Lettre n°73 – Mars 2018 - disponible sur omc.ceis.eu

TABLE DES MATIERES

RUSSIE : PROJET D'UN SYSTEME DNS INDEPENDANT

En novembre 2017, divers médias russes ont annoncé que la Russie avait décidé de mettre en place, d'ici le 1er août 2018, un système de sauvegarde répliquant le système mondial de serveurs racines pour les noms de domaine (DNS, *Domain Name System*), qui peut être utilisé par les BRICS, de manière autonome et hors du contrôle des organisations internationales, notamment de l'ICANN, en cas d'interruption de service généralisée ou ciblant les intérêts de la Russie et de ses alliés[1].

Dans quel contexte s'inscrit ce projet, est-il réalisable, quelles en sont la portée politique et les conséquences opérationnelles ? C'est ce que tente de décrire la présente note.

Le DNS : rôle, gouvernance et risques

Le DNS est un système mondial hiérarchisé et décentralisé dont la fonction principale est de traduire les noms de domaine, plus pratiques à utiliser pour les internautes, en adresses IP, numérotation spécifique au protocole internet qui permet d'atteindre les différents ordinateurs, services ou autres ressources d'Internet, par exemple pour se connecter à un site web ou envoyer un courrier électronique[2].

Ce système est géré par l'Internet Corporation for Assigned Names and Numbers (ICANN), une organisation privée de droit californien à but non lucratif. L'ICANN est en effet chargée, depuis sa création en 1998, de la gestion :

- Des adresses IP ;
- Des noms de domaine de premier niveau, génériques (.com, .net, .org, .info par exemple) ou de codes pays (.be pour la Belgique, .fr pour la France, .ch pour la Suisse par exemple)[3] ;
- Des serveurs racines de premier niveau, qui ont notamment pour fonction de rediriger les flux vers le serveur DNS du niveau concerné après traduction des noms de domaine du premier niveau en adresses IP.

Le monopole de l'ICANN dans la gestion du système DNS est contesté depuis longtemps par certains pays, notamment les BRICS (Brésil, Russie, Inde, Chine et Afrique du Sud). Ainsi, dès 2006, la Chine s'est dotée de son propre système DNS indépendant[4]. En 2012, lors de la Conférence mondiale de l'Union Internationale des télécommunications (UIT), la Russie, avec le soutien des autres membres des BRICS, a proposé de

[1] https://www.rt.com/politics/411156-russia-to-launch-independent-internet/
https://www.rbc.ru/technology_and_media/28/11/2017/5a1c1db99a794783ba546aca

[2] https://www.icann.org/fr/system/files/files/iana-functions-18dec15-fr.pdf

[3] L'enregistrement des noms de domaine de premier niveau génériques et de codes pays peut être délégué à des organismes privés comme par exemple l'Association Française pour le Nommage Internet en Coopération (AFNIC) pour les noms de domaine de premier niveau de France (.fr) : https://www.afnic.fr/fr/l-afnic-en-bref/

[4] http://www.lemonde.fr/technologies/article/2010/02/19/chine-vers-un-grand-schisme-de-l-internet_1308660_651865.html

transférer la gestion des adresses IP et du système DNS aux États[5] mais cette proposition n'a pas été suivie par la majorité des États membres de l'UIT. Les Etats-Unis ont simplement accepté en mars 2016 de renoncer à la tutelle que son département du commerce avait de fait sur l'ICANN, par le biais du contrat fondateur de l'ICANN jusqu'en 2009, puis d'un MoU (Memorandum of Understanding)[6]. L'ICANN est désormais placé sous la gouvernance d'un conseil d'administration multipartite, essentiellement composé des grands acteurs privés du Net.

Malgré sa nouvelle indépendance apparente, l'ICANN reste, aux yeux de nombreux pays, sous la pression des intérêts américains, les GAFAM ayant quasiment remplacé les autorités US.

Le risque que peut représenter l'ICANN sur l'Internet mondial réside dans son pouvoir de blacklister des noms de domaine, en supprimant leur traduction en adresses IP, pour des raisons non légitimes.

La portée politique du projet russe

Depuis les révélations d'Edward Snowden, le gouvernement russe cherche à s'affranchir de la tutelle américaine sur Internet[7], notamment en développant un cyberespace souverain disposant de ses propres infrastructures, avec le RuNet[8]. Elle a lancé en 2014 un projet de copie de sauvegarde des adresses IP, du routage du trafic et du système DNS du RuNet. Puis en 2016, le gouvernement russe a adopté sa doctrine de sécurité informationnelle, qui prévoit que 99% du trafic du RuNet et de ses infrastructures soient établis dans le territoire de la Fédération de Russie d'ici 2020. Si jusqu'ici la Russie ne s'est pas techniquement affranchie du système DNS de l'ICANN comme la Chine, le Conseil de sécurité russe aurait néanmoins décidé en 2017, de créer un système DNS indépendant[9].

Selon les déclarations des autorités russes, le projet n'aurait pas vocation à séparer physiquement la Russie ou les autres membres des BRICS de l'internet mondial mais à pouvoir faire face à une défaillance accidentelle ou volontaire de ce dernier[10].

L'annonce de la création d'un système DNS russe au profit des BRICS constituerait en réalité un nouveau message politique contre l'actuelle gouvernance de l'ICANN et l'influence des pays occidentaux dans le cyberespace. En effet, un projet de système DNS commun à l'ensemble des BRICS pourrait être difficile à mettre en place en pratique. Il impliquerait que la Russie partage la gestion du nouveau système DNS avec les BRICS au risque de reproduire la situation qu'avait l'ICANN avec les États-Unis. Par ailleurs, l'idée d'un

[5] https://www.itu.int/md/S12-WCIT12-C-0027

[6] https://www.nextinpact.com/news/101613-gouvernance-icann-semancipe-officiellement-controle-americain.htm

[7] Voir la retranscription du discours du Président russe lors du premier « Forum des médias pour les médias indépendants locaux et régionaux », qui s'est tenu à Saint-Pétersbourg à partir du 24 avril 2014 (http://en.kremlin.ru/events/president/news/20858)

[8] https://www.researchgate.net/publication/317919390_%27RuNet_2020%27_-_deploying_traditional_elements_of_combat_power_in_cyberspace

[9] https://francais.rt.com/international/46046-russie-veut-lancer-internet-independant-pays-briks

[10] https://francais.rt.com/international/46046-russie-veut-lancer-internet-independant-pays-briks

système DNS commun pour les BRICS entrerait en contradiction avec le système actuel chinois, qui dispose de son propre DNS et permet à la Chine d'assurer un contrôle très strict de son Internet.

Enfin, même si le projet russe s'inscrit dans la continuité de la proposition de 2012 pour une gouvernance de l'Internet par les États et du projet « BRICS cables » de 2013[11], les BRICS ne disposent pas d'un moyen de télécommunication autonome et le trafic de leurs internautes demeure dépendant des câbles de l'internet global.

En conclusion, il apparaît que l'extension aux BRICS du projet de DNS russe relève plus de la communication politique que d'une réelle position commune. Il n'a d'ailleurs été trouvé aucune déclaration officielle des autres États et des BRICS sur ce projet. En revanche, le projet de DNS permettra clairement aux autorités russes de disposer d'une plus grande marge de manœuvre opérationnelle dans le cyberespace.

La portée opérationnelle du projet russe

Le système DNS aurait donc pour objet d'assurer la résilience du cyberespace des BRICS contre les risques de dysfonctionnement des serveurs racines gérés par l'ICANN, notamment lorsque des cyberattaques visent ces derniers[12]. Par ailleurs, dans un contexte d'augmentation des capacités de cyberopération des États, notamment des pays occidentaux, et de multiplication des cyberattaques, l'indépendance et l'autonomie du système DNS permettraient également d'assurer la continuité du cyberespace russe qui inclurait les autres membres des BRICS en cas de cyberguerre ou de cyber-incident de grande ampleur.

Comme pour l'internet chinois, la création d'un système DNS pourrait permettre aux autorités russes de disposer d'un véritable moyen technique de délimitation du cyberespace, ce qui offrirait à l'Etat russe davantage de contrôle sur l'Internet russe. En effet, pour censurer les sites web indésirables, il suffirait aux autorités russes de faire retirer les noms de domaine concernés des serveurs racines du nouveau système DNS ou de ne pas autoriser l'enregistrement d'un nouveau nom de domaine dans le système.

Par ailleurs, si le projet constituait effectivement un moyen de défense en cas de cyberguerre, il pourrait servir à la Russie pour prendre des mesures offensives dans le cyberespace tout en limitant les effets de représailles.

En raison du peu d'informations rendues publiques sur le projet russe de création d'un système DNS, il est encore difficile de déterminer avec plus de précision les mesures concrètes que prendront les autorités russes, notamment concernant l'usage de ce système par la Russie et les BRICS. Aucune information n'est également disponible concernant l'organisme qui devrait être chargé de la gestion des noms de domaine et des serveurs racines, même s'il est possible de faire référence à certaines organisations russes telles que le *Russian*

[11] Le projet « BRICS cable » avait pour objet de permettre aux BRICS de disposer de leur propre câble sous-marin de télécommunications pour ne pas utiliser les câbles passant par les Etats-Unis et l'Europe. Ce projet n'a finalement pas abouti en raison de son coût élevé.

[12] http://datanews.levif.be/ict/actualite/une-attaque-ddos-met-trois-serveurs-racines-dns-hors-ligne/article-normal-439381.html

Institute for Public Networks (RIPN)[13] en charge du *Russian Backbone Network* (RBNet)[14], le Coordination Center for TLD RU[15] ou encore l'organisation indépendante MSK-IX. Notons que cette dernière a été chargée en 2016 de mettre en place une copie de sauvegarde du RuNet[16]. Cependant, il est probable que davantage d'informations soient communiquées dans les mois prochains étant donné que le projet devrait être lancé en août 2018 à moins qu'il ne soit finalement suspendu à l'instar du projet « BRICS cable ».

En tout état de cause, le projet de DNS souverain s'inscrit dans la doctrine de sécurité informationnelle russe de 2016, qui vise à l'indépendance numérique sous ses différents angles (logiciel, matériel, services numériques, etc.), et aux ambitions du projet RuNet 2020.

[13] http://www.ripn.net/about/en/

[14] https://translate.google.com/translate?depth=1&hl=en&ie=UTF8&prev=_t&rurl=translate.google.com&sl=auto&sp=nmt4&tl=en&u=http://www.rbnet.ru/

[15] https://cctld.ru/en/

[16] http://sevendaynews.com/2016/07/06/take-two-who-will-create-a-backup-of-the-runet/

RISQUES CYBER SUR LE SYSTEME FINANCIER

Le système financier regroupe l'ensemble des activités d'échanges de fonds. Un grand nombre d'acteurs sont impliqués et interagissent entre eux, incluant les infrastructures financières, les banques, les assurances, les autorités régulatrices et les administrations publiques (ministères des finances publiques, FMI, banque mondiale[2] et banques centrales). Cet écosystème est relié par un réseau dense assurant un très grand nombre d'opérations et de mouvements de capitaux répartis sur l'ensemble du globe, toutes les transactions devant être gérées automatiquement. Cette « ultranumérisation » induit une interconnexion et une complexité dans la structure des systèmes d'information. Cette structure offre en conséquence une surface d'attaque potentielle particulièrement étendue, et une probabilité relativement élevée que des vulnérabilités dans certaines de ses composantes en affaiblissent l'ensemble.

Très tôt, les acteurs ont pris conscience des enjeux de sécurité de cette numérisation et ont mis en place un corpus normatif et des dispositifs de protection et de défense de leurs systèmes d'information. En effet, le secteur financier, avec les sommes considérables qu'il traite, a toujours été et reste plus que jamais une cible idéale. Mais si l'appât du gain constitue l'un des principaux mobiles des attaques contre ce secteur, les banques et les institutions financières, du fait de leur rôle central dans la vie socio-économique de nos sociétés, peuvent aussi être visées à bien d'autres fins, par un État, un concurrent, des hacktivistes, des hackers ludiques, voire même un mouvement terroriste.

Dans un rapport publié en juillet 2017[17], l'Autorité française des marchés financiers (AMF) estimait que le risque d'attaques à visées criminelles et idéologiques pesant sur le système financier allait croître en 2018, du fait notamment des tensions fortes dans certaines régions du monde. Elle soulignait en outre que "la dépendance du secteur financier aux systèmes d'information et les fortes interconnexions entre ses acteurs le rendent structurellement exposé aux cyber-risques qu'il s'agisse de défaillances techniques involontaires ou d'attaques délibérées".

Les enjeux sont particulièrement élevés. En effet, comme l'affirme la Banque centrale européenne (BCE)[18], les menaces cyber pesant sur cet écosystème peuvent avoir des implications sur la stabilité financière mondiale. Et si elles ne sont pas mondiales, les conséquences d'une attaque seront certainement lourdes pour les acteurs du système à un niveau plus localisé.

Le secteur financier est ultra-numérisé et les risques pesant sur les systèmes d'information des acteurs de la finance abondent. Ces enjeux nécessitent la mise en place d'une protection adaptée.

Dans quelle mesure l'ultra-numérisation du secteur financier représente-t-elle un enjeu ? Quelles sont les cyber menaces pesant sur les acteurs de la finance ? Quelle organisation et quelles institutions ont été mises en place pour faire face aux risques et à l'ensemble de ces menaces ?

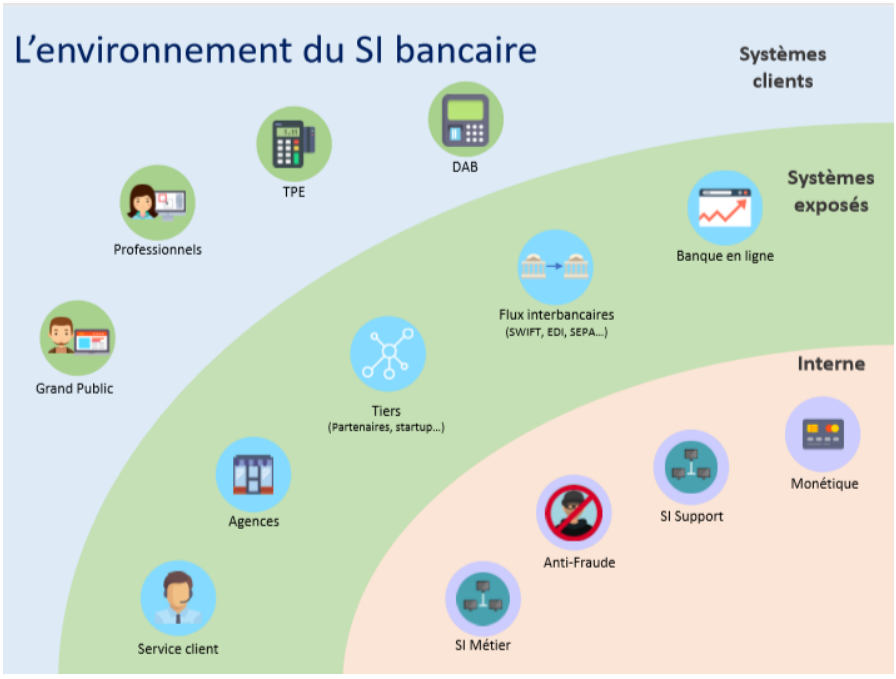
[17] http://www.amf-france.org/Actualites/Communiques-de-presse/AMF/annee-2017?docId=workspace%3A%2F%2FSpacesStore%2F741a1bf2-4c74-459c-9e09-3a4481b18cbf

[18] ECB views on the regulation of cyber security, Keynote speech by Marc Bayle de Jessé, Director General Market Infrastructure and Payments, ECB, at the Central Bank Payments Conference, Copenhagen, 21 November 2017

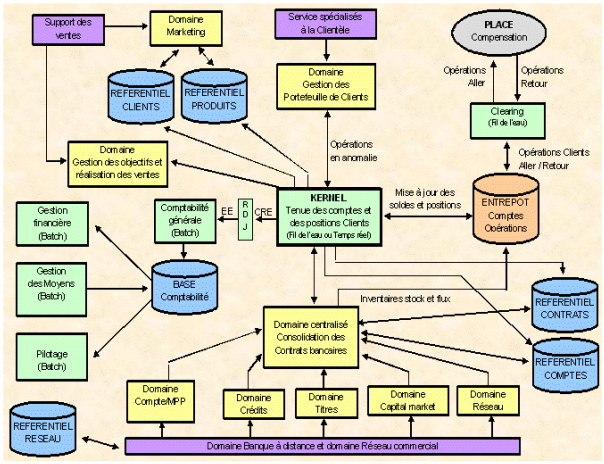
Un constat : l'interconnexion et la porosité des systèmes d'information

L'ultra-numérisation du secteur financier s'accompagne nécessairement d'une forte dépendance et de vulnérabilités des systèmes d'information. L'interconnexion des différents systèmes crée en outre une porosité, voire un décloisonnement qui les rend d'autant plus vulnérables à une contamination en cas de cyberattaque. Les acteurs utilisent les mêmes serveurs, systèmes d'exploitation, types de cloud et réseaux. Les connexions du fait des marchés interbancaires et des transferts de fond sont vectrices de contamination.

Les schémas ci-dessous, qui présentent le système d'information d'une banque dans son environnement, apportent une illustration particulièrement intéressante de sa complexité et de son interconnexion avec de nombreux équipements externes. Cet environnement, que la banque ne peut pas maîtriser et qui est souvent peu sécurisé, comme notamment les terminaux des clients et de certains prestataires logistiques, apporte au système bancaire une forte exposition aux risques.



Source : CLUSIF, Panorama de la cybercriminalité, 2016



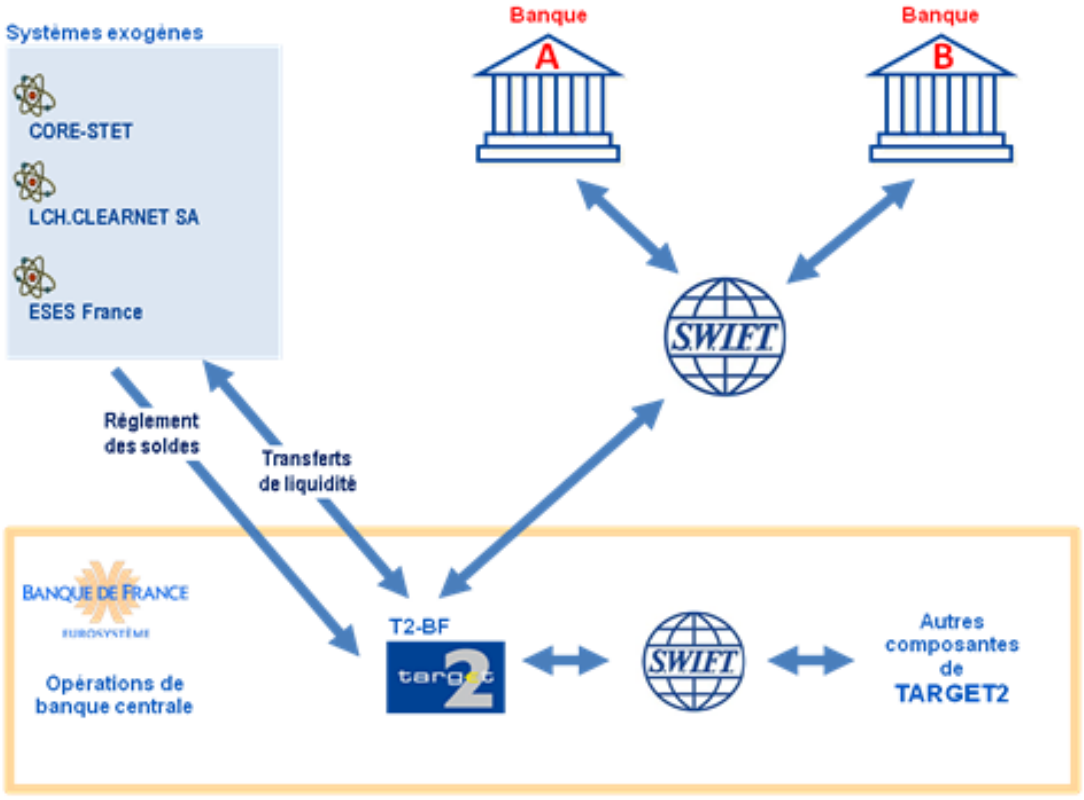
Légende des couleurs :

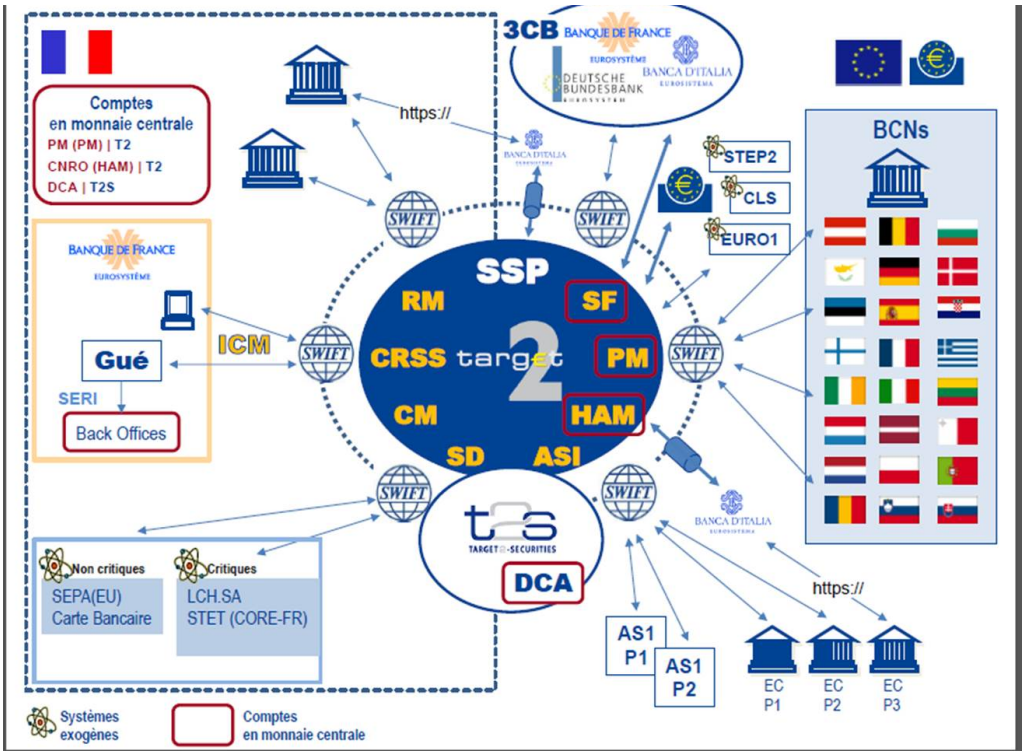
- ***Violet*** = Poste « CLIENT LEGER »,
- ***Jaune*** = Poste « SERVEUR »,
- ***Vert*** = Mode « CENTRAL »,
- ***Orange*** = Entrepôt de données,
- ***Bleu roi*** = Référentiels ou base de données.

Source : Cartographie d'un système d'information bancaire www.fimarkets.com

La complexité et l'interconnexion des systèmes d'information du secteur financier trouvent également une illustration parlante dans l'Eurosystème. Les flux financiers au niveau européen reposent sur tout un ensemble de systèmes de paiement, d'infrastructures, de procédures bancaires et interbancaires, qui doivent présenter un niveau d'efficacité et de disponibilité permanent afin de garantir son fonctionnement et la stabilité financière.

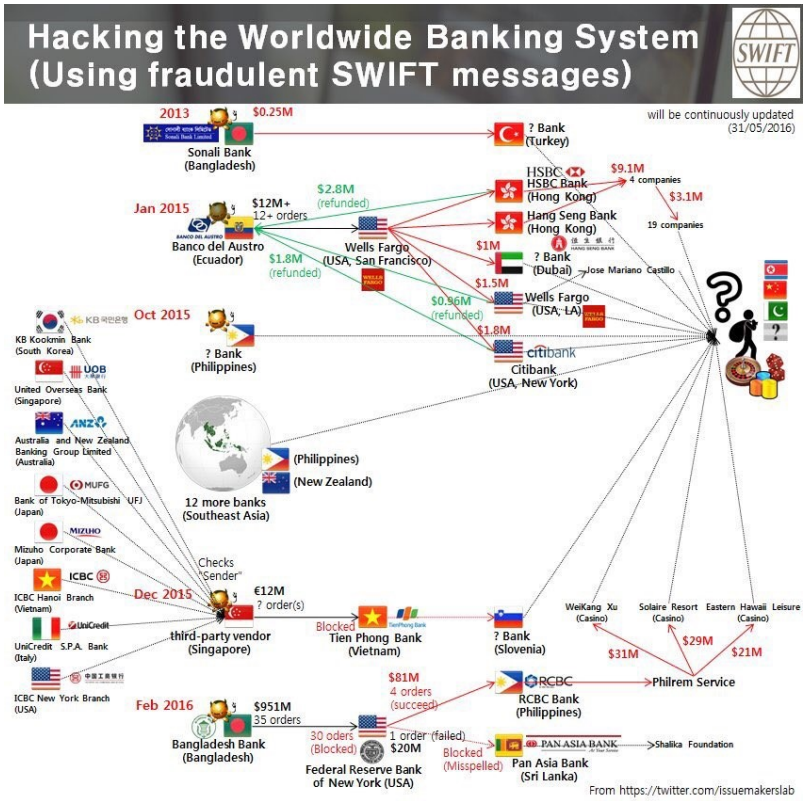
Les schémas qui suivent en donnent un exemple, basé sur TARGET 2 (Trans-european Automated Real-time Gross settlement Express Transfer), le système de traitement des paiements de montant élevé unifié au niveau européen, qu'utilisent les banques centrales et les banques commerciales.





Interactions entre le système de paiement en monnaie de la Banque Centrale, Target2 et les infrastructures de marchés financiers françaises. Source : Banque de France.

Au niveau mondial, les transferts de fonds entre les grands établissements bancaires s'effectuent via le système de transferts interbancaires SWIFT (Society for Worldwide Interbank Financial Telecommunication). Dans ce cadre, l'on comprend aisément l'impact mondial d'une cyberattaque visant le réseau SWIFT.



Les enjeux de sécurité du secteur financier

Il est donc essentiel de sécuriser au mieux ces architectures informatiques arachnéennes. L'enjeu principal est d'assurer la continuité des transactions, mais au-delà de cet objectif de disponibilité des systèmes et des données, l'authenticité, l'intégrité et la confidentialité des flux sont également des enjeux essentiels. Assurer cette cyber résilience est donc un défi mondial, compte tenu de la complexité, de la rapidité et du nombre d'opérations financières traitées chaque jour.

Les impacts potentiels d'une cyberattaque

Une cyberattaque peut provoquer des impacts variés en nature et en gravité, de la déstabilisation d'une institution financière à, dans les cas les plus dramatiques, celle du système financier mondial, et ainsi avoir des conséquences socio-économiques très graves (faillites des banques, ralentissement de la croissance économique, crise économique).

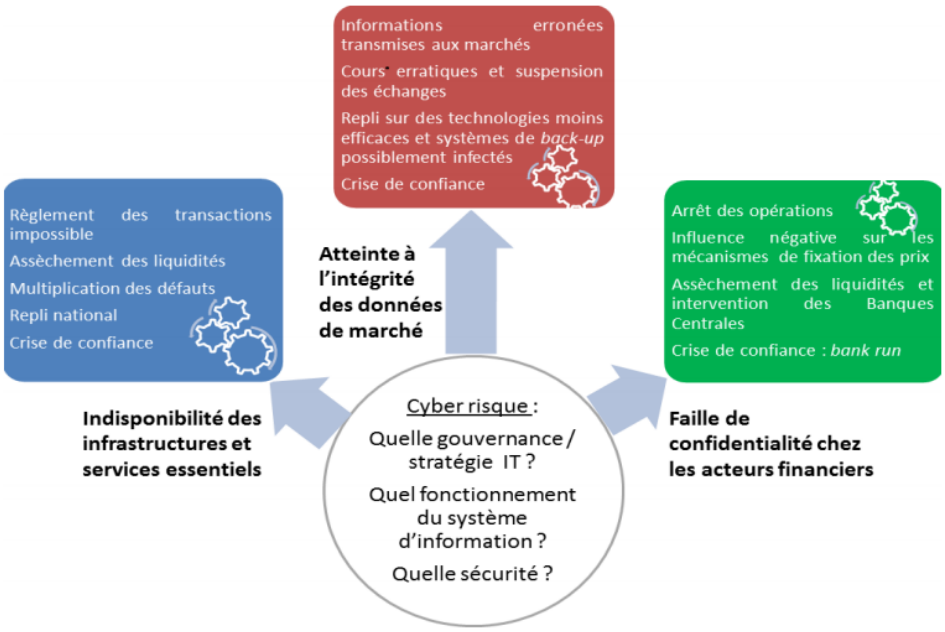
Nous allons concentrer notre qualification des impacts sur l'étude d'une banque victime d'une cyberattaque. Ceux-ci sont de nature financière essentiellement. Ils peuvent être directs. Par exemple, en cas de vol de données de particuliers, une banque devra verser aux victimes des frais juridiques et une indemnisation, payer les coûts de la réparation de la vulnérabilité et de la remise en continuité. Ces risques peuvent également être

indirects. Les affaires peuvent être fortement perturbées, selon la criticité du périmètre impacté, le nombre et la fonction des services affectés, et le nombre de clients victimes.

L'impact potentiel sur la réputation de l'établissement est proportionnel à la criticité du service bancaire affecté. La perte de confiance des clients dans une banque aura toujours des conséquences non négligeables et peut, à long terme, réduire considérablement ses bénéfices. L'impact réglementaire est aussi à prendre en compte, les banques pouvant payer des amendes, en plus des frais de mise en conformité. Enfin, l'établissement connaît un préjudice concurrentiel en cas de vol de plans stratégiques ou de données confidentielles.

Les objectifs de sécurité

Les infrastructures financières doivent pouvoir assurer la confidentialité des données, leur intégrité et leur disponibilité. En effet, un système rendu indisponible, ce qui est le cas lors d'une attaque par déni de service par exemple, affecte sérieusement toute l'infrastructure informatique d'une banque (impossibilité de régler les transactions par exemple, assèchement des liquidités). Des données erronées, manipulées, peuvent conduire à des prises de décisions incorrectes des acteurs du marché. Les éléments les plus sensibles sont les données clients, les algorithmes, la capacité à exécuter une transaction, et les sites d'accès clients. Une atteinte à la confidentialité des données peut aller jusqu'à stopper des opérations financières et nécessiter l'intervention des banques centrales.



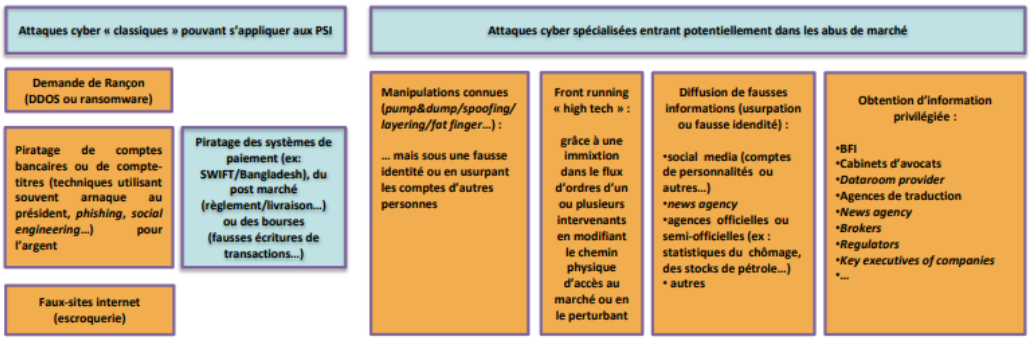
Source : https://acpr.banque-france.fr/sites/default/files/medias/documents/20180212_informatique.pdf


KASPERSKY lab
CYBER SÉCURITÉ ET FINANCE
7 BANQUES SUR 10 ON DÉJÀ ÉTÉ TOUCHÉES PAR LA CYBER FRAUDE
ET LES ATTAQUES COÛTENT CHER !
EN MOYENNE, UN INCIDENT TOUCHANT UN CLIENT COÛTE
PLUS DE 1300€ POUR LES PARTICULIERS
ET PLUS DE 9500€ POUR LES ENTREPRISES
ET QUAND LA BANQUE ELLE-MÊME EST TOUCHÉE, LE MONTANT DES PERTES PEUT AVOISINER 1 MILLION D'EUROS
63% DES BANQUES CONSIDÈRENT LEUR CLIENT COMME LE MAILLON FAIBLE
ET POUR CAUSE ILS SONT ATTAQUÉS DE TOUTES PARTS
1/4 DES PAGES FRAUDULEUSES SUR INTERNET COPIENT DES SERVICES BANCAIRES LÉGITIMES (25,76%)
1 088 900 UTILISATEURS ONT ÉTÉ ATTAQUÉS PAR DES MALWARES BANCAIRES
DONT 305 000 SUR ANDROÏD
SOIT UNE AUGMENTATION DE 430%
L'ÉMERGENCE DE NOUVEAUX SERVICES CONNECTÉS MET LE CLIENT AU CENTRE DE TOUTES LES ATTENTIONS DES BANQUES
MAIS AUSSI DES CYBER CRIMINELS
42% DES BANQUES ESTIMENT QUE LE MOBILE DEVIENDRA LE 1ER CANAL DE RELATION CLIENT POUR LA GESTION DE LEUR COMPTE AU COURS DES 3 PROCHAINES ANNÉES
75% DES BANQUES S'INQUIÈTENT DES RISQUES DE SÉCURITÉ
10% ONT DE SÉRIEUSES CRAINTES
3 INQUIÉTUDES PRINCIPALES :
LE PHISHING VISANT LES CLIENTS ET LES ATTAQUES DE SOCIAL ENGINEERING (46%)
LES NÉGLIGENCES DES CLIENTS SUR LE WEB
ET LA DIFFICULTÉ À TROUVER UN ÉQUILIBRE ENTRE CONFORT DES CLIENTS &PRÉVENTION DES FRAUDES (38%)
FACE À L'AUGMENTATION DES MENACES, LES BANQUES PRENNENT LA CYBER SÉCURITÉ TRÈS AU SÉRIEUX
53% DES INSTITUTIONS FINANCIÈRES ONT UNE PEUR DISPROPORTIONNÉE DES ATTAQUES DDOS ET APPRÉHENDENT PARTICULIÈREMENT LES ATTAQUES CIBLÉES (59%)
36% NE SAVENT PAS QUELLE STRATÉGIE ADOPTER POUR LUTTER CONTRE LES ATTAQUES CIBLÉES OU ATTAQUES DDOS
Selon une étude sur les cyber menaces financières en 2016 menée par Kaspersky Lab avec B2B International auprès de 800 représentants d'organisations financières dans 15 pays.
© 1997 – 2017 Kaspersky Lab. Tous droits réservés.

Les divers types de menaces

Une étude réalisée par Kaspersky Lab et B2B International montre qu'en moyenne, chaque attaque réussie fait subir à l'établissement financier victime des pertes d'un montant de 926 000 dollars[19]. Les banques sont régulièrement la cible d'attaques informatiques, mais beaucoup d'entre elles ne sont pas dévoilées, selon Gérôme Billois (Wavestone).

Une cartographie de la cyber-criminalité sur les marchés financiers



Source : AMF, Analyse de risques 2017

Attaques cyber « classiques » ciblant spécifiquement le secteur bancaire

- Malwares bancaires

Les familles de malwares bancaires les plus répandues sont les Zbot et les Gozi[20], qui ont été utilisés dans 60% des attaques réussies en 2016. Le trojan bancaire Retefe a ciblé de nombreuses banques, notamment en Suisse, en Autriche et en Angleterre. Les chercheurs d'Eset ont soupçonné ce malware d'avoir servi à l'attaque de la Tesco Bank qui a eu pour impact 40 000 transactions suspectes et le vol de 2,5 M£ à 9 000 clients. Le trojan Emotet est particulièrement dangereux car très difficile à détecter du fait de son caractère « polymorphe ».

La cyberattaque la plus sophistiquée est celle qui a été menée contre la banque centrale du Bengladesh en 2016. Les hackers ont réussi à s'introduire dans le réseau interne de la banque en utilisant un programme malveillant, et ont ainsi pu réaliser des transferts de fonds via le réseau SWIFT, provoquant une perte de 81 millions de dollars pour la banque centrale, et la démission de son directeur. La banque Russe GLOBEX aurait subi quelques mois plus tard des tentatives d'attaque de même nature.

- Vols de données de cartes de crédits / d'identifiants de connexion bancaires :

[19] https://www.kaspersky.fr/blog/banques-et-cybermenaces/9472/

[20] Zbot et Gozi sont des trojans bancaires, qui ont pour objectif de récupérer les informations bancaires d'un internaute afin d'effectuer des transactions frauduleuses

Dans un objectif purement lucratif, les pirates vont récupérer ces données grâce à des campagnes de phishing, du skimming[21] ou des programmes informatiques spécifiques. Ils vont ensuite les vendre sur les black Markets du Dark Web. En France, les pertes ont été chiffrées pour la simple année 2017 à 518 millions d'euros, selon l'Observatoire de la sécurité des moyens de paiement.

- Usurpation d'identité :

De faux documents d'identité acquis sur le Dark Net permettent à des escrocs d'ouvrir des comptes bancaires avec une identité usurpée, puis de contracter des crédits et d'émettre alors des chèques, avant de disparaître.

- DDOS :

En janvier dernier, trois des principales banques néerlandaises ainsi que l'équivalent du Trésor public ont été les cibles d'une attaque par déni de service distribué, attaque manifestement coordonnée (NG, ABN AMRO et Rabobank). La Lloyds Bank a également subi une attaque de cette nature, rendant indisponibles ses services durant deux jours, en 2017.

Attaques cyber spécialisées ciblant le secteur financier en général

Dans son analyse des risques de 2017, l'AMF a relevé un certain nombre d'infractions s'apparentant à des abus de marché, réalisées grâce à des moyens informatiques :

- Diffusion de fausse information : un faux communiqué de presse de Vinci a eu un impact considérable sur le cours du titre le 22 novembre 2016. Ce document annonçait la révision des comptes du groupe ainsi que le renvoi de son directeur financier après la découverte d'erreurs comptables graves. L'ampleur médiatique de cette annonce a fait baisser le cours de l'action de Vinci de 19%.
- Manipulation de cours : Une banque Kazakhe a été piratée en 2015 par des Russes, qui ont pris le contrôle d'un ordinateur connecté au marché et réalisé des ordres de bourses pour 500 millions de dollars. Ces opérations ont fait baisser de 15% le cours du rouble face au dollar, en moins d'un quart d'heure.

Attaques cyber ne ciblant pas spécifiquement le système financier

En 2011, le Ministère français de l'économie et des finances a été la cible d'une attaque cyber visant à obtenir des documents confidentiels de la Direction du Trésor liés à la présidence française du G20 et aux affaires économiques internationales. Le malware s'était introduit dans le système d'information du Ministère par l'ouverture d'un document PDF infecté joint à un mail dont rien ne pouvait laisser croire qu'il était dangereux.

En Ukraine, le ransomware NotPetya ne ciblait pas spécifiquement les banques mais a eu un impact sur la continuité des services bancaires.

[21] Le skimming consiste à copier les données magnétiques d'une carte de paiement, en général lors de son utilisation dans un distributeur automatique de billets ou un terminal de paiement, grâce à un petit dispositif quasiment invisible, et à cloner ensuite cette carte.

Assurer la cybersécurité des acteurs de l'écosystème financier

Les institutions et les organisations ont mis en place un certain nombre de mesures pour renforcer la sécurité des acteurs du système financier face aux risques cyber. L'objectif est d'imposer des exigences opérationnelles dans le domaine cyber, d'instaurer une culture de la résilience, et d'améliorer de façon continue le niveau des dispositifs de sécurité et de détection des incidents.

S'agissant d'une problématique planétaire, les institutions financières mondiales recommandent des standards de sécurité. Au niveau communautaire, les autorités instaurent des normes mises en œuvre par les Etats.

Certaines initiatives de lutte proviennent du secteur bancaire privé. La plupart des banques, en réponses aux vagues de cyberattaques de ces dernières années, se sont dotées de SOC et de CERT. Les principaux organismes émetteurs de cartes bancaires ont fondé en 2005 le Payment Card Industry Security Standard Council afin de définir et d'entretenir au niveau nécessaire des normes de sécurité, appelées PCI DSS (Payment Card Industry Data Security Standard), qui s'imposent aux banques et à l'ensemble de leurs clients professionnels utilisant des paiements par cartes bancaires. Enfin, SWIFT a lancé le Customer Security Programme pour aider les banques membres du réseau à sécuriser leurs systèmes et l'accès à leur messagerie.

Au niveau international

Au niveau international, un certain nombre de standards de sécurité sont recommandés par des instances au rôle consultatif. Au sein de la Bank of International Settlement, qui rassemble plusieurs Banques centrales nationales, le Committee on Payments and Market Infrastructures (CPMI) promeut des mesures de sécurité et d'efficacité des moyens de paiement. Le CPMI a un rôle de normalisateur au niveau mondial et prodigue des analyses et des recommandations. Dans ce cadre, et en coproduction avec l'IOSCO (International Organization of Securities Commissions), le CPMI a produit le document suivant : Guidance on Cyber Resilience for Financial Market Infrastructures. L'IOSCO a rendu des recommandations en 2016 sur le sujet suivant : Cyber Security in Securities Markets – An International Perspective. L'OCDE a également publié « Gestion du Risque de Sécurité Numérique pour la Prospérité Économique et Sociale » en 2015.

Les pays du G7 (Canada, France, Allemagne, Grande-Bretagne, Italie, Japon et États-Unis) ont créé un groupe d'experts sur le cyberespace chargé d'établir une liste d'« éléments fondamentaux » de la cybersécurité pour le secteur financier (G7 Fundamental Elements Of Cybersecurity For The Financial Sector). Cette étude, à laquelle s'est associée la Banque centrale européenne, a permis de fournir aux acteurs financiers des éléments de base sur lesquels concevoir et mettre en œuvre une stratégie de cybersécurité et un cadre opérationnel.

Au niveau communautaire : « l'Eurosystème »

L'Union Européenne a pris en compte la cybersécurité dans de nombreux domaines, et édicte régulièrement des normes applicables dans l'Union, qui viennent renforcer celles éventuellement prises au niveau mondial.

Certaines de ces normes concernent l'ensemble des secteurs, comme le Règlement général sur la protection des données à caractère personnel (RGPD), qui contribuera à renforcer la cybersécurité du secteur financier

dès son entrée en application le 25 mai prochain. D'autres sont plus sectorielles, comme la Directive NIS[22], qui érige notamment les banques ouvertes au public en "opérateurs essentiels" et leur impose à ce titre des exigences de cybersécurité que les États membres devront préciser. Enfin, d'autres normes sont spécifiques au secteur financier, comme la deuxième Directive sur les services de paiement (DSP2)[23], entrée en application en janvier dernier, qui instaure des normes de sécurité plus strictes pour les paiements en ligne, comme l'authentification forte qui sera bientôt obligatoire pour que le client puisse accéder à son compte de paiement ou effectuer des paiements en ligne de plus de 30 €. Ces normes, appelées "normes techniques de réglementation", seront fixées par la Commission européenne sur proposition de l'Autorité bancaire européenne (ABE)[24]. Il convient de noter que la DSP2 s'impose aux services de paiement innovants et aux nouveaux fournisseurs sur le marché, tels que les sociétés de technologie financière (les « FinTech »).

L'ABE a pour rôle de maintenir la stabilité financière dans l'UE et de garantir l'intégrité, l'efficience et le bon fonctionnement du secteur bancaire. Elle fait partie du système européen de surveillance financière (SESF). En application du mandat qui lui est confié par les articles 95, 96 et 98 de la DSP2, elle est chargée d'élaborer des projets de normes techniques de réglementation sur la gestion des risques opérationnels et de sécurité, sur la notification des incidents et sur l'authentification[25]. L'ABE est également chargée d'évaluer les risques et vulnérabilités dans le secteur bancaire européen, notamment à l'aide de rapports réguliers d'évaluation des risques et de simulations de crises.

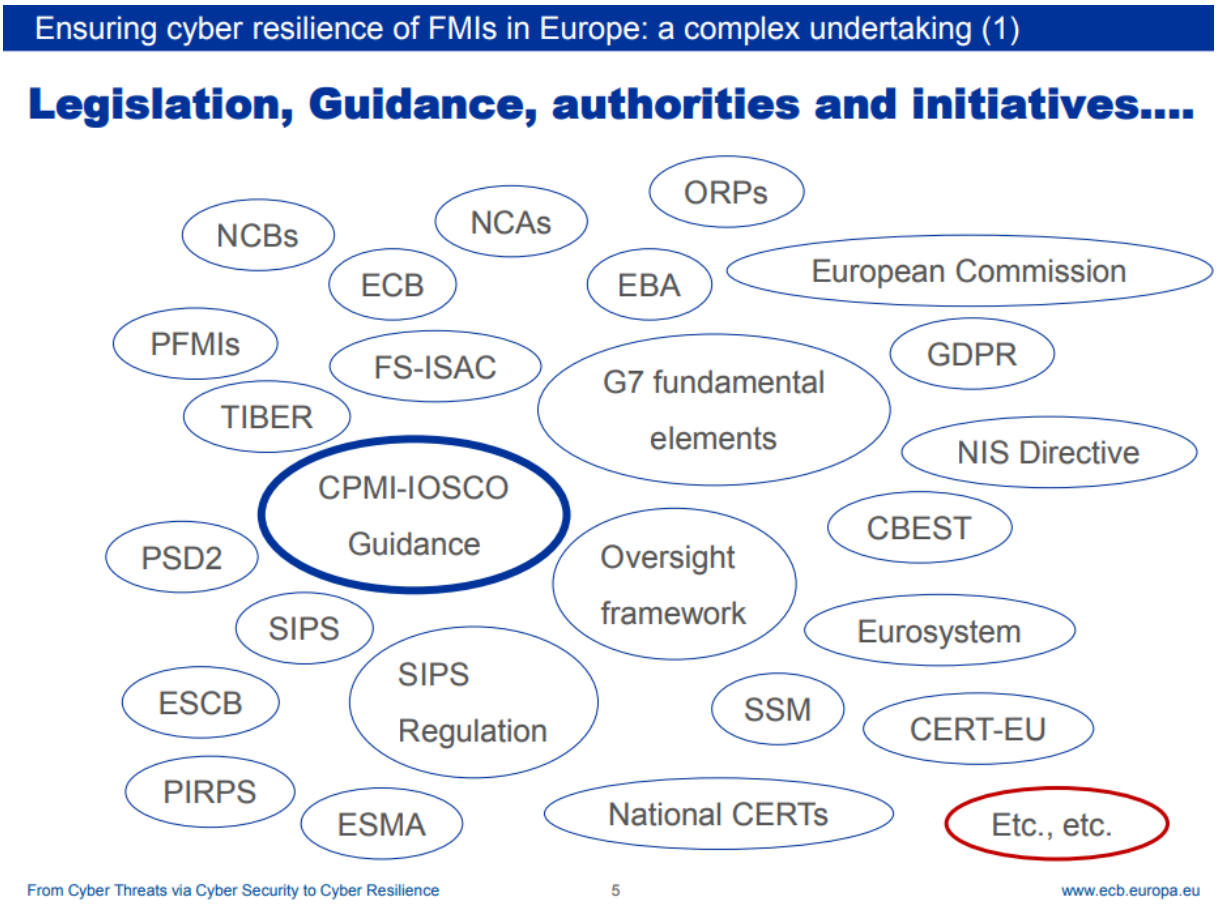
Institution de l'Union européenne au cœur de l'Eurosystème et du mécanisme de surveillance des établissements de crédit, la Banque Centrale Européenne (BCE) est associée, en vertu de la SDP2, aux travaux de l'ABE sur la gestion des risques opérationnels et de sécurité et sur l'authentification. Comme l'ABE, elle est informée des incidents opérationnels ou de sécurité majeurs survenus dans l'Union et est chargée de les analyser et d'en tirer les enseignements. Elle a récemment chargé une « Task Force » de réfléchir à d'éventuels lancements de tests de résistance des banques aux cyberattaques, dans la lignée des « stress tests » effectués par l'ABE pour tester la résistance des banques aux scénarios catastrophes.

[22] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union

[23] Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur (https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:32015L2366), transposée en droit national par l'ordonnance n° 2017-1252 du 9 août 2017 (https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000035394629), et sa fiche d'information (http://europa.eu/rapid/press-release_MEMO-17-4961_fr.pdf),

[24] https://www.eba.europa.eu/languages/home_fr

[25] Les règlements délégués de la Commission fixant des normes techniques de réglementation en matière de cybersécurité sont en cours d'approbation (voir par exemple celui sur l'authentification forte du client et sur des normes ouvertes communes et sécurisées de communication, https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=PI_COM:C(2017)7782).



La complexité et la diversité du champ général des autorités et des initiatives en matière de résilience cyber

Wiebe Ruttenberg & Emran Islam, From Cyber Threats via Cyber Security to Cyber Resilience, AMISeCo meeting, 7 March 2017, European Central Bank

Au niveau national

En France, plusieurs organismes sont chargés de superviser les risques cyber impactant le secteur de la finance.

L'ANSSI, autorité nationale en matière de sécurité et de défense des systèmes d'information, fixe les principes et règles communes, et assiste les autorités ministérielles et de régulation pour tout ce qui concerne leur déclinaison et leur mise en œuvre dans les divers secteurs, notamment sur les plans normatif, technique et opérationnel. Par ailleurs, elle élabore les normes applicables aux opérateurs d'importance vitale des différents secteurs, dont le secteur financier, et en contrôle l'application. Elle est informée des incidents de sécurité de ces opérateurs[26]. Elle assurera le même rôle pour les opérateurs essentiels, au sens de la Directive NIS de l'UE, quand ce texte sera transposé en droit national.

[26] Arrêté du 28 novembre 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au secteur d'activités d'importance vitale « Finances »

L'Autorité des marchés financiers (AMF) est l'autorité publique régulatrice des marchés financiers. Elle a une mission de protection des épargnants, d'information des investisseurs et de surveillance des marchés financiers. Dans ce cadre, l'AMF détient des pouvoirs d'enquête et de contrôle de la régularité des opérations, et un rôle répressif. Cette autorité détient également un pouvoir réglementaire en matière de marchés financiers. L'AMF partage avec l'ANSSI une part de la responsabilité de l'État de la cybersécurité du secteur financier. Pleinement conscientes de la nécessité de développer leur coopération pour faire face aux cybers menaces pesant sur ce secteur, ces deux autorités ont signé le 16 février 2018 une lettre d'intention prévoyant des échanges réguliers d'information sur les incidents de cybersécurité et une collaboration dans la gestion des crises et plus largement dans les divers aspects de la sécurité numérique.

L'autorité de contrôle prudentiel et de résolution (ACPR) a également engagé une coopération de même nature pour les secteurs de la banque et de l'assurance. L'ACPR a pour missions d'assurer la stabilité financière, de superviser le secteur de la banque et de l'assurance et de protéger les clients. Dans le cadre de ses missions de supervision de la gestion des risques, elle s'intéresse au risque opérationnel informatique. Cette entité est engagée dans les travaux d'instances internationales (ABE, G7, BCE) et publie un certain nombre de recommandations sur la gestion du risque cyber ; dans la dernière en date, elle expose ses *attentes sur le risque informatique et l'usage du cloud computing.*

La Banque de France, dans le cadre de sa place au sein de l'Eurosystème et par sa mission fondamentale d'assurer le bon fonctionnement de la sécurité du système bancaire et financier français, surveille les moyens de paiements et les systèmes de paiements, de compensation et règlement-livraison de titre. Elle préside l'Observatoire de la sécurité des moyens de paiement[27].

Conclusion

Le secteur financier fait face à de nombreuses menaces cyber, amplifiées par sa numérisation très poussée, l'étendue et la complexité des processus mis en œuvre, le nombre d'acteurs et de systèmes interconnectés dans le monde, ainsi que par les sommes considérables qu'il traite et par son importance pour toutes les activités socio-économiques des nations. Face à ces menaces, il est essentiel de mettre en place toutes les mesures de protection et de défense nécessaires pour en garantir la sécurité et la résilience. Ce secteur est certainement l'un de ceux qui ont la meilleure conscience des risques qu'ils encourent, et de très nombreuses mesures sont déjà en place, prises à l'initiative des opérateurs eux-mêmes ou, de plus en plus, édictées par les nombreuses structures concourant à la régulation du secteur

Le principal défi du secteur, en matière de cybersécurité, est de réduire les fraudes et les actes de malveillance, ou au moins de les maintenir à leur niveau actuel, malgré un double mouvement, d'une part celui des nouvelles techniques numériques qui ne cessent de se multiplier et qui sont bien souvent mises en œuvre avant même d'en avoir bien cerné les dangers, d'autre part celui de la cybercriminalité qui ne cesse de se développer en volume, en technique et en puissance.

L'open banking, porté par le secteur des Fintech et désormais réglementé par la DS2P dans l'Union européenne, est un exemple illustrant ce défi spécifique. Le secteur fait également face aux nombreuses

[27] Voir le dernier rapport annuel publié par l'OSMP ; https://www.banque-france.fr/sites/default/files/medias/documents/osmp2016_web.pdf

questions de cybersécurité qui concernent tous les secteurs, comme celle que pose la poursuite du mouvement d'externalisation de certaines fonctions, parfois essentielles (Business Process Outsourcing), dans la mesure où, mal maîtrisé, il peut induire une perte de maîtrise des systèmes et des processus et permettre l'extension de vulnérabilités aux acteurs de la finances.

La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique**, sous le numéro de marché 1502492543. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère des Armées
Direction Générale des Relations Internationales et de la Stratégie
60 Boulevard du Général Martial Valin – CS21623 – 75 509 Paris Cedex 15

CEIS
Tour Montparnasse – 33, avenue du Maine – BP 36 – 75 755 - Paris Cedex 15
Téléphone : 01 45 55 00 20
E-mail : omc@ceis.eu