

Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2018)
Heft: [2]: Numéro Thématique 2

Artikel: La France muscle sa cyberdéfense
Autor: Papaemmanuel, Alexandre
DOI: <https://doi.org/10.5169/seals-823445>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. [Siehe Rechtliche Hinweise.](#)

Conditions d'utilisation

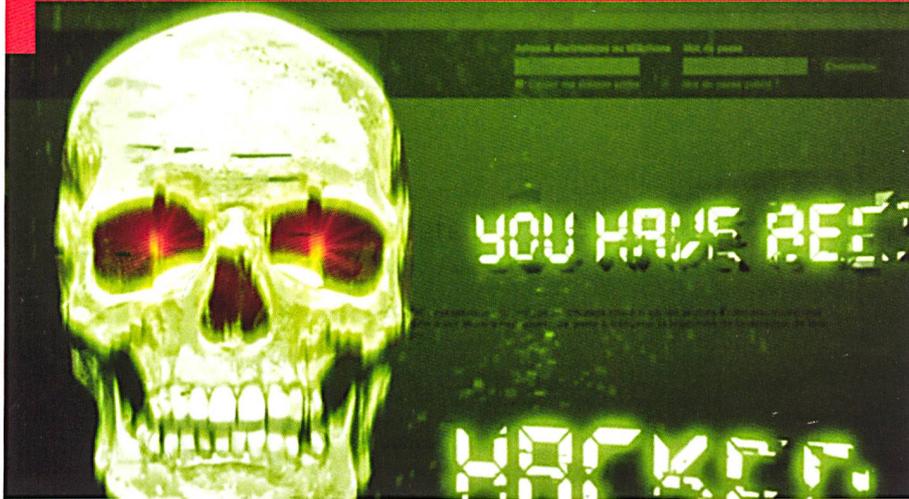
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. [Voir Informations légales.](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. [See Legal notice.](#)

Download PDF: 30.03.2025

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>



«You are hacked»: si ce message s'affiche c'est très mauvais signe! (Capture d'écran vidéo site du ministère de la défense <http://www.defense.gouv.fr/portail-defense/enjeux2/la-cyberdefense/la-cyberdefense>)

Cyber

La France muscle sa cyberdéfense

Alexandre Papaemmanuel

TTU Europe

L'ère de la cyberguerre est déjà bien entamée. Ce jeudi 15 février 2018, le ministère des Affaires étrangères britannique, soutenu par la Maison Blanche, vient d'accuser la Russie d'être derrière la cyberattaque *NotPetya*, au printemps 2017. Les cibles principales de cette attaque d'un nouveau genre? Les secteurs financiers, énergétiques et gouvernementaux ukrainiens. Sa «*conception sans discernement a entraîné sa propagation*» à travers le monde, accuse le Gouvernement britannique, multipliant ainsi les victimes collatérales.

Ces graves accusations s'appuient sur un rapport technique du centre national de cybersécurité, une division du *Government Communications Headquarters*, l'un des services de renseignement spécialisés dans les interceptions. Pour ces derniers, c'est l'Armée russe qui est responsable de cette attaque qui a coûté «*des centaines de millions de livre sterling*». Le quotidien *Le Monde* chiffre, pour sa part, les dégâts à plus d'un milliard d'euros. Le Gouvernement russe a démenti être responsable de cette attaque.

Des victimes en France

En France, le logiciel malveillant *NotPetya* a fait plusieurs victimes, le constructeur automobile Renault mais aussi l'industriel Saint-Gobain. Ce spécialiste du bâtiment a estimé l'impact de l'attaque à 250 millions d'euros sur ses ventes et à 80 millions d'euros sur le résultat d'exploitation! Contrairement aux *Fives Eyes* (l'Australie, la Nouvelle-Zélande et le Canada) qui se sont également associés à l'accusation britannique, la France n'a pas choisi d'aller sur le terrain délicat de l'attribution de cette attaque.

«*L'attribution des cyberattaques complexes demeure très difficile. Il est très ardu de récupérer une preuve scientifique formelle pour imputer l'attaque à quelqu'un*

ou une organisation. Nommer l'ennemi est un acte politique fort. Cela complexifie grandement les règles d'engagement.» Alexandre Papaemmanuel, directeur sécurité et renseignement intérieur chez Sopra Steria, à *L'Essor*.

Ce qui ne veut pas dire que les pouvoirs publics ne font rien. Ils mettent au contraire les bouchées doubles pour muscler la cyberdéfense. Coup sur coup, deux documents viennent de donner un coup de fouet à l'armée numérique française: la loi de programmation militaire et la *Revue stratégique de cyberdéfense*.

La loi de programmation militaire, présentée le 8 février 2018 en Conseil des ministres, donne la part belle à la cyberdéfense: 1,6 milliard d'euros seront consacrés à la lutte dans le cyberspace d'ici 2025 avec, comme objectif, de recruter 1'000 cybercombattants de plus, pour arriver à un total de 4'000 cybersoldats. En tout, 1'500 recrutements pour la cyberdéfense et le numérique sont prévus dans les six ans à venir, soit un quart des hausses d'effectifs prévues.¹

Menace cyber

L'utilisation des réseaux sociaux par les Russes sur le front ukrainien à des fins de propagande et d'opérations cyber sur les smartphones des militaires adverses ne serait que la face émergée d'un mode opératoire autrement plus ambitieux. Lors de la conférence sur la cyber sécurité qui s'est déroulée à Park City dans l'Utah, Dmytro Shymkiv, responsable adjoint de l'administration présidentielle ukrainienne, a déclaré que le renseignement russe avait mis en place un *pool* de psychiatres chargés d'exploiter les échanges numériques de plusieurs personnalités clés

¹ *L'Essor de la Gendarmerie nationale* française, 22 février 2018. Pour en savoir plus: <https://lessor.org/france-muscle-cyberdefense/#iLYW9UgkLisQiUEp.99>.

dans la chaîne de commandement, afin d'en identifier les vulnérabilités comportementales pour de futures opérations de manipulation et de neutralisation.

A la fin du mois de novembre 2017, un groupe de hackers commercialisera pour 50 dollars un boîtier de 24 grammes, capable non seulement d'injecter un *malware* sur un réseau via les connexions de n'importe quel périphérique, mais aussi d'identifier les paquets de données critiques avant de les enregistrer sur une carte mémoire. Une réelle menace pour l'industrie de défense.²

A. P.

THE CYBER THREAT IS REAL

■ BEING CYBER SECURE IS EVERYONE'S RESPONSIBILITY

DON'T TAKE THE PHISHING BAIT!
Always verify sources of emails and the links in emails. If you're directed to a site for an online deal that looks too good to be true, it probably is.

WHEN IN DOUBT, THROW IT OUT
Don't open suspicious links in emails, tweets, posts, messages or attachments, even if you know the source.

DON'T CONNECT UNAUTHORIZED DEVICES
Unauthorized devices may contain software that can allow an attacker inside the Navy's network.

REMOVE YOUR CAC!
Remove your CAC or lock your computer. Don't make it easy for an inside attacker by leaving your computer unlocked when you're not using it.

MAKE YOUR PASSWORDS STRONG
Don't use easily guessed or weak passwords, and safeguard them so they can't be stolen.

SAFEGUARD YOUR PII
Attackers can use information they've obtained about you to appear legitimate so they can trick you into surrendering data they need to breach our networks and systems.

DON'T USE P2P PROGRAMS
Don't use peer-to-peer (P2P) file sharing programs. These programs can spread bad software inside the Navy's network defenses.

DON'T MISUSE SYSTEMS
Don't use systems in an unauthorized way. The Navy has established policies to protect itself from compromise. Don't put others at risk by using systems in ways that aren't authorized.

Source: OPNAV N2/N6

News

La cyber armée de Pyongyang

Malgré le scepticisme de certains experts, la Corée du Nord aurait mis en place un redoutable dispositif cyber offensif, au point de déclencher, le 2 octobre 2017, une opération de rétorsion du *Cyber Command* américain. L'enquête sur l'attaque de la réserve fédérale à New York l'année dernière, sur Sony et Channel 4, qui travaillait sur une série décrivant la vie quotidienne des Nord-Coréens, le réseau Bitcoin en Corée du Sud, et le *malware* du mois de mai 2017, qui a détruit les serveurs de plusieurs administrations et groupes occidentaux, a permis de démontrer que Pyongyang disposerait d'une entité de 6'000 experts et d'une arme cybernétique similaire à celle utilisée par Téhéran pour attaquer le groupe saoudien Aramco. Jang Kil-Su et le général No Kwang-Chol pourraient être à la tête de cette cyber armée.

L'attaque américaine semble avoir déclenché plusieurs actions de rétorsion. Le groupe Symantec a détecté 48 heures plus tard une intrusion majeure sur les réseaux énergétiques européens et américains, préalables à des actions de sabotage. Puis, selon le député Lee Cheol-Hee, le plan d'opération américano-coréen 5015, destiné à frapper Pyongyang, aurait été dérobé de manière numérique. Les sous-traitants australiens travaillant sur les avions C-130, F-35, P-8 et le missile de croisière JDAM auraient perdu plus de 30 Go d'informations classifiées. La société de crédit américaine Equifax s'est fait subtiliser les informations personnelles et bancaires de 143 millions de clients. Enfin, les messageries de plus d'une centaine de parlementaires britanniques auraient été piratées, mais surtout celle de Theresa May, pourtant sécurisée directement par le GCHQ ...! Medias, banques, industriels et parlementaires sont donc les nouvelles cibles de la guerre cyber, une guerre qui bouscule les rapports de forces traditionnels.

TTU N° 1080, 18 octobre 2017.

