MINISTÈRE
DES ARMÉES

Liberté
Égalité
Fraternité

COMITÉ D'ÉTHIQUE DE LA DÉFENSE

AVIS SUR L'ENVIRONNEMENT NUMERIQUE DES COMBATTANTS

13 avril 2022

Synthèse exécutive

(1) Le numérique est omniprésent dans les armées françaises. Intégré dans les systèmes d'armes ou couplé avec ceux-ci, le numérique est également au cœur des systèmes d'aide à la décision, à la conduite des opérations, au pilotage des équipements et plateformes, au soutien des forces, à la formation des militaires. Les perspectives qu'offrent les augmentations de puissance de calcul, le développement des technologies et la réduction de l'encombrement des outils permettent d'envisager, à bref délai, de voir encore plus loin et plus près, de décider et d'agir plus vite, de frapper plus fort et de façon plus précise. Cette empreinte, voire cette emprise, accrue du numérique dans les opérations militaires et dans leur préparation est source de nouveaux questionnements éthiques. Tel est le sens de la demande d'avis sur « l'environnement numérique du combattant » adressée au Comité par la Ministre des armées le 18 janvier 2021.

(2) La saisine du Comité s'inscrit dans le prolongement de l'avis sur l'intégration de l'autonomie dans les systèmes d'armes létaux du 29 avril 2021, lequel a traité les questions induites par les développements de l'autonomie décisionnelle et de l'intelligence artificielle dans les systèmes d'armes.

(3) Au sens du présent avis l'environnement numérique des militaires comprend :

- le **« numérique militaire »,** c'est-à-dire les outils militaires (données, logiciels, matériels et équipements numériques) mis, par l'État, à la disposition des forces et utilisés par les militaires pour assurer leurs missions ;
- le **« numérique du militaire »,** c'est-à-dire les outils numériques privés du militaire (données, téléphones personnels, messageries personnelles, accès internet, ordinateurs, montres connectées) qui sont la propriété des militaires et qui les accompagnent dans leur vie professionnelle, en formation, en manœuvres , sur les théâtres d'opération;
- les **réseaux et infrastructures**, militaires et civils, utilisés par les forces et par les militaires.

(4) Les questions touchant à la **sécurité de l'environnement numérique** ont, bien sûr, été prises en considération dans le cadre du présent avis. En revanche le Comité a estimé que les questions liées au **combat numérique**, c'est-à-dire à la **lutte informatique offensive ou d'influence**, ne relevaient pas du cadre de la saisine qui lui a été adressée. Il a également fait le choix de ne pas examiner les questions induites par **l'empreinte environnementale du numérique militaire**, sujet dont il ne méconnait pas l'importance mais qui n'apparait pas détachable de l'ensemble des actions conduites par le ministère des armées et les armées en matière de transition écologique.

(5) Le **numérique militaire** innerve les cinq milieux de conflictualité (terre, mer, air, espace, cyber). Il est au service des cinq fonctions stratégiques (connaissance et anticipation, dissuasion, protection, intervention, prévention) dont la mise en œuvre est confiée aux armées de la République et qui ont pour finalité la défense de notre indépendance nationale et de nos intérêts vitaux, la sauvegarde des intérêts supérieurs de la Nation et l'intégrité du territoire. Ces fonctions impliquent la possibilité d'engager, dans le cadre du droit des conflits armés, des actions létales contre des ennemis qui menacent la paix et notre pays. Le déploiement des dispositifs numériques militaires permet ainsi d'assurer la préparation, la conduite et l'exécution des opérations. Parce qu'elles ont une assise constitutionnelle (exigence de nécessaire libre disposition de la force armée, indépendance et sauvegarde des intérêts fondamentaux de la Nation) et conventionnelle (chapitre VII de la Charte des Nations Unies : mesures de coercition, droit à la légitime défense individuelle ou collective), ces opérations et le numérique militaire qui leur est associé doivent être exclusivement appréhendés au regard de la singularité militaire. C'est le régime des opérations militaires qui est seul applicable au numérique militaire, y compris lorsque les dispositifs mis en œuvre et les infrastructures

militaires incorporent des technologies également utilisées dans le civil, sans préjudice, du respect des droits de propriété intellectuelle des industriels et sous réserve des exceptions que pourraient justifier les impératifs et urgences opérationnels.

(6) Par ailleurs, en garnison, sur les bases, en manœuvres ou en opérations, sur terre comme en mer, les militaires, et ce quelle que soit leur génération, disposent de leurs outils numériques personnels. Le numérique du militaire permet à celui-ci de conserver un lien permanent avec ses proches, de se divertir, de s'informer, d'accéder aux réseaux sociaux. Il fait désormais partie de l'univers du militaire. Si le commandement a été conduit à prendre en compte ces besoins de connexion au titre de la condition militaire, il lui appartient également, s'agissant des usages, à la fois de préserver la mission et la sécurité des militaires et de garantir le respect de leurs droits individuels (droit de propriété, respect de la vie privée et protection des données personnelles).

(7) Le numérique est ainsi devenu en deux décennies un champ traversé par des tensions multiples. Facteur incontestable de supériorité opérationnelle, il est aussi source de fragilités nouvelles. S'il permet, en principe, de renforcer la pertinence des décisions et la précision des actions et constitue, par suite, un atout du point de vue de l'éthique, le numérique soulève des questions nouvelles qui touchent au processus de décision, à la responsabilité humaine, à la bonne maîtrise des outils.

(8) Ce sont ces différents enjeux que le Comité s'est attaché à mettre en évidence. De son analyse découlent les principes directeurs et recommandations qui suivent.

Liste des principes et recommandations[1]

Les principes directeurs

P1 La problématique de « l'environnement numérique du combattant » doit être appréhendée dans sa singularité, laquelle tient notamment au caractère constitutionnel de la mission des forces armées, à l'état militaire, à l'éthique militaire et au strict encadrement par le droit, interne et international, des actions de combat.

P2 La superposition des usages personnels et professionnels impose de rechercher le juste équilibre entre des impératifs et des exigences possiblement contradictoires :

- le respect du droit de propriété du militaire ainsi que la préservation de sa vie privée et de ses données personnelles ;
- le respect de la propriété intellectuelle et les exceptions que pourraient réclamer les opérations ;
- les impératifs de la mission, la sécurité des militaires et les obligations disciplinaires résultant de l'état militaire ;
- la nécessité pour le commandement de veiller au moral de leurs subordonnés.

P3 La conception, le développement et l'emploi d'outils numériques doivent s'inscrire dans un cadre permettant de : respecter l'interdiction de produire, mettre en œuvre et vendre des armements et biens à double usage contraires aux engagements internationaux de la France ; conserver notre supériorité opérationnelle tout en préservant nos valeurs et les impératifs constitutionnels qui s'imposent à l'action de nos forces, à savoir la sauvegarde des intérêts fondamentaux de la Nation, au nombre desquels figurent l'indépendance de la Nation et l'intégrité du territoire.

[1] Les principes et recommandations sont numérotés dans la suite du document selon les présentes références (P1, P2., etc. R1, R2, etc.).

P4 Les perspectives aujourd'hui ouvertes dans le numérique imposent la poursuite des travaux de recherche dans les domaines émergents avec comme axe d'effort la performance dans l'aide à la décision associée à la maîtrise par l'être humain et le commandement en particulier.

P5 La responsabilité humaine dans la conception, le déploiement et l'emploi d'outils numériques, constitue un principe indérogeable. Les valeurs les plus hautes de notre éthique comme notre ordre constitutionnel impliquent que soit engagée en toutes circonstances la responsabilité de l'humain. Il convient de formaliser les chaînes de responsabilité du commandement, du contrôle et de l'exécution quel que soit le niveau de numérisation de l'environnement

Recommandations

R1 Analyser et mettre à jour périodiquement le présent avis pour tenir compte, en tant que de besoin, de l'évolution des technologies numériques, des doctrines opérationnelles et des réflexions en termes de prospective capacitaire.

R2 Entraîner à la résilience en conditions numériques dégradées pour assurer la meilleure décision en permanence.

R3 Peser systématiquement l'intérêt de l'ingérence du niveau hiérarchique N vers le niveau hiérarchique N-1 voire N-2.

R4 Éduquer aux risques de sécurité liés au numérique, qu'il soit à usage personnel ou professionnel.

R5 La mise en service opérationnelle doit assumer ou traiter les risques d'altération de l'autonomie d'appréciation, de la capacité de décision et de la décision elle-même, risques qui seraient liés à des défauts de sécurité ou de souveraineté.

R6 Évaluer systématiquement lors de la recherche, de la conception, du développement et de l'emploi de systèmes numériques, les effets sur la psychologie et les comportements humains tels que la distanciation et l'hypovigilance. Concevoir d'emblée les systèmes numériques comme des systèmes humains-machines et non des machines avec lesquelles les humains doivent composer.

R7 Définir un niveau de garantie des qualifications du système humain + machine. Le prendre en compte dans la formation et l'utilisation du système.

R8 Évaluer la part d'erreur humaine que le commandement est prêt à accepter lorsque les estimations ou résultats fournis par le système numérique sont contredits par l'appréciation du combattant au regard du contexte et en définitive responsable de ses actes.

R9 Assurer la remontée des retours d'expérience opérationnels liés à l'usage des systèmes d'information et leur diffusion à tous les cercles opérationnels mais aussi aux autorités compétentes dans les domaines techniques et juridiques.

R10 Définir des modalités de contrôle de licéité adaptées aux enjeux de la numérisation des outils du combattant.

R11 Assurer une préparation opérationnelle continue et à jour des outils numériques des chefs stratégiques, commandeurs de théâtres, chefs tactiques et opérateurs de systèmes numériques.

R12 Sensibiliser l'usager militaire tant sur les risques de sécurité que sur les effets de l'usage du numérique en termes de facteur humain.

R13 S'assurer de la prise de conscience des écarts entre représentation calculée et représentation ressentie de la réalité au travers d'exercices de biais, de saturation et de travail en ambiance numérique dégradée.

R14 En dépit des capacités de stockage importantes offertes par le numérique, la transparence à tout prix ne doit pas constituer un objectif en soi.

R15 Éduquer aux risques professionnels liés au numérique à usage personnel.

R16 Éduquer aux risques personnels liés au numérique à usage professionnel

R17 Former le commandement à gérer l'articulation des vies privées et professionnelles, la gestion du moral de la troupe et la sécurité de la mission, dans le respect de lois et règlements.

I. Le numérique est omniprésent dans les forces armées

(9) Le numérique est aujourd'hui omniprésent dans les systèmes d'armes, dans les systèmes d'aide à la décision, d'aide à la conduite des équipements et d'aide au soutien des forces. Les perspectives qu'offrent les augmentations de puissance de calcul, le développement des technologies et la réduction de l'encombrement des outils, permettent d'envisager de voir encore plus loin et de plus près, de décider et d'agir plus vite, de frapper plus fort et de façon plus précise. Cette emprise accrue du numérique est source de nouveaux questionnements éthiques. Tel est le sens de la demande d'avis sur **« l'environnement numérique du combattant »** adressée au COMEDEF par la Ministre des armées le18 janvier 2021.

(10) Les évolutions technologiques dans le numérique s'inscrivent dans le temps court, voire très court, alors que la conception et la mise en service des systèmes s'inscrivent dans le temps long, voire parfois plusieurs décennies, pour les systèmes d'armes complexes. Par suite, le Comité a estimé qu'il serait inopérant de fixer un horizon temporel à ses réflexions. En revanche il importe que le présent avis puisse faire l'objet de bilans périodiques pour tenir compte, en tant que de besoin, de l'évolution des technologies, des doctrines opérationnelles et des réflexions de prospective capacitaire.

R1 : Analyser et mettre à jour périodiquement le présent avis pour tenir compte, en tant que de besoin, de l'évolution des technologies numériques, des doctrines opérationnelles et des réflexions en termes de prospective capacitaire.

(11) Afin d'élaborer l'avis qui suit, le Comité a :

- analysé les normes de référence de droit interne et de droit international qui fixent le cadre des opérations militaires ;
- auditionné des personnalités et autorités compétentes en la matière qui ont nourri les réflexions du Comité ;
- intégré la réflexion de stagiaires de l'école de guerre et de GEODE, centre d'excellence du Ministère des armées sur le sujet ;
- effectué des visites dans des unités militaires ou des services recourant massivement au numérique.

A. L'environnement numérique du combattant

(12) Le Comité observe que la demande d'avis s'inscrit dans le prolongement de l'avis sur l'intégration de l'autonomie dans les systèmes d'armes létaux du 29 avril 2021 et que, par suite il devait circonscrire sa réflexion à l'environnement numérique des combattants. Au sens du présent avis l'environnement numérique des militaires comprend :

- le **« numérique militaire »,** c'est-à-dire les outils militaires (données, logiciels, matériels et équipements numériques) mis, par l'État, à la disposition des forces et utilisés par les militaires pour assurer leurs missions ;
- le **« numérique du militaire »,** c'est-à-dire les outils numériques privés du militaire (données, téléphones personnels, messageries personnelles, accès internet, ordinateurs, montres connectées) qui sont la propriété des militaires et qui les accompagnent dans leur vie professionnelle, en formation, en manœuvres , sur les théâtres d'opération;
- les **réseaux et infrastructures**, militaires et civils, utilisés par les forces et par les militaires.

(13) Le Comité a estimé que les questions liées au **combat numérique**, c'est-à-dire à la **lutte informatique offensive ou d'influence**, ne relevaient pas du cadre de la saisine qui lui a été adressée. Il a également fait le choix de ne pas examiner les questions induites par **l'empreinte environnementale du numérique militaire**, sujet dont il ne méconnait pas l'importance mais qui n'apparait pas détachable de l'ensemble des actions conduites par le ministère des armées et les armées en matière de transition écologique.

(14) Le champ du présent avis concerne les forces armées (l'armée de terre, l'armée de l'air, la marine nationale, la gendarmerie nationale, les services de soutien et les organismes interarmées), ainsi que les formations qui leur sont rattachées, au sens et pour l'application des articles L 3211-1 et L 3211-1-1 du code de la défense.

B. L'omniprésence du « numérique militaire » dans le fonctionnement des forces armées et dans les opérations

(15) Le **numérique militaire** innerve les cinq milieux de conflictualité (terre, mer, air, espace, cyber). Il est au service des cinq fonctions stratégiques (connaissance et anticipation, dissuasion, protection, intervention, prévention) dont la mise en œuvre est confiée aux armées de la République et qui ont pour finalité la défense de notre indépendance nationale et de nos intérêts vitaux, la sauvegarde des intérêts supérieurs de la Nation et l'intégrité du territoire. Ces fonctions impliquent la possibilité d'engager, dans le cadre du droit des conflits armés, des actions létales contre des ennemis qui menacent la paix et notre pays. Le déploiement des dispositifs numériques militaires permet ainsi d'assurer la préparation, la conduite et l'exécution des opérations. Parce qu'elles ont une assise constitutionnelle (exigence de nécessaire libre disposition de la force armée, indépendance et sauvegarde des intérêts fondamentaux de la Nation) et conventionnelle (chapitre VII de la Charte des Nations Unies : mesures de coercition, droit à la légitime défense individuelle ou collective), ces opérations ,le numérique militaire qui leur est associé et les infrastructures militaires qui sont utilisées doivent être exclusivement appréhendés au regard de la singularité militaire. C'est le régime des opérations militaires qui est seul applicable au numérique militaire, y compris lorsque les dispositifs mis en œuvre et les infrastructures militaires incorporent des technologies également utilisées dans le civil, sans préjudice, du respect des droits de propriété intellectuelle des industriels et sous réserve des exceptions que pourraient justifier les impératifs et urgences opérationnels.

P1 : La problématique de « l'environnement numérique du combattant » doit être appréhendée dans sa singularité, laquelle tient notamment au caractère constitutionnel de la mission des forces armées, à l'état militaire, à l'éthique militaire et au strict encadrement par le droit, interne et international, des actions de combat.

(16) Les outils numériques militaires ou civils (par exemple le GPS) permettent l'analyse du renseignement, la permanence sur zone (suivi de maintenance du porte-avions) le suivi de situation (E3F), le commandement, la conduite et le contrôle d'opérations, le travail en interalliés ou l'utilisation de vecteurs complexes (frégates multi missions – FREMM, aéronefs, hélicoptères Tigre, artillerie sol-air ou sol-sol). Les combattants disposent ainsi :

- d'une meilleure appréciation de la situation,
- d'une capacité de compte rendu améliorée,
- d'une aide à la conduite de systèmes,
- d'un délestage cognitif.

(17) Le chef d'état-major des armées commande les opérations. Il dispose du centre de planification et de conduite des opérations (CPCO) qui traduit les politiques en ordres militaires. Sur chaque théâtre, il désigne un commandant de la force (COMANFOR) qui dispose lui-même d'un état-major opératif. Ce dernier a autorité sur un ensemble de moyens (C2 orienté moyens) et donne des délégations au niveau tactique inférieur (C2 orienté opérations). L'environnement numérique permet, entre autres, de faciliter la préparation des ordres, de présenter les options au chef, d'interagir avec les alliés et de faire communiquer les différents échelons entre eux.

(18) Les postures permanentes de sûreté air et mer s'appuient sur des réseaux qui interconnectent des centres de décision (centre national des opérations aériennes, préfectures maritimes, centres de détection et de contrôle) avec des capteurs, des effecteurs (aéronefs en charge des mesures actives de sûreté aérienne) ou des administrations civiles (affaires maritimes, direction générale de l'aviation civile, etc.) L'environnement numérique y est donc tourné vers le temps réel, l'identification et la classification d'objets, mais aussi vers les outils de comptes rendus et les liaisons de données tactiques.

(19) La projection de puissance permet de réaliser des frappes à longue distance. Elle s'appuie tant sur les sous-marins, dont la connexion est intermittente, sur des bâtiments, parfois très numérisés comme les FREMM, sur les aéronefs de l'aéronautique navale, sur des outils de contrôle aérien (avion E3F) ou sur des munitions et vecteurs complexes. Les frappes peuvent être commandées depuis la métropole comme cela a été récemment démontré par l'armée de l'air et de l'espace au-dessus de la Polynésie. Ces frappes résultent du processus de planification interarmées, complété par des outils tactiques de chaque milieu. Des aides numériques à la planification, au ciblage, et à la préparation de missions sont présentes à tous les niveaux du commandement.

(20) La projection de force permet de déployer des structures de commandement, opératives et tactiques, et des réseaux dédiés pour commander et contrôler les unités de combat. Celles-ci sont capables d'utiliser des liaisons satellitaires ou radio. Les aides numériques à la planification, au ciblage et à la préparation des missions sont également présentes à tous les niveaux de commandement. Il convient cependant de noter la moindre irrigation en réseaux au plus près des combattants à terre. En effet, le « poids du sac » constitue un facteur dimensionnant en soi.

(21) Les nouveaux systèmes d'armes et les systèmes d'aide à la décision poursuivent l'intégration du numérique dans des champs variés comme le système de combat aérien du futur, la veille collaborative navale, le système de combat SCORPION de l'Armée de terre ou encore les services de gestion des ressources humaines.

(22) Les outils numériques permettent, par ailleurs, le suivi de la maintenance, la télésanté ou encore la communication avec le monde extérieur tant pour soutenir le moral des combattants que pour externaliser certaines prestations de soutien. À cet égard, les outils augmentent les synergies entre le monde industriel et le monde militaire, avec notamment différents contrats d'externalisation (maintien en condition opérationnelle par exemple) au profit d'une performance accrue. Les outils numériques permettent également d'améliorer les capacités de formation, avec la mise en place de cours en ligne. Les outils numériques civils sont indispensables dans beaucoup de systèmes militaires. Leur acquisition et mise en œuvre par les armées entraînent une expansion de l'environnement numérique militaire. À moins de faire développer des systèmes spécifiques pour les armées, voie qui serait source de coûts et de délais supplémentaires, la transformation numérique du monde civil s'impose, au moins en partie, aux armées.

C. La dualité du « numérique du militaire » : un élément du soutien du moral en même temps qu'un facteur de risque

(23) Par ailleurs, en garnison, sur les bases, en manœuvres ou en opérations, sur terre comme en mer, les militaires, et quelle que soit leur génération, disposent de leurs outils personnels. Le souhait de conserver un lien permanent avec les proches et l'utilisation de ces outils à des fins de divertissement ou d'information font désormais partie de l'univers du militaire. Si le commandement a été conduit à prendre en compte ces besoins au titre de la condition militaire, il lui appartient également, s'agissant des usages du « numérique du militaire », tout à la fois de préserver la mission et la sécurité des militaires et de garantir le respect de leurs droits individuels (droit de propriété, respect de la vie privée et protection des données personnelles.)

P2 : La superposition des usages personnels et professionnels impose de rechercher le juste équilibre entre des impératifs et des exigences possiblement contradictoires :
- le respect du droit de propriété du militaire ainsi que la préservation de sa vie privée et de ses données personnelles ;
- le respect de la propriété intellectuelle et les exceptions que pourraient réclamer les opérations ;
- les impératifs de la mission, la sécurité des militaires et les obligations disciplinaires résultant de l'état militaire ;
- la nécessité pour le commandement de veiller au moral de leurs subordonnés.

II. Analyser les avantages opérationnels pour mieux identifier les tensions

P3 : La conception, le développement et l'emploi d'outils numériques doivent s'inscrire dans un cadre permettant de : respecter l'interdiction de produire, mettre en œuvre et vendre des armements et biens à double usage contraires aux engagements internationaux de la France ; conserver notre supériorité opérationnelle tout en préservant nos valeurs et les impératifs constitutionnels qui s'imposent à l'action de nos forces, à savoir la sauvegarde des intérêts fondamentaux de la Nation, au nombre desquels figurent l'indépendance de la Nation et l'intégrité du territoire.

A. Anticipation stratégique et ambivalence numérique

(24) L'actualisation 2021 de la revue stratégique évoque un contexte géopolitique durci, dans lequel nos militaires sont extrêmement sollicités, et qui impose de rechercher les outils —notamment numériques—qui permettent de préserver ou d'améliorer la capacité opérationnelle des armées. C'est ainsi que le concept d'emploi des forces identifie neuf facteurs de supériorité opérationnelle appliqués à l'art de la guerre, dont la recherche et la combinaison sont de nature à permettre la prise d'ascendant sur l'adversaire :

- la performance du commandement, influx nerveux s'appuyant sur le principe de subsidiarité ;
- la force morale, individuelle et collective, prérequis de la résilience et facteur d'ascendant sur l'adversaire ;
- la compréhension, permettant l'anticipation optimale et l'action pertinente ;
- l'agilité, capacité permanente à aménager l'action, y compris dans des conditions hors normes ;
- l'influence, critique dans l'environnement informationnel actuel et futur ;
- l'endurance, combinant contrôle du tempo, patience et persévérance ;
- la foudroyance, aptitude à frapper avec puissance, rapidité et soudaineté pour surprendre et sidérer ;
- la crédibilité, participant à la dissuasion et appuyant la conduite de l'action ;
- la masse, pour établir les rapports de force favorables et répondre à la simultanéité des crises.

(25) Le concept d'emploi des forces évoque, toutefois le numérique dans ses ambivalences : « *La forte croissance de la numérisation de nos systèmes d'armes est un atout opérationnel mais elle crée autant de vulnérabilités potentielles à des cyberattaques qui peuvent produire des effets très ciblés ou globaux pouvant aller jusqu'à briser toute forme d'action militaire avant même son déclenchement. En sus des systèmes d'armes, le numérique innerve jusqu'à la capacité de décision. La protection et la défense de la disponibilité, de l'intégrité et de la confidentialité des données et de leur traitement sont donc essentielles. L'exploitation des vulnérabilités numériques d'un adversaire peut offrir un avantage opérationnel décisif dans l'affrontement par l'entrave de ses systèmes d'armes, la captation de ses données ou la modification de sa perception de l'environnement. (…) Accélérant la circulation de l'information, la transformation numérique entraîne une transparence accrue, réelle ou apparente, et un écrasement du temps. Elle conduit les opinions à l'impatience et met sous tension les capacités d'analyse et de décision, au risque de générer une précipitation contreproductive (…)* ».

(26) Le recours au numérique et l'affectation de certaines fonctions de calcul à des machines ne sont pas, en eux-mêmes, contraires à l'honneur militaire et aux valeurs des armées françaises.

B. Un facteur de supériorité

(27) Le recours au numérique permet d'augmenter les performances des systèmes opérationnels et constitue assurément un facteur de supériorité au titre des 5P (permanence, précision, pertinence, protection, performance), à l'instar des SALIA (systèmes d'armes létaux intégrant de l'autonomie).

(28) Le numérique offre vitesse, précision et partage de situation. Il accélère le cycle OODA[2], assure la pertinence des frappes (précision GPS) et accroît la précision du renseignement et des dossiers d'objectifs (exploitation de grandes bases de données).

(29) Il est aussi un outil de collaboration et de coordination indispensable car il assure une meilleure protection (« – géolocalisation amie, tir à distance, systèmes d'autoprotection), offre une situation tactique améliorée (liaison de données au-delà de l'horizon, information du commandement supérieur, partage avec les alliés). Il permet une collaboration aussi bien d'homme à machine qu'entre alliés, services interministériels et entreprises (maintenance).

(30) Au titre de la performance, les outils numériques permettent de :

- Faire face à l'accélération du tempo des opérations militaires : la boucle « OODA » tend à s'accélérer dans le cadre des engagements opérationnels ; cela signifie que le délai entre la perception d'une menace (ex : missiles hypervéloces…) par des capteurs (satellites, drones, guets à vue, etc.) et sa neutralisation par les forces armées tend à décroître sensiblement. Un facteur clé de succès consiste ainsi à ce que le tempo de cette boucle soit plus rapide que celui de la partie adverse. Il en va de même face à certaines attaques informatiques qui peuvent s'avérer fulgurantes, nécessitant alors une capacité de défense extrêmement réactive.

- Se défendre face à des acteurs en masse : on assiste à la réémergence de préoccupations de masse d'équipements militaires disponibles. Il devient nécessaire à la fois de disposer des forces suffisantes au sol, en mer et dans les airs pour opérer dans des zones de conflit aussi vastes que le Sahel, mais aussi d'être en mesure de se défendre contre des attaques par saturation, comme par exemple une attaque qui emploierait un essaim de petits drones armés à l'encontre d'une position stratégique, éventuellement perpétrée par un groupe terroriste. Ces attaques par saturation constituent également un mode d'action qui exploite des failles logicielles et qui pourraient émerger dans l'espace exo-atmosphérique. L'intégration des capacités avancées de calcul ou de transmission dans certains systèmes de combat permet de faire face à de telles situations opérationnelles, qui combinent un tempo rapide, un environnement complexe et une grande quantité d'objectifs. Les développements technologiques à venir dans les états-majors et systèmes d'armes sont susceptibles de donner à nos militaires une meilleure capacité d'apprécier une situation.

- Maintenir le rang des armées françaises et leur interopérabilité en coalition : la défense française doit maintenir un rythme de développement garantissant son interopérabilité, sa place parmi ses alliés et sa capacité à tenir le rôle de nation-cadre. De fait le partage d'informations reste un facteur essentiel pour toute planification interalliée et toute conduite d'opérations en coalition.

[2] observation – orientation – décision -action

(31) La **pertinence d**es outils numériques permet aux forces de :

- **S'adapter à une grande masse de données** : le développement des capteurs comme, par exemple, ceux qui produisent des images, des signaux électromagnétiques, des signatures acoustiques, des informations de détection d'attaque informatique, est arrivé à un point tel que certains parlent de « déluge de données ». Cette masse d'informations constitue un véritable défi pour l'exploitation du renseignement et la prise de décision opérationnelle au sein d'un centre de commandement. Elle affecte aussi directement le militaire engagé en opération, qu'il soit en mer, sur le terrain ou dans un cockpit, et dont l'environnement est de plus en plus numérisé et interconnecté avec l'ensemble de la chaîne de commandement, par messagerie instantanée ou par liaison de données tactiques. On parle, dès aujourd'hui, de combat connecté et d'informatique en nuage du théâtre d'opérations (*cloud* tactique). De tels moyens interconnectent les systèmes d'armes qui doivent et devront traiter toujours plus d'informations afin d'éviter la saturation cognitive du militaire contre laquelle le service de santé des armées mène déjà des recherches.

- **Affecter aux machines les tâches répétitives** : les capacités offertes par les nouvelles technologies facilitent la focalisation de l'attention humaine sur les tâches réputées à haute valeur ajoutée pour l'être humain.

(32) Les outils numériques permettent également d'améliorer **la précision des actions** : l'intégration d'algorithmes avancés et la précision poussée des images sont susceptibles d'améliorer les modèles et les options présentées au décideur, ainsi que la précision de frappes sur un objectif et l'estimation préalable de dommages collatéraux potentiels, grâce aux capacités d'intégrer davantage de paramètres, parmi lesquels les caractéristiques physiques des objets par exemple, ou une réalité « augmentée », susceptible de fournir des informations difficiles à comprendre pour un humain (cf. les photo-interprètes). Ils permettent en outre au militaire de s'affranchir de difficultés d'ordre environnemental (la nuit, la météo), sources de stress ou de fatigue (situation tactique partagée), pour mobiliser toutes ses capacités cognitives sur les aspects les plus critiques de la mission. D'autres technologies embarquées dans les systèmes d'armes sont à même d'offrir au militaire la possibilité de s'affranchir de conditions météorologiques dégradées (vent, pluie, neige, brouillard, etc.) en améliorant les conditions d'accomplissement de sa mission et en réduisant les risques d'erreur.

(33) En matière de **protection**, les outils numériques associés aux moyens de transmission modernes contribuent à préserver la vie et la santé des militaires : le combat est en partie possible à distance, les systèmes assurent la veille nécessaire.

(34) Enfin, les outils numériques autorisent une plus grande **permanence** au combat. Les développements technologiques permettent aujourd'hui de construire des systèmes pilotés ou assistés par ordinateur. Il est ainsi possible de durer en mer (bâtiment) ou dans le ciel (pilotage automatique) ou d'assurer l'observation nécessaire aux groupes de combat au sol.

(35) Ainsi le numérique est devenu, en trois décennies, l'un des facteurs essentiels de la supériorité opérationnelle.

(36) Les évolutions technologiques à venir auront un fort impact sur les opérations, ainsi par exemple le déploiement de la 5G, la cryptographie quantique, les systèmes à base d'apprentissage machine. Mais

le maintien de la chaîne de commandement et de la responsabilité humaine demeurent indispensables.

P4 : Les perspectives aujourd'hui ouvertes dans le numérique imposent la poursuite des travaux de recherche dans les domaines émergents avec comme axe d'effort la performance dans l'aide à la décision associée à la maîtrise par l'être humain et le commandement en particulier.

(37) S'il présente des intérêts certains sur le plan opérationnel, l'environnement numérique n'est pas neutre sur le plan décisionnel (risque de dilution des responsabilités, risques d'altération du contrôle de l'humain, risques induits par les vulnérabilités intrinsèques au numérique, risques de déshumanisation, risque de rupture de la continuité d'activité opérationnelle). Il en résulte des tensions éthiques variées liées à la superposition des usages personnels et professionnels, aux exigences de la transparence, à la superposition de plusieurs cadres législatifs, à l'apprentissage machine ou au choix entre sécurité et vie privée.

III. Des tensions éthiques à surmonter et dépasser

A. Résilience opérationnelle et autonomie décisionnelle du combattant

(38) La tendance au « tout numérique » rend le combattant dépendant de cet univers qui, s'il lui reste inconnu dans son fonctionnement technique, génère dans la durée une réelle dépendance fonctionnelle. La préservation de l'aptitude à décider en l'absence des moyens numériques habituels est à la fois une exigence opérationnelle et une exigence éthique. Elle constitue en effet une garantie de lucidité et de discernement La capacité de décider en environnement dégradé doit donc être préservée par des exercices réguliers.

R2 : Entraîner à la résilience en conditions numériques dégradées pour assurer la meilleure décision en permanence.

B. Commandement fluidifié et subsidiarité

(39) Le numérique permet de fluidifier la circulation des informations de circuler selon l'objectif « *la bonne information au bon endroit au bon moment* ». La tentation peut alors naître d'écraser les niveaux de commandement au détriment de la chaîne de subsidiarité. La subsidiarité doit être préservée dans toute la mesure du possible car elle permet de garantir à chaque commandant de disposer de l'information pertinente de son niveau, de décider dans le cadre des délégations qui lui ont été accordées, tout en bénéficiant d'une meilleure appréciation de situation au profit du principe stratégique de liberté d'action.

R3 : Peser systématiquement l'intérêt de l'ingérence du niveau hiérarchique N vers le niveau hiérarchique N-1 voire N-2.

C. Sécurité et autonomie de décision

(40) Le numérique est aujourd'hui présent dans l'ensemble des systèmes d'armes. Il constitue une force, en améliorant la maîtrise de l'information. Il offre, toutefois, l'opportunité à des acteurs malveillants, étatiques ou non, de conduire des attaques, elles aussi numériques. Par ailleurs, des acteurs étatiques et non étatiques sont dotés de capacités de renseignement en source ouverte ou cyber offensives qui pourraient permettre de prendre le contrôle ou de modifier l'intégrité du système, d'influencer l'appréciation de situation et ainsi de modifier des décisions (choix des cibles, règles d'engagement à respecter). Enfin, les capacités adverses exploitent les traces numériques laissées involontairement par le combattant et son environnement personnel.

R4 : Éduquer aux risques de sécurité liés au numérique, qu'il soit à usage personnel ou professionnel.

(41) Les logiciels, mécanismes et autres moyens informatiques peuvent présenter des vulnérabilités intrinsèques. Une attaque informatique pourrait leurrer le système voire en prendre le contrôle à distance. Parmi les modes d'actions identifiés, on peut citer l'empoisonnement des données, l'insertion de portes dérobées accessibles par un attaquant et la pression sur le combattant par action sur son environnement numérique personnel.

(42) L'absence de souveraineté française sur certains équipements ou fonctions, en particulier la cryptographie, laquelle permet l'autonomie du commandement à distance, pèse aussi via les atteintes possibles à l'intégrité ou à la confidentialité.

(43) Sécurité et décision sont liées. Un système au niveau de sécurité approuvé et assumé par l'autorité fonctionnelle garantit l'autonomie d'appréciation et une décision intègre.

R5 : La mise en service opérationnelle doit assumer ou traiter les risques d'altération de l'autonomie d'appréciation, de la capacité de décision et de la décision elle-même, risques qui seraient liés à des défauts de sécurité ou de souveraineté.

D. Numérique et principe de responsabilité

(44) Un outil numérique étant un objet physique, aucune responsabilité ne peut lui être imputée. Autrement dit, comme pour les systèmes d'armes, l'exploitation d'outils numériques, qu'elle soit consentie ou subie, ne saurait faire écran et exonérer de leurs responsabilités ceux qui, soldats ou non, autoriseraient, commanderaient ou conduiraient des actions militaires ayant pour effet de violer le droit des conflits armés ou de constituer des infractions au droit pénal français. Il en irait de même pour les concepteurs ou opérateurs de maintenance ou de la formation.

P5 : La responsabilité humaine dans la conception, le déploiement et l'emploi d'outils numériques, constitue un principe indérogeable. Les valeurs les plus hautes de notre éthique comme notre ordre constitutionnel impliquent que soit engagée en toutes circonstances la responsabilité de l'humain. Il convient dès lors de formaliser les chaînes de responsabilité du commandement, du contrôle et de l'exécution quel que soit le niveau de numérisation de l'environnement.

E. Appui à la décision et altération du contrôle humain

(45) Le développement de l'usage des systèmes numériques et la tendance à l'infobésité sont susceptibles d'altérer le contrôle du système par le militaire à différents titres :

- les automatismes altèrent les mécanismes de contrôle classiquement utilisés par le militaire ; par exemple : altération des mécanismes de détection des erreurs, augmentation de la divagation attentionnelle. Ces phénomènes sont susceptibles de provoquer « un risque de légitimation », se traduisant par un excès de confiance accordée aux résultats fournis par le système numérique et induisant une perte d'aptitude du militaire à les remettre en cause ;
- une dépendance[3] au numérique peut conduire l'humain à ne plus vouloir reprendre le contrôle ou à perdre confiance dans sa capacité à appréhender un niveau élevé de complexité ;
- le manque d'informations ou, au contraire, un flot trop abondant d'informations, les différents biais d'ordre cognitif (biais de confirmation, influence, « tunnélisation » attentionnelle, etc.) peuvent entraîner une mauvaise compréhension du comportement du système numérique, donc une mauvaise prédiction, et sont de nature à générer des incidents dont certains potentiellement graves ;
- une extraction progressive de l'humain peut survenir, induite par un tempo de réaction accéléré.

[3] https://www.lesechos.fr/politique-societe/societe/addiction-aux-ecrans-un-tiers-des-francais-se-disent-concernes-1141185 : selon un sondage ELABE, 60% des personnes interrogées se disent incapables de passer une journée sans téléphone.

(46) Ainsi, l'utilisation de systèmes devenus opaques ou complexes pour l'opérateur peut éventuellement aboutir à un phénomène de dépendance, de rejet ou d'ennui vis-à-vis du système. À l'extrême, ces effets peuvent diminuer chez l'humain le sentiment ou la conscience de sa responsabilité propre.

(47) Par ailleurs, l'intégration généralisée du numérique dans les fonctions critiques peut mettre à distance le militaire vis-à-vis de l'opération en cours, en altérant son jugement et sa perception de la situation opérationnelle.

(48) En effet, si l'humain n'a pas accès à certaines informations contextuelles de terrain, la question se pose de sa capacité à appréhender la globalité de ce que fait le système. Il peut s'ensuivre une perte de coordination entre les actions et une altération du sentiment de contrôle de l'humain, qui le mettrait à distance de l'opération : en particulier l'humain pourrait se sentir moins impliqué dans les actions d'ouverture du feu et il pourrait en découler un détachement et une perte d'humanité dans les actions de combat. Le sentiment de responsabilité est surtout susceptible de diminuer si la machine fait « beaucoup » à la place de l'humain, en particulier du point de vue de l'aide à la décision.

R6 : Évaluer systématiquement lors de la recherche, de la conception, du développement et de l'emploi de systèmes numériques, les effets sur la psychologie et les comportements humains tels que la distanciation et l'hypovigilance. Concevoir d'emblée les systèmes numériques comme des systèmes humains-machines et non des machines avec lesquelles les humains doivent composer.

(49) La confiance dans un système repose sur sa qualification, sa certification et sur l'assurance qu'il fait uniquement ce pour quoi il a été conçu, que ce soit dans un cadre strictement national ou en coopération. Si le système comprend des algorithmes fondés sur de l'apprentissage machine, les données utilisées pour l'apprentissage lui-même et sa qualification doivent être caractérisées. Cependant, les corrélations calculées par ce type d'algorithmes étant essentiellement asémantiques, c'est-à-dire dépourvues de sens pour un humain, il est parfois difficile de pouvoir construire une explication intelligible du résultat fourni. Une certaine méfiance pourrait s'installer à l'égard d'un système qui interviendrait pour l'identification, la désignation, voire la neutralisation d'objectifs mais qui ne pourrait fournir des explications intelligibles de ses propositions ou ses choix.

R7 : Définir un niveau de garantie des qualifications du système humain + machine. Le prendre en compte dans la formation et l'utilisation du système.

(50) En corollaire, la confiance dans le système numérique peut se trouver diminuée au regard de la situation opérationnelle. Le combattant peut devoir choisir entre suivre les résultats de calculs de la machine et sa propre appréciation de situation. Ce dilemme est courant et doit être porté à la connaissance du commandement, y compris dans un cadre multinational. Si l'humain peut aisément se reposer sur la machine, cette situation doit cependant pouvoir être remise en cause, en toute conscience et responsabilité (sortie volontaire d'un domaine de vol, connaissance d'un élément supplémentaire non calculé par la machine).

R8 : Évaluer la part d'erreur humaine que le commandement est prêt à accepter lorsque les estimations ou résultats fournis par le système numérique sont contredits par l'appréciation du combattant au regard du contexte et en définitive responsable de ses actes.

(51) L'évolutivité forte des systèmes d'information et l'apparition de nouvelles fonctionnalités devraient impliquer une revue régulière de la doctrine pour maintenir un emploi optimal des systèmes. La remontée des retours d'expérience opérationnels et leur diffusion sont donc essentielles, au sein de tous les cercles aussi bien opérationnels que techniques ou juridiques.

R9 : Assurer la remontée des retours d'expérience opérationnels liés à l'usage des systèmes d'information et leur diffusion à tous les cercles opérationnels mais aussi aux autorités compétentes dans les domaines techniques et juridiques.

F. Légitimité de la recherche et nécessité du contrôle de licéité

(52) La recherche et l'innovation dans le numérique militaire et les développements issus du numérique civil doivent demeurer des axes d'effort pour la DGA et les armées. Le Comité observe que conformément à la doctrine des armées françaises si le moyen numérique est susceptible -par lui-même ou au regard de l'outil effecteur auquel il est pleinement intégré- d'endommager ou de détruire un système ou une capacité adverses, il doit faire l'objet du contrôle de licéité mis en œuvre pour l'application de l'article 36 du protocole I additionnel aux Conventions de Genève du 12 aout 1949.

R10 : Définir des modalités de contrôle de licéité adaptées aux enjeux de la numérisation des outils du combattant.

G. Avantages induits par les outils et risques pour les utilisateurs

(53) Le Comité considère que les facteurs humains doivent faire l'objet d'une attention particulière. Les situations à risque évoquées précédemment impliquent, en effet, que la formation des militaires prenne en compte :

- l'interaction homme / machine et un possible excès de confiance dans les automatismes qui peut survenir par glissement ;
- le niveau d'implication du militaire pour éviter la distanciation par rapport aux opérations ;
- le besoin d'une juste distance par rapport aux résultats des systèmes numériques et la connaissance des limites du système que cela suppose.
- la relation à la responsabilité dans les actions de feu et à la prise de décision dans les situations de combat les plus critiques, avec un niveau d'incertitude résiduelle.
- Les risques de sécurité qui pèsent par la juxtaposition des outils numériques personnels et professionnels.

(54) La formation et l'entraînement, regroupés aujourd'hui sous le terme de préparation opérationnelle, sont essentiels à l'appropriation par les armées des systèmes numériques, et à la maîtrise de la force et de la sécurité dans les situations les plus extrêmes, en validant les acquis individuels et collectifs.

R11 : Assurer une préparation opérationnelle continue et à jour des outils numériques des chefs stratégiques, commandeurs de théâtres, chefs tactiques et opérateurs de systèmes numériques.

(55) Le Comité considère que l'effort consenti dans la formation et dans la préparation opérationnelle doit être maintenu et être adapté, autant que nécessaire, au niveau de complexité et au nombre croissant des outils numériques, même si ces derniers sont simples et ergonomiques en apparence. En vue de maîtriser parfaitement le système dans tout son spectre d'emploi et d'en connaître les limites, chaque

militaire doit être sensibilisé aux risques liés au facteur humain. Il doit également être capable d'interpréter les informations du système.

R12 : Sensibiliser l'usager militaire tant sur les risques de sécurité que sur les effets de l'usage du numérique en termes de facteur humain.

(56) Les travaux de rédaction de doctrines d'utilisation doivent veiller à éduquer et sensibiliser les acteurs militaires à l'environnement numérique. Les effets du numérique sur la subsidiarité du commandement, sur la déformation de la réalité des sens humains et sur la résilience seront également documentés.

R13 : S'assurer de la prise de conscience des écarts entre représentation calculée et représentation ressentie de la réalité au travers d'exercices de biais, de saturation et de travail en ambiance numérique dégradée.

(57) Les traces numériques générées par certains outils (journaux de sessions par exemple) sont susceptibles d'amener des questions contrefactuelles (« s'il avait suivi ou s'il n'avait pas suivi la machine il aurait ou n'aurait pas commis telle action »). La transparence (ce que je m'engage à dévoiler spontanément sur demande) doit donc se fonder sur des objectifs acceptables tant pour le commandement que pour la société, dans une logique de responsabilité pleine et entière du commandement.

R14 : En dépit des capacités de stockage importantes offertes par le numérique, la transparence à tout prix ne doit pas constituer un objectif en soi.

H. Vie privée et vie professionnelle

(58) Les outils numériques privés (personnels, massivement présents au plus près du combattant, lui permettent d'entretenir des relations avec ses proches (messagerie, réseaux sociaux), d'accéder à des loisirs (jeux en ligne) et de faciliter la gestion de ses affaires courantes (services en ligne). Ils peuvent également être utilisés pour un usage opérationnel, par commodité ou par défaut d'autres moyens, ce qui induit des problématiques spécifiques tant sur le plan de la performance opérationnelle (vulnérabilité cyber notamment) que sur un plan psychologique (brouillage des distinctions entre les différentes sphères). Il s'agit d'une thématique qui n'est pas propre au monde militaire. Mais les caractéristiques de ce dernier induisent une vigilance particulière.

(59) Ainsi qu'il a été dit ci-dessus (principe directeur n°2) les outils personnels et les données personnelles du militaire sont protégées par le Règlement général sur la protection des données (RGPD) notamment. En revanche la singularité de l'état militaire, la primauté de la mission et les devoirs qui en résultent pour tous les membres de la communauté militaire font obstacle à ce que les problématiques touchant à l'usage des outils numériques personnels soient appréhendées sous un angle purement individuel et dans le cadre du droit commun. Ainsi, tant le droit à la vie privée que les impératifs de la mission, les pouvoirs du commandement et les devoirs du militaire à l'égard de l'institution ou de ses camarades, sont encadrés par le Code de la défense (dernier alinéa de L 4121-2), ainsi que par un corpus doctrinal (Utilisation d'Internet à des fins privées dans le cadre de la condition du personnel en opération, La condition du personnel en opération, Guide du bon usage des réseaux sociaux).

(60) Il convient en outre de sensibiliser et d'éduquer en permanence les militaires aux risques d'addiction, de dépassement des interdits, d'isolement social, dans le cadre de formations adaptées aux technologies et outils numériques. La recherche par le service de santé des armées, des actions simples de cohésion ou de rappels d'hygiène numérique permettront cette sensibilisation. Les interférences entre informations issues des outils personnels et issues des outils professionnels peuvent créer des artefacts susceptibles d'orienter la décision. Il y a là une tension éthique entre possibilités techniques des outils personnels et responsabilité du décideur. Ainsi, une information issue de la presse peut arriver plus rapidement par les canaux personnels plutôt que par les canaux professionnels.

R15 : Éduquer aux risques professionnels liés au numérique à usage personnel.

R16 : Éduquer aux risques personnels liés au numérique à usage professionnel

(61) Par ailleurs, les impératifs de sécurité doivent être expliqués au regard des opérations et du personnel, par exemple le suivi géographique du personnel à bord d'un bateau pour raisons de sécurité. Dans ce cas particulier l'effacement des données personnelles numériques laissées par le militaire ou l'archivage selon des directives juridiques ministérielles doit être la règle une fois l'opération militaire réalisée.

(62) Les outils numériques personnels constituent désormais un facteur du moral du combattant. Mais les outils personnels représentent des dangers pour la sécurité des opérations. Ils sont sources de traces numériques involontaires, de vulnérabilités techniques potentielles ou de canaux d'information divergents. Le commandement doit donc concilier la gestion du moral de la troupe avec l'efficacité de la mission.

R17 : Former le commandement à gérer l'articulation des vies privées et professionnelles, la gestion du moral de la troupe et la sécurité de la mission, dans le respect de lois et règlements.

Mission et composition du comité d'éthique de la défense

Le comité d'éthique de la défense a été installé le 10 janvier 2020 par la ministre des armées. Il est chargé d'éclairer par ses avis et recommandations les autorités politiques et militaires sur les questions éthiques soulevées par les évolutions de la fonction militaire et les innovations scientifiques et technologiques dans le domaine de la défense. Il est composé de 18 personnalités qualifiées nommées par la ministre des armées.

Il est composé comme suit :

Bernard PECHEUR	Président du comité d'éthique de la défense, Président de section (h) au Conseil d'État
Henri BENTEGEAT	Vice-président du comité d'éthique de la défense, Général d'armée (2S), ancien chef d'état-major des armées
Rose-Marie ANTOINE	Administratrice générale honoraire directrice générale de l'ONACVG de 2012 à 2019
Christine BALAGUE	Professeure IMT-BS, Titulaire de la chaire Good in Tech
Marie-Germaine BOUSSER	Professeure émérite de neurologie, membre de l'Académie nationale de médecine
Frédérick DOUZET	Professeure à l'Institut Français de Géopolitique (Université Paris 8), directrice de GEODE
Hervé DREVILLON	Professeur d'Histoire à l'Université Paris I (Panthéon-Sorbonne)
Michel GOSTIAUX	Ingénieur en chef de l'armement
Laurent HERMANN	Contre-amiral
Jean-Baptiste JEANGENE VILMER	Directeur de l'Institut de recherche stratégique de l'école militaire
Aurélie LECAM	Commissaire des armées , juriste
Bruno PAUPY	Colonel de l'armée de l'air et de l'espace
Philippe ROUANET de BERCHOUX	Médecin général des armées, directeur du Service de santé des armées
Guillaume SCHLUMBERGER	Contrôleur général des armées en mission extraordinaire
Catherine TESSIER	Ingénieure experte à l'Office national d'études et de recherches aérospatiales, référente intégrité scientifique et éthique de la recherche de l'ONERA
Nicolas THERY	Président de la Confédération Nationale du Crédit Mutuel
Cathy THILLY-SOUSSAN	Conseillère financière, juridique et éthique à la direction générale de l'armement
Bernard THORETTE	Général d'armée(2S) ancien chef d'état-major de l'armée de terre