Institutions financières et cybercriminalité

Édouard FERNANDEZ-BOLLO*

Le concept de « cybercriminalité », utilisé de plus en plus fréquemment bien que parfois mal défini, renvoie en principe à une caractérisation pénale, qui n'est toutefois ni spécifique, ni uniforme dans les différents systèmes juridiques. Dans l'usage courant, qui est celui retenu ici, il sert à désigner toutes les formes d'attaques réalisées au moyen de réseaux informatiques ou de systèmes d'information, ou les ayant pour cible. La menace que fait peser la cybercriminalité sur le secteur financier suscite désormais une attention élevée de la part des superviseurs, partout dans le monde. Des cyberattaques retentissantes sur des entreprises de réputation mondiale ou la révélation de programmes massifs de surveillance informatique ont amplifié les craintes que les fragilités inhérentes aux environnements informatiques puissent être exploitées à des fins malveillantes. Dans le domaine financier, c'est évidemment la crainte de détournements massifs, de vols de données ou d'atteintes majeures à la continuité d'activité des établissements qui préoccupent les régulateurs des banques et des assurances, de même que les conséquences systémiques que pourraient avoir de telles attaques.

Le superviseur financier n'est toutefois pas une autorité judiciaire et n'a pas vocation à traquer les infractions pénales. Soucieux de la stabilité des banques et des organismes d'assurance sous son contrôle, de même que de la protection des intérêts de leurs clients, il veille à ce que ces établissements prennent toutes les mesures préventives requises

* Secrétaire général, Autorité de contrôle prudentiel et de résolution (ACPR).
Contact : Edouard.Fernandez-Bollo@acpr.banque-france.fr.

pour garantir la sécurité de leurs systèmes d'information et notamment leur cybersécurité. Ce vocable nouveau, que l'Agence nationale pour la sécurité des systèmes d'information (ANSSI) définit comme un « état recherché pour un système d'information[1] lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles », est désormais employé pour désigner les actions de prévention et de remédiation mises en œuvre pour faire face aux cyberattaques.

L'enjeu est majeur car le secteur financier joue un rôle clé dans le fonctionnement de l'économie, au point que l'atteinte à un établissement pourrait avoir des conséquences néfastes sur les opérations économiques courantes d'un pays entier. Or les menaces sont variées et leur sophistication s'accroît (première partie). En application d'une réglementation spécifique sur la sécurité des systèmes d'information et en réponse à un environnement plus menaçant, les banques et les assurances adaptent et renforcent leurs politiques de prévention des risques liés à la cybercriminalité (deuxième partie). Les superviseurs de ces institutions, en particulier l'ACPR (Autorité de contrôle prudentiel et de résolution) qui coordonne son action pour la partie bancaire avec celle de la Banque centrale européenne (BCE) au sein du Mécanisme de supervision unique (MSU), focalisent leur attention sur la cybersécurité des institutions supervisées, avec une volonté de coopération forte avec les autres acteurs impliqués (troisième partie). Enfin, l'ACPR mène régulièrement des actions de contrôle sur les entités supervisées, qui permettent de tirer des enseignements concrets en termes de supervision et de préciser les points d'attention prioritaires pour l'avenir (quatrième partie).

LES CYBERATTAQUES REPRÉSENTENT DÉSORMAIS UNE MENACE RÉELLE POUR LE SECTEUR FINANCIER

Les attaques dirigées contre les institutions financières en Europe sont restées jusqu'ici relativement limitées dans leurs effets, ce qui peut s'expliquer par une mobilisation forte des établissements tant dans le domaine de la prévention que dans celui de la réaction. Pour autant, le secteur présente des spécificités qui rendent les menaces de cyberattaques très sérieuses, à la fois en termes de probabilité d'occurrence et de sévérité potentielle des impacts. Les établissements financiers ont démarré très tôt l'informatisation de leurs métiers. Ces derniers reposent aujourd'hui entièrement sur des outils informatiques, mais ceux-ci peuvent parfois être anciens et mal adaptés face à des nouvelles menaces. Ce sont aussi très souvent des systèmes multiples, décentralisés, au

sein de grands groupes qui sont largement interconnectés et échangent de nombreuses informations avec l'extérieur, comme pour la réalisation de paiements ou dans le cas des banquiers et des assureurs en ligne. Ces caractéristiques ne permettent pas de se reposer uniquement sur des protections classiques, de type « protection périmètrique », mais obligent à développer intensivement des mécanismes plus sophistiqués de protection et de détection des attaques.

De nouvelles techniques d'attaque sont mises en œuvre, mais elles renvoient à des risques déjà bien identifiés

L'émergence récente du terme « cybercriminalité » pourrait laisser entendre que nous assistons à un phénomène nouveau, à la fois dans ses moyens et ses objectifs, mais en réalité, ce sont surtout les techniques d'attaque qui évoluent et se complexifient. Les motivations, quant à elles, demeurent largement inchangées.

En ce qui concerne les techniques, il convient de distinguer deux grands types d'attaques : les attaques de masse et les attaques ciblées. D'une manière générale, les attaques de masse utilisent des techniques relativement peu sophistiquées. Parmi les plus connues, on peut citer l'« hameçonnage[2] » (*phishing*), souvent employé pour usurper des informations nécessaires au paiement. Une autre attaque, fréquente et facile à mettre en œuvre, consiste à saturer les accès à un système par une attaque dite « distribuée » (*distributed denial of service* – DDoS), ce qui bloque, par exemple, la connexion à un site internet ou perturbe le service. Au contraire, les attaques ciblées visent des objectifs précis, généralement soigneusement choisis. Leur mise en œuvre se révèle beaucoup plus complexe, à la fois par la connaissance de la « victime » qu'elle requiert et par les techniques employées. Ces attaques reposent le plus souvent sur l'infiltration de logiciels espions ou malveillants (*malware*)[3], qui s'installent dans un système d'information pour y voler des données ou les détruire.

Cependant, quels que soient la sophistication des attaques et le caractère novateur de leur mode opératoire, leurs motivations restent inchangées. Les objectifs visés sont essentiellement de trois types : (1) l'intérêt financier direct (fraude par vol ou manipulation de données bancaires), (2) la nuisance à l'établissement par l'atteinte à sa réputation (sabotage, blocage, atteinte à l'image *via* la défiguration du site internet) ou (3) l'espionnage, qui peut être pratiqué par un concurrent ou une puissance économique étrangère. Quels que soient leurs objectifs, ces attaques menacent la confidentialité, l'intégrité ou la disponibilité des données informatiques. Ces types d'atteintes à la sécurité informatique sont identifiés depuis longtemps et constituent l'ossature de tous les dispositifs de protection. Les établissements financiers, les banques comme les assurances, y sont fortement sensibilisés. L'effort à fournir

consiste donc principalement en la nécessité de s'adapter aux nouvelles techniques d'attaques recensées et d'anticiper les techniques encore plus sophistiquées qui pourraient suivre.

L'intensification des menaces requiert cependant un renforcement des mesures de protection

Malgré l'absence de chiffres fiables concernant le recensement des cyberattaques, les différentes sources existantes s'accordent sur leur augmentation. En outre, c'est aussi la diversité des techniques utilisées qui retient l'attention. La fraude n'est plus le seul but d'attaque. Le blocage des sites ou le vol de données prennent de l'ampleur.

Depuis l'essor du commerce et de la banque en ligne au début des années 2000, les fraudeurs ont tenté d'usurper des données d'identification et des mots de passe de la clientèle (cartes de paiement ou comptes bancaires), afin de réaliser à leur profit des paiements frauduleux. Des vols massifs de données de cartes ont ainsi pu être observés, notamment aux États-Unis. L'usurpation de mots de passe de banque en ligne par *phishing* s'est également intensifiée. Le montant de la fraude est toutefois resté jusqu'à présent plutôt contenu, notamment en Europe où le niveau de sécurité des techniques d'authentification a été constamment relevé.

Les attaques destinées à bloquer les sites de banque en ligne se sont dans le même temps développées. Depuis 2012, les attaques de type DDoS n'ont cessé de se banaliser et sont désormais devenues courantes. Récemment, la plus retentissante de ces attaques a visé les grandes banques finlandaises en juillet 2014. Ce type d'attaques ne requiert plus comme autrefois de grandes puissances informatiques, mais peut être mené maintenant avec de simples *kits* de logiciels vendus illégalement sur Internet.

Les attaques portant atteinte à la confidentialité des données représentent aujourd'hui une menace forte, tant pour les établissements bancaires (comme l'illustre le cas de la banque américaine JP Morgan en 2014[4]) que pour les organismes d'assurance. Les données personnelles dont disposent ces derniers (informations médicales notamment, mais également données sur le patrimoine des clients) pourraient se révéler particulièrement lucratives en permettant, par exemple, d'établir de fausses déclarations d'assurance-santé. L'un des plus importants assureurs-santé américain Anthem a ainsi annoncé en février 2015 avoir été victime d'une attaque informatique touchant à la confidentialité des données privées de dizaines de millions d'assurés.

Désormais, la menace la plus grande est très sophistiquée et furtive, d'où l'appellation « *advanced persistent threat* » (APT). Ce type d'attaques, combinant des techniques avancées d'intrusion et d'usurpation

de droits, pourrait permettre aux pirates d'accéder aux applicatifs et aux bases de données les plus sensibles pour les institutions. Dans le cas d'une banque, il pourrait s'agir, par exemple, des applications liées à la tenue des comptes, à la gestion des espèces dans les circuits de distribution ou aux flux de paiements de masse. Une attaque réussie de ce type pourrait entraîner des dommages considérables pour un établissement, à la fois financiers et de réputation susceptibles de faire peser un risque sur sa continuité d'activité, voire sur la stabilité financière. Des attaques de ce type (appelées « Carbanak »), lancées principalement contre des banques russes, mais aussi contre quelques banques européennes, ont été découvertes en 2015. L'analyse a révélé que de telles attaques permettaient à leurs initiateurs de prendre le contrôle à distance de certains systèmes des banques (en l'occurrence les automates de distribution de billets), leur causant un préjudice financier immédiat élevé[5]. Toutefois, ces impacts n'auraient pas mis en péril les institutions financières touchées.

QUELLES SONT LES ACTIONS ENTREPRISES PAR LES INSTITUTIONS FINANCIÈRES ?

La réglementation relative au contrôle interne et à la gestion du risque opérationnel constitue un cadre de référence toujours pertinent

Les exigences de sécurité du système d'information constituent une préoccupation déjà ancienne du superviseur dans le secteur bancaire, comme en attestent le *Livre blanc sur la sécurité des systèmes d'information dans les établissements de crédit* publié par la Commission bancaire en 1996, puis le Livre blanc *Internet, quelles conséquences prudentielles ?* paru en 2001. Du point de vue réglementaire, si le terme « cybersécurité » n'est pas mentionné en tant que tel, le risque lié à la cybercriminalité est néanmoins bien appréhendé d'abord dans le cadre plus large des exigences qualitatives qui s'appliquent en termes de contrôle interne, puis de celles relatives à la prévention du risque opérationnel qui ont intégré des exigences quantitatives.

En effet, les établissements de crédit français doivent depuis longtemps se conformer à des exigences détaillées relatives à la mise en place d'un dispositif de contrôle interne. Le règlement n° 97-02 du Comité de la réglementation bancaire et financière, datant de février 1997, a donné très tôt au superviseur – à l'époque de la Commission bancaire – une base juridique pour s'assurer de l'existence au sein des établissements d'un dispositif de contrôle des systèmes d'information. Ces dispositions ont été progressivement enrichies par la suite, en 2005 et 2007, avant d'être intégralement reprises par l'arrêté du 3 novembre 2014 relatif au contrôle interne, à la suite de l'entrée en vigueur de la

directive CRD IV[6]. Les amendements de 2005, en particulier, ont introduit de nouvelles exigences relatives à l'évaluation de la sécurité informatique (obligation de revue périodique de leur niveau de sécurité par les établissements, obligation de mise en place de procédures de continuité d'activité) et ont ajouté les bases des contrôles de sécurité informatique relatives à l'intégrité et à la confidentialité des données.

En plus de ces exigences qualitatives imposées par la réglementation française, les accords de Bâle II, adoptés en 2006 et entrés en vigueur en France avec l'arrêté du 20 février 2007 transposant la directive CRD III, ont introduit des exigences en fonds propres au titre du risque opérationnel, qui englobent notamment les pertes éventuelles relatives à la cybercriminalité : le risque opérationnel vise en effet explicitement les cas de fraude ou de défaillance des systèmes, incluant le risque informatique et les atteintes à la sécurité des systèmes d'information[7].

Par ailleurs, dans le cadre de la transposition des directives européennes sur les services de paiement et sur la monnaie électronique[8], des exigences en matière de sécurité des moyens de paiement, visant notamment à limiter les risques de fraude, ont été posées. Toutes les demandes d'agrément d'établissements de paiement et de monnaie électronique – et notamment celles qui concernent les *start-up* spécialisées dans les nouvelles technologies, les FinTech – font l'objet d'une analyse approfondie des moyens mis en œuvre pour assurer cette sécurité. Un avis de la Banque de France, en charge, dans le cadre de ses missions, de la sécurité des moyens de paiement, est d'ailleurs explicitement requis. Ces règles de sécurité font, elles aussi, l'objet d'une adaptation permanente tenant compte du développement des nouvelles technologies. En témoignent l'orientation de l'Autorité bancaire européenne sur la sécurité des paiements sur Internet, issue des travaux du SecurePay[9], et les nouvelles exigences posées dans le cadre de la révision de la directive sur les services de paiement (DSP2), qui intégrera dans son périmètre d'application de nouveaux acteurs tels que les agrégateurs et les initiateurs de paiement.

Pour le secteur de l'assurance, les dispositions relatives au contrôle interne permettaient également au superviseur de contrôler notamment les dispositifs de maîtrise des risques pesant sur les systèmes d'information. Désormais, le nouveau cadre prudentiel Solvabilité II, qui entrera en vigueur à partir du 1er janvier 2016, vise à ce que les organismes d'assurance mesurent plus précisément l'ensemble de leurs risques. À ce titre, les risques opérationnels liés aux systèmes d'information doivent désormais être mieux évalués et davantage encadrés, comme dans le domaine bancaire : les organismes doivent disposer d'un système de gestion des risques qui préserve en particulier la sécurité, l'intégrité et la confidentialité des informations.

Les banques et les assurances adaptent leurs dispositifs de protection et développent une activité de veille

L'adaptation des banques au risque de cyberattaques

En application de la réglementation bancaire, les établissements ont ainsi dû définir leur stratégie informatique, sous la responsabilité de leurs instances dirigeantes, en tenant compte des exigences de sécurité nécessaires à la protection de leurs systèmes. Ils ont dû établir un cadre général de mesure et de réduction des risques, qui englobe le risque informatique et la sécurité du système d'information. Leur responsable de la sécurité des systèmes d'information (RSSI) élabore des politiques de sécurité et recommande des mesures techniques (cryptage des données, gestion des accès, etc.). Des dispositifs de contrôle interne et de recensement des incidents ont été également mis en œuvre pour veiller à l'adaptation des mesures destinées à maîtriser ces risques. En parallèle, des plans de continuité de l'activité ont dû être établis et régulièrement testés. Les quelques établissements ayant opté pour des approches de mesure avancée du risque opérationnel ont en outre la possibilité de spécifier des scénarios de risque afin de mieux quantifier les charges en capital nécessaires à la couverture du risque résiduel.

La mise en place effective de ces dispositions réglementaires, qui constituent l'ossature des exigences prudentielles en matière de sécurité informatique, est généralement bien établie. L'émergence des nouvelles techniques de cybercriminalité conduit cependant les banques à devoir adapter et renforcer leurs dispositifs. De nouvelles politiques et de nouvelles solutions doivent être élaborées en conséquence, visant en particulier le renforcement de l'expertise et la sensibilisation de l'ensemble du personnel ainsi que la mise en œuvre régulière d'exercices de crise avec des tests sur les dispositifs de gestion.

À cet égard, la participation des principales banques françaises à des tests de place constitue l'une des initiatives concrètes dans le domaine de la prévention des risques liés à la cybercriminalité. L'exercice conduit en novembre 2012 avait permis aux banques françaises d'évaluer l'impact d'une cyberattaque[10] sur leurs processus critiques, en y associant les grandes infrastructures de marché. Ce type d'exercice collectif permet de vérifier que les différents plans de continuité offrent une cohérence d'ensemble et sont bien adaptés à des menaces en constante évolution.

Cependant, la mise en place de dispositifs de protection ayant pour objectif l'inviolabilité des systèmes n'est ni réaliste ni suffisante pour gérer adéquatement les risques liés aux cyberattaques. C'est pourquoi les banques doivent désormais adopter des stratégies de protection proactives qui comportent à la fois une activité de veille afin de repérer

les cybermenaces dans l'environnement et une activité de prévention opérationnelle pour définir les moyens qui permettraient de contrer les attaques (cf. encadré 1).

Encadré 1
Équipes de détection et équipes de réaction

Face à la cybermenace, la détection des attaques et la capacité à réagir rapidement sont essentielles. Ces actions de sécurité informatique se sont progressivement structurées depuis la naissance d'Internet et l'apparition des premiers « virus » informatiques au début des années 1990. Aujourd'hui, les administrations et les grandes entreprises du monde entier s'organisent en interne et conjuguent aussi leurs efforts en partageant de l'information sur les nouvelles menaces identifiées. Les principaux établissements du secteur financier en France participent à ces réseaux d'échanges et disposent d'équipes capables d'intervenir. Ce type d'activité est également réalisé par des prestataires spécialisés. Il existe deux types d'équipes :

– les centres opérationnels de sécurité (COS) (*security operating centers* – SOC) sont chargés de la veille sécuritaire sur les plates-formes logicielles et matérielles. Ils ont la responsabilité de la détection des attaques et de toute anomalie pouvant conduire à reconnaître une action malveillante sur le système d'information. Pour une meilleure efficacité, ils comportent parfois en leur sein une équipe chargée de tester la sécurité (équipe dite d'« attaque ») et une équipe chargée de détecter au plus tôt les attaques (équipe dite de « défense »). Leur rôle est désormais crucial pour permettre une intervention rapide et contrer les attaques ;

– les équipes de réponse aux incidents de sécurité informatique, plus connues sous leur acronyme anglais CSIRT (*computer security incident response teams*), sont, quant à elles, chargées d'intervenir en cas d'incident. Les CSIRT exploitent donc les alertes produites par les COS, ainsi que d'autres alertes reçues par d'autres canaux pouvant signaler des anomalies. Ils peuvent se faire reconnaître par des réseaux internationaux comme le FIRST (Forum for Incident Response and Security Teams), le CERT (Computer Emergency Response Teams) ou le TF-CSIRT en Europe, afin de développer les capacités d'échange d'informations. Le CSIRT a la charge de l'analyse des alertes et la mise en œuvre d'une réponse appropriée. Au niveau national, l'ANSSI pilote le CERT-FR qui opère pour les administrations françaises et accompagne l'action du CERT des grandes entreprises (cf. encadré 2 ci-contre).

Encadré 2
Loi de programmation militaire et rôle de l'ANSSI

En France, la loi de programmation militaire du 18 décembre 2013 reprend les orientations du *Livre blanc sur la défense et la sécurité nationale* parues la même année. Afin de prendre en compte les risques pour la nation des cyberattaques, elle détaille les dispositions relatives à la protection des infrastructures vitales contre la cybermenace.

Cette loi s'applique aux « opérateurs d'importance vitale » (OIV), qu'ils soient privés ou publics, et qui sont désignés pour chaque secteur d'activité d'importance vitale (SIV) par arrêté du ministre coordonnateur (ministre de l'Économie et des Finances pour le secteur financier). Elle oblige notamment les OIV à mettre en œuvre des mesures de sécurité, à déclarer immédiatement tout incident affectant le système d'information et à se soumettre à des audits de leurs systèmes à la demande du Premier ministre (pas de périodicité explicitement imposée) par l'ANSSI ou autre service de l'État.

L'autorité nationale chargée de la défense des systèmes d'information est l'ANSSI, qui est placée sous l'autorité du Premier ministre. Ses missions ont été détaillées dans un décret du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale (décret n° 2015-351). Ce décret inclut notamment des précisions sur les règles de sécurité à appliquer, les modalités de mise en place de systèmes de détection des attaques au sein des OIV, la collecte des incidents de cybercriminalité et enfin les modalités de contrôle de la bonne application de ces règles. Elle prépare la stratégie nationale pour la sécurité numérique, mise à jour en octobre 2015.

L'adaptation des organismes d'assurance au risque de cyberattaques

Les organismes d'assurance n'ont pour l'instant pas été considérés comme une cible privilégiée pour les pirates informatiques, leur activité se prêtant moins naturellement aux détournements de flux financiers. Toutefois, les données gérées par ces organismes représentent une cible potentielle qui ne doit pas être sous-estimée, comme l'actualité récente aux États-Unis a pu le montrer, de même que les actifs gérés sous forme de placements assurantiels.

D'une manière générale, comme pour le secteur bancaire, les dispositifs de sécurité des systèmes d'information des organismes d'assurance doivent combiner approche préventive et approche curative. Les derniers résultats de l'enquête annuelle que l'ACPR réalise depuis 2011

sur l'état de préparation de la place à la nouvelle réglementation Solvabilité II soulignent la prise de conscience par les assureurs de l'importance de ce sujet et mettent en évidence des améliorations progressives dans ce domaine. Les réponses des organismes font ressortir qu'une majorité d'entre eux disposent désormais d'une politique de sécurité informatique, de plans de continuité de l'activité qui s'appuient sur une cartographie des systèmes d'information et des procédures de gestion des risques informatiques. Ainsi, les actions de préparation à Solvabilité II ont contribué au renforcement des dispositifs existants. L'attention portée à la sécurité des systèmes d'information apparaît en outre d'autant plus essentielle que le secteur assurantiel connaît d'importantes restructurations (rapprochements, fusions, acquisitions) qui impliquent de mettre en commun des systèmes d'information auparavant séparés et constituent ainsi un facteur de risque supplémentaire.

LA PRÉVENTION DE LA CYBERCRIMINALITÉ IMPLIQUE UN RENFORCEMENT DE LA COOPÉRATION ENTRE AUTORITÉS

Le rôle du superviseur prudentiel se concentre sur le volet préventif

Il n'entre pas dans la mission du superviseur de réprimer la cybercriminalité. Les pouvoirs publics (forces de police, justice, agences de sécurité) sont les acteurs chargés de lutter contre les activités cybercriminelles. En France, la loi de programmation militaire du 18 décembre 2013 et le décret du 27 mars 2015 confèrent en outre à l'ANSSI un rôle majeur dans la protection des organismes d'importance vitale (cf. encadré 2 *supra*).

Pour sa part, le superviseur veille à la préservation de la stabilité des établissements financiers. C'est à ce titre qu'il se préoccupe de leur cybersécurité. L'attention du superviseur se porte donc principalement, comme on l'a vu, sur les volets préventifs et défensifs de la réponse aux menaces. Il doit faire en sorte de s'assurer que les institutions agissent à la fois sur la réduction de la probabilité d'occurrence d'un dommage et sur l'atténuation de leur dangerosité en cas d'attaque réussie (limitation des impacts par la capacité de restaurer rapidement la qualité d'un système atteint ou encore possibilité de « compartimenter » les systèmes d'information afin d'éviter que les infections se propagent).

Compte tenu de ces différents rôles, la coopération et la coordination de l'ensemble des acteurs impliqués, établissements financiers eux-mêmes inclus, sont nécessaires pour assurer la cohérence et le caractère complet des actions de lutte contre les cyberattaques, de la prévention jusqu'à la répression.

Le contrôle des dispositifs de cybersécurité par le superviseur doit pouvoir s'appuyer sur des équipes spécialisées

Le superviseur prudentiel veille à ce que les établissements sous son contrôle, banques comme assurances, évaluent correctement leur niveau de risque et disposent d'un environnement sécuritaire adéquat au regard des risques que pourrait induire une cyberattaque, afin de limiter au maximum le risque résiduel pour l'entreprise et ses clients.

L'ACPR veille en particulier à ce que les dispositifs mis en place par les établissements – dispositifs de prévention, d'une part, et de gestion des risques avérés et des crises, d'autre part – soient suffisamment solides et efficaces en cas d'attaque. Des enquêtes ciblées peuvent ainsi être menées, comme en 2013, sur les risques associés au *cloud computing,* qui a conduit à interroger plus d'une vingtaine d'entreprises des secteurs de la banque et de l'assurance (ACPR, 2013). Des missions sur place dédiées à la thématique de la sécurité des systèmes d'information menées par des équipes spécialisées sont ainsi régulièrement diligentées, tant du côté des banques que du côté des assurances. Les équipes de contrôle sur place peuvent évaluer très concrètement, à travers, par exemple, le processus de vérification des habilitations aux applications les plus sensibles, si le niveau de protection mis en place par l'établissement ou l'organisme est adéquat en cas d'attaque.

Il est essentiel de préciser que ce type de contrôle par l'ACPR peut également porter sur les prestataires de services informatiques auxquels les banques et les assurances ont recours dans le cadre de l'externalisation de certaines activités (au-delà donc de l'entité juridique assujettie au contrôle de l'ACPR), ce qui permet au superviseur d'avoir une vision globale des différentes « portes d'entrée » de la menace de cyberattaques.

Compte tenu de l'importance prise par ces questions pour l'ensemble de ses domaines d'action, le secrétariat général de l'ACPR a décidé de mettre en place un réseau transversal pour suivre de façon spécifique ce risque et mieux interagir avec ses interlocuteurs au plan national, européen et international.

Les institutions internationales ont l'obligation de coordonner leurs efforts face à l'importance de la menace

Les différentes autorités prudentielles européennes ont désormais toutes intégré le risque lié à la cybercriminalité dans leur cartographie des risques du secteur financier et le classent généralement au rang de priorité élevé. Les analyses menées au sein du Mécanisme de supervision unique (MSU) depuis 2014 ont ainsi évalué le risque lié à la cybercriminalité comme l'une des menaces les plus importantes en termes d'impact potentiel pour les institutions financières. La BCE, en

conséquence, a retenu ce risque comme l'une de ses priorités de supervision pour l'année 2015 et, outre un questionnaire d'autoévaluation adressé aux banques significatives dès le premier semestre, des missions dédiées à ce thème ont été diligentées auprès d'un échantillon de banques sélectionnées, dont des banques françaises. Il est important de noter que les initiatives prises par la BCE s'inscrivent dans une démarche plus générale de redéfinition du risque dit « informatique » au sein du MSU et témoignent d'une volonté forte, d'une part, de renforcer la supervision dans le domaine informatique et, d'autre part, d'harmoniser les pratiques de supervision à travers une méthodologie commune.

Au-delà du seul secteur bancaire, le risque lié à la cybercriminalité demeure un point de vigilance comme le rappelle le rapport du *joint committee* des autorités de supervision européennes de mars 2015 sur les risques et les vulnérabilités du système financier européen. Ce rapport met en exergue le besoin de coopération internationale pour faciliter la surveillance de ce risque avec des orientations convergentes. En effet, les initiatives internationales rendues publiques en matière de cybersécurité sont pour l'heure limitées. On peut principalement relever les recommandations CPMI-IOSCO (BRI, 2014) en matière de cyberrésilience pour les infrastructures de marché financier, mais qui ne sont pas directement applicables aux banques et aux assurances. La Commission européenne a publié en 2014 une stratégie de cybersécurité pour les membres de l'Union européenne, dont l'évaluation des pratiques relatives à la protection des infrastructures essentielles constitue l'élément central.

Au-delà de la vision purement européenne, de nombreux régulateurs et superviseurs étrangers ont engagé des initiatives dans ce domaine (cf. encadré 3).

Encadré 3

Initiatives prises par les régulateurs étrangers et internationaux pour prévenir le risque et créer les conditions d'une réponse concertée

Les régulateurs nationaux comme les régulateurs européens et internationaux ont intégré la problématique de la cybercriminalité dans leur programme de travail. La menace de cyberattaques ne s'arrêtant pas aux frontières, il est également nécessaire d'avoir une approche coordonnée au niveau international.

Aux États-Unis, les régulateurs se sont largement impliqués dans le message d'alerte transmis aux banques de prendre toute la mesure du risque informatique et de ses nouvelles formes et d'y consacrer

autant de ressources que nécessaire. La Federal Rederve (Fed) a délivré ces deux dernières années plusieurs messages de sensibilisation destinés à l'ensemble du secteur financier sur le risque de cybercriminalité et a elle aussi inscrit ce sujet au rang des priorités de son action de supervision. De son côté, l'Office of the Comptroller of the Currency (OCC) prévoit d'utiliser progressivement le résultat d'un test d'autoévaluation dans son programme de contrôle des banques qu'il supervise. Enfin, le Federal Financial Institutions Examination Council (FFIEC) a publié un guide d'évaluation de la cybersécurité pour les organismes financiers en juin 2015.

Au Royaume-Uni, plusieurs exercices de *stress tests* ont été conduits sous l'égide des régulateurs nationaux. D'une part, la Financial Conduct Authority (FCA), la Prudential Regulation Authority (PRA) et la Bank of England (BoE) ont organisé en novembre 2013 un exercice dit « *walking shark II* » qui consistait à simuler une fausse attaque contre le secteur financier afin d'évaluer le degré de résilience du secteur bancaire britannique. D'autre part, un test d'évaluation (CBEST), fruit d'une coopération entre l'industrie et les institutions financières (BoE, FCA et Trésor britannique), est proposé aux grandes institutions pour évaluer leur degré de préparation face à une attaque informatique. La consolidation de ces informations permet d'évaluer le risque au niveau global.

Enfin, la cybersécurité est aussi un problème mondial : pour apporter une réponse plus efficace, il est nécessaire d'instaurer une coopération à l'échelle internationale. Dans cette perspective, différents groupes d'experts internationaux (auxquels l'ACPR participe) ont inscrit le risque de cybercriminalité à leur agenda de travail.

PLUSIEURS ENSEIGNEMENTS CONCRETS PEUVENT DÉJÀ ÊTRE TIRÉS DES CONTRÔLES MENÉS PAR LE SUPERVISEUR

Les contrôles sur place font ressortir deux points d'amélioration prioritaires : la gestion des droits d'accès et les outils de détection

Les contrôles effectués par les superviseurs font ressortir le besoin de renforcer les dispositifs de protection prioritairement sur deux axes.

Le premier concerne la gestion des droits d'accès aux applications et aux bases de données, ainsi que la gestion des comptes à privilèges. La protection de ces droits est en effet cruciale pour parer des attaques silencieuses comme les APT (*advanced persistent threats*) qui peuvent permettre de récupérer des données sensibles. Pour ce faire, le code malveillant de l'attaquant doit usurper des droits d'accès à ces données ou aux applications qui les gèrent. S'il parvient à détourner ou à casser

les mots de passe des employés de la banque habilités sur un environnement, il peut bénéficier de leurs droits de gestion sur cet environnement (en lecture, en écriture, voire en suppression). L'attaquant peut aussi viser des comptes privilégiés, qui sont ceux qui ont la faculté d'attribuer des droits aux utilisateurs ou aux informaticiens intervenant sur un environnement. Ces comptes privilégiés présentent un niveau de sensibilité encore plus élevé car leur usurpation par un attaquant permettrait à celui-ci de gérer le système et, par exemple, de créer des faux comptes utilisateurs pour lui-même. Depuis longtemps, la gestion des droits d'accès et des comptes à privilèges est un sujet d'attention pour le superviseur et pour les responsables de sécurité informatique des établissements. Pour autant, les mesures recommandées étaient inspirées à l'origine par des scénarios qui se concentraient sur des usurpations résultant d'une infiltration interne, par exemple par un salarié indélicat. La menace liée à la cybercriminalité oblige à repenser ces mesures car l'usurpation des droits peut être réalisée par un attaquant externe ayant réussi à entrer dans le système d'information en bénéficiant des nombreuses connexions informatiques qui existent aujourd'hui.

L'ampleur des travaux est considérable et se heurte à plusieurs difficultés : les systèmes d'information des établissements de banque et d'assurance sont particulièrement vastes et interconnectés ; certains composants sont anciens et gérés sur des technologies permettant difficilement une gestion individuelle des droits ; l'infogérance est un phénomène répandu et il peut être difficile d'obtenir concrètement un niveau élevé de sécurité sur des éléments du système d'information qui sont administrés par des sous-traitants. Les préconisations que le superviseur peut être dès lors amené à formuler consistent principalement à renforcer les règles d'administration des droits d'accès, en privilégiant une liaison directe avec les systèmes de gestion du personnel et à mieux isoler d'Internet les postes des administrateurs informatiques.

Le second point crucial, complexe techniquement, concerne le développement des outils de détection. Les spécialistes de la lutte contre la cybercriminalité raisonnent désormais sur la base du postulat que l'attaquant pourra probablement réussir à entrer dans le système informatique ciblé et qu'il importera donc surtout de parvenir à détecter sa présence en reconnaissant le code malveillant ou des actions anormales. Depuis les débuts de l'informatique, la traçabilité était une préoccupation, mais principalement pour assurer la preuve des opérations effectuées. Désormais, elle devient une préoccupation destinée à surveiller les réseaux, les applications et les bases de données. Les codes malveillants présentent des caractéristiques typiques qui peuvent être reconnues par des sondes de surveillance. L'analyse et la corrélation des

traces peuvent permettre d'alerter les équipes de surveillance et de repérer des attaques. L'enjeu est de taille puisqu'il s'agit désormais de développer de véritables stratégies de surveillance et d'inclure dans le champ de celles-ci les systèmes applicatifs et les bases de données devant être protégés.

L'ACPR oriente plus généralement son action dans quatre directions

Inciter les institutions supervisées à s'organiser efficacement pour répondre à la menace de cyberattaques

Les solutions face à la menace de cyberattaques devraient d'abord émaner du secteur financier lui-même. C'est pourquoi l'ACPR encourage les initiatives des banques et des assurances en la matière et requiert aussi des mesures correctives lorsqu'elle détecte des insuffisances. Les établissements doivent d'abord mettre en place une organisation interne robuste : un positionnement adéquat et des moyens suffisants doivent être garantis aux RSSI, dont l'action constitue un élément clé pour une bonne maîtrise des risques informatiques, notamment ceux liés à la cybercriminalité. L'autorité de cette fonction n'est toutefois pas encore suffisamment reconnue au sein des établissements et leur indépendance n'est pas systématiquement garantie par un rattachement hiérarchique approprié. Les établissements doivent ensuite s'organiser en externe, en collaborant avec leurs pairs dans l'identification des nouvelles menaces, en vue de l'adoption des meilleures pratiques en matière de détection et de protection.

Améliorer l'identification de la menace avec un recensement centralisé des attaques au niveau européen

Face aux enjeux posés par les cyberattaques, un axe de progrès consisterait dans la mise en place d'un recensement centralisé des incidents au niveau européen ainsi que leur communication aux autorités nationales compétentes, dès l'identification de la menace, avérée ou potentielle, et dans des conditions de confidentialité à définir. Les données collectées pourraient ainsi être utilisées à des fins microprudentielles, permettant aux autorités de mieux appréhender la capacité individuelle des banques et des assurances à répondre à ce type de menaces, mais également macroprudentielles, dans l'objectif de recueillir des données statistiques afin de mesurer l'évolution des attaques et leur sévérité et aussi d'éviter le risque de contagion en cas de crise importante. Cela pourrait également constituer un moyen d'identifier les meilleures pratiques en termes de protection et de les partager avec les institutions financières, afin d'améliorer la résilience d'ensemble de la sphère financière.

Adapter le suivi du risque opérationnel pour mieux tenir compte des spécificités du risque de cyberattaques

Comme nous l'avons vu, la supervision prudentielle aborde historiquement la sécurité informatique sous l'angle du contrôle interne et de la gestion du risque opérationnel. La logique de contrôle permanent du risque opérationnel a donc été naturellement appliquée en matière de sécurité informatique : après l'élaboration d'une cartographie des risques et la mise en place de contrôles ciblés, un risque résiduel est évalué et des exigences en fonds propres sont calculées pour couvrir les conséquences financières éventuelles d'un incident opérationnel.

La spécificité des cybermenaces, d'occurrence rare, difficiles à détecter, mais à très fort impact, conduit aujourd'hui à s'interroger sur les limites de cette approche, même si elle tient compte en partie de la qualité et de la sophistication des dispositifs de suivi des risques, et sur les moyens de la renforcer. La soudaineté et la nature de certaines attaques pourraient en effet gravement perturber une institution financière sans forcément causer une perte financière, rendant inopérante une approche principalement basée sur la mesure d'une charge en fonds propres. Il conviendrait donc de renforcer les dispositifs de contrôle interne par des exigences accrues en termes de capacité de détection des menaces et de traitement plus rapide des risques dès leur identification.

Favoriser la coopération entre tous les acteurs publics ou privés

Étant donné les répercussions qu'une cyberattaque de grande ampleur pourrait avoir, il est enfin nécessaire qu'une collaboration efficace s'installe entre les établissements financiers, leurs superviseurs et les banques centrales et les autres autorités publiques impliquées, comme l'ANSSI en France. L'ACPR considère ainsi comme primordiale la mise en œuvre d'une approche coopérative et coordonnée pour assurer en France la robustesse du système financier, bancaire et de l'assurance. En lien étroit avec la Banque de France, elle encourage les initiatives de place visant à tester le niveau de préparation des institutions financières face à des menaces en constante évolution. L'accroissement des interdépendances mondiales dans le domaine financier rend également nécessaire la coordination des actions au plan international entre les superviseurs.

NOTES

1. On entend par système d'information (SI) l'ensemble des ressources, qu'elles soient matérielles (serveurs, postes de travail, etc.), logicielles et/ou informationnelles (données informatiques, documents papiers, etc.).

2. Cette technique repose sur l'envoi de *spam*, c'est-à-dire l'envoi massif de courriels non sollicités à un grand nombre de personnes, afin d'en abuser certaines qui n'auraient pas une protection informatique suffisante.

3. Logiciel utilisé par des cyberattaquants pour porter atteinte à l'intégrité d'un système d'information par la destruction, le vol ou l'altération de données contenues dans un système d'information.

4. Vol des coordonnées personnelles d'environ 80 millions de clients (personnes physiques et PME).

5. Les experts estiment que l'attaque Carbanak s'est soldée par des retraits frauduleux et des virements d'un montant compris entre 300 M$ et 1 Md$, qui ont touché une centaine de banques dans trente pays. Par comparaison, l'attaque Anunak a concerné une cinquantaine de banques russes et causé un préjudice de 25 M$ en 2014.

6. Directive 2013/36/UE du Parlement européen et du Conseil européen du 26 juin 2013 concernant l'accès à l'activité et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, dite en anglais « CRD IV » (*Capital Requirements Directive IV*).

7. Le risque opérationnel se définit en effet comme « le risque de pertes découlant d'une inadéquation ou d'une défaillance des processus, du personnel et des systèmes internes ou d'événements extérieurs, y compris le risque juridique » (article 4, point 52, du règlement UE 575/2013 (CRR)).

8. Les directives européennes sur les services de paiement (DSP) et sur la monnaie électronique (DME), adoptées respectivement en 2007 et en 2009 et transposées dans le droit français en 2009 et 2013, fournissent le cadre juridique nécessaire à la mise en place d'un marché européen unique des paiements. Elles visent à instaurer un ensemble complet et détaillé de règles applicables à tous les services de paiement dans l'Union européenne.

9. European Forum on the Security of Retail Payments ou SecuRe Pay est un groupe de travail précédemment piloté par la BCE, puis coprésidé avec l'Autorité bancaire européenne depuis l'automne 2014.

10. Le scénario de cet exercice était une cyberattaque visant les plates-formes internes utilisées pour les transactions financières des banques et aboutissant à une paralysie de la place de Paris.

BIBLIOGRAPHIE

ACPR (Autorité de contrôle prudentiel et de résolution) (2013), « Les risques associés au *Cloud computing* », *Analyses et Synthèses*, n° 16, juillet.

ANSSI (Agence nationale pour la sécurité des systèmes d'information) (2015), *Comprendre et anticiper les attaques DDoS*, mars, www.ssi.gouv.fr/uploads/2015/03/NP_Guide_DDoS.pdf.

Banque de France (2012), *Rapport du Groupe de Place - Exercice de Place des 21 et 22 novembre 2012*, www.fbf.fr/fr/files/92HJ84/Rapport-exercice-de-place-2012.pdf.

Banque de France (2014), discours d'ouverture de Robert Ophèle, sous-gouverneur de la Banque de France, à la conférence « La cybersécurité dans le secteur financier », 17 juin, www.banque-france.fr/uploads/tx_bdfgrandesdates/discours-Robert-Ophele-20140617.pdf.

BoE (Bank of England), www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx.

BRI (Banque des règlements internationaux) (2014), *Cyber Resilience in Financial Market Infrastructures*, rapport, 11 novembre, www.bis.org/cpmi/publ/d122.pdf.

Comité de Bâle (2011), *Principles for the Sound Management of Operational Risk*, juin, www.bis.org/publ/bcbs195.pdf.

COMMISSION BANCAIRE (1996), *Livre blanc sur la sécurité des systèmes d'information dans les établissements de crédit*, mars, www.banque-france.fr/fileadmin/user_upload/banque_de_france/archipel/publications/cb_livbl/cb_livbl_securite.pdf.

CPMI (Committee on Payments and Market Infrastructures) (2014), *Cyber Resilience in Financial Market Infrastructures*, novembre, www.bis.org/cpmi/publ/d122.pdf.

ESA (Joint Committee of the European Supervisory Authorities) (2015), *Joint Committee Report on Risks and Vulnerabilities in the EU Financial System*, mars, www.esma.europa.eu/system/files/jc_2015_007_jc_report_on_risks_and_vulnerabilities_in_the_eu_financial_system.pdf.

GRACIE A. (2014), « Managing Cyber Risk – The Global Banking Perspective », discours délivré à la Bank of England le 10 juin, www.bankofengland.co.uk/publications/Documents/speeches/2014/speech735.pdf.

KASPERSKY LAB (2015), *Carbanak APT the Great Bank Robbery*, février, http://securelist.com/files/2015/02/Carbanak_APT_eng.pdf.

MARCELLIN S. (2015), « Cybersécurité : notification des incidents de sécurité », *Revue Banque* & *Droit*, n° 161.

MCAFEE (2014), *Report on the Global Cost of Cybercrime*.

MINISTÈRE DE LA DÉFENSE (2013), *Livre blanc sur la défense et la sécurité nationale*, 29 avril, www.defense.gouv.fr/actualites/la-reforme/livre-blanc-2013.

NIST (National Institute of Standards and Technology) (2014), *Framework for Improving Critical Infrastructure Cybersecurity*, 12 février, www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

QUÉMÉNER M. (2015), *Criminalité économique et financière à l'ère numérique*, Economica, juin.