

Jean-Yves
Le Drian,
ministre de
la Défense,
dans un
centre de
contrôle de
l'armée de
l'air, à Paris,
le 15 janvier



CYBERGUERRE

LES PROGRAMMES SECRETS DE LA FRANCE

En l'absence de moyens de défense efficaces, le pays est menacé de chaos en cas d'attaque généralisée contre ses réseaux. Mais les services secrets préparent déjà la contre-offensive

PAR BORIS MANENTI

Un petit « 1 » s'affiche sur la page Facebook d'un conseiller de l'Elysée: « Vous avez reçu un nouveau message. » Le collaborateur du président vient de réceptionner un courrier de l'un de ses « amis ». Ou du moins le croit-il. Le texte l'invite à cliquer sur un lien renvoyant, apparemment, au site interne de la présidence. Il livre son identifiant et son mot de passe. A aucun moment il ne s'est aperçu qu'il s'agit d'un faux site. Le précieux sésame est discrètement récupéré par un hacker qui s'introduit dans le système et infecte plusieurs ordinateurs du Palais, afin d'exfiltrer des documents confidentiels.

Révéle par « le Télégramme de Brest », l'audacieux hold-up s'est déroulé dans la foulée de l'élection présidentielle. Précisément entre le 6 et le 15 mai 2012. Depuis, l'Elysée vit dans la peur d'une nouvelle intrusion. Ses 700 ordinateurs ont été entièrement nettoyés et sa sécurité informatique, revue à la hausse. Parmi les principaux suspects figure l'Agence nationale de Sécurité, la NSA, les grandes oreilles de Washington, selon le journal « le Monde ». Les Américains, quant à eux, accusent le Mossad israélien.

La France a pris brutalement conscience de la réalité de la menace contre ses intérêts numériques, en par-

ticulier contre ses infrastructures dites « vitales ». Ministères, réseaux télécoms, de distribution d'électricité, d'approvisionnement en eau, signalisations routière et ferroviaire, centrales nucléaires, hôpitaux... Tout peut être piraté. La faute à l'informatisation galopante de la société. Des boucliers sont en mis en place, mais trop tardivement. « A ce jour, nos parades me paraissent très insuffisantes », critique, dans « la Tribune », le directeur du renseignement militaire (DRM), le général Didier Bolelli. Un constat que partage Eric Filiol, directeur du laboratoire de cryptologie de l'école d'ingénieurs Esiea: « Le jour où nous serons la cible



d'une attaque généralisée contre plusieurs de nos réseaux vitaux, on ne résistera pas, ce sera le chaos. »

Pour l'heure, les attaques se cantonnent au cyberespionnage, mais les risques d'un cyberterrorisme et d'un cybersabotage sont de plus en plus grands. *« Ce qui est en jeu, c'est la capacité de prise de contrôle à distance ou de destruction d'infrastructures vitales, a confirmé le ministre de la Défense, Jean-Yves Le Drian. Des attaques ont pour la première fois explicitement visé la neutralisation de systèmes critiques, même non connectés à internet. »* La cyberdéfense française a commencé à s'organiser en 2008, lors de la publication du livre blanc sur la défense. L'Agence nationale de Sécurité des Systèmes d'Information (Anssi) a été créée pour protéger l'informatique d'Etat, et un contre-amiral a été nommé pour diriger cette ligne Maginot virtuelle. Une amorce de prise de conscience encore loin d'une défense efficace. Début 2011, plus de 150 ordinateurs du ministère de l'Economie ont été piratés et des documents confidentiels concernant le G20 dérobés. Quelques mois plus tard, le groupe nucléaire Areva a découvert une opération de cyberespionnage massive qui durait depuis deux ans et lui a fait perdre plusieurs contrats.

François Hollande élu, le ministère de la Défense a érigé la défense numérique au rang de priorité nationale : *« Le cyberspace est devenu un champ de confrontation à part entière, une attaque informatique de grande envergure peut désormais constituer un véritable acte de guerre »,* affirme la loi de programmation militaire. D'ici à 2020, le texte prévoit de doter l'armée *« d'une doctrine nationale de réponse aux agressions informatiques majeures »* mais aussi *« de capacités défensives et offensives pour préparer ou accompagner les opérations militaires »*. Concrètement, si un Etat ou un groupuscule venait à attaquer la France à coup de virus, les militaires seraient prêts à répliquer. Et, lors d'un conflit, les opérations sur le terrain seraient appuyées par des frappes numériques.

L'armée assume désormais dans sa défense une part d'offensif, dite « de lutte informatique offensive » (ou LIO). *« Nous allons mettre en œuvre une capacité informatique offensive, associée à la capacité de renseignement »,*

fait valoir Jean-Yves Le Drian. Ce dispositif comportera *« différents stades, qui sont plus ou moins réversibles, plus ou moins discrets, mais toujours proportionnés à l'ampleur et à la gravité de la situation »*. Toutefois la LIO existe depuis plusieurs années. Alors même qu'aucune doctrine n'a été élaborée, un document de 2010 des forces armées que s'est procuré « le Nouvel Observateur » affirme que *« les forces armées développent leurs capacités de protection et de contre-mesures actives pour neutraliser les systèmes adverses »*. Plus loin y sont détaillés des moyens pour *« supprimer une menace par des missions offensives ou défensives [...] Ces capacités doivent permettre des effets de neutralisation rapidement décisifs, voire brutaux, pour déstabiliser l'adversaire et obtenir la victoire »*. Au titre d'exemple d'action « brutale », on peut citer le piratage l'an dernier du géant pétrolier

Logo de l'Agence nationale de la Sécurité des Systèmes d'Information, créée pour protéger l'informatique d'Etat



saudien Aramco qui a vu 30 000 de ses ordinateurs simultanément « effacés » par des hackers proche de l'Iran.

La LIO française serait conduite par la discrète Direction générale de la Sécurité extérieure (DGSE). *« Officiellement il n'y a aucune trace de l'existence de capacités offensives »,* souligne Michel Baud, militaire et chercheur à l'Institut français des Relations internationales (Ifri). *« Cela signifie, poursuit-il, que ce volet est aux mains des services secrets et, plus précisément, de la DGSE. »* Un ancien officier de l'armée de terre confirme, sous couvert d'anonymat : *« En 2000, nous avons conçu un programme capable de s'introduire dans n'importe quel système Windows pour en exfiltrer des informations, voire détruire les machines. Seulement, lorsque nous en avons fait la démonstration devant un général cinq étoiles, il*

a immédiatement classifié le programme en secret-défense et nous avons reçu l'ordre de ne plus nous intéresser à la LIO. C'est à cette époque que la DGSE a commencé à se pencher sur le sujet. »

Un responsable de la DGSE confirme l'existence d'un programme *« secret de chez secret »* : *« Je peux juste vous dire que nous faisons ce que font les autres, et que nous ne sommes pas les plus mauvais... »* L'armée et la DGSE, ainsi que l'Anssi, ont refusé de répondre à nos questions. *« L'armée reste très discrète sur la LIO, alors qu'elle gagnerait à assumer publiquement une doctrine d'emploi qui permettrait de dissuader les ennemis, à l'image du nucléaire »,* estime le sénateur centriste Jean-Marie Bockel, auteur du rapport « la Cyberdéfense, un enjeu mondial, une priorité nationale ». Eric Filiol, ancien de la DGSE, acquiesce : *« C'est aberrant qu'en 2013 il n'y ait toujours pas de réflexion globale sur la cyberdéfense, surtout parce qu'il n'y a pas de volonté politique de mettre les choses à plat. Il faut définir quelles sont les forces, quelles sont les cibles, quel est le cadre, quelle est la formation... »* Autant de questions auxquelles la loi de programmation militaire promet de répondre. La tâche s'annonce ardue. *« Le droit militaire est difficilement applicable au cyberspace puisque l'espace, le temps et la notion de preuve tendent à quasiment disparaître »,* explique Eric Filiol. En effet, il est possible de contrefaire jusqu'à l'origine d'une cyberattaque. En 2007, l'Estonie a été prise pour cible par de nombreux serveurs, dont plus d'un tiers étaient situés aux Etats-Unis, alors que l'agresseur était russe. D'où la nécessité de développer des programmes capables d'identifier avec certitude et précision l'origine des cyberattaques. La loi de programmation prévoit que *« la Direction générale de l'Armement [sera] chargée de connaître et d'anticiper la menace, de développer la recherche en amont et d'apporter son expertise en cas de crise informatique »*. Cela suffira-t-il à protéger la France ? Pas sûr. *« C'est le problème avec la sécurité : il s'agit d'un domaine qui coûte cher parce qu'on ne sait jamais d'où viendra la prochaine attaque, et que tout évolue à vitesse grand V, souligne Patrick Chambet, responsable de la sécurité chez Bouygues. Au final, on n'est jamais assez protégé. »* ■