RDN

L'officier au service de la Nation dans le monde du XXIe siècle

Les Cahiers de la
Revue Défense Nationale

Sigem 2018

L'officier au service de la Nation dans le monde du XXI^e siècle

Préparation
Audrey HÉRISSON

Sommaire

L'officier face aux défis du XXIe siècle

Ces articles sont issus des publications de la *Revue Défense Nationale* : dans son édition mensuelle ou dans sa *Tribune*.

La *Revue Défense Nationale* est éditée par le Comité d'études de défense nationale
(association loi de 1901)
Adresse géographique : École militaire, 1 place Joffre, bâtiment 34, PARIS VII
Adresse postale : BP 8607, 75325 PARIS CEDEX 07
Fax : 01 44 42 31 89 - www.defnat.fr - redac@defnat.com
Directeur de la publication : Alain COLDEFY - Tél. : 01 44 42 31 92
Rédacteur en chef : Jérôme PELLISTRANDI - Tél. : 01 44 42 31 90
Rédactrice en chef adjointe : Audrey HÉRISSON
Secrétaire général et *webmaster* : Paul LAPORTE - Tél. : 01 44 42 31 91
Secrétaire général de rédaction : Pascal LECARDONNEL - Tél. : 01 44 42 43 69
Assistante de direction et secrétaire de rédaction : Marie-Hélène MOUNET - Tél. : 01 44 42 43 74
Secrétaire de rédaction : Jérôme DOLLÉ - Tél. : 01 44 42 43 69
Abonnements : Éliane LECARDONNEL - Tél. : 01 44 42 38 23
Chargés d'études : Laurent HENNINGER et Emmanuel DESCLÈVES - Tél. : 01 44 42 43 72
Comité de lecture : Marie-Dominique CHARLIER-BAROU, André DUMOULIN,
Jean ESMEIN, Sabine DE MAUPEOU et Bernard NORLAIN
Régie publicitaire (ECPAD) : Karim BELGUEDOUR - Tél. : 01 49 60 58 56
DL 92885 - 1er trimestre 2018 - ISSN : 2105-7508 - CP n° 1019 G 85493 du 4 décembre 2014
Imprimée par BIALEC, 23 Allée des Grands Pâquis, 54180 HEILLECOURT

L'officier au service de la Nation dans le monde du XXIe siècle

Comme chaque année, le numéro dédié au Séminaire interarmées des grandes écoles militaires (Sigem) des *Cahiers de la* Revue Défense Nationale présente des textes rédigés par des auteurs aux parcours variés, abordant des sujets de nature à appuyer le jeune officier dans sa réflexion. Ils confortent certains acquis, apportent des amorces de réponses ou abordent des sujets prospectifs. Ce questionnement, enrichi durant les cinq jours du séminaire, contribue à donner du sens à une formation puis à un parcours empreint de tradition et de modernité, dans un monde en perpétuelle évolution auquel il convient de se donner les moyens de s'adapter. L'officier a le devoir de se remettre en cause constamment, de suivre voire d'anticiper les situations auxquelles il se trouve confronté. En effet, fort de valeurs fondatrices, il a bien pour vocation de prendre en compte la transformation inéluctable de son époque qui va de pair avec certains défis du siècle, aux contours de plus en plus difficiles à définir et se modifiant de plus en plus rapidement.

L'officier entre tradition et modernité

Il est aisé d'opposer ces deux termes qui finalement s'avèrent complémentaires et trouvent leur synthèse dans l'état d'officier. En effet, transmettre par la parole et l'exemple un héritage ancien qui lui est devenu familier correspond à cet état d'officier, à l'aune des vertus et des valeurs qu'il représente.

Si les vertus humaines et citoyennes (respect, tolérance, solidarité, honnêteté, dévouement, enthousiasme, fierté…) se trouvent partagées par un grand nombre, les qualités intellectuelles et professionnelles qui fondent la spécificité du milieu des armées (disponibilité, réactivité, initiative, autonomie, faculté d'adaptation, courage…) sont plutôt reconnues au militaire.

Le soldat est le seul, au sein de la Cité, à occuper une place unique et singulière : il porte les valeurs de la communauté, ambassadeur et symbole à la fois ; il en est le bras armé, au service de son pays dont il défend les intérêts ; il peut aller jusqu'au sacrifice de sa vie ou, pour un chef, jusqu'à celle de ses hommes. C'est cette vocation particulière, dans la relation à la Nation comme dans la relation à la mort, qui fait que les réalités et les exigences du métier militaire appellent une identité et des valeurs confirmées. Elles transcendent le temps. En outre, ce sont les valeurs éthiques qui guident l'action du chef : exemplarité, honneur, loyauté, écoute de ses subordonnés, sens du devoir, goût de l'action, esprit de sacrifice, culte

de la mission… Au moment du choix, le chef est seul face à lui-même, ce qui constitue sa force, sa liberté, mais aussi une difficulté à surmonter.

Fort de tout cela, l'officier allie tradition et modernité dans un monde qui bénéficie des progrès de la science, de la technique ; dans un monde où l'instantané s'impose. Il s'avère donc nécessaire de conserver un esprit ouvert et curieux, apte à l'intelligence de situation et à la mise en perspective des événements, au discernement, et d'être en capacité d'exercer une critique positive, de réfléchir en homme d'action. En effet, dans son rôle de chef, il lui revient de donner du sens à l'action, fort de ses compétences et de son autorité, car c'est lui qui y prépare les hommes et les femmes placés sous sa responsabilité. Pour les guider dans l'action, il lui appartient avant tout de s'adapter à ceux qu'il encadre. La sociologie des populations évolue et les jeunes engagés d'aujourd'hui revendiquent leur époque comme leurs origines.

Ensuite, il doit s'adapter au milieu professionnel dans lequel il évolue. Les textes et conventions du droit des conflits armés (DCA) viennent d'ailleurs rappeler la judiciarisation croissante, en opérations, des conséquences certes parfois négatives mais aussi positives de la moindre décision. L'institution militaire, également, n'a pas tardé à encadrer depuis plusieurs années maintenant le sujet du harcèlement dont on parle actuellement dans les domaines artistiques, avec la création d'une structure dédiée, des mesures de prévention, un traitement sévère du délinquant et un suivi des victimes.

Justification, judiciarisation, harcèlement, autant de termes conduisant naturellement à la médiatisation. Il n'est pas d'action officielle ou délictueuse qui n'échappe aux médias, à leur manière de présenter les faits au public qui doit être informé. Bien sûr, en ce qui concerne l'officier et plus largement le militaire, informer ceux qui lui font confiance, ceux qui lui reconnaissent sa légitimité au sens juridique du terme, en l'occurrence le peuple français, relève du devoir.

La « grande muette » n'est plus. Le soldat, citoyen à part entière, détient un rôle au sein de la société. Il s'exprime. Ses seules limites sont les conditions statutaires qui régissent son engagement et la sécurité des opérations. Dans ce dernier cas, trop en dire ou parler trop tôt peut engager la sécurité des acteurs impliqués, mais aussi couper court à l'effet de surprise qui constitue un des éléments majeurs du succès au combat. Ainsi, s'il s'avère nécessaire de s'adapter aux nouvelles technologies ; il est important de rappeler qu'il n'est pas possible de tout dire, par exemple sur les réseaux sociaux, même à sa propre famille. Les éléments transmis peuvent être utilisés à mauvais escient par des « *hackers* » mal intentionnés. Là aussi, l'institution militaire a choisi d'encadrer l'utilisation des nouvelles technologies (témoignages, communication institutionnelle, guide du bon usage des réseaux sociaux…).

Il y a matière à une réelle prise de conscience : les jeunes cadres, tous naturellement connectés, excellent dans l'apprentissage et l'usage des nouvelles

technologies, et maîtrisent parfaitement les systèmes d'armes en service ; mais ils ne doivent pas perdre de vue que l'espace numérique constitue un monde en lui-même, un défi de ce monde du XXIe siècle. Il faut se donner les moyens d'en connaître les contours, comme il faut se donner les moyens de connaître la teneur des autres défis modernes, afin de se positionner en conséquence.

L'officier face aux défis du XXIe siècle

Comment définir les contours d'une mondialisation qui s'impose sans limites et qui génère une complexité sans fin ?

Appréhender la complexité revient à s'interroger sur de nombreux domaines de connaissances. Celle-ci naît de l'enchevêtrement de plusieurs paramètres qui s'influencent les uns les autres. Un système se crée, qui est donc complexe par essence. Par conséquent, que dire du monde d'aujourd'hui ? Tout y est lié ; tout a une influence sur un ou plusieurs domaines de connaissance ou d'action. Ce monde constitue bien un système qui présente les caractéristiques de la complexité. L'officier, dans sa dimension citoyenne comme dans son acception humaine et professionnelle, se trouve alors, de fait, confronté à la complexité. Appelé à prendre des décisions, il appréhende nécessairement de nombreux facteurs simultanément.

Peut-on résumer les défis modernes à la complexité née des conséquences de l'après-guerre froide, c'est-à-dire à la fin de l'ordre bipolaire et à l'avènement d'une mondialisation où l'acteur privé l'emporte sur l'acteur étatique ? Cette question nécessite encore investigations et réflexions. Car pour demeurer dans l'action et ne pas subir, il faut savoir s'adapter. Et l'adaptation appelle la réflexion, le questionnement.

Le XXIe siècle (comme les précédents) comporte des caractéristiques résultant de l'histoire comme de la géographie, souvent motifs majeurs de choix stratégiques pour un État. Mais ce siècle voit aussi se développer de plus en plus de formes de guerre nouvelles. L'action militaire se déroule dans un espace où la frontière et la défense du sanctuaire national n'ont plus la même signification qu'aux siècles précédents. Ce siècle dévoile un faisceau d'acteurs multiples, des groupes armés transnationaux (*Daech*), une moindre distinction entre le militaire et le civil au combat.

Dans ces guerres sans États, sans frontières, de nouveaux acteurs veulent imposer des intérêts privés (mafias), idéologiques ou nihilistes (terrorisme). On voit bien, notamment, que le terrorisme a pour objectif de faire douter, de détruire un ordre fondé sur des valeurs universelles, afin de déstabiliser la Démocratie, l'État-Nation, la société, les traditions d'humanisme qui ont porté des générations, et instaurer, au mieux un autre ordre, au pire le chaos. Et le chaos d'aujourd'hui, loin d'être celui que la Grèce antique a pu connaître, se définit par un manque de distinction entre périodes de paix et de guerre, par une difficulté à définir ces

nouvelles guerres. Une part de l'action subversive de ce nouveau siècle a d'ailleurs commencé à s'insinuer chez chacun, par la voie d'*Internet*. C'est donc l'ensemble des citoyens qui doit prendre conscience et s'organiser pour résister à un ennemi qui attaque par voie dématérialisée, c'est-à-dire dans le champ de l'immatériel, nos valeurs morales et intellectuelles. L'institution militaire a, quant à elle, réagi par la création du Commandement de la cyberdéfense des armées, confirmant, par là, la prise en compte de l'espace numérique comme nouveau champ de bataille. La *Revue stratégique de défense et de sécurité nationale* est venue valider cette approche des nouvelles menaces qui touchent le pays.

Il revient donc à l'officier de s'adapter à ces nouveaux enjeux et d'apporter sa contribution en confirmant sans relâche les valeurs dont il est reconnu garant. Il emmènera ainsi par l'exemple, le dialogue, l'affirmation de ses convictions, la force de son opinion, le maximum de citoyens dans son sillage.

Pour se forger ou conforter une opinion, l'officier ne doit pas vivre en dehors du temps, ou trop tourné vers le passé, surtout s'il ne sait pas en transcender les valeurs utiles. Il doit se donner les moyens de s'adapter aux défis de tous ordres, qu'ils soient internes au regard de son métier ou externes, en commençant par celui apporté par les nouvelles technologies.

Servir la Nation aujourd'hui, nécessite plus que jamais une connaissance de facteurs nombreux et variés qui, telle une mosaïque, constituent le monde dans lequel l'officier évolue. Allier tradition et modernité pour s'adapter aux défis du siècle demande de l'abnégation.

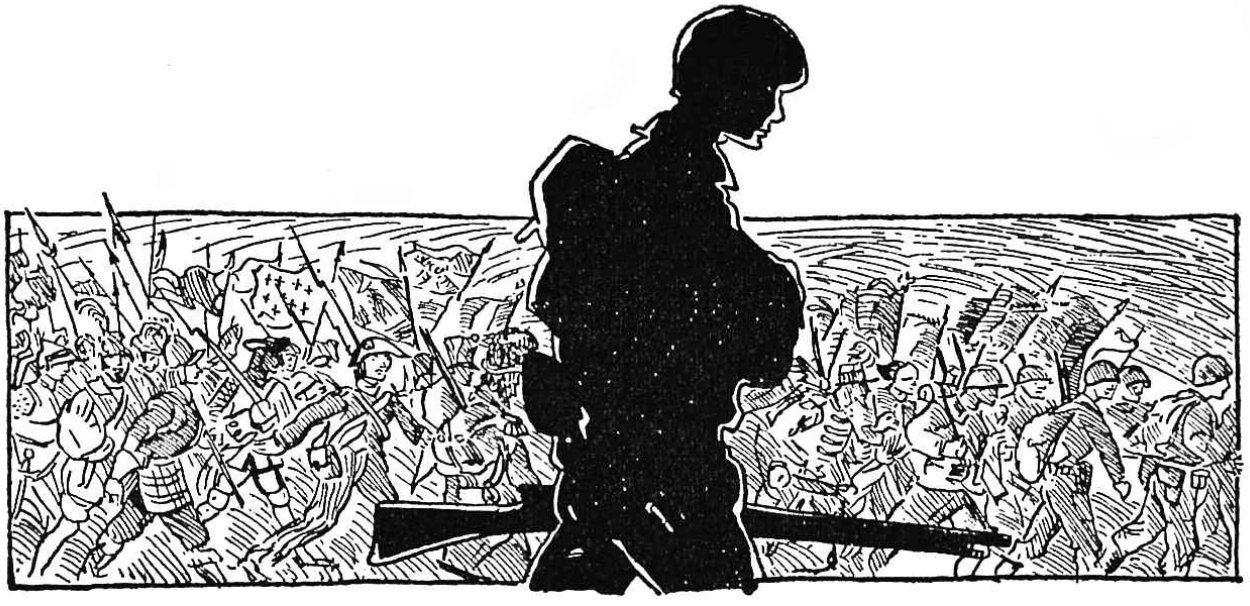
Pour aider l'officier à relever ces défis, les objectifs du Sigem s'articulent en :

- un premier brassage interarmées ;
- une réflexion approfondie sur le sens de l'engagement au service de la Nation, de l'État et de ses forces armées ;
- l'acquisition d'un début de culture sur l'outil de défense, les responsabilités de commandement et l'environnement complexe dans lequel le futur officier est appelé à évoluer.

C'est ainsi que le Sigem a pour ambition, dans le cadre des programmes de formation dispensés dans les écoles, de rappeler combien il importe d'affirmer les valeurs qui portent l'officier dans son action. Cette ambition, empreinte d'humanité, se nourrit du passé et évolue sous la poussée de paramètres extérieurs qu'il convient d'intégrer et non de rejeter. L'officier bénéficie d'une formation de nature à lui permettre d'effectuer des choix et ce, dans le périmètre de ses responsabilités. Il lui appartient de demeurer le véritable acteur de sa formation.

Général (2S) Anne GIUBBI
Directeur du Sigem 2018

L'officier entre tradition et modernité



Les Cahiers de la Revue Défense Nationale

L'officier d'aujourd'hui doit se mouvoir entre tradition et modernité, entre permanence et évolution. Dans un siècle marqué par l'accélération du tempo, que ce soit celui des échanges entre les hommes ou celui des évolutions technologiques, l'officier doit être un « socle » sûr et solide, un rappel de la permanence des grands principes qui font tourner le monde. La guerre est en effet aussi vieille que le monde des hommes, même si elle prend des aspects différents selon les époques et les lieux.

La guerre a forgé à travers les âges ce qu'est le militaire, mais également l'officier, d'aujourd'hui. L'histoire a formé les valeurs des soldats, quel que soit le milieu (terre, mer, air, Espace) ou le service dans lequel il évolue, valeurs qui sont transmises de génération en génération au travers de la formation militaire et de l'engagement opérationnel.

L'article « Vous avez dit militaire ? » rappelle que les valeurs objectives du marin comme du soldat le différencient de tout autre détenteur d'un engagement civil. L'esprit d'équipage ou de corps, l'exigence au combat, le sens de la disponibilité, l'aptitude à vivre et à durer dans des conditions contraignantes, le goût de l'aventure ou la maîtrise des risques sont quelques-unes de ces valeurs bien spécifiques au militaire.

Les extraits du texte publié en 1961 sur la « Formation des chefs » montrent aussi la pérennité de ce qui fait un chef militaire. Si, en temps de paix, « l'analyse intellectuelle des situations préparatoires à la décision et […] le calcul attentif du meilleur rendement de son action » semblent être des critères communs aux chefs civils et militaires, se découvre, en temps de guerre, une « exigence de promptitude et de réflexe qui le différencie de tout autre individu exerçant une autorité importante ». Ces qualités spécifiques ne sont pas innées et l'officier se doit de les cultiver, notamment par l'étude approfondie des actions de ses prédécesseurs.

La permanence des valeurs et des qualités militaires n'efface nullement la nécessité et le devoir qu'a l'officier de s'adapter à son monde. Les valeurs traditionnelles s'ancrent en effet sans complexe dans la modernité technique et les réalités sociales. La stratégie et la tactique de guerre sont envahies par des techniques qui se renouvellent rapidement et qui transforment peu à peu les actes de prise de décision (comme l'algorithmique et l'intelligence artificielle). Les problèmes nouveaux que cela pose mettent au défi la formation classique de l'officier.

Il lui faut savoir appréhender la « "Génération Y", une génération au combat » qui bouscule l'art traditionnel du commandement. L'article « Repenser le combattant dans le contexte stratégique français » soulève la question du glissement vers des missions « non-guerrières » ou de sécurité que pose par exemple l'opération *Sentinelle*, ainsi que la question du rapport à la mort du soldat dans notre société d'aujourd'hui.

Les enjeux sont aussi techniques et capacitaires, comme le souligne le texte « Innover pour penser et réaliser les capacités militaires de demain : un impératif catégorique ». « Répondre à l'accélération du temps et des événements, aux enjeux amplifiés ou nouveaux créés par l'évolution du contexte dans lequel s'inscrira l'action militaire, nécessite d'investir de nouveaux domaines et d'adapter nos méthodes de construction de capacités, en capitalisant sur les nombreux atouts dont nous disposons déjà. »

Audrey HÉRISSON

Vous avez dit militaire ?

Emmanuel Desclèves

Vice-amiral, de l'Académie de Marine.

Dans les débats politiques actuels sur les enjeux de défense et défis sécuritaires, policiers, gendarmes, fonctionnaires, militaires, contractuels et agents de protection sont de plus en plus souvent mélangés et comparés avec un risque important de confusion dans les esprits. Il n'est donc pas inutile de rappeler la différence fondamentale entre militaire et civil. On prendra ici l'exemple du marin d'État, significatif dans la mesure où son statut est doublement spécifique, d'abord comme marin puis comme militaire.

Civil ou militaire : les termes de l'échange

Le salarié est un travailleur qui accepte la subordination à son entreprise par le biais d'un contrat régi dans le cadre général d'un ensemble de dispositions législatives et conventionnelles, regroupées dans le Code du travail et les conventions collectives. Contre rémunération, il doit un temps de travail à l'entreprise, mais au-delà de cette durée limitée. Le salarié est libre, c'est-à-dire que l'entreprise ne peut théoriquement plus compter sur lui [1].

Le statut du militaire [2] est tout autre et les termes de l'échange avec l'institution qu'il sert sont d'un ordre bien différent, qui ne se réfèrent pas au Code du travail comme on le croit trop souvent. Ce statut permet de définir l'état militaire, le régime particulier des libertés applicables au personnel servant sous ce statut, les droits et devoirs du militaire, ses garanties, l'organisation hiérarchique, le régime des sanctions, les règles de recrutement, les conditions d'avancement et de cessation de l'état militaire. Comme le précise la loi de 2005 : « L'état militaire exige en toutes circonstances l'esprit de sacrifice, pouvant aller jusqu'au sacrifice suprême, discipline, loyalisme et neutralité. Les devoirs qu'il comporte et les sujétions qu'il implique méritent le respect des citoyens et la considération de la Nation ».

(1) La plupart des entreprises cherchent cependant à développer une « culture », pour fidéliser leur personnel et déborder du cadre strictement contractuel. Les grands managers parlent de « stratégie d'engagement des salariés ». Le terme n'est pas anodin et joue bien de l'opposition/complémentarité entre les deux pôles du contrat et de l'engagement.

(2) Loi du 24 mars 2005 portant statut général du militaire.

Le pouvoir de donner la mort *in fine* est au cœur du statut de militaire : responsabilité suprême, totalement exorbitante de notre droit commun, apanage des seuls militaires au combat. Dans une république démocratique comme la nôtre, ce pouvoir extraordinaire ne peut naturellement être confié qu'à des personnes de grande confiance, qui maîtrisent parfaitement les risques et l'usage de la force, du haut en bas de la chaîne de commandement.

En dehors du chef de l'État, aucun homme politique, aucun juge, aucun fonctionnaire, aucun civil ne dispose de ce pouvoir extrême. Et qui peut réellement prétendre en mesurer la gravité et le poids, sinon ceux qui l'ont assumé ? Qui peut sonder le cœur de celui qui ferme les yeux de son camarade, de son ami, sur le champ de bataille ? Qui peut comprendre les horreurs des combats face à face avec l'ennemi ?

D'emblée, le statut militaire se situe donc en dehors du cadre de l'échange économique contractuel du travail rémunéré, pour s'inscrire dans un espace de sens, dans lequel le militaire englobe son engagement au service et sa contrepartie, qui ne se réduit pas à un salaire. L'échange doit alors être compris d'une façon beaucoup plus globale : le militaire se place dans un rapport de contribution vis-à-vis d'une institution dont il reçoit en contrepartie une rétribution (solde, honneurs, sécurité, appartenance à l'institution, décorations…) [(3)].

Caractériser cette contribution, c'est moins définir une production à valeur économique, que se référer à des fondamentaux tels que la maîtrise du risque militaire (être tué), la responsabilité suprême (pouvoir de tuer), l'engagement (la soumission à l'autorité et à ses principes supérieurs, mais aussi l'exigence du commandement), la disponibilité (la permanence au service de la mission), l'adhésion aux valeurs (honneur, patrie, discipline) [(4)].

En contrepartie, la rétribution est composée d'une part financière à laquelle s'ajoutent d'autres éléments dont certains se situent dans l'ordre purement symbolique : les honneurs, le prestige, le rang. Cette conception spécifique de la rétribution due au militaire est mise en évidence dans la notion même de solde qui, à la différence du salaire contractuel, ne rémunère pas une prestation mais donne au militaire le « moyen de tenir son rang ».

Fondamentalement, les termes de l'échange entre le militaire et l'institution d'une part, le salarié et son entreprise d'autre part, n'utilisent donc pas les mêmes références et ne se situent pas sur le même plan. Même si l'on peut en réalité observer en temps de paix une série de situations intermédiaires assurant un *continuum* entre ces deux pôles, plutôt qu'une discontinuité radicale.

(3) « Le présent statut assure à ceux qui ont choisi cet état les garanties répondant aux obligations particulières imposées par la loi. Il prévoit des compensations aux contraintes et exigences de la vie dans les forces armées ».
(4) L'*US Navy* enseigne à ses jeunes recrues les *Cores Values* : *Honor, Courage, Commitment*.

Du statut au contrat, la relation à l'autorité

Juridiquement, le lien de subordination qui rattache le militaire à l'État n'est donc pas un contrat de travail. L'engagement au service de la Nation est en l'occurrence un acte citoyen qui relève plutôt d'une « réquisition consentie ». Ce qui est requis du militaire est l'obéissance à l'autorité, normalement compatible avec l'exercice de sa propre liberté. « L'obéissance à la loi qu'on s'est prescrite est Liberté » écrivait Jean-Jacques Rousseau. On s'inscrit là dans un système autoritaire mais non totalitaire.

C'est traditionnellement par le statut, le grade et le rang, que l'autorité militaire prend forme et incarne la légitimité ultime. Le corps des officiers destinés au commandement et porteur des valeurs comme des savoir-être, est normalement dépositaire de l'autorité militaire [5]. Le statut et le contrat relèvent ainsi de deux logiques différentes, parfois peu compatibles. D'un côté on se réfère à une carrière avec un avancement en grade, de l'autre il s'agit d'une reconnaissance fondée sur la seule compétence professionnelle.

Dès lors, on comprend le caractère inadapté d'une politique de gestion des ressources humaines qui prétendrait tout unifier et mélanger, en réduisant la responsabilité de la gestion des personnes au simple pilotage d'une masse salariale globale. Est-ce la marque d'une coupable ignorance des différences fondamentales entre statut et contrat, entre civil et militaire ?

Le bâtiment de guerre, « institution totale »

Sur un bâtiment de combat, vie de travail et vie hors travail se déroulent dans le même espace confiné, régi par une autorité supérieure unique. Les sociologues parlent, en l'occurrence, d'institution totale. Les conditions de vie à la mer et l'omniprésence du matériel sur un bâtiment de guerre ont depuis longtemps imprimé leur marque dans les règles formelles et les traditions de la Marine, dont le personnel se considère en général comme marin avant même d'être militaire.

Avant toute utilisation à des fins militaires, il faut en effet assurer le fonctionnement matériel du bâtiment qui conditionne directement (physiquement) la sécurité de l'équipage. Nous pouvons y voir une référence première à cette réalité sociotechnique complexe que constitue le tandem navire-équipage. C'est aussi ce qui explique la forte culture technique du marin, quelle que soit son appartenance ou sa nationalité, qui est aussi l'un des éléments fondateurs d'un ordre professionnel.

En complément de cette compétence professionnelle indispensable, les conditions particulières de promiscuité et d'isolement (désormais plus relatif) par rapport au milieu familial, ainsi que les risques encourus pour toutes sortes de

(5) Cf. Emmanuel Desclèves, « Du commandement à la mer », *RDN* n° 797, février 2017, p. 61-66.

raisons, ont depuis toujours justifié une organisation humaine très soudée. L'expression : « Nous sommes embarqués sur le même bateau » ne se réfère pas particulièrement à un bâtiment de combat mais illustre bien le concept même d'équipage, dont la cohésion constitue la force face à l'isolement et aux dangers environnants.

Dans la même logique, une hiérarchie forte et structurée a toujours été jugée nécessaire à la mer, de sorte que partout dans le monde et depuis la plus haute antiquité, les capitaines de navires – militaires comme civils – se sont vus arroger des pouvoirs exorbitants du droit commun (6), qu'illustre la formule ancienne du « seul maître à bord, après Dieu ».

Sur ces fondements intrinsèquement liés au métier de marin – qui se vit confiné et en équipage – vient se greffer l'ordre militaire, le navire étant en l'occurrence utilisé comme bâtiment de combat (7). C'est ce qui fonde *in fine* la prééminence de l'ordre militaire sur l'ordre professionnel à bord des bâtiments de guerre. Cette référence opérationnelle est la principale raison d'être de ceux qui ont vocation à commander les actions militaires à la mer, c'est-à-dire les officiers de marine.

Dans la vie courante et les situations normales de travail à bord, la hiérarchie se construit donc essentiellement sur le professionnalisme (métier de marin), qui se compose à la fois des compétences techniques et des savoir-être indispensables à la vie en équipage à la mer. Les problèmes et conflits internes qui font partie de la vie normale de toute vie en collectivité, sont généralement résolus par des solutions fondées dans l'ordre du savoir professionnel. En cas d'opérations en revanche, la légitimité de l'autorité dans l'ordre militaire s'impose et prend le pas sur celle issue de l'ordre professionnel.

Pour autant, la question de l'autorité à bord n'est pas réductible à celle de la subordination. Elle est aussi celle de la représentation de la communauté et même de cet ensemble indissociable que constituent un équipage et son bâtiment, personnalisés d'ailleurs par un seul et même nom. Le commandant symbolise cette entité en toutes circonstances. Vis-à-vis de son équipage comme de l'extérieur (8), il incarne la destinée collective du bâtiment, qui englobe d'une certaine façon les engagements individuels de chaque membre de l'équipage.

(6) Les lois et règlements applicables aux gens de mer diffèrent du droit commun « à terre ». Ils consacrent partout la spécificité du métier de marin, seule profession au monde ayant un statut international, étayé par de nombreuses conventions de l'OMI et de l'OIT.

(7) On ne reviendra pas ici sur les principes qui fondent la légitimité de l'emploi de la force armée, sous l'autorité du chef de l'État.

(8) L'article 6 de la loi du 24 mars 2005 prévoit que le commandant veille aux intérêts de ses subordonnés et rend compte de tout problème à caractère général à ses supérieurs hiérarchiques.

Une refondation

Dans notre monde de plus en plus mouvant et souvent flou, la vraie difficulté consiste sans doute à redéfinir et refonder les bases sur lesquelles reposent les relations entre les marins et l'institution, de façon à bien mettre en perspective toutes les évolutions engagées ou envisagées, parfois en réponse à des sollicitations simplement conjoncturelles. Il s'agit de bien prendre la mesure de l'importance relative ou conjuguée de tous ces paramètres, au regard d'un objectif de nécessaire valorisation et d'optimisation de l'emploi de la ressource humaine dans la Marine, pour garantir son efficience dans la durée. Il faut faire en sorte que les carrières et les métiers proposés, qui devraient rester largement spécifiques pour les équipages embarqués [9], suscitent encore de véritables vocations à l'engagement.

Au risque d'une confusion perverse, l'exercice ne peut s'appuyer sur une simple comparaison avec les relations habituelles de travail dans le monde de l'entreprise ou dans la fonction publique. Pour la Marine, la réflexion devrait prendre racine au cœur même de ce qui consacre sa raison d'être et fonde sa culture propre et originale : le bâtiment de combat, moyen militaire majeur au service de la Nation [10].

En faisant ressortir un fil directeur bien nécessaire au milieu des nombreux changements en cours ou intervenus ces dernières années, ces réflexions devraient en outre contribuer à apporter aux marins militaires une vision prospective claire, ancrée sur les fondements de la loi de 2005.

Bâtiment de combat et esprit d'équipage

Ce bâtiment constitue un système sociotechnique, dans lequel on ne peut dissocier l'équipage du navire en tant qu'objet matériel. Le sous-marin nucléaire lanceur d'engins (SNLE) et le porte-avions nucléaire constituent aujourd'hui au niveau mondial les réalisations humaines les plus complexes qui soient sur le plan technique [11] : cela donne une idée du professionnalisme requis pour les équipages qui les exploitent.

Le fonctionnement harmonieux de cet ensemble navire-équipage repose tout à la fois sur un principe d'autorité fort, sur un haut niveau de compétences techniques, ainsi que sur un véritable esprit d'équipage adapté aux conditions très originales de la vie à bord, singulièrement indispensable hors des situations courantes. C'est l'équilibre subtil entre ces différents paramètres qui détermine la cohésion et la force d'un équipage ; vouloir modifier l'une ou l'autre des

(9) Cela étant, la Marine a aussi besoin de personnel à terre dans des métiers parfois tout à fait éloignés de ceux pratiqués à bord, qui doivent cependant rester au cœur de la réflexion.

(10) « L'armée de la République est au service de la Nation ».

(11) Ces vérités historiques semblent un peu oubliées de nos jours : il faut rendre un hommage appuyé au personnel de nos entreprises.

composantes comporte des risques et peut être de nature à fragiliser cette identité collective très concrète sur laquelle repose *in fine* l'essentiel de la valeur d'un bâtiment de combat. Les observateurs extérieurs qui ont l'occasion d'embarquer sur un bâtiment de la Marine sont en général frappés par la puissante réalité de cette notion d'équipage.

Les évolutions actuellement observées dans notre société mettent en évidence un individualisme plus marqué, même si de grandes solidarités émergent ici et là autour de thèmes ou de valeurs considérés comme universels. C'est ainsi que certaines contraintes de la vie embarquée sont désormais plus difficiles à accepter vis-à-vis de la cellule familiale. À la référence passée au principe de réciprocité au sein de la famille ou à celui de la redistribution dans l'ordre de l'économie administrée – principes au titre desquels chacun avait son statut – se substitue souvent une relation contractuelle à caractère individuel, moins globale et plus éphémère. Cela étant, de nombreux jeunes se réfèrent aujourd'hui à des « valeurs » quasi symboliques, respectées au sein du groupe ou de la bande d'appartenance, dont certaines sont d'ailleurs de même ordre que celles en vigueur dans les armées (la subordination au chef, par exemple).

Parallèlement, on voit poindre une certaine déstabilisation des modes traditionnels de structuration et de différenciation hiérarchique. L'évolution sociétale observée d'une part, et la nécessité de recruter du personnel de haut niveau technique d'autre part, pourraient éventuellement être de nature à remettre en cause le principe hiérarchique, fondé aujourd'hui sur la seule délégation de l'autorité supérieure. C'est dire s'il est important de réexpliquer sans relâche les fondements spécifiques du statut militaire.

Pour conclure

S'engager comme militaire dans la Marine nationale dans la perspective de bénéficier d'un statut de fonctionnaire civil, voire d'un contrat de salarié d'une entreprise privée, est déplacé : les termes de l'échange entre le marin et l'institution ne se déclinent pas seulement en salaire/production/heures de travail, comme le confirme la loi de 2005 portant statut général des militaires.

L'esprit d'équipage, l'engagement au service de l'État, l'exigence du combat, la compétence professionnelle, le sens de la disponibilité, la maîtrise des technologies les plus modernes, l'aptitude à vivre et à durer dans des conditions contraignantes, la maîtrise des risques, l'ouverture à un monde de plus en plus tourné vers la mer, sans oublier le goût de l'aventure bien sûr, sont autant de valeurs objectives qui consacrent la richesse de la culture professionnelle du marin d'État.

Comme les autres militaires, les marins les mettent en avant sans complexe en ancrant ces valeurs pérennes au standard de la modernité technique et des réalités sociales. ◆

RDN n° 189 - mars 1961

Formation des chefs

Marcel Demonque

Ingénieur civil des Mines et PDG des Ciments Lafarge. Il est l'un des fondateur du Centre de recherches et d'études des chefs d'entreprises lié au Conseil national du patronat français (CNPF, futur Medef). Il est aussi l'un des dirigeants du Centre international de prospective, fondé par Gaston Berger et regroupant chefs d'entreprise, hauts-fonctionnaires et universitaires.

Dans la prise de décision, deux fonctions entrent en jeu successivement. D'abord l'intelligence qui éclaire le problème posé, en fait l'analyse et construit les éléments objectifs de la réponse. Ensuite la volonté qui assume la responsabilité et la charge, soit d'entériner la réponse de l'intelligence, soit de la modifier par des considérations subjectives qui engagent davantage encore la lucidité et la conscience.

Au-delà de la décision, il faudra convaincre ceux qui auront la charge de l'exécuter. Cette entreprise de persuasion mettra en jeu tout à la fois le caractère, la finesse, le jugement. Quand la décision est grave et qu'elle oblige à fond la responsabilité morale du chef, il faut, pour qu'elle s'impose, qu'elle soit inspirée par un idéal visible et transmissible, qui affirme son exigence par son ressort propre.

Le chef est donc un homme qui groupe en lui des qualités intellectuelles fortes et des qualités spirituelles dominatrices. Car il n'y a d'autorité qu'individuelle et l'autorité engage toute la personne.

Les qualités intellectuelles du chef ne sont pas d'abord d'érudition ; elles sont d'abord des aptitudes, des forces potentielles que l'érudition ne soutient – mais elle n'est pas nécessaire – qu'à la condition de n'être pas pesante, de savoir s'effacer. Elles doivent donner la promptitude des réflexes et la souplesse des adaptations. Leurs fondements sont de connaissance profonde et étendue ; ils sont faits de sédiments longuement et patiemment accumulés mais dans lesquels la personnalité ne s'est pas ensevelie. La personnalité du chef doit rester libre à l'égard de ses connaissances. Son intuition puise certes à la sève de ses connaissances mais elle se libère des connaissances à l'instant de son jaillissement.

Les qualités spirituelles du chef sont de force et de lucidité. C'est l'équilibre difficile de la force et de la lucidité qui permet de trancher les cas de conscience,

qui donne de la mesure, qui évite la confusion entre désir et réalité, qui ouvre la disponibilité – cette attitude fondamentale qui distingue l'homme du mécanisme.

⁂

Il y a des chefs tout au long d'une hiérarchie. Tous doivent avoir des qualités d'intelligence et des qualités de caractère. Peut-être pourrait-on dire qu'au sommet de la hiérarchie l'intelligence s'exerce en plénitude alors, qu'en bas, la décision – qui est le plus souvent volonté d'exécuter une décision venue d'en haut – appelle davantage l'énergie, le caractère, la force de persuader.

À tous les échelons, l'autorité s'exerce sur des hommes et elle prendra d'autant plus de force qu'elle s'appuiera, autour du chef, sur une équipe. Mais l'autorité, lorsqu'arrive le moment isolé où se prend la décision, ne relève que d'un individu. Tout alors en lui est dépouillé : l'instant, la conscience, l'intelligence. Le chef est tout seul et tout nu au milieu de peureux qui hésiteraient et de violents qui le dépasseraient s'ils avaient à décider à sa place. Entre les extrémistes, le chef connaît tout seul la « minute de vérité » de la décision. Cette minute de vérité est une minute d'équilibre mais elle contient en puissance tout le mouvement qui va en découler ; c'est pourquoi elle est parfois si lourde. Cette solitude, cette nudité, ce poids sont propres à la fonction de commandement. Mais la fonction elle-même n'est pas – contrairement à ce que dit une certaine école – une fonction spécifique. Elle est une fonction hétérogène par nature et par position, à la convergence de fonctions spécifiques que l'on dénomme aujourd'hui dans l'entreprise « opérationnelles » et « fonctionnelles » : c'est-à-dire qu'elle alimente sa connaissance et poursuit sa recherche à travers les services fonctionnels, alors qu'elle ramifie son action par le moyen des services opérationnels.

⁂

Cette dernière remarque montre bien l'identité de structure du commandement militaire et du commandement dans l'entreprise. Le temps n'est d'ailleurs pas très éloigné où les services fonctionnels de l'entreprise s'appelaient tout simplement « états-majors ». Cette identité, on la retrouve dans tous les aspects des deux commandements et c'est peut-être cette unicité qui fait croire faussement à la spécificité.

Pourtant, le chef militaire, s'il se sent en temps de paix très semblable au chef d'entreprise, à la fois par l'analyse intellectuelle des situations préparatoires à la décision et par le calcul attentif du meilleur rendement de son action, se découvre, au contraire, en temps de guerre, une exigence de promptitude et de réflexe qui le différencie de tout autre individu exerçant une autorité importante. Néanmoins, il sait bien que la promptitude de l'intelligence et les réflexes de situation ne sont pas nécessairement des qualités innées, qu'elles se cultivent patiemment en temps de paix par une culture militaire permanente, toujours rapprise et

approfondie aux sources authentiques. Il sait aussi que l'invasion de la stratégie et de la tactique de guerre par des techniques en renouvellement rapide et constant transforme peu à peu la nature profonde de son acte de décision et que, de ce fait, des problèmes tout nouveaux lui sont posés qui mettent en cause sa formation classique.

De son côté, le chef d'entreprise, même s'il n'a pas à faire face à des situations aussi dramatiques et condensées que l'emploie d'armes atomiques, se voit, lui aussi, soumis à un gradient d'évolution tel qu'aucun de ses prédécesseurs n'eût pu même le concevoir. Il doit donc, dans un style peut-être différent, mais par une méthode aussi rigoureuse, se soumettre à un entraînement intellectuel et à un dépouillement spirituel qui ressemblent trait pour trait à la formation intellectuelle et spirituelle du chef militaire. Ce n'est pas un des moindres traits caractéristiques de cette époque que l'homme qui exerce un commandement – militaire ou civil – voit sans cesse sa connaissance acquise dévaluée par le progrès et que le « recyclage » aux sources d'un enseignement sans cesse « actualisé » représente pour lui la plus banale et la plus rigoureuse des exigences.

⁂

À l'universitaire le chef militaire ou civil doit donc aujourd'hui poser une double question.

– Quelle formation intellectuelle de base pensez-vous qu'il faille donner à de jeunes hommes – supposés être de futurs chefs – dont les connaissances acquises seront sans cesse dépassées au cours de leur existence ?

– Êtes-vous en mesure de nous assurer le « recyclage » permanent nécessaire au renouvellement de nos connaissances ?

[…] la réponse n'est-elle pas finalement celle que donne déjà l'Armée, à savoir les sélections successives en cours de carrière et l'éducation permanente des sélectionnés ? N'est-ce pas aussi ce que fait l'industrie, à cela près qu'elle attache peut-être moins de prix à l'éducation permanente, faute peut-être d'avoir, comme l'Armée, sécrété l'organisation adéquate ? Si bien que, finalement, les deux questions posées se confondraient en une seule.

⁂

Dans la mesure où la culture fait, selon Gaston BERGER, l'enveloppe des valeurs personnelles, on ne peut pas poser le problème de la formation du chef sans poser le problème de sa culture. L'homme s'affirme à l'égard de lui-même par sa culture. Et plus encore le chef dont l'affirmation à l'égard de lui-même sous-tend son affirmation à l'égard des autres.

Mais de quelle culture s'agit-il ? Toute formule, toute recette de culture contreviennent à l'idée même de culture. Gaston BERGER répond, non pas en définissant la culture, mais en donnant une de ses qualités négatives essentielles : elle n'est pas un contenu pesant et mesurable. Elle est une puissance, un potentiel d'activités intellectuelles, sensibles, spirituelles. Il l'exprime ainsi : « le chef doit avoir des qualités intellectuelles en exercice et non point des connaissances intellectuelles acquises ».

Avoir des qualités intellectuelles en exercice c'est proprement avoir une tension intellectuelle permanente, être attentif, ouvert, avide. Le contraire serait d'être alourdi par un bagage intellectuel pesant, accumulé dans la mémoire, qui ne se serait pas dissous pour apporter un aliment subtil aux fibres profondes de l'être. Avoir des qualités intellectuelles en exercice c'est aussi penser clairement, savoir analyser et, pour cela, connaître la valeur exacte des termes et le jeu subtil de l'éclairage changeant des mots. Avoir des qualités intellectuelles en exercice c'est posséder le tonus de l'esprit qui est un véritable état de santé de l'intelligence et qui est source de rayonnement. C'est aussi être en état de liberté car, dit encore Gaston BERGER, « il faut la liberté pour inventer ». Inventer, la disponibilité pour inventer, ce sont des états et des mouvements de l'esprit sans lesquels le chef n'est pas un chef. Ils supposent la liberté de l'esprit – une liberté à laquelle s'oppose l'encombrement – mais ils supposent aussi l'humilité, car l'orgueil mène au système et le système est l'ennemi naturel de l'invention.

Infrastructure de la connaissance, qualités intellectuelles en exercice, science des mots et de l'analyse, santé de l'intelligence, liberté, invention, humilité. C'est tout cela que l'éducateur devrait donner au futur chef chez qui, à l'époque de son éducation, est encore détendu le ressort profond grâce auquel il mettra un jour en activité ce potentiel accumulé. Ce ressort profond c'est l'esprit de synthèse. Le plus généralement ce n'est pas l'éducateur qui le donne. Il fait partie du fonds propre du chef. Il n'est qu'un ressort ; il donne force d'action à une puissance intellectuelle acquise. Sans l'esprit de synthèse, toute puissance intellectuelle reste à l'état de potentiel ; sans la puissance intellectuelle acquise – et « recyclée » – l'esprit de synthèse est un ressort qui se détend dans le vide.

⁂

Il faudrait encore dire un mot du corps avant de parler de l'idéal. Car l'homme est un tout que Descartes a décomposé à tort. Son corps, son intelligence et son âme ont tous trois valeur. Le sport affirme le corps ; il donne de l'assise à la volonté et au caractère. Il incite à la patience. Il forme à la science du jeu. Par-dessus tout, il apprend à subordonner son action à celle des autres. On conçoit mal aujourd'hui que le sport ne soit pas une des pièces essentielles de la formation du chef.

Reste le problème de l'idéal. L'idéal donne au chef la force intérieure qui illumine la conscience. Il illumine aussi son visage, ses gestes, sa voix. Il sert à vivre, mais il sert aussi à faire vivre les autres en les entraînant dans le mouvement qui est vie.

Or l'idéal ne pose qu'une question, mais qui est fondamentale : la morale. Gaston BERGER, au cours de nos débats, a dit : « défendre, oui, mais défendre quoi ? Se battre, d'accord, mais se battre pour quoi ? » Et il a répondu lui-même, après avoir élagué : « pour l'idée de liberté ». Dès lors, a-t-il ajouté : « la finalité de l'éducation ce sera la liberté ». Mais il s'agit de la liberté des autres qui, pour soi, est contrainte. Respecter la liberté des autres c'est se mettre soi-même en état de respect, donc de contrainte.

Et c'est ici sans doute que l'on se trouve au centre même de la morale du chef, au point de convergence de ses exigences intérieures qui est, en même temps, le point de convergence des libertés des autres.

C'est de ce point que doit être, en particulier, considérée l'action psychologique qui est aussi bien du domaine d'action de l'entreprise que du domaine d'action de l'armée. Agir sur les autres par l'éducation, par l'entraînement intellectuel, par la publicité, ce sont des nécessités communes à l'armée et à l'entreprise. Mais ce sont des nécessités qui connaissent une limite impérative : la personne et sa liberté. Et non pas n'importe quelle sorte de liberté, mais celle qui touche à l'intégrité même de l'être.

⁂

[…] Exigences intellectuelles d'ossature solide à laquelle les mouvements de l'esprit puisent leur force tout en gardant leur mobilité. Exigences intellectuelles encore de l'éducation permanente dans un monde dont les réalités immuables se combinent et se dénouent sans cesse sous nos yeux ou s'éclairent d'éclairages toujours changeants. Exigences du corps que le sport affermit et rend plus souple. Exigences du caractère que les sautes des événements, menus ou grands, de l'histoire doivent laisser de sang-froid. Exigences de la morale qui imposent au chef le mariage difficile de l'autorité et du respect de la liberté.

Ces exigences dures sont pour le chef le ressort de toute action. […]

Tribune n° 940 - 18 octobre 2017

« Génération Y », une génération au combat

François Reynaud

Né en 1980, promotion Bethouart (2000-2003) de l'ESM de Saint-Cyr, chef de section de commandos parachutistes au 8e RPIMa et chef de centre commando à Abidjan de 2004 à 2008. Adjoint puis commandant de compagnie de combat parachutiste à Castres de 2008 à 2012 avant de rejoindre l'École des parachutistes de Pau en 2013 à la Division études et prospective. Breveté de la 23e promotion de l'École de Guerre (« Verdun »). A participé à plusieurs déploiements à l'extérieur (Afghanistan, République centrafricaine, Côte d'Ivoire, Gabon), en Nouvelle-Calédonie ainsi qu'au sein d'un état-major de l'Otan aux États-Unis. Sert actuellement au bureau finances de l'État-major de l'Armée de terre.

Depuis 2008, le Medef (Mouvement des entreprises de France, organisation patronale fondée en 1998) s'intéresse à ce qu'il est devenu courant d'appeler la « Génération Y ». Ce concept de « génération » n'est pas nouveau. Le sociologue hongrois Karl Mannheim a en effet publié en 1928 un texte fondateur : *Le problème des générations.* Celui-ci montre que les comportements et les modes de pensée d'un individu sont fortement influencés par les événements qu'il a vécus autour de sa vingtième année.

En France, en 2015, cette « génération Y » représente près de 40 % de la population active, soit 16 millions d'individus nés entre 1981 et 1999. Appelée « *Millenium Generation* » outre-Atlantique, cette classe d'âge s'est développée après la chute du Mur et de concert avec la révolution numérique. Aujourd'hui, elle présente des caractéristiques que les spécialistes des ressources humaines cherchent à analyser pour y adapter le monde de l'entreprise et les techniques de *marketing*. Enfants du chômage et du divorce, génération « connectée » bénéficiant d'un nouveau rapport au savoir, les « Y » seraient plus instables, pragmatiques, curieux, soucieux d'être informés et surtout plus individualistes que leur aînés. Grands communicants, très attentifs à leur image, innovants et indépendants, ils entreraient également en conflit avec l'autorité, privilégiant la légitimité reconnue au statut hiérarchique établi.

Dans les armées françaises, cette génération de soldats, de sous-officiers, de lieutenants et de capitaines a vécu en première ligne la période d'engagements opérationnels intenses ouverte par la chute des Tours jumelles en 2001. Nouvelle « Génération du feu » – historiquement notion apparue à l'issue de la guerre de

1914-1918 à propos des anciens combattants regroupés en associations (cf. Bruno CABANES) –, ces jeunes hommes et femmes constituent la première génération de soldats professionnels venus résolument servir la France alors que son armée connaissait des taux de pertes certes limités mais inédits depuis la fin de la guerre d'Algérie. Depuis 2002 et l'ouverture du théâtre afghan, la France a perdu plus de 130 soldats en opération et près de 1 000 blessés en Afghanistan, en Côte d'Ivoire, en République Centrafricaine ou en Guyane et encore récemment au Sahel et en Irak.

À l'heure où notre pays est engagé durablement sur le territoire national dans des missions exigeantes et nécessaires mais éloignées de l'aura aventureuse des opérations extérieures, il est important de décrire les ressorts et motivations d'une génération dont les premiers représentants atteignent 37 ans cette année et auront bientôt la charge de façonner notre outil de défense.

Une génération bien formée et exigeante

La fin de la professionnalisation de nos armées a été effective dès 2002. Autant dire que parmi les jeunes cadres et soldats, la conscription appartient à un passé révolu. Tous se sont engagés par choix. Parmi eux, du soldat de 1re classe au jeune commandant, on retrouve un niveau académique général rarement atteint jusqu'ici. Dans l'Armée de terre, qui compte plus de 100 000 hommes et dont la moyenne d'âge ne dépasse pas 32 ans (source : étude sociologique de la DRH-MD, 2010), il n'est pas rare de compter près de 50 % de bacheliers parmi les jeunes engagés d'une section en formation initiale ainsi qu'une forte proportion de jeunes diplômés de l'enseignement supérieur au sein des contingents d'élèves sous-officiers rejoignant l'École de Saint-Maixent (ENSOA).

Globalement, la « Génération Y » est consciente de sa valeur et habituée à vérifier, voire à remettre en question le savoir qui lui est dispensé (cf. Michel SERRES). Cette génération a des attentes plus élevées pour son épanouissement personnel et cherche en premier lieu un travail signifiant. Malgré le contexte actuel de crise économique, moins de 20 % des jeunes engagés ont connu une période de chômage avant de rejoindre l'institution militaire et beaucoup préfèreront l'insécurité de l'emploi à une stabilité dans un métier qui n'a pas de sens. En effet, la « Génération Y » a grandi dans un monde instable et se caractérise aujourd'hui par un investissement professionnel limité et directement lié à l'intérêt des défis proposés au quotidien. Réagissant à court terme, c'est une génération impatiente, habituée à obtenir une information exhaustive et immédiate (cf. François PICHAULT et Mathieu PLEYERS). Dans un contexte général où moins de 35 % des « Y » obtiennent un CDI pour leur premier emploi, cette génération semble avoir développée une âme de mercenaire et n'hésite pas à discuter avec son employeur du moindre détail de son contrat.

Dans les Armées qui cherchent à conserver au moins 8 ans une ressource humaine majoritairement sous contrat, le défi de la fidélisation est permanent car les « Y » ont besoin d'adhérer à un projet précis et concret. Or, malgré les réorganisations, les diminutions d'effectifs et les difficultés matérielles vécues ces 15 dernières années, l'Armée demeure attractive chez les jeunes, notamment grâce aux opérations extérieures et à la modernisation de ses matériels. Alors que la presse évoque régulièrement un risque de surchauffe dû au taux d'emploi élevé des unités, les soldats de la « Génération Y » ont montré une grande disponibilité et un fort esprit de discipline. De fait, aimant travailler en équipe, peu impliquée politiquement mais possédant un sens moral et civique avéré, cette génération conserve une attitude positive envers le travail, pourvu qu'il lui apporte une gratification rapide et un sentiment de plaisir et d'appartenance à une communauté. Ce sont là des éléments de réflexion utiles pour conserver intacte la motivation des soldats, quelles que soient leurs conditions d'engagement, en France ou en opération.

Un rapport particulier à l'autorité et à la technologie

Premiers enfants nés après la généralisation du contrôle des naissances, les « Y » sont les « enfants-rois » de Françoise DOLTO. Désirés par leurs parents, issus de fratries limitées, ils ont pris l'habitude d'être écoutés, réconfortés et encouragés à « s'épanouir ». Cependant, cette génération est également celle du divorce et des familles monoparentales. Auprès de ces grands sensibles, les remontrances et les injonctions passent mal. Les jeunes cadres, lors de leurs premières expériences de commandement, n'ont guère l'habitude d'une fermeté et d'une discipline peu pratiquées dans le champ social ou scolaire. Ce manque de culture hiérarchique crée donc un rapport particulier à l'autorité. Désormais, la crédibilité du chef repose davantage sur sa compétence, notamment technique, que sur le statut ou le grade pour rester dans la sphère militaire.

En contrepartie, cette génération « communautaire » possède une aptitude reconnue à travailler en équipe. Or, comme ses prédécesseurs, le « Y » entrant dans la vie active a besoin d'être (re)cadré et de s'affirmer au sein d'un groupe. De fait, la jeunesse a toujours été considérée comme agitée, créative et insoumise *. Et les armées ont toujours recruté des hommes jeunes pour porter les armes de la France. Si les rapports hiérarchiques peuvent sembler moins formels aujourd'hui, la discipline demeure une valeur essentielle à la bonne marche de l'entraînement et à la cohérence des actions individuelles en opération extérieure. D'ailleurs, les succès des engagements militaires récents reposent largement sur son application. En réalité, la discipline est davantage garantie par le respect des principes bien connus

*** Une jeunesse agitée, créative et insoumise : une tradition historique**

Sous Philippe Auguste, dès 1215, l'Université reconnaît officiellement aux étudiants le droit de faire grève. Puis, sous Saint Louis, de graves incidents lors du Carême de 1229 ne seront réglés qu'à l'issue de la promulgation de la bulle *Parens scientiarum* (Paris, mère des sciences) par le pape Grégoire IX le 13 avril 1231.

décrits par le colonel de Maud'huy à la tête du 35e Régiment d'infanterie avant la Grande Guerre * et illustrés par « l'obéissance d'amitié » formulée par le général Frère que par l'acceptation d'emblée d'une pyramide hiérarchique.

Néanmoins, commander la « Génération Y » impose d'avoir une vraie légitimité, en particulier dans le domaine technique. Dans l'Armée de terre, cette exigence impose aux officiers et sous-officiers de s'approprier rapidement les innovations matérielles et technologiques afin de conserver leur autorité face à des soldats qui s'adaptent facilement aux nouveaux équipements comme ceux du programme *Félin* **. De même, la maîtrise de l'environnement cyber ou la compréhension du fonctionnement des réseaux sociaux constituera certainement, à l'avenir, un sérieux gage de crédibilité face à de jeunes officiers qui refusent la passivité du rapport classique « maître-élève ».

* **« Testament militaire » du colonel de Maud'huy à son régiment, 1912**

« J'ai toujours été convaincu que le supérieur doit respecter la personnalité de son subordonné ; (…) Nous devons nous servir de nos subordonnés tels qu'ils sont, en utilisant leurs qualités et même leurs défauts (…) Pas d'exigences inutiles. Le Français n'aime pas être perpétuellement ennuyé pour des vétilles. »

** **Programme *Félin***

Le programme « *Fantassin à équipement et liaisons intégrés* » permet, notamment, de faire remonter la position d'un soldat sur l'écran tactile de son chef, d'envoyer une photographie de l'image vue dans la lunette de son fusil ou d'activer les boutons de sa radio individuelle sans lâcher son arme. Lors de la dotation des premiers régiments d'Infanterie, les plus jeunes ont très rapidement adapté leurs comportements tactiques aux nouvelles possibilités offertes, tandis qu'une appropriation plus lente était constatée pour de nombreux cadres.

Un besoin de reconnaissance et d'identification

Enfin, cette génération « connectée » gère son image extérieure comme un patrimoine vital. Les « Y » ont besoin d'être populaires et considérés comme un exemple au sein de leur groupe familial, professionnel ou amical. C'est pourquoi ils sont sensibles à des figures héroïques auxquelles ils peuvent s'identifier. Dans le monde actuel, les figures tutélaires incarnant l'abnégation, la volonté d'aboutir, l'ouverture d'esprit, la soif de victoire et de gloire ou tout simplement le génie ne sont pas des hommes en uniforme. Ce sont essentiellement des sportifs, des artistes ou des icônes de mode. Peu de français savent qu'Éric Tabarly était officier de Marine, qu'Alain Bernard est gendarme ou que Martin Fourcade sert comme caporal-chef au sein des Troupes de Montagne. À l'heure où le renforcement de nos Armées nécessite un recrutement important, il serait intéressant de s'appuyer sur l'aura des quelque 160 sportifs de haut niveau servant au sein du ministère des Armées pour attirer les jeunes vers un engagement qui valorise les qualités incarnées par ces athlètes.

Par ailleurs, l'armée manque de héros reconnus. La personnalité médiatique familière au « Y » est souvent une femme ou un homme considéré comme

« engagé » pour défendre des valeurs ou un idéal de vie. Individualité forte et charismatique, cette personne est fière de ses qualités professionnelles et capable de fédérer des groupes d'individus autour d'une cause. Cette description, que l'on pourrait croire guerrière, renvoie généralement à l'univers artistique ou sportif. Dans le cas des militaires, malgré de nombreux engagements récents et difficiles, malgré une ressource humaine de grande qualité que l'État forme techniquement et intellectuellement, aucun nom n'est réellement connu au sein de la population française, à part quelques figures comme de Gaulle ou Bigeard. Même au sein de l'institution, peu de soldats sont capables d'identifier une personnalité militaire contemporaine, hormis des officiers américains comme les généraux Norman Schwarzkopf (guerre du Golfe), Stanley McChrystal ou David Petraeus (Irak et Afghanistan). La composition de l'équipe de France de football est connue dans les cours d'école et les vainqueurs de concours audiovisuels de chanson ou de danse font la Une des journaux : *a contrario*, combien de Français peuvent citer le nom d'un soldat tombé pour la France durant ces deux dernières années ?

Il y a certainement une figure du Héros à reconstruire et à redécouvrir, non seulement pour attirer les jeunes de la « Génération Y » vers le métier militaire mais également pour honorer ceux dont le sacrifice ne peut être réduit à une statistique d'accident professionnel.

⁂

Finalement, cette « Génération Y » qui semble remettre en cause les schémas managériaux de l'entreprise n'a pas bouleversé la nature de l'engagement dans les Armées. Certes, leurs qualités et leurs défauts (qui ne sont souvent « que des exagérations de leurs qualités » selon François PICHAULT et Mathieu PLEYERS) nécessitent certaines prises de conscience. Néanmoins, ils présentent autant d'opportunités que de contraintes. Le seul point délicat demeure ce besoin de mouvement résultant d'une perte de confiance dans la stabilité du monde professionnel et la recherche d'une « séquence d'aventure de vie ». [Leur] épanouissement personnel n'est pas négociable » selon Christine Charlotin (citée par Guillemette FAURE).

Il s'agit donc de convaincre ces mercenaires du travail que l'Armée incarne bien les valeurs qu'ils recherchent et permettra leur épanouissement. Puis, pour les garder dans nos rangs, il faut une exemplarité accrue et une crédibilité des chefs, mais également répondre à leur espoir d'aventure et de participation à des projets concrets. Enfin, du soldat à l'officier, chacun a besoin de s'identifier à une figure héroïque dont il se sente proche. Or, en sus de nombreux français œuvrant au bien commun dans tous les domaines de la vie civile, cette génération engagée depuis 15 ans dans les opérations conduites par la France dans ses zones d'intérêt et sur son territoire ne manque pas de héros à mettre en avant.

Éléments de bibliographie

CABANES Bruno, « “Génération du feu” : aux origines d'une notion », *Revue historique* n° 641, janvier 2007, p. 139-150 (www.cairn.info/revue-historique-2007-1-page-139.htm).

FAURE Guillemette, « Génération Y… Les empêcheurs de travailler en rond », *Le Monde*, 11 mai 2013 (www.lemonde.fr/).

COUPLAND Douglas, *Generation X: Tales for an Accelerated Culture* ; 1991, St. Martin's Press ; 192 pages.

PICHAULT François et PLEYERS Mathieu, « Pour en finir avec la génération Y. Enquête d'une représentation managériale », *Annales des Mines*, *Gérer et Comprendre* n° 108, février 2012, p. 39-54 (www.cairn.info/revue-gerer-et-comprendre1-2012-2-page-39.htm).

SERRES Michel, *Petite poucette*, Éditions Le Pommiers, 2012, 84 pages.

RDN n° 803 - octobre 2017

Repenser le combattant dans le contexte stratégique français ?

Amaury de Pillot de Coligny

Étudiant à l'Institut de préparation à l'Administration générale (Ipag) de l'Université Panthéon-Assas (Paris 2) et représentant de l'ANAJ-IHEDN auprès de la Commission Armées-Jeunesse.

Le déploiement de milliers de combattants sur les théâtres d'opérations extérieures et sur le territoire national dans le cadre de l'opération *Sentinelle*, semble valider l'interdépendance entre les questions de défense et de sécurité. Il est vrai que la globalisation de la menace et l'apparition de groupes ou entités non-étatiques utilisant des techniques de terrorisme aux niveaux national et international semble le justifier. Toutefois, l'apparition de « nouvelles menaces » (1) ne fait pas disparaître le possible recours à la guerre étatique par des moyens conventionnels. Certaines régularités doivent interroger les tentations de penser un changement stratégique en dehors de toute dimension systémique. Celles-ci nécessitent davantage de penser le combattant comme soldat plutôt que d'adapter sa nature et ses fonctions aux problématiques sécuritaires.

De la nature du combattant dans le contexte stratégique français

Même si l'évolution du système international – chute du bloc de l'Est, attentats du 11 septembre 2001 – induit des tournants de la politique de défense et donc l'écriture d'un nouveau *Livre blanc*, certaines régularités demeurent. On peut en relever trois, bien qu'elles soient parfois contestées par divers courants théoriques. La première, largement développée par les théoriciens, est celle de l'anarchie dans les relations internationales qui rend le système international instable et laisse les États dans une incertitude constante et donc dans la nécessité de se protéger militairement contre de potentielles velléités belliqueuses. L'absence d'une force suprême capable de contraindre les États est un leitmotiv majeur dans la conduite d'une politique de défense. Ensuite, on peut noter la persistance de la

(1) Nous entendons comme « nouvelles menaces » la menace du terrorisme islamiste à la fois interne et international, la menace cyber, et les menaces issues du changement climatique (menaces sécuritaires liées aux migrations climatiques, menaces liées à la raréfaction des ressources naturelles et menaces liées à la nouvelle donne géopolitique issue du changement climatique notamment en Arctique).

guerre interétatique comme possible continuation d'une politique. Face à la tentation de penser un « monde sans guerre », un monde « arrivé à la fin de l'Histoire » dans lequel l'État serait devenu impuissant, rappelons que la guerre interétatique est toujours possible et que sa nature n'a pas changé [2]. Enfin, dernière régularité : l'ennemi existe toujours, même si celui-ci n'est plus clairement identifiable ou plus clairement identifié [3]. L'interpénétration des menaces internes et externes ne fait pas disparaître les seules menaces extérieures. Si la menace du terrorisme islamiste semble prééminente, elle ne fait pas disparaître d'autres ennemis, étatiques ou non, et peut-être même plus dangereux. Au final, le contexte stratégique français – bien qu'il ait sensiblement changé [4] – reste marqué par plusieurs régularités. C'est face à celles-ci que le combattant doit continuer d'être pensé.

Le combattant est avant tout un soldat dont la fonction première est de faire la guerre ; il est « guerrier » [5]. Il ne lui appartient pas de faire la paix. Pour le théoricien prussien CLAUSEWITZ, c'est au politique qu'il appartient de faire la paix. C'est lui qui désigne l'ennemi, décide d'entrer en guerre et de signer la paix. À ce titre, les appellations de « soldat de la paix » ou même « d'opération de maintien ou de rétablissement de la paix », si elles constituent un procédé rhétorique légitime, contiennent une ambiguïté stratégique certaine et complexifient à identifier clairement ce que sont réellement la paix et la guerre. Puisque le combattant est un soldat, il ne lui appartient pas non plus d'assurer la sécurité intérieure – hors temps de guerre bien entendu. À ce titre la mobilisation de soldats sur le territoire national pour assurer des missions « non-guerrières », comme les déambulations sur les trottoirs des grandes villes de France, pose un vrai problème. Parce que le contexte international reste fondé sur certaines régularités – anarchie, guerre interétatique, ennemi – le combattant doit continuer d'être pensé comme soldat et non comme suppléant aux agents de la paix ou aux fonctionnaires de sécurité. Ses fonctions et sa nature doivent rester inchangées, l'apparition de nouvelles menaces non-étatiques, intérieures, terroristes, appelant davantage une réponse sécuritaire (policière) et judiciaire que « guerrière » (cf. David CUMIN). Si les problématiques de la défense et de la sécurité s'interpénètrent elles ne doivent pas être mélangées.

De la mort du combattant dans le contexte stratégique français

Penser le combattant en tant que soldat permet de comprendre la normalité de sa mort à la guerre. Cette dure réalité paraît aujourd'hui difficile à entendre pour plusieurs raisons. D'abord l'évolution progressive des mentalités occidentales

(2) Colin GRAY, *La guerre au XXIe siècle* ; Paris, Économica, 2005, 423 pages.

(3) Amaury DE PILLOT DE COLIGNY, « Qui est l'ennemi ? Approche polémologique », Conseil supérieur de la formation et de la recherche stratégiques, 2015 (www.csfrs.fr/sites/default/files/approche_polemologique.pdf).

(4) Voir le premier paragraphe et les premiers mots de la préface : « J'ai en effet considéré que l'état du monde appelait de nouvelles évolutions stratégiques. Qui ne voit que le contexte a sensiblement changé depuis 2008 ? », *Livre blanc sur la défense et la sécurité nationale*, ministère de la Défense, 2013, p. 7.

(5) À ce titre, voir les ouvrages de David CUMIN, *Histoire de la guerre*, Ellipses, 2014, 288 pages et *Manuel de Droit de la guerre*, Bruxelles, Larcier, 2014, 534 pages.

depuis les deux guerres mondiales et la guerre du Vietnam a rendu anormale la mort du soldat à la guerre. Cette évolution n'est pas dénuée de sens. Lorsque l'on transforme le « guerrier » en « soldat de la paix » ou en « gardien de la sécurité », sa mort à la « guerre » semble logiquement plus anormale et plus incompréhensible. Toutefois, au-delà de cette évolution historique, il semble que « ce syndrome repose sur une évolution beaucoup plus fondamentale des sociétés développées, à savoir leur structure démographique » (6). Autrement dit « aussi longtemps que la mort a fait partie intégrante de la vie, qu'il a fallu concevoir dix enfants pour espérer en voir quatre ou cinq atteindre l'âge adulte, l'idée de sacrifier l'un d'entre eux sur les champs de bataille n'a pas provoqué de sentiment de révolte » (7). La baisse de la mortalité infantile et du taux de fécondité ont conséquemment concouru à ce que « ces rares enfants élevés dans un environnement où les risques principaux encourus sont ceux liés à la circulation automobile, se voient investis d'un capital affectif qui laisse peu de place au sacrifice militaire » (8). Ensuite, la technologisation des champs de bataille a laissé à penser à une possible guerre sans combattant et donc sans mort. Les victoires militaires remportées grâce à la puissance aérienne sans causer de pertes humaines participent malgré elles à rendre anormale la mort du combattant à la guerre. Enfin, si « l'économie des forces », l'un des « trois principes » du maréchal FOCH, est louable et légitime, le développement aux États-Unis lors de la première guerre du Golfe de la « théorie du zéro mort », qui préconise une guerre « sans mort » semble l'être beaucoup moins. Cette théorie n'a certes pas été érigée en doctrine mais tend à rendre anormale la mort du soldat qui était pourtant largement admise (9).

De l'anormalité de la mort du combattant, c'est-à-dire de la non-acceptation du combattant comme soldat à proprement parler, découle parfois l'incompréhension des familles qui se retournent contre l'armée ou les officiers supérieurs jugés responsables de la mort du combattant en demandant la tenue d'explications, un jugement ou une condamnation disciplinaire. L'anormalité de la mort du combattant participe aussi à considérer le soldat tombé à la guerre comme une victime davantage que comme un héros. Cette mentalité est totalement différente aux États-Unis où les hommages civils et militaires, déploiement de drapeaux, cérémonies dans les stades de football, convois mortuaires pavoisés sur les grandes routes, « héroïsent » le combattant. Au contraire, la prise en compte du combattant comme soldat dans un monde anarchique où la guerre et l'ennemi existent toujours permet de mieux penser la mort du soldat et sa signification.

(6) Claude ROOSENS, Valérie-Barbara ROSOUX, Tanguy DE WILDE D'ESTMAEL, *La politique étrangère : le modèle classique à l'épreuve*, Bruxelles, Peter Lang, p. 411.
(7) *Idem*, p. 411.
(8) *Idem*, p. 412.
(9) « On mesure l'importance de l'évolution lorsque l'on se remémore le départ précipité des soldats américains de Somalie, après la mort de dix-huit d'entre eux à Mogadisco, en octobre 1993 ou encore le retrait immédiat des Casques bleus belges de la *Minuar* après le massacre de dix soldats à Kigali, en avril 1994 », *Idem*, p. 411.

Enfin, la normalité de la mort du combattant est impérative dans le contexte stratégique français « parce que la réticence des populations à risquer la vie des soldats se répercute sur les décideurs, ce qui contribue à refermer un peu plus la fenêtre d'opportunité d'emploi des forces armées » (10). À titre d'exemple, lors de l'embuscade d'Uzbin en août 2008 qui a coûté la vie à dix soldats français, une partie de l'opinion publique a questionné le bien-fondé de la place de la France en Afghanistan. Mais quelle crédibilité aurait notre politique étrangère si nous choisissons de quitter un théâtre d'opération au-delà d'un certain nombre de morts ? Dit crûment, combien de soldats français l'ennemi devrait-il tuer pour que l'opinion publique ou les instances dirigeantes remettent en cause le bien-fondé d'une opération donnée ? De telles questions ne se poseraient pas dans ces termes si la mort du combattant à la guerre était normale et légitimement admise par l'opinion publique et les instances dirigeantes (11). Certes, on pourrait nous opposer que les guerres dans lesquelles la France est engagée ne sont pas totales dans leurs moyens et que le coût humain est bien entendu une condition de l'engagement de la France. Dans ce cas, la question serait de savoir jusqu'à combien de morts la France accepterait d'intervenir sur un théâtre d'opérations, la réponse engageant la capacité et la crédibilité de la France à intervenir.

⁂

Au terme de ces développements, il semble que le combattant soit aujourd'hui dans un entre-deux, exerçant des missions militaires sur les théâtres d'opérations extérieures et des missions de sécurité intérieure dans la lutte contre le terrorisme islamiste. La volonté de mêler les questions de défense et de sécurité tend à faire perdurer ce modèle. Pourtant la tentation de croire en l'apparition de « nouvelles menaces » nécessitant l'interpénétration des questions internes et externes, du militaire et du sécuritaire, est dangereuse. Les relations internationales restent anarchiques, la guerre interétatique est toujours possible et l'ennemi existe toujours. En cela la nature du combattant doit rester immuable, le soldat doit rester « guerrier » et sa mort à la guerre doit rester normale. Car si l'inadaptation aux mutations du système international est une erreur, la transformation de la nature du combattant ou de ses fonctions face aux régularités du système en est une encore plus grande et plus dommageable à l'avenir. ◆

(10) *Idem*, p. 412.

(11) Il convient de souligner toutefois qu'il ne s'agit pas là d'un apanage des sociétés démocratiques occidentales comme en témoigne la stratégie soviétique de 1989 en Afghanistan visant à éviter au maximum les pertes humaines mal acceptées par la population. Claude Roosens, Valérie-Barbara Rosoux, Tanguy de Wilde d'Estmael, *op. cit.*, p. 411 et Luttwak Edward, *Le grand livre de la stratégie. De la paix et de la guerre*, Odile Jacob, 2002, p. 111.

Innover pour penser et réaliser les capacités militaires de demain : un impératif catégorique

Jean-Philippe Rolland

Contre-amiral. Chef de la division cohérence capacitaire de l'État-major des armées (EMA).

Si toutes les menaces et tous les risques décrits dans notre référentiel de défense et de sécurité ne se sont pas concrétisés, tous ont évolué dans le sens d'une montée des tensions. Ce caractère est particulièrement perceptible pour nos concitoyens depuis la multiplication des actes terroristes commis sur notre territoire et en Europe « proche », mais les événements de Crimée, d'Ukraine, de Syrie, de Turquie, de mer de Chine, ont aussi manifesté le retour des États-puissances et de la géopolitique.

Cet état de fait a mis notre système de défense sous forte pression. Or, une révision à la baisse de nos intérêts de sécurité en 2017 est peu probable. Ce *stress* opérationnel pourrait en revanche diminuer si un effort résolu était fait pour remettre nos capacités d'action en mesure de soutenir durablement un tel rythme. Ce retour à une plus grande robustesse nécessitera d'adapter nos méthodes et d'améliorer nos travaux de préparation de l'avenir si l'on veut conserver l'avantage opérationnel, tant les choses évoluent rapidement.

C'est à cette entreprise que l'état-major des armées, avec le soutien des armées et de la DGA, s'est attelé dans le domaine des équipements, domaine structurant pour l'ensemble d'un système de défense car tout le reste en découle : savoir-faire, concepts de soutien, doctrine, organisation… Ce travail répond à la question : quels effets militaires nos armées doivent-elles être capables de produire pour gagner en opérations en 2030 ? Ses résultats confirment que des évolutions très significatives sont devant nous. Des voies se dessinent pour capitaliser sur les atouts dont nous disposons aujourd'hui, qui sont plus nombreux qu'on ne le croit souvent.

⁂

Les effets que nos forces, en 2030, seront capables de produire dépendent pour une large part des équipements que nous sommes en train d'acquérir, voire des plus récents déjà entrés en service. Porte-avions *Charles-de-Gaulle*, *Rafale*,

A400M, hélicoptères *Tigre* et *Caïman*, blindés de la future force *Scorpion*, *Frégates multimissions* (*Fremm*) figurent parmi les équipements qui constitueront encore l'ossature de nos armées. Ces capacités militaires, qui s'inscrivent dans un champ d'action toujours plus global, doivent pouvoir continuer à produire leurs effets, si possible bénéficier d'amélioration de leurs performances et s'adapter à l'évolution de leur environnement opérationnel.

Consolider les capacités d'aujourd'hui doit néanmoins s'accompagner d'un effort résolu pour penser l'avenir. De nouvelles capacités à même d'influer fortement sur la façon de conduire nos opérations, tels que des engins non pilotés ou bien de nombreux équipements de mission (capteurs, armement, systèmes d'information et de communication), restent à concevoir et à réaliser.

Que ces capacités soient à maintenir en service, à renouveler ou à créer, toutes doivent intégrer plus étroitement le caractère très évolutif de l'environnement opérationnel dans lequel elles seront déployées.

La proximité, voire la dilution, des espaces de confrontation militaire avec les champs d'activité de la vie économique, sociale et numérique n'est pas un facteur alternatif. Cela l'est d'autant moins que défense et sécurité continueront à voir leurs limites respectives s'estomper. La légitimité juridique mais aussi la « légitimité numérique » de nos actions, c'est-à-dire leur acceptabilité par les personnes façonnant leur opinion grâce aux réseaux sociaux, nécessitent une attention croissante et il ne peut être exclu qu'un jour les deux s'opposent. Des vulnérabilités vont revêtir une sensibilité accrue ou émerger, telles que l'environnement familial, social, ainsi que le profil digital de chacun de nos militaires, sphères individuelles qu'il faudra pouvoir protéger si l'on veut continuer à recruter et à fidéliser. Les champs de l'influence et des entraves nécessitent donc une attention particulière. Sur les théâtres d'opération comme au sein de l'opinion publique, la finalité et la légitimité des actions conduites doivent pouvoir être en permanence, non seulement rappelées ou démontrées, mais portées de façon dynamique et proactive afin d'écarter tout effondrement, soudain, immaîtrisable, du socle sur lequel ces actions sont bâties. Or les constantes de temps médiatique et politique, les possibilités ouvertes par les réseaux sociaux, l'émergence voire l'éruption de mouvements d'opinons qui ne connaissent pas de frontières, sont aujourd'hui telles que le « façonnage » de l'environnement opérationnel doit intégrer cette dimension dès les premiers stades de planification d'une opération… mais aussi dans la façon dont sont conçues, réalisées et employées les capacités militaires. Respect des conventions internationales, des traités et des lois, au premier chef, naturellement, mais en allant au-delà, par l'adaptation rapide des doctrines d'emploi de ces capacités selon les conditions du moment, en tenant compte des mouvements de l'opinion publique sur les réseaux et les médias.

Sinon, nos capacités opérationnelles verront apparaître des « entraves » à leur déploiement et à leur action, bien plus difficiles à prendre en compte que les

menaces classiques ou les risques que tout officier d'état-major est habitué à intégrer dans sa réflexion.

Autre facteur très évolutif, les nouvelles technologies issues du monde civil apporteront aussi des pistes exploitables positivement au plan militaire, en particulier dans le champ de la logistique, du soutien des forces, dans la gestion des données en masse et des réseaux. La recherche et le développement spécifiquement militaires resteront nécessaires pour conserver l'avantage technologique dans des domaines précis, pas directement profitables pour les grands acteurs économiques. La variété et le nombre des domaines d'investigation nécessiteront de continuer à sélectionner soigneusement les axes prioritaires.

⁂

Au-delà de l'environnement des opérations et de l'évolution technologique, les champs de l'action militaire seront eux-mêmes touchés par d'importantes transformations. La principale d'entre elles portera sur la nécessité de pouvoir combiner de façon plus rapide, plus précise, plus sécurisée, les effets apportés par des éléments de force. Il est même envisageable de créer de nouveaux modes d'action en mettant certains de ces éléments de force en situation de conjuguer leurs propres effets alors qu'ils n'en sont aujourd'hui pas capables. Cette voie permettra de conserver l'avantage malgré le caractère évolutif de la menace et le rattrapage technologique constaté chez certains acteurs stratégiques.

Ainsi, avec la numérisation du combat terrestre et la multiplication des capteurs contribuant à l'élaboration de la situation au sol, l'action des éléments combattants embarqués ou débarqués sera toujours orientée par le « renseignement » mais de plus en plus déterminée par une image tactique, construite et entretenue en temps réel ou quasi-réel, à l'instar de ce qui sous-tend l'action aérienne et navale. Avec le développement d'objets aériens à forte autonomie (drones de surveillance, capteurs embarqués sous ballons captifs ou mobiles, constellation de divers satellites basse couche), de nouveaux modes d'action s'ouvrent aussi à partir de la troisième dimension. Nous ne sommes qu'au début de leur identification.

Dès lors, les forces des trois milieux physiques classiques devront pouvoir construire leurs actions sur une approche mieux partagée d'une situation tactique désormais entretenue en permanence, qui devra être complète, unique, précise et fidèle. Nos réseaux, nos systèmes d'information et de commandement, nos capteurs doivent y pourvoir, en répondant, élargissement oblige, à une exigence très forte de résistance, passive et active, aux risques et attaques cybernétiques.

Les transformations rapides dans l'emploi de nos moyens devront s'accompagner d'une réflexion doctrinale tout aussi réactive pour que ces mutations soient maîtrisées, accompagnées et, pourquoi pas, suscitées. Dans l'instauration de cette dynamique, la préservation de l'interopérabilité avec nos Alliés restera primordiale.

Notre façon de concevoir nos futures capacités doit donc évoluer, tout comme notre industrie de l'armement qui doit aussi s'organiser pour répondre à ces nouveaux besoins. Cette démarche, déjà entreprise, doit être poursuivie rapidement car la menace, elle, n'attend pas. Elle devra s'attacher à intégrer le délai d'appropriation de ces nouveaux équipements par les utilisateurs et par ceux qui œuvrent dans leur environnement, techniciens et formateurs en particulier.

Au cœur de cette adaptation résident en particulier trois enjeux.

• L'enjeu de la connectivité est majeur. Les technologies nécessaires pour transmettre des volumes sans cesse croissants de données entre échelons de commandement et éléments de force tactiques sont identifiées. Leur intégration dans des capacités qui doivent répondre à des exigences d'interopérabilité interarmées, interalliée (et l'exigence de compatibilité avec les générations précédentes non encore remplacées) est loin d'être simple, en particulier lorsque, et c'est notre cas, des impératifs de souveraineté coexistent avec ces besoins d'interconnexion entre partenaires.

• Deuxième enjeu, souvent méconnu, la maîtrise de la datation, de la position et plus généralement du contenu de l'information tactique est, elle aussi, une exigence cardinale. Y répondre nécessite d'investir de nombreux champs dont celui de la géographie, de l'océanographie, de la navigation et du positionnement, par satellite ou autre moyen, mais aussi celui des normes et standards relatifs aux modèles numériques associés.

• La robustesse des réseaux et des équipements vis-à-vis des risques et menaces, en particulier numériques, constitue le troisième enjeu. Il s'agit de pouvoir continuer à compter sur les équipements, leurs logiciels, les flux et bases de données nécessaires, quelle que soit la nature de l'action conduite et quels que soient ceux qui s'y opposent. La résilience de capacités toujours plus connectées, inter agissantes, vis-à-vis d'attaques cybernétiques est un défi en organisation autant qu'un défi technologique. Il s'agit aussi d'éviter les déclassements d'équipements liés à l'asphyxie de leur cœur informatique ou à leur inaptitude à rester interfacés avec d'autres équipements plus modernes. Les armées, avec le soutien des services concernés de l'État, à commencer par la DGA, se sont mises en ordre de bataille pour relever ces défis.

⁂

Répondre à l'accélération du temps et des événements, aux enjeux amplifiés ou nouveaux créés par l'évolution du contexte dans lequel s'inscrira l'action militaire, nécessite d'investir de nouveaux domaines et d'adapter nos méthodes de construction de capacités, en capitalisant sur les nombreux atouts dont nous disposons déjà.

La Base industrielle et technologique de défense (BITD) est en France particulièrement solide, articulée autour de grands groupes de dimension mondiale qui nous ont placés à la pointe, en particulier dans les domaines stratégiques que sont les missiles, les communications, l'aéronautique de combat, la lutte sous la mer. Elle profite du dynamisme innovant de nombreuses ETI (Entreprises de taille intermédiaire) et PME (Petites et moyennes entreprises). Lorsqu'il faut imaginer des combinaisons de technologies, ces entités plus agiles savent répondre rapidement et de façon très créative. Mais n'apparaît pas encore clairement, à l'heure actuelle, d'acteur industriel français à même d'appréhender, dans sa globalité et dans une perspective de long terme, les exigences de connectivité et de répartition des performances entre plusieurs composantes d'un « système de systèmes ». Tout simplement parce que notre système de défense, comme tous ceux qui sont comparables au nôtre, s'est construit brique par brique, capacité par capacité. Il n'est sans doute pas possible de modifier cet état de fait et de repartir d'une page blanche. Il est en revanche nécessaire, pour les raisons indiquées en début d'article, de compléter cette marche en avant par une approche de renforcement de la cohérence d'ensemble, plus adaptative, afin de pouvoir produire demain les effets attendus, dans tous les champs de l'action militaire. Noble ambition et vaste entreprise, auxquelles les officiers et ingénieurs des armées et de la DGA se sont attelés et qui, inévitablement, auront des conséquences sur les méthodes de construction de nos futures capacités, sur la conduite des prochaines opérations d'armement et, probablement, pour les industriels.

Ces méthodes, pour être plus rapides, plus englobantes, passeront par un rapprochement de tous les acteurs concernés. Nous partons heureusement d'une situation très favorable : la préparation de l'avenir repose pour les équipements sur une étroite concertation interarmées, animée par l'EMA et la DGA, celle-ci entretenant avec la BITD des échanges permanents dans les champs technologiques et pour la préparation des opérations d'armement, bien avant leur lancement.

Notre industrie couvre tous les secteurs de l'armement et est de plus en plus étroitement associée aux enseignements tirés des opérations, conduites sous le commandement opérationnel du Chef d'état-major des armées (Céma), et qui se caractérisent déjà, et de plus en plus, par leur dimension interarmées.

Les conditions sont donc réunies pour que le haut degré d'engagement des forces contribue, en boucle courte, à adapter notre outil de défense aux exigences des opérations d'aujourd'hui et, si l'effort est maintenu, à celles de demain. ◆

L'officier face aux défis du XXIe siècle

Les Cahiers de la Revue Défense Nationale

Dans ce monde complexe qu'est celui du XXIe siècle, les défis sont nombreux et très variés. Nous l'avons vu dans la première partie de ce Cahier : de la modernité de notre temps découlent des enjeux humains de commandement, des enjeux politiques pour l'emploi de la violence légitime qu'incarnent les armées, et des enjeux technologiques pour les capacités militaires.

La guerre est un « fait social total » au sens de Marcel Mauss, c'est-à-dire un fait social qui peut être étendu à tous les domaines sociaux (juridique, politique, économique, etc.) et qui, s'il est décrypté, explique le fonctionnement de la société. Aujourd'hui, des formes nouvelles de guerre (sans États, sans frontières, impliquant de nouveaux acteurs, etc.) donnent lieu à un foisonnement de concepts nouveaux, tel que ceux de l'hybridité, de la surprise stratégique ou encore de la résilience.

L'article « Surprise stratégique ou défaillance de l'intelligence stratégique ? » met en garde contre l'utilisation tous azimuts du concept de « surprise stratégique » : dans la plupart des cas, l'intelligence est trompée par un excès de confiance dans l'expérience acquise, ou par une incapacité à traiter correctement le renseignement obtenu. Si l'intelligence doit permettre d'appréhender la complexité des situations et ce, notamment grâce à des compétences particulières en géopolitique ou géostratégie, elle ne peut s'exercer convenablement qu'à travers le discernement, conjonction de l'intelligence et de l'expérience.

De la même façon, l'application du concept de résilience à la lutte contre le terrorisme sur le territoire national demande une certaine profondeur d'analyse contextuelle et théorique, ce que fait admirablement bien l'auteur de l'article choisi sur ce sujet.

La complexité du XXIe siècle fait entrevoir à certains de nouvelles formes de guerre à conceptualiser, quand d'autres n'y voient qu'un retour de formes classiques de guerre. Le débat est nourri… Il semble indéniable cependant que ce siècle projette la guerre dans de nouvelles dimensions, dont le cyberespace et l'intelligence artificielle (IA) sont les plus emblématiques.

L'article « La Russie et le cyberespace, mythes et réalités d'une stratégie d'État » montre un acteur étatique usant de l'espace cybernétique dans une véritable stratégie de guerre de l'information. Devenu espace de confrontation à part entière, le cyberespace diffère dans ses caractéristiques des espaces physiques (terre, air, mer, espace extra-atmosphérique). Rendant possible l'anonymat des attaquants, il renverse par exemple le rapport de force classique entre la défense et l'attaque ; les « cyber-armes » se confondent avec les outils de la cybercriminalité, comme le montre le texte « De *Petya* à *NotPetya* : du cybercrime à la cyberguerre ? ».

Le domaine de l'IA est certainement le prochain à servir de terrain de confrontation. Connue depuis les années 1950, elle subit une accélération inédite, aujourd'hui où se conjuguent un accès à un volume de données conséquent (*Big Data*), grâce au cyberbespace, et des progrès en capacité de calcul sans précédent. L'article « À propos d'intelligence artificielle » propose une lecture des promesses actuelles faites par les algorithmes et de ces perspectives dont on ne perçoit pas encore les limites. Si l'aide à la décision est indéniablement un apport précieux de l'IA, elle comportera toujours le risque d'être leurrée et donc utilisée comme une « arme » de guerre.

Audrey Hérisson

RDN n° 800 - mai 2017

Surprise stratégique ou défaillance de l'intelligence stratégique ?

Mustapha Benchenane

Docteur d'État en science politique. Conférencier au Collège de défense de l'Otan.

Dans une relation conflictuelle, ou qui risque de le devenir, chacune des parties, chacun des belligérants, a la volonté de percer les intentions de l'autre, de le devancer, de bousculer ses forces, afin d'obtenir par les armes – au moindre coût pour lui-même – ce qu'il n'a pas pu obtenir par d'autres moyens. On parle alors de « surprise stratégique ». Celui qui en est l'auteur y a recours afin d'obtenir un avantage décisif. Selon Clausewitz, la « surprise devient par conséquent le moyen d'acquérir la supériorité… Lorsqu'elle réussit, elle sème la confusion et brise le courage de l'ennemi ». Ceux qui travaillent sur ces questions affirment que la surprise est « consubstantielle au domaine conflictuel » (cf. Vincent Desportes). S'il en était ainsi, il ne resterait plus qu'à y faire face, notamment, par une grande capacité d'adaptation, par la « résilience ». Seraient des « surprises stratégiques », l'opération *Barbarossa*, l'attaque japonaise contre Pearl Harbor, la chute du mur de Berlin, les attentats du 11 septembre 2001, etc. En réalité, dans la très grande majorité des cas, il s'agit d'une défaillance de l'intelligence stratégique.

Un échec de la veille stratégique

L'expérience qui inhibe l'intelligence

Il ne s'agit pas de faire preuve de lucidité *a posteriori*, mais de constater que ceux qui étaient en charge de la protection de leur pays n'ont pas respecté l'obligation de moyens. La France aurait été victime d'une « surprise stratégique » en 1940, parce que les Allemands sont passés par la « trouée des Ardennes » et non là où on les attendait, le long de la « ligne Maginot »… L'une des fautes les plus graves commise par les stratèges en général, consiste à penser les conflits du futur exclusivement à l'aune des conflits du passé. La « ligne Maginot » est l'une des illustrations de cet enfermement dans une seule hypothèse. On donne ainsi à l'adversaire le monopole de la « surprise stratégique ».

S'agissant plus précisément de la Seconde Guerre mondiale, le général de Gaulle avait publié *La France et son armée* (1938) et *Vers l'armée de métier* (1934), ouvrages dans lesquels il décrivait la nature des prochains conflits et les moyens modernes qui seront mobilisés. Il n'a pas été entendu.

La manière dont les Allemands ont procédé est pratiquée depuis de très nombreux siècles : depuis Epaminondas lors de la bataille de Leuctres (371 av. J.-C.) et surtout par Hannibal contre les armées de Rome (218-216 av. J.-C.) : une audace tactique produisant un avantage stratégique, le « coup de massue » décisif aux forces adverses. C'est de la sorte que s'y sont pris les Israéliens lors de la guerre de juin 1967 dite « guerre des Six Jours » : les aviations égyptienne et syrienne ont été détruites au sol en moins de quarante-huit heures. Il y a eu une défaillance des services de renseignements du Caire et de Damas. En effet, lors d'un colloque organisé par les Israéliens et auquel participaient les généraux de ce pays, ces derniers ont ouvertement reconnu que le plan qu'ils avaient mis en œuvre était prêt depuis plusieurs années, et qu'ils n'attendaient que le moment propice pour passer à l'action.

Les mêmes Israéliens qui s'étaient montrés si efficaces en 1967 le seront beaucoup moins lors de la guerre d'octobre 1973 qui les a opposés à l'Égypte et à la Syrie. Croyant être à l'abri derrière la ligne Bar-Lev, ils ont fait preuve d'un manque de vigilance flagrant. La ligne Bar-Lev a été édifiée par les Israéliens après la guerre de juin 1967 sur la rive orientale du Canal de Suez. Haute d'une vingtaine de mètres, sur 200 kilomètres, faite de sable et de terre compactés, une pente de 45 à 60°, les berges minées, une trentaine de fortins, des tranchées, etc., donc, « infranchissable ». En outre, l'armée israélienne contrôlait les cols de Mittla et de Giddi, ce qui renforçait ses lignes de défense.

Or, les Égyptiens vont se lancer à l'assaut de la ligne Bar-Lev et réussir à faire passer leurs troupes de l'autre côté du Canal, dans le Sinaï. Cette attaque s'est produite dans le contexte de la fête du Kippour, ce qui expliquerait, du moins partiellement, l'effet de surprise. Mais s'agit-il d'une surprise stratégique ? Oui, du point de vue israélien qui consistait à mépriser les armées arabes, donc à les croire incapables de monter une opération d'une telle envergure et d'une si grande complexité. Le 5 octobre 1973, veille de la fête juive du Kippour et de l'offensive égyptienne, le journal israélien *Maarive* affirmait : « Les forces de *Tsahal* surveillent de près tout ce qui se passe du côté égyptien sur le Canal de Suez. Toutes les mesures ont été prises pour éviter une attaque surprise »… Henri KISSINGER écrivait : « Toute analyse israélienne (ou américaine) corroborait l'idée que l'Égypte et la Syrie ne possédaient pas les capacités militaires nécessaires pour reconquérir leurs territoires par la force des armes, donc il n'y aurait pas de guerre » (cf. Pierre MILZA). Or, Michel JOBERT, ministre des Affaires étrangères déclara : « … des territoires étaient occupés et des gens souhaitaient y rentrer, parce que les considérant comme les leurs. Dans ces conditions, leur agression ne devait pas être imprévue » [(1)].

L'incapacité à traiter le renseignement

L'attaque japonaise contre Pearl Harbor le 7 décembre 1941 nous est présentée comme l'exemple même de la « surprise stratégique ». En réalité, cette offensive

(1) Déclaration de Michel JOBERT devant l'Assemblée nationale sur le conflit du Proche-Orient, 17 octobre 1973.

n'a pas éclaté comme un « coup de tonnerre dans un ciel serein ». Elle est intervenue dans un contexte international conflictuel marqué par la guerre en Europe, l'impérialisme japonais en Asie et les initiatives américaines pour contrarier la politique de Tokyo dans la région. Le choix américain d'Hawaï pour y déployer sa flotte a fait l'objet de controverses. Des simulations d'attaques avaient été réalisées en 1932 et en 1938. Elles avaient démontré la vulnérabilité de cette zone. Le commandant japonais Fuchida, responsable de l'opération contre Pearl Harbor (2), dit avoir été « frappé par l'imprévoyance et le manque de préparation des États-Unis, en particulier par le fait qu'ils n'ont pas pensé à protéger leurs cuirassés avec des filets pour torpilles ». Charles LINDBERGH écrit dans le *Journal du Temps de Guerre* : « …. l'attaque des Japonais ne me surprend aucunement. Nous les poussons à la guerre depuis plusieurs semaines. Ils ont simplement pris les devants ».

Sans prétendre à l'exhaustivité, on peut aussi se référer à l'opération *Barbarossa* comme un autre exemple de fausse « surprise stratégique ». Ce nom de code concerne l'attaque allemande contre l'URSS le 22 juin 1941. En principe, l'Allemagne et l'URSS étaient à l'abri de ce type de surprise, puisque les deux puissances avaient signé le 23 août 1939 le « Pacte de non-agression ». Chacun voulait gagner du temps. Mais nous savons, au moins depuis MACHIAVEL, qu'un Traité ne met jamais à l'abri de façon absolue : il est le reflet des intérêts et des rapports de force du moment. D'autre part, nous savons depuis plusieurs décennies que STALINE avait été informé, par plusieurs sources concordantes, de l'imminence d'une attaque allemande contre son pays. Il s'est entêté à ne pas y croire, notamment parce qu'il était persuadé que Hitler ne tenterait rien contre l'URSS avant d'avoir gagné la guerre contre la Grande-Bretagne (*cf.* David E. MURPHY).

En revanche, l'action terroriste contre les tours jumelles à New York et contre le Pentagone, le 11 septembre 2001, est celle qui se rapproche le plus de la « surprise stratégique ». Les États-Unis étaient devenus une « hyperpuissance » depuis la chute du mur de Berlin en 1989 et la dislocation de l'Union soviétique en 1991. De plus, les Américains avaient l'ambition de mettre en place un système de défense d'une redoutable efficacité : le bouclier antimissiles. C'est à ce moment-là que survient la surprise : ils furent attaqués de l'intérieur par des individus armés de cutters qui ont détourné des avions de ligne pour en faire des armes d'une capacité de destruction inimaginable. Les tours jumelles symbolisaient le savoir-faire des Américains en même temps qu'elles semblaient défier le ciel et même au-delà. Quant au Pentagone, il est le cœur de la dimension militaire et la marque de la suprématie militaire.

L'impact de cette action terroriste est considérable et son onde de choc propagera ses effets négatifs sur plusieurs générations d'Américains. À court terme, l'effet de sidération recherché a été largement atteint.

(2) C'est l'Amiral Yamamoto qui a conçu et préparé l'opération contre Pearl Harbor.

Les attaques auraient-elles pu être évitées ? La théorie du « complot » des États-Unis contre eux-mêmes étant absurde, il reste à constater que les services de sécurité de Washington disposaient de renseignements qu'ils n'ont pas exploités, qu'ils n'ont pas su interpréter. C'est ainsi que le *FBI* avait remarqué une activité « anormale » : des étrangers de confession musulmane s'entraînaient de façon intensive au pilotage d'avions en Floride. Des services de renseignements étrangers (dont la France), avaient prévenu les autorités américaines que leur pays allait faire l'objet d'une attaque.

Dans la plupart des cas que l'on dit relever de la « surprise stratégique », il n'aurait pas dû y avoir de surprise. Des informations étaient entre les mains des décideurs mais ces derniers ont fait preuve, au minimum, de légèreté.

« Surprise stratégique » et effet *boomerang*

Le prix d'une faute stratégique

Dans la plupart des cas dits de « surprise stratégique », l'État qui en est l'auteur non seulement n'a pas atteint les objectifs qu'il visait, mais plus encore a payé un prix très lourd et, parfois, il ne s'en est jamais remis.

Hitler, grisé par des victoires obtenues trop facilement en Europe, a commis la faute qui lui sera fatale en s'attaquant à l'URSS le 22 juin 1941 et en déclarant la guerre aux États-Unis le 11 décembre 1941 alors qu'il était encore engagé dans le conflit contre l'Angleterre.

Or, l'intelligence stratégique consiste, notamment, à éviter d'avoir trop d'ennemis à la fois, d'une part pour ne pas disperser ses forces, d'autre part pour ne pas induire une coalition de tous ceux dont on a fait des ennemis. C'est ce qui va se produire : lors de la Conférence Acadia qui s'est tenue à Washington le 1er janvier 1942, un Pacte a été conclu entre 26 États. Il s'agit de la « Déclaration des Nations unies ». Par la suite, un traité a porté sur « une alliance militaire contre l'Allemagne d'Hitler et ses alliés », entre le Royaume-Uni et l'URSS le 26 mai 1942, et entre l'URSS et les États-Unis le 11 juin.

En s'attaquant aux États-Unis à Pearl Harbor le 7 décembre 1941, les dirigeants japonais étaient loin d'imaginer la tragédie dans laquelle ils allaient plonger leur peuple quelques années plus tard. Cela commence à Pearl Harbor et se termine par les bombes atomiques sur Hiroshima et Nagasaki, ce qui oblige Tokyo à une capitulation sans condition comme ce fut le cas pour l'Allemagne nazie.

S'agissant d'un conflit régional telle la guerre d'octobre 1973 entre d'une part Israël et d'autre part l'Égypte et la Syrie, l'offensive audacieuse et réussie contre la ligne Bar-Lev a tourné en défaveur de l'armée égyptienne dans le Sinaï. Celle-ci a stoppé son offensive après avoir bousculé les défenses israéliennes sur une profondeur de 15 km en laissant un vide, une brèche de 40 km sans aucune

surveillance entre la 2e et la 3e armée, espace que le général Sharon a utilisé pour passer sur la rive occidentale du Canal de Suez où les Égyptiens ne disposaient d'aucune force de réserve. C'est ainsi que l'initiative du Caire s'est terminée par une cuisante défaite de l'armée égyptienne.

L'attaque du 11 septembre 2001 contre les États-Unis présentée comme « surprise stratégique » s'est, elle aussi, terminée par un désastre pour ses auteurs. L'effet de sidération obtenu par les terroristes n'a pas duré très longtemps puisque, dès octobre 2011, les États-Unis se prévalant du droit de légitime défense, reconnu par la Charte des Nations unies, ont porté la guerre en Afghanistan. Ce pays était gouverné par les *taliban*, extrémistes se réclamant de l'Islam, qui hébergeaient Ben Laden et son mouvement, *Al-Qaïda*, responsables de cette tragédie. En application de l'article 5 de la Charte de l'Otan qui prévoit une solidarité automatique si l'un des membres de l'Organisation était victime d'une agression, plusieurs alliés des États-Unis envoyèrent des troupes pour épauler les Américains.

Au 31 décembre 2011, les résultats obtenus étaient impressionnants : les *taliban* avaient été chassés du pouvoir et ceux qui purent s'échapper allèrent se réfugier dans les zones tribales du Pakistan. Quant à *Al-Qaïda*, beaucoup de ses membres furent tués, en particulier par des bombardements intensifs, et ceux qui ont survécu partirent eux aussi pour le Pakistan. L'objectif fixé a été atteint. Ben Laden lui-même fut exécuté au Pakistan en 2011 par un commando des forces spéciales américaines, opération au cours de laquelle l'effet de surprise et, en amont, le renseignement, ont été décisifs. Mais là encore, les *taliban* et *Al-Qaïda* firent preuve d'une capacité de résilience que personne n'avait prévue : ni les États-Unis, ni les autres membres de l'Otan ne s'attendaient à ce que ce conflit dure quatre fois plus longtemps que la Seconde Guerre mondiale. Cette réalité n'est-elle pas une autre forme de « surprise stratégique » ? Ne peut-on pas considérer que la situation créée en Irak par les Américains à partir de 2003 en est une autre ? Les conséquences de l'intervention de l'Otan en Libye seraient-elles constitutives d'une « surprise stratégique » ?

S'agirait-il d'une dynamique déclenchée par la guerre et qui échappe aux puissances qui en ont pris l'initiative ?

« Surprise stratégique » ou dynamique de la guerre non maîtrisée ?

Les exemples afghan, irakien, libyen sont, à cet égard édifiants, sans oublier la guerre israélo-arabe d'octobre 1973 qui fût à l'origine du premier choc pétrolier, c'est-à-dire le quadruplement du prix du pétrole et la fin, en Occident, des Trente Glorieuses.

En Afghanistan, l'objectif de guerre autour duquel il y a eu consensus tant à l'ONU qu'au sein de l'Otan, consistait à chasser les *taliban* du pouvoir et venir à bout d'*Al-Qaïda*. Mais les vrais problèmes sont apparus à partir du moment où

les Américains décidèrent, sans concertation avec leurs alliés, de poursuivre d'autres objectifs de guerre : démocratiser l'Afghanistan, mettre en place une « armée nationale », « gagner les esprits et les cœurs ». Ce fût le début d'une autre guerre qu'aucune puissance étrangère ne pouvait gagner pour deux ou trois raisons fondamentales : la démocratie est une culture, on ne peut donc pas l'imposer par la force ; les populations de ce pays sont structurées sur des bases ethniques et tribales, or, tuer les *taliban* et, en même temps « gagner les esprits et les cœurs » sont deux objectifs irréductiblement antagonistes ; enfin, créer une « armée nationale » là où il n'y a pas de nation, est un non-sens. Cet échec relève-t-il de la catégorie « surprise stratégique » ou de celle d'une dynamique propre à la guerre ?

Dans le cas de l'Afghanistan comme dans celui de l'Irak et de la Libye, le chaos provoqué par ces guerres a pour cause principale une méconnaissance des réalités historiques, culturelles, sociologiques, religieuses de ces pays.

En Irak, les Américains ont déclenché une guerre illégale au regard de la Charte des Nations unies. L'attaque américaine a commencé le 20 mars 2003, la chute de Saddam Hussein s'est produite le 12 avril 2003, et George W. Bush a déclaré l'achèvement des combats, « Mission accomplie », le 1er mai 2003. Mais c'est à partir de ce moment-là qu'une autre guerre a commencé. Les Américains ont commis la faute politique consistant à chasser de leur poste tous ceux qui étaient compromis avec l'ancien régime, c'est-à-dire, à peu près tous les Irakiens sunnites. Ils confièrent le pouvoir aux seuls chiites tout en laissant les Kurdes s'organiser selon des modalités proches de l'Indépendance. Sans l'avoir voulu, Washington offrit à l'Iran chiite une zone d'influence en Irak. La conjonction de tous ces facteurs se traduisit par une guerre civile dont l'un des acteurs – *Daech* – est le produit de l'initiative guerrière américaine en 2003. Dans ce cas, comme en Afghanistan, les responsables américains se sont lancés dans des conflits armés sans aucune étude de faisabilité.

On peut en dire autant de l'action de l'Otan en Libye : l'objectif de guerre était la protection de la population de Benghazi. Mais l'Otan a outrepassé le cadre tracé par la Résolution 1973 du Conseil de sécurité, et s'est fixé pour objectif la chute de Kadhafi… C'est ce qui fut accompli mais avec comme conséquence l'implosion de l'État et du peuple Libyen. Là encore, « surprise stratégique » ou aléas de la guerre ? En ayant une vraie connaissance des réalités du pays et en respectant scrupuleusement le Droit international, la tragédie que vivent les Libyens depuis six années aurait pu être évitée.

⁂

La « surprise stratégique » ne doit pas être l'habillage de la défaillance de l'intelligence stratégique. Par ailleurs, verser dans le fantasme de toute puissance et croire que l'on peut tout prévoir et tout maîtriser, n'est pas raisonnable. Néanmoins quand, par exemple, le général DE GAULLE et le général AILLERET présentent leur

conception de la « défense tous azimuts », ils tirent les leçons de l'Histoire en même temps qu'ils ont une vision réaliste du présent et de l'avenir (cf. Charles AILLERET).

Pour imaginer et créer une surprise stratégique, de même que pour l'éviter – dans ce cas elle n'est plus une surprise – il faut que les stratèges – et les États – rassemblent un certain nombre de qualités et de conditions. C'est un « *cocktail* » composé de force et de ruse. Mais cela ne suffit pas. Il convient d'ajouter l'intelligence qui permet d'appréhender la complexité, des compétences particulières dans les domaines de la géopolitique, de la géostratégie, un dispositif efficace de collecte et de traitement du renseignement afin de bien connaître l'adversaire, ses points forts, ses vulnérabilités. Le discernement, qui se situe à la conjonction de l'intelligence et de l'expérience, n'est pas la moindre des exigences. Deux autres « ingrédients » sont utiles : une certaine part de paranoïa et une autre de perversité afin d'être toujours en avance d'une anticipation, d'une ruse sur celui que l'on veut surprendre ou sur celui dont on veut percer les arrière-pensées malignes.

Pour toutes ces raisons, l'intelligence stratégique ne peut être qu'une intelligence collective…

Éléments de bibliographie

AILLERET Charles, « Un système de défense qui ne soit dirigé contre personne, mais mondial et tous azimuts », *Revue de Défense Nationale*, décembre 1967, p. 1923-1932.

DESPORTES Vincent, « Penser la surprise stratégique » (Libre opinion), Association de soutien à l'armée française (ASAF), 10 novembre 2014 (www.asafrance.fr).

MILZA Pierre, « La guerre du Kippour », *L'Histoire*, n° 60, octobre 1983.

MURPHY David E., *Ce que savait Staline, l'énigme de l'opération* Barbarossa, Éditions Stock, 2006, 462 pages.

RDN n° 803 - octobre 2017

Le concept de résilience face au terrorisme

Albin Leprince

Chef d'escadron (Gendarmerie), stagiaire de la 24e promotion de l'École de Guerre (« Général Gallois »).

Terme jusque-là principalement usité dans les sciences (1), notamment dans la métallurgie et la mécanique pour mesurer la résistance de certains matériaux à différentes contraintes jusqu'au point de rupture, puis vulgarisé ensuite par le psychiatre Boris Cyrulnik pour désigner la capacité individuelle à surmonter un traumatisme (2), le concept de résilience a été introduit dans le champ des sciences sociales et de la stratégie, essentiellement depuis les attentats du 11 septembre 2001, pour qualifier la capacité de l'ensemble d'une entité politico-stratégique à fonctionner en absorbant les chocs d'attaques répétées.

Au niveau de la nation entière, « la résilience se définit comme la volonté et la capacité d'un pays, de la société et des pouvoirs publics à résister aux conséquences d'une agression ou d'une catastrophe majeure, puis à rétablir rapidement leur capacité de fonctionner normalement, ou tout au moins dans un mode socialement acceptable. Elle concerne non seulement les pouvoirs publics, mais encore les acteurs économiques et la société civile tout entière » (3). Apparu dans les textes officiels avec le *Livre blanc sur la défense et la sécurité nationale* de 2008, le concept de résilience prend d'abord en France un caractère essentiellement institutionnel, touchant l'organisation des pouvoirs publics, les priorités retenues dans les capacités de renseignement, d'analyse et de décision, ainsi que la coopération entre l'État, les collectivités territoriales et les entreprises privées dans les secteurs considérés ici comme stratégiques : énergie, communication, santé, alimentation (4). En revanche, le rôle des forces morales en général et de la population en tant que telle n'est pas mentionné. Par la suite, le *Livre blanc* de 2013 témoigne cependant d'une évolution à cet égard. Sans abandonner son lien avec la notion de continuité des fonctions essentielles du pays, la résilience y est appréhendée comme un objectif situé dans le prolongement du lien armées-nation, considérant que « [l']appropriation

(1) Écologie, biologie, physique, thermique, informatique. Gestion d'entreprise : résilience organisationnelle, capacité à s'adapter après un incident.

(2) Boris Cyrulnik et Gérard Jorland, *Résiliences. Connaissances de bases*, Odile Jacob, 2012, 224 pages.

(3) Direction générale des relations internationales et de la stratégie (DGRIS) : « Contribution des armées à la résilience des nations : aspects humains et organisationnels » (www.defense.gouv.fr/), ajoutant que « l'accroissement de la résilience sociétale a été défini comme l'un des objectifs de la stratégie de sécurité nationale française ».

(4) *Défense et Sécurité nationale : le Livre blanc*, Odile Jacob - La Documentaion française, 2008, p. 64.

collective de la stratégie de défense et de sécurité nationale est la condition *sine qua non* de la résilience de la Nation » et que « le recrutement, la reconnaissance du métier des armes, le soutien de la population à l'action des forces ainsi que la capacité de résilience face à une crise dépendent en grande partie de la vigueur du lien qui unit ces forces à la société française » (5).

Un concept miroir de la vulnérabilité des sociétés hétérogènes

En ce sens, la résilience se rapporte aux forces morales et à la volonté collective, mais ne s'y réduit pas, sous-entendant le maintien des fonctions essentielles, non seulement à la survie mais aussi à la préservation d'une capacité à manœuvrer. Ce concept renvoie donc intrinsèquement à la notion de système, au sens de tout organisme fondé sur l'interdépendance de ses composants, interagissant entre eux selon certains principes ou certaines règles (6). À ce titre, tout système présente une capacité structurelle de résilience, qu'il est théoriquement possible d'optimiser en agissant tant dans le domaine de l'anticipation et de la préparation des crises, que, s'agissant d'un système sociopolitique, sur le plan de l'information de la population ou sur celui de la conscience collective. Sur ce dernier point cependant, les sociétés postmodernes présentent des vulnérabilités plus manifestes, de par la montée de l'individualisme, qui sous-tend la progression des logiques du droit et du marché au détriment du primat du politique. Comme souvent, l'apparition formelle d'un concept dans le champ des sciences sociales est constatée quand la chose ne va plus de soi.

En effet, à travers la globalisation des échanges, le développement continu des réseaux et l'intensification des flux de personnes, de marchandises et de capitaux atténuent les logiques de frontières, et donc « facilitent la propagation des crises et peuvent en augmenter l'impact » (7). Cette mobilité et cette volatilité sont mises à profit par le terroriste, qui conçoit lui aussi son action comme l'élément local d'un combat mondial (8) : comme le constate le sociologue Zygmunt BAUMAN, « les participants des conflits asymétriques sont tous en définitive "transnationaux" (…) mobiles, affectés à aucun lieu, ils changent facilement de cible et ne reconnaissent aucune frontière (…) les guerres vraiment asymétriques sont un événement concomitant du processus de globalisation » (9). De ce fait, sécurité intérieure et défense extérieure, longtemps séparées, s'inscrivent à présent dans un vaste

(5) *Ibidem*, p. 23 et 122.

(6) Selon Ludwig VON BERTALANFFY, *Théorie générale des systèmes*, Dunod, 1973.

(7) *Défense et Sécurité nationale : le Livre blanc, op. cit.*, p. 11.

(8) David GALULA, *Contre-insurrection, Théorie et pratique*, Économica, 2008, p. 75 : « Une guerre révolutionnaire locale n'est qu'un élément du combat mondial contre le capitalisme et l'impérialisme. Une victoire militaire contre un ennemi local représente en fait une victoire sur l'ennemi global et contribue à sa défaite finale. »

(9) Zygmunt BAUMAN, *La société assiégée* (traduction de *Society under Siege*, Polity Press, Cambridge, 2002), Rodez, Le Rouergue/Chambon, 2005, p. 142 et 146.

continuum, traitant de menaces aux ramifications potentielles multiples, rehaussant l'importance de la résilience.

De plus, le développement des technologies de la communication et de l'information, conjugué au phénomène d'urbanisation, permet à des groupuscules marginaux de profiter d'une caisse de résonance de leurs actions disproportionnée à leur importance réelle. Un tel contexte fournit au terrorisme une nouvelle dimension, que Raymond ARON annonçait déjà dès 1962 : « Une action violente est dénommée terroriste lorsque ses effets psychologiques sont hors de proportion avec ses résultats purement physiques. » (10).

Enfin, le caractère composite de ces sociétés, regroupant des populations de provenances et de cultures sensiblement différentes et s'organisant volontiers sur la base du communautarisme, affaiblit le sentiment commun d'appartenance, en affectant notamment les soubassements culturels et politiques de la conception volontariste française de la nation, qui repose sur l'idée, développée notamment par Ernest Renan, d'une sociabilité commune (11).

Pour toutes ces raisons, la formule célèbre attribuée à MAO, selon laquelle « le partisan est dans le peuple comme un poisson dans l'eau » (12), se vérifie d'autant plus aisément. Ainsi, viser le délitement de la cohésion sociale en tablant sur la fragilité d'ensemble des « sociétés complexes » (13), gripper le fonctionnement normal des institutions, empêcher une société de réagir de manière rationnelle et coordonnée en exploitant le désordre et la peur, tels sont les objectifs du terrorisme de la vague actuelle. La résilience se comprend au contraire comme la résistance physique et psychologique à la pression, voire aux tentatives de disruption (14).

Les cibles civiles : ligne de moindre résistance morale ?

Un système politico-stratégique est d'abord un tout organique. Bien avant les facteurs de vulnérabilité susmentionnés et liés aux évolutions contemporaines, CLAUSEWITZ, dans son traité *De la Guerre*, relie le peuple au domaine de l'irrationnel et des passions, comme composante de l'« étonnante trinité », aux côtés de l'entendement et de la libre activité de l'âme qu'il associe aux figures du politique et du chef d'armée (15). Source et véhicule des forces morales, la population présente

(10) Raymond ARON, *Paix et guerre entre les Nations*,Calman-Levy, 1962, p. 176.

(11) Ernest RENAN, *Qu'est-ce qu'une nation ?*, Éditions Mille et une nuits, 2009, p. 31. « Deux choses qui, à vrai dire, n'en font qu'une, constituent cette âme (…) l'une est la possession en commun d'un riche legs de souvenirs ; l'autre est le consentement actuel, le désir de vivre ensemble, la volonté de continuer à faire valoir l'héritage que l'on a reçu *indivis* (…) La nation est l'aboutissant d'un long passé d'efforts, de sacrifice et de dévouements ».

(12) David GALULA, *Contre-insurrection, Théorie et pratique, op. cit.*, p. 77.

(13) Terme de Joseph A. TAINTER, *L'effondrement des sociétés complexes* ; Paris, Éditions « Le retour aux sources », 2013.

(14) « Résilience et moral », *Histoire et Stratégie* n° 20, *Résilience – Ou comment combattre le terrorisme*, décembre 2014-février 2015, p. 83.

(15) Carl VON CLAUSEWITZ, *De la Guerre*, Éditions Perrin, 1999.

donc *a priori* une vulnérabilité critique qui en fait également la cible de toute stratégie de la terreur.

Historiquement, ce sont les doctrines de la première génération des théoriciens du bombardement stratégique qui sont à l'origine du raisonnement, puis de la pratique à grande échelle de l'emploi de la terreur contre les populations civiles. Le point commun avec le terrorisme réside dans la capacité à atteindre l'ennemi par-delà les barrières physiques, ainsi que dans l'intention de le faire capituler en brisant sa force morale dans le cadre d'une approche indirecte : au-delà des victimes, la véritable cible est le gouvernement ennemi. Le principe est ainsi affirmé par le général italien DOUHET : « Parce que, et il faut bien garder cela à l'esprit, la frappe aérienne est dirigée non seulement contre les cibles de moindre résistance physique, mais aussi contre celles de moindre résistance morale (…) Une débâcle doit nécessairement se produire, une débâcle profonde de tout l'organisme, et le moment ne peut qu'arriver rapidement où, pour fuir l'angoisse, les populations, poussées uniquement par instinct de conservation, réclameront, à n'importe quelle condition, la cessation du combat. » (16).

Ne pouvant quant à lui délivrer des frappes massives, le terrorisme asymétrique privilégie une logique d'attrition tout en recherchant la psychose et en s'appuyant sur sa capacité à surgir partout : « Le désordre, état normal de la nature, est beaucoup moins cher à créer qu'à combattre : (…) il lui suffit de lancer une grenade dans un cinéma pour qu'il faille faire fouiller toutes les personnes entrant dans un endroit public (…) En lançant de simples alertes à la bombe par coup de téléphone anonyme dans une bagagerie d'aéroport, l'insurgé peut bouleverser le trafic aérien et terroriser les voyageurs. » (17).

Ainsi, la finalité poursuivie par les actuels groupes djihadistes n'est pas tant l'effondrement d'un territoire que la substitution d'un système de normes à un autre (18), par remplacement des modes de régulation sociaux, et en tirant parti de l'affaiblissement des institutions. Contrairement au terrorisme des guerres révolutionnaires, celui-ci vise moins à « tirer les masses de leur apathie » qu'à « les y plonger et inhiber leurs facultés de défense ou d'initiative » (19). Cet aspect de la menace renvoie donc à un niveau plus profond de résilience, celui de la résilience dite sociétale, se rapportant aux représentations culturelles collectives, notamment en ce qu'elles touchent la cohésion sociale, la représentation de l'ennemi, le rapport à la mort. C'est sans doute sur ce point que la lutte asymétrique opposant des groupes ou des cellules terroristes fanatiques à nos sociétés occidentales *post*-modernes induit le rapport le plus défavorable à celles-ci : le matérialisme ambiant et les modes de vie fondés sur l'immédiateté tendent à l'accroissement de la crainte

(16) Giulio DOUHET, *La Maîtrise de l'air*, Économica, 2007, p. 75 et 142.
(17) David GALULA, *Contre-insurrection, Théorie et pratique, op. cit.*, p. 20-21.
(18) « La disruption en stratégie », *Histoire et Stratégie* n° 20, *op. cit.*, p. 36.
(19) Pierre MANNONI, *Les logiques du terrorisme*, In Press, 2004, p. 10.

de la mort ; fragilisant d'emblée la résilience. Tendance à laquelle la suspension du service national ne contribue pas à remédier, accroissant la distinction structurelle entre « sécurisants » et « sécurisés » [20], distinction qui finit par devenir pénalisante dans le cadre d'une approche strictement institutionnelle ou administrative de la question de la résilience.

Or, si l'attitude de la population s'avère déterminante au plan politico-stratégique, sa réaction apparaît déterminée non pas tant par l'ampleur des attaques – en témoigne l'échec des campagnes de bombardement stratégiques sur l'Angleterre et sur l'Allemagne à provoquer le renoncement ou le retournement des populations – mais par le rapport de confiance qui les attache aux pouvoirs publics. C'est pourquoi les bombardements allemands de 1917 sur Londres, qui ont constitué une surprise stratégique, ont suscité au sein de la population un émoi bien supérieur à ceux du *Blitz* de 1940, malgré le changement d'échelle des destructions [21]. À l'inverse, le retrait d'Irak des troupes espagnoles, à la suite du changement de majorité politique intervenu au lendemain des attentats de Madrid en 2004, a pu être en partie imputé à l'attitude du gouvernement Aznar, accusant l'organisation terroriste basque *ETA* en dépit de la revendication de l'attaque par un groupe de la mouvance *Al-Qaïda*. Élément central de la résilience, la confiance repose donc largement sur le rôle de l'information, ce qui nous conduit à la question de son traitement médiatique.

La position ambivalente des médias

Le rôle des médias dans le processus de résilience est reconnu dans le *Livre blanc* de 2008, les désignant comme « partenaires indépendants mais responsables ». Ils informent la population moyennant la sensibilisation de professionnels à l'organisation et aux moyens de gestion de crise des pouvoirs publics, sur la base du principe qu'« une vulnérabilité de la vie sociale ou économique connue de tous peut être mieux assumée » [22].

Certes, les informations visant à préparer l'opinion, à diffuser des informations d'alerte, et surtout à remettre en perspectives les enjeux, menaces et réponses liées au terrorisme confèrent aux médias un rôle important dans le processus de résilience. Et pourtant, c'est également par leur truchement que la logique du terrorisme atteint son effet majeur. Cela tient au fait qu'un acte terroriste fait toujours moins de victimes qu'il n'a de spectateurs : son retentissement, et donc son impact symbolique et psychologique, dépend étroitement de la relation qui en est faite par les médias ; cela implique que, comme l'explique le philosophe Alain DE BENOIST, « les médias font eux-mêmes partie de la terreur. En ce sens, le terrorisme est bien

(20) « Les limites de la résilience virtuelle », *Histoire et Stratégie* n° 20, *op. cit.*, p. 53.

(21) George H. QUESTER, « The Psychological Effects of Bombing on Civilian Populations: Wars of the Past », *in* Betty GLAD (dir.), *Psychological Dimension of War*, Sage, Newbury Park, 1990.

(22) *Défense et Sécurité nationale : le Livre blanc, op. cit.*, p. 190.

le fils de la société de consommation et du spectacle » [23]. Cette problématique est effectivement avivée par l'exigence actuelle de diffusion instantanée de l'information, qui favorise l'amplification de la dimension émotionnelle de l'actualité au détriment de l'analyse critique. De même, la concentration capitalistique des médias privés peut être mise en rapport avec leur manque de neutralité axiologique, selon le mot de Max WEBER [24]. Ce défaut, provoquant leur discrédit, favorise *in fine* l'éparpillement des audiences au profit de médias de niche sur *Internet*, au détriment d'une perception commune. En somme, tout cela concourt à perpétuer une sorte de culture de la peur : « Les uns produisent la terreur dans l'attente que les autres la propagent. » [25]

La résilience doit reposer avant tout sur une distance critique

Il est en fait impossible de décréter la résilience, car la liberté est une condition essentielle du rapport de confiance qui doit en constituer l'armature. C'est pourquoi les effets les plus pertinents et les plus durables d'une politique de résilience bien comprise résulteront plutôt de comportements cultivant une distance critique raisonnable vis-à-vis des médias, se dégageant de l'immédiateté audiovisuelle, et participant d'initiatives de la société civile. Deux exemples-types de résilience spontanée peuvent être relevés : dans les heures consécutives à l'attentat du 11 septembre 2001, plus d'un million de personnes ont été évacuées de Manhattan par l'Hudson et l'East River sur des ferries de la ville ou sur des bateaux de particuliers, sans qu'aucun ordre n'ait été donné par les pouvoirs publics. De même, à New York ainsi qu'à Paris après les attentats de novembre 2015, de nombreux habitants se sont spontanément présentés dans les hôpitaux pour donner leur sang ou proposer leur aide [26].

Afin de susciter ou d'encourager de semblables initiatives tout en veillant à ce que leur déroulement n'interfère pas avec la manœuvre opérationnelle des forces de sécurité et de secours, un mode d'optimisation de la résilience spontanée consiste à bénéficier, pour les encadrer, de relais déconcentrés, voire informels, des forces de sécurité. Ces relais s'appuieraient notamment sur les viviers de la réserve opérationnelle, parallèlement à la conduite de campagnes de sensibilisation plus larges et bien étudiées. À terme, en valorisant de tels comportements, même à petite échelle et dans les circonstances les plus diverses de péril et de calamité publique, le développement d'une culture commune de sécurité et de défense pourra permettre, dans une logique de subsidiarité et de cohésion active, de responsabiliser les citoyens en vue de rendre irréalisable l'objectif poursuivi par le terrorisme : la dissociation de la population et du pouvoir politique. ◆

(23) Alain DE BENOIST, « Les sociétés libérales piégées par le terrorisme », *Éléments* n° 123, hiver 2006-2007.
(24) Max WEBER, *Le Savant et le Politique*, Bibliothèques 10/18, 1963 (édition originale allemande 1919).
(25) Rüdiger SAFRANSKI, *Quelle dose de mondialisation l'homme peut-il supporter ?,* Arles, Actes Sud, 2005, p. 84.
(26) « Les formes de la lutte antiterroriste », *Histoire et Stratégie* n° 20, *op. cit.*, p. 38 et 48.

RDN n° 802 - été 2017

La Russie et le cyberespace, mythes et réalités d'une stratégie d'État

Nicolas Mazzucchi

Docteur en géographie économique, chercheur associé à l'Institut de relations internationales et stratégiques (Iris). Professeur de relations internationales au sein de l'Enseignement militaire supérieur. Conseiller scientifique de Futuribles International.

Soupçons de cyberattaques en Ukraine et dans les pays occidentaux, *trolls* œuvrant sur les réseaux sociaux du monde entier pour changer les opinions, *hackers* dérobant des *emails* du Parti Démocrate… : la présence de la Russie dans le cyberespace peut sembler *a priori* intimidante. Depuis quelques années, le Kremlin, revenant sur le mépris qu'il affichait à propos d'*Internet* du temps où il le qualifiait de « projet de la *CIA* », semble avoir découvert les potentialités du *web*. Il convient toutefois de faire la part des choses et de démêler la vérité des faux-semblants. Comment ce pays qui semblait, il y a peu, loin du niveau des États-Unis et de la Chine serait-il devenu en quelques années le principal cyberagresseur mondial, au point que certains emploient de manière systématique le terme erroné de « cyberguerre » ? Cette vision d'un éveil du cyber-ours russe, utilisant le *Net* pour mener des actions à visée géopolitique, doit être mise en balance avec la réalité des potentiels techniques et économiques nationaux autant qu'avec les visées stratégiques d'un pays dont les priorités demeurent orientées vers son « étranger proche ».

Le nouvel ogre du cyberespace ?

Dénoncer et revendiquer

Un élément frappe de prime abord lorsqu'on s'intéresse au rapport entre la Russie et le cyberespace, c'est le nombre d'attaques dans lesquelles Moscou est mis en cause depuis 2014. La Russie fait ainsi figure, entre hackers attaquant des entreprises et des partis politiques et *trolls* se livrant à la désinformation sur des forums, de nouveau cyber-ennemi universel. Cette place, qui était auparavant dévolue à la Chine, est maintenant l'apanage de la Russie, à tel point qu'une analyse plus fine s'impose. En effet, entre le début des années 2000 et 2013-2014, la Chine était vue comme l'agresseur numéro un, disposant d'une véritable cyberarmée, dont des officines proches des services de renseignement américains allaient jusqu'à donner

le nom (Unité 61398) et la localisation des bureaux. Durant cette période, Pékin aurait ainsi attaqué des entreprises, des institutions militaires et des gouvernements, dérobant nombre d'informations sensibles, dont les plans des derniers armements américains. Depuis, plus rien, comme si la Chine avait disparu dans un trou noir du cyberespace. La Russie quant à elle faisait figure d'acteur important, mais non majeur, dans ce domaine. Les *hackers* russes apparaissaient, avant 2013-2014, comme étant d'un bon niveau, mais incapables d'atteindre la masse critique nécessaire à la formation d'un bloc unifié et organisé, brique de base d'une force cyber respectable. Que s'est-il donc passé en l'espace de quelques années pour arriver à un tel renversement, suscitant des craintes parfois exagérées pendant les élections présidentielles américaines et françaises ou au moment du référendum britannique sur le *Brexit* ?

Cette peur du cyber-ours russe, réveillé et agressif, renseigne avant tout sur l'un des mécanismes fondamentaux de la cyberstratégie, celui de la dénonciation/revendication. Comme pour les questions de terrorisme, la perception de l'acteur passe le plus souvent au travers de la revendication de ses actions. Celui qui accomplit un « exploit », comme l'intrusion dans un système complexe, a tendance à le faire savoir, souvent en ridiculisant sa victime par un « défacement ». Néanmoins, dans le cas d'actions souveraines ou supposées telles, la publicité de la part de l'agresseur n'est pas l'effet recherché, bien au contraire. Ici, la connaissance de l'attaquant tient le plus souvent au fait que la victime choisit de révéler avoir été victime d'une visée maligne. Cela suppose, d'une part, que l'attaqué accepte de se mettre en position de faiblesse en révélant qu'il a été atteint, et cela lui laisse, d'autre part, une grande latitude de dénonciation de ses agresseurs. La question de l'identité dans le cyberespace fonctionne donc au travers de cette double mécanique de revendication/dénonciation et, dans le cas des États, c'est avant tout la seconde option qui est considérée.

Dans le cas du basculement de la Chine vers la Russie dans la désignation du principal agresseur du cyberespace, cela induit que les pays occidentaux, majoritairement les États-Unis en ce cas, ont fait le choix de mettre les projecteurs sur l'un plutôt que sur l'autre. Stratégiquement parlant, ce paradigme remet la question des perceptions au cœur de la cyberstratégie, confirmant son caractère profondément clausewitzien, avec le moral de l'adversaire comme principale cible, et demande une focalisation sur les faits avant de se livrer à toute analyse plus globale.

Chronique des opérations

En se fondant sur une approche plus dépassionnée du cyberespace, où il est extrêmement difficile d'échapper aux influences contradictoires, il paraît nécessaire d'établir une chronique des actions imputées à la Russie. Alors que Moscou se manifestait assez peu dans le cyberespace avant le milieu des années 2000, deux événements ont contribué à faire de la Russie un acteur crédible du cyber.

Le premier a lieu en 2007, lorsqu'une cyberattaque massive prend pour cible le gouvernement estonien, lequel vient de décider de déboulonner une statue dédiée aux « libérateurs » soviétiques de la Seconde Guerre mondiale. Cette attaque vise de nombreux organismes gouvernementaux, la bourse, les banques, etc. Elle a pour effet de paralyser le pays pendant 48 heures et fait craindre l'avènement des cyberguerres prophétisées depuis le début des années 1990. Pour impressionnante qu'elle soit, cette agression ne cause cependant aucun dommage important, seulement une gigantesque paralysie du système, la première disruption *2.0* de masse [(1)]. La principale originalité de cette attaque, dont l'origine russe ne fait aucun doute dès le début, est qu'elle a eu lieu au travers d'une coalition hétéroclite de *hackers* patriotes, revendiquant la vengeance symbolique pour le retrait de la statue, et des cybermafias comme le Russian Business Network. *Quid* du rôle de l'État russe ? Aucune preuve ne vient étayer sa participation directe ou indirecte à l'attaque, mais il est certain que la cyberattaque servait ses orientations géopolitiques et l'affirmation du nationalisme russe dans les pays occidentaux au cours du deuxième mandat de Vladimir Poutine.

Le second grand événement survient peu après avec la guerre contre la Géorgie de 2008. Les performances de l'armée russe ont, à cette occasion, été supérieures aux attendus des observateurs occidentaux, malgré la persistance de nombreux problèmes. En matière cyber, les unités russes engagées contre la Géorgie utilisent l'ensemble de l'éventail des actions de guerre électronique et de cyberagression pour paralyser les systèmes de communication et de commandement de l'armée géorgienne, sans parler des efforts entrepris dans le domaine informationnel, qui rappellent fortement l'attaque contre l'Estonie [(2)]. L'armée russe prouve à cette occasion qu'elle possède des capacités d'un niveau respectable, surtout en ce qui concerne la coordination des actions à plusieurs niveaux – un savoir-faire critique dans les conflits actuels.

Dans les deux cas, estonien et géorgien, que l'on peut également étendre à l'Ukraine en 2014, il convient de considérer la relative faiblesse de l'adversaire en termes techniques. La cybersécurité des infrastructures publiques ou des éléments militaires dans ces deux pays semble faible, loin des standards européens, américains ou chinois. Sans vouloir minimiser les compétences de la Russie ou des acteurs de nationalité russe, le niveau des adversaires ou des opposants est à prendre en compte dans l'analyse qui peut être faite *a posteriori* des cyberattaques. Toutefois, ces actions démontrent également que la Russie n'est jamais là où on l'attend. Dans le cas estonien, même s'il ne s'agit que d'un faisceau de présomptions, la coordination des actions des *hackers* et des *trolls* pour l'accomplissement de la punition symbolique d'un gouvernement ayant, selon Moscou, bafoué l'histoire, est particulièrement

(1) Sergei A. Medvedev, *Offense-Defense Theory Analysis of Russian Cyber Capability*, Naval Postgraduate School, Monterrey, 2015-03 (https://calhoun.nps.edu/bitstream/handle/10945/45225/15Mar_Medvedev_Sergei.pdf).
(2) Eneken Tikk, Kadri Kaska et Liis Vihul, *International Cyber Incidents, Legal Considerations*, Tallinn, CCD-COE, 2010 (https://ccdcoe.org/publications/books/legalconsiderations.pdf).

fine dans l'utilisation de la dissimulation. Dans le cas géorgien, la Russie a surpris par le niveau de ses opérations combinées, utilisant le cyberespace en complément des moyens conventionnels. La dissimulation – la *maskirovka* – permanente des capacités de la Russie soulève de nombreuses interrogations sur ses buts et ses capacités réelles, ce qui ne fait qu'entretenir l'idée du cyber-ours attendant le moment idoine pour sortir de sa torpeur.

Une stratégie de la faiblesse ?

La couche informationnelle, une focalisation obligatoire ?

L'ensemble de la cyberstratégie de la Russie tourne autour de la guerre de l'information. Il s'agit ainsi, suivant, en partie, la doctrine GERASIMOV [3] – du nom du Chef d'état-major de l'armée russe – d'utiliser les armes traditionnelles de la subversion et de la désinformation afin d'obnubiler l'ennemi. Cette application dans le domaine militaire trouve également un écho dans le domaine politique puisque la stratégie de la Fédération de Russie dans son ensemble définit le cyberespace comme un « espace informationnel » qu'il appartient de contrôler, à défaut de le dominer [4]. On pourrait ainsi croire à un retour de l'*habitus* stratégique russe hérité tant de l'époque tsariste avec l'*Okhrana* [5] que de la guerre civile ou de l'ère soviétique. Après tout la propagande en ligne utilisant des *trolls* est assez proche dans sa conception de celle, plus traditionnelle, que Serge TCHAKOTINE, l'auteur du *Viol des foules par la propagande* (1939), mettait en scène au profit des armées blanches au sein de l'*Osvag* [6]. S'il est impossible de nier cet héritage, il appartient néanmoins de se demander jusqu'à quel point cette sur-focalisation stratégique ne cache pas en fait une faiblesse intrinsèque au sein des deux couches techniques, matérielle et logicielle.

La Russie se rapproche des positions chinoises quant à la nécessité de passer d'une gouvernance américano-nippo-européenne du cyberespace à un mode plus global. Elle s'avère cependant moins avancée que la Chine sur le plan technique. Alors que Pékin a œuvré depuis les années 1990 au développement d'un écosystème cyber complet, s'étendant sur toutes les couches, à commencer par la couche matérielle, la Russie est demeurée dépendante des solutions développées par d'autres sur les couches techniques, même si elle a connu un certain succès dans les antivirus à la fin des années 1990. Même l'existence d'une communauté de sites en langue russe – le *RuNet* – ne saurait masquer la limite qui existe sur la

(3) Charles K. BARTLES, « Getting Gerasimov Right », *Military Review*, janvier-février 2016, p. 30-38.
(4) Andrei SOLDATOV, « Under Siege from Putin's Private Hackers », *The World Today*, février-mars 2017 (www.chathamhouse.org/publications/twt/putin-s-private-hackers).
(5) L'*Okhrana* était la police secrète mise en place par Alexandre III, utilisant grandement la désinformation et la provocation, et à l'origine, notamment, de l'écriture des Protocoles des sages de Sion.
(6) Organisme de propagande des Blancs (Armée des Volontaires) pendant la guerre civile (voir Jean-Jacques MARIE, *La guerre des russes blancs 1917-1920*, Tallandier, 2017, 528 pages).

technique. En Russie, nul constructeur d'ordinateurs ou de routeurs comparable à Lenovo ou à Huawei, nul site qui ait la popularité d'Alibaba ou de Baidu. Malgré l'importance de la population de l'espace *post*-soviétique, Yandex, le méta-site à la fois moteur de recherche, fournisseur *email* et portail de contenu, n'est que le 30e site mondial [7]. La Russie s'est enfermée dans une certaine balkanisation, c'est-à-dire la volonté de créer au sein du cyberespace des îlots, techniques ou informationnels, partiellement cloisonnés. Mais cette balkanisation est plus culturelle qu'informatique, elle n'est une réalité que dans les perceptions. La Russie ne dispose ainsi pas des moyens, à l'heure actuelle, de séparer techniquement son espace de communications cyber comme la Chine le fait avec la Grande Muraille dorée. Que ce soit par choix ou par nécessité, le cyberespace russe n'est une réalité que dans les pratiques culturelles et linguistiques.

La formation des cyber-combattants, une problématique ouverte

Cette analyse sur la focalisation russe sur la couche informationnelle du cyberespace induit celle sur les capacités humaines en matière de cybercombattants. Dire que la première vulnérabilité du cyberespace réside dans l'être humain revient à énoncer une vérité particulièrement connue, mais celle-ci ne doit pas occulter que l'Homme est également la première ressource du cyberespace. C'est en effet sur la créativité, la capacité intellectuelle, le savoir-faire technique et l'adaptabilité des individus que reposent les cyber-capacités. Aucune cyber-arme absolue n'existe en effet, et, au-delà même, les armes du cyberespace sont en quelque sorte des fusils à un coup. Elles sont étudiées pour agir de manière précise sur une faille qu'on aura, au choix, découverte ou provoquée en amont, dans le cas des États qui sont capables d'instrumentaliser des entreprises pour que ces dernières cachent des backdoors, c'est-à-dire des portes dérobées sciemment installées dans des systèmes ou des matériels, permettant d'y avoir accès ultérieurement, notamment pour dérober des données. Il s'agit là du cinquième niveau de menace sur les six que compte l'échelle conceptuelle élaborée par le *Department of Defense* américain, la sixième correspondant à l'utilisation offensive du cyber dans un conflit ouvert. Plus que la donnée, l'or noir du cyber, ce sont les ingénieurs et les techniciens.

Pour comprendre le niveau de menace que peut représenter un État ou une force armée décidant d'investir le cyberespace, il convient donc de regarder son système d'enseignement supérieur et les individus qu'il produit. Les études sur l'enseignement supérieur en Russie, à commencer par celle de Tatiana KASTOUEVA-JEAN, ne mettent pas en lumière une bonne santé du système russe, loin s'en faut [8]. La fuite des cerveaux depuis la fin de l'époque soviétique et la situation actuelle du pays, marquée par une faiblesse de la formation, ont transformé

(7) Google a même dépassé Yandex en termes de popularité en Russie à la mi-2016.
(8) Tatiana KASTOUEVA-JEAN, « Entreprises et universités russes : de la coopération au recrutement », *Russie.Nei.Reports* n° 13, Ifri, octobre 2012 (www.ifri.org/).

l'éducation supérieure russe en un système moribond où seules quelques institutions surnagent.

Si la formation académique en Russie s'avère de bonne qualité en ce qui concerne les éléments théoriques, en mathématiques notamment, elle est bien plus défaillante dans les domaines appliqués. La pénurie chronique d'ingénieurs, en particulier, se fait de plus en plus sentir dans de nombreux secteurs, ce qui explique en partie la lenteur de la réindustrialisation du pays, à l'exception de quelques entités bien spécifiques comme Rosatom [(9)] ou Rostec [(10)]. Il n'est d'ailleurs pas étonnant de voir que ces dernières ont la haute main sur certaines institutions et universités comme l'Institut de physique de Moscou (*MEPhI*) dans le cas de Rosatom, ce qui lui garantit de disposer d'étudiants d'un niveau suffisant. Ce problème récurrent de formation provoque un éclatement de l'enseignement des savoir-faire nécessaires au développement d'un écosystème cyber cohérent et, par-là, explique non seulement la faiblesse de la Russie dans les domaines matériel et logiciel – les meilleurs préférant de toute façon s'expatrier – mais aussi la nécessité de recourir à des *trolls* mercenaires.

Le *RuNet* et le cyberespace

La galaxie des sites en langue russe, connue sous le nom de *RuNet*, présente les attributs d'un écosystème russophone, sans toutefois avoir la cohérence d'ensemble de son homologue chinois. Le *RuNet* est en réalité structuré autour de trois sites majeurs que sont Yandex, Vkontakte et Mail.ru. En offrant le triptyque moteur de recherche/réseau social/suite *mail*, le *RuNet* donne aux utilisateurs russophones les moyens de la communication *2.0* à un espace culturel singulier. Il constitue un ensemble avec lequel il faut compter dans le cyberespace même s'il ne dispose pas des mastodontes de l'*e*-commerce comme Amazon ou Alibaba et si des sites comme Yandex ou Vkontakte ont une audience limitée hors de la sphère russe.

La structuration de ces sites, leur interface linguistique et leur ouverture dans l'espace *post*-soviétique constituent également pour la Russie une manière de promouvoir sa culture. Vkontakte, notamment, dispose d'une grande popularité dans l'ensemble des territoires de l'ex-URSS, de même que l'autre grand réseau social en Russie, Odnoklassniki (équivalent de Copains d'avant) – les deux étant majoritaires en termes d'utilisateurs en Russie, Biélorussie, au Kazakhstan, au Kirghizstan, etc. En Asie centrale en particulier, la promotion de la culture russe – la population d'origine russe représente une partie souvent importante, même si elle demeure minoritaire, de celle de ces pays – passe au travers de ces sites, permettant une diffusion des orientations du gouvernement de Moscou.

(9) Corporation d'État pour le nucléaire, en charge des volets civil et militaire.
(10) Corporation d'État pour la production et la vente d'armements, principalement terrestres.

Constatant l'importance de ces sites, le Kremlin tente d'établir un contrôle strict sur eux. En 2014, le site Vkontakte, créé par Pavel Dourov, passait sous la tutelle de l'État. Après avoir organisé le rachat des parts de l'entreprise par Mail.ru, le gouvernement choisissait finalement de mettre la pression sur le créateur du site, lequel refusait la coopération sur la censure des opposants depuis plusieurs années, ce qui aboutit finalement au départ de ce dernier de Russie. Avec l'exil de Pavel Dourov, la Russie perdait l'un de ses plus brillants talents du *web 2.0*, laissant apparaître le paradoxe fondamental du cyberespace russe qui voit l'État chercher à l'instrumentaliser du fait des leviers qu'il offre, mais étouffer de par cette même volonté de contrôler les talents créatifs. Si le dirigisme étatique inhérent à l'*habitus* russe porte ses fruits dans un certain nombre de secteurs souverains, il peut se révéler contre-productif dans le cyberespace. Le changement de président de Vkontakte, remplacé par Boris Dobrodeyev, fils d'Oleg Dobrodeyev, un magnat des médias proche du Kremlin, représente cette mainmise de l'État sur le secteur. En choisissant un dirigeant obéissant fidèlement aux ordres, Moscou envoie un signal qui peut apparaître négatif aux nombreux créateurs de *start-ups*. La fuite de Pavel Dourov risque ainsi d'accentuer l'hémorragie de cerveaux qui existe depuis le début des années 1990 [(11)].

⁂

Considéré par le Kremlin comme une création de la *CIA* servant à propager les informations du gouvernement américain, *Internet* est devenu depuis quelques années un terrain d'action privilégié de la Russie. Toutefois, si l'on s'abstrait du jeu géopolitique des dénonciations-revendications, force est de reconnaître que les actions de la Russie s'orientent avant tout sur la couche informationnelle. L'action des *trolls* et des *hackers*, dont les liens avec le pouvoir sont supposés mais demandent encore à être confirmés, est ainsi gênante, mais non bloquante. À l'exception des actions menées en Géorgie et en Ukraine, la main visible de la Russie dans le cyberespace s'avère moins puissante qu'on pourrait le croire. Avec un retard important dans les domaines techniques et une tutelle étatique parfois étouffante sur les entreprises du *web*, le secteur de l'*IT* (*Information Technology*) russe paraît moins développé que celui d'autres puissances – les États-Unis et la Chine notamment. La question centrale qui détermine le futur, en Russie, tant de la géopolitique du cyberespace que de l'économie numérique, est la place de l'État dans le secteur. Trop présent, celui-ci contraint et stérilise la créativité, encourageant la fuite des cerveaux. Trop absent, il court le risque de se voir dépassé dans un contexte stratégique mouvant où le cyberespace est autant un territoire de développement que d'affrontement. Pour passer de la stratégie de la faiblesse à celle de la force, l'État devra se faire plus discret en Russie. ◆

(11) Sur l'exemple de la perte des compétences techniques voir l'exemple du nucléaire avec Roald Z. Sagdeev, *The Making of a Soviet Scientist: My Adventures in Nuclear Fusion and Space from Stalin to Star Wars*, New York, John Wiley & Sons, 1994.

TRIBUNE N° 909, 30 JUIN 2017

De *Petya* à *NotPetya* : du cybercrime à la cyberguerre ?

Christine DUGOIN-CLÉMENT

Chercheur au *think tank* CAPE Europe (www.capeurope.eu/fr/).

Alors que l'attaque qualifiée de plus massive jamais connue déferle sur les ordinateurs du monde entier depuis quelques jours, la réalité de la nature du « *worm* » (ver informatique) se fait jour. D'abord appelé *Petya*, pour être ensuite différencié de ce *ransomware* (logiciel de rançon) et rebaptisé *NotPetya*, il semble maintenant qu'il ne s'agit même pas d'un *ransomware*.

Un encodage indéchiffrable ?

En effet, il n'y aurait aucun moyen de récupérer les données encryptées par ce logiciel. Cette impossibilité n'aurait pas de rapport avec la fermeture de l'adresse *mail* utilisée par les concepteurs de *NotPetya* pour s'assurer du paiement par les victimes, mais serait un effet de la nature même de *NotPetya*. Dans son rapport paru le 27 juin, l'expert en sécurité connu sous le pseudonyme de « the grugq » affirme que *NotPetya* est conçu pour se propager rapidement et causer des dégâts, pas pour collecter des fonds. Ainsi, il utilise une couverture plausible de *ransomware* sans en être un.

Il semblerait que le logiciel jette la clef permettant le décryptage des données qu'il verrouille, comme le rappelle la société de cybersécurité Comae Technologies : un *ransomware* comme *Petya* modifie le disque de manière à ce que le changement puisse être réversible, ce que ne permet pas *NotPetya*.

Il utiliserait des infections aléatoires et propres à chaque victime. Or, en l'absence de récurrence, il n'y aurait pas une clef possible pour décoder toutes données encodées par le virus, mais une clef par groupe de données infectées. C'est, selon les experts de chez Kasperky, ce qui rend le décodage impossible.

Si d'autres experts passent par d'autres analyses que la firme russe, ils en arrivent à la même conclusion. Pour Comae Technologies, nous serions face à une séquence d'opérations erronées qui rendrait impossible la récupération de l'arborescence mise en place par *NotPetya*. En clair, cette séquence gérerait l'emplacement des données sur un disque dur, mais ce fichier restant chiffré, il n'y aurait aucun moyen de retrouver le chemin vers l'emplacement de chaque fichier sur l'ordinateur infecté.

Comment qualifier *Petya* désormais ?

La question peut paraître rhétorique mais elle ne l'est pas, car elle porte en son sein la façon d'analyser l'attaque. Une chose est certaine : ce glissement du crime à but lucratif vers une attaque de destruction a un impact sur les *hackers* eux-mêmes. Ainsi « Janus », le créateur de *Petya* a trouvé utile de communiquer *via* son compte Twitter pour se dissocier de ce logiciel affirmant ne pas en assumer la paternité. Cette déclaration suit de près celle de l'auteur d'un autre *ransomware* bien connu, *AES-NI*, qui avait annoncé ne pas être à l'origine de *XData*, autre logiciel malveillant qui avait été utilisé pour attaquer l'Ukraine qui se trouve être l'une des premières victimes de *NotPetya*. Rappelons que c'est avec un *tweet* de Pavlo Rozenko, vice-Premier ministre ukrainien, que *NotPetya* a fait son entrée dans le monde médiatique *via* la photo d'un écran infecté. Cette déclaration intervient alors que *XData* et *NotPetya* semblent avoir utilisé le même vecteur de distribution en Ukraine à savoir le serveur de mise à jour d'un fabricant de logiciel comptable.

Il semble que le concepteur de *NotPetya* connaît assez bien les familles de *ransomware* pour les utiliser comme couverture afin d'attaquer les utilisateurs, notamment ukrainiens. On comprend alors mieux pourquoi les *hackers* connus ou suspectés d'avoir participé à la conception de ce type de logiciels tiennent à se dissocier de *NotPetya* qu'ils ont bien cerné comme visant le chaos et non le gain financier.

Camoufler un logiciel visant le chaos en *ransomware* agressif : une « innovation » ?

Si on parle aujourd'hui beaucoup de *NotPetya* et de sa nature, ce logiciel n'est pas pour autant le premier du genre. Bien au contraire, utiliser une couverture de *ransomware* pour en réalité détruire définitivement des données a déjà été fait. Cette méthode de camouflage permet de passer au travers les investigations d'incidents spécifiques. *Shamoon* et *Killdisk* * avaient déjà été pensés et conçus de cette manière l'an passé. Par contre, passer de la famille des *ransomware* à celle des *diskwiper* (ou effaceur de disque) permet de glisser du cybercrime vers l'arme cyber. Cette différenciation a pour effet de changer la perspective de l'analyse.

* ***Shamoon* et *Killdisk***

Le premier est un *malware* (logiciel malveillant) apparut en 2012 qui frappa plusieurs entreprises saoudiennes (dont Saudi Aramco), les estimations parlent de 35 000 ordinateurs infectés. Il fait un retour en 2016 toujours en Arabie saoudite, avec une variante : une fois la machine infectée il n'affiche plus de l'image d'un drapeau américain en flammes mais de la photo d'Alyan Kurdi, l'enfant syrien retrouvé mort sur une plage dont la photo avait fait le tour du monde. Pour infecter les machines, *Shamoon* utilisé le logiciel commercial, *RawDisk*, qui permet l'accès direct aux disques durs permettant d'intervenir sur les données et au cas particulier, de les écraser.

Le second est un logiciel permettant de détruire complètement toutes les données se trouvant sur les disques durs interdisant toute récupération des dossiers et documents infectés.

Ainsi, le fait que l'attaque ait pris racine en Ukraine est un signal fort. Le pays est toujours en guerre, affrontant dans l'Est de son territoire les séparatistes de Donetsk et Luhansk et accusant la Russie d'un soutien actif au conflit. En outre, l'Ukraine a été le théâtre d'un déploiement massif d'une cyberguerre touchant toutes les strates d'individus en utilisant le vecteur informationnel depuis maintenant plusieurs années : ce qui fait de ce pays le plus grand laboratoire de *cyber warefare* connu jusqu'à aujourd'hui. Ainsi, alors qu'au premier moment du déploiement de *NotPetya*, les yeux se tournaient vers le collectif de *hackers* Lazarus, déjà soupçonné pour le *ransomware Wannacry* qui s'était répandu en mai 2017, certains Ukrainiens soupçonnent ouvertement leur grand voisin russe d'être à l'origine, ou tout au moins d'être l'un des moteurs, de *NotPetya*. Que certaines entreprises russes soient également touchées par *NotPetya* ne semblant pas être une raison suffisante pour disculper la Russie aux yeux ukrainiens. Notons ici que l'attribution d'une attaque à un auteur précis est toujours tâche risquée, voire impossible avec certitude et cela est encore plus vrai quand on parle d'un État. Ainsi, pour le célèbre *Wannacry* par exemple, mais comme pour nombre d'autres logiciels malveillants avant lui, l'attribution de l'attaque restant floue, il n'y a que peu de moyen d'agir en terme punitif, ce qui peut conférer une certaine impunité à beaucoup de *hackers*.

⁂

Le consensus semble donc se faire jour et *NotPetya* appartiendrait à une tout autre famille de logiciels où l'on retrouve le célèbre *Stuxnet* * ou encore *BlackEnergy* **. Nous ne serions donc plus dans le cybercrime mais dans l'arme cyber, glissant doucement du civil au militaire au moins dans la terminologie. Reste à prouver que *NotPetya* a bien eu une utilisation géopolitique comme ce fut le cas de ces deux logiciels.

**** Stuxnet***

C'est un ver informatique découvert en 2010 dont la création est attribué à la *National Security Agency* (*NSA*), qui s'attaquait aux centrales nucléaires iraniennes, plus précisément aux centrifugeuses d'enrichissement d'uranium. Il est qualifié de cyber-arme conçu pour des attaques spécifiques, ici les systèmes SCADA (Système d'acquisition et de contrôle de données). Ce ver a infecté 45 000 systèmes dont 30 000 en Iran, notamment dans la centrale de Bouchehr. Le virus était inoculé par clef *USB* et comportait 4 attaques dont 3 « *0 day* » (une vulnérabilité informatique n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu).

***** BlackEnergy***

C'est un *malware* de la famille des « chevaux de Troie » (*trojan horse*) conçu pour attaquer les centrales électriques. Il provoqua une coupure d'électricité touchant 70 000 foyers ukrainiens le 23 décembre 2015. Il interdit d'abord tout redémarrage du système d'exploitation des ordinateurs infectés mais peut aussi effacer des données et détruire le disque dur, permettant ainsi aux *hackers* de prendre le contrôle du système.

Éléments de bibliographie

SUICH Matt, « Petya.2017 is a Wiper not a Ransomware », Comae Technologie, 28 juin 2017 (https://blog.comae.io/petya-2017-is-a-wiper-not-a-ransomware-9ea1d8961d3b).

IVANOV Anton et MAMEDOV Orkhan, « ExPetr/Petya/NotPetya is a Wiper, Not Ransomware », Kaspersky security list, 28 juin 2017 (https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/).

THE GRUGQ, « Pnyetya: Yet Another Ransomware Outbreak », *Medium.com*, 27 juin 2017 (https://medium.com/@thegrugq/pnyetya-yet-another-ransomware-outbreak-59afd1ee89d4).

JANUS, *Tweet* du 28 juin 2017 (https://twitter.com/janussecretary?lang=fr).

RDN n° 805 - décembre 2017

À propos d'intelligence artificielle (1/2)

Emmanuel Desclèves

Vice-amiral, de l'Académie de Marine.

La grande erreur de notre temps, cela a été de pencher, je dis même de courber l'esprit des hommes vers la recherche du bien matériel. Il faut relever l'esprit de l'homme, le tourner vers la conscience, le beau, le juste et le vrai, le désintéressé et le grand. C'est là et seulement là, que vous trouverez la paix de l'homme avec lui-même et par conséquent avec la société (1).

L'humanité s'installe dans la monoculture ; elle s'apprête à produire la civilisation de masse, comme la betterave. Son ordinaire ne comportera plus que ce plat (2).

Au regard du volume croissant d'articles, ouvrages et vidéos nouveaux mettant en exergue la révolution impulsée par l'intelligence artificielle (IA), nous pourrions croire qu'il s'agit d'un domaine de recherche tout à fait récent. Il n'en est rien : le concept d'IA date des années 1950 et une bonne partie des algorithmes (3) que nous semblons (re)découvrir à l'œuvre aujourd'hui ont en réalité été produits dans les années 1980. Ce qui constitue vraiment la révolution que nous connaissons depuis peu est le couplage désormais possible de ces algorithmes avec des données et une capacité de calcul qui n'étaient pas accessibles alors, ouvrant des perspectives dont on ne perçoit pas encore les limites.

Avec des puissances de calcul de plus en plus importantes et disponibles à des coûts toujours plus bas, des technologies de traitement des données massives de plus en plus matures, une augmentation des capacités de stockage et un développement continu de nouvelles méthodes algorithmiques comme l'apprentissage profond (*deep learning*), l'IA connaît depuis cinq ans une accélération inédite (4).

Ce constat factuel et technique focalise l'attention sur la conjugaison inédite d'outils de traitement de données de plus en plus performants avec des bases de

(1) Victor Hugo, Discours à l'Assemblée nationale, séance du 11 novembre 1848.
(2) Claude Lévi-Strauss, *Tristes tropiques* ; Plon, 1955.
(3) Défini dans un arrêté du 12 juillet 2011 comme une méthode opérationnelle permettant de résoudre, en un nombre fini d'étapes clairement spécifiées, toutes les instances d'un problème donné.
(4) France Intelligence Artificielle, *Rapport de synthèse* ; 2017.

données de plus en plus gigantesques (*Big Data*). Mais ce qui est en jeu n'est pas tant l'aspect technique des choses que ses conséquences prévisibles comme imprévisibles, qui constituent à bien des égards un véritable défi pour l'humanité.

Comme le dit le mathématicien et député Cédric VILLANI qui vient d'être mandaté pour faire des propositions au gouvernement sur le sujet : « Un enjeu très important est comment faire en sorte que l'intelligence artificielle (IA) profite à tout le monde, soit associée à un renforcement de la démocratie et pas le contraire. Un certain nombre d'exemples montrent que dans certains cas l'utilisation de l'IA peut avoir des effets ravageurs sur les questions économiques et le tissu démocratique. » (5).

Les géants de l'*Internet*

Si nous considérons simplement les fameux géants américains de l'*Internet* Gafam (Google, Apple, Facebook, Amazon, Microsoft), sans parler des Chinois ou des Russes, nous observons que leur maîtrise intelligente d'immenses bases de données à l'échelle de la planète, leur permet de contrôler *de facto* et en situation de quasi-monopole un champ de plus en plus vaste d'activités humaines. De sorte que l'influence, et donc le pouvoir réel de ces sociétés industrielles et commerciales, déborde de beaucoup le domaine strictement économique qui est normalement leur seule raison sociale. Par ailleurs, leur puissance financière considérable leur donne des moyens d'action qui dépassent ceux de la plupart des acteurs publics nationaux ou internationaux, y compris ceux de très nombreux États. Enfin, ils utilisent l'*Internet* comme un instrument supranational alors que la législation qui leur est opposable est le plus souvent celle de l'État où est installé le siège de ces grandes sociétés multinationales.

Se pose dès lors la question de la légitimité du pouvoir qu'elles exercent *de facto* sur une partie de la population mondiale, en tirant profit des données fournies gratuitement par cette population et plus ou moins à son insu, *via* l'*Internet*. Par ailleurs, les méthodes et outils de gouvernance de ces entreprises, adaptés à leur finalité commerciale fixée par leurs conseils d'administration et leurs actionnaires, sont-ils pertinents pour gérer ce qui s'apparente désormais dans bien des cas à un service public ? L'*Internet* est en effet largement utilisé par les services de l'État qui imposent de plus en plus son usage aux citoyens, sans pour autant avoir fixé de règles de concession pour ce nouveau type de service public.

À travers ces questions fondamentales de légitimité et de gouvernance, on observe que les principes mêmes qui fondent aujourd'hui le droit positif sont inadaptés à ce type de situation qui repose sur l'utilisation massive d'*Internet* et de réseaux supranationaux. Principaux piliers du droit international, les deux grands

(5) *Le Monde* du 9 septembre 2017.

principes de la propriété privée exclusive d'une part et de l'État-nation d'autre part (6), sont inopérants s'agissant des espaces communs mondiaux.

Il semble, en réalité, que les instruments de droit dont nous disposons à l'heure actuelle soient insuffisants voire impuissants pour répondre aux questions liées à la gestion de ces *Global Commons*, espaces fluides sans frontières qui s'apparentent au *Res nullius* de la Haute Mer. Rappelons que cette qualification ouvre à quiconque la possibilité d'accaparer à son profit et sans aucune contrainte les ressources de ces espaces ouverts à tous (7).

C'est bien ce qui se passe aujourd'hui en ce qui concerne les métadonnées accumulées *via* l'*Internet* : dans le silence du droit, de multiples prédateurs sont là pour prendre possession des immenses richesses que recèlent ces *data*, pour autant que l'on dispose des outils techniques nécessaires. C'est le cas des grandes firmes citées ci-dessus, mais aussi d'organismes étatiques qui – au nom de la sécurité et de la défense nationale – ne se privent pas d'espionner tout ce qui transite dans ces réseaux. Sous couvert de lutte contre le terrorisme et au nom du *Patriot Act* qui leur donne des droits extraterritoriaux, les États-Unis par exemple disposent de stations d'écoute dans le monde entier (réseau *Échelon* de la *NSA*).

Il semble que personne ne se soit encore avisé d'organiser l'exploitation partagée de ces données immatérielles au niveau international. *Internet* est en effet un cyberespace polymorphe décentralisé, virtuel et non hiérarchique, qui ignore les frontières et ne se contrôle donc pas facilement. Cela étant, l'analogie est pertinente avec les ressources biologiques et génétiques de la Haute Mer, qui sont aujourd'hui encore *Res nullius* à la merci du premier prédateur.

L'ONU a récemment pris conscience de la nécessité de leur attribuer de préférence un statut de *Res Communes*, de façon à pouvoir en partager les fruits avec l'ensemble de la communauté mondiale. Des discussions sont donc engagées pour traiter de ces ressources vivantes susceptibles de répondre demain aux nombreux défis d'une humanité en pleine expansion (protéines, médicaments, génétique, énergie). On pourrait imaginer un processus du même ordre pour les données immatérielles des *Big Data*.

Robots et drones

Le développement spectaculaire des drones, véhicules autonomes et autres robots intelligents est rendu possible par les progrès exponentiels de l'IA. Ils répondent à de multiples besoins et leurs applications apparaissent sans limites, tant le champ des possibilités est divers. Ils s'avèrent en effet capables de remplacer l'homme

(6) La notion de propriété privée exclusive a été introduite dans le droit occidental par John Locke (*Of Property*, 1690). Le concept d'État-nation souverain s'est imposé à l'occasion des Traités de Westphalie (1648), avec la délimitation précise des frontières entre les États européens.

(7) Cf. Emmanuel Desclèves, « L'empreinte de l'océan », *RDN* n° 789, avril 2016, p. 17-23.

dans bien des domaines avec un coût inférieur et une meilleure fiabilité. Comme lors de toutes les avancées technologiques majeures, il y a des côtés positifs avec des avancées très favorables à de nombreux points de vue, mais c'est en général au prix de bouleversements considérables pour les sociétés humaines qu'elles affectent très directement, sans parler de l'usage dévoyé que l'on peut faire de chaque invention nouvelle.

On peut toujours présenter des verres à moitié vides et d'autres à moitié pleins, ou encore de subtiles balances avantages/inconvénients avec des évaluations de type *best value for money*. En tout état de cause, nous pressentons bien que personne n'arrêtera la marche des inventions et du progrès technologique. Les robots et les drones sont là, ils vont certainement se multiplier et s'immiscer dans tous les domaines de la vie courante ou professionnelle, et dans dix ou vingt ans personne ne s'étonnera plus de monter dans une voiture sans chauffeur ou se faire livrer ses courses par un drone.

Du point de vue stratégique, la robotisation des systèmes d'armes est également une réalité qui va bouleverser l'ensemble des doctrines militaires et l'art de la guerre en général. L'avance technologique se traduira immédiatement par une avance opérationnelle sur le terrain procurant un avantage tactique puis stratégique sur l'ennemi.

La lettre et l'esprit

Bien entendu, chaque inventeur ou créateur met en avant les côtés indéniablement positifs de ses travaux, laissant aux futurs utilisateurs la complète responsabilité de l'exploitation de son invention à des fins utiles ou néfastes. Même au niveau de la recherche et du développement, les équipes concernées ont beau jeu de présenter leurs inventions comme inéluctables, compte tenu de la concurrence mondiale et des différences entre les législations nationales et internationales. Ce qui aurait été limité voire interdit dans un pays trouvera en effet le moyen de se développer dans un autre cadre étatique voire en dehors de tout cadre légal, y compris dans ces espaces communs non administrés que sont les *Global Commons*. La logique est simple : ce n'est pas illégal tant qu'il n'y a pas de règle de droit applicable.

La question n'est donc pas tellement technique, ni même économique. Elle se situe sur les hauteurs de la politique au sens premier du terme, de l'éthique, voire de la morale.

En dehors de toute éthique autoproclamée ou acceptée *de facto* par les acteurs concernés, on en revient simplement à la loi du plus fort. Malgré tout, les grandes firmes et les organisations transnationales sont sensibles à la pression de l'opinion publique, de sorte qu'elles ne peuvent pas faire n'importe quoi, même en zone de non droit ou hors juridiction des États. Il reste heureusement une sorte de conscience collective qui interdit ou tout au moins condamne certaines pratiques,

en dehors même de toute référence juridique. Ces grandes organisations l'ont bien compris et elles ont mis en place des dispositifs plus ou moins élaborés pour afficher une certaine transparence et s'imposer de « bonnes » pratiques.

Pour agir plus facilement hors du cadre économique de leurs activités professionnelles, elles ont souvent créé des fondations et ONG qui leur permettent d'intervenir en toute légitimité dans d'autres contextes, notamment au niveau de l'opinion publique et des médias. C'est ainsi que peuvent être conduites des opérations qui répondent *in fine* à un objectif exclusivement économique, sous couvert de la défense de « droits » ou « valeurs » immatériels habilement mis en avant auprès de l'opinion publique, grâce à l'action orchestrée d'organisations sans but lucratif et sans lien direct avec les acteurs économiques concernés. De nombreux exemples illustrent ces pratiques, y compris dans les espaces non administrés comme la Haute Mer, l'*Internet*, etc.

Fraus omnia corrumpit

Bien conscients des limites du droit positif élaboré par le législateur mais plus encore de la fragilité de la nature humaine, les Romains avaient décrété plusieurs grands principes généraux pour coiffer en quelque sorte l'ensemble de la législation du droit positif, principes intangibles auxquels il convenait de se référer en dernier ressort. En décrétant ainsi que « la fraude corrompt tout », les Romains voulaient que le juge ait à sa disposition cet outil de droit pour dénoncer « en son intime conviction » les manœuvres frauduleuses conduites en ayant uniquement recours à des moyens légaux. En d'autres termes, pour dénoncer celui qui utilise la législation à des fins détournées, rendant son action inattaquable sur le plan du droit positif.

Ce principe a été repris dans le droit français mais il est assez peu usité. On y a souvent recours en matière financière pour dénoncer et sanctionner ceux qui fraudent intentionnellement le fisc en utilisant tous les artifices du droit. Il pourrait utilement être remis en exergue dans de nombreux autres cas où l'intention frauduleuse détermine en réalité l'action des auteurs, au détriment *in fine* de la communauté.

L'algorithme et le système

L'algorithme est censé mettre de l'ordre dans un processus. Il fixe des règles, il normalise, il rationalise, il dit oui ou non. Derrière ces mots qui fleurent bon la rigueur supposée implacable de la logique mathématique, se cache *a contrario* une certaine stigmatisation du chaos, de la désorganisation et de l'irrationnel qui seraient l'apanage de l'homme. La machine heureusement ne connaît pas l'écueil fatal de l'erreur humaine.

C'est ainsi qu'une procédure informatisée bien maîtrisée va pouvoir remplacer des employés parfois peu fiables et distraits, voire insouciants ou même rêveurs. On se méfie désormais de ces individus plus ou moins compétents et imprévisibles, dont les « défauts » sont mis en lumière par comparaison avec la rigueur de la machine. L'homme est imparfait, chacun en est bien conscient, alors autant le remplacer partout où c'est techniquement possible par un système fiable piloté par une intelligence artificielle que l'on peut contrôler rationnellement, améliorer et corriger autant que nécessaire. Mais que faire de ces individus peu fiables ? Ne faut-il pas les aider à progresser en les adossant justement à un système rationnel qui stimulera et augmentera même leurs capacités physiques et mentales limitées, tout en leur imposant une rigueur bien nécessaire ? On dispose aujourd'hui des moyens techniques de « parfaire » les hommes, pour les emmener vers leur destin supposé d'immortels.

Certains croient rêver mais malheureusement il n'en est rien, car cette vision qui peut sembler caricaturale est celle qui sous-tend plus ou moins consciemment une partie des recherches scientifiques actuelles, portées par une foi irréductible dans le progrès technique renforcée notamment par les avancées spectaculaires de l'IA couplée au *Big Data*. Éliminer l'erreur humaine est le rêve utopique de bien des idéologues du progrès technologique. Mais comment un monde sans erreur serait-il perfectible ? Paradoxalement n'est-ce pas justement la richesse de la condition humaine que d'apprendre de ses propres erreurs en exerçant son libre-arbitre, afin de pouvoir progresser ?

L'homme augmenté

Pour pallier ces insupportables imperfections, les démiurges californiens ou autres prennent le parti d'implanter dans notre chair des puces électroniques qui nous doteront de capacités physiques et intellectuelles augmentées. Imaginons une puce mémoire intégrée au sein même de notre cerveau et connectée à nos réseaux neuronaux mais communiquant également avec l'extérieur.

De façon paradoxale, ceux qui prônent ces évolutions expliquent aussi qu'ils veulent nous prémunir des dangers d'une IA dont les créatures robotisées dépasseraient bientôt l'homme. « Nous ferons des machines qui raisonnent, pensent et font toutes les choses mieux que nous le pouvons », déclarait ainsi Sergey Brin, cofondateur de Google.

Les progrès de la génétique et de l'IA permettent dès à présent de transformer en données la plus grande partie des opérations humaines, y compris ce qui touche à la sphère de l'esprit et des émotions. Les données se gèrent et s'analysent grâce à des algorithmes de plus en plus puissants, à qui il devient presque naturel et plus efficace de déléguer un nombre croissant de décisions ou d'actions : la conduite d'une voiture, un diagnostic de santé, le choix d'un livre…

La seconde partie a été publié dans le numéro de février 2018.

Officiers de demain,

plongez-vous au cœur de l'actualité de défense…

octobre 2017

décembre 2017

mars 2018

Abonnez-vous au tarif étudiant : 50 €(papier) ou 30 €(PDF)

La *Revue Défense Nationale* est aussi sur le *web* en accès libre :

- articles d'actualité (Tribune),
- articles d'archives (Florilège),
- recensions d'ouvrages récents.

www.defnat.com

Sigem 2018

L'officier au service de la Nation dans le monde du XXIe siècle

Depuis 2001, le Séminaire interarmées des grandes écoles militaires (Sigem) rassemble chaque année les élèves des grandes écoles militaires auxquels se joignent quelques étudiants de grandes écoles civiles.

Le thème du Sigem 2018, tenant lieu de fil conducteur aux différentes interventions et activités organisées, s'articule autour de l'idée suivante : choisir de servir la Nation repose plus que jamais sur l'adhésion à des valeurs fondamentales qui conservent leur acuité dans un monde devenu fort complexe, ce qui doit conduire chacun à s'interroger pour donner du sens à son action.

Le jeune officier, comme tout être humain, a besoin de repères de temps et de perspective pour mieux se situer dans le présent afin de se projeter dans l'avenir. Il lui est pour cela nécessaire de s'appuyer sur un héritage, un corpus de valeurs et de connaissances, solides.

Confronté à la complexité du monde de ce début de XXIe siècle, l'officier, militaire professionnel et citoyen, doit disposer d'une sérieuse culture générale. Elle seule peut lui assurer les clés de compréhension historique, sociale, géographique, économique, technologique, du choix ou du comportement de l'autre, qu'il soit ennemi ou ami.

Mais cela ne suffit pas à faire de l'officier un chef. Au moment de la décision, ce dernier est seul face à lui-même. Il lui est donc nécessaire d'avoir un esprit ouvert et curieux, apte à l'intelligence de situation et au discernement, c'est-à-dire en capacité de réfléchir sur une philosophie de l'action.