Diner-débat du JEUDI 23 JANVIER 2020

LE NUMERIQUE ET LA CYBER-DEFENSE CITOYENNE

***Isabelle RAIMOND-PAVERO**, Sénatrice d'Indre-et-Loire, Commission des Affaires Etrangères, de la Défense et des Forces Armées, Auditrice CHEID, Conseillère Départementale du Canton de Chinon*

***Franck PAVERO**, officier cyber-défense*

Aujourd'hui, les politiques doivent être de plus en plus attentifs aux enjeux de notre société si numérisée et interconnectée avec le choix d'un Protocole Internet (IP) sans sécurité. La cyber sécurité représente un défi majeur urgent pour la protection de la vie sociale, industrielle et privée. Internet, surnommé « La Toile » s'avère un outil simple, rapide, puissant et étendu mondialement, avec des atouts mais aussi des inconvénients. N'importe quelle donnée se transmet sans contrôle et très rapidement d'un bout à l'autre du globe. Au fur et à mesure des années, il y a eu un changement d'échelle de transmission, avec de nos jours la possibilité, par exemple, de déplacer des capitaux d'un pays à l'autre en quelques clics et quelques secondes. C'est une révolution culturelle, sociale, philosophique, toujours en cours, qui s'est immiscée dans chaque strate de l'activité humaine. De plus, une captation voire une manipulation des données, des idées, des conceptions globales ou spécifiques ont été constatées, imposant de faire plus attention à la sécurité numérique. Sans une prise de conscience politique majeure, l'impact économique, social et humain peut s'avérer conséquent.

Internet est un outil de développement formidable, mais aussi une menace, passée longtemps inaperçue. La confiance aveugle que les chefs d'entreprise, décideurs et citoyens y mettent dans leur quotidien est une porte ouverte à tous les dangers d'intrusion, vol, manipulation, voire sabotage (virus Stunex dans les centrales nucléaires en Iran pourtant non-connectées, arrêt électrique en Ukraine, paralysie de l'administration en Estonie …). Jusqu'à présent, la réglementation internationale était quasi inexistante et notre législation européenne et nationale est très récente (règlement n° 2016/679, dit règlement général sur la protection des données de l'Union européenne RGPD).

De fait, en raison de la fragilité de nos choix, inconscients des risques, à toujours choir la technologie la moins couteuse, mais faible en sécurité et aussi notre inhibition culturelle qui a laissé des pays d'Asie fabriquer tous nos appareils électroniques et les Anglo-américains imposer tous leurs outils, il en résulte que depuis longtemps la souveraineté du pays est menacée par les activités criminelles et étatiques.

Nous devons donc trouver les bonnes formes de régulation, les bonnes formes d'espace collectif, parce que les faiblesses et les failles du système ne sont à ce jour contenues que par les moyens considérables déployés par les services de l'Etat.

Outre la protection législative et réglementaire à mettre en œuvre, à laquelle les décideurs publics et les élus travaillent depuis peu, il faut aussi agir ensemble citoyennement pour échanger sur les bonnes pratiques à adopter, pour devenir cyber-irréprochable.

De nos jours, la prise de conscience progresse, mais les attaques se développent aussi et nos vulnérabilités restent trop importantes. Le problème n'est plus de savoir si on va être piraté mais quand ?

Le gouvernement essaie de régler ce problème en créant des infrastructures nationales avec l'armée et les forces de sécurité intérieure et extérieure, mais aussi avec l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), un service français créé par décret en juillet 2009, véritable pôle d'excellence.

La désinformation, avec la découverte des « Fake news », et le buzz se révèlent des problèmes majeurs pour les entreprises, les gouvernants et les citoyens. Dans de nombreux conflits, les Etats coupent les réseaux sociaux pour lutter contre des émeutes.

L'Intelligence Artificielle (IA), outil de performance extrêmement important pour notre humanité, peut aussi devenir un danger et nous rendre vulnérables, si elle n'est pas encadrée par un code d'éthique. Cependant, l'évolution des nouvelles technologies est toujours plus rapide que celle de la mise en œuvre de code législatif et réglementaire. Les politiques et les parlementaires se retrouvent dans la même situation d'urgence. Nous devons ensemble concevoir et échanger les bonnes méthodes et les bonnes pratiques.

Grâce à l'action la sénatrice Isabelle Raimond-Pavero, notamment dans les missions d'élue locale et sa position au sein de la commission de la défense du Sénat, les politiques locaux et nationaux sont de plus en plus sensibilisés mais des formations restent à mettre en place. D'importantes menaces ont encore des réponses insuffisantes.

Les objets interconnectés sont aussi un énorme danger. Chacun à une montre, un smartphone et bientôt encore plus d'appareils interconnectés avec l'Internet (voiture, compteur, télévision, balance, réfrigérateur, alarme, chauffage, lave-linge, lave-vaisselle … 50 objets/personnes prévus en 2030), avec une confusion entre les domaines personnels et professionnels offrant encore plus de failles aux malveillants.

En premier lieu, la sécurité reste principalement une obligation étatique régalienne. Comme le rappel Franck PAVERO, officier cyber-défense en activité dans ce domaine depuis des années, pour les systèmes d'informations et de programmations militaires, grâce aux derniers Livre blanc sur la défense et la sécurité nationale, les différents défis sont pris en compte et sont prévus de 2019 jusqu'en 2025 sous réserve de budget attribué. Cependant, la France n'a pas que des outils défensifs, lors du précédent Livre Blanc, l'ancien ministre de la défense, Jean-Yves Le Drian, avait même fait état des capacités d'actions offensives françaises contre des cyber-hackers souvent moins criminels que mercenaires étatiques.

Néanmoins, ces dispositifs étatiques sont nécessaires mais pas suffisants. Il convient de donner aux citoyens une cyberculture. Tous les utilisateurs doivent être informés à tous les niveaux des risques qu'ils

prennent sur internet sans le savoir. La cyber-sécurité constitue un défi de taille auquel nous sommes tous confrontés, que l'on travaille dans le domaine des services, de l'industrie ou plus encore dans des administrations ou des entreprises d'importance vitale ou leurs sous-traitants. Elle est beaucoup mieux prise en compte de nos jours, avant elle était presque inexistante. Cependant les décideurs comme les utilisateurs manquent de connaissance au quotidien et d'hygiène informatique pour éviter les virus, afin de respecter l'intégrité et la confidentialité des informations tant personnelles que professionnelles.

Une ingénierie sociale peut être mise en place, en cas de situation extrême avec la gestion de crise. Certes, le système industriel risque de tomber, mais sans pouvoir prévoir ni quand, ni comment cela arrivera. Les cyber-risques peuvent impacter le business, ainsi que les entreprises. Une forme de résilience est à prévoir en cas de paralysie des systèmes dont dépendent nos sociétés.

Certains combats que les services de sécurité étatiques tant civils que militaires mènent quotidiennement, sont de moins en moins des combats physiques et matériels, mais relèvent de la guerre électronique au cyber-guerrier d'une cyber-armée développée à ces fins. Les risques subsistent malgré les solutions mises en place et doivent constamment être réévaluées et nos boucliers virtuels comme nos guerriers doivent être régulièrement mieux armés.

Le capital humain en la matière reste faible. Les cyber-combattants civils et militaires sont avant tout des techniciens et ingénieurs de haut niveau en la matière. Le manque de personnel compétent sur le marché amène le recrutement occasionnel de hackers blancs et la pratique du « Bug Bounty ». Ainsi, une entreprise ou même l'armée offre une prime à des "hackers éthiques", souvent membres de la Réserve de Cyber défense, pour attaquer des systèmes en test afin de déceler les « bugs », erreurs de conception et autres failles présents dans les systèmes informatiques et électroniques.

Afin d'augmenter nos capacités en connaissance et en ressources humaines, un cyber-campus dédié aux enjeux du numérique visant à renforcer les synergies entre acteurs publics, privés et académiques.

Il reste à développer la cyberculture citoyenne. Selon IPSOS, les enfants français âgés de 1 à 6 ans passaient en moyenne 4h37 sur internet par semaine en 2017, ce chiffre s'élève à 6h10 pour les 7-12 ans, et va jusqu'à 15h11 pour les 13-19 ans. Comme, il est nécessaire d'apprendre à un enfant les règles d'hygiène en se lavant les mains avant de manger, et les règles de sécurité sur les passages au feu rouge, les éducateurs, parents et enseignants ont pour mission aussi d'expliquer les règles d'hygiène informatique qu'ils doivent souvent apprendre eux-mêmes d'abord.

Les actions des élus, des forces de sécurité mais aussi des citoyens doivent converger vers une-cyber culture générale et protectrice de nos institutions, de notre industrie et de notre modèle démocratique.