La Jaune et la Rouge
Polytechnique
8 € - Janvier 2016 - N° 711

PORTRAIT
Gilles Dowek (85), la passion d'enseigner

DANS LE MONDE
Regards croisés sur l'Allemagne

INTERNATIONAL
Joaquim Nassar (91), de Palaiseau à Shangh

La CYBERSÉCURITÉ au cœur du monde de demain

Revue mensuelle de l'Association des anciens élèves et diplômés de l'École polytechnique
l'X AX

ÉRIC FREYSSINET (92) *conseiller auprès du préfet, chargé de la lutte contre les cybermenaces*

LA CYBERSÉCURITÉ DES MENACES ET DES STRATÉGIES

LA CYBERSÉCURITÉ recouvre l'ensemble des politiques et des actions de sécurisation des systèmes d'information, de lutte contre la cybercriminalité et de cyberdéfense. Il s'agit donc d'une posture qui vise à répondre à l'ensemble des cybermenaces auxquelles nous sommes collectivement ou individuellement confrontés. En effet, dans un contexte où nous sommes tous de plus en plus connectés, nos données de plus en plus partagées et où des domaines aussi variés que notre santé, les échanges économiques ou les transports sont de plus en plus dépendants de la connectivité et de l'échange d'informations, il est indispensable pour tous d'être informés, voire mobilisés pour la cybersécurité.

Les chiffres s'entrechoquent dans l'actualité, qui évoquent des centaines de milliards d'euros de pertes liées à la cybercriminalité chaque année dans le monde. C'est certainement assez proche de la réalité, nos services de police et de gendarmerie recueillant chaque mois pour la France de l'ordre de dix millions d'euros de pertes signalées par les plaignants.

« Des centaines de milliards d'euros de pertes liées à la cybercriminalité chaque année »

Mais la cybersécurité est aussi un champ important de découvertes, d'invention et de développement économique. L'Europe – et la France en particulier – a tous les atouts pour devenir le creuset des champions de la cybersécurité, tant par la richesse de nos formations, la qualité de nos entreprises et des entrepreneurs, que par notre capacité à partager et à lancer des actions partenariales.

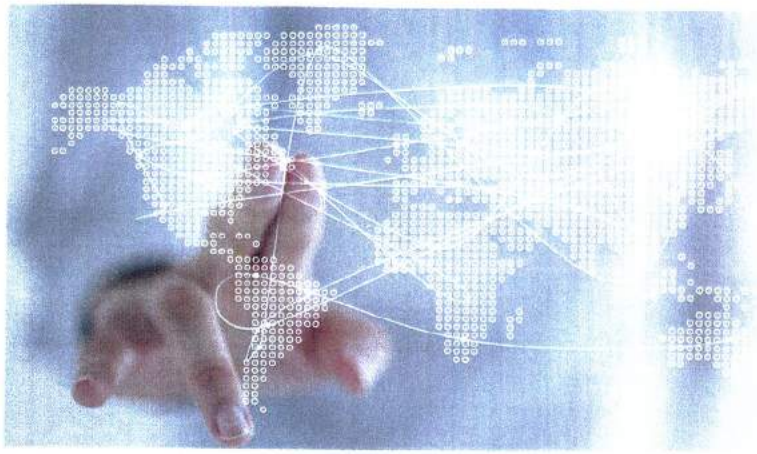
Notre pays se mobilise. Ainsi, le Premier ministre présentait en octobre 2015 la Stratégie nationale pour la sécurité du numérique, contenant sous cinq titres un ensemble d'actions par lesquelles l'État s'engage auprès des victimes, auprès des offreurs de produits et de services, et évidemment aux côtés des opérateurs d'importance vitale qu'il faut plus particulièrement protéger.

Enfin, c'est à chacun d'entre nous, ou plutôt à chaque secteur, de construire une stratégie adaptée aux cybermenaces, elles-mêmes en évolution. Ces stratégies doivent comprendre ces dimensions de compréhension et d'analyse, de prévention, d'innovation et de partage. ■

BERTRAND DE LA CHAPELLE (78) *cofondateur et directeur du projet « Internet & Jurisdiction »*

GOUVERNANCE DE L'INTERNET ET GOUVERNANCE SUR L'INTERNET

L'architecture du réseau Internet est gouvernée par des principes et mécanismes institutionnels globaux qui ont largement contribué à son succès. En revanche, les usages de l'Internet restent essentiellement régis par des législations et règles nationales, ce qui peut à terme devenir un handicap pour un réseau techniquement sans frontières. La question se pose de savoir si la gouvernance *sur* l'Internet peut fonctionner comme la gouvernance *de* l'Internet, ou au moins s'en inspirer.



© VEGE / FOTOLIA

On dit souvent que l'Internet est sans frontières mais il est plus exact de dire qu'il est transfrontière.

Le Sommet mondial sur la société de l'information (SMSI) a adopté en 2005 la définition suivante de la « gouvernance Internet » : « L'élaboration et l'application par les États, le secteur privé et la société civile, chacun selon son rôle, de principes, normes, règles, procédures de prise de décision et programmes communs propres à modeler l'évolution et l'utilisation de l'Internet. »

« La gouvernance Internet concerne à la fois l'évolution du réseau et ses usages »

UN JEU MULTIACTEURS

Deux éléments méritent une attention particulière dans cette définition. En premier lieu, la reconnaissance que les différentes catégories d'acteurs (en anglais : *stakeholders*) ont un rôle, certes variable, à jouer dans l'élaboration et la mise en œuvre des régimes de gouvernance relatifs à l'Internet. C'est le fondement de l'approche dite « multiacteurs ». Le second élément est le fait que la gouvernance Internet concerne à la fois l'évolution du réseau et ses usages, en d'autres termes : la gouvernance « de » l'Internet et la gouvernance « sur » l'Internet.

UN ÉCOSYSTÈME INSTITUTIONNEL DISTRIBUÉ

Contrairement au réseau téléphonique, constitué progressivement par la connexion entre réseaux nationaux (comme en

REPÈRES

Liberté d'expression, vie privée, cybercriminalité, surveillance de masse, bouleversement de secteurs traditionnellement régulés, lutte contre le terrorisme : les enjeux liés aux usages de l'Internet ne cessent de se multiplier et occupent désormais la première page des journaux. Les règles applicables n'en sont pas claires pour autant et les débats s'intensifient entre les partisans d'une réglementation la plus légère possible pour favoriser l'innovation et les tenants de l'instauration nécessaire d'un « code de la route » pour limiter les usages abusifs du réseau.

témoignent les indicatifs des pays), l'architecture technique de l'Internet a été conçue sans référence particulière au découpage territorial entre États. On dit souvent que l'Internet est sans frontières mais il est plus exact de dire qu'il est transfrontière.

Un ensemble d'institutions a été progressivement mis en place pour développer et administrer chacune des composantes de la couche logique de l'Internet : l'*Internet Engineering Task Force* (IETF) et le *World Wide Web Consortium* (W3C) respectivement pour les protocoles TCP/IP et HTML/http ; les Registres Internet régionaux (RIRs) pour la distribution des adresses IP ; un réseau de « serveurs racine » et l'*Internet Corporation for Assigned Names and Numbers* (ICANN) pour coordonner plus particulièrement le système de noms de domaines.

UNE CONSTRUCTION PROGRESSIVE

Chacune de ces entités a été créée à mesure que le besoin s'en faisait sentir, par une coopération entre les acteurs concernés et non dans un cadre intergouvernemental. Leurs modalités de fonctionnement sont variables, mais elles fonctionnent toutes sur un modèle participatif, dit multiacteurs, ouvert à tous. Elles constituent un système de gouvernance distribué qui a garanti l'interopérabilité globale d'une infrastructure servant désormais plus de trois milliards d'utilisateurs.

Ce succès peut-il être reproduit pour la gouvernance « sur » l'Internet ?

UNE GOUVERNANCE SUR L'INTERNET ENCORE EMBRYONNAIRE

Si l'architecture technique du réseau Internet est foncièrement globale et agéographique, il n'en va pas de même du système juridique international. Celui-ci repose en effet sur des juridictions définies par les limites territoriales des États. Par conséquent, la tension entre les espaces et services en ligne – transfrontières – et le patchwork des législations nationales ne cesse de s'accroître. La plupart des problèmes liés à l'utilisation de l'Internet sont extrêmement difficiles à résoudre dans le cadre du système westphalien de séparation des souverainetés et de non-ingérence dans les affaires intérieures des États.

LE DILEMME DU PRISONNIER

Imaginé par Tucker en 1950, le « dilemme du prisonnier » est celui auquel sont confrontés deux prisonniers qui auraient intérêt à coopérer, mais ne le font pas car ils ne peuvent communiquer. Cet exemple est transposable à de multiples domaines et peut s'appliquer à la gouvernance sur l'Internet : il illustre la nécessité d'une coopération internationale pour éviter une situation sous-optimale.

UN ENCHEVÊTREMENT DE RÈGLES INCOMPATIBLES

Pire, en l'absence de traités ou d'accords internationaux (à la notable exception de la convention de Budapest sur la cybercriminalité), gouvernements et plateformes Internet s'en remettent aux outils dont ils disposent : lois nationales à l'application de plus en plus extraterritoriale et conditions d'utilisation (*Terms of Service*) élaborées unila-

« Une gouvernance qui garantit l'interopérabilité globale de l'infrastructure »

DR

Bertrand de La Chapelle préside la réunion annuelle du projet « Internet & Jurisdiction » à Berlin en octobre 2015.

Conférence sur la géographie du cyberespace. DR

téralement. Le résultat de ce « dilemme du prisonnier » est un enchevêtrement de règles potentiellement incompatibles rendant le problème encore plus difficile à résoudre. Cette course aux armements légale risque de fragmenter le cyberespace et menace les bénéfices apportés par cette infrastructure globale.

DES INSTANCES DE DIALOGUE À CRÉER

Une coopération internationale est nécessaire entre les différents acteurs pour élaborer les règles applicables à ces cyberespaces communs. Malheureusement, les lieux permettant un tel dialogue n'existent pratiquement pas. Certes, le Forum sur la gouvernance Internet (IGF), création du SMSI, offre depuis 2006 un espace de dialogue permettant la mise à l'agenda et une discussion entre tous les acteurs de leurs sujets d'intérêt ou de préoccupation communs. Mais la réussite indéniable de cette rencontre annuelle, qui a suscité des imitations intéressantes aux niveaux régional (tel EuroDIG) ou national (tel le FGI-France), ne permet pas encore un travail récurrent en groupes de travail pour élaborer, valider et mettre en œuvre de véritables régimes opérationnels. Le système demeure incomplet, embryonnaire. Comment aller plus loin ?

« Des initiatives spontanées émergeant à mesure que les besoins sont identifiés »

UNE APPROCHE PRAGMATIQUE, SUJET PAR SUJET

Le panel d'experts réuni en 2014 sous la présidence de Toomas Ilves, président de l'Estonie, a, dans son rapport, entériné l'idée d'une approche pragmatique, sujet par sujet, selon un concept de « groupes de gouvernance distribués ». Formés à l'initiative d'un facilitateur neutre, de tels réseaux de gouvernance thématiques (*issue-based governance networks*) rassembleraient les acteurs concernés pour développer et mettre en œuvre des régimes volontaires. Cette méthodologie est conforme à la pratique de coopération qui a donné naissance à l'écosystème décrit plus haut pour la gouvernance de l'Internet : des initiatives spontanées (*bottom-up*), émergeant à mesure que les besoins sont identifiés, ne nécessitant pas d'autorisation préalable et jugées uniquement sur leur capacité à obtenir un consensus autour de pratiques standard.

DR

Un atelier du Forum sur la gouvernance Internet (IGF) à Istanbul en 2014.

LES CONDITIONS DE LA RÉUSSITE

La neutralité des facilitateurs, un effort d'identification et d'implication des divers acteurs pertinents pour le sujet traité (gouvernements, société civile, business, milieu académique, organisations internationales, opérateurs techniques), et une transparence dans le compte rendu de l'avancement des travaux, tels sont quelques-uns des critères nécessaires à la légitimité de telles initiatives.

C'est l'approche retenue depuis 2012 par le projet « Internet & Jurisdiction ». Ce processus de dialogue multiacteurs implique plus d'une centaine d'acteurs des divers secteurs à travers le monde autour des conflits de juridiction relatifs à l'Internet. Le premier résultat de ce dialogue est la proposition d'un cadre de coopération et de *due process* relatif aux requêtes transfrontières en matière de saisie de noms de domaines, de retrait de contenus jugés illégaux et d'identification des utilisateurs. Le nombre croissant de requêtes directes adressées par les autorités publiques d'un pays à des opérateurs Internet situés à l'étranger soulève en effet des questions essentielles de transparence et de garanties procédurales.

« L'approche multiacteurs peut fournir des solutions de coopération transnationale »

UN LABORATOIRE DE LA BONNE GOUVERNANCE

L'ère numérique lancée par le développement irrépressible de l'Internet a peu à peu des effets sur toutes les activités humaines. Sans surprise, politique et réglementation n'y échappent pas, plaçant des problématiques anciennes dans un cadre de plus en plus transnational ou soulevant des difficultés entièrement nouvelles.

En s'appuyant sur les leçons du système qui a prouvé son efficacité dans la gouvernance du réseau lui-même (sans pour autant le reproduire à l'identique), il nous appartient aujourd'hui de développer les nouveaux outils de la gouvernance sur l'Internet et de prouver que l'approche multiacteurs peut fournir des solutions pragmatiques de coopération transnationale.

La gouvernance Internet est un laboratoire. Si nous parvenons à développer de nouveaux mécanismes de dialogue et de coopération dans ce domaine complexe, tout laisse à penser que cette méthodologie trouvera de nouvelles applications dans d'autres domaines. Nous passerons ainsi de la gouvernance « de » et « sur » l'Internet à la nécessaire gouvernance à l'ère de l'Internet. C'est dire l'importance des enjeux. ■

© DAVID WEEKLY

Le sommet mondial sur la société de l'information (SMSI) de Tunis a fourni une définition de la Gouvernance Internet.

LUC RENOUIL (89) *directeur du développement et de la stratégie défense-sécurité de Bertin Technologies-groupe CNIM*

DÉVELOPPER UNE INDUSTRIE FRANÇAISE ET EUROPÉENNE DE CONFIANCE

La création aux niveaux français et européen d'une industrie de la confiance forte et autonome nécessite « l'union sacrée » des acteurs publics et privés et le développement d'un écosystème industriel dans lequel coopèrent des entreprises de toute taille.

LA TRANSFORMATION NUMÉRIQUE promet des lendemains qui chantent et des gisements de croissance et de productivité. En France, la part de PIB issue du numérique est de plus de 100 milliards d'euros, la valeur du commerce en ligne depuis 2007 a été multipliée par trois, le taux d'équipement en tablettes entre 2011 et 2013 a été multiplié par quatre. Dans notre pays, les ventes de smartphones ont été multipliées par six depuis 2008, la capacité de stockage de données a été multipliée par douze depuis 2005 [1], enrichissant de manière radicale l'expérience client et révolutionnant les organisations.

« Les attaques informatiques croissent de près de 50 % par an depuis trois ans »

LENDEMAINS QUI CHANTENT

Avec l'accès à Internet et la mobilité, on a démultiplié la productivité des cadres, l'accès aux données de l'entreprise depuis le monde extérieur, en calquant les usages de l'entreprise sur les usages personnels pour s'assurer l'adhésion des salariés. Avec le *cloud*, c'est-à-dire l'informatique externalisée, l'usine à gaz informatique interne est rationalisée par des professionnels sur leur propre infrastructure optimisée. Qui aurait, de nos jours, l'idée de produire soi-même son électricité ? À chacun son métier. Les dépenses en *cloud* progressent toujours sur un rythme supérieur à 15 % en *cloud* privé et près de 30 % en *cloud* public [2]. Avec l'Internet des objets, c'est la promesse de contrôler à distance les états des matériels connectés qui se profile, sans que soient encore assurées la fiabilité et la non-compromission de ces objets.

UN RISQUE QUI PEUT DEVENIR UNE CHANCE

L'existence de menaces persistantes sur la sécurité informatique est devenue le cauchemar des responsables de sécurité informatique et désormais des dirigeants. L'augmentation du nombre des attaques informatiques est de près de 50 % par an depuis trois ans.

La sécurité n'est pas un business de la peur, mais suppose une coopération efficace entre acteurs publics – en particulier les régulateurs, en tant que primo-intervenants et tours de contrôle de la menace, garants du bien public de sécurité – et acteurs privés, qui doivent intégrer la sécurité dans leur modèle économique comme un risque propre, avec ses conséquences au plan concurrentiel, au plan humain et sur la continuité d'activité.

Cette coopération entre public et privé est le point fort culturel du modèle écono-

REPÈRES

Récemment, la société Sony a subi un vol massif de données *via* Internet. Puis TV5 Monde a été victime d'un *malware* provoquant la discontinuité d'activité pour un groupe média moyen, vraisemblablement utilisé comme vengeance de nos engagements diplomatiques. Les services de renseignement américains auraient eu accès aux outils de génération de secrets de la société Gemalto, pourtant un des acteurs essentiels de la sécurité informatique. Des événements qui montrent que le risque numérique peut devenir un sérieux obstacle au progrès de la transformation numérique.

© VIPERAGP / FOTOLIA

Les dépenses en *cloud* augmentent de 15 à 30 % par an.

mique français, quand elle est bien opérée. La loi de programmation militaire et le plan cybersécurité ont donné à la France une impulsion décisive depuis 2014. Mais tout est à mettre en place, et s'il y a une contrainte à concilier les différentes réglementations nationales pour une société privée aux multiples implantations nationales, autant démontrer que l'approche française est efficace.

CROISSANCE FORTE ET DOMINANCE ANGLO-SAXONNE

Selon les chiffres de différents cabinets d'études, le marché de la cybersécurité sera de près de 100 milliards de dollars en 2015, près de 170 milliards de dollars en 2020. Il atteint près de 3 milliards d'euros en France et plus de 30 milliards d'euros en Europe.

Ce marché ne se limite pas à la stricte sécurité informatique mais la dépasse, puisque de nombreux systèmes informatiques industriels du « cyberespace » peuvent être défaillants ou attaqués (automobile, aéronautique, exploitation des infrastructures, etc.).

« Le marché de la cybersécurité est calqué sur celui du logiciel et des services associés »

Sa croissance selon les régions du marché est supérieure à 10 % annuellement. Le marché est dominé par l'Amérique du Nord et l'Europe, mais l'Asie prend de l'importance.

La cybersécurité est un marché globalement calqué sur le marché du logiciel et des services associés, plus que sur le marché de la sécurité. Dans les services, les missions confiées à des tiers de confiance sont en très forte croissance. Elles correspondent à l'externalisation du service de supervision de la sécurité informatique.

Le marché des produits comprend notamment le marché de l'édition de logiciels et, dans une moindre mesure, des produits de sécurité (aussi appelés *appliances*). C'est un marché industriel, pour lequel les positions et les cycles d'investissements sont dominés par les grands éditeurs anglo-saxons.

UN RECOURS CROISSANT À L'EXTERNALISATION

Avec l'évolution vers l'externalisation des infrastructures et des services, les modèles économiques se rapprochent. Les prestataires doivent proposer une expertise outillée différenciante au moindre coût.

Les marchés verticaux introduisent eux-mêmes une segmentation, car l'usage de l'informatique et ses enjeux ne sont pas les mêmes dans le domaine de l'énergie ou dans le domaine bancaire.

Finalement, la grande particularité du domaine de la cybersécurité est sa forte adhérence au besoin gouvernemental. Ce besoin doit être pensé comme l'occasion de promouvoir des offres et des fonctionnalités qui favorisent le tissu industriel domestique.

Le domaine industriel des services informatiques et du logiciel reste dominé par les acteurs américains, qui regroupent plus

LOI DE PROGRAMMATION MILITAIRE

L'article 22 de la loi de programmation militaire concerne les systèmes d'information. L'objectif de cet article et des décrets afférents est de définir les systèmes d'information concernés et des règles efficaces, soutenables et adaptées aux métiers et spécificités des opérateurs industriels dont la défaillance ou l'attaque pourrait porter atteinte à la sécurité de l'État, et de garantir la bonne articulation de ce nouveau dispositif avec les réglementations préexistantes. D'où la mise en place au début de l'année 2015, pour chaque domaine d'activité (eau, énergie, finances, transports, etc.), de groupes de travail rassemblant, autour de l'ANSSI, les opérateurs d'importance vitale, les ministères coordonnateurs et les autorités sectorielles.

UN ÉCOSYSTÈME EN ÉBULLITION

Dans le domaine des fusions acquisitions et des opérations en Bourse, nous avons assisté en France à une opération emblématique en octobre 2015 : le rachat de l'éditeur américain Vormetric par Thales pour près de 400 millions de dollars. Mais cela n'atteint pas les sommets de l'écosystème anglo-saxon. L'éditeur Sophos a été coté à Londres et valorisé pour 1,6 milliard de dollars, Microsoft a racheté la société israélienne Adallom, spécialisée dans la sécurité du *cloud* pour 320 millions de dollars, tandis que Cisco a acquis Open DNS pour 635 millions de dollars. Ce sont des dizaines d'opérations de plusieurs dizaines de millions de dollars qui ont eu lieu à un rythme s'accélérant au cours des douze derniers mois. Pour ce qui est du capital investissement, près de 2 milliards de dollars ont été investis dans des *start-ups* cyber aux USA l'an dernier et plus de 1 milliard de dollars au premier semestre 2015. Signalons que plusieurs levées de fonds aux USA ont concerné des montants de plusieurs dizaines de millions de dollars, Google Capital ayant investi 100 millions de dollars sur Crowdstrike.

de 70 % des principaux acteurs (IBM, Microsoft Oracle, tous intéressés de près ou de loin à la sécurité informatique).

La même domination s'observe dans le domaine de la cybersécurité, puisque les cinq plus gros acteurs du secteur sont Symantec, IBM, Intel Security, Trend Micro (Japon) et EMC. Leur activité approche ou dépasse largement le milliard de dollars annuel. L'émergence de Trend Micro, voire de Kaspersky, est peut-être le signal d'une remise en cause de cette hégémonie.

UN PLAN DE TRAVAIL COMPLET À METTRE EN ŒUVRE

En France, la cybersécurité, en première approche, c'est 700 entreprises dont 100 se spécialisent réellement sur des produits et services de haute technologie. Une vingtaine tout au plus exportent. Il faut être champion sur son territoire pour pouvoir aller à l'international.

Au sein de Hexatrust, cluster de vingt-cinq éditeurs de cybersécurité français créé en 2014[3], rassemblant plus de 1 500 employés, nous générons une croissance annuelle de 25 % à 30 %.

Dans le contexte de dialogue public-privé évoqué préalablement, nous préconisons qu'une image globale de la situation du tissu industriel soit élaborée et partagée par l'ensemble des acteurs du secteur.

L'écosystème européen de la cybersécurité se limite encore à quelques actions communes de recherche et développement. Il faut une volonté industrielle et normative forte, comme ce fut le cas avec Airbus, pour dégager des capacités d'investissement européen à la hauteur de l'enjeu industriel. Les initiatives d'investissement qui pourraient être prises en France et en Europe, visant à donner aux meilleures innovations les moyens de passer à l'échelle industrielle globale, seront bienvenues.

« En France, la cybersécurité, c'est 700 entreprises »

CONSTRUIRE UN MARCHÉ EUROPÉEN DE LA CYBERSÉCURITÉ

Le problème n'est pas tant la nationalité des entreprises que la richesse de l'écosystème qui doit être construit. Il faut rendre la cybersécurité attractive pour y attirer des investisseurs. Cela exige croissance et rentabilité. La première exige d'ouvrir les horizons de marché : le marché européen de la cybersécurité doit devenir une réalité. Si la seconde tarde à se concrétiser, cela fragilisera l'ensemble du dispositif, sauf présence d'acteurs capables de consolider l'ensemble. Les initiatives doivent venir du monde industriel. Le rachat par Thales de Vormetric (déjà précédé de celui de Sysgo par le même Thales) doit être suivi d'autres opérations avec d'autres acteurs au plan européen pour donner crédit à la démarche. Les annonces d'investissements importants de Cisco et Microsoft en France doivent être suivies. La rentabilité des acteurs de la filière doit pouvoir être améliorée, pour faciliter leur solidité et leur capacité d'investissement autonome.

© GEORGEJMCLITTLE / FOTOLIA

En France, le nombre de tablettes a été multiplié par 4 entre 2011 et 2013.

AGIR SANS DÉLAI

L'achat public doit, comme aux États-Unis, être utilisé en France comme un accélérateur de croissance pour les acteurs industriels nationaux. Les intérêts essentiels de sécurité permettent de justifier cette approche.

À court terme, des solutions hybridant intégrateur français et éditeurs étrangers permettent de préserver nos intérêts et de développer la filière sans hypothéquer l'avenir. Ainsi, la mise en place de la notion de service souverain pour garantir une solution sur la base de composants étrangers est l'approche choisie par Orange en France (comme par IBM en Chine). L'analyse de code doit être autant que possible privilégiée. Les données doivent être stockées en France. Il faut assurer un juste report des contraintes opérationnelles dans les contrats des donneurs d'ordre vers les fournisseurs. Enfin, comme tout domaine industriel, la cybersécurité devra intégrer des modèles d'externalisation du risque vers les assureurs, ce qui permettra peu à peu au risque cyber de se financiariser et, par là, de pénétrer transversalement l'entreprise.

IL N'Y A DE RICHESSE QUE D'HOMMES

Les prévisions font état d'un besoin de plusieurs centaines de milliers de spécialistes par an dans les prochaines années en Europe[4]. Les filières de formation en France dans le développement informatique sont encore trop peu développées et n'incluent pas suffisamment la sécurité informatique. La cybersécurité appelle des transferts de compétences, notamment des spécialistes d'autres domaines en retournement comme les systèmes embarqués et les réseaux.

Techniquement, la sécurité n'est pas que périphérique, mais doit être pensée en profondeur. Le contrôle d'exécution et la sécurité des plateformes sont des domaines techniques à réinvestir. La cryptologie a de beaux jours devant elle, car elle reste un ultime rempart important, et porte ses propres innovations comme la cryptologie dite homomorphe, qui permet de confier les calculs à un tiers sans que celui-ci ne connaisse ni les données ni les résultats. En termes d'innovation, l'analyse comportementale dans le flot de données va faire la différence à l'avenir. Développer de telles solutions requiert des profils de très haut niveau, capables de faire le pont entre statistiques et comportement des acteurs.

En termes d'ingénierie, le principal défi sera de passer à une conception produit intégrant plus fortement la sécurité et les usages. Une mauvaise qualité de développement logiciel est la pire menace informatique qui existe. Nous devons développer les métiers industriels du logiciel : programmation et développement produit, test et validation, incluant les méthodes et outils formels générateurs de productivité dans une logique de certification et de qualité produit.

© BERNARD ROUSSEAU / THALES

Thales a acheté Vormetric pour près de 400 millions de dollars.

« L'achat public doit être utilisé comme un accélérateur de croissance »

Enfin, il faut adapter les dépenses en marketing, gestion du produit, commercial et juridique à une vision ambitieuse de conquête. Un cycle de vie du produit dynamique et une adaptation native à l'environnement du client doivent être le standard et non l'exception pour nos produits. ■

1. Mc Kinsey, *Accélérer la mutation numérique des entreprises : un gisement de croissance et de compétitivité pour la France.*
2. Source IDC 2015.
3. Dont Bertin Technologies est une des fondatrices.
4. Le besoin aux États-Unis est évalué à 1 million de personnes à former annuellement.

RAPHAËL MARICHEZ (2002) *fonctionnaire de la sécurité des systèmes d'information (FSSI), ministère de l'Intérieur*

SÉCURITÉ DES SYSTÈMES D'INFORMATION : LA NÉCESSAIRE CLARIFICATION DES RÔLES

Le rôle du « responsable de la sécurité des systèmes d'information » (RSSI) est très mal défini. Parfois craint, parfois rejeté, il suscite l'intérêt lorsque surviennent des cyberattaques. Une clarification de son rôle et la mise en place d'une gouvernance collégiale de la sécurité sont indispensables pour assurer une vraie gestion des risques liés aux systèmes d'information.

Le RSSI n'est certainement pas « responsable » du niveau de sécurité informatique atteint par la structure qu'il représente. Le vocable même de RSSI trompe le dirigeant, qui, victime de l'illusion de pouvoir se reposer sur une seule personne ou équipe, se désintéresse du sujet.

L'ILLUSION DU TRANSFERT DE RESPONSABILITÉ

Lorsque les choses vont mal en matière de systèmes d'information, c'est bien auprès du DSI que les autorités cherchent des explications et des solutions. Après tout, l'essentiel des dispositifs de traitement, de diffusion ou de protection de l'information relèvent du système d'information proprement dit : les réseaux informatiques, les ordinateurs, les logiciels. Si les secrets commerciaux sont captés par la concurrence lors d'un piratage informatique, il serait difficile d'en attribuer la responsabilité au seul directeur commercial.

« La fonction SSI relève davantage d'un processus que de l'incarnation d'un pouvoir »

DES RESPONSABILITÉS IMBRIQUÉES

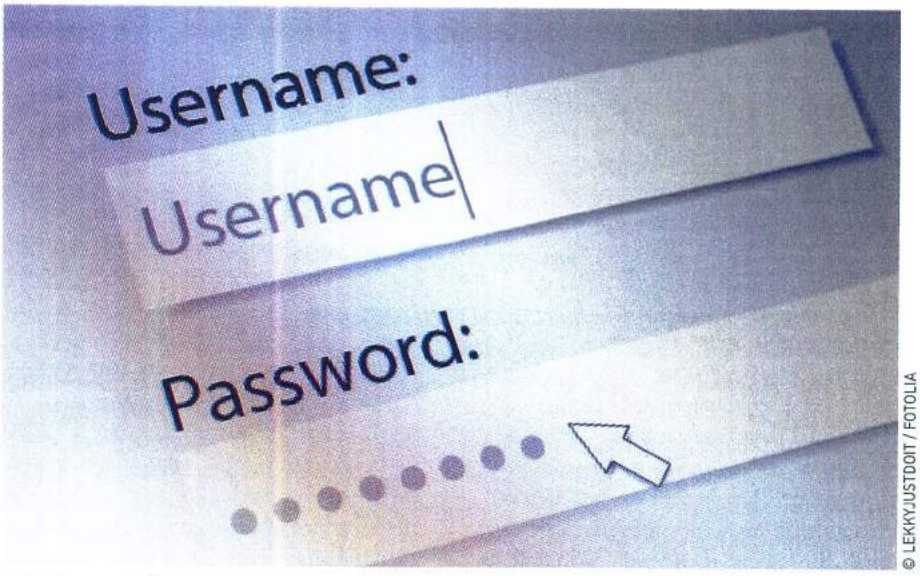
En pratique, le RSSI est un rouage d'une plus vaste structure transversale au sein de laquelle les responsabilités sont fortement imbriquées. Penser que le RSSI pourrait être comptable du niveau de sécurité, et donc des incidents et des préjudices subis, crée une distorsion néfaste au fonctionnement efficace de l'organisation : soit en concentrant exagérément les moyens et le pouvoir auprès d'une personne ou d'une équipe, soit, beaucoup plus souvent, en déresponsabilisant les autres parties prenantes de l'entreprise à l'égard du risque SSI.
La fonction SSI relève davantage d'un processus que de l'incarnation d'un pouvoir quelconque : un processus de gestion des moyens (financiers, techniques, humains), des risques, des coûts de la sécurité et de ceux de l'absence de sécurité. Ce processus doit idéalement irriguer de manière continue et homogène toute la structure jusqu'à ses interfaces, des actionnaires aux utilisateurs finaux. C'est pourquoi la protection et la défense des SI doivent être pensées dans leur ensemble et en lien avec les métiers, au risque, sinon, de menacer la structure entière à cause d'une seule défaillance localisée.

DES MOYENS GÉRÉS PAR LA DIRECTION DES SYSTÈMES D'INFORMATION

Puisque le DSI est sans nul doute le principal responsable du bon fonctionnement des systèmes d'information, il semble naturel, en première approche, que la fonction de pilotage de la SSI et des risques associés s'incarne en son sein. Le RSSI a donc longtemps été en charge de la mise en œuvre de briques de sécurité technologique nécessaires au bon fonctionnement des systèmes. Mais, aujourd'hui, il doit agir en liaison avec la gestion des risques métier réels.
La sécurité des SI ne se limite plus, en effet, au seul bon fonctionnement du système :

REPÈRES

RSSI pour responsable sécurité des SI, DSSI (directeur) ou FSSI (fonctionnaire), ou RSSI-groupe, RSSI opérationnel, OSSI (officier SSI)... Malgré les efforts des réglementations administratives ou internes aux compagnies privées, le rôle et les missions de ces acteurs en charge de la sécurité des systèmes d'information ne peuvent cependant pas être référencés sous un vocabulaire interchangeable. Leur activité au quotidien dépend étroitement de leur environnement professionnel immédiat, de la culture et des priorités de l'entreprise.



© LEKKYJUSTDOIT / FOTOLIA

La tendance est à la recherche de sécurité *by design*.

il faut compter avec l'espionnage économique, l'altération invisible des paramètres du système, le chantage au sabotage ou à la divulgation massive de données.

LES LIMITES D'UNE APPROCHE BUDGÉTAIRE

Les métriques les plus faciles à utiliser pour jauger du degré de prise en compte de la sécurité dans les SI reposent évidemment sur le budget. Les études publiées exposent une part de dépenses consacrées à la sécurité de l'ordre de 6 % à 12 % du budget des systèmes d'information. Ces chiffres masquent des réalités fort variables selon la façon de prendre en compte les dépenses. Aujourd'hui, la tendance est à la recherche de la sécurité *by design*, fondue au sein du produit, comme lorsqu'on achète une voiture sans se poser la question de la part du prix liée à l'airbag ou à l'ABS. La généralisation, notamment dans le monde anglo-saxon, des mécanismes de couverture du risque par des mécanismes de mutualisation (assurances) favorise cette tendance à la contractualisation d'une garantie de sécurité, notamment par le truchement de la certification de produits (critères communs), ou de processus (ISO 27001).

PILOTER LA SÉCURITÉ PAR LES RISQUES MÉTIER

Le pilotage moderne de la sécurité des systèmes d'information, ou plus exactement du risque lié à la (non-)sécurité, s'inscrit plus aisément dans la logique verticale de l'appareil productif de l'entreprise : le responsable de la *business unit* doit être amené à arbitrer le bon niveau de sécurité, au regard de ses enjeux métier propres, à la lumière d'une expertise avisée en matière d'évaluation des risques circonstanciés au métier. Le RSSI moderne est donc un expert et conseiller, apte à vulgariser le risque d'origine informatique qui pèse sur l'activité métier, force de propositions pour réduire ce risque, pilote des actions associées.

Cette démarche vise finalement à trouver un juste compromis entre risques, moyens de sécurité et priorités opérationnelles.

Les qualités d'expertise, de pédagogie, d'ouverture d'esprit, et la force de conviction du RSSI sont fondamentales. Le responsable métier (maître d'ouvrage) doit pouvoir s'appuyer avec une confiance quasi totale sur son RSSI, dans un monde technique au vocabulaire incompréhensible, face à une ou plusieurs DSI confrontées à leurs propres enjeux, face aux prestataires et fournisseurs, face aux clients indécis, face aux autorités réglementaires exigeantes, le tout sous contraintes de moyens et de calendrier. Cette confiance ne se décrète pas par un titre, mais se gagne au mérite.

« Le RSSI devient à la fois un stratège et un lobbyiste »

ARBITRER LA SÉCURITÉ DANS LES APPLICATIONS TRANSVERSES

Dès lors qu'un système d'information, généralement de soutien (messagerie, réseau, hébergement, bureautique, téléphonie, etc.) est transversal aux différents métiers, le juste équilibre entre investissement et bénéfice est beaucoup plus difficile

à déterminer. Les différentes populations bénéficiaires n'ont en effet pas la même appétence au risque : chacune n'est pas prête à contribuer au même niveau à l'effort collectif. L'arbitrage devient délicat.
Dans le domaine des systèmes d'information transverses, les méthodes de gestion des coûts de soutien mutualisés, et, à travers elles, les méthodes d'arbitrages des projets de sécurisation des SI, constituent aujourd'hui un domaine d'exploration et de recherche passionnant. Le RSSI appréhendera les mécanismes budgétaires et décisionnels de sa structure afin d'orienter les efforts de sécurité dans la direction qu'il pense être la plus adaptée : il devient à la fois un stratège et un lobbyiste.

DIFFUSER UNE CULTURE DE CYBERSÉCURITÉ

La fonction SSI moderne s'oriente vers des actions de long terme, influençant lentement les habitudes de travail et les structures décisionnelles au sein de l'entreprise. C'est ainsi tout naturellement que cette fonction SSI se rapproche étroitement de celle d'un communicant, voire d'un « évangéliste » : sensibiliser, former, promouvoir, diffuser et infuser, vendre la sécurité en interne, ainsi qu'auprès des clients, fournisseurs et partenaires, jusque dans les comportements de la vie privée, afin d'impulser le changement.
Cette activité est en concurrence avec d'autres activités transversales non moins légitimes : politique sur le handicap, sécurité incendie, développement durable, etc. En outre, son efficacité est extrêmement difficile à mesurer. C'est pourquoi il s'agit très certainement de la tâche la plus difficile du RSSI, du reste rarement formé aux techniques de la communication et du marketing.

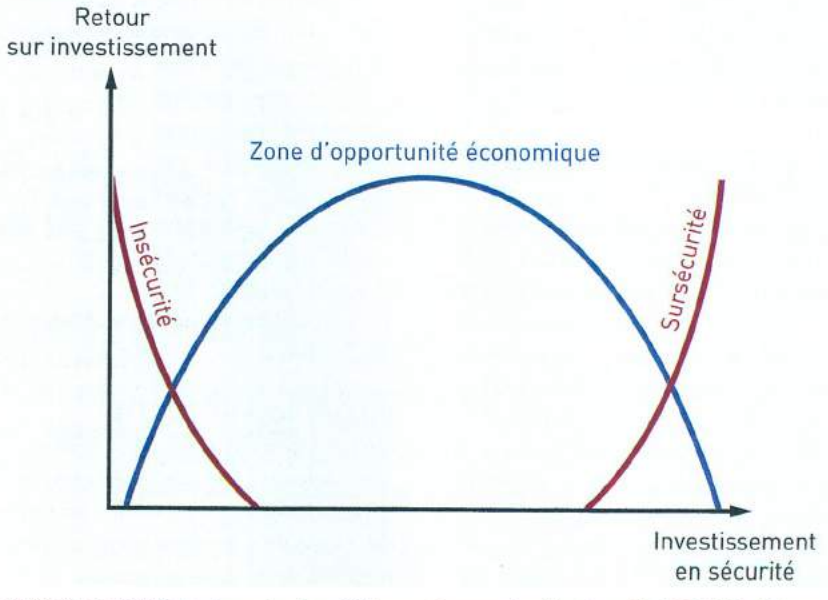
GÉRER LES CRISES

Parmi les leviers de la communication, la capitalisation sur les incidents de sécurité, voire les crises, est un atout évidemment essentiel à exploiter. Cette capitalisation ne peut compenser à elle seule les coûts et préjudices liés à l'incident, mais exige néanmoins une préparation en amont trop souvent oubliée, notamment en matière d'indicateurs sur les impacts des incidents (RH consommée, perte d'exploitation, coût des investigations et de la reconstruction).
L'acteur de la SSI doit être au cœur de la gestion de la crise cyber, sauf à s'interdire d'exploiter une formidable caisse de résonance : la proximité avec les responsables métier, l'indépendance complète à l'égard de la DSI, l'attention de la part de la haute hiérarchie sont autant de facteurs, qui, bien qu'éphémères et simultanés, favorisent la capacité du RSSI à convaincre pour impulser des changements significatifs dans les habitudes, les procédures ou les architectures.
Le volet communication ne doit pas rimer pour autant avec gesticulation. Un grand doigté est requis pour gérer les attentes, souvent irrationnelles et éphémères de l'échelon supérieur (quel pays nous attaque ? pour quel motif ? quand pourra-t-on reprendre une vie normale ?) et en tout cas sans lien avec les actions à mener en résolution de crise (exploiter les traces, reproduire le chemin d'attaque voire l'anticiper, prioriser les RH disponibles, sacrifier des systèmes, tenir une main courante et faire circuler l'information).
Bien qu'évidemment non souhaitable, une crise bien préparée et bien gérée est un formidable outil de sensibilisation et de collecte de métriques au profit du pilotage de la SSI dans sa globalité.

« Communication ne doit pas rimer avec gesticulation »

CHERCHER LE BON COMPROMIS ENTRE COÛTS ET EFFICACITÉ

En aval du marketing interne de la SSI, les actions variées d'un acteur de la SSI, qui serait économiquement rationnel, concourent finalement toutes à un objectif de maximisation des effets positifs de la SSI sur le *business*, évidemment, sous contrainte des moyens alloués.
Faut-il en effet s'efforcer de trouver (et de prouver) le graal du RSSI, le « retour sur investissement (ROI) de la sécurité » ? J'ai expliqué la grande difficulté à calculer le coût de la sécurité. Évaluer objectivement le coût de la non-sécurité (perte d'exploitation, gestion de l'incident, reconstruction, sans compter



DR

Il est difficile de définir le niveau de sécurité économiquement optimal, mais le RSSI doit s'efforcer de s'en rapprocher en moyenne.

© MIMADEO / FOTOLIA

Diriger les moyens disponibles de la meilleure façon qui soit.

le préjudice invisible comme l'espionnage économique) est certainement encore plus utopique, surtout au milieu d'une gestion de crise. L'extrême volatilité de la probabilité d'occurrence du sinistre ne milite pas non plus en faveur d'une approche de type assurance du risque cyber : la fréquence des cyberattaques sur des sites Internet français a par exemple connu une explosion sans précédent la semaine ayant suivi les attentats de *Charlie Hebdo*. Pour ne rien arranger, les statistiques de sinistralité dans ce domaine ne dépassent évidemment pas quelques années d'historique.

Au lieu de tenter de calculer en vain un ROI crédible, une autre approche est possible : simplement diriger les moyens disponibles de la meilleure façon qui soit, en proscrivant les extrêmes, et en recherchant une certaine homogénéité du niveau de sécurité au sein d'un périmètre de sensibilité homogène. Il vaut généralement mieux s'attacher à fiabiliser un système de chiffrement de données partagé (par exemple : HTTPS) plutôt que d'ajouter une surcouche de chiffrement applicatif spécifique au projet.

Ce pilotage optimal des moyens alloués (ou allouables) à la sécurisation des SI, au sens large, doit être la ligne de conduite permanente du RSSI. Celui-ci doit ainsi rechercher les leviers d'action, la plupart du temps évidemment sans autorité hiérarchique directe, sur les grandes masses de moyens. Il s'agit tout autant des moyens financiers, humains, que matériels, et tout autant des moyens de pure sécurité (pare-feux, antivirus, sondes, etc.) que des moyens annexes utilisables au profit de la sécurité (systèmes bureautiques, annuaires, cœurs de réseaux, badges avec puce électronique, etc.).

« Le risque cyber est sous-jacent à la gestion du risque lié à l'activité »

INSTAURER UNE GOUVERNANCE DE LA SÉCURITÉ

Le rôle moderne du RSSI, quelle que soit sa dénomination exacte, ne peut donc faire l'économie d'un pilotage transverse de moyens qu'il ne possède pas, au travers de leviers tactiques sur lesquels il n'a aucune prise directe. Comment faire ?

D'une part, la méthode la plus complète repose sur une bonne connaissance de l'existant par les audits et les tests d'intrusion (patrimoine informatique, ou numérique pour les plus avancés, ses vulnérabilités, ses atouts), une gestion-capitalisation des incidents de sécurité, et une gestion des risques à plusieurs niveaux (entreprise, *business unit*, projet) liant le risque porté par le système d'information aux intérêts du projet, du *business*, de l'entreprise.

D'autre part, le « savoir-être » des acteurs mettant en œuvre ces trois processus est indispensable : les qualités de relations humaines, de communicant et de conviction permettent le « management transverse », une espèce de *soft power* influençant les structures de l'entreprise échappant à son autorité hiérarchique. Ces qualités favorisent également la création d'un quasi-service de renseignement interne, absolument nécessaire au travail du RSSI.

VALORISER LA SÉCURITÉ PAR UN VRAI MARKETING INTERNE

Ce portrait d'un RSSI modèle et moderne n'est certainement pas parfait, immuable ni absolu. Il traduit une vision répondant aux besoins actuels des grandes organisations de culture francophone, et au constat malheureux d'un véritable divorce entre le RSSI et les bénéficiaires de son action en entreprise ou en administration. La faute est largement partagée : trop rares sont les RSSI qui prennent le temps d'aller rencontrer les « métiers » pour « vendre » de la sécurité qui corresponde à leurs besoins, trop rares sont les dirigeants qui acceptent de perdre en confort pour protéger le patrimoine de la société.

La cybersécurité en entreprise ou en administration est résolument à la confluence de la gestion du risque opérationnel et du numérique, dont le système d'information est le socle. De même que les géants du Web tirent leur prodigieuse efficacité de l'intégration verticale des composantes du numérique (du dimensionnement de la fibre optique transatlantique au modèle économique de diffusion du contenu en Europe), les dirigeants publics et privés doivent intégrer le risque cyber comme un sous-jacent de la gestion du risque lié à l'activité qu'ils dirigent, risque dont la responsabilité leur incombe *in fine*. ■

ÉRIC FREYSSINET (92) *conseiller auprès du préfet, chargé de la lutte contre les cybermenaces*

CYBERCRIMINELS : UN ARSENAL EN PERPÉTUELLE ÉVOLUTION

Les menaces de la cybercriminalité sont multiformes et changent en permanence. La lutte contre les menaces qu'elle induit passe d'abord par une connaissance intime de ce monde, par des actions tout aussi rapides que coordonnées et par un travail constant de sensibilisation des victimes potentielles.

© RAWPIXEL.COM / FOTOLIA

La forme la plus courante d'installation d'un logiciel malveillant est l'installation volontaire d'une application d'apparence banale.

LE MODE DE DIFFUSION des logiciels malveillants prend aujourd'hui plusieurs formes. La première est la propagation automatique, par la découverte sur les réseaux de nouvelles machines vulnérables. On parle alors de vers qui se propagent ainsi d'une machine à une autre.

« Certains délinquants installent plusieurs logiciels malveillants à la fois »

DES LOGICIELS MALVEILLANTS QUI SE RÉPANDENT EN CASCADE

La seconde est la diffusion par pièce jointe à un courrier électronique ou en téléchargement direct depuis un site Web, la victime cliquant sur le lien de téléchargement ou la pièce jointe. C'est notamment le cas sur les plates-formes mobiles où la forme la plus courante d'installation d'un logiciel malveillant est l'installation volontaire d'une application d'apparence banale depuis un magasin d'applications. Enfin, le téléchargement au cours de la navigation (ou *drive-by download*) se déroule à l'insu de la victime lorsqu'elle utilise son navigateur Internet. Ce dernier mode d'infection est le plus courant aujourd'hui, car il touche un plus

REPÈRES

Comprendre la menace est essentiel à la lutte contre la cybercriminalité. C'est essentiel bien évidemment pour ceux qui sont en première ligne, services d'investigation ou équipes œuvrant dans le domaine de la sécurité des systèmes d'information, mais c'est tout aussi important pour les victimes potentielles, ne serait-ce que pour prévenir ces menaces. L'arsenal moderne des cybercriminels comprend un certain nombre d'outils et de plates-formes basés autour des logiciels malveillants : *botnets*, plates-formes d'*exploits*, systèmes de distribution de trafic. Un univers à explorer pour mieux l'appréhender, mieux se protéger voire participer à la lutte contre ces phénomènes.

grand nombre de victimes potentielles, mais il suppose de mettre en œuvre une infrastructure plus complexe.

LES CINQ COMPOSANTES DE L'ARSENAL CYBERCRIMINEL

Premier type d'arme utilisé : les *botnets*, réseaux de machines utilisant un programme malveillant. Une machine infectée par un de ces logiciels malveillants devient un *bot*, qui dès lors communique avec une infrastructure de commande et de contrôle permettant au maître du *botnet* de piloter l'ensemble des *bots* et de recueillir les informations confidentielles collectées.

Une telle architecture permet de combiner un grand nombre de fonctionnalités. Ainsi, les délinquants peuvent installer d'autres logiciels malveillants ou collecter des mots de passe, même si la fonction première est autre, comme l'envoi de courriers électroniques non sollicités (spam).

L'infrastructure de commande et de contrôle du *botnet* peut prendre différentes formes, des architectures centralisées (reposant par exemple sur un simple serveur Web) aux architectures décentralisées (sur le principe des réseaux pair-à-pair). Ces dernières sont les plus résilientes et sont choisies pour les *botnets* les plus aboutis et, au bout du compte, les plus difficiles à démanteler.

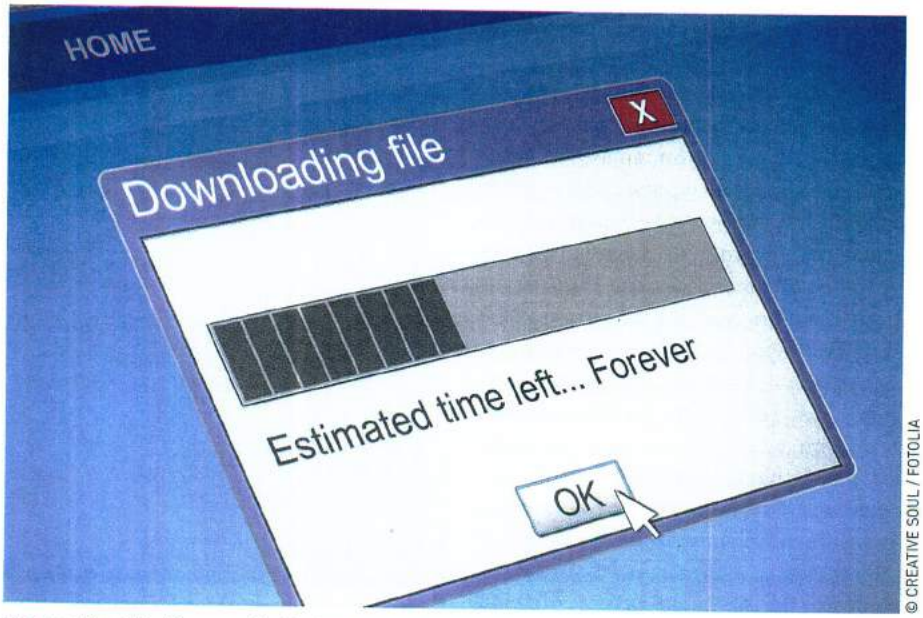
LES BANQUES EN LIGNE DE MIRE

Selon nos observations, recoupées par exemple par la synthèse qu'en réalise Europol, les *botnets* les plus préoccupants actuellement sont ceux qui ciblent les transactions bancaires avec un développement croissant de ceux qui s'en prennent aux terminaux de points de vente, ainsi que les *cryptolockers* (ou « rançongiciels chiffrants », qui rendent inaccessibles les fichiers personnels trouvés sur l'ordinateur et réclament le paiement d'une rançon). De même, des architectures de *botnets* sont utilisées pour la réalisation d'étapes importantes des opérations d'espionnage industriel qui ciblent de nombreuses administrations ou entreprises aujourd'hui.

DES ACTIONS EN RÉSEAU

Autre aspect intéressant des *botnets* : les mécanismes de valorisation utilisés. Bien entendu, le maître du *botnet* cherche à commercialiser les données qu'il en tire, ou à sous-louer ses services (des attaques pour bloquer l'accès à un service par exemple). Dans d'autres cas, il peut se contenter d'administrer le *botnet* et confier le « recrutement » de victimes à des affiliés – à charge pour eux d'envoyer des spams ou de faire appel aux services d'un gestionnaire de plate-forme d'*exploit* pour infecter les systèmes de leurs futures victimes. Dans d'autres cas, le logiciel malveillant est commercialisé sous forme de kit, le développeur n'ayant alors pas à se soucier de prendre le risque de le mettre en œuvre lui-même : c'est le cas notamment de beaucoup de catégories de logiciels malveillants qui ont du succès dans la communauté cybercriminelle comme les *botnets* bancaires ou plus récemment les *cryptolockers*.

« L'Angler exploit kit générerait 60 millions de dollars par an de revenus criminels »



© CREATIVE SOUL / FOTOLIA

Une machine infectée par un logiciel malveillant devient un *bot*.

PLATES-FORMES D'EXPLOITS

Lorsqu'un internaute se connecte, volontairement ou à son insu, sur une plate-forme d'*exploit*, celle-ci teste un certain nombre de vulnérabilités connues en vue de les exploiter. Il peut s'agir de vulnérabilités du système d'exploitation, du navigateur Web ou encore d'extensions logicielles (extensions pour visualiser des animations, des vidéos ou des fichiers PDF par exemple).

La plate-forme d'*exploit* la plus célèbre était pendant quelques années le *Black Hole exploit kit*, développé et commercialisé par un citoyen russe agissant sous le pseudonyme Paunch et qui a été interpellé en octobre 2013 par la police de Moscou. La plate-forme qui tient actuellement le haut du pavé est certainement l'*Angler exploit kit*. Celui-ci générerait des revenus criminels atteignant 60 millions de dollars par an rien qu'en diffusant une campagne de rançongiciels.

LES DEALERS DU CYBERCRIME

Les systèmes de distribution de trafic (TDS) sont une catégorie de services cybercriminels qui montre la complexification de cet écosystème. Il s'agit, pour la personne qui l'administre, d'être en mesure d'offrir à ses clients du trafic garanti avec un certain nombre de caractéristiques : pays d'origine, version du système d'exploitation ou encore volumétrie. En amont, lui-même ou des sous-traitants attirent des victimes vers le TDS, puis le système réalise un tri au profit des différents clients. Sutra TDS, Kallisto TDS ou Simple TDS sont quelques-uns des noms des « produits » commercialisés pour mettre en œuvre un tel système.

HÉBERGEMENT : LA STRATÉGIE DU COUCOU

L'ensemble des cybercriminels utilisent les infrastructures Internet existantes pour accomplir leurs méfaits. Mais ils ont besoin de certaines qualités complémentaires pour être encore plus efficaces. Certains d'entre eux se sont donc spécialisés dans l'administration de serveurs, le détournement de serveurs légitimes ou encore la création de véritables hébergeurs à l'abri des enquêtes judiciaires (autrement appelés *bullet-proof hosters*). Ils réalisent cela en abusant leurs employeurs, en louant des services chez des hébergeurs légitimes (tous les grands hébergeurs français et européens en sont régulièrement victimes), ou encore en mettant en place des sociétés ayant pignon sur rue.

LA PISTE DE L'ARGENT

Une des catégories d'acteurs qui intéresse les enquêteurs est celle des intermédiaires financiers, c'est-à-dire l'ensemble de ceux qui permettent de blanchir les revenus de ces trafics. Certains se sont spécialisés dans le recrutement et la gestion de mules qui font transiter sur leurs comptes bancaires l'argent détourné ou réexpédient les colis. Ces activités se complexifient avec l'avènement des services de monnaie électronique. Même s'ils semblent évidents à cibler dans l'enquête judiciaire (avec l'idée de remonter la piste de l'argent), leur action constitue souvent un véritable paravent qui rend très complexe et coûteuse en temps l'identification des véritables commanditaires.

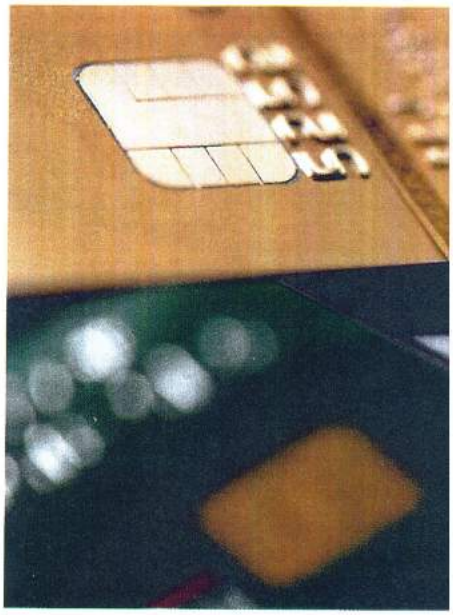
L'une des fonctions particulièrement attendues des cyberdélinquants est la possibilité de mettre en place très rapidement un serveur proche de ses victimes potentielles et d'en changer rapidement en laissant le moins de traces possibles.

« Une véritable balkanisation des acteurs, chacun s'étant spécialisé dans un rôle »

PLATES-FORMES DE MARCHÉ ET OUTILS DE COMMUNICATION

Ces activités ne pourraient se développer sans la capacité pour les cyberdélinquants de rentrer en contact les uns avec les autres. Ils se rencontrent traditionnellement sur des espaces de discussion dédiés (forums Web, canaux de discussion IRC), aussi certains d'entre eux se sont-ils spécialisés dans l'animation de tels espaces avec des fonctionnalités supplémentaires : procédure d'intégration, notation, garantie de l'anonymat, notation des services offerts par les uns et les autres, services de vérification de numéros de carte bancaire volés ou encore de logiciels malveillants pour s'assurer que le produit commercialisé n'est pas détecté par les antivirus. Ces plates-formes de discussion sont hébergées aussi bien sur des serveurs librement accessibles sur Internet (avec un simple navigateur Web) ou uniquement *via* une connexion sécurisée par le protocole d'anonymisation Tor. Les délinquants y apprennent les méthodes, discutent les offres ou encore affichent leurs publicités.

Assez rapidement, la discussion se porte ensuite sur d'autres moyens de communication plus confidentiels, comme des courriers électroniques jetables et chiffrés ou l'utilisation de messageries instantanées. Ainsi, le logiciel de discussion interpersonnelle ICQ était très utilisé dans la première moitié des années 2000 ; il a été progressivement remplacé par le protocole Jabber/XMPP, indépendant d'un quelconque fournisseur de services et permettant d'y rajouter facilement une couche de chiffrement.



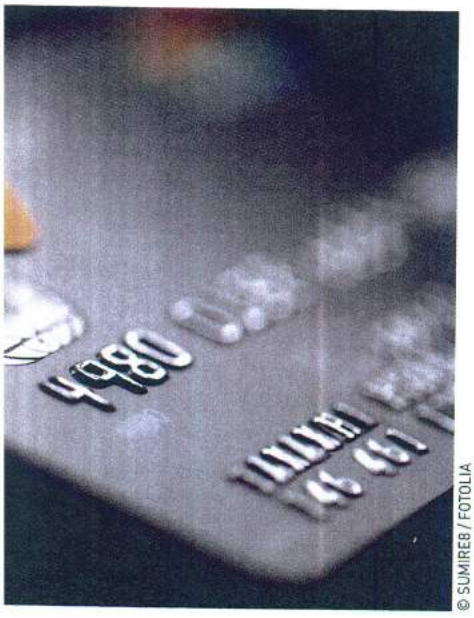
Certains délinquants offrent des services de vérification de numéros de carte bancaire volés.

UN ÉCOSYSTÈME EN MUTATION

L'évolution de la délinquance numérique au cours des vingt dernières années a d'abord marqué un retrait des formes classiques de criminalité organisée (structurées, stables, dont la taille est moyenne à grande) pour des formes d'organisation plus diffuse. On voit apparaître une véritable balkanisation des acteurs, chacun s'étant spécialisé dans un rôle donné, cherchant un maximum de flexibilité pour les uns ou un minimum de risques pour les autres.

« Le développement de la cyberdélinquance est en accélération »

Cette fragmentation contribue à rendre encore plus complexes les enquêtes judiciaires. Ainsi, si l'on arrive plusieurs semaines après le début d'une campagne de diffusion d'un logiciel malveillant, il est possible que le maître du *botnet* fasse appel à un TDS différent, un autre administrateur de plate-forme d'*exploit* ou un fournisseur de spam moins coûteux ou plus efficace. Et évidemment les traces des opérations correspondant aux victimes qui ont d'abord contacté les services d'enquête ont alors totalement disparu.



© SUMIREB / FOTOLIA

Pour cette raison, il est indispensable que la justice, les enquêteurs et les groupes de spécialistes ou entreprises spécialisées travaillant sur ce type de menaces prennent rapidement le recul nécessaire: comprendre comment les menaces sont distribuées, comment elles sont organisées et quelle est leur dynamique, sans jamais s'arrêter à une photographie dans le temps, pour être en mesure d'identifier les cibles de leur action.

Cela veut aussi dire qu'il ne faut pas forcément s'intéresser à un logiciel malveillant en particulier, mais à l'ensemble de l'écosystème qui tourne autour. Il sera parfois plus efficace de chercher à s'en prendre à une infrastructure de distribution de trafic ou une plate-forme d'*exploit* qu'à un petit *botnet* opéré par un délinquant ayant acquis un simple kit.

UNE LUTTE IMPLIQUANT DE NOMBREUX ACTEURS

Les pistes pour lutter contre ces nouvelles menaces sont complexes, mais la difficulté de la tâche rend cette complexité nécessaire. En effet, les succès sont encore trop peu nombreux et le développement de la cyberdélinquance est en accélération.

Il est d'abord important de bien comprendre les menaces, de partager cette compréhension et de prendre systématiquement le recul nécessaire pour bien comprendre l'ensemble des acteurs auxquels on peut être confronté.

Il faut être en mesure d'inventer les techniques permettant de détecter ces menaces, mais aussi d'imaginer celles qui permettront de lutter activement contre elles, par exemple identifier les faiblesses dans les infrastructures de commande et de contrôle qui pourront être exploitées.

Il est indispensable que les actions menées contre ces acteurs soient coordonnées entre les différentes parties prenantes. Aucune action technique ne sera efficace si elle n'est associée à l'identification et à l'arrestation des auteurs des méfaits, qui sans cela auront tout loisir de relancer leurs activités.

Ces actions peuvent évidemment avoir pour objectif de rendre plus coûteux le déploiement des menaces, par exemple en démantelant systématiquement les infrastructures utilisées chez les hébergeurs légitimes ou encore en informant les victimes potentielles et en les dotant d'outils permettant de détecter et nettoyer ces menaces dès qu'elles apparaissent.

Tous ont donc un rôle à jouer dans cette lutte, en particulier les acteurs de la réponse à incidents, voire de la réparation informatique, qui collectent potentiellement tous des informations essentielles sur la réalité de cette menace au contact des victimes. C'est aussi un champ d'action pour les hébergeurs, les fournisseurs d'accès à Internet et très certainement la communauté académique. Il faut souhaiter que se multiplient les initiatives leur permettant d'échanger et de se coordonner. ■

DES GROUPES CRIMINELS TRÈS ORGANISÉS

En parallèle d'un écosystème cybercriminel diffus, certains indices récents font apparaître l'émergence de nouvelles formes de groupes criminels très organisés. D'abord, on note un investissement croissant des groupes criminels organisés classiques dans certaines de ces délinquances numériques, comme lors des attaques massives contre le marché du carbone. Ainsi, de nombreux observateurs notent l'apparition de groupes très structurés, comme le groupe Carbanak qui serait derrière un détournement massif dans des banques notamment situées en Russie.

POUR ALLER PLUS LOIN

Éric Freyssinet, « Lutte contre les botnets : analyse et stratégie », mémoire de thèse de doctorat : http://blog.crimenumerique.fr/2015/11/21/lutte-contre-les-botnets/

GUILLAUME POUPARD (92) *directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)*

CHACUN EST RESPONSABLE DE TOUS

Au sein d'un monde numérique en construction, les équipes de l'ANSSI sont en lien étroit avec ceux qui détiennent des leviers politiques, économiques et technologiques permettant de garantir la sécurité, condition indispensable de la réussite de la transition numérique qui permettra à la France de rester parmi le premier cercle des nations.

TROIS IDÉES irriguent la stratégie nationale pour la sécurité du numérique.

La première idée est commune dans son expression mais prend ici une dimension particulière. Au sein d'un monde numérique en construction, chacun d'entre nous a une part de responsabilité effective dans la sécurité et la défense nationale.

Il ne s'agit pas simplement d'une sorte d'incarnation numérique de « l'esprit de défense » que chacun connaît bien et qu'il faudrait développer dans les réseaux. Comme le montrent les traitements de nombreuses attaques informatiques, les caractéristiques propres au cyberespace font que le comportement d'un seul peut compromettre la sécurité de beaucoup, de tous.

« Le comportement d'un seul peut compromettre la sécurité de beaucoup, de tous »

TROIS COMMUNAUTÉS

Trois communautés sont identifiées.

Il y a d'abord celle qui regroupe les innovateurs, les créateurs des nouveaux usages, services et produits du numérique, les chercheurs, les opérateurs de réseaux de communications électroniques, les entreprises du domaine de la cybersécurité, les équipementiers et les intégrateurs. Cette communauté a le devoir de proposer des produits et services dont le niveau de sécurité correspond aux besoins exprimés par la nécessaire analyse de risque qui doit accompagner tout projet numérique.

La deuxième communauté est constituée de tous ceux qui prennent les décisions concernant la « gestion de la cité » : élus, gouvernement, administrations centrales et territoriales et syndicats. La mission de cette communauté est d'intégrer la sécurité et la défense du numérique dans leur vision politique des entités dont ils ont la charge. Il appartient, par exemple, à l'élu d'une collectivité territoriale de demander à ses services que le site Internet de sa collectivité bénéficie du niveau de sécurité nécessaire, comme il lui appartient de faire voter les budgets requis.

Beaucoup parmi les polytechniciens appartiennent à cette communauté ou la servent. La complexité du gouvernement de sociétés avancées comme la nôtre fait que des questions apparaissant d'abord comme techniques sont rarement débattues au plus haut niveau. Le décideur politique et ceux qui le conseillent doivent bien comprendre l'étroitesse des

UN ENJEU À NOTRE PORTÉE

Les X sont nombreux parmi les bâtisseurs du numérique, dans les laboratoires ou à des postes clés d'opérateurs ou d'entreprises du domaine. Moi-même, à la tête d'une agence en forte croissance, je constate combien est importante la compréhension par cette communauté du niveau de la menace à laquelle nous sommes confrontés. Il s'agit de construire un monde numérique durable – et il ne le sera que s'il est sûr. C'est un enjeu à notre portée pour peu que soient prises suffisamment en amont les questions de sécurité.

REPÈRES

Le Premier ministre a présenté, le 16 octobre 2015, la « stratégie nationale pour la sécurité du numérique », en présence notamment de la secrétaire d'État chargée du numérique, du secrétaire général de la Défense et de la sécurité nationale, du président du Conseil national du numérique et de nombreux responsables d'entreprises. Cette participation des plus hautes instances de l'État et d'acteurs économiques de premier plan montre que, transition numérique aidant, les questions liées à la cybersécurité, issues de la seule sphère technique, sont devenues de réels enjeux de société.

© SYDA PRODUCTIONS / FOTOLIA

Il revient à chaque utilisateur d'exploiter les ressources du numérique avec la prudence nécessaire pour ne pas se mettre en danger.

liens entre la confiance que les administrés attendent – et qui sera demain la condition de leur utilisation des services publics numériques – et la sécurité informatique. Ce point est essentiel. Cette confiance doit être visée et financée dès la construction de projets dont la robustesse aux attaques informatiques doit être régulièrement mesurée.

La troisième communauté, la plus large, est constituée de tous les utilisateurs du numérique, des chefs d'entreprises ou des responsables d'associations, de tous les citoyens. Il leur revient d'utiliser les ressources du numérique avec la prudence nécessaire pour ne pas se mettre en danger, mettre en danger leurs proches ou leur entreprise, leurs clients ou leurs fournisseurs.

Dans les faits, chacun appartient au moins à deux communautés. Dans le cyberespace, comme l'a écrit Antoine de Saint-Exupéry : « Chacun est responsable de tous. Chacun est seul responsable. Chacun est seul responsable de tous. »

DONNÉES PERSONNELLES

La deuxième idée contenue dans la stratégie nationale pour la sécurité du numérique est encore naissante même si, intuitivement, chacun peut en comprendre les fondements. Elle a trait à la captation des données personnelles des Français. On peut l'illustrer par deux exemples. D'une part, une captation massive de ces données personnelles à des fins d'exploitation économiques par des acteurs étrangers peut entraîner un déséquilibre défavorable susceptible de mettre en danger une part de l'économie nationale voire européenne. D'autre part, et dans certains cas, une captation ciblée de données personnelles – par exemple celles disponibles sur les réseaux sociaux concernant directement ou indirectement tous les personnels du ministère de la Défense – et leur exploitation peuvent constituer un problème de sécurité nationale.

« Une captation ciblée de données personnelles peut constituer un problème de sécurité nationale »

Si quelques cas d'exploitation de données personnelles obtenues par attaque informatique ont mis en danger les personnes concernées ou les entreprises victimes, il n'y a pas, à ce jour, de démonstration corroborant cette menace, même si on en comprend aisément les mécanismes.

INVERSER LA CHARGE DE LA PREUVE

La troisième idée est issue d'une anticipation fondée sur l'observation des faits : depuis plusieurs années, les attaques informatiques sont en croissance forte en nombre et en sophistication. Plus la France avance dans sa transition numérique, plus elle augmente sa « surface d'attaque » et plus grand est le risque d'être victime d'une attaque informatique. Ce raisonnement est applicable pour tout pays. Pourtant, pour l'entreprise, pour l'administration et pour chacun d'entre nous, la sécurité est régulièrement présentée et toujours vécue comme une contrainte et un coût.

La stratégie nationale pour la sécurité du numérique propose en quelque sorte d'inverser la charge de la preuve. La sécurité informatique doit devenir un avantage concurrentiel pour les produits et services proposés par les entreprises françaises. Dans un marché mondial concurrentiel et face à

© SKYLINE / FOTOLIA

Toute formation initiale supérieure doit intégrer une sensibilisation à la cybersécurité.

des menaces révélées quotidiennement, notamment contre la confidentialité des données ou la résilience de produits connectés, les utilisateurs se tourneront demain vers les produits et services qu'ils estimeront de confiance. Ainsi, pensée et intégrée en amont de la conception, la sécurité numérique des produits et services proposés par les entreprises françaises sera, à performance égale, en position favorable sur les marchés internationaux.

CINQ OBJECTIFS

Le 16 octobre 2015, le Premier ministre a présenté les grands axes et orientations de la stratégie nationale pour le numérique. Issue d'un travail interministériel engagé en juin 2014, cette stratégie présente cinq objectifs et propose pour chacun d'entre eux des orientations. Il appartient désormais aux ministères, soutenus par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), de contribuer à l'atteinte de ces objectifs par des actions relevant de leurs champs de compétences.

Le premier axe de la stratégie est dans la continuité des orientations données par les Livres blancs sur la défense et la sécurité nationale de 2008 et 2013. Il vise à renforcer la protection des infrastructures critiques de la France par une croissance de la sécurité de leurs systèmes d'information. C'est le sens du travail engagé entre l'ANSSI et les opérateurs d'importance vitale pour la mise en œuvre des dispositions législatives relatives à la sécurité des systèmes d'information contenues dans la loi de programmation militaire de décembre 2013.

« Promouvoir et défendre dans le cyberespace les valeurs de la République »

PROTÉGER LA VIE NUMÉRIQUE DES FRANÇAIS

Le deuxième axe concerne plus particulièrement la protection de la vie numérique des Français. En complément du premier axe, il s'agit d'une part de promouvoir et défendre dans le cyberespace les valeurs de la République, et d'autre part d'apporter une aide aux entreprises et particuliers victimes d'actes de cybermalveillance. Sur ce dernier point, un groupe de travail copiloté par le préfet chargé de la lutte contre les cybermenaces du ministère de l'Intérieur et l'ANSSI a permis de poser les bases de ce que sera le dispositif d'aide qui sera mis en place courant 2016.

Le troisième axe aborde les enjeux des formations initiales et continues. La stratégie souligne que l'ensemble des Français doivent être sensibilisés et que toute formation initiale supérieure doit intégrer un volet sensibilisation ou formation à la cybersécurité adapté à la filière.

Le quatrième axe vise à favoriser le développement d'un écosystème favorable au développement de produits et services de sécurité performants et de confiance. Il s'agit également de transformer la contrainte budgétaire et humaine liée à l'intégration de la sécurité informatique dans les produits et services en avantage concurrentiel pour l'entreprise et en valeur ajoutée pour le client.

MOBILISER L'UNION EUROPÉENNE

Le cinquième axe, enfin, vise à mobiliser les États membres de l'Union européenne pour atteindre une véritable souveraineté numérique propice au développement d'acteurs européens de la cybersécurité. L'objectif est également de renforcer l'influence française dans les instances internationales.

Notre formation et nos responsabilités nous placent en première ligne pour la mise en œuvre de l'effort qui permettra à notre nation d'être résiliente à des attaques informatiques qui aujourd'hui grèvent notre compétitivité, nous appauvrissent et détruisent des emplois et demain viseront nos infrastructures critiques, au risque de pertes de vies humaines et de dommages économiques graves. ■