Par Christine Dugoin-Clément
Chercheuse à la Chaire Risque de l'IAE Paris-Sorbonne, à l'Observatoire de l'Intelligence Artificielle de Paris 1 Panthéon-Sorbonne.

INGÉRENCE ÉTRANGÈRE ET DÉSINFORMATION,

LES ÉVOLUTIONS LIÉES AUX TECHNOLOGIES DU NUMÉRIQUE

Les stratèges militaires ont depuis longtemps compris l'importance de la guerre informationnelle et du levier populaire qu'il constitue en complément du rapport de force. En effet, nombre d'auteurs y font référence, que l'on pense à Sun Tzu ou plus récemment encore, aux penseurs de l'Armée rouge qui, dès 1927 voyaient l'utilité de la guerre psychologique comme moyen de pression sur les populations derrière le front.

Dans le manuel sur le renseignement militaire paru à cette époque, il est stipulé que « *le sentiment politique de la population à l'arrière de l'ennemi joue un grand rôle dans les activités réussies d'un adversaire ; à cause de cela, il est extrêmement important de générer des sentiments parmi les populations contre l'ennemi et de les utiliser pour organiser des soulèvements populaires et des détachements de partisans* » (Shil'bakh and Sventsitskiy 1927).

Avec l'explosion des nouvelles technologies modernes, notamment le développement d'Internet et des technologies du numérique, le champ des possibles en matière d'influence a été décuplé, et les opérations mettant en danger les processus démocratiques se répandent dans le monde, par le biais de méthodes de plus en plus diverses.

Une démultiplication depuis 2016

En 2016, les soupçons d'ingérences russes dans le processus électoral américain participaient à une prise de conscience générale du risque pesant sur les processus démocratiques (Eady, Paskhalis et al. 2023). Cette prise de conscience fut telle que l'Union européenne appelait à la vigilance pour les scrutins européens de 2017, notamment par la voix de la Commissaire européenne à la justice, Věra Jourová, qui annonçait que le risque d'ingérence et de manipulation dans les élections n'avait jamais été aussi élevé (Stolton 2018).

Outre les pays occidentaux parmi lesquels le Canada (McCulloch 2024), la Grande-Bretagne (Del Vicario, Zollo et al. 2016), les Pays-Bas ou encore la France (Ferrara 2017), d'autres actions visant à influencer le résultat des élections pouvaient être observées, notamment en Asie lors des élections présidentielles de Taïwan en 2020 (Barss 2022, Wilson 2022), ou encore en Australie (Searight 2020) et en Nouvelle-Zélande (Fitzgerald 2018). Plus récemment, des « leaks » révélaient l'intérêt que le Kremlin portait à sa propre sphère informationnelle afin d'asseoir le résultat de l'élection présidentielle de mars 2024 (Roonemaa and Vunsh 2024).

Même si les périodes de campagnes électorales marquent souvent une intensification de l'ingérence, certaines opérations trouvent à s'inscrire dans le temps long. Leurs objectifs peuvent alors être multiples, mais participent généralement à façonner les opinions publiques pour qu'elles soient plus réactives sur des sujets clivants, ou plus sceptiques vis-à-vis des pouvoirs publics, quand il ne s'agit pas d'instiller le doute dans les personnes publiques, voire dans les processus démocratiques eux-mêmes.

En effet, perturber les processus électoraux peut permettre de faciliter une prise de pouvoir par des personnalités plus sensibles aux visées géopolitiques des stratèges informationnels, ou d'arriver à un morcellement du paysage politique qui pourrait rendre toute prise de décision a minima lente, si ce n'est délicate.

Dans la situation actuelle où la Russie parie plus que jamais sur l'usure des soutiens à l'Ukraine (Dennison and Zerka 2023, the Economist 2023) pour obtenir les victoires qui du reste, leur font défaut sur le terrain militaire, viser les processus électoraux prend une importance toute particulière. Cela est tout spécifiquement notable pour les élections touchant les États membres de l'Union et l'institution elle-même, alors même que les élections américaines pourraient voir revenir au pouvoir un président plus favorable au Kremlin.

Une pluralité de méthodes

Si l'usage de trolls sur les réseaux sociaux est maintenant de notoriété publique quand il s'agit d'influencer les opinions publiques (McCombie, Uhlmann and Morrison 2020, Morrison 2021), de même que l'usage de faux profils ou « sockpuppets », les méthodes utilisant les technologies de l'information ont connu une importante diversification.

La récente opération Döppelganger remettait au goût du jour une méthode connue pendant la période soviétique qui consiste à usurper l'identité graphique d'un tiers, en particulier des journaux de confiance et des institutions publiques, afin de bénéficier de la confiance qui leur est accordée pour disséminer des contenus servant une stratégie informationnelle précise, ici, dénigrer l'Ukraine et tenter de semer la division au sein de ses soutiens (Dugoin-Clément 2023).

Si l'approche n'est pas nouvelle et rappelait des actions menées pendant l'ère soviétiques (Kux 1985, Abrams 2016), la masse des usurpations attirait l'attention, de même que la technologie mise en œuvre pour tenter de mesurer l'effet de la campagne.

Plus récemment encore, on a pu observer certaines opérations qui visaient à saturer les groupes chargés de vérifier des contenus et éléments diffusés. Cette opération appelée « Matriochka » (AFP 2023) permettait de saturer les structures de fact checking et, si ces dernières se refusaient à opérer la vérification demandée, de les accuser de clientélisme, voire de saisir l'occasion pour porter un discours complotiste.

La massification observée lors de Döppelganger a aussi pu être notée lors de la mise à nu du Portal Kombat par Viginum (Viginum 2024), un réseau de plus de 190 sites visant à diffuser de la désinformation.
En outre, la désinformation russe a souvent recours à des prestataires de services ou à des « proxis » (Audinet, Le Meitour and Piveteau 2023) qui participent à diversifier les méthodes et canaux tout en complexifiant l'attribution finale, laissant toujours une part au déni plausible (Borghard and Lonergan 2023).

Enfin, les développements connus par l'IA, et plus particulièrement par sa branche de Deep Learning, permettent de créer des « deep fakes », autrement dit des contenus générés par des systèmes algorithmiques, que l'on parle de contenus visuels, audio, ou écrits. L'augmentation de la puissance de calcul a permis une forme de popularisation de ces technologies et si leurs usages restaient minimes dans les premiers mois de la guerre, on a pu observer une augmentation notable de l'usage de « deep fakes » à des fins d'influence lors de ces six derniers mois.