ASSEMBLEE PARLEMENTAIRE DE L'OTAN

COMMISSION
SUR LA DIMENSION CIVILE
DE LA SÉCURITÉ (CDS)

PARADES AUX MENACES HYBRIDES ÉMANANT DE LA RUSSIE : UNE MISE À JOUR

Rapport spécial

par Lord JOPLING (Royaume-Uni)
Rapporteur spécial

166 CDS 18 F fin| Original : anglais | 28 septembre 2018

TABLE DES MATIÈRES

I. INTRODUCTION

1. Bien qu'elle ne soit pas nouvelle, l'expression « guerre hybride »[1] a fait florès dans le discours politique international après l'invasion de l'Ukraine et l'annexion de la Crimée par la Russie en 2014. La guerre hybride peut être définie comme « l'utilisation de tactiques asymétriques pour repérer et exploiter les faiblesses du camp adverse par des moyens non militaires (tels que l'intimidation et la manipulation politiques, informationnelles et économiques) s'appuyant sur la menace d'un recours à des moyens militaires classiques ou non »[2]. Dans le contexte de l'OTAN, la guerre hybride est une campagne menée contre l'Alliance (ou l'un de ses membres) par des moyens non susceptibles de déclencher l'application de l'article 5 du Traité de Washington, dans lequel est inscrit le principe de la défense collective.

2. En Europe et en Amérique du Nord, la situation sécuritaire regorge d'exemples d'activités hybrides. Le présent rapport spécial est spécifiquement consacré à la panoplie des tactiques hybrides du Kremlin et à son utilisation, dès lors que lesdites tactiques sont très probablement les plus perfectionnées, les plus ingénieuses, les plus complètes et les plus concertées. Mais il traite aussi de la Russie elle-même, qui, dans sa doctrine militaire de 2014, désigne clairement l'OTAN comme la principale menace pesant sur sa sécurité. La guerre hybride russe vise avant tout la communauté euro-atlantique et les pays de la « zone grise » qui sépare l'OTAN et l'Union européenne, d'une part, et la Russie, d'autre part.

3. Les spécialistes occidentaux s'accordent à penser que la Russie est une puissance en déclin et que l'avenir recèle sans doute des défis bien plus grands mais que, à court terme, elle représente la menace la plus grave pour l'ordre international. En fait, le déclin russe pourrait encourager Vladimir Poutine à user des moyens dont il dispose pour revisiter tôt ou tard – avec une préférence pour la première échéance – les arrangements passés à la fin de la guerre froide (Foreign Affairs, 2017). Les tactiques hybrides peuvent conférer un avantage significatif au « plus faible des deux camps » (Saarelainen, 2017). Par exemple, elles mettent à profit le problème de l'attribution, autrement dit la difficulté en cas d'attaque de remonter la piste de l'État qui en est l'auteur, et la mondialisation. La dynamique des pouvoirs ne repose plus uniquement sur les moyens matériels et se fonde de plus en plus sur l'aptitude à influencer les convictions, les attitudes et les aspirations d'autrui, aptitude que les nouvelles technologies et l'interconnexion propre à l'ère de l'information ont décuplée (Smith, 2017).

4. L'utilisation par Moscou de tactiques hybrides ne doit rien au hasard ou à l'improvisation. C'est le fruit d'une stratégie coordonnée dûment réfléchie et financée, en attestent les récentes enquêtes du renseignement aux États-Unis, dont les résultats concernant l'emploi de ces deux tactiques hybrides très différentes, que sont l'ingérence dans l'élection présidentielle aux États-Unis et l'envoi de mercenaires russes en Syrie, pointent tous vers un seul et même homme, l'oligarque proche du Kremlin, Evguéni Prigojine[3].

5. Depuis l'invasion de la Géorgie en 2008 et, surtout, depuis l'occupation et l'annexion de la Crimée en 2014, les pays occidentaux sont bien plus conscients des manœuvres perturbatrices de la Russie. Dans un discours de novembre 2017, la première ministre du Royaume-Uni,

---

1 L'expression date au moins de la guerre du Liban de 2006 ; elle désignait à l'époque la stratégie employée par le Hezbollah.

2 Selon la définition qu'en donne le rapport général 2015 de la commission de la défense et de la sécurité de l'AP-OTAN *La guerre hybride : un nouveau défi stratégique pour l'OTAN ?* [166 DSC 15 F bis]

3 M. Prigojine, surnommé « le cuistot de Poutine », a bâti son empire de la restauration (y compris collective) grâce, pour une bonne part, à la passation de contrats avec l'État et aux rapports étroits qu'il entretient avec M. Poutine. Le *New York Times* rapporte que, selon les personnes qui se montrent critiques à l'égard de l'intéressé – parmi lesquels des membres de l'opposition politique, des journalistes et des membres d'associations diverses, ainsi que le ministère des finances des États-Unis et Robert S. Mueller III, procureur spécial auprès du ministère de la justice –, il est l'oligarque expert en missions secrètes du Kremlin.

Theresa May, a explicitement accusé le Kremlin de tenter de « saper les sociétés libres » et de « semer la discorde à l'Ouest » en menant une longue campagne de cyberespionnage et de déstabilisation des gouvernements et des parlements européens. Dans une déclaration commune – fait assez rare pour être signalé – datant du 15 mars 2018, les dirigeants britanniques, français, allemands et états-uniens ont condamné l'attentat à l'arme chimique de Salisbury, attentat dont ils ont estimé qu'il portait atteinte à la souveraineté du Royaume-Uni et qu'il avait « très probablement » été commis par la Russie. En août 2018, faisant suite à cet attentat, Washington a pris de nouvelles sanctions à l'encontre de Moscou, sanctions conçues pour empêcher la Russie d'obtenir des États-Unis des composants électroniques d'importance névralgique et diverses technologies à double application. Vingt-huit pays membres ou partenaires de l'OTAN avaient alors manifesté leur solidarité avec Londres en expulsant plus de 150 agents diplomatiques russes. L'OTAN a condamné cette première utilisation d'un gaz innervant sur son territoire et a réduit d'un tiers la taille maximale de l'effectif de la délégation dont la Russie dispose auprès de l'Organisation ; elle a, ce faisant, signifié clairement au Kremlin qu'il devait subir les conséquences d'un comportement aussi inacceptable que dangereux.

6. Le présent rapport vise à générer une plus grande prise de conscience des activités hybrides de Moscou (ingérence politique, utilisation d'une force de faible intensité, espionnage, assassinats et corruption, désinformation et propagande, cyberattaques, pressions économiques et contournement des sanctions) et à montrer de quelle façon certaines techniques se renforcent et se complètent mutuellement. Il passera en revue les contre-mesures adoptées par la communauté euro-atlantique et proposera des méthodes supplémentaires pour renforcer la résilience et la défense des populations des pays de l'Alliance face à ces menaces complexes.

II. PETIT MANUEL DES TECHNIQUES HYBRIDES DU KREMLIN

A. ORIGINES ET CONTEXTE

7. Le recours de la Russie à la guerre hybride remonte à l'époque soviétique, au moment de la création des concepts de « mesures actives »[4], « maskirovka »[5] et « contrôle réflexif »[6]. Les tactiques hybrides sont redevenues d'actualité dans les années 2000 lorsqu'une fois de plus la Russie a désigné l'Ouest comme son adversaire stratégique, démarche attestée par l'intervention de M. Poutine à la Conférence de Munich sur la sécurité en 2007. Elles ont aussi été adoptées en raison de la comparaison désavantageuse entre les capacités militaires classiques, les moyens technologiques et les instruments de « puissance douce » de la Russie, d'une part, et ceux de l'Ouest, d'autre part, ainsi qu'au vu des progrès enregistrés dans les domaines de l'informatique et de la communication, progrès qui ont fait apparaître de nouvelles possibilités de prendre à partie la société et le système politique d'adversaires potentiels.

8. L'intention de la Russie de recourir à des tactiques hybrides transparaît dans divers documents, dont les plus récents sont la Doctrine militaire de 2014, la Stratégie de sécurité nationale de 2015 et la Doctrine pour la sécurité informatique et informationnelle de 2015. Ces textes préconisent l'élaboration de moyens effectifs d'influencer l'opinion publique à l'étranger et, en cas de besoin, l'emploi de méthodes « non traditionnelles ». Dans un article souvent évoqué où il expose les principes de la guerre hybride, le chef d'état-major des forces armées russes,

4 Opérations de subversion politique allant de la manipulation des médias à la prise pour cibles d'opposants politiques

5 Dissimulation d'activités militaires à des fins de dénégation ou de tromperie. Par exemple : la dissimulation d'armes offensives à destination de Cuba, qui a donné lieu à la crise des missiles de 1962.

6 Communication à un opposant d'informations susceptibles de l'inciter à réagir impulsivement en faveur du Kremlin. Un éminent expert en « contrôle réflexif » soviétique, Timothy L. Thomas, donne l'exemple de la façon dont les dirigeants soviétiques avaient fait défiler de faux missiles et mis en circulation de faux documents, l'objectif étant d'amener les services de renseignement occidentaux à conclure que l'URSS disposait d'un arsenal nucléaire plus impressionnant qu'il ne l'était en réalité.

Valeri Guerassimov, fait observer entre autres que « l'espace informationnel offre de vastes possibilités asymétriques de réduire le potentiel de combat de l'ennemi » (NATO StratCom, 2015). En février 2017, le ministre de la défense, Serguei Choigou, a annoncé la création de forces d'opérations informationnelles pour « lutter contre la propagande ». Par ailleurs, le Kremlin a institutionnalisé le processus décisionnel de la guerre hybride en créant, en 2014, le centre de contrôle de la défense nationale (NTsUO). Cet organe coordonne les activités des structures militaires, certes, mais aussi d'agences de sécurité ou d'entités civiles telles que le service fédéral de sécurité (FSB), le service fédéral de protection (FSO), le service des renseignements extérieurs (SVR), le ministère de l'intérieur et l'agence fédérale de l'énergie atomique (RosAtom). Il semble être doté d'« un nombre incroyable de fonctions de contrôle, de supervision et de décision dans le secteur de la défense nationale ». Selon le spécialiste de la Russie Roger McDermott, le NTsUO marque le franchissement d'une étape « sur la voie de l'élaboration d'opérations sécuritaires plus intégrées ». Il est conçu pour donner à la Russie l'avantage sur l'OTAN, s'agissant de prendre des décisions dans des délais plus courts. En même temps, d'autres tactiques figurant dans l'arsenal de guerre hybride russe sont destinées à semer la discorde entre Alliés ou à l'intérieur même des pays de l'Alliance pour ralentir le processus décisionnel de l'OTAN (Thornton, 2016).

9. Moscou justifie son emploi de tactiques hybrides en se présentant comme la victime de « l'agression informationnelle » occidentale. Le chef du SVR, Serguei Narychkine, a accusé les États-Unis et leurs alliés (dont le Royaume-Uni, la Pologne, les pays baltes et la Suède) de mener une guerre hybride occulte contre les États souverains membres de la Communauté des États indépendants (CEI). Il a également accusé l'Ouest de tenter d'enfoncer un coin entre ces mêmes États, de s'immiscer dans leurs « processus démocratiques » et de faire obstacle à l'intégration eurasienne (Belsat, 2017).

10. Comme l'a fait remarquer Mark Galeotti, grand spécialiste de la Russie, l'accent que le Kremlin met sur les techniques hybrides « témoigne de l'opportunisme parcimonieux d'une Russie faible mais impitoyable qui veut jouer à la grande puissance sans en avoir les moyens » (Calabresi, 2017). Les chapitres suivants passeront succinctement en revue les techniques hybrides de la Russie.

B. INGÉRENCES POLITIQUES

11. La Russie était déjà soupçonnée depuis longtemps d'immixtion dans la politique des pays de son « étranger proche » ; désormais, les preuves s'accumulent des efforts qu'elle consent pour influer sur l'évolution de la situation politique dans des démocraties établies de longue date en conjuguant cyberattaques, divulgation de données volées, utilisation de machines zombies (bots)[7] et de trolls[8], désinformation et soutien à des partis extrémistes[9]. Selon les services de renseignement extérieur estoniens, la Russie entretient un réseau d'« agents d'influence » – membres de la classe politique et des milieux d'affaires, journalistes ou diplomates – qui promeuvent ses objectifs en Europe occidentale. Le rapporteur souhaite mentionner ici quelques faits et déclarations qui, pris dans leur ensemble, suggèrent l'application par Moscou d'une politique visant délibérément à interférer avec des élections ou des référendums récemment organisés dans des pays occidentaux. Ces interférences tendent à prendre la forme d'un soutien à des partis, candidats ou propositions de référendum s'opposant au système en place (Galeoti, 2017). Le rapporteur souhaite également souligner que l'existence d'une telle politique ne signifie en aucun cas que cette dernière a joué un rôle décisif dans le résultat des élections et référendums concernés.

---

7 Logiciel conçu pour générer automatiquement des messages (comme des tweets, par exemple)

8 Individus qui affichent en ligne des messages provocateurs, incendiaires, prêtant à controverse ou hors sujet

9 Les techniques utilisées par le Kremlin pour interférer avec les processus électoraux des pays occidentaux sont étudiées en détail dans le rapport général 2018 de la commission des sciences et des technologies *L'ingérence de la Russie dans les processus électoraux et référendaires des pays de l'Alliance* [181 STC 18 F fin].

12. L'exemple le plus marquant des ingérences de la Russie est la tentative d'influer sur le résultat de l'élection présidentielle de 2016 aux **États-Unis**. En janvier 2017, les services de renseignement américains ont publié un rapport dans lequel on pouvait lire ceci : « M. Poutine et le gouvernement russe ont souhaité aider M. Trump à remporter l'élection présidentielle, si possible en discréditant M^me^ Clinton ». Les auteurs du rapport tenaient « pour hautement probable que les services du renseignement militaire russes [avaient divulgué] les données de victimes américaines obtenues au cours de cyberopérations, données communiquées publiquement ou en exclusivité à des médias et transmises à *WikiLeaks* ». Ils observaient en outre que « ces activités attest[aient] une escalade notable du triple point de vue du caractère direct de ces activités, de leur niveau et de leur ampleur par comparaison à de précédentes opérations ». Les responsables du département de la sécurité intérieure des États-Unis (DHS) ont admis que les Russes avaient tenté d'accéder aux listes électorales de 21 États américains et qu'ils y étaient parvenus « dans un nombre de cas exceptionnellement réduit ». Le DHS a pu déterminer que « l'analyse et l'étude des bases de données électorales étaient le fait du gouvernement russe » (McFadden, Arkin et Monahan, 2018).

13. Des individus liés aux autorités russes ont dérobé et publié des milliers de messages électroniques de responsables politiques états-uniens et ont acheté des encarts publicitaires sur Facebook, tandis que des bots et des trolls soutenus par la Russie postaient des histoires mensongères sur les réseaux sociaux et la section « commentaires » de divers articles. À l'occasion de l'élection présidentielle, les Russes ont affiché sur Facebook et Instagram plus de 3 000 messages renvoyant à 120 pages de Facebook dans une campagne qui a touché 126 millions d'États-uniens (*UK House of Commons*, juillet 2018).

14. De hauts responsables de l'administration Trump, dont Rex Tillerson (à l'époque secrétaire d'État) et Nikki Haley, ambassadrice des États-Unis à l'ONU, ont qualifié l'ingérence supposée de la Russie dans l'élection présidentielle d'« acte de guerre hybride » et accusé Moscou de tenter de « semer le chaos » dans les processus électoraux du monde entier.

15. Au **Royaume-Uni**, le Parlement enquête sur l'immixtion de la Russie dans le référendum consacré au Brexit. Le président de la commission parlementaire sur le numérique, la culture, les médias et le sport, Damian Collins, a indiqué que, à en juger par le premier lot de données reçues des entreprises de réseaux sociaux, des comptes pro-Kremlin essayaient « d'influencer le débat politique au Royaume-Uni, d'inciter à la haine et de dresser les communautés les unes contre les autres » ; il a reconnu que les preuves recueillies « pouvaient n'être que la partie émergée de l'iceberg » (Burgess, 2017). Un rapport de la société britannique *89up.org* indique que les médias appartenant au gouvernement russe, RT (*Russia Today*) et *Sputnik* avaient publié au moins 261 articles manifestement anti-Union européenne, tandis que des trolls et des bots favorables au gouvernement russe veillaient à une large diffusion de ces articles dans les réseaux sociaux (Euronews, 2018). Une autre étude de spécialistes britanniques a recensé, dans les quelques jours qui ont précédé le vote, plus de 156 000 comptes Twitter ouverts en Russie et mentionnant #Brexit dans des messages originaux ou republiés et majoritairement favorables à la sortie de l'Union européenne. Ces messages ont été vus des centaines de millions de fois (BBC, novembre 2017).

16. Des incidents similaires ont eu lieu en **France** lors de l'élection présidentielle. Le plus notable d'entre eux est la divulgation, avant le vote, de milliers de documents (l'équivalent de huit gigabytes) se rapportant à la campagne de M. Macron et dont plusieurs ont été signalés comme étant falsifiés ou fabriqués de toutes pièces. Si les autorités responsables de la cybersécurité en France estiment qu'elles ne disposent pas d'informations suffisantes pour établir que la fuite est d'origine russe, la société de cybersécurité *Trend Micro* affirme pour sa part que ladite fuite présente de fortes similitudes avec l'ingérence qu'aurait commise la Russie dans l'élection présidentielle états-unienne (Willsher et Henley, 2017). Pour sa part, le directeur de l'agence nationale de la sécurité (NSA) des États-Unis, Michael Rogers, a indiqué que ses services avaient pu imputer à la Russie au moins plusieurs actes d'ingérence dans l'élection présidentielle française. Durant la campagne électorale, la NSA avait indiqué aux responsables de la cybersécurité française que des pirates informatiques

russes avaient peut-être altéré certains éléments du scrutin (Greenberg, 2017). Une banque russe a aidé au financement de la campagne électorale de la dirigeante d'extrême droite Marine Le Pen, bien que le parti de cette dernière nie toute malversation (Chekhovtsov, 2015).

17. En **Espagne** également, on parle d'une éventuelle immixtion de Moscou dans les affaires intérieures du pays, dont la plus récente stratégie de sécurité nationale inclut la menace des campagnes de désinformation. Le document ne mentionne pas spécifiquement la Russie, mais des responsables espagnols parlent ouvertement d'une ingérence russe dans le référendum sur l'indépendance de la Catalogne. Les ministres de la défense et des affaires étrangères d'Espagne ont indiqué que bon nombre des profils qui répandaient de fausses nouvelles se situaient sur le territoire russe. On rapporte que des comptes Twitter pro-Kremlin, dont des bots, et des médias du service public russe tels que *Pierviy Kanal*, *Vesti* et *Izvestia* auraient diffusé des informations mensongères ou incendiaires à l'encontre de l'Espagne. Il faut toutefois noter que la chaîne RT semble avoir assuré une couverture plus équilibrée du référendum en question, peut-être parce que certains dirigeants russes ont pensé qu'une attitude trop agressive envers Madrid pourrait déboucher sur des résultats contraires à ceux escomptés (Rettman, 2017).

18. Aux **Pays-Bas**, le service général de renseignement et de sécurité (AIVD) a signalé que, dans le contexte des élections législatives néerlandaises, « la Russie n'a[vait] pas hésité à recourir à des méthodes datant de la guerre froide pour acquérir une influence politique ». Dans son rapport annuel, l'AIVD affirme que les Russes ont tenté d'influer sur ces élections en propageant de fausses nouvelles, mais qu'ils ont échoué « à exercer une influence substantielle » sur le processus électoral.

19. La Russie continue d'entretenir des liens avec les partis politiques occidentaux opposés à l'*establishment* et, en particulier, avec les partis d'extrême droite. En **Allemagne**, l'AfD (Alternative pour l'Allemagne), formation arrivée en troisième position aux élections législatives de 2017 avec 12,6 % des voix, jouit d'une popularité remarquable auprès de la communauté russophone du pays. Selon ses propres estimations, son électorat compte jusqu'à un tiers de russophones. Les dirigeants du parti se sont rendus en Russie et y ont rencontré des représentants du parti de M. Poutine, Russie unie, et d'autres responsables du Kremlin. Le succès électoral de l'AfD s'explique en partie par la montée de l'hostilité vis-à-vis des immigrés dans la société allemande. Il est notoire que des trolls et des bots pro-Kremlin ont fait en sorte d'intensifier le phénomène. Il faut évoquer à cet égard l'affaire Lisa, où des médias russes avaient affirmé mensongèrement qu'une adolescente russo-allemande avait été violée par des immigrés (Shuster, 2017).

20. La **Grèce**, elle aussi, accuse la Russie de corruption et d'ingérence dans ses affaires intérieures. En juillet 2018, quatre diplomates russes ont été expulsés du pays après qu'il a été prouvé que Moscou essayait de saborder « l'accord sur le nom » entre Athènes et Skopje, accord susceptible d'ouvrir les portes de l'OTAN à l'ex-République yougoslave de Macédoine[10]. Les informations recueillies ont révélé que des agents russes (officiels et simples citoyens) ont tenté de soudoyer de hauts responsables des services de renseignement et des forces armées grecs et de financer des groupes d'extrême droite. Cette situation reflète l'apparente volonté de la Russie d'influer sur la politique dans les Balkans occidentaux et d'entraver la concrétisation des aspirations de l'Union européenne et de l'OTAN dans la région. Des spécialistes tirent la sonnette d'alarme et prédisent pour 2018 le lancement d'une nouvelle campagne russe dans les Balkans (Galeotti, 2018).

21. L'une des principales conclusions du rapport de l'agence pour la sécurité de l'État de **Lituanie** en 2018 est que les services de renseignement et de sécurité russes sont particulièrement intéressés par la prochaine élection présidentielle dans le pays, qui doit avoir lieu en 2019.

22. La Russie mène une politique spécifiquement destinée à atteindre et à aider les communautés russophones de l'étranger et, plus spécialement, celles qui sont installées dans les anciennes

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

républiques soviétiques. Moscou estime à quelque 17 millions le nombre de ces « **compatriotes** » vivant dans son voisinage. Les trois principaux instruments mis en place pour les assister sont l'agence gouvernementale *Rossotroudnitchestvo* (Agence fédérale pour la CEI, la diaspora russe et la coopération humanitaire), dotée d'un budget de 95,5 millions de dollars financé sur les fonds publics, la Fondation *Rousskii Mir*, dotée d'un budget de 15 millions de dollars, et la Fondation *Gortchakov* pour le soutien de la diplomatie publique, dotée d'un budget de 2 millions de dollars (Kuhrt et Feklyunina, 2017). Si les objectifs officiels de ces trois entités semblent légitimes (promotion de la culture, de la langue et de la vision du monde de la Russie), leurs activités peuvent avoir des aspects politiques, par exemple en incitant ces communautés à faire pression sur les gouvernements des pays où elles vivent pour obtenir la levée des sanctions contre Moscou.

23. Il est difficile d'évaluer et de prouver telle ingérence politique tout autant que d'en mesurer les conséquences réelles. Qu'il s'agisse de financement par une banque russe ou de cyberattaques par des groupes dont on remonte la trace jusqu'en Russie, il est souvent malaisé d'établir l'existence d'un lien clair et direct entre ces actes et le Kremlin.

24. Dans la plupart des cas, l'immixtion de la Russie ne provoque pas l'apparition de nouveaux clivages sociétaux ou tendances négatives : elle vise simplement à les renforcer. La montée des forces politiques opposées au système est une vieille tendance. Cependant, l'attitude pro-russe affichée par l'extrême droite occidentale – dont des exemples sont donnés aux paragraphes 16 et 19 du présent rapport – est un phénomène récent qui coïncide avec l'intérêt que leur porte maintenant le Kremlin et avec l'aide qu'il leur accorde (Polyakova, 2016). Il pourrait être contre-productif, en fait, d'exagérer l'impact des ingérences russes, car cela reviendrait à donner au Kremlin plus d'importance qu'il n'en a vraiment. Toutefois, il ne s'agirait pas non plus de minimiser cet impact et il est urgent de prendre des mesures pour protéger les systèmes politiques du monde libre.

C. OPÉRATIONS CINÉTIQUES

25. La guerre hybride ne se compose pas uniquement d'opérations non cinétiques. Les spécialistes font observer que, dans le contexte de ses tactiques hybrides, la Russie a recouru « aux activités les plus diverses, allant de l'incitation à la violence, de l'enlèvement et de la tentative d'assassinat à l'infiltration et aux menées clandestines conjuguées à des opérations militaires » (Kramer et Speranza, 2017). L'exemple paradigmatique d'une opération cinétique est le déploiement de soldats professionnels sans insignes distinctifs – il s'agissait probablement de membres des forces spéciales russes – lors de l'occupation de la Crimée et du Donbass. Ces soldats ont été désignés depuis lors sous les appellations d'« hommes gentils » ou d'« hommes en vert ». Si aucun doute n'a jamais plané sur l'origine de ces troupes, l'absence d'insignes a permis, du moins formellement et temporairement, à M. Poutine de les dissocier de l'État russe et d'atténuer les réactions internationales. Les preuves de la présence militaire russe dans le Donbass abondent mais, faute d'identification formelle de ces forces, la Russie continue à se dire étrangère au conflit.

26. Le degré de « dénégation plausible » varie en fonction des circonstances. Si l'occupation de la Crimée consistait en une opération mal déguisée des forces spéciales russes, la revendication de la « rébellion » du Donbass par des forces locales a permis significativement à M. Poutine de minimiser l'implication de la Russie en la réduisant à la simple participation de quelques « volontaires en congé temporaire » des forces armées russes. En Syrie, le maintien en place de troupes russes après l'annonce officielle de leur retrait est entouré d'un flou encore plus grand et repose sur la présence du groupe Wagner, une société paramilitaire privée qui a également opéré en Ukraine au début de l'année 2014 et qui, selon les médias et les services de renseignement états-uniens, est associée à M. Prigojine. Depuis septembre 2015, le groupe Wagner joue un rôle majeur dans la reconquête du territoire syrien par les autorités de Bagdad et agit au côté des forces armées russes en tant qu'élément non déclaré de celles-ci (Hauer, 2018). Un affrontement entre ces mercenaires russes bien entraînés et les forces états-uniennes a fait une centaine de morts dans les rangs du groupe. Un affrontement aussi direct entre militaires russes et états-uniens n'a pas de

précédent dans l'histoire moderne et aurait pu provoquer une dangereuse montée des tensions. Toutefois, M. Poutine a pu nier l'existence de tout rapport entre son pays et ces mercenaires.

27. La présence de sociétés militaires privées russes a également été signalée dans plusieurs pays africains et arabes, dont la République centrafricaine[11], le Soudan et la Libye. Des sociétés telles que le groupe Wagner permettent aux autorités russes « de pénétrer dans un environnement (...) étranger à moindre risque et d'exploiter les possibilités politiques et économiques qu'elles y trouvent ». Les dirigeants du Kremlin se voient ainsi en mesure de nier plausiblement leur implication (Hauer, 2018).

28. Une tendance particulièrement inquiétante est la volonté apparente des autorités russes de prendre pour cibles à l'étranger ceux qu'elles considèrent comme leurs ennemis, y compris au moyen d'armes de destruction massive. L'attaque chimique qui a visé M. Skripal et sa fille à Salisbury en mars 2018 a causé des dommages collatéraux : une citoyenne britannique a perdu la vie et son mari a dû être hospitalisé. L'enquête a permis d'identifier deux suspects principaux – des ressortissants russes arrivés au Royaume-Uni sous les noms d'Alexandre Petrov et de Rouslan Bochirov – et de les rattacher aux services de renseignement militaire russes (GRU). Des enquêtes indépendantes, dont celle du célèbre site Bellingcat, vont dans ce sens. Les Russes ont affirmé que ces deux personnes s'étaient rendues de Moscou à Londres pour un séjour de deux ou trois jours dans le but de visiter la cathédrale de Salisbury. Ils ont commodément omis d'évoquer la présence de traces d'un agent innervant, le Novitchok, dans la chambre de leur hôtel londonien. De récents compléments d'enquête ont permis d'identifier l'un des deux voyageurs comme étant Anatoli Tchepiga, un colonel du GRU décoré de multiples fois.

29. Parmi les autres cas d'utilisation d'une force de faible intensité, citons les violations répétées de l'espace aérien de l'OTAN[12], la participation supposée à une tentative de coup d'État anti-OTAN au Monténégro en octobre 2016 et diverses actions ciblées telles que l'enlèvement d'un officier estonien en septembre 2014.

30. Par ailleurs, la Russie participe à des exercices périodiques de grande envergure comme les *Zapad* et les *Kavkaz*, conçus pour démontrer ses capacités offensives en Europe de l'Est à des fins d'intimidation ou, comme cela a été le cas en 2008 et en 2014, pour dissimuler les invasions de la Géorgie et de l'Ukraine. Lorsqu'elle organise ces exercices, elle déroge régulièrement aux obligations que lui impose le Document de Vienne, s'agissant de la communication d'informations à ce propos et de la notification desdits exercices aux autres États membres. En général, la taille de ces exercices excède de beaucoup celle officiellement déclarée par Moscou. Par exemple, de 60 000 à 70 000 soldats auraient pris part à *Zapad 2017*, contre les 12 700 annoncés officiellement.

---

11 Trois journalistes indépendants russes ont été tués en République centrafricaine alors qu'ils enquêtaient sur les activités du groupe Wagner dans ce pays.

12 L'une de ces violations les plus récentes s'était produite le 12 mars 2018 au-dessus de l'île estonienne de Vaindloo. Selon les autorités militaires de l'OTAN, le comportement des pilotes russes lors de ces violations était plus empreint d'un manque de professionnalisme que de véritable hostilité. Cependant, ce type de comportement peut déboucher sur des incidents graves, tel celui du chasseur russe abattu au-dessus de la Turquie en 2017. Une étude de l'*European Leadership Network* portant sur 39 « rencontres » entre des forces aériennes ou navales russes et alliées indiquait dans ses conclusions que des violations « très préoccupantes » d'espaces aériens nationaux avaient débouché sur plusieurs incidents à l'occasion desquels le déclenchement d'un conflit ouvert ou des pertes en vies humaines avaient été évités de justesse.

D. DÉSINFORMATION ET PROPAGANDE

31. Le rapport de la CDS *La bataille des cœurs et des esprits : répondre aux campagnes de propagande à l'encontre de la communauté euro-atlantique* [164 CDSDG 15 F] publié en 2015 ainsi que celui de 2017 sur *La révolution des médias sociaux : incidences politiques et sécuritaires* [158 CDSDG 17 F bis] analysent dans le détail la machine de désinformation et de propagande russe. Ils montrent que les grands médias traditionnels russes ne sont pas seulement partiaux : ils ont été transformés en armes et sont devenus l'un des instruments de la politique étrangère du Kremlin. Margarita Simonian, la rédactrice en chef de la chaîne RT (qui, avec *Sputnik*, est le vaisseau amiral des services multimédias en langue étrangère dont se sert Moscou pour influencer l'opinion publique internationale), affirme que la Russie a besoin de sa chaîne « pour pratiquement la même raison qu'elle a besoin d'un ministère de la défense » et que RT est capable de « mener une guerre de l'information contre le monde occidental tout entier » en utilisant « l'arme informationnelle » (EUvsDisinfo, janvier 2018).

32. Les médias russes contrôlés par l'État ne répondent pas aux exigences journalistiques élémentaires : ils ne sont pas indépendants et reçoivent des instructions hebdomadaires du Kremlin (EUvsDisinfo, septembre 2017). Plus grave encore, ils n'ont ni scrupules ni éthique et sont capables de falsifier la réalité de manière éhontée ou de publier des mensonges purs et simples. De nombreux exemples de ce « journalisme » en mal d'éthique ont été exposés dans les rapports cités plus haut. Emmanuel Macron a exclu les représentants de RT et de *Sputnik* du groupe de journalistes accrédités auprès de l'Élysée au motif qu'il ne s'agissait pas de journalistes, mais d'agents d'influence.

33. En 2017, la Russie a poursuivi sa vaste campagne de désinformation. Dans leur analyse annuelle, les spécialistes de l'Union européenne en contre-propagande ont mentionné quelques-unes des affirmations les plus spectaculaires des caisses de résonance du Kremlin, telles que l'imminence d'une guerre civile en Suède, le lâcher d'une bombe nucléaire sur la Lituanie par un appareil états-unien, ou encore, une augmentation de 1 000 % du nombre de viols en Suède (en fait, ce nombre a progressé de 1,4 % depuis 2015). L'Ukraine demeure la cible d'une grande partie de ces fausses nouvelles : les Ukrainiens sont souvent décrits comme des fascistes et des oppresseurs, tandis que l'Ukraine est dépeinte comme un pays artificiel et un État failli (EUvsDisinfo, décembre 2017).

34. Tout en exploitant le paysage médiatique occidental, libre et diversifié, les médias russes appartenant à l'État tiennent un discours uniforme. À la différence de ce qui se passait du temps de l'URSS, le discours repose sur une base idéologique moins solide et s'adresse à des personnes venues d'horizons les plus divers en relayant des idées antioccidentales, antilibérales et antimondialistes. L'antiaméricanisme est un élément majeur du discours et vise à enfoncer un coin entre les États-Unis et l'Europe. Le discours porte pratiquement sur tous les concepts marginaux qui vont à l'encontre du courant de pensée occidental traditionnel. Exemple d'une initiative dans ce domaine : le lancement d'un nouveau média – *USA Really. Wake Up Americans* – par une usine à trolls russe, l'Agence d'investigation de l'internet. Cette agence est accusée d'ingérence dans l'élection présidentielle américaine de 2016 et est liée, selon les conclusions de nombreuses enquêtes journalistiques, à Evgueni Prigojine (EUvsDisinfo, avril 2018). Créée pour « lutter contre la censure politique de plus en plus étouffante pratiquée par les États-Unis », elle vise avant tout une audience hostile aux corps constitués. Active dans les réseaux sociaux, elle se répand essentiellement en opinions antiaméricaines et se concentre sur des questions sociales et politiques controversées.

35. Comme cela a déjà été indiqué, de nouvelles avancées dans les technologies de l'information et de la communication, y compris l'expansion des réseaux sociaux, ont permis à Moscou de faire passer ses activités de désinformation et de propagande à la vitesse supérieure. De nombreux rapports montrent comment des trolls et des bots pro-Kremlin répandent des infox et des nouvelles susceptibles d'engendrer des divisions sociales au sein des sociétés occidentales. Le centre

d'excellence de l'OTAN pour la communication stratégique précise que deux tiers des usagers de Twitter qui écrivent en russe à propos de la présence de l'OTAN en Europe de l'Est sont des comptes bots. Les chaînes en ligne sont utilisées de manière différente, par exemple pour semer la panique dans l'État de la Louisiane en faisant croire à une fuite de produits chimiques grâce à une vague de tweets, ou encore, pour affecter les employés des usines à trolls russes à la création de faux sites internet (Chen, 2015). Les Russes imitent aussi les sites officiels d'institutions occidentales ; ils ont ainsi reproduit le site du centre d'excellence européen pour la lutte contre les menaces hybrides (*Hybrid CoE Helsinki*) en y instillant une dimension pro-russe. L'adresse internet du centre – https://www.hybridcoe.fi/ – a été remplacée par http://hybridcoe.ru/, ce qui donne un aspect professionnel et légitime au site russe, lequel diffuse des considérations défavorables à l'OTAN et à l'Union européenne.

36. Il convient de noter que la « machine à désinformer » du Kremlin pourrait se doter à l'avenir d'outils encore plus efficaces. La conception d'algorithmes d'intelligence artificielle appelés « réseaux adversaires génératifs » (GAN) offre la possibilité de pirater aisément des bandes sonores et vidéos et de créer des images qui, par exemple, pourraient décrire de manière convaincante un dirigeant occidental tenir des propos pro-russes ou faire des déclarations destinées à semer la panique et la confusion dans les populations occidentales (*The Economist*, 2017).

E. CYBERGUERRE ET GUERRE ÉLECTRONIQUE

37. La Russie emploie des cyberarmes pour mener des opérations hybrides telles que de l'ingérence électorale, de l'espionnage ou des campagnes de désinformation. Cependant, une cyberattaque peut en soi constituer un type de guerre hybride à part entière. En 2017, des cyberattaques de grande ampleur ont été lancées contre des infrastructures d'importance critique ; elles ont eu de graves conséquences dans le monde réel. L'attaque mettant en œuvre le logiciel d'extorsion WannaCry[13], imputée à la Corée du Nord, a mis à mal les services de santé du Royaume-Uni et d'autres pays de l'Alliance ; celle qui a utilisé un autre logiciel d'extorsion, NotPetya, et qui a été attribuée à des pirates russes par le Royaume-Uni et d'autres pays alliés, visait le système fiscal ukrainien, mais elle s'est étendue à des entreprises de tout le pays et au-delà. Les pertes subies par ces entreprises sont de l'ordre de plusieurs centaines de millions de dollars. En novembre 2017, le chef du centre national de cybersécurité (NCSC) du Royaume-Uni, Ciaran Martin, a signalé que des pirates russes avaient pris pour cibles les secteurs britanniques de l'énergie, des télécommunications et des médias. La Russie est également accusée d'attaques commises contre le *Bundestag* et le ministère allemand des affaires étrangères, respectivement en 2015 et en 2017, ainsi que du sabotage d'un réseau de télévision français (TV5 Monde) en 2016. Cette année, le BSI (Office fédéral de la sécurité des technologies de l'information) a accusé le gouvernement russe d'avoir lancé une cyberattaque de grande envergure contre des fournisseurs d'énergie allemands. Á l'approche des élections de mi-mandat aux États-Unis, Microsoft a révélé qu'il avait saisi de faux sites internet créés par des pirates en cheville avec le GRU. Ces sites reproduisaient ceux du *Hudson Institute* et de l'*International Republican Institute* et renvoyaient les visiteurs sur des pages internet destinées à subtiliser mots de passe et autres données d'identification (Sanger et Frenkel, 2018).

38. Une affaire intéressante – en ce qu'elle démontre l'existence de liens entre des pirates informatiques russes, des agents russes spécialisés dans la « manière douce » et le Kremlin – est celle de la controverse suscitée par l'éventualité d'une scission entre l'Église orthodoxe d'Ukraine et le Patriarcat de Moscou. En Russie, autorités religieuses et responsables gouvernementaux ont travaillé main dans la main pour empêcher une telle scission, qui aurait certainement pour effet d'amoindrir l'influence de la Russie en Ukraine. Alors que la scission avait été provisoirement approuvée par le patriarche œcuménique Bartholomée I[er] de Constantinople[14], on a appris que des

[13] Les pirates qui utilisent des logiciels d'extorsion bloquent les ordinateurs de leurs victimes ou menacent d'en publier le contenu et exigent le paiement d'une rançon.

[14] Considéré comme *primus inter pares* au sein de l'Église chrétienne orthodoxe

pirates russes avaient pris pour cibles de hauts dignitaires de l'Église chrétienne orthodoxe, y compris les principaux assistants de Bartholomée I[er]. Il s'agirait de Fancy Bear, un groupe déjà impliqué dans le piratage de la messagerie électronique du comité national démocrate des États-Unis en 2016 (Satter, 2018).

39. Le Kremlin est aussi soupçonné de lancer des attaques de guerre électronique. Le général Ben Hodges, ancien commandant de l'armée des États-Unis en Europe (*United States Army Europe)*, a fait observer que, ces trois dernières années, la Russie avait mis au point des « capacités de guerre électronique significatives ». À la veille de l'exercice *Zapad 2017*, le réseau de télécommunications mobile de la Lettonie orientale a été brouillé par, semble-t-il, un brouilleur situé à Kaliningrad et visant la Suède. Un responsable de l'OTAN a affirmé que l'incident démontrait l'aptitude de la Russie à intercepter ou brouiller des réseaux civils « dans un rayon non négligeable et avec une relative aisance » (Gelzis et Emmott, 2017). En Norvège, la radio du service public a révélé que, pendant *Zapad 2017*, des appareils civils survolant le Finnmark oriental avaient signalé la perte de leur signal GPS. Les mesures relevées ont montré que les perturbations venaient de l'Est. Un rapport du centre international pour la défense et la sécurité (ICDS) estime que l'élaboration de nouveaux moyens de guerre électronique par la Russie engendrerait un grave problème sur le flanc Est de l'OTAN. Le Kremlin recourt en outre à des techniques de surveillance très avancées, tels que des drones ou des antennes camouflées, pour extraire des renseignements des smartphones qu'utilisent les troupes de l'OTAN dans les pays baltes et en Pologne (Grove, Barnes et Hinshaw, 2017).

40. Si le problème de l'attribution dans le cyberespace se pose avec beaucoup d'acuité, la trace de la plupart des cyberattaques de cette ampleur a pu être remontée jusqu'en Russie : il s'agit souvent de groupes de pirates baptisés *Cosy Bear*, également connu sous le sigle APT29, ou *Fancy Bear* (APT28)[15]. Le NCSC a accusé le Kremlin de recourir à des cyberattaques « pour saper le système international ». Selon un rapport datant de 2017 de la commission sur le renseignement et la sécurité de la Chambre des communes britannique, la multiplication de leurs cyberactivités montre que les autorités russes ne se soucient plus d'avancer masquées et qu'elles font montre d'une plus grande hardiesse.

F. AUTRES TYPES DE MENACES HYBRIDES

41. La plupart des pays pratiquent l'une ou l'autre forme d'**espionnage** ou de collecte de renseignements, mais les activités des espions russes paraissent disproportionnées par rapport à l'importance de la Russie sur la scène mondiale. Des experts états-uniens du renseignement signalent que la confrontation entre la communauté du renseignement des États-Unis et les services spéciaux russes s'intensifie au point qu'elle menace de déstabiliser les relations bilatérales et, au-delà, l'ordre mondial (Beebe, 2017). L'administration états-unienne affirme que le nombre d'espions russes présents aux États-Unis a considérablement augmenté ces 15 dernières années (Schmidle, 2017). Elle soupçonne aussi l'entreprise *Kaspersky Lab*, sise à Moscou, d'utiliser l'antivirus qui a fait sa renommée pour espionner les États-Unis et entraver les activités états-uniennes de collecte de renseignements. Autre exemple de l'espionnage russe aux États-Unis : l'affaire Maria Boutina, une ressortissante russe accusée « d'infiltrer la *National Rifle Association* (NRA) et d'influencer la politique états-unienne » (Swaine, 2018). L'enquête a mis au jour les liens qu'entretenait M[me] Boutina avec des banques soutenues par le Kremlin et des oligarques russes visés par des sanctions états-uniennes.

42. De son côté, le service de renseignement britannique MI6 a déplacé la Russie dans la catégorie des « menaces de classe 1 », sur le même plan que le terrorisme islamiste. Cette information est à mettre en parallèle avec l'absence de toute mention de la Russie dans l'examen stratégique annuel de la défense et de la sécurité publié en 2010 par le conseil de sécurité nationale

[15] Selon la société de cybersécurité *CrowdStrike*, *Cozy Bear* et *Fancy Bear* sont en cheville avec, respectivement, le FSB et la direction générale des renseignements (GRU).

du Royaume-Uni. Selon les spécialistes britanniques, la Russie emploie entre 705 000 et 940 000 personnes dans ses services de sécurité. Par comparaison, le Royaume-Uni en emploie quelque 16 500. Des responsables estiment par ailleurs que les budgets des services de sécurité et de renseignement russes augmentent de 15 à 20 % chaque année et qu'ils servent essentiellement au financement d'opérations (Edwards, 2017). Des pays voisins de la Russie et non membres de l'OTAN signalent que les activités d'espionnage se sont multipliées depuis l'annexion de la Crimée (Ringstrom, 2015).

43. Des experts de la Russie comme M. Galeotti, qui s'est adressé à la présente commission lors de la session de Bucarest de 2017, constatent l'existence de liens entre le Kremlin et des **associations de malfaiteurs** d'origine russe opérant en Europe. Ces mêmes spécialistes disent détenir la preuve que les autorités russes font appel à ces associations pour se procurer de l'« argent sale » et qu'elles recrutent en leur sein des meneurs de cyberattaques, des trafiquants et des criminels spécialisés dans la traite des êtres humains, voire des tueurs à gages, en leur ouvrant l'accès aux réseaux du renseignement russe. Il a été signalé que des gangs locaux auraient pris part à l'invasion de la Crimée et du Donbass (Galeotti, 2017). En mai 2018, un rapport de la commission des affaires étrangères du Parlement britannique intitulé *Moscow's Gold : Russian Corruption in the U.K.* (L'or de Moscou : la corruption russe au Royaume-Uni) révélait que Londres « abritait les moyens de corruption » utilisés par des personnes liées au Kremlin, que ces activités financières « s'inscriv[aient] manifestement dans un plan de plus grande ampleur » et qu'elles menaçaient la sécurité du Royaume-Uni. Les auteurs du rapport demandaient « l'application vis-à-vis de Moscou d'une stratégie préventive cohérente combinant de manière visible les instruments diplomatiques, militaires et financiers dont le Royaume-Uni peut user pour contrer l'agression d'État commise par la Russie ». Au nombre des mesures concrètes proposées figure la création d'un registre de propriété destiné aux compagnies étrangères qui souhaitent acquérir des biens au Royaume-Uni, l'objectif étant de débusquer « ceux qui achètent des biens au Royaume-Uni par l'intermédiaire de sociétés-écrans extraterritoriales en dissimulant leur identité et leurs sources de financement potentiellement alimentées par la corruption » (*UK House of Commons*, 2018a).

44. La Russie se sert depuis longtemps de ses **ressources énergétiques** comme d'un instrument de politique étrangère[16]. Il convient de souligner que la vulnérabilité énergétique de l'Europe a fortement diminué, ce qui s'explique par 1) la diversification des approvisionnements grâce à des infrastructures supplémentaires telles que les nouveaux terminaux de gaz naturel liquéfié construits en Pologne et en Lituanie, 2) le développement de l'exploitation des réserves de pétrole bitumineux et de gaz aux États-Unis, 3) les mesures prises par l'Union européenne dans le sens de la création d'un marché énergétique intégré au moyen du 3e « paquet énergie », qui oblige *Gazprom* à vendre ses parts dans les réseaux de transmission européens, et 4) la « révolution verte » dans le secteur de l'énergie et, notamment, les avancées enregistrées dans les domaines des énergies renouvelables et de l'efficacité énergétique (la stratégie de sécurité économique de la Russie qualifie l'essor des technologies vertes de menace pour la sécurité économique du pays, précisément).

45. Toutefois, la Russie conserve une influence considérable sur le marché énergétique européen. Ses livraisons de gaz à l'Europe vont en augmentant et près de 40 % des importations européennes de gaz proviennent de Russie. L'Union européenne discute actuellement d'un projet controversé : la construction d'un nouvel oléoduc, le *Nord Stream 2*, qui relierait l'Allemagne et la Russie en contournant des pays comme l'Ukraine ou la Pologne. Les adversaires du projet font valoir que celui-ci porte atteinte à la solidarité énergétique à laquelle aspire l'initiative de l'Union européenne de l'énergie. Les pays baltes ont pris de fortes mesures pour réduire leur dépendance énergétique, mais leurs marchés de l'électricité restent synchronisés avec le Réseau électrique interconnecté (BRELL), qui est contrôlé par Moscou, et ils redoutent que les Russes ne sabotent leurs plans de désynchronisation. La Lituanie est, elle aussi, préoccupée par les activités de RosAtom, qui a entrepris la construction dissimulée d'une centrale nucléaire au Bélarus, à 50 km de Vilnius. Dans

16 Cette question fait l'objet d'une analyse détaillée dans le rapport 2018 de la commission de l'économie et de la sécurité *Le défi de la sécurité énergétique en Europe centrale et orientale* [175 ESCTD 18 F].

l'ensemble, le secteur énergétique européen doit améliorer sa cybersécurité pour être plus résistant aux menées d'agents hostiles étrangers (Grigas, 2017).

46. Selon les informations contenues dans un récent rapport de l'*Asan Institute for Policy Studies*, la Russie a fait du **contournement des sanctions** un instrument de politique étrangère. Plus précisément, les auteurs du rapport pensent que, faisant fi des sanctions de l'ONU contre la Corée du Nord, Moscou a fourni 622 878 tonnes non déclarées de pétrole raffiné à ce pays entre 2015 et 2017; ce volume correspond à environ un tiers du total des importations nord-coréennes de pétrole raffiné pendant la même période (Asan, 2018).

47. Certains spécialistes de la question, dont Sir Stuart Peach, général de l'armée de l'air et chef d'état-major des forces armées britanniques, le député britannique Rishi Sunak et l'amiral James Stavridis, ancien commandant suprême des forces alliées en Europe, pensent que la marine russe pourrait représenter une menace pour les **câbles sous-marins** qui acheminent 97 % des télécommunications mondiales et permettent 10 billions de dollars de transferts financiers par jour. Rien ne peut remplacer ces câbles. Les économies et les sociétés modernes dépendent de manière vitale de ces infrastructures dépourvues des défenses les plus élémentaires (Murphy, Hoffman, et Schaub, 2016). L'activité des sous-marins russes dans la partie septentrionale de l'Atlantique s'est sensiblement accrue ces dernières années et lesdits sous-marins « évoluent de manière agressive » à proximité des câbles. La Russie procède à un renforcement non négligeable de ses capacités navales avec, entre autres, l'adjonction de navires de collecte de renseignements de classe *Yantar* et de sous-marins auxiliaires, deux types de bâtiment capables de détériorer les câbles. Sir Stuart Peach affirme que le Royaume-Uni et ses partenaires de l'OTAN sont mal préparés à l'éventualité d'une attaque de cette nature (BBC, décembre 2017). En juin 2018, les États-Unis ont décrété des sanctions visant des moyens sous-marins dont les autorités russes se servent pour exploiter les câbles de communication sous-marins des pays occidentaux.

48. D'une façon générale, les activités hybrides de la Russie constituent une menace pour l'environnement **maritime**. Les ports comme les navires marchands et militaires sont des cibles très exposées aux sabotages, au piratage des systèmes de navigation et aux cyberattaques (Kremidas-Courtney, 2018). Compte tenu de leur grande dépendance envers leurs cybercapacités, les navires peuvent être gravement endommagés par des cyberattaques.

III. FAIRE FACE AUX MENACES HYBRIDES

A. OTAN

49. Comme cela a été dit, les attaques hybrides posent un problème à l'Alliance en ce qu'elles ne sont généralement pas susceptibles de déclencher l'application des dispositions de l'article 5 du Traité de Washington. En ces temps de guerre hybride, il faut se rabattre sur l'article 3, qui évoque la collaboration et l'assistance mutuelle sans aller jusqu'à la défense collective, et sur l'article 4, qui oblige les Alliés à se consulter lorsque la sécurité de l'un d'eux est menacée. À son Sommet de Varsovie, en 2016, l'OTAN a adopté une stratégie relative à son rôle dans la lutte contre la guerre hybride. Ce document réaffirmait que la riposte aux menaces hybrides incombait d'abord et avant tout au pays pris pour cible. Cependant, l'OTAN est disposée à aider un Allié à n'importe quel stade d'une campagne hybride. Les dirigeants alliés ont par ailleurs annoncé que les pays membres de l'OTAN étaient prêts à lutter contre la guerre hybride dans le contexte de la défense collective et que le Conseil de l'Atlantique Nord pouvait décider d'invoquer l'article 5 du Traité de Washington[17]. L'action collective est fonction d'une évaluation unanime de la menace, évaluation que les tactiques hybrides de la Russie visent à empêcher.

[17] Toutes les décisions de l'OTAN sont le fruit d'un consensus après débats et consultations entre pays membres.

50. Dans le prolongement de l'agression russe contre l'Ukraine, l'OTAN a élaboré un plan d'action « réactivité » (RAP) afin de tripler la taille de la Force de réaction de l'OTAN (NRF) et de créer une Force opérationnelle interarmées à très haut niveau de préparation (VJTF) mobilisable en quelques jours pour des missions de dissuasion. Pour garantir l'efficacité de la VJTF, l'OTAN a également mis sur pied des unités d'intégration de ses forces (NFIU) en Europe centrale et orientale. Une mesure remarquée a été le déploiement de quatre bataillons dans les pays baltes et en Pologne, ce qui a eu pour effet d'augmenter considérablement le coût d'une éventuelle agression dirigée contre ces Alliés[18].

51. Pour être pleinement effectives, ces ripostes militaires doivent être complétées par des efforts visant à assurer la résilience nationale dans des domaines tels que la continuité de l'action gouvernementale et des services publics d'importance majeure, la préservation des réseaux informatiques, l'approvisionnement en énergie, en denrées alimentaires et en eau et enfin, l'aptitude à faire face à des mouvements de foule incontrôlés. En 2017, l'OTAN a mené à l'échelle de l'Alliance une évaluation de la résilience nationale, laquelle a donné lieu à un examen général de l'état de préparation du secteur civil. Cela a permis de repérer les domaines dans lesquels la résilience doit faire l'objet d'une amélioration.

52. L'OTAN a aussi amélioré la coopération entre Alliés dans le domaine du renseignement en se dotant d'une division civilo-militaire renseignement et sécurité (JISD). Compte tenu de la nécessité croissante d'une stratégie holistique, un service chargé de l'analyse hybride a été créé au sein de la JISD ; il est chargé d'analyser toute la gamme des tactiques hybrides en puisant dans des sources civiles et militaires, ouvertes ou classifiées. De nombreux aspects de la guerre hybride – lutte contre la désinformation, cybermenaces et sécurité énergétique – sont également traités par la division Diplomatie publique et la division Défis de sécurité émergents de l'OTAN. Celle-ci a en outre mis en place une plateforme de coopération avec l'Ukraine ; cette structure est spécifiquement destinée à réunir des spécialistes en menaces hybrides.

53. Plusieurs centres d'excellence homologués ou appuyés par l'OTAN – dont le centre d'excellence de l'OTAN pour la communication stratégique (Riga), le centre d'excellence de cyberdéfense coopérative de l'OTAN (Tallinn), le centre d'excellence de l'OTAN pour la sécurité énergétique (Vilnius) et le centre d'excellence pour la lutte contre les menaces hybrides (Helsinki)[19] – analysent les menaces et formulent des recommandations pratiques.

54. Depuis la cyberattaque massive menée en 2007 contre l'Estonie par des pirates russes, l'OTAN a progressé à pas de géant dans le développement de ses capacités de cyberdéfense. La déclaration publiée au sommet de Varsovie de 2016 désignait le cyberespace comme le cinquième « domaine d'opérations dans lequel l'OTAN [devait] se défendre ». En février 2017, les Alliés ont souscrit à un plan d'action qui plaçait la cyberdéfense au cœur de la défense collective de l'OTAN et qui promouvait la coopération entre cette dernière et l'industrie. Chaque année depuis 10 ans, l'OTAN organise un cyberexercice d'une semaine pendant lequel les pays membres et partenaires réagissent à des cyberattaques simulées reflétant des menaces réelles. Grâce à l'engagement en faveur de la cyberdéfense, les pays de l'Alliance ont accepté de donner la priorité à l'amélioration de la défense de leurs réseaux nationaux, défense d'une importance critique, compte tenu du fait que la cybersécurité de l'Alliance est fonction des capacités de son membre le plus faible. Pour sa part, l'OTAN a consolidé la défense de ses propres réseaux[20].

---

18 Pour plus de détails sur la présence avancée rehaussée (EFP) de l'OTAN, voir le rapport général 2018 de la commission de la défense et de la sécurité *Renforcer la dissuasion de l'OTAN à l'Est* [168 DSC 18 F fin].

19 Le centre d'excellence pour la lutte contre les menaces hybrides d'Helsinki est un projet conjoint de l'OTAN, de l'Union européenne et de plusieurs pays membres des deux entités ; son inauguration remonte à octobre 2017.

20 En 2016, l'OTAN a dû parer à quelque 500 cyberattaques par mois.

55. De même, l'OTAN coopère de plus en plus avec l'Union européenne dans le domaine de la cyberdéfense : les deux entités ont intensifié leurs échanges d'informations et participent à des exercices communs. Elles ont également décidé de coopérer dans les secteurs de la réaction aux incidents et de la gestion des crises.

B. UNION EUROPÉENNE

56. Ses ressources considérables et sa puissance douce font de l'Union européenne un protagoniste du processus visant à rendre l'Europe résistante aux menaces hybrides et, singulièrement, à la désinformation et aux cyberattaques. La déclaration commune OTAN-UE de 2016 contient une liste de plus de 40 secteurs spécifiques de coopération, dont pas moins de 10 concernent le renforcement de la collaboration dans la lutte contre les menaces hybrides. Cependant, la coopération entre les deux institutions se limite à leurs secrétariats internationaux et ne fait pas intervenir les pays membres.

57. En avril 2016, la Commission européenne et la haute représentante de l'Union européenne pour les affaires étrangères et la politique de sécurité ont adopté un cadre commun en matière de lutte contre les menaces hybrides. Ce cadre définit les mesures que prend l'Union en faveur de ses États membres pour les rendre résistants aux menaces hybrides, tout en reconnaissant que la lutte contre ce genre de menaces incombe avant tout aux États membres eux-mêmes. Pour améliorer la compréhension de la situation par le partage des analyses des renseignements, l'Union a créé une cellule de fusion contre les menaces hybrides.

58. Soucieuse de riposter aux campagnes de désinformation russes, l'Union a également mis sur pied un groupe de travail sur la communication stratégique de l'Est dont les membres sont aussi connus sous le nom de « briseurs de mythes ». Une équipe d'une douzaine de diplomates dénoncent quotidiennement les manœuvres de désinformation en ligne auxquelles se livre la Russie. Après des demandes répétées de la part du Parlement européen, le groupe a finalement été doté d'un budget distinct dépassant à peine un million d'euros par an. Le rapporteur est convaincu que ce montant reste insuffisant au vu de l'ampleur du problème et des vastes capacités financières de l'Union.

59. Si la coopération structurée permanente (PESCO) pour la défense récemment mise en place par l'Union se concentre sur les investissements dans la sécurité dure, l'un de ses 17 projets de collaboration – dirigé par la Lituanie et rassemblant neuf États membres – a débouché sur la création d'un système d'équipes d'intervention rapide en cas de cyberincident, système fonctionnant par roulement. En 2017, l'Union a créé une équipe d'intervention en cas d'urgence informatique (CERT-EU) couvrant l'ensemble de ses institutions, organes et agences. Elle a consacré 50 millions d'euros à l'élaboration d'un réseau de compétences en cybersécurité, réseau qui réunit des entités des secteurs public et privé (centres de recherche, programmes universitaires et partenaires du monde de l'industrie), l'objectif étant de s'atteler aux problèmes de cybersécurité et de renforcer les capacités de chaque État membre de la meilleure façon qui soit.

C. NIVEAU NATIONAL

60. En réponse aux activités hybrides de la Russie, de nombreux pays membres de l'OTAN et de l'Union européenne ainsi que des candidats à l'adhésion ont revu leur politique de sécurité nationale. Il est certes impossible de présenter ici une analyse exhaustive des travaux effectués dans ce contexte, mais le rapporteur aimerait s'attarder sur plusieurs initiatives nationales importantes.

61. En ce qui concerne l'**ingérence politique**, les États-Unis ont confié à Robert Mueller, procureur spécial et ancien directeur du FBI, une enquête sur l'immixtion de Moscou dans l'élection présidentielle de 2016 ; à la suite de cette enquête, 32 ressortissants russes et trois entités russes ont été inculpés. Le ministère de la justice a également mis en accusation 12 agents du GRU pour

le piratage de la messagerie électronique de représentants du parti démocrate au moyen de messages de harponnage et de logiciels malveillants. Ces agents ont également été inculpés de divulgation de documents d'importance névralgique et de vol des données personnelles d'un demi-million d'électeurs. C'était la première fois que les États-Unis accusaient officiellement les autorités russes d'avoir voulu peser sur le résultat de l'élection présidentielle de 2016. Moscou nie toute implication et dénonce une « conspiration ».

62. Au vu de l'accumulation de preuves selon lesquelles la Russie s'efforce d'interférer cette année avec les élections de mi-mandat aux États-Unis – y compris par des actes de piratage contre des sénateurs et par la création de faux « sites officiels » sur internet –, un groupe de sénateurs républicains et démocrates ont déposé un projet de loi visant à infliger de nouvelles sanctions à la Russie pour ingérence dans le processus électoral. Ces sanctions porteraient essentiellement sur la dette souveraine de la Russie, ses projets énergétiques et ses oligarques corrompus.

63. Alertés par les événements aux États-Unis et informés par les services de renseignement états-uniens, les milieux politiques français ont pu se préparer à des interférences avec la campagne présidentielle. L'équipe de M. Macron a engagé des cyberspécialistes qui ont suggéré la création de « comptes-leurres » de messagerie électronique et préparé une stratégie de communication en prévision de fuites éventuelles.

64. Les services de sécurité allemands sont parvenus à minimiser les ingérences étrangères dans les élections de 2017 en recherchant et en éliminant les points faibles des réseaux. De façon inhabituelle, le chef des services chargés du renseignement intérieur s'est adressé à la population pour la mettre en garde contre les campagnes de désinformation et les cyberattaques en provenance de Russie (EUvsDisinfo, 2016). Pour leur part, les autorités britanniques ont contribué à la protection du système politique en remontant la piste des principaux auteurs de cyberattaques, en fournissant aux membres de la classe politique les services de professionnels spécialisés dans la sécurité des communications et en collaborant avec des médias et des groupes de réflexion pour la mise au point d'un discours franc, susceptible de contrer la propagande. Abordant la dernière ligne droite des élections législatives, prévues pour septembre 2018, la Suède a donné au personnel affecté aux opérations électorales une formation leur permettant de repérer les manipulations venues de l'étranger et d'y résister, tandis que les partis politiques ont amélioré la sécurité de leurs messageries électroniques. Le premier ministre a annoncé la création d'une agence responsable de promouvoir la « défense psychologique » de la population en « repérant les campagnes extérieures visant à influencer cette dernière, en les analysant et en y ripostant » (Rettman, 2018).

65. Comme indiqué auparavant, les pays de l'Alliance qui se trouvent sur la ligne de front sont particulièrement préoccupés par les **menaces cinétiques**, telles que les opérations de groupes armés dépourvus d'insignes militaires distinctifs. Indépendamment du soutien qu'ils attendent de l'OTAN, ces pays ont une vision de la défense qui englobe la société tout entière. Ainsi, la Lituanie a réinstauré le service militaire et publié un manuel de 75 pages intitulé *Guide de résistance active,* disponible dans les écoles et les bibliothèques. Ce manuel contient des conseils de désobéissance civile en cas d'invasion. De la même manière, une nouvelle stratégie a été rédigée à l'usage des forces terrestres états-uniennes pour la période 2025-2040 ; elle s'attarde sur les ennemis qui ne se déclarent pas en tant que combattants dans un contexte où la ligne de démarcation entre guerre et paix n'apparaît plus distinctement. On s'attend à ce que, pour faire face à de tels ennemis, les forces terrestres privilégient des formations plus petites, « semi-autonomes » et dotées d'une polyvalence beaucoup plus grande qui seraient capables d'opérer simultanément dans tous les types de guerre (Tucker, 2017).

66. Pour ce qui est de la **désinformation**, l'Allemagne a arrêté de strictes mesures visant à limiter la propagation de discours haineux et d'infox sur les réseaux sociaux et inflige de lourdes amendes (jusqu'à 50 millions d'euros) aux sociétés – de Facebook à Google – qui ne supprimeraient pas les appels à la haine et à la violence. En France, une loi a été proposée, qui autoriserait le conseil supérieur de l'audiovisuel (CSA) à supprimer des messages, fermer les comptes des utilisateurs

fautifs et bloquer des sites internet pour protéger le processus démocratique français contre la propagation de fausses nouvelles pendant les élections. En vertu de cette loi, il incomberait aux médias de coopérer avec les pouvoirs publics et de faire montre de transparence quant au parrainage de leur contenu.

67. En Europe centrale et orientale, les Alliés ont pris des mesures énergiques pour contrer la désinformation russe. Récemment, l'Estonie a multiplié par 13 et même plus le budget de ses services de communication stratégique, qui sont responsables de la lutte contre la propagande. Au sein de son ministère de l'intérieur, la République tchèque a créé un centre de lutte contre le terrorisme et les menaces hybrides chargé de faire pièce à la propagande. Ce centre utilise un compte Twitter pour réfuter les histoires mensongères. La Lituanie accueille sur son territoire *Radio Liberty*, une station financée par les États-Unis qui émet à destination des Russes et des Bélarussiens dans leurs langues respectives.

68. Dans le domaine de la **cyberdéfense**, un fait notable a été l'annonce par le Royaume-Uni de la création d'une cyberforce offensive dotée d'un effectif pouvant aller jusqu'à 2 000 personnes, soit près de quatre fois plus que l'effectif affecté jusqu'ici aux cyberopérations offensives (Haynes, 2018).

69. La Suède et la Finlande, qui ne sont pas des pays partenaires de l'OTAN, sont de plus en plus fréquemment visées par des activités hybrides russes. Ces deux pays mettent l'accent sur l'éducation pour faire face aux fausses informations, plutôt que d'en restreindre l'accès. Ils ont mis en chantier des programmes destinés à apprendre aux enfants, dès l'école primaire, à distinguer les vraies des fausses sources d'information. Ces programmes sont présentés sous des formes amusantes, parmi lesquelles l'une des bandes dessinées les plus populaires de Suède. Des responsables du ministère des affaires étrangères de Finlande affirment que la formation à une lecture critique des médias aide la population à se détourner des sites de fausses nouvelles et de propagande et a entraîné la fermeture de l'antenne en langue finnoise de *Sputnik*, faute d'audience suffisante (Standish, 2017).

D. MÉDIAS ET SOCIÉTÉ CIVILE

70. La lutte contre les menaces hybrides ne se confine pas aux milieux gouvernementaux et prend de l'ampleur parmi les entités civiles, universitaires et médiatiques. Les plus connues des démarches citoyennes et universitaires visant à démonter les mensonges russes sont *StopFake.org*, une initiative de journalistes et d'étudiants ukrainiens, le *Digital Forensic Research Lab*, entité mise en place par le Conseil atlantique (un groupe de réflexion installé aux États-Unis), et les « Elfes baltes », des volontaires des pays baltes qui interviennent sur internet pour prendre à partie les trolls pro-Kremlin.

71. Les médias classiques ont instauré de nombreux mécanismes de vérification des faits, tels que le *Reality Check* de la BBC ou *Les décodeurs* du journal *Le Monde*. En période d'élections, de grands journaux allemands et suédois ont conjugué leurs efforts pour prévenir toute immixtion étrangère dans le domaine de l'information. Récemment, tous les grands médias de Lituanie, les « Elfes » et l'unité des communications stratégiques des forces armées du pays ont lancé une initiative conjointe baptisée *Demaskuok.lt* (Démystification.lt). Cette initiative a pour objet de guetter et de dénoncer les fausses nouvelles avant que celles-ci se répandent dans le pays. Les partenaires de l'initiative recourent à des algorithmes très élaborés et à l'intelligence artificielle pour passer en revue des milliers d'articles de presse en russe et en lituanien pour y détecter fausses nouvelles et manœuvres d'intoxication. *Demaskuok.lt* a suscité un vif intérêt dans les milieux de l'OTAN et de l'Union européenne.

72. Les géants des réseaux sociaux et de la technologie comme Facebook, Microsoft, Twitter et YouTube se concentrent spécifiquement sur le retrait des contenus liés au terrorisme, mais Facebook coopère dans une certaine mesure avec Washington dans le contexte de l'enquête sur l'ingérence russe dans l'élection présidentielle aux États-Unis et a publié de nouvelles lignes

directrices en matière de publicité. De la même manière, Twitter a déclaré la guerre aux fausses nouvelles et aux comptes louches. Il s'agit d'enrayer la désinformation et de « mieux protéger les utilisateurs de la manipulation et des abus », a déclaré le vice-président du réseau social, Del Harvey. Plus de 70 millions de comptes ont été suspendus en mai et juin et le sont toujours. La plupart d'entre eux sont russes et ressemblent aux faux comptes utilisés pour l'ingérence dans l'élection américaine de 2016. Twitter a annoncé en outre « des changements de grande ampleur dans les algorithmes utilisés pour sanctionner les mauvais comportements » (Timberg et Dwoskin, 2018).

73. Toutefois, les entreprises de réseaux sociaux sont de plus en plus instamment priées d'en faire davantage. En mai 2017, la commission des affaires intérieures de la Chambre des communes du Royaume-Uni a publié un rapport reprochant à ces entreprises d'être « scandaleusement loin » de faire échec aux contenus illégaux ou dangereux. En l'absence de frontières nationales dans le cyberespace, il est difficile pour les législateurs d'introduire de force des changements significatifs, dès lors qu'aucune mesure d'incitation commerciale ne pousse ces entreprises à partager des informations avec eux ou à les autoriser à passer leurs contenus au crible.

IV. CONCLUSIONS ET RECOMMANDATIONS

74. L'emploi de tactiques hybrides par la Russie constitue manifestement un défi pour la communauté euro-atlantique. Si ce pays est plus faible sur le double plan économique et culturel, il semble souvent avoir l'avantage sur le terrain de la guerre hybride en raison de son processus décisionnel unifié et de son programme résolument antioccidental. De plus, le Kremlin n'est pas tenu par les mêmes contraintes éthiques que de nombreux pays membres de l'OTAN, comme il l'a montré, notamment, en truquant la récente « élection » présidentielle au profit du titulaire de la fonction (qui est même allé jusqu'à bourrer les urnes devant les caméras), en créant des usines à trolls, voire en utilisant contre une population des armes de destruction massive sur un territoire étranger. Il tire parti de la liberté de la presse dont jouit le monde libre, mais élimine la liberté d'expression en Russie et utilise ses propres médias comme autant d'armes de tromperie massive. Enfin, il soutient des mouvements politiques extrémistes à l'Ouest, tout en persécutant les opposants sur la scène intérieure.

75. La machinerie hybride russe est innovante et difficilement prévisible. La plupart du temps, le Kremlin exploite les divisions existantes au sein des sociétés occidentales et cherche à les approfondir. Il est donc impératif de se concentrer sur un renforcement de la résilience générale de la société et sur la résolution des différends internes, plutôt que de tenter de prévoir le prochain mouvement des Russes. Les exemples qui nous viennent de la Suède et de la Finlande sont, à cet égard, d'une grande importance. Les efforts en matière de défense contre les menaces hybrides doivent être orientés vers l'intérieur plutôt que dirigés vers l'extérieur, à l'encontre d'un pays en particulier. L'Alliance devrait agir plus promptement, s'agissant de tirer parti des atouts de la démocratie – liberté d'expression, droits humains fondamentaux et État de droit – pour exploiter les points faibles d'une menace hybride.

76. Cela dit, le rapporteur voudrait soumettre ici diverses propositions concrètes visant à améliorer la riposte de la communauté euro-atlantique aux opérations hybrides du Kremlin :

- Les Alliés devraient revoir leurs politiques en matière d'éducation et veiller à ce que les écoles encouragent de vrais débats factuels et la formation d'un véritable esprit critique. Les nouvelles générations, ferventes utilisatrices des réseaux sociaux, devraient être incitées à s'extirper de leur bulle virtuelle et à repérer les trolls et les bots. Dans la guerre hybride, les forces armées ont un rôle d'appui, mais notre première ligne de défense est une société éduquée, patriote et résiliente.

- Pour être efficace, la riposte aux menaces hybrides doit être le fruit d'une collaboration sans faille entre divers secteurs. Il convient d'instaurer au sein de l'OTAN une cohérence et une coordination accrues, notamment en conjuguant les moyens civils et militaires disponibles.

- Il faut accroître la prise de conscience stratégique. Les Alliés doivent être à même d'évaluer rapidement et unanimement les événements sur le terrain pour parer effectivement aux menaces hybrides russes. Cela demande un plus large partage des données du renseignement, le resserrement des liens entre services d'un même pays et la reprise du débat sur le rôle des forces spéciales dans la coordination de l'aide militaire entre membres et partenaires de l'OTAN. Certains commentateurs préconisent la création d'un pôle OTAN pour l'Est, sur le modèle du pôle pour le Sud installé à Naples. Le rapporteur pense toutefois qu'il convient en priorité d'exploiter au maximum les structures existantes, telles que le commandement allié des forces interarmées de l'OTAN sis à Brunssum, aux Pays-Bas.

- Ceux des Alliés qui ne l'ont pas encore fait devraient mettre sur pied des services gouvernementaux spécifiques chargés de faire constamment barrage aux fausses nouvelles et à la propagande hostile en leur opposant des faits concrets. Les structures existantes telles que la division Diplomatie publique de l'OTAN ou le groupe de travail sur la communication stratégique de l'Est de l'Union européenne devraient recevoir des moyens financiers et humains supplémentaires pour riposter de manière crédible aux opérations de guerre hybride chaque fois que possible.

- Tout en se concentrant sur la résilience sur le plan intérieur, il conviendrait de continuer à appliquer des mesures restrictives (retrait des infox, sanctions pour incitation à la haine, inscription sur une liste noire des « guerriers de la désinformation » russes les plus actifs et gel de leurs avoirs, etc.). Les Alliés devraient sérieusement réfléchir à une confiscation des avoirs des élites russes corrompues dans les pays occidentaux.

- Les structures électorales devraient être considérées comme des infrastructures d'importance stratégique. Les institutions vouées à la sécurité nationale et à la cybersécurité devraient aider les partis et candidats politiques à protéger leurs données et leurs réseaux.

- Si la priorité accordée à la cyberdéfense va en augmentant, il n'en reste pas moins que l'amélioration de la sécurité de nos réseaux et systèmes passe par une réflexion plus créative et par une coopération multilatérale s'étendant à toute l'Alliance. Les membres de cette dernière devraient songer à renforcer leurs capacités de riposte dans le cyberespace et à permettre à l'OTAN de faire appel à eux pour utiliser à bon escient leurs cybercapacités offensives et appuyer ses opérations. La protection des câbles de communication sous-marins doit être assurée en priorité.

- Il faut certes se féliciter de l'approfondissement de la coopération entre l'OTAN et l'UE dans le domaine de la lutte contre les menaces hybrides, mais il est possible de progresser davantage. Le rapporteur recommande aux deux entités de réfléchir à la création d'une plateforme commune de lutte contre ces menaces, plateforme qui serait sise à Bruxelles. L'OTAN et l'Union européenne devraient aussi envisager de mettre sur pied de petites équipes mixtes anti-guerre hybride qui seraient chargées de réunir et d'analyser les informations disponibles pour une meilleure vue d'ensemble de la situation (Parlement européen, 2017).

- Il est impératif de poursuivre les efforts consacrés à la diversification des importations de produits énergétiques et de promouvoir l'efficacité énergétique, y compris en donnant corps au projet d'Union européenne de l'énergie.

- Pour enrayer l'expansion de la guerre hybride russe, il faut s'atteler à la résolution du problème des « zones grises » en Europe de l'Est. Abandonner les pays est-européens dans les limbes revient à inciter la Russie à perpétrer de nouvelles agressions et à attiser les tensions avec

l'Ouest. Il conviendrait d'offrir à la Géorgie, à l'Ukraine et à la République de Moldova, de même qu'aux pays des Balkans occidentaux, des perspectives claires d'adhésion à l'OTAN comme à l'Union européenne. L'accession de ces pays devrait seulement être fonction de leur satisfaction aux critères fixés en la matière.

77. Le rapporteur estime que les documents stratégiques de l'OTAN devraient affermir le rôle de cette dernière dans la riposte aux menaces hybrides. Il y a peu, l'ancien secrétaire aux affaires étrangères du Royaume-Uni, William Hague, a pressé les Alliés de remanier le traité de Washington en y introduisant un article 5 *bis*, lequel préciserait qu'une attaque hybride déclencherait également une riposte collective de l'Alliance. Il se peut que l'idée de modifier un traité qui a subi avec succès l'épreuve du temps ne séduise pas tous les Alliés, mais le rapporteur a la conviction que les dirigeants des pays membres devraient entamer la rédaction d'un nouveau concept stratégique de l'Alliance qui refléterait la nouvelle réalité mondiale en matière de sécurité, à commencer par la montée des menaces hybrides. Comme l'a dit M. Hague : « La remise à niveau de l'OTAN [...] signifierait que l'Alliance occidentale, tellement habituée à choisir entre le noir de la guerre et le blanc de la paix, s'adapterait enfin au monde nouveau que chérit passionnément M. Poutine et que reflète la victoire électorale de ce dernier : un monde d'un gris permanent ».

78. Pour conclure, le rapporteur voudrait souligner que le Kremlin semble déterminé à perturber le processus décisionnel collectif européen et à réduire l'influence des États-Unis sur le continent. Dans ses efforts pour affaiblir la communauté de la sécurité euro-atlantique, il remet en cause notre vision commune d'une Europe entière et paisible. C'est là un redoutable défi, mais la communauté euro-atlantique est capable d'en venir à bout si elle agit dans un esprit de solidarité. L'ampleur de la réaction internationale à la scandaleuse utilisation d'une arme chimique sur le territoire britannique prouve que les tactiques hybrides de la Russie commencent à susciter dans le monde un sentiment d'impatience teintée d'agressivité. Ainsi que l'a déclaré la première ministre du Royaume-Uni, Theresa May, en s'adressant aux dirigeants russes : « Nous savons ce que vous cherchez à faire et vous n'y parviendrez pas. Car vous sous-estimez la résistance de nos démocraties, l'attrait éternel des sociétés libres et ouvertes et l'attachement des nations occidentales aux alliances qui les unissent ».

BIBLIOGRAPHIE

Asan. (2018, July 31). The Rise of Phantom Traders: Russian Oil Exports to North Korea. Retrieved from The Asian Insitute for Policy Studies: http://en.asaninst.org/contents/the-rise-of-phantom-traders-russian-oil-exports-to-north-korea/

BBC. (2017, December 15). Russia a 'risk' to undersea cables, defence chief warns. http://www.bbc.com/news/uk-42362500

BBC. (2017, November 17). UK cyber-defence chief accuses Russia of hack attacks. http://www.bbc.com/news/technology-41997262

Beebe, G. (2017, October 31). Containing Our Intelligence War with Russia. Retrieved from The National Interest: http://nationalinterest.org/feature/containing-our-intelligence-war-russia-22985

Belsat. (2017, December 22). Russia's foreign intelligence chief accuses West of waging hybrid war. Retrieved from Belsat: http://belsat.eu/en/news/russia-s-foreign-intelligence-chief-accuses-west-of-waging-hybrid-war/

Burgess, M. (2017, November 10). Here's the first evidence Russia used Twitter to influence Brexit. Retrieved from Wired: http://www.wired.co.uk/article/brexit-russia-influence-twitter-bots-internet-research-agency

Calabresi, Massimo. "Inside Russia's Social Media War on America." Time, 18 May 2017. http://time.com/4783932/inside-russia-social-media-war-america/

Chen, Adrian, "The Agency", The New York Times Magazine, 2 June 2015, https://www.nytimes.com/2015/06/07/magazine/the-agency.html

Edwards, J. (2017, December 3). British security services are vastly outgunned by the Russian counterintelligence threat. Retrieved from Business Insider: http://uk.businessinsider.com/british-security-services-vs-russian-counterintelligence-threat-2017-12?r=UK&IR=T

Parlement européen (mars 2017) (en anglais seulement)
Countering hybrid threats: EU-NATO cooperation. http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017)599315_EN.pdf

Euronews. (2018, February 12). New report concludes Russian social media interfered in UK's EU referendum. Retrieved from Euronews: http://www.euronews.com/2018/02/12/new-report-concludes-russian-social-media-interfered-in-uk-s-eu-referendum

EUvsDisinfo. (2016, December 16). A threat to democracy. Retrieved from EUvsDisinfo: https://euvsdisinfo.eu/a-threat-to-democracy/

EUvsDisinfo. (2017, September 11). Three things you should know about RT and Sputnik. Retrieved from EUvsDisinfo: https://euvsdisinfo.eu/three-things-you-should-know-about-rt-and-sputnik/

EUvsDisinfo. (2017, December 21). What didn't happen in 2017? Retrieved from EUvsDisinfo: https://euvsdisinfo.eu/what-didnt-happen-in-2017/

EUvsDisinfo. (2018, January 15). Chief Editor: RT is like "a defence ministry". Retrieved from EUvsDisinfo: https://euvsdisinfo.eu/chief-editor-rt-is-like-a-defence-ministry/

EUvsDisinfo. (2018, April 16). "USA Really. Wake Up Americans". The story of Russia's new private propaganda outlet. Retrieved from EUvsDisinfo: https://euvsdisinfo.eu/usa-really-wake-up-americans-the-story-of-russias-new-private-propaganda-outlet/

Foreign Affairs. (2017, November 13). How Big a Challenge Is Russia? Retrieved from Foreign Affairs: https://www.foreignaffairs.com/ask-the-experts/2017-11-13/how-big-challenge-russia

Galeotti, Mark, "The Kremlin's Newest Hybrid Warfare Asset: Gangsters", Foreign Policy, 12 June 2017, http://foreignpolicy.com/2017/06/12/how-the-world-of-spies-became-a-gangsters-paradise-russia-cyberattack-hack/

Galeotti, Mark, "Do the Western Balkans face a coming Russian storm?", European Council on Foreign Relations, ECFR/250, April 2018, https://www.ecfr.eu/page/-/ECFR250_do_the_western_balkans_face_a_coming_russian_storm.pdf

Gelzis, G., & Emmott, R. (2017, October 5). Russia may have tested cyber warfare on Latvia, Western officials say. Retrieved from Reuters: https://www.reuters.com/article/us-russia-nato/russia-may-have-tested-cyber-warfare-on-latvia-western-officials-say-idUSKBN1CA142

Greenberg, A. (2017, September 5). The NSA confirms it: Russia hacked French election 'infrastructure'. Retrieved from Wired: https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/

Grigas, A. (2017, November). Is Russia's Energy Weapon Still Potent in the Era of Integrated Energy Markets? Retrieved from Hybrid CoE: https://www.hybridcoe.fi/wp-content/uploads/2017/12/Strategic-Analysis-November-2017.pdf

Grove, T., Barnes, J., & Hinshaw, D. (2017, October 4). Russia Targets NATO Soldier Smartphones, Western Officials Say. Retrieved from Wall Street Journal: https://www.wsj.com/articles/russia-targets-soldier-smartphones-western-officials-say-1507109402?utm_content=buffer2da6c&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

Hauer, N. (2018, August 27). Russia's Favorite Mercenaries. Retrieved from The Atlantic: https://www.theatlantic.com/international/archive/2018/08/russian-mercenaries-wagner-africa/568435/

Haynes, D. (2018, September 21). Britain to create 2,000-strong cyber force to tackle Russia threat. Retrieved from SkyNews: https://news.sky.com/story/britain-to-create-2000-strong-cyber-force-to-tackle-russia-threat-11503653

House of Commons. (2018b, July 29). Disinformation and 'fake news': Interim Report. Retrieved from Digital, Culture, Media and Sport Committee: UK - Disinformation and 'fake news': Interim Report

House of Commons. (2018a, May 21). Moscow's Gold: Russian Corruption in the UK. Retrieved from Foreign Affairs Committee: https://publications.parliament.uk/pa/cm201719/cmselect/cmfaff/932/932.pdf

Kramer, F. D. & Speranza, L. M. (2017, May). Meeting the Russian Hybrid Challenge. Retrieved from Atlantic Council: https://euagenda.eu/upload/publications/untitled-92736-ea.pdf

Kremidas-Courtney, C. (2018, June 11). Countering Hybrid Threats in the Maritime Environment. Retrieved from CIMSEC: http://cimsec.org/countering-hybrid-threats-in-the-maritime-environment/36553

Kuhrt, N., & Feklyunina, V. (2017). Assessing Russia's Power: A Report. Retrieved from King's College London and Newcastle University: https://www.bisa.ac.uk/files/working%20groups/Assessing_Russias_Power_Report_2017.pdf

McFadden, C., Arkin, W. M. & Monahan, K. (2018, February 7). Russians penetrated U.S. voter systems, top U.S. official says. Retrieved from NBC News: https://www.nbcnews.com/politics/elections/russians-penetrated-u-s-voter-systems-says-top-u-s-n845721?cid=db_npd_nn_fb_fbbot

Murphy, M., Hoffman, F. G. & Schaub, G. (2016, November). Hybrid Maritime Warfare and the Baltic Sea Region. Retrieved from Centre for Military Studies, University of Copenhagen: http://cms.polsci.ku.dk/publikationer/hybrid-maritim-krigsfoerelse/Hybrid_Maritime_Warfare_and_the_Baltic_Sea_Region.pdf

NATO StratCom Centre of Excellence, "Countering propaganda: NATO spearheads use of behavioural change science", 12 May 2015, https://www.stratcomcoe.org/countering-propaganda-nato-spearheads-use-behavioural-change-science

Polyakova, Alina, "Why Europe Is Right to Fear Putin's Useful Idiots", Foreign Policy, 23 February 2016, http://foreignpolicy.com/2016/02/23/why-europe-is-right-to-fear-putins-useful-idiots/

Rettman, A. (2017, November 13). Spain joins call for EU action on propaganda. Retrieved from EU Observer: https://euobserver.com/foreign/139843

Rettman, A. (2018, January 15). Sweden raises alarm on election meddling. Retrieved from EU Observer: https://euobserver.com/foreign/140542

Ringstrom, Anna, "Sweden security forces fear Russian military operations", Reuters, 18 March 2015, https://www.reuters.com/article/us-sweden-espionnage-russia/sweden-security-forces-fear-russian-military-operations-idUSKBN0ME1H620150318

Saarelainen, M. (2017, September 4). Hybrid threats – what are we talking about? Retrieved from Hybrid CoE: https://www.hybridcoe.fi/hybrid-threats-what-are-we-talking-about/

Sanger, D. E., & Frenkel, S. (2018, August 21). New Russian Hacking Targeted Republican Groups, Microsoft Says. Retrieved from The New York Times: https://www.nytimes.com/2018/08/21/us/politics/russia-cyber-hack.html

Satter, R. (2018. August 28). Ungodly espionage: Russian hackers targeted Orthodox clergy. Associated Press: https://www.apnews.com/26815e0d06d348f4b85350e96b78f6a8/Nothing-sacred:-Russian-spies-tried-hacking-Orthodox-clergy

Shekhovtsov, Anton, "Russia and Front National: Following the Money", The Interpreter, 3 May 2015, http://www.interpretermag.com/russia-and-front-national-following-the-money/

Schmidle, Nicholas, "The U.S. Has More to Lose Than Russia in Spy Expulsions", The New Yorker, 7 August 2017, https://www.newyorker.com/news/news-desk/the-us-has-more-to-lose-than-russia-in-spy-expulsions

Shuster, S. (2017, September 25). How Russian Voters Fueled the Rise of Germany's Far-Right. Retrieved from Time: http://time.com/4955503/germany-elections-2017-far-right-russia-angela-merkel/

Smith, H. (2017, October). In the era of hybrid threats: Power of the powerful or power of the "weak"? Retrieved from Hybrid CoE: https://www.hybridcoe.fi/wp-content/uploads/2017/11/Strategic-Analysis-October-2017.pdf

Standish, R. (2017, October 12). Russia's Neighbors Respond to Putin's 'Hybrid War'. Retrieved from Foreign Policy: http://foreignpolicy.com/2017/10/12/russias-neighbors-respond-to-putins-hybrid-warlatvia-estonia-lithuania-finland/

Swaine, J. (2018, August 6). Maria Butina's alleged backer linked to Kremlin-financed bank and Putin associates. Retrieved from The Guardian: https://www.theguardian.com/world/2018/aug/06/maria-butina-charged-spying-putin-russia-kremlin

The Economist. (2017, July 1). Fake news: you ain't seen nothing yet. Retrieved from The Economist: https://www.economist.com/news/science-and-technology/21724370-generating-convincing-audio-and-video-fake-events-fake-news-you-aint-seen

Timberg, C., & Dwoskin, E. (2018, July 6). Twitter is sweeping out fake accounts like never before, putting user growth at risk. Retrieved from The Washington Post: https://www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk/?noredirect=on&utm_term=.e2d094395640

Thornton, R. (2016, October 27). Russian "Hybrid Warfare" and the National Defence Management Centre (NTsUO). Retrieved from After 'hybrid warfare', what next? http://tietokayttoon.fi/documents/10616/1266558/Understanding+and+respond-ing+to+contemporary+Russia/49bdb37f-11da-4b4a-8b0d-0e297af39abd?ver-sion=1.0

Tucker, P. (2017, October 9). How the US Army is Preparing to Fight Hybrid War in 2030. Retrieved from Defense One: http://www.defenseone.com/technology/2017/10/how-us-army-preparing-fight-hybrid-war-2030/141634/?oref=d-topstory&utm_source=Sailthru&utm_medium=email&utm_campaign=EBB+10.10.2017&utm_term=Editorial+-+Early+Bird+Brief

Willsher, Kim, and Henley, Jon, "Emmanuel Macron's campaign hacked on eve of French election", The Guardian, 6 May 2017, https://www.theguardian.com/world/2017/may/06/emmanuel-macron-targeted-by-hackers-on-eve-of-french-election