Les pré-requis de la vie sur la Toile

Par le Pr Houda Imane Faraoun, ministre de la Poste et des TIC

Depuis la naissance des civilisations humaines, les échanges d'informations entre les individus ont constitué une nécessité absolue : un moyen d'acquisition de connaissances, de développement et de maintien des liens sociaux. Ces échanges nécessitent parfois d'être sécurisés, protégés et tenus secrets, afin de protéger une information capitale, de partager des confidences intimes ou de préserver la confidentialité d'une donnée utile.

Le besoin de sécuriser les communications est aussi ancien que les communications elles-mêmes. Durant les conflits des civilisations les plus anciennes, la protection d'une communication, ou plus particulièrement d'une information, se faisait en cachant sont existence. Les Chinois de l'Antiquité dissimulaient leurs envois en les inscrivant sur de la soie roulée en boule et recouverte de cire, que le porteur dissimulait sur lui, voire même avalait. En Europe, les Romains rasaient la tête du messager avant de lui inscrire le message dessus et laissaient pousser les cheveux. De telles méthodes, dites «stéganographiques», ont servi longtemps, mais se sont rapidement avérées insuffisantes, car la simple connaissance de l'existence du message induisait sa divulgation. La stéganographie a donc été délaissée au profit d'une autre façon de gérer la confidentialité : la «cryptographie». En cryptographie, l'existence du message n'est pas cachée, il peut même être publiquement examiné. Par contre, il n'est pas transmis dans sa forme originale, mais est transcrit de manière à le rendre confus, ambiguë et incompréhensible sauf par son destinataire légitime. Un intercepteur non autorisé, n'est en mesure de déduire aucune donnée utile du message, en analysant la version transportée sous sa forme chiffrée, ou cryptée. L'art de la cryptographie est très ancien. On retrouve ses traces dans presque toutes les civilisations anciennes depuis la scytale des Babyloniens, le carré de Polybe, et jusqu'à la première utilisation confirmée d'un cryptosystème (un système de chiffrement) par Jules César pendant la guerre des Gaules. César écrivait à Ciceron en remplaçant chaque lettre de son message par celle située un rang plus loin dans l'alphabet. Le chiffrement de César a pleinement évolué par la suite, avec des truchements de plus en plus complexes. Ce genre de techniques a parfaitement servi pendant des siècles, et il a fallu attendre le IXe pour que les Arabes parviennent à briser ce mode de chiffrement à travers les travaux d'Al-Kindi, qui inventa ainsi la cryptanalyse. Pendant encore des siècles, la technique d'Al-Kindi fut utilisée pour briser les codes de chiffrement, et ce n'est qu'au XVIe que Vigènaire inventa un mode de chiffrement plus fiable, poly-alphabétique. Il introduisait pour la première fois la notion de code (mot de passe dans la terminologie moderne). Il a fallu trois siècles pour que Charles Babbage réussit à briser ce mode de chiffrement, soit au XIXe.

Pendant la Première et la Deuxième Guerres mondiales, aussi bien que pendant la guerre froide, la cryptographie a joué un rôle décisif. Même si l'objectif était le même, chiffrer un message pour le transmettre d'une manière sécurisée, les méthodes et les techniques utilisées ont largement évolué pour profiter du progrès scientifique et plus précisément celui des mathématiques. Une nouvelle ère est toutefois arrivée avec l'avènement de l'informatique. Les choses prennent une autre tournure pour la cryptographie. L'alphabet manipulé n'est plus celui de la langue courante mais celui de la machine. La puissance du calcul de la machine ajoute une autre dimension de complexité, car le nombre de possibilités est désormais gigantesque. Du premier né d'IBM, Lucifer en 1971, les algorithmes de cryptographie sont passés par les méthodes linéaires puis différentielles, puis par les travaux des Américains Rivest, Shamir et Adelman, pionniers de la crypto-asymétrique qui a abouti à l'algorithme RSA, et ceux de Taher El-Gamal, mathématicien égyptien ayant introduit l'algorithme de cryptographie à clé publique qui fut adopté comme le standard des communications par le NIST en 1996. Aujourd'hui les noms des développeurs de codes ne sont plus retenus, ils sont des milliers de part le monde. Inconnus pour la plupart. Avec l'évolution de l'internet, et la révolution planétaire de la communication et du partage de l'information, la cryptographie devient une science multidisciplinaire qui combine les mathématiques, l'informatique et même l'électronique et la physique dans certaines situations. La nature des problèmes à résoudre a évolué pleinement par rapport à la cryptographie classique, où le problème était seulement de protéger le contenu d'un message secret.

Il s'agit désormais de partager les données en ligne, de garantir l'authenticité de l'identité d'un utilisateur avant de lui accorder l'accès sur une machine, un réseau ou un système informatique quelconque, selon une politique de sécurité qui peut être parfois complexe et dynamique dans le temps. Ainsi, de nouveaux outils cryptographiques sont apparus (fonctions de hachage cryptographique, signature numérique, systèmes de partage de secrets, calcul multiparties…). D'un autre côté, il n'est plus suffisant de considérer la protection contre un intrus qui tente de déchiffrer et comprendre un message, mais aussi contre quelqu'un qui souhaiterait en modifier le contenu. Il s'agit dans ce cas de protéger l'intégrité de l'information cryptée, ou ce que l'on appelle actuellement la cryptographie authentifiée. Préserver l'anonymat d'un utilisateur sur internet pendant une communication sécurisée est également un nouvel enjeu majeur.

Avec l'évolution de l'internet, et la révolution planétaire de la communication et du partage de l'information, la cryptographie devient une science multidisciplinaire qui combine les mathématiques, l'informatique et même l'électronique et la physique dans certaines situations. La nature des problèmes à résoudre a évolué pleinement par rapport à la cryptographie classique, où le problème était seulement de protéger le contenu d'un message secret.

À vrai dire, le nombre de problèmes à résoudre et de techniques cryptographiques à développer ne cesse de croître chaque jour, et aucune limite de cette dynamique ne semble envisageable. Même l'art antique de la stéganographie est ressuscité sous une nouvelle forme nommée tatouage numérique ou watermarking, servant à assurer la sécurité des droits d'auteur (copyright) et à préserver l'originalité des documents multimédias, et l'authentification des enregistrements vidéo et son. L'imagination et le besoin d'évolution chez l'être humain étant sans limite, le développement de la cryptographie ne cesse d'avancer, et les problèmes abordés ne cessent de se complexifier avec la diversification des aspects de l'utilisation des ressources en ligne.

Aujourd'hui, la cryptographie ouvre de nouvelles perspectives à la technologie du Cloud Computing, où le prestataire peut fournir aux usagers en supplément à l'espace de stockage gigantesque et les puissances de calcul colossales, la possibilité d'effectuer des opérations confidentielles, des prévisions budgétaires ou même des expérimentations scientifiques, sans que le prestataire ne soit autorisé à accéder aux contenu. Cette technologie révolutionnera définitivement la face du monde virtuel dans lequel évolue désormais la société planétaire. Dans cette société, où divers aspects se développent en ligne, la guerre est déclarée entre cryptographes (développeurs de codes) et cryptanalystes (briseurs de codes). Il ne s'agit plus d'instrument pour livrer bataille lors de conflits militaires, mais d'un enjeu stratégique dans l'économie, l'industrie, la politique, la vie sociale, et plus encore. Dans les cercles concernés par la sécurité de l'information de part le monde, les bilans de l'année 2014 affirment qu'elle a connu un flot incessant de cyber-menaces et de violations de données, affectant des industriels, des banques, des réseaux sociaux, des gouvernements... Les indicateurs confirment que nous pouvons nous attendre à ce que la taille, la gravité et la complexité des menaces cybernétiques continuent à augmenter. La tendance principale ne sera pas le nombre ou l'insistance des attaques, mais bien leur complexité et leur degré de sophistication. Les enjeux des années à venir tourneront au tour de quelques axes :

La cybercriminalité…

L'internet est un terrain de chasse de plus en plus attrayant pour les criminels, les militants et les terroristes motivés pour se faire de l'argent, se faire remarquer, causer des perturbations ou même renverser les entreprises et les gouvernements à travers des attaques en ligne. Les cybercriminels d'aujourd'hui opèrent en réseau. Ils sont hautement qualifiés et équipés avec des outils très modernes, ils utilisent souvent des outils du XXIe siècle pour s'en prendre aux systèmes en place utilisant des technologies du XXe siècle.

Pendant les dernières cinq années, nous avons vu des cybercriminels qui ont démontré un degré plus élevé de collaboration entre eux et un degré de compétence technique qui ont pris de nombreuses grandes organisations au dépourvu. Désormais, il faut se préparer à l'imprévisible afin d'avoir la capacité de résistance à des manœuvres insoupçonnées à fort impact. La cybercriminalité, ainsi que l'accroissement des causes en ligne (hacktivisme), l'augmentation du coût de la conformité pour faire face à la hausse dans les exigences réglementaires couplées avec les progrès incessants de la technologie dans un contexte de sous-investissement dans les services de sécurité dans la plupart des entreprises, peuvent se combiner pour concourir à une parfaite tempête de menace.

La confidentialité et sa réglementation…

La plupart des gouvernements ont déjà créé, ou conduisent le processus de création, des règlements qui imposent des conditions sur la sauvegarde et l'utilisation des informations personnelles identifiables (Personally Identifiable Information - PII), avec des pénalités pour les entités qui ne les protègent pas suffisamment.

En conséquence, les entités responsables de données privées en ligne ont besoin de les traiter avec une double vigilance : un souci de conformité à la réglementation, et un risque de divulgation. Il s'agira pour ces entités de veiller à réduire les sanctions réglementaires aussi bien que les coûts pouvant être engendrés par les dommages à leur réputation induisant la perte de clients en raison de violations de la confidentialité. La nature disparate de la réglementation dans le monde est susceptible de devenir un fardeau croissant. Nous assistons de par le monde à un affermissement des plans de la réglementation autour de la collecte, du stockage et de l'utilisation des informations ainsi que des peines sévères pour la perte de données et notification des violations. Il faut s'attendre à ce que cette tendance se poursuive et se développe en imposant une surcharge en gestion de la réglementation au-delà de la fonction de sécurité et nécessairement comprenant les aspects juridiques des droits de l'Homme. Les régulateurs et les gouvernements tentent de s'impliquer en plaçant un fardeau plus lourd sur les entités et organismes dépositaires de données privées en ligne. Ils ont besoin d'avoir des ressources en place pour en répondre et ils ont besoin d'être conscient des évolutions qui s'opèrent.

Les indicateurs confirment que nous pouvons nous attendre à ce que la taille, la gravité et la complexité des menaces cybernétiques continuent à augmenter. La tendance principale ne sera pas le nombre ou l'insistance des attaques, mais bien leur complexité et leur degré de sophistication.

L'engagement des usagers…

Au cours des dernières décennies, les entreprises ont dépensé des millions, voire des milliards, de dollars sur les activités de sensibilisation du public à la sécurité de l'information. La logique derrière cette approche est de prendre leur plus grand actif — les usagers — et de changer leurs comportements en ligne, réduisant ainsi le risque en leur fournissant des connaissances de leurs responsabilités et ce qu'ils doivent faire pour préserver au mieux leurs données privées. Cette approche ne s'applique par contre pas aux usagers particuliers, notamment les employés d'entreprise. En effet, les entreprises, pour préserver leur intégrité numérique ont besoin d'adopter des comportements positifs en matière de sécurité. Leurs employés doivent être transformés en première ligne de défense dans le système de sécurité numérique. Les entités faisant appel aux échanges et stockage de données numériques ont besoin de passer de la promotion et de la sensibilisation à la création de solutions et l'intégration, de manière positive, des comportements de sécurité de l'information qui influent sur le risque. Les risques liés au facteur humain sont réels parce que les comportements des usagers restent une «wild card» (carte sauvage), difficile à manager. Au lieu de simplement promouvoir auprès des usagers la conscience de leurs responsabilités par rapport à la sécurité de l'information et comment ils doivent réagir, les entreprises doivent intégrer les comportements positifs de sécurité de l'information qui se traduisent par des pratiques rigoureuses dans la manipulation des données numériques.

En Algérie, l'entrée au monde du tout numérique s'opère tardivement. Au-delà des efforts à fournir pour garantir l'accès à la connexion pour l'ensemble des citoyens, il y a un effort encore plus important à déployer pour préparer le passage à la vie sur la Toile de la société algérienne. Disposer d'un terminal connecté n'est que le début de l'épreuve ; il sera désormais impératif de développer des services et des applications qui permettent aux usagers du Net de profiter de cette connexion dans le sens de la société numérique moderne.

Plus encore, il sera question de préparer la réglementation, en l'adaptant aux exigences du tout numérique, afin de protéger les citoyens des aléas des échanges des données privées en lignes. Toute une culture de l'usage du numérique doit être entretenue, où la promotion des bonnes pratiques et la sensibilisation à la vigilance joueront un rôle important. Développeurs d'applications, développeurs de systèmes, de codes, cryptographes, cryptanalystes… autant de métiers à promouvoir, qui ne nécessitent rien de plus que de la matière grise fraîche qu'il faudra drainer vers les mathématiques, l'informatique, l'électronique… rien dont notre jeune génération ne puisse garantir.

I. H. F.