L'OTAN face aux conflits contemporains : enjeux opérationnels et juridiques de l'implication des acteurs privés

Angèle Billaud

Analyste en droit international, sécurité internationale, cybersécurité et défense, diplômée de l'Université Grenoble Alpes, France.

19 janvier 2026

ISSN : 2739-3283

Comment citer cette publication :

Angèle Billaud, *L'OTAN face aux conflits contemporains : enjeux opérationnels et juridiques de l'implication des acteurs privés,* Institut d'études de géopolitique appliquée, Paris, 19 janvier 2026.

66 avenue des Champs-Élysées, 75008 Paris
Courriel : secretariat@institut-ega.org
Site internet : www.institut-ega.org

SOMMAIRE

Introduction

Les conflits armés contemporains auxquels l'OTAN se prépare s'inscrivent dans une transformation profonde des modalités de l'action militaire, marquée par l'implication croissante des acteurs privés, entendus ici comme les acteurs privés de la sphère militaire et de la sphère civile, et par le recours accru aux technologies qu'ils développent. Le conflit russo-ukrainien en offre des exemples révélateurs : des technologies issues de l'innovation civile, et notamment les drones, permettent de frapper à distance, avec une discrétion accrue et sans exposition humaine directe. L'Ukraine a, par exemple, été en mesure de neutraliser un sous-marin russe Kilo dans un port, sans présence humaine sur la zone d'opération[1]. Ce type d'action met en lumière les avantages liés à l'application militaire de technologies d'origine civile et souligne la place désormais centrale qu'occupent les acteurs privés dans les conflits armés contemporains.

Le conflit russo-ukrainien agit comme un révélateur de dynamiques à l'œuvre depuis plusieurs années, à savoir le retour de conflits de haute intensité, l'hybridation des opérations et l'importance grandissante des technologies numériques et autonomes. En modifiant les capacités opérationnelles et les modes d'engagement, ces technologies sont susceptibles de transformer les équilibres militaires et stratégiques, ce qui accélère leur intégration au sein des opérations militaires. Or, ces nouvelles technologies, dites « émergentes et de rupture », sont souvent développées dans le secteur civil et relèvent d'un usage dual, à la fois civil et militaire. Cette réalité tend à estomper la distinction entre la sphère civile et la sphère militaire dans la conduite des conflits. L'imbrication croissante des acteurs privés dans les écosystèmes d'innovation, de logistique, d'information ou encore de capacité opérationnelle contribue ainsi à une conflictualité qualifiée d'hybride, dans laquelle les actions militaires conventionnelles coexistent avec des opérations informationnelles, cyber et économiques.

Si le recours accru aux acteurs privés offre des avantages opérationnels indéniables, tels qu'une capacité d'innovation rapide, un déploiement accéléré de technologies critiques, ou le renforcement de la résilience face aux frappes adverses, cette dynamique s'accompagne également de risques majeurs. La dépendance à des infrastructures privées, parfois étrangères, interroge quant à la fiabilité de ces acteurs, mais aussi quant à ses effets sur la chaîne de commandement et la continuité des opérations. Par ailleurs, l'intégration de technologies issues du secteur privé et civil au sein des opérations militaires progresse souvent plus rapidement que l'adaptation des cadres juridiques et doctrinaux qui encadrent leur emploi. Ce décalage alimente des inquiétudes croissantes quant à l'application du droit international aux conflits contemporains.

[1] MELKOZEROVA Veronika, *Ukraine blows up Russian submarine using underwater drone,* Politico, 15 déc. 2025.

Dans le cadre d’opérations multinationales, ces risques se trouvent encore amplifiés par la multiplicité des chaînes de commandement, la diversité des systèmes de régulation, ainsi que par la nécessité de maintenir un haut niveau d’interopérabilité entre les forces. Dans ce contexte, l’enjeu pour l’OTAN n’est pas seulement d’intégrer efficacement les acteurs privés dans ses capacités militaires, mais de le faire sans remettre en cause les principes du droit international humanitaire, en particulier la distinction entre civils et combattants, la qualification des objectifs militaires et l’attribution claire des responsabilités.

Les acteurs privés sont devenus des composantes incontournables des capacités militaires contemporaines, dont l’intégration transforme en profondeur les dynamiques des conflits armés. Cette évolution crée toutefois des tensions juridiques quant à l’application effective des fondements du droit international humanitaire.

L’intégration structurelle des acteurs privés dans les capacités militaires de l’OTAN

L’implication croissante des acteurs privés dans les capacités militaires des États membres de l’OTAN s’inscrit dans une dynamique de long terme, qui dépasse le simple recours ponctuel à la sous-traitance. Cette intégration est devenue structurelle et ses modalités entraînent des conséquences en matière d’innovation, d’interopérabilité et de dépendances stratégiques.

De la sous-traitance au rôle stratégique des acteurs privés

L’intégration d’acteurs privés dans le domaine de la défense n’est pas nouvelle. Elle s’inscrit dans un processus de délégation progressive de certaines compétences nationales vers des prestataires privés. En France, cette évolution s’amorce au début des années 2000, dans le sillage de la professionnalisation des armées. La diminution du nombre de conscrits, auparavant affectés à des tâches telles que l’entretien des infrastructures, conduit, parmi d’autres facteurs, à un recours accru à des contrats de sous-traitance.

Initialement cantonnée à des fonctions de soutien, cette externalisation s’est progressivement étendue à des domaines clés, tels que la production de matériel militaire ou le soutien logistique, et occupe aujourd’hui une place stratégique dans la posture opérationnelle des États. Le secrétaire à la Défense américain, Pete Hegseth, a identifié deux piliers fondamentaux dont dépend la « létalité » des soldats, érigée en priorité stratégique : les technologies de guerre employées par les forces armées et l’ensemble de la logistique encadrant

les opérations[2]. Pour chaque composante de ces deux piliers, les acteurs privés apparaissent comme des intervenants incontournables.

De la conception à la fabrication, puis à la maintenance des équipements et des infrastructures, les armées font appel à l'expertise et aux ressources du secteur privé. Le contrat conclu entre Airbus et la Direction générale de l'Armement pour l'intégration de capacités d'intelligence artificielle dans des systèmes militaires français illustre l'ampleur de cette coopération, y compris dans des domaines technologiques particulièrement sensibles[3]. L'externalisation de la modernisation des systèmes d'armes, des réseaux d'information et de la cybersécurité révèle ainsi le rôle indispensable de ces entreprises, auxquelles les forces armées confient désormais une part significative de leur capacité opérationnelle, notamment dans des secteurs stratégiques tels que le renseignement, la cybersécurité ou l'interopérabilité des systèmes[4].

Cette intégration à l'échelle nationale influe également sur l'interopérabilité des forces à l'échelle de l'OTAN. Si l'Alliance encourage les partenariats civil-militaires et public-privé dans le champ de l'innovation et des technologies émergentes, une implication accrue des entreprises exige un haut degré de coordination entre États, autorités militaires et acteurs privés. La diversité de solutions technologiques nationales crée en effet un risque de fragmentation, susceptible de fragiliser l'interopérabilité des forces en situation de défense collective. Le partage d'informations et la coordination sont donc indispensables pour intégrer des acteurs privés dans l'effort d'innovation, tout en composant avec les rivalités industrielles.

Technologies émergentes, dual-use et accélération de l'innovation

La montée en puissance du rôle stratégique des acteurs privés se manifeste de manière particulièrement visible dans le domaine de l'innovation technologique, qui s'inscrit dans un contexte sécuritaire marqué par un sentiment d'urgence croissant au sein de nombreux États. Selon Mark Rutte, secrétaire général de l'OTAN, l'économie de guerre mise en place par la Russie pourrait lui permettre d'attaquer l'Alliance d'ici cinq ans[5]. Face à cette perspective, le renforcement des équipements et la préparation des forces des États membres à un potentiel conflit hybride nécessitent une accélération significative de l'innovation militaire.

L'hybridation des conflits, telle qu'observée en Ukraine, met en lumière le rôle central du numérique dans la conduite des hostilités (traitement de l'information, communications, capteurs). Cette réalité a conduit plusieurs forces armées à reconnaître la nécessité d'une transformation numérique en profondeur. L'armée de Terre française, par exemple, s'appuie sur le développement de nouvelles technologies, telles que les robots autonomes ou le cloud sécurisé, afin de garantir une « supériorité opérationnelle et une maîtrise de l'information sur

[2] Jim, GROTTO Andrew, *The Pentagon's Operational Technology Problem,* Lawfare, 15 déc. 2025.
[3] CHRETIEN Daniel*, IA : Airbus signe un contrat avec la DGA,* Air&Cosmos, 10 déc. 2025.
[4] *Ibid*.
[5] NÖSTLINGER Nette, *NATO's Rutte says Europe must prepare for 'scale of war our grandparents' endured,* Politico, 11 déc. 2025.

les théâtres d'opération. »[6] Atteindre ces objectifs requiert toutefois une capacité d'innovation rapide, des ressources financières et humaines substantielles et des compétences techniques souvent plus disponibles dans le secteur civil et privé. À l'instar du contrat conclu avec Airbus, la coopération avec le secteur privé apparaît alors comme une solution privilégiée pour répondre à ces besoins.

À l'échelle de l'OTAN, l'intégration de technologies civiles et l'adoption rapide de technologies émergentes et de rupture (TE/TR) constituent des leviers pour obtenir un avantage stratégique, mais s'accompagnent de risques qui exigent des garde-fous. Le positionnement de l'Alliance sur les TE/TR vise à développer une approche cohérente en matière de création et d'adoption de technologies à usage dual[7]. Cet intérêt pour les technologies civiles adaptables au contexte militaire est étroitement lié aux enseignements tirés du conflit russo-ukrainien. L'emploi de technologies et d'équipements civils dans des actions militaires a en effet révélé plusieurs avantages stratégiques, tels qu'un coût plus faible, une facilité d'adoption liée à leur conception pour le grand public et un niveau technologique parfois supérieur à celui des équipements strictement militaires.

Si l'armée ukrainienne a intégré ces technologies de manière réactive, en s'adaptant directement aux contraintes du champ de bataille, les forces de l'OTAN disposent de la capacité d'anticiper leur intégration et d'en encadrer l'utilisation en amont. Dans cette optique, l'Alliance a mis en place en 2022 l'Accélérateur d'innovation de défense pour l'Atlantique Nord (DIANA), un dispositif visant à rapprocher start-ups civiles et besoins militaires pour accélérer l'adoption de solutions *dual-use*[8].

Plus largement, l'OTAN encourage des activités d'innovation dans neuf domaines prioritaires des TE/TR : intelligence artificielle, systèmes autonomes, technologies quantiques, biotechnologies et technologies d'amélioration des capacités humaines, espace, systèmes hypersoniques, matériaux et procédés de fabrication innovants, énergie et systèmes de propulsion, ainsi que réseaux de communication de nouvelle génération[9]. Chacun de ces domaines fait l'objet de plans d'action ou de stratégies visant à accélérer l'innovation par la coopération entre États et entre secteurs. Ces partenariats s'appuient sur plusieurs outils développés au sein de l'Alliance, tels que le Fonds OTAN pour l'innovation, doté d'un milliard d'euros pour investir dans des start-up développant des TE/TR dans des domaines clés pour la sécurité des Alliés, le Groupe consultatif OTAN sur les technologies émergentes et de rupture, composé d'experts issus du secteur privé et du monde universitaire, ou encore la Communauté transatlantique du quantique, qui favorise l'échange d'informations et la coordination des actions[10].

L'ensemble de ces initiatives témoigne de la volonté de l'OTAN d'accélérer l'intégration de technologies de pointe au sein de ses forces armées afin d'en exploiter les avantages stratégiques. Sous l'effet de la menace russe, la rapidité d'adoption apparaît comme un enjeu

[6] Armée de Terre, *La transformation numérique dans l'armée de Terre,* https://www.defense.gouv.fr/
[7] OTAN, *Technologies émergentes et technologies de rupture,* 25 juin 2025
[8] *Ibid*.
[9] *Ibid*.
[10] *Ibid*.

central, illustré par le plan d'action adopté lors du sommet de La Haye en 2025, qui fixe un délai maximal de vingt-quatre mois pour l'adoption des technologies par les forces armées, tout en prévoyant des mesures facilitant cette intégration, telles que l'accélération des processus nationaux d'acquisition et une communication claire des priorités de l'OTAN à l'industrie de défense[11].

Toutefois, cette approche crée une tension entre la volonté d'adopter rapidement des technologies afin de bénéficier de la dynamique d'innovation et la nécessité de maintenir un contrôle stratégique sur les outils employés. Les avantages associés à ces technologies restent en effet conditionnés à leur adéquation à un usage militaire, ce qui suppose des tests approfondis en conditions réelles, l'identification de leurs limites, la formation des combattants à leur utilisation et leur capacité d'adaptation à des contextes opérationnels variés. Si le plan d'action inclut des phases de test destinées à réduire les risques liés aux TE/TR, le risque est de les voir écartées au profit de l'intégration rapide.

L'équilibre entre encadrement et vitesse d'adoption demeure essentiel pour assurer l'adoption sécurisée et efficace des technologies issues du secteur privé et doit se traduire par des processus opérationnels clairs, liés à des calendriers appropriés au niveau de risque.

Dépendances industrielles et technologies critiques

Cette accélération de l'innovation et cette dépendance accrue aux technologies privées soulèvent des vulnérabilités nouvelles, notamment en matière de dépendances industrielles et de sécurité des technologies critiques. Le domaine militaire intègre non seulement les capacités des acteurs privés, mais également leurs vulnérabilités techniques et logistiques. La dépendance stratégique aux équipements du privé implique ainsi pour les forces armées de prendre en compte la résilience de ces acteurs, tant dans la planification des opérations que dans la posture de défense en temps de paix. Parmi les préoccupations sécuritaires majeures associées à cette dépendance, deux catégories de vulnérabilités se distinguent : celles liées à la chaîne d'approvisionnement et celles d'ordre cyber.

Les vulnérabilités de la chaîne d'approvisionnement affectent en premier lieu la continuité opérationnelle des forces, dans la mesure où l'approvisionnement en équipements en temps de guerre pourrait être perturbé par les faiblesses propres aux acteurs privés. Un risque majeur tient à la dépendance de ces derniers à des sous-traitants ou transporteurs situés hors des États alliés, exposant les chaînes à des risques politiques, d'espionnage ou de sabotage. La fiabilité de chaque maillon devrait donc être vérifiée par un contrôle et une certification des étapes de fabrication et de transport. Cela peut notamment passer par des audits, une exigence contractuelle de traçabilité de la provenance de composants critiques, ou la mise en place d'une liste de sources non-fiables qui ne doivent pas figurer dans la chaîne d'approvisionnement. Les États pourraient également envisager d'imposer l'obligation contractuelle d'identifier les

[11] OTAN, Plan d'action pour une adoption rapide, 25 juin 2025.

fournisseurs critiques en cascade et d'établir des plans de substitution activables dans un délai restreint.

Les vulnérabilités cyber, quant à elles, concernent l'ensemble de la capacité opérationnelle de l'OTAN, puisqu'elles peuvent impacter les logiciels, les équipements, les services cloud et tout autre élément numérique utilisé. L'intégration d'acteurs privés étend ainsi le périmètre de la menace cyber, puisqu'une attaque ciblant des acteurs coopérants peut créer une passerelle vers les infrastructures et équipements militaires. Protéger la capacité opérationnelle implique donc de sécuriser informations, équipements et infrastructures des deux sphères, avec une responsabilité partagée entre autorités militaires et acteurs privés. Dans cette optique, le Pentagone a notamment tenté d'isoler les infrastructures et le matériel militaires des réseaux publics afin de réduire leur exposition aux cybermenaces[12].

Si cette démarche de segmentation contribue à renforcer la résilience de la sphère militaire, elle demeure toutefois insuffisante. Les régulations et standards de cybersécurité ciblent généralement les systèmes d'information mais tendent à occulter l'encadrement de produits numériques. Ces éléments, qui sont ensuite intégrés aux équipements militaires, constituent pourtant une vulnérabilité puisqu'ils peuvent servir de vecteurs d'attaques cyber, surtout lorsqu'ils sont connectés à internet. L'isolement de la sphère militaire apparaît alors comme un effort limité, dans la mesure où un grand nombre d'équipements contient de tels composants numériques, tels que les batteries, les capteurs ou les interrupteurs[13].

Le lien avec le numérique étant inévitable, l'enjeu ne réside donc pas dans l'isolement du domaine militaire, mais dans la sécurisation systématique des composants numériques. Dans la mesure où ces composants sont intégrés à des technologies issues du secteur privé, il est nécessaire d'établir un cadre de sécurité adapté à ces acteurs, intégrant exigences de conception sécurisée (*security by design*), certifications et obligations de transparence sur la chaine de fabrication. Cet encadrement pourrait être simplifié par la création d'une certification OTAN sur la sécurité des fournisseurs privés, permettant de conditionner l'habilitation à fournir certaines technologies critiques. Cette certification permettrait également aux acteurs privés de coopérer avec différents Alliés et favoriserait une interopérabilité sécurisée entre les forces armées des États membres. L'OTAN et les États membres pourraient aussi établir un inventaire priorisé des ressources numériques critiques, cartographier leurs dépendances et identifier les potentielles vulnérabilités, afin de soumettre les technologies les plus sensibles à des contrôles renforcés.

À l'échelle de l'OTAN, ces mesures apparaissent d'autant plus nécessaires qu'une attaque visant la chaîne d'approvisionnement ou les infrastructures numériques pourrait compromettre la capacité opérationnelle de l'Alliance dans son ensemble, en déstabilisant l'interopérabilité des forces. L'hybridation technologique des conflits contemporains n'a pas seulement brouillé les frontières entre sphères civiles et militaires dans leur participation aux hostilités. Elle a également estompé la distinction entre la sécurité du secteur privé et celle du domaine militaire. Dès lors, si l'OTAN entend préserver sa capacité opérationnelle et l'interopérabilité de ses

[12] DEMPSEY Jim, GROTTO Andrew, *The Pentagon's Operational Technology Problem,* Lawfare, 15 déc. 2025
[13] *Ibid*.

forces, la résilience industrielle doit être envisagée comme un enjeu de sécurité nationale et collective à part entière. Cela implique, entre autres, de dresser des inventaires critiques, des redondances d'approvisionnement ainsi que des clauses contractuelles de continuité.

Acteurs privés, transformation de la guerre et nouvelles vulnérabilités

L'implication croissante des acteurs privés ne transforme pas uniquement les capacités matérielles des forces armées, mais modifie plus profondément la manière dont la guerre est conduite, pensée et encadrée. En contribuant au développement de technologies permettant l'action à distance, l'automatisation des processus militaires ou encore la résilience des systèmes, ces acteurs participent à une transformation des dynamiques stratégiques, tout en faisant émerger de nouvelles vulnérabilités opérationnelles pour les États et l'OTAN.

Automatisation, distance et abaissement du seuil de violence

Les acteurs privés, par leur expertise et leurs ressources, sont à l'origine d'innovations technologiques majeures qui repoussent continuellement les limites des capacités militaires. Ces avancées sont attentivement observées par les forces armées, qui cherchent à maintenir leur avantage stratégique et à anticiper les transformations induites par ces nouvelles technologies. Parmi ces évolutions, l'opérabilité à distance occupe une place centrale, notamment à travers le développement de systèmes téléopérés ou autonomes.

Les technologies permettant de conduire des opérations militaires à distance constituent un facteur déterminant dans la conduite des hostilités. En réduisant la présence humaine dans la zone d'opération, elles permettent de limiter le coût humain tout en facilitant l'accès à des zones sensibles ou fortement défendues. La guerre d'Ukraine illustre clairement cette dynamique, où la capacité à frapper loin à l'arrière du front est devenue un avantage stratégique majeur[14]. Dans ce contexte, plus la distance de téléopération est importante, plus l'avantage opérationnel est significatif, ce qui explique l'intérêt croissant porté aux innovations dans ce domaine.

Les drones, qu'ils soient de reconnaissance ou d'attaque, se sont ainsi imposés comme des outils indispensables pour la défense ukrainienne. Le retrait de la présence humaine à bord de ces engins permet en outre le développement de systèmes plus petits et moins détectables, capables de s'adapter à différents théâtres d'opération et de se rapprocher plus aisément de

[14] DUNDA Oleg, *The art of war is undergoing a technological revolution in Ukraine,* Atlantic Council, 24 déc. 2025 ; Il convient de préciser que l'avantage lié à la distance dépend toutefois de la résilience des liaisons, de la latence et des capacités de commandement et contrôle.

leurs cibles[15]. L'attaque menée à l'aide du drone sous-marin *Sub Sea Baby*[16] illustre de manière emblématique les bénéfices de la téléopération : une capacité d'action dans une zone sensible, un impact stratégique élevé et une réduction significative des risques humains.

Par ailleurs, la capacité de certains drones à opérer à courte distance de la cible peut améliorer la précision, limitant les dommage collatéraux et facilitant ainsi le respect des principes de distinction, de précaution et de proportionnalité du droit international humanitaire. Cette amélioration dépend toutefois d'un ensemble de facteurs, notamment la qualité des capteurs, des algorithmes de ciblage et des procédures humaines d'autorisation.

En parallèle de ces systèmes téléopérés, certains acteurs privés développent des technologies reposant sur l'automatisation des processus militaires. À l'aide d'outils numériques, notamment d'intelligence artificielle, ces technologies permettent d'effectuer automatiquement certaines actions, accélérant ainsi le tempo des opérations. Ces mécanismes d'automatisation sont notamment présents dans des systèmes de ciblage, capables de proposer des objectifs sur la base du traitement automatisé de données issues d'images, de renseignements humains ou du croisement de multiples sources d'information.

Si certaines de ces technologies conservent un rôle central pour l'humain dans la prise de décision et le contrôle de l'action militaire, ce n'est pas le cas de l'ensemble. Certains acteurs développent en effet des systèmes capables de prendre une décision et d'agir sans intervention humaine. Lorsqu'ils sont en mesure de mener une action létale de manière autonome, ces systèmes sont couramment qualifiés de systèmes d'armes létales autonomes (SALA)[17] dans les débats académiques et diplomatiques, bien il n'existe pas de définition juridique internationale consensuelle. Des exemples de technologies s'en rapprochant incluent le robot Samsung déployé à la frontière entre les deux Corées, le drone israélien Harpy ou encore le système russe S-400 Triumf.

Le développement de ces technologies, stimulé notamment par les progrès de l'intelligence artificielle et par la volonté de réduire le coût humain de l'usage de la force, pose des défis juridiques et éthiques majeurs. En favorisant une potentielle course à l'armement axée sur la performance technologique et l'automatisation, ces systèmes risquent de dépasser les limites fixées par le droit international, notamment en raison des biais algorithmiques, des hallucinations de l'IA, des vulnérabilités cyber ou encore des risques de perte de contrôle. Ces failles soulignent l'importance du contrôle humain sur les actions létales, car elles présentent un risque d'erreurs de ciblage ou d'exécution, qui peuvent entraîner des attaques contre des population civiles, des frappes disproportionnées, ou encore des incidents impliquant les forces alliées.

Si les technologies téléopérées et autonomes constituent un avantage stratégique indéniable et réduisent le coût de l'usage de la force, elles participent également à une possible

[15] *Ibid*. ; Ici aussi, des désavantages sont à considérer, notamment une endurance et une charge utile limitées.
[16] MELKOZEROVA Veronika, *Ukraine blows up Russian submarine using underwater drone,* Politico, 15 dec. 2025
[17] RUFFO DE CALABRE Marie-des-Neiges, *Avons-nous le choix d'utiliser l'IA en temps de guerre ?* Cahiers de la sécurité et de la justice (n°47), Institution des hautes études du ministère de l'intérieur (IHEMI), 2023.

banalisation de cet usage et à un abaissement progressif des seuils de violence. Dans ce contexte, une coopération internationale renforcée apparaît indispensable pour encadrer leur développement et plus particulièrement celui des SALA. L'OTAN peut jouer un rôle central de coordination et de promotion de bonnes pratiques, d'orientations politiques et de standards techniques entre Alliés. Une mesure envisageable serait notamment de mandater un groupe OTAN d'experts techniques et juridiques pour produire un cadre d'exigences minimales sur le contrôle humain, la transparence dans les données d'entraînement, ou encore un processus d'élimination des biais algorithmique. Ce cadre harmoniser pourrait ainsi servir de référence aux États dans leurs efforts de développement de normes contraignantes au sein de forums multinationaux.

Résilience, technologie et dissuasion

Les nouvelles technologies, loin de se limiter au renforcement des capacités opérationnelles des forces armées, participent également aux stratégies de dissuasion des États et de l'OTAN. Plus précisément, la résilience technologique qu'elles incarnent reflète la capacité d'une armée à résister aux attaques, à absorber les chocs et à s'adapter rapidement aux contraintes opérationnelles. Lorsqu'elle est consolidée en amont d'un conflit, cette résilience peut constituer un outil de dissuasion à part entière.

La guerre d'Ukraine illustre bien la place centrale qu'occupe la résilience d'un pays dans un conflit hybride, qu'elle s'opère sur le plan civil, technologique ou opérationnel. La capacité de l'Ukraine à se remettre des frappes, à produire des armements et à répondre aux attaques constitue un levier d'influence majeur dans le rapport de force avec la Russie et toutes les parties prenantes aux discussions sur l'avenir du conflit, malgré la supériorité militaire présumée de Moscou[18]. Dans ce contexte, la coopération avec le secteur privé et civil peut être une solution à privilégier pour renforcer la résilience technologique des forces armées.

Les technologies issues du secteur civil sont, d'une part, souvent conçues pour une utilisation massive et une prise en main rapide, ce qui les rend accessibles à un grand nombre d'utilisateurs sans formation approfondie[19]. Cette simplicité d'usage permet une intégration accélérée de ces technologies et une réponse plus efficace à des besoins urgents, en comparaison avec des équipements exclusivement militaires, souvent plus complexes et longs à déployer. Les entreprises privées, d'autre part, disposent généralement d'équipes techniques dédiées à la résolution d'incidents, qu'ils soient accidentels ou intentionnels, garantissant une capacité de réaction rapide et une continuité opérationnelle accrue des équipements[20].

Les technologies civiles et privées jouent également un rôle important dans le renforcement de la coopération internationale, contribuant ainsi à la dissuasion collective. Ces dernières années, la Corée du Sud s'est imposée comme un acteur central de cette dynamique, en

[18] *Ibid*.
[19] JAYANTI Amritha, *Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?*, Belfer Center for Science and International Affairs, Harvard Kennedy School, 9 mars 2023
[20] *Ibid*.

particulier dans ses relations avec l'Union européenne et l'OTAN. L'expansion rapide des partenariats industriels de défense entre Séoul et les États membres de l'Alliance s'est traduite par la conclusion de contrats majeurs, notamment avec la Pologne, faisant de la Corée du Sud le deuxième fournisseur de défense du pays après les États-Unis[21].

Cette coopération industrielle favorise également le rapprochement de différents secteurs au sein des États partenaires, facilitant l'échange d'informations, l'amélioration des performances technologiques et l'adaptation des équipements aux réalités du champ de bataille. La Corée du Sud bénéficie par ailleurs d'un programme de partenariat personnalisé avec l'OTAN, offrant un cadre structuré pour une collaboration dans des domaines clés tels que la cyberdéfense, les technologies émergentes, l'interopérabilité et la résilience[22].

En développant et en diversifiant ses partenariats avec des pays tiers, l'OTAN pourrait ainsi renforcer sa compréhension des conflits contemporains, en particulier dans les domaines du numérique et des communications, affiner la préparation de ses forces avec la coopération d'acteurs privés et, in fine, accroître sa capacité de dissuasion.

Acteurs privés et dépendance opérationnelle

La dépendance aux infrastructures privées expose les forces armées à des risques de rupture brutale de capacités essentielles, que ce soit par leur destruction, par des attaques cyber ou par un conditionnement de l'accès aux services imposé par l'acteur privé. La dépendance aux technologies critiques, notamment dans les domaines de la communication, des données et de la connectivité, constitue ainsi un risque stratégique majeur, dans la mesure où un acteur privé, et d'autant plus civil, peut décider unilatéralement de suspendre ou de restreindre ses services en fonction de ses intérêts économiques, politiques ou idéologiques.

L'utilisation massive du système Starlink par les forces armées ukrainiennes illustre concrètement ces risques. Cette technologie a permis le contrôle de drones de reconnaissance et de combat, le maintien des communications civiles, la connectivité des équipements médicaux hospitaliers ainsi que la continuité des activités des entreprises et des ONG à travers le pays[23]. Lorsque SpaceX annonce en février 2023 son intention de restreindre l'utilisation militaire de Starlink[24], la dépendance à un service privé à double-usage se révèle comme une vulnérabilité pour la continuité opérationnelle et met en lumière la nécessité d'anticiper des scénarios d'accès conditionné. La déclaration d'Elon Musk selon laquelle le front ukrainien s'effondrerait sans Starlink[25] illustre davantage la position de force qu'un acteur privé peut acquérir du fait de cette dépendance, soulevant des interrogations majeures sur la fiabilité de

[21] HELVEY David, *South Korea and Europe are stepping up on security cooperation. Here's why,* Atlantic Council, 18 déc. 2025.
[22] *Ibid*.
[23] JAYANTI Amritha, *Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?* op.cit. 2023.
[24] *Ibid*.
[25] DENISOVA Kateryna, *Ukrainian front line 'would collapse' if Starlink is turned off, Musk claims,* The Kyiv Independent, 9 mars 2025.

ces acteurs, d'autant plus sensibles lorsqu'ils sont étrangers, au regard des enjeux de souveraineté.

La provenance des technologies et de leurs composants constitue en effet un facteur potentiellement déterminant dans le déroulement d'un conflit. Le fait que 80 % des composants électroniques critiques des équipements russes utilisés en Ukraine proviennent de Chine[26] interroge sur les dépendances aux sources étrangères de cette ampleur au sein des États membres de l'OTAN. Au sein de l'Alliance, la part réelle de composants ou de services étrangers dans les capacités militaires demeure une donnée essentielle à identifier. Une dépendance excessive à des acteurs extérieurs, notamment à des puissances stratégiques concurrentes, pourrait se traduire par une interruption de l'approvisionnement, des risques de sabotage, de prise de contrôle, ou même l'activation de *kill switch*, entraînant une paralysie opérationnelle à l'échelle de l'OTAN. La création d'un audit par un bureau OTAN ou à l'échelle de chaque État pour identifier les dépendances critiques permettrait de classer les composants selon leur niveau de criticité et d'exposition géopolitique, puis faciliterait l'identification de solutions moins risquées en cas de vulnérabilité majeure.

Cette connaissance des dépendances permettrait également d'anticiper les aléas liés au modèle économique des acteurs privés. Le recours à des technologies privées, en particulier à double usage, introduit une dépendance financière et contractuelle (coûts de déploiement, modèles de financement et conditions commerciales) susceptible de limiter l'autonomie opérationnelle des forces armées. Cette dépendance peut engendrer des négociations récurrentes entre acteurs militaires et civils, affectant la continuité des opérations et pouvant aboutir à un accès conditionné ou restreint aux technologies, y compris après leur déploiement. Les restrictions imposées par SpaceX sur l'usage de Starlink[27] montrent qu'une technologie intégrée et financée peut néanmoins voir son emploi limité.

Par ailleurs, la demande de SpaceX visant à ce que les États-Unis couvrent la quasi-totalité des coûts liés aux terminaux et à la connectivité en Ukraine[28] révèle que cette dépendance peut également s'avérer particulièrement coûteuse. Si de telles dynamiques économiques imprévisibles venaient à se multiplier, elles pourraient fragiliser la coopération entre sphère militaire et secteur privé, voire conduire à un renoncement à certaines avancées technologiques pourtant stratégiques. Anticiper les coûts est donc indispensable et implique de clarifier les clauses financières intégrées dans les accords avec les partenaires privés, particulièrement civils, dès le début de la coopération. L'État pourrait, par exemple, s'engager à financer la fabrication des outils nécessaires au service en temps de crise en contrepartie d'une continuité de ce dernier, instaurant une relation transparente et gagnant-gagnant entre les partenaires.

Au-delà des infrastructures et des technologies, la dépendance s'étend désormais à la maîtrise de l'information et de l'espace numérique. Les GAFAM[29] sont devenus des acteurs

[26] NÖSTLINGER Nette, *NATO's Rutte says Europe must prepare for 'scale of war our grandparents' endured,* Politico, 11 déc. 2025.
[27] JAYANTI Amritha, *Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?* op.cit. 2023.
[28] *Ibid*.
[29] Google, Amazon, Facebook, Apple, Microsoft.

centraux de la dimension informationnelle des conflits, disposant d'un pouvoir d'influence parfois déstabilisateur dans les dynamiques stratégiques. Ce pouvoir repose sur leur capacité à moduler l'accès à l'information, la visibilité des contenus et les formes d'expression politique. Depuis le déclenchement de la guerre en Ukraine, leur positionnement pro-ukrainien, matérialisé par la suspension de ventes en Russie ou l'assouplissement de certaines règles de modération, illustre l'importance de leur rôle dans un contexte de guerre hybride[30].

Le monopole des GAFAM sur la couche informationnelle du cyberespace leur permettrait également d'orienter, voire de manipuler, l'information selon leurs intérêts ou leurs idéaux, en contournant parfois les régulations étatiques[31]. Face à ce pouvoir, une rupture entre États et GAFAM apparaît irréaliste, ces entreprises fournissant des services devenus essentiels aux sociétés contemporaines[32]. À mesure que la numérisation s'intensifie et que les risques sécuritaires associés augmentent, la place des GAFAM dans la sphère politique est amenée à croître. La recherche d'une dépendance réciproque, fondée sur des politiques de marché et des régulations adaptées, apparaît ainsi comme une voie plus réaliste que des mesures extrêmes telles que la nationalisation ou la mise sous tutelle[33].

Cet encadrement suppose néanmoins d'anticiper les stratégies de contournement et de lobbying de ces groupes. Les révélations des ONG Corporate Europe Observatory et Lobby Control, selon lesquelles les GAFAM dépenseraient près de 100 millions d'euros par an pour influencer les législateurs européens[34], témoignent de l'ampleur de ces enjeux. Toutefois, si les GAFAM exploitent leur réputation et leur monopole technologique pour s'étendre et influencer les marchés numériques peu régulés, ils ont également démontré leur capacité à s'adapter à des cadres juridiques stricts, comme en Chine[35]. Sans les restreindre excessivement, les pouvoirs publics peuvent dès lors rééquilibrer les rapports de force informationnels et faire du monopole des GAFAM un atout stratégique, ou à tout le moins éviter qu'il ne devienne un facteur de déstabilisation dans la conduite des hostilités.

En somme, la dépendance aux acteurs privés offre des capacités stratégiques mais crée des vulnérabilités opérationnelles, économiques et informationnelles. Pour en tirer parti sans s'exposer, il convient de combiner cartographie des dépendances, clauses contractuelles robustes, planification en amont de mécanismes financiers de soutien et régulation de la gestion de l'information.

[30] BENABID Mohamed, *The territorialization of cyberspace and GAFAM geopolitics: driving forces and new risks in the wake of the Ukrainian crisis,* Policy Center for the New South, 26 sep. 2022.
[31] *Ibid*.
[32] THIBOUT Charles, *Les GAFAM et l'État : quelles évolutions du champ du pouvoir ?,* IRIS, 13 mai 2022.
[33] *Ibid*.
[34] GAILLARD Barthélémy, *Numérique : une enquête souligne le pouvoir d'influence des GAFAM à Bruxelles,* Toute l'Europe, 2 sep. 2021.
[35] FONTANEL Jacques, SUSHCHEVA Natalia, *La puissance des GAFAM : réalités, apports et dangers,* Université Panthéon-Assas Centre Thucydide, Annuaire français de relations internationales, Volume 20, 2019.

Responsabilité juridique et préservation du statut civil à l'ère des acteurs privés

L'implication croissante d'acteurs privés dans les conflits armés contemporains met à l'épreuve la préservation effective de la distinction entre civils et combattants, ainsi que de la protection qui en découle, dans un environnement opérationnel marqué par l'hybridation des fonctions, des technologies et des chaînes décisionnelles. Pour l'OTAN, ces évolutions soulèvent des questions juridiques étroitement liées aux enjeux opérationnels et stratégiques : qualification des acteurs privés civils au regard de la participation aux hostilités, maintien d'une responsabilité étatique claire malgré l'externalisation de capacités critiques et protection des infrastructures civiles à usage dual face à une interprétation extensive de la notion d'objectif militaire.

Les acteurs civils et la notion de participation directe aux hostilités

Le DIH repose sur une distinction fondamentale entre civils et combattants, les premiers bénéficiant d'une protection générale contre les hostilités, sauf et tant qu'ils ne participent pas directement aux hostilités[36]. Au regard de sa portée, la notion de participation directe aux hostilités[37] ne saurait être remise en cause du seul fait de l'utilité militaire croissante de certaines activités civiles.

Les acteurs privés civils concernés sont principalement des entreprises et des personnels civils qui assurent des fonctions techniques ou opérationnelles critiques, telles que la fourniture de capacités de communication et de connectivité, le traitement de données de renseignement, la maintenance et la mise à jour de systèmes d'armes, ou le développement d'outils d'aide à la décision. Leur contribution peut être déterminante pour la conduite des opérations, sans pour autant s'inscrire nécessairement dans une participation directe aux hostilités au sens du DIH.

La qualification juridique de ces acteurs ne dépend ni de leur importance stratégique, ni de la sophistication des technologies qu'ils développent, mais d'une analyse fonctionnelle fondée sur le seuil de nuisance, la causation directe et le lien de belligérance d'une action spécifique[38]. L'acte de participation doit être susceptible de nuire aux opérations ou à la capacité militaire d'une partie au conflit ou de causer des pertes en vies humaines, des blessures ou des destructions touchant des personnes ou des biens protégés (seuil de nuisance), présenter une relation de causalité directe entre l'acte et les effets nuisibles attendus (causation directe) et

[36] Protocole additionnel I, 1977 ; CICR Base de données, DIH Coutumier, *Le principe de la distinction entre civils et combattants*.
[37] MELZER Nils, Guide interprétatif sur la notion de participation directe aux hostilités en droit international humanitaire, CICR, Genève, octobre 2010.
[38] *Id*. pp. 48-67.

être spécifiquement destiné à provoquer directement ces effets nuisibles au profit d'une partie au conflit et au détriment d'une autre[39]. Selon une interprétation stricte, les acteurs privés civils dont l'activité relève d'un soutien général ou structurel à l'effort militaire conservent en principe leur statut civil, même lorsque leurs produits ou services sont utilisés par les forces armées dans la conduite des hostilités.

Toutefois, une interprétation plus large de ces conditions bousculerait les repères de la qualification des acteurs civils, notamment lorsque cela implique des technologies d'aide à la décision. D'aucuns pourraient estimer que lorsque ces outils influencent substantiellement la prise de décision, le concepteur devient un acteur direct dans les hostilités puisqu'il est l'auteur de l'algorithme et donc à l'origine de la décision. À l'inverse, une interprétation plus restrictive suggèrerait que ces technologies sont des instruments passifs, comparables à des manuels, des cartes ou des doctrines, dont l'utilisation et les effets relèvent exclusivement de la responsabilité du décideur humain et *in fine*, d'un combattant. Cette divergence potentielle créerait une ligne de fracture majeure : plus la technologie serait perçue comme autonome ou déterminante, plus il est probable que l'on suggère de tenir juridiquement responsable l'acteur civil qui l'a conçue.

Une interprétation extensive de la participation aux hostilités risquerait alors d'éroder progressivement la protection du statut civil et de fragiliser l'application des principes fondamentaux du droit international humanitaire. L'OTAN pourrait promouvoir une clarification doctrinale et opérationnelle des seuils de participation directe, adaptés notamment aux technologies d'aide à la décision, afin de limiter les interprétations divergentes entre Alliés et de préserver les fondements du DIH.

La responsabilité dans les chaînes décisionnelles hybrides

Lorsque des décisions militaires reposent sur des systèmes développés, maintenus ou exploités par des acteurs privés civils, la frontière entre décision humaine, choix militaire et contribution technique devient parfois floue. Cette difficulté est accentuée dans les opérations multinationales conduites sous l'égide de l'OTAN, où la pluralité des États contributeurs complexifie déjà l'attribution de la responsabilité étatique. L'intervention d'acteurs privés civils ajoute une couche supplémentaire, susceptible de créer des zones grises juridiques, voire des situations d'impunité de fait.

Dans ce contexte, il convient de rappeler que la responsabilité internationale demeure, en principe, celle des États, et que le recours à des acteurs privés civils ne saurait constituer un moyen de contourner les obligations de respecter et de faire respecter le DIH. Toutefois, l'hybridation des chaînes décisionnelles et l'intervention de prestataires privés peuvent obscurcir l'identification du décideur effectif et donc de la responsabilité individuelle, notamment en cas de poursuites pour violation grave.

[39] *Ibid*.

Les technologies d'aide à la décision illustrent particulièrement ce défi. Si elles sont assimilées à de simples outils d'assistance, la responsabilité repose pleinement sur le commandement militaire. En revanche, plus ces systèmes influencent substantiellement la décision, plus la question de la responsabilité partagée se pose, notamment en cas de défaillance prévisible, de biais algorithmiques ou de limites connues du système. Dans ce contexte, l'exigence d'un contrôle humain effectif revêt une importance centrale, tant sur le plan juridique qu'opérationnel. Pour l'OTAN, cette exigence devrait impliquer non seulement la présence formelle d'un humain dans la boucle, mais également sa capacité réelle à comprendre, contester et, le cas échéant, interrompre l'action du système. À défaut, le risque est double : une perte de maîtrise opérationnelle et une fragilisation de l'imputabilité juridique en cas de violation du DIH.

Pour l'OTAN, l'enjeu n'est pas de transférer la responsabilité juridique vers les acteurs privés civils, mais de prévenir sa dilution et l'impunité des violations. Plusieurs exigences apparaissent alors comme essentielles. En amont, les contrats liant les forces armées aux acteurs privés doivent intégrer des obligations renforcées de transparence, de traçabilité des décisions techniques, de documentation des données utilisées et de coopération en cas d'incident. En aval, les chaînes de commandement doivent rester clairement identifiables et les décisions critiques, notamment celles impliquant l'usage de la force, doivent demeurer sous l'autorité d'un commandement militaire responsable. L'OTAN pourrait jouer un rôle de coordination en favorisant l'harmonisation de ces exigences contractuelles et opérationnelles entre Alliés.

Les infrastructures civiles à usage dual et la notion d'objectif militaire

L'un des enjeux juridiques les plus sensibles soulevés par l'implication croissante des acteurs privés civils dans les conflits armés contemporains concerne la qualification de leurs infrastructures et technologies à usage dual au regard de la notion d'objectif militaire. Selon le droit international humanitaire, cette notion désigne les biens « *qui, par leur nature, leur emplacement, leur destination ou leur utilisation, apportent une contribution effective à l'action militaire et dont la destruction totale ou partielle, la capture ou la neutralisation offrent un avantage militaire précis* ».[40] Une distinction nette s'opère entre les biens militaires et civils, ces derniers bénéficiant d'une protection contre les hostilités. Cette distinction est toutefois mise à l'épreuve par l'implication croissante de biens civils dans la sphère militaire.

Les infrastructures privées civiles contemporaines telles que les réseaux de communication, les services cloud, les plateformes numériques, les systèmes satellitaires ou encore les capacités de traitement de données ou d'aide à la décision, sont fréquemment utilisées de manière simultanée à des fins civiles et militaires. Pour certains, considérant la dépendance du domaine militaire à ces infrastructures, leur contribution à l'effort de guerre peut donc être considérée comme déterminante, rendant leur destruction avantageuse pour le compétiteur stratégique.

[40] CICR Base de données, *La définition des objectifs militaires*, DIH Coutumier.

Selon cette interprétation, elles constitueraient donc un objectif militaire légitime, malgré leurs applications civiles.

Une logique similaire apparaît dans les débats assimilant certains acteurs privés civils à des usines d'armement traditionnel[41]. Si cette analogie peut se justifier dans des cas limités, notamment lorsque des infrastructures sont exclusivement dédiées à la production d'armements, son extension aux entreprises civiles développant ou hébergeant des technologies duales comporte un risque majeur : celui d'élargir excessivement la catégorie des objectifs militaires et d'exposer des infrastructures civiles, ainsi que les populations qui en dépendent, aux effets directs des hostilités. Une telle évolution irait à l'encontre de l'esprit et de la finalité protectrice du DIH, notamment l'interdiction « d'attaquer, de détruire, d'enlever ou de mettre hors d'usage des biens indispensables à la survie de la population civile. »[42] Certaines infrastructures civiles à usage dual fournissent également des services civils essentiels, tels que les soins de santé, les communications d'urgence ou l'approvisionnement énergétique, dont la destruction ou la neutralisation provoquerait des dommages collatéraux importants.

Dans ce contexte, l'implication des acteurs privés civils ne peut plus être appréhendée uniquement sous l'angle capacitaire. Elle appelle un encadrement juridique intégré, visant explicitement à préserver les fondements du droit international humanitaire, en particulier le statut civil des acteurs privés. L'OTAN dispose, à cet égard, d'un rôle structurant. Sans se substituer aux États dans la production du droit international, l'Alliance peut contribuer à la protection du DIH en élaborant des lignes directrices communes sur l'usage des infrastructures privées civiles en opérations, en clarifiant les critères de qualification des objectifs militaires et en conditionnant la coopération avec les acteurs privés au respect de standards juridiques partagés (par exemple, l'inclusion de ces principes dans les algorithmes d'aide à la décision).

La maîtrise juridique de l'implication des acteurs privés civils apparaît ainsi comme une condition de la conformité au droit international humanitaire. En intégrant ces exigences dès la phase de conception et d'acquisition des technologies, en sécurisant les chaînes de responsabilité et en limitant les interprétations extensives de la notion d'objectif militaire, l'OTAN peut jouer un rôle central dans la préservation de la distinction entre sphères civile et militaire.

[41] RUFFO DE CALABRE Marie-des-Neiges, *Avons-nous le choix d'utiliser l'IA en temps de guerre ?* op.cit.
[42] CICR Base de données, *Les attaques contre des biens indispensables à la survie de la population civile*, DIH Coutumier.

Conclusion

L’implication croissante des acteurs privés civils dans les conflits armés contemporains met en lumière une évolution structurelle de l’action militaire, qui dépasse largement le cadre de l’externalisation ou du soutien ponctuel. Ces acteurs sont désormais intégrés au cœur même des capacités militaires des États membres de l’OTAN, qu’il s’agisse de l’innovation technologique, du soutien logistique, des infrastructures numériques ou des chaînes d’approvisionnement critiques. Cette intégration confère à l’Alliance des avantages opérationnels déterminants, mais l’expose également à de nouvelles formes de dépendances industrielles, technologiques et informationnelles, qui affectent directement sa résilience et son interopérabilité.

Cette évolution ne transforme pas seulement les moyens de la guerre, mais également ses modalités et ses dynamiques stratégiques. En facilitant l’action à distance, l’automatisation des processus militaires et l’accélération du tempo opérationnel, les technologies développées par des acteurs privés civils contribuent à un abaissement potentiel des seuils de violence et à une hybridation accrue des conflits. Si ces capacités renforcent la dissuasion et la résilience collective, elles génèrent également des vulnérabilités nouvelles, liées à la dépendance à des infrastructures privées, à la maîtrise de l’information et à la continuité des services critiques, comme l’illustre de manière emblématique le conflit russo-ukrainien.

Ces transformations soulèvent enfin des enjeux juridiques majeurs, en particulier au regard des fondements du droit international humanitaire. L’implication croissante d’acteurs privés civils dans des fonctions essentielles à la conduite des hostilités met à l’épreuve la distinction entre civils et combattants, ainsi que la qualification des biens civils et des objectifs militaires, notamment lorsque des infrastructures et technologies à usage dual sont concernées. Si le DIH demeure pleinement applicable, son effectivité repose désormais sur une interprétation rigoureuse et restrictive des notions de participation directe aux hostilités et d’objectif militaire, afin d’éviter une érosion progressive de la protection accordée aux populations et biens civils. Dans ce contexte, la clarification des chaînes de responsabilité et le maintien d’un contrôle humain effectif sur les décisions critiques apparaissent comme des exigences centrales.

Face à ces défis, l’OTAN occupe une position singulière. Sans se substituer aux États dans la production du droit international, l’Alliance peut jouer un rôle structurant en harmonisant les pratiques de ses membres, en intégrant les exigences du droit international humanitaire dès la conception et l’acquisition des technologies et en conditionnant la coopération avec les acteurs privés civils à des standards juridiques, opérationnels et éthiques clairs. En agissant en amont sur les doctrines, les cadres contractuels et les mécanismes de contrôle, l’OTAN peut renforcer l’efficacité militaire tout en préservant le respect des principes fondamentaux du droit international humanitaire.

Bibliographie

Armée de Terre, *La transformation numérique dans l'armée de Terre,* https://www.defense.gouv.fr/

BENABID Mohamed, *The territorialization of cyberspace and GAFAM geopolitics: driving forces and new risks in the wake of the Ukrainian crisis,* Policy Center for the New South, 26 sep. 2022, pp.8, https://www.policycenter.ma/

CHRETIEN Daniel*, IA : Airbus signe un contrat avec la DGA,* Air&Cosmos, 10 déc. 2025, https://air-cosmos.com/

CICR Base de données, *La définition des objectifs militaires*, DIH Coutumier, https://ihl-databases.icrc.org/fr/

CICR Base de données, *Le principe de la distinction entre civils et combattants*, DIH Coutumier, https://ihl-databases.icrc.org/fr/

CICR Base de données, *Les attaques contre des biens indispensables à la survie de la population civile*, DIH Coutumier, https://ihl-databases.icrc.org/fr/

DEMPSEY Jim, GROTTO Andrew, *The Pentagon's Operational Technology Problem,* Lawfare, 15 déc. 2025, https://www.lawfaremedia.org/article/

DENISOVA Kateryna, *Ukrainian front line 'would collapse' if Starlink is turned off, Musk claims,* The Kyiv Independent, 9 mars 2025, https://kyivindependent.com/

DUNDA Oleg, *The art of war is undergoing a technological revolution in Ukraine,* Atlantic Council, 24 déc. 2025, https://www.atlanticcouncil.org/

FONTANEL Jacques, SUSHCHEVA Natalia, *La puissance des GAFAM : réalités, apports et dangers,* Université Panthéon-Assas Centre Thucydide, Annuaire français de relations internationales, Volume 20, 2019, pp. 25, https://www.afri-ct.org/

GAILLARD Barthélémy, *Numérique : une enquête souligne le pouvoir d'influence des GAFAM à Bruxelles,* Toute l'Europe, 2 sep. 2021, https://www.touteleurope.eu/

HELVEY David, *South Korea and Europe are stepping up on security cooperation. Here's why,* Atlantic Council, 18 déc. 2025, https://www.atlanticcouncil.org/

JAYANTI Amritha, *Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?*, Belfer Center for Science and International Affairs, Harvard Kennedy School, 9 mars 2023, https://www.belfercenter.org/

MELKOZEROVA Veronika, *Ukraine blows up Russian submarine using underwater drone,* Politico, 15 déc. 2025, https://www.politico.eu/article/

MELZER Nils, Guide interprétatif sur la notion de participation directe aux hostilités en droit international humanitaire, CICR, Genève, octobre 2010, https://www.icrc.org/

NÖSTLINGER Nette, *NATO's Rutte says Europe must prepare for 'scale of war our grandparents' endured,* Politico, 11 déc. 2025, https://www.politico.eu/article/

OTAN, Plan d'action pour une adoption rapide, 25 juin 2025, https://www.nato.int/fr/

OTAN, *Technologies émergentes et technologies de rupture,* 25 juin 2025, https://www.nato.int/

RUFFO DE CALABRE Marie-des-Neiges, *Avons-nous le choix d'utiliser l'IA en temps de guerre ?* Cahiers de la sécurité et de la justice (n°47), Institution des hautes études du ministère de l'intérieur (IHEMI), 2023, https://www.ihemi.fr/

THIBOUT Charles, *Les GAFAM et l'État : quelles évolutions du champ du pouvoir ?,* IRIS, 13 mai 2022, www.iris-france.org/

Institut
EGA

ISSN : 2739-3283

Institut d'études de géopolitique appliquée
66 avenue des Champs-Élysées, 75008 Paris
Courriel : secretariat@institut-ega.org
Site internet : www.institut-ega.org