



CHRONIQUES DES NOUVELLES CONFLICTUALITÉS



Opérations *Pinball* et *Secondary Infektion* : la contrefaçon au service de la désinformation

Par Danny Gagné

Alors que l'ingérence russe dans les élections américaines de 2016 a considérablement retenu notre attention ces dernières années, d'autres incidents semblables, mais tout aussi importants sont passés plus inaperçus. Loin d'être exceptionnelle, l'ingérence électorale semble être devenue la norme.

Le 22 avril 2020, la Pologne a été secouée par une intense controverse : une [lettre](#) publiée sur le site internet de la *Polish War Studies Academy*, la plus haute académie militaire du pays, critiquait la collaboration stratégique de ce pays avec les États-Unis. Loin d'être anodine, la missive, signée

de la main du brigadier général Ryszard Parafianowicz, figure de proue de l'armée polonaise et recteur de l'académie, dénonçait « l'occupation » américaine de la Pologne et critiquait le parti au pouvoir de laisser celle-ci perdurer. En réalité, la lettre en question était contrefaite, et

jamais le général Parafianowicz n'avait émis publiquement de tels propos. La Pologne venait d'être la cible d'une opération passablement sophistiquée.

Le moment choisi est caractéristique d'une tentative d'ingérence dans le processus politique d'un autre pays : non seulement la Pologne était en pleine campagne électorale en vue du scrutin du 10 mai, mais elle traversait aussi une crise politique puisque les partis d'opposition et le gouvernement ne s'entendaient pas sur la nécessité ou non de maintenir la date du scrutin en pleine pandémie. La remise en question de la posture stratégique du pays sur fond de campagne électorale houleuse poussa les services de renseignement polonais à pointer la Russie du doigt. Ce qui leur mit la puce à l'oreille : l'hésitation de l'OTAN à tenir l'opération *Defender Europe 20* prévue en juin, une simulation de guerre en sol polonais, à proximité de l'enclave russe de Kaliningrad. L'opération, dite défensive, est vertement critiquée par Moscou qui y voit plutôt les préparatifs d'une invasion.

Si l'ingérence russe dans les élections américaines de 2016 fut fortement médiatisée, beaucoup de cas européens ne font cependant pas les manchettes en Amérique du Nord. Pourtant, la Pologne venait de faire les frais d'une opération de désinformation de grande envergure, qui allait bientôt être surnommée *Operation Pinball* par la firme de cybersécurité américaine *Recorded Future*.

Opération Pinball

Plusieurs pays proches de la Russie ont également été visés par l'opération *Pinball*. Au mois d'avril, en Géorgie, où se chevauchent les sphères d'influence russe et américaine, un document rédigé (en apparence) par le ministre de la Défense de ce pays fut publié sur une page Reddit. Cette lettre, adressée au secrétariat général de l'OTAN, révélait que la Géorgie s'apprêtait à [céder](#) à l'Abkhazie des droits de propriété sur des instal-

lations hydroélectriques. L'Abkhazie, république autoproclamée indépendante au nord-est de la Géorgie et occupée militairement par la Russie, est un sujet de discorde entre les deux pays. Ladite lettre visait donc à laisser croire à un rapprochement entre la Russie et la Géorgie, un sujet qui divise autant les parlementaires que la population de ce pays.

En octobre 2019, plus de 2000 sites gouvernementaux et médiatiques furent victimes d'une attaque de type DDoS¹. Les États-Unis et le Royaume-Uni [attribuèrent](#) l'attaque au groupe de pirates APT28 (ou *Fancy Bear*) rattaché aux services de renseignement militaire russes. Sur de nombreux sites, une photo de Mikheil Saakashvili apparaissait avec la mention « I'll be back ». Saakashvili, président de la Géorgie de 2004 à 2013, vit actuellement en exil en Ukraine. Lors de son mandat, il prônait une adhésion de la Géorgie à l'OTAN² (projet dans les cartons depuis 1994). Or, plus récemment, des membres du parti au pouvoir ont commencé à discuter d'un rapprochement avec la Russie. Son éventuel retour, à moins d'un an de la tenue des élections parlementaires, troublerait le rendez-vous électoral.

En juin 2019, la Russie s'en prenait à la Moldavie, en recourant à la contrefaçon pour s'immiscer dans le processus politique moldave. L'identité de Mike Pompeo, secrétaire d'État américain, fut usurpée pour adresser une [lettre](#) contrefaite à Vladimir Plahotniuc, ancien président moldave, battu aux élections de février 2019. Selon ce document, la nouvelle présidente, Maia Sandu³, aurait été élue de manière anticonstitutionnelle et sa nomination serait condamnée par les États-Unis (accusations démenties par le département d'État américain). La Moldavie, la Géorgie et la

1 *Distributed Denial Of Service* : ce type d'attaque vise à compromettre l'accès à des systèmes informatiques ou à un site Internet.

2 La Géorgie est l'un des pays non-membres de l'OTAN collaborant le plus avec l'alliance, surtout depuis la signature du *Substantial Nato-Georgia Package* en 2014.

3 Sandu fut chassée du pouvoir cinq mois plus tard.

Pologne venaient ainsi d'être tour à tour frappées par des campagnes de désinformation et d'usurpation d'identité à des moments clés de leurs vies politiques respectives. Plusieurs autres pays, dont notamment l'Estonie, devaient aussi faire les frais de *Pinball*.

Opération *Secondary Infektion*

L'opération *Pinball* est aujourd'hui considérée comme la sœur cadette de l'opération *Secondary Infektion*, qui s'est déroulée entre 2018 et 2019. Encore ici, le mot d'ordre semblait le même : attaquer des pays vulnérables en période électorale. Ébranlée par la crise du Brexit, l'Europe a été la cible de la stratégie dite du *wedging* : la Russie a travaillé d'arrache-pied pour tenter de monter les membres de l'Union européenne les uns contre les autres. C'est ainsi que débuta *Secondary Infektion*⁴ (appellation utilisée par le *Digital Forensic Research Lab* du think tank américain *Atlantic Council*), une vaste campagne de fausses nouvelles diffusées à l'aide de *burner accounts*⁵ sur différents médias sociaux. Le Royaume-Uni fut alors la cible de prédilection.

Parmi les incidents les plus importants en lien avec le Brexit, on retrouve quelques cas notoires. Tout d'abord, entre mars 2018 et avril 2019, les projecteurs furent braqués sur l'Irlande du Nord. Le 22 mars, un compte Facebook fut utilisé pour partager auprès de quinze organes de presse européens une nouvelle selon laquelle des membres de l'IRA véritable⁶ avaient participé à la tentative d'assassinat de Sergei Skripal. En août de la même année, toujours en utilisant Facebook, un [courriel](#) soi-disant rédigé par Arlene Foster (cheffe du Parti démocratique

unioniste nord-irlandais), affirmait que l'Irlande du Nord allait obtenir un statut spécial au sein de l'Union européenne. Finalement, le 22 avril 2019, une publication fallacieuse, qui se voulait être un appel d'extrémistes musulmans à se joindre à l'IRA véritable, fut partagée sur Reddit puis de nombreuses fois sur Facebook.

D'autres pays alliés du Royaume-Uni furent instrumentalisés, autant en Europe qu'en Amérique. Twitter fut utilisé pour répandre une fausse nouvelle disant que les services secrets espagnols détenaient des informations sur un plan d'opposants au Brexit voulant [assassiner](#) Boris Johnson. Cette lettre contrefaite au thème étonnant a rapidement été dénoncée comme étant fautive, notamment parce qu'elle contenait une faute d'orthographe dans le nom du ministre qui était censé l'avoir rédigée. Du côté des États-Unis, l'identité du sénateur républicain de Floride, Marco Rubio, fut [usurpée](#) pour publier un *tweet* qui détaillait l'intervention des services de renseignement britanniques en faveur des démocrates en 2016 et leur intention de récidiver lors des élections sénatoriales de 2018.

Dans tous les cas, le *modus operandi* était le même. La création d'un faux compte sur les réseaux sociaux, suivi de la publication de la nouvelle, de l'utilisation d'autres comptes fictifs pour partager la même nouvelle et, peu de temps après, la fermeture du compte. Le 6 mai 2019, Facebook [annonçait](#) d'ailleurs avoir fermé 97 comptes suspectés d'être opérés par des groupuscules russes. 21 d'entre eux avaient été particulièrement actifs sur la question du Brexit.

Le Canada loin d'être en reste

Qu'en est-il du Canada? En juillet 2018, on apprenait que des [soldats canadiens](#) déployés en Lettonie dans le cadre de l'opération *Reassurance* étaient victimes d'une campagne de désinformation. De fausses nouvelles, diffusées à partir de sites internet hébergés en Russie, laissaient notamment entendre que les soldats habitaient des appartements de luxe aux frais des contribuables

4 L'opération *Infektion* remonte à la période soviétique et cherchait à répandre l'idée que le sida avait été créé en laboratoire par les États-Unis.

5 Des comptes (Facebook, Twitter, Pinterest, etc.) activés pour publier une nouvelle et ensuite fermés une fois la nouvelle partagée.

6 L'IRA véritable (RIRA) est une branche dissidente de l'IRA qui a refusé de signer le cessez-le-feu de 1997.

lettons. Dans le cas letton, l'incident survenait à moins de trois mois du scrutin présidentiel. Depuis l'annexion de la Crimée par Moscou, les États membres de l'OTAN situés aux portes de la Russie, les pays baltes notamment, sont davantage inquiets pour leur avenir. Petits États situés à la périphérie de l'Europe, ceux-ci font figure de cible idéale pour tester la solidité de l'alliance atlantique. Le Canada a donc indirectement fait les frais de ces opérations insidieuses visant avant tout l'opinion publique locale.

Les élections américaines auront lieu dans quelques mois et risquent de se dérouler dans un climat très volatile dû à la pandémie et l'affaire

George Floyd. Le Canada devra donc également garder un œil sur le scrutin présidentiel se déroulant chez son principal allié, car ses voisins du Sud pourraient encore une fois être la cible d'ingérence électorale étrangère.

Danny Gagné est chercheur à l'Observatoire des conflits multidimensionnels de la Chaire Raoul-Dandurand.

Pour en savoir plus sur la Chaire Raoul-Dandurand et ses travaux:

<https://dandurand.uqam.ca/>

