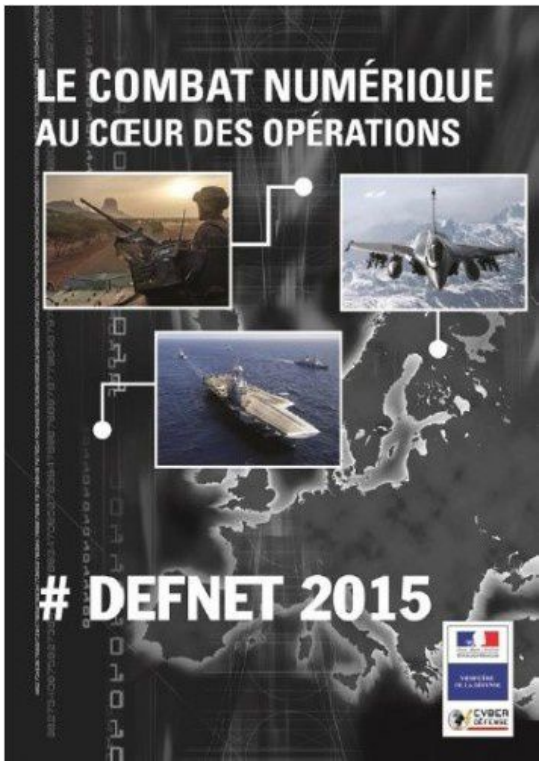
Deux bâtiments de notre marine nationale victime d’une cyberattaque sans précédent | Le Net Expert Informatique



Deux bâtiments de notre marine nationale victime d’une cyberattaque sans précédent

Vengeance de Vladimir Poutine ? Malveillance d'un hacker jihadiste ? On ne sait pas… Toujours est-il que deux bâtiments de notre marine nationale, le « Mistral » et son jumeau le «Tonnerre », actuellement en opérations en Méditerranée, viennent de faire de l'objet de cyberattaques simultanées. Leurs ordinateurs de bord ont été infectés par un virus informatique, générant un dysfonctionnement du SCADA, le système de contrôle automatisé qui permet gérer les principales fonctions de ces bateaux de guerre, à commencer par leurs radars et leurs systèmes d'armes. Un groupe d'intervention rapide composé de six membres de nos forces spéciales de cyberdéfense est en cours de déploiement sur les deux navires afin de résoudre la crise au plus vite.

Jusqu'au 27 mars, ce second exercice interarmées doit valider les choix de la chaîne de cyber-défense des armées françaises. Les administrations et opérateurs vitaux sont également concernés.

La cyberdéfense monte en puissance au sein des armées françaises avec la tenue jusqu'au 27 mars de DEFNET 2015, le second exercice interarmées grandeur nature consacré à ce thème.
« Il s'agit d'entraîner l'ensemble de la chaîne de cyber-défense » explique Le lieutenant-colonel Stéphane Dossé, le directeur de l'exercice, qui précise : « Il ne faut pas voir la cyber-défense comme un grand show hollywoodien. C'est un travail opérationnel du quotidien où il faut maintenir et renforcer une ligne de défense, comme dans l'armée de terre ».
Dans la forme, on risque donc d'être bien loin de la vidéo promotionnelle publiée par le Ministère de la Défense en février dernier sur la cyber-guerre : pas de terroristes encagoulés tapis dans l'ombre, pas de missiles expédiés en salve depuis un bâtiment de marine, pas de sergent chef Néo pour prendre à bras le corps la Matrice.
'La cyberdéfense : le combat numérique au coeur des opérations ', vidéo promotionnelle publiée en février 2015 par le Ministère de la Défense.

Un premier exercice avait eu lieu en octobre dernier, avec « un thème simple, sur un seul lieu ». DEFNET 2015 s'articule lui sur une dimension multi-sites. Sept sites militaires sont concernés, ainsi que deux bâtiments de la Marine nationale.
Le scenario de DEFNET 2015 simule, dans un contexte international fictif, des menaces et des attaques cyber multiples contre plusieurs sites sur des thèmes très différents, mentionne le communiqué de presse du Ministère de la Défense. Il associe les spécialistes de cyberdéfense des unités interarmées et des trois armées.
SI militaire, opérateurs vitaux et administrations
Le Ministère de la défense définit la cyberdéfence comme « l'ensemble des actions défensives et offensives conduites dans le cyberespace pour garantir le bon fonctionnement du ministère de la Défense et l'efficacité de l'action des forces armées en préparation ou dans la planification et la conduite des opérations ».
Mais dans le cadre de cet exercice, le périmètre de protection couvre en plus des systèmes d'information militaires, les opérateurs d'importance vitale et les administrations, raison pour laquelle l'Anssi est associée au projet.
A noter que cet exercice est l'occasion de tester le nouveau modèle de réserve cyber. Il s'agit d'accueillir des équipes de volontaires sur des sites militaires, simulant des sites d'intervention. Des équipes d'expérimentation sont constituées d'un réserviste des armées, d'un ou deux enseignants et de 10 à 12 étudiants en informatique et télécommunication d'un niveau bac+ à bac+5 (CentraleSupélec, Telecom Paris Tech ou encore l'Epita sont partenaires).
Elles devront effectuer un travail d'éradication de code malveillant et de réinstallation de système. L'exercice rassemble en tout un effectif de 580 personnes.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://www.zdnet.fr/actualites/defnet-2015-un-exercice-de-cyberdefense-multi-sites-est-en-cours-39816640.htm
Par Guillaume Serries