



## Les cyberattaques: les pays occidentaux victimes de l'Otan, de leurs alliés et du dilettantisme?

Par [Olivier Renault](#)

Mondialisation.ca, 15 juin 2021

[Observateur continental](#)

Région : [L'Europe](#)

Thème: [Guerre USA OTAN](#), [Services de renseignements](#)

Par une publication sur Twitter, le compte officiel de l'état-major français des Armées, avec plus de 166 000 abonnés, a partagé récemment une photo mettant en scène un exercice sensible concernant la sécurité publique. Une feuille, affichée à un mur et bien visible, a dévoilé un mot de passe sur le document publié censé être réservé en interne aux experts en charge de la sécurité de la France.

Cette grave erreur soulève des questions sur la sécurité stratégique de la France, mais aussi sur les accusations de pays de l'Otan, dont la France, envers la Chine et la Russie de hacker leurs systèmes secrets.

«Pour faire face aux risques naturels, technologiques ou sanitaires, ainsi qu'aux menaces qui peuvent peser sur la population, les acteurs de la sécurité se réunissent régulièrement dans des exercices proches du réel», a publié, accompagné d'une photo, l'état-major français des Armées sur son compte Twitter le 8 juin dernier. Sur la photo, on peut voir un mot de passe en clair. L'affaire provoque une grande inquiétude auprès des observateurs d'autant plus qu'avant de s'envoler pour l'Europe et la Suisse, Joe Biden [a déclaré](#) à la question, «Vous attendez-vous à ce que Poutine parvienne à s'entendre avec vous sur les cyberattaques?» : «Qui sait à ce stade? Ce sera le sujet de notre discussion».

La bourde réalisée par la France montre déjà que les Etats-Unis devraient, avant tout, chercher chez ses alliés surtout qu' Edward Snowden [a annoncé](#) l'implication de Joe Biden dans le scandale d'espionnage en UE.

Les erreurs à chercher chez les alliés des Etats-Unis. En fait, à voir la grave erreur réalisée par l'armée française, le danger de fuite viendrait essentiellement du fait du manque du sérieux du travail des services occidentaux, eux-mêmes. En publiant une photo montrant l'identifiant et le mot de passe d'une «session Windows» scotchée, en clair et non flouté, sur une armoire technique, on peut, en outre, se demander si les experts en question pourront, le jour venu, faire face aux risques technologiques et donc aux menaces qui peuvent peser sur le pays.

Le site Next INpact [indique](#) que «c'est grâce à l'alerte donnée par par @TomDAAVID, un étudiant en M1 à l'ENS de Lyon qui s'intéresse aux enjeux de santé publique des armes, munitions et substances en matière de maintien de l'ordre (ce pourquoi il avait vu passer le tweet)», que «le compte Twitter de l'état-major français a retiré le tweet», avant de le

republier tel quel, puis de le réeffacer une seconde fois». Si au travail, ces experts font une telle erreur, qu'en est-il durant leur vie privée?

Microsoft dans l'armée française! Au-delà de cette fuite faisant douter de la qualité des experts français sur le terrain de la sécurité, on constate que ces derniers utilisent un système d'exploitation américain du géant Microsoft qui est connu pour capter des informations dans des pays et de les donner aux services secrets américains tout en étant aussi connu pour avoir des failles utiles aux hackers.

D'ailleurs, en janvier 2020, l'Agence nationale de la sécurité (NSA), [avait contacté](#) Microsoft pour l'informer d'une faille de sécurité majeure dans Windows 10, montrant ainsi, encore une fois, la collaboration entre les deux entités. En mars dernier de 2021, la Maison Blanche, comme [l'indiquait](#) *Le Figaro*, mettait en garde les sociétés ou les structures d'Etat utilisatrices du logiciel Exchange de Microsoft en raison des failles de sécurité dans ses services de messagerie car cela permettait de voler les données de ses utilisateurs professionnels.

Microsoft avait désigné les hackers du groupe baptisé «Hafnium», une unité chinoise de cyber espionnage. Malgré les nombreuses mises en garde, un groupe en charge de la sécurité en France, utilise un produit Microsoft. Plus que des menaces venant de l'étranger, elles viennent du leader de l'Otan en personne, sans oublier que ces alliés entre eux s'espionnent. Clément Beaune, secrétaire d'Etat auprès du ministre de l'Europe et des Affaires étrangères, chargé des Affaires européennes, a révélé, fin mai, que les Etats-Unis, le plus grand allié de la France, [ont écouté](#) les faits et gestes de plusieurs personnalités européennes dont des Français.

En mai dernier, la Chine [a accusé](#) Microsoft d'avoir collecté illégalement les données des utilisateurs chinois. Dès le mois de décembre 2019, la Chine avait déclaré vouloir supprimer tous les logiciels étrangers de son administration d'ici à 2022. Selon les *Echos*, «Pékin aurait, en effet, [demandé](#) à ses services de privilégier les fournisseurs locaux pour l'équipement informatique de ses administrations. Ce, tant en ce qui concerne les ordinateurs eux-mêmes que les logiciels utilisés». La France, elle, continue d'utiliser des logiciels étrangers dont Microsoft.

La publication de cette photo révélant un mot de passe d'un service de l'armée française au monde entier permet d'expliquer les causes fondamentales des fuites et autres interventions d'individus dans des systèmes sensibles français. Même les accusations d'avoir les preuves de l'ingérence russe dans la campagne de Macron en 2017, posent des questions. Est-ce qu'un membre de la campagne de Macron a négligé des principes de sécurité de base? En tout cas, «tous les tableurs que renferme une des archives les moins volumineuses de la publication [MacronLeaks] semblent, comme [indiqué](#) par le site Silicon, avoir été édités via une version de Microsoft Excel».

Microsoft qui comporte de nombreuses failles et qui travaillent avec le NSA, apparaît encore dans ce dossier. En juin 2013, l'ancien agent de la NSA Edward Snowden [a confirmé](#) que Microsoft travaille en étroite collaboration avec la NSA tout comme avec Google, Facebook. La fuite d'informations sensibles provient du dilettantisme affiché de pays de l'Otan et certainement de l'espionnage réciproque mené par ces derniers.

Olivier Renault

Articles Par : [Olivier Renault](#)

### A propos :

Olivier Renault, journaliste. Il travaillé, entre autres, pour RUE89, Die Junge Freiheit, des sociétés de production à Berlin et Hambourg pour la télévision allemande...

**Avis de non-responsabilité** : Les opinions exprimées dans cet article n'engagent que le ou les auteurs. Le Centre de recherche sur la mondialisation se dégage de toute responsabilité concernant le contenu de cet article et ne sera pas tenu responsable pour des erreurs ou informations incorrectes ou inexactes.

Le Centre de recherche sur la mondialisation (CRM) accorde la permission de reproduire la version intégrale ou des extraits d'articles du site [Mondialisation.ca](#) sur des sites de médias alternatifs. La source de l'article, l'adresse url ainsi qu'un hyperlien vers l'article original du CRM doivent être indiqués. Une note de droit d'auteur (copyright) doit également être indiquée.

Pour publier des articles de [Mondialisation.ca](#) en format papier ou autre, y compris les sites Internet commerciaux, contactez: [media@globalresearch.ca](mailto:media@globalresearch.ca)

[Mondialisation.ca](#) contient du matériel protégé par le droit d'auteur, dont le détenteur n'a pas toujours autorisé l'utilisation. Nous mettons ce matériel à la disposition de nos lecteurs en vertu du principe "d'utilisation équitable", dans le but d'améliorer la compréhension des enjeux politiques, économiques et sociaux. Tout le matériel mis en ligne sur ce site est à but non lucratif. Il est mis à la disposition de tous ceux qui s'y intéressent dans le but de faire de la recherche ainsi qu'à des fins éducatives. Si vous désirez utiliser du matériel protégé par le droit d'auteur pour des raisons autres que "l'utilisation équitable", vous devez demander la permission au détenteur du droit d'auteur.

Contact média: [media@globalresearch.ca](mailto:media@globalresearch.ca)