CDS

064 CDSDG 17 F
Original : anglais

Assemblée parlementaire de l'OTAN

COMMISSION
SUR LA DIMENSION CIVILE DE LA SÉCURITÉ

LA RÉVOLUTION DES MÉDIAS SOCIAUX : INCIDENCES POLITIQUES ET SÉCURITAIRES

PROJET DE RAPPORT*

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

www.nato-pa.int 13 avril 2017

* Aussi longtemps que ce document n'a pas été adopté par la commission sur la dimension civile de la sécurité, il ne représente que le point de vue de la rapporteure.

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 ces dernières années, véritablement inouïe[2] a été facilitée par l'essor rapide des appareils mobiles connectés à Internet (smartphones) (Poushter). 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 % seulement sur Facebook (Gottfried et Shearer). Dans le monde libre, les médias sociaux supplantent déjà la télévision comme principale source d'information parmi la jeune génération (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 également la façon dont nous envisageons la sécurité, souvent de manière imprévue et exige de trouver des réponses innovantes. Twitter et Facebook font entendre la voix des citoyens tout en leur permettant de se connecter à moindre coût et de manière plus intime et de communiquer et de s'organiser entre eux et avec leur gouvernement. Toutefois, les médias sociaux offrent aussi de nouvelles possibilités à ceux qui cherchent à perturber l'ordre démocratique progressiste en tirant profit de l'ouverture intrinsèque au cyberespace. L'anonymat qui est possible sur les réseaux sociaux enhardit ceux qui propagent un discours haineux mais également les militants des droits civils qui peuvent dénoncer des régimes autoritaires sans crainte de représailles. Les médias sociaux étant un phénomène récent, il est difficile de prévoir toutes les conséquences possibles d'une telle révolution. L'objectif du présent projet de rapport est, avant tout, de sensibiliser les membres de l'Assemblée parlementaire de l'OTAN et 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.

II. MÉDIAS SOCIAUX ET GOUVERNANCE DÉMOCRATIQUE

3. 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 sur le gouvernement et la vie politique. Twitter signalait que l'élection présidentielle aux États-Unis a généré plus d'un milliard de tweets, et que

---

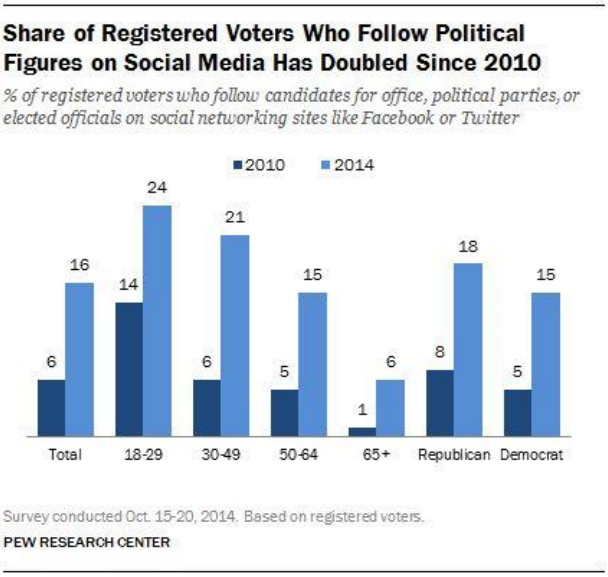
1 Les « médias sociaux » se définissent ainsi : les utilisateurs créent leur compte/profil personnel, le rendant totalement ou partiellement public ; le profil des utilisateurs et le contenu qu'ils génèrent sont mis en réseau. Diverses plateformes de réseaux sociaux ont des spécificités propres : par exemple, Twitter est dédié à des messages courts, Instagram se spécialise dans les vidéos et les images 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 dans les pays en développement.

près de 128 millions d'internautes ont parlé de l'élection présidentielle sur Facebook aux États-Unis (Thompson). 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 (InNetworkNet).

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)

4. Bien plus qu'une simple source d'information et une caisse de résonance, l'activité des internautes sur les sites des réseaux sociaux permet, empiriquement, d'envisager les campagnes. 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 aussi constaté que l'activité des internautes sur Facebook laissait présager du résultat d'élection américaine alors que les sondages traditionnels ne le permettaient pas. Durant le référendum du Royaume-Uni sur l'Union européenne, des chercheurs ont observé une plus grande activité et soutien pour la campagne du '*Leave*' sur Instagram et Twitter que pour la campagne en faveur du '*Remain*'. Ils ont conclu que durant le référendum, les militants ont sous-estimé le soutien des réseaux sociaux pour la campagne du '*Leave*' et la façon dont il se traduirait dans les urnes (Polonski).

5. 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 fragmentés. De même, les médias sociaux génèrent des informations en cascade – lorsque quelqu'un prend le risque d'exprimer un avis différent en premier, ceux qui autrement ne se seraient pas manifestés 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 faire du bruit autour des violences faites envers les manifestants » (Lynch).

6. Les manifestations iraniennes en 2009 (lorsque la population est descendue dans la rue pour protester contre la victoire électorale de 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. Ce sont les soulèvements arabes, en 2011, qui ont cependant 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 central des médias sociaux dans la mobilisation sociale : 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 (Barberá et Metzger).

7. 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, Alexei Navalny, qui a produit une vidéo de 50 minutes exposant au grand public la richesse phénoménale du premier ministre Dimitry Medvedev, tirant parti, entre autres, des pulsions immodérées 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.

8. 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, en 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 (Güner). Les réseaux sociaux ont joué un rôle déterminant dans l'échec de la tentative de coup d'État de juillet 2016 en Turquie : 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.

9. 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 nécessairement 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 MIT, le commentaire politique en ligne est cloisonné car les internautes occupent 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).

10. Rien ne prouve que le cloisonnement des réseaux contribue à polariser le monde politique. Les données elles-mêmes ne suffisent pas à expliquer pourquoi les utilisateurs sont si polarisés. Les algorithmes « préférence utilisateur » et les « bots » 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 organiser les contenus destinés aux abonnés. À l'aide des données recueillies sur leurs comportements et préférences manifestés 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 la vision

que l'utilisateur a du monde. Par ailleurs, la probabilité d'être confronté(e) à des opinions dissidentes ou contradictoires est réduite (Lee ; Thompson). De manière caractéristique, Facebook et d'autres plateformes répugnent à l'idée d'introduire un bouton « j'aime pas ». La fréquence accrue du débat ne se traduit donc pas nécessairement par une réelle confrontation d'idées, qu'elles soient différentes ou contradictoires.

11. 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. Ils sont largement utilisés et ont déjà démontré 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 sensible pour donner davantage de poids à leur thématique, notamment lorsqu'ils programment des « bots » pour en relayer le contenu en leur nom. Les titulaires de compte qui reçoivent un contenu relayé, le plus souvent, ne savent pas qu'ils interagissent avec un « bot » (Guilbeault et Woolley).

12. 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).

13. 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 minent 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 modèle « par click » (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 contester la source (BBC, 2016). Selon une étude de l'*Ithaca College* (New York) parmi les salles de rédaction locales qui ont adopté une politique en matière de réseaux sociaux, 40 % d'entre elles n'ont pas de procédures permettant de vérifier le contenu des médias sociaux avant de le diffuser (Adornato). Les sondages semblent indiquer qu'une relation positive pourrait exister entre la prolifération d'informations fausses et excessivement partisanes et la perception qu'ont les citoyens de leur gouvernement. Les données des sondages Gallup confirment l'idée que la défiance envers les gouvernements s'accroît et n'a jamais été aussi forte (Gallup, 2017).

14. En résumé, les médias sociaux ont un impact profond sur les démocraties. Les médias sociaux peuvent rendre les sociétés démocratiques plus pluralistes, mais pas dans le sens traditionnel où on l'entend. Certains experts dénoncent, au contraire, l'émergence d'un « pluralisme chaotique » (*The Economist*, 2016b), à savoir, un pluralisme qui offre une diversité de voix mobilisées [et de mouvements], mais qui est souvent imprévisible, instable et précaire (*Princeton Publishing*). 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

15. 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 peut 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 (Apps). 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).

16. Les frappes aériennes des États-Unis contre l'un des commandements de Daech à partir d'informations postées sur un réseau social par un militant de Daech en juin 2015 (Yeung et Oliker), la surveillance des messages sur Twitter en provenance de Tripoli par des responsables du renseignement de l'OTAN durant la campagne de Libye (Norton-Taylor et Hopkins), de très nombreux tweets par des équipes dédiées de l'armée israélienne durant le conflit de 2014 à Gaza, échangeant parfois directement des messages en ligne avec des agents du Hamas (MacAskill) 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 (Westcott) 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 participant à l'exercice en analysant les informations librement accessibles sur les réseaux sociaux (Ryan et Thompson).

17. La section suivante explique comment un acteur non étatique et un État – respectivement l'organisation terroriste Daech[3] et la Russie – sont passés maîtres dans l'art de transformer ce nouveau moyen de communication en arme de guerre.

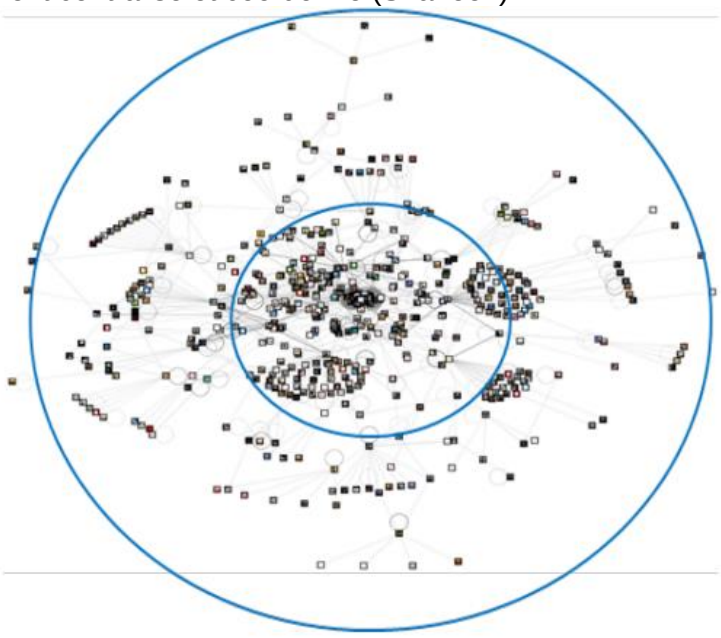
A. DAECH ET LES MÉDIAS SOCIAUX

18. 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 Shabaab 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 (Ruane). 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 (Sheikh Ali). 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 l'Occident se sont inspirés de sermons en ligne du prédicateur radical Anwar al-Awlaki (Ruane).

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

19. Cependant, il est communément admis que Daech a donné une nouvelle dimension à l'utilisation malveillante des réseaux sociaux. Daech semble avoir compris la dimension des réseaux sociaux désignée par l'expression « 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).

20. Les experts du 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).



Core-periphery structures are noted for a central group of actors followed by a larger but less dense network. This figure shows an example of one of our collected traffic networks with an added circular visualization to illustrate coreness.

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

21. 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 éviter cet écueil, les agents de Daech ont mis au point une série de mesures. Les cyber agents 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 inhérent 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).

22. 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 chaque 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, 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 tweets, produisant 50 % de tweets en plus par jour (Bodine-Baron et al.).

23. 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) (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 (StratCom, 2016b) ;
- On estime aussi qu'au moins 16 % des comptes liés à Daech sont en fait automatisés (« bots ») (Shaheen).

24. 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 (StratCom, 2016a). Daech se présente sur les réseaux sociaux comme un véritable défenseur de l'Islam et

[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.

comme un facteur 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 Califat plutôt que des contenus mettant en scène des actes de violence (Matejic). Ce récit semble avoir réussi à attirer de nouvelles recrues pour Daech.

25. Selon les estimations, plus de 30 000 personnes, dont environ 5 000 citoyens européens, se sont rendus 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 (Taylor). Le recrutement commence généralement sur une plateforme publique, sous forme d'échange d'idées radicales ; la conversation passe ensuite sur l'une des plateformes encryptées (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 (StratCom, 2016b).

26. 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 (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).

27. 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 sur les réseaux sociaux de jeunes palestiniens afin d'identifier de éventuels terroristes et, dans certains cas, ont réussi à déjouer des attaques suicides (*The Economist*, 2016a), Les analystes du 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

28. La Russie de Poutine exploite et mobilise diverses formes de médias, dont les réseaux sociaux pour atteindre ses objectifs de politique étrangère. Le Kremlin a « arsenalisé » l'information[5] en faisant des médias une arme d'illusion/distraction massive, et *de fait* 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.

29. 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

[5] Le terme a été popularisé par Pomerantsev et Weiss.

informatiques contre la sécurité et la souveraineté de la Russie et préconisent la mise au point de moyens efficaces 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, Valery Gerasimov, fait observer, entre autres, que « [l]'espace d'information ouvre de vastes possibilités asymétriques pour réduire le potentiel militaire de l'ennemi » (StratCom, 2015). S'exprimant devant la Douma d'État, le 22 février 2017, le ministre de la défense Sergey Shoigu 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).

30. 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 » (Coalson) ; et
    2) protéger les intérêts de la Russie à l'étranger au moyen de nouvelles capacités technologiques.

31. Sur le plan du contrôle des médias nationaux, Vladimir Poutine est arrivé au pouvoir avec un objectif clair : bâtir un « pouvoir vertical » et progressivement museler tous les acteurs clés, y compris les organes de presse, les plaçant sous le contrôle du Kremlin. Depuis l'arrivée de Poutine à la tête du pays, la note de la Russie par *Freedom House*[6] 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 autorités 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 ont aussi imposé un changement de propriétaire du géant des réseaux sociaux russes *VKontakte*. 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 (RFE/RL, 2016). Enfin, des hackeurs pro-gouvernementaux et des trolls ciblent régulièrement des hommes politiques et des journalistes de l'opposition, notamment via de fréquentes attaques de déni de service contre ce qui reste des 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.

32. Tout en renforçant le contrôle des médias nationaux, Moscou tire habilement parti de la nature pluraliste du paysage médiatique du monde libre et du fait que les gouvernements occidentaux n'ont guère de contrôle sur les médias dans leur pays. Les ressources économiques et en matière d'information 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 fictions pures et simples (Paul et Matthews). Ces dernières

[6] *Freedom House* est un organisme indépendant de surveillance dédié à la progression de la liberté et de la démocratie à travers le monde.

années, la Russie a considérablement augmenté sa présence dans les médias mondiaux en dépensant des centaines de millions de dollars pour développer des organes d'information multilingues tels que RT et *Sputnik*.

33. La stratégie d'information extérieure du Kremlin est également efficace car, à l'inverse de l'Union soviétique, la Russie de Poutine ne projette pas une idéologie claire ; sa machine de propagande n'a pas pour but de convaincre les opinions publiques que le modèle de la Russie est supérieur. 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 l'Occident en dénonçant l'hypocrisie occidentale. 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). Grâce à cette stratégie, si le Kremlin 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 ont contribué à accroître l'incertitude et la division en Occident. 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'existe une 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 » (Zappone). 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.

34. 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 réseaux sociaux, évoquée dans les chapitres précédents, est propice à la stratégie de propagande du Kremlin, qui consiste à jeter la confusion plutôt qu'à convaincre et à remettre en cause l'existence même d'une vérité objective. Les cyberguerriers russes 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 que l'information venant de multiples sources est plus valable, sans se soucier de la crédibilité de ces sources (Paul et Matthews). Dans le cadre des médias sociaux, où la quantité d'information tient lieu de qualité, l'appareil russe à fabriquer l'information sait parfaitement tirer profit de cette caractéristique en usant abondamment de trolls[7] et de « bots » pour atteindre les objectifs suivants :

35. **Semer la confusion et désinformer.** 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 cyberguerriers russes ont inondé les réseaux sociaux de rapports fabriqués ou d'images trafiquées d'atrocités soi-disant commises par les forces ukrainiennes, de tortures et de meurtres d'enfants, de civils utilisés pour le trafic d'organes, voire d'actes de cannibalisme (StratCom, 2016a). 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

[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 certaines d'entre eux–par exemple, ceux appelés « bikini trolls » par les experts du Centre d'excellence de l'OTAN pour la communication stratégique – 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 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.

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 couramment décrit l'Ukraine et les Ukrainiens dans des contextes de violence et de symbolique fasciste (Szwed). 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.

36. 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. 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 présence avancée réhaussée de l'OTAN dans les États baltes et en Pologne (Copley). Ces dernières années, la Russie a aussi clairement intensifié ses attaques virtuelles contre ses voisins nordiques, le Danemark, la Suède et la Finlande.

37. Les troupes virtuelles du Kremlin propagent de fausses informations 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), 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) (BBC Monitoring Europe), et *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 soutenir l'Ukraine, pour poster des tweets avec les commentaires de Sergey Lavrov, le ministre des affaires étrangères russe (Sergey Lavrov) (StratCom, 2016a).

38. Les trolls peuvent aussi servir à **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 soi-disant 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. Le succès de cette campagne de désinformation pourrait encourager des manœuvres de ce type à plus grande échelle (Amann et al.). 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 (StratCom, 2016a).

39. Des trolls d'État orchestrent 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 la publication d'informations concernant sa vie privée. Autre cible de premier plan : Elliot 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 a piraté son compte email, 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 (Nakashima). Le trolling pro-russe agressif et visant à intimider a conduit plusieurs portails de média, tels Reuters et CNN, à fermer leur rubrique "commentaires" (Gross), ce qui a pour inconvénient de réduire les possibilités d'engager un débat en ligne constructif avec des personnes animées par des intentions résolument démocratiques (StratCom, 2016a).

40. 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 services russes l'occasion de récolter de vastes quantités de données personnelles. Puisant dans ces données, en novembre 2015, les cyberguerriers russes ont téléphoné massivement à des soldats polonais et, en janvier 2014, ont envoyé des messages SMS

menaçants à des personnes qui participaient aux manifestations de Maïdan à Kiev. Lors d'un prochain conflit, il est probable que le Kremlin utilisera ces outils pour démoraliser et neutraliser ses adversaires (Giles).

41. 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. Cela étant, 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*, 2016c). 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 le lien plus étroit entre médias sociaux et médias traditionnels joue dans les deux sens. Par exemple, quand 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), cela 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 (Wesel).

42. L'usage que fait la Russie des médias sociaux est éminemment sophistiqué, ingénieux et pose un réel défi à la communauté euro-atlantique. Cela étant, le Kremlin n'est pas invincible dans ce domaine. Notamment 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. 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, la Russie devrait continuer à développer des techniques et des capacités de guerre de l'information en réaction aux contre-mesures mises en place par l'Occident. 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

43. 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 internationales, régionales et nationales, 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. 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 (SHAPE).

44. 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 « rétablir la vérité » 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 soi-disant 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[8]. 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 informationnel constamment mis à jour ayant pour objet de comprendre les objectifs et les méthodes utilisées par les adversaires dans l'espace informationnel (StratCom, 2016c).

45. L'OTAN commence aussi à intégrer une dimension réseaux sociaux dans ses exercices : dans le cadre de l'exercice *Trident Juncture 2015*, les participants ont appris à produire rapidement de grands volumes de contenu pro-OTAN 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) (StratCom, 2016c). Il faut souligner que la doctrine de l'OTAN ne prévoit pas le recours à des opérations clandestines d'information contre des audiences ciblées et que les opérations psychologiques (PSYOPS) ne peuvent être utilisées que dans le contexte d'une opération militaire déclarée par le Conseil de l'Atlantique Nord (StratCom, 2016a).

46. Les efforts déployés par l'**UE** pour contrer les fausses informations en ligne et la propagande hostile sont confiés à deux nouveaux organismes : le groupe de travail East StratCom (*East Stratcom Task Force*) et l'Unité d'Interpol chargée du signalement des contenus sur Internet (IRU). Le premier, également appelé « Briser les mythes », 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 fortement sur des données fournies par un réseau de plus de 400 experts, journalistes, responsables, ONG et groupes de réflexion, dans plus de 30 pays (EEAS, 2017). En novembre 2016, le Parlement européen a adopté une résolution demandant une augmentation des capacités du groupe de travail (Stupp). 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 ce contenu. Selon un rapport publié en juillet 2016, l'IRU a évalué et signalé en vue de leur suppression plus de 11 000 messages à travers 31 plateformes en ligne, et les fournisseurs ont supprimé plus de 91 % de ce contenu (Morelli et Archick).

47. 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 rebaptisé 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 des ONG et des journalistes d'investigation (Parlement européen). 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*. Autres exemples de l'utilisation que font les autorités états-uniennes des réseaux sociaux en matière de sécurité : a) l'initiative du directeur du renseignement national, James Clapper, annoncée en mai 2016, d'intégrer des informations affichées publiquement sur les réseaux sociaux dans 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 : les enquêteurs peuvent uniquement recueillir ce type d'informations si elles sont susceptibles de mettre la sécurité nationale en péril (ODNI) ; et b) la législation présentée, en janvier 2017, devant le Congrès américain visant à imposer de nouvelles sanctions contre la Russie suite au rapport des services du renseignement américain établissant que des agences russes ont

[8] 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).

piraté les serveurs du Comité national démocrate et ont divulgué des informations dans le but d'influencer l'issue de l'élection présidentielle américaine (Ansley). Il convient aussi de noter que le département américain de la sécurité intérieure a qualifié le système électoral des États-Unis d'« infrastructure critique ».

48. Au **Royaume-Uni,** le service public de radiodiffusion BBC s'est joint à la lutte contre les fausses nouvelles en renforçant *Reality Check*, un service de vérification des faits qui collaborera avec Facebook (Rajan). En 2015, l'armée britannique aurait créé une force spéciale – la 77^{e} 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.

49. **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 et que 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.

50. Les pouvoirs publics en Allemagne, en France et en République tchèque, à quelques semaines des élections qui doivent se tenir dans leur pays en 2017, sont de plus en plus préoccupés par les attaques dont leurs systèmes politiques sont 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 (Stern). 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 seront dénoncées comme telles (Toonkel). Le journal français *Le Monde* a aussi créé un service de vérification des faits *Les Décodeurs* et prévoit d'établir une base de données de hoax qui permettra aux lecteurs de faire la distinction entre les sites diffusant de fausses nouvelles et les sites vérifiés (EEAS, 2016). 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 cyberguerriers du Kremlin dans le but probable de peser sur les résultats des prochaines élections qui doivent se tenir en octobre (Tait).

51. 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 le nombre restreint des principaux **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. 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 ou images / vidéos aux fins de recrutement terroriste), retirés de leurs plateformes (Facebook). La plateforme de partage de photos Instagram a introduit un outil de modération par mot clé pour permettre à ses utilisateurs d'éviter que des commentaires offensants ou des trolls ne polluent leurs photos (Reuters). 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 (Stop Fake). 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 « califat » de Daech (Greenberg).

52. Si les réseaux sociaux prennent un certain nombre de mesures pour supprimer les contenus liés au terrorisme – de fait Twitter affirme avoir supprimé 235 000 comptes accusés de faire l'apologie du terrorisme dans les six premiers mois de 2016 – certains hommes politiques insistent sur le fait qu'il faut aller plus loin. Keith Vaz, président de la commission spéciale des affaires intérieures de la Chambre des communes britannique, qualifiant ces suppressions de « goutte d'eau dans l'océan » a accusé les principaux géants du Web de « se renvoyer la balle en se cachant derrière leur statut juridique supranational, alors qu'ils savent pertinemment que leurs sites sont utilisés par les instigateurs de la terreur ». M. Vaz a déclaré que ces entreprises manquent de moyens humains pour surveiller les milliards de comptes (Travis). Un responsable allemand a proposé de condamner Facebook à payer une amende de 500 000 euros pour n'avoir pas supprimé, dans les 24h, de fausses informations et des messages de haine affichées sur son site. Pour autant, les défenseurs de la liberté d'expression, tels que Joe McNamee, directeur exécutif de *European Digital Rights*, se disent sceptiques à l'égard de propositions visant à rendre une société privée responsable de décider de ce qui est bon pour l'intérêt public et estiment que de telles initiatives pourraient avoir l'effet inverse (Stern).

V. CONCLUSIONS PROVISOIRES ET RECOMMENDATIONS

53. 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.

54. 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. Les internautes devraient bien connaître les meilleures 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 véritable 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.

55. 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. Citons à cet égard l'algorithme de Reuters (l'agence de presse internationale basée au Royaume-Uni), conçu pour évaluer la véracité des messages postés sur les réseaux sociaux concernant un sujet brûlant d'actualité (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 valable dans cet environnement informationnel en constante évolution (EEAS, 2016). 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 centrer 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 à exécution des normes objectives dans les médias en dénonçant et en pénalisant les organes de presse qui relaient délibérément de fausses informations » (Dempsey).

56. Les pays membres de l'OTAN, du moins ceux qui ne l'ont pas encore fait, devraient créer ou désigner des unités spéciales chargées – 24 h/ 24 – de surveiller 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 réflexions, 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. 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.

57. 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 d'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). Les efforts visant à supprimer les contenus radicaux, les discours haineux et les fausses informations des plateformes en ligne doivent être poursuivis, et les cyberguerriers les plus influents, tels les principaux propagandistes de Russie, doivent être soumis à des sanctions occidentales.

58. Face à la structure centre/périphérie mise en place par Daech sur les réseaux sociaux, les experts du StratCom de l'OTAN proposent de supprimer autant que possible les 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.

59. La plupart des médias sociaux étant la propriété de sociétés multinationales privées, il est nécessaire d'améliorer la coopération avec ces entreprises. Notamment, la mise au point et l'utilisation de logiciels anti-trolling et de vérification de faits ainsi qu'une surveillance accrue des réseaux doivent être encouragés. 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 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 plateforme chinoise WeChat qui connait un succès grandissant.

60. 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 au monde libre l'avantage dans l'espace informationnel.

61. L'Occident a inventé les médias sociaux mais ceux-ci se sont retournés contre ses propres valeurs. 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[9]. La rapporteure espère que ce projet de rapport contribuera à mieux prendre conscience de l'ampleur de ce défi.

[9] 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 Wikipedia.

BIBLIOGRAPHIE

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.

Amann, Melanie, Markus Becker, Benjamin Bidder, Hubert Gude, Konstantin von Hammersein, Alexej Hock, Hubert Hoffmann, et al. “The Hybrid War: Russia’s Propaganda Campaign Against Germany.” SPIEGEL ONLINE, 5 février 2016. http://www.spiegel.de/international/europe/putin-wages-hybrid-war-on-germany-and-west-a-1075483.html.

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.

Apps, Peter. “From Syria to Ukraine, Social Media Opens up Warfare.” *Reuters India*, 4 August 2014. http://in.reuters.com/article/us-security-socialmedia-idINKBN0G61MU20140806.

Ashkenas, Jeremy, and Gregor Aisch. “European Populism in the Age of Donald Trump.” The New York Times, 5 décembre 2016. https://www.nytimes.com/interactive/2016/12/05/world/europe/populism-in-age-of-trump.html.

Barberá, Pablo, and Megan Metzger. “How Ukrainian Protestors Are Using Twitter and Facebook.” Washington Post, 4 décembre 2013. https://www.washingtonpost.com/news/monkey-cage/wp/2013/12/04/strategic-use-of-facebook-and-twitter-in-ukrainian-protests/.

BBC Monitoring Europe. “Swedish institute accuses Russia of media manipulation,” 9 janvier 2017. By BBC Worldwide Monitoring

BBC Trending. “The Rise and Rise of Fake News.” 6 novembre 2016, http://www.bbc.com/news/blogs-trending-37846860.

Bentzen, Naja, and Martin Russell. “Russia’s Disinformation on Ukraine and the EU’s Response.” European Parliamentary Research Service, novembre 2015. http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2015)571339.

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.

Cambanis, Thanassis. “The Arab Spring Was a Revolution of the Hungry.” BostonGlobe.com, 22 août 2015. https://www.bostonglobe.com/ideas/2015/08/22/the-arab-spring-was-revolution-hungry/K15S1kGeO5Y6gsJwAYHejI/story.html.

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.

Coalson, Robert. “New Kremlin Security Doctrine Raises Internet-Freedom Concerns.” RadioFreeEurope/RadioLiberty, 6 décembre 2016. http://www.rferl.org/a/russia-informaiton-security-internet-freedome-concerns/28159130.html.

Copley, Caroline. “Angela Merkel Fears Social Bots May Manipulate German Election.” The Age, 25 novembre 2016. http://www.theage.com.au/world/angela-merkel-fears-social-bots-may-manipulate-german-election-20161124-gsx5cu.

Dempsey, Judy. “Judy Asks: Can Fake News Be Beaten?” Carnegie Europe, 25 janvier 2017. http://carnegieeurope.eu/strategiceurope/?fa=67789&mkt_tok=eyJpIjoiWmprd1pEYzRabUUxWmpkaSIsInQiOiJcL1hRcnFkUzErTmR5bEk3Y1pBcDRHSzMzeUFleDQ3YThUbkk5MjNHeVJyb2xDck0xNEhYZUJDWjM5ODkrVDFjSVByNTNwQUNIc2FDd1J2M3dPajBiN0I3TTdxM0NLeFRXN0sxNlVJZ3RicDJDOGdCZ3NoaXdJdFVqcHpTbFwvVHBuIn0%3D.

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, “Politics by Numbers”, 26 mars 2016b. http://www.economist.com/news/special-report/21695190-voters-america-and-increasingly-elsewhere-too-are-being-ever-more-precisely.

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

European Union External Action Service (EEAS). “Questions and Answers about the East StratCom Task Force.” Eeas, 14 janvier 2017. https://eeas.europa.eu/headquarters/headquarters-homepage_en/2116/ Questions and Answers about the East StratCom Task Force.

European Union External Action Service (EEAS). “New Initiatives against Fake News - Disinformation Digest.” 12 décembre 2016. http://us11.campaign-archive2.com/?u=cd23226ada1699a77000eb60b&id=c648da6b81.

Facebook. “Partnering to Help Curb Spread of Online Terrorist Content,” 5 décembre 2016. https://newsroom.fb.com/news/2016/12/partnering-to-help-curb-spread-of-online-terrorist-content/.

Fairless, Tom, “Why Wages Have Lagged Behind the Global Jobs Recovery.” Wall Street Journal, 8 janvier 2017, http://www.wsj.com/articles/why-economic-growth-has-lagged-behind-the-global-jobs-recovery-1483895696.

Farwell, James P. “The Media Strategy of ISIS,” 1 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.

Gallup Inc. “Confidence in Institutions.” Accessed 26 janvier, 2017. http://www.gallup.com/poll/1597/Confidence-Institutions.aspx.

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/.

Greenberg, Andy. “Google’s Clever Plan to Stop Aspiring ISIS Recruits.” WIRED, 7 septembre 2016. https://www.wired.com/2016/09/googles-clever-plan-stop-aspiring-isis-recruits/.

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/.

Gross, Doug. “Online Comments Are Being Phased out.” CNN, 21 novembre 2014. http://www.cnn.com/2014/11/21/tech/web/online-comment-sections/index.html.

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

Güner, S.E., “The impact of social media on political change: Gezi protests in Turkey”, Centre for Policy and Research on Turkey (Research Turkey) vol. V, Issue 6, 25 juin 2016. (http://researchturkey.org/?p=12181)

InNetworkNet. “The Powerful Role of Social Media in the Canadian Election.” InNetwork Inc., 15 octobre, 2015. http://innetwork.net/2015/10/powerful-role-social-media-canadian-election/.

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.

Kooli, Rain. “Rain Kooli: Calling Fake News ‘Alternative Media’ like Calling Outhouse ‘Alternative Restaurant.’” ERR, 10 janvier 2017. http://news.err.ee/v/opinion/1188aab2-3c20-4ae7-aa31-15ed4fcab401/rain-kooli-calling-fake-news-alternative-media-like-calling-outhouse-alternative-restaurant.

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.

MacAskill, Ewen. “British Army Creates Team of Facebook Warriors.” The Guardian, 31 janvier 2015, sec. UK news. https://www.theguardian.com/uk-news/2015/jan/31/british-army-facebook-warriors-77th-brigade.

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.

Nakashima, Ellen. “Russian Hackers Harassed Journalists Who Were Investigating Malaysia Airlines Plane Crash.” Washington Post, 28 septembre 2016. https://www.washingtonpost.com/world/national-security/russian-hackers-harass-researchers-who-documented-russian-involvement-in-shootdown-of-malaysian-jetliner-over-ukraine-in-2014/2016/09/28/d086c8bc-84f7-11e6-ac72-a29979381495_story.html.

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.

Norton-Taylor, Richard, and Nick Hopkins. “Libya Air Strikes: Nato Uses Twitter to Help Gather Targets.” The Guardian, 15 juin 2011, sec. World news. https://www.theguardian.com/world/2011/jun/15/libya-nato-gathers-targets-twitter.

Office of the Director of National Intelligence (ODNI). “DNI CLapper Signs New Policy on Social Media for Federal Background Investigations for Security Clearances,” 13 mai 2016. https://www.dni.gov/index.php/newsroom/press-releases/215-press-releases-2016/1374-dni-clapper-signs-new-policy-on-social-media-for-federal-background-investigations-for-security-clearances-1.

Parlement européen. “US Strategic Communications to Counter Foreign Propaganda,” octobre 2016.http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589812/EPRS_BRI(2016)589812_EN.pdf.

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.

Pearce, Gregor Aisch, Adam, and Bryant Rousseau. “How Far Is Europe Swinging to the Right?” The New York Times, 22 mai 2016. https://www.nytimes.com/interactive/2016/05/22/world/europe/europe-right-wing-austria-hungary.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.

Phillips, Amber. “The Surprising Genius of Donald Trump’s Twitter Account.” Washington Post, 10 décembre 2015. https://www.washingtonpost.com/news/the-fix/wp/2015/12/10/reading-6000-of-his-tweets-has-convinced-us-donald-trump-is-a-social-media-master/.

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.

Poushter, Jacob. “Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies.” Pew Research Center’s Global Attitudes Project, 22 février 2016. http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/.

Radio Free Europe (RFE)/Radio Liberty (RL). “Q&A: Russia, China Swapping Cybersecurity, Censorship Tips.” *RadioFreeEurope/RadioLiberty*, 4 décembre 2016. http://www.rferl.org/a/russia-china-swapping-cybersecurity-censorship-tips-internet/28155171.html.

Rajan, Amol. “Fake News: Too Important to Ignore.” BBC News, 16 janvier 2017, sec. Entertainment & Arts. http://www.bbc.com/news/entertainment-arts-38636042.

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

Reuters. “Instagram Launches New Tool to Monitor Offensive Comments.” Reuters, 12 septembre 2016. http://www.reuters.com/article/us-instagram-comments-idUSKCN11I2NL.

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.

Ryan, Mick, and Marcus Thompson. “Social Media in the Military: Opportunities, Perils and a Safe Middle Path,” 21 août 2016. http://groundedcuriosity.com/social-media-in-the-military-opportunities-perils-and-a-safe-middle-path/.

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.

Sheikh Ali, Sarah. “Nusra’s ‘Mobilize’ Campaign to Recruit Children.” Atlantic Council, 1 novembre 2016. http://www.atlanticcouncil.org/blogs/syriasource/nusra-s-mobilize-campaign-to-recruit-children.

Stern, Rachel. “Germany’s Plan to Fight Fake News.” Christian Science Monitor, 9 janvier 2017. http://www.csmonitor.com/World/Passcode/2017/0109/Germany-s-plan-to-fight-fake-news.

Stop Fake. “Kremlin Watch Monitor.” StopFake.org, 25 janvier 2017. http://www.stopfake.org/en/kremlin-watch-monitor-january-25-2017/

StratCom (NATO Strategic Communications Centre of Excellence). “Internet Trolling as a Hybrid Warfare Tool: The Case of Latvia,” 2015. http://www.stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia-0.

StratCom (NATO Strategic Communications Centre of Excellence). “Social Media as a Tool of Hybrid Warfare,” mai 2016a. http://www.stratcomcoe.org/social-media-tool-hybrid-warfare.

StratCom (NATO Strategic Communications Centre of Excellence).. “Daesh Recruitment: How the Group Attracts Supporters,” novembre 2016b. http://www.stratcomcoe.org/daesh-recruitment-how-group-attracts-supporters-0.

StratCom (NATO Strategic Communications Centre of Excellence). “New Trends in Social Media,” décembre 2016. http://www.stratcomcoe.org/new-trends-social-media.

Stupp, Catherine. “Parliament Votes to Expand EU Units That Debunk Online Propaganda.” EURACTIV.com, 24 novembre 2016. http://www.euractiv.com/section/digital/news/parliament-votes-to-expand-eu-units-that-debunk-online-propaganda/.

Supreme Headquarters Allied Powers Europe (SHAPE). “ACO Directive on Social Media,” 16 septembre 2014. https://www.shape.nato.int/aco-social-media-policy.

Szwed, Robert. “Framing of the Ukraine-Russia Conflict in Online and Social Media,” mai 2016. http://www.stratcomcoe.org/framing-ukraine-russia-conflict-online-and-social-media.

Tait, Robert. “Czech Republic to Fight ‘Fake News’ with Specialist Unit.” The Guardian, 28 décembre 2016. https://www.theguardian.com/media/2016/dec/28/czech-republic-to-fight-fake-news-with-specialist-unit.

Taylor, Harriet. “Most Young Terrorist Recruitment Is Linked to Social Media, DOJ Official Says.” CNBC, 5 octobre 2016. http://www.cnbc.com/2016/10/05/most-young-terrorist-recruitment-is-linked-to-social-media-said-doj-official.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.

Toonkel, Jessica. “NBCUniversal Invests $500 Million in Snap’s IPO.” Reuters, 3 mars 2017. http://www.reuters.com/article/us-snap-inc-ipo-nbcuniversal-idUSKBN16A1K6.

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.

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.

Wesel, Barbara. “Hunting for Fake News.” DW.COM, 9 février 2017. http://www.dw.com/en/hunting-for-fake-news/a-37478731.

Westcott, Ben. “Duped by Fake News Story, Pakistani Minister Threatens Nuclear War with Israel.” CNN, 26 décembre 2016. http://www.cnn.com/2016/12/26/middleeast/israel-pakistan-fake-news-nuclear/index.html.

Yeung, Douglas, and Olga Oliker. “Loose Clicks Sink Ships: When Social Media Meets Military Intelligence,” 14 août 2015. https://www.rand.org/blog/2015/08/loose-clicks-sink-ships-when-social-media-meets-military.html.

Zappone, Chris. “Who Controls Our News? Welcome to the Era of Russian and Chinese Information War.” *The Age*, 9 septembre 2016. http://www.theage.com.au/world/who-controls-our-news-welcome-to-the-era-of-russian-and-chinese-information-war-20160907-grapkr.