

PENSER SON ENNEMI

Modélisations de l'adversaire dans les forces armées

Serge CAPLAIN

Juillet 2018

L’Ifri est, en France, le principal centre indépendant de recherche, d’information et de débat sur les grandes questions internationales. Créé en 1979 par Thierry de Montbrial, l’Ifri est une association reconnue d’utilité publique (loi de 1901). Il n’est soumis à aucune tutelle administrative, définit librement ses activités et publie régulièrement ses travaux.

L’Ifri associe, au travers de ses études et de ses débats, dans une démarche interdisciplinaire, décideurs politiques et experts à l’échelle internationale.

Les opinions exprimées dans ce texte n’engagent que la responsabilité de l’auteur.

ISBN : 978-2-36567-899-5

© Tous droits réservés, Ifri, 2018

Comment citer cette publication :

Serge Caplain, « Penser son ennemi. Modélisations de l’adversaire dans les forces armées », *Focus stratégique*, n° 82, Ifri, juillet 2018.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tél. : +33 (0)1 40 61 60 00 – Fax : +33 (0)1 40 61 60 60

E-mail : accueil@ifri.org

Site internet : Ifri.org

Focus stratégique

Les questions de sécurité exigent une approche intégrée, qui prenne en compte à la fois les aspects régionaux et globaux, les dynamiques technologiques et militaires mais aussi médiatiques et humaines, ou encore la dimension nouvelle acquise par le terrorisme ou la stabilisation post-conflit. Dans cette perspective, le Centre des études de sécurité se propose, par la collection ***Focus stratégique***, d'éclairer par des perspectives renouvelées toutes les problématiques actuelles de la sécurité.

Associant les chercheurs du centre des études de sécurité de l'Ifri et des experts extérieurs, ***Focus stratégique*** fait alterner travaux généralistes et analyses plus spécialisées, réalisées en particulier par l'équipe du Laboratoire de Recherche sur la Défense (LRD).

Auteur

Le lieutenant-colonel **Serge Caplain** est chercheur au sein du Laboratoire de Recherche sur la Défense (LRD). Officier d'active de l'armée de Terre, diplômé de l'École militaire interarmes et breveté de l'École de Guerre, il est détaché par le ministère des Armées auprès de l'Ifri où il apporte une expérience opérationnelle aux différentes études relatives aux engagements militaires contemporains ainsi qu'à l'adaptation de l'outil de défense.

Comité de rédaction

Rédacteur en chef : Élie Tenenbaum

Assistantes d'édition : Esther Soulard et Marie-Emilie Hennequart

Résumé

La désignation d'un ennemi est toujours le fruit d'une décision politique, laquelle débouche en principe sur l'ouverture d'hostilités. Si l'ennemi résulte d'un choix politique, il est en revanche une nécessité militaire pour les armées qui se doivent de l'étudier et de le décliner à chaque niveau d'analyse, qu'il soit stratégique, opératif ou tactique. Le chef militaire entretient donc un lien particulier avec « son » ennemi, qu'il prend en compte au moyen de son système de renseignement dans le contexte unique de sa mission. Si les principes fondamentaux de l'étude de l'ennemi se retrouvent dans la plupart des armées, des différences de méthodes d'analyse et de modélisation persistent, même au sein des pays de l'OTAN, attestant ainsi des diverses façons d'aborder un adversaire. Ces approches traditionnelles pourraient toutefois être bientôt bousculées par les innovations en matière de renseignement militaire et les applications de l'intelligence artificielle.

Abstract

The designation of an enemy is always the result of a political decision, which generally leads to the opening of hostilities. If the enemy is the result of a political choice, it is though a military necessity for armed forces which have to carry out an analysis of the enemy at each level of analysis, be it strategic, operational or tactical. The military leader thus has a special bond with "his" enemy, taking him into account through his intelligence system in the unique context of his mission. If the fundamental principles of enemy study recur in most armies, differences in methods of analysis and modeling persist, even within NATO countries, showing the diversity of how to address an adversary. These traditional approaches could however soon be challenged by innovations in military intelligence and applications of artificial intelligence.

Sommaire

INTRODUCTION	9
L'ENNEMI, NÉCESSAIRE ET TOUJOURS INCERTAIN	13
Décision politique, nécessité militaire	13
<i>Le choix politique de l'ennemi.....</i>	<i>13</i>
<i>L'étude de l'ennemi : un devoir d'anticipation ?</i>	<i>15</i>
<i>L'ennemi : une nécessité militaire.....</i>	<i>17</i>
L'ennemi incertain	18
<i>De la symétrie à l'asymétrie</i>	<i>18</i>
<i>L'ennemi inatteignable, anonyme, insaisissable</i>	<i>19</i>
Réduire l'incertitude par le renseignement militaire ?	21
<i>Du renseignement militaire</i>	<i>22</i>
<i>Le renseignement au sein des états-majors</i>	<i>23</i>
<i>« Rien n'est plus dangereux que la certitude d'avoir toujours raison »</i>	<i>24</i>
LES APPROCHES ANALYTIQUES DE L'ENNEMI AU SEIN DE L'OTAN.....	27
Les principes de l'étude de l'ennemi	27
<i>Les caractéristiques intrinsèques</i>	<i>28</i>
<i>L'ennemi dans son environnement</i>	<i>29</i>
<i>Les hypothèses de travail.....</i>	<i>30</i>
<i>Face à l'inconnu, partir du connu</i>	<i>31</i>
Des approches analytiques variées.....	33
<i>Description de l'ennemi : de l'approche déductive à l'analyse systémique</i>	<i>33</i>
<i>Définir les modes d'action : approches probabiliste et possibiliste</i>	<i>38</i>
DES APPROCHES TRADITIONNELLES BOUSCULÉES ?.....	45
Un ennemi plus visible et prévisible ?.....	45
<i>Un développement sans précédent du renseignement militaire.....</i>	<i>46</i>

<i>L'intrusion de l'intelligence artificielle.....</i>	<i>48</i>
<i>L'apport des sciences cognitives</i>	<i>49</i>
<i>De la simulation au « Red teaming »</i>	<i>50</i>
Penser « rouge » : limites et implications	54
<i>La modélisation de l'irrationnel et le remplacement de l'altérité</i>	<i>54</i>
<i>Moins d'initiative et de subsidiarité ?</i>	<i>56</i>
CONCLUSION	61
Intégrer les approches de l'OTAN, tout en préservant la spécificité française.....	61
Développer l'intelligence artificielle, tout en cultivant la capacité de s'en passer	62
Mieux prendre en compte l'apport des sciences cognitives.....	62
Cultiver la diversité des analystes.....	62

Introduction

« Connais ton ennemi et connais-toi toi-même, même avec cent guerres à soutenir, cent fois tu seras victorieux¹. » Cette citation de Sun Tsu a traversé les âges pour résumer à elle seule l'intérêt que revêt la connaissance de l'ennemi dans un conflit armé. Pourtant, il n'en a pas toujours été ainsi : longtemps le sort d'une bataille a été attribué à la volonté des dieux, à la force physique des combattants ou à leur seul courage. L'idée d'étudier l'ennemi pour pouvoir adapter ses propres actions en conséquence était certes bien connue, mais elle mit étonnamment quelques centaines d'années à s'imposer². Les choix tactiques étaient en effet largement le produit de normes sociales, politiques ou religieuses et ne reflétaient pas forcément une rationalité unique. Même lorsqu'à l'époque moderne et contemporaine, la pensée stratégique a rendu toute sa place à la figure de l'ennemi, ce dernier n'était pas toujours aisé à saisir. Ainsi, avec la fin de la guerre froide et l'avènement d'un monde multipolaire, analystes et stratèges ne cessent de théoriser le « temps de l'incertitude » : dans une Europe n'ayant plus de menace déclarée à ses portes, la question de la connaissance de l'ennemi semble plus que jamais centrale.

Mais qu'est-ce qu'un ennemi ? Aujourd'hui, les mondes politique et médiatique empruntent trop facilement ce mot au registre guerrier pour que l'on puisse s'abstenir de le définir. Nous retiendrons pour cette étude sa définition militaire d'« individu, groupe d'individus (organisé ou non), force paramilitaire ou militaire, entité nationale ou alliance nationale qui se manifeste par des actes délibérément hostiles aux forces amies et qui doivent être combattus³ ». L'ennemi est donc pluriel : à partir de l'ennemi « institutionnel » auquel se confronte toute la nation, se décline un ennemi particulier, propre à chaque chef militaire, tel qu'il aura à l'affronter dans le contexte unique de la mission reçue. Chaque soldat se représente donc son ennemi et toute son action ne vise qu'à le contraindre « à la négociation ou à la défaite⁴ ». En cela, l'ennemi se distingue de la notion d'adversaire⁵, qui

1. Sun Tsu, *L'art de la guerre*, Paris, Flammarion, 2008.

2. Bien que le débat soit encore ouvert : pour certains comme John Keegan, force et volonté priment sur le renseignement pour vaincre. Sur ce point, lire J. Keegan, *Intelligence and War: Knowledge of the Enemy from Napoleon to Al-Qaeda*, New York, Alfred Knopf, 2003.

3. EMP 60.641, *Glossaire de l'armée de Terre*, CDEF, Armée de Terre, Paris, 2013, p. 227.

4. FT 02, *Tactique générale*, CDEF, Armée de Terre, Paris, 2008, p. 13.

n'a pas la même « connotation politique et psychologique [...] : l'adversaire est temporaire et une conciliation ultérieure est envisageable⁵ ». En fin de compte, l'ennemi est bien l'affaire des militaires, rarement celui du politique qui peut difficilement exclure tout règlement amiable d'un conflit. Compte tenu de ce lien si particulier, il est légitime de s'interroger sur la manière dont les militaires appréhendent leur ennemi dès le temps de paix. Par quels procédés et moyens, arrivent-ils à le concevoir, dans sa nature comme dans ses intentions, à comprendre ce qu'il veut, ce qu'il peut et la façon dont il compte parvenir à ses fins ? Quelles tendances ou quelles évolutions semblent se dessiner dans la réflexion actuelle sur l'ennemi ? Autant de questions que cette étude se propose d'aborder.

Parce que la représentation et les façons d'aborder l'ennemi reposent largement sur des schémas culturels et nationaux, il sera essentiellement question ici des pays de l'OTAN et particulièrement de la France. De même, si le renseignement est indissociable de l'analyse de l'ennemi, son champ d'action est bien trop vaste (renseignement d'ambiance, d'environnement, aspects économiques, sociétaux, politiques, etc.) pour être évoqué dans son exhaustivité ici. La question de l'ennemi préoccupe bien au-delà du spécialiste du renseignement car elle est au cœur de la nature de la guerre.

Quelles que soient les méthodes et les approches, la conception de l'ennemi au sein des forces armées repose *in fine* sur une décision, un pari, un choix dans l'inconnu. La quête effrénée visant à dissiper le « brouillard de la guerre », particulièrement visible depuis la fin de la guerre froide, n'a fait qu'effleurer la dimension humaine et subjective qui entoure l'analyse de l'ennemi. Face à ces problèmes anciens, cultiver la diversité des approches et des moyens semble rester une réponse abordable et crédible pour un état-major, toujours confronté au doute.

Cette étude abordera tout d'abord les fondements de la réflexion sur la nature de l'ennemi. Sera évoqué en particulier le caractère incontournable de cette réflexion, tant au niveau politique qu'au niveau militaire, et ce dès le temps de paix. On s'intéressera également aux moyens spécifiques dédiés à cette analyse et aux risques inhérents à ces efforts, notamment la création de fausses certitudes. Les principales approches françaises et de l'OTAN dans ce domaine seront ensuite présentées et comparées. Elles révéleront qu'à travers des démarches différentes s'expriment également des conceptions particulières. Les forces et limites de chaque modèle seront

5. Afin d'éviter les répétitions, il arrivera que le mot « adversaire » et ses dérivés soient employés tout au long de cette étude. Que le lecteur soit assuré que c'est bien de l'ennemi, dans sa définition supra, dont il est uniquement question ici.

6. EMP 60.641, *Glossaire de l'armée de Terre*, CDEF, Armée de Terre, Paris, 2013, p. 71.

déterminées en mettant en exergue leurs convergences ou leurs dissonances. Enfin, dans une approche prospective seront évoquées les nouvelles tendances et évolutions récentes des méthodes d'analyse, avec ce qu'elles comportent d'espoir mais aussi d'illusions.

L'ennemi, nécessaire et toujours incertain

On choisit ses amis mais rarement ses ennemis, du moins est-on porté à le croire. Pourtant, l'identification d'un ennemi demeure d'abord le fruit d'un processus, d'une décision politique plus ou moins contrainte, fondée sur les déclarations et actes d'une autre entité autant que sur l'anticipation de ses actions potentielles. L'avènement de nouveaux modes de confrontation reposant sur l'ambiguïté et l'opacité rend ce processus très difficile à conduire aujourd'hui. C'est toutefois une décision indispensable car, pour le militaire, l'ennemi est une nécessité : pour préparer la guerre autant que pour la conduire, la confrontation doit avoir un visage. Par ailleurs, contrairement au politique qui, décision prise, sait qui est son ennemi parce qu'il l'a choisi ou accepté en tant que tel, le militaire ne cesse jamais de le redessiner. L'adversité à laquelle se prépare le militaire est mouvante, toujours liée à la mission, au contexte ou aux délais. Même s'il dispose d'organismes et de moyens dédiés pour minimiser son incertitude, le combattant n'est jamais assuré de connaître parfaitement son ennemi.

Décision politique, nécessité militaire

La désignation de l'ennemi incombe à l'autorité politique, qui seule peut lancer et coordonner l'action de l'ensemble des moyens de l'État, au premier rang desquels se trouve l'outil militaire. Le caractère symbolique de cette décision la rend d'autant plus difficile à prendre qu'elle consiste bien souvent à déceler les intentions de l'autre. Pourtant, toute difficile qu'elle puisse être, cette désignation demeure une nécessité militaire : les forces armées ne peuvent envisager leur action, ni même se préparer, sans un ennemi – avéré ou potentiel – dûment désigné.

Le choix politique de l'ennemi

Avoir un ennemi n'est pas une fatalité politique et bien heureuses les nations qui en sont dépourvues. Pourtant, la notion d'ennemi est considérée par certains auteurs comme intrinsèquement liée à l'existence d'une nation, une altérité hostile qui viendrait s'opposer à l'identité collective bienveillante. C'est donc naturellement que l'autorité politique légitime présidant au gouvernement d'une nation a la charge de désigner

l'ennemi. Cette idée n'est pas neuve. Platon déjà, dans sa *République*, convient du caractère inévitable des conflits⁷. Il réserve toutefois la notion d'ennemi à ceux qui ne partagent pas une culture commune, des liens « naturels ». Si des conflits peuvent les déchirer, des Grecs ne sauraient être des ennemis les uns pour les autres, seuls les barbares sont susceptibles de revêtir cette catégorie⁸. Le philosophe allemand Carl Schmitt ira plus loin en faisant de la distinction entre ami et ennemi le socle constitutif de toute politique : c'est en se positionnant par rapport à son adversaire que la pensée et l'action politique prennent corps⁹. La désignation de l'ennemi est ainsi donc un acte souverain par excellence, une prérogative du politique.

L'identification de l'ennemi permet de conduire une politique adaptée et cohérente avec l'ensemble des services de l'État, visant en principe à l'abandon de sa politique jugée hostile, que cela soit par la destruction, la reddition ou la négociation. La longue période de la guerre froide (1947-1991) entre les États-Unis et l'URSS a ainsi complètement façonné le paysage stratégique de ces nations, même sans confrontation directe. Les armées étaient façonnées selon les capacités du camp adverse, les politiques étrangères vouées au ralliement de pays tiers ou au maintien des alliances, les politiques économiques soutenaient la course technologique, et même les politiques culturelles contribuaient à l'affrontement idéologique. Enfin, l'ensemble des services de renseignement était tout entier consacré à l'étude du camp ennemi et à contrer la menace qu'il représentait.

La désignation d'un ennemi peut également avoir une portée éminemment symbolique ou stratégique. Définir l'ennemi semble parfois aider à se définir soi-même. En désignant une altérité hostile, le politique peut espérer resserrer les liens avec sa population et ses alliés, voire requalifier la nature de ce qui les unit (le territoire, la culture, la langue, les valeurs, etc.). Désigner son ennemi revient aussi à une déclaration d'intention, à un moyen d'afficher sa détermination et de renforcer son influence à l'aune des échos perçus chez ses partisans. Cela permet également d'expliquer l'action de l'État, de lui donner un sens, que ce soit de manière sincère ou instrumentale. Quel que soit le régime politique, les

7. Platon, *La République*, II, 373 d-e, trad. L. Robin, Paris, Gallimard, 1959, p. 921.

8. Platon fait ainsi la différence entre les conflits armés selon s'ils sont internes aux Grecs (qu'il faut alors appeler « dissensions » ou *Stásis*, forme de maladie de la Grèce) ou entre Grecs et non-Grecs (qui méritent seuls le nom de « Guerre » ou *Pólemos*). *Ibid.*, V, 470 c-d, p. 1048.

9. C. Schmitt, *Théologie politique*, (1922), trad. J.L. Schlegel, Paris, Gallimard, 1988.

contraintes et sacrifices nécessaires à la poursuite du conflit sont ainsi plus facilement consentis¹⁰.

La tentation est parfois grande pour le politique de criminaliser l'ennemi (le considérer comme relevant du droit commun) ou de l'« essentialiser » (le considérer comme nuisible pour ce qu'il est, un ennemi par nature et non le fruit des circonstances¹¹). Dans le premier cas, on lui nie sa légitimité même à se battre tout en s'engageant du même coup à le juger et non à le vaincre. Dans le second cas, on rend l'affrontement « absolu » ouvrant la voie à une guerre d'éradication, car « sa destruction devient un objectif métaphysique¹² ». L'essentialisation profite toutefois rarement à ceux qui s'y adonnent ; au contraire, procédant d'un élan idéologique, elle ne laisse souvent à l'ennemi que le choix entre la lutte acharnée et la mort¹³.

Même s'il a participé à la prise de décision, le militaire hérite donc de l'ennemi tel que défini par le politique, mais aussi de toute la grande stratégie¹⁴ dont découlera la capacité d'action des armées. Il doit également assumer le sens que l'autorité politique donne l'inimitié : cette représentation mentale influencera la perception militaire de la menace, son analyse et aura également des effets sur son aptitude à remplir sa mission¹⁵.

L'étude de l'ennemi : un devoir d'anticipation ?

Qui étudie l'ennemi doit tenter de lire l'avenir. Que ce soit au niveau politique ou militaire, l'identification et la compréhension de la menace ne commencent pas à la déclaration des hostilités mais doivent être anticipées autant que possible. Il est aisé de se méprendre sur les intentions des décideurs d'un État. La découverte soudaine et imprévue d'un ennemi non identifié au préalable peut se traduire par une surprise stratégique, acculant à la réaction et à l'improvisation plutôt qu'à la conduite rationnelle et soigneusement planifiée : elle « impose d'ajuster ses moyens,

10. Ce qui explique les appels récurrents au sein des démocraties aux « Unions Sacrées » en cas d'acte hostile, dans le but de faire taire les dissensions internes face aux menaces extérieures.

11. J.-Y. le Drian, *Qui est l'ennemi ?*, Paris, Éditions du Cerf, 2016, p. 29.

12. H. Pierre, « L'ennemi », *Inflexions*, n° 28, 2015, p. 14-15.

13. Ainsi, Daech, en décrétant ennemis tous ceux qui ne partageaient pas sa vision du monde, a permis la création contre lui d'une coalition des plus cosmopolites, fédérant des nations ou des entités aux intérêts pourtant très divergents.

14. Au sens d'une stratégie interministérielle mise en place par l'action politique.

15. Un ennemi criminalisé ou « essentialisé » ne pouvant être un interlocuteur acceptable, la paix sera d'autant plus difficile à conclure : tout conflit ne se terminant que par le consentement des protagonistes.

voire [ses] objectifs¹⁶ », et peut même temporairement paralyser une nation. L'opération allemande *Barbarossa* du 22 juin 1941 ou l'attaque japonaise sur Pearl Harbor le 7 décembre de la même année, permirent de déstabiliser respectivement Soviétiques et Américains en donnant l'avantage de l'initiative à leurs ennemis. Pour l'État, il est donc indispensable de « voir venir » son ennemi : l'anticipation est un impératif de sécurité.

Or, particulièrement sur le plan politique ou stratégique, la volonté de nuisance d'un adversaire peut s'avérer difficile à évaluer. Les intentions sont changeantes et toujours plus incertaines que les capacités d'action. Ainsi, l'étude de l'ennemi repose sur un dilemme¹⁷ : tandis qu'un ennemi se révèle souvent par ses actes, son étude doit être nécessairement antérieure à la première manifestation directe d'hostilité. En outre, si la désignation publique d'un ennemi peut contribuer à alimenter une montée vers la confrontation, une forme de communication stratégique plus ou moins explicite est néanmoins requise dès lors que l'on souhaite prévenir une agression, principalement dans le cadre de stratégies dissuasives. Incertain des intentions hostiles d'un acteur avant que la menace ne se matérialise, le décideur est donc contraint de faire étudier non pas un unique ennemi clairement identifié, mais l'ensemble des menaces potentielles qu'il considère prioritaires, que ce soit en raison de leur gravité ou de leur probabilité.

Cette nécessaire anticipation s'étend bien au-delà du seul ennemi « politique ». Sur le plan des opérations militaires, pour prévenir la surprise (opérative ou tactique), le militaire doit en effet savoir anticiper sur toute menace, potentielle ou avérée, estimer ses intentions, ses préférences stratégiques, supposer ses modes d'actions. Or, tout échelon de commandement guide la réflexion de ses subordonnés en leur fournissant son appréciation. S'inscrivant normalement dans le strict cadre défini par son supérieur, à chaque niveau, le chef militaire prend position pour ce qui relève de ses attributions. En fonction de ses directives, des renseignements qui lui sont communiqués et de ses attributions, il fait donc un « pari » sur les caractéristiques de l'ennemi (nature, volume, mode d'action, etc.) qu'il fait le choix de prendre en compte.

En somme, ni le politique ni le militaire ne peuvent attendre d'être assurés de l'intention hostile d'une menace avant la survenue du fait déclencheur qui fera d'elle un ennemi. Même sans agression manifeste,

16. C. Brustlein, « La surprise stratégique, de la notion aux implications », *Focus stratégique*, n° 10, Ifri, octobre 2008, p. 13.

17. La notion de dilemme de sécurité, voir J. H. Hertz, « Idealist Internationalism and the Security Dilemma », *World Politics*, vol. 2, n° 2, 1950, p.157.

désigner l'ennemi, l'étudier, l'analyser, est une action qui ne peut se faire que par anticipation et dans le doute.

L'ennemi : une nécessité militaire

Pourtant, l'anticipation est un impératif de sécurité et le militaire a besoin d'un ennemi, qu'il soit réel, probable, potentiel, ou simplement d'exercice. Les forces armées ont structurellement besoin d'un ennemi pour s'organiser, se préparer, s'entraîner, quitte à en créer s'il n'y en a pas.

Sur le plan stratégique, connaître les priorités politiques en termes de menaces (avérées ou potentielles) est nécessaire : il faut « savoir pour prévoir, prévoir pour pouvoir », comme le disait Auguste Comte. En premier lieu, cette ligne politique permet d'adapter l'outil de défense tant dans le domaine de l'équipement que des procédés. Quand un ennemi est clairement désigné, les armées sont dimensionnées directement par cette menace principale (*threat-based planning*), comme ce fut le cas durant la guerre froide où le format et les doctrines occidentales étaient généralement construits en corrélation avec la menace soviétique. Plus tard, en l'absence d'adversaire identifié, certaines armées comme celles des États-Unis, ont eu tendance à se construire par rapport à des capacités militaires à détenir (*capabilities-based planning*). Cette approche a notamment permis après la fin de la guerre froide de justifier d'importants crédits de défense en l'absence de menace désignée. Cependant, il s'est avéré par la suite nécessaire de lier à des scénarios d'engagement crédibles voire probables pour ne pas courir le risque de se retrouver avec un outil de défense cohérent mais parfaitement inadapté à la situation du moment¹⁸.

Par ailleurs, l'enseignement militaire et l'entraînement peuvent également être adaptés, avec toute l'anticipation nécessaire qu'il convient quand on sait le temps et les moyens nécessaires pour créer un soldat¹⁹. En effet, pour les échelons subordonnés, un ennemi, même théorique, est indispensable, l'essentiel de l'action militaire hors opération étant de se préparer à l'engagement. Tout exercice, quel que soit le niveau, nécessite une force d'opposition pour pouvoir animer l'ensemble d'une unité. L'action militaire ne peut être pensée sans altérité. À ce titre, les armées se sont dotées d'ennemis « génériques ». Des catalogues d'ennemis – États ou organisations – imaginaires présentant toutes les données utiles pour réaliser des exercices ou des entraînements : cadre géographique,

18. J.-B. Kendall, *Capabilities-Based Military Planning: The Myth*, National War College, Washington D.C., 2002.

19. En France, il faut plusieurs mois pour former un militaire du rang, presque un an pour former un jeune sous-officier, un chef de section requiert environ 3 à 4 ans de formation et un colonel, au moment de commander son régiment, a passé presque 7 années en écoles au cours de sa carrière.

organisation de la force, équipement, stratégie, tactiques et modes d'actions de chacune de leurs composantes (terre, air, et mer)²⁰. Ils s'inspirent également d'informations provenant de sources ouvertes, d'expérience terrain et, parfois, de l'appui de la direction du renseignement militaire (DRM). Pour être toutefois crédibles et utiles à la préparation des forces, ces documents de référence reprennent des typologies d'ennemis correspondant à des adversaires réels, susceptibles d'être rencontrés par les armées, et cohérents avec les orientations politiques.

Mais surtout, pour toutes ces problématiques liées à la connaissance des menaces potentielles, à la caractérisation de la menace et à la préparation à l'engagement, les militaires ont besoin des informations fournies par l'ensemble des services de renseignement. Or, ces services, qui ne relèvent pas forcément des armées, ont besoin d'être orientés par le politique qui doit leur donner des priorités. Sans direction claire, les militaires risquent de manquer d'informations utiles par dispersion ou sous-utilisation des moyens.

Ainsi, disposer des priorités politiques sur les menaces à étudier est une nécessité militaire à tous les échelons – qu'il s'agisse de directives identifiant clairement un ennemi principal ou plusieurs adversaires potentiels, ou encore d'orientations plus ouvertes appelées à se traduire par une planification plus générique. Il est donc de la responsabilité du pouvoir politique de se prononcer sur le sujet.

L'ennemi incertain

Si la définition d'un ennemi incombe à l'échelon politique, cette décision est sûrement rendue plus difficile du fait du contexte dans lequel les forces sont employées actuellement. À des ennemis clairement identifiés, connus et fonctionnant sur un modèle westphalien, se sont substituées des menaces diffuses et difficiles à identifier.

De la symétrie à l'asymétrie

Longtemps les forces armées ont été employées face à des ennemis clairement désignés, de type étatique. Mais la diversité des ennemis actuels et leur imprévisibilité troublent la perception de la menace. En effet, les années 1990 ont vu les menaces potentielles en Occident évoluer du fait de la transformation des conflits d'une forme symétrique (impliquant des

20. En France, ce sont les différents volumes du document d'emploi EMP 20.615, *Ennemi générique pour l'entraînement et l'instruction des forces terrestres* (ex-TTA 808), CDEF, Armée de Terre, Paris, 2009. Datant de près de 10 ans, ces scénarios d'emploi et les ennemis d'exercice rattachés sont en train d'être revus par l'armée de Terre.

« forces armées de nature similaire dans leurs volumes, équipements, technologies et doctrines, et usant des mêmes modèles stratégiques militaires ») à une forme dissymétrique (avec des forces « de nature similaire, mais de structures, de volumes, d'équipements et technologies et de doctrines différents ») voire asymétrique (dans lesquels il y a « disparité totale d'ordre et de nature des buts de guerre, des moyens et des manières d'agir des adversaires en présence »)²¹.

Or, plus le combat est irrégulier, plus le degré d'incertitude augmente quant à la nature et aux intentions de l'ennemi. Face à des combattants dissimulés au sein des populations, dispersés en une multitude de groupes ayant chacun des objectifs propres et formant des alliances de circonstance, la définition de l'ennemi est toujours complexe : trop exclusive, trop incomplète, ou trop éphémère. On se souvient par exemple des discussions sur la position à adopter face au front Jabhat al-Nosra au sommet de Marrakech en décembre 2012²². Ce groupe, reconnu comme terroriste par les États-Unis de par ses liens avec Al-Qaïda, combattait les troupes de Bachar Al-Assad en Syrie, ce qui en faisait un allié de circonstance acceptable pour certains pays de la coalition.

L'ennemi inatteignable, anonyme, insaisissable

D'autres formes de conflictualité rendent également difficile la désignation d'un ennemi clair. Le cas des confrontations par « proxy » (des combattants asymétriques soutenus, plus ou moins secrètement, par un pays tiers) est également problématique. Une définition exhaustive de l'ennemi inclurait les combattants irréguliers comme leurs soutiens étatiques éventuels. Or, la mise en cause directe de l'État soutenant le « proxy » peut poser problème au politique, soucieux d'éviter une extension du conflit. L'ennemi officiel est alors bien souvent minoré, circonscrit à une zone, une nationalité ou une activité. Si le politique fait ce choix de restreindre sa liberté d'action, il obère *de facto* celle des militaires²³.

Cette problématique bien connue du temps de la guerre froide, a connu un regain d'intérêt depuis quelques années sous la forme de « l'ambiguïté stratégique ». Tirant parti de la posture légitimiste des politiques de défense occidentale, connaissant la dépendance des décideurs vis-à-vis de leurs opinions publiques, certains pays dénie à leurs adversaires la capacité de

21. FT-02, *Tactique générale*, CDEF, Armée de Terre, Paris, 2008, p. 11.

22. « 4^e réunion des amis du peuple syrien », conférence de presse de Laurent Fabius, ministre des Affaires étrangères à Marrakech, 12 décembre 2012, disponible sur : www.diplomatie.gouv.fr.

23. C'est en effet l'un des effets recherchés par ceux qui ont recours à la guerre dite « hybride ». Voir le discours du général Gerasimov, chef d'état-major des armées russes, février 2013.

les désigner comme ennemis²⁴. Agissant juste en dessous du seuil de tolérance de leurs compétiteurs, niant si besoin leur implication même quand celle-ci se fait évidente, ces pays manœuvrent pour ne pas être ouvertement désignés comme ennemis²⁵. La « guerre » de l'information prend alors tout son sens : avec l'appui de médias acquis à la cause d'un des adversaires, toute tentative d'une des parties pour désigner l'autre comme responsable sera immanquablement contrebalancée par des messages contradictoires, jetant la confusion sur l'identité des agresseurs et des agressés, empêchant la mobilisation nationale contre un ennemi faisant consensus.

Le cas de la menace terroriste est également assez emblématique de cette difficulté à nommer l'ennemi. Quand le Président américain George W. Bush, déclare la « guerre contre le terrorisme » au lendemain des attentats de 11 septembre 2001, il désigne un ennemi qui n'est plus un État ou une organisation précise, mais un procédé, une façon de faire la guerre. Cette confusion sémantique crée un flou stratégique dans la définition de l'ennemi. Tout peut dès lors en faire partie : Al-Qaïda, des États soutenant ses activités, des insurgés non djihadistes, des Américains auteurs d'attentats, etc. La France a évité de refaire cette erreur²⁶, mais les mots pour désigner l'ennemi ont également été difficiles à trouver. Après avoir nommé officiellement « l'Islam radical et le djihadisme²⁷ », c'est « Daech » qui fut finalement désigné comme ennemi institutionnel²⁸ pour justifier les opérations Chammal²⁹ et Sentinelle, dans une logique de « continuum » de la menace. Cette désignation a le mérite d'être claire et permet de réaffirmer la volonté française de bien distinguer les nationaux qui se livrent au terrorisme et qui relèvent du droit commun comme tous criminels, de l'ennemi de la Nation (Daech) qui est l'affaire des forces armées. Dans la pratique, la distinction n'est pas aisée pour autant, car elle repose à la fois sur la nationalité de l'auteur comme sur le lieu de son méfait. Si un Français capturé en Syrie est jugé comme un criminel, un Irakien commettant un acte terroriste en France le sera tout également.

24. On pourra évoquer ici le conflit ukrainien du Donbass, dans lequel la Russie a toujours nié être impliquée militairement, mais où les rapports faisant état de « petits hommes verts » russophones aux côtés des rebelles ont laissé penser le contraire. Lire B. Vitkine, « Les moments qui accréditent l'intervention des soldats russes en Ukraine », *Le Monde*, 28 août 2014.

25. *Ibid.*

26. « Généralisation et anonymisation de l'ennemi sont deux travers dont la France s'est toujours gardée », cité in J. Y le Drian, *Qui est l'ennemi*, op. cit., p. 24.

27. *Livre blanc du gouvernement sur la sécurité intérieure face au terrorisme*, Paris, La Documentation française, 18 mai 2005, p. 140.

28. Discours de François Hollande, Président de la république, devant le Parlement le 16 novembre 2015 suite aux attentats de Paris.

29. Nom donné au volet français de l'opération interalliée « Inherent Resolve (OIR) » et qui mobilise aujourd'hui près de 1 200 militaires (Ministère des Armées, janvier 2017).

Enfin, il y a des cas où l'ennemi est très difficilement identifiable, c'est notamment le cas du domaine cyber. Les dégâts peuvent y être considérables pour un État³⁰, même si la qualification d'une attaque de ce type comme acte de guerre fait encore débat³¹. Les auteurs cherchent souvent à masquer leurs traces, à compliquer l'attribution d'une attaque, et l'identification n'est jamais une certitude. N'ayant – pour le moment – pas encore de mort directement imputable à son actif, il est toujours délicat de qualifier le « cyber-ennemi » tant que celui-ci ne poursuit pas son agression dans le champ matériel³². Le « pur ennemi cyber » n'existe donc probablement pas encore³³, mais la notion pourrait s'appliquer à terme dans le cas d'une nation hostile répétant régulièrement et ostensiblement ce type d'agression. La menace a donc été prise en compte par les armées³⁴.

Réduire l'incertitude par le renseignement militaire ?

La fonction des services de renseignement est d'informer le gouvernement, d'éclairer et de faciliter ses décisions ayant trait à la sécurité nationale. Une partie des informations interservices collectées est exploitée par les armées pour leur permettre d'assurer leurs missions : il s'agit du « renseignement d'intérêt militaire », qui recouvre « les informations et les évaluations nécessaires à l'appréciation de situation et à la prise de décision, à tous les niveaux de commandement³⁵ ». Pour caractériser leur ennemi, les forces armées ont toutefois besoin de moyens propres de renseignement qui agissent prioritairement à leur profit. Innervant chaque niveau hiérarchique, ce système permet au chef militaire de réduire l'incertitude sur la nature ou les intentions ennemies, sans toutefois pouvoir jamais la dissiper totalement. La conscience de cette imperfection est indispensable et prémunit contre la certitude qui guette toujours le chef militaire.

30. L'attaque « Stuxnet » en juillet 2009, attribuée aux États-Unis et visant le programme nucléaire de l'Iran, aurait retardé de plusieurs années les travaux perses d'enrichissement de l'Uranium. À ce propos lire, S. McBride, « Cyber-Attacks: Who's Keeping Score? », *War on the Rocks*, 18 juillet 2017, disponible sur : warontherocks.com.

31. J. Crisp, « EU Governments to Warn Cyber-Attacks Can Be an Act of War », *The Telegraph*, 29 octobre 2017, disponible sur : www.telegraph.co.uk.

32. On distingue ce qui relève du champ « matériel » de la conflictualité (la confrontation physique, la destruction, etc.) de ce qui est rattaché au champ « immatériel » (l'influence, le cyber, etc.).

33. D. Danet, « L'ennemi Cyber : entre nécessité épistémologique et bourrage de crâne », *Inflexions*, n° 28, 2015, p. 172.

34. Un « Commandement de la Cyberdéfense » a notamment été créé en France au 1^{er} janvier 2017.

35. PIA 00.401, *Glossaire interarmées de terminologie opérationnelle*, État-major des Armées, Ministère de la Défense, Paris, 2007.

Du renseignement militaire

Une fois la menace définie et les options stratégiques validées par le gouvernement, l'échelon militaire dispose déjà d'une présentation de l'ennemi dans sa globalité, rendue possible par les grandes agences nationales de renseignement stratégique. Cette vision est toutefois souvent trop généraliste pour couvrir les besoins, essentiellement locaux, d'une opération. C'est pourquoi, dans la planification comme dans la conduite des opérations, les militaires disposent de moyens et de procédés de renseignement qui leur sont propres. Ce « renseignement militaire », « processus de collecte, d'analyse, de dissémination et d'exploitation de l'information d'origine et d'intérêt militaire³⁶ », utilise des moyens spécifiques et dédiés au chef militaire. Ils sont essentiels pour lui permettre de décliner, à chaque niveau de la chaîne de commandement, l'ennemi correspondant à sa mission, à son cadre espace-temps et à sa situation : « son » ennemi.

Le renseignement militaire fonctionne assez classiquement selon le principe du cycle du renseignement³⁷. Tout commence par *l'orientation* qui recouvre l'expression de besoins (le chef fixe ce qu'il cherche à savoir) et les directives pour les capteurs (humains, techniques) de renseignement. Vient alors *la recherche* ou la collecte des informations liées à ces directives, qui seront recoupées dans la phase suivante, *l'exploitation* ou l'analyse. Enfin, il restera à en faire la *diffusion*, par laquelle on répond finalement aux questions posées par le décideur en première phase.

Les intervenants de ce renseignement militaire sont présents à tous les niveaux hiérarchiques, chacun participant à la connaissance globale de la situation par la transmission d'informations aux échelons immédiatement supérieurs et subordonnés. En France, la Direction du Renseignement Militaire (DRM) a été créée en 1991. Dépendant directement du chef d'état-major des armées, elle a pour mission d'appuyer « la planification et la conduite des opérations au niveau stratégique » et de « contribue[r] à l'orientation de la manœuvre au niveau tactique³⁸ ». Disposant de moyens propres – centres spécialisés et moyens satellitaires –, elle anime et coordonne également ceux de chaque armée.

36. J. Henrotin, « Les mutations du renseignement militaire », *Focus stratégique*, n° 71, Ifri, janvier 2007, p. 9.

37. DIA-2(A), *Renseignement d'intérêt militaire et contre-ingérence*, CICDE, Ministère de la Défense, 2016. Plusieurs variantes (à 4 ou 5 phases) avec d'autres appellations existent également dans la littérature spécialisée.

38. « Missions de la DRM », Ministère des Armées, septembre 2016, disponible sur : www.defense.gouv.fr.

Cependant, du fait de la singularité de sa mission, le chef militaire ne peut pas compter uniquement sur le renseignement diffusé par le niveau supérieur. Il doit disposer de moyens dédiés qui lui sont indispensables pour se faire sa propre appréciation sur l'ennemi. C'est pourquoi, en plus des unités spécialisées, les armées disposent au niveau tactique d'unités affectées à la collecte du renseignement, ou pouvant occasionnellement conduire ce type de mission³⁹. De taille et de capacités diverses, appartenant à toutes les armes⁴⁰ et présentes dans la plupart des formations, elles permettent, à chaque échelon tactique ou presque, de disposer – de façon *ad hoc* ou organique – d'une cellule de renseignement au sein de son état-major (de bataillon, de brigade, de division, etc.). Par ce dispositif, chaque unité alimente la chaîne du renseignement avec les éléments qu'elle collecte et en fait bénéficier l'ensemble de la force. Tout chef militaire peut ainsi appréhender l'ennemi qu'il pourrait avoir à affronter en réduisant au mieux l'incertitude liée à ses capacités ou à ses pratiques, ainsi qu'aux spécificités de la mission.

Le renseignement au sein des états-majors

Quel que soit le niveau d'un état-major, celui-ci dispose d'une cellule chargée du renseignement : le 2^e bureau⁴¹ plus communément appelé B2⁴². Son rôle est « d'apporter la connaissance et la compréhension de la situation [...] et de fournir les analyses nécessaires au chef [...] pour prendre des décisions tant dans les phases de préparation que de conduite des opérations⁴³ ». De taille et d'organisation variables en fonction de sa composante et de son niveau de commandement, cette cellule a pour mission d'assurer au minimum deux fonctions essentielles : le recueil, qui consiste à collecter les informations et coordonner les moyens, et l'analyse,

39. La plupart des unités de Cavalerie, dont la finalité reste le combat embarqué, sont également aptes à des missions de renseignement (éclairage ou reconnaissance par exemple).

40. Pour l'armée de Terre et sans être exhaustif, on pourra citer les Escadrons de Reconnaissance et d'Investigation (ERI) de l'Arme-Blindée Cavalerie, les Sections d'Aide à l'Engagement Débarqué (SAED) de l'Infanterie ou bien les Détachements de Liaison d'Observation et de Coordination (DLOC) de l'Artillerie.

41. Depuis la fin de la guerre d'Algérie (1962), cette appellation n'est plus couramment employée en France, même si elle reste sémantiquement correcte.

42. Dans la terminologie de l'OTAN, chaque cellule fonctionnelle d'un état-major est référencée selon ses attributions : 1 pour l'administratif, 2 pour le renseignement, 3 pour les opérations, 4 pour la logistique, 5 pour la planification, 6 pour les transmissions, etc. Une lettre définissant le niveau de commandement accompagne cette dénomination : J pour *Joint* (interarmées), G pour *Ground* (composante terrestre de théâtre), S pour *Subordinate* (unité tactique de manœuvre), etc. La lettre B n'est pas une appellation de l'OTAN mais le terme générique français pour « Bureau » : un « B2 » est donc une cellule renseignement d'un état-major, quel que soit son niveau de commandement (J, G, S...) ou sa composante (Terre/G, Air/A, Mer/M, Forces Spéciales/SOC).

43. *Base documentaire tactique à l'usage des stagiaires de l'école d'état-major*, 2016-2017, EEM, Armée de Terre, Paris, 2016, p. 200.

qui est l'interprétation et l'élaboration du renseignement. Le B2 conseille également le chef quant au caractère de la menace et s'assure donc de la bonne diffusion du renseignement à ceux qui ont « besoin d'en connaître ». Cependant, le chef militaire reste entièrement responsable de la définition de son ennemi, et qui à ce titre valide ou non les conclusions de son B2.

Le B2 a un rôle à la fois transverse et vertical. Au sein de l'état-major, il se coordonne avec l'ensemble des autres cellules (opérations, plans, logistique, etc.) et leur apporte son expertise technique. Dans la chaîne du renseignement, chaque B2 reçoit des informations et des directives spécifiques du B2 du niveau supérieur auquel il doit envoyer ses comptes rendus et peut demander un appui. En fonction de son niveau de commandement, un B2 peut être amené à recevoir des directives des instances nationales, dont il peut également bénéficier de l'appui⁴⁴.

Enfin, la cellule Renseignement a la particularité de travailler sur plusieurs temporalités, plusieurs « ennemis » simultanément. D'une part, elle suit la situation actuelle et les opérations courantes, et doit donner au chef la vision de l'ennemi qui se dévoile pour anticiper le futur proche. Mais le B2 doit surtout permettre de conserver un temps d'avance dans la manœuvre, et donc être capable de définir l'ennemi que l'unité aura à affronter lors de la prochaine mission⁴⁵. Enfin, en alimentant sa chaîne fonctionnelle, le B2 répond aux questions ou envoie des demandes à des correspondants qui n'appartiennent pas à l'état-major, mais à d'autres organismes qui ont chacun leur propre temporalité. Il doit alors, à chaque fois, recadrer son analyse selon le cadre temporel particulier de ses interlocuteurs.

S'intéressant à l'ensemble du renseignement d'intérêt militaire dans sa diversité, chargée de définir l'ennemi présent comme à venir, contrainte d'envisager tous les possibles, la cellule renseignement assure une fonction capitale mais éminemment complexe au sein de l'état-major.

« Rien n'est plus dangereux que la certitude d'avoir toujours raison »

La solidité du travail de renseignement peut parfois conduire le chef militaire à penser tout connaître de l'ennemi. Il n'en est rien : tout renseignement est susceptible d'être biaisé par la subjectivité de l'humain. La perception de l'ennemi est une vue sur l'autre, aussi l'une des pires

44. Pour la France, typiquement, le B2 du centre de planification et de conduite des opérations (J2/CPCO) ou la direction du renseignement militaire (DRM).

45. Le B2 travaille donc étroitement avec la cellule responsable de la planification (B5).

erreurs d'un chef militaire serait-elle de croire avoir parfaitement compris l'ennemi, et de diffuser cette certitude à l'ensemble de son état-major.

L'ennemi ne partage pas forcément les mêmes références sociétales et culturelles que soi. Il ne vit pas dans le même environnement, n'a pas la même histoire, les mêmes codes, ni donc la même façon de penser et de se comporter. Sa singularité influence directement son raisonnement, ses décisions, ses objectifs politiques et militaires, les moyens qu'il mettra en œuvre pour les réaliser. Même si la connaissance des aspects socioculturels⁴⁶ de l'ennemi est considérée dorénavant comme un impératif dans tous les pays de l'OTAN⁴⁷, il n'est jamais possible de connaître suffisamment une population, au point de savoir avec certitude « comment » elle pense. Les conflits asymétriques récents tendent en outre à impliquer des populations extrêmement diverses partageant le même territoire. Il est d'autant plus complexe pour les militaires qui n'y séjournent généralement que quelques mois⁴⁸ d'appréhender toutes les interactions et les motivations des peuples et autres groupes armés. Le cas de la mosaïque culturelle libanaise est emblématique de la difficulté de bâtir une bonne appréciation de situation : sur 10 452 km² cohabitent des musulmans (sunnites, chiites, druzes ou alaouites), des chrétiens (maronites, orthodoxes, arméniens ou catholiques), des réfugiés palestiniens installés depuis plusieurs générations et, depuis peu, plus d'un million de migrants⁴⁹ venant essentiellement de Syrie.

À cette complexité liée à l'altérité, se rajoutent les limites inhérentes à la nature humaine des intervenants de l'ensemble du cycle du renseignement. En effet, tout observateur est sujet à un certain nombre d'influences inconscientes, les biais cognitifs, qui pèsent à la fois sur ses perceptions et ses décisions. On pense ainsi au biais d'attention (quand son jugement est altéré par ses propres intérêts), au biais mnésique (lorsque l'expérience d'une situation similaire affecte une décision), au biais culturel (l'importance de la culture dans la perception) ou encore au biais affectif (comment les émotions prennent le pas sur la décision⁵⁰). Celui qui a

46. Ou « cultural awareness », expression américaine fréquemment privilégiée dans la littérature militaire pour évoquer ces aspects.

47. « Conducting a successful counterinsurgency campaign requires a flexible, adaptive force led by agile, well-informed, culturally astute leaders », cité in FM 3-24, *Counterinsurgency*, U.S. Army and U.S. Marine Corps, décembre 2006.

48. Un soldat américain est généralement déployé un an sur un théâtre d'opérations. Un soldat français entre 4 et 6 mois, selon les théâtres ou les missions.

49. L. Kabbanji et L. Drapeau, « Étudier les migrations de Syrie au Liban : propositions méthodologiques », *Working Paper du Ceped*, n° 36, Ceped (UMR 196 Université Paris Descartes IRD), décembre 2017.

50. A. Tversky et D. Kahneman, « Judgment under Uncertainty: Heuristics and Biases Science », *New Series*, vol. 185, n° 4157, 27 septembre 1974, p. 1124-1131.

grandi et a été éduqué dans une rationalité occidentale aura par exemple du mal à anticiper des actions pouvant lui paraître irrationnelles car fondées sur la tradition, l'honneur, la spiritualité, et non sur un raisonnement logique. De fait, et quelle que soit la qualité du personnel, la perception de la menace à chaque étape du cycle du renseignement est toujours susceptible d'être biaisée : l'appréciation de l'ennemi reste une activité humaine, donc faillible⁵¹.

Mais le principal biais du cycle est probablement le biais bureaucratique apporté par la position du chef militaire lui-même. Les moyens dont il dispose peuvent affecter son jugement⁵², et celui-ci subit également les perceptions de ses intervenants (subordonnés, homologues, supérieurs). Or, les schémas mentaux du chef sont déterminants : chargé d'orienter le renseignement, seul à décider des conclusions, sa subjectivité se répercute structurellement sur toute la chaîne. Tout avis *a priori* de sa part risque de diriger le renseignement vers une confirmation plutôt qu'un avis objectif, restreignant *de facto* le champ d'investigation des spécialistes⁵³. Plus tard, le biais de confirmation l'incitera toujours à préférer la réponse qui valide les idées préconçues. Les autres options peineront à s'imposer, d'autant qu'un décideur est souvent plus influencé par ses propres ressentis que par les critères objectifs des spécialistes⁵⁴.

Ces phénomènes sont particulièrement marquants dans le système militaire en raison de sa hiérarchisation. Le chef y est parfois idéalisé et la carrière des subordonnés dépend souvent beaucoup de l'appréciation de leur supérieur. La tentation peut donc exister, chez les conseillers, de ne proposer que des avis qui viennent corroborer la vision initiale de leur supérieur. Le système engendre ainsi une forme de « tunnellisation » du raisonnement, susceptible de déboucher sur un dangereux sentiment de certitude. Celle-ci enferme l'action dans un carcan intellectuel qui rend impossible toute adaptation réactive face à l'imprévu. Parmi les raisons de la débâcle de mai 1940, la certitude de l'invulnérabilité des Ardennes a empêché les armées franco-britanniques d'envisager à temps un contournement opératif sur leur flanc droit. Le résultat fut funeste car jamais l'initiative ne put être reprise.

51. Voir l'analyse critique du cycle du renseignement de J. Marchand, « La production du renseignement comme système d'action », *Communication et organisation*, n° 14, 1998.

52. R. Kagan, « Qui dispose d'un marteau voit des clous partout [...], qui n'a pas de marteau ne voit pas les clous », *La puissance et la faiblesse*, Paris, Plon, 2003, p. 52.

53. Échanges avec des officiers du renseignement.

54. K. Yarhi-Milo, *Knowing the Adversary: Leaders, Intelligence and Assessment of Intentions in International Relations*, Princeton, Princeton University Press, 2014.

Les approches analytiques de l'ennemi au sein de l'OTAN

Le politique désigne l'ennemi aux armées qui l'étudient pour conduire la bataille. Or, si l'ennemi est généralement unique au niveau politique, il est multiple pour le militaire, chaque échelon se devant de le décliner en fonction de ses besoins propres. L'étude de l'ennemi suit un processus incrémental qui implique l'ensemble de la hiérarchie jusqu'aux plus petits niveaux tactiques. À partir des informations dont il dispose, le chef militaire a la responsabilité de modéliser son ennemi et de diffuser son appréciation à ses subordonnés, afin qu'ils puissent à leur tour bâtir le leur. Le militaire a donc un rapport « intime » avec son ennemi : il est pour partie le sien, le produit de sa propre réflexion, spécifique à son action.

Chaque culture militaire a sa méthode en vue d'analyser l'ennemi et de le décrire. Initialement pourtant, la plupart des démarches analytiques reposent sur des principes largement partagés, et la nécessité de prendre en compte l'ensemble de l'environnement est unanime. Mais si tout militaire a besoin a priori des mêmes informations pour pouvoir concevoir sa manœuvre, plusieurs approches sont possibles en vue de modéliser l'ennemi. Ainsi, une fois qu'une certaine convergence a été obtenue quant à la description de l'ennemi (qui est-il, que veut-il ?), il existe des différences peuvent perdurer pour ce qui relève de la façon d'aborder les modes d'action (comment peut-il l'obtenir ?). Sur ce dernier point en particulier, aux côtés d'une méthode traditionnellement française « par les possibles », cohabite une approche plus probabiliste venue du monde anglo-saxon et adoptée aujourd'hui par l'OTAN. Si ces concepts peuvent parfois diverger, ils offrent surtout une intéressante complémentarité, notamment selon le niveau de guerre (stratégique, opératif ou tactique) considéré.

Les principes de l'étude de l'ennemi

La finalité des différentes méthodes est la même : caractériser l'ennemi, au travers de certains critères universels tels que sa nature, son volume, ses objectifs et ses modes d'action. Défini à travers le prisme de la mission considérée, l'ennemi ainsi modélisé va permettre au chef militaire de construire sa propre manœuvre.

Sous un angle militaire, en effet, tout ennemi ne se conçoit que dans le cadre défini par la mission reçue. C'est elle qui donne à la fois l'effet à obtenir, les conditions du succès, les limites temporelles et spatiales, tous les éléments indispensables pour borner l'action, et donc l'ennemi particulier à affronter. Une unité n'a pas à affronter l'ensemble des forces de l'adversaire, mais qu'une partie : « son » ennemi, « celui qui peut s'opposer à l'exécution de sa mission dans toute la zone d'action et la totalité du cadre temporel fixé de sa mission⁵⁵ ». C'est seulement une fois que cette mission et ses implications sont parfaitement comprises que l'étude de l'ennemi peut véritablement commencer.

Les caractéristiques intrinsèques

En premier lieu, il s'agit de définir l'état quantitatif et qualitatif de l'ennemi, ce qui permet de déduire ses capacités, de les comparer à celles des forces amies pour déterminer le rapport de force⁵⁶ global dans le cadre espace-temps de la mission reçue. Une fois cet ennemi identifié (« ce qu'il est »), son objectif (« ce qu'il veut ») doit être déterminé car celui-ci va orienter son action. Enfin, l'ensemble de ces éléments sont synthétisés et étudiés afin de présupposer les manœuvres adverses possibles ou probables, ses modes d'action (« comment il peut l'obtenir »). Chaque étape est importante car elle conditionne la suivante. Par exemple, les capacités de l'ennemi permettent de supposer ses intentions en déterminant ses forces et faiblesses et les comportements qui en découlent. Les intentions de l'ennemi sont constitutives de son action car toute manœuvre n'est réalisée que pour réaliser un objectif, malgré l'opposition de la force adverse. Ce n'est qu'une fois les hypothèses de manœuvre ennemies identifiées que le chef militaire va pouvoir choisir sa propre action. Là est toute la finalité de l'étude de l'ennemi : choisir la manœuvre amie.

Cependant l'importance de ces critères et le niveau de précision ou d'incertitude acceptable peuvent varier selon le niveau considéré. Au niveau stratégique, déterminer les intentions de l'ennemi (ses objectifs stratégiques) est capital car cela participe à déterminer les conditions de la victoire. Ses options stratégiques sont en revanche définies de façon très générale et bien souvent déduites des principales capacités adverses. À l'inverse, au niveau tactique, les objectifs de l'ennemi sont pour partie déjà fixés : ils sont bien souvent déduits des appréciations du niveau supérieur, ramenés dans le cadre espace-temps de la mission. La détermination des

55. *Base documentaire tactique à l'usage des officiers d'État-major*, Armée de Terre, Paris, 2017.

56. EMP 60.641, *Glossaire Français/Anglais de l'armée de Terre*, CDEC, 2013, p. 409.

modes d'actions ennemis est en revanche cruciale car toute la manœuvre amie est construite en conséquence.

L'ennemi dans son environnement

L'ennemi n'est pas « hors sol » : il interagit avec son environnement qui va influencer à la fois ce qu'il est, ce qu'il veut et ce qu'il peut faire. L'ensemble des éléments exogènes qui peuvent avoir une incidence sur l'ennemi sont impérativement pris en compte pour sa modélisation, dans une approche la plus « globale » possible. Ces données d'environnement sont extrêmement diverses et il est difficile d'en faire une liste exhaustive. Elles peuvent inclure des aspects politiques (interne, externe), géographiques (terrain, climat, populations, etc.), météorologiques, économiques (richesses et répartitions, tissu industriel ou agricole, etc.) ou même sociaux (culture, histoire, religion, ethnicité, etc.).

L'importance relative de ces aspects et la quantité d'information nécessaire pour une étude de l'ennemi dépendent en partie du niveau du chef militaire. Au niveau stratégique et opératif, le développement de la connaissance⁵⁷ (*Knowledge Development*) est un préalable incontournable de la planification. Ce procédé permet de nourrir la réflexion grâce à des informations utiles regroupées sous le signe PMESII (Politique, Militaire, Économique, Social, Industriel, Information⁵⁸). Aux niveaux opératifs ou tactiques, les besoins ne sont pas les mêmes et sont plus centrés sur l'adversaire. Une préparation renseignement de l'espace des opérations⁵⁹ (PREO), appelée en anglais *Intelligence Preparation of the Battlefield*⁶⁰, sous la responsabilité du B2, va permettre au chef militaire d'identifier les éléments clés de l'environnement nécessaire à la connaissance de son ennemi, toujours dans le cadre espace-temps de sa mission.

Le spectre des informations d'environnement nécessaires dépend également du type de conflit dans lequel la force est engagée. En phase d'intervention dans un conflit symétrique ou dissymétrique, où l'important est de vaincre l'ennemi par la destruction de ses capacités militaires, les aspects socioculturels pourront avoir une importance limitée. En revanche, en phase de stabilisation ou lors d'opérations de contre-insurrection, l'objectif est d'apporter les conditions de la paix : ces aspects deviennent

57. Le *knowledge development* est défini comme un « processus collaboratif et itératif assurant la collecte de données et d'informations, leurs analyses et le partage des connaissances ainsi obtenues », cité in RDIA-004, *Knowledge Development*, CIDCE, Ministère de la Défense, juin 2010, p. 13.

58. *Ibid.*

59. RENS-60.001, *Méthode de renseignement des forces terrestres* (MRFT), Ministère de la Défense, Paris, 2014.

60. Pour l'armée américaine, FM 34-130, *IPB*, Department of the Army, Washington D.C., 1994.

alors cruciaux. Il est peu probable que le soldat américain, passant par Strasbourg en 1944, connaissait les subtilités des particularités culturelles alsaciennes et allemandes : elles n'étaient pas nécessaires à sa mission. En revanche, le soldat français de 2018 au Mali a impérativement besoin de connaître les usages, les moteurs et les ressorts des peuples au sein desquels il combat, et dont sont issus ses alliés comme son ennemi.

Les hypothèses de travail

Toute étude prospective se fonde sur des « hypothèses conditionnant la validité de la planification étudiée⁶¹ », sans lesquelles aucun raisonnement n'est possible. L'étude de l'ennemi n'échappe pas à la règle et implique des présuppositions liées à la nécessité d'anticipation : les plus communes sont la primauté du renseignement supérieur, le comportement rationnel des acteurs et la complémentarité des objectifs.

La primauté du renseignement supérieur n'est pas l'application d'un principe d'autorité ou de respect hiérarchique mais découle naturellement du mécanisme de la planification. En effet, celle-ci est amorcée suite à une directive du supérieur. De fait, en particulier aux niveaux opératifs et tactiques, le supérieur a toujours un temps d'avance sur la mission confiée à ses subordonnés. En principe, chaque échelon garde un tiers du temps utile (ou disponible) à sa propre planification, puis réserve les deux tiers restants à ses subordonnés. Si une division a trois jours pour planifier sa manœuvre, elle diffusera ses ordres à ses brigades au bout d'une journée, leur laissant deux jours pour établir leurs ordres⁶². Ainsi, lorsqu'un échelon entame l'étude de son ennemi, son supérieur y a déjà réfléchi, avec des moyens généralement plus performants. Voyant plus loin, mieux et ayant plus de temps pour l'analyse, le renseignement de niveau supérieur est donc considéré comme vrai *a priori*.

Ce partage des tâches ne dédouane toutefois pas le subordonné de ses propres responsabilités en matière de renseignement : il connaît généralement mieux son terrain et son environnement immédiat que son supérieur et peut donc étudier son ennemi avec une granularité beaucoup plus fine et surtout, adaptée au contexte de sa mission. Il peut également disposer, dans sa zone de responsabilité, d'informations capitales capables de remettre en question la perception de son chef. Ce principe général

61. DC-004, *Glossaire interarmées de terminologie opérationnelle*, Ministère de la Défense, Paris, juin 2015, p. 119.

62. Ce principe de planification est appelé la « règle du 1/3 temps », *Base documentaire tactique de l'école d'état-major*, Armée de Terre, Paris, 2016, p. 62.

impose donc de nombreux échanges au cours du processus qui assurent une convergence des vues entre supérieur et subordonnés.

De même, l'ennemi est par principe considéré comme rationnel, c'est-à-dire agissant conformément à ses intérêts. Il cherche à réaliser son objectif malgré l'action amie, en cherchant à minimiser les moyens requis et à maximiser ses profits. Au niveau stratégique, ce principe de rationalité guide la réflexion jusqu'aux conditions de la victoire, qui revient à « convaincre [l'ennemi] qu'engager ou poursuivre la lutte est inutile⁶³ ». Pour ce qui relève des opérations, l'ennemi est considéré comme n'étant ni suicidaire ni stupide. De sa description à la définition de son objectif, jusqu'à l'estimation de ses modes d'actions, tout est construit sur la présupposition d'un comportement rationnel. De ce principe découle celui de la complémentarité des objectifs, qui stipule que chaque acteur de niveau N-1 concourt à la réussite des acteurs du niveau N. C'est la raison pour laquelle, lorsqu'un subordonné évalue l'objectif que pourrait poursuivre son ennemi, il reprend généralement l'objectif ennemi retenu par son supérieur, mais en le déclinant à son propre cadre espace-temps et à sa mission. Ce postulat de rationalité des acteurs a bien sûr ses limites bien connues, dans le champ de la stratégie comme d'ailleurs dans celui des sciences économiques. En l'absence d'autre modèle systématique, il est pourtant encore un outil indispensable à l'anticipation et à la planification militaire.

Face à l'inconnu, partir du connu

Enfin, toutes les méthodes se rejoignent sur la nécessité de partir de ce que l'on sait pour en déduire ce que l'on ignore. Chaque élément d'information reçu ultérieurement vient alors amender la connaissance initiale pour relancer ce processus incrémental et cyclique. Or, grâce à la permanence du renseignement militaire, un certain nombre d'éléments sur l'ennemi sont déjà connus et servent de base de travail : ses forces disponibles, leurs capacités, leur doctrine et leur comportement habituel.

L'étude des forces en présence, caractérisées par l'ordre de bataille (ODB) de l'ennemi, fait partie des préalables indispensables. Ces tableaux, renseignés et mis à jour en permanence par le renseignement militaire, répertorient les éléments suivants : « identification, effectifs, structure de commandement et disposition du personnel, des unités et des matériels d'une force militaire⁶⁴ ». Dans le contexte d'un conflit interétatique, les

63. A. Beaufre, *Introduction à la Stratégie*, Paris, Armand Colin, 1963, p. 17.

64. DC-004, *Glossaire interarmées de terminologie opérationnelle*, Ministère de la Défense, Paris, juin 2015, p. 110.

ODB sont riches d'enseignement, et permettent bien souvent de définir et d'identifier toutes les unités adverses qui risquent de s'opposer à l'action amie dans le cadre espace-temps de la manœuvre. Dans le cas de conflits asymétriques, ils sont beaucoup plus difficiles à déterminer avant l'engagement, du fait d'alliances versatiles, des structures mouvantes et bien souvent clandestines.

La connaissance des moyens déployés par l'ennemi est tout aussi précieuse car en découlent non seulement ses possibilités d'action, mais aussi sa façon de manœuvrer, de s'organiser en vue de la bataille. Elle permet surtout d'estimer la capacité réelle de combat de l'ennemi : le volume et la qualité de son matériel, mais aussi le niveau de formation de son personnel, la disponibilité de ses équipements, etc. La connaissance de la portée de ses armes et de leurs effets va donner des indications importantes sur le déploiement de la force et la menace qu'elle représente. L'étude des moyens permet également de pondérer le rapport de force local, en ajoutant une dimension qualitative à la seule comparaison numérique⁶⁵.

L'étude de la doctrine permet en particulier d'anticiper l'action ennemie et d'avoir une bonne estimation des choix de l'adversaire en termes d'organisation. Certaines armées ont par exemple l'habitude de mutualiser leurs moyens en créant des unités interarmes voire interarmées⁶⁶, alors que d'autres y sont plus rétives. Sur le terrain, la doctrine peut également révéler les distances « normales » entre les unités (distance entre deux unités de même pied, ou entre les éléments de combat et les éléments d'appuis, etc.), ce qui permet de « tailler » l'ennemi dans le temps et l'espace, d'estimer son échelonnement. Ces éléments sont théoriques et il conviendra de les amender en fonction des choix effectifs de l'ennemi qui, lui aussi, s'adapte à la situation, au contexte et à la manœuvre adverse. Ils restent cependant de bons indicateurs sur la façon dont l'ennemi s'est entraîné, ce qui imprègne toujours en partie sa manœuvre.

Enfin, l'historique des comportements est aussi un élément fondamental, car il présuppose la répétition de certaines actions si l'ennemi est replacé dans les mêmes conditions. Pour cet aspect, l'étude de la personnalité du chef ennemi est capitale : une unité manœuvrant à l'image de son chef, percer le caractère du décideur peut être un excellent indicateur de sa manœuvre future. C'est entre autres par sa connaissance

65. Un rapport de force s'estime plus souvent localement : il s'agit de calculer, en un endroit à un moment donné, la supériorité numérique et matérielle théorique d'un camp sur l'autre.

66. C'est notamment le cas de l'armée de terre française qui, bien que s'étant organisée en « régiments » d'une seule arme ou spécialité en France, ne projette en opérations que des « groupements tactiques interarmes (GTIA) », des bataillons mixant plusieurs spécialités (infanterie, cavalerie, artillerie, etc.) pour en maximiser l'utilité et les potentialités d'emploi.

de l'esprit de l'Empereur que Jomini a pu efficacement conseiller les Alliés et participer à la victoire des coalisés sur Napoléon 1^{er}.

Des approches analytiques variées

L'étude de l'ennemi permet à l'état-major de définir la manœuvre future et d'envisager ses aménagements possibles : la connaissance n'a d'autres fins que l'action. Les évolutions méthodologiques liées à l'étude de l'ennemi ont par conséquent assez logiquement suivi celles des processus de planification opérationnelle⁶⁷, les deux démarches étant intimement liées. La modélisation de l'ennemi est de façon générale divisée en deux grandes étapes successives et complémentaires : la description d'une part (qui est-il, que veut-il), puis ses modes d'action (comment peut-il l'obtenir).

L'approche « classique » française était initialement très – voire exclusivement – déductive dans le volet descriptif de cette démarche (quantitatif, qualitatif, objectifs). Cependant, la réintégration dans le commandement intégré de l'OTAN⁶⁸ et la complexité accrue des conflits ont imposé peu à peu l'analyse systémique, qui a complété plutôt qu'elle n'a remplacé la précédente. Une différence de fond subsiste en revanche dans la façon d'anticiper les modes d'actions adverses : l'approche « par les possibles » reste très ancrée dans la culture militaire française, tandis que la méthode probabiliste est la norme au sein du reste de l'OTAN⁶⁹. Ces deux démarches dissemblables au sein de la même alliance révèlent une posture intellectuelle et un rapport à l'ennemi assez différents.

Description de l'ennemi : de l'approche déductive à l'analyse systémique

Née de la volonté d'aborder l'étude de l'ennemi de façon scientifique, l'approche classique repose essentiellement sur un raisonnement déductif. Celui-ci s'appuie sur le triptyque « constat – déduction – conclusion⁷⁰ » pour bâtir l'ensemble de l'analyse, lequel est suivi d'une synthèse générale permettant de caractériser l'ensemble de l'ennemi étudié.

67. La planification opérationnelle se définit comme une « Procédure formelle d'élaboration de la suite ordonnée des effets destinée à atteindre un état final recherché », *Glossaire interarmées de terminologie opérationnelle*, Ministère de la Défense, Paris, juin 2015, p. 116.

68. Décidée en 2007, votée le 17 mars 2009, elle est entérinée lors du sommet de l'OTAN des 3 et 4 avril 2009.

69. Cette approche a été consacrée par l'adoption de la *Comprehensive Operations Planning Process* (COPD) en 2010 comme méthode officielle de l'OTAN pour ce qui relève de la planification opérationnelle.

70. PIA-5(B), *Planification du niveau opératif : guide méthodologique*, Centre interarmées de concepts, doctrine et expérimentation, Ministère de la Défense, Paris, 2014.

Le constat s'appuie sur des faits observés ou reconnus, tels que des informations provenant de capteurs, qu'ils soient humains ou techniques. Il peut s'agir d'une unité décelée ou d'un élément de l'environnement qui a une incidence sur l'adversaire. La déduction reprend certains de ces constats et les associe pour en déterminer les conséquences ou les enseignements possibles dans le contexte espace-temps de la mission. La conclusion fait la synthèse des éléments utiles à la compréhension de l'ennemi parmi les déductions et permet de conclure sur des effets escomptés, les actions possibles, les besoins en information supplémentaires, des demandes, etc. L'ensemble « constat – déduction – conclusion » peut ainsi être représenté sous la forme d'un tableau :

Tableau analytique d'une approche déductive

Constat	Déduction	Conclusion
Unités ennemies décelées	Format probable de l'ennemi	Impératifs
Moyens détectés (type, volume et positions des aéronefs, navires, matériels divers, etc.)		
Capacités ennemies reconnues	Possibilités d'action	Demandes et besoins
Éléments particuliers d'environnement ayant une incidence sur l'ennemi (géographie, météorologie, population, etc.)	Conséquences diverses sur son organisation, ses besoins, ses forces et faiblesses	Conséquences sur l'action ennemie

Cette approche déductive est à la base des méthodes d'analyse et s'applique à toute réflexion d'un état-major, quel que soit le domaine. Pédagogique, elle part du connu et de l'objectif (le constat) pour estimer l'inconnu et le subjectif (les conclusions). En dissociant bien la typologie de chaque item, ce modèle est résilient aux évolutions. Toute erreur d'interprétation finale peut être révisée sans remettre en cause les observations initiales, mais toute modification d'un des constats initiaux oblige de revoir l'ensemble du processus d'analyse.

Ce genre de procédé simple et pragmatique convient parfaitement à l'étude d'un ennemi unique : il permet rapidement de déduire son volume, sa qualité, ses intentions estimées et ses modes d'actions probables. Cette démarche a cependant vite trouvé ses limites dans le cadre des situations complexes apportées par les conflits récents. L'étude de l'ennemi a alors été intégrée dans une analyse plus ouverte et globale en ayant recours à la science systémique⁷¹.

Reposant sur des principes développés dans les années 1970⁷², l'analyse systémique est arrivée récemment en France par l'intermédiaire des méthodes de planification de l'OTAN où elle était déjà employée⁷³. Cette approche vise à « identifier l'existence de systèmes adverses, leurs buts, leur organisation, leurs objectifs, leurs modes de fonctionnement, leurs forces et leurs faiblesses, en vue d'orienter la recherche et l'élaboration du renseignement⁷⁴ ». Elle se propose de pallier les lacunes d'une analyse purement déductive, notamment dans les environnements complexes, sans toutefois s'y substituer.

L'analyse systémique consiste à considérer chaque acteur d'un environnement donné comme un système : « un ensemble d'éléments en interaction dynamique, organisé en fonction d'un but⁷⁵ ». Chaque système étant relié à d'autres systèmes également par des liens à déterminer, cette approche permet de décrire l'ensemble d'un théâtre d'opérations comme un « système de systèmes » interactifs, où l'ennemi – lui-même décomposé, le cas échéant – n'est qu'un élément parmi d'autres.

L'analyse systémique étudie autant les acteurs que les interactions qui les relient. La notion d'acteur est à prendre ici au sens large et peut comprendre des personnes physiques (chefs rebelles, personnalités politiques influentes, chefs mafieux, etc.) des unités ou des groupes d'individus (groupe armé, ethnie, force militaire), ou même des personnes morales avec lesquelles l'ennemi peut avoir une relation particulière (entreprise, ONG, parti politique, etc.). Une fois les acteurs définis, il s'agit de les caractériser selon leurs facteurs internes (organisation, ressources, faiblesses structurelles), externes (pouvoir, objectifs, fragilités) et cognitifs (motivation, références culturelles, limites intellectuelles, etc.)⁷⁶. Les

71. DIA 01, *Doctrine d'emploi des forces*, Centre interarmées de concepts, doctrine et expérimentation, Ministère de la Défense, Paris, 2014, p. 17.

72. Lire les travaux de L. von Bertalanffy, *La théorie générale des systèmes*, New York, Georges Brazziller, 1968 ; J. de Rosnay, *Le macroscopie*, Paris, Seuil, 1975.

73. Et popularisée probablement grâce aux travaux du colonel américain J.A. Warden et sa théorie des 5 cercles, publiée dès 1995.

74. EMP 60.641, *Glossaire Français/Anglais de l'armée de Terre*, CDEC, Paris, 2013, p. 82.

75. RDIA-008, *Éléments d'analyse systémique pour la planification opérationnelle*, CICDE, Ministère de la Défense, Paris, 2012, p. 13.

76. *Ibid.*, p.21.

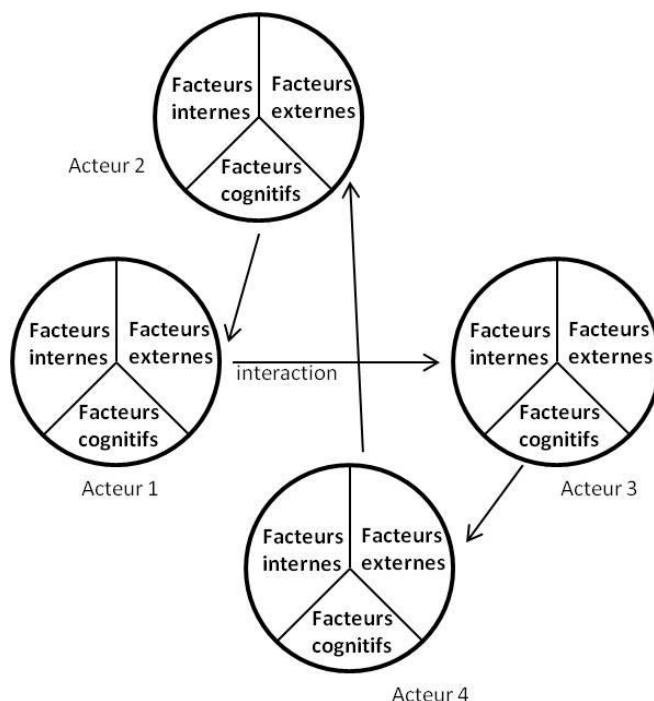
interactions, ces « actions réciproques qui se réalisent provoquant un changement d'état pour les deux entités⁷⁷ » sont alors déterminées pour étudier en quoi et par quoi ces acteurs sont reliés. Ces relations comportementales, physiques ou fonctionnelles peuvent être de toute nature : subordination, affective, intérêt, filiation, influence, etc.⁷⁸ Tous ces liens sont soumis au principe de rétroaction : toute relation d'un acteur A vers un acteur B suppose une relation inverse de B vers A (un lien de commandement suppose un lien de subordination, un corrompu suppose un corrupteur, un parent suppose un enfant, etc.).

Le système de systèmes ainsi construit, il sera généralement représenté sous la forme d'un schéma : les acteurs sont représentés comme des centres nodaux, unis par des flèches orientées représentant les interactions. Synthétisant l'ensemble du travail pour faciliter la compréhension de l'ennemi, cette représentation graphique a vocation à délivrer par elle-même des informations utiles qui vont au-delà de la somme des données collectées. Par exemple, des réseaux informels (avec des liens basés sur la filiation ou la tradition) peuvent apparaître qui transcendent, voire contredisent les organisations formelles (reposant sur la hiérarchie militaire). Parfois aussi, un acteur majeur peut être découvert grâce à une convergence d'interactions dans sa direction. Enfin, des relations indirectes peuvent être mises en évidence, comme dans le graphique 1 où, sans lien direct, voire sans qu'il en ait peut-être conscience, l'acteur 4 a une influence sur l'acteur 1 par l'intermédiaire de l'acteur 2. Ce type d'analyses se veut aussi incrémental et évolutif : le système doit être en permanence amendé et développé à chaque apparition d'un acteur ou d'une relation.

77. *Ibid.*, p.13.

78. Des listes non exhaustives ont été établies pour aider les états-majors à déterminer quels liens pouvaient exister entre des acteurs. Voir *Campaign Planification Handbook*, version DEEP, traduction OTAN, United States War College, Carlisle, 2016.

Graphique 1. Exemple d'analyse systémique



Par les apports qu'il apporte au développement de la connaissance, cet outil s'est peu à peu imposé au sein de l'OTAN, même en France où il figure en bonne place dans la méthodologie du renseignement⁷⁹. De fait, l'analyse systémique offre de nombreux compléments à une simple analyse déductive classique. Concernant l'ennemi, elle est particulièrement adaptée à l'étude d'acteurs protéiformes, sans organisation structurée, qui peuvent changer d'alliances ou de subordination selon les circonstances. Elle met en exergue les interactions, là où l'analyse déductive peine à les mettre en évidence. À ce titre, l'analyse systémique est particulièrement utile pour préparer l'utilisation efficiente de moyens autres que strictement militaires : la communication, les opérations d'influence, le cyber. En revanche, elle peut s'avérer très consommatrice de temps et de moyens car la perception des interactions humaines exige une connaissance en profondeur des acteurs. Comme cette approche ne considère aucune limite temporelle ou géographique, les possibilités d'extension d'un « système de systèmes » sont infinies et sa mise à jour doit être permanente. De fait, la tentation de sa représentation exhaustive peut devenir totalement confuse, donc inutilisable pour les besoins militaires. Ces schémas

79. RENS 60.001, *Méthode de renseignement des forces terrestres*, Tome 3, CEERAT, Ministère de la Défense, Paris, janvier 2015.

incompréhensibles⁸⁰, représentant une myriade d'acteurs, tous reliés les uns aux autres par des flèches enchevêtrées, sont qualifiés souvent de « bols de spaghetti » par les opérationnels. Enfin, « toute modélisation comporte inévitablement un biais⁸¹ » et celle-ci ne fait pas exception. Ces biais peuvent par exemple apparaître lors de la sélection des liens pertinents, ceux « qui [...] ont des répercussions directes ou indirectes sur le problème à résoudre⁸² », choix est souvent basé sur des critères éminemment subjectifs.

Si l'analyse systémique a démontré sa pertinence pour comprendre l'ennemi, cette méthode permet difficilement à elle seule une description pratique à vocation opérationnelle immédiate. Elle est donc appréciée voire devenue indispensable pour le *knowledge development* des niveaux stratégiques ou opératifs, où les états-majors ont les moyens, le temps et le recul pour s'y atteler. En revanche, au niveau tactique, la description de l'ennemi se fait généralement par une méthode déductive classique, du fait des délais d'anticipation réduits et du faible volume de personnel. Dans un environnement tactique complexe, l'enjeu est donc de faire bénéficier aux plus petits échelons de la connaissance développée par les niveaux supérieurs, sans entraver la capacité des subordonnés à peindre leur ennemi en les noyant dans une profusion d'informations inutiles.

Définir les modes d'action : approches probabiliste et possibiliste

Une fois l'ennemi modélisé et ses objectifs identifiés, des hypothèses concernant ses modes d'action sont formulées en vue d'en déduire la manœuvre amie la plus adéquate. Or, plus que dans la façon de décrire l'ennemi, c'est dans la façon d'appréhender ses modes d'actions que des dissonances apparaissent au sein de l'OTAN. L'alliance a opté depuis longtemps pour une approche probabiliste qui imprègne beaucoup sa méthodologie, dans ses analyses des risques et des menaces comme dans le cas particulier de la définition des modes d'action⁸³. La France, quant à elle, conserve une vision plus « possibiliste », qu'elle a réaffirmé en 2014, à la fois dans sa doctrine du renseignement et dans ses documents

80. Ce qui fera dire au général McChrystal en 2010, alors qu'on lui présentait l'analyse systémique de l'ennemi en Afghanistan : « quand nous comprendrons cette diapositive, nous aurons gagné la guerre. », cité in « US Generals Given Baffling PowerPoint Presentation to Try to Explain Afghanistan Mess », *Daily Mail*, 28 avril 2010.

81. RDIA-008, *Éléments d'analyse systémique pour la planification opérationnelle*, CICDE, Ministère de la Défense, Paris, 2012.

82. *Campaign Planification Handbook*, op. cit., p. 15.

83. *Comprehensive Operations Planning Directive* (COPD), Allied Command for Operations, 2010.

méthodologiques pour la conception opérationnelle⁸⁴. L'origine de cette différence est peut-être à rechercher dans la façon même d'aborder le renseignement militaire.

Dès les années trente, le colonel Bernis, stratège français et auteur d'un *Essai sur le renseignement à la guerre* évoquait ainsi deux écoles de pensées théorisées par, qui se seraient affrontées depuis le XIX^e siècle⁸⁵. L'École dite « des possibilités » est associée à Napoléon qui se méfiait d'un renseignement qu'il jugeait toujours prompt à confirmer la première impression. Cette approche recommande de « ne jamais chercher à imaginer ce que fera l'adversaire⁸⁶ », mais plutôt de se focaliser sur ce qui est à sa portée, étant donné ses moyens et sa situation. Il faut donc envisager toutes les hypothèses, les possibilités techniques et tactiques et orienter le renseignement en conséquence. À l'inverse, l'École « des intentions », que Bernis rattache au maréchal prussien Helmut von Moltke, consiste « à partir d'une situation [...] de la doctrine et des procédés [...], déterminer l'intention de l'adversaire et la manœuvre qu'il exécutera⁸⁷ ». L'idée est de concentrer les moyens sur quelques hypothèses, les plus probables uniquement, afin de « réduire le champ des possibles ». Chaque école possède ses avantages et ses faiblesses. La première est plus ouverte mais disperse ses ressources, la seconde rationalise ses moyens mais focalise la réflexion dans une direction très intuitive, voire arbitraire. Le parallèle avec les deux façons actuelles d'appréhender les modes d'actions ennemis est si flagrant qu'il est difficile de ne pas y voir une filiation.

L'OTAN en la matière a clairement une « approche probabiliste », peut-être liée à la vision de Moltke, mais en ayant pour partie corrigé les excès. Ce procédé consiste à concevoir un large panel de modes d'actions ennemis et à les classer selon deux critères : la probabilité et la dangerosité. Seuls le mode d'action le plus dangereux et celui le plus probable sont retenus pour être ultérieurement confrontés aux différentes options amies et déterminer ainsi la manœuvre la plus souhaitable. De façon quelque peu dogmatique, ce procédé exclut par construction que la plus probable des options puisse être également la plus dangereuse. Il est possible de modéliser cette approche selon une courbe des modes d'action ennemis (ME), fonction de la probabilité et de la dangerosité (graphique 2). Celle-ci ressemble alors à une branche d'hyperbole décroissante : les options à la fois improbables et inoffensives sont naturellement érudées.

84. CDT 60.001, *Méthodologie d'élaboration d'une décision opérationnelle tactique*, CDEF, armée de Terre, Ministère de la Défense, Paris, 2014.

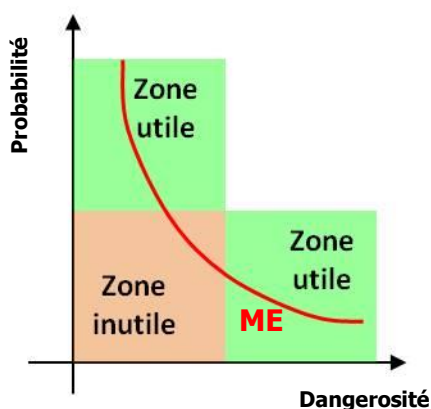
85. H. Coutau-Bégarie, « Le renseignement dans la pensée militaire française », *Stratégie*, n° 73, 1991, disponible sur : www.institut-strategie.fr.

86. *Ibid.*, p. 30.

87. *Ibid.*, p. 31.

Dans les faits, l'effort intellectuel est donc mis sur la recherche et le développement de l'option la plus probable. En pratique, le mode d'action le plus dangereux est souvent assez caricatural, prenant la forme d'un ennemi se jetant avec tous ses moyens et toute sa brutalité dans une opération quasi-suicidaire, mais destructrice. En partant d'une sélection de nombreuses hypothèses (la méthode en préconise au minimum trois) et en essayant de les classer selon des critères précis, cette approche évite l'écueil de Moltke qui se concentrait sur une seule option, celle qu'il jugeait la plus probable. Ce modèle en garde l'esprit, en essayant de deviner ce que l'adversaire va le plus logiquement faire pour y porter l'effort du renseignement. Enfin, le risque de « tunnellation » de l'école des intentions est pondéré par la détermination de l'hypothèse la plus dangereuse. Cette dernière sert avant tout à se prémunir d'une surprise opérationnelle : « même si le pire arrive, nous l'avons anticipé, et notre manœuvre reste tenable⁸⁸ ».

Graphique 2. Représentation des modes d'action ennemis (ME) étudiés selon l'approche OTAN

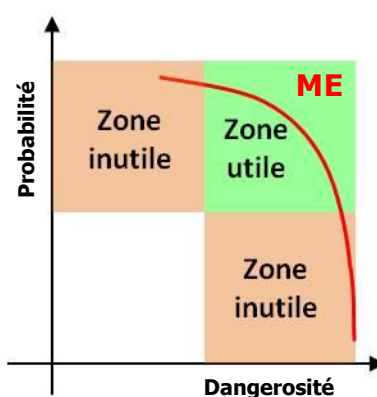


La doctrine française opte pour une approche dite « des possibles ». Tout comme la précédente, elle a également été adaptée pour en éviter les écueils. Dans cette démarche, il n'y a pas d'évaluation ni de distinction entre probabilité et dangérosité : deux et seulement deux modes d'actions sont déterminés qui doivent être à la fois probables et dangereux. Ils sont définis en essayant de se mettre à la place de l'ennemi, de manœuvrer comme lui à partir des éléments déterminés par l'étude préalable (capacités, doctrine, objectifs, etc.) et considérant l'environnement particulier. S'il fallait la représenter graphiquement, la courbe des modes

88. Entretien avec un officier américain en stage à l'école de guerre, octobre 2017.

d'action serait différente de l'approche OTAN (graphique 3). Le champ des hypothèses y est volontairement réduit : les plus probables non dangereuses ou les très dangereuses non probables ne sont pas étudiées pour des raisons pragmatiques. Dans le premier cas, une simple mesure en conduite permettra de faire face à la situation, mieux vaut donc se concentrer sur des hypothèses les plus dangereuses. Dans l'autre cas, l'improbabilité du scénario incite l'état-major à réserver ses ressources pour des cas plus réalistes. La difficulté de l'exercice est que ces deux modes d'action étudiés doivent également être suffisamment différenciés⁸⁹ pour permettre un véritable choix dans la manœuvre amie.

Graphique 3. Représentation des modes d'action ennemis (ME) étudiés selon l'approche française



En limitant le champ d'investigation à deux hypothèses crédibles, ce modèle cherche à compenser les inconvénients de l'école initiale en y insérant une dose d'intention. Elle en a surtout gardé l'esprit : l'ennemi est perçu comme imprévisible par nature. Les modes d'actions retenus par l'étude sont considérés comme probables, mais foncièrement incertains⁹⁰ : ils sont donc décrits de façon assez générale, peu précise et correspondent presque à deux « familles » de modes d'action possibles plutôt qu'à deux réelles hypothèses de manœuvre détaillées.

Ainsi donc, ces deux modèles analytiques ne sont pas seulement méthodologiques : ils révèlent une différence fondamentale dans la façon de « penser » la manœuvre de l'ennemi. La singularité du côté français est

89. Les modes d'actions ennemis doivent à la fois être suffisamment généraux pour être inclusifs et assez différenciés pour pouvoir être bien caractérisés et dissociés. Seules ces conditions permettent d'offrir au chef un choix net dans la manœuvre à adopter.

90. À ce titre, il est intéressant de noter qu'en France, l'usage du conditionnel est obligatoire dès lors qu'il est question de décrire l'ennemi dans les documents opérationnels.

d'adopter une démarche pragmatique, économisant les moyens et laissant plus de place à l'incertitude. C'est aussi révélateur d'une posture plus humble face à l'ennemi, considéré capable de conjuguer originalité et dangerosité.

Ces deux postures intellectuelles différentes sont lourdes de conséquences sur la conception de l'ennemi, comme sur l'orientation de la recherche du renseignement. Une approche probabiliste demande des moyens importants et de qualité. En effet, il faut qu'un « échantillon statistique » suffisant de modes d'action soit élaboré (ce qui nécessite du personnel) puis classé selon la probabilité et la dangerosité (ce qui pose la question des critères d'évaluation, de la disponibilité de moyens précis de renseignement et d'analyse, et des arguments pour justifier un tel classement). Enfin, pour que le mode d'action « le plus dangereux » ait une certaine pertinence, il faut que la force soit suffisamment robuste pour y faire face malgré tout, sans remettre fondamentalement en cause sa mission ou son intégrité. Cette méthode convient donc plutôt aux états-majors stratégiques et opératifs, ayant de grandes capacités ou des forces capables d'affronter le « pire » s'il advient. L'approche française, peut-être influencée par un manque chronique de moyens et quelques réticences quant aux attentes pouvant être nourries concernant le renseignement, cultive l'idée qu'il est impossible de savoir ce que va faire l'ennemi. Elle limite volontairement ses investigations à deux options, bien différentes mais crédibles, sur lesquelles construire une manœuvre par nature imparfaite. Elle demande donc initialement moins de moyens de recherche et d'analyse⁹¹. De fait, elle est bien adaptée aux états-majors opératifs et tactiques, aux capacités plus réduites.

L'approche française a la faiblesse d'ignorer les hypothèses hétérodoxes, ce qui l'expose potentiellement à une surprise tactique voire opérative. Ainsi, une attaque ennemie consistant à jeter toutes ses forces de façon inconsidérée, sur la ligne de défense principale et par l'axe d'approche le plus probable sera sûrement écartée de l'étude, car jugée trop irrationnelle. Pourtant, ce type de manœuvre peut potentiellement réussir par l'effet de surprise qu'elle peut générer. La démarche française toutefois accepte intellectuellement une incertitude supérieure quant aux intentions ennemies. En créant une culture de l'action dans l'inconnu, elle oblige et habitue l'état-major à une certaine réactivité face à une situation inattendue. Dans la culture OTAN, à l'inverse, le risque principal est la création d'un « effet tunnel » : l'ensemble des ressources cognitives des analystes peut se trouver focalisé sur l'hypothèse la plus probable, dans la

91. Ces moyens sont plutôt réservés pour la phase de conduite (non évoquée ici) où il faudra, pendant l'action, confirmer ou informer les hypothèses de manœuvre avant de relancer le processus pour l'action suivante.

mesure où elle est la seule crédible, et ne considérer la plus dangereuse que comme un exercice de pure forme. Sa capacité de réaction étant moindre en cas de mode d'action ennemi imprévu, l'état-major doit compenser par une connaissance supérieure de l'adversaire. De fait, l'approche probabiliste rend l'état-major structurellement plus dépendant du renseignement, et ce, dès le début de la planification. Si la démarche par « les possibles » fait de la résistance du fait de l'agilité intellectuelle qu'elle laisse aux opérationnels, l'approche probabiliste s'impose peu à peu et malgré tout en France, notamment au sein des états-majors interarmées ou interalliés par l'intermédiaire de l'OTAN⁹².

92. Notamment au sein du Commandement pour les opérations interalliées (CPOIA), état-major « référent opératif » français, qui ne dépend pourtant pas de l'OTAN.

Des approches traditionnelles bousculées ?

La révolution produite par l'introduction des technologies de l'information qui s'est opérée dans le renseignement pourrait être de nature à affecter certains principes sur lesquelles reposait la définition de l'ennemi. En effet, les nouvelles technologies qui se développent ou qui équipent déjà les armées occidentales augmentent non seulement la lisibilité du champ de bataille, mais permettront probablement demain de mieux anticiper les actions d'un acteur, en dépit de la nature éminemment humaine de sa décision ou des contre-mesures qu'il sera susceptible de mettre en œuvre. Mais ces évolutions ont aussi leurs limites et pourraient avoir des conséquences sur la subsidiarité et l'esprit d'anticipation qui prévalaient jusqu'à présent.

Un ennemi plus visible et prévisible ?

La révolution de l'information et la prise de conscience généralisée de l'importance du renseignement militaire⁹³ ont amené à un développement sans précédent de capteurs de plus en plus sophistiqués. À cette profusion de moyens s'ajoute une capacité accrue de fusion et de traitement automatisé des données permettant l'élaboration d'un renseignement d'une qualité jamais atteinte. Ce phénomène est tel que l'on évoque à nouveau une possible « transparence du champ de bataille⁹⁴ ». En outre, les progrès des sciences cognitives et le développement de l'intelligence artificielle permettent de mieux modéliser la pensée humaine, aussi les biais inhérents au facteur humain lors de l'analyse de l'ennemi pourraient demain être complètement pris en compte et corrigés, ce qui rendrait l'ennemi beaucoup plus prévisible qu'il ne l'est actuellement.

93. C'est ainsi la « connaissance et l'anticipation » a été consacrée comme une fonction stratégique à part entière dès le *Livre Blanc sur la Défense et la Sécurité nationale* de 2008, termes qui ont été repris dans les Livres Blancs suivants.

94. R. Hémez, « L'avenir de la surprise tactique à l'heure de la numérisation », *Focus stratégique*, n° 69, Ifri, 2016, p. 20.

Un développement sans précédent du renseignement militaire

La « révolution dans les affaires militaires » du début des années 1990 avait amorcé une transformation du monde du renseignement en développant de façon exponentielle le renseignement militaire ainsi que les moyens de surveillance et de ciblage (ISTAR), mis en réseau en « boucle courte⁹⁵ » avec les moyens de décision (C2) et de traitement (« *sensor-to-shooter* »)⁹⁶. L'accroissement généralisé des performances de ces systèmes d'armes est venu accentuer ce phénomène : l'ennemi est plus visible que jamais.

Les États poursuivent la quête d'acquisition de capteurs de plus en plus performants, ainsi que le confirme, pour la France, la loi de programmation militaire 2019-2025. Dans le domaine satellitaire, il est ainsi prévu de placer sur orbite les systèmes spatiaux CERES (ROEM) et CSO/MUSIS (ROIM). Ces derniers offriront une résolution inégalée (de l'ordre de 20 cm pour CSO-2), opéreront dans le spectre visible comme infrarouge, de jour comme de nuit, et seront manœuvrables⁹⁷. Dans le domaine aérien, le renseignement se généralise et se perfectionne, à la fois par l'arrivée de nouveaux matériels (remplacement des C-160 *Gabriel* par le système CUGÉ⁹⁸), la généralisation de la capacité reconnaissance sur les appareils de combat (tous les *Rafale* seront désormais capables d'emporter le pod RECO-NG) ou le développement des drones (dotation portée à 6 systèmes *Reaper* et développement du futur drone MALE européen⁹⁹).

De nouvelles technologies trouvent aussi des applications militaires comme la détection par LIDAR¹⁰⁰ qui permet des représentations en trois dimensions de zones survolées avec une précision de l'ordre de 10 cm en

95. Terme souvent employé pour désigner le raccourcissement extrême des délais de transmission entre acquisition et tir par tous les moyens possibles. La doctrine française ne définit toutefois que deux modes de mise en réseau senseur-effecteur : la liaison courte (subordination d'un moyen feu directement à un moyen de renseignement par l'intermédiaire d'un détachement de liaison) et la boucle rapide (automatisation des transmissions permettant à l'information issue de l'acquisition d'arriver le plus rapidement possible à l'effecteur, sans intervention humaine). ART 20.001, *Manuel d'emploi des formations d'artillerie sol-sol*, CDES/CREDAT, Paris, octobre 2001, p. 64-65.

96. J. Henrotin, « Les mutations du renseignement militaire », *Focus stratégique*, n° 71, Ifri, janvier 2007, p. 15-16.

97. *Gunter's Space Page*, 12 février 2018, disponible sur : space.skyrocket.de.

97. D'après le site du Centre national d'études spatiales (CNES), disponible sur : cso.cnes.fr.

98. *Charge universelle de guerre électronique* qui devrait être adaptée sur des appareils du type *Falcon* de Dassault.

99. Ce dernier sera développé conjointement par Airbus, Dassault Aviation et Leonardo. « Drone Male Rpas: les Images de la future arme autonome 100 % européenne », *Capital*, 4 mai 2018, disponible sur : www.capital.fr.

100. *Light Detection and Ranging*, qui utilise un faisceau laser pour mesurer les distances à la manière d'un radar. Voir sur ce sujet J. P. Morisseau, « La technologie LIDAR au service des forces armées », *Geospatial Intelligence*, 6 février 2017, disponible sur : geointblog.wordpress.com.

s'affranchissant de certaines couvertures (feuillage, bâches, filets, etc.). Le domaine terrestre n'est pas en reste de cette révolution informationnelle. Le programme Scorpion de l'armée de terre française prévoit en effet que tous les futurs blindés, depuis le véhicule de transport de troupe *Griffon* à l'engin de reconnaissance et de combat *Jaguar*, soient équipés d'alerteurs de désignation laser, de détecteurs acoustiques, et même de brouilleurs capables de rendre inopérants les engins explosifs commandés à distance. Chaque véhicule sera par ailleurs interconnecté pour que les détections de quelques-uns puissent servir automatiquement à l'ensemble de la troupe.

À une meilleure résolution des images fournies par les satellites, capteurs aériens ou terrestres, les progrès en matière de communication permettent la transmission de données volumineuses en temps quasi-réel. Ces éléments peuvent être recroisés avec ceux provenant d'autres capteurs, désormais joignables immédiatement malgré des distances plus grandes. Devenue possible, cette fusion des données permet d'obtenir du renseignement toujours plus fiable, et participe de l'émergence d'autres domaines de la spécialité comme le GEOINT¹⁰¹. Ce dernier s'est largement développé du fait de la généralisation de la géolocalisation satellitaire mais aussi par une fusion plus efficace des données, rendue possible par leur traitement informatisé apporté par des ordinateurs dont la puissance continue de progresser.

Enfin, ces informations plus précises, plus fiables, recoupées et synthétisées sont diffusées par les moyens de communication modernes vers les systèmes de commandement informatisés, équipant l'ensemble des forces. Ceux-ci disposent d'interfaces homme-machine conviviales, conçues pour permettre une compréhension rapide par les analystes, indispensable à une bonne prise de décision. C'est tout l'esprit qui guide le développement d'un système comme le Système d'information du combat Scorpion (SICS) en France¹⁰².

Du fait de ces progrès et de la banalisation des systèmes sur lesquels ils reposent, il n'est pas interdit d'envisager un ennemi dont la posture physique deviendrait quasi parfaitement lisible, du moins dans ses aspects quantitatifs et qualitatifs. Un tel champ de bataille ressemble dès lors à un vaste jeu d'échecs, où chaque joueur sait exactement où se situent les pièces de l'autre. Dans de telles conditions, l'effort des analystes devrait s'orienter davantage sur les intentions adverses : ce que veut l'ennemi et comment il compte l'obtenir.

101. *Geospatial Intelligence* – Renseignement d'origine géospatiale.

102. Entretien avec un officier de programme, Satory, octobre 2017.

L'intrusion de l'intelligence artificielle

Dans un espace de conflictualité où chaque acteur est visible de l'autre, le seul champ où le « brouillard de la guerre¹⁰³ » persiste encore, reste l'esprit humain : ce qui l'anime, ce qu'il espère, comment il va tenter de l'obtenir. Dans ce domaine, l'arrivée de l'intelligence artificielle (IA)¹⁰⁴ risque de modifier en profondeur la façon dont les analystes anticipent les intentions ennemies. En « réfléchissant » mieux et plus vite que tout un état-major réuni, en s'affranchissant des biais cognitifs qui « tunnellent » la réflexion, en intégrant la dimension humaine comme une donnée parmi d'autres, l'IA pourrait révolutionner l'analyse de l'ennemi en offrant au chef le mieux informé des avis pour éclairer sa décision : précis, exhaustif et objectif.

L'accroissement continu de la puissance de calcul a considérablement amélioré la rapidité de traitement de la masse des données générée par des capteurs toujours plus nombreux. Cependant, toute utilisation dans le contexte souhaité relève encore des hommes du renseignement. Face aux défis pour l'esprit humain que posent l'interprétation et la synthèse de cette « infobésité¹⁰⁵ », l'IA peut être une solution. En effet, les mécanismes d'apprentissage profond (*deep learning*¹⁰⁶) permettent de produire de la part de machines une réponse adaptée et inédite à une question complexe. C'est ainsi que le projet américain Maven (reconnaissance de formes) a été déployé en Syrie et en Iraq en janvier 2018¹⁰⁷ pour analyser automatiquement les milliers d'heures de vidéos filmées par les centaines de drones déployés dans la région à la recherche de systèmes d'armes – permettant ainsi l'exploitation de films dont la plupart n'étaient jamais visionnés faute d'analystes. Un autre exemple d'application est l'imagerie spatiale. En juin 2017, Robert Cardillo, directeur d'une agence américaine de renseignement géospatial affirmait que pour exploiter « manuellement » toutes les images satellites auxquelles son agence aurait accès au cours des 20 prochaines années, il lui faudrait embaucher huit millions d'analystes image¹⁰⁸.

103. C. von Clausewitz, *De la Guerre*, Paris, Perrin, 1999, p. 101.

104. « Ensemble de théories et de techniques mises en œuvre en vue de réaliser des machines capables de simuler l'intelligence », *Encyclopédie Larousse*.

105. Mot dont l'invention est attribuée à David Shenk en 1993. Ce terme désigne l'excès de « masse grasse formée par le bombardement d'informations qui étouffe nos processus intellectuels », cité in C. Sauvajol-Rialland, *Infobésité : comprendre et maîtriser la déferlante d'informations*, Paris, Éditions Vuibert, 2013.

106. Dans le domaine de l'IA, on distingue le « *machine learning* » (la capacité pour une machine d'apprendre seule à partir d'une base de données servant d'exemple et en permanence réalimentée) du « *deep learning* » (qui dispose de la capacité supplémentaire d'apprendre sur la base de l'expérience des échecs et des succès précédents).

107. « Drones et intelligence artificielle », *TTU*, n° 1091 du 10 janvier 2018, p. 5.

108. « Le renseignement américain mise sur l'intelligence artificielle », *France Soir*, 10 septembre 2017.

De telles machines seraient débarrassées des biais cognitifs (sensoriels, émotionnels, etc.) bien ancrés dans la nature humaine. Il suffirait d'entrer l'ensemble des données collectées sur un ennemi (organisation, capacités, actions précédentes, personnalité de ses chefs, données historiques et d'environnement, etc.) pour que de solides hypothèses quant à ses intentions les plus probables soient formulées, sans être polluées par l'affect ou les aspects socioculturels des analystes. En plus de permettre de s'affranchir des biais internes, et en admettant qu'il soit possible à terme de cartographier la pensée humaine, l'intelligence artificielle pourrait demain intégrer la personnalité de l'ennemi comme une donnée ordinaire et ainsi estimer ses modes d'action avec encore plus de fiabilité.

Ainsi, les avancées technologiques dans le domaine de l'IA permettront peut-être demain de s'affranchir du facteur humain qui est la principale cause de l'incertitude de l'action ennemie. Ces évolutions sont d'autant plus crédibles si on considère l'apport significatif des sciences cognitives au renseignement.

L'apport des sciences cognitives

Si leur origine peut remonter au moins à la philosophie des Lumières, les sciences cognitives se sont surtout développées depuis les années 1950 et ont connu récemment une avancée fulgurante du fait du développement de l'informatique et de l'imagerie médicale. Celle-ci pour objet « de décrire, d'expliquer et le cas échéant de simuler voire d'amplifier les principales dispositions et capacités de l'esprit humain – langage, raisonnement, perception, coordination motrice, planification, décision, émotion, conscience, culture, etc.¹⁰⁹ » Au croisement de plusieurs disciplines comme la philosophie, la psychologie, l'anthropologie, la neurologie ou encore la robotique, leur adaptation au domaine militaire offre des perspectives prometteuses pour l'analyse de l'ennemi.

Une étude récente du Centre de Doctrine et d'Enseignement au Combat estime ainsi que, prises en compte par l'état-major ou la cellule de renseignement, les sciences cognitives pourraient permettre de mieux comprendre les constructions intellectuelles qui ont débouché sur la définition de l'ennemi et ainsi identifier les biais humains¹¹⁰. Analystes comme décideurs prenant conscience de leurs propres biais cognitifs, ces

109. D. Andler, « Cognitives Sciences », *Encyclopædia Universalis*, 1989, disponible sur : www.universalis.fr.

110. L. G. Larchet, A. Sennyey et A. Leboeuf, « Les sciences cognitives et l'organisation des postes de commandement », *Lettre de la prospective* n° 1, CDEC, mai 2017.

travers peuvent être corrigés pour arriver à un travail plus objectif, basé sur des arguments scientifiquement démontrés plus que sur des impressions.

Les sciences cognitives cherchent en parallèle l'amélioration des capacités humaines. Ce domaine particulier comporte des techniques pour certaines déjà connues (pharmacopée, thérapie comportementale) qui ont pour objet de faire progresser l'Homme « en lucidité (contre la fatigue, le stress) et en efficacité (rapidité, complexité)¹¹¹ » et qui, rapportées à l'étude de l'ennemi, permettraient d'augmenter l'objectivité et la rapidité de travail des analystes du renseignement et de leurs chefs.

Par extrapolation, il sera alors possible de décrypter les mécanismes de la pensée dans l'état-major adverse. Les modes d'actions ennemis ne seront plus alors construits sur la seule présupposition d'un comportement rationnel, mais en tenant compte de toutes les informations cognitives recueillies : caractère de chaque intervenant, émotions dominantes, humeur du décideur. Cependant, même si la connaissance du fonctionnement du cerveau humain progresse chaque jour, une modélisation parfaite de ces aspects plus liés à l'émotivité et à la subjectivité semble, pour le moment, assez hypothétique¹¹².

Domaine en plein essor, se nourrissant réciproquement des progrès de l'intelligence artificielle, les sciences cognitives ont vocation à rendre l'ennemi plus prévisible dans ses intentions et ses actions. Toutefois, sans attendre l'arrivée de ces nouvelles technologies, les armées ont déjà développé des moyens, techniques ou procédés novateurs participant à la modélisation de l'ennemi.

De la simulation au « Red teaming »

« À la guerre il n'y a pas de meilleur professeur que l'ennemi, mais ses leçons coûtent cher¹¹³ ». Parce que les armées ne peuvent pas attendre la confrontation pour s'assurer de la justesse de leur appréciation sur l'ennemi, la plupart des forces occidentales se sont dotées de moyens de simulation. Ces systèmes, centres ou procédés ont vocation à créer une altérité artificielle la plus réaliste possible afin d'acquérir de l'expérience sans combat, de développer la connaissance de l'ennemi en son absence.

Initialement cantonnée à l'apprentissage de techniques individuelles (pilotage, utilisation d'un système d'armes, etc.), la simulation bénéficie

111. *Ibid.*, p. 14.

112. *Ibid.*, p. 8.

113. Propos attribués au général Moltke, in J.-M. Marril, « L'offensive à outrance : une doctrine unanimement partagée par les grandes puissances militaires en 1914 », *Revue historique des armées*, n° 274, 2014, p. 2.

depuis les années 1990 de l'essor de l'informatique pour gagner en possibilités. On la classe généralement en fonction du degré de simulation de l'environnement¹¹⁴ :

- La simulation virtuelle, où le système d'armes est reproduit à l'identique mais l'environnement tout comme l'ennemi est virtuel. Ce type de simulation est surtout destiné à l'apprentissage ou l'entraînement pratique (simulateur de pilotage d'engin blindé ou d'aéronef).
- La simulation constructive, où le combattant fait face à un avatar d'ennemi, réalisé par un programme informatique qui agit selon une doctrine définie. Les systèmes d'armes sont simulés et l'environnement est virtuel.
- La simulation vivante¹¹⁵, dans laquelle les hommes, le matériel et l'environnement sont réels et où seuls les effets des armes sont simulés.

Les deux derniers types de simulation se prêtent particulièrement au développement de la connaissance de l'ennemi. En particulier, la simulation constructive participe à l'entraînement des états-majors. Dans ces centres spécialisés¹¹⁶, face à un ennemi artificiel animé par ordinateur¹¹⁷, le B2 s'entraîne à déceler sa présence, à estimer son volume et ses moyens, à imaginer ses modes d'actions, etc. L'ensemble du cycle du renseignement est déroulé au cours d'affrontements virtuels parfaitement inoffensifs. La pratique s'est généralisée tant pour la préparation aux opérations que pour la formation : les états-majors opérationnels français sont évalués annuellement avec ce type d'outils, et c'est sur ce type de simulateur que les stagiaires de l'École de Guerre effectuent leur exercice de fin d'études.

Car l'appui aux opérations (AAO) est une mission à part entière de la simulation¹¹⁸. En effet, une bonne connaissance d'un adversaire peut être développée car l'ennemi simulé est paramétrable en grande partie (nature, volume, équipement¹¹⁹, etc.). Un état-major partant en opération peut ainsi

114. RDIA 2015/02, *Simulation en appui à l'engagement opérationnel des armées*, Centre interarmées des concepts, doctrines et expérimentations, Ministère de la Défense, Paris, 2015.

115. Également appelée « embarquée » ou « instrumentée » selon le niveau d'intégration de simulation. Voir *Ibid*, p. 28.

116. En France, c'est la vocation du Centre d'entraînement des postes de commandement (CEPC) à Mailly-le-camp. Les écoles militaires de Paris et de Saumur disposent également de centres de simulation de ce type.

117. En France, avec des plateformes de simulation telles que JANUS ou SOULT.

118. Entretien avec un officier de la division simulation et numérisation des espaces de bataille (NEB), Écoles militaires de Saumur, janvier 2018.

119. L'ordre de bataille de l'ennemi, son organisation et ses équipements sont définis préalablement au « jeu » de simulation. Les équipements font partie d'une vaste base de données reprenant la plupart des matériels actuellement en service dans les armées.

se préparer à affronter son futur adversaire : le système pouvant générer un ennemi symétrique aux réactions rationnelles et conformes à une doctrine paramétrée, ou bien des combattants asymétriques (des animateurs humains devront alors décider des actions ennemies). Par le truchement de la simulation, avant l'affrontement, la façon de combattre de l'ennemi peut être déjà – pour partie – connue¹²⁰.

Mais c'est en cas de conflit relativement long, que l'AOO trouve sa pleine pertinence : chaque retour d'expérience sur le terrain permet alors de nourrir et d'affiner la simulation pour la rendre toujours plus réaliste, et mieux préparer les futures troupes à partir. En temps de paix, les hypothèses d'entrée sur l'ennemi demeurent en revanche assez théoriques, même si elles peuvent être établies sur la base de données fournies par les services de renseignement militaire qui tiennent à jour les ordres de bataille et entretiennent les connaissances sur les adversaires potentiels.

À des niveaux plus tactiques, la simulation vivante ou instrumentée permet aux unités plus modestes de se préparer à un ennemi « humain ». Des centres d'entraînement donnent ainsi la possibilité à une unité partant en opération de se confronter à d'autres militaires qui vont manœuvrer contre elle. L'effet des armes est simulé grâce à des lasers placés sur les canons des armes et les vêtements des soldats pour plus de réalisme. Parfois, le « plastron » est même composé de soldats permanents affectés à cette tâche, comme c'est le cas en France, où le centre d'entraînement aux actions en zone urbaine (CENZUB) de Sissonne, dispose de forces adverses (FORAD) en propre. En appliquant les procédés connus de l'ennemi (à partir des retours d'expérience des opérations) et en expérimentant des modes d'actions innovants, ces unités alimentent la réflexion sur les tactiques que l'ennemi pourrait employer et donc sur les pratiques permettant de les contrer. À ce titre, le CENZUB dispose d'un centre études et prospective qui est associé à la recherche doctrinale française¹²¹.

D'autres procédés sont plus orientés vers la performance du cycle décisionnel, notamment aux échelons supérieurs du commandement, c'est le cas du *Red teaming*¹²². Initialement venue des États-Unis et passée par l'OTAN, cette pratique a connu un réel essor depuis les années 2000¹²³.

120. Dans le cadre de leur mission « préparation de l'avenir (PDA) » ces centres sont utilisés pour tester les premiers éléments de la doctrine SCORPION, sur ce point lire « Quand les écoles militaires de Saumur simulent », Armée de Terre, 29 mars 2016, disponible sur : www.defense.gouv.fr.

121. Entretien avec un officier du CENZUB, janvier 2018.

122. L'OTAN reconnaît depuis 2012 la terminologie *Alternative analysis* (Alta) : « deliberate application of independent critical thought and alternative perspectives to improve decision making » et a récemment réédité son manuel : *The NATO Alternative Analysis Handbook*, OTAN, décembre 2017.

123. M. Zenko, *Red Team: How to Succeed by Thinking Like the Enemy*, New York, Basic Books, 2015.

Le principe est de créer une cellule d'experts, spécialement dédiée à la critique objective, rigoureuse et en toute indépendance des conclusions, des hypothèses, des idées ou des plans d'une organisation¹²⁴ afin de tester sa production ou de lutter contre ses principaux biais (biais de conformité en particulier). Le champ d'action d'une *Red team* s'étend normalement à toutes les activités de production de l'état-major, elle n'est donc pas ordinairement chargée de l'étude de l'ennemi. Pourtant, son appui peut être particulièrement utile au B2 dans la phase de définition des modes d'action adverses : la *Red Team* apporte un regard extérieur qui permet de confronter les hypothèses définies par les spécialistes à des critères exogènes.

Parce que ce procédé permet de décloisonner le raisonnement et de lutter contre la tunnellisation de la pensée, les militaires américains ont spécialisé certains de leurs cadres dans ce domaine, en créant en 2004 un cursus de formation *ad hoc*¹²⁵. Les Britanniques intègrent pour leur part le *Red teaming* dans le processus de validation des hypothèses sur l'ennemi, essentiellement au niveau opératif¹²⁶. En France, le procédé reste très marginal et bien souvent inconnu. D'une part, la tendance est à la réduction du volume de spécialistes dans les états-majors, mais surtout, le concept peine à convaincre dans l'hexagone où il est jugé accessoire. Si le *Red teaming* est globalement jugé utile dans les organisations à la hiérarchie très stricte et formelle, l'esprit « grognard » français, allié à un style de commandement plus souple sont supposés garantir que les individualités qui seraient opposées à l'orientation suivie par le groupe oseront toujours s'exprimer, même devant le chef¹²⁷.

Ainsi, que ce soit par les nouvelles technologies, par les progrès scientifiques, par l'amélioration de procédés existants ou par la création de nouvelles fonctionnalités au sein des organes de commandement, l'étude de l'ennemi connaît des avancées significatives. Mais les limites inhérentes à ces approches perdurent, et ne seront pas sans implication dans la façon même de concevoir l'ennemi.

124. D'après *Red Teaming Guide (2nd edition)*, Development, Concepts and Doctrine Center, Ministère de la Défense, Shrivenham, Royaume-Uni, 2013.

125. Au sein de l'*University of Foreign Military and Cultural Studies (UFMCS)*, Fort Leavenworth, Kansas, USA.

126. JDP 2.00, *Understanding and Intelligence Support to Joint Operations*, Ministère de la Défense, Shrivenham, Royaume-Uni, 2011.

127. Entretien avec un officier supérieur de l'armée de Terre, Paris, décembre 2017.

Penser « rouge » : limites et implications

Les progrès réalisés ou prévisibles dans le domaine de la modélisation de l'ennemi laissent envisager un contexte opérationnel où la connaissance réciproque serait la norme. Comme lors des combats médiévaux en champ clos, rien de l'ennemi ne serait plus ignoré, pas même ses intentions ou ses procédés. Pourtant, des limites indépassables viennent relativiser cette dissipation annoncée du « brouillard de la guerre ». La plupart des approches anticipent par hypothèse des comportements rationnels des acteurs, qui plus est avec une définition restrictive de la rationalité, ce qui est loin d'être toujours le cas à la guerre. De plus, ces outils de compréhension de l'ennemi peuvent parfois être influencés par la subjectivité des concepteurs et programmeurs, eux-mêmes soumis aux biais cognitifs. Ainsi, l'impression d'une totale lisibilité de l'adversaire pourrait avoir des conséquences sur certains fondamentaux liés à la perception de l'ennemi. En déniaient à chaque échelon la liberté de choisir son ennemi, des risques sur la capacité d'anticipation des unités subordonnées peuvent apparaître.

La modélisation de l'irrationnel et le remplacement de l'altérité

L'un des principes communs à toutes les approches de la définition de l'ennemi repose sur la rationalité des acteurs. Pour prévoir ses objectifs et ses modes d'actions, l'ennemi est présumé agir conformément à ses intérêts. Or le combattant n'a pas toujours, loin s'en faut, un comportement rationnel. Les facteurs psychologiques, les forces morales¹²⁸, la pression liée aux enjeux ou tout simplement la peur de la mort influencent les actions sans qu'il soit toujours possible de le prévoir. L'histoire militaire est riche de ces mouvements incompréhensibles liés à l'instabilité des hommes, comme la panique de Bulson, le 13 mai 1940, qui participa à la retraite de la 55^e division d'infanterie gardant la Meuse ou bien l'atermoisement salubre d'Hitler entre le 24 et le 26 mai, lors de l'offensive sur Dunkerque, qui permet le rembarquement des Franco-Britanniques¹²⁹. Rappelons aussi que l'ennemi peut choisir d'opter pour des modes d'actions irrationnels, par

128. « Les forces morales entrent pour les trois quarts dans le résultat final ; les forces numériques et matérielles n'y comptent que pour un quart. Le moral et l'opinion font plus que la moitié de la réalité », Napoléon Bonaparte.

129. K.-H. Frieser, *Le mythe de la guerre-éclair, la campagne de l'Ouest de 1940*, Paris, Belin, 2003.

exemple dans le cadre d'une opération de déception, afin de créer la surprise¹³⁰.

Dans un autre registre, le comportement d'acteurs asymétriques tels que les terroristes, pose parfois de réelles difficultés d'anticipation, car reposant essentiellement sur des rationalités particulières (dévotion à la famille, spiritualité, code de l'honneur, etc.), qu'un analyste étranger peine à comprendre. La logique d'action qui fait foi habituellement – celle d'une opération ennemie conçue pour atteindre un objectif servant des intérêts – n'est pas toujours applicable au terrorisme. Ceci brouille tout spécialement les perceptions des militaires occidentaux, formés selon les principes de la guerre en vigueur dans leur pays¹³¹. Imaginer l'impensable, quand ce n'est pas prévoir l'absurde, est conceptuellement difficile, ardu à modéliser, et donc bien souvent imprédictible.

L'étude psycho-cognitive des acteurs et l'historique comportemental peuvent aider à anticiper ces phénomènes, et de nombreuses études civiles¹³² comme militaires pensent recourir à l'intelligence artificielle pour prévoir les comportements. Toutefois, du point de vue des forces armées, les résultats ne sont pas tous probants¹³³ : les évaluations des émotions ou des intentions reposent sur des critères comportementaux qui sont difficiles à déterminer. Mais c'est surtout l'irrationalité humaine, le comportement pulsionnel, qui reste encore très difficile à modéliser et donc à prévoir.

Par ailleurs, est-il réellement possible de modéliser parfaitement l'altérité ? La simulation de l'altérité est bien souvent limitée par les développeurs eux-mêmes, qui peuvent difficilement éviter d'imprégner de leur propre subjectivité les systèmes de simulation de l'ennemi qu'ils conçoivent. La recherche scientifique comme la création technologique étant elle aussi une activité humaine, la simulation comporte des limites intrinsèques. Se pose en effet la question de la capacité des programmeurs à développer des outils de simulation ou d'évaluation de l'ennemi, sans être biaisés par leurs propres structures organisationnelles ou mentales. C'est

130. R. Hémez, « Opérations de déception. Repenser la ruse au XXI^e siècle », *Focus stratégique*, n° 81, Ifri, juin 2018.

131. En France par exemple, sont enseignés les principes de la guerre de Foch : liberté d'action, économie des moyens, concentration des efforts. Toute évaluation d'une opération tient compte de ces principes, qui ne sont pourtant pas toujours applicables à l'action terroriste.

132. Notamment pour anticiper les comportements liés à la consommation des individus ou des ménages.

133. On pense à l'IA (*machine learning*) *Skynet* de la NSA, utilisée au Pakistan à partir de 2007 sur 55 millions de personnes, qui a classé comme terroristes des milliers d'innocents, dont la plupart des taxis de la région étudiée et un célèbre journaliste d'investigation. Leur comportement hors normes les rendait suspects selon l'algorithme de la machine (séminaire IA de l'Ifri, 28 septembre 2017). Voir aussi C. Grothoff et J. M. Porup, « The NSA's SKYNET Program May Be Killing Thousands of Innocent People », *Ars technica*, 2 février 2016, disponible sur : arstechnica.com.

notamment le cas pour les plateformes techniques de simulation. Les données qui les alimentent (les capacités des matériels par exemple) sont habituellement fournies par les armées ou des industriels : si elles sont initialement faussées, le système entier sera biaisé d'entrée de jeu. Ainsi, il est fréquent qu'à l'occasion d'exercices, des militaires constatent que certains matériels virtuels sont rendus beaucoup plus puissants, ou au contraire nettement plus vulnérables qu'ils ne le sont en réalité. L'influence nationale semble jouer : si les matériels français sont particulièrement performants sur les simulateurs nourris par des bases de données françaises, certains matériels américains sont parfois invulnérables dans les simulateurs développés par les États-Unis¹³⁴.

La simulation vivante n'est pas épargnée par ces limites conceptuelles. Ainsi un soldat, formé selon les critères de son pays pourra avoir du mal à simuler le comportement d'un soldat ennemi, dont la formation, la culture, les schémas mentaux diffèrent. Il est possible de se rapprocher le plus possible de l'altérité avec des troupes exclusivement dédiées à l'activité de FORAD, en les séparant et les distinguant des troupes ordinaires de façon à réduire au maximum la reproduction de schémas connus. Cependant, la pression opérationnelle sur les armées et la nécessité d'assurer un cursus de carrière équitable et attractif pour tous les soldats font que ce type de mission est de plus en plus assuré par des unités tournantes, ou ayant une autre fonction opérationnelle¹³⁵. Le « plastronnage » n'étant plus assuré par des spécialistes mais par des nationaux formés aux mêmes techniques et tactiques que les soldats qui s'entraînent, la simulation de l'altérité peut sembler par trop incomplète.

Ainsi, du fait de l'irrationalité humaine et de la part de subjectivité inévitablement insérée dans les outils de simulation ou lors d'exercices, il est encore difficile de considérer que l'on puisse parfaitement combattre, réagir, penser à la place de l'ennemi. La confrontation avec l'adversaire reste le meilleur des apprentissages.

Moins d'initiative et de subsidiarité ?

Les évolutions scientifiques et technologiques permettront sans doute une meilleure lisibilité de la menace et une plus grande anticipation des comportements adverses, même si certaines incertitudes perdureront

134. Expérience personnelle du rédacteur appuyée par des entretiens avec plusieurs officiers de la section technique de l'armée de Terre de Satory et des écoles militaires de Saumur, septembre 2017 - février 2018.

135. C'est ainsi qu'en France, la mission de Force Adverse du CENTAC est assurée depuis 2016 par des unités du 5^e régiment de Dragons, un régiment qui participe également aux missions habituelles des forces terrestres.

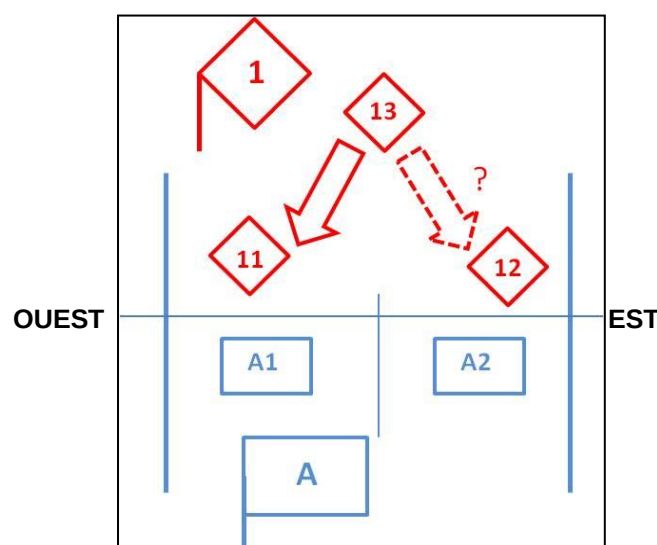
toujours. Sans affirmer que le « brouillard de la guerre » sera complètement dissipé, l'ennemi sera probablement plus transparent, plus prévisible qu'il ne le fut depuis bien longtemps.

Cette situation ne manquera pas d'avoir des conséquences sur les principes mêmes de la modélisation de l'ennemi qui prévalaient jusqu'alors. En particulier, la subsidiarité permettant à chaque échelon de décliner son propre ennemi pourrait à terme être largement remise en cause. Dès lors, c'est peut-être toute la capacité d'anticipation des unités qui pourraient en pâtir. Maintenue par la technique dans l'illusion de la certitude, leur faculté d'envisager l'impensable, donc de réagir à la surprise, pourrait être compromise.

La subsidiarité est l'un des principes fondateurs de la définition de l'ennemi : chaque subordonné décline son ennemi à son niveau, en fonction des éléments donnés par son chef, de ses propres collectes et évaluations. Cette liberté traditionnellement accordée permet non seulement d'entretenir l'agilité intellectuelle des subordonnés mais offre surtout un moyen efficace de se prémunir de la surprise.

L'exemple suivant illustre cette idée (graphique 4) : l'unité A (composée de deux unités subordonnées, A1 et A2) est confrontée à une attaque de l'unité ennemie 1 (avec trois unités subordonnées 11, 12, et 13). L'estimation de A est que 11 se dirige vers A1 et que 12 se dirige vers A2. 13 devrait appuyer 11 dans son attaque, mais il n'est pas exclu qu'elle passe dans le « fuseau Est » et vienne finalement soutenir 12. L'unité A doute des intentions ennemies mais son volume est clair : elle sera confrontée à 3 sous-unités (11, 12 et 13).

Graphique 4. Illustration du principe du choix de l'ennemi



En revanche, la situation est différente pour A1 et A2. Chacune de ces unités va non seulement anticiper l'attaque de l'ennemi « assuré » dans son fuseau, mais également envisager l'arrivée de 13, même si ce n'est pas certain. Pour prévenir toute surprise A2 adopte l'hypothèse « la plus dangereuse », ce qui permet d'écrire, si l'on synthétise l'ennemi étudié par chaque élément de la zone d'action :

- Ennemi de A1 = 11 + 13 soient 2 sous-unités ennemies ;
- Ennemi de A2 = 12 + 13 soient 2 sous-unités ennemies ;
- Ennemi de A = 11 + 12 + 13 soient 3 sous-unités ennemies.

L'indétermination sur l'action ennemie fait que la somme des ennemis des subordonnés (ennemi de A1 + ennemi de A2 = 4 sous-unités) est supérieure à l'ennemi total présent (3).

Ce phénomène bien connu des tacticiens n'est pas sans poser quelques problèmes : A recevra de ses subordonnés autant de demandes d'information et de soutien que s'il y avait 4 sous-unités présentes dans la zone au lieu de 3. L'unité A devra donc faire des choix et définir dans quel fuseau faire l'effort. Cependant, cette subsidiarité laissée à ses subordonnés pour décrire leur ennemi permet d'éviter à A2 d'être prise au dépourvu si jamais 13 décide finalement de basculer dans le fuseau Est, même si ce n'était pas l'hypothèse la plus probable. L'entretien de l'incertitude permet donc d'imaginer tous les possibles et évite ainsi l'effet de surprise.

Cependant, ce principe de subsidiarité est mis à mal à la fois par les nouvelles techniques mais aussi par les modèles « otaniens » de conception des modes d'action. Avec un meilleur renseignement, une analyse plus efficace et plus rapide, une transmission plus élaborée et en temps quasi-réel, les nouveaux et futurs moyens de modélisation optimiseront le cycle du renseignement militaire au point de délivrer à chaque échelon toute l'information nécessaire à la définition de son ennemi. Anticipant l'infovalorisation¹³⁶ des forces, les prospectives doctrinales envisagent déjà cette notion de « situation partagée¹³⁷ », où l'ensemble des informations disponibles sur l'ennemi serait, une fois validé, mis en commun au sein du « système de combat » qu'est devenue une force en opération. Si cette tendance peut apporter de réelles plus-values en termes de réactivité, elle pose question sur l'avenir du principe de libre choix de l'ennemi en anticipation.

136. L'infovalorisation est définie comme « l'exploitation de la valeur ajoutée apportée par les ressources informationnelles permises par les nouvelles technologies de l'information et de la communication pour améliorer l'efficacité opérationnelle », RFT 3221/4, *Doctrines exploratoire Scorpion*, CDEC, Ministère des Armées, Paris, 2017, p. 13.

137. *Ibid.*, p. 14.

Si l'on reprend l'exemple précédent mais en considérant une parfaite transparence du champ de bataille, l'unité A fixerait le volume de l'ennemi à ses subordonnés. Il est probable alors qu'A2 ne se préoccupe que de sa menace immédiate, c'est-à-dire 12. Les demandes et besoins exprimés vers A seront beaucoup plus conformes à la réalité de la menace (3 sous-unités réelles au total et non pas 4 théoriques), permettant sûrement une meilleure économie des moyens et une plus grande rapidité de réaction (la position de 13 sera suivie en permanence, permettant de s'assurer de ses intentions et confirmer les hypothèses envisagées).

En revanche, les conséquences seraient désastreuses en cas de surprise opérative ou tactique, qu'elle soit liée à la déception de l'ennemi, la défaillance provoquée ou technique des systèmes ou des analystes amis. En cas d'arrivée brutale et imprévue de 13 dans le fuseau de A2, celle-ci se retrouverait avec un ennemi doublé en volume, sans qu'elle n'ait vraiment eu la possibilité de l'anticiper, et surtout sans qu'elle ait été habituée (c'est-à-dire formée et entraînée) à envisager cette possibilité.

Ce phénomène se conjugue avec le développement de l'approche probabiliste de l'OTAN. Les nouvelles technologies, basées sur des algorithmes et sur la logique, sont particulièrement adaptées à ce modèle prédictif des intentions de l'ennemi. L'intelligence artificielle pourra être employée dès demain pour déterminer le mode d'action probable de l'adversaire, en affichant un taux d'erreur estimé à la façon d'une prévision météo. En cas de scénario à très forte probabilité, le chef militaire aura beaucoup de mal à ne pas tenir compte de l'estimation de l'ordinateur, et sera tenté de le suivre systématiquement. De façon assez logique, particulièrement en situation de stress, le décideur réduira volontairement sa réflexion face à des résultats considérés comme « intelligents », objectifs et fiables. Par effet domino, le jeu naturel de la hiérarchie risque de restreindre alors l'imagination des subordonnés, qui verront leurs études limitées aux seuls scénarios considérés comme les plus probables.

Ainsi, si les échelons subordonnés arrivent à disposer de la même vision et de la même appréciation que leurs chefs, si ces mêmes chefs se cloisonnent dans une vision probabiliste de l'appréciation de l'ennemi, une partie importante des modèles traditionnels sera mise en question. Par extrapolation, on peut supposer qu'un état-major habitué à opérer avec un ennemi parfaitement partagé par l'ensemble des forces en présence, se fiant uniquement aux résultats statistiques de ses outils de renseignement, puisse perdre l'habitude d'envisager toutes les alternatives à la vision commune. Bercés dans l'illusion d'une parfaite connaissance de l'ennemi, les esprits pourraient ne plus entretenir leur capacité d'imaginer les possibilités et tunneller ainsi leur réflexion. Or, l'imagination est

indispensable à toute réflexion s'inscrivant dans cette activité humaine qu'est et restera la guerre.

Conclusion

Le militaire entretient un lien particulier avec son ennemi. Si celui-ci est issu d'un choix éminemment politique, il l'a fait sien, l'a décliné compte tenu de sa mission, du contexte particulier dans lequel est conduite ou prévue l'opération. Il est le fruit de sa propre réflexion, basée à la fois sur des faits objectifs observés mais aussi sur ses représentations subjectives, forcément biaisées par la nature humaine de l'analyste comme de l'ennemi.

Pour décliner leur ennemi à chaque échelon de la hiérarchie, les états-majors ont développé des méthodologies adaptées aux nouveaux contextes d'engagement, toujours plus complexes. Si des différences peuvent apparaître dans ces modèles, ceux-ci reflètent les cultures militaires diverses au sein de l'OTAN et restent plus complémentaires qu'opposés.

Dans leur démarche, les armées bénéficient plus que jamais de moyens techniques et d'un développement scientifique qui leur permettent d'envisager à terme la capacité de rendre leur ennemi plus prévisible. Engagées dans une course au renseignement, les forces doivent savoir et anticiper plus vite, essayer de penser à la place de l'ennemi en utilisant tous les leviers possibles – nouvelles pratiques, nouveaux modèles, technologies innovantes, révision de l'organisation des états-majors, etc. Dans ce contexte, quelques priorités émergent pour que les organismes chargés de la conception de l'ennemi puissent se prémunir de la tunnellation de la pensée et conserver la capacité à envisager la diversité des possibles.

Intégrer les approches de l'OTAN, tout en préservant la spécificité française

La France, depuis sa réintégration dans les organes de commandement de l'OTAN, peut difficilement s'abstenir de poursuivre son appropriation des modèles de l'Alliance¹³⁸. Généraliser l'enseignement de l'approche « otanienne » dans les états-majors principaux pourrait assurer une meilleure interopérabilité et surtout une convergence des perceptions avec les alliés pour ce qui relève de l'ennemi. En revanche, la démarche française demeure particulièrement adaptée aux échelons tactiques, faiblement dotés en renseignement initial et en ressources humaines. Par

138. A.-H. de Russé, « La France dans l'OTAN : la culture militaire française et l'identité stratégique en question », *Focus stratégique*, n° 22, Ifri, juin 2010.

son attachement au principe de l'incertitude de l'action ennemie, elle conserve également une forte valeur éducative. Cette complémentarité entre ces deux approches milite pour la préservation et la défense de la spécificité analytique française.

Développer l'intelligence artificielle, tout en cultivant la capacité de s'en passer

L'IA semble désormais incontournable dans tous les aspects liés à la définition de l'ennemi, y compris en matière de simulation. Les états-majors ont des ressources humaines contraintes et doivent pouvoir décharger une partie de leur travail sur des systèmes automatisés de traitement de données fiables et rapides. Toutefois, leur coût actuel les rend difficilement accessibles à tous et partout. Pour pallier ce problème, le partage et le transfert de données entre les échelons tactiques, opératifs et stratégiques doivent être développés ou réaffirmés pour que des IA centralisées au plus haut niveau puissent travailler indirectement au profit des subordonnés. Pour autant, les doutes qui persistent sur la fiabilité absolue de tels outils devraient inciter les militaires à garder l'habitude de s'en passer. Une capacité minimale de recherche et d'analyse du renseignement, pour le propre usage du décideur militaire, reste indispensable même au niveau tactique.

Mieux prendre en compte l'apport des sciences cognitives

Les sciences cognitives sont encore rarement évoquées dans les documents méthodologiques du renseignement. La prise en compte des avantages apportés par les sciences cognitives peut sembler utile, notamment pour sensibiliser les intervenants du renseignement et leurs chefs aux biais cognitifs et à leurs conséquences. L'évaluation des biais internes pourrait même devenir un acte réflexe au sein des bureaux renseignement, une étape obligatoire dans le processus d'analyse. Toutefois, leur adoption dans les armées pourrait s'avérer problématique, dans la mesure où elles obligent à une dose d'autocritique dans des organismes à la hiérarchie très marquée.

Cultiver la diversité des analystes

Les biais cognitifs ont tendance à se renforcer lorsqu'ils sont partagés : quand les schémas de pensée sont uniformes au sein d'un groupe, chaque individu est conforté dans sa perception par l'approbation des autres

membres. Une telle communauté est alors incapable de se remettre en question. Or, « l'absence de confrontation intellectuelle et la culture unique conduisent directement aux désastres stratégiques¹³⁹ ». Le *Red teaming* propose de lutter contre le risque d'erreur collective, testant la norme commune par l'introduction d'un élément volontairement dissonant. Si l'approche est intéressante, elle nécessite toutefois du personnel supplémentaire spécialement formé. En revanche, la simple diversité d'une équipe (d'âge, de sexe, de niveau d'étude, de spécialité, d'origines sociales et culturelles), semble être de nature à minimiser les biais collectifs. Chaque individu, par ses propres schémas mentaux qu'il apporte, atténue de fait les schémas mentaux des autres, pour peu que ces perceptions différentes puissent être exprimées librement et considérées équitablement. Les hauts niveaux de commandement, les armées riches et puissantes pourront toujours compter sur des réseaux d'experts régionaux, connaissant bien le terrain, la culture et la langue. Mais pour un état-major avec des moyens limités, la diversité et l'équité dans le recrutement des analystes du renseignement semblent participer à moindres frais à la lutte contre le risque de cloisonnement de la réflexion.

La révolution en cours dans le domaine du renseignement réaffirme que l'incertitude, notamment liée aux intentions de l'ennemi, ne pourra jamais être totalement levée. L'imprévisibilité inhérente à la nature humaine fait qu'une parfaite connaissance de l'adversaire reste encore illusoire. Comme disait le philosophe Jean Bodin « il n'y a de richesse que d'hommes » : la formation, la connaissance générale et la diversité des hommes plus que des approches seront toujours indispensables au militaire du XXI^e siècle pour arriver à concevoir au mieux son ennemi. S'il est désormais plus facile de lire à travers le brouillard de la guerre, l'incertitude reste un facteur fondamental de l'art de la guerre. Le chef militaire, s'il ne pourra probablement jamais penser exactement comme son adversaire, devra toujours cultiver la volonté de s'imposer malgré l'inconnu et le doute en gardant à l'esprit la formule d'Isaac Asimov : « pour réussir, il ne suffit pas de prévoir. Il faut aussi savoir improviser¹⁴⁰. »

139. V. Desportes, *Défendre la France au XXI^e siècle*, Paris, IHEDN-Economica, 2015, p. 105.

140. I. Asimov, *Fondation*, Paris, Denoël, 2000, p. 182.



ifri institut français
des relations
internationales