Mondialisation.ca
Centre de recherche sur la mondialisation

Les USA et la Russie sont ils déjà engagés dans une guerre numérique?

Ce serait une deuxième situation de MAD; plus instable, puisque les deux factions manœuvrent continuellement pour occuper la meilleure position et frapper la première.

Par Philip Giraldi
Mondialisation.ca, 12 juillet 2019
Checkpoint Asia 24 juin 2019

Région : États-Unis, Russie et CEI
Thème: Guerre USA OTAN

Bien que le cas de l'Iran fasse légitimement la une des journaux, deux autres histoires confirment que des zombies cannibales décérébrés ont pris le contrôle de la Maison-Blanche. La première émane de David Sanger, journaliste au New York Times, qui rapportait la semaine dernière l'introduction par les États-Unis dans le réseau électrique russe de logiciels malveillants [malware] destinés non seulement à donner un avertissement, mais aussi à être activé par mesure de rétorsion si le Kremlin poursuit ses efforts de guerre numérique.

Ce qui surprend dans cette histoire, c'est la désinvolture avec laquelle elle est présentée. Après tout, introduire un *malware* dans le réseau électrique de qui que ce soit pourrait constituer un acte de guerre. Pour toute réaction, la Maison-Blanche s'est fendue d'un tweet présidentiel : *«Il s'agit d'un acte de trahison virtuelle commis par un journal autrefois admirable, mais qui ne cherche désormais qu'une bonne histoire, même si elle doit nuire à notre pays...»,* omettant de préciser que cette histoire était fausse. En fait, si la trahison était avérée, cela pourrait donner à penser que l'article de presse dévoile justement ce qui aurait du rester classé *Top Secret*. C'est alors que Trump, ou l'un de ses conseillers, se rendant compte de la négligence, a enchaîné d'un nouveau tweet : *« ... ET EN PLUS C'EST FAUX ! »*

Si Sanger a bien travaillé, et que l'histoire est vraie, il convient de s'attarder sur plusieurs points. Tout d'abord, s'ingérer dans le réseau électrique d'un pays, dont dépendent de nombreuses infrastructures, est un acte extrêmement téméraire, surtout lorsqu'il est exposé dans la presse. Sanger a retracé la genèse de son récit, révélant qu'il y travaillait depuis plusieurs mois. Il écrit :

> Selon d'anciens et actuels responsables gouvernementaux, les États-Unis intensifient leurs incursions numériques dans le réseau électrique russe. Il s'agit de mettre en garde le président Poutine et de montrer que l'administration Trump s'autorise à faire usage de cyber-outils toujours plus agressifs.
>
> Au cours d'entretiens menés durant les trois derniers mois, différents haut placés ont évoqué le déploiement – maintenu secret jusque là – du code informatique américain dans de nombreuses cibles, dont le réseau électrique Russe. Cette botte secrète accompagne les discussions publiques portant sur

> les unités de désinformation et de piratage utilisées par Moscou lors des élections de mi-mandat de 2018. Les partisans d'une stratégie plus agressive, tels le Département de sécurité intérieure et le FBI ne l'espéraient plus; eux qui depuis plusieurs années avertissent le public que la Russie a introduit des logiciels malveillants susceptibles, en cas de conflit avec les États-Unis, de saboter les oléoducs, gazoducs, centrales électriques, et sources d'approvisionnement en eau.

Sanger développe :

> De haut responsables gouvernementaux, retraités ou actifs, affirment que depuis 2012 au moins les États-Unis placent des sondes de reconnaissance dans les systèmes de contrôle du réseau électrique russe. Mais aujourd'hui, la stratégie américaine prend une tournure plus offensive, par l'introduction toujours plus profonde et agressive de programmes malveillants potentiellement paralysants. Ce qui n'est en principe qu'un avertissement peut servir à mener des cyber-attaques en cas de conflit majeur entre Washington et Moscou. Le commandant du Cyber Command américain, le général Paul M. Nakasone, évoque ouvertement la nécessité de « se défendre » jusque dans les profondeurs des réseaux ennemis, pour montrer que les États-Unis sont prêts à réagir aux nombreuses attaques en ligne dont ils pourraient être la cible. John R. Bolton, le conseiller à la sécurité nationale du président Trump, affirmait quant à lui que les États-Unis envisageaient un nombre toujours croissant de cibles numériques potentielles, ne serait-ce que pour prévenir quiconque «tenterait une cyber-opération à notre encontre». « Ils n'ont pas peur de nous », se lamentait-il l'année dernière lors de sa confirmation devant le Sénat.

Si le récit de Sanger est avéré – il semblerait d'ailleurs qu'il contienne nombre d'informations crédibles, il signifie que les États-Unis veulent répondre œil pour œil aux attaques russe visant les réseaux électriques, essentiellement *«pour qu'ils aient peur de nous»*. Tout porte à croire que les deux pays sont déjà en guerre, et ce n'est dans l'intérêt de personne, d'autant que les signaux ainsi envoyés pourraient très rapidement faire dégénérer la situation. L'article précise étonnamment que le président Donald Trump ignore ce programme, qui peut pourtant mener tout droit à la Troisième Guerre mondiale. Ce qui conduit certains lecteurs à se demander pourquoi Sanger n'a pas été arrêté pour avoir divulgué des informations relevant de la sécurité nationale… contrairement à Julian Assange.

Philip Giraldi

Article original en anglais : Are US and Russia Already in a Cyber War? Checkpoint Asia, le 24 juin 2019.

Traduit par jj, relu par Olivier pour le Saker Francophone

La source originale de cet article est Checkpoint Asia

Articles Par : Philip Giraldi