La boîte à outils des gendarmes du Net pour lutter contre la Cybercriminalité

	La boîte à outils des gendarmes du Net pour lutter contre la Cybercriminalité

Installé au sein du pôle judiciaire de la gendarmerie nationale à Cergy-Pontoise, le centre de lutte contre les criminalités numériques (C3N) utilise une palette d'outils pour patrouiller sur le web et détecter toutes sortes d'infractions en ligne.
Depuis un an, l'unité lutte de manière active contre la propagande djihadiste et l'apologie du terrorisme. Elle s'est dotée pour cela de nouveaux outils et a renforcé ses équipes.
« Nous sommes un peu la Bac du net. Notre travail consiste à patrouiller sur Internet pour détecter des infractions », explique le colonel de gendarmerie **Nicolas Duvinage**, chef du centre de lutte contre les criminalités numériques. Cette entité, baptisée le **C3N**, rassemble 35 militaires. Elle est installée au Pôle judiciaire de la gendarmerie nationale (**PJGN**), dont les nouveaux locaux se situent à Cergy-Pontoise (Val d'Oise).
Le C3N mène trois principales missions : il anime et coordonne le réseau **CyberGend,** déployé sur tout le territoire, effectue du renseignement criminel (pour réaliser une cartographie et une typologie des auteurs et des victimes et détecter les modes opératoires émergents) et réalise des enquêtes judiciaires pour détecter les fameuses infractions commises en ligne. Dans le cadre de cette mission, les gendarmes interviennent dans plusieurs cas : pour les atteintes aux stades (attaques informatiques), les atteintes aux biens (contrefaçon), et les atteintes aux personnes (porno-pédographie). *« Depuis janvier 2015, nous participons également de manière active à la lutte contre la propagande djihadiste et l'apologie du terrorisme. Nous nous inscrivons dans une activité plus pérenne dans ce domaine»,* confie le colonel Nicolas Duvinage, avant de poursuivre : *« Le but n'est pas simplement de fermer un site ou de retirer des tweets, mais d'identifier les auteurs des tweets et de les interpeller pour les juger ».*

OsintLab pour patrouiller sur Twitter
35 personnes pour patrouiller sur la toile cela fait peu… Les équipes se sont donc équipées d'une palette d'outils de surveillance automatique ou semi-automatique. Un investissement logiciel qui représente plusieurs centaines de milliers d'euros par an. Parmi ces outils, le logiciel **OsintLab** développé par **Thales**et acheté en 2015. Celui-ci permet de sillonner **Twitter** en s'appuyant sur des mots clefs. *« Cet outil nous a permis de mener plusieurs dizaines d'enquêtes judiciaires au travers desquelles nous avons pu identifier des personnes radicalisées »,* assure le colonel. Après avoir « logé » ces personnes, les équipes du C3N transfèrent le dossier à l'échelon spécialisé ou l'échelon territorial compétent, qui se chargera de réaliser l'interpellation.

Advestisearch pour identifier les primo-diffuseurs
Le C3N utilise également le logiciel **Advestisearch** d'**Hologram Industries**, qui permet de rechercher et d'identifier des contenus illégaux et illicites sous forme de texte, d'image ou de vidéo. *« Grâce à une image fournie en entrée, nous pouvons trouver en sortie des images similaires. Par exemple, lorsqu'une équipe de gendarmes récupère une vidéo de 10 secondes, l'outil nous permet de retrouver la vidéo complète. Cela nous permet aussi de détecter les primo-diffuseurs »,* détaille le colonel.

Et bientôt un *Scraper Deep Web* maison
Le C3N n'utilise pas uniquement des logiciels « sur étagère », mais développe également ses propres outils. L'unité s'attèle, par exemple, à mettre au point son propre *Scraper Deep Web*, un outil qui permet de collecter automatiquement des petits morceaux d'information sur des réseaux comme **TOR.** Une démarche qui rappelle le projet **Memex** mené par la **Darpa.** L'agence pour les projets de recherche avancés de défense américaine a, en effet, récemment créé un « *Google du Deep Web* » afin d'aider la police dans ses enquêtes en tout genre.

Le C3N s'emploie également à scruter les jeux en ligne. *« Les auteurs détournent de plus en plus les jeux en ligne comme **Clash of Clan**, **Call of Duty** ou encore **Oh My Dollz** »*, assure le spécialiste. *« Sur Clash of Clan, par exemple, nous avons identifié en 2015 plusieurs dizaines de cas d'apologie du terrorisme et de menaces d'attentats ».*
Outre les logiciels, le C3N mise également sur les compétences humaines. L'unité a récemment recruté plusieurs officiers commissaires, dont un docteur en informatique, un ingénieur en électronique et un universitaire spécialiste des systèmes d'information.

Réagissez à cet article

Source : *Cybercriminalité : la boîte à outils des gendarmes du Net*