Colloque sur la sécurité

Un demi-siècle après le Général Guisan,

Quelle sécurité pour la Suisse?

vendredi 16 avril 2010 à Pully

Table ronde « Sécurité et Technologie »

Cybersécurité contre cyberattaques : mission impossible ?

INTERVENTION DE MADAME LA PROFESSEURE SOLANGE GHERNAOUTI-HELIE

Rebondissons sur le titre de cette table ronde « Sécurité et Technologie » et émettons quelques réflexions selon les deux aspects, les deux axes qu'il soulève. En effet, « Sécurité et Technologie » peut être comprise comme :

- d'une part, la technologie a besoin d'être sécurisée, sous entendu, elle génère de l'insécurité ;
- d'autre part, la technologie est au service de la sécurité

Tout d'abord précisons que le terme générique Technologie correspond aux technologies de l'information et des communications. Il s'agit des technologies du numérique au sens large qui comprend toute sorte de moyens et outils intégrant une composante électronique (puce électronique, équipement multimédia, téléphonie, internet, etc.).

Nous sommes depuis quelques années déjà, entré dans la société de l'information avec une informatique de plus en plus omniprésente et invisible, communicante et mobile, avec une communication extensive qui peut se résumer avec le slogan « depuis n'importe où, avec n'importe qu'elle entité, tout le temps ». Désormais toute activité est médiée par des équipements informatiques et des réseaux et la dimension planétaire des échanges n'est plus à démontrer.

Le postulat que les technologies génèrent de l'insécurité repose sur plusieurs facteurs notamment :

Leur adoption rapide, leur évolution, leur complexité, leur maitrise difficile, la dématérialisation de l'information, comme la globalisation de la communication, l'interdépendance des infrastructures critiques en sont quelques uns.

A ceux –ci s'ajoute le fait qu'elles sont devenues le support des nouvelles valeurs de notre société : celui de l'information. Ainsi, les technologies et les informations sont des valeurs et des outils et moyens de contrôle et de pouvoir économique et politique

Par conséquent, elles sont vues par certains acteurs, comme étant des sources d'enrichissement et des moyens de déstabilisation, de pression ou de contrôle.

Elles font donc l'objet de convoitise ou de menaces d'appropriation illégale, de destruction, ou d'altération par exemple. Elles constituent alors des cibles de la malveillance (nouveaux outils – nouveaux délits) et des moyens de réaliser de vieux crimes avec de nouveaux outils. De plus, elles sont porteuses de vulnérabilité et de failles, qui génèrent des menaces, dont l'origine peut être criminelle ou non.

Il existe de nos jours, une forte demande pour avoir de plus en plus de sécurité, tout en réfutant la réalité de l'incertitude, du risque et le recul des libertés. L'exigence de sécurité maximale est également omniprésente. Si la pensée scientifique et philosophique des siècles passés a pu laissé croire à la possibilité d'atteindre une sécurité absolue, à l'effacement de l'incertitude et à la maitrise absolue du risque ; Aujourd'hui les systèmes informatiques et leur complexité inhérente, ont permis de réinventer la peur et ce n'est plus seulement la nature qui engendre les risques ou des catastrophes majeures, c'est la science et la technique !

Dès lors, quelles réponses sécuritaires donner aux cyberattaques et à la cybercriminalité au sens large ?

Difficile de répondre à la question de la cybersécurité sans passer par une réflexion approfondie sur les origines des violences actuelles perpétrées à l'encontre des personnes, des organisations et des états.

Au 21ème siècle, la cybercriminalité constitue un prolongement de la criminalité classique, et s'inscrit dans un contexte général de crise et de guerre économiques, de guerre de l'information, par l'information, pour l'information.

Les technologies de l'Internet sont indifféremment au service des Individus, des Organisations, des Etats, et qui selon les circonstances, peuvent être bienveillants et / ou malveillants et toujours selon les circonstances, agir de manières licites ou illicites, mais ce n'est pas l'objet de ce débat.

Ainsi, Internet autorise une proximité criminelle entre tous ces acteurs et leur offre à la fois des opportunités criminelles et des moyens performants pour réaliser des délits et des crimes.

Par ailleurs, pour ce qui concerne la technologie au service de la sécurité, sans vouloir évoquer toutes les technologies existantes ou à venir comme la vidéosurveillance, la cryptographie ou la biométrie par exemple, retenons seulement que quelle que soit la technologie considérée, la technologie à elle seule ne peut répondre à des problèmes de société.

En effet rappelons que :

- La technologie ne peut pas être un remède miracle à l'injustice sociale ;
- La technologie ne peut pallier un défaut de gouvernance, de vision, de culture, d'avenir de notre société ;
- La technologie ne peut se substituer à un défaut d'analyse et de gestion efficace des risques, ni remplacer la prise de responsabilité de certains acteurs en matière de développement durable de la société de l'information.

Quelle que soit la technologie aussi novatrice, aussi performante soit-elle, est toujours faillible et porteuse de vulnérabilités. Elle est donc plus ou moins robuste, et elle doit être elle aussi sécurisée (Quelle sécurité pour la sécurité ?).

La technologie sera toujours l'objet de détournement et de cassage, elle aura toujours des effets de bords , le plus souvent elle déplacera le problème de la sécurité sans pour autant le résoudre complètement mais en faisant généralement porter la responsabilité de sécurité sur d'autres entités.

Remarquons également, que les commanditaires des technologies de sécurité seront toujours dépendants de leurs fournisseurs. Et la vraie question devient alors « Qui contrôle la sécurité ? Qui garde le gardien ? »

Ainsi la dépendance à la technologie, à des infrastructures comme Internet, à des fournisseurs de services comme Google par exemple, que nous ne maîtrisons pas, se double de la dépendance envers les fournisseurs de sécurité. La dépendance à des acteurs incontournables qui sont des supra structures hyperpuissantes, nous invite à réfléchir au problème de la confiance dans des acteurs les plus forts, qui maîtrisent les moyens de communication (infrastructures de routage, de gestion des noms et des adresses de l'Internet (routeurs, DNS)) ; les données, les identités, les profils des utilisateurs, leurs goûts, leurs habitudes, … les flux de communication (qui communique avec qui), …du fait du mode de fonctionnement du numérique, des traces laissées, des informations livrées par l'utilisateur, de celles collectées à sont insu ou soutirées par escroquerie, leurre ou par malveillance (les cas de vol ou de perte de données sont fréquents) …

Attention donc à la prolifération de mesures juridiques ou technologiques, à l'escalade de mesures favorisée par un contexte de peur généralisée, ces mesures possèdent un coût non négligeable pour notre société et l'impactent fortement, sans pour répondre efficacement au besoin de sécurité et de protection.

La sécurité doit contribuer à contrecarrer les accidents, les erreurs, les malveillances. Elle doit être un dispositif cohérent, efficace, efficient et qui tient compte de manière systémique, interdisciplinaire et intégrée de toutes ses dimensions politique, organisationnelle, technique, juridique et humaine.

Elle nécessite une organisation particulière, des moyens spécifiques et des compétences réelles pour répondre à une vision stratégique et politique déterminée. Celle ci doit non seulement être réalisable à l'échelon national mais compatible au niveau mondial !

Ainsi donc « Cybersécurité contre cyberattaques : mission impossible ? »

Non, pas forcément mais mission difficile certainement.

Car cela soulève des questions fondamentales et complexes relatives :

- à la collaboration et coopération internationale : harmonisation des cadres légaux, disparition de paradis digitaux, coopération entre des instances de justice et de police, etc.
- aux partenariats entre les acteurs publics et privés ;
- à la disponibilité et à la maîtrise des mesures proactives et réactives de sécurité qui permettent une protection efficace des valeurs matérielles, immatérielles et des personnes ;
- à la formation de l'ensemble des acteurs impliqués (population, dirigeants, professionnels de justice, police, développeurs et fournisseurs de services, intermédiaires techniques, etc.).

Diriger la sécurité c'est prévoir, anticiper, déceler les signaux avant-coureurs et réagir si les stratégies d'évitement ne sont pas efficaces. Dans ce domaine nous nous devons d'être proactifs et pas seulement adopter dans l'urgence, des dispositifs légaux ou technologiques, à la manière de rustines suite à une crevaison ou à l'application de remèdes placébos pour répondre à des menaces mal identifiées ou encore pour répondre à des pressions politiques ou économiques ou à des exigences du marché. C'est développer une culture de la sécurité qui satisfasse avec cohérence, nos besoins de société en protégeant nos valeurs, sans syndrome sécuritaire, ni aveuglement laxiste.

Solange Ghernaouti-Hélie, Docteur en Informatique de l'université Paris VI, première femme professeure à l'école des HEC de l'Université de Lausanne est l'auteure de plus d'une vingtaine d'ouvrages sur les télécommunications et la sécurité, dont certains sont traduits en plusieurs langues. Expert international dans le domaine de la sécurité et de la criminalité du numérique, la professeure Ghernaouti-Hélie est présidente de la commission sociale et présidente de la commission égalité des chances de l'université de Lausanne et également professeure invitée au département de sociologie de l'Université de Genève.

Ouvrage pour en savoir plus : « La cybercriminalité : le visible et l'invisible »

Collection le Savoir Suisse – PPUR 2009