Défense : guerre informationnelle et cyberdéfense

Fiche méthode

(EMC 4e · La sécurité et la défense)

La démarche pour analyser une menace nouvelle

1. Je décris l'action. Qui agit (un État, un groupe, une personne) ? Avec quel moyen : la violence, un réseau informatique, l'information, la destruction d'une installation ?

2. Je nomme la menace et son but. Terrorisme, cyberattaque, manipulation de l'information ou sabotage ; pour terroriser, gagner de l'argent, voler des secrets, bloquer, détruire, tromper ou diviser.

3. Je trouve qui répond. L'ANSSI protège et répare, le COMCYBER défend les armées, Viginum détecte les ingérences, les enquêteurs et la justice poursuivent.

4. Je montre le rôle du citoyen et la limite démocratique. Gestes de sécurité, ne pas relayer, signaler ; mais une opinion critique reste libre.

Le réflexe — une menace nouvelle = un auteur, un moyen, un but, une réponse de l'État et des citoyens vigilants.

Cas 1 · Les nouvelles menaces

Réflexe — qui agit ? avec quel moyen ? sous le seuil de la guerre ?

Exemple. Plusieurs nuits de suite, des drones inconnus survolent une base militaire ; personne ne revendique.

Ni attentat ni déclaration de guerre : une **provocation** ou un espionnage possible, sous le seuil de la guerre ouverte. Sans auteur connu, l'**attribution** est difficile : c'est le propre d'une stratégie hybride.

Attention — une menace hybride ne commence pas par une déclaration de guerre.

Cas 2 · Les cyberattaques

Réflexe — argent, secrets, bloquer ou détruire ?

Exemple. En plein hiver, des pirates prennent la commande du chauffage d'un hôpital et l'éteignent.

Prendre le contrôle pour arrêter une installation : un **sabotage**. L'ANSSI aide l'hôpital à reprendre la main ; les enquêteurs cherchent les auteurs.

Attention — l'ANSSI protège et répare ; elle ne riposte pas.

Cas 3 · L'ingérence numérique étrangère

Réflexe — acteur étranger, contenu trompeur, diffusion artificielle, intérêts fondamentaux ?

Exemple. Des sites créés par une agence liée à un État étranger publient une fausse carte des bureaux de vote « fermés » ; des robots la relaient le jour du scrutin.

Acteur étranger, contenu faux, diffusion automatisée, vote visé : les **quatre critères** sont réunis. Viginum la caractérise.

Attention — une critique exacte, même venue de l'étranger, n'est pas une ingérence.

Cas 4 · Repérer une opération

Réflexe — la source, les comptes, le contenu, le moment.

Exemple. Un site nommé « info-prefecture-actu » annonce le rationnement de l'essence dès demain ; il existe depuis huit jours.

Deux indices sur la **source** : un nom qui imite un service officiel, un site tout récent. Je cherche l'annonce sur le site de la préfecture, je ne partage pas, je signale.

Attention — un seul indice ne prouve rien ; plusieurs ensemble doivent alerter.

Les pièges

- Croire qu'une menace hybride est une guerre déclarée : elle reste volontairement sous le seuil et ambiguë.
- Confondre l'ANSSI (protéger les réseaux de l'État et des opérateurs vitaux) et le COMCYBER (cyberdéfense des armées).
- Croire que Viginum supprime des contenus ou dit ce qui est vrai : il détecte et caractérise les ingérences.
- Appeler « ingérence » toute critique venue de l'étranger : il faut les quatre critères à la fois.

Ce document est la propriété intellectuelle de Ben, professeur particulier (benprofparticulier.fr), protégée par le Code de la propriété intellectuelle (art. L. 111-1 et L. 122-4). Il est mis à disposition pour un usage personnel de révision. Toute reproduction, diffusion, mise en ligne ou revente, totale ou partielle, sans autorisation écrite est interdite et constitue une contrefaçon (art. L. 335-2).