L'exploitation des applications de rencontre en nouvelles armes informationnelles

Nicolas ZUBINSKI | Consultant en Intelligence économique ; Rédacteur « Sécurité nationale » du site *infoguerre.fr*, Centre de réflexion sur la guerre économique, École de guerre économique.

Note préliminaire : L'article a été publié initialement le 4 octobre 2019 sur *Infoguerre*, Centre de réflexion sur la guerre économique, École de guerre économique (www.infoguerre.fr).

Tinder, Happn, Grindr, Shapr, Gleeden, Attractive World, Momo, Tantan, Russiancupid, les applications de rencontre séduisent et fleurissent. Toutefois, leur fonctionnement favorise la captation d'informations sensibles, le profilage et la compromission de leurs utilisateurs. La menace ne se limite pas à la sauvegarde de la *e*-réputation, à la protection de la vie privée ou à la gestion de la confidentialité. La démocratisation des *Dating Apps* et l'ampleur de leur instrumentalisation orientent le risque sécuritaire vers la désinformation de masse et le chantage à grande échelle. L'innovation ne porte pas tant sur la nature de la menace que sur l'utilisation d'un nouveau vecteur de disruption informationnelle. Celui-ci a la particularité de produire des effets d'émulation entre les méthodes de ciblage individuelle (compromission et déstabilisation) et celles de ciblage à large éventail (désinformation massive). Ces capacités d'origines militaires prolifèrent dangereusement dans le secteur privé à la faveur de la commercialisation des intelligences artificielles (IA) et font peser un risque systémique sur la sécurité nationale française.

La prolifération des *modèles* psycho-sociaux prédictifs

Les applications de rencontre ont construit leur modèle économique sur la collecte massive d'informations hautement sensibles (cf. Judith DUPORTAIL). La valeur ajoutée des *Dating Apps* réside dans la capacité à proposer à leurs utilisateurs des rencontres avec des correspondances élevées de profils. Pour satisfaire ces exigences, les utilisateurs sont encouragés à renseigner des informations intimes (orientations et habitudes sexuelles, préférences politiques et religieuses, revenus,

lieux de vacances, cercles privés, etc.). Ce profilage volontaire s'effectue généralement sous couvert d'un pseudo-anonymat. Le seuil d'acceptabilité individuel dans la divulgation de ces informations avait déjà atteint des niveaux problématiques lorsque les réseaux sociaux classiques ont émergé dans l'écosystème numérique. Néanmoins, l'utilisation de ces bases de données nécessitait un travail de retraitement conséquent et la construction de grilles de recoupement complexes. Avec les *Dating Apps*, le degré d'intimité des informations est tel que le profilage psycho-social gagne dangereusement en précision. La construction de *patterns* comportementaux psychosociaux prédictifs aura ainsi été facilitée par la démocratisation des applications de rencontre.

Le *leader* chinois des applications de rencontre a annoncé l'exploitation de ces banques de données intimes *via* le déploiement d'IA (cf. Li TAO et Iris DENG), initialement pour optimiser les *matching*. Bien que le potentiel des IA soit à relativiser (cf. Olivier PICHOT), la construction de technologies alliant *deep learning* et le *data mining*, appliquées aux sciences cognitives, va faciliter l'acquisition par des sociétés privées d'armes informationnelles. La fonction déstabilisatrice de ces procédés aurait pu les faire tomber sous la qualification d'armes militaires par destination pour en limiter le déploiement. Assimiler ces produits technologiques à du commerce de matériel de guerre permettrait d'édifier une régulation sectorielle mieux adaptée.

Une globalisation des possibilités de ciblage de personnes d'intérêt

Le recours à ces applications se démocratise et dépasse les frontières générationnelles. Il est courant de retrouver des traces d'utilisations sur les outils de télécommunication des personnels politiques (affaires Benalla à l'été 2018 en France – cf. Julien LAUSSON – et Sich en Australie début 2019 – cf. Brendan CRABB et Alexandra SMITH), militaires (« *F-35 Tinder leak* » [1], cf. Mark NICHOL), cadres supérieurs et dirigeants d'entreprises. Du fait de leurs activités, ces individus sont susceptibles de constituer des points de déstabilisation d'institutions stratégiques par ciblage de *Key Leaders Engagement*.

Le risque est d'autant plus préoccupant que les différents réseaux sociaux échangent ces informations (cf. *Zednet*) et que des vulnérabilités sont régulièrement découvertes (cf. Andy GREENBERG). Par ailleurs, le développement des législations ouvrant l'accès des agences gouvernementales aux données aggrave l'exposition des utilisateurs aux puissances étrangères comme les États-Unis (cf. Leïla ACKERMAN), la Chine (cf. Sophia YAN) ou la Russie (cf. Basile DEKONIK).

Enfin, les habitudes d'utilisation des générations Y et Z feront perdurer le risque d'exploitation des données dans l'avenir. La prise de mesures de protection,

[1] Le profil Tinder d'une pilote de *F-35* de la *RAF* a été piraté : le pirate aurait ensuite contacté *via* l'application d'autres pilotes et aurait obtenu des informations confidentielles sur l'appareil.

même immédiate, ne fera pas disparaître la menace ainsi créée. L'absence de souveraineté de la donnée crée ainsi, non seulement une faille instantanément exploitable, mais également un risque perpétuel d'exploitation. Il est donc nécessaire de prendre en compte cet effet d'enlisement dans l'édification d'une résilience informationnelle nationale. Souveraineté numérique et résilience informationnelle doivent être pensées conjointement, à l'instar de l'ensemble des champs opérationnels de la Sécurité nationale.

Un vecteur d'encerclement cognitif renouvelant la problématique de l'affaire Cambridge Analytica

L'instrumentalisation des *Dating Apps* change progressivement de nature et s'intègre désormais dans des opérations de déstabilisation à grande échelle. Un rapport parlementaire britannique a récemment mis en exergue l'impact de la désinformation de masse dans le jeu politique anglais (HC 1791) et relance l'intérêt d'enquêter sur les techniques de manipulation par encerclement cognitif dans les réseaux sociaux (cf. Christian HARBULOT). Cette tendance s'est propagée aux *Dating Apps* (campagnes électorales anglaises et américaines de 2016, cf. Phillippe N. HOWARD), dans la lignée du scandale Cambridge Analytica (cf. Kévin DENIAU). Ces actions sont d'autant plus problématiques qu'elles relèvent d'une utilisation civile de techniques militaires.

Cette porosité a même été érigée en principe institutionnel aux États-Unis (quelques illustrations d'inspiration doctrinale : RAND, US Army, INSS). À titre illustratif, la société SCL Group, prestataire privé du *MoD* américain spécialisé dans les opérations psychologiques, était également une société parente de Cambridge Analytica. Ainsi SCL Group aurait servi d'interface de transfert de compétences entre les techniques militaires américaines de l'information warfare et les outils de ciblage électoral de Cambridge Analytica (cf. Carole CADWALLADR). Cette conjonction aura permis un travail de sape des fondements sociétaux européens dont les lignes de fracture sont exploitées par des intérêts étrangers dans un contexte de guerre économique.

Cette affaire aura révélé la puissance de l'instrumentalisation des réseaux sociaux dans des politiques de déstabilisation à large spectre. En réponse à ce risque, des chercheurs de l'Université d'Oxford ont développé une base de recueil des actions de propagande (*Computational Propaganda Research Project*, *COMPROP*).

Mais en se propageant aux applications de rencontre, le dépistage des actions se complexifie. En devenant un outil de plus en plus déterminant dans les habitudes sexuelles de la population, les manœuvres de manipulation et d'encerclement cognitif sont moins perceptibles. Cette problématique s'apparente à celle du recensement des agressions sexuelles auquel se confronte l'Observatoire national de la délinquance et des réponses pénales (ONDRP). L'instrumentalisation des

applications de rencontre n'aura pas uniquement permis une amélioration de la précision des données pour effectuer du ciblage. Elle aura utilisé les barrières morales et cognitives des utilisateurs pour abaisser à la fois leur seuil de vigilance et leur taux de divulgation des actes de compromission.

Du *Kompromat* au *Deep fake* : les chantages numériques de demain

Le recours aux missions de courtoisie aux fins de chantage a toujours été un classique de l'action clandestine. La Russie a d'ailleurs adapté les méthodes soviétiques du *Kompromat* aux nouvelles possibilités offertes par les *Dating Apps*, sous la forme de « *Tinder attacks* » comme dans l'affaire Bureiko [(2)] (cf. Veronika VELCH, Just Security et Rainy Center).

Le risque s'accentue avec les nouvelles IA de modélisation faciale permettant la création de *Deep fake kompromat* particulièrement réalistes. Plusieurs technologies sont actuellement développées avec des applications à première vue inoffensives (secteurs de la retouche photo et du jeu vidéo). Or, le libre accès à des logiciels de retouche photo permet de constituer gratuitement une base de données avec suffisamment d'entrées pour édifier un programme de *deep learning* capable de reconnaitre l'environnement extérieur. Pour ce qui est du jeu vidéo, la création d'images intégralement artificielles de très haute définition permettra de diffuser des *deep fake* quasiment indécelables. C'est donc une altération sans précédente du rapport individuel à la vérité qui s'opère.

Remis dans la perspective d'une utilisation militaire, ces deux technologies préfigurent une guerre cognitive particulièrement redoutable et structurante de notre siècle. Il est ainsi plus que nécessaire d'éduquer les nouvelles générations au *fact-checking*, les initier à la gestion de leurs données personnelles et à la protection de leur vie privée. Les premiers outils pédagogiques ont commencé à essaimer à la faveur d'initiatives citoyennes (Rose-Marie Farinella, professeure des écoles, ayant introduit cette discipline dans certains cours élémentaires de CM2). Irriguer la société d'une culture de la confidentialité est absolument nécessaire. Cette première étape permettrait, plus largement, d'édifier une résilience informationnelle d'échelle nationale.

La construction d'une résilience informationnelle à l'échelle nationale

L'instrumentalisation des réseaux sociaux classiques posait déjà des défis considérables à la sécurité nationale. En s'attaquant à la sphère la plus intime des individus, le détournement des *Dating Apps* facilite la compromission.

[(2)] Du nom d'une étudiante ukrainienne qui a accusé un haut fonctionnaire de police de son pays de chantage sexuel en publiant, sur Facebook, un extrait de conversation Tinder. Elle s'est ensuite rétractée en avouant avoir été payée : l'objectif était de jeter le discrédit sur les hautes autorités ukrainiennes. L'affaire a divisé le pays.

Sensibilisation et anticipation s'avèrent particulièrement efficaces pour limiter ce risque. Quelques projets rapides et impactant amorceraient la construction d'une résilience informationnelle nationale :

• Plan de sensibilisation commun à l'ensemble de l'Éducation nationale pour protéger l'avenir des jeunes générations (utilisation raisonnée des réseaux sociaux, prévention du cyber-harcèlement, protection de la vie privée sur *Internet*).

• Sensibilisation des professionnels face aux nouvelles menaces de compromission.

• Acquisition de technologies défensives de la guerre informationnelle.

• Assimilation des IA de *Deep Learning Social* et de *Data Mining* au régime des matériels de guerre.

• Introduction de la résilience informationnelle dans le concept de sécurité nationale.

Éléments de bibliographie

ACKERMAN Leïla, « Cloud Act, l'offensive américaine pour contrer le RGPD », Portail de l'IE, 22 juin 2018 (https://portail-ie.fr/analysis/1902/cloud-act-loffensive-americaine-pour-contrer-le-rgpd).

BRADSHAW Samantha et HOWARD Philipp N., « The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation », University of Oxford – Oxford Internet Institute, 2019 (https://comprop.oii.ox.ac.uk/research/cybertroops2019/).

CADWALLADR Carole, « The Cambridge Analytica Files », *The Guardian*, 17 mars 2018 (www.theguardian.com/).

CHAMBRE DES COMMUNES, *Disinformation and fake news: Final Report* (HC 1791), 18 février 2019 (https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf).

COLDEWEY Devin, « Mona Lisa frown: Machine learning brings old paintings and photos to life », *Techcrunch*, 23 mai 2019.

CRABB Brendan et SMITH Alexandra, « Wollongong Young Liberal Jacob Sich sacked from Gareth Ward's office over Tinder scandal », South Coast Register, 18 février 2019 (www.southcoastregister.com.au/).

DEKONIK Basile, « La Russie veut accéder aux données de Tinder », *Les Échos*, 4 juin 2019 (www.lesechos.fr/).

DENIAU Kévin, « Cambridge Analytica : tout comprendre sur la plus grande crise de l'histoire de Facebook », *Siècle Digital*, 23 mars 2018 (https://siecledigital.fr/).

DUPORTAIL Judith, « Tinder : I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets », *The Guardian*, 26 septembre 2017 (www.theguardian.com/).

Greenberg Andy, « Tinder's Lack of Encryption Lets Strangers Spy on Your Swipes », *Wired.com*, 23 janvier 2018 (www.wired.com/story/tinder-lack-of-encryption-lets-strangers-spy-on-swipes/).

HARBULOT Christian, « Manipulation sur le *web* et les réseaux sociaux : encerclement cognitif » (*interview*), *XerfiCanal*, 20 mai 2019 (www.xerficanal.com/).

HOWARD Philip N., « How Political Campaigns Weaponize Social Media Bots », *IEEE Spectrum*, 18 octobre 2018 (https://spectrum.ieee.org/computing/software/how-political-campaigns-weaponize-social-media-bots).

LAUSSON Julien, « Affaire Benalla : quels risques y a-t-il à utiliser Tinder quand on est le chargé de mission du Président ? », *Numerama*, 3 août 2018 (www.numerama.com/).

NICHOL Mark, « Honeytrap spy stole secrets of new RAF jet: Female agent hacked airwoman's Tinder profile to target stealth fighter crews involved in the £9bn F-35 project », *Daily Mail*, 4 août 2018 (www.dailymail.co.uk/).

PICHOT Olivier, « L'Intelligence Artificielle ou comment promettre des choses qui n'existeront jamais ! » *InfoGuerre*, 20 mai 2019 (https://infoguerre.fr/2019/05/lintelligence-artificielle-promettre-choses-nexisteront-jamais/).

ROCH Arène, « Cette IA permet de faire de la retouche photo en quelques clics », *CNET*, 1er juillet 2019 (www.cnetfrance.fr/news/cette-ia-permet-de-faire-de-la-retouche-photo-en-quelques-clics-39886921.htm).

TAO Li et DENG Iris, « China's Tinder embraces AI as it eyes growth from the country's singles », *South China Morning Post*, 11 juillet 2018 (www.scmp.com/).

US ARMY, *Restricted U.S. Army Psychological Operations Process Tactics, Techniques, and Procedures Manual*, 8 juin 2012 (https://publicintelligence.net/restricted-u-s-army-psyops-manual/).

VELCH Veronika, « Next Step in Disinformation: How a Dating App Becomes a Weapon », *Justsecurity.org*, 21 mars 2019 (www.justsecurity.org/63315/next-step-in-disinformation-how-a-dating-app-becomes-a-weapon/).

VELCH Veronika, « Post-Soviet Disinformation: How Tinder Becomes a Weapon », *Rainey Center*, 14 février 2019 (https://raineycenter.org/wp-content/uploads/2019/02/PostSovietDisinformation_FINAL.pdf).

WHEATLEY Gary F. et HAYES Richard E., « Information Warfare and Deterrence », Institute for National Strategic Studies, décembre 1996 (www.dodccrp.org/files/Wheatley_Deterrence.pdf).

YAN Sophia, « China's new cybersecurity law takes effect today, and many are confused », *CNBC*, 1er juin 2017 (www.cnbc.com/2017/05/31/chinas-new-cybersecurity-law-takes-effect-today.html).

« Facebook recueillerait des données personnelles sur Tinder, Pregnancy+… », *ZDNet*, 20 décembre 2018 (www.zdnet.fr/actualites/facebook-recueillerait-des-donnees-personnelles-sur-tinder-pregnancy-39878363.htm).