اقتصاديات الأمن السيبراني
في القطاع المصرفي

إعداد

د/مروة فتحى السيد البغدادى
مدرس الاقتصاد والمالية العامة بالمعهد المصرى
لأكاديمية الاسكندرية للإدارة والمحاسبة

مقدمة:

تعتبر الصيرفة الإلكترونية جانبا هاما من جوانب التجديد في القطاع المصرفي، في خضم عديد التحديات التي يفرضها الاندماج في الاقتصاد العالمي على هذا القطاع الاقتصادي الهام، خصوصا و أن من أبرز ملامح المرحلة الراهنة المنافسة الشديدة المستفيدة من آخر ثمار تكنولوجيا الإعلام و الإتصال، قد طرأت على الساحة المصرفية تغيرات متلاحقة و بإيقاع متسارع على نحو بات معه الشكل التقليدي للبنوك محل تهديد، و قد أصبحت الأعمال التي تقوم بها البنوك على درجة كبيرة من التعقيد و بصورة غير مسبقة تستلزم الاهتمام أكثر بقضية إدارة المخاطر، حيث أن القطاع المالي -ضمنيا المصرفي- من أكثر القطاعات الاقتصادية تعرضا للمخاطر، لاسيما المخاطر المستقبلية منها، و من هنا ازداد الوعي بأهمية سلامة النظام المصرفي واستقراره بعد أن أكدت البحوث الاقتصادية أنهما يعتبران شرطا أساسيا لتحقيق التخصيص الأفضل للموارد المالية في الاقتصاد، وذلك بترقية ممارسات إدارة المخاطر لدى البنوك.

منذ ربع القرن الماضى، برزت أعمال لجنة بازل الدولية اتجاه مجتمع الأعمال المصرفية بمقترحات يمكن أن يقال عنها معايير دولية، إن لم تكن ملزمة قانونيا أو تنظيميا إلا أن هذه الهيئة تحظى بالقيمة الأدبية المعنوية ، حيث تستهدف هذه اللجنة بأعمالها: ترقية ممارسات البنوك إزاء المخاطر، حماية حقوق المودعين وتحقيق الاستقرار في المنظومة المصرفية وتطهيرها من المنافسة غير الشريفة الناتجة عن فوارق في الإشراف على البنوك بين الدول. فكانت من أبرز جهود اللجنة لخدمة الصناعة المصرفية اتفاقية بازلI عام ١٩٨٨ واتفاقية بازلII عام ٢٠٠٤، على غرار توصيات أصدرتها اللجنة منذ نشأتها لتوضيح أطر أو للتعبير عن رأيها في مسائل جاثمة في تلك الفترة، أيضا انشغالها بالمخاطر التي تكتنف من يزاول أنشطة البنوك

الإلكترونية بما أضحت تخلفه من آثار وخيمة على استقرار النظام المالي و صلابته، فأصدرت جملة من المعايير للرقابة المصرفية إلى سلطات الرقابة في أصقاع العالم من أجل الاسترشاد بها في وضع قواعد احترازية بصددها.

يشهد قطاع الخدمات المالية هجمات سيبرانية تفوق القطاعات الأخرى بنسبة ٦٥ % وفق تقديرات البنك الدولى ، وقد تصل تكلفة الهجمات السيبرانية في قطاع الخدمات المالية إلى ما يقدر بنحو ٢٧٠ إلى ٣٥٠ مليار دولار سنوياً حال اتساع نطاق انتشارها وفقا لتقديرات صندوق النقد الدولي الامر الذى دفع المصارف المركزية العربية إلى تشديد التعليمات الرقابية والتى تُلزم المصارف بوضع لائحة من التعليمات لتأمين التطبيقات الإلكترونية، ومن أهمها تثبيت برامج الحماية ضد الاختراق.([1])

ومع استمرار تقنيات المعلومات والاتصالات في الابتكار في إيجاد وتقديم طرق جديدة للوصول إلى العملاء، فإن تلك المؤسسات تتعرض في الوقت نفسه لمخاطر جديدة. حيث أن الاستخدام الضار لتقنية المعلومات والاتصالات يمكن أن يؤدي إلى تعطيل الخدمات المالية الضرورية للأنظمة المالية الوطنية والدولية، وتقويض الأمن والثقة، وتعريض الاستقرار المالي للخطر. إن الهجمات السيبرانية تشكل تهديدًا للنظام المالي بأكمله، وهي حقيقة تؤكدها التقارير الصادرة في هذا الشأن على المستوى الدولي والإقليمي والمحلي.

فقد بلغت نسبة العملاء الذين عانوا من الهجمات السيبرانية خلال عام ٢٠١٦ نحو٦٥ %، بنسبة زيادة قدرها حوالي ٢٩ % مقارنة بالعام السابق وذلك وفقاً للتقرير الصادر عن البنك الدولي في هذا الشأن. نتيجة لذلك، واعترافاً بالتهديدات الناجمة عن المخاطر السيبرانية، ومدى أهمية تعزيز قدرة الأجهزة المصرفية على

(١) صنـــدوق النقد العربي: سلسلة "موجز سياسات" حول " أمن الفضاء السيبراني في القطاع المصرفي، العدد الرابع ، 08-07-2019 "

تحمل هذه المخاطر والتحوط منها، فقد اتخذت السلطات الرقابية على مستوى العالم خطوات تنظيمية وإشرافية تهدف إلى تجنب أثر تلك المخاطر السيبرانية على المصارف. في هذا الصدد قامت المصارف المركزية العربية بإصدار التعليمات المصرفية التي تحث فيها البنوك على تعزيز قدراتها لمواجهة تلك الهجمات الإلكترونية.

هدف البحث:

تستهدف الدراسة إبراز التحديات التي تواجه المجتمع من أجل تحقيق الأمن السيبراني، والذى يلعب دورًا محوريًا في معالجة التحديات المستقبلية نظرًا لاستخدامه كتكنولوجيا لإدارة الشبكات. الامر الذى يساعد في تحقيق عدد من أهداف التنمية المستدامة: كتحسين إدارة استخدام المعدات وصيانتها، وزيادة الإنتاج الزراعي، وتوسيع نطاق الوصول إلى المعلومات المتعلقة بالتفاعل الاقتصادي بين المؤسسات الخاصة والعامة (الهدف التاسع).

أهمية الدراسة:

هو إلقاء الضوء على الدور المنوط بالدولة في عصر تسوده العولمة الالكترونية حتى تخرج من النمط الكلاسيكي إلى النمط الحديث القائم على التصدي لهذه الظاهرة الخطيرة والوقاية منها ، لهذا تتجلي الأهمية في تطوير الدولة لمنظومتها ماديا وبشريا لكبح جماح تطورها والسيطرة عليها بوضع سياسة جنائية وفق أجهزة ومنظومة تشريعية.

منهج البحث:

لقد اعتمدنا في معالجة هذا الموضوع المنهج التحليلي و المقارن، وهذا يعطينا دفعا للنظر في الموضوع من جميع جوانبه وتحليل عناصره، وتتبع مراحل تطوره.

الإشكالية الاقتصادية : ماهي مظاهر تهديدات الامن السيبرانى على المصارف الالكترونية ، وهل هناك جهود لمكافحة تلك التهديدات لاستقرار التنمية الاقتصادية ؟

مشكلة البحث:

على ضوء ما سبق، يتبلور لدينا التساؤل التالي: إلى أى مدى يمكن تحقيق الأمن السيبرانى فى العمليات المصرفية الإلكترونية ؟ إلى أي مدى يمكن أن تساهم عمليات البنوك الالكترونية في تحسين الخدمة البنكية؟ما المخاطر المرتبطة بالعمليات البنكية الإلكترونية؟ كيف تتحوط البنوك الإلكترونية من مخاطرها؟

خطة البحث:

المبحث الاول: ماهية الأمن السيبراني

المطلب الاول : مفهوم و أبعاد الأمن السيبراني

المطلب الثانى : ما هية المخاطر السيبرانية " المفهوم-الطبيعة -الأنواع "

المبحث الثانى : تهديدات الأمن السيبراني للمصارف الإلكترونية وآليات مواجهتها

المطلب الأول : ماهية المصارف الإلكترونية

المطلب الثاني : طبيعة مخاطر وتهديدات الأمن السيبراني فى المصارف الإلكترونية

المطلب الثالث : إدارة مخاطر العمليات المصرفية الإلكترونية

المبحث الثالث: آليات تعزيز الأمن السيبرانى فى المصارف الإلكترونية

المطلب الاول: معوقات تعزيز الأمن السيبرانى فى المصارف الإلكترونية

المطلب الثانى: آليات تعزيز الأمن السيبرانى فى المصارف الإلكترونية

المبحث الاول
ماهية الأمن السيبراني

تمهيد:

يعتبر الأمن الركيزة الاساسية للمجتمع، بحيث لا يمكن تصور نمو أي نشاط بعيدا عن تحققه، سواء اكان ذلك، على المستوى التقني، أم على المستوى القانوني. وقد تحول الأمن ، مع بروز مجتمع المعلومات، والفضاء السيبراني، إلى واحد من أهم القطاعات الخدمية التي تشكل قيمة مضافة، ودعامة أساسية، لأنشطة الحكومات والأفراد، على السواء، كما هو الحال، مع التطبيقات الخاصة بالحكومة الإلكترونية، والصحة الإلكترونية، والتعليم عن بعد، والإستعلام، والتجارة الإلكترونية، وغيرها الكثير.

إلا أن الوجوه المتعددة للأمن السيبراني، ومضاعفاتها الخطيرة التي لا تقف عند حدود الاساءة إلى الأفراد والمؤسسات، بل تتعداها إلى تعريض سلامة الدول والحكومات تزيد مهمة القائمين على الموضوع تعقيدا وصعوبة. وتستدعي مقاربة شاملة ومتكاملة لجميع التحديات التي يطرحها الفضاء السيبراني، بحيث تأتي الردود والحلول المقترحة ناجحة وفاعلة. فى تحقيق الأمن وبناء الثقة في الفضاء السيبيراني.

من أساسيات تسخير تقنيات المعلومات والاتصالات، في مجالات التنمية خدمة للمجتمعات الانسانية، على ما جاء في التوصيات الصادرة عن القمة العالمية لمجتمع المعلومات والمنعقدة في تونس عام ٢٠٠٥. لذلك، لا بد من التوقف بداية، عند ماهية الأمن السيبراني، والأخطار السيبرانية، لنستعرض بعدها

أبعاد هذا الامن،، وما يرتبط به من تحديات، مع التركيز على الاطارين التشريعي والتنظيمي في العالم العربي، والصعوبات الأكثر بروزا، لنصل الى أساسيات المواجهة، والمقترحات.

المطلب الاول

مفهوم وأبعاد الأمن السيبراني

مفهوم الأمن السيبراني

يعطى الامن، تعريفات عديدة، تنطلق من الإمكانات العسكرية، مرورا بالحفاظ على استقرار النظام، وصولا إلى حماية القيم الجوهرية لمجتمع ما. لكن وبغض النظر، عن تقارب أو اختلاف النظرات الفلسفية والسياسية للموضوع، فإن المؤكد هو القلق الذي ينتاب معظم الدول حاليا من تعرض أمنها القومي للاعتداءات السيبرانية.لاسيما وأن تقنيات المعلومات والاتصالات قد رفعت مستوى الخطر عبر اتاحتها لمصادر جديدة متعددة، فضلا عن الإمكانات الهائلة لتحقيق هذا الخطر، مقابل انخفاض نسبة المخاطر وإمكانية اكتشاف الجهة المعتدية.

وذلك، نتيجة للتنسيق المتبادل بين إدارات الامن والاقتصاد. فضلا عن الترابط الذي يجمع بين أمن الفضاء السيبيراني، والاقتصاد والامن القومي.

فقد اعتبر المسؤول السابق عن الأمن الوطني الاميركي مايكل ماكونال، أن الانترنت، قد رفعت مستوى الأخطار التي يتعرض لها النظام بشكل غير مسبوق([1]).

(1) McConnell said the Internet has "introduced a level of vulnerability that is unprecedented." Cybersecurity starts at home and in the office. http://www.google.com:80/hostednews/ap/article/ALeqM5gkZ5sKNT86kqT9TWeDlogVPoASyQD9B469980

وفى ذلك اشارة واضحة الى التهديدات الجديدة التي تستهدف الأمن القومي والتي يمكن أن تتخذ أشكالا غير متوقعة تتعلق مجالات أساسية وحيوية.

فالأمن السيبراني وفقا لما ورد في التقرير الصادر عن الاتحاد الدولي للاتصالات حول "اتجاهات الاصلاح في الاتصالات للعام ٢٠١٠-٢٠١١ هو" مجموعة من المهمات، مثل تجميع وسائل، وسياسات، واجراءات امنية، ومبادىء توجيهية، ومقاربات لادارة المخاطر، وتدريبات، وممارسات فضلى، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين" [١].

و يمكن تعريف الامن السيبراني استنادا لأهدافه بأنه" النشاط الذي يؤمن حماية الموارد البشرية، والمالية، المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن امكانات الحد من الخسائر والاضرار، التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح اعادة الوضع الى ما كان عليه، باسرع وقت ممكن، بحيث لا تتوقف عجلة الانتاج، وبحيث، لا تتحول الاضرار الى خسائر دائمة".([٢])

(1)Trends in Telecommunication Reform 2010-11- ITU-" The term "cyber security" refers to various activities such as the collection of tools, policies, security safeguards, guidelines, risk management approaches, training, best practices, and technologies that can be used to protect the cyber environment and the assets of organizations and Users".

(٢) د/منى الأشقر جبور: السيبرانية: هاجس العصر، دراسات وابحاث (١)، جامعة الدول العربية، المركز العربي للبحوث القانونية، بيروت،٢٠١٦، ص ٢٦ وما بعدها .

أبعاد الأمن السيبرانى:

يمتد الأمن السيبرانى ليشمل جميع المجالات الاقتصادية، والاجتماعية، والسياسية، والقانونية لكافة المجتمعات المعاصرة، واستنادا لما سبق فإن الأمن السيبرانى يرتبط ارتباطا وثيقا بسلامة مصادر الثروة والتقدم في الوقت الراهن، والتى تشمل: القدرة على الاتصال والتواصل، والبيانات والمعلومات، التي يستند عليها الانتاج، والابداع، والقدرة على المنافسة. لذا نحاول فى هذا المقام فهم أبعاد الأمن السيبراني كما يلي:([1])

١- الابعاد العسكرية:

غنى عن البيان أن بدء استخدام الانترنت قد تم في بيئة عسكرية ، ثم تطور الأمر ليشمل البعد الأكاديمي لها بهدف تطوير القدرات العسكرية والانجازات العلمية التي تضمن تقدم دولة على آخرى، خاصة في مجال تطوير الاسلحة النووية.ومن أبرز الامثلة التي يمكن عرضها في هذا المجال، لتوضيح الابعاد العسكرية للأمن السيبراني، وخطورة الهجمات السيبرانية، ما حدث في جورجيا، وكوريا الجنوبية، وإيران مثال على بعض الهجمات والاختراقات، والتي انتهت بالصراع المسلح لاحق، أوبانقطاع الاتصال بالفضاء السيبراني داخل الدولة أو التشويش على الإدارات الحكومية.

فضلا عن ذلك، فإن النتائج الكارثية، التي يمكن ان تتجسد فيها التهديدات، هي أفضل ما يمكن أن يعبر عن جدية الأمر، وحاجتنا إلى تحقيق الامن السيبرانى خاصة وأن تكلفة التقاعس يجعل النتائج أكثر سوءً .خاصة أن هذه الهجمات قد تأتي دون مقدمات، الأمر الذى يؤدى إلى عجز السلطات الحكومية عن معرفة مدى الضرر أو

---

(١) المرجع السابق مباشرة ، ص ٢٨-٣٠

حماية مواطنيها من الهجمات التالية. وهذا هو التدمير الذي يُمكن أن ينجم عن نوع جديد من الحروب هي "الحرب السيبرانية" ([1]).

٢- الابعاد الاجتماعية :

تسمح طبيعة الفضاء السيبراني المفتوحة عبر وسائل التواصل الاجتماعية لكل مواطن بالتعبير عن تطلعاته السياسية، وطموحاته الاجتماعية. كذلك تعتبر فرص ميسرة للإطلاع على الافكار والمعلومات المتباينة. مما يسمح بتبادل الخبرات، وتحقيق التعاون والتقارب بين المجتمعات المختلفة. كما أنة لا يمكن تجاهل الدور الفضاء السيبراني في تبادل المعلومات فى المجالات العلمية والثقافية، والخدمية، وفي أوقات الأزمات والكوارث،...الخ. إذ لا تقف الأبعاد الإجتماعية، عندهذة الحدود فقط، بل تتعداها إلى صيانة القيم الجوهرية في المجتمع: كالانتماء، والمعتقدات، اضافة الى العادات والتقاليد.

ومن جهة أخرى، يأتي حرص الهيئات الدولية على نشر ثقافة الأمن السيبراني، وضرورة تعاون كل فئات المجتمع على تحقيقة وضمانه. مع القدرة على التعامل بحد أدنى من قواعد السلامة، و إدراك العواقب القانونية التي يمكن أن تنتج عن التصرفات التي تعرض سلامة الافراد و الاموال للخطر.

٣- الأبعاد السياسية:

تتمثل الأبعاد السياسية للأمن السيبراني في حق الدولة في حماية نظامها السياسي، ومصالحها في وقت تؤثر التقنيات على موازين القوى داخل المجتمع نفسه،

(١) حمدون إ. توريه وآخرين:البحث عن السلام السيبراني، الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء، يناير ٢٠١١

حيث أصبح من حق المواطن الاطلاع على خلفيات ومبررات القرارات السياسية داخل بلادة ، والإطلاع على نظيرتها فى الدول الاخرى. بالمقابل، يحاول العاملون في الشأن السياسي الافادة مما تقدمه هذه التقنيات والترويج لسياساتهم في العالم. وغني عن البيان، مدى التأثير الذي يتركه هذا الامر بغض النظرعن صحة السياسات والمبادىء والمواقف التي يروج لها. إذ تستخدم الشبكات الاجتماعية بشكل كثيف فى الحملات الانتخابية.

٤- الأبعاد الاقتصادية:

يرتبط الأمن السيبيراني ارتباطا وثيقا بالاقتصاد. فالتلازم واضح بين اقتصاد المعرفة وتوسع استخدام تقنيات المعلومات والاتصالات. كما تتيح تقنيات المعلومات والاتصالات تعزيز التنمية الاقتصادية لدول كثيرة عبر إفادتها من فرص الاستخدام التي تقدمها الشركات الدولية التي تبحث عن إدارة تكلفة انتاجها بأفضل الشروط. الا أن هذا الواقع يطرح مسائل مختلفة تتعلق بحماية مقدم الخدمة أو حماية المستهلك على الانترنت.

يضاف إلى ذلك دخول العالم عصر المال الالكتروني، ضمن بيئة تقنية متحركة، إذ تتزايد استثمارات المصارف، والمؤسسات المالية، في مجال المال الرقمي. وتتنافس الشركات على اصدار تطبيقات تسمح بآليات دفع آمنة، وحفظ المال في المحفظة الالكترونية واستخدامها كرصيد افتراضي. وقد وضعت بعض الدول تشريعات خاصة بهذا المال، لما يثيره هذا الأمر من صعوبات و للحد أيضا من الجرائم الاقتصادية والمالية العابرة للحدود كتبييض الاموال، والتهرب من الضريبة. ([1])

(1) Electronic money regulations 2011 (EMR 2011) & the payment Services Regulations 2009

وهنا يثور : ما هى طبيعة العلاقة بين الأمن السيبرانى النمو الاقتصادي؟

وغني عن البيان، أن هناك علاقة قوية بين الأمن السيبرانى والنمو الاقتصادي فالامن السيبراني يضمن إقبال الأفراد على الخدمات التي تقدم بواسطة تقنيات المعلومات والاتصالات، الأمر الذى يترجم عمليا بتطوير أسس الاقتصاد. ولعل هذا هو الهدف الرئيسى لإستهداف المعلومات منذ القدم سواء من خلال عمليات التجسس الصناعي والعسكري التقليدية، أو من خلال الإعتداء على الملكية الفكرية. هذا بالإضافة إلى التأثيرات المالية السلبية التي يخلفها الإعتداء على أنظمة المعلومات وتعطيلها.

٥- الابعاد القانونية:

يرتب النشاط الفردي والحكومي في الفضاء السيبراني نتائج قانونية تتطلب اهتماما لحل النزاعات التي يمكن ان تنشأ عنها. ونظرا لنشأة مجتمع المعلومات وتطورة السريع. فقد أضيف إلى قائمة الحقوق الأساسية والحريات المعترف بها في الدساتير والتشريعات الدولية حقوقا أخرى، كحق النفاذ إلى الشبكة العالمية للمعلومات، كما توسعت بعض المفاهيم، لتشمل أساليب ممارسة واستخدام تقنيات المعلومات والاتصالات، كالحق في إنشاء المدونات الالكترونية، والحق في إنشاء التجمعات على الانترنت، و الحق في حماية ملكية البرامج المعلوماتية.

وفى المقابل ظهرت إلتزامات جديدة ذات طابع اقتصادي، كالإلتزام بحفظ بيانات الاتصالات للاشخاص الطبيعيين والمعنويين على السواء، مع ضرورة الإلتزام بحماية البيانات بالاضافة الى حماية الحق في الخصوصية.

يضاف إلى هذا، ما يتوقع من تحولات على مستوى سياسات القطاعات الصناعية، والتجارية، والتى تشهد تزايدا في الاعمال الإجرامية والممارسات غير

القانونية في الفضاء السيبراني، الأمر الذى يتطلب إعداد البيئة التنظيمية والتشريعية، وبناء قدرات هيئات المكافحة والرقابة.

المطلب الثانى

ماهية المخاطر السيبرانية " المفهوم -الطبيعة-الأنواع"

تمهيد:

سبق ورأينا إلى أن الفضاء السيبرانى لة عدة أبعاد ، أولها البعد الاقتصادي، والذى يقسم الاقتصاد السيبرانى إلي مجالين رئيسيين: المجال الأول يتعلق بصناعة تكنولوجيا المعلومات والاتصالات (ICT)، ويشمل إنتاج و تطوير الأجهزة والبرمجيات وخدمات أخري. بينما المجال الثاني فهو مجال التجارة الإلكترونية من خلال فتح سوق حر علي شبكة الإنترنت.

أما البعد الثاني فهو يتعلق بأمن المعلومات، حيث نجد أن العديد من الدول تقوم بتخصيص قيمة كبيرة من ميزانيتها لأجل مجابهة الهجمات الإلكترونية وتحديث وتطوير أنظمة الأمان لديها. أما البعد الثالث فهو البعد الأمني، وخير مثال علي ذلك هو مركز تكامل استخبارات التهديد السيبراني (CTIIC) بالولايات المتحدة الأمريكية الذي يعمل علي التنسيق بين مختلف أجهزة الأمن الأمريكية الأخري، مثل : المركز المصرى للاستجابة للطوارئ المعلوماتية ، ومكتب التحقيقات الفيدرالي، ووكالة الأمن القومي. وكذلك والهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية ([1]).

(١) د/ محمود عزت: الفضاء السيبراني وتحديات الأمن المعلوماتي العربي، المجلة العربية العدد ٤٩٨، أبريل ٢٠١٨، ص.ص ٣٥، ٣٦.

على ضوء ما تقدم، تتطلب مواجهة المخاطر السيبرانية تحديد مفهوم التصرفات التي تمثل مصادر حتمية للمخاطر السيبرانية، كذلك تحديد السلوك الواجب اتباعه، والذي ينتج عن عدم الالتزام به أو الإهمال فية مسؤولية قانونية . وذلك على النحو التالى...

أولا: مفهوم الجريمة السيبرانية

يتطلب الامر بداية، التعرف على طبيعة الجريمة السيبرانية، التي تشكل الخطر الأساسى الواجب مكافحته. واستنادا إلى مبدأ " لا جريمة ولا عقاب دون نص" عمدت العديد من الدول الى وضع نصوص قانونية خاص بهذة الجرائم، التي يمكنها ان تشمل قطاع واسع من الاعمال غير الشرعية، كتلك التي تستخدم أجهزة الكمبيوتر والشبكات كوسيلة لتنفيذ الجريمة، أو كهدف لها بدءا من عمليات اختراق الانظمة المعلوماتية وأنظمة الاتصالات، وصولا الى الهجمات التي تعطل الخدمات.

إلا أن عدم وجود تعريف شامل للجريمة السيبرانية ، يجعل من الأفضل أن نستند إلى التعريفات التي إعتمدتها الهيئات والمنظمات الدولية المتخصصة. ففي ورشة عمل متخصصة حول المسائل التي تثيرها الجرائم المتصلة بالشبكات، قسمت هذه الجرائم، الى مجموعتين[1] :

- المجموعة الاولى: و ضمنت حسب المفهوم الضيق" كل تصرف غير شرعي موجه بالوسائل الالكترونية، نحو أمن انظمة المعلومات، والبيانات التي تحويها ."

(1)Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders - Vienna, 10-17 April 2000- A/CONF.187/10- Distr.: General 3 February 2000- Background paper for the workshop on crimes related to the computer network.

- المجموعة الثانية: والتى ضمنت حسب المفهوم الاوسع، كل تصرف غير شرعي يرتكب بواسطة، الأنظمة المعلوماتية،أو بطريقة متصلة بها،ويشمل جرائم كالحيازة غير المشروعة، أو عرض الخدمات وتوزيع المعلومات، بواسطة انظمة معلومات او شبكات معلومات.

ومن جهة أخرى،عمدت الإتفاقية الأوروبية لمكافحة الجريمة السيبرانية، إلى إيراد ما تعتبره أعمالا غير شرعية، تناولت الجرائم ضد سرية الأنظمة والبيانات، وسلامتها، وتوفرها، والجرائم المتصلة بالاجهزة، والجرائم الخاصة بالمحتوى، والجرائم الخاصة بالملكية الفكرية.([1])

مفهوم مخاطر السيبرانية

يقصد بالمخاطر السيبرانية بأنها " مخاطر تشغيلية على أصول المعلومات والتكنولوجيا التي لها عواقب تؤثر على سرية أو توفر أو سلامة المعلومات أو نظم المعلومات . مقارنة بفئات المخاطر التي يغطيها التأمين . فإن المخاطر السيبرانية تتفق من حيث الخصائص والمسؤولية ، مع مخاطر كل من الممتلكات والخصوم، وكذلك المخاطر الكارثية والتشغيلية. ([2])

من ناحية أخرى، يمكن أن تؤثر المخاطر السيبرانية أولاً على الهدف والأطراف المقابلة لة. و من ناحية أخرى، تكون الخسائر الناتجة عن المخاطر

(1) Convention on Cybercrime- Budapest, 23.XI.2001

(2) Cebula , J.J. and L.R. Young: "A taxonomy of Operational Cyber Security Risks", Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University, 2010, .

السيبرانية صغيرة ومستقلة في أغلب الأحيان، ولكنها قد تكون أيضًا منخفضة التردد وتأثير كبير"سياسة التعتيم".

كما يمكن أن تكون مخاطر الإنترنت غير مرتبطة بمخاطر الهجمات الإلكترونية:على سبيل المثال ، يمكن أن تؤدي تحديثات البرامج أو الكوارث الطبيعية إلى تبلور مخاطر الإنترنت من خلال اضطرابات العمل دون أي نية سيئة ، كما هو موضح في تعريف الحوادث السيبرانية . ([1])

ثانيا : طبيعة المخاطر السيبرانية

مما لا شك فيه، أن تكنولوجيا المعلومات والاتصالات، تتيح إمكانات هائلة، وغير مسبوقة، لإنتاجية أفضل في جميع القطاعات، وللتواصل عبر القارات. إلا أن البنية التحتية لهذه التقنيات، تمثل ارتباطا بين مصالح متعددة، وخدمات مختلفة، ودول عديدة، الأمر الذي يجعل من الاخطار في المجال السيبراني، أخطارا عالمية. فلا يمكن لاي جهة، أن تضمن بقاءها في منأى عن الاخطار، ما دامت سلامة الآخرين معرضة للخطر.

- المخاطر التقنية:

تترافق طبيعة التقنيات والاتصالات، مع اخطار خاصة، مرتبطة بهندستها الخاصة، وبالبيئة التي تعمل في اطارها، أي الفضاء السيبيري. واذا كانت التقنية، والرقمنة، تتحكم بتوسع تقنيات المعلومات والاتصالات، وبالولوج إلى الفضاء السيبيري، ورسم حدوده، بما جعل البعض يعتبرونها، قادرة على لعب دور القانون في

(1) Eling, M. and J. H. Wirfs: "Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class", Institute of Insurance Economics, University of St. Gallen, 2016 .

تنظيم الفضاء السيبراني، وضبط الاعمال المخلة بأمنه وصولا الى انكارهم على المشرع،حق الاضطلاع بمهمة هذا التنظيم.

إلا أن هذا الأمر لا يستقيم، فقد أثبتت هذه التقنية أنها ليست قادرة على ضبط التصرف الانساني وتأمين سلامة الأفراد والمؤسسات والدول التي أصبحت اكثر اعتمادا عليها.

فقد عمدت أكثر الدول تقدما إلى لفت الانتباه إلى هشاشة الوضع، فضلا عن الخلل العضوي الذي يعترى البرمجيات والتجهيزات على السواء، والذي يشكل نقاط ضعف يمكن استغلالها بسهولة من قبل الخبراء في خرق الأنظمة المعلوماتية، وإلى حجم المخاطر الذي يرتبها هذا الامر.

وإذا كان صحيحا أن الحلول التقنية موجودة. فإن الصحيح أيضا، أنها حلول قاصرة لا تستطيع مواكبة التحولات المستمرة في طبيعة المخاطر. فهي تتبع بروز المشكلة وبالتالي تشكل، رداً محدوداً بالزمان والمكان، كما وبمسألة معينة.

هذا عدا عن مهارات المتسللين الى الانظمة ، وتعدد الجهات المعنية بالأمن السيبراني (تقنيين، مستثمرين، عملاء، مهندسين، مطوري برامج وتطبيقات...)، وانعكاس ذلك تعقيدات على مستوى الرؤية والفهم الجامع للمخاطر، فضلا عن التدابير الواجب اتخاذها. إذ أن تقنيات الحماية نفسها بحاجة الى الحماية.

من هنا يمكننا القول، بأن الإلتجاء إلى الحلول التقنية، هو إلتجاء الى المجهول، خاصة مع صعوبة التحكم بهذه التقنيات، ومع الأعطال التي يمكن أن تطرأ عليها، هذا فضلا عن العيوب الخفية التي تعتريها، والتي لا يمكن إكتشافها إلا بعد وضعها قيد التنفيذ.

غير أن الاقرار بقصور التقنية لا يعني عدم الإهتمام بتطوير آليات الحماية التقنية، والإستعانة بالبرامج والتطبيقات الخاصة منع الوصول إلى البنى التحتية و الأنظمة المعلوماتية لمن ليس له الحق في ذلك، من خلال تدابير تقنية ترتكز على إدارة الهوية الإلكترونية ،واستخدام برامج الحماية من الفيروسات، وبروتوكولات التشفير، وغيرها.

- المخاطر القانونية

تتمثل المخاطر القانونية بشكل أساسي، في غياب الهيكل التشريعي والتنظيمي المناسب للتعامل مع نتائج الأعمال القانونية وغير القانونية منها، والتي تتم في الفضاء السيبرانى. فالنشاط الاقتصادي والتجاري وغيره، يتطلب تحديدا واضحاً للحقوق والواجبات بما يساهم في تعزيز الثقة بقدرات تكنولوجيا المعلومات والاتصالات، في مجال الخدمات عبر الفضاء الإلكتروني.

وعلية، فإن المخاطر القانونية تتمثل في :غياب الأمن القانوني، و تناقض الاحكام والقوانين وتنازع الانظمة القانونية من جهة، وفي اتساع امكانات انتشار الجريمة الإلكترونية من جهة أخرى. حيث يرتفع نسبة هذه المخاطر، مع انعدام او ضعف التعاون بين الدول المختلفة فى ملاحقة مرتكبى تتلاءم الاعتداءات الإلكترونية التي لا تقتصر على الافراد فحسب بل تمتد لتطول أمن الدول واستقرارها.

ثالثا: أنواع المخاطر السيبرانية

يتمثل تأثير الهجمات السيبرانية من خلال المساس بالجوانب الرئيسة الثلاثة لأمن المعلومات، والتى تتمثل فى : السرية و النزاهة و استمرارية الأداء.

- السرية :حيث تنشأ عندما يتم الكشف عن المعلومات الخاصة داخل الشركة إلى أطراف ثالثة كما في حالة حدوث إختراق البيانات.

- النزاهة: والتى تتعلق بإساءة استخدام الأنظمة ، كما هو الحال بالنسبة للاحتيال.
- استمراية الأداء: و التى تتلخص فى تعطل أو التوقف عن ممارسة الأعمال .

هذة الأنواع الثلاثة من الهجمات الإلكترونية لها تأثيرات مباشرة و مختلفة على الأهداف، حيث يؤدى تعطل الأعمال إلى المنع من العمل، مما ينتج عنة خسارة في الإيرادات(بالنسبة للشركات) أو تعطل فى تحقيق الأهداف بالنسبة للأفراد ؛ كما يؤدى الإحتيال إلى خسائر مالية مباشرة ؛ في الوقت الذى يستغرق التحقيق فى تأثيرات إختراق البيانات وقتًا أطول ، الأمر الذى ينتج عنة أضرار معنوية تمس السمعة وفضلا عن تكاليف التقاضي. وبصفة عامة ، فإن خطر فقدان الثقة في أعقاب الهجمات الإلكترونية قد يكون عاليا بالنسبة للقطاع المالي، بالنظر إلى اعتماد المؤسسات المالية على ثقة عملائها. ([1])

و فيما يتعلق بالنظام المالي، فمن المرجح أن يكون لتعطل الأعمال آثار عدوى مباشرة على المدى القصير أكثر من الإحتيال أو خرق البيانات ، والتي تميل إلى التأثير بشكل رئيسي على الشركة المستهدفة على المدى القصير.

وعلية، فإن التطوير العالمي لشبكات التواصل الاجتماعي وأسواق الجريمة الدولية الناشئة جميعها تُثير القلق الجدي من ارتفاع نسبة الجريمة السيبرانية. وبالتالي استدامة المجتمع المستقر كأساس للتنمية والرخاء الاقتصادي.

فضلا عن ضعف البنية التحتية المجتمعية لتكنولوجيا المعلومات والاتصالات ، وجمع وتخزين البيانات بدون حدود يهددان الحرية الشخصية والاستقرار الدولي.

---

(1)Antoine Bouveret : Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment, Working Paper, IMF, June 2018.

ويزعزع ثقة المواطنين في المجتمع والحكومة لحماية أمنهم ورخائهم ، بفعل الأخطار والشكوك الناشئة عن التطورات التقنية مع ما ينطوي عليه ذلك من خسائر اقتصادية باهظة. لذلك فإننا ضرورة الاستعجال فى اتخاذ إجراءات عالمية للتصدي لهذه الأخطار السيبرانية. استناداً إلى تحليل متماسك للاتجاهات والعواقب التكنولوجية والمجتمعية والاقتصادية والسياسية.

المبحث الثانى

تهديدات الأمن السيبراني للمصارف الإلكترونية وآليات مواجهتها

تمهيد:

شهدت الصناعة المصرفية فى العقود الأخيرة تقدما ملموسا تطور مستمر فى مجال التقنية المصرفية من حيث قدرة عملاء البنوك على إجراء العمليات المصرفية من خلال شبكات الإتصال الالكترونية. ونظرا لما يصاحب إجراء العمليات المصرفية الإلكترونية من مخاطر متعددة لاتقتصر فقط على المخاطر التقليدية، فإن الأمر يستلزم وضع أسس إدارة هذه المخاطر ، مع التحديد الدقيق لمسئوليات الجهات ذات العلاقة بها وفقا لضوابط البنك المركزى المصرى. لذلك نتناول هذا المبحث من خلال ما يلى:

المطلب الأول : ماهية المصارف الإلكترونية

المطلب الثاني : طبيعة مظاهر مخاطر وتهديدات الأمن السيبراني

المطلب الثالث : إدارة مخاطر العمليات المصرفية الإلكترونية

المطلب الأول

ماهية المصارف الإلكترونية

تمهيد:

ارتبطت ظاهرة العولمة المالية بالتحرير المالى الذى نتج عنة تشابك واندماج الأنظمة المالية والنقدية للدول، بهدف تيسير الأعمال المالية والمصرفية للعملاء، وإزالة القيود التى تحول دون تدفق رووس الأموال وحرية المؤسسات المالية والمصرفية. فكان من انجازات الدولة الحديثة اليوم هي الحكومة الإلكترونية التي دخلت في مجالات العمل التقليدية منها التجارة الالكترونية، و التسويق الإلكتروني ، والبنوك الإلكترونية ، هذه التركيبة الإلكترونية هي نتاج الثورة التكنولوجية. لذا نحاول توضيح طبيعة العمليات المصرفية الإلكترونييه فيما يلى...

طبيعة العمليات المصرفية الإلكترونية

يستخدم اصطلاح البنوك الإلكترونية E-Banking كتعبير متطور وشامل للمفاهيم التي تبلورت مع بداية التسعينات، مثل: مفهوم الخدمات المصرفية عن بعد، البنوك الإلكترونية عن بعد، البنك المنزلي Banking Home، الخدمات المصرفية الذاتية Self–Service Banking. وجميعها تتعلق بقيام العميل بإدارة حساباته و إنجاز أعماله المتصلة بالبنك عن طريق المنزل أو المكتب أو أي مكان آخر وفي الوقت الذي يريده.

لذا، يقصد بالعمليات المصرفية الإلكترونية ما يقدمه البنك من خدمات مصرفية تقليدية أو متطورة من خلال قنوات اتصال الإلكترونية، يخول الدخول فيها بعد استيفاء

شروط العضوية المحددة من طرف البنك، وهي بذلك تحقق للبنك فوائد عديدة، لاسيما تخفيض تكاليف الاستغلال و رفع الكفاءة العملياتية ومستويات الجودة.([1])

وتتمثل أهم صور العمليات المصرفية الالكترونية في الوقت الراهن، فيما يلى: ([2])

- النقود الالكترونية Electronic money : يصدر البنك وسائل الدفع هذه في شكل وسائط تحتوي على شرائح ممغنطة و تدعى ببطاقات القيمة المخزنة، يقابلها مقدار من الوحدات النقدية، بحيث يزود العميل بها للتعامل مع جهاز الصرف الآلي من أجل السحب النقدي أو لطلب كشف الحساب ودفتر الشيكات وكذا تحويل أموال أو دفع فواتير مستحقة، و يفترض الاستفادة من هذه الخدمة على مدار ٢٤ ساعة يوميا.
- البنك المنزلي Home Banking : يتم تحميل الحاسوب الشخصي ببرنامج خاص، يوفره البنك مجانا أو لقاء رسوم للعملاء، لأغراض الإطلاع على الحساب و السحب أوالإيداع في أرصدة الحسابات المصرفية . إذ يتمكن العميل من الدخول وإجراء المعاملات عبر الاتصال بالانترنت، في ظل ضوابط تتحكم في حركة هذه الأنشطة وتضمن حقوق العميل و البنك على حد سواء.
- الخدمات المصرفية التليفونية Telebanking: هي أنظمة تخدم العملاء عبر جهاز التليفون، خاصة التليفونات المحمولة، على مدار اليوم ، وضمن سياق منظم

(١) رحيم حسين و هواري معراج: الصيرفة الإلكترونية كمدخل لعصرنة المصارف الجزائرية، ملتقى المنظومة المصرفية الجزائرية و التحولات الاقتصادية- واقع و تحديات، ص: ٣١٥-٣١٦.

(٢) د/زديك الطاهر& د/ محمد ورنيقي : استراتيجية مكافحة الارهاب الالكتروني في المجال الاقتصادي المركز العربي الديمقراطي- مجلة الدراسات الأفريقية و حوض النيل ، المجلد الثاني ، العدد الخامس، مارس/ اذار ٢٠١٩

يحدد العميل نوع الخدمة المصرفية التي يريدها من خلال البرنامج الصوتي الذي يضعه البنك في متناول عملائه.([1])

أهداف العمليات المصرفية الإلكترونية:([2])

تقدم البنوك المصرفية الإلكترونية خدمات تقتصر على المشاركين فيها وفقا لشروط العضوية التى تحددها البنوك، وذلك من خلال أحد المنافذ على الشبكة كوسيلة لإتصال العملاء بها لتحقيق عدة أهداف. من أهمها :

(أ) إتاحة معلومات عن الخدمات التى يؤديها البنك دون تقديم خدمات مصرفية على الشبكة.

(ب) حصول العملاء على خدمات محدودة كالتعرف على معاملاتهم وأرصدة حساباتهم وتحديث بياناتهم وطلب الحصول على قروض.

(ج) طلب العملاء تنفيذ عمليات مصرفية مثل تحويل الأموال.

(د) توفير المزيد من فرص العمل والاستثمار

(ه)اختصار المسافات الجغرافية ورفع الحواجز التقليدية

(و) تعزيز رأس المال الفكرى وتطوير تكنولوجيا امعلومات.

---

(١) د/علم الدين بانقا : مخاطر الهجمات الالكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجى، سلسلة دراسات تنموية ، المعهد العربى للتخطيط ، الكويت ،العدد٦٣ ، ابريل ٢٠١٩

(٢) د/خالد ممدوح العزى : الجرائم المالية الإلكترونية -الجرائم المصرفية أنموذجا، بحث مقدم فى المؤتمر الدولى الرابع عشر :الجرائم الالكترونية ،طرابلس ،لبنان ،٢٤-٢٥ مارس ٢٠١٧ ، ص ٦-٧ .

وتتمثل مزايا العمليات المصرفية الالكترونية فيما يلى:

- إمكان وصول البنوك إلى قاعدة عريضة من العملاء المودعين والمقترضين وطالبى الخدمات المصرفية.
- تقديم خدمات مصرفية جديدة.
- خفض تكاليف التشغيل بالبنوك وتكاليف إنجاز عمليات التجزئة محليا ودوليا.
- زيادة كفاءة أداء البنوك.

وفى سبيل تحقيق هذة الأهداف تصدر البنوك أنواع عديدة من وسائل دفع النقود الالكترونية، ويتمثل أبرز أنواع وسائل دفع النقود الالكترونية المصدرة كما يلى: (١)

أ- إصدار البنك لبطاقات القيمة المخزنة Stored – value cards كالبطاقات الذكية Smart cards، أو غيرها، وذلك بالسماح بتخزين وحدات من النقود على هذه البطاقات التى تحمل شرائح ممغنطة تسمح بذلك.

ب- إتاحة البنك للنقدية الإلكترونية Electronic cash بتخزين وحدات من النقود على وسائط الكترونية Electronic device مثل الحاسب الشخصى الذى يتم تحميله ببرنامج خاص لهذا الغرض، وتستخدم هذه النقود لإجراء مدفوعات ذات قيم محدودة بتحويلها إلى الوسائط الالكترونية الخاصة بالأطراف المقابلة.

وفى ضوء ذلك تلتزم البنوك أيضا بإدارة المخاطر المرتبطة بوسائل الدفع الأخرى والتى من بينها:

---

(١) د/عبد الله خبابة: الاقتصاد المصرفي، مؤسسة شباب الجامعة، الإسكندرية، ٢٠٠٨ ، ص ٩١

- بطاقات الخصم Debit cards ويقتصر إستخدامها خصما على حسابات دائنة للعملاء.
- بطاقات الإئتمان Credit cards ويتم إستخدامها خصما على حسابات مدينة وفقا للحدود المقررة. وتستخدم الوحدات الطرفية لنقاط البيع Point of sale terminals وآلات الصرف الآلى Automatic teller machines وغيرها كوسائط لإتصال حائزى بطاقات الخصم والإئتمان بشبكة الإتصال الإلكترونية.

وحيث أن البنك المركزى المصرى هو الجهة المنوط بها قانونا إصدار أوراق النقد للإستخدام كوسيلة دفع لها قوة إبراء، تخضع عملية إصدار وسائل دفع لنقود الكترونية لرقابة البنك المركزى المصرى خاصة أنه ليس لها قوة إبراء إلا بعد تسوية قيمة المدفوعات التى تمت بها طرف كل من بنك المشترى وبنك البائع.

المطلب الثاني

طبيعة مخاطر وتهديدات الأمن السيبراني فى المصارف الإلكترونية

يصاحب تقديم العمليات المصرفية الالكترونية مخاطر متعددة وقد أشارت لجنة بازل للرقابة المصرفية إلى أنه ينبغى قيام البنوك بوضع السياسات والإجراءات التى تتيح لها إدارة هذه المخاطر من خلال تقييمها والرقابة عليها ومتابعتها، وقد سبق وأشرنا إلى أن المخاطر السيبرانية تندرج تحت مسمى المخاطر التشغيلية التى تواجه المصارف عموما، الكترونية كانت أم تقليدية([1]). وهنا يثور التساءل التالى:

(١) د/محمد فلاق& د/ رضوان انساعد: الإدارة الإلكترونية مفهومها متطلباتها تطبيقاتها، الملتقي الدولي، متطلبات ارساء الحكومة الإلكترونية في الجزائر، دراسة تجارب بعض الدول ، جامعة سعد دحل ،البليدة ، الجزائر، ٢٠١٣ ،ص ١٧

لماذا تتعرض المصارف الإلكترونية بدرجة كبيرة للمخاطر السيبرانية؟

في إدارة مخاطر أمن المعلومات ، يتم تعريف المخاطر السيبرانية على أنها مزيج من العواقب والاحتمالات، إذ يتمثل الإحتمال الرئيسى للتعرض المؤسسات المالية للمخاطر السيبرانية فى حجم مستويات التهديد وسهولة إستغلال مرتكبى الجرائم السيبرانية لنقاط ضعف تلك المؤسسات فى الاختراق ،أو التجسس على المستفيد ، أومراقبة الاتصالات من قبل أطراف ثالثة.([1])

تعتبر المؤسسات المالية ذات النظم القديمة هى الأكثر عرضة لخطر التهديد بالهجمات السيبرانية ، فضلا عن إنخفاض تكلفة شن هذة الهجمات ، وفى المقابل نجد أن عواقب تلك الهجمات مرتفعة أيضًا لأن النشاط المالي غير ملموس و يعتمد بشكل كبير على التكنولوجيا. ويرجع ذلك إلى الأسباب التالية :

١- استهداف البنية التحتية للمصرف الالكترونى أو تعطيل عملها:

تشمل البنية التحتية فى أى قطاع مالى: أنظمة الدفع والتسوية، ومنصات التداول ، ودائع الأوراق المالية المركزية ، والأطراف المقابلة المركزية. وتعتبر البنى التحتية للقطاعات المالية فى الدولة -خاصة الدول النامية – نقطة الضعف الرئيسة فى فشل الأمن السيبرانى لهذة القطاعات والذى قد يتحقق نتيجة لتهالك أوتعطل عمل البنية التحتية للقطاع ذاتة أو لمجموعة من المؤسسات المالية الرئيسة فى القطاع نتيجة لتركز المخاطر، أو عدم وجود بدائل في حالة البنية التحتية. ([2])

---

(1) Emanuel Kopp ، Lincoln Kaffenberger , and Christopher Wilson : "Cyber Risk ,Market Failures,and Financial Stability",Working Paper No.17/185,IMF, 2017.

(2) S.Friedman :"Taking cyber risk management to the next level - Lessons learned From the front lines at financial institutions", Deloitte Insight, June 2016.

وهو الامر الذى يمكن أن يؤدي إلى اضطرابات كبيرة فى سير العمل بالقطاع المالي. أو تقويض ثقة العملاء في المصارف . فعلى سبيل المثال ، في ٢٧ يونيو ٢٠١٤ شهد أكبر بنك محلي في بلغاريا FIB عملية تشغيل من جانب المودعين وسط حالة من عدم اليقين بسبب قرار بنك آخر- بعد رسائل البريد الإلكتروني المخادعة التي تشير إلى أن FIB كان يعاني من نقص في السيولة. بلغت ودائع التدفقات الخارجة في ذلك اليوم ١٠% من إجمالي الودائع لدى البنوك ، وكان على البنك استخدام خطة لمساعدة السيولة مقدمة من السلطات.

٢- استغلال الثغرات:

ويسمى أيضا بالهجوم دون انتظار Zero Day Attack وهو عبارة عن إستغلال نقاط الضعف فى برمجيات وثغراتها الأمنية خاصة غير المعروفة ، وغالبا ما يتم إستغلال هذة الثغرات ومشاركتها من قبل المهاجمين قبل أن تكتشف الجهات المطورة برامج تصحيحية مواجهة لها.

٣- إختراق البيانات :

تتعرض المؤسسات المالية بشكل خاص لانتهاكات البيانات. نظرًا لاعتمادها على بيانات العميل في إدارة الأعمال ، فقد عانى القطاع المالي فى العديد من الدول حتى الدول الكبرى من حوادث إختراق البيانات أو فقدانها في السنوات الأخيرة - بما في ذلك اختراق بيانات . فقد تم سرقة المعلومات الشخصية لأكثر من ١٤٥ مليون عميل فى مصارف الولايات المتحدة خلال الفترة من عام ٢٠١٥ وحتى عام ٢٠١٧.

ويصعب تقييم الأثر الاقتصادي لإنتهاكات البيانات نظرًا لأن التأثيرات غير المباشرة (فقدان العملاء ، مخاطر السمعة) من المحتمل أن تكون أكثر أهمية من التأثيرات المباشرة (تكاليف الاسترداد والتقاضي). فقد تم اختراق أكثر من ٢٦٠ مليون

سجل في الولايات المتحدة وحدها ، بسبب الهجمات السيبرانية على القطاع المالي فى تلك الفترة ، وتقدر الخسائر الناجمة عن خرق البيانات خلال هذة الفترة بحوالي ٣٨ مليار دولار للشركات المالية الأمريكية وحدها. ([1])

٤- استهداف الهواتف الذكية :

والتى أصبحت وسيلة الإتصال السيبرانى ودخول الكثير من العملاء على حساباتهم المصرفية من خلالها ، أو إجراء عمليات البيع والشراء من خلال تلك الهواتف ، ويحاول المهاجمون تركيز اهتمامهم على اختراق هذة الأجهزة . والتى ينشأ تهديدها نتيجة للأسباب التالية:

- أن غالبية مستخدمى الهواتف الذكية ليس لديهم المعرفة الكافية بالثغرات الأمنية لهذة الهواتف .
- أن المهاجمين دائما ما يلجأون إلى التحايل على مالكى الهواتف الذكية لتوجيههم على تحميل تطبيقات تحت سيطرتهم.
- يكمن خطر الهواتف الذكية فى تطبيقاتها الخاصة بدخول العملاء من خلالها لحساباتهم المصرفية ، الأمر الذى يتيح للمهاجمين فرصة الحصول على المعلومات المصرفية أو إصابة النظام الإلكترونى للمصرف بالفيروسات التى تعطل عمل النظام أو بعض أجزائة.

(١) د/مريم خالص حسين: الحكومة الالكترونية ، مجلة كلية بغداد للعلوم الاقتصادية ،عدد خاص بالمؤتمر، العراق ،٢٠١٣ ، ص ٤٤٣ .

مظاهر التهديدات السيبراني في القطاع المصرفي الإلكتروني :

تتمثل أبرز مظاهر التهديدات السيبرانية فى القطاع المصرفي الإلكتروني فيما يلى: ([1])

أ- البرمجيات الخبيثة malicious software وتعطيل الخدمة: البرمجة الخبيثة هى برمجة يمكن تضمينها أو إدراجها عمدا فى نظام الحاسوب لتحقيق أهداف سيئة، مثل: عرقلة عمل النظام، أو جمع معلومات حساسة ، أو الوصول إلى أنظمة الكمبيونر الخاصة . وتسمى بالخبيثة لصعوبة إزالتها بعد التثبيت، ومن أبرز صورها:هجوم الحرمان من الخدمة Denial-of-Service والذى عادة مايستهدف المؤسسات الحكومية، و الشركات الكبرى ، والمصارف . وذلك بهدف منع المستخدمين من الوصول إلى النظام .

ب- الرسائل المزيفة عبر وسائل الإتصال المختلفة " الإستدراج الإلكترونى":

والذى يتمثل فى الهجوم على على هوية أحد العملاء لدى البنك ، والغرض من هذا الهجوم هو الحصول على البيانات الشخصية باستخدام تقنيات مختلفة كالمواقع الوهمية والرسائل الإلكترونية المزيفة...الخ. للحصول على معلومات حسابية: كهوية المستخدم ، أوكلمة السر ، أو بيانات الحسابات عن طريق الإحتيال من خلال انتحال هوية صديق موثوق أو مصرف فى رسالة إلكترونية.

---

(١) صندوق النقد العربى: سلامة وأمن المعلومات المصرفية الإلكترونية ،اللجنة العربية للرقابة المصرفية ، أمانة مجلس محافظى المصارف المركزية ومؤسسات النقد العربية، العدد ٧٢،أبوظبى ،الامارات العربية المتحدة،٢٠١٧، ص٨-٩

وتعد الأخيرة من اكثر وسائل الإستدراج الإلكترونى انتشارا سواء عن طريق الهواتف النقالة أو رسائل نصية الكترونية، وتعتبر الشركات والمصارف التى تقدم خدمات استثمارية الكترونية مواقع مستهدفة لعمليات الاستدراج .

المطلب الثالث

إدارة مخاطر العمليات المصرفية الإلكترونية

أولا : إدارة مخاطر العمليات المصرفية الإلكترونية

أشارت لجنة بازل للرقابة المصرفية إلى أهمية قيام البنوك بوضع السياسات والإجراءات التي تتيح إدارة مخاطر العمل المصرفي الإلكتروني من خلال تقييمها والرقابة عليها ومتابعتها، تندرج إدارة مخاطر العمليات المصرفية الإلكترونية تحت طائفة مخاطر التشغيل risk Operational التى أصدرتها لجنة بازل للرقابة المصرفية فى مارس ١٩٩٨ ومايو ٢٠٠١. ولايمنع ذلك من توافر بعض أنواع المخاطر الاخرى: كمخاطر السمعة، والمخاطر القانونية. وفيما يلى عرض موجز لهذه المخاطر:([1])

١- مخاطر التشغيل risk Operational

تنشأ مخاطر التشغيل من عدم التأمين الكافى للنظم أو عدم ملاءمة تصميم النظم أو إنجاز العمل أو أعمال الصيانة وكذا نتيجة إساءة الإستخدام من قبل العملاء وذلك على النحو التالى:

(١) بنك الإسكندرية : النشرة الاقتصادية ،المجلد الخامس والثلاثون ،الإسكندرية، مصر، ٢٠٠٣ ، ص ٣٤

(أ) عدم التأمين الكافي للنظم: System security

تنشأ هذه المخاطر عن إمكان إختراق غير المرخص لهم access Unauthorized لنظم حسابات البنك بهدف التعرف على المعلومات الخاصة بالعملاء وإستغلالها سواء تم ذلك من خارج البنك أو من العاملين به، بما يستلزم توافر إجراءات كافية لكشف وإعاقة ذلك الإختراق.

(ب) عدم ملاءمة تصميم النظم أو إنجاز العمل أو أعمال الصيانة:

Systems design, implementation, and maintenance

وهى تنشأ من إخفاق النظم أو عدم كفاءتها " ضعف الاداء Slow- Down " لمواجهة متطلبات المستخدمين وعدم السرعة فى حل هذه المشاكل وصيانة النظم وخاصة إذا زاد الإعتماد على مصادر خارج البنوك لتقديم الدعم الفنى بشأن البنية الأساسية اللازمة Outsourcing.

(ج) إساءة الإستخدام من قبل العملاء: Customer misuse of services

ويرد ذلك نتيجة عدم إحاطة العملاء بإجراءات التأمين الوقائية Security precautions أو بسماحهم لعناصر إجرامية بالدخول إلى حسابات عملاء آخرين أو القيام بعمليات غسيل الأموال بإستخدام معلوماتهم الشخصية أو قيامهم بعدم إتباع إجراءات التأمين الواجبة.

٢- مخاطر السمعة:

تنشأ مخاطر السمعة نتيجة عدم مقدرة البنك على إدارة أنظمته بكفاءة أو حدوث اختراق مؤثر لها. ومن أجل حماية البنك يتعين عليه تطوير ورقابة ومتابعة معايير الأداء بالنسبة إلى عمليات المصارف الإلكترونية بحيث أنه:

- تُقدم البنوك المعلومات المناسبة عن مواقعها على الإنترنت للعملاء المحتملين بالتوصل إلى استنتاجات مدروسة حول هوية البنك ومركزه القانوني ، وذلك قبل الدخول بتنفيذ معاملات مصرفية إلكترونية .
- تتخذ البنوك الإجراءات المناسبة للتأكد من الوفاء بمتطلبات سرية العميل حسب الدول التي يقدم فيها البنك منتجاته وخدماته المصرفية إلكترونيا.
- أن تتوفر للبنوك القدرة على استمرار النشاط وعمليات التخطيط للطوارئ للمساعدة على ضمان توافر النظم والخدمات من خلال العمليات الإلكترونية .
- تلتزم البنوك بإعداد خطط مناسبة تتضمن الاستجابة للحوادث، والحد منها وخفض المشكلات الناتجة عن الحوادث غير المتوقعة، بما في ذلك أنواع الهجوم الداخلي والخارجي، التي قد تعوق تزويد النظم والخدمات المتعلقة بالعمليات المصرفية الإلكترونية .

٣- المخاطر القانونية:

وهى تلك المخاطر الناجمة عن عدم التحديد الواضح للحقوق والالتزامات القانونية الناتجة عن العمليات المصرفية الإلكترونية ، وتبرز أهم التحديات القانونية في تحدي قبول القانون لحجية التعاقدات الإلكترونية في الإثبات، وسائل الدفع ، التحديات الضريبية ، إثبات الشخصية، التواقيع الإلكترونية، أنظمة الدفع النقدي، المال النقدي أو الإلكتروني، سرية المعلومات وأمنها من مخاطر إجرام التقنية العالية خصوصية العميل، علاقة وتعاقدات المصرف مع الجهات المزودة للتقنية أو الموردة لخدمات أو مشاريع الاندماج والمشاركة والتعاون المعلوماتية.([1])

(١) د/عصام إبراهيم الترساوي: غسيل الأموال، الهيئة المصرية العامة للكتاب، القاهرة ، ٢٠٠٢ ، ص ٢٠٩-٢١٠

ثانيا: الضوابط الأساسية فى إدارة العمليات المصرفية الالكترونية

واستنادا لما سبق نشير إلى أهم الضوابط الأساسية فى إدارة العمليات المصرفية الإلكترونية، سواء لكل من البنك والعملاء([1])

أ- بالنسبة للبنك عند تقديم خدماته عبر شبكات الإتصال الإلكترونية

(١) موافقة مجلس إدارة البنك على إستراتيجية تتضمن قيام البنك بتقديم خدماته عبر الشبكات على أن يحاط المجلس بكافة المخاطر الناشئة عن ذلك.

(٢) موافقة مجلس إدارة البنك على سياسة الإدارة التنفيذية للبنك فيما يتعلق بأسلوب إدارة المخاطر، وتدعيم نظم الرقابة الداخلية بشأن تلك المخاطر.

(٣) تصميم نماذج عقود لتأدية مختلف الخدمات المصرفية التى تؤدى عبر شبكات الإتصال الالكترونية وأن يتأكد البنك من توافر القوى البشرية المؤهلة للتعامل مع عملاء البنك عبر الشبكات، مع تحديد ساعات تقديم هذه الخدمات.

(٤) فى حالة وجود طرف آخر تقدم من خلاله الخدمة فيتعين على مجلس إدارة البنك إقرار إتفاقية التشغيل التى تنظم العلاقة بين البنك مع هذا الطرف وتحديد مسئوليته فى الحفاظ على سرية التعليمات والمعاملات التى تتم عبر الشبكات وأية معلومات تتاح له.

---

(١) د/أحمد جمال الدين موسى: النقود الالكترونية وتأثيرها على المصارف المركزية في إدارة السياسة النقدية، الجديد في أعمال المصارف من الوجهتين القانونية والاقتصادية، أعمال المؤتمر العلمي السنوي لكلية الحقوق، جامعة بيروت العربية، الجزء الأول، الجديد في التقنيات المصرفية، منشوارت الحلبي الحقوقية، بيروت ٢٠٠٢ ، ص ١٢١

(٥) إفصاح البنك على صفحة ال Web الخاصة به بما يفيد حصوله على ترخيص بتقديم خدماته عبر الشبكات من البنك المركزى المصرى ورقم وتاريخ الحصول على الترخيص والخدمات التى يجوز للبنك تقديمها عبر الشبكات، مع ربط هذا الموقع بصفحة البنك المركزى المصرى المعلن فيها عن أسماء البنوك المرخص لها بذلك من خلال Hypertext Links حتى يتحقق العملاء من صحة التصريح.

(٦) إفصاح البنك عن أن القوانين المصرية هى التى تحكم الخدمات التى يقوم بتأديتها للعملاء عبر الشبكات.

(٧) ضرورة أن يتحقق البنك من شخصية طالب/ متلقى الخدمة بأساليب قانونية ثابتة تضمن الحقوق المتبادلة.

ب- بالنسبة للعميل عند تلقى خدماته عبر شبكات الإتصال الالكترونية

(١) يتحمل العميل مسئولية صحة المعلومات التى يقوم بإدخالها عبر الشبكات بإعتباره مستخدما للخدمات التى تؤدى من خلالها، ويقر العميل بأن التعليمات والمعاملات التى يدخلها يتم التعامل عليها بدون أية مراجعة إضافية من البنك أو إشعارات خطية أو التأكد منها بطرق أخرى.

(٢) لايلتزم البنك بقبول أية تعديلات أو الغاء تعليمات أو معاملات سبق أن أرسلها العميل عبر الشبكات.

(٣) يتحمل العميل مسئولية إعداد البيانات الخاصة بالمستفيد أو الإضافة أو التعديل عليها.

(٤) يلتزم العميل بمراعاة إجراءات الحماية فى التعامل عبر الشبكات مع البنك.

(٥) يتحمل العميل مسئولية سوء إستخدام الخدمة الناتج عن عدم الإلتزام بإجراءات الحماية أو الشروط والأحكام الواردة فى العقد الذى يتم إبرامه مع البنك بشأن العمليات المصرفية الألكترونية، أو الناتج عن قيامه بالكشف عن إجراءات الحماية أو مخالفتها لدى الإستخدام.

(٦) عدم تحمل البنك مسئولية تعطل الخدمة لظروف خارجة عن إرادته.

(٧) تعتبر سجلات البنك حجة قاطعة ملزمة قانونا على صحة المعاملات والتعليمات.

(٨) يلتزم العميل فى حالة فقد أو سرقة جهاز الشفرة بإخطار البنك لكى يقوم بإبطال هذا الجهاز.

(٩) تعتبر أدوات الحماية وسيلة للتعرف والتحقق من شخصية العميل، وبمجرد إتمام إدخالها بنجاح يعتبر العميل هو مصدر جميع التعليمات والمعاملات.

ثالثا: استراتيجية إدارة مخاطر العمليات المصرفية الالكترونية

تشتمل استراتيجية إدارة المخاطر على التقييم والرقابة والمتابعة وذلك على النحو التالى: ([1])

(١) تقييم المخاطرAssessing risks

ويشمل التقييم مايلى:

- تحديد المخاطر التى قد يتعرض لها البنك، ومدى تأثيرها عليه.

(١) د/ شريف محمد غنام: مسئولية البنك عن أخطاء الكمبيوتر فى النقل الإلكترونى للنقود ، الطبعة الأولى ، دار الجامعة الجديدة للنشر ،الاسكندرية ،٢٠٠٦ ،ص ١٠١

- وضع حدود قصوى لما يمكن للبنك أن يتحمله من خسائر نتيجة التعامل مع هذه المخاطر.

(٢) الرقابة على التعرض للمخاطر Controlling risk exposures فى حالة الإعتماد على مصادر خارج البنك لتقديم الدعم الفنى:(١)

تشتمل هذه الضوابط على مايلى:

- متابعة الأداء المالى والتشغيلى لمقدمى الدعم الفنى.
- التأكد من توافر إتفاقيات تعاقدية مع مقدمى الدعم الفنى تحدد التزامات الأطراف تفصيليا.
- التأكد من مقدرة مقدمى الدعم الفنى على توفير التأمين بما يتفق و المتبع داخل البنك فى حالة تعرفهم على بيانات ذات حساسية تخص البنك، و ذلك من خلال مراجعة سياساتهم و اجراءاتهم فى هذا المجال.
- توفير ترتيبات طوارئ لتغطية إحتمالات حدوث تغيير مفاجئ فى مقدمى الدعم الفنى.
- متابعة إحاطة العملاء عن العمليات المصرفية الالكترونية وكيفية إستخدامها

Providing customer education and disclosure

(١) د/موسى خليل متري: القواعد القانونية الناظمة للصيرفة الالكترونية، الجديد في أعمال المصارف من الوجهتين القانونية والاقتصادية، أعمال المؤتمرالعلمي السنوي لكلية الحقوق، جامعة بيروت العربية، الجزء الأول، الجديد في التقنيات المصرفية، منشو ا رت الحقوق الحلبي، بيروت ٢٠٠٢ ، ص ٢٦٧

(٣) إعداد خطط طوارئ Contingency planning بديلة فى حالة اخفاق النظم عن أداء الخدمات وذلك فيما يتعلق بما يلى:

- إعادة البيانات إلى الوضع الذى كانت عليه قبل الإخفاق Data recovery.
- توفير قدرات بديلة لتشغيل البيانات Alternative data – processing capabilities.
- توفير عاملين لمواجهة الظروف الطارئة.
- إختبار نظم التشغيل البديلة Backup systems بصفة دورية للتأكد من فاعليتها.
- توافر التأمين اللازم فى حالة تنفيذ خطط الطوارىء وكذا توافر تعليمات لإستخدام هذه الخطط لدى مقدمى الدعم الفنى.
- إبرام عقود بديلة مع مقدمى دعم فنى آخرين تنفذ فى حالة إخفاق المقدمين الأساسيين.

(٤) متابعة المخاطر Monitoring risks:

تتمثل متابعة المخاطر فى إختبار النظم وإجراء المراجعة الداخلية والخارجية System testing and auditing وذلك على النحو التالى:

(أ) إجراء اختبارات دورية للنظم، والتى يكون من ضمنها:

- إجراء إختبار إمكان الإختراق Penetration testing الذى يهدف الى تحديد وعزل وتعزيز تدفق البيانات من خلال النظم وإتباع إجراءات لحماية النظم من المحاولات غير العادية للإختراق.

- إجراء مراجعة دورية من خلال النظم للتأكد من فاعلية اجراءات التامين والوقوف على مدى اتساقها مع سياسات واجراءات التامين المقررة.

(ب) اجراءات المراجعة الداخلية والخارجية:

تسهم المراجعة الداخلية والخارجية فى تتبع الثغرات وحالات عدم الكفاءة وتخفيض حجم المخاطر بهدف التحقق من توافر سياسات وإجراءات مطورة والتزام البنك بها.

المبحث الثالث

آليات تعزيز الأمن السيبرانى فى المصارف الالكترونية

ترك التطور التكنولوجي بشتى أنواعه أثر خطير يهدد الانسان والمجتمع من جهة والدولة والجماعات الدولية من جهة ثانية ،هذا التأثير التكنولوجي سببه وجود قاعدة اقتصادية قوية توفر التمويل للحصول على تكنولوجية الاساسية في جميع القطاعات من شبكة مواصلات بأنواعها " البرية والجوية والبحرية" الى الكهرباء المسهلة للوسائل الاتصال بأنواعها " من انترنت وما يحتويه "، هذا التمويل في بعض الاحيان يكون سبب غير مباشر في استعمال التكنولوجية بالطريقة غير الصحيحة.

وعلية ،نتناول هذا المبحث من خلال ما يلى...

المطلب الأول : معوقات تعزيز الأمن السيبرانى فى المصارف الإلكترونية

المطلب الثانى : آليات تعزيز الأمن السيبرانى فى المصارف الإلكترونية

المطلب الثالث : الجهود المبذولة في مجال الأمن السيبرانى

المطلب الأول

معوقات تعزيز الأمن السيبرانى فى المصارف الإلكترونية

إن غياب الأمن السيبرانى وهو ما يمكن تسميتة بالإرهاب الإلكتروني.هو نموذج جديد لهذا العصر التكنولوجي القائم على العولمة، و الذى يعتبر في ذات الوقت صورة للإرهاب التقليدي. لهذا نرى - في تقديرنا - أن الإرهاب الإلكتروني سوف يكون عدو للحكومة الإلكترونية، وإن كان هذا التطور موجود فقط في الدول المتقدمة ، ومازال

فكرة أو مشروع بالنسبة للدول النامية ،لأن الإرهاب الإلكتروني يرى في هذا النوع من التطور عرقلة لمشاريعه غير المشروعة وبالتالي يصعب عليه كل التصرفات من غسيل وتحويل وتبيض الأموال ، أو حتى اختراق هذا النظام.

أولا : معوقات تعزيز الأمن السيبرانى

بالنظر إلى طبيعة مخاطر وتهديدات الأمن السيبرانى ، يمكن تحديد المشكلات التي تواجهها الدول وخاصة فى العالم العربي، كما يلى: ([1])

- نقص وعدم وضوح البيئة التشريعية.
- بيئة تنفيذية غير ملائمة.

وفيما يلى نشير إلى كل منهما على النحو التالى...

١- نقص وعدم وضوح البيئة التشريعية:

شهد العالم العربي حركة تشريعية وتنظيمية بطيئة فيما يتعلق بإقرار تشريعات تنظم استخدام المعلومات الإلكترونية وتحديد كيفية إدارة محطات الإتصالات. وهذان الموضوعان، لم تشر اليهما، أي من التشريعات العربية حتى الآن باستثناء تونس التى تميزت باقرار قانون توجيهي رقم ١٣-٢٠٠٧، حول الاقتصاد الرقمي، وقانون رقم ١٨ عام ٢٠١٠ ، الهادف الى خلق نظام تحفيز للابداع والاختراع، في مجال تكنولوجيا المعلومات والاتصالات. وهذان الموضوعان، لم تشر اليهما، أي من التشريعات العربية حتى الآن. ([2])

---

(١) ديفيد ليبتون : تهديدات الأمن الإلكتروني تدعو إلى تحرك عالمي، صندوق النقد الدولى، يناير ٢٠٢٠

(2) World Bank: "Cybersecurity, Cyber Risk and Financial Sector Regulation and Supervision", Feb. 2018

٢- بيئة تنفيذية غير ملائمة:

ويقصد بذلك تناول حق التنفيذ فيما يخص المجال الإلكترونى من حماية سابقة أو عقوبات لاحقة على ارتكاب الجريمة الالكترونية ، ويشمل ذلك مجالات عدة ، من أبرزها: ([1])

- الملكية الفكرية

تعتبر التشريعات العربية في مجال حماية الملكية الفكرية التي تتعلق بحق المؤلف، والعلامات التجارية، والملكية الصناعية، وبراءات الاختراع الأكثر كثافة من غيرها، مثل: قانون حماية الملكية الفكرية عام ٢٠٠٢ في مصر، وقانون حماية حق المؤلف للعام ٢٠٠٣ في السعودية... الخ.

إذ تميل غالبية التشريعات العربية إلى اعتبار البرامج الإلكترونية مصنفات جديرة بالحماية، إلا أنها تبقى بعيدة عن تأمين حماية فعالة نظرا لكونها لا تتطرق إلى مسائل أخرى، كحماية أسماء المواقع، أو قواعد البيانات، أو الاعتداء على العلامات التجارية.

- حماية المستهلك

وفي مجال حماية المستهلك، يعتبر غياب هذه الحماية شديد الارتباط بالمعاملات الالكترونية، من جهة، وبعقود الإذعان من جهة أخرى، ما يشكل عامل خطر مزدوج، في غياب التشريع الملائم، كون المستهلك في الفضاء السيبرانى، أكثر

(١) د/منى الأشقر جبور: الأمن السيبراني: التحديات ومستلزمات المواجهة ، جامعة الدول العربية ، المركز العربي للبحوث القانونية والقضائية، اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني ، بيروت ٢٧ – ٢٨ أغسطس (آب) ٢٠١٢

تـأثرا بمخـاطر العلاقـة التـي تـضم شخـصا محترفـا، هـو التـاجر أو مقـدم الخدمـة علـى الانترنت، من جهة، والمستهلك نفسه من جهة أخرى.

الأمر الذي يجعل القواعد التقليدية الخاصة بحماية المستهلك، غير صالحة للتطبيق، في جميع اوجه الحماية، ما يستدعي، ضرورة ايجاد قواعد خاصة بالحماية في البيئة الرقمية، على غرار ما ذهب اليه المشرع اللبناني.

- المواكبة الادارية

أما على المستوى الهيكلي والتنظيمي ، فقد أنشأت مصر إدارة متخصصة لمكافحة جرائم الحاسبات والشبكات في وزارة الداخلية، بمقتضى قرار وزاري رقم ٣٢٧ عام ٢٠٠٥. كما أنشىء في لبنان، مكتب مكافحة الملكية الفكرية والجرائم المعلوماتية في وزارة الداخلية، نتيجة ضرورة الاستجابة لمتطلبت مكافحة نوع جديد من النشاط غير الشرعي و المرتبط بالفضاء الإلكتروني والمعلوماتية.

- المعاملات الإلكترونية

حظيت المعاملات الإلكترونية باصدار تشريعات عدة خاصة بالتوقيع الإلكتروني، والمعاملات الإلكترونية والاثبات، على الرغم من الثغرات العديدة التي مازالت قائمة على هذا المستوى، خاصة فيما يتعلق بإجراءات حجية الاثبات للمراسلات الالكترونية، وحجية العقود والعلاقات التجارية، بما في ذلك البيع والأعمال المصرفية، والخدمات الالكترونية.

ففي هذا المجال صدرت عدة قوانين، مثل قانون التوقيع الالكتروني في مصر، ومشروع قانون التجارة الالكترونية في الكويت، وقانون الاوراق المالية لعام ٢٠٠٤ في فلسطين، الذي خصص مادة منه للتوقيع الالكتروني (مادة ٢٦)، والمرسوم الملكي

رقم ١٨ حول نظام التعاملات الالكترونية، واللائحة التنفيذية لنظام التعاملات الالكترونية للعام ٢٠٠٧ في السعودية.

واستنادا لماسبق ، يمكننا القول بأن البيئة التنظيمية والتشريعية العربية، مازالت في طور التكوين. ذلك أن فاعلية هذه البيئة تقاس بمدى إنسجامها مع المجتمع من جهة، وبمدى احتوائها لطبيعة الموضوع الذي تنظمه من جهة اخرى، كما بمدى القدرة على التجاوب معه واستيعابه من قبل المعنيين من جهة ثالثة.

المطلب الثانى

آليات تعزيز الأمن السيبرانى فى المصارف الإلكترونية

أولا: استراتيجيات التغلب على التحديات في مجال أمن نظم المعلومات والفضاء الإلكتروني في الدول العربية:

تتمثل أهم استراتيجيات التغلب على التحديات في مجال أمن نظم المعلومات والفضاء الإلكتروني في الدول العربية فيما يلى:

- أهمية قيام الأجهزة الرقابية والمؤسسات بتوفير الدورات التدريبية عالية المستوى وتنظيم الندوات، وورش العمل والمؤتمرات بمشاركة الشركات والمؤسسات الدولية المتطورة في مجال تقنية المعلومات لاطلاع الكوادر الفنية على أحدث التقنيات لمواكبة التطور السريع والتعرف على التقنيات الحديثة في مجال الخدمات الإلكترونية على المستوى العالمي. وذلك بهدف خلق كوادر فنية عالية المستوى قادرة على التصدي للتحديات الجديدة المرتبطة بهذه التقنيات وكيفية التغلب عليها.

- أهمية وضع الأجهزة الرقابية العربية لآلية رقابية واضحة على البنوك والمؤسسات المالية للتأكد من وجود ضوابط وسياسات لتحقيق الأمن السيبراني.
- أهمية حصول المؤسسات المالية والمصارف بالدول العربية على أحدث التقنيات سواء فيما يتعلق بالأجهزة(Hardware) ، أو البرامج (Software) لمواجهة أحدث التطورات والأساليب المتبعة في مجال الهجمات والقرصنة الإلكترونية الدولية، بهدف اقتناء جدار أمني أكثر فعالية قادر على التصدي لأحدث الأساليب المتبعة في هذا الشأن.
- أهمية استحداث تخصص الأمن السيبراني في الجامعات العربية المتخصصة في مجال تقنيات المعلومات أسوة بالجامعات العالمية، بهدف خلق الكوادر العربية المتخصصة ذات المستوى العالي في هذا المجال.
- قيام الهيئات والجهات الرقابية في الدول العربية بإصدار التعليمات والقواعد المنظمة الخاصة بقيام المصارف والمؤسسات المالية بإجراء عقود لأطراف ثالثه تختص بأمن نظم المعلومات، على أن تخضع تلك الشركات التي يتم التعهيد إليها، للرقابة الصارمة من قبل الأجهزة الأمنية العربية، للقضاء على عمليات الاحتيال والقرصنة على الأنظمة الإلكترونية في تلك البنوك والمؤسسات.
- مدى أهمية قيام المصارف والمؤسسات المالية العربية بتخصيص الموارد والمخصصات الكافية للحصول على أحدث التقنيات في مجال أمن نظم المعلومات والفضاء السيبراني، حيث تتسم تلك التقنيات بالارتفاع الملحوظ في تكلفة اقتناءها.
- العمل على تكثيف التوعية لدى العملاء من خلال البرامج المسموعة والمرئية والندوات التثقيفية لرفع المستوى الخاص بثقافة الأمن السيبراني لدى المتعاملين

بالقطاع المالي والمصرفي، بهدف تفهم الضوابط والتعليمات الخاصة بأمن نظم المعلومات والفضاء السيبراني.

ثانيا: الجوانب المتعلقة بأمن الفضاء الإلكتروني في إطار المخاطر التشغيلية للبنوك المركزية العربية.([1])

وتتمثل أهم هذة الجوانب المتعلقة بأمن الفضاء الإلكترونى في إطار المخاطر التشغيلية للبنوك المركزية العربية فيما يلى:

١- الإطار الرقابي العام للمخاطر المرتبطة بأمن نظم المعلومات والفضاء السيبراني:

تتسم التعليمات الرقابية الصادرة من معظم السلطات الرقابية في الدول العربية والخاصة بإطار المخاطر التشغيلية Operational Risks بتضمنها جزءً متعلقاً بمخاطر نظم المعلومات وأمن الفضاء الإلكتروني في القطاع المصرفي يحدد المعايير اللازم توافرها لضمان أمن المعاملات المصرفية المنفذة عبر الفضاء الإلكتروني، من أهمها ما يلى:

- تعليمات من السلطات الرقابية تلزم المصارف بتضمين استراتيجيات المخاطر المقرة من قبل مجالس إدارات البنوك، إطاراً يتعلق بالمخاطر الإلكترونية ومخاطر نظم المعلومات والهجمات الإلكترونية (Cyber attacks) يتم التحقق من ذلك من خلال عمليات الرقابة، التي تتم بصورة دورية، بما يشمل وجود سياسة واضحة لحوكمة إدارة المخاطر السيبرانية في غالبية الدول العربية.

(١) د/ إبراهيم الكرسانة: طرق أساسية ومعاصرة في الرقابة على البنوك و إدارة المخاطر، صندوق النقد العربي، أبوظبي، مارس ٢٠٠٦ ، ص، ٤

- تصدر السلطات في الدول العربية العديد من التعليمات الواجب اتباعها عند القيام بعمليات الإسناد الخارجي لخدمات تقنية المعلومات وتقديم الخدمات المصرفية عبر الإنترنت، من أهمها وجود إطار عمل لإدارة المخاطر وضمان جودة الخدمات المقدمة من شركات الإسناد الخارجي، إضافة إلى القيام بعمليات دورية لتقييم المخاطر المتعلقة بالتعاقد مع مزودي هذه الخدمات.

٢- تنظيم وإدارة الحسابات والخدمات المصرفية المقدمة عبر الإنترنت

تتمثل مسئولية البنك في اتخاذ الاعتبارات اللازمة نحو الحفاظ على سرية البيانات التي توثق وتحقق هوية العميل عند الاستفادة من الخدمات المصرفية عبر الإنترنت . وفيما يخص العملاء الراغبين في الاستفادة من الخدمات المصرفية من خلال شبكة الإنترنت، تقوم البنوك في هذا الشأن بالحصول على توقيع يدوي من العميل على استمارة طلب الخدمة التي تحتوي على البيانات الأساسية للعميل كحد أدنى (البريد الإلكتروني، رقم الهاتف المحمول والأرضي، عنوان المراسلات)، كما تطبق المتطلبات والأحكام التي تحدد الحقوق والالتزامات بين المصارف والعملاء بشكل واضح.

كما تلتزم المصارف في معظم الدول العربية، وفقا للتعليمات الصادرة عن السلطات الرقابية، بتطبيق أساليب يمكن الاعتماد عليها للتحقق من هوية وصلاحيات العملاء الراغبين في الاشتراك في خدمات الإنترنت البنكي. وتلتزم المصارف أيضا بالحصول على كافة المستندات القانونية اللازمة لإثبات تفويض الصلاحيات للمستخدمين بإجراء معاملات على حسابات الأشخاص الاعتبارية.

٣- وسائل إثبات الهوية عبر الإنترنت

تعتمد معظم البنوك في المنطقة العربية على استخدام مبدأ الدخول المزدوج (Tow Factor Authentication) للتحقق من هوية العميل المستفيد من الخدمات المصرفية من خلال الإنترنت، حيث تقوم المصارف المركزية بالدول العربية بصفتها السلطة الرقابية على الجهاز المصرفي بعملية التقييم الفني والأمني للخدمات المصرفية المقدمة من البنوك عبر الإنترنت. ذلك خاصة فيما يتعلق بالسرية والخصوصية والتحقق من الهوية وذلك قبل تقديم الخدمة للعميل. كما تقوم المصارف بالتقييم الأمني للخدمات المقدمة من خلالها وذلك بصفة مستمرة وفق الإجراءات والقواعد الخاصة بالرقابة الداخلية المتبعة في كل بنك وقياس مدى فعالية الأداء والوسائل التقنية المستخدمة للتحقق من هوية العميل وقياس مؤشرات التعرض لحوادث أمن المعلومات.

كما تشير التعليمات الصادرة عن المؤسسات الرقابية في معظم الدول العربية، إلى أنه يتعين على كافة البنوك وضع حد أقصى للمحاولات الخاطئة للدخول على الموقع الإلكتروني للبنك وذلك بما لا يزيد عن ٣ محاولات خاطئة في اليوم الواحد، ومن ثم يتم إيقاف التعاملات البنكية الإلكترونية. هذا، ولا تتم عمل ية إعادة التفعيل للخدمة إلا من خلال القنوات الآمنة مثل قيام العميل بالاتصال بمركز خدمة العملاء في البنك وتنفيذ الإجراءات المعتمدة والمطلوبة للتحقق من الهوية.

٤- الضوابط والتعليمات الرقابية الخاصة بإدارة كلمة السرPassword :

وفقا للتعليمات الصادرة عن معظم المصارف المركزية العربية، فإنه يجب على كل بنك مراعاة التدابير الرقابية عند التعامل مع كلمة السر الخاصة بالعملاء، بحيث يتم تطبيق الرقابة المزدوجة وأن يتم الفصل بين عملية إنشاء كلمات السر وتسليمها للعملاء وعملية تفعيل حسابات خدمات الإنترنت البنكي، وتعزيز تأمين عملية إنشاء

كلمة السر لضمان عدم تعرضها للكشف. كما أنه يجب التأكد من أن كلمات السر لا يتم معالجتها أو إرسالها أو تخزينها كنص واضح، وإعطاء تعليمات لمستخدمي ومديري أنظمة الإنترنت البنكي لتغيير كلمة السر الصادرة فور الدخول إلى النظام لأول مرة، وتحديد مدة صلاحية كلمة السر من جانب المصارف.

٥- عمليات تحويل الأموال من خلال خدمات الإنترنت:

تلزم الضوابط والتعليمات الصادرة عن معظم السلطات الرقابية في الدول العربية البنوك التي تقدم خدمة تحويل الأموال من حسابات عملائها إلى حسابات أطراف أخرى من خلال الإنترنت، بوضع الضوابط المناسبة التي تساعد على خفض مستوى المخاطر المصاحبة لتلك الخدمة لتصل إلى مستوى مقبول ومعتمد من البنك. فقد أجازت تلك التعليمات للمصارف استخدام وسيلة تصديق أحادية أو مزدوجة لعمليات تحويل الأموال بين الحسابات الخاصة لذات العميل داخل نطاق الدولة التابع لها، وعند سداد الإلتزامات الناتجة عن بطاقات الائتمان أو القروض الخاصة بالعميل.

كما أوصت تعليمات السلطات الإشرافية البنوك بتطبيق مبدأ الرقابة المزدوجة على تحويلات أموال الأشاخاص الاعتبارية إلى مستفيدين آخرين، بحيث يلتزم المصرف بوضع حد أقصى يومي لعمليات تحويل الأموال من حسابات عملائها لصالح مستفيدين آخرين بحيث لا يكون هناك تعارض مع أي حدود أخرى يحددها المصارف في هذا الصدد.

٦- سرية وسلامة المعلومات:

تتمثل الضوابط والتعليمات الصادرة عن المصارف المركزية العربية المعنية بسرية وسلامة المعلومات المرتبطة بالإنترنت البنكي، في أمن وسلامة البيانات

والأنظمة، لضمان عدم تعديل معلومات العملاء وأن الأنظمة لا يمكن الوصول إليها بصورة غير مصرح بها، وكذا أهمية سرية بيانات العملاء وحفظها بشكل آمن.

كما تتناول تلك التعليمات أهمية اتباع نهج استباقي للكشف عن المعاملات الاحتيالية المحتملة. إضافة الى ذلك، وتتضمن أيضا وسائل لتحقيق المساءلة عن طريق تصميم إجراءات التشغيل الموحدة والسياسات والضوابط لضمان إمكانية تتبع جميع المعاملات.

٧- تأمين التطبيقات الإلكترونية المستخدمة في تقديم الخدمات والمعاملات البنكية من خلال شبكة الإنترنت:

قامت معظم المصارف المركزية في الدول العربية بوضع لائحة من التعليمات لتأمين التطبيقات الإلكترونية الخاصة بالبنوك، ومن أهمها تثبيت برامج الحماية للحفاظ على هذه التطبيقات من الاختراق، بالإضافة إلى إجراء الاختبارات الأمنية على التطبيقات قبل تثبيتها وبعده. كما تشير تلك التعليمات إلى ضرورة قيام البنوك بتقييم نقاط الضعف الموجودة في التطبيقات مرتين على الأقل سنوياً، ووضع خطة للحد من نقاط الضعف ومشاركة الخطة مع الإدارة العليا. إضافة إلى العديد من التعليمات والضوابط الأخرى التي تهدف إلى حماية التطبيقات الإلكترونية المستخدمة في البنوك من الاختراقات.

٨- المخاطر المرتبطة بأمن نظم المعلومات والفضاء السيبراني:

تفرض المصارف المركزية العربية على المصارف القيام بعمل اختبارات الضغط (Stress Testing) لتحديد حجم الآثار المترتبة على نجاح أية عمليات قرصنة تتعرض لها الأنظمة الإلكترونية بتلك المصارف، بصورة دورية سنوية أو نصف سنوية.

كما يجب على البنك، وفقا للتعليمات الرقابية الصادرة في هذا الشأن، الإبلاغ عن الاختراقات وأية عمليات قرصنة إلكترونية خلال ساعة من وقوعها في بعض الاادول العربية (Cyber-event reporting) ، في غضون يوم أو يومين على الأكثر من التعرض في بعض الدول العربية الأخرى، وذلك لكافة حالات الإختراقات الخاصة بأمن الفضاء الإلكتروني التي يترتب عليها خسائر ملموسة للعملاء وتؤثر سلبا على عمليات المصرف.

٩- بناء القدرات الرقابية والتحديات في مجال أمن نظم المعلومات والفضاء الإلكتروني :

تقوم المصارف المركزية العربية بتدريب وتعزيز القدرات البشرية في القطاع المصرفي في مجال أمن الفضاء الإلكتروني مع الأخذ بالاعتبار المقترحات والمبادئ الرقابية الصادرة عن المؤسسات الدولية في هذا الشأن.

كما تقوم بعض المصارف المركزية العربية بتوجيه القطاع المصرفي بشكل عام إلى تكثيف الجهود لتهيئة وتعزيز القدرات البشرية في هذا المجال وذلك عن طريق دعم التعليم الأكاديمي والبعثات الدراسية الخارجية للحصول على شهادات أكاديمية عليا من جامعات خارجية مرموقة. في هذا السياق، تتمثل أهم التحديات التي تواجه الدول العربية في هذا الشأن في:

- التطور السريع في مجال تقنية المعلومات والاعتماد المتزايد على التقنيات للقيام بمعظم العمليات المالية، مما يؤدي إلى زيادة التعرض للتهديدات والحوادث الإلكترونية.
- الهجمات والقرصنة الإلكترونية الدولية التي تتعرض لها المصارف ببعض الدول العربية وآليه البنوك في التصدي لها ومدى فعالية الجدار الأمني في هذا الشأن.

- حداثة مفهوم الأمن السيبراني على مستوى الدول العربية والحاجة إلى تقوية الخبرات المصرفية في هذا المجال ببعض الدول العربية.
- ضمان تحقق الأمن السيبراني عند قيام المصارف بإجراء عقود لأطراف ثالثه تختص بأمن نظم المعلومات، للحد من وجود عمليات احتيال وقرصنة على الأنظمة الإلكترونية في تلك البنوك الارتفاع النسبي في تكلفة تطبيق تقنيات أمن نظم المعلومات والفضاء السيبراني بصورة ملحوظة.
- صعوبة تطبيق ضوابط أمن نظم المعلومات والفضاء السيبراني نظراً لضعف ثقافة الأمن السيبراني لدى بعض العاملين في القطاع المالي والمصرفي.
- الحاجة إلى وجود آلية رقابة واضحة على البنوك والشركات المالية للتأكد من وجود ضوابط وسياسات لتحقيق الأمن السيبراني .

المطلب الثالث

الجهود المبذولة في مجال الأمن السيبرانى

يبدو أن مجال الأمن السيبرانى قد لاقي اهتمامًا كبيرًا من كل الفواعل الدولية في الفترة الأخيرة، وسنتطرق إلي الجهود المبذولة في مجال الأمن السيبرانى في الوطن العربي بشكل عام ثم فى مصر.

١- على الصعيد العربي

تستثمر الكثير من الدول في الأنظمة والتشريعات والتقنيات والجاهزية للحروب السيبرانية لما تشكله من خطر عليها، وتضع الكثير من الدول الكبرى الأمن السيبراني ضمن أولوياتها للحد من الحروب الإلكترونية ولتأمين الخدمات والتطبيقات بمختلف القطاعات؛ وتعتبر التجربة العربية جديدة في هذا المجال، وازدادت قدرات كل

من عمان وقطر والسعودية، والتي ازدادت قدرتها مؤخرًا في هذا المجال بشكل مطرد حيث أنشأت السعودية الهيئة الوطنية للأمن السيبراني، كما أنشأت أيضًا الاتحاد المحلي للأمن السيبراني، وتأتي هذه القرارات ضمن خطة استراتيجية لبناء ترسانة قوية للأمن السيبراني مما يمكنها من حماية حدودها الإلكترونية بشكل جيد وصارم (١) .

وتبذل الدول العربية كل مافي وسعها للحاق بالركب العالمي في مجال تطوير الأمن السيبراني، وفي هذا الصدد عقدت المنظمة العربية للتنمية الإدارية التابعة لجامعة الدول العربية، والمكتب الإقليمي العربي للاتحاد الدولي للاتصالات في شهر نوفمبر ٢٠١٧، فعالية (الأمن السيبراني في المنطقة العربية)، والتي تتضمن اللقاء الثاني للتجارب الإدارية الناجحة في مجال أمن المعلومات، والمنتدي الإقليمي حول الأمن السيبراني في عصر التكنولوجيا الناشئة، وهدفت هذه الفعالية إلي التعريف بالتجارب الإدارية الناجحة في مجال أمن المعلومات من أجل تعميمها ونشرها والاستفادة منها في الدول العربية مع إقامة حوار مفتوح في الدول العربية لمناقشة تحديات الأمن السيبراني المتعلقة بالتكنولوجيات الناشئة وتطوير آليات دفاعية مبتكرة وفعّالة من منطلق المنظور الوطني، وقد شاركت في الفعالية دول مصر والسعودية وسلطنة عمان والأردن ولبنان وفلسطين والمغرب وسوريا واليمن وجزر القمر وموريتانيا بحضور ممثل عن الأمم المتحدة.

وعلية، يقع على عاتق واضعي قوانين تأمين وضمان أمن الفضاء الإلكترونى، مع مراعاة أمور عدة ، من أهممها: طبيعة الفضاء الإلكترونى العالمي، والتقنية.

(١) حسن بن علي العجمي، الثورة الصناعية الرابعة وتغييرات الحياة الإنسانية، المجلة العربية العدد ٤٩٨، إبريل ٢٠١٨، ص.١٥.

وضرورة توافق الاطار القانوني مع النزعة التقنية العالمية، والتى تتشكل مصادره من: [١]

- اتفاقيات دولية أو اقليمية، متعددة الاطراف، تحدد موجبات وحقوق الدول، واصول التعامل والتعاون فيما بينها، ومجالاته.
- اتفاقيات او ملاحق تقنية، تحدد المقاييس والمعايير التقنية العامة، الخاصة بالامن والسلامة، على ان يتم تعديلها وتيويمها بشكل متواصل، لتنسجم مع المستجدات.
- الارشادات والتوصيات، الصادرة عن الهيئات الدولية المتخصصة، والعاملة في المجال.
- القواعد التي تصدر عن هيئات مهنية متخصصة، ذات طابع عالمي، أو اقليمي.

حيث تبذل الهيئات الدولية، وفي مقدمها، الاتحاد الدولي للاتصالات، جهودا حثيثة ، تؤكد على حتمية الأمن السيبرانى. ويخصص الاتحاد هذا الاخير، بجزء أساسي من برامجه وخطط عمله المختلفة[٢].

لقد تعاملت الامم المتحدة، مع تقنيات المعلومات والاتصالات، خاصة فيما يتعلق بالانترنت، من منطلق كونها أداة للتنمية الاجتماعية والاقتصادية، فقد عهدت إلى

---

(1) Resolution 60/252, adopted by the General Assembly -World Summit on the Information Society"Reaffirming the potential of information and communication technologies as powerful tools to foster socio-economic development and contribute to the realization of the internationally agreed development goals, including the Millennium Development Goals," , 27 April 2006

(٢) الاتحاد الدولي للاتصالات: دليل الامن السيبراني للبلدان النامية ٢٠٠٧،الموجز التنفيذي المعلومات والاتصالات".

المجلس الاقتصادي الاجتماعي، لمتابعة قضايا التنمية المتعلقة بالانترنت. في المقابل، تهتم اللجنة الخاصة بالعدالة الجنائية ومنع الجريمة، الموكلة بمتابعة الجهود الدولية في مكافحة ومنع الجرائم الوطنية والعابرة للحدود، بالقضايا المتعلقة بجرائم الانترنت. (١)

وكان المجلس الاوروبي، قد اقر معاهدة مكافحة الجريمة الإلكترونية، التي دخات حيز التنفيذ، سنة ٢٠٠٤، داعيا جميع الدول الى التوقيع عليها، منذ تاريخ اقرارها في العام٢٠٠١. وتعتبر احكام هذه المعاهدة، منسجمة مع متطلبات مكافحة الجريمة الإلكترونية، لاسيما وانها تطلب من الدول الاعضاء، إنشاء مراكز اتصال، تعمل بحسب مبدأ استمرارية الخدمة، أي تأمين متابعة على امتداد ساعات اليوم، بحيث تكون دائمة الاستعداد، للتجاوب مع الطلبات القادمة من خارج الحدود الجغرافية، وللتعاون مع القوات المعنية بمكافحة الجريمة، بسرعة وفعالية.(٢)

وفى المقابل، اتجهت معظم الدول المتقدمة، الى اقرار سياسات وقائية ودفاعية، ضد الهجمات الإلكترونية ، وخصصت الدول الكبرى، مثل الولايات المتحدة الاميركية واستراليا، والمملكة المتحدة، مبالغ طائلة، لمعالجة مسائل الامن السيبرانى، واستقرار الفضاء الإلكترونى. لإرساء الثقة والاستقرار، كما السلامة والامن في هذا الفضاء.

---

(1) Economic and Social Council Resolution 1992/22: Implementation of General Assembly Resolution 46/152 concerning operational activities and coordination in the field of crime prevention and criminal justice, E/1992/92, 30 July 1992.

(٢) د/منار على حسن :التجارة الإلكترونية "متطلباتها واستراتيجية تنميتها مع الاشارة لمصر" ،مجلة النهضة ،العدد الثانى، كلية الاقتصاد والعلوم السياسية ،جامعة القاهرة ،ابريل ٢٠٠٥ .

فبعد انتقال الخدمات الكلاسيكية، كالبريد الالكتروني، والرسائل القصيرة، وشبكات ادارة العمل، الى الافادة من خدمات الحوسبة السحابية، ستنتقل دون ادنى شك، ادارة المحفظة الالكترونية، والخدمات المالية والمصرفية، والنشاطات الحكومية، من نقل وموارد طاقة وغيرها. وبالتالي، يصبح ملحا، تقرير الواجبات والحقوق، بما يضمن، الانسياب السهل للمعلومات وتفادي ممارسات مزودي الخدمات التي تمنحهم ارباحا غير محقة. كما يبدو ضروريا، استيعاب الحاجة الى مقاربة جديدة لحماية المعلومات تبعا لحساسيتها انطلاقا، من الاعتماد على المعايير والمقاييس الدولية في هذا المجال. ([1])

وهنا أيضا، يطرح المختصون أهمية سياسات الوصول إلى المعلومات وحماية البيانات، لاسيما مع الصعوبات التي مازالت تتحكم في هذا الموضوع، ومع إنعدام الانسجام بين القواعد التشريعية الوطنية. فمع انتقال المعلومات، عقود ونوعية خدمات، وصيانة، لا بد من إيجاد نماذج جديدة، تأخذ كل هذه العناصر بعين الاعتبار.

٢- رؤية جمهورية مصر العربية ٢٠٣٠ فى مجال الامن السيبرانى:

عندما ننظر إلي رؤية جمهورية مصر العربية ٢٠٣٠ ، والتي تؤكد من خلالها علي أهمية التوسع في الاستخدام الإلكتروني في الأعمال الحكومية والعلمية والتجارية، فقد أشارت كثير من التقارير العالمية والمحلية إلي تعرّض مصر إلي العديد من الهجمات السيبرانية، ولكن تم اتخاذ اجراءات الأمان والتحصين وبحسب ما أعلنت عنه إحدى الشركات الأمنية السيبيرية الفرنسية، فإن هذا الهجوم يشل عمل الأجهزة الالكترونية ويستغل ثغرة موجودة في نظام تشغيل "ويندوز".

(1)PricewaterhouseCoopers, Cyber Security M&A: Decoding Deals in the Global Cyber Security Industry (Nov. 2011)

فى إبريل عام٢٠٠٩ أنشأ الجهاز القومى لتنظيم الاتصالات، التابع لوزارة الاتصالات، المركز المصرى للاستجابة للطوارئ المعلوماتية (سيرت)، وذلك لتعزيز أمن البنية المعلوماتية وبنية الاتصالات فى مصر من خلال خطوات إيجابية، وجمع المعلومات حول الحوادث الأمنية وتحليلها، والتنسيق والوساطة بين كل الأطراف لحل مثل تلك الحوادث، بالإضافة إلى التعاون الدولى مع مختلف الفرق الأخرى .

تلتزم جميع الجهات الحكومية بكل مستوياتها وشركات قطاع الأعمال العام بتنفيذ قرارات وتوصيات المجلس الأعلى للأمن السيبرانى، فيما يتعلق بتأمين البنية التحتية الحرجة للاتصالات وتكنولوجيا المعلومات الخاصة بها، واتخاذ جميع الإجراءات الفنية والإدارية لمواجهة الأخطار والهجمات السيبرانية وتنفيذ الاستراتيجية الوطنية للأمن السبرانى يتولى وزير الاتصالات وتكنولوجيا المعلومات وضع وتحديد قواعد وإجراءات تأمين البنية المعلوماتية الحرجة لقطاعات الدولة ومتابعة تنفيذ قرارات وتوصيات المجلس الأعلى للأمن السيبرانى وتطبق أحكام هذا القرار. ([1])

ويقدم المركز المصري للاستجابة لطوارئ الإنترنت والحاسب منذ عام ٢٠١٢ الدعم لمختلف الجهات عبر قطاعات تكنولوجيا المعلومات والاتصالات، والخدمات المصرفية والحكومية من أجل مساعدتهم على مواجهة تهديدات الأمن السيبراني بما في ذلك هجمات الحرمان من الخدمة. ويُعد المركز المصري للاستجابة لطوارئ الإنترنت والحاسب مسؤولاً عن الاستجابة لحوادث أمن الكمبيوتر والمعلومات، وتوفير الدعم والدفاع والتحليل في مجال الهجمات السيبرانية والتعاون مع الهيئات الحكومية والمالية وأي قطاعات معنية بالبنية التحتية المعلوماتية الحرجة، كما يوفر المركز أيضاً

(١) هبة أحمد عبدالدايم & منار محمد شعبان : الهجمات السيبرانية ، دراسات دورية بنك الاستثمار القومي قطاع الاستثمار والموارد - الدعم الفني للاستثمار، العدد التاسع ، يوليو ٢٠١٧ ، ص ١٧

الإنذار المبكر ضد انتشار البرمجيات الخبيثة والهجمات السيبرانية الضخمة ضد البنية التحتية للاتصالات في مصر.

ويتكون المركز من أربع إدارات رئيسية، وهي مراقبة المخاطر والتعامل مع الحوادث السيبرانية، وتحليل الأدلة السيبرانية، وتحليل البرمجيات الخبيثة، وفحص الثغرات واختبارات الاختراق. وتتمحور مهمة المركز المصري للاستجابة لطوارئ الإنترنت والحاسب حول توفير نظام للإنذار المبكر ضد البرمجيات الخبيثة والهجمات السيبرانية التي تنتشر بنطاق واسع ضد البنية التحتية الحيوية للمعلومات المصرية.

ويأتى ذلك مع عدم الإخلال بأى عقوبات جنائية قد تنشأ نتيجة وقوع أضرار جسيمة تتعلق بعدم الالتزام بتأمين البنية التحتية الحرجة للاتصالات وتكنولوجيا المعلومات، يسأل تأديبيا كل موظف أو عامل يخالف قرارات المجلس الأعلى للأمن السيبرانى.

كما قام الجهاز القومي لتنظيم الاتصالات لشئون الأمن السيبراني المصري بتطوير الضوابط الأساسية للأمن السيبراني ، بعد دراسة عدة معايير وأطر وضوابط للأمن السيبراني قامت بإعدادها سابقاً عدة جهات ومنظمات محلية ودولية، ودراسة متطلبات التشريعات والتنظيمات والقرارات الوطنية ذات العلاقة.

وبعد الإطلاع على أفضل الممارسات والتجارب في مجال الأمن السيبراني والاستفادة منها، وتحليل ما تم رصده من حوادث وهجمات سيبرانية على مستوى الجهات الحكومية وغيرها من الجهات الحساسة؛ وتُطبق هذه الضوابط على الجهات الحكومية في مصر وتشمل الوزارات والهيئات والوحدات التابعة لها، وهيئات القطاع الخاص ذات البنى التحتية الحساسة .

الخاتمة:

يظل القطاع المالي وبشكل خاص المصرفي منه هو أكثر القطاعات الاقتصادية تعرضا للمخاطر، لاسيما المخاطر المستقبلية و يرجع هذا إلى طبيعة تخصصه الذي يستقطب بدرجة كبيرة ما تضفي إليه تحديات زيادة معدلات التغيير والتداخل بين القطاعات الاقتصادية.

وفى ضوء ما سبق انتهى البحث إلى النتائج التالية:

١- أن الطبيعة المتطورة للمخاطر السيبرانية ليست قابلة للتنظيم بشكل محدد، كما أن القضايا الخاصة بالإنترنت(cyber issues) يمكن معالجتها من خلال اللوائح الحالية المتعلقة بكل من المخاطر التشغيلية والتقنيات.

٢- كما أن التطور الحادث في المخاطر السيبرانية يحفز المؤسسات المالية على البحث المستمر والمكثف نحو اتخاذ إجراءات وقائية من تلك المخاطر من خلال لوائح تجعل تلك الإجراءات أكثر وضوحاً أمام مجالس إدارات تلك المؤسسات، الأمر الذي يؤدي إلى خلق حافز أكبر على الاستثمار بشكل مستمر في تحسين الأمن السيبراني.

٣- إضافة إلى أن إدراج المخاطر السيبرانية ضمن المخاطر التشغيلية للمؤسسات المالية يعتبر غير كافي، حيث أن المعايير الرقابية على المصارف تتطلب أهمية تضمين الإستراتيجيات والسياسات الخاصة بتلك المصارف، جزء خاص بإدارة المخاطر السيبرانية، والتي يتم مراجعتها بانتظام من قبل مجالس إدارات تلك البنوك مع زيادة حجم المخاطر السيبرانية.

توصيات البحث:

نظراً لما يصاحب إجراء العمليات المصرفية التقليدية و الإلكترونية وإصدار وسائل دفع النقود الكترونية من مخاطر متعددة، فإن البحث يوصى بالتالى:

١- وضع أسس لمراجعة وإدارة هذه المخاطر والتحديد الدقيق لمسئوليات مختلف الجهات ذات العلاقة بها وما يستلزم ذلك من الحصول على ترخيص من البنك وموافاته بالبيانات اللازمة.

٢- ضرورة قيام الأجهزة الرقابية والمؤسسات بتوفير الدورات التدريبية العالية المستوى وتنظيم الندوات، وورش العمل والمؤتمرات بمشاركة الشركات والمؤسسات الدولية المتطورة في مجال تقنيات المعلومات، وذلك بهدف خلق كوادر فنية عالية قادرة على التصدي للتحديات الجديدة المرتبطة بهذه التقنيات وكيفية التغلب عليها.

٣- وضع الأجهزة الرقابية العربية لآلية رقابية واضحة على البنوك والمؤسسات المالية للتأكد من وجود ضوابط وسياسات لتحقيق الأمن السيبراني.

٤- قيام الهيئات والجهات الرقابية في الدول العربية بإصدار التعليمات والقواعد المنظمة الخاصة بقيام المصارف والمؤسسات المالية بإجراء عقود لأطراف ثالثه تختص بأمن نظم المعلومات، على تخضع تلك الشركات التي يتم التعهيد اليها للرقابة الصارمة من قبل الأجهزة الأمنية العربية للقضاء على عمليات الاحتيال والقرصنة على الأنظمة الإلكترونية في تلك البنوك والمؤسسات.

٥- العمل على تكثيف التوعية لدى العملاء من خلال البرامج المسموعة والمرئية والندوات التثقيفية لرفع المستوى الخاص بثقافة الأمن السيبراني لدى

المتعاملين بالقطاع المالي والمصرفي، بهدف تفهم الضوابط والتعليمات الخاصة بأمن نظم المعلومات والفضاء السيبراني.

٦- ضرورة الاطلاع على التجارب الرائدة في مجال عمليات البنوك الالكترونية وإدارة مخاطرها ومحاولة استخراج نقاط القوة ومعرفة الاستفادة منها.

٧- تحتاج الدول العربية للمزيد من الاستثمار في مجال الأمن السيبراني من خلال توطين التكنولوجيا والبني التحتية السيبرانية، الثاني تطوير المهارات والخبرات في سبيل امتلاك قدرات وطنية قادرة علي بناء وإدارة وتحليل الأنظمة السيبرانية وتطويرها.

٨- تشجيع مجالات البحث العلمي والابتكار؛ بالإضافة لضرورة توعية العاملين بكافة مؤسسات الدولة وتنمية المعايير المهنية الاحترافية لديهم وإرساء بنية تحتية للدخول إلي مجال صناعة البرمجيات العالمية والقدرة علي منافسة المنتج المستورد؛ واهتمام الحكومات العربية بتحفيز الاستثمارات والشركات العاملة في هذا القطاع والتعاون بينها وبين القطاعين الحكومي والعسكري، بحيث يستفيد كل قطاع من الآخر بما لا يخل بمبدأي السرية والخصوصية.

وختاماً، يمكن القول أن التحول الرقمي في مصر أدي إلى نمو استخدام الإنترنت والتكنولوجيا والمعاملات الإلكترونية لذلك، زادت الهجمات السيبرانية منذ ذلك الحين، مما دفع الحكومة لتخصيص جهد أكبر في هذا المجال، ومن هنا يجب علي الدول العربية الاستفادة من التجارب المعاصرة وغيرها من الدول المتطورة في مجال الأمن السيبراني ، وأن يتم تأسيس إطار تعاوني للدول العربية فيما بينها في مجال الأمن السيبراني.

المراجع:

١- د/ إبراهيم الكرسانة: طرق أساسية ومعاصرة في الرقابة على البنوك و إدارة المخاطر، صندوق النقد العربي، أبوظبي، مارس ٢٠٠٦

٢- د/أحمد جمال الدين موسى: النقود الالكترونية وتأثيرها على المصارف المركزية في إدارة السياسة النقدية، الجديد في أعمال المصارف من الوجهتين القانونية والاقتصادية، أعمال المؤتمر العلمي السنوي لكلية الحقوق، جامعة بيروت العربية، الجزء الأول، الجديد في التقنيات المصرفية، منشوارت الحلبي الحقوقية، بيروت ٢٠٠٢ .

٣- الاتحاد الدولي للاتصالات: دليل الامن السيبراني للبلدان النامية ٢٠٠٧،الموجز التنفيذي المعلومات والاتصالات."

٤- بنك الإسكندرية : النشرة الاقتصادية ،المجلد الخامس والثلاثون ،الإسكندرية، مصر، ٢٠٠٣

٥- د/خالد ممدوح العزى :الجرائم المالية الإلكترونية -الجرائم المصرفية أنموذجا، بحث مقدم فى المؤتمر الدولى الرابع عشر :الجرائم الالكترونية ،طرابلس ،لبنان ،٢٤-٢٥ مارس ٢٠١٧.

٦- حسن بن علي العجمي : الثورة الصناعية الرابعة وتغييرات الحياة الإنسانية، المجلة العربية العدد ٤٩٨، إبريل ٢٠١٨

٧- حمدون إ. توريه وآخرين: البحث عن السلام السيبراني، الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء، يناير ٢٠١١

٨- ديفيد ليبتون: تهديدات الأمن الإلكتروني تدعو إلى تحرك عالمي، صندوق النقد الدولى، يناير ٢٠٢٠

٩- د/رحيم حسين& د/ هواري معراج : الصيرفة الإلكترونية كمدخل لعصرنة المصارف الجزائرية، ملتقى المنظومة المصرفية الجزائرية و التحولات الاقتصادية- واقع و تحديات.

١٠-د/زديك الطاهر& د/ محمد ورنيقي: إستراتيجية مكافحة الإرهاب الإلكتروني في المجال الاقتصادي المركز العربي الديمقراطي-مجلة الدراسات الأفريقية و حوض النيل، المجلد الثاني، العدد الخامس، مارس/ اذار ٢٠١٩ .

١١- د/ شريف محمد غنام: مسئولية البنك عن أخطاء الكمبيوتر فى النقل الإلكترونى للنقود، الطبعة الأولى ، دار الجامعة الجديدة للنشر،الاسكندرية ،٢٠٠٦ .

١٢- صندوق النقد العربي: سلامة وأمن المعلومات المصرفية الإلكترونية ،اللجنة العربية للرقابة المصرفية ، أمانة مجلس محافظى المصارف المركزية ومؤسسات النقد العربية ، العدد ٧٢ ، أبوظبى ،الامارات العربية المتحدة ،٢٠١٧.

١٣- ــــــــــــــــ : سلسلة "موجز سياسات" حول" أمن الفضاء السيبراني في القطاع المصرفي، العدد الرابع، أبوظبى ،الامارات العربية المتحدة ،" ٢٠١٩-٠٧-٠٨ .

١٤-د/عبد الله خبابة: الاقتصاد المصرفي، مؤسسة شباب الجامعة للنشر والتوزيع ، الإسكندرية، ٢٠٠٨

١٥-د/عصام إبراهيم الترساوي: غسيل الأموال، الهيئة المصرية العامة للكتاب، القاهرة ، ٢٠٠٢

١٦-د/علم الدين بانقا: مخاطر الهجمات الالكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجى، سلسلة دراسات تنموية ، المعهد العربى للتخطيط ، الكويت ،العدد٦٣ ، ابريل ٢٠١٩

١٧-د/محمد فلاق & د/ رضوان انساعد: الادارة الالكترونية مفهومها متطلباتها تطبيقاتها، الملتقي الدولي، متطلبات إرساء الحكومة الإلكترونية في الجزائر، دراسة تجارب بعض الدول ، جامعة سعد دحل ،البليدة ، الجزائر، ٢٠١٣

١٨-د/محمود عزت: الفضاء السيبراني وتحديات الأمن المعلوماتي العربي، المجلة العربية، العدد ٤٩٨، أبريل ٢٠١٨ .

١٩- د/مريم خالص حسين : الحكومة الالكترونية ، مجلة كلية بغداد للعلوم الاقتصادية،عدد خاص بالمؤتمر، العراق ،٢٠١٣

٢٠-د/منار على حسن :التجارة الإلكترونية "متطلباتها واستراتيجية تنميتها مع الاشارة لمصر" ،مجلة النهضة ، العدد الثانى، كلية الاقتصاد والعلوم السياسية،جامعة القاهرة ،ابريل ٢٠٠٥ .

٢١- د/منى الأشقر جبور: السيبرانية: هاجس العصر ، دراسات وابحاث (١)، جامعة الدول العربية، المركز العربي للبحوث القانونية، بيروت،٢٠١٦ .

٢٢- ــــــــــــ: الأمن السيبراني: التحديات ومستلزمات المواجهة ، جامعة الدول العربية ، المركز العربي للبحوث القانونية والقضائية، اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني ، بيروت ٢٧ – ٢٨ أغسطس (آب) ٢٠١٢

٢٣-د/موسى خليل متري: القواعد القانونية الناظمة للصيرفة الالكترونية، الجديد في أعمال المصارف من الوجهتين القانونية والاقتصادية، أعمال المؤتمرالعلمي السنوي لكلية الحقوق، جامعة بيروت العربية، الجزء الأول، الجديد في التقنيات المصرفية، منشو ا رت الحقوق الحلبي، بيروت ٢٠٠٢ .

٢٤-د/هبة أحمد عبدالدايم & د/منار محمد شعبان : الهجمات السيبرانية ، دراسات دورية بنك الاستثمار القومي قطاع الاستثمار والموارد - الدعم الفني للاستثمار، العدد التاسع ، يوليو ٢٠١٧

ثانيا: المراجع الاجنبية

1- Antoine Bouveret : Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment, Working Paper, IMF, June 2018.

2- Convention on Cybercrime- Budapest, 23.XI.2001

3- Cebula, J.J. and L.R. Young : "A taxonomy of Operational Cyber Security Risks", Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University, 2010.

4- Eling , M. and J. H. Wirfs : " Cyber Risk : Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class", Institute of Insurance Economics, University of St. Gallen, 2016 .

5- Emanuel Kopp, Lincoln Kaffenberger, and Christopher Wilson : "Cyber Risk , Market Failures, and Financial Stability", Working Paper No. 17/185 , IMF, 2017 .

6- International Telecommunication Union (ITU) : Trends in Telecommunication Reform " The term " cybersecurity", 11- 2010.

7- Price water house Coopers : Cyber Security M & A : Decoding Deals in the Global Cyber Security Industry , Nov. 2011.

8- S. Friedman :"Taking cyber risk management to the next level - Lessons learned from the front lines at financial institutions", Deloitte Insight, June 2016.

9- World Bank: "Cybersecurity, Cyber Risk and Financial Sector Regulation and Supervision", Feb. 2018