« LE COMCYBERGEND TOUT SEUL NE SERA RIEN »

Le Commandement de la gendarmerie dans le cyberespace, a été créé fin février et lancé de façon opérationnelle le 1er août de cette année. Il correspond à une volonté très forte, très claire du directeur général de la Gendarmerie, le Général d'armée Christian Rodriguez, de regrouper l'ensemble des forces cyber de la mission gendarmerie sous un seul chef, sous un commandement unique.

La volonté du Directeur Général était de se baser sur quatre grandes lignes directrices :

- performances,
- lisibilité,
- cohérence,
- simplicité.

En créant ce grand commandement et en le rattachant directement au directeur général, la gendarmerie crée une structure lisible, un fonctionnement éminemment transverse avec des interactions permanentes entre l'ensemble des acteurs. La cohérence veut que le champ d'action confié au Comcyber va de la prévention jusqu'à l'investigation. Ce qui induit une vraie synergie entre les acteurs et un gage d'efficacité, de meilleures performances. Nous appliquons dans le domaine cyber ce qui fait notre force, un principe de poupées russes d'agrégation de ressources, la capacité qu'a la gendarmerie de monter en puissance en fonction de la complexité de l'affaire. Une affaire peut démarrer avec des enquêteurs au niveau des unités élémentaires. Si jamais ils n'y arrivent pas parce que c'est trop compliqué, c'est l'échelon départemental qui vient et qui agrège ces ressources. Cet échelon départemental est lui-même coordonné par l'échelon régional avec les onze antennes du C3E au sein des SR. Et enfin, si jamais on est vraiment sur un dossier très complexe, c'est la pointe de diamant de l'échelon central qui va intervenir, avec des enquêteurs et des experts techniques chevronnés.

MARC BOGET

Général de division, commandant de la Gendarmerie dans le cyberespace

Écusson du commandement de la gendarmerie dans le cyberespace

Cette recherche de cohérence et de performance pose les bases du futur Service à Compétence Nationale voulu par le mi-

nistre de l'Intérieur, pour lequel il a mandaté le Directeur Général de la Gendarmerie. Ce SCN sera une unité mixte police-gendarmerie.

Il faut distinguer deux grands objectifs :

- une vision ministérielle de très haut niveau sur l'état de la menace, la préparation de l'État, la crise, la formation, les mutualisations des acquisitions, etc.
- un pilier judiciaire, car le SCN aura une compétence judiciaire sur le très haut du spectre.

Il me faut préciser de manière très claire que le service n'a pas vocation à prendre la direction d'enquêtes en propre mais bien de venir en co-saisine, pour appuyer avec des enquêteurs chevronnés et des experts techniques, les directeurs d'enquête policiers ou gendarmes. La crise du coronavirus, avec ses différentes phases de confinement, a entraîné une dématérialisation généralisée. Elle a démontré, si c'était nécessaire, l'importance de fédérer, de coordonner et de collaborer entre forces.

Le Comcybergend a quatre missions :

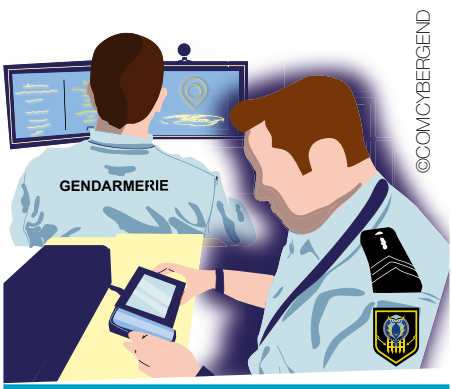
- stratégie et partenariat,
- prévention et proximité numérique,
- investigations,
- appui technique aux opérations numériques.

Logo ComCyberGend

J'en reviens à la fameuse pyramide que j'évoquais plus haut. l'Unité élémentaire est coordonnée par l'échelon départemental, lui-même coordonné par l'échelon régional, puis par l'échelon centre. Le Comcybergend, c'est 7 000 cyber-enquêteurs, ce qui représente une force de frappe non négligeable. Nous nous appuyons sur ce qui fait aussi la spécificité et la force de la gendarmerie nationale, son allonge dans les territoires. Les 7 000 enquêteurs, ils sont répartis dans tous les départements de France, en métropole comme outremer. Ce maillage territorial, ce maillage cyber, allié avec cette capacité d'agrégation de ressources, me permettent une montée rapide en compétences et en puissance, face à la problématique cyber qu'on rencontre à un instant T. C'est exactement le même modèle que celui qu'on en PJ classique, mais dans le monde cyber.

Sur le volet prévention, l'action est encore enrichie, renforcée, au travers de multiples partenariats soit existants, soit à venir. J'ai trois cibles prioritaires en l'occurrence : les

élus, les acteurs économiques et la population au sens large. Nous avons commencé à travailler avec les associations et les structures représentant ces différentes cibles prioritaires et je me dois de constater l'excellent état d'esprit que je rencontre. Ils sont tous convaincus de l'importance de travailler ensemble sur ce sujet, notamment avec les gendarmes. Travailler en amont, c'est leur faire prendre conscience du danger et les conseiller, les aider à se protéger d'attaques futures.



Expertise ComCyberGend

À l'inverse, lorsque nous agissons sur le post-incident, il faut identifier et interpeller les auteurs des faits. C'est grâce à des enquêteurs et des experts techniques partout sur le territoire, capable de prendre des sujets complexes. Nous pouvons en permanence avoir des messages de prévention adaptés à ce que l'on constate dans les enquêtes judiciaires. Mais aussi, à l'inverse, des enquêtes judiciaires d'initiative déclenchées par les signaux faibles qui remontent des actions de prévention.

Dans le cadre du plan Gend 2024, le directeur général a voulu mettre un accent très fort sur nos capacités numériques.

Premièrement, en recrutant a minima 40 de nos officiers comme ayant un profil scientifique. Or, dès cette année, nous sommes à plus de 50. À court terme nous ciblons le passage de 7 000 cyber-enquêteurs à 10 000. Quand je suis rentré en gendarmerie, on n'était pas du tout sur ce portage-là. À l'époque, le cœur du recrutement était constitué de juristes et de littéraires. Les scientifiques comme moi étaient plutôt considérés comme des gens bizarres, qu'on ne comprenait pas très bien. C'est désormais complètement derrière nous, on est vraiment sur une nouvelle ère.

Deuxièmement, le général Rodriguez a lancé les E-Compagnies : Ce sont des formations spécifiques au sein des écoles de sous-officiers, à destination des personnels identifiés comme ayant une appétence numérique. Classiquement un élève gendarme « classique » entend parler de numérique sur 7 à 8 % de son temps de formation. Dans une E-Compagnie, ce chiffre monte à 30 %.

Troisièmement, il a été créé une branche de gestion spécifique pour le cyber au niveau Ressources Humaines. Désormais, l'ensemble des personnels va être regardé et suivi avec une dominante cyber. Le but est de travailler sur les parcours de carrière, sur les formations, sur les capacités, pour faire monter en compétence les gendarmes et être capable d'irriguer toute la chaîne. Si j'emploie une expression cyber, je dirais que l'on va surveiller la « mise à jour », on va travailler dans la durée pour identifier les

profils. Le but est de progresser, de pouvoir dire à un gendarme : « Vous avez besoin de telles capacités, on va vous envoyer en formation, vous êtes une connaissance terrain, on va vous envoyer sur le terrain, puis après, vous viendrez prendre un poste plus important. » C'est une vraie gestion de carrière. C'est ce qui existe pour des pharmaciens, les chimistes, dans le cadre de l'IRCGN[1], et pour la partie système d'information au sein du STSISI[2]. Désormais, il y a une troisième branche qui est le cyber qui se hisse au niveau.

Il faut insister sur la densité, la richesse, de l'écosystème. Ma conviction est que si on ne travaille pas en collaboration les uns avec les autres, on n'arrivera à rien. Le Comcyber tout seul ne sera rien, comme chaque autre acteur isolé. Nous travaillons avec l'autorité judiciaire, parce que nous agissons sous sa direction, avec les services de la Police Nationale, des douanes, les entreprises privées, les élus. Nous venons d'adresser à l'ensemble des 30 000 élus adhérents de l'Association des Maires de France un dispositif d'auto évaluation cyber qu'on a appelé immunité cyber. En dix questions, l'élu peut avoir un diagnostic et, le cas échéant, se rapprocher de la Gendarmerie. Il faut un outil pédagogique, simple, lisible. Car le cyber, reste assez nébuleux dans l'esprit du public. Mais il suffit de quelques chiffres pour appréhender la gravité de la délinquance en la matière : au niveau international, c'est mille milliards de dollars de préjudice. Le nombre de plaintes déposées en 2020 a augmenté de 20 % par rapport en 2019. En 2021, au premier semestre, on est déjà à 28 % d'augmentation. Or seule une affaire sur 250 donne lieu à un dépôt de plainte. C'est devant cette ampleur qu'il est urgent de passer à un vrai travail collaboratif. Particulièrement au niveau international car on a bien compris que les frontières n'existent pas en matière de délinquance cyber. Or, je suis très agréablement surpris par l'esprit de collaboration qui existe au plan international. Notamment d'un certain nombre de pays qu'on n'aurait pas spontanément cité dans les pays les plus collaboratifs.

Proximité ComCyberGend

Il faut bien comprendre que deux types de délinquants sont présents dans le domaine cyber. Les hackers extrêmement chevronnés, du très haut du spectre, s'attaquent aux grosses structures. Mais toute une population beaucoup moins chevronnée

1 Institut de Recherche Criminelle de la Gendarmerie Nationale

2 ST(SI)² - Service des Technologies et des Systèmes d'Information de la Sécurité Intérieure, dit STSI carré

s'inscrit dans un vrai cadre mis en place par les délinquants. Celui qui vend la vulnérabilité, celui qui vend la puissance de calcul, celui qui vend le système pour blanchir l'argent, etc. Cette délinquance de masse fait le même calcul que tous les délinquants, la balance du ratio risques et revenus. La cyberattaque, la cybercriminalité, cela rapporte et c'est moins compliqué, moins risqué qu'un acte criminel comme un trafic de stupéfiant.

Il y a aussi tout ce qui se passe sur les réseaux sociaux, la cybermalveillance, la diffamation, le harcèlement.

C'est ce constat et cette préscience de l'importance de ce monde cyber qui amène la création du Comcybergend.

Investigation ComCyberGend