

Calid : Centre d'analyse en lutte informatique défensive

Date de publication : septembre 2011 (JDD 59)

Copyright : ECPAD

Durée : 2' 20"

Axe de travail : La réforme comme chantier permanent – Moyens humains, financiers et industriels

Fiche rédigée par Nghia Nguyen

PRÉSENTATION DE LA VIDÉO

Le Centre d'analyse en lutte informatique défensive (Calid) est la cellule en charge de la protection des réseaux informatiques et des systèmes d'information du ministère de la Défense (Mindef). Il s'inscrit dans une stratégie interministérielle que coordonne l'Agence nationale de la sécurité des systèmes d'information (Anssi). Il assure une veille sur les réseaux, identifie les virus et les neutralise. Sa protection n'est pas limitée à la seule administration du Mindef ; elle couvre aussi les systèmes d'information utilisés par les forces armées, de la transmission des données à l'emploi des systèmes d'armes. La lutte informatique défensive se développe au plus près des unités et des théâtres d'opération.

CONTENUS COMPLÉMENTAIRES

La cyberdéfense est une priorité nationale. Elle est indispensable à la protection des secrets politiques, économiques, scientifiques, industriels et militaires qui garantissent l'indépendance de la France.

Elle assure aussi directement la protection des infrastructures et des réseaux nationaux dans une société où toute gestion est désormais informatisée. Une cyberattaque peut désorganiser les opérateurs d'un ou de plusieurs réseaux, interrompre un service, détruire une infrastructure en provoquant un accident technologique de grande ampleur. Par le vol de données, les cyberattaques s'inscrivent dans l'espionnage politique et économique.

Les États organisent régulièrement des exercices de cyberdéfense interministériels, afin de tester la résilience de leurs institutions, infrastructures et réseaux (Piranet en France, Cyber Storm aux États-Unis).

INTÉRÊT PÉDAGOGIQUE DE L'EXTRAIT

La cyberdéfense s'inscrit dans la réforme de la défense nationale qui a débuté au cours des années 1990 et illustre le chantier permanent qui la caractérise. Elle vise à assurer la sécurité de la société civile ainsi que celle des armées françaises, de l'échelle nationale aux

échelles européenne et mondiale. L'enjeu de cette lutte est aussi la sensibilisation des individus à un devoir de protection des données quelles qu'elles soient, ainsi que l'acquisition de réflexes de sécurité devant un ordinateur.

COMPÉTENCES MOBILISÉES

- Savoir expliquer ce qu'est la cyberdéfense
- Maîtriser différents langages (vidéo : lecture des images)
- Identifier, classer, confronter, organiser et synthétiser des informations
- Mener à bien une recherche personnelle

NOTIONS CLÉS

- Cyberdéfense/cybersécurité
- Cybermenace/cyberattaque
- Espionnage/renseignement

EXPLOITATION PÉDAGOGIQUE DE LA VIDÉO

QUESTIONNEMENT

1. Qu'est-ce que le Calid ? Avec qui cet organisme collabore-t-il ?
2. Dans le cadre de la cyberdéfense, à quelles échelles le ministère de la Défense agit-il ? Que doit-il protéger ?
3. Quelles infrastructures vitales peuvent être atteintes par des cyberattaques ? Contre ces attaques, quel est le rôle du Calid ?
4. Quelles sont les fonctions du personnel du Calid ? Comment sont traités les virus ?
5. Dans le cadre des opérations menées par des unités de combat, comment agit le ministère de la Défense par l'intermédiaire du Calid ? Pourquoi ?

BILAN

En prenant appui sur les informations de la vidéo, expliquez le rôle du Calid dans le cadre de la cyberdéfense de la France, à l'échelle nationale et internationale.

POUR ALLER PLUS LOIN

Recherches autonomes sur la sensibilisation à la cyber-sécurité, par une réflexion sur deux thèmes : les cyber-attaques et la mise en ligne de données personnelles.

COLLÈGE ET LYCÉE

- Qu'est-ce qu'une cyberattaque : types, formes, vecteurs ?
- Un ordinateur infecté peut servir de relais à une cyberattaque à l'insu de son utilisateur. Comment utiliser une messagerie électronique ?
- Quels dangers présentent les périphériques de type clés USB, mais aussi les Smartphones ?
- En quoi la mise en ligne de données personnelles peut menacer un individu, une entreprise, un réseau ?
- Quels doivent être les réflexes de sécurité sur un blog, un forum communautaire, un réseau social ?

RESSOURCES**BIBLIOGRAPHIE**

- Nicolas ARPAGIAN, *La Cybersécurité*, Paris, PUF, 2010.
- Nicolas ARPAGIAN, *La Cyberguerre : la guerre numérique a commencé*, Paris, Vuibert, 2009.
- Bertrand BOYER, *Cyberstratégie : l'art de la guerre numérique*, Paris, Nuvis, 2012.
- Laurence IFRAH, *L'Information et le Renseignement par Internet*, Paris, PUF, 2010.
- Olivier KEMPF, *Introduction à la cyberstratégie*, Paris, Economica, 2012.
- Daniel VENTRE, *Cyberattaque et cyberdéfense*, Paris, Hermès sciences publications-Lavoisier, 2011.
- Daniel VENTRE, *Cyberespace et acteurs du cyberconflit*, Paris, Hermès sciences publications-Lavoisier, 2011.
- Daniel VENTRE (dir.), *Cyberguerre et guerre de l'information : stratégies, règles, enjeux*, Paris, Hermès sciences publications-Lavoisier, 2010.

SITOGRAFIE

- Page Cyberdéfense sur le site du ministère de la Défense : www.defense.gouv.fr (rubriques Enjeux).
- Site Prévention des risques majeurs : www.risques.gouv.fr.
- Site de la Sécurité informatique : www.securite-informatique.gouv.fr.