CDS

158 CDSDG 17 F bis
Original : anglais

Assemblée parlementaire de l'OTAN

COMMISSION
SUR LA DIMENSION CIVILE DE LA SÉCURITÉ

LA RÉVOLUTION DES MÉDIAS SOCIAUX : INCIDENCES POLITIQUES ET SÉCURITAIRES

RAPPORT

Jane CORDY (Canada)
Rapporteure
Sous-commission sur la gouvernance démocratique

TABLE DES MATIÈRES

I. INTRODUCTION

1. La montée en puissance des médias sociaux[1] constitue l'une des manifestations les plus récentes et les plus importantes de la révolution numérique et des techniques de communication qui, il y a plusieurs décennies, a marqué le début de l'ère post-industrielle (à savoir l'ère de l'information). La prolifération des médias sociaux véritablement inouïe[2] observée ces dernières années, a été facilitée par l'essor rapide des appareils mobiles connectés à Internet (smartphones). Pour de nombreuses personnes de par le monde, les médias sociaux constituaient la principale source d'information en 2016, 62 % des citoyens états-uniens s'informant sur les réseaux sociaux – 44 % rien que sur Facebook (Gottfried et Shearer). Selon une étude portant sur quelque 50 000 jeunes de 26 pays, les médias sociaux supplantent déjà, pour cette génération, la télévision comme principale source d'information (Wakefield).

2. Cette transformation spectaculaire des technologies de l'information et de la communication a inéluctablement un impact sur tous les aspects de la vie : l'éducation, l'économie et la politique. L'évolution des communications, de l'informatique et des modes de stockage des données bouscule les notions de vie privée, d'identité et de frontières nationales. Les profonds changements inhérents à cette révolution modifient notre perception de la sécurité, ils ont des conséquences inattendues et exigent de trouver des réponses innovantes. Twitter et Facebook font entendre la voix des citoyens tout en leur permettant de se connecter à moindre coût, de manière plus privée et de communiquer entre eux et plus directement avec leurs dirigeants. De même, l'anonymat qui est possible sur les médias sociaux peut enhardir ceux qui propagent un discours haineux, mais également ceux qui se battent contre les régimes autoritaires et ce, sans crainte de représailles.

3. Mais les médias sociaux offrent aussi de nouvelles possibilités à ceux qui cherchent à perturber l'ordre du monde démocratique progressiste en tirant profit de l'ouverture intrinsèque au cyberespace. Les médias sociaux sont exploités par les organisations terroristes comme arme de recrutement et de propagande. Ils sont aussi utilisés par des États qui cherchent à influencer et à saper les démocraties progressistes, leurs institutions publiques et leur tissu social – parfois avec succès. C'est ce que l'on appelle « l'arsenalisation » des médias sociaux. Les médias sociaux étant un phénomène récent, il est difficile de prévoir toutes les conséquences possibles d'une telle révolution. L'objectif du présent rapport est, avant tout, de sensibiliser les membres de l'Assemblée parlementaire de l'OTAN, de lancer un débat sur ce thème émergent et de soumettre quelques premières réflexions sur les moyens de contrer l'usage malveillant des médias sociaux.

---

1 Les « médias sociaux » se définissent ainsi : les utilisateurs créent leur compte/profil personnel qu'ils rendent totalement ou partiellement public ; le profil des utilisateurs et le contenu qu'ils génèrent sont mis en réseau. Diverses plateformes de réseaux sociaux ont des spécificités propres : par exemple, Twitter est axé sur la publication de messages courts, Instagram spécialisé dans les photos et vidéos et LinkedIn dans les informations à caractère professionnel. Facebook est la plateforme la plus complète. Certaines plateformes de messagerie comme WhatsApp sont aussi appelées médias sociaux alors qu'elles servent principalement à discuter et à échanger des fichiers entre un petit groupe de personnes, souvent entre deux utilisateurs.

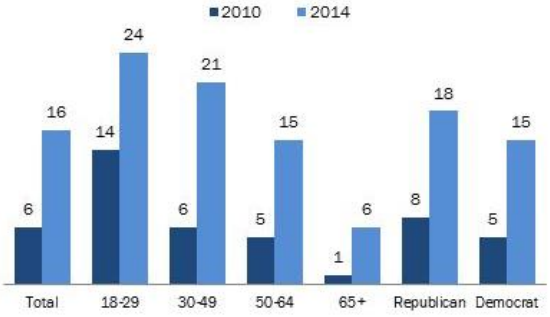
2 En 2005, seulement 5 % de la population adulte aux États-Unis utilisaient l'une de ces plateformes ; en 2011, ce pourcentage est passé à 50 %, et il atteint aujourd'hui près de 70 %. Quelque 88 % de jeunes adultes (18-29 ans) aux États-Unis sont sur Facebook. Au niveau mondial, on comptait quelque 2,7 milliards d'utilisateurs de réseaux sociaux en janvier 2017 (37 % de la population mondiale), près d'un demi-milliard de plus qu'en janvier 2016. Facebook, à lui seul, compte près de 2 milliards d'abonnés, la croissance la plus rapide étant observée dans les pays en développement.

II. MÉDIAS SOCIAUX ET GOUVERNANCE DÉMOCRATIQUE

4. La révolution des médias sociaux a eu un impact profond sur les institutions démocratiques et la vie politique à travers le monde. Au cours de la dernière décennie, les citoyens en général, et ceux qui s'engagent en politique en particulier, ont utilisé les sites des réseaux sociaux, tels que Twitter et Facebook, pour contester l'establishment politique et mobiliser le soutien de tous bords. Aux États-Unis, par exemple, plus d'un tiers des utilisateurs des nouveaux réseaux sociaux consacrent régulièrement du temps à commenter l'action du gouvernement et la vie politique. L'élection présidentielle aux États-Unis a généré plus d'un milliard de tweets selon Twitter, et près de 128 millions d'utilisateurs ont mentionné l'élection présidentielle sur Facebook aux États-Unis. En sa qualité de président des États-Unis, Donald Trump a souligné la valeur de la communication via les médias sociaux, notamment par Twitter, qui lui donne la possibilité, fait-il observer, de se connecter directement aux citoyens, et de court-circuiter certains médias grand public qui, d'après lui, produisent des « fake news » (fausses nouvelles). Plus au nord, lors des élections fédérales au Canada en 2015, la société civile s'est associée à Google pour trouver des moyens novateurs d'accroître la participation électorale.

Le pourcentage des électeurs inscrits qui suivent les hommes politiques sur les réseaux sociaux a doublé depuis 2010

% des électeurs inscrits qui suivent les candidats à des fonctions publiques, les partis politiques ou les élus sur des sites de réseaux sociaux comme Facebook ou Twitter



Enquête menée du 15 au 20 octobre 2014, sur la base des électeurs inscrits
Source : Pew Research Center

5. Bien plus qu'une simple source d'information et qu'une caisse de résonance, l'activité des internautes sur les sites des réseaux sociaux permet, empiriquement, d'anticiper les résultats d'une campagne électorale. Après l'élection présidentielle aux États-Unis, des chercheurs ont constaté une forte corrélation entre le candidat que suivait un électeur sur Twitter et celui pour lequel il a voté le jour des élections (Thompson). Les instituts de sondage ont même constaté que l'activité des internautes sur Facebook permettait davantage de prévoir le résultat de l'élection américaine que les sondages traditionnels. Durant le référendum au Royaume-Uni sur l'Union européenne, des chercheurs ont observé davantage d'activité et de soutien pour la campagne du « Leave » sur Instagram et Twitter que pour la campagne en faveur du « Remain ». Même si activité ne veut pas dire soutien, des observateurs en ont conclu que les militants ont sous-estimé l'attrait du « Leave » dans les médias sociaux et la façon dont cela se traduirait dans les urnes (Polonski).

6. La capacité des réseaux sociaux de transformer toute personne en un acteur ou une actrice de l'information joue en faveur de la société civile et des militants des droits humains, à la fois dans les pays démocratiques et dans les régimes autoritaires. Les médias sociaux réduisent les coûts de communication entre les appareils reliés à Internet, contribuant à ce que les mouvements ne soient pas isolés ou morcelés. De même, les médias sociaux génèrent des informations en cascade – lorsque quelqu'un prend le risque d'exprimer ses griefs en premier, ceux qui ne se seraient pas manifestés d'ordinaire se sentent plus à l'aise pour y réagir. Ce qui se traduit de deux façons : la sphère publique s'élargit et les protestations peuvent être coordonnées sur de vastes zones géographiques. De même, le coût de la répression, notamment pour les régimes

autoritaires, augmente car, grâce aux réseaux sociaux, certaines régions (par exemple le Moyen-Orient) ont « mis en place une infrastructure solide pour dénoncer les violences faites aux les manifestants » (Lynch).

7. Les manifestations iraniennes de 2009 (lorsque la population est descendue dans la rue pour protester contre la victoire électorale de l'ancien président Mahmoud Ahmadinejad, forçant le régime iranien à suspendre temporairement l'accès aux nouveaux médias sociaux jusqu'à ce que le gouvernement reprenne la situation en main), constituent l'un des exemples les plus flagrants du rôle central des réseaux sociaux dans la mobilisation politique à grande échelle. Toutefois, ce sont les printemps arabes, en 2011, qui ont clairement affiché le pouvoir des réseaux sociaux. Les manifestations organisées, le 25 janvier 2011, via Facebook, ont appelé les Égyptiens à se rassembler sur les places publiques à travers le pays pour réclamer pain, dignité et liberté. Le régime du président égyptien Hosni Moubarak, au pouvoir depuis 29 ans, a fini par être renversé sous la pression de l'armée et des mouvements civils de protestation. Autre exemple convaincant du rôle des médias sociaux dans la mobilisation de masse : le mouvement pro-démocratie en Ukraine qui a chassé le président Viktor Ianoukovitch. Twitter et Facebook ont été utilisés pour organiser et consolider le mouvement contestataire Euromaïdan et permettre aux personnalités clés de communiquer efficacement avec les manifestants.

8. Les médias sociaux renforcent également la position des défenseurs des droits humains et des militants anticorruption. On peut citer l'exemple du célèbre militant russe anticorruption, Alexeï Navalny, qui a produit une vidéo de 50 minutes exposant au grand public l'immense fortune du premier ministre Dimitri Medvedev, tirant parti, entre autres, de la forte propension de celui-ci à publier des photos sur les réseaux sociaux. Alors que les médias contrôlés par l'État russe ont feint d'ignorer la vidéo de M. Navalny, celle-ci s'est propagée rapidement dans toutes les couches de la société russe via les réseaux sociaux et YouTube.

9. Les manifestants dans les pays de l'OTAN utilisent couramment les réseaux sociaux. La campagne *Occupy Wall Street* en 2011 à New York, et les manifestations de 2013 à Istanbul dans le parc Gezi en sont deux exemples notables. Dans ce dernier cas, Twitter a été si efficace que le gouvernement turc a désactivé temporairement le service pour les internautes turcs durant les manifestations. Également en Turquie, les médias sociaux ont joué un rôle déterminant dans l'échec de la tentative de coup d'État de juillet 2016 : le président Recep Tayyip Erdogan a diffusé son célèbre discours à la nation via une application FaceTime sur son smartphone. Son message exhortant la population à descendre dans la rue a été rapidement relayé via Twitter, Facebook, WhatsApp et autres réseaux sociaux.

10. Cela dit, la corrélation entre l'émergence des médias sociaux et la démocratisation n'est pas aussi forte qu'espérée. L'utilisation habile des médias sociaux ne nourrit pas toujours un discours productif et ne renforce pas forcément les institutions démocratiques. Qui plus est, tous les acteurs ne sont pas nécessairement intéressés par la démocratisation de leur société. Un élément important de l'activité politique en ligne est son caractère profondément cloisonné. Selon une enquête sur l'élection présidentielle de 2016 aux États-Unis, conduite par un journaliste spécialiste des données au *Media Lab* du *Massachussetts Institute of Technology* (MIT), le commentaire politique en ligne est cloisonné car les internautes se complaisent dans des bulles idéologiques ou thématiques au sein desquelles ils sont confortés dans leurs opinions (par exemple sur des thèmes comme l'immigration ou le droit de porter des armes). Rien ne prouve que le cloisonnement des réseaux contribue à polariser le monde politique.

11. Les données elles-mêmes ne suffisent pas à expliquer pourquoi les utilisateurs sont si polarisés. Les algorithmes « préférence utilisateur » et les botnets des médias sociaux semblent, en revanche, jouer un rôle important. Facebook et Twitter favorisent « l'entre-soi » dans la mesure où ils sont conçus pour fournir un contenu personnalisé et organisé en fonction des préférences des abonnés (par exemple l'historique de leur « like »). Les deux plateformes utilisent des algorithmes pour établir les contenus destinés aux abonnés. À l'aide des données recueillies sur

les comportements et préférences manifestés par ceux-ci dans le passé, ces algorithmes filtrent le contenu affiché sur le fil d'information de tel ou tel abonné en fonction de ses intérêts et de ses préférences. Ceci augmente la probabilité d'entrer en relation avec des internautes partageant les mêmes idées et d'être confronté à des images, des discussions, des nouvelles et des opinions qui confortent les préférences de chaque utilisateur. Par ailleurs, la probabilité d'être confronté(e) à des opinions divergentes ou contradictoires est réduite (Lee ; Thompson). Il est à noter que Facebook et d'autres plateformes répugnent à l'idée d'introduire un bouton « j'aime pas ».

12. La fréquence accrue des débats ne se traduit donc pas nécessairement par une réelle confrontation d'idées, qu'elles soient différentes ou contradictoires. Les « bots » des réseaux sociaux accentuent la polarisation en fabriquant et en diffusant du contenu qui renforce les croyances biaisées de l'utilisateur. Les « bots » sont des comptes facilement programmables sur Facebook et notamment sur Twitter qui génèrent automatiquement du contenu. Il n'est pas rare que de vrais utilisateurs, qui reçoivent un contenu fabriqué de toutes pièces, ignorent qu'ils interagissent avec un « bot » (Guilbeault et Woolley). Les « bots » sont largement utilisés et ont déjà prouvé leur pouvoir de nuisance. Par exemple, une étude sur la récente campagne présidentielle aux États-Unis révèle qu'une part non négligeable des tweets pro-Trump et pro-Clinton durant la campagne ont été générés par des « bots », programmés pour chercher et diffuser instantanément des messages spécifiques. Un seul compte « bot » peut envoyer des milliers de tweets par jour, couvrant la voix des réels utilisateurs de Twitter qui peuvent offrir un dialogue pertinent, et potentiellement productif sur les réseaux sociaux. Cherchant du contenu au moyen de mots clés, les « bots » ont pour but de relayer (par exemple retweeter) le contenu en question sans en vérifier la validité. Des acteurs marginaux ou extrêmement partisans peuvent s'approprier une discussion naissante pour donner davantage de poids à leur thématique, notamment lorsqu'ils programment des « bots » pour en relayer le contenu en leur nom. On a découvert récemment que des « bots » avaient été utilisés contre la campagne d'Emmanuel Macron pour perturber les derniers jours de l'élection présidentielle en France.

13. Le succès relatif de plusieurs partis contestataires dans la région euro-atlantique peut être attribué à d'habiles stratégies déployées sur les réseaux sociaux. Souvent les comptes politiques les plus prolifiques sont ceux de groupes ou de dirigeants de partis contestataires d'extrême gauche ou d'extrême droite. En général, ils postent sur leurs comptes davantage de contenu, utilisent un langage coloré voire provocateur, et communiquent plus étroitement avec leurs électeurs que leurs homologues plus traditionnels (*The Economist*, 2015).

14. Les réseaux sociaux ont facilité la propagation d'informations fausses et perturbantes que les internautes prennent pour argent comptant. Le danger est que ces fausses informations commencent à saper la confiance des citoyens dans leurs institutions et leurs dirigeants. La prolifération de sites alternatifs, non traditionnels (en l'occurrence les fausses informations), s'est accélérée ces dernières années. Le but de la désinformation sur les réseaux sociaux est, en réalité, de générer des profits. Des histoires spectaculaires, et souvent fausses, augmentent le nombre de clics sur des sites cherchant à attirer des lecteurs. Le système de paiement de la publicité sur Google et Facebook est fondé sur ce système « par clic » (Alexander et Silverman). Les fausses informations peuvent rapidement être relayées sur de multiples sites Internet, gagnant du terrain dans le cycle des nouvelles avant que les éditeurs de contenu des principales agences de presse puissent intervenir pour en vérifier les sources (BBC, 2016). Selon une enquête de l'*Ithaca College* (New York), 40 % des salles de rédaction locales n'ont pas de procédures permettant de contrôler le contenu des médias sociaux avant de le diffuser (Adornato). Ce qui peut avoir des conséquences désastreuses sur la perception par l'opinion publique d'un certain nombre de questions. Par exemple, les sondages semblent indiquer qu'il existe une corrélation systématique entre la prolifération d'informations fausses ou excessivement partisanes et la perception de plus en plus négative que l'on a de son gouvernement. Les données des sondages Gallup confirment l'idée que la défiance envers les gouvernements s'accroît et n'a jamais été aussi forte.

15. En résumé, les médias sociaux ont eu un impact profond sur les démocraties et dans les régimes autoritaires. Les médias sociaux peuvent rendre les sociétés démocratiques plus pluralistes, mais pas dans le sens traditionnel où on l'entend. Il est peut-être plus juste de décrire la convergence entre démocratie, activisme politique et médias sociaux par l'expression « pluralisme chaotique », comme le suggèrent certains experts. À savoir, un pluralisme qui offre une diversité de voix mobilisées [et de mouvements], mais qui est souvent imprévisible, instable et éphémère (Margetts et al.). Si l'engagement politique sur les médias sociaux a enrichi la parole démocratique et ouvert de nouvelles perspectives pour le flux d'information, il a aussi enfermé les internautes dans des cocons idéologiques. Les voix les plus fortes et les plus actives en ligne bouleversent le paysage politique, mais ces voix proviennent de plus en plus des deux extrêmes du spectre politique.

III. L'ARSENALISATION DES MÉDIAS SOCIAUX

16. L'ampleur de la révolution des réseaux sociaux a inéluctablement un impact sur la sécurité mondiale. Certains États et acteurs non étatiques s'intéressent de plus en plus à l'usage qu'ils peuvent faire des médias sociaux contre leurs adversaires – un processus que Thomas Elkjer Nissen, du *Royal Danish Defence College*, appelle « l'arsenalisation » des médias sociaux. M. Nissen identifie plusieurs façons d'utiliser les médias sociaux à des fins militaires, dont la collecte de renseignements, la guerre psychologique et même les activités de commandement et de contrôle (par exemple des groupes d'opposition en Syrie qui n'ont pas de structure formelle C2 recourent aux réseaux sociaux pour coordonner et synchroniser leurs actions et, dans certains cas, pour donner des ordres ou des orientations) (Nissen). Nigel Inkster, ancien numéro deux des services secrets britanniques (MI6), indique que l'analyse des réseaux sociaux par les responsables du renseignement permet de dresser un tableau d'une précision sans précédent car les images prises au sol apportent souvent plus d'informations que les images de reconnaissance par satellite ou aérienne. Si les activités sur les médias sociaux sont virtuelles, elles peuvent néanmoins avoir des effets concrets, par exemple en suscitant des manifestations de masse, en provoquant le retrait de l'argent des banques, ou encore des attaques contre certains groupes ou individus décrits comme l'ennemi (Lange-Ionatamishvili et Svetoka).

17. Les frappes aériennes des États-Unis contre l'un des commandements de Daech[3] à partir d'informations postées sur un réseau social par un militant de Daech en juin 2015, la surveillance des messages sur Twitter en provenance de Tripoli par des responsables du renseignement de l'OTAN durant la campagne de Libye, de très nombreux tweets postés par des équipes spéciales de l'armée israélienne durant le conflit de 2014 à Gaza, échangeant parfois directement des messages en ligne avec des agents du Hamas et la confusion suscitée par de fausses informations sur Twitter qui a poussé le ministre de la défense du Pakistan à menacer d'utiliser l'arme nucléaire contre Israël sont autant d'exemples de convergence entre médias sociaux et domaines militaires. Lors d'un exercice militaire en juin 2016, les experts du renseignement australien ont pu identifier l'emplacement, le matériel et l'organisation de forces adverses participant à l'exercice en analysant les informations librement accessibles sur les réseaux sociaux.

18. Si les armées des pays membres et partenaires de l'Alliance ont réussi à rendre opérationnelles les plateformes des médias sociaux dans les combats, des acteurs non étatiques tels que Daech et des États comme la Russie, sont également passés maîtres dans l'art de transformer ce nouveau moyen de communication en arme de guerre.

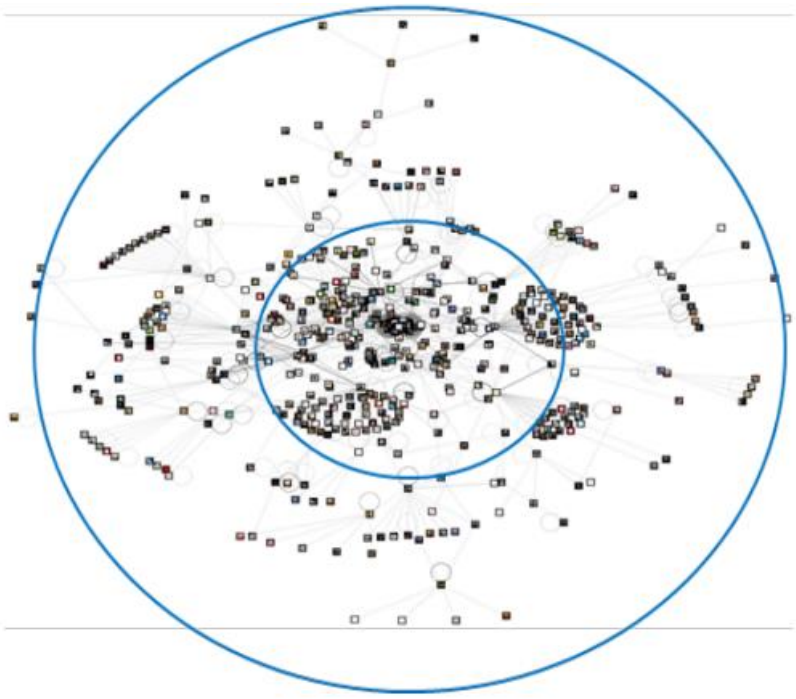
3 Acronyme arabe utilisé pour désigner l'organisation terroriste État islamique (EI)

A. DAECH ET LES MÉDIAS SOCIAUX

19. Daech n'est pas la première organisation terroriste à comprendre l'importance des médias sociaux. Des membres du Hamas auraient utilisé des plateformes comme Facebook et Twitter pour diffuser leur idéologie. Al Shabab s'est servi de Twitter pour revendiquer son attaque contre le centre commercial *Westgate* de Nairobi, postant des photos de ce dernier en temps quasi réel. En avril 2015, le Front al-Nosra a lancé une campagne via les réseaux sociaux appelée « Mobiliser », qui a incité quelque 5 000 enfants à rejoindre ses rangs. Plusieurs Alliés ont été la cible d'attaques fomentées par des terroristes d'origine locale qui ont trouvé leur source d'inspiration sur les réseaux sociaux : ainsi, les auteurs de certaines attaques qui ont durement frappé les pays occidentaux se sont inspirés de sermons en ligne du prédicateur radical Anwar al-Awlaki (Ruane).

20. Cependant, il est communément admis que Daech a donné une nouvelle dimension à l'utilisation malveillante des médias sociaux. Daech semble avoir compris comment utiliser ce qu'on appelle sur les réseaux sociaux la « courbe de puissance ». À une extrémité de la courbe, quelques contributeurs de premier plan dirigent la conversation sur le réseau selon ce qu'il est convenu d'appeler « mode diffusion ». À l'autre extrémité, les réseaux mettent en relation de très petits groupes au sein desquels se déroule une conversation de haut niveau (« mode conversation »). Les terroristes modernes ont compris que l'intérêt est de travailler aux deux extrémités de la courbe : ils se débrouillent pour qu'un acteur influent de premier plan relaie leurs messages, tout en incitant par la ruse des internautes à rejoindre des conversations en petits groupes où ils peuvent attirer de nouvelles recrues ou radicaliser les autres participants (Carafano). L'architecture de Twitter est particulièrement attrayante pour Daech car elle est parfaitement adaptée aux communications anonymes touchant un public très large et permet la récupération plus rapide de comptes désactivés (Shaheen).

21. Les experts du Centre d'excellence pour la communication stratégique (COE Stratcom) de l'OTAN, qui ont analysé le trafic réseau de Daech sur Twitter, ont découvert que le groupe terroriste a développé ce qu'il est convenu d'appeler une structure centre-périphérie sur Twitter : à savoir, qu'il y a un nombre élevé de comptes ayant un faible indice de centralité (périphérique), et seulement quelques comptes ayant un fort indice de centralité (groupe central). Or le groupe central est à l'origine de 76 % du trafic. Il est plausible que les comptes du groupe central soient aux mains d'un groupe encore plus restreint d'agents de Daech. Si les ramifications de Daech dans d'autres parties de la région Moyen-Orient et Afrique du nord (MOAN) peuvent conserver une certaine autonomie, le dispositif global de messagerie de Daech est apparemment fortement centralisé et coordonné (Shaheen).



Les structures centre/périphérie se caractérisent par un groupe central d'acteurs, suivi par un réseau plus étendu mais moins dense. Cette figure est un exemple de l'un des réseaux de trafic recueillis, représenté à l'aide d'un cercle pour illustrer sa centralité

Source: http://stratcomcoe.org/network-terror-how-daesh-uses-adaptive-social-networks-spread-its-message

22. On pourrait penser que la centralisation de l'activité de Daech sur les réseaux sociaux constitue un handicap, les principaux comptes du groupe pouvant de ce fait être identifiés et désactivés. Toutefois, pour contourner ce problème, les agents de Daech ont mis au point toute une série de mesures. Les cyberagents de Daech créent généralement plusieurs comptes twitter inactifs qui font partie d'un réseau entourant un compte central. Dès l'instant où un compte central est désactivé, un compte inactif est activé et devient lui-même un compte central ou sert à informer le reste des « followers » – au moyen d'un système de hashtags et de symboles – sur l'identité de l'ancien compte lorsqu'il est réactivé sous un nouveau nom. Daech utilise aussi certaines techniques pour éviter la détection et la désactivation des comptes. Par exemple, les noms des utilisateurs et, par conséquent, les URL[4] de ses principaux comptes changent périodiquement, ce qui permet à ces comptes d'échapper à la vigilance des logiciels de détection d'URL qu'utilisent les services de sécurité des États. Les images connues rattachées à Daech sont, d'autre part, légèrement modifiées pour ne pas être détectées par le logiciel de reconnaissance d'images. Les agents de Daech sont apparemment très au fait des dangers de la fonction de géolocalisation inhérente à Twitter qui fournit par GPS les coordonnées géographiques associées à chaque tweet : de fait, en décembre 2014, Daech a émis une directive interdisant à ses combattants d'activer la fonction de géolocalisation de Twitter (Shaheen). Enfin, les agents de Daech savent comment poster des tweets, y compris des liens, hashtags et images sans déclencher les algorithmes de détection de spams de Twitter (Farwell).

23. Pour résumer, Daech qui semble maîtriser parfaitement ces technologies est réellement devenue l'hydre à multiples têtes de Twitter. On estime que depuis 2013, des dizaines voire des centaines de milliers de comptes Twitter de Daech ont été désactivés ou supprimés (Shaheen) mais cela n'a pas empêché Daech de générer jusqu'à 90 000 tweets par jour (Schmitt). La technique de Daech centre-périphérie et une utilisation habile des hashtags assurent au groupe terroriste une forte visibilité sur les réseaux sociaux. Ainsi alors que Daech entrait dans Mossoul,

[4] Une URL (de l'anglais *Uniform Resource Locator*) est l'adresse du lien hypertexte introduit sur un navigateur pour accéder directement à la page Internet recherchée.

ses partisans ont envoyé jusqu'à 44 000 tweets par jour, faisant apparaitre le message du groupe en tête de liste lorsqu'on tapait « Bagdad » sur Twitter (Farwell). D'après *RAND Corporation*, le nombre d'opposants de Daech actifs sur les réseaux sociaux est six fois plus élevé que les comptes pro-Daech. Or les partisans de Daech dépassent régulièrement les opposants en nombre de tweets, produisant 50 % de tweets en plus par jour (Bodine-Baron et al.).

24. Les autres caractéristiques de l'usage par Daech des réseaux sociaux sont notamment :

- Daech est parfaitement conscient de l'importance des contenus visuels sur les médias sociaux : on estime que 88 % du contenu de Daech est visuel (63 % d'images, 20 % de vidéos, 5 % de graphiques) (OTAN, COE Stratcom, 2016a), ce qui est particulièrement attrayant pour la jeune génération. Le contenu visuel est de qualité hautement professionnelle ;
- Daech tweete dans plusieurs langues dont l'anglais, l'arabe, l'allemand, le farsi, l'hindi et le français ;
- Les messages de Daech sont en lien avec l'actualité, ils sont courts et faciles à comprendre ;
- Daech détourne également des hashtags recherchés comme ceux liés à la coupe du monde de football au Brésil (Farwell) ou #*Bruxelles* et #*Belgique* qui, apparus au lendemain des attaques terroristes qui ont frappé Bruxelles, avaient été créés pour exprimer un soutien aux victimes (OTAN, COE Stratcom, 2016b) ;
- On estime aussi qu'au moins 16 % des comptes liés à Daech sont en fait automatisés (« bots ») (Shaheen).

25. Sur le terrain, Daech bat en retraite. L'année dernière, le prétendu Califat a perdu plus de 50% de son territoire en Syrie et plus de 70% en Iraq. Pour autant, on estime que Daech va renforcer ses activités en ligne. La sophistication de l'instrumentalisation des médias sociaux par Daech donne l'impression d'une organisation solide et efficace qu'il est apparemment intéressant de rejoindre (OTAN, COE Stratcom, 2016a). Daech se présente sur les réseaux sociaux comme un véritable défenseur de l'islam et comme un vecteur de changement. Son image de machine de guerre brutale et redoutable est associée à des images plus douces, montrant par exemple des soldats en train de manger des barres chocolatées *Snickers* et nourrissant des chatons (Farwell). Certains experts font observer que, depuis 2015, Daech produit davantage de contenu visant à normaliser le prétendu Califat plutôt que des contenus mettant en scène des actes de violence (Matejic). Cette présentation des choses semble avoir réussi à attirer de nouvelles recrues pour Daech.

26. Selon les estimations, plus de 30 000 personnes, dont environ 5 000 citoyens européens, se sont rendues en Syrie et en Iraq pour grossir les rangs d'organisations terroristes depuis le début du conflit dans ces deux pays en 2011. Il est difficile de savoir combien d'entre eux ont été radicalisés et recrutés via des réseaux sociaux, mais d'après le département de la justice des États-Unis, l'essentiel du recrutement de jeunes terroristes est lié aux médias sociaux. Le recrutement commence généralement sur une plateforme publique, sous forme d'échange d'idées radicales ; la conversation passe ensuite sur l'une des plateformes cryptées (telles que *WhatsApp*, *Kik* ou *Telegram*) où le recrutement peut se poursuivre en privé. Daech soumet les éventuels candidats à un ensemble de questions détaillées pour s'assurer qu'il ou elle n'est pas un agent du renseignement (OTAN, COE Stratcom, 2016b).

27. Outre la propagande et le recrutement, Daech utilise également les médias sociaux pour donner des conseils technologiques et des orientations à ses partisans. Les médias sociaux jouent aussi un rôle capital dans la stratégie de collecte de fonds de Daech (OTAN, COE Stratcom, 2016b). Toutefois, Daech s'efforce de limiter l'utilisation des réseaux sociaux pour les fonctions de commandement et de contrôle dans le but de cacher l'identité et la localisation de ses dirigeants (Farwell).

28. Quoi qu'il en soit, les réseaux sociaux sont une arme à double tranchant : ils servent également aux organismes de lutte contre le terrorisme pour collecter des informations et déjouer des attaques terroristes. À titre d'exemple, les services de sécurité israéliens se servent d'algorithmes spécialement conçus pour contrôler les comptes de jeunes palestiniens sur les réseaux sociaux afin d'identifier d'éventuels terroristes et, dans certains cas, ont réussi à déjouer des attaques suicide (*The Economist*, 2016a), Les analystes du COE Stratcom de l'OTAN affirment par ailleurs que, sous réserve d'obtenir des données suffisantes, ils pourraient déduire le nombre total de personnes recrutées par Daech dans le futur via des plateformes comme Twitter mais également le nombre total de combattants sur le terrain, certaines de leurs caractéristiques (âge, sexe, niveau d'éducation, etc.), et même, obtenir certaines informations sur les tactiques possibles et les stratégies employées (Shaheen).

B. LES MÉDIAS SOCIAUX COMME OUTIL DE POLITIQUE ÉTRANGÈRE : LE CAS DE LA RUSSIE

29. La Russie du président Vladimir Poutine exploite et mobilise, par le biais d'opérations d'information, des formes anciennes et nouvelles de médias pour atteindre ses objectifs de politique étrangère. Le Kremlin a « arsenalisé » l'information en faisant des médias une arme d'illusion/ de distraction massive, et *de facto* un prolongement de sa diplomatie et de son armée. Les origines de cette stratégie remontent à l'ère soviétique lorsque l'URSS employait des méthodes telles que le « contrôle réflexif » et les « mesures actives » pour tromper, manipuler et intimider ses adversaires en Occident. L'efficacité de ces méthodes durant la guerre froide a été limitée. Pour autant, l'essor d'Internet et des réseaux sociaux offre d'incroyables perspectives pour le Kremlin dans le domaine de la guerre de l'information.

30. L'intention de Moscou d'utiliser l'information et le cyberespace comme éléments essentiels de la sécurité nationale est exposée clairement dans plusieurs documents, les plus récents étant la Doctrine militaire de 2014, la Stratégie de sécurité nationale de 2015 et la Doctrine de sécurité de l'information de 2015. Ces documents présentent la Russie comme une victime de l'agression informationnelle des pays occidentaux, soulignent la nécessité de faire échec aux menaces informatiques pesant sur la sécurité et la souveraineté de la Russie et préconisent la mise au point d'un moyen efficace d'influencer l'opinion publique des autres pays. Dans son article souvent cité exposant les principes de la guerre hybride, le chef d'état-major des forces armées russes, Valéri Guérassimov, fait observer, entre autres, que « [l]'espace d'information ouvre de vastes possibilités asymétriques pour réduire le potentiel militaire de l'ennemi » (OTAN, COE Stratcom, 2015). S'exprimant devant la Douma d'État, le 22 février 2017, le ministre de la défense Sergueï Choïgu a annoncé que « les forces d'opérations informationnelles établies devraient être un outil bien plus efficace que tous ceux que nous avons utilisés jusqu'à présent à des fins de contre-propagande » (Rettman).

31. Selon Timothy Thomas, un expert renommé de la guerre de l'information soviétique/russe, la Russie considère que la guerre de l'information comporte deux aspects : un aspect technique et un aspect psychologique. Le premier couvre les moyens technologiques de collecter des données numériques utiles. Le deuxième inclut le concept de « psycho-virus » destiné à influer sur le subconscient et le comportement de la population. Selon un autre spécialiste réputé de la Russie, Mark Galeotti, l'importance que le Kremlin accorde à la guerre de l'information et autres techniques de la guerre hybride « trahit l'opportunisme parcimonieux d'une Russie faible mais impitoyable qui veut jouer le jeu d'une grande puissance sans en avoir les moyens ». Pour l'ancien directeur adjoint de la NSA (agence nationale de sécurité), John Chris Inglis, la Russie a dix ans d'avance sur les États-Unis dans le domaine de l'utilisation des médias sociaux dans des opérations d'information (Calabresi).

32. Les objectifs de la guerre de l'information menée par la Russie sont de deux ordres :

1) permettre à l'État de monopoliser l'espace informationnel au sein de la Russie afin de « neutraliser » les informations externes ciblant les Russes, « notamment la jeune génération, ayant pour but de porter atteinte aux valeurs spirituelles et morales traditionnelles de la Russie » ; et
2) projeter les intérêts de la Russie à l'étranger au moyen de nouvelles capacités technologiques.

33. Sur le plan du contrôle des médias nationaux, le président Poutine est arrivé au pouvoir avec un objectif clair : bâtir une « verticale du pouvoir » toute-puissante et progressivement museler tous les acteurs clés, y compris les organes de presse, les plaçant sous le contrôle du Kremlin. Depuis l'arrivée du président Poutine à la tête du pays, la note de la Russie par *Freedom House*[5] s'est peu à peu dégradée, le pays figurant dans la catégorie « non libres » depuis 2005. Jusqu'à récemment, l'accès à Internet en Russie était quasiment illimité. Toutefois, la liberté des activités en ligne en Russie a été remise en question par une série de mesures adoptées ces dernières années : la loi sur l'inscription des blogueurs (exigeant que les blogueurs ayant plus de 3 000 visiteurs s'enregistrent comme un organe de presse ; et donnant le droit aux autorités d'accéder aux informations de l'utilisateur), une loi qui permet au gouvernement de fermer n'importe quel site Web (ce droit a été utilisé pour bloquer les sites Internet des opposants Alexeï Navalny et Garry Kasparov) ; la loi sur le stockage des données personnelles (exigeant des fournisseurs d'accès Internet qui gèrent les données des clients russes de maintenir matériellement leurs serveurs sur le territoire russe, permettant ainsi aux services de sécurité de contrôler leurs activités) (Giles) et une nouvelle législation « antiterroriste » qui permet aux pouvoirs publics de sanctionner, voire d'emprisonner, des citoyens russes pour avoir partagé ou « liké » des articles sur les réseaux sociaux que le régime jugeait hostiles (Gregory). Les autorités publiques russes ont aussi imposé un changement de propriétaire au géant des réseaux sociaux russes *VKontakte*[6]. Le fondateur de *VKontakte*, Pavel Durov, a quitté l'entreprise en 2014, invoquant des difficultés à « préserver les principes sur lesquels notre réseau social est fondé ».

34. Selon certaines informations, la Russie renforce sa cybercoopération avec la Chine et étudie les méthodes de la « Grande muraille pare-feu de Chine » pour contrôler Internet. En juillet 2017, le président Poutine a signé une loi interdisant l'utilisation de ce que l'on appelle les « réseaux privés virtuels » et autres technologies « d'anonymat ». Ces technologies permettaient aux internautes de masquer leur identité pour être actifs sur les réseaux via un ordinateur tiers. Les internautes pouvaient ainsi accéder à des contenus en ligne interdits par des fournisseurs d'accès Internet contrôlés par l'État. En interdisant les réseaux privés virtuels, le gouvernement russe est en principe capable de censurer l'Internet par le biais d'une méthode proche de celle utilisée par la Chine.

5 *Freedom House* est un organisme indépendant de surveillance dédié à la progression de la liberté et de la démocratie à travers le monde. *Freedom House* utilise un système de notation pour évaluer les droits politiques et les libertés civiles dont jouissent les individus dans des pays donnés. Les notes sont attribuées chaque année au moyen d'une évaluation réalisée par une équipe composée d'analystes internes et externes ainsi que d'experts issus du milieu universitaire, de groupes de réflexion et de communautés de défense des droits humains. L'analyse fait appel à toute une série de sources parmi lesquelles : articles de presse, études universitaires, rapports d'organisations non gouvernementales, et contacts individuels avec des professionnels.

6 Les soupçons selon lesquels *VKontakte* serait contrôlé et exploité par les services de sécurité russes ont incité le gouvernement ukrainien à interdire l'utilisation de plateformes de médias sociaux russes sur le territoire ukrainien.

35. Enfin, des hackeurs pro-Russie et des trolls[7] ciblent régulièrement des hommes politiques et des journalistes de l'opposition. Parmi les méthodes utilisées, il y a notamment de fréquentes attaques de déni de service contre ce qu'il reste de médias libres, comme la station de radio *Ekho Moskvy* et le journal *Novaya Gazeta*, et la diffusion en ligne de documents compromettants (*kompromats*) sur les opposants au régime, obtenus auprès des services de sécurité russes.

36. Tout en renforçant le contrôle des médias nationaux, Moscou tire habilement parti de la nature pluraliste des médias dans les sociétés occidentales et du fait que les gouvernements occidentaux n'ont guère de contrôle sur les médias dans leur pays. Les ressources économiques et informationnelles sont infiniment plus importantes dans les pays occidentaux, mais la machine de désinformation russe semble avoir le dessus en raison de son professionnalisme ainsi que de son absence de scrupules et de frontières éthiques. Des experts de RAND Corporation ont qualifié le modèle de propagande russe de « lance à incendie mensongère » compte tenu de ses deux caractéristiques : un très grand nombre de canaux et de messages et une volonté éhontée de propager des vérités partielles ou des pures fictions (Paul et Matthews). Ces dernières années, la Russie a considérablement augmenté sa présence dans les médias mondiaux en dépensant des centaines de millions de dollars pour développer ses organes d'information multilingues tels que *RT* et *Sputnik*.

37. La stratégie d'information extérieure du Kremlin est également efficace car, à l'inverse de l'Union soviétique, la Russie du président Poutine ne projette pas une idéologie claire : sa machine de propagande n'a pas pour but de convaincre les opinions publiques de la supériorité du modèle russe. *RT* et *Sputnik* ne sont pas centrés sur la Russie. Le but est de démoraliser et de diviser les sociétés occidentales et d'établir une équivalence morale entre la Russie et les pays occidentaux en dénonçant l'hypocrisie occidentale. Par exemple, la réponse du Kremlin aux nombreuses déclarations en provenance des pays occidentaux selon lesquelles les élections législatives et présidentielle russes étaient truquées a été d'affirmer que les élections dans d'autres pays ne valaient pas mieux (IISS, 2016). D'après Matthew Sussex, expert de la politique étrangère et de sécurité russe, « les Russes ont compris que l'ensemble de l'Occident souffre d'une apathie générale des électeurs et qu'il existe une certaine défiance vis-à-vis de la politique et du gouvernement. Tout ce qui peut être fait pour renforcer cette défiance sert les intérêts de la Russie ». Cette méthode est par ailleurs relativement peu coûteuse car nul n'est besoin de pratiquer un journalisme d'investigation qui demande beaucoup de temps et d'argent. En conséquence, si la Russie n'a pas réussi à éviter la détérioration de son image dans le monde au lendemain de l'agression contre l'Ukraine, ses activités dans le domaine cybernétique et de l'information n'en ont pas moins contribué à accroître l'incertitude générale et à diviser l'Occident.

38. L'explosion de l'utilisation des médias sociaux offre de nouvelles possibilités pour la Russie d'influencer les populations et les hommes politiques dans des pays ciblés. La nature des techniques des réseaux sociaux, évoquées dans ce rapport, est propice à la stratégie de propagande du Kremlin, qui consiste à jeter la confusion plutôt qu'à convaincre et à remettre en

[7] Les *trolls* sont des individus qui créent et gèrent plusieurs faux comptes et identités en ligne afin d'atteindre un objectif donné et d'attaquer les opposants sur les réseaux sociaux. De nombreux rapports font état des activités que mène le gouvernement russe pour bâtir une « armée de trolls ». Si « l'usine à trolls » de Saint-Pétersbourg est un exemple souvent cité, il en existe bien d'autres sur l'ensemble du territoire russe. Les activités des trolls deviennent de plus en plus sophistiquées, et certains d'entre eux – par exemple, ceux appelés « bikini trolls » par les experts du COE Stratcom de l'OTAN – parviennent à créer une interaction avec leur cible, gagnant ainsi un certain degré de légitimité apparente et échappant à la vigilance des mécanismes anti-trolls. Selon une étude du COE Stratcom de l'OTAN portant sur 200 000 commentaires postés sur les trois principaux portails d'informations en ligne lettons, entre le 29 juillet et le 5 août 2014, 1,45 % de ces commentaires provenaient de « trolls hybrides », identifiés en partie par des fautes de grammaire, une répétition de contenu et les adresses IP. Mais dans certains récits concernant la Russie, plus de la moitié des commentaires provenaient de trolls russes.

cause l'existence même d'une vérité objective. Les guerriers russes de l'information réagissent aux grands événements internationaux avec une incroyable célérité et atteignent de vastes publics aux quatre coins du globe en diffusant des récits pro-Kremlin et en répandant des histoires non vérifiées ou fausses et des théories du complot. Selon les experts de RAND, les gens partent du principe qu'une information répétée et émanant de sources variées doit être vraie, sans se soucier de la crédibilité de ces sources (Paul et Matthews). C'est ce que l'on appelle en psychologie sociale « effet de vérité illusoire ». Dans le cadre des médias sociaux, où la quantité d'information est gage de crédibilité, l'appareil russe à fabriquer l'information sait parfaitement tirer profit de cette caractéristique en usant abondamment de trolls et de « bots[8] » pour atteindre ses objectifs.

39. Le Kremlin se livre à une vaste campagne de désinformation via les réseaux sociaux, lancée durant la révolution de l'Euromaïdan en Ukraine et qui se poursuit aujourd'hui. Depuis 2014, les guerriers russes de l'information ont inondé les réseaux sociaux de rapports fabriqués de toute pièce ou d'images trafiquées d'atrocités prétendument commises par les forces ukrainiennes, notamment de tortures et de meurtres d'enfants, de civils utilisés pour le trafic d'organes, voire d'actes de cannibalisme. Plusieurs théories du complot les plus folles ont fleuri sur les réseaux sociaux russes après le crash du vol MH17 de la Malaysia Airlines, en 2014, dans le but de convaincre le public que la vérité objective à propos de l'accident ne sera jamais établie. Exploitant le fait que l'information sur les réseaux sociaux est souvent transmise à travers des d'images, les pro-Kremlin ont largement représenté l'Ukraine et les Ukrainiens dans des contextes de violence et de symbolique fasciste. Ces campagnes de désinformation ont pour but de **semer la confusion et de désinformer** les utilisateurs des médias sociaux. Des équipes de lutte contre la propagande telles que *StopFake.org* et *EU Mythbusters* continuent à dénoncer, presque quotidiennement, les fausses informations que les réseaux sociaux russes déversent sur l'Ukraine.

40. Qui plus est, les campagnes russes de « fausses informations » sur les réseaux sociaux ciblent de plus en plus les publics occidentaux. En novembre 2016, la chancelière allemande Angela Merkel s'est inquiétée du fait que les « bots sociaux » et les trolls puissent servir à influencer l'opinion publique lors de la prochaine campagne électorale en Allemagne à l'instar de ce qui s'est passé en France et aux États-Unis. Le chef des services du renseignement allemand s'est également dit préoccupé face à la possible ingérence russe dans l'élection allemande par le biais de fausses informations. L'Alliance atlantique continue à être la cible de trolls russes, le plus récent exemple étant la diffusion d'une histoire inventée de toutes pièces à propos d'une jeune adolescente lituanienne violée par un soldat allemand qui faisait partie des troupes déployées en Lituanie, dans le cadre de la mission de présence avancée rehaussée (eFP) de l'OTAN dans les États baltes et en Pologne. Ces dernières années, la Russie a aussi clairement intensifié ses attaques virtuelles contre ses voisins nordiques, le Danemark, la Suède et la Finlande. La Russie aurait également ciblé des pays ne faisant pas partie de la communauté euro-atlantique. Par exemple en mai 2017, selon les conclusions auxquelles sont parvenus des membres des forces de police et des services du renseignement des États-Unis, des hackers pro-russes auraient lancé une cyberattaque contre l'agence de presse qatarie, en diffusant de fausses informations qui ont provoqué une onde de choc dans plusieurs États du Golfe et aux États-Unis.

41. Les guerriers virtuels du Kremlin propagent de fausses informations de diverses manières :

a) en créant de multiples comptes sur les réseaux sociaux, y compris des comptes en apparence dignes de foi, tels que des comptes en finnois *@Vaalit* (élections), *@Eduskuntavaalit* (élections législatives) (Giles),
b) en détournant des comptes (par exemple, le compte Twitter de la chaîne suédoise TV4 et un compte Twitter ouvert au nom de Peter Hultqvist, le ministre suédois de la défense) et,
c) en détournant des hashtags (par exemple le ministère russe des affaires étrangères a utilisé le hashtag *#UnitedforUkraine*, hashtag créé par le département d'État américain pour

[8] Selon une étude récente de l'Université d'Oxford, environ 45 % des comptes Twitter très actifs en Russie sont des bots.

soutenir l'Ukraine, pour poster des tweets avec les commentaires de Sergueï Lavrov, le ministre des affaires étrangères russe.

42. Les trolls d'État sont aussi utilisés par la Russie pour **semer la panique** : en 2014, une campagne coordonnée de plusieurs centaines de tweets a fait souffler un vent de panique aux États-Unis en annonçant un prétendu accident chimique dans une usine de Louisiane. Une enquête conduite par le *New York Times* a permis de déterminer que les tweets provenaient de Saint-Pétersbourg. Jeter l'effroi au sein de la population du Donbass en prétendant sur les réseaux sociaux que le réseau régional d'approvisionnement en eau était empoisonné est un autre exemple (OTAN, COE Stratcom, 2016a). Le succès de ces campagnes de désinformation pourrait encourager des manœuvres de ce type à plus grande échelle.

43. Ces trolls orchestrent par ailleurs des attaques visant à **intimider** et à réduire au silence les opposants du Kremlin comme en témoigne l'impressionnante campagne de harcèlement en ligne dont a été la cible la journaliste finnoise Jessikka Aro, y compris par la publication d'informations concernant sa vie privée. Autre cible de premier plan : Eliot Higgins, le fondateur du réseau de journalisme d'investigation *Bellingcat*, qui rendait compte des activités de la Russie en Ukraine. Le groupe de hackeurs pro-Kremlin *CyberBerkut* a piraté son compte email, son compte iCloud et son profil sur les réseaux sociaux et a mis en ligne sa photo, une copie scannée de son passeport, le nom de sa petite amie et d'autres informations privées. En mai 2017, un organisme de recherche canadien *The Citizens Lab* a publié un rapport révélant qu'une « cyber-campagne » de grande envergure avait été orchestrée contre plus de 200 opposants au Kremlin fortement médiatisés (responsables du gouvernement, journalistes et militants de la société civile) dans 39 pays. Le but de cette campagne était de voler des données numériques personnelles, de les trafiquer et de les divulguer pour discréditer les victimes de ce piratage. Le trolling pro-russe agressif et utilisé pour intimider a conduit plusieurs portails de médias, tels *Reuters* et *CNN*, à fermer leur rubrique « commentaires », ce qui a pour inconvénient de réduire les possibilités d'engager un débat en ligne constructif.

44. La Russie cible ses adversaires non seulement au niveau individuel, mais aussi à l'échelle industrielle. L'utilisation des réseaux sociaux, par exemple, par les militaires occidentaux déployés en Ukraine, donne aux organismes du gouvernement russe et à leurs sympathisants l'occasion de récolter de vastes quantités de données personnelles. Par le passé, des guerriers de l'information pro-russes se sont servis de ce genre de données pour harceler et intimider : par exemple, en janvier 2014, lorsque des personnes participant aux manifestations de Maïdan à Kiev ont reçu des messages SMS menaçants et, en novembre 2015, lorsqu'ils ont téléphoné massivement à des soldats polonais (Giles). Des hackers pro-russes auraient par ailleurs envoyé des messages personnalisés renfermant un virus à plus de 10 000 utilisateurs de Twitter au département de la défense dans le but d'accéder à leur téléphone ou ordinateur ainsi qu'à leurs comptes Twitter et d'en prendre le contrôle (Calabresi). Il est probable que le Kremlin va continuer à utiliser ces outils pour démoraliser et neutraliser ses adversaires, une réalité que les Alliés qui participent à la mission eFP doivent prendre tout particulièrement en compte.

45. Enfin, les réseaux sociaux peuvent **renforcer** les messages propagés par des **médias plus traditionnels**, tels que *RT* et *Sputnik*. *RT* produit un tweet toutes les deux minutes, dont grand nombre sont partagés des centaines de fois. Toutefois, l'analyse montre que la plupart des « retweets » et des « likes » sur Facebook de publications de *RT* ne viennent que relativement peu de ses abonnés. Une analyse révèle que sur les 50 comptes retweetant le plus souvent *RT*, 16 sont probablement des « bots » (*The Economist*, 2016b). C'est en partie grâce à ces manipulations que *RT* prétend être l'un des principaux organes de presse au monde. Il convient de noter que la relation de renforcement mutuel entre médias sociaux et médias traditionnels joue dans les deux sens. Par exemple, l'agence de presse russe *Ria Novosti* a relayé l'information - clairement fabriquée de toutes pièces - que 3 600 chars états-uniens devaient être déployés en Pologne (le nombre réel étant 87), ce qui a donné une certaine crédibilité et un écho plus large à ce récit qui a été produit par un groupe obscur de propagandistes en ligne basés dans le Donbass.

46. L'usage que fait la Russie des médias sociaux est éminemment sophistiqué et ingénieux, et pose un réel défi à la communauté euro-atlantique. Cela étant, le Kremlin n'est pas invincible dans ce domaine. Depuis le début de l'agression russe contre l'Ukraine, les pays occidentaux ont véritablement pris conscience de l'ampleur de la guerre de l'information que mène la Russie et en comprennent mieux les enjeux. Des techniques sont mises au point pour identifier les trolls et les « bots » avec davantage de précision. En Lettonie et en Lituanie, par exemple, des communautés qui se désignent sous le nom de « elfes » identifient les bots pro-russes et débusquent les fausses informations, faisant office de garde nationale civile et bénévole. Qui plus est, les médias sociaux ne sont pas sans danger pour la Russie : l'utilisation imprudente des réseaux sociaux par les soldats russes déployés dans le Donbass et en Crimée a fourni des preuves nombreuses et convaincantes de l'implication militaire de la Russie en Ukraine, discréditant les démentis du Kremlin. Cela dit, il faut s'attendre à ce que la Russie continue à développer des techniques et des capacités de guerre de l'information en réaction aux contre-mesures mises en place par les pays occidentaux. Par conséquent, les activités de la Russie dans le domaine de l'information devraient demeurer l'un des principaux défis pour la communauté euro-atlantique dans l'avenir proche.

IV. RELEVER LES DÉFIS POSÉS PAR LES MÉDIAS SOCIAUX POUR LA SÉCURITÉ

47. Les défis que pose la révolution des médias sociaux pour la sécurité nationale et internationale sont éminemment complexes et requièrent les efforts conjugués des autorités régionales, nationales et internationales, du secteur privé ainsi que de groupes infranationaux et transnationaux de militants. L'OTAN a pris certaines mesures pour intégrer la dimension des médias sociaux dans ses activités, notamment en matière de sensibilisation du public. L'OTAN compte plus de 1,2 millions d'abonnés sur Facebook et plus de 400 000 sur Twitter. Le secrétaire général de l'OTAN, le SACEUR et d'autres hauts responsables utilisent les réseaux sociaux, certains de manière plus active que d'autres. L'OTAN a lancé au printemps dernier la campagne en ligne *We Are NATO* pour « expliquer la mission fondamentale de l'OTAN qui est de garantir la liberté et la sécurité ». Le secrétaire général adjoint de l'OTAN pour la diplomatie publique, Tacan Ildem, a expliqué que la campagne entend éduquer et informer les jeunes générations des pays membres de l'OTAN et du monde entier au sujet du rôle que joue l'Alliance en matière de sécurité mondiale. Conformément à la politique militaire de l'OTAN en matière d'affaires publiques, il est rappelé au personnel de l'OTAN de se montrer prudent lorsqu'il utilise les réseaux sociaux et il est « recommandé au personnel de l'OTAN de consulter sa chaîne de commandement avant de publier sur l'Internet des informations et des images ayant trait à l'OTAN ». En septembre 2014, le SHAPE a adopté une directive sur les médias sociaux qui identifie les meilleures pratiques pour l'utilisation des médias sociaux en vue de renforcer l'engagement de l'OTAN auprès des audiences clés en temps de paix et pendant des opérations militaires.

48. Depuis le début du conflit russo-ukrainien, l'OTAN a accru ses capacités de communication et a renforcé sa division Diplomatie publique. Elle a augmenté l'aide en matière de sensibilisation du public à des pays partenaires comme l'Ukraine et la Géorgie. Le site Internet de l'OTAN « Relations OTAN-Russie : les faits » s'appuie sur les faits pour dénoncer les mythes que propage le Kremlin sur des questions telles que l'élargissement de l'OTAN ou la prétendue menace que représente l'OTAN pour la Russie. En janvier 2014, plusieurs pays de l'Alliance ont franchi une étape importante en établissant un Centre d'excellence de l'OTAN pour la communication stratégique à Riga, Lettonie. Le Centre a produit une série d'études de premier plan qui indiquent comment l'OTAN et ses membres peuvent faire face à des cyberactivités hostiles et déstabilisantes[9]. L'Organisation OTAN pour la science et la technologie a également mis au point le *Digital and Social Media Playbook*, qui est un outil d'évaluation de l'environnement

[9] Plusieurs études récentes sont en rapport direct avec l'objet de ce rapport, notamment *New Trends in Social Media* (décembre 2016), *Daesh Recruitment. How the Group Attracts Supporters* (novembre 2016), *The Kremlin and Daesh information Activities* (octobre 2016) et *Social media's role in 'Hybrid Strategies'* (septembre 2016).

informationnel constamment mis à jour ayant pour objet de comprendre les objectifs et les méthodes utilisées par les adversaires dans l'espace informationnel.

49. L'OTAN commence aussi à intégrer des opérations d'information ouverte via les réseaux sociaux dans ses exercices militaires : dans le cadre de l'exercice *Trident Juncture 2015*, les participants ont appris à produire rapidement de grands volumes de contenu pro-OTAN par le biais de comptes officiels sur les réseaux sociaux pour contrer les messages anti-OTAN. Il a été établi, au cours de l'exercice, que les sentiments hostiles à l'OTAN diminuaient à mesure que se faisaient entendre des voix pro-OTAN (en langues locales). Il faut souligner que la doctrine de l'OTAN ne prévoit pas, pour l'instant, le recours à des opérations clandestines d'information telles que l'utilisation de fausses identités, bots et trolls contre des audiences ciblées tandis qu'en règle générale, les opérations psychologiques ne peuvent être utilisées que dans le contexte d'une opération militaire déclarée par le Conseil de l'Atlantique Nord (OTAN, COE Stratcom, 2016a).

50. Les efforts déployés par l'**UE** pour contrer les fausses informations en ligne et la propagande hostile ont été confiés à deux nouveaux organismes : le groupe de travail *East StratCom Task Force* et l'Unité d'Interpol chargée du signalement des contenus sur Internet (IRU). Le premier, également appelé *Mythbusters*, est constitué d'une équipe de dix diplomates détachés au niveau national, ayant pour tâche de dénoncer la campagne de désinformation que mène quotidiennement la Russie. Il diffuse ses résultats sur son site Internet – via email et sur les plateformes des réseaux sociaux. Il n'a pas de budget propre et s'appuie essentiellement sur des données fournies par un réseau de plus de 400 experts, journalistes, responsables, ONG et groupes de réflexion, dans plus de 30 pays. En novembre 2016, le Parlement européen a adopté une résolution demandant à augmenter les capacités du groupe de travail. L'IRU, chargée de surveiller le contenu à caractère terroriste sur Internet et les plateformes des réseaux sociaux, collabore avec des fournisseurs de services pour dénoncer et supprimer ces contenus. Selon un rapport publié en juillet 2016, l'IRU a évalué et signalé en vue de leur suppression plus de 11 000 messages sur 31 plateformes en ligne. De ce fait, les fournisseurs en question ont supprimé plus de 91 % de ces contenus (Morelli et Archick).

51. Une série de mesures ont été adoptées ces dernières années à l'échelle nationale. Le principal instrument de contre-propagande des **États-Unis**, le Centre d'engagement mondial (GEC) du département d'État, créé en 2011, a été remodelé et renforcé en 2016. Le GEC est chargé de coordonner les messages antiterroristes américains (principalement anti-Daech) à destination des audiences étrangères, principalement en favorisant le développement d'un réseau mondial de « messagers positifs », notamment au travers des ONG et des journalistes d'investigation. Le GEC est relativement actif sur Twitter et l'une de ses tactiques consiste à encourager les messages anti-radicaux via des hashtags pro-Daech tels que *#accomplishmentsofISIS*. Les autorités états-uniennes ont également pris des mesures concernant l'utilisation des réseaux en matière de sécurité, parmi lesquelles :

a) une directive de mai 2016 signée par l'ancien directeur du renseignement national, James Clapper qui autorise la collecte d'informations affichées publiquement sur les réseaux sociaux sur de potentiels fonctionnaires fédéraux dans le cadre de la procédure d'habilitation de sécurité (il est important de souligner que cette politique impose d'importantes restrictions aux agences fédérales en matière de protection de la vie privée. Ainsi, les enquêteurs ne peuvent pas demander à quelqu'un, ou lui imposer, de communiquer le mot de passe de comptes privés ou encore de collecter des informations sur des individus autres que ceux faisant l'objet de l'enquête, sauf si la sécurité nationale est en jeu ; et
b) le projet de loi de juillet 2017, adopté à une large majorité par le Congrès américain, qui impose de nouvelles sanctions contre la Russie suite au rapport des services du renseignement américain établissant que des agences pro-russes ont piraté les serveurs du Comité national démocrate et ont divulgué des informations dans le but d'influencer l'issue de l'élection présidentielle américaine.

Il convient aussi de noter que le département de la sécurité intérieure a qualifié le système électoral des États-Unis d'« infrastructure critique », permettant ainsi à ce dernier d'aider plus facilement les administrations gouvernementales et locales à protéger leur système électoral.

52. Au **Royaume-Uni,** l'Unité de lutte contre le terrorisme sur Internet (CTIRU) porte à l'attention des fournisseurs de services les contenus qu'elle juge contraires à la législation antiterroriste du Royaume-Uni. Les plateformes suppriment de leur plein gré ces contenus si elles jugent qu'ils vont à l'encontre de leurs propres conditions de service. La CTIRU ne supprime pas d'elle-même un contenu. Depuis sa mise en place en février 2010, la CTIRU a collaboré avec plus de 200 fournisseurs de services de télécommunications et a réussi à faire supprimer plus de 260 000 contenus de type terroriste. Le service public de radiodiffusion BBC s'est joint à la lutte contre les fausses informations en renforçant *Reality Check*, un service de vérification des faits qui collaborera avec Facebook. En 2015, l'armée britannique aurait créé la 77e brigade, formée d'experts passés maîtres dans l'art d'utiliser les médias sociaux pour mener des opérations d'information non létales et pour lutter contre les messages hostiles.

53. **Le Canada**, lui aussi, juge les fausses informations - et autres usages des médias sociaux à des fins hostiles - préoccupantes. Le Comité permanent du patrimoine canadien de la Chambre des communes a récemment examiné cette question dans le cadre d'une étude plus large sur l'évolution du paysage médiatique au Canada. Le gouvernement canadien estime que la collecte de données fiables et l'identification des meilleures pratiques internationales pour contrer les messages terroristes sont des éléments fondamentaux de sa stratégie de lutte contre le terrorisme. Le Réseau canadien pour la recherche sur le terrorisme, la sécurité et la société (TSAS) joue un rôle clé dans la réalisation de ces objectifs. Établi en 2010 sous les auspices de Sécurité publique Canada (SP), le réseau d'universitaires nationaux et internationaux associés à TSAS, contribue au corpus mondial de connaissances sur l'utilisation des médias sociaux par les terroristes et les stratégies pour la contrer.

54. Les pouvoirs publics en **Allemagne**, en **France** et en **République tchèque**, à quelques semaines des élections qui devaient se tenir dans leur pays en 2017, étaient de plus en plus préoccupés par les attaques dont leurs systèmes politiques seraient la cible via les médias sociaux. En décembre 2016, le ministère allemand de l'intérieur a proposé de créer un Centre de défense contre la désinformation dans le but de contrer les fausses informations diffusées sur Internet et favoriser une nouvelle culture en matière de comportement en ligne, notamment le rejet de l'utilisation des « bots » sur les réseaux sociaux. Huit organes de presse français, dont l'AFP, BFM TV, L'Express et Le Monde se sont associés à Facebook et à Google pour lancer de nouveaux outils de vérification des faits visant à venir à bout des fausses informations. Toutes informations jugées fausses par au moins deux des partenaires du projet sont dénoncées comme telles. Le journal français Le Monde a aussi créé un service de vérification des faits *Les Décodeurs* et prévoit d'établir une base de données pour débusquer les *hoax*, qui permettra aux lecteurs de faire la distinction entre les sites diffusant de fausses nouvelles et les sites vérifiés. Le gouvernement tchèque a annoncé la création d'un Centre contre le terrorisme et les menaces hybrides, composé de 20 spécialistes à plein temps, chargés de lutter contre la désinformation, notamment à propos des migrants, que propagent les guerriers de l'information du Kremlin dans le but supposé de peser sur les résultats des prochaines élections qui doivent se tenir en octobre.

55. Compte tenu des caractéristiques du nouvel environnement informationnel mondial, les actions menées par les pouvoirs publics et les médias traditionnels ne suffiront pas, à elles seules, à remédier au problème. Des actions responsables menées par les quelques **réseaux sociaux** eux-mêmes, de par le contrôle qu'ils exercent, est essentiel au succès des efforts déployés par les pays occidentaux. Récemment, les principales entreprises des médias sociaux ont lancé plusieurs nouvelles initiatives. Au printemps dernier, Facebook a annoncé qu'il allait recruter 3 000 personnes supplémentaires pour signaler et repérer tout contenu mensonger. En décembre 2016, Facebook, Microsoft, Twitter et YouTube ont annoncé la création d'une base de données commune comprenant les empreintes numériques des contenus (images terroristes violentes,

vidéos aux fins de recrutement terroriste et autres images qui seront retirés de leurs plateformes). En juin, ces quatre grands groupes ont annoncé la création du Forum mondial de l'Internet contre le terrorisme, une plateforme de partage d'informations entre les géants de l'Internet, de sorte que les extrémistes violents ne soient plus accueillis par leurs services. En avril 2017, Facebook a pris des mesures à l'encontre de 30 000 faux comptes en France, ou les a supprimés, dans les mois qui ont précédé l'élection présidentielle française. Twitter dit avoir supprimé 235 000 comptes faisant l'apologie du terrorisme au cours des six premiers mois de 2016. Certains hommes politiques insistent sur le fait qu'il faut aller plus loin. La plateforme de partage de photos Instagram a introduit un outil de modération par mot clé pour éviter que des commentaires offensants ne soient affichés et pour réduire l'efficacité des trolls en supprimant automatiquement les commentaires qui renferment des mots inappropriés et/ou offensants que le titulaire du compte aura préalablement définis. Le navigateur Google Chrome a lancé une nouvelle extension appelée *First Draft NewsCheck*, qui aident les utilisateurs à authentifier les images et les vidéos et permet de partager ses conclusions avec d'autres utilisateurs. Google collabore par ailleurs avec YouTube, dans le cadre d'un programme appelé *Redirect Method*, pour viser les recrues potentielles de Daech et, à terme, les dissuader de rejoindre le groupe. Au moyen de mots clés et de phrases que recherchent souvent les gens attirés par Daech, ce programme redirige les internautes vers des clips sur YouTube, en arabe et en anglais, qui montrent des témoignages d'anciens extrémistes, des imams dénonçant le fait que Daech est une perversion de l'islam, et des clips décrivant les dysfonctionnements du prétendu califat de Daech.

56. Si les réseaux sociaux prennent un certain nombre de mesures pour supprimer les contenus liés au terrorisme, ils font l'objet de pressions croissantes pour faire davantage en la matière. En mai 2017, la commission spéciale des affaires intérieures du parlement britannique a publié un rapport selon lequel les grands groupes des réseaux sociaux sont « loin et c'est scandaleux » de prendre des mesures à l'égard des contenus illégaux et dangereux et le plus souvent « ne satisfont pas à une demande de suppression d'un contenu illégal ». La commission a demandé au gouvernement britannique d'envisager la possibilité d'exiger des groupes de médias sociaux de participer au coût de l'Unité de lutte contre le terrorisme sur l'Internet ainsi que d'imposer des « amendes significatives » aux entreprises qui omettent de supprimer un contenu illégal dans un délai précis[10]. Le Royaume-Uni et la France travailleraient déjà à mettre en place des politiques visant à établir une nouvelle responsabilité juridique pour les entreprises de technologie qui négligent de prendre des mesures contre les contenus inacceptables. En juin 2017, les législateurs allemands ont adopté la loi de contrôle des réseaux (communément appelée Loi Facebook) permettant d'infliger des amendes pouvant aller jusqu'à 55 millions d'euros aux géants de l'internet et aux médias sociaux qui ne suppriment pas un contenu haineux dans les 24 heures après avoir été posté.

57. Toutefois, certains spécialistes mettent en doute l'efficacité de ces nouvelles mesures. Par exemple, certains se montrent sceptiques à l'égard de plateformes de partage de l'information faisant observer que les grands groupes de médias sociaux demeurent avant tout des entreprises concurrentes qui n'ont aucun intérêt commercial à partager des informations. De même, les défenseurs de la liberté d'expression, tels que Joe McNamee, directeur exécutif de *European Digital Rights*, se disent préoccupés par des propositions laissant à des sociétés privées l'entière discrétion et responsabilité de décider si tel ou tel contenu est bon pour l'intérêt public ; ils estiment que de telles initiatives pourraient avoir l'effet inverse. Les opérateurs des médias sociaux peuvent aussi ne pas avoir les connaissances suffisantes pour déterminer si oui ou non ils ont affaire à des terroristes. Par exemple, Facebook a récemment censuré à tort un groupe de partisans de l'indépendance tchétchène, *Independence for Chechnya!,* en qualifiant ces opposants de terroristes.

---

10 En conséquence, en juin 2017, Facebook a lancé « Initiative pour le courage civil en ligne » (*Online Civil Courage Initiative*) qui a pour but de former les organisations à contrôler et à faire face au contenu extrémiste. Facebook a par ailleurs créé un service d'appui spécialisé où les problèmes peuvent être signalés. https://www.theguardian.com/technology/2017/jun/23/facebook-launches-drive-in-uk-to-tackle-online-extremist-material ,

V. CONCLUSIONS ET RECOMMENDATIONS

58. Comme toute avancée technologique majeure, l'explosion des médias sociaux présente à la fois des avantages et des inconvénients. Des acteurs non étatiques hostiles et des États autoritaires agressifs font preuve d'une grande habilité et d'une propension certaine à exploiter ces nouveaux moyens de communication pour parvenir à leurs fins. La réponse de la communauté euro-atlantique, jusqu'à présent, peut être décrite comme aléatoire, hésitante et non coordonnée. Dans une certaine mesure, cela est dû aux contraintes morales et juridiques inhérentes aux sociétés démocratiques. Pour autant, un certain nombre de mesures devraient être envisagées sérieusement par les pays membres de la communauté euro-atlantique afin de mieux s'adapter aux nouvelles réalités de l'ère de l'information.

59. Il faut apprendre à la population, et notamment à la jeune génération, à se montrer prudente dans la manipulation des médias sociaux. Des techniques sont mises au point pour reconnaître l'utilisation de trolls et de « bots » et ces techniques devraient être largement partagées – à l'instar de celles mises en œuvre dans les écoles primaires suédoises, où l'on enseigne notamment aux enfants, pour améliorer leur compétence numérique, à faire la distinction entre les sources qui sont fiables et celles qui ne le sont pas. Quant à la protection du processus électoral, les pouvoirs publics, les partis politiques et les commissions électorales doivent examiner les meilleures pratiques, notamment la stratégie adoptée par le nouveau président français Emmanuel Macron, dont l'équipe technique très compétente a mis en échec les tentatives du Kremlin de nuire à sa campagne. Les internautes devraient, quant à eux, être informés des bonnes pratiques, notamment les mesures de sécurité servant à protéger les informations privées qu'ils affichent sur leurs comptes. Les établissements scolaires et les grands médias devraient promouvoir la valeur d'un débat véritablement fondé sur des faits, et la réflexion critique, encourager les utilisateurs des réseaux sociaux à sortir de leurs bulles virtuelles, à élargir leurs interactions sur les réseaux sociaux et à nouer des échanges constructifs avec des personnes défendant des points de vue différents.

60. Face à ce déferlement d'informations, les gens continueront à rechercher des sources d'informations fiables. Les médias responsables peuvent rester compétitifs à condition qu'ils adoptent des solutions technologiques innovantes permettant d'évaluer la véracité des messages postés sur les réseaux sociaux concernant un sujet brûlant d'actualité. Par exemple, l'agence de presse internationale basée au Royaume-Uni *Reuters* a mis au point un algorithme basé sur le nombre de personnes qui suivent la source de la nouvelle et la structure même des messages. Soit un gage de confiance suffisant pour que Reuters tweete une nouvelle de dernière heure et demeure un acteur pertinent dans cet environnement informationnel en constante évolution. Comme l'a déclaré le secrétaire général adjoint de l'OTAN, Jamie Shea : « Les [médias] traditionnels ne doivent pas être réduits au silence mais doivent se concentrer sur les reportages traditionnels et la vérification des faits. Un public désorienté reviendra vers le journalisme de qualité – à condition qu'il existe encore. Les gouvernements doivent charger les conseils de presse de mettre en œuvre des normes objectives dans les médias en dénonçant et en pénalisant les organes de presse qui relaient délibérément de fausses informations ».

61. Les pays membres de l'OTAN, du moins ceux qui ne l'ont pas encore fait, devraient créer ou désigner des services spéciaux au sein de l'administration chargés de surveiller 24/24h – en collaboration avec les grandes plateformes - les utilisations malveillantes des médias sociaux, de dénoncer les fausses informations et la propagande hostile, et de les combattre en leur opposant des faits. Les chercheurs et les groupes de réflexion, spécialisés dans les communications en ligne, devraient bénéficier d'un soutien accru pour garder une longueur d'avance. Les capacités existantes de l'OTAN et de l'UE telles que la division Diplomatie publique de l'OTAN et *East StratCom Task Force* de l'UE devraient se voir accorder des moyens financiers et technologiques supplémentaires ainsi que des ressources humaines afin de continuer à fournir en ligne, aussi souvent que possible, des réponses convaincantes (même s'il ne sera peut-être jamais possible de suivre le rythme de propagation des fausses informations). La politique des services de

renseignement en matière d'informations classifiées doit être revue pour permettre aux responsables des relations publiques de pouvoir utiliser des informations jugées moins sensibles, et notamment des images satellites, pour contrer la désinformation.

62. Les institutions euro-atlantiques devraient régulièrement revoir leurs politiques en matière de médias sociaux, adapter le contenu et le format de leurs communications aux besoins des utilisateurs mobiles (les messages doivent être courts, cohérents, graphiques, ciblés et nombreux), et intégrer un volet « réseaux sociaux » à la formation et aux travaux de leur personnel. Des mesures de défense destinées à protéger l'identité et les adresses personnelles des membres de la famille des soldats doivent être mises en place au sein de l'Alliance. Dans les quartiers généraux, la capacité d'utiliser les médias sociaux doit être mise en place à tous les niveaux de commandement et non pas exclusivement au profit des attachés de relations publiques et des officiers de renseignement. Avec toute la prudence requise, les médias sociaux et les plateformes de messagerie peuvent offrir des solutions pratiques et conviviales aux opérations de commandement et de contrôle – le conflit entre le FBI et Apple à propos du chiffrement semble indiquer que les protocoles de sécurité mis en place par les entreprises commerciales sont au moins aussi efficaces que nombre de ceux utilisés par les autorités (Tunnicliffe & Tatham).

63. Outre la présence accrue sur les réseaux sociaux d'internautes qui font entendre un discours démocratique, modéré et basé sur des faits, certaines mesures restrictives sont également nécessaires pour supprimer la cyberactivité des terroristes et le trolling sponsorisé par l'État. Selon les termes de la RAND Corporation, « n'espérez pas contrer une lance à incendie mensongère avec un pistolet à eau de la vérité (Paul et Matthews). La coopération avec le monde des médias sociaux pour supprimer les contenus radicaux, les discours haineux et les fausses informations des plateformes en ligne doit se poursuivre et les guerriers de l'information les plus influents, tels les principaux propagandistes de Russie, doivent être soumis à des sanctions occidentales.

64. Face à la structure centre-périphérie mise en place par Daech sur les réseaux sociaux, les experts du COE Stratcom de l'OTAN proposent de supprimer autant que possible des groupes entiers de comptes associés à Daech, qu'ils soient actifs ou inactifs, pour éviter que des comptes inactifs relaient la propagande lorsque ceux qui sont actifs sont fermés. Cette méthode pourrait accroître les coûts de transaction marginaux pour les activités terroristes sur les réseaux sociaux, les forçant à continuellement reconstruire leur infrastructure à partir de zéro (Shaheen). Ces activités des services de sécurité ont aussi besoin d'être mieux coordonnées dans l'ensemble de la communauté euro-atlantique.

65. La plupart des médias sociaux étant la propriété de sociétés multinationales privées, il est nécessaire d'améliorer la coopération avec ces entreprises. Des mesures prises à l'échelle nationale pour lutter contre les contenus illégaux sont souvent inefficaces car, la plupart du temps, ces contenus sont hébergés sur des sites situés en dehors des frontières nationales. Il est donc important que la mise au point et l'utilisation volontaires de logiciels anti-trolling et de vérification de faits ainsi qu'une surveillance accrue des réseaux par les entreprises soient encouragées. Pour éviter que les pouvoirs publics n'imposent des règles excessives au domaine cybernétique, il serait préférable que les médias sociaux adoptent eux-mêmes des politiques internes rigoureuses. Ces groupes doivent aussi continuer à revoir certains des nouveaux outils qu'ils ont créés pour identifier tout contenu néfaste[11], s'assurer qu'ils ne sont pas plus nuisibles que bénéfiques, et adopter les algorithmes permettant de promouvoir un bon journalisme d'investigation et non des histoires à sensation. Si l'on demande à des plateformes telles que Twitter et Facebook d'assumer une plus grande responsabilité dans la suppression de messages terroristes et de fausses

[11] Par exemple, des experts notent que les premiers efforts déployés par Facebook pour lutter contre la désinformation en qualifiant un post de « litigieux » semblent avoir contribué à générer du trafic vers ce contenu. Facebook a été fortement incité à appeler les choses par leur nom et à remplacer ce qualificatif par « fausse ». http://www.atlanticcouncil.org/blogs/ukrainealert/will-facebook-finally-fight-disinformation-or-just-make-things-worse

informations, il faut que les gouvernements occidentaux le fassent de manière constructive et concertée. Il ne faut pas oublier que les entreprises occidentales n'ont pas le monopole des médias sociaux, et que les utilisateurs peuvent rapidement migrer vers d'autres plateformes, notamment la célèbre plateforme chinoise WeChat (même si elle est pour l'instant essentiellement destinée au marché chinois). Les pouvoirs publics doivent aider à former les acteurs des médias sociaux pour leur permettre de repérer plus efficacement un contenu et des activités terroristes et extrémistes.

66. La société civile est un allié puissant des gouvernements démocratiques pour lutter contre l'extrémisme et les fausses informations. Soutenir des initiatives locales telles que *Stopfake.org* (qui dénonce les fausses informations du Kremlin) et mobiliser des responsables locaux crédibles ainsi que des « elfes » (les chasseurs volontaires de trolls) pourrait donner aux sociétés occidentales l'avantage dans l'espace informationnel.

67. Si l'Occident a inventé les médias sociaux, rien dans leur genèse n'a jamais permis d'assurer que leurs réseaux ou utilisateurs adopteraient les valeurs occidentales. La lutte contre ces nouvelles menaces doit être placée au premier rang des priorités de la communauté euro-atlantique. L'utilisation à des fins terroristes et autres usages hostiles des médias sociaux ont déjà provoqué la perte de vies humaines et menacent d'affaiblir et de diviser le monde occidental. Pour autant, il est important que la communauté euro-atlantique maintienne un sens moral élevé dans les médias sociaux et s'abstienne de recourir aux méthodes peu scrupuleuses de ses ennemis. L'ouverture, le pluralisme et l'inclusion sont indispensables pour discerner le vrai du faux[12]. La rapporteure espère que ce rapport contribuera à mieux prendre conscience de l'ampleur de ce défi.

[12] L'architecture de Wikipédia est un exemple type : son contenu très pointu est dû au fait que toute personne peut y apporter des éléments et que chacun peut les contester en fournissant des sources vérifiables. Durant ce processus ouvert, de nombreuses révisions permettent de réduire les distorsions, les incohérences et les inexactitudes du contenu de Wikipédia.

BIBLIOGRAPHIE SÉLECTIVE

Adornato, Anthony C. “Forces at the Gate: Social Media’s Influence on Editorial and Production Decisions in Local Television Newsrooms.” *SAGE*, vol. 10, no. 2, 2016.

Alexander, Lawrence, and Craig Silverman. “How Teens In The Balkans Are Duping Trump Supporters With Fake News.” BuzzFeed, 4 novembre 2016. https://www.buzzfeed.com/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo

Anderson, Monica. “More Americans Are Using Social Media to Connect with Politicians.” Pew Research Center, 19 mai 2015. http://www.pewresearch.org/fact-tank/2015/05/19/more-americans-are-using-social-media-to-connect-with-politicians/

Ansley, Rachel. “Trump Must Stand Up to Russian Cyberattacks.” Atlantic Council, 11 janvier 2017. http://www.atlanticcouncil.org/blogs/new-atlanticist/trump-must-stand-up-to-russian-cyberattacks

Bodine-Baron, Elizabeth, Todd Helmus, Madeline Magnuson and Zev Winkelman. Examining ISIS Support and Opposition Networks on Twitter. RAND Corporation, 2016. https://www.rand.org/pubs/research_reports/RR1328.html. Also available in print form.

Calabresi, Massimo. “Inside Russia’s Social Media War on America.” *Time*, 18 mai 2017. http://time.com/4783932/inside-russia-social-media-war-america/

Carafano, James Jay. “Twitter Kills: How Online Networks Became a National-Security Threat.” Text. The Heritage Foundation, 8 juin 2015. http://www.heritage.org/defense/commentary/twitter-kills-how-online-networks-became-national-security-threat

Duggan, Maeve, and Aaron Smith. “The Political Environment on Social Media.” Pew Research Center, 25 octobre 2016

The Economist. “Extreme Tweeting.” 19 novembre 2015. http://www.economist.com/news/europe/21678828-few-social-media-stars-among-europes-politicians-are-centrists-extreme-tweeting

The Economist. “Israel Is Using Social Media to Prevent Terrorist Attacks.” The Economist, 18 avril 2016a. http://www.economist.com/news/middle-east-and-africa/21697083-new-paradigm-intelligence-israel-using-social-media-prevent-terrorist

The Economist. “Tweetaganda.” The Economist, 10 septembre 2016c. http://www.economist.com/news/europe/21706534-tweetaganda

Farwell, James P. “The Media Strategy of ISIS,” 1er décembre 2014. https://www.iiss.org/en/publications/survival/sections/2014-4667/survival--global-politics-and-strategy-%20december-2014-january-2015-bf83/56-6-04-farwell-97ca

Giles, Keir. “The Next Phase of Russian Information Warfare,” 2016. http://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles

Gottfried, Jeffrey, and Elisa Shearer. “News Use Across Social Media Platforms 2016.” Pew Research Center’s Journalism Project, 26 mai 2016. http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/

Gregory, Paul Roderick. “Under Russia’s New Extremism Laws, Liking My Writings On Ukraine Could Mean Jail Terms.” Forbes, 29 août 2016. http://www.forbes.com/sites/paulroderickgregory/2016/08/29/under-russias-new-extremism-laws-liking-my-writings-on-ukraine-could-mean-jail-terms/

Guilbeault, Douglas, and Samuel Woolley. “How Twitter Bots Are Shaping the Election.” The Atlantic, 1er novembre 2016. https://www.theatlantic.com/technology/archive/2016/11/election-bots/506072/

International Institute of Security Studies (IISS). “Informationi Warfare and the US Presidential Election,” 12 septembre 2016. https://www.iiss.org/publications/survival/sections/2016-5e13/survival--global-politics-and-strategy-october-november-2016-ff0a/58-5-03-inkster-bafe

Lange-Ionatamishvili, Elina, and Sanda Svetoka. “Strategic Communications and Social Media in the Russia Ukraine Conflict.” NATO Cooperative Cyber Defence Centre of Excellence, 2015. http://www.stratcomcoe.org/strategic-communications-and-social-media-russia-ukraine-conflict

Lee, Timothy B. “Facebook’s Fake News Problem, Explained.” Vox, 16 novembre 2016. http://www.vox.com/new-money/2016/11/16/13637310/facebook-fake-news-explained

Lynch, Marc. “After Egypt: The Limits and Promise of Online Challenges to the Authoritarian Arab State.” Perspectives on Politics vol. 9, no. 2, 3 juin 2011.

Margetts, Helen, Peter John, Scott Hale, and Taha Yasseri. “Political Turbulence: How Social Media Shape Collective Action.” Princeton University Press, 11 janvier 2017. http://press.princeton.edu/titles/10582.html

Matejic, Nicole. “Content Wars: Daesh’s Sophisticated Use of Communications.” NATO Review, 2016. http://www.nato.int/docu/review/2016/Also-in-2016/wars-media-daesh-communications-solis/EN/index.htm

Morelli, Vincent L., and Kristin Archick. “European Union Efforts to Counter Disinformation.” Congressional Research Service, 1 décembre2016. https://fas.org/sgp/crs/row/IN10614.pdf

Nissen, Thomas Elkjer. “#TheWeaponizationOfSocialMedia: @Characteristics_of_Contemporary_Conflicts.” Royal Danish Defence College, 2015. http://www.fak.dk/publikationer/Documents/The%20Weaponization%20of%20Social%20Media.pdf?pd%20fdl=theweaponizationofsocialmedia?pdfdl=TheWeaponizationOfSocialMedia

OTAN, Centre d’excellence pour la communication stratégique (StratCom). “Internet Trolling as a Hybrid Warfare Tool: The Case of Latvia,” 2015. http://www.stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia-0

OTAN, Centre d’excellence pour la communication stratégique (Stratcom). “Social Media as a Tool of Hybrid Warfare,” May 2016a. http://www.stratcomcoe.org/social-media-tool-hybrid-warfare

OTAN, Centre d’excellence pour la communication stratégique (Stratcom). “Daesh Recruitment: How the Group Attracts Supporters,” Novembre 2016b. http://www.stratcomcoe.org/daesh-recruitment-how-group-attracts-supporters-0

OTAN, Centre d’excellence pour la communication stratégique (StratCom). “New Trends in Social Media,” Décembre 2016. http://www.stratcomcoe.org/new-trends-social-media.

Paul, Christopher and Miriam Matthews. The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It. RAND Corporation, 2016. https://www.rand.org/pubs/perspectives/PE198.html

Pettigrew, Erin. “How Facebook Saw Trump Coming When No One Else Did.” 9 novembre 2016. https://medium.com/@erinpettigrew/how-facebook-saw-trump-coming-when-no-one-else-did-84cd6b4e0d8e

Polonski, Vyacheslav. “Impact of Social Media on the Outcome of the EU Referendum.” The Centre for the Study of Journalism, Culture and Community, juillet 2016.

Rettman, Andrew. “Russian Military Creates ‘Information Force,’” 23 février 2017. https://euobserver.com/foreign/137004

Ruane, Kathleen Ann. “The Advocacy of Terrorism on the Internet Freedom of Speech Issues and the Material Support Statutes.” Congressional Research Service, 8 septembre 2016. https://fas.org/sgp/crs/terror/R44626.pdf

Schmitt, Eric. “U.S. Intensifies Effort to Blunt ISIS’ Message.” The New York Times, 16 février 2015. https://www.nytimes.com/2015/02/17/world/middleeast/us-intensifies-effort-to-blunt-isis-message.html

Schultz, Teri. “Why the ‘Fake Rape’ Story against German NATO Forces Fell Flat in Lithuania.” DW.COM, 23 février 2017. http://www.dw.com/en/why-the-fake-rape-story-against-german-nato-forces-fell-flat-in-lithuania/a-37694870

Shaheen, Joseph. “Network of Terror: How Daesh Uses Adaptive Social Networks to Spread Its Message,” novembre 2015. http://stratcomcoe.org/network-terror-how-daesh-uses-adaptive-social-networks-spread-its-message

Shane, Scott. “From Headline to Photograph, a Fake News Masterpiece,” The New York Times, 18 janvier 2017. https://www.nytimes.com/2017/01/18/us/fake-news-hillary-clinton-cameron-harris.html

Thompson, Alex. “Journalists and Trump Voters Live in Separate Online Bubbles, MIT Analysis Shows,” 8 décembre 2016. https://news.vice.com/story/journalists-and-trump-voters-live-in-separate-online-bubbles-mit-analysis-shows

Travis, Alan. “MPs Say Facebook, Twitter and YouTube ‘Consciously Failing’ to Tackle Extremism.” The Guardian, 25 août 2016, https://www.theguardian.com/politics/2016/aug/25/mps-facebook-twitter-youtube-extremism-isis

Tunnicliffe, I., & Tatham, S. (2017, avril 21). *Social Media—The Vital Ground: Can We Hold It? War College of US Army: http://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1349*

Wakefield, Jane. “Social Media ‘Outstrips TV’ as News Source for Young People.” BBC News, 15 juin 2016, sec. Technology. http://www.bbc.com/news/uk-36528256