



Doc. 14523

06 avril 2018

Problèmes juridiques posés par la guerre hybride et obligations en matière de droits de l'homme

Rapport¹

Commission des questions juridiques et des droits de l'homme

Rapporteur: M. Boriss CILEVIČS, Lettonie, Groupe des socialistes, démocrates et verts

Résumé

Les États sont de plus en plus souvent confrontés au phénomène de «guerre hybride», qui couvre non seulement des actions militaires mais aussi d'autres actes hostiles, comme des campagnes de désinformation sur les médias sociaux ou des cyberattaques.

La notion de «guerre hybride» ou de «menace hybride» soulève plusieurs questions. Selon la commission des questions juridiques et des droits de l'homme, alors qu'il n'existe pas de définition universelle de ces termes, la principale caractéristique d'une guerre hybride est son «asymétrie juridique», car les adversaires «hybrides» nient leurs activités et agissent à la limite de la légalité. Lorsque des actions militaires sont entreprises, le droit international, et notamment le droit à la défense et le droit humanitaire, s'appliquent. En cas d'actions non-militaires, c'est surtout le droit pénal interne qui entre en jeu. En tout état de cause, les droits de l'homme doivent être respectés. Toute restriction de ces droits doit respecter les exigences découlant de la Convention européenne des droits de l'homme.

La commission propose aussi un certain nombre de recommandations à adresser aux États membres et au Comité des Ministres afin de mieux combattre la guerre hybride et de respecter les droits de l'homme dans la lutte contre ce phénomène.

1. Renvoi en commission: [Doc. 14044](#) et [Doc. 14048](#), Renvoi 4217 du 20 juin 2016.



Sommaire

Page

A. Projet de résolution	3
B. Projet de recommandation	5
C. Exposé des motifs, par M. Boriss Cilevičs, rapporteur	6
1. Introduction	6
1.1. La procédure	6
1.2. Les questions en jeu	6
1.3. Les menaces hybrides: un phénomène croissant	7
2. Problèmes juridiques liés aux menaces hybrides	9
2.1. Définitions	9
2.2. Le cadre juridique applicable	11
2.3. Les vides juridiques et les solutions possibles	14
3. Dans quelle mesure les menaces hybrides peuvent-elles justifier des restrictions aux droits de l'homme?	15
4. Conclusion	16

A. Projet de résolution²

1. L'Assemblée parlementaire rappelle ses [Résolutions 2133 \(2016\)](#) sur les recours juridiques contre les violations des droits de l'homme sur les territoires ukrainiens échappant au contrôle des autorités ukrainiennes et [2132 \(2016\)](#) sur les conséquences politiques du conflit en Ukraine, ainsi que sa [Résolution 2198 \(2018\)](#) et sa [Recommandation 2119 \(2018\)](#) sur les conséquences humanitaires de la guerre en Ukraine, qui concernent les opérations militaires menées dans ce pays. Elle rappelle également sa [Résolution 2190 \(2016\)](#) «Poursuivre et punir les crimes contre l'humanité, voire l'éventuel génocide commis par Daech».
2. L'Assemblée constate avec inquiétude que les États sont désormais de plus en plus souvent confrontés au phénomène de «guerre hybride», qui représente un nouveau type de menace fondée sur la combinaison de moyens militaires et non militaires, notamment des cyberattaques, des campagnes de désinformation massive, y compris sous forme de fausses nouvelles, lancées notamment sur les médias sociaux, la perturbation des communications et d'autres réseaux et d'autres encore. Les cyberattaques sont particulièrement dangereuses, car elles peuvent frapper les infrastructures stratégiques d'un pays comme le système de contrôle du trafic aérien ou les centrales nucléaires. Une guerre hybride peut donc déstabiliser et saper l'ensemble d'une société ainsi que causer de nombreuses pertes humaines. Face au recours généralisé à ces nouvelles tactiques, surtout lorsqu'elles sont combinées, il y a lieu de se demander si les outils législatifs existants sont adaptés.
3. L'Assemblée note qu'il n'existe pas de définition universellement acceptée de la «guerre hybride» et qu'il n'y a pas de «droit de la guerre hybride». Cependant, il est communément admis que la principale caractéristique de ce phénomène est son «asymétrie juridique», car les adversaires hybrides, en règle générale, nient leur responsabilité dans les opérations hybrides et essaient d'échapper aux conséquences juridiques de leurs actes. Ils exploitent les lacunes du droit et la complexité de la législation, agissent par-delà les frontières législatives et dans les espaces sous-réglementés, exploitent les seuils légaux, sont prêts à commettre de graves violations de la loi et créent de la confusion et de l'ambiguïté pour masquer leurs actions.
4. Malgré la complexité de la guerre hybride, l'Assemblée souligne que les adversaires hybrides n'opèrent pas dans un vide juridique et que leurs actions sont soumises aux normes pertinentes du droit international et du droit interne, notamment le droit international relatif aux droits de l'homme, même si la question de l'attribution de la paternité de ces actes, et donc de la responsabilité de leurs auteurs, peut soulever des difficultés. Si, dans le cadre d'une guerre hybride, un État recourt à la force contre un autre État, ce dernier est autorisé à invoquer le droit de légitime défense découlant de l'article 51 de la Charte des Nations Unies et les normes du droit international humanitaire s'appliqueront. Or, dans la pratique, les adversaires hybrides évitent de faire un usage manifeste de la force qui atteindrait le seuil requis pour déclencher l'application des normes précitées, ce qui crée une zone grise du droit.
5. L'Assemblée note que lorsqu'un adversaire hybride s'abstient d'utiliser des moyens militaires, ses actes devraient être examinés à la lumière du droit pénal interne et, si nécessaire et selon la situation, des instruments juridiques internationaux pertinents couvrant des domaines d'action particuliers (tels que le droit de la mer ou les normes relatives à la lutte contre la cybercriminalité, le terrorisme, le discours de haine ou le blanchiment d'argent).
6. L'Assemblée rappelle que, pour contrer la guerre hybride, les États sont tenus de respecter le droit des droits de l'homme. Elle s'inquiète du fait que certains États membres du Conseil de l'Europe ont déjà pris des mesures (telles que des condamnations pénales pour des déclarations en ligne, des mesures de surveillance, le blocage de sites ou des expulsions) qui soulèvent des questions relatives au respect des droits de l'homme, notamment la liberté d'expression, qui comporte le droit à l'information, le droit au respect de la vie privée ou le droit à la liberté de circulation.
7. L'Assemblée rappelle également que l'article 15 de la Convention européenne des droits de l'homme (STE n° 5, «la Convention») autorise les États Parties à déroger à certaines obligations «en temps de guerre ou en cas d'autre danger public menaçant la vie de la nation», mais que toute dérogation aux droits qui y sont consacrés doit être effectuée dans le respect de certaines exigences de fond et de procédure. Pour contrer les menaces de guerre hybride, les États Parties à la Convention peuvent également invoquer le «but légitime» de la «sécurité nationale», qui permet de restreindre certains droits: le droit au respect de la vie privée et familiale (article 8), la liberté d'expression (article 10), la liberté de réunion et d'association (article 11), la liberté de circulation (article 2.3 du Protocole n° 4 à la Convention (STE n° 46)), ainsi que les garanties procédurales prévues en cas d'expulsion de ressortissants étrangers (article 1.2 du Protocole n° 7 à la

2. Projet de résolution adopté à l'unanimité par la commission le 14 mars 2018.

Convention (STE n° 117). Toute restriction à ces droits doit être «prévues par la loi», «nécessaire dans une société démocratique» et proportionnée. L'expérience acquise par les États dans le domaine de la lutte contre le terrorisme peut être une source d'informations utile pour déterminer les limites imposées par le droit international aux mesures visant à contrer les menaces de guerre hybride.

8. Par conséquent, l'Assemblée invite les États membres:

8.1. à s'abstenir de recourir à la guerre hybride dans les relations internationales et à respecter pleinement les dispositions du droit international, conformément à leur objet et à leur but, en n'exploitant pas abusivement les lacunes ou les ambiguïtés apparentes;

8.2. à intensifier la coopération internationale, afin d'identifier les adversaires hybrides et tous les types de menaces de guerre hybride, et d'établir le cadre juridique applicable;

8.3. à prendre des mesures pour mieux sensibiliser l'opinion publique aux menaces de guerre hybride et renforcer sa capacité à réagir rapidement à de telles menaces;

8.4. à mettre en œuvre la Convention du Conseil de l'Europe sur la cybercriminalité (STE n° 185), à la signer et la ratifier, si ce n'est déjà fait, et à promouvoir sa ratification par les États non membres.

9. L'Assemblée se félicite des mesures prises par l'Union européenne et l'Organisation du Traité de l'Atlantique Nord (OTAN) pour contrer les menaces de guerre hybride et établir une coopération dans ce domaine. Elle appelle également tous les États membres du Conseil de l'Europe qui sont membres de l'Union européenne et de l'OTAN à partager leurs meilleures pratiques en matière de lutte contre la guerre hybride avec les autres États membres susceptibles d'être touchés par ce phénomène.

10. En ce qui concerne les mesures visant à lutter contre la guerre hybride, l'Assemblée rappelle sa [Résolution 1840 \(2011\)](#) sur les droits de l'homme et la lutte contre le terrorisme, et demande aux États membres de veiller à ce que ces mesures respectent les obligations nées de la Convention européenne des droits de l'homme, conformément à l'interprétation que lui donne la Cour européenne des droits de l'homme. S'agissant, en particulier, des droits soumis à des restrictions au titre de la Convention, toute limitation doit être prévue par la loi, proportionnée au but légitime poursuivi (par exemple la sécurité nationale) et «nécessaire dans une société démocratique».

B. Projet de recommandation³

1. L'Assemblée parlementaire renvoie à sa Résolution ... (2018) sur les problèmes juridiques posés par la guerre hybride et obligations en matière de droits de l'homme.
2. L'Assemblée recommande au Comité des Ministres:
 - 2.1. de mener une étude sur les menaces de guerre hybride, en mettant l'accent sur les moyens non militaires, afin de recenser les lacunes juridiques et d'élaborer des normes juridiques appropriées, notamment en envisageant une nouvelle convention du Conseil de l'Europe en la matière;
 - 2.2. d'élaborer des principes pour la réforme réglementaire des plates-formes de médias sociaux pour garantir la transparence du déroulement d'élections libres et équitables;
 - 2.3. d'examiner la pratique des États dans la lutte contre les menaces de guerre hybride, en vue d'identifier les normes juridiques et les bonnes pratiques et d'assurer que ces pratiques soient conformes aux garanties juridiques contenues dans la Convention européenne des droits de l'homme (STE n° 5);
 - 2.4. d'intensifier la coopération avec d'autres organisations internationales actives dans ce domaine, en particulier l'Union européenne et l'Organisation du traité de l'Atlantique Nord (OTAN);
 - 2.5. de promouvoir la ratification de la Convention sur la cybercriminalité (STE n° 185) par les États membres et non membres;
 - 2.6. d'examiner la façon dont la Convention sur la cybercriminalité est mise en œuvre par ses États Parties et d'engager une réflexion sur son éventuelle amélioration.

3. Projet de recommandation adopté à l'unanimité par la commission le 14 mars 2018.

C. Exposé des motifs, par M. Boriss Cilevičs, rapporteur

1. Introduction

1.1. La procédure

1. Le 20 juin 2016, l'Assemblée parlementaire a renvoyé à la commission des questions juridiques et des droits de l'homme deux propositions de résolution, intitulées «Restreindre les droits pour protéger la sécurité nationale – jusqu'où les États peuvent-ils aller?» et «Problèmes juridiques posés par la guerre hybride», pour qu'elles fassent l'objet d'un rapport unique⁴. À l'occasion de sa réunion du 10 octobre 2016, à Strasbourg, la commission m'a nommé rapporteur. Au cours de sa réunion du 13 novembre 2017 à Paris, la commission a procédé à une audition avec la participation de M. Andrey L. Kozik, professeur agrégé, Secrétaire général de l'Association internationale de droit international et d'arbitrage (Biélorus), de M. Robin Geiß, professeur, chaire de droit international et de sécurité, Faculté de droit de l'Université de Glasgow (Royaume-Uni), et Dr Aurel Sari, maître de conférences en droit, Directeur du Centre de droit international, Faculté de droit de l'université d'Exeter (Royaume-Uni).

1.2. Les questions en jeu

2. Pour établir ce rapport, je prendrai en compte diverses questions soulevées dans ces deux propositions. La proposition intitulée «Restreindre les droits pour protéger la sécurité nationale – jusqu'où les États peuvent-ils aller?» indique que les tentatives de restrictions des libertés fondamentales prétextent désormais la nécessité de se défendre contre une «guerre hybride» non déclarée, une notion qui n'a pas de définition juridique. Certains États membres du Conseil de l'Europe incriminent ainsi l'expression d'opinions considérées comme une menace pour l'État. Les signataires de cette proposition rappellent que la défense de l'ordre constitutionnel et de la sécurité nationale peuvent être des buts légitimes justifiant les restrictions imposées à certains droits de l'homme et libertés fondamentales, à la condition que ces restrictions soient compatibles avec les exigences de la Convention européenne des droits de l'homme (STE n° 5, «la Convention»), telle qu'interprétée par la Cour européenne des droits de l'homme («la Cour»). L'Assemblée devrait examiner ces questions à la lumière des normes du Conseil de l'Europe pour déterminer si ces restrictions peuvent se justifier et à quelles conditions.

3. La seconde proposition de résolution porte sur la notion de guerre hybride, fréquemment utilisée, par exemple, au sujet du conflit militaire en cours en Ukraine et des activités de Daech. Selon cette proposition, la guerre hybride constitue une menace d'un genre nouveau, fondée sur la combinaison de moyens militaires et non militaires, notamment les cyberattaques, les campagnes de désinformation massive lancées sur des médias sociaux, la perturbation des communications et bien d'autres moyens. Face au recours généralisé à ces nouvelles tactiques, surtout lorsqu'elles sont combinées, il y a lieu de se demander si les normes existantes sont adaptées. L'Assemblée devrait donc recenser les lacunes du droit pour élaborer des normes appropriées permettant de prendre des mesures défensives, même en l'absence d'attaque armée directe par un autre État. Ces mesures offriraient également des garanties contre l'application sélective du droit international.

4. Vu le contenu de ces deux propositions, je me sens obligé, en ma qualité de rapporteur, d'examiner en même temps deux ambitions aussi bien contradictoires que complémentaires: d'une part, comment définir la «guerre hybride» ou les «menaces de guerre hybride» et identifier les mesures qu'un État peut prendre à juste titre pour se défendre contre ces actes, dans le respect du droit international et, d'autre part, comment protéger les droits de l'homme et les libertés fondamentales lorsqu'un État les restreint dans le but de se défendre contre les divers actes de guerre hybride dont il est la cible de la part d'un autre État ou d'un acteur non étatique puissant, comme Daech. Pour ce qui est de la deuxième question, rappelons que l'Assemblée a déjà examiné le problème des restrictions imposées aux droits de l'homme et aux libertés fondamentales dans l'intérêt de la sécurité nationale et de la sûreté publique dans le contexte de la lutte contre le terrorisme (voir, en particulier, les rapports et les résolutions sur «Les droits de l'homme et la lutte contre le terrorisme» et «La sécurité nationale et l'accès à l'information»⁵). L'Assemblée a réaffirmé à de nombreuses occasions que le terrorisme peut et doit être effectivement combattu par des moyens qui respectent pleinement les droits de l'homme et l'État de droit⁶.

4. [Doc. 14044](#) et [Doc. 14048](#).

5. Voir, respectivement, [Doc. 12712](#) du 16 septembre 2011 (rapporteur: Lord John Tomlinson) et [Doc. 13293](#) du 3 septembre 2013 (rapporteur: M. Arcadio Díaz Tejera), ainsi que la [Résolution 1840 \(2011\)](#), la [Résolution 1954 \(2013\)](#) et la [Recommandation 2024 \(2013\)](#) de l'Assemblée.

1.3. Les menaces hybrides: un phénomène croissant

5. Ces dernières années, les menaces de guerre hybrides sont devenues l'une des premières préoccupations de sécurité dans les États membres du Conseil de l'Europe. D'une part, les experts américains et européens en matière de sécurité évoquent souvent la menace croissante à plusieurs niveaux que représente la Fédération de Russie pour la sécurité, en citant l'exemple des opérations hybrides russes menées dans l'est de l'Ukraine, en Crimée ou en Géorgie⁷. En 2016, les questions relatives à ce conflit ont été examinées par notre commission dans le rapport de M^{me} Marieluise Beck (Allemagne, ADLE) sur «Les recours juridiques contre les violations des droits de l'homme sur les territoires ukrainiens échappant au contrôle des autorités ukrainiennes» par la commission des questions politiques et de la démocratie dans le rapport de M^{me} Kristýna Zelienková (République tchèque, ADLE) sur les «Conséquences politiques du conflit en Ukraine» et par la commission des migrations, des réfugiés et des personnes déplacées dans le rapport de M. Egidijus Vareikis (Lituanie, PPE/DC) sur les «Conséquences humanitaires de la guerre en Ukraine»⁸. D'autre part, ce terme est aussi utilisé par les stratèges russes pour désigner les initiatives prises par les pays occidentaux pour déstabiliser des «gouvernements inamicaux»⁹. Ainsi, les responsables russes établissent un parallèle direct entre la guerre hybride et les tentatives visant à porter atteinte à l'intégrité de gouvernements dans le cadre des révolutions dites «de couleur» dans les anciennes républiques soviétiques, par exemple en Géorgie en 2003 ou en Ukraine en 2004. Pour le ministre russe de la Défense, Sergueï Choïgou, «les révolutions de couleur prennent de plus en plus la forme de guerres et sont conçues selon les règles de la guerre»¹⁰.

6. Il convient de noter que l'utilisation de moyens de guerre non militaires n'est ni nouvelle (selon certains chercheurs, cette «hybridité» remonte à la guerre du Péloponnèse¹¹) ni propre à un pays¹². Les avancées technologiques s'accompagnent cependant de nouveaux moyens de guerre et de pouvoir souples. Les menaces hybrides visent les points faibles d'un pays, souvent dans le but de mettre à mal ses caractéristiques essentielles (par exemple son régime et son idéologie politiques, son économie, son intégrité territoriale). C'est tout particulièrement le cas dans le domaine de la cybersécurité. Aujourd'hui, notre grande dépendance vis-à-vis des systèmes informatiques et des réseaux numériques a complètement reconfiguré la conception et le fonctionnement des systèmes énergétiques, financiers, de télécommunication et de transport – c'est-à-dire tout ce qui constitue l'infrastructure essentielle d'un pays. Elle a également changé la manière de protéger la démocratie et les droits fondamentaux, en particulier la liberté d'expression et l'accès à l'information. Certains phénomènes récents, tels que la «guerre de l'information» (qui n'est pas nouvelle en soi mais qui a pris une dimension redoutable) et les «cyberattaques», qui ne sont pas géographiquement limitées, illustrent parfaitement ces nouveaux défis.

7. La «guerre de l'information», qui est définie par certains chercheurs comme le «conflit ou la lutte entre deux ou plusieurs groupes dans l'environnement de l'information»¹³, vise à imposer un point de vue particulier à une population en «créant [une] domination impénétrable, active et offensive de l'information»¹⁴. Le but d'une «guerre de l'information» est de gagner la confiance de la population¹⁵. En fait, cette forme de guerre associe la guerre électronique (notamment les contre-mesures électroniques et le brouillage), la cyberguerre (qui sera analysée en détail plus loin) et les opérations psychologiques («psyops») qui visent à saper le moral et altérer le bien-être des citoyens d'un pays, par exemple en diffusant de fausses informations dans les réseaux sociaux et les médias). Ces campagnes semblent avoir le plus de succès dans des régions déjà instables. Les campagnes russes de désinformation, par exemple, ont trouvé un terrain propice en Crimée et dans la région du Donbass, où une partie de la population était déjà prête à accepter la lecture russe des événements¹⁶. Dans son rapport sur «les conséquences politiques du conflit en Ukraine», la

6. Par exemple, dans la [Résolution 1840 \(2011\)](#), paragraphes 5-7.

7. OTAN, [La guerre hybride existe-t-elle vraiment?](#) NATO Review, 2015, et [Discours liminaire du Secrétaire général de l'OTAN Jens Stoltenberg](#) à l'ouverture du séminaire sur la transformation de l'OTAN, 25 mars 2015; voir aussi, John Swaine, «Georgia: Russia "conducting cyber war"», *The Telegraph*, 11 août 2008.

8. Voir, respectivement, [Doc. 14139](#) du 26 septembre 2016 et la [Résolution 2133 \(2016\)](#) de l'Assemblée; [Doc. 14130](#) du 31 août 2016 et [Résolution 2132 \(2016\)](#) de l'Assemblée, ainsi que [Doc. 14463](#) et [Résolution 2198 \(2018\)](#) et [Recommandation 2119 \(2018\)](#) de l'Assemblée.

9. Samuel Charap, *The Ghost of Hybrid Warfare*, *Survival, Global Politics and Strategy*, n° 57/6, 51-56.

10. Alexander Golts, [Are Colour Revolutions a New Form of War?](#), *The Moscow Times*, 2 juin 2014.

11. A. Sari, *Hybrid Warfare, Law and the Fulda Gap*, University d'Exeter, École de droit, 2017, p. 9.

12. B. Renz et H. Smith et autres, *Russia and Hybrid Warfare, Going Beyond the Label*, *Aleksanteri Papers 2016/1*, Kikimora Publications, université de Helsinki, 2016, p. 11.

13. I. Porche III et autres, *Redefining Information Warfare Boundaries for an Army in a Wireless World*, RAND Corporation, 2013, p. XV.

14. Christian Bahnareanu, *The evolution of warfare from classic to hybrid actions*, *Strategic Impact*, n° 2/2015, p. 61-62.

15. B. Renz et H. Smith, voir note 12 ci-dessus, p. 6.

commission des questions politiques et de la démocratie a souligné que l'action de la Russie se traduisait également par une intense guerre d'information ou de propagande «qui est presque aussi dangereuse que le conflit militaire»¹⁷. Il est donc compréhensible que les États qui comptent une minorité ethnique russe soient préoccupés par une telle menace, même si l'on constate que les États-Unis et d'autres pays européens sont également exposés à ce phénomène. En outre, le fait de vouloir exercer une influence systématique sur l'opinion publique et les processus électoraux n'est pas un phénomène nouveau en soi, mais son ampleur a considérablement augmenté ces dernières années. L'exemple des États-Unis, où 126 millions de citoyens ont été prétendument soumis à la désinformation russe avant l'élection présidentielle de 2016, est un exemple particulièrement frappant à cet égard¹⁸. On note que des ingérences similaires dans le processus électoral ont apparemment eu lieu en Allemagne, en France et dans certains pays de la région des Balkans.

8. Dans la guerre de l'information, l'absence d'obligation de rendre des comptes pour les propos tenus en ligne et l'absence d'attribution de la paternité de ces propos ne facilitent pas la tâche des États qui cherchent à déterminer ce qui relève de la liberté d'expression et ce qui peut être qualifié d'ingérence étrangère. Cette tâche est particulièrement difficile en cas de financement étranger. *Sputnik news* et *RT* (anciennement *Russia Today*), par exemple, ont des filiales européennes et sont financés par des actifs russes, tandis que le média conservateur américain *Breitbart News* a ouvert des bureaux en Europe. Dans le débat actuel sur la façon dont les «fausses nouvelles» (*fake news*) en ligne façonnent l'opinion publique, les enquêtes sur le lien qui existe entre les puissances étrangères et ces organes de presse sont déterminantes. Même sans une présence physique dans un pays donné, des sources de désinformation peuvent pénétrer l'environnement de l'information et influencer le discours public, en particulier lorsque l'accès à internet et les contenus en ligne sont libres et peu réglementés. Les «trolls en ligne» se situent également dans une zone grise, à mi-chemin entre des individus qui expriment leurs opinions et des acteurs non étatiques semi-organisés qui agissent en fonction des priorités politiques d'un État précis. L'exemple des «usines de trolls» russes¹⁹ montre qu'il est de plus en plus difficile de faire la distinction entre la liberté d'expression des militants en ligne et l'ingérence des États. De plus, l'émission des programmes audiovisuels au-delà des frontières étatiques soulève des questions quant au contrôle et à la juridiction exercés sur le contenu diffusé dans des États dans lesquels le radiodiffuseur n'est pas établi (par exemple, un radiodiffuseur russe établi en Suède qui diffuse des programmes dans les pays baltes); ainsi, une révision de la Directive «Services des médias européens» de l'Union européenne (2010/13/UE) et de la [Convention européenne sur la télévision transfrontière](#) du Conseil de l'Europe (STE n° 132) pourrait s'imposer.

9. La cyberguerre et les cyberattaques sont une forme de «menace hybride» particulièrement violente et dangereuse, car elle peut toucher des infrastructures stratégiques, notamment les systèmes de contrôle du trafic aérien, les systèmes d'écoulement des oléoducs ou les centrales nucléaires. Au cours des dix dernières années, plusieurs pays, notamment des anciennes républiques soviétiques (Estonie, Géorgie, Lituanie et Ukraine) ou des pays occidentaux (Allemagne, Finlande, Pays-Bas et États-Unis) prétendent avoir été la cible de cyberattaques russes. Un certain nombre d'ingérences très médiatisées ont également eu lieu à plusieurs niveaux stratégiques, notamment les ingérences russes dans les élections présidentielles aux États-Unis en 2016 et en Ukraine en 2014. En France, en mai 2017, des dizaines de milliers de messages électroniques et de documents issus de la campagne d'Emmanuel Macron ont été diffusés juste avant le second tour de l'élection présidentielle.

10. Certains États ont déjà pris des mesures pour se protéger des menaces terroristes hybrides. Plusieurs pays européens ont adopté des lois antiterroristes qui peuvent être utilisées contre de telles menaces, mais certaines de ces mesures pourraient porter atteinte aux droits de l'homme (ce que dénonce Amnesty International)²⁰. La cyberguerre peut conduire les États à restreindre la liberté d'accès des citoyens à internet, en développant des «techniques de filtrage» visant à limiter l'accès à certains sites, ainsi que des mécanismes de surveillance de l'usage que les citoyens font de l'internet, et en poursuivant pénalement les auteurs d'infractions commises en ligne. Les réactions des États face aux campagnes de désinformation

16. David Stupples, *What is information warfare?*

17. Voir paragraphe 84 du rapport.

18. Ces données proviennent de représentants de Facebook, Twitter et Google qui ont témoigné lors d'une audition qui s'est tenue le 31 octobre 2017 au Congrès américain. Voir, par exemple, [Russia used mainstream media to manipulate American voters](#), *Washington Post*, 15 février 2018.

19. Mike Wendling et Will Yates, [NATO says viral news outlet is part of «Kremlin misinformation machine»](#), BBC, 11 février 2017; Emily Flitter, [Riding Trump wave, Breitbart News plans U.S., European Expansion](#), Reuters, 9 novembre 2016, et Andrew Higgins, [Effort to Expose Russia's «Troll Army» Draws vicious Retaliation](#), *New York Times*, 30 mai 2016.

20. Amnesty international, Des mesures disproportionnées: L'ampleur grandissante des politiques sécuritaires dans les pays de l'UE est dangereuse, [rapport](#), janvier 2017.

russe ont déjà des effets sur leurs citoyens. Par exemple, en Lettonie, Maksim Koptelov a été condamné à six mois de prison pour une pétition en ligne pacifique proposant que la Lettonie intègre la Russie. Quelques jours plus tard, la police a enquêté sur un autre citoyen letton, Deniss Barteckis, qui avait publié une pétition en ligne appelant la Lettonie à fusionner avec les États-Unis. Il est tout à fait normal que les États incriminent des actes qui menacent leur indépendance et leur intégrité territoriale mais, dans ces deux cas, la réaction des autorités face à une expression politique pacifique semble disproportionnée. D'autres États ont également pris des mesures controversées pour contrer des menaces hybrides. Par exemple, en mai 2017, le président ukrainien, Petro Porochenko, a pris un décret bloquant l'accès à de nombreux sites internet russes (y compris des réseaux sociaux). En Allemagne, en juin 2017, le *Bundestag* a adopté la loi sur l'amélioration de l'application des droits sur les réseaux sociaux, qui permet aux autorités d'infliger des amendes allant jusqu'à 50 millions d'euros aux entreprises de médias sociaux qui ne seraient pas capables de supprimer, dans les 24 heures, les discours haineux, les incitations à la violence et les propos diffamatoires. En France, en janvier 2018, le président Macron a annoncé qu'il fallait une loi spéciale pour lutter contre les *fake news*. Toutes ces mesures peuvent soulever des questions quant à leur compatibilité avec la liberté d'expression.

11. Les États sont donc aujourd'hui confrontés à des menaces complexes à plusieurs niveaux pour la sécurité et prennent des mesures en conséquence pour remédier à leur vulnérabilité face à ces menaces. Cependant, cette tendance étant relativement récente, aussi bien au niveau de la sécurité internationale que nationale, la notion de guerre hybride reste relativement ambiguë. Ainsi, le premier objectif de mon rapport sera d'examiner les différentes notions et les défis juridiques qui en découlent, et en particulier de se demander si la guerre hybride est une «guerre» au sens du droit international humanitaire. En outre, le fait que les «guerres hybrides» soient déjà prises en compte dans les stratégies de sécurité nationale des États nous permet de passer en revue certaines mesures prises pour contrer ce type de menaces que présentent les États et/ou les acteurs non étatiques. Rappelons que la Convention considère la sécurité nationale comme un but légitime, qui autorise une ingérence dans les droits de l'homme, sous certaines conditions. Bien qu'une marge d'appréciation relativement large soit habituellement laissée aux États pour évaluer les menaces pour la sécurité et décider des mesures à prendre pour y faire face, les nouvelles mesures prises dans ce contexte doivent néanmoins respecter le droit des droits de l'homme. S'agissant des mesures prises pour protéger la sécurité nationale contre les menaces hybrides, il conviendra donc d'examiner aussi les limites légales imposées aux États sur le plan des droits de l'homme et des libertés fondamentales.

2. Problèmes juridiques liés aux menaces hybrides

2.1. Définitions

12. Selon le Service de recherche du Parlement européen (EPRS)²¹, une «menace hybride» est un phénomène résultant de la convergence et de l'interconnexion de différents éléments, qui forment ensemble une menace multidimensionnelle et plus complexe. L'EPRS définit aussi les notions de conflit et de guerre hybrides en fonction des différents niveaux d'intensité d'une menace et de l'intention des acteurs impliqués. Un «conflit hybride» est une situation dans laquelle les parties s'abstiennent de recourir ouvertement aux forces armées les unes à l'encontre des autres, privilégiant plutôt une combinaison d'intimidation militaire (sans aller jusqu'à l'agression), d'exploitation des fragilités économiques et politiques et de moyens diplomatiques ou technologiques dans la poursuite de leurs objectifs. Enfin, la guerre hybride est une situation dans laquelle un pays recourt ouvertement à l'usage de forces armées contre un autre pays ou un acteur non étatique, en plus d'une combinaison d'autres moyens (économiques, politiques et diplomatiques).

13. S'agissant des pratiques des États en matière de protection de la sécurité nationale et de leurs limites légales, il est plus exact de parler de «menace hybride» ou de «conflit hybride». «Bien qu'il existe plusieurs définitions des menaces hybrides et que celles-ci doivent rester adaptables en raison du caractère évolutif desdites menaces, cette notion vise à exprimer le mélange d'activités coercitives et subversives, de méthodes conventionnelles et non conventionnelles (c'est-à-dire diplomatiques, militaires, économiques, technologiques), susceptibles d'être utilisées de façon coordonnée par des acteurs étatiques ou non étatiques en vue d'atteindre certains objectifs, sans que le seuil d'une guerre déclarée officiellement ne soit dépassé»²². De fait, la notion de «menace hybride» est souvent perçue comme un concept «fourre-tout», utilisé pour désigner la survenance de menaces simultanées pour la sécurité. Selon l'EPRS, elle peut couvrir diverses situations, notamment des actes terroristes (de Boko Haram, d'Al-Qaïda ou de Daech), des actions

21. [At a glance. Understanding hybrid threats](#), Service de recherche du Parlement européen (EPRS), juin 2015.

22. Commission européenne, «Communication conjointe au Parlement européen et au Conseil, Cadre commun en matière de lutte contre les menaces hybrides, une réponse de l'Union européenne», Bruxelles, le 6 avril 2016, [JOIN\(2016\) 18 final, paragraphe 1](#).

contre la cybersécurité (voir ci-dessous), des actions de groupes criminels armés (tels que ceux des cartels mexicains), des différends maritimes (en mer de Chine méridionale), des contraintes sur l'utilisation de l'espace orbital, des actes économiques hostiles (comme le blocage des exportations japonaises par la Chine en 2010) ou des opérations militaires secrètes (comme l'utilisation d'«hommes verts» en Crimée). Les «menaces hybrides» peuvent émaner à la fois d'États et d'acteurs non étatiques et englober des formes de confrontation violentes et non violentes; l'Union européenne a donné la préférence à ce terme en raison de la portée de son mandat et s'est principalement concentrée sur les «menaces pour la sécurité». Cependant, le terme «guerre hybride», qui met l'accent sur des activités violentes, ne devrait poser aucun problème à l'OTAN²³.

14. Du point de vue juridique, il est plus exact d'utiliser le terme de «guerre hybride» uniquement lorsqu'il y a conflit armé et que le droit international humanitaire est, par conséquent, applicable. Les spécialistes des relations internationales et de l'analyse des conflits conçoivent la guerre hybride comme la combinaison de menaces pour la sécurité qui étaient auparavant envisagées séparément. La notion de guerre hybride combine les capacités cinétiques conventionnelles à des tactiques et formations irrégulières, comme le terrorisme, la criminalité transnationale et la prolifération des armes, surtout lorsque ces agressions sont commises par des acteurs qui sont apparemment associés à un État particulier sans être officiellement soumis à son autorité. D'autres moyens non cinétiques et de faible intensité peuvent aussi entrer dans cette définition, comme les cyberopérations, la désinformation et la propagande, visant aussi des minorités nationales ou autres, et la corruption d'acteurs clés au moyen de «fonds occultes» ou de «budgets parallèles»²⁴. La guerre hybride désigne à la fois les activités des États et celles d'acteurs non étatiques, dont on estime qu'elles sont dirigées et coordonnées dans le but de produire un «effet synergique dans les dimensions physiques et psychologiques du conflit»²⁵.

15. Pour de nombreux spécialistes, ce type de menaces est intrinsèquement nouveau. La prolifération de la guerre hybride est encouragée par «l'émergence de nouveaux acteurs sous-étatiques, de nouveaux types d'armes et d'une nouvelle représentation idéologique»²⁶. D'autres chercheurs considèrent que la notion de guerre hybride est une simple appellation et que les caractéristiques présentées comme nouvelles pouvaient déjà être observées par le passé dans les pratiques des États et des acteurs non étatiques. De plus, ces spécialistes estiment que le terme de «guerre» prête à confusion dans ce contexte. Néanmoins, il est généralement admis qu'il y a aujourd'hui, outre les actes de guerre classiques, une prédominance d'actions asymétriques, non conventionnelles et hybrides, qui sont souvent le fait d'acteurs non étatiques²⁷. D'ailleurs, les experts qui ont participé à l'audition qui s'est tenue devant la commission en novembre 2017 ont souligné que la guerre hybride est une notion plus politique que juridique et que l'asymétrie est sa principale caractéristique. Un de ces experts, M. Robin Geiß, a expliqué qu'il existe de nombreuses définitions de la guerre hybride et que chacune d'elles renvoie, au fond, à un «usage inattendu et peu orthodoxe de tactiques de subversion». Un autre, M. Aurel Sari, a affirmé que la définition des «menaces que représente la guerre hybride», qui figure dans la [Déclaration du sommet du Pays de Galles](#) publiée à la réunion du Conseil de l'Atlantique Nord en septembre 2014, insiste à juste titre sur le fait qu'il s'agit d'un «large éventail de mesures militaires, paramilitaires ou civiles, dissimulées ou non» qui sont mises en œuvre «de façon très intégrée». Cet expert privilégie la notion d'«adversaire hybride» qui vise à créer cette asymétrie en exploitant les seuils légaux, la complexité et l'incertitude, en créant une ambiguïté juridique, en violant ses obligations légales et en utilisant le droit pour appuyer son discours stratégique et son contre-discours. Toutes ces actions visent à créer un environnement juridique qui favorise ses propres opérations au détriment de celles de sa cible. Cette définition met l'accent sur l'utilisation du droit comme instrument de guerre et sur ses aspects aussi bien défensifs qu'offensifs.

16. Il est intéressant de constater que, selon M. Sari, le fait d'exclure l'usage de la force armée de la définition des «menaces hybrides» «réduit l'hybridité à un vague synonyme de la complexité». La notion de «menaces hybrides» devrait être réservée aux situations dans lesquelles les États ou les acteurs non étatiques emploient des moyens de guerre non violents comme instruments de guerre, en les intégrant à

23. A. Sari, voir note n° 11, p. 15. Néanmoins, officiellement, l'OTAN utilise largement le terme de «menaces» hybrides dans ses déclarations ainsi que dans ses travaux de recherche connexes. Voir [NATO Countering the hybrid threat](#), site internet de l'OTAN, ou Guillaume Lasconjarias et Jeffrey A. Larsen, *NATO's Response to Hybrid-Threats*, NATO Defence College, NDC Forum Papers Series, Rome, 2015.

24. Voir le rapport de M. Andreas Gross (Suisse, SOC), «Refuser l'impunité pour les meurtriers de Sergueï Magnitski», [Doc. 13356](#), paragraphe 171.

25. Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Warfare*, Potomac Institute for Policy Studies, Arlington, Virginia, décembre 2007, p. 8.

26. François-Bernard Huyghe, «The impurity of war», *International Review of the Red Cross*, Vol. 91/873, mars 2009.

27. Voir B. Renz et H. Smith, note 12 ci-dessus, et Christian Bahnareanu, note 14 ci-dessus, p. 57-66.

l'usage de la force armée ou à la menace du recours à la force. Les spécialistes n'ont pas montré beaucoup d'intérêt pour les aspects juridiques de la guerre hybride, car la plupart des problèmes juridiques liés à cette notion – violation de l'intégrité territoriale, soutien aux mouvements séparatistes ou non-respect des accords internationaux – ne sont pas nouveaux. L'ampleur et la fluidité de cette notion ne facilitent pas son appréciation juridique²⁸.

17. Bien que la notion de menaces hybrides soit qualifiée de concept «fourre-tout», il n'existe pas de définition universellement admise et certaines différences conceptuelles peuvent être observées. M. Geiß affirme qu'il n'est pas nécessaire de définir la guerre hybride, car la définition actuelle de la «guerre» est suffisante, mais qu'il convient de préciser en quoi consistent les menaces hybrides. Juridiquement, l'expression «guerre hybride», qui est de nature politique, désigne un conflit armé dans lequel sont utilisées des techniques militaires conventionnelles (mais pas uniquement). J'utiliserai ce terme dans ce sens. Les autres termes – «menaces hybrides» ou «conflits hybrides» – sont utilisés pour d'autres moyens «hybrides» – non militaires – de conflit. Sur la base de cette définition, je n'utiliserai donc que le terme «menaces hybrides».

2.2. Le cadre juridique applicable

2.2.1. La guerre hybride

18. En droit international, le recours à la force par les États est réglementé par le droit de faire la guerre ou *jus ad bellum*. L'article 2 de la Charte des Nations Unies interdit de recourir à la menace ou à l'emploi de la force, «soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies» (paragraphe 4) et réaffirme le principe de la non-intervention dans des affaires qui relèvent essentiellement de la compétence nationale d'un État (paragraphe 7). L'article 51 de la Charte prévoit une exception au principe énoncé à l'article 2.4: les États ont le droit naturel de légitime défense, individuelle ou collective, en cas d'agression armée²⁹. La Résolution 2625 de l'Assemblée générale des Nations Unies (25 octobre 1970) réaffirme l'interdiction de la menace ou de l'usage de la force et le principe de non-intervention. Elle souligne également que «les États ont le devoir de s'abstenir de toute propagande en faveur des guerres d'agression».

19. Le droit de légitime défense, qui est bien établi en droit international coutumier, naît d'une attaque armée. Si l'intensité des opérations d'un adversaire hybride n'atteint pas le niveau nécessaire ou se limite à la menace du recours à la force, le droit de riposter en utilisant la force en légitime défense ne peut être invoqué. Dans l'affaire *Nicaragua c. États-Unis*, la Cour internationale de justice (CIJ) a réaffirmé que le droit de légitime défense ne peut être exercé qu'en réponse à une «attaque armée» (interprétation à la lumière de l'article 3(g) de la définition de l'agression jointe en annexe à la Résolution 3314 (XXIX) de l'Assemblée générale des Nations Unies de 1974). La CIJ a estimé, notamment, qu'une assistance dispensée à des rebelles sous la forme de fourniture d'armes ou d'assistance logistique ou autre ne relevait pas de ce droit; elle précise cependant que l'on peut voir «dans une telle assistance une menace ou un emploi de la force, ou l'équivalent d'une intervention dans les affaires intérieures ou extérieures d'autres États³⁰». Or cette interprétation crée un vide juridique entre l'usage de la force et une attaque armée, vide qui n'est pas pris en compte par les États-Unis, qui considèrent que tout recours à la force donne, en principe, le droit de légitime défense. Ils ont donc, tout en luttant contre le terrorisme, élargi à l'excès la notion de «guerre», tant sur le plan géographique que temporel.

20. Un autre problème se pose avec les attaques armées lancées par des acteurs non étatiques. Bien que la pratique internationale ait reconnu que le droit de légitime défense s'étendait à de telles attaques, la CIJ a déclaré que ce droit ne devait pas être utilisé si l'attaque trouve son origine à l'intérieur et non en dehors du territoire de la cible (puisque cela mettrait en jeu l'intégrité territoriale de l'autre État)³¹. Cela signifie que si un État recrute des groupes non étatiques pour mener une guerre par procuration, il sera plus difficile pour l'État visé d'attribuer les actes de violence à son adversaire³².

28. A. Sari, voir note 11 ci-dessus, p. 16 et 18.

29. La deuxième exception figure à l'article 42 de la Charte des Nations Unies, qui autorise le Conseil de sécurité à prendre des mesures militaires pour maintenir ou rétablir la paix et la sécurité internationales.

30. CIJ, arrêt du 27 juin 1986, paragraphe 195: «(...) par agression armée il faut entendre non seulement l'action des forces armées régulières à travers une frontière internationale» mais encore «l'envoi par un État ou en son nom de bandes ou de groupes armés, de forces irrégulières ou de mercenaires qui se livrent à des actes de force armée contre un autre État d'une gravité telle qu'ils équivalent» (entre autres) à une véritable agression armée accomplie par des forces régulières, «ou [au] fait de s'engager d'une manière substantielle dans une telle action».

21. Le *jus in bello* (ou droit international humanitaire) énonce des principes sur la façon dont les opérations peuvent être menées pendant un conflit armé. Les conflits armés sont réglementés non seulement par les [conventions de Genève](#) de 1949 (qui visent à protéger les personnes ne participant pas aux hostilités) mais aussi par les normes du droit international coutumier. Ces conventions mentionnent encore le terme «guerre», mais il a été largement remplacé par le terme «conflit armé» dans la doctrine du droit international et les instruments juridiques (voir, en particulier, [la Convention de La Haye de 1954 pour la protection des biens culturels en cas de conflit armé et ses deux Protocoles de 1954 et 1999](#)).

22. Un conflit armé peut présenter un caractère international (CAI) ou non international (CANI). Le CAI est défini dans l'article 2 commun aux [conventions de Genève](#) et dans l'[article 1, section 4, du protocole additionnel I](#), tandis que le CANI est défini dans l'article 3 commun et dans l'[article 1, section 1 du protocole additionnel II](#). L'article 2 commun aux conventions de Genève dispose qu'un CAI est une «guerre déclarée ou (...) tout autre conflit armé surgissant entre deux ou plusieurs des Hautes Parties contractantes». L'article 3 commun aux conventions de Genève s'applique «en cas de conflit armé ne présentant pas un caractère international et surgissant sur le territoire de l'une des Hautes Parties contractantes» (CANI). Il est généralement admis que deux conditions doivent être remplies: 1) un niveau minimum d'intensité, ce qui signifie que les hostilités doivent avoir un «caractère collectif» ou que le gouvernement doit avoir recours à la force militaire plutôt qu'aux forces de police; et 2) les groupes non gouvernementaux doivent être des «parties au conflit». Plus précisément, les groupes doivent être organisés, avoir une structure de commandement et mener des opérations militaires³³.

23. Si une guerre hybride est considérée comme un CAI, les questions d'attribution découlant du droit international humanitaire et des droits de l'homme sont plus simples. Le seuil d'applicabilité du droit des conflits armés internationaux étant bas, l'adversaire hybride peut nier sa participation à un conflit armé ou éviter de participer directement aux opérations de combat. Si les hostilités sont inévitables, il est dans l'intérêt de l'adversaire d'utiliser des tactiques hybrides et de mandater des groupes non étatiques afin de dissimuler sa propre implication. Dans ce cas, c'est le droit des conflits armés non internationaux, moins contraignant, qui s'applique. La pratique montre que les États hésitent généralement à reconnaître l'existence d'un CANI, ce qui affaiblit encore plus la position de l'État cible et signifie que le conflit doit être traité comme un conflit interne.

24. De nos jours, les guerres officiellement déclarées sont rares dans les relations internationales. Cependant, ni une déclaration officielle de guerre ni la reconnaissance officielle d'un état de guerre ne sont nécessaires pour que le droit humanitaire international s'applique (voir, par exemple, les articles 2 et 3 de la [IVe Convention de Genève](#)). Il est intéressant de noter que les États n'ont plus le monopole de la violence, que le nombre de conflits entre États a diminué, mais que le nombre de conflits armés non internationaux (CANI) a considérablement augmenté. De nombreux CANI ont pris une dimension internationale parce que d'autres États sont intervenus en faveur d'une ou de plusieurs des parties belligérantes. Les progrès technologiques ont rendu les conflits actuels plus asymétriques.

25. En cas de conflit armé, notamment de guerre hybride, le droit international humanitaire et le droit international des droits de l'homme s'appliquent. La Cour européenne des droits de l'homme a précisé que, dans des circonstances exceptionnelles, la Convention peut être appliquée de manière extraterritoriale, en particulier dans les cas de conflits armés qui surviennent en dehors de la zone géographique du Conseil de l'Europe³⁴. Cependant, l'application du droit international des droits de l'homme est limitée par le droit international humanitaire, qui fonctionne comme des dispositions particulières (*lex specialis*)³⁵. Conformément à la jurisprudence de la CIJ, la Cour a considéré dans l'affaire *Hassan c. Royaume-Uni* que «même en cas de conflit armé international, les garanties énoncées dans la Convention continuent de

31. CIJ, [Conséquences juridiques de l'édification d'un mur dans le territoire palestinien occupé](#), Avis consultatif du 9 juillet 2004, paragraphe 139.

32. A. Sari, note 11 ci-dessus, p. 25.

33. Comité international de la Croix-Rouge (CICR), [Comment le terme «conflit armé» est-il défini dans le droit international humanitaire?](#) Prise de position, mars 2008, p. 3. En outre, l'article 1, section 1, du Protocole additionnel II aux Conventions de Genève définit les conflits armés internationaux (plus étroitement) comme des conflits «(...) qui se déroulent sur le territoire d'une Haute Partie contractante entre ses forces armées et des forces armées dissidentes ou des groupes armés organisés qui, sous la conduite d'un commandement responsable, exercent sur une partie de son territoire un contrôle tel qu'il leur permette de mener des opérations militaires continues et concertées et d'appliquer le présent Protocole».

34. Voir les affaires concernant les opérations militaires internationales en Irak: *Al-Sadoon et Mufdhi c. Royaume-Uni*, Requête n° 61498/08, arrêt du 2 mars 2010; *Al-Skeini et autres c. Royaume-Uni*, Requête n° 61498/08, et *Al-Jedda c. Royaume-Uni*, Requête n° 55721/07, arrêt du 7 juillet 2011 (Grande Chambre). Voir aussi une affaire concernant l'intervention de soldats turcs en Iran: *Pad et autres c. Turquie*, Requête n° 60167/00, arrêt du 28 juin 2007.

s'appliquer, quoiqu'en étant interprétées à l'aune des règles du droit international humanitaire³⁶». En cas de violation de ce droit, les États sont tenus de poursuivre les auteurs présumés au titre du droit interne. Divers tribunaux pénaux internationaux peuvent également engager des poursuites contre les auteurs de ces violations. Cependant, M. Kozik a expliqué lors de l'audition de novembre 2017 que le droit international humanitaire comporte des lacunes et que le mécanisme visant à le faire respecter disposait de faibles moyens.

2.2.2. Les menaces hybrides

26. En cas de «menaces hybrides», qui ne couvrent pas les actions militaires relevant du droit international humanitaire, les États devraient en général recourir au droit pénal interne (notamment aux dispositions sur les crimes terroristes) et au cadre juridique relatif aux droits de l'homme. Ils peuvent également s'appuyer, en fonction du type de menace, sur un éventail d'instruments juridiques internationaux visant des domaines d'action particuliers (tels que le droit de la mer, la lutte contre le terrorisme, le discours de haine, le blanchiment de capitaux et le financement du terrorisme).

27. En cas d'actes hostiles non militaires à grande échelle, par exemple les campagnes de désinformation, il est possible d'invoquer l'article 17 de la Convention européenne des droits de l'homme, qui interdit la violation des droits garantis par la Convention. M. Kozik a souligné qu'un État partie peut, par conséquent, saisir la Cour européenne des droits de l'homme afin d'engager une action contre un autre État Partie au titre de l'article 33 de la Convention, mais il a précisé que l'article 33 ne s'appliquait pas aux groupes non étatiques employés par des adversaires utilisant des tactiques hybrides.

28. Concernant les cyberattaques, l'application du droit en vigueur dans le cyberspace est assez floue, tout comme la riposte que les États doivent opposer à des cyberattaques pour lesquelles il n'existe même pas de définition uniformément admise³⁷. En 2013, le Groupe d'experts gouvernementaux des Nations Unies a publié un rapport dans lequel il déclarait que le droit international s'appliquait au cyberspace. Deux ans plus tard, il publiait un [rapport de consensus](#) sur les normes, règles ou principes du comportement responsable des États dans le cyberspace, y compris un engagement en faveur de «la non-intervention dans les affaires intérieures des autres États»³⁸. La [Convention sur la cybercriminalité](#) du Conseil de l'Europe de 2001 (STE n° 185) est le seul instrument international contraignant dans ce domaine. Également ouverte aux États non membres, elle sert de ligne directrice à tout pays qui élabore une législation nationale complète contre la cybercriminalité et de cadre à la coopération internationale.

29. Le Manuel de Tallinn 2.0 sur le droit international applicable aux cyber-opérations ([Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations](#)) a été publié en février 2017. Cette publication, rédigée par un groupe de 19 experts en droit international sous les auspices du Centre d'excellence de l'OTAN pour la cyberdéfense en coopération (dont le siège se trouve à Tallinn, Estonie), est une initiative dépourvue de caractère contraignant prise en vue de codifier l'application du droit international au cyberspace. Il convient cependant de noter que le manuel représente le point de vue de ses auteurs (et non la position officielle de l'OTAN) et que les experts ne sont pas parvenus à se mettre d'accord sur la façon dont le droit international s'applique à des situations précises (par exemple, les cyberattaques russes qui auraient été lancées en 2016 contre des serveurs du Comité national démocrate aux États-Unis). À cet égard, M. Kozik a souligné lors de l'audition de novembre 2017 que le droit international humanitaire interdit les attaques directes contre les populations civiles et les objectifs civils mais que son application n'exclut pas tous les types de cyberactions visant ces populations et objectifs. La majorité des auteurs du Manuel 2.0 de Tallinn étaient d'avis qu'il fallait qu'une cyberagression cause au moins des dommages fonctionnels (par exemple une panne d'électricité) pour qu'elle soit considérée comme une «attaque» au sens du droit international humanitaire. Le Comité international de la Croix-Rouge (CICR) estime que la définition de «l'attaque» donnée par le droit international humanitaire s'applique aux cyberattaques, mais cette opinion fait des controverses parmi les juristes internationaux³⁹. En outre, il n'est pas facile de savoir dans quelles situations un État peut

35. CIJ, *Licéité de la menace ou de l'emploi d'armes nucléaires*, Avis consultatif, 8 juillet 1996, Recueil des arrêts de la CIJ, 1996, paragraphe 25. Voir également Noam Lubell, «Challenges in applying human rights law to armed conflict», *International review of the Red Cross*, vol. 87/860, décembre 2005.

36. Cour européenne des droits de l'homme, *Hassan c. Royaume-Uni*, Requête n° 29750/09, arrêt du 16 septembre 2014, paragraphes 102-103.

37. Bruce H. McClintock, [Russian Information Warfare: A Reality That Needs a Response](#), 21 juillet, 2017. Par attaque contre des réseaux informatiques (cyberattaques), le CICR, par exemple, entend toute opération hostile lancée contre un ennemi pour «obtenir, altérer, détruire, perturber ou transférer des données stockées sur un ordinateur, traitées par un ordinateur ou transmises au moyen d'un ordinateur»; voir: <https://www.icrc.org/fr/document/cyber-warfare>.

38. Nations Unies, Rapports du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale, A/68/98, 24 juin 2013, et A/70/174, 22 juillet 2015.

invoquer le droit de légitime défense en cas de cyberattaque. Les États doivent être au moins autorisés à prendre toutes les mesures proportionnées nécessaires pour éviter les conséquences préjudiciables continues ou imminentes d'une cyberattaque.

2.3. Les vides juridiques et les solutions possibles

30. En masquant son implication indirecte dans le conflit, en utilisant des groupes armés non étatiques pour faire usage de la force et en menant ses opérations à un niveau d'intensité qui contourne les seuils légaux applicables, un adversaire hybride peut employer des forces armées contre un autre État tout en empêchant celui-ci d'assurer sa propre défense, ce qui crée une asymétrie juridique. L'utilisation du droit pour justifier une guerre n'est pas une nouveauté (par exemple, l'invasion japonaise de la Mandchourie en 1931 présente de nombreuses similitudes avec l'annexion russe de la Crimée en 2014). Pour M. Sari, trois tâches (qui n'ont pas été examinées jusqu'ici par l'OTAN et l'Union européenne) doivent être réalisées pour relever ces défis juridiques: 1) élaborer une définition de la dynamique juridique des menaces hybrides; 2) comprendre les vulnérabilités juridiques; et 3) renforcer la capacité de préparation, de dissuasion et de défense dans le domaine juridique⁴⁰.

31. En ce qui concerne la première proposition, il convient de souligner que l'asymétrie juridique est une caractéristique propre à la guerre hybride. S'agissant des vulnérabilités et des défis juridiques, il est bon de rappeler que, face à des actes qui sont assimilables à une attaque armée, l'État visé peut recourir à la force au titre de la légitime défense. Il est clair que le Conseil de l'Europe n'a aucune compétence dans ce domaine puisque les «questions de défense nationale» sont exclues du champ d'application de ses activités sur la base de l'article 1.d de son [Statut](#) (STE n° 1). Il ne serait pas inutile, cependant, de se pencher sur les moyens légaux dont disposent, en cas d'attaque armée, les nombreux États membres de notre Organisation qui sont membres de l'OTAN et/ou de l'Union européenne.

32. Toute attaque armée contre un membre de l'OTAN déclenche l'article 5 du [Traité de l'Atlantique Nord](#), qui permet une réponse collective. Cette disposition s'étend également aux attaques terroristes dirigées contre un pays allié depuis l'étranger⁴¹. Les menaces hybrides qui n'atteignent pas le seuil d'une attaque armée peuvent être traitées sous l'angle de l'article 4 du Traité de l'Atlantique Nord, qui prévoit que les membres de l'OTAN peuvent se consulter lorsque l'intégrité territoriale, l'indépendance politique ou la sécurité de l'un d'entre eux est menacée. En général, les États doivent être capables de contrer les menaces hybrides en recourant à des contre-mesures proportionnées (représailles).

33. Dans l'Union européenne, l'article 42, paragraphes 1 et 2, du [Traité sur l'Union européenne](#) (TUE) précise que «la politique de sécurité et de défense commune fait partie intégrante de la politique étrangère et de sécurité commune» et «inclut la définition progressive d'une politique de défense commune de l'Union» (dont la mise en place est soumise à une décision du Conseil européen). L'article 42.6 du TUE permet aux États membres dont les capacités militaires satisfont à des critères plus exigeants d'établir une coopération structurée permanente (PESCO). Cette coopération permanente a été établie par [une décision du Conseil de l'Union européenne du 8 décembre 2017](#). En outre, l'article 42.7 du TUE comporte une clause d'assistance mutuelle en cas d'agression armée, mais sa portée reste floue.

34. Il serait bon que l'OTAN et l'Union européenne travaillent en étroite collaboration pour trouver une définition commune de la dynamique juridique des menaces hybrides et parvenir à une conception commune des vulnérabilités juridiques et des problèmes qui en découlent, notamment l'asymétrie juridique créée par l'utilisation de tactiques hybrides, les défis à relever sur le plan du droit international, ainsi que la répartition institutionnelle des travaux menés en vue de contrer les menaces hybrides. Il faudrait également que les deux organisations renforcent leurs capacités de préparation, de dissuasion et de défense dans le domaine juridique. Notons qu'elles ont déjà commencé à prendre des mesures pour riposter aux menaces hybrides⁴². En avril 2017, par exemple, ces deux organisations ont créé [le Centre européen d'excellence pour la lutte contre les menaces hybrides](#), un groupe de réflexion intergouvernemental basé à Helsinki, composé de 13 États membres et des représentants de l'Union européenne et de l'OTAN.

39. <https://www.icrc.org/en/document/cyber-warfare> et https://ccdcoe.org/cycon/2012/proceedings/d3r1s1_schmitt.pdf.

40. A. Sari, voir note 11 ci-dessus, p. 26-27.

41. OTAN, [communiqué de presse \(2001\) 124](#) du 12 septembre 2001.

42. Pour de plus amples informations, voir: EPRS, [Countering hybrid threats: EU-NATO cooperation](#), Briefing, mai 2017.

3. Dans quelle mesure les menaces hybrides peuvent-elles justifier des restrictions aux droits de l'homme?

35. Pour contrer les menaces hybrides (en particulier les guerres hybrides), les États Parties à la Convention européenne des droits de l'homme peuvent se référer à son article 15.1, qui permet aux États Parties de prendre des mesures dérogeant aux obligations prévues par la Convention, «en cas de guerre ou en cas d'autre danger public menaçant la vie de la nation». Une telle dérogation devrait être faite «dans la stricte mesure où la situation l'exige» et ne devrait pas être en contradiction avec les autres obligations découlant du droit international. Les États ne peuvent pas déroger à certains droits: le droit à la vie (sauf pour les décès résultant d'actes licites de guerre), l'interdiction de la torture et des peines ou traitements inhumains ou dégradants, l'interdiction de l'esclavage et du travail forcé, le principe «pas de peine sans loi», l'interdiction de la peine de mort et le droit de ne pas être jugé ou puni deux fois pour une même infraction. L'État qui déroge à la Convention doit en informer le Secrétaire Général du Conseil de l'Europe. Dans l'affaire *Hassan c. Royaume-Uni*⁴³, la Cour européenne des droits de l'homme a estimé qu'une dérogation formelle au titre de l'article 15 de la Convention n'est peut-être pas nécessaire lorsque le droit international humanitaire s'applique, car la Convention doit être interprétée conformément à d'autres dispositions du droit international, notamment le droit international humanitaire. Récemment, la France, l'Ukraine et la Turquie ont déposé des dérogations au titre de l'article 15 de la Convention⁴⁴.

36. Les États invoquent généralement la «sécurité nationale» lorsqu'ils luttent contre les menaces hybrides. En vertu de la Convention, la sécurité nationale (ainsi que, notamment la «sûreté publique» et la «défense de l'ordre et la prévention du crime») est considérée comme un «but légitime» permettant aux États de limiter certains droits: le droit au respect de la vie privée et familiale, la liberté d'expression et la liberté de réunion et d'association (voir le paragraphe 2 des articles 8, 10 et 11 de la Convention) ainsi que la liberté de circulation (article 2.3 du Protocole n° 4 à la Convention (STE n° 46)), ce droit pouvant également être restreint pour des questions de «maintien de l'ordre public»). En outre, elle peut justifier l'expulsion d'un étranger résidant légalement sur le territoire d'un État sans respecter les garanties procédurales (article 1.2 du Protocole n° 7 à la Convention (STE n° 117)). «L'intégrité territoriale» constitue un autre but légitime de restriction de la liberté d'expression. Toute restriction à ces droits doit être «prévue par la loi», «nécessaire dans une société démocratique» et proportionnée. Une garantie supplémentaire contre les abus est prévue à l'article 18 de la Convention, qui énonce que les restrictions permises par la Convention «ne peuvent être appliquées que dans le but pour lequel elles ont été prévues».

37. La Cour européenne des droits de l'homme a examiné de nombreuses affaires dans lesquelles des États ont invoqué la «sécurité nationale» pour restreindre certains droits de l'homme. Le terme en question n'est pas clairement défini et reste vague étant donné la marge d'appréciation dont les États disposent. La Cour lui a donné un certain poids en l'appliquant à des affaires concernant la protection de la sécurité de l'État et de la démocratie constitutionnelle contre l'espionnage, le terrorisme, le soutien au terrorisme, le séparatisme et l'incitation à la violation des obligations militaires. À l'heure actuelle, elle demande généralement aux organismes nationaux de vérifier que toute menace invoquée a un fondement raisonnable et d'évaluer soigneusement la qualité de la loi, la nécessité de l'ingérence ou sa proportionnalité par rapport à la menace pesant sur la «sécurité nationale». Je citerai ci-dessous quelques exemples pertinents de la jurisprudence de la Cour au sujet des articles 8, 10 et 11 de la Convention⁴⁵.

38. La surveillance secrète est l'un des principaux cas pour lesquels la «sécurité nationale» a été invoquée. La Cour considère que la législation sur laquelle cette ingérence se fonde doit non seulement être «accessible» et «prévisible», mais encore suffisamment détaillée. Elle souligne que les États doivent démontrer l'existence de garanties adéquates et efficaces contre les abus et que l'intérêt des États à protéger leur sécurité nationale doit être mis en balance avec la gravité de l'atteinte aux droits consacrés à l'article 8 de la Convention. Dans l'affaire *Roman Zakharov c. Russie*, qui concerne la surveillance générale des communications téléphoniques sur le fondement de la loi antiterroriste, la Cour a relevé des lacunes dans le cadre juridique et a estimé «qu'un système de surveillance secrète destiné à protéger la sécurité nationale risque de saper, voire de détruire, la démocratie au motif de la défendre» (violation de l'article 8 de la Convention)⁴⁶. Il est intéressant de noter que la Cour examine actuellement un certain nombre d'affaires

43. *Hassan c. Royaume-Uni*, *op. cit.*, paragraphes 102-103.

44. Voir [Doc. 14506](#), rapport «État d'urgence: questions de proportionnalité relatives à la dérogation prévue à l'article 15 de la Convention européenne des droits de l'homme» (rapporteur: M. Raphaël Comte, Suisse, ADLE).

45. Cour européenne des droits de l'homme, rapport de la Division de la recherche: [Sécurité nationale et jurisprudence de la Cour européenne des droits de l'homme](#), p. 5.

46. *Roman Zakharov c. Russie*, Requête n° 47143/06, arrêt du 4 décembre 2015 (Grande Chambre), paragraphe 232.

concernant l'interception massive de communications externes par les services de renseignement britanniques et le partage de renseignements entre le Royaume-Uni et les États-Unis telles que révélées par Edward Snowden⁴⁷.

39. S'agissant de la liberté d'expression, la jurisprudence de la Cour montre que cette juridiction a tendance à ne pas conclure à des violations de l'article 10 dans les affaires concernant l'interdiction des incitations manifestes et sans équivoque à la violence. Le droit à la liberté d'expression n'est pas un droit d'incitation à la violence⁴⁸. La Cour a même tendance, au titre de l'article 17 de la Convention, à exclure de sa protection les commentaires qui peuvent être assimilés à un discours de haine et à une négation des valeurs fondamentales de la Convention⁴⁹. Récemment, la Cour a également reconnu l'importance d'internet lorsque des individus exercent leur droit à la liberté de recevoir et de communiquer des informations et a examiné les mesures qui bloquent l'accès à ce réseau. Dans les affaires *Ahmet Yildirim c. Turquie* (portant sur une décision d'un tribunal de bloquer l'accès à Google Sites) et *Cengiz et autres c. Turquie* (concernant le blocage général de l'accès à YouTube), elle a constaté des violations de l'article 10 de la Convention⁵⁰. La Cour n'a pas, cependant, étudié la question de la «sécurité nationale» dans ces deux affaires, car elle a jugé que les restrictions n'étaient pas «prévues par la loi» et n'a pas examiné d'autres critères découlant du deuxième paragraphe de l'article 10.

40. Dans l'affaire *Stankov et Organisation macédonienne unie Ilinden c. Bulgarie* concernant l'interdiction de rassemblements organisés par l'association requérante visant à «la reconnaissance de la minorité macédonienne en Bulgarie», les autorités ont invoqué, entre autres, la sécurité nationale pour justifier la mesure contestée. Or, selon la Cour européenne des droits de l'homme, «exiger des changements territoriaux dans des discours et manifestations ne s'analyse pas automatiquement en une menace pour l'intégrité territoriale et la sécurité nationale du pays»⁵¹. La Cour a jugé que les preuves d'une incitation généralisée à la violence ou d'un rejet des principes démocratiques étaient rares et a estimé qu'il était tout aussi important de sauvegarder les institutions et pratiques démocratiques que de répondre aux préoccupations de sécurité nationale (violation de l'article 11 de la Convention).

41. Dans un document thématique intitulé «La prééminence du droit sur l'internet et dans le monde numérique en général», le Commissaire aux droits de l'homme du Conseil de l'Europe a conclu que «les États qui veulent poser des limites aux droits fondamentaux sur la base d'une menace supposée contre la sécurité nationale doivent apporter la preuve que la menace en question ne peut être contrée au moyen du droit pénal commun, notamment par des lois spéciales de lutte contre le terrorisme qui restent dans les limites admises du droit pénal et de procédure pénale applicables et qui satisfont aux normes internationales en matière de droit pénal et de procédure pénale». Cette obligation s'applique également aux mesures prises par les États en lien avec internet et les communications électroniques. Le non-respect de celle-ci «porte atteinte à la prééminence du droit international»⁵².

4. Conclusion

42. Le phénomène des «menaces hybrides» exige une attention particulière. Bien que ce terme soit largement utilisé, ses conséquences sur le plan juridique sont moins bien comprises. Or, de ce point de vue, ce n'est pas tant la définition de ce phénomène qui importe le plus, mais l'application des normes du droit international telles que l'interdiction du recours à la force, le droit international humanitaire et le droit des droits de l'homme. Il n'existe pas de «droit de la guerre hybride», mais on compte plusieurs définitions de la guerre hybride. La plupart des experts conviennent que la principale caractéristique de ce phénomène est son asymétrie juridique. Les adversaires hybrides exploitent les lacunes du droit et la complexité de la législation, agissent par-delà les frontières législatives et dans les espaces sous-réglementés, exploitent les seuils légaux qui limitent les ripostes et sont prêts à commettre de graves violations du droit en profitant de l'ambiguïté du

47. *Big Brother Watch et autres c. Royaume-Uni*, Requête n° 58170/13; *Bureau of Investigative Journalism et Alice Ross c. Royaume-Uni*, Requête n° 62322/14, et *10 organisations de défense des droits de l'homme et autres c. Royaume-Uni*, Requête n° 24960/15.

48. *Zana c. Turquie*, Requête n° 18954/91, arrêt du 25 novembre 1997, paragraphe 60.

49. Voir, par exemple, *Seurot c. France*, Requête n° 57383/00, décision sur la recevabilité du 18 mai 2004.

50. *Ahmet Yildirim c. Turquie*, Requête n° 311/10, arrêt du 18 décembre 2012, et *Cengiz et autres c. Turquie*, Requêtes n°s 48226/10 et 14017/11, arrêt du 1^{er} décembre 2015.

51. *Affaire Stankov et Organisation macédonienne unie Ilinden c. Bulgarie*, Requêtes n°s 29221/95 et 29225/95, arrêt du 2 octobre 2001, paragraphe 97.

52. Conseil de l'Europe, Commissaire aux droits de l'homme, *The rule of law on the Internet and in the wider digital world, Issue Paper*, décembre 2014, p. 108. [En français: La prééminence du droit sur l'internet et dans le monde numérique en général, Document thématique publié par le Commissaire aux droits de l'homme du Conseil de l'Europe.]

droit et des faits. Ils nient leurs opérations hybrides, afin de créer une zone grise du droit à l'intérieur de laquelle ils peuvent agir librement. Parvenir à réglementer la guerre hybride est un défi, car l'une des parties cherche systématiquement à se soustraire à ses responsabilités légales.

43. Les inquiétudes des États à l'égard des menaces hybrides qui pèsent sur leur sécurité nationale sont légitimes, notamment parce que ces menaces peuvent porter atteinte au cœur même de nos sociétés démocratiques d'une manière sans équivalent. Comme l'utilisation du large éventail de moyens hybrides disponibles pour mener un conflit ne fait l'objet d'aucune limitation internationalement reconnue, les États tentent de contrer ces nouvelles menaces à l'aide du droit pénal interne. Certaines mesures internes prises pour faire face à des menaces hybrides peuvent à leur tour porter atteinte aux droits fondamentaux. Si les menaces hybrides sont considérées comme un nouveau type de danger, il n'en reste pas moins que la Convention européenne des droits de l'homme continue de s'appliquer et que la jurisprudence de la Cour européenne des droits de l'homme répond aux questions soulevées par ces nouveaux phénomènes. Les craintes que peut soulever la lutte contre les menaces hybrides en matière de droits de l'homme peuvent être atténuées en adoptant l'approche retenue pour les mesures antiterroristes. Les ripostes des États aux menaces hybrides devraient être légales et proportionnées. En cas de doute, les États peuvent toujours demander l'expertise de la Commission européenne pour la démocratie par le droit (Commission de Venise) sur des projets de loi spécifiques. En ce qui concerne la liberté d'expression, certaines restrictions visant à contrôler le contenu des informations peuvent être imposées (en particulier pour lutter contre le discours de haine), mais elles ne devraient pas être discriminatoires ni entraîner une censure générale. D'autres difficultés doivent être surmontées. Il n'est pas toujours possible, par exemple, d'identifier l'adversaire hybride et d'attribuer la responsabilité des menaces hybrides à un État précis. De plus, des phénomènes tels que les campagnes de désinformation peuvent créer un conflit entre certains droits de l'homme et certaines libertés fondamentales, comme la liberté d'expression, le droit à l'information et le droit à des élections libres (garanti par l'article 3 du Protocole n° 1 à la Convention (STE n° 9)).

44. Toute riposte aux menaces hybrides devrait recourir à des moyens légaux, de contre-espionnage, diplomatiques et militaires. Bien qu'il ne soit pas compétent en matière de défense, il importe que le Conseil de l'Europe participe à l'élaboration de réponses juridiques, en apportant son expertise dans le domaine des droits de l'homme et en s'appuyant sur l'expérience de l'Union européenne et de l'OTAN en matière de défense. Si les menaces hybrides et certaines mesures prises en réaction constituent un danger pour les droits fondamentaux, la «zone grise» juridique qui entoure actuellement ces nouvelles menaces met aussi en danger la coopération juridique fondée sur la confiance mutuelle et la compréhension commune des règles applicables. Le recours aux menaces hybrides peut également avoir des conséquences juridiques sur le statut de certains groupes de personnes, notamment ceux qui appartiennent à des minorités nationales.

45. Pour contrer les menaces hybrides, les États pourraient s'appuyer sur l'expérience qu'ils ont acquise dans la lutte contre le terrorisme. Les institutions internationales et les services de répression nationaux se sont beaucoup investis dans la lutte contre la menace terroriste et sont particulièrement conscients de la nature transnationale et évolutive des acteurs non étatiques, qui transparaît dans les traités internationaux (comme la [Convention du Conseil de l'Europe pour la prévention du terrorisme](#) (STCE n° 196)) et le droit pénal national en matière de lutte contre le terrorisme. Le Conseil de l'Europe a élaboré un cadre général, qui vise à promouvoir et à protéger les droits fondamentaux dans la lutte contre le terrorisme⁵³. Ce cadre pourrait servir de modèle pour contrer les menaces hybrides, en respectant pleinement les droits de l'homme. En outre, le Conseil de l'Europe devrait encourager les États membres et non membres qui ne l'ont pas encore fait à ratifier la Convention sur la cybercriminalité et entamer une réflexion sur son application et son éventuelle amélioration.

53. Voir, par exemple, les Résolutions de l'Assemblée 2045 (2015) «Les opérations de surveillance massive» ou 2090 (2016) «Combattre le terrorisme international tout en protégeant les normes et les valeurs du Conseil de l'Europe». Pour un examen plus complet, voir: <https://www.coe.int/fr/web/counter-terrorism/codexter>.