Études de l'Ifri
Focus stratégique 81

# OPÉRATIONS DE DÉCEPTION
## Repenser la ruse au XXIe siècle

Rémy HÉMEZ

Juin 2018

ifri Laboratoire de recherche sur la défense

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.



ISBN : 978-2-36567-885-8


**Comment citer cette publication :**
Rémy Hémez, « Opérations de déception. Repenser la ruse au XXIe siècle », *Focus stratégique*, n° 81, Ifri, juin 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

**Rémy Hémez** est officier de l'armée de Terre. Il a été détaché comme chercheur au sein du Laboratoire de recherche sur la défense (LRD) de l'Ifri de 2015 à 2017. Il est diplômé de l'École spéciale militaire de Saint-Cyr et de l'École de guerre. Il est l'auteur de plusieurs articles portant sur la stratégie, la tactique, l'histoire militaire et la Corée du Sud notamment dans la *Revue Défense nationale, Politique étrangère* et *Défense & sécurité internationale*.

# Comité de rédaction

# Résumé

Souvent assimilées à la ruse et aux stratagèmes, les opérations de déception sont une pratique de guerre à la fois ancienne et méconnue, tant au niveau stratégique que tactique ou opératif. Leurs principaux procédés sont la dissimulation, la simulation et l'intoxication, qui toutes contribuent à tromper l'ennemi et lui faire croire à une illusion qui doit causer sa perte. Malgré une efficacité maintes fois démontrée dans l'histoire, cette pratique ne va pas sans poser de dilemmes – d'ordre culturel et éthique mais aussi en matière d'allocation des ressources. Alors que progressent sans cesse dans les armées le développement des réseaux, la numérisation et l'intelligence artificielle, les nouvelles technologies semblent toutefois offrir un terrain fertile à un renouveau des opérations de déception. Bien employées, celles-ci permettraient de nuancer la fin du confort opératif prédit aux forces occidentales et d'éviter l'avènement d'un nouveau blocage tactique.

# Abstract

Often associated with cunning and stratagems, deception operations are as old as warfare while frequently neglected, whether at the strategic, tactical, or operational levels. Its main methods are concealment, simulation and intoxication, all of which help to deceive the enemy and make him believe in an illusion aimed at causing his loss. Despite an effectiveness proven many times in history, this practice is not without its dilemmas-cultural and ethical, but also in terms of resources allocation. As modern armed forces witness the constant progress of information networks, digitalization and artificial intelligence, new technologies seem to provide a fertile ground for a renewal of deception operations. If well used, these would help mitigate the end of the operational comfort predicted to Western forces and avoid the advent of a new tactical blockage.

# Sommaire

# Introduction

> « On se sert alternativement dans la Guerre de la peau du Lion et de celle du Renard. La ruse réussit là où la force échoue. Il est donc absolument nécessaire de se servir de l'une et de l'autre, puisque souvent la force est repoussée par la force ; au lieu que plusieurs fois la force est obligée de céder à la ruse.[1] »
>
> Fréderic II de Prusse, 1761.

Dans l'art de la guerre « violence et intelligence sont indissociables[2] ». La déception représente particulièrement bien cette part d'intelligence. En termes de principes de la guerre, elle renvoie à la manœuvre, à l'économie des forces et à la surprise, tandis que la force est davantage liée au choc, à la concentration des moyens et au nombre.

La déception n'est pas un synonyme de la ruse, qui « peut être définie comme un procédé tactique combinant la dissimulation et la tromperie dans le but de provoquer la surprise[3] », c'est l'une de ses déclinaisons. Elle n'équivaut pas non plus à la dissimulation, qui est l'une de ses composantes. Ces raccourcis, fréquents, n'aident pas à comprendre ce concept. La déception est en revanche proche du « stratagème », un procédé qui, contrairement à la ruse, peut s'enseigner et doit être planifié[4]. Le terme de déception lui-même pose problème, étant peu signifiant pour certains. Même si l'on peut discuter de sa pertinence, il est établi dans le vocabulaire militaire français depuis la fin de la Seconde Guerre mondiale et partagé avec de nombreux pays. Le mot déception, souvent considéré comme un anglicisme, est employé depuis au moins le XV^e^ siècle, en français, dans le sens de tromperie[5]. La racine latine du mot est *deceptum* (forme du verbe *decipere*) qui signifie attraper, tromper, abuser. De façon générale, « la déception est le travestissement volontaire de la réalité dans le but de gagner un avantage compétitif[6] ». Aujourd'hui, la définition doctrinale de la déception est claire :

---

1. Fréderic II de Prusse, *Instruction militaire du roi de Prusse pour ses généraux*, 1761, p. 70.
2. J.-V. Holeindre, *La ruse et la force: une autre histoire de la stratégie*, Paris, Perrin, 2017, p. 13.
3. *Ibid*., p. 19.
4. Entretien avec T. Widemann, Paris, 22 mars 2018.
5. H. Coutau-Bégarie, « Ruse », *in* T. de Montbrial et J. Klein (dir.), *Dictionnaire de stratégie*, Paris, PUF, 2007, p. 494-495.
6. D. C. Daniel et K. L. Herbig, « Propositions on Military Deception », *Journal of Strategic Studies,* vol. 5, n° 1, 1982, p. 155-177.

> « Effet résultant de mesures visant à tromper l'adversaire en l'amenant à une fausse interprétation des attitudes amies en vue de l'inciter à réagir d'une manière préjudiciable à ses propres intérêts et de réduire ses capacités de riposte. La déception comprend la dissimulation, la diversion et l'intoxication.[7] »

L'épisode mythique du cheval de Troie est un exemple assez typique de déception. Le cheval de bois géant conçu par Épéios permet de dissimuler le groupe de combattants conduits pas Ulysse. Le grec Sinon est laissé sur la plage et intoxique les Troyens pour les convaincre de faire entrer le cheval dans la ville. Les navires grecs font diversion en levant le siège et se regroupant derrière l'île voisine de Ténédos.

Une opération de déception implique bien une combinaison d'actions planifiées et coordonnées visant à tromper le chef ou à tout le moins le « système » de commandement et de décision de l'ennemi. Elle est en cela l'un des moyens d'obtenir la surprise. La déception vise à créer une ligne de moindre attente en fixant l'adversaire, physiquement ou psychologiquement, dans une zone qui n'est pas celle de notre effort pour le surprendre et le frapper. Sa valeur réside en outre dans son effet sur le moral d'un adversaire qui découvre, trop tard, qu'il a été dupé. La déception est toujours un acte volontaire destiné à « dominer mentalement son adversaire[8] » et à le faire réagir. Il ne s'agit donc pas tant de faire *penser* l'ennemi d'une certaine façon, que de le faire *agir* dans la direction souhaitée. Cette précision est importante car il existe toujours un risque de convaincre un adversaire mais que sa réaction soit contraire à celle voulue[9].

La déception peut être utilisée dans tout le spectre de la stratégie. Elle est employée dans les conflits conventionnels comme non conventionnels, en offensive et en défensive. Elle peut s'appliquer aux trois niveaux de la guerre : stratégique, opératif et tactique. Elle prend plutôt place pendant les phases préliminaires de l'action afin, dans l'idéal, de forcer l'ennemi à se dévoiler, voire à engager ses réserves à faux, mais elle peut agir sur toute la durée de l'action. La déception occupe bien entendu une place centrale dans les stratégies indirectes « qui ne recherchent pas directement la

7. EMP 60.641, *Glossaire français/anglais de l'armée de Terre*, CDEF, janvier 2013, p. 182.
8. M. Yakovleff, *Tactique théorique*, Paris, Economica, 2006.
9. En 1941, le général Wavell veut que les Italiens déplacent leurs réserves au sud de l'Abyssinie afin de faciliter son offensive vers le nord. Il monte alors un plan de déception visant à les persuader que les Britanniques vont envahir la province du Somaliland. Le plan est un succès mais ses conséquences se révèlent bien différentes de celles espérées : les Italiens, se sentant en infériorité, choisissent d'évacuer le Somaliland, laissant de nouvelles troupes libres pour défendre le nord de l'Abyssinie. Voir D. Clarke, « Some Notes on the Organization of Deception » *in* H. S. Rothstein et B. Whaley (dir.), *The Art and Science of Military Deception*, Boston, Artech House, 2013, p. 167-165.

décision par l'affrontement des forces militaires[10] » dès lors que « l'idée centrale de cette conception est de renverser le rapport de forces opposées avant l'épreuve de la bataille par une manœuvre et non par le combat[11] ». On la retrouve assez logiquement comme une composante importante des opérations spéciales[12], tandis qu'au niveau tactique, elle est presque toujours valorisée dans les actions de guérilla[13]. Malgré cette image fortement teintée « d'irrégularité », la déception n'est aucunement absente de la stratégie directe et de la guerre conventionnelle.

Jusqu'à l'époque moderne, la déception est essentiellement le fait du « génie » du chef militaire. Elle est rendue difficile par la dimension limitée du champ de bataille. La révolution industrielle, l'augmentation de la taille des armées, l'accroissement de la mobilité, l'avènement de la troisième dimension ainsi que les premiers pas des technologies de l'information offrent l'opportunité de synchroniser les opérations de déception sur des fronts entiers, voire jusqu'au niveau stratégique, ce qui était jusqu'alors impossible. C'est ainsi que la déception est institutionnalisée et fait son entrée dans les états-majors[14]. Après des débuts discrets lors de la Grande Guerre, la déception émerge véritablement comme un « art majeur » avec sa pratique par les Britanniques sur le théâtre nord-africain lors du second conflit mondial[15]. Au sortir de grandes difficultés pendant les deux premières années de la guerre, les Soviétiques montrent eux aussi leur maîtrise de la *maskirovka*[16].

La guerre froide et la dissuasion nucléaire vont ensuite mettre au second plan les considérations de ce type au sein de l'OTAN. Dans les années 1980, la déception revient au premier plan aux États-Unis. Ce retour en grâce s'explique tant par l'intérêt provoqué par la déclassification de certaines opérations de la Seconde Guerre mondiale que par les nombreux échecs du renseignement américain face aux actions soviétiques, pour qui la *maskirovka* n'a pas perdu de sa vigueur[17]. C'est la naissance du concept de « *denial and deception* », largement inspiré de la *maskirovka*

10. A. Beaufre, *Introduction à la stratégie*, Paris, Pluriel, 2017, p. 63.
11. *Ibid*., p. 146.
12. W. H. McRaven, *Spec Ops: Case Studies in Special Operations Warfare: Theory and Practice*, New York, Ballantine Books/Random House Publishing Group, 1996.
13. S. G. Jones, *Waging Insurgent Warfare: Lessons from the Vietcong to the Islamic State*, New York, Oxford University Press, 2017.
14. J.-V. Holeindre, *La ruse et la force*, *op. cit.*, p. 309-338.
15. L'un des exemples les plus connus est l'opération « Bertram », le plan de déception de la bataille d'El Alamein.
16. D. M. Glantz, *Soviet Military Deception in the Second World War*, London/Totowa, F. Cass, 1989.
17. « Deception Maxims: Fact and Folklore », Deception Research Program, CIA, juin 1981.

soviétique[18]. La guerre de Golfe (1990-1991), où la déception est employée avec succès, parachève cette réhabilitation.

Deux phénomènes vont pourtant contribuer à renvoyer à nouveau ce concept au second plan de la culture militaire occidentale. Tout d'abord, dans les années 1990-2010, l'ennemi symétrique n'est plus la préoccupation principale. Les « longues guerres » d'Afghanistan et d'Irak attestent d'un contexte d'engagement très différent. Fort de sa supériorité, le belligérant le plus puissant s'autorise à abandonner l'emploi de la déception au plus faible, pour lequel elle est d'ailleurs une nécessité[19]. De fait, la tendance à recourir ou non à la déception résulte souvent de la perception d'une position de force ou de faiblesse, bien plus que d'une tradition militaire, ou d'une influence culturelle[20]. Les Britanniques, qui l'ont peu utilisée pendant leurs campagnes coloniales, en sont devenus les maîtres pendant la Seconde Guerre mondiale alors qu'ils se trouvaient en infériorité face à la puissance militaire allemande.

Le deuxième phénomène qui a contribué à renvoyer dans l'ombre les opérations de déception tient à l'évolution de l'environnement opérationnel. La « révolution dans les affaires militaires » et l'avènement, prophétisé par certains, d'un champ de bataille transparent rendrait vaine toute tentative de surprendre et donc toute déception. Si ces développements contemporains et à venir rendent certainement les opérations de déception plus complexes, celles-ci ne sont cependant pas impossibles car comme pour le duel entre l'épée et la cuirasse, l'oscillation entre opacité et transparence est en mouvement perpétuel. Surtout, la déception est peut-être plus utile que jamais comme adjuvant nécessaire à la surprise, aussi bien tactique que stratégique, afin de ne pas faire face à un nouveau « blocage » tactique[21].

18. C. L. Smith, « Soviet Maskirovka », *Air Power Journal*, vol. 2, n° 1, 1988, p. 28-39.
19. J. B. Bell, « Toward a Theory of Deception », *International Journal of Intelligence and Counterintelligence*, n° 16, 2003, p. 244-279.
20. J.-V. Holeindre, *La ruse et la force, op. cit*.
21. R. Hémez, « Les développements techniques nous entraînent-ils vers un nouveau blocage tactique ? », *Stratégique*, vol. 112, n° 2, 2016, p. 113-124.

# Fondements théoriques des opérations de déception

La déception est une manipulation de l'incertitude inhérente au combat, elle-même fruit de l'imprévisibilité de la nature humaine (le combat est un duel de libertés) et de l'environnement. C'est pourquoi, en dépit des progrès technologiques, la déception demeure possible. Il est cependant nécessaire de bien connaître ses différentes dimensions et les facteurs qui permettent de réussir sa mise en œuvre pour l'employer à bon escient.

## Pourquoi est-il possible de tromper ?

La stratégie et la tactique sont avant tout des duels de volontés humaines. Or, l'Homme demeure imprévisible. Son imagination est sans limite. Il n'est pas possible d'anticiper à coup sûr un mode d'action, et donc de savoir si l'adversaire cherche à nous tromper. De façon générale, le commandement prend ses décisions sur la base d'hypothèses. Pour le reste, il doit s'en remettre à la loi des probabilités, ou à son intuition, le célèbre « coup d'œil » du chef militaire. L'accélération des opérations actuelles rend cette prise de décision encore plus difficile et offre davantage d'opportunités pour des opérations de déception.

Conscients de ces limites, les états-majors sont entièrement tournés vers la réduction de l'ambiguïté. C'est la mission principale de la fonction renseignement, qui est en première ligne de la contre-déception[22]. Cependant, le renseignement est de nature spéculative. Les analystes aboutissent à des conclusions à partir de données toujours incomplètes et parcellaires. Le seul système qui permet de juger de leur crédibilité est la traditionnelle cotation par lettres et chiffres[23]. Le flot d'informations rend complexe la distinction entre le « bruit » et le « signal », et cette problématique ne fait que s'accroître avec le temps. D'autant que l'urgence des opérations laisse souvent peu de place à l'analyse. Le renseignement

22. Sur la question du renseignement lire notamment : J. Henrotin, « Les mutations du renseignement militaire, dissiper le brouillard de la guerre ? », *Focus stratégique*, n° 71, Ifri, p. 13 ; et Y. Trotignon, « L'analyse du renseignement : savoir et comprendre pour agir », *in* S. Taillat, J. Henrotin et O. Schmitt (dir.), *Guerre et Stratégie*, Paris, PUF, 2015, p. 271-286.

23. La cotation d'un renseignement est attribuée par l'analyste pendant son exploitation. Elle se présente sous la forme d'un bigramme dont la lettre indique la qualité de la source et le chiffre donne la valeur du renseignement. La qualité de la source est codifiée de A à F (d'une source complètement sûre pour A, à celle dont la sûreté ne peut être appréciée pour F). La valeur du renseignement est, elle, codifiée de 1 à 6 (de confirmée par d'autres sources pour 1, à un niveau d'exactitude ne pouvant être apprécié pour 6). TTA 150*, Titre VI, Renseignement*, COFAT, 2001, p. 9-10.

fait aussi face à un paradoxe. Répondre à des questions conduit en général à en soulever de nouvelles et la quête de la certitude peut aboutir ainsi à davantage d'incertitude. Enfin, il est par définition toujours ardu pour un analyste de démontrer l'existence d'une opération de déception si celle-ci est bien orchestrée. Il devra donc se contenter d'une hypothèse, ce qui convaincra difficilement sa chaîne hiérarchique[24].

La possibilité de tromper, ou d'être trompé, ne dépend pas que du renseignement. Elle repose aussi sur l'inaptitude de certains chefs. Ainsi parmi les quatorze caractéristiques de « l'incompétence militaire[25] » recensées par le psychologue britannique Norman Dixon, on trouve : le conservatisme, qui a notamment pour conséquence l'inaptitude à prendre en compte les leçons du passé ; la tendance à rejeter les informations dérangeantes ; le penchant à sous-estimer l'ennemi et à surestimer ses propres capacités ; la propension à abdiquer son rôle de décideur ; l'obstination à exécuter une tâche malgré des preuves de son inefficacité ; l'incapacité à réaliser des reconnaissances correctes ; la croyance en la force brute davantage que dans la ruse ; etc. Autant de limites qui rendent moins efficace le processus de décision et donnent prise à la déception ennemie.

Finalement, la déception est possible parce que la guerre est une activité éminemment humaine et que l'homme a ses propres limites. Face à la complexité, l'esprit fait preuve d'une « rationalité limitée[26] ». Il n'est pas possible d'être totalement objectif et nous sommes tous soumis à de nombreuses interférences dans nos jugements. Les psychologues parlent de biais cognitifs, des « erreurs mentales causées par nos stratégies simplifiées de traitement de l'information[27] ». Ils ne nous rendent pas prédictibles dans le sens où toute personne se trouvant dans une situation donnée ferait systématiquement la même erreur. En revanche, ils sont fréquents et largement partagés, ce qui peut donner de précieuses indications lorsqu'il s'agit de penser une opération de déception. Il n'est pas possible de décrire ici tous ces biais[28]. Nous pouvons cependant en évoquer quatre.

Le « biais de représentativité », ou « loi des petits nombres », rend compte du fait que les analystes ont tendance à surestimer la fiabilité des

24. E. Kam, *Surprise Attack: The Victim's Perspective*, Cambridge, MA, Harvard University Press, 2004, p. 145.
25. N. Dixon, *On the Psychology of Military Incompetence*, PIMLICO, 1994, p. 152-153.
26. H. A. Simon, *Models of Man: Social and National*, Londres, Wiley, 1957.
27. R. Heuer, *Psychology of Intelligence Analysis*, Center for the Study of Intelligence/CIA, 1999, p. 112. A. Dyèvre, « Renseignement, facteur humain et biais cognitifs. *Gnothi seauton* », *Les notes stratégiques*, CEIS, juin 2015.
28. Pour une tentative de systématisation, B. Benson, « Cognitive Bias Cheat Sheet : Because Thinking Is Hard », 1er septembre 2016, blog *Better Humans*, disponible sur : betterhumans.coach.me.

petites séries statistiques[29]. Il existe une propension à accorder davantage de crédit à une petite série de données cohérentes, mais non statistiquement représentatives, plutôt qu'à une grande série de données qui le seraient moins. Peu d'informations peuvent donc suffire pour obtenir un effet de déception, et il y a un grand intérêt à contrôler les canaux de renseignement de l'adversaire afin de réduire le volume de signaux discordants.

Le deuxième biais, celui « d'ancrage », consiste à utiliser indûment une hypothèse comme une réalité[30]. Une fois adoptée en vue d'un plan précis, une hypothèse de travail est souvent « ancrée » dans les esprits et n'est généralement remise en cause qu'à la marge. C'est pourquoi, plutôt que de vouloir le pousser à changer d'avis, il est préférable de chercher à renforcer les préconceptions de l'adversaire que l'on désire tromper. Les Alliés savaient par exemple qu'Hitler, et la plupart des hauts gradés de son état-major, croyait en un débarquement dans le Pas de Calais. C'est ce qui constitua la base du plan *Fortitude* visant à cacher aux Allemands que cette opération aurait lieu en Normandie en confirmant leurs attentes[31].

Le biais de « conditionnement » décrit quant à lui la difficulté à détecter des changements graduels, y compris ceux qui, cumulés, entraînent une évolution majeure[32]. Lors de l'opération *Cerberus* en 1942, les Allemands utilisèrent cette faille pour préparer la sortie des navires *Scharnhorst*, *Gneisnau* et *Prinz Eugen* du port de Brest. Quotidiennement à l'aube, ils brouillaient pendant quelques minutes les stations radio britanniques pour faire croire à un effet des conditions atmosphériques. Chaque jour, la durée du brouillage était légèrement augmentée, permettant de crédibiliser l'hypothèse de la cause météorologique. Cette action a facilité la sortie des navires le jour voulu[33].

Enfin, le « biais de confirmation » exprime la tendance à ne rechercher, et à ne trouver pertinentes, que les informations qui confirment nos préconceptions. Cette propension est renforcée dans les organisations militaires où, trop souvent

> « la tentation de dire à un chef ayant une position importante les choses qu'il aime le plus entendre est l'explication la plus commune des actions erronées[34] ».

29. A. Tversky et D. Kahneman, « Belief in the Law of Small Numbers », *Psychological Bulletin*, vol. 76, n° 2, 1971, p. 105-110.
30. A. Tversky et D. Kahneman, « Judgment under Uncertainty: Heuristics and Biases », *Science,* vol. 185, n° 4157, septembre 1974, p. 1124-1131.
31. A. C. Brown, *Bodyguard of Lies*, New York, Harper & Row, 1975, p. 437.
32. « Deception Maxims: Fact and Folklore », *op. cit.*
33. J. D. Potter, *Fiasco: The Break-Out of the German Batlleships*, Bershire, Slough Bucks, 1970, p. 30.
34. W. Churchill, *The World Crisis 1916-1918*, Londres, Macmillan, 1941, p. 653.

C'est ainsi qu'en 1944 l'imminence d'une offensive allemande dans les Ardennes fut ignorée malgré le grand nombre d'indices l'accréditant[35]. Des interceptions Enigma évoquaient, par exemple, des reconnaissances de points de franchissement sur la Meuse. Tous ces signaux furent négligés. Le commandement allié ne voulait pas croire que les Allemands, dans un état de faiblesse critique, lanceraient une offensive ambitieuse. À plus forte raison au moment où ils devaient plutôt chercher à rassembler leurs forces pour faire face à l'offensive soviétique d'hiver. Ils renforcèrent cette croyance des Alliés avec une opération de déception visant à les persuader de la préparation d'une contre-attaque sur le Rhin. Elle reposait, notamment, sur le silence radio, des déplacements uniquement de nuit, un positionnement de la V$^{e}$ Division Panzer aux environs de Cologne jusqu'à trois jours avant l'attaque, etc.

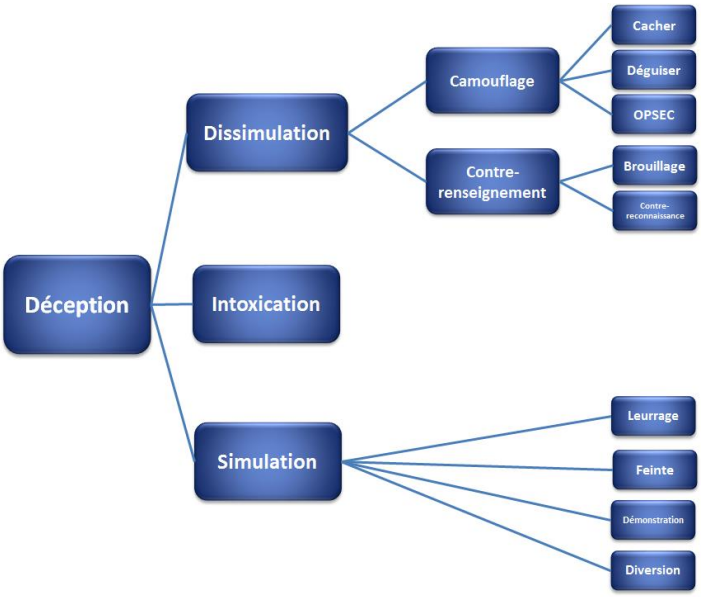
Il est impossible de lire dans l'esprit de l'adversaire et donc de prévoir ses intentions. Comme le dit une veille expression militaire, « l'ennemi a toujours son mot à dire ». Par ailleurs, les rationalités individuelles et collectives des décideurs et des organisations sont toujours limitées : les émotions et les biais cognitifs, mais également les calculs d'ordre non militaire (impératifs politiques, enjeux bureaucratiques ou stratégies personnelles) sont irréductibles des processus de décision. Autant de failles impossibles à combler totalement et dans lesquelles peut s'immiscer la déception, d'autant plus que cette dernière présente de nombreux visages et peut compter sur pléthore de procédés pour se renouveler à loisir.

## Typologie de la déception

Il y a plusieurs façons de dresser une typologie de la déception. Il est possible de citer, par exemple, la distinction binaire entre celle qui cherche à augmenter l'ambiguïté en inondant l'adversaire d'information (« bruit ») et l'autre, plus ambitieuse, qui vise à le tromper en le persuadant d'une hypothèse en réalité fausse[36]. Dans la pratique, les deux coexistent souvent. Il est également possible de décomposer la déception selon les procédés utilisés. C'est ce que nous allons nous attacher à faire ici[37].

35. J. R. Arnold, *Hitler's Last Gamble in the West*, Londres, Osprey, 1998, p. 25-26.
36. D. C. Daniel et K. L. Herbig, « Propositions on Military Deception », *Journal of Strategic Studies*, vol. 5, n° 1, 1982, p. 155-177.
37. La doctrine française retient trois modes d'actions principaux pour la déception : dissimulation, diversion et intoxication.

**Schéma 1. Typologie de la déception**




*Source : Adapté de J. D. Monroe, « Deception: Theory and Practice », Naval Postgraduate School Thesis, juin 2012, p. 44. et C. de Lajudie, « La déception », site* Pensée mili-terre.

Il faut d'abord opérer une première distinction entre déception active, passive et intoxication. La déception passive, aussi dénommée dissimulation, est destinée à cacher quelque chose qui existe vraiment (moyens, actions, intentions). Elle regroupe deux procédés principaux. Il y a d'abord le camouflage, c'est-à-dire l'action visant à soustraire le personnel, le matériel, les installations, les activités et les informations de toutes natures aux investigations de l'ennemi. Manœuvre, utilisation du terrain, banalisation de moyens, discrétion optique, radioélectrique, thermique, radar, ou, plus généralement, mise en œuvre de procédures de sécurité opérationnelle (OPSEC), sont autant d'actions possibles pour se camoufler. Vient ensuite le contre-renseignement, dont le but est de neutraliser et détruire les moyens de renseignement adverses[38]. Parmi les procédés possibles, on compte la contre-reconnaissance qui consiste à

> « prendre l'ensemble des mesures actives (recherche et destruction) et passives (redéploiements et mesures de sauvegarde) nécessaires pour, au mieux, neutraliser la collecte et la transmission du renseignement par l'ennemi sur la zone, au minimum, en dégrader l'efficacité[39] ».

38. « Ensemble des actions ou des procédés, élaborés par le B2, qui consiste à empêcher l'adversaire d'employer efficacement sa chaîne renseignement en agissant sur : a- les informations, collectées (par la déception) ; b- les capteurs (par leur neutralisation) ; c- la sûreté (par la contre-ingérence). » EMP 60.641, *Glossaire français/anglais de l'armée de Terre*, CDEF, janvier 2013, p. 168.
39. M. Yakovleff, « La contre-reconnaissance », *Pensée mili-terre*, 2014, disponible sur : penseemiliterre.fr.

Le deuxième procédé possible est la déception active, ou simulation, terme plus englobant que celui de diversion utilisé dans la définition doctrinale française. La simulation consiste à fournir à l'adversaire des preuves d'intentions et de capacités que l'on ne détient pas en réalité[40]. Elle regroupe quatre modes d'action.

Les actions de leurrage sont des représentations d'équipements, de forces, ou d'activités. Au-delà de l'utilisation de faux engins et véhicules, elles comprennent aussi la représentation d'une unité par une autre, généralement pour faire croire à une force en présence plus importante que ce qu'elle est en réalité. Au cours de la guerre froide, l'exercice annuel *Reforger* de 1988 a vu une tentative de simuler la 8e division d'infanterie américaine par une *task force* (TF) composée de 294 véhicules et 1 000 soldats, soit 25 % environ de l'unité[41]. Les procédés de déception utilisés sont nombreux. La TF a fait mouvement de jour des positions initiales de la division vers une zone de regroupement, un faux réseau radio a été mis en place, des éléments *psyops* ont diffusé des sons de véhicules en mouvement, etc. Tout ceci permet de berner, au moins partiellement, l'adversaire.

Un autre mode d'action est la diversion qui vise à « attirer les moyens de l'adversaire vers une zone ou un point différent de celui sur lequel on compte exercer l'effort principal[42] ». C'est une action secondaire, mais au cours de laquelle il peut s'avérer nécessaire d'engager le combat. Les forces qui y participent sont donc en général « consommées » et ne peuvent être engagées dans l'action principale. Une diversion est particulièrement efficace lorsqu'elle provoque l'engagement de la réserve de l'adversaire. Un procédé de ce type est utilisé par les Britanniques pour la prise du mont Tumbledown lors de la guerre des Malouines (1982)[43]. Face à une position tenue fermement par les Argentins, le commandant des Scots Guards envoie sa section de reconnaissance renforcée de quatre chars légers pour mener une attaque de diversion par le nord-ouest. Environ 2 h 30 de violents combats ont l'effet escompté : les Argentins sont persuadés de faire face à l'assaut principal, et le gros des forces britanniques peut s'infiltrer par l'ouest sans être détecté.

40. J. W. Caddell, « Deception 101-Primer on Deception », décembre 2004 et J. D. Monroe, « Deception: Theory and Practice », Naval Postgraduate School Thesis, juin 2012, p. 45 et suivantes.
41. Cette simulation est néanmoins très difficile à réaliser. Pendant ce même exercice la force adverse n'a pas été complètement bernée car la signature de cette *task force* ne correspondait pas exactement. En particulier, l'absence de deux signatures critiques (l'artillerie divisionnaire et le bataillon de renseignement) a semé le doute. Voir P. A. Haveles, « Deception Operations in Reforger 88 », *Military Review,* vol. 70, n° 8, août 1990, p. 35-41.
42. EMP 60.641, *Glossaire français/anglais de l'armée de Terre*, CDEF, janvier 2013, p. 212. On y trouve aussi la définition retenue par l'OTAN de la *feinte* : « détourner l'attention de l'ennemi loin du secteur de l'action décisive en cherchant le contact, mais en évitant un engagement décisif. »
43. D. Anderson, *The Falklands War – 1982*, Oxford, Osprey, 2002, p. 83-87.

Troisième type de déception active, la démonstration est généralement une action secondaire qui consiste à se faire voir, ou entendre, dans une direction ou une zone pour montrer sa force[44]. La démonstration se différencie de la diversion car le contact n'y est pas recherché. Le volume de forces utilisé peut donc être moindre et les unités qui y sont consacrées ne sont pas fixées et sont susceptibles d'être utilisées ailleurs. C'est la mission reçue par la cavalerie du comte de Lorgnes lors de la bataille de Turckheim en 1675[45]. Alors que les troupes françaises progressent vers le nord en trois colonnes, au nord de Pfaffenheim, celle commandée par Turenne bascule hors des vues de l'ennemi et s'infiltre par les Vosges. Pendant ce temps-là, le comte de Lorgnes se déploie face à l'ennemi pour faire croire à une attaque venant du sud. Cette manœuvre permet à Turenne de prendre Turckheim, au nord-ouest, sans opposition majeure.

Dernier procédé actif, la feinte « désigne une manœuvre principale dont on fait effectuer (et observer) le premier temps vers un objectif attendu, pour en changer brutalement l'orientation en cours d'action[46] ». Patton réalise avec succès un mouvement de ce type lors de la campagne du Palatinat en mars 1945[47]. Il estime que si sa III^e armée atteint le Rhin lors de sa progression dans l'Eifel, les Allemands penseront, logiquement, qu'il poursuivra vers le nord-est en franchissant le fleuve. Pour les tromper, une fois le Rhin atteint, il pivote de 90 degrés vers le sud, franchit la Moselle, les montagnes d'Hunsrück et traverse le Palatinat pour atteindre à nouveau le Rhin entre Mainz et Karlsruhe. Il prend les Allemands par surprise, ce qui permet la destruction de leurs I^ère et VII^e armées.

Le troisième grand type de déception est l'intoxication, ou désinformation[48]. Elle a « pour effet de tromper l'adversaire sur les intentions et les possibilités amies en lui faisant acquérir de fausses informations[49] ». Le but est de créer confusion et erreur dans son jugement par une « véritable offensive intellectuelle[50] ». Les opérations

44. EMP 60.641, *Glossaire français/anglais de l'armée de Terre*, CDEF, janvier 2013, p. 194. « Tromper ou dissuader un individu, un groupe d'individus ou une organisation en montrant sa force sans chercher le contact »

45. G. Haberey et H. Perot, *L'art de conduire une bataille*, Paris, Pierre de Taillac, 2016, p. 220-226.

46. C. de Lajudie, « La déception », publié le 16 mars 2018, site *Pensée mili-terre*, disponible sur : www.penseemiliterre.fr.

47. J. K. Morningstar, *Patton's Way: A Radical Theory of War*, Annapolis, Naval Press Institute, 2017, p. 142.

48. « La désinformation consiste à propager délibérément des informations fausses en les faisant apparaître comme venant de source neutre ou amie pour influencer une opinion et affaiblir l'adversaire. » L'intoxication, elle, « consiste à injecter une fausse nouvelle par une source indirecte dans un circuit qui est plutôt destiné aux décideurs. » Voir F.B Huyghe, « De la désinformation à la post-vérité », 6 mai 2017, disponible sur le blog de l'auteur : huygues.fr.

49. EMP 60.641, *Glossaire français/anglais de l'armée de Terre*, CDEF, janvier 2013, p. 198.

50. Colonel Berteil, « Réflexions sur la surprise », *Revue de défense nationale*, mars 1952, p. 262-275.

psychologiques (PsyOps), sont l'un de ses outils majeurs[51]. Elles regroupent l'ensemble des activités dont l'objet est d'obtenir des changements de perceptions de la part d'individus, de groupes, ou d'organisations, afin de contribuer à la réalisation de l'état final recherché (EFR). Un des procédés d'intoxication utilisable est celui du conditionnement[52]. Le déploiement de l'armée égyptienne au déclenchement de la guerre du Kippour a ainsi suscité peu de suspicions puisque pendant les neuf premiers mois de 1973, elle avait conduit pas moins de 20 exercices de mobilisation, tous observés par les Israéliens[53]. De nombreux entraînements au franchissement du canal de Suez avaient aussi été menés[54].

**Tableau 1. Exemples de modes d'action concourant à la déception**

| Types | Procédés | Modes d'action |
|---|---|---|
| **Dissimulation** | **Camouflage** | Fausses désignations d'unités |
| | | Filets de camouflage |
| | | Écrans de fumée. Produit par des générateurs montés sur un véhicule, le nuage peut faire deux à trois kilomètres. Efficace dans les domaines infrarouge et radar |
| | | Dissimulation des mouvements de troupes, de concentrations, ou d'installations en utilisant le terrain ou des artifices |
| | **Contre-renseignement** | Brouillage des capteurs adverses |
| | | Destruction des capteurs adverses |

51. En 2018, la France a de nouveau adopté le terme d'opérations psychologiques en remplacement de celui d'opérations militaires d'influence (OMI). Le but est, d'une part, d'éviter les confusions avec la SMI, stratégie militaire d'influence et, d'autre part, de souligner l'interopérabilité avec l'OTAN.
52. S. Gerwher et R. W. Glenn, *The Art of Darkness: Deception and Urban Operations,* Santa Monica, RAND Corporation, 2000, p. 21.
53. R. M. Clark et W. L. Mitchell, *Deception: Counterdeception and Counterintelligence*, New York, Sage publications, 2018, p. 18-19.
54. E. Kam, *Surprise Attack the Victim's Perspective*, *op. cit.*, p. 49-50 et M. Dewar, *The Art of Deception in Warfare*, M. Dewar, *The Art of Deception in warfare*, New York, David & Charles Publishers, 1989.

| | | |
|---|---|---|
| **Intoxication** | S'entraîner pour un type d'opération (amphibie, par exemple) qui n'est pas celui que l'on veut mener | |
| | Actions politico-diplomatiques, comme des déclarations dans les médias ; entrer en négociations avant une offensive, ou plus généralement se montrer bienveillant | |
| | Utilisation d'agents doubles, ou retournés, pour diffuser des informations sélectionnées chez l'adversaire | |
| | Diffusion de faux ordres | |
| | Diffusion de rumeurs | |
| | « Double bluff », en révélant volontairement la vérité à l'ennemi, tout en pensant qu'il ne la croira pas et la prendra pour une déception | |
| | Faire croire qu'une information a été délivrée par négligence ou inefficacité | |
| | Multiplier les incidents avant l'action principale pour désensibiliser l'adversaire | |
| **Simulation** | **Leurrage** | Travaux du génie factices : faux emplacements de combat, faux champs de mines, déploiement de moyens de franchissement à proximité d'un obstacle qu'on ne compte pas franchir, etc. |
| | | Simulation sonore d'unités ou d'activités en utilisant des haut-parleurs |
| | | Simulation lumineuse d'unités ou d'activités |
| | | *Spoofing,* par exemple, pour faire croire qu'une unité est restée sur sa position alors qu'elle est en fait en mouvement en silence radio, ou pour créer une unité entièrement factice |
| | | Trafic radio factice |
| | | Faux messages radio en clair (ou si l'on sait que l'adversaire déchiffre nos codes) |
| | | Reconnaissances sur une zone où l'on ne compte pas faire effort |
| | | Concentration d'activités dans une zone autre que celle où l'on veut faire effort. Peut se faire avec des reconnaissances, des tirs d'artillerie, des frappes aériennes, des déploiements logistiques, etc. |

| | | |
|---|---|---|
| | | Simulation d'unités par des unités moins importantes |
| | | Utilisation de leurres (ou simulacres) |
| | **Feinte** | Mouvement dans une direction avec tout ou partie de ses unités avant de changer brutalement de direction |
| | **Démonstration** | Faire voir une partie de ses forces dans une direction ou une zone qui n'est pas celle de l'effort. Possibilité d'utiliser des leurres visuels et sonores pour réaliser tout ou partie de l'effet recherché |
| | **Diversion** | Menace de débordement ou de manœuvre d'aile pour forcer l'ennemi à puiser des moyens de contre-manœuvre ou de couverture dans sa masse principale |

L'utilisation d'un seul de ces procédés ne suffit pas pour constituer une opération de déception. Il faut en combiner plusieurs au sein d'une manœuvre visant à influencer le comportement de l'adversaire. Bien entendu, cette association ne doit pas être une simple juxtaposition mais répondre à certains critères afin que l'opération de déception soit efficace.

## Facteurs de réussite

Une littérature abondante traite la question des facteurs de réussite d'une opération de déception, nous en avons retenu sept[55]. Le premier est le secret. Il doit être maintenu à propos de ce qu'on a l'intention de faire réellement et de l'existence d'une opération de déception. Cette condition est si essentielle que le commandement peut être amené à cacher la vérité à ses propres unités, ou à ses alliés pour éviter les risques de fuite et renforcer au maximum la crédibilité de la manœuvre de déception. C'était souvent le cas pour les unités soviétiques qui menaient des opérations de diversion pendant la Seconde Guerre mondiale – le but étant aussi de s'assurer de leur combativité[56].

Le deuxième facteur de succès est une planification et une coordination très fines. Une opération de déception, même au niveau

55. « Deception Maxims: Fact and Folklore », *op. cit.* ; M. Dewar, *The Art of Deception in Warfare*, *op. cit.*, p. 14-15 ; J. Latimer, *Deception in War*, New York, Overlook Press, 2003, p. 60-70; J. Haswell, *The Tangled Web: The Art of Tactical and Strategic Deception*, *op. cit.* ; D. Clarke, « Some Personal Reflections on the Practice of Deception in the Mediterranean Theatre from 1941 to 1945 », in D. Mure, *Master of Deception: Tangled Webs in London and the Middle East*, Londres, W. Kimber, 1980 ; C. de Lajudie, « La deception », *art. cit.*

56. D. M. Glantz, *Soviet Military Deception in the Second World War*, *op. cit.*, p. 569.

tactique, ne s'improvise pas et nécessite du temps pour être préparée. Pour que le message soit cohérent et reçu par les bons canaux adverses, il est nécessaire de planifier avec soin. Des actions de déception isolées peuvent, occasionnellement, avoir des résultats au niveau tactique, mais seules des manœuvres adroitement coordonnées aboutissent à de véritables succès opératifs et stratégiques. En cours d'action, la déconfliction avec les unités voisines est cruciale pour éviter de « polluer » leur collecte de renseignements avec les effets de la déception et qu'elles deviennent ainsi les victimes d'une « déception collatérale ». Tout cela milite pour un style de commandement centralisé – un point à prendre en compte alors que la tendance est plutôt, actuellement, à la décentralisation[57].

Ensuite, une opération de déception doit être crédible aux yeux de l'adversaire. Pour ce faire, elle doit d'abord reposer sur une « bonne histoire ». Comme dans le domaine littéraire, l'important n'est pas ce que l'auteur voulait dire lorsqu'il a écrit l'histoire mais bien ce que le lecteur pense et ressent lorsqu'il la lit, d'où l'importance de la connaissance de l'adversaire. Par exemple, un dirigeant paranoïaque sera sensible à un narratif incluant un complot contre lui. De plus, on ne saurait faire croire l'adversaire à une manœuvre qui semble par trop improbable. Ce critère implique par exemple que l'action de déception soit cohérente avec la doctrine. La crédibilité et la simplicité de la manœuvre sont aussi favorisées si le mode d'action réel et celui de déception ont le plus possible d'éléments en commun. Par ailleurs, un mensonge est davantage crédible lorsqu'il est confirmé par de multiples sources, d'où l'importance d'utiliser plusieurs canaux pour transmettre le « message ». Enfin, les informations ne doivent pas arriver de façon trop évidente à la cible car cela amènerait cette dernière à douter de leur véracité.

Le quatrième facteur de succès est de renforcer les croyances de l'ennemi[58] : « ce qui est capital dans les opérations militaires, c'est de faire croire que l'on s'ajuste aux desseins de l'ennemi[59] ». Comme nous l'avons vu ci-dessus, c'est une nécessité confirmée par la psychologie expérimentale. Il s'agit en fait de tirer profit du biais de confirmation évoqué.

Le cinquième facteur de succès d'une opération de déception est la capacité à en évaluer le succès à mesure qu'elle est conduite. Le but est de pouvoir répondre à la question suivante : « Est-ce que quelqu'un est à

57. G. Soulié, C. Maurin, V. Lehmuller et R. Jaillet, « Le style de commandement dans les armées depuis le XVIIIe siècle : évolutions et perspectives pour les notions de commandement », *Cahiers de la pensée mili-terre*, n° 49, 2017, p. 25-44.
58. R. Jervis, *Perceptions and Misperceptions in International Politics*, Princeton, Princeton University Press, 2017, p. 117 et suivantes.
59. Sun Tzu, *L'art de la guerre*, Paris, Flammarion, 2002, p. 185.

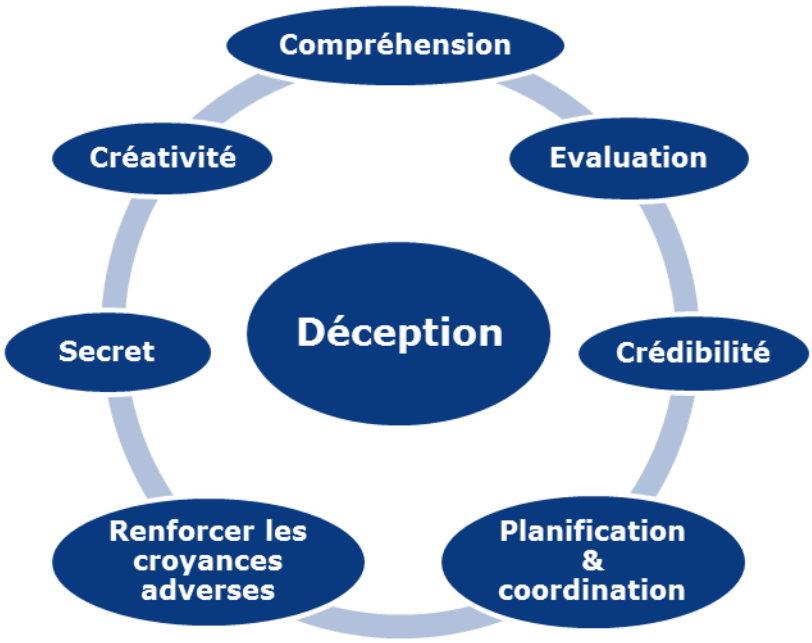
l'écoute ? [60] ». Il faut donc que des capteurs soient dédiés à cette tâche et que des indicateurs aient été pensés[61]. Dans le cadre d'une diversion, il pourrait s'agir, par exemple, de détecter l'engagement de la réserve de l'adversaire en direction du point d'application de la déception. Un contrôle des effets permet, si nécessaire, de modifier la manœuvre. Si elle ne fonctionne pas, il est alors possible, dans certains cas, de réaffecter les moyens qui lui étaient alloués.

Une opération de déception réussie implique la compréhension de l'environnement et, en particulier, des chefs adverses : la déception vise avant tout la « tête », les services de renseignement sont ses « clients »[62]. Il faut alors étudier leur arrière-plan culturel, organisationnel (cycle de décision) et personnel, mais aussi cartographier les moyens de collecte du renseignement, canaux par lesquels passeront les informations. Il est nécessaire de comprendre quels indices doivent être perçus par le renseignement adverse pour provoquer le comportement attendu. Il s'agit de se poser la question de ce qu'il se croit capable de faire et de comprendre son intention – et pas seulement ses capacités – pour construire sa stratégie et anticiper ses réactions[63]. En milieu interculturel un effort supplémentaire est indispensable pour y parvenir car les pièges sont nombreux : ethnocentrisme, dénigrement, etc. Enfin, il est aussi primordial de comprendre comment la cible nous perçoit (et en particulier notre cycle de décision) afin d'ajuster la déception et renforcer le secret[64].

Le dernier facteur de succès pour la déception est la créativité. Pour planifier ce type d'opération, il est essentiel de faire preuve d'imagination, notamment afin de s'assurer de la diversité des modes de transmission des informations et des modes d'action. Utiliser régulièrement les mêmes procédés de déception serait contre-productif puisque cela rendrait la manœuvre prévisible. Par exemple, un usage excessif ou trop systématique du silence électromagnétique pourrait vite être perçu comme le signe d'une attaque imminente. Finalement, il s'agit bien de « ne faire ni ce qu'on attend de nous, ni le contraire, mais tout autre chose[65] ».

60. « Deception Maxims: Fact and Folklore », Washington D.C., Office of Research and Development, CIA, 1980.
61. Une méthode de la communauté du renseignement américaine pour parvenir à ce type de *monitoring* est décrite ici : « A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis », Prepared by the US Government, mars 2009, disponible sur : www.cia.gov.
62. T. Holt, *The Deceivers: Allied Military Deception in the Second World War*, New York, Scribner, 2010, p. 54-61.
63. V. Desportes, « L'Autre en stratégie », *DSI*, n° 133, janvier-février 2018, p. 72-78.
64. J. D. Monroe, « Deception: Theory and Practice », Naval Postgraduate School Thesis, juin 2012, p. 66.
65. Capitaine Stéphane, « La guérilla en montagne », *Revue historique de l'armée*, 1968, n° 3, p. 163-180.

**Schéma 2. Les facteurs de réussite de la déception**




Bien entendu, chaque situation est unique et les modes d'action mis en œuvre peuvent prendre des formes multiples, la seule limite étant l'imagination humaine. Cependant, la compréhension théorique de la logique des opérations de déception est indispensable au praticien pour lui servir de garde-fou et lui éviter de penser que tout succès dans ce domaine n'est dû qu'à la chance ou à l'incompétence de l'adversaire.

# Déception et manœuvre

La nature de la déception et ce que l'on s'autorise à faire ou non dans le cadre d'une manœuvre vont dépendre des enjeux du conflit considéré (limité ou total). Par ailleurs, la déception n'agit jamais pour elle-même. Elle n'est pas une manœuvre en soi, mais doit, pour être exploitée, s'intégrer dans un effort d'ensemble visant un résultat plus positif. En découle que les enjeux et les modes d'action des opérations de déception sont différents selon que l'on se place au niveau stratégique ou au niveau tactico-opératif. Pour autant, les dilemmes qui se posent au chef militaire à chacun de ces niveaux sont bien souvent de nature similaire.

## Les dilemmes de la déception

Les opérations de déception posent plusieurs dilemmes d'ordre culturel, éthique et pour l'emploi des forces. Ils représentent l'une des explications du peu d'utilisation des opérations de déception en France. Ils éclairent aussi sur la difficulté à planifier et à conduire ce type d'action.

Tout d'abord, sur le plan culturel, il a souvent été avancé que la ruse, et donc la déception, aurait historiquement été marginalisée par un « modèle occidental de la guerre » la jugeant à la fois inefficace et illégitime. Il n'en est rien. La ruse n'est pas absente de l'histoire stratégique occidentale[66]. En fait, ce qui évolue c'est l'intensité de son emploi dans le temps :

> « Certaines cultures sont plus enclines à la déception que d'autres, mais seulement sur une période donnée. Aucune culture n'a excellé dans le domaine de la déception pendant toute son histoire.[67] »

Pour l'Occident, le goût du stratagème a décliné à partir de la bataille d'Eylau (1807) et jusqu'à la Seconde Guerre mondiale. En cause : des effectifs de plus en plus importants qui autorisent des pertes plus élevées, des idéologies messianistes qui poussent au sacrifice et des armées de masse qui sont difficilement manœuvrables[68]. Cependant, si toutes les cultures ont utilisé la ruse, il faut bien admettre que certaines ne la favorisent pas. La volonté d'aller droit à l'objectif, qui a pu apparaître comme

66. Sur cette question, lire J.-V. Holeindre, *La ruse et la force*, *op. cit.*
67. B. Whaley, *Practise to Deceive: Learning Curves of Military Deception Planners*, Annapolis, Naval Institute Press, 2016, p. XII.
68. M. Motte, G.-H. Soutou, J. de Lespinois, et O. Zajec, *La mesure de la force : traité de stratégie de l'École de guerre*, Paris, Tallandier, 2018.

une caractéristique occidentale, présente notamment dans la tradition philosophique gréco-latine, laisse peu de place à la déception :

> « Nous dressons une forme idéale (*eidos*), que nous posons comme but (*telos*) et nous agissons ensuite pour la faire passer dans les faits[69]. »

En comparaison, la pensée antique chinoise a pu mettre en avant une attitude différente : « au lieu d'imposer son plan au monde, [elle] s'appuie sur le potentiel de situation[70] ». Le stratège suivant ce principe est concentré sur le cours des choses tel qu'il y est engagé pour en déceler la cohérence et profiter de son évolution. Plutôt qu'au couple « moyens-fins », il s'attache à celui « conditions-circonstances ». Ainsi, le bon général attaque au moment le plus facile car il ne faut pas chercher l'effet, mais se mettre en position de le recueillir. Cet état d'esprit est plus favorable aux opérations de déception. Au-delà de ces réflexions générales qui tendant parfois à l'essentialisme, la culture institutionnelle d'une armée peut favoriser la déception. C'est le cas de l'armée sud-africaine pour trois raisons principales : elle a longtemps été marquée par l'usage de tactiques de guérilla (Voortrekkers, Boers, Angola, etc.), dans le folklore afrikaner les histoires de ruse ont une place de premier plan et l'importance de la déception est inculquée aux officiers dès leur formation initiale[71].

Toujours dans le domaine culturel, les opérations de déception posent aussi problème de par la prise de risque qu'elles impliquent. En effet, pour les mettre en œuvre, il faut que le chef ait suffisamment confiance en lui-même et en ses unités pour accepter de se priver d'une partie de ses forces au point d'application de son effort[72]. Or, aujourd'hui, en France,

> « le risque est la plupart du temps vécu comme une contrainte, un défaut de la guerre, et la décision vise avant tout à en limiter l'impact possible ou prévisible sur la manœuvre. Ceci est, fondamentalement, un non-sens. En effet, le risque doit être utilisé, et donc vécu, par le chef comme une *chance*, à saisir ou pas.[73] »

Cette conception dépasse largement les cercles militaires. L'inscription du principe de précaution dans la constitution en est une illustration.

69. François Jullien, *Traité de l'efficacité*, Paris, Le Livre de poche, 2011. La culture militaire Hindoue est un autre exemple : « bien que les exemples de déceptions existent, le code hindou de la guerre se distingue dans l'Histoire par l'esprit chevaleresque », Général K. Singh cité par O. Fort, *L'artillerie des stratagèmes*, Paris, Economica, 2016, p. 119.
70. *Ibid.*, p. 32.
71. O. Fort, *L'artillerie des stratagèmes*, *op. cit*, p. 119-125. C'est aussi le cas chez les US Marines.
72. On estime généralement que la déception ne doit pas consommer plus d'un tiers du total des forces. Chef d'escadron Casanova, « La déception tactique (1ère partie) », *Objectif Doctrine*, septembre 2000, p. 52-57.
73. M. Yakovleff, *Tactique théorique*, *op. cit.*

Cette aversion au risque qui est devenue une dimension structurante de notre société limite considérablement les options d'un décideur, militaire ou non, et réduit l'attractivité d'une opération de déception. Il n'est bien entendu pas question d'y « jouer son va-tout[74] ». Il faut savoir mesurer le risque avec un critère d'acceptabilité clair et avoir élaboré une manœuvre alternative en cas d'échec du stratagème.

Vient ensuite un dilemme d'ordre éthique et juridique. Le recours à la ruse et à la déception soulève souvent des questionnements, voire un rejet : Il pourrait être contraire à l'honneur de la guerre, voire illégal. Ainsi, le droit des conflits armés fait clairement la distinction entre la ruse (légale) et la perfidie (illégale) :

> « Constituent une perfidie les actes faisant appel, avec l'intention de la tromper, à la bonne foi d'un adversaire pour lui faire croire qu'il a le droit de recevoir ou l'obligation d'accorder la protection prévue par les règles du droit international applicable dans les conflits armés. Les actes suivants sont des exemples de perfidie : a) feindre l'intention de négocier sous le couvert du pavillon parlementaire, ou feindre la reddition ; b) feindre une incapacité due à des blessures ou à la maladie ; c) feindre d'avoir le statut de civil ou de non-combattant ; d) feindre d'avoir un statut protégé en utilisant des signes, emblèmes ou uniformes des Nations Unies, d'États neutres ou d'autres États non Parties au conflit.[75] »

Au-delà de cette question juridique, relativement aisée à trancher, la problématique est aussi éthique. Il est difficile, pour une démocratie d'utiliser certaines méthodes s'inscrivant dans une démarche de déception : la transparence est une valeur sans cesse valorisée, de même que le devoir de vérité de l'exécutif à l'égard des citoyens comme des contre-pouvoirs (parlement, corps intermédiaires), les médias ne peuvent pas être contrôlés, etc. Les opérations psychologiques offrent un bon exemple de ces contraintes éthiques et politiques. Selon la doctrine interarmées française, elles doivent se conformer au principe de véracité

74. « Le problème de la déception », École supérieure de guerre, 74e promotion, 1961.
75. Article 24 du règlement concernant les lois et coutumes de la guerre, signé à La Haye le 18 octobre 1907 ; Articles 37 à 39 du protocole I du 8 juin 1977, additionnel aux conventions de Genève du 12 août 1949, disponible à l'adresse : ihl-databases.icrc.org. J-B. Jeangène Vilmer, « Éthique et stratégie » in J. Henrotin, O. Schmitt, et S. Taillat (dir.), *Guerre et stratégie: approches, concepts*, 1ère édition., Paris, PUF, 2015, p. 171-195.

des messages et des informations diffusés par la force afin d'assurer et sa crédibilité[76].

La troisième catégorie de dilemmes concerne l'emploi des forces. Il y a, en effet, une concurrence apparente entre l'économie des forces – un des trois principes de la guerre reconnus dans la doctrine française – et les opérations de déception[77]. Pour Clausewitz, la ruse est un obstacle qui empêche la force de se déployer pleinement :

> « Il est en effet dangereux de n'user qu'en apparence de forces considérables pendant un certain laps de temps. On risque toujours que ce soit en vain, et de voir ces forces faire défaut plus tard au point décisif.[78] »

Il est vrai que, pour être crédibles, les opérations de déception nécessitent des moyens. L'équilibre avec l'action principale est toujours difficile à trouver. La problématique est encore renforcée aujourd'hui par le manque de masse – pour les effectifs comme pour les équipements – qui caractérise la plupart des armées occidentales. Cependant, les forces nécessaires pour réussir une opération de déception ne doivent pas être surestimées. *Fortitude*, certainement la plus ambitieuse de l'histoire, a mobilisé environ 4 500 personnes, soit 0,2 % du potentiel de combat de la force alliée, 0,5 % des navires et 0,6 % des sorties aériennes du jour J[79]. Un coût modeste comparé aux 19 divisions allemandes maintenues en réserve pendant 66 jours grâce à elle.

Il existe aussi une tension entre l'ordre nécessaire à une opération de déception et le chaos inhérent aux opérations militaires. La maxime bien connue, et fréquemment vérifiée, « aucun plan de bataille ne survit au premier contact avec l'adversaire » n'encourage pas à échafauder des opérations de déception complexes à coordonner. La simplicité, souvent mise en avant lorsqu'il s'agit de comparer des modes d'actions, met facilement de côté toute manœuvre ambitieuse de déception[80].

76. Ceci concerne les psyops « blanches », effectuées en toute transparence par les forces conventionnelles. « Des opérations grises (l'auteur n'est pas spécifié) ou noires (un faux auteur est spécifié) peuvent en revanche être pratiquées par les forces spéciales ou les services de renseignement », cité *in* R. Mielcarek, « L'armée française se remet progressivement à l'action psychologique », *DSI*, hors série, n°41, avril-mai 2015, p. 58-62.

77. Les deux autres sont la concentration des efforts et la liberté d'action.

78. C. von Clausewitz, *De la Guerre*, Paris, Éditions de Minuit, 1955, p. 213. Il est vrai qu'au XIXe siècle les moyens de communication très limités rendaient complexe la réussite d'une diversion. Cette analyse est d'ailleurs partagée par Jomini.

79. B. Whaley, « The 1 % Solution: Costs and Benefits of Military Deception » *in* J. Arquilla et D. Borer (dir.), *Information Strategy and Warfare*, Routledge, 2007, p. 127-159.

80. R. Powl Smith, « BCTP: Be Unpredictable, Take Risks-or Lose », *Field Artillery*, mars-avril 1997, p. 16-21.

En conduite, « la bataille est une orgie de désordre[81] ». Or, les opérations de déception requièrent une organisation détaillée et un certain degré de centralisation. Une solution possible pour tenter de dépasser ces tensions consiste à ne pas adopter de manœuvre de déception qui soit à l'opposé de la manœuvre réelle afin que la cohérence entre les deux puisse être assurée à moindre coût.

Tous ces dilemmes et ces tensions entre les opérations de déception et notre culture, notre éthique et la pratique du combat expliquent en partie le peu d'empressement à les utiliser. Inversement, cette marginalité relative peut rendre la déception d'autant plus attractive aux yeux d'adversaires qui ne partageraient pas nos états d'âme. Afin de se prémunir d'une telle menace, il est indispensable de s'attacher à étudier la déception en relation avec les trois niveaux de la guerre que sont le stratégique, l'opératif et le tactique.

## La déception au niveau stratégique

La déception au niveau stratégique a pour objectif premier de manipuler les décideurs politiques, les chefs militaires de très haut rang, ou les opinions publiques adverses. L'objectif peut être de complexifier la prise de décision, de favoriser ses intérêts, ou encore de créer une surprise stratégique[82]. À ce niveau, les outils à la disposition des décideurs proviennent de domaines très divers : politique, économie, diplomatie, services spéciaux, etc. Le militaire y a, bien entendu, sa place mais celle-ci n'est généralement pas centrale.

La pratique russo-soviétique de la *maskirovka* est le parfait exemple de cette approche globale de la déception. Intégrant les niveaux de la guerre du stratégique au tactique, elle est utilisée aussi bien en période de guerre qu'en temps de paix. L'échelon politique le plus haut est impliqué, en particulier avant le déclenchement d'un conflit, de façon à créer la surprise[83]. La crise des missiles de Cuba en 1962 est un bon exemple. Au cours de celle-ci, l'URSS mène une manœuvre de déception globale. Tandis qu'il prépare l'installation de missiles nucléaires SS-4 et SS-5 sur l'île des Caraïbes, le Kremlin déclare officiellement, et à plusieurs reprises, fournir de l'aide aux paysans cubains. Khrouchtchev lui-même met l'accent sur les affaires agricoles dans ses discours. Les diplomates soviétiques multiplient les messages rassurants. À l'inverse, des « demi-vérités » quant

81. G. S. Patton, « Why Men Fight? », 1927, in *Military Essays and Articles 1885-1945*, The George S. Patton Historical Society, 2002.
82. C. Brustlein, « La surprise stratégique. De la notion aux implications », *Focus stratégique*, n° 10, Ifri, octobre 2008, disponible sur : www.ifri.org.
83. D. M. Glantz, *Soviet Military Deception in the Second World War*, *op. cit.*, p. 3.

à une aide militaire sont distillées à des groupes d'opposants cubains que Moscou sait jugés peu fiables par la CIA. Leurs rapports inondent l'agence américaine, ce qui contribue à la « désensibiliser » vis-à-vis de toute rumeur d'installation de missiles[84]. Au niveau militaire, tout est fait pour préserver le secret. Par exemple, aucun moyen de transmission électronique n'est utilisé et tous les mouvements logistiques sont effectués de nuit. Le nom de l'opération, Anadyr, une rivière du nord de la Sibérie, est lui-même une tentative de déception, à destination des soldats soviétiques comme des Occidentaux, alors que des équipements arctiques sont distribués aux troupes se dirigeant vers l'île[85]. Si les Soviétiques échouent à cacher les sites de missiles, ils réussissent en revanche à infiltrer plus de 42 000 militaires à Cuba là où les Américains n'estiment pas leur présence au-delà de 4 000 ou 5 000[86].

La déception stratégique requiert une structure de coordination robuste. À ce niveau, si l'on veut obtenir un véritable effet, tous les échelons subordonnés doivent mettre en œuvre des mesures du même type. La coordination doit aussi être verticale. Il faut pouvoir accéder aux plus hautes autorités de l'État si l'on souhaite faire jouer les leviers politiques et diplomatiques. Ainsi lors de la Seconde Guerre mondiale, les Britanniques ont progressivement mis en place des outils de coordination d'une grande efficacité[87]. Cette transformation réussie est en particulier le résultat d'un effort de coordination[88]. Fort de l'exemple de la Force A pour le niveau opératif en Afrique du Nord[89], un *controlling officer* est nommé en octobre 1941 au sein du *Joint Planning Staff* afin de coordonner les opérations de déception au niveau stratégique. Il forme la *London controlling section* (LCS). Après des débuts difficiles, 1942 marque un tournant[90]. La LCS se développe sous l'impulsion d'un nouveau chef. Le 21 juin 1942, une directive est enfin signée par le *Joint Planning Staff*. La LCS a une mission claire : prendre en charge la préparation des plans de déception au niveau mondial, la coordination des actions de déception des

84. J. H. Hansen, « Soviet Deception in the Cuban Missile Crisis » *Studies in Intelligence*, vol. 46, n° 1, 2002, p. 49-58.
85. A. I. Gribkov, W. Y. Smith, et A. Friendly, *Operation ANADYR: U.S. and Soviet Generals Recount the Cuban Missile Crisis*, Chicago, Edition Q, 1994.
86. D. T. Moore and W. N. Reynolds, « So Many Ways to Lie: The Complexity of Denial and Deception », *American Intelligence Journal*, vol. 32, n° 2, p. 61-70.
87. J. Latimer, *Deception in War*, New York, Overlook Press, 2003.
88. Le « Twenty Committee » (pour le chiffre romain XX, « *double cross* ») préexistait à cette structure, mais il n'était en charge que de la gestion des agents doubles. J. C. Masterman, *The Double-Cross System: The Incredible Story of How Nazi Spies Were Turned into Double Agents*, Guilford, Connecticut, Lyons Press, 2012, p. 9.
89. Sur la force A, lire notamment : J. Deuve, « Déception au Moyen-Orient et en Tripolitaine (1940-1941) », *Guerres mondiales et conflits contemporains*, 2008, vol. 229, n° 1, p. 103.
90. J. C. Masterman, *The Double-Cross System*, *op. cit.*, p. 107.

différents théâtres, et vérifier que les actions de déception sont correctement menées par les différents services et ministères[91]. Une coordination avec les Américains est aussi mise en place. Au final, même si cette structure a souffert de son manque d'autorité sur les différents services, son action a permis de répandre les bonnes pratiques.

À la même époque, les Soviétiques font eux aussi cet effort de structuration. À partir de 1943, les opérations de déception des différents fronts sont synchronisées par la *Stavka*, état-major du commandement suprême[92]. Cette centralisation permet en particulier des bascules de force secrètes entre les fronts afin de mener des attaques surprises. À l'inverse, l'une des principales raisons de l'échec relatif des opérations de déception américaines dans le Pacifique tient à l'absence de structure de coordination. Le *Joint Security Control* (JSC), petite structure intégrée au *Joint Chiefs of Staff,* lutta jusqu'à la fin de la guerre pour se faire une place. Fin 1944, il est officiellement chargé de rédiger les « annexes déception » des plans de guerre, mais il n'a jamais obtenu d'accès aux plus hautes autorités[93].

Tous les modes d'action décrits dans la typologie peuvent être utilisés au niveau stratégique, même si la désinformation et l'intoxication semblent y prendre une place de plus en plus importante. C'est le résultat de l'accroissement de la connectivité au niveau mondial, mais peut-être aussi la reconnaissance que les moyens de détection sont trop puissants pour pouvoir véritablement dissimuler une action d'ampleur[94]. C'est d'ailleurs une évolution que l'on peut constater pour la *maskirovka*. Employée dès 2014 par la Russie à l'occasion de la crise en Ukraine, elle a servi à masquer l'engagement militaire, à dissuader les interventions extérieures et à influencer l'opinion publique nationale et internationale. En Crimée, avec l'utilisation, désormais bien connue, des « petits hommes verts » qui s'emparent d'infrastructures clés le 27 février 2014, il s'agit en fait de mettre en avant un « mensonge plausible » afin de créer de l'ambiguïté et d'offrir à Moscou une liberté d'action stratégique. Jusqu'à l'annonce de l'annexion, les responsables politiques russes s'évertueront à nier l'existence de toute action militaire russe[95]. Le gouvernement ukrainien avait conscience de la présence de ces forces mais n'a pas été capable de déterminer leur

91. M. Howard, *British Intelligence in the Second World War: Strategic Deception*, New York, Cambridge University Press, 1990.
92. D. M. Glantz, *Soviet Military Deception in the Second World War*, *op. cit.*, p. 562.
93. K. L. Herbig, « American Strategic Deception in the Pacific », *Intelligence and National Security* », vol. 2, n° 3, 1967, p. 260-300.
94. M. Maier, « A Little Masquerade: Russia's Evolving Employment of Maskirovka », School of Advanced Military Studies, United States Army Command and General Staff College, 2016.
95. M. Snegovaya, « Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare », Institute for the Study of War, 2015.

intention. Il a alors choisi de se restreindre de peur de provoquer une escalade de la violence, voire une invasion générale, comme cela avait été le cas en Géorgie[96]. De façon plus large, les Occidentaux se sont fourvoyés sur les intentions de Moscou en estimant que ce « mensonge plausible » visait à créer les conditions pour engager une négociation.

## La déception aux niveaux opératif et tactique

Aux niveaux tactique et opératif, la manœuvre de déception idéale est celle qui permet de tromper l'ennemi sur l'attitude générale des forces amies à l'échelon considéré[97]. Une opération de déception réussie fait se concentrer les forces ennemies au mauvais endroit, l'affaiblissant ainsi au point décisif de l'action. Si cet idéal n'est pas acquis, il y a tout au moins de grandes chances de pouvoir ralentir le processus décisionnel de l'adversaire ou de le forcer à disperser ses efforts s'il ne parvient pas à lever le doute. La déception participe ainsi clairement à la survivabilité des forces – un point crucial étant donné l'accroissement de la létalité sur le champ de bataille[98]. Dans son étude de 138 cas historiques de 1914 à 1967, B. Whaley montre que lorsque l'adversaire est surpris grâce à une opération de déception le taux de pertes est de 1 pour 6,3 contre 1 pour 2 pour une surprise obtenue grâce à un autre procédé et 1 pour 1,1 lorsqu'il n'y a pas d'effet de surprise[99]. Contrairement au niveau stratégique, il est possible de mener une opération de déception tactique avec des procédés relativement simples. Néanmoins, la mise en œuvre d'un plan de déception impose un niveau tactique « haut », correspondant traditionnellement à la division ou au corps d'armée[100]. Cependant, il semble aujourd'hui possible de descendre au niveau du GTIA dans le cadre des conflits de basse intensité.

Mener une opération de déception est possible dans tous types de conflits. Dans le cadre des guerres asymétriques, il est tentant pour le plus puissant de ne recourir qu'à la force, d'autant qu'il est souvent difficile de conserver le secret lorsqu'on agit au milieu d'une population qui est aussi

96. M. Kofman, *Lessons from Russia's Operations in Crimea and Eastern Ukraine*, Santa Monica, RAND Corporation, 2017, 109 p.
97. Chef de bataillon Lemattre, « La déception dans les opérations de surface en milieu hostile », *L'Armée*, n° 6, septembre 1960.
98. R. Hémez, « La survivabilité sur le champ de bataille, entre technologie et manœuvre », *Focus stratégique*, n° 72, Ifri, mars 2017, disponible sur : www.ifri.org.
99. B. Whaley, *Stratagem: Deception and Surprise in War*, Boston, Artech House, 2007, p. 104.
100. Notice provisoire sur l'emploi de la brigade dans le cadre de la division française, armée de Terre, 1959.

régulièrement un indicateur pour les insurgés[101]. Trop fréquemment, la ruse est abandonnée au plus faible, lequel est obligé d'y recourir pour compenser son désavantage. Lors de la seconde guerre de Tchétchénie (1999-2009) par exemple, les insurgés souffrant d'un rapport de force largement défavorable ont souvent eu recours à des « bases-pièges » destinées à attirer les Russes loin de leurs vrais maquis[102]. Pour ce faire, des fuites d'information étaient organisées et des simulations visuelles mises en place (fumées, mouvement, etc.). La zone était méthodiquement minée tandis qu'une embuscade était préparée contre les forces russes à l'approche.

Pour autant, dans un contexte asymétrique, la déception tactique est aussi possible – et souhaitable – pour le « fort ». L'exemple d'*Altor Incudine*, opération menée par les unités françaises en Afghanistan (16-18 juin 2010), est à ce titre éclairant[103]. Afin de créer les conditions nécessaires pour que le détachement de fouille opérationnelle spécialisée (FOS) puisse être engagé dans le village de Badspah, à l'est de la vallée d'Uzbin, la task force *Altor* va simuler la construction d'un faux avant-poste dans la vallée voisine de Sper Kundai. Pour crédibiliser l'action, un SGTIA assure même la protection des sapeurs et des devis sont demandés à des entrepreneurs locaux. Parallèlement à l'infiltration de deux compagnies pour l'action principale, une opération héliportée simule des posers de combattants sur un col au nord des villages insurgés afin de semer le trouble. La déception est un succès. Des insurgés en train de préparer une attaque sur ce faux avant-poste sont même détectés, et le village est abordé par surprise.

Se pose régulièrement la question de la place de la déception dans la manœuvre. Il est en fait nécessaire de rappeler l'unicité de cette dernière. La déception n'agit jamais pour elle-même et l'effet qu'elle produit ne résulte pas d'une activité spécifiquement dédiée à la déception. Mystifier l'ennemi, c'est toujours mener une manœuvre inattendue, renforcée par la tromperie. Pour être efficace, la déception doit donc être pleinement intégrée à la manœuvre qui, elle-même, participe à la déception[104]. Les activités de déception doivent être séquencées de façon à maximiser la persistance de la fausse hypothèse et couvrir, dans l'idéal, la totalité de la

101. R. Hémez, « Tactical Surprise in Small Wars: Lessons from French Wars in Afghanistan and Mali », *Long War Journal*, 2 mai 2017, disponible sur : smallwarsjournal.com.
102. T. L. Thomas, « Russian Tactical Lessons Learned Fighting Chechen Separatists », *The Journal of Slavic Military Studies*, vol. 18, n° 4, 2005, p. 731-766.
103. C. Lafaye, « Le génie en Afghanistan. Adaptation d'une arme en situation de contre-insurrection (2001-2012) hommes, matériels, emploi », Thèse, 2013, p. 359-362 ; R. Oudot de Dainville, « Opération Altor Incudine : un coup de main niveau GTIA », *Le Casoar*, n° 200, janvier 2011, p 29.
104. C. de Lajudie, « La déception », site *Pensée Mili-Terre*, disponible sur : www.penseemiliterre.fr.

manœuvre (et pas seulement les phases préliminaire et initiale), même si bien entendu les effets recherchés peuvent décroître dans le temps.

La mise en œuvre de la déception aux niveaux opératif et tactique renvoie aussi à la nécessité de réapprendre certains savoir-faire fondamentaux, parfois délaissés du fait du « confort opératif » dont ont pu jouir les forces occidentales depuis la fin de la guerre froide. Par exemple, pour favoriser la discrétion, la notion de camouflage doit être remise au goût du jour, alors qu'elle a été un peu laissée pour compte au cours des conflits récents. Il en va de même des règles de discrétion électromagnétique comme le silence radio avant l'engagement[105]. Dernier exemple, il est nécessaire que les postes de commandement (PC) retrouvent leur agilité pour qu'ils soient plus discrets. La complexité croissante des opérations, du fait notamment des flux d'information, rend la coordination de plus en plus difficile avec pour conséquence l'inflation des effectifs des PC[106]. En 1961, un PC de division comptait 260 hommes ; en 2018, il n'en mobilise pas moins de 550 personnes (dont une compagnie d'infanterie) lesquels ont besoin de 55 abris modulaires poste de commandement (AMPC). Les PC de brigade, eux, sont passés de 20 personnes en 1944 à 162 en 2017[107]. L'inflation des PC joue sur l'agilité intellectuelle du commandement et pèse sur sa performance. De façon générale, le travail d'état-major tend trop souvent à la production de produits consensuels. Le labyrinthe de la bureaucratie interarmées, voire interalliée, est souvent si complexe qu'il rend difficile de mettre en œuvre des opérations de déception.

Enfin, se pose aussi la question de la pertinence de détenir des unités dédiées aux opérations de déception. En effet, pour qu'une opération de déception soit crédible, il faut y consacrer des moyens qui entrent inévitablement en concurrence avec ceux destinés à l'action principale. Avoir des unités spécialisées pourrait apaiser ce dilemme. Bien que peu nombreux, des exemples historiques existent. Pendant la Seconde Guerre mondiale, les retours d'expérience des premières opérations de déception menées par les Américains en Tunisie soulignent qu'elles pourraient être plus efficaces si elles étaient, en partie, mises en œuvre par des spécialistes[108]. C'est ainsi que naquit le 23rd *Headquarters Special Troops*, surnommée *Ghost Army*, une unité d'un millier d'hommes qui comprenait un bataillon du génie équipé de leurres gonflables, une compagnie de

105. F. Jordan, « Plaidoyer pour une *maskirovka* à la française », *art. cit.*
106. B. Durieux, « La manœuvre future », *in* C. Malis (dir.), *Guerre et manœuvre : héritages et renouveau*, Paris, Economica, 2009, p. 253-263.
107. K. Assad et L. Puga, « Comment réduire la vulnérabilité des postes de commandement de niveau tactique en opérations ? », Cours supérieur interarmes, CDEC, 2018.
108. Official History of the 23rd Headquarters Special Troops, p. 1.

transmissions spécialisée dans le contre-renseignement, et une autre dédiée à la simulation sonore. Après des débuts difficiles, cette unité connaît quelques beaux succès, comme lors de l'opération *Bettembourg*, où elle réussit à faire croire aux Allemands qu'une division blindée défend un espace en fait laissé libre par des Alliés alors occupés à rassembler leurs troupes pour attaquer Metz[109]. Des effets sonores et des véhicules gonflables furent notamment utilisés, et le subterfuge fonctionna pendant une semaine. Aujourd'hui, de par la place que jouent les technologies de l'information et des communications, il paraît raisonnable d'envisager que les unités de guerre électronique auront une place majeure dans toute opération de déception[110]. Si elles font actuellement porter l'effort sur l'écoute et le brouillage, l'accent pourrait demain être davantage mis sur leurs capacités d'intrusion dans les réseaux adverses à des fins, entre autres, de déception.

La pratique des opérations de déception montre qu'elles sont complexes à mettre en œuvre. Lorsqu'il s'agit de les envisager et de les planifier, plusieurs dilemmes surviennent. Au niveau stratégique, leur coordination est difficile et nécessite des organismes qui existent dans peu de pays, et le plus souvent uniquement en temps de guerre. Au niveau tactique, il n'est jamais facile de s'assurer de l'unicité de la manœuvre, car la déception n'est pas une « deuxième manœuvre » mais doit toujours être au service de l'action principale. Cependant, cette complexité ne saurait être un argument pour écarter les opérations de déception d'autant plus importantes étant donné le contexte opérationnel d'aujourd'hui et les tendances pour l'avenir.

109. J. Gawne, *Ghosts of the Eto American Tactical Deception Units in the European Theater, 1944–1945*, Havertown, Casemate Pub, 2002 ; R. Beyer, *The Ghost Army of World War II: How One Top-Secret Unit Deceived the Enemy with Inflatable Tanks, Sound Effects, and Other Audacious Fakery*, Princeton, Architectural Press, 2015.

110. G. Hubin, « Réflexions sur la manœuvre future » *in* C. Malis (dir.), *Guerre et manoeuvre*, *op. cit.*

# La déception d'aujourd'hui à demain

Certaines tendances actuelles semblent annoncer l'avènement d'un nouveau « blocage tactique[111] ». Après plusieurs décennies d'un relatif confort opératif, la supériorité aérienne occidentale est aujourd'hui remise en question, notamment par la prolifération de systèmes de missiles anti-aériens de plus en plus perfectionnés[112]. Les réseaux, dont les armées sont de plus en plus dépendantes, sont de façon croissante la cible de nos adversaires. La létalité sur le champ de bataille va augmentant et, de plus en plus, la détection devient synonyme de destruction. Face à ces contraintes, la dilution apparente des intentions devient un complément indispensable à la dissimulation physique[113]. Les opérations de déception, combinant un volet technologique avec des modes d'action particuliers, apparaissent comme le moyen privilégié d'atteindre cet objectif. Sur le plan stratégique, c'est dans les domaines cyber et liés à l'intelligence artificielle que les opportunités semblent être les plus grandes. Au niveau tactique, de nouvelles capacités de simulation pourront y aider. Dans tous les cas cependant, des mesures devront être prises pour conduire à un renouveau de la déception.

## Intelligence artificielle et cyber : renouveau de la déception stratégique ?

Au niveau stratégique, les progrès de l'intelligence artificielle (IA) et l'élargissement du domaine cyber laissent d'ores et déjà entrevoir des possibilités renouvelées pour la déception. L'une des principales portées stratégiques de l'IA réside dans son potentiel en matière d'aide à la décision. Avec la numérisation du champ de bataille, le volume des informations remontées est considérable, au point de pouvoir provoquer une surcharge cognitive. Il faut donc structurer ces données pour qu'elles puissent être interprétées par les décideurs. C'est ce que permet l'IA via l'exploitation directe des *big data*. Ce n'est pas sans effets dans le domaine de la déception. La capacité à détecter des signaux faibles peut contribuer à déterminer la probabilité d'occurrence d'un évènement et à déclencher les

111. R. Hémez, « Les développements techniques nous entraînent-ils vers un nouveau blocage tactique ? », *art. cit.*
112. Sur ce sujet, lire C. Brustlein, É. de Durand, et É. Tenenbaum, *La suprématie aérienne en péril : menaces et contre-stratégies à l'horizon 2030*, Paris, La Documentation française, 2014.
113. G. Hubin, *Perspectives tactiques*, Paris, Economica, 2000.

alertes éventuelles[114]. Il devrait de même être possible de mieux comprendre l'ennemi en visualisant des masses de données le concernant. Appliquée à l'aide à la décision, l'IA pourrait également proposer une grande variété de modes d'action de déception en s'appuyant sur la « mémoire » de centaines d'opérations passées. Il faut cependant ici souligner le fait que l'IA est pareillement sujette à la contre-déception. D'abord, il sera toujours possible d'interdire aux capteurs qui « nourrissent » l'IA l'accès aux signaux. De plus, dès lors que l'IA repose sur un algorithme entraîné à réaliser une tâche définie, il lui est difficile de faire preuve de discernement face à un leurre, pour peu que ce dernier réponde bien aux critères de sa programmation[115]. Enfin, il n'est pas certain que l'IA permette d'être moins prédictible. Une connaissance des algorithmes, des données utilisées et du « degré » d'entraînement (dans le cas du *machine learning*) permettrait d'évaluer les réponses données, d'autant qu'il est fort probable que l'adversaire dispose lui aussi d'IA pour l'aider dans cette tâche[116].

L'IA est de la même façon un facteur clé dans la facilité croissante à falsifier des informations[117]. Or, la désinformation joue un rôle majeur pour les opérations de déception au niveau stratégique. À ce niveau sont visées des organisations, voire une population entière et la désinformation (associée, entre autres, à la subversion et au sabotage) peut préparer le terrain (en créant de l'ambiguïté, en favorisant les dissensions, etc.) à des opérations davantage cinétiques. Elle cherche à créer de l'ambiguïté pour obtenir une situation favorable. Ce sont des actions de désinformation qui ont permis d'altérer les perceptions des intentions stratégiques russes en Crimée en 2009 et de faciliter ainsi la prise le contrôle de la péninsule en deux semaines, sans tirer un coup de feu[118]. On peut désormais créer de toutes pièces des images quasiment impossibles à distinguer de photographies[119]. Les vidéos ne sont pas épargnées, comme le montre la polémique autour de l'application *Deepfakes* permettant d'aisément

114. Comme la détection de l'imminence du déclenchement d'une attaque au travers de l'analyse des flux logistiques et de communication adverses. Entretien avec un officier français, Paris, 2 mars 2018. Sur les limites de cette approche par les signaux faibles pour prédire l'avenir : P. Silberzahn, « Ne comptez pas trop sur les signaux faibles pour anticiper l'avenir », 25 septembre 2017, disponible sur : philippesilberzahn.com.

115. Certains programmes d'IA ont cependant une capacité à apprendre à ne pas prendre en compte les leurres.

116. D'où, pour certains, l'importance de classifier les algorithmes alors que le secteur de l'IA se caractérise par sa grande transparence dans ce domaine.

117. M. Brundage *et al.*, « The Malicious Use of AI », Future of Humanity Institute, février 2018.

118. M. Snegovaya, « Putin's Information Warfare in Ukraine Soviet Origins Of Russia's Hybrid Warfare », Institute for the Study of Warfare, septembre 2015.

119. T. Karras *et al.*, « Progressive Growing of GANs for Improved Quality, Stability, and Variation », Nvidia Research, 2017.

remplacer le visage d'une personne par celui d'une autre[120]. Grâce à l'IA, transformer une vidéo tournée le jour en scène de nuit, ou un paysage enneigé en scène estivale, est aujourd'hui facile[121].

Associées à des techniques largement disponibles sur le marché, ces nouvelles capacités de falsification permettent de mener des opérations psychologiques d'une ampleur renouvelée. Ce nouvel âge de la propagande bénéficie d'une ingénierie inédite de la désinformation. Des techniques de ciblage sont utilisées depuis plusieurs années dans le marketing digital[122]. Ces derniers temps, des campagnes de *spams,* ou des armées de bots, ont été employées à maintes reprises pour tenter de manipuler l'opinion. Selon une étude de l'Université de l'Indiana parue en 2017, 9 à 15 % des comptes Twitter seraient en fait des *bots*, c'est-à-dire des programmes destinés à produire ou rediffuser certaines informations[123]. Leur nombre atteindrait 60 millions sur Facebook[124]. La création et la vente de ces agents logiciels se situent dans une « zone grise légale ». Ces faux comptes, peuvent amplifier très rapidement une rumeur et mettre à mal des entreprises, ruiner des réputations, influencer un débat politique. Ils sont la version en ligne des pseudos-opérations. On imagine facilement comment les employer dans des opérations de déception[125]. Les actions de ce type buttent pour le moment sur la facilité à identifier des faux comptes qui répètent souvent le même message et dont les photos de profils sont généralement récupérées ailleurs. À l'avenir, ils pourraient cependant bénéficier des progrès dans le domaine de la falsification en ayant la possibilité de varier considérablement les profils grâce à des visages et des voix de synthèse avec une capacité de conversation crédible[126].

120. M. Tual, « Du porno aux fausses informations, l'intelligence artificielle manipule désormais la vidéo », *Le Monde*, 4 février 2018. On peut aussi souligner les progrès de la traduction automatique. Microsoft AI translator a traduit un texte du chinois à l'anglais avec une précision comparable à celle d'une personne bilingue. Le but est d'aller vers la traduction en temps réel d'articles en ligne. Voir L. del Bello, « AI Translates News Just as Well as a Human Would », *Futurism*, 16 mars 2018.

121. T. Greene, « Nvidia's New AI Creates Disturbingly Convincing Fake Videos », *TNW*, 4 décembre 2017.

122. D. Ghosh et B. Scott, « #Digitaldeceit: The Technologies behind Precision Propaganda on the Internet », Public Interest Technology Program, janvier 2018 et D. Ghosh et B. Scott, « Russia's Election Interference Is Digital Marketing 101 », *The Atlantic*, 19 février 2018.

123. O. Varol, E. Ferrara, C. A. Davis, F. Menczer et A. Flammini, « Online Human-Bot Interactions: Detection, Estimation, and Characterization », Center for Complex Networks and Systems Research, Indiana University, Bloomington, 27 mars 2017.

124. N. Confessore, « The Follower Factory », *The New York Times*, 27 janvier 2018.

125. T. Hwang et L. Rosen, « Harder, Better, Faster, Stronger: International Law and the Future of Online Psyops », *Comprop Working Paper* n° 1, University of Oxford, 17 janvier 2017.

126. M. Ohana, O. Dunkelman, S. Gibson, M. Osadchy, « HoneyFaces: Increasing the Security and Privacy of Authentication Using Synthetic Facial Images », CoRR abs/1611.03811, 2016 ; A. van den Oord, S. Dieleman, H. Zen, « WaveNet: A Generative Model for Raw Audio », *Deep Mind*, 8 septembre 2016 ; K. Schwab « AI Is Giving Brands Eerily Human Voices », *C.O Design*, 4 février 2018.

Les campagnes d'influence profitent aussi de masses toujours plus importantes de données personnelles transmises volontairement, ou à leur insu, par les utilisateurs de sites et des réseaux sociaux[127]. Agrégées et associées à des algorithmes tenant compte des progrès dans le domaine des sciences du comportement, elles permettent un « micro-ciblage » inédit de pans entiers de la population avec des messages toujours mieux adaptés à leurs cibles[128]. Elles offrent également la possibilité d'analyser les phénomènes sociaux, comme la propagation des rumeurs et donc de mieux les manipuler[129]. Toutes ces évolutions autorisent des campagnes d'influence relativement peu coûteuses, à la diffusion extrêmement rapide et difficilement attribuable. Il est de plus possible d'obtenir des données en retour en observant si le comportement des cibles a été modifié, un critère important pour les opérations de déception[130].

Les moyens pour faire face à la montée de ce phénomène de désinformation sont limités[131]. Les algorithmes mis en place par les grandes sociétés de médias sociaux sont encore loin d'être capables de détecter les images trafiquées ou utilisées hors contexte. C'est d'autant plus problématique que les tweets incluant des photos sont deux fois plus rediffusés que ceux uniquement composés de texte. De fait, les contre-mesures reposent encore essentiellement sur les signalements des utilisateurs. Ce constat est inquiétant quand on connaît l'effet de polarisation des réseaux sociaux, la prégnance de la théorie du complot et la difficulté du public à juger de la crédibilité des sources[132]. Les sociétés modernes sont de plus en plus influencées par ce qu'elles ressentent comme étant vrai (perceptions, croyances, etc.) plutôt que par ce qu'elles savent être vrai (faits, preuves, etc.)[133]. Lorsqu'un agent extérieur cherche à influencer nos sociétés, il trouve un terreau particulièrement favorable.

127. Facebook a franchi la barre des deux milliards d'utilisateurs actifs mensuels en 2017, ce qui signifie qu'un peu plus d'un quart de la population mondiale se connecte au moins une fois par mois sur son compte ; Twitter compte 330 millions d'abonnés ; YouTube annonce 1,5 milliard d'utilisateurs actifs, etc. En 2017, en moyenne, toutes les 60 secondes, 240 000 photos sont téléchargées dans Facebook et 350 000 tweets sont envoyés (source : *Statista*).

128. T. Shaw, « The New Military-Industrial Complex of Big Data Psy Ops », *The New York Review*, 21 mars 2018.

129. A. Pentland, *Social Physics: How Social Networks Can Make Us Smarter*, New York, Penguin Press, 2015.

130. T. Hwang et L. Rosen, « Harder, Better, Faster, Stronger: International Law and the Future of Online Psyops », *art. cit.*

131. G. Wells, S. Holliday et D. Seetharaman, « The Big Loophole That Left Facebook Vulnerable to Russian Propaganda », *The Washington Post*, 22 février 2018.

132. B. Donald, « Stanford Researchers Find Students Have Trouble Judging the Credibility of Information Online », Stanford, University of Stanford, 22 novembre 2016, disponible sur : ed.stanford.edu.

133. N. Verrall et D. Mason, « The Taming of the Shrewd », *The RUSI Journal*, vol. 163, n° 1, 2018.

La manipulation de systèmes d'information par l'emploi de moyens cyber offre d'autres possibilités d'intoxication et de désinformation[134]. Par exemple, les techniques d'optimisation pour les moteurs de recherche, dites « *black hat SEO* », permettent de dominer la liste de résultats sur des mots-clés pendant quelques heures avant que Google ne corrige la distorsion. Ce type d'effet est loin d'être négligeable lorsque l'on sait qu'un tiers des utilisateurs clique sur le premier lien après les publicités et que les cinq premiers liens drainent 75 % du trafic[135]. Des exemples d'actions de ce type existent déjà. En janvier 2017, des termes recherchés tournant autour du rapport des renseignements américains sur les interférences russes dans les élections pointaient d'abord sur un article de *Russia Today* niant ces allégations[136]. Les actions offensives cyber peuvent aussi participer à des opérations de déception : déni de service, insertion de malware pour toucher les systèmes de communication et de commandement ennemis, ou opération de diversion.

Ainsi, grâce à l'IA et au cyber, les opérations psychologiques bénéficient d'un renouvellement, peut-être sans précédent, de leurs possibilités d'action, pour devenir des « armes de déception massives[137] ». À tel point que le vieil adage « il faut le voir pour le croire » pourrait être remis en question. Couplées et coordonnées avec d'autres modes d'action, ces évolutions permettent d'envisager la déception autrement. Si le niveau stratégique est aujourd'hui le plus visé, l'un des enjeux majeurs pour demain est de disposer de capacités cyber à bas niveau (forces spéciales puis GTIA, voire SGTIA)[138]. Une des difficultés principales pour y parvenir relève de l'impérative déconfliction évoquée *supra*, très difficile à réaliser dans le domaine cyber, lui qui a une capacité inhérente à dépasser les organisations et à franchir les frontières en un clic.

134. Dans le domaine de la cybersécurité, le terme « déception » est couramment utilisé. Apparu dans ce champ dans les années 1990 suite au constat qu'aucune organisation ne pouvait se protéger à 100 % des cyberattaques, il recouvrait à l'origine essentiellement le concept de *honeypot*, un ordinateur configuré pour ressembler à un serveur typique d'une entreprise aux yeux des outils automatiques qu'utilisent les hackers à la recherche de cibles. La déception dans le domaine de la cybersécurité a pris depuis des formes multiples, plus actives, via l'emploi de leurres. S. R. Calder, « A Case for Deception in the Defense », *Military Cyber Affairs*, vol. 2, n° 1, 2016.

135. J. Lee, « No. 1 Position in Google Gets 33 % of Search Traffic [Study] », *Search Engine Watch*, 20 juin 2013 ; M. Jacobson, « How Far Down the Search Engine Results Page Will Most People Go? » *Leverage Marketing*, disponible sur : www.theleverageway.com ; L. Kaye, « 95 Percent of Web Traffic Goes to Sites on Page 1 of Google Serps (Study) », *Brafton*, 21 juin 2013.

136. K. Waddell, « Kremlin Sponsored News Does Really Well on Google », *The Atlantic*, 25 janvier 2017.

137. R. M. Clark et W. L. Mitchell, *Deception*, *op. cit.*, p. 122.

138. A. White, « Screen Shots », *Jane's Intelligence Review*, janvier 2018, p. 50-53.

## Détection contre simulation, ou le futur de la déception tactique

Aux niveaux tactique et opératif se joue une véritable lutte entre capacités de détection et de simulation. Cette dynamique a des répercussions très importantes sur les opérations de déception. Pour beaucoup d'analystes, les évolutions en matière de détection vont vouer – ou vouent déjà – à l'échec toute tentative de surprendre l'ennemi. Cinq tendances principales rendent de plus en plus difficile la dissimulation physique[139].

- La première est la multiplication des capteurs : drones aériens ou sous-marins, capteurs autonomes, cyber (y compris en sources ouvertes), etc. En comparaison, il convient de garder à l'esprit que jusqu'à la fin de la Seconde Guerre mondiale, l'observation du champ de bataille était quasi exclusivement visuelle ou utilisait les premiers radars (pour l'espace aérien).
- La deuxième tendance est la collecte d'une variété de plus en plus grande de signaux par ces capteurs, permettant d'éviter « l'effet paille[140] ».
- La persistance croissante de l'observation est la troisième tendance, pour le moment essentiellement le fait des drones. Demain, de nouveaux vecteurs comme les stratollites (ballons haute altitude) y contribueront.
- La quatrième tendance correspond à la progression rapide de la précision des capteurs. C'est vrai dans le domaine des satellites (le CSO-2 français devrait avoir une résolution de 20 centimètres) mais aussi sur le plan tactique avec, par exemple, des caméras spectrales en mesure d'enregistrer des images dans neuf bandes infrarouges, contre trois pour l'œil humain, ce qui aiderait, notamment, à la détection de véhicules camouflés[141].
- La cinquième et dernière tendance est l'accélération de la vitesse de transmission des informations, diffusées en temps réel aux décideurs politiques, aux chefs militaires et aux analystes.

Mises ensemble, ces cinq dynamiques créent un niveau de transparence inconnu jusqu'ici. Elles changent d'autant plus la donne,

139. K. A. Lieber and D. G. Press, « The New Era of Counterforce. Technological Change and the Future of Nuclear Deterrence », *International Security*, vol. 41, n° 4, printemps 2017, p. 9-49.
140. L'effet paille désigne le phénomène où un chef militaire n'a qu'une vue très partielle de son environnement à cause d'un nombre et d'un type limités de capteurs.
141. L. Lagneau, « Développée par Silios Technologies et Safran, la caméra 2SID rend le camouflage inefficace », *Zone Militaire*, 24 décembre 2017.

qu'elles ne se limitent pas aux pays les plus avancés en particulier parce que nombre des technologies évoquées sont duales. Cependant, se concentrer sur l'amélioration de capacités de détection revient à mal comprendre le concept de déception, qui ne se limite pas à la dissimulation et inclut la simulation et l'intoxication. C'est aussi perdre de vue que la tactique, comme la stratégie, est un duel : les nouveaux procédés et progrès technologiques ne font pas que contrer la déception, certains la favorisent également[142] :

> « obtenir une connaissance parfaite de son ennemi est tributaire d'un ennemi stupide incapable de suivre le rythme avec des contre-mesures pertinentes. De tels d'ennemis sont rares.[143] »

Par exemple, dans le domaine des leurres, des équipements beaucoup plus évolués que les méthodes traditionnelles associent au visuel une signature thermique, infrarouge, voire radar en intégrant, par exemple, des résistances et des tissus conducteurs[144]. Malgré leur efficacité et leur relative simplicité d'emploi (15 minutes de mise en œuvre pour deux soldats), ces leurres terrestres sont encore très peu répandus. Entrés en service dans l'US Army à la fin des années 1980, les *Multispectral close combat decoys* (MCCD) furent peu employés sur le terrain, faute de doctrine d'emploi[145]. L'armée russe semble en revanche avoir quant à elle renouvelé son intérêt pour ce type d'équipement[146]. Les armées françaises n'en disposent pas.

Demain, il sera possible d'aller beaucoup plus loin. Les avancées de la guerre électronique permettent ainsi d'imaginer la création de fausses unités numériques. Le maniement d'essaims de drones pourrait aussi être envisagé afin de simuler des formations d'aéronefs de plus grande taille, ou simplement de saturer les capteurs ennemis. À plus long terme, la technologie holographique, qui n'en est qu'à ses prémisses, pourrait être exploitée pour créer des leurres visuels convaincants – dans la mesure où

142. R. Hémez et L. Nerich, « Combat terrestre futur : vers un retour de la déception », *DSI*, n° 134, mars-avril 2018, p. 86-91.
143. D. Betz, *Carnage and Connectivity*, Londres, Hurst, 2015, p. 179.
144. Voir, par exemple, les leurres gonflables de l'entreprise thèque Inflatech (www.inflatechdecoy.com) ou ceux de Saab, en métal ou gonflables (saab.com).
145. K. S. Blanks « An Effectiveness Analysis of the Tactical Employment of Decoys », U.S. Army, n.d. Les MCCD sont des leurres thermiques via de l'air chaud et visuels.
146. A. E. Kramer, « À New Weapon in Russia's Arsenal, and It's Inflatable », *The New York Times*, 12 octobre 2016 ; R. Beckhusen, « The Russian Army Is Inflating Giant Dummy Tanks », *War is Boring*, 1er décembre 2017.

elle deviendrait portable avec un affichage suffisamment grand et une résolution adaptée[147].

La dissimulation profite, elle aussi, des progrès technologiques. En ce qui concerne le camouflage, des revêtements absorbant les ondes radars existent d'ores et déjà, et certaines peintures ont des propriétés de plus en plus intéressantes. Des équipements de camouflage « dynamique » sont aussi en développement à l'instar du système *Adaptiv* de BAE Systems, constitué de tuiles thermoréactives permettant de masquer l'empreinte thermique d'un engin ou de lui donner les propriétés d'un autre[148]. Le camouflage devient ainsi un procédé de dissimulation n'étant plus uniquement visuel mais bien multispectral[149]. Les capacités « obscurcissantes » qui ont peu à peu disparu des stocks des armées occidentales pourraient faire leur retour. Les fumigènes par exemple, connus dès la guerre du Péloponnèse et qui ont été très employés pendant la Seconde Guerre mondiale et la guerre de Corée, conservent une grande utilité[150]. Sur le champ de bataille moderne, ils peuvent, par exemple, bloquer les lasers. L'usage de flocons métalliques sub-microniques et nanométriques ainsi que de fibres conductrices et diélectriques pourrait également empêcher la détection de l'optique à l'infrarouge, et ce en restant en suspension beaucoup plus longtemps[151]. Demain, ces moyens émetteurs de fumée pourraient être téléopérés, voire autonomes ; des expérimentations vont d'ores et déjà dans ce sens[152]. Une capacité « d'obscuration » inter-domaines est envisagée par l'US Army intégrant des procédés éprouvés, et des moyens électromagnétiques et cyber qui dégradent les capteurs de l'ennemi ou surpassent son aptitude à discerner les cibles[153].

La place grandissante de la guerre électronique se traduira également sur le champ de bataille. Il en est de même en ce qui concerne son rôle pour les opérations de déception. Historiquement, la généralisation de la mise

147. T. Sano, « Holography: The Next Disruptive Technology », US Army Research Laboratory, avril 2017.
148. P. Langloit, « Adaptiv, la révolution de la protection passive ? », *DSI*, n° 76, décembre 2011.
149. B. Bihan, « Se camoufler. Approches nouvelles d'un problème ancien », *DSI* hors-série n° 24 « Combat terrestre. Nouvelle donne ? », juin-juillet 2012, p. 47-49 et R. Hémez, « Le camouflage d'hier à demain », blog *Ultima Ratio*, 19 septembre 2016.
150. J. C. Bond, « The Fog of War: Large-Scale Smoke Screening Operations of First Canadian Army in Northwest Europe », *Canadian Military History*, vol. 8, n° 1, 1998 ; E. King, « Chemical Corps Smoke: Is There a Future in the Army of the Twenty First Century? », US Army Command and General Staff College, 1998.
151. « ECBC Researchers Work to Develop the Next Generation of Battlefield Obscurants », ECBC, 27 novembre 2017, disponible sur : www.ecbc.army.mil.
152. L'US Army a testé des engins robotisés agissant en équipe. Parmi eux se trouvait un M-113 *Wolf*, un blindé lanceur de fumée. Voir J. Judson, « US Army Tackels Teaming Robots and Ground Forces on the Battlefield », *Defense News*, 25 août 2017.
153. TRADOC Pamphlet 525-3-6, *The US Army Functional Concept for Movement and Maneuver 2020-2040*, 2017.

en œuvre de moyens radios a très rapidement été suivie par leur utilisation pour des manœuvres de déception. De faux réseaux radio ont été utilisés dès 1916 par les belligérants[154]. La déception électronique consiste en l'émission délibérée, en l'altération, en l'absorption ou en la réflexion d'énergie électromagnétique en vue de perturber un adversaire ou l'un de ses systèmes électroniques, ou de détourner ou de capter son attention. Elle est d'autant plus efficace que l'adversaire est dépendant de ses systèmes de transmission, ce qui est naturellement de plus en plus le cas. L'usage de la déception électronique peut aussi être « défensive », en employant, par exemple, des leurres et des répéteurs générant de fausses cibles, en imitant des signaux ou en falsifiant la signature électromagnétique de certaines unités amies.

L'évolution des technologies liée à la robotique et aux drones rend leur présence croissante inévitable sur le futur champ de bataille[155]. La tactique devra probablement être en partie repensée pour tenir compte de ces nouveaux venus. À l'horizon 2030-2040, des formations de robots ou de drones pourraient voir le jour[156] et « constituer la pointe combattante des armées futures[157] ». Elles joueraient alors un rôle majeur dans les opérations de déception. Les projets les plus emblématiques concernent les essaims[158]. Leur emploi avec des drones emportant des équipements de brouillage légers et endurants permettrait de façonner l'environnement électromagnétique de l'adversaire. On peut ainsi imaginer un « écran robotique[159] » qui serait en charge d'une démonstration. De façon plus iconoclaste, parachuter des robots sur les arrières de l'adversaire pourrait créer une diversion[160]. Ce duel technologique entre les capacités de détection et d'analyse et celles de simulation et de dissimulation est permanent et extrêmement changeant selon les adversaires et le milieu d'engagement.

154. La première utilisation à grande échelle de la radio pour une opération de déception a lieu pendant la bataille de Caporetto en octobre 1917, où les Allemands ont combiné silence radio pour les troupes « réelles », et simulation d'une concentration de troupes dans le Tyrol. Barton Whaley, *Strategem Deception and Surprise in War*, MIT, 1969, p. 50 et p. 95-96 et L. Farago (dir.), *The Axis Grand Strategy*, New York, Farrar & Rinehart, 1942, p. 397.

155. L. Kamienski, « Toward Robotic Warfare » *in* S. N. Romaniuk et F. Grice (dir.), *The Future of US Warfare*, Londres, Routledge, 2017, p. 193-207.

156. B. Sadowski, « Shaping the Future: Army Robotics and Autonomous Systems », TARDEC, mars 2016.

157. C. Malis, « Horizon 2030 : réflexions prospectives sur le combat terrestre », *Revue de la défense nationale*, mars 2015, p. 110-115.

158. Sur l'emploi tactique futur des essaims, lire : J. Hurst, « Robotic Swarms in Offensive Maneuver », *Joint Forces Quarterly*, n° 87, 2017, p. 105-111.

159. D. Rieutord, *Les robots terrestres parmi les hommes*, Paris, L'Harmattan, 2017, p. 119.

160. J. Ray, « China's Industrial and Military Robotics Development », Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission, octobre 2016.

# Le besoin en déception

La déception n'est pas étrangère à la culture stratégique et tactique française mais demeure trop souvent aujourd'hui « un artifice esthétique[161] ». En France, une certaine condamnation du recours à la ruse demeure : la figure de Bayard continue à dominer celle de du Guesclin, et le « beau geste » est mis en valeur. La guerre d'Algérie, au cours de laquelle la déception s'est mêlée aux exactions et à la sédition, n'est pas étrangère à la méfiance à l'égard de ces procédés à grande échelle[162]. Or, le recours à la déception sera davantage nécessaire demain pour obtenir la surprise et le succès tactique. L'expérience soviétique pendant la Seconde Guerre mondiale montre toutefois qu'il est possible d'apprendre la pratique de la déception. Grâce à un effort conséquent sur la formation des officiers et l'entraînement individuel et collectif, l'Armée rouge s'est montrée très efficace dans ce domaine pendant les deux dernières années de la guerre[163]. Ainsi, en s'attachant à mieux prendre en compte la déception et en y accordant des moyens humains et matériels, il est possible de lui donner la place qui lui revient dans une manœuvre.

Une telle réhabilitation passe d'abord par la doctrine. Dans le domaine interarmées, il n'y a pas de document dédié à la déception. Le concept n'est évoqué que dans plusieurs opus traitant des opérations d'information. Dans l'armée de Terre, le terme de déception apparaît peu dans les doctrines. Alors qu'il est employé à 59 reprises dans le *FM 3-0* américain (en 364 pages), le mot n'est cité que 14 fois dans le FT-02 (en 112 pages), une fois dans le FT-03 (sur 86 pages), et 6 fois dans le FT-04 (en 84 pages)[164]. Une doctrine de la déception, datée de 2010, existe bien dans le corpus français, mais elle est très peu connue et tombée en désuétude[165]. Elle se concentre beaucoup trop sur les procédés classiques de dissimulation avec trente pages sur ce sujet, seulement deux pour la diversion et une pour l'intoxication[166].

161. F. Jordan, « Plaidoyer pour une *maskirovka* à la française », blog *L'écho du champ de bataille*, 5 novembre 2011, disponible sur : lechoduchampdebataille.blogspot.fr.
162. Entretien avec T. Widemann, Paris, 22 mars 2018.
163. D. M. Glantz, *Soviet Military Deception in the Second World War*, *op. cit.*
164. FM 3-0, Operations, Headquarters, Department of the Army, octobre 2017 ; FT-01, *Gagner la bataille, conduire à la paix*, CDEF, janvier 2007 ; *FT-02 Tactique générale*, CDEF, juillet 2008 ; *FT-03 L'emploi des forces terrestres dans les opérations interarmées*, CDEF, juillet 2015 : FT-04 *Les fondamentaux de la manœuvre interarmes*, CDEF, juin 2011.
165. EMP 20 561, *Doctrine de la déception*, CDEF, 2010, diffusion restreinte.
166. Il faut dire que ce document remplace le TTA 712, *Notice sur l'emploi et la mise en œuvre de la dissimulation*, et qu'il a clairement gardé ce tropisme.

Pour être plus englobant, il serait possible d'envisager la rédaction d'une doctrine consacrée à la surprise dans laquelle la déception prendrait toute sa place, ce qui pourrait se combiner à l'ajout de la surprise dans les principes de la guerre reconnus[167]. À ce titre, le chantier de refonte des principes de la guerre, lancé par le CEMAT en février 2018 est une opportunité à saisir[168].

En ce qui concerne les procédures, on pourrait envisager la création d'un paragraphe spécifique dans les formats d'ordres d'opération jusqu'au niveau brigade et d'un *supporting plan* dédié à partir du niveau division. Toutefois, cette option séduisante présente le risque de contrevenir au principe fondamental d'unicité de la manœuvre. Il apparaît en revanche souhaitable d'adjoindre des éléments de déception dans « l'idée de manœuvre » des ordres d'opération (du niveau stratégique à celui du GTIA), afin qu'ils irriguent la conception globale de la manœuvre[169]. De façon plus globale, il est primordial de susciter recherches et études sur le sujet de la déception.

Dans le domaine de l'organisation, il est d'abord indispensable d'installer une structure de coordination stratégique, sans laquelle il est impossible d'envisager la mise en œuvre d'opérations de déception de ce niveau. Une entité de ce type demeurera toutefois démunie sans un renforcement de la culture stratégique des élites politiques[170]. Si la création de cellules spécialisées dans les états-majors opérationnels paraît excessive, un « *board* » ou « *working group* » pourrait avoir toute sa place au sein des états-majors de division. Lorsque l'on aborde la question de la mise en œuvre, il pourrait être judicieux de constituer une unité dédiée aux opérations de déception. Le Centre interarmées des actions sur l'environnement (CIAE), qui dispose déjà de certains moyens comme des haut-parleurs, pourrait l'accueillir. Équipée de moyens de guerre électronique et de simulation visuelle et sonore, elle aurait pour mission de simuler par elle-même, ou en recevant du renfort d'autres unités, une unité de type brigade ou GTIA. Elle se chargerait des procédés les plus techniques et servirait de réservoir de spécialistes du domaine. Bien qu'envisagé à un niveau très inférieur, le concept britannique de *Future Combat Team* (sous-groupement tactique renforcé), ouvre la voie à cette

167. *Action terrestre future. Demain se gagne aujourd'hui*, EMAT, 2016. Pour un éclairage sur le débat autour des principes de la guerre dans l'armée de Terre, lire : « Les principes de la guerre : clarification sémantique, point de situation et cadre de départ pour de nouvelles réflexions doctrinales », Lettre de la doctrine n° 9, CDEC, janvier 2018. Pour une vision plus générale : M. Motte, G.-H. Soutou, J. de Lespinois, et O. Zajec, *La mesure de la force*, *op. cit.*

168. Allocution du général Bosser, « 100 ans après 1918, Vaincre au XXIe siècle », colloque pensée militaire du CDEC, École militaire, 6 février 2018.

169. Entretien avec le colonel C. Franc, Paris, 25 janvier 2018.

170. Entretien avec T. Widemann, Paris, 22 mars 2018.

réflexion. Il prévoit en effet une équipe dédiée à la déception composée d'une dizaine d'hommes et de deux engins blindés *Ajax*[171].

En termes de ressources humaines, il importe de ne pas confier la déception à des spécialistes, tenus à l'écart de la réflexion générale sur la manœuvre. Il faut au contraire que l'ensemble des cadres soient pénétrés de l'utilité de ce procédé et solidement formés à sa mise en œuvre. La déception doit donc prendre toute sa place dans l'enseignement militaire. Cependant, un effort sur la déception, pour porter ses fruits, doit accompagner une action plus globale de revitalisation de l'enseignement de la tactique générale. Par ailleurs, lorsqu'il est question de déception, l'état d'esprit est peut-être tout aussi important que les connaissances théoriques. Il faut développer chez les chefs militaires une mentalité mêlant volonté de « casser les codes », audace et imagination[172]. Le sens de l'humour est souvent cité comme une caractéristique nécessaire au bon planificateur d'opérations de déception[173]. En effet, la conception d'opérations de déception et celle de certaines plaisanteries, et notamment des canulars, reposent sur des mécanismes similaires, jouant entre autres sur « la même manipulation de convenances et d'incongruités[174] ».

Si l'état d'esprit et la formation jouent un grand rôle, réhabiliter la déception impliquerait aussi de fournir un – modeste – effort capacitaire. La guerre électronique doit évidemment en faire partie, tant dans sa part défensive qu'offensive. Par exemple, un outil de visualisation de la signature électronique, comme le logiciel *RadioMap* testé depuis 2015 par les Marines américains, pourrait être très précieux afin d'améliorer notre capacité de camouflage électronique. Des capacités existent aussi pour « noyer » le signal radio, afin de ne pas pouvoir être repéré trop facilement[175]. L'utilisation de lasers pour les communications pourrait, par ailleurs, permettre d'être plus discrets[176]. Dans le domaine de la dissimulation, les systèmes de diffusion de fumigènes mériteraient de nouveau notre attention. Il en va de même pour les leurres terrestres, équipements relativement peu coûteux qui ont prouvé leur efficacité. Ils pourraient équiper les unités spécialisées mais aussi toutes les unités de cavalerie et d'infanterie.

171. Les contours exacts de la mission de cette équipe ne sont pas connus.
172. R. Hémez, « Tactique : le devoir d'imagination », blog *La voie de l'épée*, 14 juin 2015, disponible sur : lavoiedelepee.blogspot.fr.
173. B. Whaley et S. Stratton Aykroyd, *Practise to Deceive: Learning Curves of Military Deception Planners*, Annapolis, Naval Institute Press, 2016, p. 197-200.
174. *Ibid*. p. 200.
175. P. Tucker, « Forget Radio Silence. Tomorrow's Soldiers Will Move Under Cover of Electronic Noise », *Defense One*, 25 juillet 2017.
176. G. Rowlands, « When Radio Silence Is Not Enough: Signature Suppression & The Fight for Surprise », *Grounded Curiosity*, 15 août 2018.

Pour que les opérations de déception ne restent pas en marge de nos pratiques, elles doivent être présentes dans tous les exercices, du niveau du corps d'armée à celui du GTIA[177]. Ces exercices doivent permettre la maîtrise des procédés élémentaires comme l'infiltration, l'art du camouflage, le combat de nuit[178], etc. En outre, il est nécessaire d'améliorer nos capacités de manœuvre en silence électronique. La numérisation rend les fuites plus difficiles à contrôler. Bradley Manning, Edward Snowden et autres « lanceurs d'alerte » l'ont amplement démontré au niveau politico-stratégique, mais c'est également vrai au niveau tactique, de façon volontaire ou non[179].

La déception doit aussi être mieux intégrée dans les moyens de simulation à disposition pour la formation et l'entraînement. Il faudrait, par exemple, que les actions de guerre électronique soient incluses, ce qui n'est pas le cas dans Soult[180] actuellement. Il est de même souhaitable de profiter de l'élan créé par Scorpion dans le domaine de la réflexion tactique pour remettre en avant le principe de déception, en s'appuyant sur le Laboratoire du Combat Scorpion (LCS) ainsi que la Force d'expertise du combat Scorpion (FECS), nouvellement créée au Centre d'entraînement au combat de manière à intégrer la déception à ces expérimentations qui visent à tester les nouveaux matériels et des modes d'action innovants.

Il est important d'étudier davantage les aspects humains de la guerre. Reconnus comme cruciaux, ils sont pourtant trop souvent laissés de côté. Les publications doctrinales n'abordent que rarement, par exemple, l'étude des processus de décision ennemis[181]. De même, un concept ou une méthode vont être interprétés et mis en pratique différemment suivant la culture militaire qui les accueille. Des outils existent pour aider à appréhender cette donnée. C'est par exemple le cas de la théorie des six dimensions culturelles de Geert Hofstede qui permet une analyse

177. P. A. Haveles, « Deception Operations in Reforger 88 », *Military Review*, vol. 70, n° 8, août 1990, p. 35-41.
178. J. Coppolani, « Le combat de nuit, ou la nécessité de garder un temps d'avance », *Lettre du RETEX opérations,* n° 36, CDEC, mars 2018.
179. La diffusion incontrôlée de données personnelles via les objets connectés a par exemple posé aux Russes de sérieuses difficultés en Ukraine, suite à la publication de certaines photos incriminantes par des soldats sur les réseaux.
180. SOULT : Simulation pour les opérations des unités interarmes et de la logistique terrestre, remplaçant de l'ancien système, Janus, pour l'entraînement du personnel d'encadrement de l'échelon division jusqu'au niveau GTIA.
181. Au niveau stratégique des méthodes de simulation de prise de décision de chefs d'États et de gouvernements existent. Ayant une ambition prédictive, elles peuvent être une aide précieuse pour planifier une opération de déception. C'est par exemple le cas d'*Athena Prism*. Voir B. G. Silverman, *et al.*, « Athena's Prism – A Diplomatic Strategy Role Playing Simulation for Generating Ideas and Exploring Alternatives », Philadelphie, University of Pennsylvania Press, mai 2005.

systématique des différences entre les cultures[182]. Pour mieux prendre en compte cette dimension l'acculturation serait souhaitable mais elle est difficile d'exécution dès lors qu'elle implique une immersion de longue durée[183]. Il est toujours utile d'entretenir des bases de données sur tous les pays qui se trouvent dans nos zones de priorité stratégique. Ce travail est déjà fait mais gagnerait à être mieux diffusé. Les individualités jouent aussi un rôle. Un chef militaire, comme un artiste, développe un style. C'est dans ce but que, pendant la guerre du désert, Rommel avait toujours avec lui une traduction annotée par ses soins de *Generals and Generalship* écrit par son principal adversaire, le général britannique Wavell[184]. Ce dernier préférait pour sa part les biographies, mémoires, et même romans historiques aux traités de stratégie, pour « aller à la chair et au sang et pas au squelette[185] ».

Enfin, et peut-être pourrions-nous commencer par-là, un effort doit être fait à tous les niveaux pour accroître notre capacité de contre-déception. C'est loin d'être évident : « quand devrions-nous ne pas croire nos yeux et nos oreilles et les conclusions apparemment logiques de notre intellect ?[186] » Aucune mesure n'éliminera jamais le risque de se faire mystifier. En revanche, il est possible de réduire de façon incrémentale la vulnérabilité d'une organisation à la déception[187]. Deux mesures principales doivent être prises en amont. La première est d'évaluer la vulnérabilité des organismes de décision, de commandement et de renseignement, afin de déterminer le plus honnêtement possible les canaux par lesquels ceux-ci sont les plus fragiles. Généralement, ce sont les segments de notre cycle de décision dont l'adversaire est le plus familier. La deuxième mesure consiste à évaluer en permanence les menaces potentielles en se posant, entre autres, la question de précédents historiques de l'emploi de la déception par les adversaires potentiels. Il faut

182. Une valeur (allant de 1 à 120), obtenue par des enquêtes, est placée sur six dimensions culturelles. Il s'agit du pouvoir (égalité contre inégalité), du collectivisme (par opposition à l'individualisme), de l'évitement de l'incertitude (par opposition à l'acceptation de l'incertitude), de la masculinité (par opposition à la féminité), de l'orientation temporelle (temps long ou court terme) et le plaisir (par opposition à la modération). L'explication de cette théorie et une partie des résultats sont disponibles sur le site de G. Hofstede : geerthofstede.com.

183. R. Johnston, « The Question of Foreign Cultures: Combating Ethnocentrism in Intelligence Analysis », *Analytic Culture in the US Intelligence Community*, Michigan, University of Michigan Library, 2005.

184. R. Mead, *Churchill's Lions a Biographical Guide to the Key British Generals of World War II*, Stroud (Gloucestershire) Spellmount LtD, 2007, p. 280. *Generals and Generalship* est une conference donnée en 1939 et qui a été publiée dans A. Wavell, *Soldiers and Soldiering*, Londres, Jonathan Cape, 1953, p. 33-34.

185. *Ibid*.

186. R. J. Heuer, « Cognitive Factors in Deception and Counterdeception », in *Strategic Military Deception*, *op. cit*., p. 31-69.

187. R. M. Clark et W. L. Mitchell, *Deception*, *op. cit.,* p. 161-189.

ensuite être capable de contrer une opération de déception en cours. Un plan de déception ne peut être parfait. Le but est donc de détecter une incongruité, ce qui impose de questionner toutes les preuves. À tous niveaux, l'instrument principal de la contre-déception est un système de renseignement efficace ; mais l'augmentation du volume d'informations collecté n'est pas la solution. L'effort doit porter sur la phase d'analyse, en se gardant bien de sauter trop vite aux conclusions[188].

Des méthodes peuvent aider : la sensibilisation à la déception et à ses mécanismes tout d'abord, pour provoquer une vision plus critique des informations, des séances de réflexion interdisciplinaires ensuite, complétées d'analyses contradictoires (dont le *red teaming*)[189]. Au niveau stratégique, l'éducation joue bien entendu un rôle majeur pour contrer la désinformation (singulièrement l'éducation aux médias[190]), de même que les organisations de la société civile (journalistes en particulier), pour identifier et endiguer les campagnes de propagande étrangère. Mais il est aussi nécessaire de créer ou de renforcer des organes dédiés à leur surveillance comme l'équipe de l'East StratCom au sein du service diplomatique de l'Union Européenne ou le centre d'excellence StratCom de l'OTAN[191]. L'État peut aussi utiliser le droit dans cette lutte. C'est l'objet, en France, du projet de « loi de fiabilité et de confiance de l'information[192] ». Au niveau tactique, la contre-déception se pratique selon divers procédés : contre-reconnaissance, camouflage et discrétion, changement de dispositif de dernière minute, dissimulation de la réserve, etc.[193]. À tous les niveaux, la connaissance de son ennemi – incluant celle de ses méthodes de déception – est cruciale. Le but est de ne pas se contenter de la description des capacités mais de réussir à estimer les intentions. C'est ce qui fait la différence entre un bon et un médiocre service de renseignement.

188. M. Dewar, *The art of deception in warfare*, *op. cit.*, p. 194-203.
189. R. J. Heuer, « Strategic Deception and Counterdeception: A Cognitive Process Approach », *International Studies Quarterly,* vol. 25, n° 2, 1981, p. 294-327.
190. Voir, par exemple, le projet « S'informer et communiquer sur les réseaux sociaux » de R.-M. Farinella, visant à fournir aux élèves de primaire des outils d'autodéfense contre les fausses nouvelles, et disponible sur : www.ac-grenoble.fr.
191. D. Fried et A. Polyakova, « Democratic Defense Against Disinformation », *Atlantic Council*, 5 mars 2018.
192. Ce projet de loi vise notamment à renforcer le pouvoir du CSA sur les chaînes sous contrôle étranger et à responsabiliser davantage les plateformes numériques quant aux contenus illicites. Une procédure de référé est aussi prévue pour pouvoir suspendre un contenu en 48 heures.
193. M. Yakovleff, *Tactique théorique*, *op. cit.*

# Conclusion

La réussite d'une illusion n'a rien de magique. Elle repose sur des éléments suggérés, la compréhension de la nature humaine, des techniques de manipulation relativement simples et le soin pris de répondre aux attentes du public[194]. Malgré toute l'attention qu'il peut porter aux tours du prestidigitateur, le spectateur est toujours surpris. La déception s'inscrit dans la même logique.

Les évolutions technologiques, et en particulier la multiplication des capteurs et des moyens de frappe à distance, ne remettent pas en question la possibilité de réaliser ce type d'opérations, ni leur efficacité. Même, au moment où la transparence du champ de bataille s'accroît, la capacité à mener des opérations de déception, parce qu'elles cherchent à tromper sur l'intention et pas seulement sur les capacités, est plus précieuse que jamais pour créer la surprise. Pour ne pas être trompé, il ne suffit pas de tout voir il faut aussi comprendre, ce qui constitue un défi bien supérieur. La déception est probablement de plus en plus complexe à appréhender, à planifier et à exécuter, notamment parce qu'il faut prendre en compte toujours plus de canaux de transmission des informations ; mais cela ne signifie en rien qu'il faille la mettre de côté. Bien au contraire, les opérations de déception semblent plus nécessaires que jamais pour être en capacité de manœuvrer dans l'environnement opérationnel d'aujourd'hui et de demain.

Pourtant, nous sommes aujourd'hui le plus souvent les spectateurs, voire les victimes, d'opérations de déception menées par d'autres. L'intérêt qu'on leur porte au sein de l'armée française est cyclique. Des études sont menées, des doctrines sont rédigées, mais, en fin de compte, la déception reste très peu utilisée, en opération comme à l'entraînement. La surprise est encore trop envisagée comme un simple produit de la chance. Elle demeure mal comprise et souvent vue comme un artifice sous le prétexte qu'on ne peut pas faire reposer le succès d'une manœuvre sur l'éventualité très hypothétique de duper l'ennemi. L'augmentation des moyens de collecte du renseignement permet encore à trop de décideurs et d'analystes de s'abriter derrière l'opinion qu'il n'y a plus de dissimulation possible, et par conséquent, pas davantage de déception. À tous les niveaux, il s'agit

194. R. N. Armstrong, « Soviet Operational Deception: The Red Cloak », Combat Studies Institute, 1989, p. 1.

désormais de prendre conscience que ce procédé n'a jamais perdu d'importance dans la guerre et de démentir enfin Guibert pour qui « nous n'avons pas, il faut en convenir, la moindre idée de ce genre de [195]guerre ».

Pour la France, il convient *a minima* de prendre des mesures pour améliorer les capacités de contre-déception. Il faudrait cependant aller plus loin afin d'être capables de mener ce type d'opérations. Au niveau stratégique, et en dehors des opérations que mènent les services, cela semble difficile pour une démocratie en dehors d'un conflit où les intérêts vitaux sont en jeu. On peut aussi avancer l'idée de la nécessité d'un rapprochement des sphères politiques et militaires. La méconnaissance des questions stratégiques et militaires par les hommes politiques et l'avènement d'une classe d'officiers professionnels, ayant tendance à se replier sur leur « cœur de métier » et éloignés des questions diplomatiques et politiques ne facilitent pas le recours aux opérations de déception[196]. Cependant, si l'on prend au sérieux les observations du dernier *Livre Blanc* (« menaces de la force ») et de la *Revue stratégique de défense et de sécurité nationale* (« retour de la guerre aux frontières européennes ») qui mettent en garde contre le risque de guerre majeure, il serait au moins nécessaire d'amorcer une réflexion sur le concept et d'identifier une autorité de coordination. Au niveau tactique et opératif, les possibilités d'actions semblent beaucoup plus importantes. Des mesures assez simples et peu coûteuses, que nous avons rapidement décrites ici, peuvent permettre de placer la déception au cœur de la manœuvre, ce qui, encore une fois, nous semble impératif pour éviter un blocage tactique et une guerre d'attrition.

195. Guibert, *Œuvres militaires de Guibert, t. II, Essai général de tactique*, Paris, Barrois, 1803, p. 123.
196. M. Motte, G.-H. Soutou, J. de Lespinois, et O. Zajec, *La mesure de la force*, *op. cit.* et H. Goldhammer, *Reality and belief in Military Affairs*, Santa Monica, RAND Corporation, 1977, p. 103-104.

ifri
institut français
des relations
internationales