PV Audition
Didier Tisseyre (COMCYBER)

Didier Tisseyre, Général, Commandant la cyber-défense des Armée.

Présentation et mission

Le Commandement de la cyber-défense (COMCYBER) poursuit trois missions principales:

1) La **protection et la défense** des systèmes d'information du Ministère des Armées (de ses outils et opérations militaires). Cette mission revient à assurer la résilience de systèmes militaires face aux agressions, pour garantir la défense du territoire national, de la population et des intérêts fondamentaux de la nation.

2) L'**identification et la planification** d'opérations militaires dans le cyber-espace, nouvel espace de conflictualité. Le COMCYBER a pour objectif d'identifier les acteurs malveillants investissant l'espace numérique à des fins violentes et de mener des opérations militaires strictement défensives.

Pour contrer ce type d'attaques, une opération est découpée en plusieurs phases. Il faut faire de la veille, analyser et caractériser pour savoir s'il s'agit d'une véritable organisation qui vise à nuire et à désinformer. Les phases qui suivent la caractérisation de l'attaque sont les suivantes:

- *Fact-checking* / *debunking*
- Mise en contexte et présentation des trouvailles de l'analyse et des recherches
- Mise au point du contre-discours

3) La **coordination** du recrutement de la cyber-défense, des parcours de carrière (formation et entraînement des forces de cyber-défense du Ministère des Armées), du développement d'outils techniques, des doctrines d'emploi de l'ensemble de ces systèmes, etc.

Le COMCYBER est composé de 3,500 cyber-combattants pour couvrir la totalité du spectre numérique.

L'ampleur de l'enjeu de la cyber-défense et l'augmentation des attaques tant en quantité qu'en qualité font du recrutement et de l'amélioration des outils techniques des enjeux stratégiques pour le COMCYBER.

Coopération entre le COMCYBER et les autres services

Comment la société démocratique peut se défendre contre des manipulations et ingérences?

Le travail du COMCYBER se fait de manière relativement étanche par rapport aux autres outils que l'État a mis en place pour lutter contre les perturbations numériques de la vie démocratique (Pharos, Viginum) lorsqu'il n'y a pas de lien direct avec les questions militaires. Le périmètre d'action du COMCYBER est relativement circonscrit. Il ne mène aucune action sur le territoire national.

En revanche, le COMCYBER peut procéder à des partages de connaissances sur les acteurs identifiés, les modes opératoires, les stratégies employées, etc. avec d'autres organismes étatiques chargés d'analyser certains phénomènes malveillants en ligne (protocole avec Pharos).

Par exemple, lorsque le COMCYBER était chargé d'analyser la propagande de Daesh et lorsque des liens avec le territoire national pouvaient être établis (grâce à l'analyse et aux outils), ces informations étaient directement transmises au Ministère de l'Intérieur.

Il existe également une coordination avec les services tels que Viginum mais les modalités de collaboration n'ont pas encore été fixées. Si l'objectif est le même, si les démarches peuvent être complémentaires, les périmètres d'action restent différents.

Négociations avec les GAFAM

Didier Tisseyre note une progression significative du dialogue avec les GAFAM, beaucoup plus réactifs. En 2017, les discussions n'étaient pas évidentes. L'identification et le pointage de comptes problématiques via Pharos ne suscitaient que très peu de réaction des réseaux sociaux notamment. Aujourd'hui, on voit que les GAFAM prennent de plus en plus leurs responsabilités sur ces questions en réduisant notamment le délai de retrait d'un contenu (passé de 1 semaine à 1 jour, voire 1h selon le sérieux de la menace).

Quelle est la raison de ce changement de politiques?

L'accumulation des événements, l'environnement médiatique, le développement commercial et donc les risques pour l'image de marque ont poussé à ce changement.

La question du chantier de coordination avec l'international
Dans le cadre de l'OTAN ainsi que de l'UE, de nombreuses entités et centres d'excellence travaillant sur les menaces hybrides et la guerre de l'information par le numérique ont émergé. La coopération internationale doit se poursuivre.

Nature des opérations du COMCYBER
Les opérations menées par le COMCYBER sont toujours des contre-opérations qui se font dans un cadre légal très strict.
Face à une attaque, la riposte n'est pas envisageable (impossibilité de créer des *fake news* pour porter atteinte et se venger de l'attaquant).

En quoi consistent les stratégies de "déception" (qui rentrent dans le cadre de la Doctrine militaire de lutte informatique d influence, selon les déclarations récentes de la Ministre)?

Il s'agit de stratégies de ruse militaire, c'est-à-dire de faire croire à un ennemi militaire qu'on va mener tel type d'opérations. Cette stratégie est cadrée juridiquement et se distingue de la perfidie (faire croire que l'on est blessé pour pouvoir mieux attaquer). Il s'agit d'appliquer ces principes dans le cyber-espace.