Général Thierry Bauer (ComCyber) : « bloquer une cyberattaque va vite, la comprendre, moins »

Par Bertrand Lemaire | Le vendredi 9 juin 2023 | Gouvernance

Le cyber-espace est devenu un terrain d'affrontement au même titre que la terre, les océans ou l'espace aérien. Le Général Thierry Bauer explique ici comment la France gère les cyber-conflits. Parmi les éléments clés, la formation des talents de la cyber-guerre est primordial.

Le général Thierry Bauer est adjoint au général commandant la Cyberdéfense. - © Cyrielle Sicard/ECPAD/Défense

Quels sont les rôles et la position du Commandement de la Cyberdéfense (ComCyber) au sein du Ministère des Armées ?

Le ComCyber est sous l'autorité du chef d'état-major des armées et conduit les opérations de cyberdéfense.

Celle-ci commence par la lutte informatique défensive, c'est à dire la réaction lorsque nous sommes attaqués. Notre périmètre est, sur délégation de l'ANSSI, celui du Ministère des Armées. Le Renseignement est, s'agissant de la DGSE et de la DRSD autonome. Par contre, le Secrétariat général pour l'administration (SGA) et la Direction Générale de l'Armement (DGA) sont bien dans notre périmètre.

Nous menons également de la lutte informatique d'influence. Notre doctrine en la matière a été publiée en octobre 2021. Il s'agit là de répondre aux attaques informationnelles (ce qui se dit des armées, fake news…), notamment sur les réseaux sociaux. Il s'agit donc de lutter contre la désinformation et aussi de faire passer nos propres messages.

Enfin, nous réalisons également de la lutte informatique offensive. Le domaine du cyber-espace est un domaine de conflit au même titre que la terre, l'espace aérien ou la mer.

Vous avez publié des éléments de doctrine sur ces trois types de luttes. Pouvez-vous nous en résumer l'essentiel ?

Le cyber-espace n'est maîtrisé par aucune armée en particulier et nous ne sommes pas une

Dans le cas d'une cyber-attaque, il faut d'abord la contenir puis la repousser et tirer des conclusions. Il s'agit, en effet, de faire en sorte qu'une attaque similaire ne puisse plus se reproduire. Bloquer une cyberattaque va vite, la comprendre va beaucoup moins vite.

La France est sur la même ligne que l'OTAN sur le fait que la riposte à une cyber-attaque ne doit pas forcément être sur le terrain cyber. On peut très bien envisager une riposte diplomatique, financière voire une intervention militaire. Une cyber-attaque peut être considérée, dans certains cas, comme similaire à un tir de canon. La vraie difficulté est d'identifier l'attaquant.

Le Centre de Coordination des Crises Cyber (C4) réunit l'ANSSI, le ComCyber, le ministère des Affaires Etrangères, les services de renseignement… Son rôle est d'imputer une agression avec une probabilité d'attribution. Le C4 est parfois très affirmatif, parfois beaucoup moins.

Le ComCyber a publié ses doctrines de lutte informatique. - © D.R.

Pouvez-vous donner un exemple ?

Bien entendu, je ne vais pas rentrer dans des détails devant rester confidentiels. En 2019, le Service de Santé des Armées a été attaqué par des cyber-criminels. L'attaque a été assez vite analysée. Le Centre d'Analyse et de Lutte Informatique Défensive (notre SOC) est intervenu dans le cadre de sa mission de gestion des crises et en aidant à la remise en l'état du système d'information.

Les attaques courantes sont évidemment bloquées systématiquement. Nous gérons assez bien les attaques de bas niveau. Nous avons pu découvrir quelques exemples de pénétration mais l'agent infectieux n'a pas pu reprendre contact avec ses commanditaires.Notre vraie difficulté est sur les systèmes périphériques à la Défense.

Par exemple, l'ONACVG (Office National des Anciens Combattants et des Victimes de Guerre) a subi une attaque par rançongiciel et il lui a fallu reconstruire son SI.

Pour remplir vos missions, vous avez besoin de moyens humains. Comment les recrutez-vous ?

Nous ratissons très large avec des profils et des statuts variés. Nous pouvons recruter des civils, éventuellement des catégories B, la plupart étant des ingénieurs sous contrat en catégorie A. Pour les militaires, ils sont au minimum sous-officiers. Nous cherchons un équilibre entre civils et militaires car la Loi ne permet pas à un civil de combattre, même dans le cyber-espace. Et le problème est d'autant plus sensible lorsqu'il s'agit d'accompagner les troupes sur le terrain où il y a des systèmes d'armes complexes. Techniquement, un système d'armes est très proche d'un système industriel type SCADA. Parfois, des civils prennent le statut de réservistes pour pouvoir se rendre sur un théâtre d'opération. Nous avons toujours des équipes en astreinte pour partir sur le terrain dans des cas graves.

François-Xavier Pierrel (JCDecaux) : « la data transforme la vente de la communication extérieure »

La data est devenu un enjeu majeur pour JCDecaux. François-Xavier Pierrel, Group Chief Data…

Stéphane Rousseau nommé Group CIO d'Ingenico

Fort d'une notoriété et d'une reconnaissance certaine de ses pairs, Stéphane Rousseau a quitt…

David Lepicier (Pernod Ricard) : « l'expérience employé est clé pour gagner la guerre des talents »

Le groupe Pernod Ricard a mis la data au coeur de sa transformation comme l'explique David…

Mathieu Ovaert (Nestlé) : « je suis là pour générer de la valeur, pas seulement financière »

Chez Nestlé France, première filiale du groupe agro-alimentaire mondial, l'IT et la data sont…

Pour ceux qui optent pour le statut militaire, nous pouvons les recruter dès le bac, les former et leur faire gravir les échelons. Ils peuvent suivre la formation de Saint-Cyr, une école militaire scientifique et technique comme l'école de l'ANSSI qui est une excellente formation en cybersécurité et en chiffrement de l'information. Dans la cybersécurité, beaucoup de sous-officiers deviennent officiers. De plus en plus d'officiers sont sous contrat : nous les formons en échange d'un engagement d'une certaine durée. Et, au bout de leur engagement, un grand nombre des jeunes que nous avons formés sont recrutés comme ingénieurs en cybersécurité dans des entreprises privées. Nous voulons, au nom de l'intérêt national, une cyber-défense de haut niveau partout, y compris dans les entreprises françaises. Et c'est donc volontiers que nous participons, par ce biais, à la formation des futurs experts en cybersécurité des entreprises. Nous essayons d'accompagner de façon intelligente la transition vers le civil de ces spécialistes.

Nous recrutons aussi des officiers commissionnés : ce sont des experts reconnus qui sont directement recrutés à un grade lié à leur niveau d'expertise (par exemple : commandant).

Cependant, les recruteurs restent les armées (Terre, Air, Mer), pas nous directement. Il n'y a pas « d'armée cyber » car nous voulons restés connectés aux armées qui demeurent ainsi multi-domaines et multi-champs. Notre rôle est bien, aussi, de sensibiliser et former les forces à la lutte informatique.

Il est souvent dit que, en matière de cyberguerre, le conflit ukrainien a été une rupture. Mais est-ce exact ?

Oui, c'est exact, mais la rupture date de 2014 avec les premières cyber-attaques contre, par exemple, des SI administratifs, la production d'électricité, etc. Dès la crise de Crimée, il y a eu des cyber-attaques.

Nous avons aussi pu constater un pic d'attaques quelques jours avant l'agression de 2022. Mais les Ukrainiens avaient huit ans d'expérience : leur cyber-défense a très bien résisté.

Dans ce conflit, il ne faut pas négliger le soutien des entreprises privées qui a eu un rôle prépondérant. Microsoft a, par exemple, contribué à héberger hors d'Ukraine les données d'État. Et notre homologue des Etats-Unis a évidemment appuyé la cyber-défense ukrainienne.

En fait, nous avons été surpris par les effets limités de toutes ces cyber-attaques. L'attaque qui a fait le plus mal à la défense ukrainienne est celle contre le système de communication satellitaire. Or, si les armées ne peuvent plus communiquer et sont désorganisées, on ne peut pas se battre très longtemps. Les forces armées ont alors basculé sur le réseau GSM, avant d'être aidées par la constellation d'Elon Musk, Starlink.

La vraie rupture de ce conflit, c'est que le cyber-espace est devenu un terrain de combat au même titre que la terre, la mer ou l'air.

Quels défis avez-vous encore à relever ?

Le défi permanent reste bien sûr celui des ressources humaines. Il nous faut former et attirer des jeunes. Il faut déconstruire le mythe du hacker à capuche vivant en ermite. La cyberguerre, comme toute guerre, est un travail d'équipe, avec émulation et collaboration. Mais c'est une voie où l'on peut vraiment s'épanouir. C'est le sens d'opérations comme Passe Ton Hack d'Abord : faire connaître les métiers de la cybersécurité aux jeunes. Passe Ton Hack d'Abord est destiné aux lycéens sous la forme d'un « capture the flag ». Cyber Humanum Est est, lui, un exercice annuel destiné aux étudiants : il s'agit d'une bataille cyber qui dure une semaine, 24 heures sur 24 pour bien comprendre la vie d'un expert en cybersécurité où rien ne se répète deux fois.

Un autre défi est davantage militaire. Il s'agit de mieux intégrer la cyberguerre dans la stratégie militaire. Clairement, au cours du conflit ukrainien, les Russes ont manqué de coordination entre les cyber-attaques et les attaques classiques sur le terrain.

Enfin, il nous faut développer les partenariats avec nos alliés, y compris en acceptant d'exposer certaines de nos faiblesses, ce qui n'est bien sûr pas simple. Ce développement avance bien aussi bien au sein de l'Union Européenne que de l'OTAN.

Podcast - Comment le ComCyber veut gagner la guerre des talents

Au sein des forces armées françaises, le ComCyber est l'organisme en charge de la Cyberdéfense tant défensive qu'offensive ou d'influence. Le général Thierry Bauer, adjoint au général commandant la Cyberdéfense, explique comment il entend gagner la guerre des talents. Le « pipeline cyber » part de la sensibilisation chez les lycéens ou les étudiants. Les armées recrutent et forment les jeunes talents qui, ensuite, peuvent poursuivre leurs carrières dans les entreprises privées, au bénéfice bien compris de l'intérêt national.

Sur le même sujet

- La Cyberdéfense à la découverte des cybertalents de demain

- Si tu veux la cybersécurité, prépare la cyberguerre

Républik IT Le Média est édité par
Républik Group