BANQUE DE FRANCE
EUROSYSTÈME

CONFÉRENCE « LA CYBERSÉCURITÉ DANS LE SECTEUR FINANCIER »
17 juin 2014

Discours d'ouverture[1] de Robert Ophèle, Sous-gouverneur de la Banque de France

Mesdames et messieurs, je suis très heureux d'inaugurer cette conférence traitant de la cybersécurité dans le secteur financier. Ce sujet pourrait être jugé de prime abord comme très technique, et de nature à n'être abordé que dans le cadre restreint d'une réunion d'experts. Ce serait une erreur et il importe au contraire que les autorités publiques, y compris les banques centrales, prêtent une attention suffisante à la cybersécurité, compte tenu de ses implications à l'échelle du système, notamment pour le fonctionnement du système financier.

Au cours des dix dernières années, le secteur financier a changé profondément avec l'apparition d'internet et l'utilisation des nouvelles technologies de l'information. Le marché s'est montré capable d'innover et d'améliorer la qualité, les performances et l'efficience de services, tels que la banque en ligne, les paiements par téléphone mobile et les plates-formes de règlement-livraison. Les autorités publiques ont en effet encouragé la dématérialisation dans le secteur financier afin de favoriser la croissance économique ainsi que pour réduire les risques opérationnels inhérents aux procédures antérieurement non automatisées. Par exemple, le nouveau règlement européen relatif aux *dépositaires centraux de titres* nécessite de recourir à des titres dématérialisés et encourage le traitement automatique de bout en bout dans les systèmes de règlement-livraison de titres.

En ce sens, les évolutions technologiques ont permis de faire face à certains risques opérationnels inhérents aux activités financières, notamment de réduire les erreurs d'exécution dans les procédures (qui représentent une source importante de pertes liées aux risques opérationnels). De ce point de vue, la cyberactivité est une source de croissance économique et de progrès, essentielle pour le secteur financier.

Toutefois, bien que le développement d'internet et la croissance des transactions électroniques aient permis de mieux contrôler les risques opérationnels grâce à la réduction des facteurs d'erreurs humaines ou opérationnelles, il a également fait émerger de nouveaux risques. La rapide expansion

[1] Emmanuelle Assouan, Frédéric Hervo, Claudine Hurman, Caroline Keribin, Clément Martin et Axel Petitprez ont également contribué à l'élaboration de ce discours

des réseaux et des technologies, l'ouverture des systèmes d'information aux échanges externes, le nombre croissant de transactions électroniques ont provoqué l'émergence d'une nouvelle forme de criminalité, la « cybercriminalité ».

Le secteur financier est effectivement une cible attrayante pour les cybercriminels : une étude américaine[2] menée par Symantec montre que le secteur de la finance et de l'assurance est l'un des principaux secteurs visés par les cyberattaques, juste après l'Administration publique. Cela n'a bien entendu pas échappé aux autorités de surveillance, qui ont déjà pris un certain nombre de mesures pour aider le secteur à résoudre ce problème, mais qui rencontrent certaines difficultés à y faire face.

I. De fait, les orientations émanant des autorités de surveillance, comme celles relatives au risque opérationnel publiées par le Comité de Bâle en 2011[3], soulignent que la prévention et la bonne gestion de ce risque relèvent de la stabilité financière, dans la mesure où les défaillances opérationnelles peuvent être source de risque systémique.

Le risque systémique découle en premier lieu du développement spectaculaire des interdépendances entre intermédiaires financiers lié à l'automatisation accrue des activités financières, notamment les activités de compensation et de paiement, qui sont un des principaux vecteurs d'interconnexion.

Ce risque résulte également de la possible perte de confiance du grand public dans les paiements électroniques pouvant être causée par un défaut de protection de l'intégrité et de la fiabilité des données traitées par ces systèmes.

Cela étant, les réponses aux cybermenaces peuvent entrer en conflit avec d'autres priorités établies, tout particulièrement en ce qui concerne les infrastructures de marchés financiers. Par exemple, le principe 17 du CSPR–OICV relatif au risque opérationnel définit clairement les exigences de continuité d'exploitation pour les infrastructures de marchés financiers. Les plans de continuité opérationnelle doivent avoir pour objectif la reprise rapide des opérations, un redémarrage de l'activité dans les deux heures suivant l'interruption, et la garantie d'un règlement avant la fin de la journée dans les conditions extrêmes. Toutefois, le respect de cette exigence soulève des difficultés particulières en cas de cyberattaque ou d'altération des données, la priorité absolue n'étant alors pas de reprendre rapidement les opérations, mais d'abord de restaurer la qualité et l'intégrité des données pour éviter tout risque de contagion.

Cela vaut également pour l'autorisation qui pourrait être accordée à des tiers d'accéder à un compte de paiement en ligne afin d'apporter une assistance à l'initiation des paiements. Un accès de cette nature

---

[2] *Internet Security Threat Report* 2014
http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

[3] *Principles for the sound management of operational risk*, (Principes de saine gestion du risque opérationnel), CBCB 2011

favoriserait la concurrence et l'innovation dans le secteur des paiements, mais multiplierait de toute évidence les risques de cyberattaques.

En outre, il est nécessaire de trouver le juste équilibre entre la nécessité de prévenir et de gérer correctement les cybermenaces et l'impératif, pour les acteurs acteurs financiers, de mettre en œuvre des solutions économiquement viables. Par exemple, la mise en place d'un double système informatique de secours pourrait constituer une réponse efficace à certaines cyberattaques, mais elle a un coût.

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 et dans les différents secteurs, bien au-delà du secteur financier. Dans cette perspective, il convient de saluer les initiatives du *Financial Stability Oversight Council* (FSOC) aux États–Unis visant à améliorer la coopération entre les secteurs, en particulier ceux qui dépendent du secteur financier, comme les secteurs des services collectifs ou des télécommunications, ou la création de l'Agence européenne chargée de la sécurité des réseaux et de l'information.

II. Dans ce contexte, comprendre les menaces, organiser la protection et la prévention ainsi que la coordination des actions privées et publiques sont des conditions préalables à une lutte efficace contre la cybercriminalité. L'objectif de la session d'aujourd'hui est de réfléchir collectivement sur ce thème et de mettre en commun nos expériences.

La première étape importante est de comprendre pourquoi le secteur financier est une cible de prédilection des attaques des pirates informatiques. C'est l'un des objectifs assignés au premier groupe d'intervenants de haut niveau. Ils vont tenter de répondre à des questions comme : quels sont les facteurs qui font du secteur financier une cible privilégiée pour la cybercriminalité ? Comment détecter et quantifier les cyberattaques ? Quels sont les incidences de la cybercriminalité sur la stabilité financière ?

Un sujet doit retenir particulièrement notre attention: les monnaies virtuelles. Les récentes opérations de lutte contre la délinquance financière ont montré que les nouveaux modes de paiements faisant appel à internet, et reliant la sphère virtuelle à la sphère réelle, représentent pour les cybercriminels un moyen privilégié pour blanchir de l'argent. Ainsi, les monnaies virtuelles ont récemment attiré l'attention des autorités et, en particulier, celle des banques centrales. Conçues comme des alternatives

aux monnaies officielles mais sans garantie de remboursement, elles ne peuvent pas être répertoriées comme des monnaies parce qu'elles n'ont pas cours légal et n'empiètent donc pas sur le monopole d'émission de la monnaie par la banque centrale. Toutefois, même si elles ne constituent pas pour l'instant une menace importante pour la stabilité financière, elles soulèvent de graves problèmes en termes de blanchiment d'argent et peuvent être perçues comme des véhicules destinés à des investissements spéculatifs. Par conséquent, la réglementation des monnaies virtuelles représente un défi pour les autorités. Les questions abordées par les intervenants qui traiteront de ce sujet pourraient être, par exemple : Devons-nous interdire l'utilisation des monnaies virtuelles pour nous protéger de la cybercriminalité et du développement du blanchiment d'argent et du terrorisme ? Ou vaut-il mieux définir la problématique juridique, réglementaire et éthique que soulèvent les monnaies virtuelles ?

Ces interventions seront suivies d'une table ronde consacrée aux solutions envisagées par le secteur financier pour contrecarrer les nouvelles stratégies des cybercriminels. Dans quelle mesure les orientations et les principes en vigueur permettent-ils de gérer la menace que représente la cybercriminalité ? Peut-on réellement décourager la cybercriminalité ou tout au moins s'en défendre ? Les institutions financières ont-elles pris des mesures structurelles et technologiques efficaces pour améliorer leur cyberdéfense ? L'assurance contre la cybercriminalité fonctionne-t-elle et comment le risque est-il valorisé ? De quel type de communication destinée au public avons-nous besoin pour lutter contre ces nouvelles menaces ? Nos débats devraient aborder ces questions fondamentales.

En outre, les autorités de surveillance et de contrôle doivent s'assurer qu'au niveau individuel, la gestion du risque est efficace. Un cadre normatif a été mis en place par les institutions européennes pour lutter contre la cybercriminalité et garantir la robustesse des marchés financiers (notamment grâce à l'adoption par le Parlement européen de la directive concernant la sécurité des réseaux et de l'information) ; un comité de la BRI, le CSPR, est en cours de réflexion sur la cybersécurité des infrastructures de marché. Dans un échange de vues, deux éminents intervenants nous indiqueront s'ils estiment que le cadre réglementaire existant offre une garantie suffisante contre la cybercriminalité.

Enfin, en tant que banque centrale, il est de la plus haute importance de s'assurer que le marché peut résister à des cybermenaces. La dernière table ronde s'attachera à déterminer dans quelle mesure la

résistance des places financières doit évoluer sous l'influence des menaces que représente la cybercriminalité : l'accroissement des interdépendances transfrontières entre les places financières (utilisation d'infrastructures de marché communes, existence d'acteurs financiers de dimension internationale et de fournisseurs transnationaux) nécessite-t-il une approche internationale ? Faut-il réfléchir également à une approche multi-sectorielle, la dépendance vis-à-vis de fournisseurs d'accès communs (comme les opérateurs de télécommunication) créant une importante communauté d'intérêt autour de l'enjeu de la cybersécurité ? Ces réflexions devraient, je l'espère, renvoyer aux priorités définies par la Banque de France, qui consistent à promouvoir une approche coopérative et coordonnée pour assurer la robustesse de la place financière de Paris et à vérifier, grâce à des tests de résistance collectifs, que les différents plans de continuité offrent une cohérence d'ensemble et sont bien adaptés à des menaces en constante évolution.

Enfin, pour conclure, et je m'arrêterai là, j'aimerais attirer votre attention sur deux points :

Premièrement, la Banque de France considère véritablement comme une priorité le fait que les actions soient coordonnées au plan international, compte tenu de l'accroissement des interdépendances mondiales.

Deuxièmement, les solutions devraient émaner du secteur financier et la régulation ne devrait être utilisée qu'en cas de défaillance du marché. Les meilleures pratiques en vue d'améliorer la cybersécurité doivent être identifiées et adoptées par les différents acteurs. Les banques centrales pourraient avoir un rôle à jouer dans ce processus ; à titre d'exemple, la Banque de France a recommandé pendant de nombreuses années la mise en œuvre d'une authentification rigoureuse pour protéger les paiements en ligne. De nombreuses attaques peuvent ainsi être efficacement déjouées.

Je vous remercie de votre attention et je vous souhaite des discussions fructueuses et animées sur l'ensemble de ces aspects, dans l'espoir que cette conférence vous donnera une vision exhaustive des enjeux de la cybersécurité et des réactions possibles aux cybermenaces. Je cède maintenant la parole à M. Steve Purser.