Piratage

Cyber-menaces sur la présidentielle

Les autorités craignent que des hackers cherchent, comme aux Etats-Unis, à influer sur le cours de la campagne. L'Allemagne s'y prépare. Les politiques français semblent sous-estimer les risques

Les faits — Aux Etats-Unis, la CIA et Donald Trump s'affrontent sur l'implication de la Russie dans les piratages ayant pesé sur l'élection, le président élu contestant les conclusions de l'agence de renseignement. La France et l'Allemagne, où auront lieu deux scrutins d'importance en 2017, ont exprimé des craintes similaires. Dans ce contexte de menace, le ministre de la Défense Jean-Yves Le Drian a annoncé lundi la création d'un commandement cyber, le Cybercom. Il sera chargé, à partir de janvier 2017, de mener des opérations militaires dans l'espace numérique.

Jamais la cybermenace n'a été aussi élevée. A quelques mois d'un scrutin qui s'annonce imprévisible, les autorités françaises s'inquiètent des risques qui pèsent sur le bon déroulement de l'élection présidentielle de 2017.

Un scénario qui pourrait ressembler à ce qui se passe aux Etats-Unis, où la période de transition avant l'investiture de Donald Trump est parasitée par la question d'un éventuel piratage russe de l'élection, dénoncé par la CIA mais réfuté par le président élu. Outre-Rhin, le patron des renseignements s'est fait l'écho à plusieurs reprises de menaces similaires pour les élections allemandes qui auront lieu à l'automne 2017.

En France, les déboires de l'équipe Clinton n'ont pas non plus manqué d'alerter. Le 26 octobre, le Secrétariat général de la défense et de la sécurité nationale (SGDSN) a ainsi organisé une réunion de sensibilisation en direction des acteurs de la vie politique. Sur la base d'une analyse de la situation américaine rendue par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), le SGDSN a décidé de réunir les responsables du numérique des partis politiques représentés au Parlement, ainsi que ceux des groupes parlementaires, notamment en raison de l'imminence des primaires. C'est la première fois qu'une réunion de ce type était organisée.

« Il fallait se poser la question de savoir si ce qui se produisait aux Etats-Unis pouvait également se produire en France. Etant donné le niveau de la menace, il fallait de toute manière prévenir les partis politiques qu'une page s'était tournée. Nous voulions aussi savoir s'ils étaient complètement à la rue sur ces sujets », explique-t-on dans les milieux gouvernementaux. Le SGDSN a indiqué aux participants la marche à suivre et les personnes à contacter afin de faire examiner (et éventuellement sécuriser) leurs systèmes informatiques.

Menace sous-estimée. « Il y avait ceux, en minorité, qui n'avaient pas d'idée précise de la menace et ceux qui en étaient bien conscients, raconte une source gouvernementale. Ces derniers ont d'ailleurs dit qu'ils essayaient depuis des années d'alerter leur hiérarchie. On leur a

permis de retourner voir leurs patrons avec plus d'arguments ». Une prise de conscience trop tardive, à moins de cinq mois du premier tour de l'élection présidentielle ?

« On est dans une sous-estimation de la menace », estime Fabrice Epelboin, enseignant à Sciences Po et cofondateur de Yogosha, une entreprise dédiée à la sécurité informatique. « Comme les Etats-Unis, la France est dans le viseur de la Russie en raison de son soutien à la politique européenne de sanctions et en paiera les mêmes conséquences », poursuit-il. Faut-il, par exemple, s'attendre à la publication par WikiLeaks de documents personnels subtilisés à certains candidats ?

C'est que François Hollande est un ennemi de l'organisation. Enfermé depuis des années dans l'ambassade équatorienne de Londres, Julian Assange a récemment qualifié le Président d'« escroquerie comme de nombreux politiciens », dans une interview réalisée en mai par iTélé. L'année dernière, l'Australien lui avait demandé l'asile politique dans une lettre ouverte publiée dans la presse à laquelle l'Elysée avait très rapidement opposé une fin de non-recevoir.

Le spectre des attaquants potentiels est toutefois plus large. Individus, groupes d'activistes politiques étrangers ou nationaux, voire des puissances étrangères… « Il y a dans le monde des gens qui s'intéressent aux campagnes électorales, ce n'est pas un fantasme et nous avons affaire à des personnes qui ne sont pas des amateurs mais réalisent des attaques haut de gamme », alerte-t-on du côté du gouvernement. Un constat inquiétant, d'autant plus que les partis politiques semblent dépassés.

Vol et désinformation. « Pendant des années, le Parti socialiste a laissé fuiter des données sur son site où la liste des primo-adhérents était très facile à récupérer », rappelle Fabrice Epelboin. Fin octobre, l'épisode a valu au PS un avertissement public de la Commission nationale informatiques et libertés (Cnil). L'exemple ne risque pas de venir d'en haut puisque, comme le rapportent les auteurs du livre *Un Président ne devrait pas dire ça…*, François Hollande lui-même a longtemps utilisé un téléphone non sécurisé pour passer des appels à des chefs d'Etat étrangers.

Pour 2017, les craintes sont de deux natures. Le vol de données d'abord : liste d'adhérents, de prospects, comptabilité, agendas, correspondance… autant d'éléments sensibles dont l'accès est souvent mal protégé. Les campagnes de dénigrement ensuite. Si les médias pro-russes concentrent aujourd'hui l'attention, les Etats-Unis avaient mis sur pied pendant la guerre froide tout un éventail de médias censés « réinformer » les populations du bloc soviétique.

« La question est surtout de savoir quelle information est susceptible d'avoir un impact sur l'élection », souligne Nicolas Arpagian, directeur scientifique à l'Institut national des hautes études de la sécurité et de la justice (INHESJ). Le spécialiste de la cybersécurité remarque, à juste titre, que les accusations de Ziad Takieddine contre Nicolas Sarkozy en pleine campagne de la primaire ne l'ont pas plus pénalisé que cela…