ASSEMBLEE PARLEMENTAIRE DE L'OTAN

COMMISSION
DES SCIENCES ET DES
TECHNOLOGIES (STC)

L'INGÉRENCE DE LA RUSSIE DANS LES ÉLECTIONS ET LES RÉFÉRENDUMS DES PAYS DE L'ALLIANCE

Rapport général

par Susan DAVIS (États-Unis)
Rapporteure générale

181 STC 18 F fin | Original : anglais | 18 novembre 2018

TABLE DES MATIÈRES

I. INTRODUCTION

1. La Russie du président Poutine a développé une profonde aversion à l'égard de l'ordre international libéral, à tel point que l'État russe cherche activement à l'ébranler. Il est difficile de cerner à quel stade s'est produit le tournant. De nombreux observateurs considèrent qu'il a eu lieu lors de la conférence sur la sécurité de Munich, en 2007, conférence au cours de laquelle Vladimir Poutine a sévèrement critiqué les États-Unis, l'OTAN et même l'Union européenne et appelé à la création d'un nouvel ordre mondial. D'autres pointent du doigt les opérations militaires de la Russie en Géorgie en 2008 ou encore en Ukraine depuis 2014. Ce qui est clair aujourd'hui, c'est que la Russie souhaite revenir à un jeu géopolitique à somme nulle et réclame des droits sur ce qu'elle considère être ses sphères d'influence. Pour redessiner l'ordre mondial selon ses désirs et dans le but de se mettre en avant, la Russie essaie de fragiliser les plus fidèles partisans de l'ordre actuel à la fois en Europe et en Amérique du Nord, en cherchant à en déstabiliser les démocraties et, de fait, le concept même de démocratie libérale.

2. Les actions subversives de la Russie prennent de nombreuses formes et configurations différentes. Si le pays a fait usage de la force pour mettre en œuvre sa stratégie, la plupart de ses actions ne sont pas militaires mais visent à tester et exploiter les faiblesses des autres pays par le truchement – entre autres – de la politique, de l'information, de l'intimidation économique et de la manipulation (AP-OTAN, 2015). La commission sur la dimension civile de la sécurité (CDS) de l'Assemblée parlementaire de l'OTAN examine cette année l'ensemble des opérations hybrides menées par la Russie dans un rapport spécial intitulé « Parades aux menaces hybrides émanant de la Russie : une mise à jour » et présenté par Lord Jopling du Royaume-Uni (AP-OTAN, 2018).

3. Pour compléter ce rapport spécial de la CDS, la rapporteure de la commission des sciences et des technologies (STC) a décidé de s'intéresser dans le présent rapport à l'une des menaces hybrides les plus préoccupantes, à savoir l'ingérence dans les élections et les référendums au moyen d'opérations cybernétiques et informationnelles. La guerre cybernétique et informationnelle pratiquée par la Russie consiste à attaquer les acquis qui font la force même des démocraties libérales, notamment la liberté de la presse, la liberté d'expression, ainsi que la conduite d'élections libres et équitables et à s'en servir. Il apparaît aujourd'hui plus que clairement que la Russie s'est immiscée ces dernières années dans un certain nombre de processus électoraux et référendaires. Cette démarche est inacceptable. La crédibilité des élections et des référendums est au cœur de la démocratie libérale. Les élections sont l'expression de la volonté du peuple, et donc le fondement de l'autorité de l'État. Les référendums sont une forme très prisée de démocratie directe dans un grand nombre de régimes politiques, y compris dans l'État d'origine de la rapporteure, la Californie. Lorsque les citoyens n'ont plus confiance dans l'un ou l'autre de ces systèmes de consultation, cela veut dire que leurs démocraties courent un grand danger.

4. Les opérations cybernétiques et informationnelles de la Russie, menées notamment aux fins de perturber des élections et des référendums, représentent un défi stratégique pour l'Alliance. Elles requièrent des ripostes à tous les niveaux, dans toutes les instances et par tous les moyens. Il est extrêmement important que les parlementaires de l'Alliance – en tant que représentants élus du peuple – relèvent ce défi et que l'AP-OTAN émette des recommandations claires et énergiques à l'intention des gouvernements et des parlements des pays de l'Alliance.

5. Ce rapport général, adopté à Halifax (Canada) en novembre 2018, examine dans un premier temps les différentes motivations de la Russie pour s'ingérer dans les élections et les référendums de pays de l'Alliance. Il décrit ensuite les principaux cas d'ingérence de ce type (dont les cas d'ingérence les plus préoccupants), avant de présenter les différentes mesures pouvant être prises, lesquelles ont servi de base à une résolution également adoptée lors de la session annuelle.

II. LES MOTIVATIONS DE LA RUSSIE

6. Malgré les grands discours de ses responsables, la Russie n'est pas en mesure de rivaliser directement avec les membres de l'OTAN. Son PIB s'élève à quelque 1 300 milliards de dollars US, contre 19 000 milliards pour les États-Unis et 17 000 milliards pour l'UE. D'ici à 2020, le budget de la défense de la Russie devrait atteindre 41 milliards de dollars, alors que celui de l'OTAN est de 892 milliards. Les ressources militaires de la Russie sont aujourd'hui utilisées à leur maximum dans des conflits aux quatre coins de la planète (Meakins, 2017). Par ailleurs, les autorités russes sont en proie à de graves problèmes de corruption et sont incapables de résoudre des problèmes sociaux qui ne cessent de croître, notamment la grande pauvreté et les inégalités.

7. Tandis que la Russie se considère très désavantagée par rapport à des adversaires potentiels, « sa position géopolitique affaiblie l'oblige à jouer le rôle du méchant pour protéger ses intérêts » (Beaulieu et Keil, 2018). Les dirigeants russes ont donc eu recours, entre autres, aux cyberattaques et à d'autres instruments – que l'Union soviétique appelait autrefois « mesures actives » ou opérations informationnelles – pour discréditer les idéaux libéraux et fragiliser les démocraties. Les opérations informationnelles ne sont pas nouvelles dans l'arsenal russe, mais leur portée et leur efficacité ont été amplifiées par le vaste et souvent dangereux cyberespace, qui « permet une diffusion ultra-rapide d'infox » (Fried et Polyakova, 2018).

8. Si la technologie numérique agit indéniablement comme un amplificateur, il est impératif de rappeler que « les opérations informationnelles ont une grande dimension humaine, tant dans leur conception que dans leur mise en œuvre » (Watts, 2017). Les auteurs de ces opérations essaient « de modifier les choix du destinataire conformément à des objectifs prédéfinis par l'expéditeur », ce qui suppose une « démarche d'apprentissage actif de la part de la cible » (Splidsboel Hansen, 2017). Les opérations informationnelles reposent donc dans une très large mesure sur les dernières innovations dans le domaine des sciences sociales, comportementales et cognitives (Paul et Matthews, 2016).

9. Les objectifs de l'ingérence de la Russie varient selon les cas et ne s'excluent pas mutuellement. Selon les analystes, les autorités russes adoptent « une approche opérationnelle opportuniste » (Beaulieu et Keil, 2018). Le premier de leur objectif est d'**exacerber les tensions sociales préexistantes au sein d'une société**. Dans tous les cas de suspicion d'ingérence russe, les pirates et les trolls ont su faire preuve d'une grande habileté pour comprendre les angoisses qui divisent un pays. Aux États-Unis, les agents russes ont acheté des publicités qui ont attisé les tensions politiques et religieuses, de façon à ébranler la société civile (Lecher, 2017). En Allemagne, les réseaux de zombies (ou bots) russes se sont servis des débats concernant la politique gouvernementale à l'égard des réfugiés pour essayer d'affaiblir la chancelière Angela Merkel (Meister, 2016). En Espagne, les médias et les bots russes ont alimenté le sentiment nationaliste en Catalogne, contribuant ainsi à l'une des plus grandes crises constitutionnelles de l'époque moderne (Emmott, 2017). Ces incidents montrent comment la Russie fait usage de la technologie pour affaiblir un gouvernement en place, fragiliser l'opposition ou encore discréditer la démocratie libérale (Alandete, 2017b).

10. Il est important de préciser que les divisions précitées ne sont toutefois pas créées de toutes pièces. Un individu qui intervient dans une polémique politique pour l'exacerber n'est pas forcément un agent russe, de même qu'un bot n'est pas toujours au service du gouvernement russe. En fait, les agents russes s'immiscent là où ils pensent pouvoir avoir un impact. Partant des animosités existantes, ils amplifient et alimentent les points de vue les plus extrêmes, de façon à fausser le discours public d'un pays. Les organes d'information comme RT – qui dispose d'un budget équivalant à celui de quelques-uns des plus grands groupes d'information du monde – offrent aux partisans des thèses conspirationnistes et aux groupes radicaux la possibilité de diffuser leur message. Lors des élections de 2016 aux États-Unis, des agents russes se sont fait passer pour des Américains sur Facebook et Twitter pour alimenter des débats très partisans. S'exprimant sur

les activités des bots russes, John Kelly, fondateur d'une entreprise de marketing pour les médias sociaux, note que « les Russes ne se contentent pas de gonfler l'aile droite américaine. Ils attisent aussi l'aile gauche. En fait, ils essaient d'exacerber les extrêmes aux dépens du centre. » (Rutenberg, 2017). Comme l'a déclaré M. Kelly devant le sénat des États-Unis, « les extrêmes hurlent pendant que la majorité chuchote » (Kelly, 2018). Pour résumer, l'ingérence russe exploite les lignes de fracture existantes au sein de toute société.

11. Deuxièmement, l'ingérence russe cherche à **ébranler la confiance des citoyens dans les institutions démocratiques libérales**. Depuis ce que l'on a appelé les « révolutions de couleur » au début des années 2000, les dirigeants russes se sont, selon les termes du sociologue et politologue Larry Diamond, « comportés comme s'ils étaient obsédés par la crainte que le virus de la mobilisation démocratique de masse ne se propage en Russie » (Diamond, 2016). En affaiblissant les institutions démocratiques, les responsables russes ont l'impression d'affaiblir ceux qu'ils considèrent comme leurs adversaires et de mettre tous les concurrents à égalité. Le fait de suggérer qu'il existe de la corruption ou que les fonctionnaires ont un comportement répréhensible peut obliger les gouvernements démocratiques à se concentrer sur leur politique intérieure pour faire face au mécontentement et à l'apathie de leurs électorats. Dès les élections présidentielles de 2012 aux États-Unis, les médias russes indiquaient que la démocratie américaine était « une imposture » et que « les résultats des élections n'étaient pas fiables et ne reflétaient pas la volonté du peuple » (*Office of the Director of National Intelligence*, 2017). Suite aux manifestations qui ont eu lieu en Catalogne, des observateurs ont fait savoir que des comptes robots russes diffusaient des messages laissant entendre que l'Espagne était un pays violent et non démocratique (Milosevich-Juaristi, 2017).

12. Par ailleurs, le fait de délégitimer la démocratie aide les dirigeants russes à « vendre » leur système de gouvernement aux citoyens, en Russie et ailleurs. Comme l'indique le groupe minoritaire de la commission du sénat américain chargée des relations étrangères : « Si Poutine peut démontrer au peuple russe que les élections qui ont lieu ailleurs sont frauduleuses et entachées par la corruption, que la démocratie libérale est un régime politique qui ne fonctionne pas et qui est voué à disparaître, alors, leur propre système de « démocratie souveraine » […] ne paraît finalement pas si mauvais » (*Minority Staff of the Committee on Foreign Relations*, 2018). [Les responsables russes emploient l'expression « démocratie souveraine » pour décrire le système politique actuellement en place dans leur pays]. L'image d'un Occident faible fait oublier les problèmes intérieurs et justifie le maintien au pouvoir d'un dirigeant. Elle rend également la Russie plus attrayante pour des alliés potentiels qui pourraient ainsi être dégoûtés par les défaillances et les hypocrisies – ou perçues comme telles – de l'ordre démocratique libéral mondial. Si tous les responsables politiques sont corrompus et toutes les élections frauduleuses, cela ne vaut pas la peine d'aspirer à la démocratie (Zygar, 2016).

13. Troisièmement, l'ingérence russe tente de **mettre en avant les personnalités et les groupes politiques considérés comme favorables ou perméables à l'influence russe et de discréditer ceux qui sont perçus comme hostiles**. En Europe, les services de renseignement occidentaux ont, par exemple, constaté que Moscou apportait son soutien à des partis et des organisations qui sapent la cohésion de l'OTAN et de l'UE, ou qui favorisent les intérêts économiques et politiques de la Russie (Foster, 2016). En France, le président Emmanuel Macron qui, lorsqu'il était candidat était connu pour son opposition à de nombreuses politiques russes, a fait l'objet d'une cyberattaque de grande ampleur qui aurait pu faire échouer sa candidature. À l'opposé, sa principale rivale, connue pour ses idées pro-russes, a été invitée au Kremlin et a eu droit à une ample couverture élogieuse de la part des médias russes.

14. Selon une étude réalisée par le *Center for European Policy Analysis*, l'organe d'information russe *Sputnik* a réservé « une couverture disproportionnée aux membres du Parlement européen contestataires, opposés à l'ordre établi et pro-russes » et l'a fait dans une optique de tromperie « conforme au discours général de la station, à savoir celui d'un Occident corrompu, décadent et

russophobe » (Nimmo, 2016). Les mouvements ayant exacerbé les tensions internes, menacé la cohésion de l'UE et critiqué l'élargissement de l'OTAN ont généralement reçu le soutien de l'État russe. En revanche, ceux qui ont affiché des tendances inverses ont généralement été attaqués ou calomniés.

15. Enfin, l'ingérence russe tente de **susciter le chaos et l'incertitude dans les pays occidentaux.** En juillet 2016, *RT* et *Sputnik News* ont diffusé de fausses informations concernant l'occupation d'une base aérienne états-unienne à Incirlik, en Turquie, par des extrémistes (Sputnik News, 2016). Les observateurs ont constaté une intense activité de la part des bots et des agrégateurs de contenus des médias sociaux pro-russes, qui ont amplifié le récit et ont inventé une histoire de complot au sujet de la capture imminente de missiles nucléaires par des terroristes (Fox, 2017). En janvier 2016, les communautés russophones d'Allemagne ont été dévastées par la rumeur selon laquelle le gouvernement allemand avait dissimulé le viol d'une jeune fille par des migrants. Les médias russes puis, plus tard, le ministère russe des affaires étrangères, ont relayé cette version, ce qui a laissé entendre que la version officielle des événements n'était pas fiable (Rutenberg, 2017).

16. Selon Alina Polyakova, de l'*Atlantic Council*, l'objectif de telles histoires et, plus généralement, de l'ingérence russe est de « créer une espèce de paralysie politique tout en permettant aux voix pro-russes d'être mieux entendues » afin de « déstabiliser la classe politique et de semer le chaos » (Luhn, 2017). Les citoyens sont incités à se méfier de leurs gouvernements et des médias classiques, et à prêter attention aux rumeurs et aux théories conspirationnistes. La frontière entre les faits et la fiction devient floue, ce qui facilite l'insertion dans le discours public de propos mensongers ou trompeurs (Fox, 2017). Cette confusion peut être utilisée pour défaire le tissu constitutif d'une société. Elle peut aussi servir le discours qui est tenu en Russie au sujet de l'imminence d'un désastre mondial nécessitant un leadership fort au niveau intérieur (Weisburd, Watts, et Berger, 2016).

17. Pour résumer, la désinformation russe (tout comme sa mésinformation) poursuit des objectifs multiples et connexes, dans le but de nuire à l'Occident et de promouvoir les intérêts des dirigeants russes. Elle permet à la Russie de diffuser des discours pouvant influencer à son avantage la façon dont les individus, que ce soit en son sein ou à l'étranger, interagissent avec les systèmes politiques. Sans devoir recourir à un affrontement militaire direct ou à de gros investissements, les dirigeants russes cherchent à orienter les affaires internationales en leur faveur.

III. CE QUE L'ON SAIT : L'INGÉRENCE RÉCENTE DE LA RUSSIE DANS LES PAYS DE L'ALLIANCE

18. Il est bien connu que des faits commis dans le cyberespace sont difficiles à attribuer. Cela est particulièrement vrai pour les opérations informationnelles, dont le but est de créer une atmosphère de doute, de défiance et de confusion. Les cibles préfèrent souvent dissimuler ou minimiser les failles de sécurité dont elles ont été les victimes plutôt que de s'exposer à un embarras public. Les médias sociaux utilisés pour diffuser des informations mensongères ou trompeuses ont tendance à conserver jalousement leurs données. Les services gouvernementaux chargés d'enquêter sur ces incidents opèrent généralement avec discrétion. Par ailleurs, dans des opérations informationnelles, un grand nombre de ses composantes (opérations de piratage, infox et bots) peuvent être utilisées aussi bien par des individus que par des acteurs étatiques.

19. Par conséquent, il convient d'aborder la question de l'ingérence de la Russie avec prudence. Bien qu'il soit largement reconnu que le gouvernement russe a soutenu des opérations visant à discréditer et déstabiliser les démocraties libérales, l'ampleur et les caractéristiques de ces opérations sont souvent loin d'être limpides. En règle générale, il est rare que les rapports officiels, qu'ils soient gouvernementaux ou parlementaires, fournissent des informations détaillées ou

étayées sur les manœuvres d'influence menées dans les pays de l'Alliance. Cette section se base donc en partie sur certaines informations publiques et les déclarations officielles pour mieux comprendre les allégations d'immixtion de la Russie dans les élections et/ou les référendums qui se sont tenus aux États-Unis, au Royaume-Uni, en France, en Allemagne, en Espagne et aux Pays-Bas. Ces exemples sont représentatifs car ils comportent un nombre élevé de récits fiables faisant état d'une cyberingérence russe, et/ou montrent les dispositions prises par les gouvernements et les parlements pour se préparer à l'éventualité d'une ingérence étrangère.

20. Pour lui permettre de rester concis, ce rapport s'intéresse uniquement aux cas d'ingérence dans les élections et les référendums ayant été constatés dans les pays de l'Alliance. Cela dit, un grand nombre des scénarios décrits ici se sont produits de façon très semblable dans d'autres pays, notamment dans l'ex-République yougoslave de Macédoine[1], en Géorgie, en République de Moldova, au Monténégro (avant qu'il ne devienne membre de l'Alliance), en Suède et en Ukraine. Il s'avère que la Russie a tout d'abord testé ses capacités opérationnelles dans le domaine cybernétique et informationnel par des tentatives d'influencer les politiques intérieures des pays partenaires de l'OTAN, notamment en Géorgie et en Ukraine. L'expérience de leurs partenaires a permis aux Alliés d'en tirer un certain nombre d'enseignements et de bonnes pratiques, comme ont pu le constater les membres de la commission lors de la session de printemps 2018 à Varsovie. Pour ce qui est de l'avenir, l'Alliance va non seulement devoir continuer à s'inspirer de l'expérience de ses partenaires, mais aussi les aider à se protéger contre de telles menées.

A. ÉTATS-UNIS

21. Les élections présidentielles qui ont eu lieu aux États-Unis en 2016 sont l'exemple le plus flagrant d'immixtion de la Russie dans un processus électoral. Quatre grands types d'action ont été menés : vol d'informations ; diffusion sélective des informations ; campagne de propagande ; enfin, des tentatives de piratage des systèmes de vote du pays (Van de Velde, 2017).

22. Plusieurs évaluations importantes – émanant du pouvoir exécutif, du Congrès ou d'experts – ont déjà été rendues publiques, mais les enquêtes sur l'ingérence russe se poursuivent. Les principaux documents émis par l'exécutif et le Congrès américains sont les suivants :

- Janvier 2017 : Évaluation de la communauté du renseignement américaine (*US Intelligence Community Assessment*) émanant de la CIA, de la NSA et du FBI ;
- Mars 2018 : rapport de la commission du renseignement de la Chambre des représentants (*House Permanent Select Committee on Intelligence),* adopté par le parti de la majorité ;
- Mars 2018 : rapport de la commission du renseignement de la Chambre des réprésentants (*House Permanent Select Committee on Intelligence),* adopté par l'opposition *(Minority views)* ; et
- Juillet 2018 : premières conclusions de la commission du renseignement du Sénat américain « Évaluation de la communauté du renseignement en 2017 » *(2017 Intelligence Community Assessment*).

23. Il ressort très clairement de toutes les enquêtes officielles et expertises que la Russie a fait de l'ingérence et a cherché à ébranler la confiance du peuple états-unien dans le processus démocratique de leur pays. Si la Russie et, avant elle, l'Union soviétique s'en sont fréquemment pris aux démocraties libérales et notamment tenté d'influencer les résultats de certaines élections aux États-Unis, les menées de Moscou en 2016 représentent une escalade majeure de par leur nature, leur portée et le caractère direct de l'ingérence.

24. Des intrusions non dissimulées dans des organisations publiques et privées, ainsi que de la propagande et de la désinformation, ont facilité les activités russes. Comme le signalait l'*Intelligence*

[1] La Turquie reconnaît la République de Macédoine sous son nom constitutionnel.

Community Assessment de janvier 2017, les agents du renseignement russes ont ciblé des comptes de messagerie électronique à la fois personnels et professionnels, appartenant à des personnalités des deux partis politiques (*Office of the Director of National Intelligence*, 2017). Le responsable de l'équipe de campagne d'Hillary Clinton, John Podesta, s'est fait pirater sa messagerie après avoir cliqué par mégarde sur un e-mail d'hameçonnage (*phishing*) (Osnos, Remnick, et Yaffa, 2017). Au cours de son audition en janvier 2017 devant la commission du renseignement du Sénat, le directeur du FBI de l'époque, James Comey, a également indiqué que les services de renseignement russes avaient réussi à obtenir un « accès limité » au comité national républicain en piratant d'anciens comptes de messagerie électronique, ainsi qu'à des organisations du parti républicain au niveau étatique (*Senate Select Intelligence Committee*, 2017). L'*Intelligence Community Assessment* de janvier 2017 indique toutefois que la Russie n'aurait pas « mené une campagne aussi vaste de divulgation en retour » (*Office of the Director of National Intelligence*, 2017). Des groupes de réflexion, groupes de pression et autres personnalités politiques importantes ont également été ciblés dès le mois de mars 2016 (*Office of the Director of National Intelligence*, 2017).

25. Les responsables russes ont ensuite utilisé ces informations recueillies illicitement pour lancer des opérations de propagande et de désinformation à l'aide de médias financés par l'État, d'intermédiaires indépendants et de trolls rémunérés. Tout au long de la campagne électorale, les fictifs *DCLeaks* et *Guccifer 2.0* ainsi que *WikiLeaks* ont pris contact avec des journalistes et rendu publics des e-mails, des numéros de téléphone privés et divers documents (notamment de la campagne présidentielle). Le procureur général adjoint, Rod Rosenstein, a clairement indiqué que *DCLeaks* et *Guccifer 2.0* « avaient été créés et étaient contrôlés par la GRU russe [la direction générale du renseignement russe] » (De La Garza 2018). Ces révélations ont entraîné une couverture négative de la campagne par les médias reconnus et influents comme le *New York Times* (Watts et Rothschild, 2017).

26. Par ailleurs, ces événements ont fait l'objet d'une vaste couverture médiatique en Russie, y compris de la part de réseaux d'information anglophones comme RT et *Sputnik*. RT (anciennement *Russia Today*), est un réseau international de télévision par câble et satellite conçu sur le modèle des chaînes d'information continue occidentales (comme CNN et la BBC). *Sputnik*, qui est financé par l'État russe, comprend un site internet d'actualités et une radio, qui s'inspirent de sites d'information désinvoltes tels que *Buzzfeed*. Les deux organes d'information se voient souvent accusés de véhiculer la propagande russe et d'amplifier les points de vue extrémistes dans les pays hôtes (Rutenberg, 2017). En 2017, *RT America* a été contraint par le département états-unien de la justice de déclarer son existence, en vertu de la loi sur l'inscription des agents étrangers. Lors des élections, les sites de RT et de *Sputnik* ont étayé leur discours sur les défaillances de la démocratie libérale occidentale en divulguant des informations confidentielles.

27. Ces activités ont été relayées par une campagne menée de façon coordonnée sur les médias sociaux afin de donner plus d'écho aux révélations, de propager des infox et de délégitimer l'administration des États-Unis. Sur *Facebook*, pas moins de 120 comptes factices orchestrés par la Russie, et qui avaient diffusé des messages lus par quelque 29 millions d'États-uniens, ont été percés à jour (Solon et Siddiqui, 2017). Les messages diffusés, qui concernaient notamment des projets d'organisation de 129 vrais événements, ont été consultés par 338 300 personnes aux États-Unis (Volz et Ingram, 2018). Il est difficile de déterminer combien de ces événements ont finalement eu lieu et combien de participants ils ont attiré (Seetharaman, 2017). Jusqu'en janvier 2018, *Twitter* a recensé au moins 50 258 bots russes ayant publié des informations sur les élections aux États-Unis.

28. Sur *Facebook* et sur *Twitter*, des comptes russes auraient diffusé des messages jugés déstabilisants pour la société civile états-unienne ou favorables aux objectifs russes. Cette volonté de créer la rupture s'est traduite notamment par l'usurpation et la simulation d'identités, par la publication de pages sur les médias sociaux et d'autres sites Internet s'adressant à un public

américain, et par l'amplification des points de vue d'États-uniens qui existent réellement mais qui ont des idées clivantes (*Department of Justice*, 2018). Les messages avaient pour but d'enflammer les débats sur des questions portant à polémique telles que l'autorisation du port d'armes, l'immigration, les droits des communautés LGBT et l'usage de la force par la police (Lecher, 2017). Ils avaient également pour but d'influer directement sur les résultats de l'élection présidentielle. Cette « pompe à mensonges », comme l'ont décrite les analystes de la société RAND, a produit une énorme quantité de fausses informations sur différents supports, dans le but de démoraliser et de diviser la population (Paul et Matthews, 2016).

29. Outre ces attaques, les responsables états-uniens indiquent que la Russie a également ciblé certaines bases de données d'électeurs lors des élections de 2016. Le 22 septembre 2017, le département de la sécurité intérieure des États-Unis a en effet informé 21 États que la Russie avait tenté d'accéder à leurs bases de données électorales (Borchers, 2017). La commission du renseignement du Sénat a estimé que « dans un petit nombre d'États, les pirates ont tout au moins été en mesure de modifier ou de supprimer les données d'inscription des électeurs ; en revanche, il ne semble pas qu'ils aient été capables de manipuler les votes individuels ou d'ajouter des voix au total du scrutin » (Burr, Warner et al., 2018). Ces bases de données pouvaient contenir les noms d'utilisateur et mots de passe des agents électoraux, ou bien les noms, date de naissance, sexe, numéro de permis de conduire et numéro partiel de sécurité sociale des électeurs, reste à savoir ce que les pirates comptaient faire de ces informations.

30. Entre la rédaction du présent rapport et son examen lors de la session annuelle, les élections de mi-mandat en 2018 ont eu lieu aux États-Unis. Nombreux sont ceux qui s'attendaient à ce que ces élections constituent une cible pour la Russie, ainsi que pour d'éventuels autres pays étrangers souhaitant exercer une influence sur la politique états-unienne. À vrai dire, quelques actes d'ingérence avaient déjà été enregistrés au moment de la rédaction de ces lignes. En juillet et août 2018, *Facebook*, *Twitter* et *Microsoft* ont annoncé la suppression d'un certain nombre de comptes. Le 31 juillet 2018, *Facebook* a retiré 32 pages et comptes des sites *Facebook* et *Instagram*, sans indiquer qui était tenu pour responsable de tentatives d'ingérence dans ces élections de mi-mandat (Roose, 2018). Le 22 août, 652 groupes et comptes ont été supprimés par *Facebook* et 284 comptes par *Twitter* (Lapowsky, 2018). Des comptes russes, mais aussi iraniens faisaient partie de ces groupes, ce qui montre que la menace d'une ingérence étrangère ne provient pas uniquement de la Russie mais aussi d'autres pays (Solon, 2018). La société *Microsoft* a quant à elle également supprimé / saisi des comptes – censés avoir été créés par la GRU – qui essayaient de s'attaquer au *Hudson Institute* et à l'*International Republican Institute*, deux groupes de réflexion influents appartenant au camp des conservateurs. Ces deux dernières années, *Microsoft* a également fermé 84 faux sites internet soupçonnés d'utiliser la méthode de l'hameçonnage pour accéder à certains réseaux (Dwoskin, 2018). Le harponnage de membres du Congrès (ou candidats aux élections) semble également s'être poursuivi après les élections de 2016, ce qui a conduit les différents candidats à recruter les services coûteux d'experts en opérations cybernétiques et informationnelle pour leurs campagnes.

31. En réaction aux apparentes nouvelles tentatives d'ingérence, le pouvoir exécutif et le Congrès des États-Unis ont pris des mesures énergiques pour sécuriser les élections de mi-mandat. Depuis janvier 2017, plus de 60 projets de loi relatifs à la sécurité des élections ont été présentés au Congrès. Dans le projet de loi de finances général 2018, le Congrès a budgété quelque 380 millions de dollars pour financer la loi *Help America Vote Act* (HAVA). La mise en place de dispositifs précis visant à sanctionner l'ingérence électorale a en outre été encouragée. Les sénateurs Marco Rubio et Chris Van Hollen ont plaidé en faveur de la loi bipartisane de protection des élections par l'établissement de lignes rouges (*Defending Elections from Threats by Establishing Redlines Act* ou *Deter Act*), qu'ils ont présentée comme un moyen de dissuader l'ingérence étrangère dans les élections de mi-mandat. En septembre 2018, le président Donald Trump a signé un décret relatif à l'application de sanctions en cas d'ingérence étrangère dans des élections aux États-Unis. Dans une déclaration conjointe, les sénateurs Rubio et

Van Hollen ont dit espérer pouvoir aller plus loin dans l'application de sanctions à l'encontre de ceux qui pourraient attaquer les systèmes électoraux états-uniens (Van Hollen et Rubio, 2018).

B. ROYAUME-UNI

32. Après que des récits sur une ingérence de la Russie dans les élections présidentielles aux États-Unis ont commencé à surgir, une partie de l'opinion publique britannique s'est inquiétée d'une possible ingérence des Russes dans le référendum de 2016 sur le maintien du Royaume-Uni dans l'UE et dans les élections générales britanniques de 2017. Le 8 juin 2017, jour des élections générales au Royaume-Uni, le GCHQ (l'agence de renseignement britannique) a prévenu les fournisseurs d'énergie du pays que leurs systèmes pouvaient avoir été piratés par « des acteurs hostiles soutenus par des États et utilisant des méthodes sophistiquées ». On ignore cependant si l'incident était en lien avec les élections. En effet, il n'existe aucun fait avéré de piratage ou d'intrusion au cours de la campagne du référendum ni de celle des élections générales (Williams-Grut, 2017). Le gouvernement a fait savoir « qu'à ce jour, il n'existe aucune preuve d'une ingérence extérieure réussie dans les élections britanniques » (Roberts et Nokes, 2017).

33. On ne sait pas dans quelle mesure la Russie influe sur le discours public. Bien que la première ministre britannique, Theresa May, accuse Moscou « de propager des fausses informations » dans le but « d'ébranler les sociétés libres » et « de semer la discorde en Occident », les études réalisées pour évaluer l'influence de la Russie au Royaume-Uni ont donné des résultats contrastés (BBC News, 2017). L'université d'Oxford a par exemple recensé 105 comptes proches de la Russie, d'où ont été envoyés 16 000 tweets. Globalement, seuls 0,6 % des tweets *#Brexit* étaient liés à des sources d'information russes. L'université d'Edimbourg, qui s'est servi d'une liste de profils fournis par le Congrès des États-Unis, a constaté que 419 comptes Twitter russes avaient twitté à la fois au sujet des élections présidentielles aux États-Unis et du référendum britannique sur la sortie de l'UE (Booth, Weaver, Hern, et Walker, 2017). Le quotidien national *The Guardian* a relevé que ces comptes étaient cités plus de 80 fois dans la presse britannique (Hern, Duncan, Bengtsson, 2017). Une troisième étude réalisée par la *City University of London* a référencé 13 500 bots twittant au sujet du référendum. Ces bots fonctionnaient comme un « réseau supervisé d'ordinateurs zombies » et ont été désactivés ou supprimés par *Twitter* peu après la clôture du vote. Ils twittaient principalement des messages en faveur du retrait de l'Union européenne, mais les analystes n'ont trouvé aucune preuve d'un mouvement de désinformation à grande échelle et ne se sont guère efforcés d'identifier l'instigateur du réseau (*City Press Office*, 2017). De leur côté, les universités de Swansea et de Berkeley disent avoir découvert 156 252 comptes russes mentionnant le mot *Brexit* dans les jours précédant le référendum (Reuters, 2017). La disparité des résultats de ces études est due aux différences de méthodologie et au refus par *Twitter* de mettre à la disposition des chercheurs une grande partie de ses données.

34. Ces études – ainsi que d'autres – ont déclenché des enquêtes officielles. En octobre 2017, la commission de la Chambre des communes chargée du numérique, de la culture, des médias et des sports a entrepris une vaste enquête sur le rôle de la Russie lors du référendum sur le Brexit et dans les élections générales de 2017. En novembre 2017, la commission chargée du renseignement et de la sécurité a annoncé qu'elle allait enquêter sur les activités de la Russie au Royaume-Uni (*Intelligence and Security Committee of Parliament*, 2017). Une autre enquête sur la campagne numérique, menée cette fois par la commission électorale, est également en cours (Posner, 2017).

36. En juillet 2018, la commission chargée du numérique, de la culture, des médias et des sports a diffusé un rapport provisoire sur la désinformation et les infox (*UK House of Commons Digital, Culture, Media and Sport Committee*, 2018). Cette commission a reconnu le rôle qu'a joué la Russie en manipulant l'opinion publique lors de référendums et d'élections nationales en Europe et aux États-Unis. Elle a émis des suggestions concernant les voies possibles pour engager la responsabilité des entreprises technologiques en cas de désinformation et de propagation d'infox

sur les médias sociaux. La commission a également appelé à la réalisation d'une enquête de grande envergure pour évaluer l'ampleur du problème, afin d'émettre des recommandations d'actions.

37. Depuis juin 2018, les agissements de deux adeptes bien connus du *Brexit* font l'objet d'un examen approfondi au Royaume-Uni. Andy Wigmore, porte-parole de la campagne *Leave.EU* et Arron Banks, important bailleur de fonds dans la campagne en faveur du *Brexit*, ont été critiqués pour avoir été en contact avec l'ambassade de Russie dans la période qui a précédé le référendum, notamment sur un prétendu échange de documents juridiques confidentiels avec cette même ambassade, ainsi que des allégations de discussions sur des accords commerciaux (Cadwalladr and Jukes, 2018 ; *UK House of Commons Digital, Culture, Media and Sport Committee*, 2018). Une enquête est toujours en cours à ce sujet et, selon la commission chargée du numérique, de la culture, des médias et des sports, la *National Crime Agency* britannique était en charge du dossier au moment de la rédaction du rapport.

C. FRANCE

38. Lors de l'élection présidentielle en 2017, le candidat Emmanuel Macron et son parti ont indiqué avoir fait l'objet de cyberattaques et d'annonces mensongères sur les médias sociaux. En février 2017, l'équipe de campagne numérique de M. Macron ont expliqué avoir été la cible « de milliers de tentatives d'attaques contre les serveurs [du candidat] émanant simultanément de dizaines de milliers d'ordinateurs » (Beardsley, 2017). Les responsables de la campagne de M. Macron ont été victimes d'hameçonnage qui ont exposé leurs réseaux à de multiples intrusions extérieures (Hacquebord, 2017). Sur les médias sociaux, M. Macron a fait l'objet de plusieurs infox (Chrisafis, 2018). L'origine de ces attaques n'est toujours pas clairement établie à ce jour.

39. L'attaque la plus notable a consisté en une vaste fuite d'informations coordonnée, visant à nuire à la candidature de M. Macron. Le 5 mai 2017, soit 36 heures à peine avant le second tour de l'élection présidentielle, un fichier de 9 giga-octets est soudainement apparu sur les forums Internet et les sites de partage (Greenberg, 2017a). D'après ce que l'on sait, ce fichier contenait des courriels, des documents, des tableurs de comptabilité, des contrats et d'autres informations relatives à la campagne de M. Macron et était censé mettre le candidat dans l'embarras. Selon les responsables de campagne d'Emmanuel Macron, ce fichier contenait également « de nombreux documents forgés de toutes pièces visant à semer le doute et diffuser des informations mensongères » (Greenberg, 2017a). La diffusion de ce fichier a été stratégiquement planifiée dans le but d'aller à l'encontre du droit français, qui interdit la poursuite d'une campagne électorale moins de 48 heures avant la tenue du scrutin. Malgré l'interdiction de la publication du contenu du fichier par la presse, les informations se sont propagées rapidement sur les médias sociaux (Dearden, 2017). Comme pour les élections présidentielles aux États-Unis, le fichier et les hashtags le concernant ont reçu un écho qui a été amplifié par les bots, les militants d'extrême droite et WikiLeaks (Volz, 2017).

40. La plupart des experts français en cybersécurité ont refusé d'attribuer officiellement cet incident à la Russie. Après l'élection, le chef de la cybersécurité du gouvernement français a indiqué qu'il n'existait pas suffisamment de preuves pour remonter jusqu'aux auteurs de l'attaque (*Associated Press*, 2017). D'autres sources françaises ont souligné l'amateurisme de l'attaque, comparé à la plupart des cyberattaques commanditées par des États. D'ailleurs, l'équipe de campagne de M. Macron a pu déjouer plusieurs autres offensives en inondant les attaquants de faux comptes pour ralentir et discréditer les intrusions (Challenges, 2017).

41. Certains experts extérieurs ont toutefois laissé entendre que la Russie pourrait bel et bien être la commanditaire de cette attaque. Le directeur de la NSA, Michael Rogers, a déclaré que les États-Unis « avaient eu connaissance d'agissements de la Russie » dans le cadre de l'élection française, et que les responsables états-uniens l'avaient mentionné à leurs homologues français (Greenberg, 2017b). En avril 2017, une société privée spécialisée dans la cybersécurité, *Trend Micro*, a fait savoir que l'attaque contre Macron présentait les mêmes caractéristiques que celle perpétrée à l'encontre du comité national démocrate aux États-Unis (Hacquebord, 2017).

42. Comme d'autres Alliés, la France a pris des mesures énergiques pour contrer ces opérations cybernétiques et informationnelles. Une mesure récente importante a été l'adoption en juillet 2018 d'une loi sur la manipulation de l'information en période pré-électorale. Cette loi dite « sur les fausses informations » autorise les tribunaux à déterminer si des articles publiés jusqu'à trois mois avant une élection sont crédibles ou doivent être retirés. Elle autorise également les candidats aux élections à engager une action en justice pour demander la suppression de fausses informations et oblige les médias sociaux comme *Facebook* et *Twitter* à communiquer la source de financement des contenus publicitaires (Young, 2018).

D. ALLEMAGNE

43. L'Allemagne a fait l'objet de plusieurs menaces ayant prétendument un lien avec la Russie. En mai 2015, des pirates russes ont envoyé des courriels d'hameçonnage à des membres du gouvernement allemand, notamment au cabinet de la chancelière. Ces courriels avaient en fait installé un « cheval de Troie » sur les ordinateurs des parlementaires et des fonctionnaires qui avaient cliqué dessus. Au cours des trois semaines qui avaient suivi, les pirates avaient ratissé le réseau du parlement allemand et recueilli 16 giga-octets de données (Beuth, Biermann, Klingst, Stark, 2017). Il est important de noter que les pirates avaient misé sur la défaillance humaine en ciblant le parlement la veille d'un jour férié, afin de profiter de la fermeture du service informatique. Ultérieurement, en 2016, les médias russes ont diffusé une fausse histoire de viol pour délégitimer le gouvernement allemand (Meister, 2016). Suite aux protestations d'Allemands russophones, l'incident a soulevé l'indignation des dirigeants allemands, qui ont accusé Moscou de « propagande politique » (Witte, 2017). Entre mars et avril 2017, une société privée spécialisée dans la cybersécurité a découvert que la Russie avait tenté – sans succès – d'infiltrer des organisations en lien avec les deux grands partis politiques allemands (Barker, 2017). En mars 2018, le gouvernement allemand a confirmé les rumeurs selon lesquelles son intranet – utilisé pour garantir des échanges d'informations sécurisés entre les différents ministères et services gouvernementaux – avait été attaqué par un groupe de pirates russes. L'attaque, qui ciblait vraisemblablement le ministère des affaires étrangères, a été traitée comme « attaque en cours, cernée et mise sous contrôle » (Oltermann, 2018).

44. L'ingérence russe semble, en revanche, avoir été absente lors des élections fédérales qui ont eu lieu en Allemagne en 2017. Bien que les médias russes aient diffusé toutes sortes d'informations donnant une image négative des dirigeants allemands et européens, les fichiers dérobés au parlement allemand ne sont pas sortis au grand jour. Des chercheurs de la *London School of Economics* ont néanmoins fait état « d'opérations coordonnées par des bots russophones sur Twitter », mais dont l'ampleur était vraisemblablement moins importante que celles déployées dans d'autres pays (Applebaum, Pomerantsev, Smith, et Colliver, 2017). Des chercheurs de l'université d'Oxford ont découvert que 15 % du trafic de Twitter attribué au parti pro-russe l'Alternative pour l'Allemagne provenaient de comptes automatisés ; les grands partis politiques représentaient quant à eux entre 7,3 et 9,4 % du trafic (Neudert, Kollanyi, et Howard, 2017). Il n'existe aucune preuve officielle de l'implication de la Russie dans les activités de ces robots, et la plupart des observateurs estiment que ces opérations n'ont eu qu'une influence minime sur les élections.

E. ESPAGNE

45. Les autorités espagnoles considèrent que l'ingérence de la Russie dans les affaires du pays a exacerbé les tensions survenues lors du référendum de 2017 en Catalogne (Emmott, 2017). En novembre 2017, des ministres espagnols ont indiqué que des contenus traitant de la Catalogne provenaient du « territoire russe » et « d'autres pays » comme le Venezuela (Alandete, 2017a). Ces allégations ont été confirmées par un chercheur du *Real Instituto Elacano*, un groupe de réflexion espagnol. Dans un rapport concernant le référendum en Catalogne, le chercheur a signalé que des trolls et des bots avaient diffusé sur *Facebook* et *Twitter* deux types de messages – vrais et faux – dans le but de susciter l'indignation à l'égard du gouvernement espagnol. Ces messages présentaient l'Espagne comme un pays violent et non démocratique et renforçaient les images d'instabilité en Occident (Milosevich-Juaristi, 2017).

46. Certaines de ces allégations ont été corroborées par quelques observateurs. Un chercheur de l'université de George Washington a ainsi remarqué que les informations provenant de médias russes (comme RT et *Sputnik*) étaient beaucoup plus fréquemment diffusées que celles émanant des autres médias internationaux et encore 10 fois plus que celles des médias espagnols (Alandete, 2017b). Les « comptes zombies » propagent en ligne des messages favorables à la sécession de la Catalogne et opposés au gouvernement espagnol (Alandete, 2017a). De son côté, le plus grand quotidien espagnol, *El Pais,* a découvert que les tweets de Julian Assange et d'Edward Snowden en faveur de la sécession de la Catalogne étaient vraisemblablement amplifiés par des bots qui les retwittaient plus de 60 fois par minute, l'activité de ces bots étant attribuée à la Russie (Alandete, 2017c). Le laboratoire de recherche sur l'inforensique (*Digital Forensic Research Lab*) de l'*Atlantic Council* a relevé des éléments prouvant que la propagande russe a bel et bien influencé le débat sur la Catalogne. Des chercheurs ont détecté que les tweets de Julian Assange, notamment, faisaient l'objet d'une « nette amplification » de la part des bots pro-russes (Nimmo, 2017).

F. PAYS-BAS

47. Préoccupés par l'ingérence dont ont été victimes les États-Unis lors des élections présidentielles de 2016, les Pays-Bas ont pris des mesures énergiques pour se prémunir contre une éventuelle ingérence russe dans les élections générales néerlandaises de mars 2017, notamment sous forme de prises de contact avec les responsables états-uniens par l'ex-président de l'AP-OTAN, Bert Koenders, alors ministre des affaires étrangères (Brattberg et Maurer, 2018). Cela dit, la Russie s'était déjà immiscée dans les affaires politiques des Pays-Bas à deux reprises. En octobre 2015, un groupe de pirates russes ayant déjà participé à plusieurs grandes cyberattaques aurait attaqué le système de la commission de sécurité néerlandaise avant et après la publication de son rapport sur le crash, en 2014, du vol MH17 au-dessus de l'est de l'Ukraine. L'ingérence de la Russie avait également été remarquée en avril 2016 dans le débat qui avait précédé le référendum sur la conclusion d'un accord d'association entre l'UE et l'Ukraine, des agents russes s'étant notamment fait passer pour des Ukrainiens pour influencer les débats politiques locaux.

48. Pour garantir la confiance de l'opinion publique dans le processus électoral, les Pays-Bas ont interdit le vote électronique dès 2007 (Brattberg et Maurer, 2018). Avant l'élection de mars 2017, le gouvernement avait renforcé l'infrastructure électorale en interdisant le comptage électronique des voix ainsi que l'utilisation de clés USB et l'envoi de courriels par les responsables des élections (Chan, 2017). Le gouvernement néerlandais a en outre lancé une campagne de sensibilisation sur les faits passés d'ingérence de la Russie dans des élections étrangères, et informé son opinion publique sur le phénomène de la mésinformation et de la diffusion d'infox. D'autre part, les plateformes de médias sociaux ont mis en place une fonction de vérification des faits sur les articles des journaux néerlandais (Brattberg et Maurer, 2018). Enfin, la direction générale de la sécurité et du renseignement a conclu que la Russie n'était pas en mesure « d'influencer substantiellement » les élections néerlandaises de 2017 au-delà de la diffusion d'infox. Selon des experts indépendants,

le fait que les élections aient eu lieu « sans ingérence notoire » peut s'expliquer « soit par les actions de prévention, soit par l'absence apparente de volonté d'ingérence de la part de la Russie », peut-être parce que les autorités russes n'ont pas souhaité attiser la colère des Pays-Bas.

IV. LES MESURES POSSIBLES ET LA VOIE À SUIVRE

49. Dans presque tous les cas d'ingérence présumée de la Russie, le même schéma se répète. Dans un premier temps, les partis politiques ou les instances gouvernementales signalent des intrusions non autorisées sur leurs réseaux. Des courriels sont piratés, des données personnelles dérobées. Ces intrusions sont suivies par des fuites importantes et systématiques, diffusées sur les médias sociaux et amplifiées par des bots, trolls ou autres. Enfin, les fuites sont relayées dans la presse influente traditionnelle, qui rend publiques les révélations les plus sensationnelles. Pendant ce temps, des organes d'information contrôlés par le gouvernement russe ou partageant ses idées diffusent des informations mensongères ou trompeuses qui alimentent les polémiques et les thèses conspirationnistes. Cela crée une bulle de confusion, où la circulation d'une immense quantité d'informations fausses ou volées donne comme un parfum de scandale (Toucas, 2017).

50. Comme le montrent les précédentes sections, il est relativement clair que les autorités russes ont utilisé la liberté d'expression et la liberté de la presse pour tenter de délégitimer les institutions démocratiques des États membres de l'OTAN. Il est clair aussi que la participation de la Russie à ce type d'opérations n'est pas près de s'arrêter.

51. Les sections qui suivent présentent quelques mesures pouvant être prises face à l'ingérence de la Russie. Ces recommandations ne sauraient être considérées comme exhaustives au regard de l'évolution rapide de la situation et du fait qu'une grande partie des analyses qui s'y rapportent ne sont pas accessibles publiquement. Ces sections citent donc les pratiques prometteuses des membres de l'OTAN, les approches recommandées par les experts ainsi que d'autres aspects abordés collectivement dans le cadre du débat sur l'ingérence russe (voir par exemple : Fly, Rosenberger et Salvo, 2018 ; ou Salvo et Beaulieu, 2018). Les solutions varient en fonction des États et des cibles. Pour plus de clarté, les mesures détaillées sont classées par thème : celles qui concernent l'infrastructure électorale, les systèmes d'information, ainsi que les médias sociaux et de masse, et enfin les autres approches.

A. INFRASTRUCTURE ÉLECTORALE

52. Il n'existe pas à ce jour de cas connu de piratage ayant réussi à dénaturer le résultat d'une élection. En revanche, on dispose d'éléments démontrant l'intérêt spécifique de la Russie pour les infrastructures électorales (qui comprennent les systèmes d'enregistrement des électeurs, les machines à voter, les serveurs de comptabilisation et la présentation des résultats le soir de l'élection). Il est donc recommandé aux États membres de l'Alliance d'analyser attentivement le risques à cet égard. Aux États-Unis, par exemple, les hauts responsables du renseignement ont clâmé disposer de « preuves substantielles » attestant que des pirates en lien avec la Russie ont réussi à accéder – sans toutefois porter atteinte à leur contenu – aux sites internet du gouvernement et aux systèmes d'enregistrement des électeurs d'un petit nombre d'États lors de l'élection présidentielle de 2016.

53. Pour dissuader les pirates de s'attaquer à ces systèmes, le département états-unien de la sécurité intérieure a, le 6 janvier 2017, classé les systèmes électoraux dans la catégorie « infrastructures critiques », afin d'améliorer la communication entre le gouvernement fédéral et les agents électoraux, et de débloquer des fonds supplémentaires pour assurer la protection des élections (Newman, 2017). Deux projets de lois bipartites – l'un sur la sécurisation des élections et l'autre sur la protection du processus d'enregistrement des résultats électoraux – ont été soumis au Congrès des États-Unis ; le but étant de supprimer les machines de vote électronique, de fournir

des fonds et une aide supplémentaires aux organes électoraux, ainsi que d'organiser des contrôles de sécurité post-électoraux (Stewart, 2018). À l'échelle infranationale, plusieurs États ont pris des précautions telles que des tests pré-électoraux, la certification des systèmes de vote et l'imposition d'opérations de contrôle et de réconciliation des résultats (*National Conference of State Legislatures*, 2018).

54. S'appuyant sur les enseignements tirés et les meilleures pratiques, la rapporteure encourage tout particulièrement les membres de cette commission à envisager de prendre les mesures suivantes par l'intermédiaire de leurs parlements et gouvernements respectifs :

- prévoir une évaluation régulière des risques encourus par l'infrastructure électorale et remédier à toute lacune ou vulnérabilité constatée ;
- institutionnaliser une préparation pré-électorale contre les actes d'ingérence ;
- organiser des audits de sécurité post-électoraux ;
- prévoir un financement et une assistance adéquats pour les organes électoraux ; et
- classer l'infrastructure électorale dans la catégorie « infrastructures critiques ».

B. SYSTÈMES D'INFORMATION

55. Les attaques plus courantes sont celles qui compromettent la sécurité d'informations confidentielles embarrassantes. Comme l'indique un chercheur du *Center for Strategic and International Studies* : « Il est capital, pour un(e) pirate informatique, de verser dans le domaine public des informations personnelles authentiques : elles lui permettent d'acquérir une certaine crédibilité et de s'attirer un public qu'il/elle pourra ensuite manipuler » (Toucas, 2017). Les informations authentiques servent d'appâts dans le cadre des campagnes de désinformation de plus grande ampleur.

56. Les gouvernements peuvent stopper ou prévenir certaines attaques en encourageant les organisations vulnérables à prendre des mesures classiques en matière de cybersécurité. Ainsi, la plupart des experts considèrent que les organisations devraient se doter d'un service informatique ayant un accès et une visibilité sur l'ensemble de leur structure. Ce service devrait être composé d'un personnel formé et expérimenté et à même de se procurer le matériel et les logiciels nécessaires sans délai excessif. D'autre part, tous les membres du personnel doivent être informés sur les menaces potentielles et sur les dispositions qu'ils peuvent prendre pour éviter tout risque inutile. Ils doivent être conscients qu'ils ne doivent pas cliquer sur des liens ou télécharger des contenus provenant de sources inconnues, communiquer de mots de passe ou de données personnelles. Ils doivent également savoir que les informations publiées sur les médias sociaux peuvent être utilisées contre eux. Enfin, en cas de suspicion de cyberattaque, ils doivent savoir à qui s'adresser.

57. Les organisations doivent en outre disposer de protocoles clairs et faciles à mettre en œuvre en cas d'intrusion, et savoir à quel moment il faut contacter les services de police ou les services de renseignement compétents. Aux États-Unis, par exemple, les membres du Comité national démocrate ont mis longtemps avant de signaler au FBI les intrusions prétendument commanditées par la Russie dont faisait l'objet leur réseau (Lipton, Sanger, et Shane, 2016). En Allemagne, les parlementaires ont refusé toute assistance en matière de cybersécurité de la part de l'Office fédéral chargé de la protection de l'information car ils craignaient que « cette agence ne cherche à les épier » (Beuth et al., 2017).

58. Indépendamment des activités menées par la Russie, le développement de solides capacités en matière de cybersécurité apparaît de plus en plus comme une nécessité. En 2016, l'UE a adopté une directive sur les réseaux et les systèmes d'information, première pierre d'une législation communautaire sur la cybersécurité. Cette directive impose aux États membres de créer des centres de réponse aux incidents ainsi qu'une autorité nationale chargée de la cybersécurité (*Cybersecurity*

and Digital Privacy Unit, 2017). Les membres de l'UE sont invités à transposer sans délai cette directive dans le droit national si ce n'est pas déjà fait. Aux États-Unis, outre les diverses lois adoptées au niveau des États, le gouvernement fédéral a voté en 2015 la loi sur le partage des informations en matière de cybersécurité, afin de permettre aux services de renseignement d'échanger ce genre d'informations avec les entreprises de technologie et les fabricants (Karp, 2016). Dans le même temps, plusieurs États membres de l'OTAN ont mis en place des cybercommandements militaires afin de lutter spécifiquement contre les intrusions non souhaitées. La France a créé une structure de ce type en décembre 2017, c'est-à-dire peu après l'élection présidentielle ; les États-Unis et l'Allemagne en ont fait de même (Gramer, 2017). Tous les pays membres de l'OTAN ont mis au point, sous une forme ou une autre, une stratégie relative à la cybersécurité, mais celle-ci doit être régulièrement actualisée pour conserver sa pertinence (*Centre d'excellence de cyberdéfense coopérative de l'OTAN*, 2018).

59. Plusieurs pays ont également mis en œuvre des lois et des réglementations qui engagent la responsabilité des organisations en cas d'atteinte à la sécurité. En France, la commission nationale de l'informatique et des libertés (CNIL) est un organe de réglementation sur la cybersécurité qui est habilité à inspecter les réseaux des organisations et à faire respecter la législation nationale sur la protection des données. En 2015, la CNIL a réalisé 550 inspections et a sanctionné au moins une entreprise en lui infligeant une amende de 50 000 euros pour défaut de sécurité (Raul, Smith, et Sulmeyer, 2016). Malgré son retrait futur de l'UE, le Royaume-Uni va transposer la directive communautaire sur les réseaux et les systèmes d'information dans son droit national ; suite à une consultation publique en janvier 2018, le gouvernement britannique a confirmé qu'il sanctionnerait les organisations à hauteur de 17 millions de livres (20 millions d'euros) en cas de non-coopération avec les autorités chargées de la cybersécurité, absence de notification d'un incident ou défaut de mise en œuvre des mesures de sécurité appropriées.

60. À l'échelle internationale, plusieurs actions multilatérales ont été engagées de façon prolongée pour lutter contre les cyberattaques et les opérations informationnelles de la Russie. En juillet 2014, l'Alliance a créé à Riga (Lettonie) le centre d'excellence pour la communication stratégique, dont la mission est d'effectuer des recherches sur la guerre de l'information.

61. La politique de cyberdéfense et son plan d'action connexe, approuvés par l'ensemble des membres de l'OTAN lors du sommet du pays de Galles en septembre 2014, réaffirmaient la position de l'Alliance, à savoir que le droit international s'applique également dans le cyberespace et que l'article 5 peut donc être invoqué en cas de cyberattaque. Le sommet précité a également vu le lancement d'un cyberpartenariat OTAN-industrie, destiné à renforcer les liens de l'OTAN avec le secteur privé et à atteindre des objectifs spécifiques en matière de cybersécurité (Maldre, 2016). Lors du sommet de l'Alliance à Varsovie en 2016, le cyberespace a été reconnu comme l'un des domaines d'opération de l'OTAN. La cybersécurité et la défense ont également occupé une place importante lors du sommet de Bruxelles en 2018. Les Alliés se sont notamment accordés sur la manière d'intégrer les capacités cybernétiques souveraines dans les opérations et missions de l'Alliance, et ont décidé de créer un centre des cyberopérations, en Belgique, chargé d'assurer la connaissance de la situation et la coordination de l'activité opérationnelle de l'OTAN. La rapporteure se félicite de ces avancées en ce qui concerne les politiques de l'OTAN en matière de cyberdéfense, soulignant toutefois que l'OTAN doit être plus rapide dans l'analyse des cybermenaces et plus efficace en apportant, si nécessaire, des réponses coordonnées et pluridisciplinaires. La rapporteure encourage également les parlementaires de chaque État membre à déployer des efforts supplémentaires pour mettre en œuvre des plans d'action individuels, des lignes hiérarchiques et une coordination aux niveaux local, national et régional.

62. L'amélioration de la coordination dans le domaine de la cybersécurité et de la cyberdéfense a été retenue comme l'un des sept axes d'action urgents de la coopération OTAN-UE. La déclaration conjointe sur la coopération entre l'UE et l'OTAN, de juillet 2018, note une intensification de la collaboration entre les deux organisations sur les menaces hybrides, en ce compris les

cyberattaques. Le fait que ces deux organisations participent ensemble au centre d'excellence pour la lutte contre les menaces hybrides créé à Helsinki (Finlande) est, à cet égard, satisfaisant. Si les circonstances le permettent, l'UE pourrait également être invitée à participer au centre d'excellence de l'OTAN pour la cyberdéfense en coopération, qui se trouve à Tallinn (Estonie). Par ailleurs, le manuel des médias sociaux et numériques, élaboré par l'Organisation OTAN pour la science et la technologie, fournit un outil d'évaluation mis à jour régulièrement, qui permet de mieux comprendre les objectifs et les méthodes des pirates du web (AP-OTAN, 2017).

C. MÉDIAS SOCIAUX ET MÉDIAS DE MASSE

63. Bien que la mise en place de mesures de cybersécurité plus strictes puisse réduire les risques, elle ne saurait les éliminer complètement. Les erreurs techniques et humaines sont indéniablement des sources de vulnérabilité, même au sein des organisations les plus disciplinées (Inglis, 2017). Par ailleurs, si l'accès à des informations personnelles peut être recherché dans le cadre d'une campagne de désinformation, il n'est pas indispensable. Des informations mensongères ou forgées de toutes pièces peuvent proliférer sur les médias sociaux et de masse, même sans pirates ou fuites.

64. Face à la désinformation régnant sur les médias sociaux, deux types de réponses prédominent : celle qui met l'accent sur les **responsabilités des entreprises de médias et de technologie**, et celle qui pointe la **responsabilité des autorités**. Dans la première approche, les législateurs et les journalistes se sont intéressés de plus en plus près au mode de fonctionnement des entreprises de médias, en particulier au lendemain du scandale de *Cambridge Analytica*. Suite à un exposé de l'une de ces entreprises devant le Sénat des États-Unis, le sénateur Mark Warner a décrit les activités du média social concerné comme « attestant d'un manque énorme de compréhension de la gravité du problème et de la menace qu'il représente pour les institutions démocratiques » et a demandé que « des réponses beaucoup plus approfondies soient apportées » (Fandos et Shane, 2017). De la même manière, des parlementaires britanniques ont qualifié de « strict minimum » les efforts déployés par les entreprises de médias pour traiter le problème (Shaban, 2018). Qui plus est, des experts extérieurs ont fait état des efforts pugnaces déployés par *Facebook* et *Twitter* pour effacer de leurs plateformes les données relatives à l'ingérence russe, empêchant ainsi toute évaluation indépendante (Timberg et Dwoskin, 2017). Même au sein de ces entreprises, les responsables « reconnaissent aujourd'hui qu'ils sont passés à côté de signes évidents d'utilisations abusives de leurs plateformes » (Thompson et Vogelstein, 2018).

65. Face aux critiques générales de l'opinion publique, ces entreprises ont procédé à quelques changements pour régler le problème de l'utilisation abusive de leurs sites par des acteurs malveillants. En avril 2017, Facebook a publié le document « Opérations d'information et Facebook », qui explique comment un adversaire étranger peut utiliser la plateforme pour manipuler l'opinion publique. Le même mois, l'entreprise a suspendu 30 000 faux comptes qui avaient été créés pour peser sur le résultat de l'élection présidentielle française de 2017 (Weedon, Nuland, et Stamos, 2017). En novembre 2017, Google a annoncé qu'il allait « déclasser » RT et Sputnik – un processus consistant à rétrograder un site dans les résultats des recherches – pour leur rôle dans la propagation de fausses informations (BBC News, 2017). *Twitter* a repéré et suspendu 3 814 comptes liés aux opérations d'ingérence de la Russie. Ces comptes avaient au total quelque 2,7 millions de « followers ». La plateforme a également indiqué qu'elle allait faire la chasse aux comptes automatisés (bots) grâce à un certain nombre d'outils de détection utilisant les données – publiques et non publiques – des comptes et les caractéristiques de leur activité (Edgett, 2018). Cela dit, d'autres sites internet et applications mobiles n'ont pas fait l'objet d'un examen aussi minutieux. Pourtant, il existe des preuves de campagnes de désinformation menées par la Russie sur *Reddit* par exemple, un site internet combinant média social et agrégation de contenus sur l'actualité, ou sur *Instagram*, une application mobile de partage de photos (DiResta, 2018). Cette question doit être suivie de près. Les entreprises doivent continuer à exploiter le potentiel des technologies émergentes en affinant leur approche eu égard à la désinformation, notamment en utilisant l'intelligence artificielle et l'analytique des données massives.

66. D'autres initiatives ont également été prises en ce qui concerne la vérification des faits et le signalement des contenus mensongers aux utilisateurs. En novembre 2017, Facebook a annoncé la création d'un nouveau portail qui permet aux utilisateurs d'indiquer s'ils ont aimé ou suivi tel ou tel compte lié à la propagande russe (Yurieff, 2017). En janvier 2018, l'entreprise a fait savoir qu'elle avait modifié son algorithme de suivi de l'actualité ; elle avait déjà annoncé, en octobre 2017, son intention de recruter de nouvelles personnes pour scruter les publicités (Vogelstein, 2018). Avant les élections législatives allemandes de 2017, Facebook avait commencé à signaler les informations mensongères et à alerter les utilisateurs sur les supercheries (Stetler, 2017). Une autre initiative similaire, quoique plus énergique, a également été prise avant la tenue des élections législatives italiennes de 2018, Facebook s'étant associé avec des organismes spécialisés dans la vérification des faits, ce qui permettait d'avertir les utilisateurs qui partageaient des infox sur le résultat des vérifications effectuées (Serhan, 2018). Un certain nombre de groupes indépendants de vérification des faits ont en outre été créés au sein même de la société civile, comme par exemple : StopFake, le laboratoire de recherche en criminalistique numérique d'*Atlantic Council*, le *German Marshall Fund of the United States*, *Hamilton 68* ou encor *Baltic Elves* (Fried and Polyakova, 2018).

67. Parallèlement, les médias traditionnels ont pris des dispositions pour éduquer le public sur les risques de désinformation. En France, huit organes d'information – dont l'*agence France-Presse (AFP), L'Express et Le Monde* – ont uni leurs forces avec *Facebook* et *Google* pour repérer les fausses informations circulant sur les médias sociaux (Barzic, Kar-Gupta, Heavens, et Lough, 2017). *Le Monde* a créé son propre site de vérification des faits – *Les Décodeurs* – pour aider les utilisateurs à déterminer si une information en particulier est digne de confiance ou pas (Albeanu, 2017). Ces initiatives d'un genre nouveau s'appuient sur les efforts passés et actuels en matière de vérification des faits, une fonction essentielle des salles de rédaction des pays occidentaux depuis le début de ce XXI^{e} siècle. Selon certaines estimations, il n'y aurait pas moins d 34 groupes permanents chargés de vérifier les faits dans 20 pays européens (Graves et Cherubini, 2016). D'un autre côté, les journalistes indiquent que des discussions sont menées au sein des rédactions sur « les normes à adopter en ce qui concerne l'utilisation des informations provenant de sources douteuses » et sur les motivations que peut avoir une source (Peters, 2017).

68. Certains législateurs estiment que ces efforts sont nécessaires mais insuffisants. De nouvelles initiatives ont également été prises pour réglementer l'activité des médias sociaux ou rendre les entreprises responsables des contenus illicites qu'elles publient. Aux États-Unis, un groupe de parlementaires bipartite a proposé d'interdire, sur les médias sociaux, les publicités à caractère politique financées par l'étranger, et de rendre ces publicités globalement plus transparentes en les soumettant au même régime réglementaire que la radio et la télévision (Kelly et Warner, 2017). Certains hauts fonctionnaires des États membres de l'OTAN se montrent de plus en plus favorables à ce que les médias sociaux soient tenus pour responsables s'ils ne réagissent pas aux activités illicites sur leurs plateformes (Rozenshtein, 2017). Le parlement allemand a adopté une nouvelle loi exigeant que les médias sociaux retirent de leurs plateformes les contenus « manifestement illicites » dans les 24 heures suivant leur notification et infligeant une amende pouvant aller jusqu'à 50 millions d'euros en cas de refus d'obtempérer. Le président français, Emmanuel Macron, s'est dit très intéressé par un renforcement de la réglementation des médias « afin de lutter contre les tentatives de déstabilisation menées par des chaînes de télévision contrôlées ou influencées par des États étrangers », ainsi que par une régulation des informations mensongères diffusées sur les médias sociaux (BBC News, 2018). Cela a donné lieu à une proposition de loi relative à la lutte contre la manipulation de l'information en période pré-électorale (voir au paragraphe 42). M. Macron a promis une loi sur le sujet dans un proche avenir. Dans l'Union européenne, l'unité d'Europol chargée du signalement des contenus sur Internet a, selon un rapport de juillet 2016, évalué et sélectionné en vue de leur suppression plus de 11 000 messages ayant des contenus à caractère terroriste ; 91 % de ces contenus ont été retirés (Europol, 2016). Bien que cette unité se concentre sur les contenus extrémistes, ses activités pourraient servir de modèles pour d'autres usages.

69. La seconde approche possible à l'égard de la désinformation consiste à faire reposer la responsabilité sur les autorités, en mettant l'accent sur leur obligation d'informer le public. Si l'ingérence russe exacerbe les divisions au sein de la société, ce n'est pas elle qui les crée. Une campagne de désinformation ne peut prendre racine si personne ou presque, sur le plan intérieur, n'est réceptif aux messages clivants et conspirationnistes qui sont amplifiés par les agents russes. Cette approche repose donc sur le fait qu'il est de la responsabilité des démocraties d'instituer les sources qui font autorité et de s'assurer que les débats qui ont lieu s'appuient sur les mêmes faits, quelle que soit la tendance politique.

70. Un grand nombre des efforts précités incombent aux groupes de travail gouvernementaux spécialisés dans la désinformation. L'UE a par exemple mis en place la *Task force East Stratcom* – constituée par une équipe de diplomates dont la tâche est de mettre au jour les informations publiées en ligne par la Russie et de les présenter sur un site Internet *EU vs Disinfo* , avec l'appui d'un réseau de plus de 400 experts, journalistes et groupes de réflexion. La Commission européenne a publié une communication intitulée « Lutter contre la désinformation en ligne » (Commission européenne, 2018), qui présente les défis et définit les grands principes et objectifs qui doivent guider son action. À l'appui de ces travaux, un groupe d'experts de haut niveau de l'UE a publié un rapport détaillé formulant un certain nombre de recommandations en vue d'adopter une approche pluridimensionnelle de la désinformation en ligne (*High Level Group on Fake News and Online Disinformation*, 2018). En République tchèque, un centre de lutte contre le terrorisme et les menaces hybrides a été créé dans le but de faire obstacle aux infox, aux canulars, à la propagande étrangère et aux messages extrémistes diffusés dans le pays (Colborne, 2017). En décembre 2016, le Congrès des États-Unis a élargi la mission du *Global Engagement Center* du département d'État – qui était, à l'origine, de combattre la propagande terroriste – en y incluant la lutte contre la propagande et la désinformation orchestrées par des États. Cependant, malgré la réaffectation budgétaire par les législateurs de 120 millions de dollars (attribués initialement au département de la défense), ce centre n'a encore rien vu venir ni dépensé. En janvier 2018, le gouvernement britannique a annoncé son intention de créer une nouvelle unité de sécurité nationale chargée de « combattre la désinformation provenant d'acteurs étatiques et autres », mais l'on ne sait pas encore comment cette unité fonctionnera, ni quelle sera précisément sa mission (Walker, 2018). En Allemagne, le ministère de l'intérieur a, lui aussi, proposé la mise en place d'un centre de protection contre la désinformation, dans le but de repérer les fausses informations et d'éduquer le grand public sur les dangers qu'elles représentent (Deutsche Welle, 2016). À la veille des élections législatives, le gouvernement possédait son propre portail, sur lequel les utilisateurs d'internet peuvent signaler des contenus mensongers (Serhan, 2018). À une échelle moindre, les parlements peuvent eux aussi jouer un rôle dans la lutte contre la désinformation en organisant des auditions et en publiant des rapports pour appeler l'attention sur les fausses informations et les protagonistes qui se cachent derrière.

71. Comme le soulignent deux experts de l'*Atlantic Council* : « Pour gagner la guerre de l'information, une approche englobant l'ensemble de la société sera nécessaire. » (Fried et Polyakova, 2018). D'autres initiatives mettent donc l'accent sur la société civile ainsi que sur la promotion de l'éducation civique et la connaissance des médias. En Italie, par exemple, le ministère de l'éducation a dévoilé un nouveau programme d'études incluant des cours visant à apprendre aux jeunes à repérer les informations mensongères et à leur expliquer comment les réseaux sociaux peuvent être manipulés (Horowitz, 2017). Aux États-Unis, plusieurs établissements scolaires ont mis en œuvre des programmes pour aider les étudiants à comprendre comment les infox sont créées et comment les repérer (Rosenwald, 2017). En France, toutes les écoles primaires et secondaires dispensent depuis 2015 un cours d'éducation civique et morale. Bien qu'il soit principalement conçu pour lutter contre l'extrémisme violent, ce cours pourrait servir de cadre à des discussions sur les campagnes de désinformation. Des programmes similaires ont été mis en place dans d'autres pays de l'Alliance. Bien qu'il soit encore difficile de dire quelle influence ces programmes peuvent avoir sur les débats publics actuels, plusieurs études récentes semblent indiquer qu'ils aident les citoyens à s'engager dans le processus politique (Figueroa, 2017).

72. Une approche connexe consiste à accroître la recherche sur les opérations cybernétiques et informationnelles, et à développer des outils technologiques pour y faire face. Au sein de l'UE, par exemple, un groupe d'experts de haut niveau propose la création « d'un réseau de centres européens indépendants de recherche (universitaire) sur la désinformation » et exhorte la Commission européenne à réfléchir à la mise en place d'un centre d'excellence indépendant (*High Level Group on Fake News and Online Disinformation*, 2018). Un expert de *RAND corporation* a également avancé l'idée de créer un centre pluridisciplinaire de recherche sur la sécurité cognitive (Waltzman, 2017).

D. AUTRES APPROCHES

73. La Russie exploite la guerre de l'information car c'est un procédé qui peut visiblement provoquer d'importantes perturbations à un moindre coût. Le cas échéant, les démocraties pourraient contrer ces manœuvres d'influence en engageant des actions concrètes. Tout d'abord, lorsqu'elles sont confrontées à des cas d'ingérence électorale, les démocraties doivent engager des poursuites judiciaires, comme cela a été le cas aux États-Unis en février et juillet 2018, où le département de la justice a inculpé plusieurs ressortissants et entreprises russes. Un deuxième instrument possible est celui des sanctions. Tous les membres de l'OTAN ont adopté des sanctions à l'encontre de la Fédération de Russie après que le pays ait annexé illégalement la Crimée en 2014, et ces sanctions doivent être maintenues jusqu'à ce que la situation évolue. En revanche, un seul membre de l'OTAN a infligé des sanctions à la Russie en réaction à son ingérence dans le processus électoral. À l'été 2017, le Congrès des États-Unis a, lors d'un vote bipartite quasi-unanime, autorisé l'application de nouvelles sanctions à la Russie, notamment du fait de son ingérence dans les élections de 2016. En mars 2018, la Maison Blanche a finalement entériné ces sanctions prévues par la loi. L'administration états-unienne a ciblé cinq entités et 19 individus, dont la société *Internet Research Agency* ainsi que des individus identifiés, au cours de l'enquête menée par un conseil juridique spécial, comme ayant participé à la campagne d'ingérence électorale de la Russie. La rapporteure se félicite de ces premiers pas et prend acte d'une application accrue des sanctions ces derniers mois, mais note que ces avancées sont insuffisantes eu égard au large éventail de sanctions autorisées par le Congrès. La rapporteure préconise en outre que des discussions aient lieu au niveau national et collectif en vue de mettre en œuvre de nouvelles sanctions, compte tenu des preuves supplémentaires attestant de l'ingérence de la Russie dans les processus démocratiques.

74. Les démocraties peuvent et doivent, lorsqu'elles sont confrontées à des manœuvres d'influence, afficher une unité au niveau national et à l'échelle internationale. La Russie s'efforce d'exploiter et d'exacerber les polarisations préexistantes au sein des sociétés. Une ingérence est réussie lorsque des acteurs politiques utilisent la désinformation pour en tirer des avantages à court terme, par exemple en exploitant des fuites à des fins politiques. Pour éviter qu'elle ne se reproduise à l'avenir, l'ingérence doit donc être fermement et rapidement repoussée dans un esprit d'unité. Les responsables politiques doivent être capables d'admettre qu'une ingérence russe a eu lieu lorsque c'est manifestement le cas. Les opposants politiques doivent la condamner en parlant d'une seule voix, en émettant des messages clairs et en adoptant des mesures faciles à mettre en œuvre. En concevant des normes et des procédures qui dissuadent d'exploiter la désinformation, les systèmes politiques peuvent améliorer leur résilience et décourager toute guerre de l'information future. Le choix du peuple lors d'élections ou de référendums doit être fermement protégé.

IV. CONCLUSIONS

75. En février 2018 aux États-Unis, le directeur de la NSA, Dan Coats, a témoigné devant les membres de la commission du renseignement du Sénat. Lors de son évaluation des menaces mondiales pour les États-Unis et ses alliés, M. Coats a indiqué : « Nous nous attendons à ce que la Russie continue à utiliser la propagande, les médias sociaux, des fausses bannières, le prosélytisme et tout moyen d'influence pour tenter d'accroître les divisions sociales et politiques aux États-Unis […]. Il ne fait aucun doute que la Russie considère ses efforts passés comme des réussites et les élections américaines de mi-mandat de 2018 comme une cible potentielle de ses manœuvres d'influence » (*Senate Select Intelligence Committee*, 2018).

76. Comme l'indique la déclaration de M. Coats et comme le montre ce rapport, le problème de l'ingérence russe dans les processus électoraux ne va pas disparaître de lui-même. Les événements récents semblent indiquer au contraire que ce procédé occupera désormais une place plus importante que jamais dans l'arsenal de la Russie. Avec un budget de plusieurs millions de dollars américains, les forces russes ont les moyens de susciter la méfiance et de semer la discorde, d'orienter les soutiens en faveur des personnalités politiques amies comme de mettre en danger leurs opposants. Bien que certaines dispositions aient été prises pour faire obstacle à l'ingérence russe conduite au moyen d'opérations cybernétiques et informationnelles, la Russie a pour l'heure subi peu de représailles. Parmi les cibles présumées de ses activités, un grand nombre sont toujours engluées dans des débats internes qui paralysent toute riposte collective.

77. Pour empêcher une nouvelle érosion des principes démocratiques libéraux, les États membres de l'OTAN auront besoin de renforcer leurs processus électoraux et de concerter leurs efforts en la matière. Cette nécessité deviendra de plus en plus pressante, car il existe de plus en plus de preuves démontrant que d'autres pays (dont la Chine et l'Iran) ont utilisé des tactiques semblables à celles de la Russie. Si certains de ces efforts sont décrits en détail dans les sections précédentes, il n'empêche que chaque pays devra examiner les pressions et les événements dont il est victime, et concevoir une riposte adaptée. Si la Russie adapte ses opérations à ses cibles, les ripostes doivent être, elles aussi, adaptées. La rapporteure tient toutefois à souligner que les ripostes individuelles et collectives doivent être conformes à nos valeurs communes, que sont notamment les libertés individuelles, les droits humains, la démocratie et l'État de droit. Si ces valeurs peuvent être exploitées par un adversaire, elles peuvent aussi représenter notre plus grand atout. Si nous ne leur restons pas fidèles, nous mettrons en danger les processus démocratiques que nous souhaitons tant préserver et perdrons tout bienfait que ces valeurs peuvent procurer.

78. Parce qu'ils contribuent à l'élaboration des politiques et fixent les programmes d'action, les parlementaires jouent un rôle particulièrement important dans le processus précité. Ils auront donc besoin d'encourager le dialogue, dans leurs pays respectifs, sur l'attitude à avoir face aux allégations d'ingérence. Ils devront collaborer avec leurs homologues des autres partis pour s'assurer que leurs administrés, et la société civile au sens large, accordent du crédit à des informations fiables. Ils devront également veiller à ce que les allégations qui sont rapportées fassent l'objet d'une enquête équitable et impartiale. Si la rapporteure reconnaît volontiers la difficulté de la tâche, elle espère néanmoins que ce rapport pourra alimenter les discussions et aider les États membres à prendre conscience des menaces que représentent les opérations d'ingérence. La rapporteure apprécie sincèrement les commentaires qui ont été apportés sur la précédente version du rapport à de la session de printemps par les membres de la commission, à la fois ceux représentant les pays membres et les pays associés – qui ont souvent été victimes d'opérations cybernétiques et informationnelles menées par la Russie. Elle se réjouit en particulier des commentaires qui lui ont été transmis sur les enseignements que les parlementaires – et leurs gouvernements – ont tirés de leur expérience en matière de guerre de l'information, avec des indications sur ce qui a fonctionné ou pas. Ces contributions ont été précieuses pour rédiger des recommandations de politique générale concrètes qui sont présentées dans ce rapport final, ainsi que dans la résolution établie à

l'intention du secrétaire général de l'OTAN et des gouvernements et des parlements des pays membres de l'Alliance.

79. Comme le montrent clairement les travaux menés par la commission des sciences et des technologies ces dernières années, les menaces qui se présentent dans le cyberspace et le secteur de l'information deviennent extrêmement préoccupantes. Avant les attentats terroristes du 11 septembre 2001, les États-Unis souffraient d'un certain manque d'imagination. L'Alliance – dans son ensemble ou à travers chacun de ses membres – ne doit pas reproduire ce scénario. Or, comme l'a récemment indiqué M. Coats : « Presque 20 ans ont passé, mais je peux vous dire que tous les témoins lumineux sont repassés au rouge » (Coats, 2018). La commission et l'Assemblée parlementaire de l'OTAN ne doivent donc certainement pas baisser la garde, mais au contraire, veiller à rester vigilantes face aux menaces qui touchent le cyberespace et l'information. La rapporteure est déterminée à apporter tout le soutien qu'elle pourra à cette entreprise.

BIBLIOGRAPHIE

Alandete, David, "How the Russian Meddling Machine Won the Online Battle of the Illegal Referendum", *El Pais*, 13 November 2017a,

Alandete, David, "Russian Meddling Machine Sets Sights on Catalonia", *El Pais*, 28 September 2017b

Alandete, David, "Russian Network Used Venezuelan Accounts to Deepen Catalan crisis", *El Pais*, 11 November 2017c

Albeanu, Catalina, "3 Fact-Checking Initiatives at Le Monde as the Newsroom Gears Up for the French Election", *Journalism.co.uk*, 28 March 2017

Applebaum, Anne; Pomerantsev, Peter; Smith, Melanie; and Colliver, Chloe, "'Make Germany Great Again': Kremlin, Alt-Right, and International Influences in the 2017 German Elections", *London School of Economics*, 2017

AP-OTAN, *La Guerre Hybride : Un Nouveau Défi Stratégique pour l'OTAN ?* [166 DSC 15 F BIS], présenté par Julio Miranda Calha, 2015

AP-OTAN, La Révolution des Medias Sociaux [158 CDSDG 17 F bis], présenté par Jane Cordy, 7 octobre 2017

AP-OTAN, Parades aux Menaces Hybrides Émanant de la Russie : une Mise à Jour [166 CDS 18 F], rapport présenté par Lord Jopling, 2018

Associated Press, "The Latest: France Says No Trace of Russian Hacking Macron", *Associated Press*, 1 June 2017

Barker, Tyson, "Germany Strengthens Its Cyber Defense", *Foreign Affairs*, 26 May 2017

Barzic, Gwenaelle; Kar-Gupta, Sudip; Heavens, Andrew; and Lough, Richard, "Facebook, Google Join Drive Against Fake News in France", *Reuters*, 6 February 2017

BBC News, "Theresa May Accuses Vladimir Putin of Election Meddling", *BBC* News, 14 November 2017

BBC News, "Emmanuel Macron: French President Announces 'Fake News' Law", *BBC News*, 3 January 2018

Beardsley, Eleanor, "France Warns Russia to Stay Out Of Its Presidential Election", *National Public Radio*, 21 February 2017

Beaulieu, Britanny and Keil, Steven, *Russia as Spoiler: Projecting Division in Transatlantic Societies*, Alliance for Securing Democracy, German Marshall Fund of the United States, 2018

Beuth, Patrick; Biermann, Kai; Klingst, Martin; and Stark, Holger, "Merkel and the Fancy Bear", *Zeit Online*, 12 May 2017

Booth, Robert; Weaver, Matthew; Hern, Alex; and Walker, Shaun, "Russia Used Hundreds Of Fake Accounts to Tweet about Brexit, Data Shows", *The Guardian*, 14 November 2017

Borchers, Callum, "What We Know about the 21 States Targeted by Russian Hackers", *Washington Post*, 23 September 2017

Brattberg, Erik and Maurer, Tim, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*, Carnegie Endowment for International Peace, 2018

Burr, Warner et al., *Senate Intel Committee Releases Unclassified 1st Installment in Russia Report, Updated Recommendations on Election Security*, Senate Intelligence Committee, 2018

Cadwalladr, Carole and Jukes, Peter, "Leave.EU Faces New Questions over Contacts with Russia", *The Guardian*, 16 June 2018

Centre d'excellence de cyberdéfense coopérative de l'OTAN, *Cyber Security Strategy Documents*, Centre d'excellence de cyberdéfense coopérative de l'OTAN, 2018

Challenges, "Cyberattaques contre l'équipe Macron: le point sur la situation", 5 October 2017

Chrisafis, Angelique, "Emmanuel Macron Promises Ban on Fake News During Elections", The Guardian, 3 January 2018

City Press Office, "13,500-Strong Twitter Bot Army Disappeared Shortly after EU Referendum, research reveals", *City, University of London*, 20 October 2017

Coats, Dan, *Transcript: Dan Coats Warns the Lights Are 'Blinking Red' On Russian Cyberattacks*, NPR, 18 July 2018

Cole, Harry "Dressing Down: Web Firms Facebook and Google 'Should Be Legally to Blame for Fake News', MPs Warn", 28 July 2018
Colborne, Michael, "The Brief Life, and Looming Death, of Europe's 'SWAT Team for Truth'", *Foreign Policy*, 20 September 2017
Commissariato di PS, *Report Fake News*, *Commission of Public Security Online*, 2018
Commission européenne, *Lutter contre la désinformation en ligne*, 2018
Corera, Gordon, "Russia 'Will Target US Mid-Term Elections' Says CIA Chief", *BBC News*, 29 January 2018
Cybersecurity and Digital Privacy Unit, The Directive on Security of Network and Information Systems (NIS Directive), European Commission, 19 September 2017
Dearden, Lizzie, "Emmanuel Macron Email Leaks 'Linked to Russian-Backed Hackers Who Attacked Democratic National Committee'", *The Independent*, 6 May 2017
De La Garza, Alejandro, "Here's What Deputy Attorney General Rod Rosenstein Said About Indicting Russian Intelligence Officers for Election Hacking", *Time*, 13 July 2018
Deutsche Welle, "Germany Plans Creation of 'Center Of Defense' Against Fake News, Report Says", *Deutsche Welle*, 23 December 2016
Diamond, Larry, "Russia and the Threat to Liberal Democracy", *The Atlantic*, 9 December 2016
DiResta, Renee, *Statement for the Record from Renee DiResta*, US Senate Select Committee on Intelligence, 2018
Dwoskin, Elizabeth and Timberg, Craig, "Microsoft Says It Has Found a Russian Operation Targeting U.S. Political Institutions", *The Washington Post*, 21 August 2018
Edgett, Sean, *Sean Edgett's Answers to Questions for the Record*, Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism, 19 January 2018
Emmott, Robin, "Spain Sees Russian Interference in Catalonia Separatist Vote", *Reuters*, 13 November 2017
Europol, Europol Internet Referral Unit One Year On, *Europol*, 22 Juillet 2016
Fandos, Nicholas and Shane, Scott, "Senator Berates Twitter Over 'Inadequate' Inquiry Into Russian Meddling", *New York Times*, 28 September 2017
Figueroa, Ariana, "Can Teaching Civics Save Democracy?", *National Public Radio*, 22 September 2017
Fly, Jamie, Rosenberger, Laura and Salvo, David, *Policy Blueprint for Countering Authoritarian in Democracies*, Alliance for Securing Democracy, German Marshall Fund of the United States, 2018
Foster, Peter, "Russia Accused of Clandestine Funding of European Parties as US Conducts Major Review of Vladimir Putin's Strategy", *The Telegraph*, 16 January 2016
Fox, Robert A., Statement Prepared for the U.S. Senate Select Committee on Intelligence hearing: Disinformation: A Primer In Russian Active Measures And Influence Campaigns', United States Senate Committee on Intelligence, 30 March 2017
Fried, Daniel and Polyakova, *Democratic Defense against Disinformation*, Atlantic Council, 2018
Gramer, Robbie, "Wary of Russian Cyber Threat, France Plans to Bolster its Army of 'Digital Soldiers'", *Foreign Policy*, 10 January 2017,
Graves, Lucas and Cherubini, Federica, *The Rise of Fact-Checking Sites in Europe*, Reuters Institute for the Study of Journalism, 2016
Greenberg, Andy, "Hackers Hit Macron With Huge Email Leak Ahead of French Election", *Wired*, 5 May 2017a,
Greenberg, Andy, "The NSA Confirms It: Russia Hacked French Election 'Infrastructure'", *Wired*, 9 May 2017b
Hacquebord, Feike, *Two Years of Pawn Storm*, Trend Micro, 2017
Harris, Gardiner, "State Dept. Was Granted $120 Million to Fight Russian Meddling. It Has Spent $0.", *The New York Times*, 4 March 2018
Hern, Alex; Duncan, Pamela; and Bengtsson, Helena, "Russian 'Troll Army' Tweets Cited More than 80 Times in UK Media", *The Guardian*, 20 November 2017
High Level Group on Fake News and Online Disinformation, *A Multi-Dimensional Approach to Disinformation*, Report of the High Level Group on Fake News and Online Disinformation, 2018

Horowitz, Jason, "In Italian Schools, Reading, Writing, and Recognizing Fake News", *New York Times*, 18 October 2017
Inglis, Chris, *Statement of Chris Inglis before the Senate Armed Services Committee*, US Senate, 27 April 2017
Intelligence and Security Committee of Parliament, *Press Release: 23 November 2017*, *Intelligence and Security Committee of Parliament*, 23 November 2017
Karp, Brad S., *Federal Guidance on the Cybersecurity Information Sharing Act of 2015*, Harvard Law School Forum on Corporate Governance and Financial Regulation, 2016
Kelly, John W., *Briefing for the United States Senate Select Committee on Intelligence*, US Senate Select Committee on Intelligence, 1 August 2018
McFadden, Cynthia; Arkin, William M.; Monahan, Kevin; and Dilanian, Ken, "U.S. Intel: Russia Compromised Seven States Prior to 2016 Election", *NBC News*, 28 February 2018
Kelly, Mary Louise and Warner, Mark, "What You Need To Know About The Honest Ads Act", *National Public Radio*, 19 October 2017
Lapowsky, Issie, "Iran Emerges as Latest Threat to Facebook and Twitter", *Wired*, 21 August 2018
Lecher, Colin, "Here Are the Russia-Linked Facebook Ads Released by Congress", *The Verge*, 1 November 2017
Lipton, Eric; Sanger, David E.; and Shane, Scott, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.", *New York Times*, 13 December 2016
Luhn, Alec, "From Russia, with Love", *Vice News*, 5 May 2017
Maldre, Patrik, *Moving Toward NATO Deterrence for the Cyber Deterrence for the Cyber Domain: Cyber Intelligence Brief No. 1*, Center for European Policy Analysis, May 2016
Maness, Ryan C. and Jaltner, Margarita, "There's More to Russia's Cyber Interference than the Mueller Probe Suggests", *The Washington Post*, 12 March 2018
Meakins, Joss, "Why Russia is far less threatening than it seems", *Washington Post*, 8 March 2017
Meister, Stefan, "The 'Lisa Case': Germany as a Target Of Russian Disinformation", *NATO Review Magazine*, 2016
Milosevich-Juaristi, Mira, *The Combination': An Instrument in Russia's Information War in Catalonia*, Real Instituto Elcano, 20 November 2017
Minority Staff of the Committee on Foreign Relations of the United States Senate, *Putin's Asymmetric Assault on Democracy In Russia And Europe: Implications For U.S. National Security*, United States Senate, 2018
National Conference of State Legislatures, *Election Security: State Policies*, *National Conference of State Legislatures*, 13 February 2018
Neudert, Lisa-Maria; Kollanyi, Bence; and Howard, Philip N., *Junk News and Bots during the German Parliamentary Election: What are German Voters Sharing over Twitter?*, Oxford University, 19 September 2017
Newman, Lily Hay, "Securing Elections Remain Surprisingly Controversial", Wired, 13 July 2017
Nimmo, Ben, *Propaganda in a New Orbit: Information Warfare Initiative Paper No 2*, Center for European Policy Analysis, 2016
Nimmo, Ben, *#ElectionWatch: Russia and Referendums in Catalonia?*, Atlantic Council, 2017
Office of the Director of National Intelligence, *Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution*, 2017
Oltermann, Philip, "German Government Intranet Under 'Ongoing Attack'", *The Guardian*, 1 March 2018
Osnos, Evan; Remnick, David; and Yaffa, Joshua, "Trump, Putin, and the New Cold War", *The New Yorker*, 6 March 2017
Paul, Christopher and Matthews, Miriam, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*, RAND Corporation, 2016
Peters, Jonathan, *Putin, Politics, and the Press*, Columbia Journalism Review, 3 March 2017
Posner, Bob, *Responding to the Rise of Digital Campaigning*, *UK Electoral Commission blog*, 31 October 2017
Raul, Alan Charles; Smith, John; and Sulmeyer, Michael, *Touring the World of Cybersecurity Law*, RSA Conference 2016, 2016

Reuters, "Russian Twitter Accounts Promoted Brexit ahead of EU Referendum: Times Newspaper", *Reuters*, 15 November 2017
Roberts, Liz Saville and Caroline Nokes, Elections: Written question – 113484, Minister for the Cabinet Office, 2017
Roose, Kevin, "Facebook Grapples With a Maturing Adversary in Election Meddling", *TheNew York Times*, 1 August 2018
Rosenwald, Michael, *Making Media Literacy Great Again*, Columbia Journalism Review, 2017
Rozenshtein, Alan, *"It's the Beginning of the End of the Internet's Legal Immunity", Foreign Policy,* 13 November 2017
Rutenberg, Jim, "RT, Sputnik and Russia's New Theory of War", *New York Times*, 13 September 2017
Salvo, David and Beaulieu, Brittany, *NATO and Asymmetric Threats: A Blueprint for Defense and Deterrence*, Alliance for Securing Democracy, German Marshall Fund of the United States, 2018
Satter, Raphael; Donn, Jeff; and Day, Chad, "Inside Story: How Russians Hacked the Democrats' Emails", *U.S. News and World Report*, 4 November 2017
Seetharaman, Deepa, "Russian-Backed Facebook Accounts Staged Events Around Divisive Issues", *Wall Street Journal*, 30 October 2017
Senate Select Intelligence Committee, *"Global Threats and National Security"*, C-SPAN, 13 February 2018
Senate Select Intelligence Committee, "Russia's Role in Election-Year Hacking", *C-SPAN*, 10 January 2017
Serhan, Yasmeen, "Italy Scrambles to Fight Misinformation Ahead of Its Elections", *The Atlantic*, 24 February 2018
Shaban, Hamza, "Members of the U.K. Parliament Grill American Tech Giants over the Spread of Fake News", *Washington Post*, 8 February 2018
Solon, Olivia and Siddiqui, Sabrina, "Russia-backed Facebook posts 'reached 126m Americans' during US election", *The Guardian*, 31 October 2017
Solon, Olivia, "Facebook Removes 652 Fake Accounts and Pages Meant to Influence World Politics", *The* Guardian, 22 August 2018
Splidsboel Hansen, Flemming, *The Weaponization of Information: News from the Cognitive Domain*, DIIS, 14 December 2017
Sputnik News, "Thousands Yell 'Death to US' Near Turkey's Incirlik Base, Home to US Nukes", *Sputnik News*, 28 July 2016
Stetler, Brian, "Facebook to begin warning users of fake news before German election", CNN, 15 January 2017
Stewart, Emily, "Russian Election Interference is Far From Over. I Asked 9 Experts How to Stop It.", *Vox*, 19 February 2018,
Strobel, Warren and Walcott, John, "Top NSA official Says Telephone Surveillance Should Have Been Disclosed", *Reuters*, 22 March 2017
Swell Chan, "Fearful of Hacking, Dutch Will Count Ballots by Hands", *The New York Times*, 1 February 2017
Thompson, Nicholas and Vogelstein, Fred, "Inside The Two Years That Shook Facebook—And The World", *Wired*, 12 February 2018
Timberg, Craig and Elizabeth Dwoskin, "Facebook Takes Down Data and Thousands Of Posts, Obscuring Reach OF Russian Disinformation", *Washington Post*, 12 October 2017
Toucas, Boris, *The Macron Leaks: The Defeat of Informational Warfare*, Center for Strategic & International Studies, 30 May 2017
UK House of Commons Digital, Culture, Media and Sport Committee, *Disinformation and 'Fake News': Interim Report*, UK House of Commons Digital, Culture, Media and Sport Committee, 29 July 2018
Van de Velde, Jacqueline, *The Law of Cyber Interference in Elections*, SSRN, 2017
Van Hollen and Rubio, Van Hollen, Rubio Statement on Election Security Executive Order, 12 September 2018

US Department of Justice, *United States of America v. Internet Research Agency…*, 16 February 2018
Vogelstein, Fred, "Facebook Tweaks Newsfeed To Favor Content From Friends, Family", *Wired*, 11 January 2018
Volz, Dustin, "U.S. Far-Right Activists, WikiLeaks and Bots Help Amplify Macron Leaks: researchers", *Reuters*, 7 May 2017
Volz, Dustin and David Ingram, "Facebook: Russian Agents Created 129 U.S. Election Events", *Reuters*, 25 January 2018
Walker, Peter, "New National Security Unit Set Up to Tackle Fake News in UK", *The Guardian*, 23 January 2018
Waltzman, Rand, *The Weaponization of Information: The Need for Cognitive Security,* RAND Corporation, 2017
Watts, Clint, *Cyber-Enabled Information Operations*, Statement Prepared for the US Senate Committee on Armed Services, 2017
Watts, Duncan J. and Rothschild, David M., *Don't Blame the Election on Fake News. Blame it on the Media*, Columbia Journalism Review, 2017
Weedon, Jen; Nuland, William; and Stamos, Alex, *Information Operations and Facebook*, Facebook, 2017
Weisburd, Andrew; Watts, Clint; and Berger, J.M., *Trolling for Trump: How Russia is Trying to Destroy our Democracy*, War on the Rocks, 6 November 2016
Williams-Grut, Oscar, "REPORT: Russia hacked UK energy companies on election day", *Business Insider*, 19 July 2017
Witte, Griff, "As Germans Prepare to Vote, a Mystery Grows: Where are the Russians?", *Washington Post*, 10 September 2017
Young, Zachary, "French Parliament Passes Law Against 'Fake News'," *Politico*, 4 July 2018
Yurieff, Kaya, "Facebook Will Show Users What Russian Propaganda They Liked or Followed", *CNN*, 22 November 2017
Zygar, Mikhail, "Why Putin Prefers Trump", *Politico*, 27 July 2016