UQÀM | CHAIRE RAOUL-DANDURAND EN ÉTUDES STRATÉGIQUES ET DIPLOMATIQUES 25 ans

CHRONIQUES DES NOUVELLES CONFLICTUALITÉS

@U.S. Navy

Personnel militaire : de la sextorsion au « sexpionnage » ?

Par Alexis Rapin

Alors que de plus en plus de membres de forces armées à travers le monde recourent aux plateformes de rencontre pour pallier la solitude de la vie en caserne, les institutions militaires s'inquiètent : les fausses romances en ligne peuvent représenter un moyen de soutirer de l'information à valeur stratégique.

La géopolitique s'arrête-t-elle à la sphère intime ? Rien n'est moins sûr. À travers le monde, de plus en plus de forces armées s'inquiètent du fléau grandissant de la sextorsion, soit l'usage d'images ou de vidéos à caractère sexuel comme moyen de pression contre des individus. Entre autres craintes : que des puissances adverses en viennent à soutirer des informations sensibles à du personnel militaire par l'entremise de contenus intimes, par exemple obtenus via de fausses romances sur internet.

Si le scénario peut faire sourire, les forces armées américaines, elles, prennent le problème très au sérieux : en 2019, le département de la Défense et l'US Army diffusaient déjà à leur personnel des avertissements officiels à ce sujet. Bien que la préoccupation majeure reste pour l'heure le bien-être des victimes, de plus en plus de voix font remarquer que le phénomène pourrait à l'avenir soulever des enjeux plus stratégiques : les actes de sextorsion, jusqu'ici utilisés par des criminels pour s'enrichir, pourraient tout aussi bien servir à des acteurs politiques pour obtenir des informations à valeur stratégique. Tinder, Bumble et autres Hinge seraient-ils en passe de devenir les nouveaux terrains de chasse du renseignement militaire ?

Groupes bien organisés

À l'origine du problème, on trouve un phénomène à bien des égards facile à appréhender : les forces armées comptent dans leurs rangs beaucoup de jeunes individus déployés loin de chez eux et de leur cercle social, et bien souvent aux prises avec la solitude de la vie en caserne. En quête de romance (et plus si affinités), de nombreux militaires recourent à des sites ou des applications de rencontres, sur lesquels tout le monde n'est pas forcément qui il ou elle prétend être. On imagine aisément la suite : discussions aguichantes, proposition d'échanges de photos intimes et potentiellement appels vidéo, à travers lesquels les victimes en viennent à s'exposer. Pour arriver à leurs fins, les fraudeurs utilisent le plus souvent des photos volées ou des vidéos pornographiques préenregistrées. Et voilà le piège refermé.

De quelques cas isolés à partir de 2012, le phénomène n'a pas tardé à faire les manchettes aux États-Unis : en novembre 2018, le Pentagone annonçait le démantèlement d'un réseau criminel ayant « sextorqué » plus d'un demi-million de dollars américains à quelque 440 membres des forces armées. Derrière de charmants faux profils sur les réseaux sociaux se cachait en fait… un groupe de détenus sévissant discrètement depuis une prison de Caroline du Sud. D'autres cas traités par les unités d'investigation criminelles des forces armées américaines mettaient en cause des entités basées aux Philippines ou en Côte d'Ivoire, présentant parfois un haut degré d'organisation. L'un des réseaux philippins comptait par exemple près d'une cinquantaine de membres travaillant dans un bureau centralisé, et fonctionnait sur la base d'une grille salariale bien établie, prévoyant des bonus pour les individus ayant extorqué les plus grosses sommes.

Scandales sur demande

De quoi donner quelques sueurs froides aux agences de contre-espionnage. De telles officines ne sont en effet pas sans rappeler les usines à trolls qui, aux quatre coins du monde, sont de plus en plus mandatées par des acteurs malveillants pour mener des campagnes de désinformation

à l'étranger. Profitant de systèmes judiciaires locaux souvent dysfonctionnels et offrant un potentiel de déni plausible aux acteurs qui les emploient, ces entités agissent de plus en plus comme des sous-traitants d'opérations clandestines orchestrées par des États. On peut ainsi craindre que les groupes organisés pratiquant la sextorsion n'en viennent à s'inspirer de ce modèle d'affaires, en louant par exemple leurs services à des puissances étrangères pour piéger et faire chanter des individus en position de pouvoir dans des pays rivaux.

De premiers cas de scandales à caractère intime s'approchent de tels schémas. En 2018 en Ukraine, deux sulfureux consultants en relations publiques ont été arrêtés pour avoir orchestré une fausse relation Tinder impliquant un haut placé de la police nationale. Empruntant le compte Tinder d'une jeune étudiante, les malfaiteurs ont créé de toute pièce une discussion en ligne dans laquelle le haut fonctionnaire semblait solliciter des faveurs sexuelles, échange par la suite fuité dans la presse ukrainienne. Alors que les consultants semblent avoir reçu une somme importante pour leurs services, l'identité des mandataires du coup monté reste inconnue, mais divers observateurs furent prompts à suggérer une possible implication de la Russie.

Des « *kompromats* 2.0 »

Si le « scandale Tinder » en Ukraine n'était que supercherie, d'autres tentatives d'instrumentalisation stratégique de relations intimes en ligne s'accumulent. En 2018 par exemple, l'armée israélienne révélait que le Hamas avait mis sur pied plusieurs applications de rencontre frauduleuses, truffées de faux profils de jeunes femmes, pour tenter de duper des soldats de Tsahal et de leur soutirer des renseignements. En 2020, l'armée indienne interdisait à ses soldats l'usage de près de 90 applications de rencontre, affirmant que le renseignement pakistanais les utilisait à des fins d'espionnage.

Dans certains cas, ces fausses romances servent seulement à faciliter des piratages informatiques classiques, les échanges de mots doux endormant la vigilance des utilisateurs, les poussant ainsi à cliquer sur des liens infectés par exemple. Parfois, c'est davantage le chantage émotionnel qui semble exploité : le partenaire virtuel force subtilement la cible à révéler des informations confidentielles à grand renfort de jeu sentimental. Dans d'autres cas, enfin, ces opérations semblent carrément avoir vocation à piéger la victime et récolter des « *kompromats* 2.0 », des contenus embarrassants, bien souvent à caractère sexuel, susceptibles de la faire chanter. L'information ainsi obtenue peut prendre de nombreuses formes : emplacements et rotations d'unités, détails sensibles sur du matériel ou des infrastructures militaires, structure et organisation des chaînes de commandement, etc.

Au Canada, un avertissement

Si les institutions militaires se montrent actuellement parmi les plus préoccupées face au péril du « sexpionnage », il est clair que la problématique ne se cantonne pas aux seules forces armées : diplomates, haut fonctionnaires et autres figures en position de pouvoir constituent aussi d'évidentes cibles potentielles à qui soutirer de l'information sensible par l'entremise de fausses romances en ligne. Début 2022, dans son allocution annuelle, le directeur du renseignement intérieur australien avertissait publi-

quement ses concitoyennes et concitoyens des risques géopolitiques posés par les plateformes de rencontre instrumentalisées par des services d'espionnage étrangers.

Le Canada, quant à lui, a même déjà senti le vent du boulet : en novembre 2018, le député conservateur et ex-ministre Tony Clement s'est retrouvé au cœur d'une affaire de sextorsion menée depuis l'étranger. Croyant entretenir une relation en ligne avec une femme « en quête d'amour », le politicien avait envoyé des photos sexuellement explicites à celle-ci, sans se douter qu'il était en fait piégé par les membres d'un réseau d'escroquerie basé en Côte d'Ivoire. Tony Clement s'était ensuite fait réclamer le versement de 75 000 dollars, faute de quoi les photos seraient publiées. Le député fut poussé à la démission à la suite du scandale, et deux des malfaiteurs furent plus tard appréhendés par les autorités ivoiriennes.

L'affaire livra toutefois un aperçu, voire un avertissement, quant aux potentielles retombées géopolitiques de la sextorsion : au moment des faits, Tony Clement était en effet appelé à siéger prochainement sur le Comité des parlementaires sur la sécurité nationale et le renseignement, alors fraichement créé par le gouvernement Trudeau. Il aurait eu, dans le cadre de cette fonction, accès à des informations classifiées et extrêmement sensibles, touchant par exemple aux activités du Service canadien de renseignement de sécurité, du Centre pour la sécurité des télécommunications ou encore du ministère de la Défense. Certains observateurs firent ainsi remarquer que l'affaire, si elle n'avait pas été révélée à temps, aurait fourni un potentiel outil de chantage de premier choix à des puissances étrangères en quête de secrets d'État.

Alexis Rapin 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/

@176th Wing, Alaska Air National Guard