Réserve opérationnelle de cyberdéfense: enjeux et défis

cahier de la pensée mili-Terre

le Chef de bataillon David KAUFMANN

publié le 06/06/2018

Sciences & technologies

Alors que le livre blanc annonçait dès 2013 la création d'une nouvelle force de cyberdéfense, peu d'informations ont été diffusées depuis à ce sujet. Cette force pourrait jouer un rôle bien adapté au concept du continuum défense-sécurité, mais sa montée en puissance s'accompagne de nombreux défis à relever.

L'affaire Snowden[1] nous rappelle quasi quotidiennement que le cyberespace est un terrain de confrontation aux enjeux stratégiques. Certains États consentent d'importants efforts financiers pour développer leurs capacités informatiques, y compris offensives. Depuis plusieurs années, la France a pris la mesure de ces nouvelles menaces et tente de trouver une place parmi les grandes puissances de cyberdéfense. Les efforts consentis sont significatifs, mais les moyens demeurent limités par la nécessaire réduction des dépenses publiques. La création d'une branche de la réserve opérationnelle dédiée à la cyberdéfense permet de disposer ponctuellement de ressources spécialisées sans avoir à supporter le surcoût excessif qu'impliquerait un recrutement à titre permanent. La phase de constitution de cette force ne fait que débuter, ce qui explique le caractère très général des informations diffusées à son sujet, comme dans la loi de programmation militaire par exemple. Il est donc légitime de s'intéresser à la nature des missions susceptibles de lui être confiées, puis d'exposer les défis auxquels la force pourrait être confrontée lors de sa montée en puissance.

Certes, la révolution numérique continue de bouleverser nos habitudes et offre des opportunités extraordinaires en matière de développement social, d'accès à la culture et à l'information. Cependant, la croissance exponentielle des réseaux de toutes sortes et du trafic sur Internet complexifie d'autant la maîtrise de l'information. La publicité du programme Prism a déclenché une prise de conscience collective des menaces potentielles qui pèsent sur l'interconnexion généralisée des systèmes d'information. En particulier, le cyberespace constitue un terrain propice à l'espionnage économique et

industriel, terrain sur lequel l'Europe montre d'importantes faiblesses. En effet, alors que la majorité des matériels informatiques est d'origine asiatique, les États-Unis conservent une mainmise sur les produits logiciels et applicatifs. Dans ce jeu stratégique, les dés sont pipés à la défaveur des nations européennes, qui accusent un retard dorénavant impossible à rattraper.

La France n'est pas épargnée par la menace cybernétique qui pourrait porter gravement atteinte à ses intérêts nationaux. Au-delà des attaques visant quotidiennement les institutions et les grandes entreprises, une crise informatique majeure, loin d'être improbable, pourrait avoir des conséquences potentiellement désastreuses pour le pays. Sans une défense forte, organisée et coordonnée des systèmes d'information, l'accès aux sites institutionnels, l'alimentation en énergie et en eau, le fonctionnement des hôpitaux, les télécommunications et les transactions bancaires par exemple, peuvent être fortement perturbés. L'expérience vécue par l'Estonie en 2007 montre bien la dépendance grandissante des sociétés développées aux technologies de l'information et de la communication. Le sénateur Jean-Marie Bockel rapporte à ce sujet que les attaques subies «ont perturbé de manière spectaculaire le fonctionnement de la vie courante du pays, en privant les usagers de l'accès à certains services en ligne essentiels»[2].

Dans ce cadre et depuis le livre blanc de 2008, la France a augmenté significativement les moyens dédiés à la défense de ses intérêts dans le cyberespace, prenant acte de son retard en la matière et concédant que «l'enjeu a été sous-estimé». L'ANSSI[3] agit en tant qu'autorité nationale reconnue et dispose désormais d'un pouvoir étendu sur l'ensemble des acteurs concernés.

Bien entendu, le ministère de la Défense joue un rôle de premier plan en vue d'atteindre les objectifs stratégiques[4] fixés dès 2009. La défense a naturellement vocation à protéger l'information de souveraineté et à contribuer à placer la France au sein des puissances mondiales de cyberdéfense. La nouvelle loi de programmation militaire confirme également l'approche globale et interministérielle dans la prévention et la réponse aux crises majeures: «L'action des forces armées s'envisage conjointement avec celle de l'ensemble de l'appareil d'État (…) et des opérateurs, publics et privés, d'infrastructures et de réseaux vitaux»[5]. Le continuum défense-sécurité trouve toute sa pertinence dans un cyberespace aux frontières incontrôlables. Les moyens spécifiques de la défense pourraient donc renforcer ceux de l'ANSSI en cas de crise informatique sur le territoire national. L'organisation unifiée et centralisée de la chaîne de cyberdéfense offre un atout supplémentaire en matière de réactivité, qualité essentielle lorsque survient une crise.

Ce contexte d'intervention sur le territoire national est tout à fait adapté à la réserve opérationnelle. S'appuyant sur une formation régulièrement entretenue, les réservistes sont capables de répondre rapidement à un besoin temporaire en main-d'œuvre qualifiée. En matière de cyberdéfense, le livre blanc de 2013 évoque une composante dédiée au sein de la réserve opérationnelle, qui «sera prévue et organisée spécifiquement pour permettre au ministère de la Défense de disposer d'une capacité de cyberdéfense démultipliée en cas d'attaque informatique majeure»[6]. La loi de programmation militaire 2014-2019 confirme la nécessité de développer cette composante nouvelle, sans toutefois en détailler le calendrier de montée en puissance ni les effectifs prévisionnels.

Le recours à des réservistes, qui par nature servent à la fois la société civile et les armées, se justifie par le caractère dual des missions susceptibles de leur être confiées. En effet, ces unités de techniciens pourraient venir renforcer la sécurité des sites institutionnels, mais aussi contribuer à la résilience des opérateurs d'importance vitale (OIV). Derrière ce sigle se cachent plusieurs centaines d'entreprises assurant la sécurité et la satisfaction des besoins principaux de la société, contre lesquelles une attaque de leurs systèmes d'information pourrait avoir de graves conséquences. La loi de programmation militaire impose à ces opérateurs une obligation de moyens concourant à la sécurité des systèmes d'information et les contraint dorénavant à déclarer les attaques subies.

Par ailleurs, toute aide internationale dans la gestion d'une crise de grande ampleur semble difficilement envisageable. Sans évoquer le risque bien réel de compromission d'informations relatives à la souveraineté étatique, l'accès à des données industrielles confidentielles ne serait pas maîtrisé. Dès lors, toute intervention étrangère pourrait impliquer a minima une charge supplémentaire de surveillance, voire constituer une menace d'espionnage économique et industriel. L'absence de débat à l'OTAN au sujet de l'applicabilité de l'article 5 en cas de cyberattaque illustre bien la faiblesse des coopérations internationales en matière de défense dans le cyberespace.

La nouvelle force de réserve opérationnelle de cyberdéfense représente ainsi une main-d'œuvre spécialisée ayant vocation à contribuer à la résilience des systèmes d'information vitaux en cas de crise majeure. Sa montée en puissance progressive au cours des prochaines années s'accompagne de nombreux défis auxquels il faut répondre.

En premier lieu, le cadre d'emploi de ces unités nécessite d'être précisé. En cas de crise cybernétique, il est probable que les autorités cherchent initialement à la gérer avec leurs moyens propres respectifs, éventuellement assistés d'équipes d'intervention rapide ultraspécialisées pilotées par l'ANSSI et le ministère de la Défense. Face à des incidents multiples menaçant la cybersécurité nationale, les réservistes seraient alors sollicités en seconde ligne et toujours en complément des moyens du premier cercle. Leur mission principale pourrait consister à participer au maintien en condition opérationnelle des systèmes d'information des infrastructures critiques, militaires ou civiles.

L'urgence relative associée à la mobilisation de la réserve ne doit pas occulter la nécessité d'encadrer strictement ses activités. Alors que les équipes engagées jouiront d'un accès privilégié au système à protéger, il faudra s'assurer du caractère purement défensif des actions entreprises. La volonté de démontrer ses capacités pourrait inciter l'un des membres à outrepasser ses prérogatives et basculer dans le domaine offensif. Afin d'éviter que ce «caporal cyberstratégique» ne vienne amplifier la crise, des mesures spécifiques devraient être mises en œuvre : définition claire des tâches confiées à chacun, enregistrement des actions effectuées, formation à l'éthique, menace de sanctions disciplinaires et légales. De plus, les organismes soutenus seront particulièrement attentifs au maintien de la confidentialité de leurs données industrielles sensibles, voire classifiées de défense le cas échéant. Des mesures de réduction des risques de fuite devront être instaurées en complément des filtres inhérents aux procédures d'habilitation.

L'étape préalable à son déploiement consiste à mettre progressivement sur pied une telle force, probablement composée de plusieurs centaines d'hommes. Recrutés en priorité parmi la population étudiante, ces techniciens en informatique devront être

évalués au préalable sur leurs compétences techniques mais aussi au plan humain. Étant donné la sensibilité des conditions d'engagement, il est sans doute préférable de privilégier la qualité à la quantité des effectifs retenus. À l'instar du fort engouement suscité par la réserve citoyenne de cyberdéfense, les postulants devraient se présenter en nombre, attirés par le caractère inhabituel et exclusif des missions qui pourraient leur être confiées. En effet, la perspective d'intervenir en situation de crise pour défendre ou remettre en condition opérationnelle un système informatique peut déclencher de nombreux actes de candidature. La qualité de réserviste opérationnel offre également un atout supplémentaire indéniable lors de la recherche d'un emploi.

Néanmoins, le principal challenge à relever sera sans doute celui de la fidélisation. La motivation initiale de cette ressource majoritairement jeune doit être régulièrement entretenue, notamment par des conditions d'entraînement réalistes et attractives. Même si la virtualisation offre des possibilités de simulation très étendues, les ressources matérielles nécessaires à la formation et l'entraînement demanderont un budget conséquent. Dans ce cadre, le futur pôle d'excellence de cyberdéfense implanté en région Bretagne au sein d'un réseau d'écoles et d'entreprises particulièrement développé peut offrir un terrain propice aux grandes manœuvres informatiques.

Enfin, le personnel retenu devra se montrer disponible en cas de sollicitation pour que la réserve joue pleinement son rôle d'assistance et de renforcement des moyens spécialisés. Si la disponibilité ne soulève pas d'interrogations au sujet de la population étudiante, le doute est davantage permis concernant les employés des entreprises. Dans le cas d'une crise de grande ampleur, ces dernières auront sans doute des réticences à se séparer, même temporairement, de leurs techniciens. En conséquence, la montée en puissance de la force doit s'accompagner a minima d'un effort de communication vers les entreprises, en insistant sur l'efficacité de la gestion centralisée des moyens dans le règlement d'une crise nationale.

La croissance exponentielle des cybermenaces conjuguée à la faible priorité accordée par les entreprises à la protection de leurs systèmes d'information impose le renforcement des moyens dédiés à la cyberdéfense à l'échelle nationale. Les dépenses publiques fortement contraintes militent pour l'emploi d'une main-d'œuvre temporaire, déployable sur court préavis. La réserve opérationnelle offre un cadre d'emploi bien adapté à l'engagement sur le territoire national, en complément des forces conventionnelles. Le recrutement et la fidélisation d'un vivier de techniciens compétents constituent un vrai challenge alors que beaucoup reste à construire. La satisfaction des besoins en effectifs sera en particulier conditionnée par les moyens consentis pour la formation et l'entraînement. Quoi qu'il en soit, il faudra sans doute plusieurs années pour intégrer pleinement la réserve opérationnelle au sein du dispositif global de cyberdéfense nationale.

Les mesures de réaction face aux agressions informatiques concourent à la gestion du risque d'occurrence d'une crise nationale. Elles sont complétées par une posture de protection des systèmes d'information visant à prévenir et détecter les signes précurseurs d'une telle crise. Cette approche globale de la cyberdéfense n'exclut pas de

détenir une capacité informatique offensive, désormais ouvertement assumée par le livre blanc de 2013. Même si le volet dissuasif n'est pas évoqué par la doctrine officielle, une communication savamment dosée sur cette capacité d'attaque pourrait contribuer à dissuader les agresseurs potentiels.

[1] Edward Snowden, ancien employé de la NSA, a révélé les détails de plusieurs programmes de surveillance américains et britanniques, dont le programme Prism d'écoute sur Internet. Source fr.wikipedia.org

[2] Rapport d'information du Sénat du 18 juillet 2012 sur la cyberdéfense

[3] Discours de M.Jean-Yves Le Drian, ministre de la Défense, 3 juin 2013

[4] Défense et sécurité des systèmes d'information, stratégie de la France. ANSSI, 2009

[5] Loi de programmation militaire 2014-2019 du 18 décembre 2013

[6] Livre blanc sur la défense et la sécurité nationale, 2013

Officier des troupes de marine, l'auteur a effectué une première partie de carrière dans les systèmes d'information et de communication, avant d'intégrer la 20ème promotion de l'École de guerre. Il suit actuellement un mastère spécialisé en cyber sécurité à Télécom Bretagne et Supélec Rennes.

Titre : le Chef de bataillon David KAUFMANN

Auteur(s) : le Chef de bataillon David KAUFMANN

Date de parution 22/05/2018