FIC 2017 : les démocraties face à leurs fragilités numériques

C'est un nouveau record d'affluence que devrait battre le FIC (Forum international de la cybersécurité) qui se tient les 24 et 25 janvier à Lille. Les organisateurs annoncent quelque 7 000 participants à une manifestation de plus en plus tournée vers le business et de moins en moins centrée sur les activités régaliennes en matière de cybersécurité, comme en témoigne l'espace exposition où l'industrie est présente en masse.

Le FIC n'en demeure pas moins un passage obligé pour les ministres de l'Intérieur et de la Défense, qui y trouvent l'occasion de dresser le bilan de leurs actions dans le cyberespace. Le ministre de l'Intérieur, Bruno Le Roux (ci-dessus), a ainsi annoncé la création d'une délégation ministérielle à la lutte contre les cybermenaces. En réalité, il s'agit d'une extension des fonctions actuelles de Thierry Delville, le délégué ministériel aux industries de sécurité. « *Le périmètre d'intervention de la nouvelle délégation est large : la lutte contre la cybercriminalité, la cyberdéfense économique, la cybersécurité, le développement et la protection de la capacité industrielle et technologique du pays en matière de sécurité et de lutte contre les cybermenaces* », explique le ministre, qui compte sur cette délégation pour définir la stratégie du ministère tant en termes de prévention des cybermenaces que de répression.

« La complexité de la menace augmente »

Pour ce faire, le ministère affirme se baser sur un état des lieux des cybermenaces en permanence chiffré et actualisé. « *Car on ne peut pas lutter contre un ennemi que l'on ne connaît pas, dans un contexte où les systèmes d'information sont régulièrement l'objet d'attaques venant d'organisations criminelles, voire d'États étrangers, lesquels se montrent toujours plus inventifs*, ajoute Bruno Le Roux. *Plus que le volume, c'est une augmentation du niveau de complexité de la menace qui est constatée* ». Pour répondre à ce défi, le ministre explique que son administration tient compte des enjeux sécuritaires dès la conception des projets informatiques. Un renforcement qui n'a toutefois pas totalement convaincu l'Anssi (Agence nationale de la sécurité des systèmes d'information) et la Dinsic (la DSI de l'Etat), qui ont récemment critiqué le niveau de sécurité du fichier TES (Titres électroniques sécurisés), renfermant actuellement des données biométriques pour les passeports et appelé à s'étendre aux cartes d'identité nationales.

Le hacking pour déstabiliser l'opinion publique

Pour le reste, fin de mandature oblige, l'action de Bruno Le Roux semble s'inscrire dans les pas de son prédécesseur, l'actuel Premier ministre Bernard Cazeneuve. Le ministre met ainsi en avant la collaboration avec les grandes plates-formes d'Internet. Au bilan de 2016, selon l'Intérieur, 834 demandes de blocage, 1 929 demandes de déréférencement et 3 129 demandes de retrait transmises aux opérateurs d'Internet par la police judiciaire. Autre axe de la politique du gouvernement : la lutte contre la propagande djihadiste, avec la loi de juin dernier venue renforcer les moyens mis à disposition des enquêteurs. Notamment avec la possibilité d'enquêter sur Internet sous pseudonyme.

Mais, comme l'a souligné en creux le commissaire européen à la sécurité Julian King, les Etats doivent désormais faire face à de nouvelles menaces, en particulier des « *campagnes hybrides* » visant à déstabiliser l'opinion publique. « *Nous ne pouvons pas laisser ces attaques, émanant y compris de gouvernements étrangers, ébranler nos démocraties* », martèle le Commissaire, qui s'empresse toutefois de rappeler que ce sont les Etats qui sont en première ligne face à ces nouvelles menaces. Même si la future directive NIS devrait favoriser la préparation des Etats membres aux crises cyber en les obligeant à se doter d'un centre de réponse aux incidents et d'une autorité compétente, comme l'est l'Anssi dans l'Hexagone.

Toutefois, comme l'a montré les mésaventures du parti démocrate aux Etats-Unis, les démocraties restent peu préparées face à des attaques protéiformes visant à saper leurs fondements démocratiques. En France, l'Anssi a bien organisé une séance de sensibilisation des partis politiques, en vue de la prochaine présidentielle, mais l'agence dirigée par Guillaume Poupard a aussitôt précisé que ces organisations n'avaient aucune obligation d'appliquer les mesures de précaution qu'elle préconise et qu'elles restaient avant tout des PME aux budgets limités. Une façon de dire que l'Agence ne se fait guère d'illusions en cas d'attaques menées par des acteurs étatiques, disposant de compétences pointues, de moyens importants et de temps. Les interrogations autour de la participation à la primaire socialiste – qui feraient suite à une erreur humaine selon les organisateurs – prouvent, une fois encore, le caractère délétère des doutes entourant la sincérité d'un scrutin.

Chiffrement : le « *désarroi des politiques* » selon Klaba

L'autre limite de l'action du gouvernement tient, elle, toute entière dans une autre partie du discours du ministre de l'Intérieur, un passage relatif au chiffrement. « Nous devons en garantir la fiabilité en respectant l'équilibre entre le respect de la vie privée et les besoins des services d'enquête », estime le ministre. Ce qui revient, selon l'avis de quasiment tous les experts du sujet, à démontrer la quadrature du cercle. Selon l'Anssi, il est ainsi « *techniquement impossible d'assurer qu'un dispositif visant à affaiblir des mécanismes cryptographiques ne bénéficie qu'aux seules personnes autorisées* ».

Rappelons que Bernard Cazeneuve et son homologue allemand, Thomas de Maizière, ont lancé en août 2016 une initiative visant, précisément, à trouver des solutions techniques garantissant la sécurité des échanges tout en permettant leur déchiffrement par les autorités, afin de lutter contre des terroristes accusés d'avoir massivement recours aux messageries chiffrées de bout en bout comme Telegram. On attend toujours les premières pistes de réflexion concrètes sur ce terrain… Interrogé par *Silicon.fr,* Octave Klaba, le fondateur et directeur technique d'OVH, estime que cette question illustre le désarroi des politiques face au monde très décentralisé que fait naître Internet : « *il s'agit davantage de postures que d'actions concrètes. Une façon de dire aux citoyens : j'ai fait ce que j'ai pu.* »

A lire aussi :

Hacking des élections : les partis politiques français sont-ils prêts ?

Hacker éthique : la législation française enfin claire ?