Les mercenaires de la cyberguerre

Logiciels espions, systèmes de surveillance des réseaux… les conflits d'aujourd'hui se déroulent déjà sur le terrain informatique. En guise de troupes, des sociétés high-tech assistent les armées. Mais ces francs-tireurs peuvent devenir une menace. C'est pourquoi la France et d'autres Etats s'apprêtent à mieux les encadrer.

Par **Emmanuel Paquette**

ESPIONNAGE Un « cheval de Troie » peut enregistrer les frappes d'un clavier, activer la caméra d'un ordinateur, etc., sans être détecté.

K. PEMPEL/REUTERS

En ce début de mois d'octobre, l'ambiance est détendue au Grimaldi Forum de Monaco, où se retrouvent, chaque année, les responsables informatiques de plusieurs grands groupes industriels. Mais elle va changer très vite. Le directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi), placée sous l'autorité du Premier ministre, vient à peine de terminer son discours qu'un nom fuse dans la salle. A l'évocation de Vupen, Guillaume Poupard se crispe légèrement. Le militaire, ingénieur, marque une pause et choisit soigneusement ses mots avant de s'exprimer. « Cette société flirte avec la ligne rouge, lance-t-il, énigmatique, mais ce problème va se résoudre d'ici peu. »

Que peuvent bien reprocher les services de Matignon à cette petite start-up montpelliéraine ? Pour avoir déniché plusieurs failles inconnues – des « trous » – dans des logiciels grand public, Vupen a été primée trois années de suite lors du célèbre tournoi de hackers Pwn2Own. Son talent est reconnu sur toute la planète. Pour autant, pas question d'offrir ses découvertes gratuitement aux riches éditeurs tels que Microsoft, Adobe ou Google, et de les aider ainsi à protéger leurs produits. La PME préfère les vendre à des gouvernements étrangers ou à de grandes entreprises à prix d'or, quitte à froisser les autorités françaises. Et pour cause : les acheteurs de ces précieux sésames peuvent s'infiltrer dans les ordinateurs et les réseaux en toute discrétion lors d'opérations de renseignement ou de sabotage. Y compris contre des intérêts français ? •••

VIGILANCE L'Agence nationale de la sécurité des systèmes d'information (Anssi) traque les infiltrations et les attaques informatiques.

M. AWAAD/IP3

La start-up Vupen quitte la France : « L'overdose administrative est devenue trop pesante »

••• Présidée par Chaouki Bekrar – dont le profil sur Twitter n'est autre que le visage de Dark Vador, figure du mal de *La Guerre des étoiles* – Vupen compte parmi ses clients l'Agence nationale de sécurité (NSA) américaine, celle-là même mise en cause par l'ancien consultant Edward Snowden pour avoir développé un programme mondial de surveillance. Après avoir ouvert une filiale dans le Maryland, aux Etats-Unis, les francs-tireurs de Vupen s'apprêtent à plier bagage et à ouvrir, mi-2015, des bureaux au Luxembourg et à Singapour. « L'overdose administrative et les incertitudes juridiques sur nos activités sont devenues trop pesantes. Nous allons par conséquent liquider la société avant la fin de cette année », révèle Chaouki Bekrar à L'Express.

La nouvelle tombe au plus mal – au moment même où l'Hexagone affiche ses ambitions dans le cyberespace, le théâtre des guerres modernes. La loi de programmation militaire, adoptée voilà quelques jours, prévoit, sous le contrôle du Premier ministre, une riposte informatique en cas d'attaque majeure affectant, notamment, l'économie, la sécurité ou la capacité de survie de la nation. Derrière les mots, il s'agit de protéger la prise de contrôle, par des puissances étrangères, des réseaux de transport, d'eau, d'électricité, ou encore de télécommunications. Vital. Face à cette menace d'un nouveau genre, le ministre de la Défense, Jean-Yves Le Drian, n'a pas hésité à évoquer la création d'une cyberarmée aux côtés des trois autres, l'air, la terre, et la marine.

Sur ce terrain d'affrontements, tous les pays augmentent leurs efforts financiers. Mais, dans ce monde virtuel, aux conséquences bien réelles, pas question de s'appuyer sur les avions Rafale du groupe Dassault ou les hélicoptères Tigre d'Airbus. Ici, le sur-mesure fourni par une kyrielle de petites entreprises prime bien souvent sur le prêt-à-porter des grands industriels. Autant d'électrons libres à encadrer et qui vont devoir se plier à de nouvelles règles.

Paraphée par 42 pays, une nouvelle version de l'arrangement de Wassenaar – du nom d'une ville des Pays-Bas – devrait, en effet, entrer en vigueur au mois de décembre. Ce texte vise à lutter contre la prolifération d'armes potentielles. Depuis 1996, il permet aux Etats de contrôler les exportations de technologies à double usage, civil et militaire, comme les réacteurs nucléaires, les radars, les calculateurs et, bientôt, les logiciels d'intrusion et les dispositifs de surveillance des réseaux de télécommunication. La société Vupen est donc concernée au premier chef, et son expatriation n'est pas totalement étrangère à ce durcissement. « Je suis un fervent partisan de toute régulation permettant de contrôler l'export de ces technologies, malheureusement les délais administratifs français sont excessivement longs et incompatibles avec le caractère éphémère des solutions que nous développons », déplore Chaouki Bekrar.

Lieutenant-colonel de l'armée de Terre, à la retraite et libre de s'exprimer, Eric Filiol ne décolère pas : « Vupen est la seule société tricolore à briller sur la scène internationale et nous allons la perdre. Mais elle dérange, alors qu'elle fait honneur à notre pays. »

La nouvelle ébranle peu le patron de l'Anssi, qui se veut rassurant : « Nous comptons d'autres acteurs de bon niveau », confiait-il lors des Assises de la sécurité, à Monaco. Guillaume Poupard pensait sans doute à QuarksLab. Frédéric Raynal, PDG de la société parisienne, annonce : « Nous nous lancerons en 2015, mais en collaboration avec les éditeurs de logiciels. L'idée est de trouver des failles par nous-mêmes ou d'en acheter. Cela pourrait évidemment servir à des gouvernements, mais aussi à tester la solidité de produits ou de réseaux d'entreprise. Mais, promet-il, nous serons sélectifs sur nos clients. »

Pour le compte de la police secrète de Kadhafi

Déjà, un acteur a, sans bruit, obtenu l'autorisation du gouvernement de produire un logiciel espion tirant parti de failles. La société Ercom, plus connue dans le domaine de la sécurité que pour ses capacités offensives, a développé un cheval de Troie. Le programme peut s'installer en toute discrétion et enregistrer à distance les frappes d'un clavier, activer un micro, la caméra d'un ordinateur ou d'un smartphone, le tout sans être détecté par l'utilisateur ou les antivirus ! Ce type d'outil devrait •••

●●● être couvert par l'arrangement de Wassenaar, mais ce n'est pas le seul. A l'initiative de Fleur Pellerin, lorsqu'elle était encore ministre chargée du Numérique, une nouvelle catégorie a vu le jour. Elle concerne les systèmes de surveillance de réseaux de télécommunication, qui, « mal utilisés, peuvent servir à violer les droits de l'homme ou porter atteinte à la sécurité », selon la Commission européenne.

La France en sait quelque chose. « Cette volonté nationale est née après l'affaire Amesys pour instituer un contrôle minimal », explique Guillaume Poupard. Cette société a aidé à mettre sur pied un centre d'écoutes à Tripoli, en Libye, entre 2007 et 2008, pour le compte de la police secrète de Mouammar Kadhafi. Grâce au programme Eagle, les autorités ont pu repérer,

J.-C. MOSCHETTI/REA

STRATÉGIQUE Le ministre de la Défense, Jean-Yves Le Drian, pose la première pierre d'un centre d'expertise, le 6 octobre, à Bruz (Ille-et-Vilaine).

« L'Etat français a poussé Qosmos à travailler avec des régimes autoritaires pour garder un œil sur ces pays »

arrêter, et torturer des opposants au régime en étant capables de collecter et d'analyser à l'échelle du pays les e-mails, les sites consultés, les messages privés des dissidents. Après la chute du tyran, des documents retrouvés sur place par le *Wall Street Journal* confirment l'implication d'Amesys. Dès 2011, la Fédération internationale des ligues des droits de l'homme (FIDH) et la Ligue des droits de l'homme portent plainte pour complicité de torture à travers la fourniture d'un matériel de surveillance. Deux ans plus tard, cinq victimes sont entendues par la justice française à la suite de l'ouverture d'une information judiciaire toujours en cours. « Non seulement il y a bien eu vente de matériel, mais des salariés français ont fait le déplacement à Tripoli pour former le personnel libyen », détaille Clémence Bectarte, coordinatrice du groupe d'action judiciaire de la FIDH.

Pour mettre fin à ce scandale, Amesys, devenu entre-temps une filiale de Bull, cède l'activité Eagle en 2012. Mais le repreneur n'est autre que l'un des concepteurs du système et ex-directeur général d'Amesys, Stéphane Salies. Un tour de passe-passe, un changement de nom, et voilà Eagle rebaptisé Cerebro, commercialisé par l'entreprise Advanced Middle East Systems, installée à Dubai. La ficelle est un peu grosse : les Emirats arabes unis ne sont pas signataires de l'arrangement de Wassenaar. « Voilà bien la preuve que l'on a voulu mettre à l'abri cette technologie », estime Clémence Bectarte.

Un lanceur d'alerte licencié, un militant arrêté...

L'histoire ne s'arrête pas là. Afin de déployer son système, Amesys a fait appel à une autre société tricolore, Qosmos. Grâce aux travaux menés au sein du laboratoire d'informatique de l'université de Paris-VI, cette entreprise a développé des sondes pour intercepter massivement le trafic Internet à des points clefs. Bien que testées en Libye, elles n'auraient jamais été opérationnelles, plaide Qosmos. Une ligne de défense également avancée dans un autre dossier, en Syrie, avec le programme Asfador, piloté par un sous-traitant allemand. « Une information judiciaire a été ouverte contre eux pour vérifier si tout cela est vrai, et si l'entreprise n'a pas aidé le régime de Bachar al-Assad à surveiller sa population », ajoute la juriste.

Car, dès 2011, un lanceur d'alerte sort de l'ombre. James Dunne s'inquiète publiquement de voir la technologie de Qosmos se transformer en arme de répression entre les mains de régimes autoritaires. Quelques mois plus tard, ce responsable de la documentation technique est licencié pour faute lourde, puis attaqué en diffamation par son ex-employeur.

Plus trouble est la position du gouvernement français. Si Paris milite pour le contrôle de l'exportation de ce genre de dispositif, il ne pouvait ignorer l'activité de Qosmos en Syrie. En effet, cette entreprise a été financée par l'Etat, dès 2011. Dès le printemps 2009, elle avait reçu une habilitation « confidentiel-défense ». Des portes et vitres blindées sont alors installées au siège de la société, et des détecteurs de mouvements et de chaleur équipent le bâtiment. Des précautions nécessaires car l'entreprise travaille pour les ministères de la Défense et de l'Intérieur, et a même passé un contrat avec les services secrets français, la Direction générale de la sécurité extérieure (DGSE). Nom du projet : Kairos. Des liens confirmés par le cofondateur de la société, Eric Horlait, dans un enregistrement audio diffusé par le site Reflets.info. « Les autorités françaises ont poussé Qosmos à travailler avec des régimes autoritaires pour garder un œil sur ces pays et, lorsque cela ●●●

••• s'est su, on les a lâchés et abandonnés en rase campagne », précise un proche du dossier sous couvert d'anonymat.

Aujourd'hui, Qosmos explique ne plus livrer son dispositif d'interceptions légales à des tiers depuis 2011, mais seulement à des gouvernements démocratiques. Pourtant, la société a travaillé avec la firme allemande Trovicor, au moins jusqu'en 2012, pour améliorer ses produits d'interception d'e-mails et de messageries instantanées, selon des documents obtenus par L'Express. Or cette ex-filiale de Nokia Siemens Networks a fourni des systèmes de surveillance à 12 pays d'Afrique du Nord et du Moyen-Orient, comme L'Egypte, le Yémen, ou encore Bahreïn, entraînant l'arrestation d'un militant des droits de l'homme.

R. WILKING/REUTERS

EFFORT Pour se doter de nouveaux moyens, les Etats-Unis investiront 4 milliards d'euros en 2015.

USA/NSA/REUTERS

COMPÉTITION La NSA est un des clients de la start-up française Vupen.

D'autres acteurs hexagonaux proposent des solutions d'interceptions légales, comme Alcatel-Lucent (Ulis), Aqsacom (Alis) ou encore Thales (Spyder), mais aucun n'a souhaité nous répondre. « Tous les services juridiques sont en train d'étudier les impacts de l'arrangement de Wassenaar sur leurs activités, car il n'existe aucune jurisprudence en la matière », indique Gérôme Billois, directeur sécurité chez Solucom.

Les outils défensifs peuvent se transformer en armes

Les cyberarmes ont fait l'objet d'une réflexion dès la fin des années 1990, confie le général Jean-Marc Degoulange, aujourd'hui à la retraite. La 785e compagnie de guerre électronique, dont il a fait partie, a même simulé très tôt des attaques. « Afin d'évaluer les outils de surveillance et de protection de nos réseaux informatiques, nous les soumettions à des épreuves de résistance, se souvient le militaire, à présent président de l'association des anciens de cette compagnie. Pour bien se défendre, il convient d'appréhender au mieux la menace. » Pour se doter de nouveaux moyens dans cette course mondiale au cyberarmement, un plan quinquennal prévoit d'investir 1 milliard d'euros d'ici à 2019, alors même que les militaires doivent faire face à des coupes budgétaires sans précédent. Ce montant reste cependant bien loin de l'effort américain de 4 milliards d'euros pour la seule année 2015. « Mais, sur certains aspects offensifs, nous sommes meilleurs qu'eux, estime Jean-Marie Bockel, ancien secrétaire d'Etat à la Défense. Le gigantisme des efforts déployés outre-Atlantique par la NSA peut nuire à leur efficacité en rendant les organisations lourdes et complexes. Nous, nous disposons de moyens financiers moins importants et nous devons faire des choix. »

Pourtant, le départ de Vupen, conjugué aux affaires judiciaires d'Amesys et de Qosmos, fragilise le volontarisme français. « Pour développer des capacités de combat numérique, l'armée travaille avec beaucoup de monde en faisant appel à des ressources extérieures et à un tissu de PME, explique le contre-amiral Arnaud Coustillière. Dans ce contexte, le choix de certaines d'entre elles de s'expatrier n'est pas une bonne nouvelle. » Car, dans la guerre cybernétique qui s'annonce, le renseignement n'a jamais été aussi central. En effet, quand les outils défensifs sont susceptibles de se transformer en armes, la confiance entre alliés peut s'émousser très rapidement. Comme le conseillait déjà, au VIe siècle avant Jésus-Christ, le général chinois Sun Tzu dans *L'Art de la guerre* : « Multipliez les espions, ayez-en partout, dans le propre palais du prince ennemi, dans l'hôtel de ses ministres, sous les tentes de ses généraux ; ayez une liste des principaux officiers qui sont à son service. » Grâce à la technologie, il n'aura jamais été aussi facile de suivre ce précepte et, même, d'aller au-delà. En l'étendant à l'ensemble des populations. • **E. Pa.**