر 2020 الموقع الإلكتروني الرسمي لصندوق النقد الدولي :

https://www.imf.org/ar/News/Articles/2020/12/07/blog-cyber-risk-is-the-new-threat-to-financial-stability