Sommaire

Connaissances et anticipation sur les groupes APT

Par le Chef d'escadron Maxime SERRES, stagiaires EMSST 2024-2025,

Mastère spécialisé cybersécurité attaque et défense des systèmes informatiques,

École nationale supérieure des Mines de Nancy

Derrière chaque organisation se trouvent des Hommes ; les groupes APT (*Advanced Persistent Threats*) n'échappent pas à cette règle. D'un point de vue sécuritaire, il est donc légitime, afin de s'en protéger, de mieux connaître ces organisations malveillantes

➢ Concepts entourant les APT

Dans le paysage des cybermenaces, les groupes APT (que nous appellerons plus facilement les APT) agissent principalement dans le champ de conflictualité qu'est le cyberespace. La connaissance de leurs procédés d'exécution relève du renseignement sur la menace cyber plus fréquemment appelée CTI pour *Cyber Threat Intelligence*.

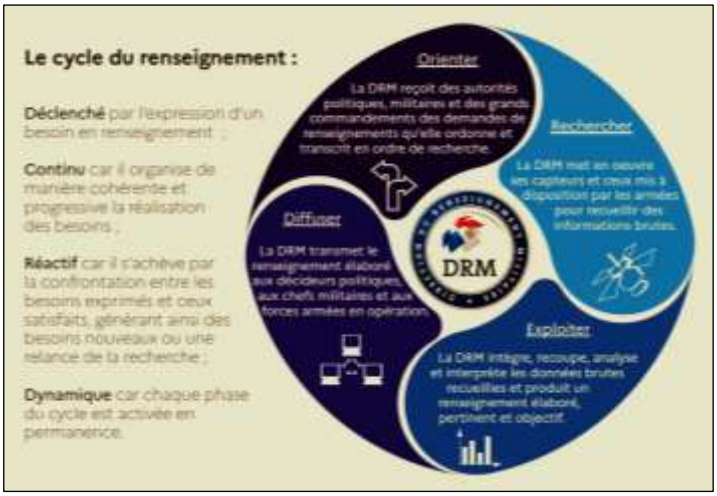
Aucun consensus ne se dégage clairement quant à la définition de la menace APT. La menace est-elle prégnante car elle est sophistiquée ou bien parce qu'elle est de nature pénétrante vis-à-vis des systèmes informatiques ? En l'appliquant à un groupe d'individus, nous retiendrons la définition que donne l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) d'une cyberattaque.

Définition : une cyberattaque est un ensemble coordonné d'actions menées dans le cyberespace qui visent des informations ou les systèmes qui les traitent, en portant atteinte à leur disponibilité, à leur intégrité ou à leur confidentialité. Une cyberattaque peut être ponctuelle ou s'inscrire dans la durée.

Nous nuancerons cette définition en y apportant les caractéristiques d'une opération qui s'inscrit dans le temps long et qui a trait au cyber-espionnage, au sabotage ou à des activités de subversion voire d'ingérence.

À l'heure du *Big data*, la cible principale de ces groupes demeure l'information. Les APT représentent une menace qui ne se cantonne pas à cibler le monde occidental. Militaires ou civils, à vocation idéologique ou à but lucratif, éventuellement soutenus par des gouvernements à travers le monde, ces groupes sont de toutes origines. La MITRE Corporation en recense 152 au moment de la rédaction de ces lignes.

➢ L'organisation des APT



La structure des groupes APT demeure en grande partie opaque. La collecte de renseignements sur leur organisation peut être réalisée avec l'emploi controversé de méthodes dîtes de sécurité offensive : attaquer les attaquants soulève des problèmes éthiques et légaux.

Parmi les APT, outre l'aspect technicien des hackers et autres développeurs de malware, voire d'administrateurs systèmes, deux types de profils plus spécialisés existent : l'analyste *threat intelligence* et l'analyste *competitive intelligence* :

- le premier agit dans le montage de l'infrastructure attaquante notamment via l'enregistrement de noms de domaines DNS dynamiques à la typologie variée et dépendants de la cible.

- le second est, quant à lui, davantage lié au commanditaire de l'opération. Il s'agit d'un spécialiste de la filière d'appartenance de l'entreprise ciblée qui aurait un œil critique sur les informations dénichées par les hackers du groupe et serait apte à juger de la pertinence d'exfiltrer ou pas les données auxquelles ils ont accès. Cet expert – éventuellement intérimaire du groupe APT – apporte vraisemblablement sa valeur à la masse d'informations traitée. En se référant au cycle du renseignement militaire, il pourrait être responsable des phases d'orientation et d'exploitation.

Un critère de caractérisation de ces groupes de hackers est souvent leur nationalité. Russie, Chine, Corée du Nord et Iran mettent sur pied ces capacités d'attaques dans le cyberespace. Cependant, ces pays ne sont pas exempts des menaces ciblant leurs propres réseaux parce que , par exemple, 10 millions de cyberattaques quotidiennes auraient ciblé la Russie en 2020.

Côté occidental, les 5-EYES ne sont pas en reste avec notamment les agences de renseignement américaines. La CIA disposerait de 5.000 agents dédiés aux activités de cyber-espionnage tandis que la NSA *« tire parti de ses avantages en matière de technologie et de cybersécurité, conformément aux pouvoirs qui lui sont conférés, pour renforcer la défense nationale et sécuriser les systèmes de sécurité nationale. »* Ainsi, les actions de l'APT dénommé *Equation Group* ont été attribuées aux États-Unis (NSA) par la société Kaspersky en 2015 au même titre que la menace APT1 l'a été à la Chine par la société Mandiant en 2013.

La délicate question de l'attribution – ou le fait de désigner un groupe ou un État responsable derrière une cyberattaque de type APT – requiert d'être appuyé par des preuves irréfutables. Dans ce cadre, le *threat hunter* joue un rôle primordial en disposant d'une base de CTI la plus exhaustive possible.

Exemple : le groupe connu sous le code APT1 et sous l'alias Comment Crew aurait conduit l'opération Aurora entre 2009 et 2010 visant des entreprises du secteur financier, des médias et plusieurs autres firmes technologiques. Derrière cette structure, l'Armée Populaire de Libération (Chine) dissimulerait une unité cyber de premier plan. Cette unité militaire parmi les plus connues intégrerait l'ensemble du spectre des capacités d'un APT.

Qualifié de tentaculaire, le groupe APT1 a ainsi fait l'objet d'une attribution directe de la firme internationale de cybersécurité Mandiant dès février 2013. Les APT disposent de ressources financières et humaines parfois considérables estimées à l'aune de la persistance et de la patience qu'ils savent mettre en œuvre pour atteindre leurs objectifs.

Une analogie peut être faite avec un procédé entrepreneurial de sécurité offensive appelé le *red teaming*.

Définition : le red teaming est la pratique qui consiste à tester la sécurité de systèmes d'une organisation en essayant de les pirater. Une *Red Team* (« équipe rouge ») peut être un groupe externe de pentesters (testeurs d'intrusion) ou une équipe propre à l'organisation. Dans les deux cas, le rôle est le même : émuler un acteur réellement malveillant et tenter de pénétrer dans les systèmes.

Par essence, le *red teaming* se veut réaliste pour préparer une organisation à faire face aux menaces cyber. La mise en œuvre d'une *Red Team* sert à mettre en lumière des vulnérabilités mais sert aussi au maintien et à l'acquisition de compétences pour les équipes de défenseurs (équipe bleue ou *Blue Team*). Les scenarii d'attaques et les outils employés se calquent sur des opérations réellement conduites par les APT. Les *Red Teams* ciblent les infrastructures essentielles et de haute-valeur pour l'entreprise puis sont capables de proposer une remédiation aux problèmes de cybersécurité rencontrés.

Au sens large, une autre catégorie de *Red Team* composée de spécialistes hors domaine cybersécurité peut être sollicitée pour réaliser un travail de prospective vis-à-vis de la menace.
Exemple : l'initiative *Red Team* décidée à l'été 2019 par l'Agence de l'innovation de Défense (AID) avec l'État-major des armées (EMA), la Direction générale de l'armement (DGA) et la Direction générale des relations internationales et de la stratégie (DGRIS) dans le cadre du Document d'orientation de l'innovation de Défense.

Les groupes APT sont souvent organisés de manière hiérarchique et spécialisée, similaire à ce qui se fait en entreprise classique mais en se focalisant sur les opérations clandestines. Dans certains cas, un groupe APT peut reproduire la structure numérique d'une cible pour s'entraîner à l'attaquer avant de procéder réellement à

l'intrusion. Les opérations stratégiques conduites par les APT nécessitent une indéniable part de créativité et de manœuvrabilité.

- Le renseignement en cybersécurité

Pour déjouer les vols de données et se prémunir contre l'intrusion des APT dans les systèmes informatiques, le premier rempart demeure la formation et la sensibilisation du personnel. Considérant que de nombreux groupes APT sont gouvernementaux ou sponsorisés par des gouvernements, les enjeux militaires et d'influences géostratégiques trouvent un écho dans le cyberespace.

En opération comme dans le monde de l'entreprise, le contexte est à prendre en compte. L'environnement tactique, opératif et stratégique, influe directement sur le déroulement et la collecte d'informations de toutes origines (ROHUM, ROEM et ROIM[1]). Il en est de même pour le Renseignement d'Origine Cyber (ROC) qui – dans le cadre de la lutte contre les APT – fait sens sous la forme du recueil d'indices de compromission (plus généralement énoncé en anglais en tant qu'IOC ou *Indicators of Compromise*).

Définition : un IoC (indicateur de compromission) en sécurité informatique est une donnée technique qualifiée qui permet de détecter des activités malveillantes sur un système d'information. Ces indicateurs peuvent s'appuyer sur des données de types variés comme, par exemple, un hash de fichiers, une signature, une adresse IP, une URL[2], un nom de domaine… mais dans tous les cas, la donnée technique seule ne suffit pas pour parler d'IoC.

Selon cette définition, la donnée brute n'est pas suffisante. Elle doit être raffinée et contextualisée pour devenir un renseignement, une empreinte numérique qui peut laisser présumer de la survenue d'un opérateur APT dans un système.

Sur le terrain, cela se traduit par la mise en place planifiée et coordonnée de moyens de détection sur les systèmes déployés en opérations mais également par la création d'un circuit de traitement des supports physiques. En effet, une stratification de l'analyse est requise ; de la primo-analyse sur le théâtre d'opération à l'analyse exhaustive réalisée par exemple au CRAC (Centre de Recherche Avancée Cyber) appartenant à la DRM (Direction du Renseignent Militaire), un cheminement clair et une traçabilité sans faille sont nécessaires.

Élever des remparts adaptés pour protéger les systèmes nécessite une analyse poussée de la menace. Exploiter les renseignements cyber collectés, c'est le domaine de la *Cyber Threat Intelligence* (CTI) qui utilise diverses plateformes pour mettre en forme et présenter la masse de données. La CTI suit une méthodologie similaire au cycle du renseignement.

Après exploitation, la mise à jour des TTPs (Techniques Tactiques et Procédures) des groupes APT découle de recoupements d'informations qui permettent de rendre opérationnel le renseignement cyber. La CTI peut elle-même être subdivisées en différents sous-domaines :

- ***tactical threat intelligence****,* qui comprend notamment la collecte des IOCs ;
- ***operational threat intelligence****,* afin de discerner l'objectif régionalisé d'une cyberattaque ou d'un opérateur APT ;
- ***strategic threat intelligence****,* pour obtenir une vision globale la menace.

[1] Renseignement d'Origine HUMaine, Électromagnétique, IMagerie

[2] Hash : fonction de conversion ; IP n° d'identification de chaque ordinateur connecté à Internet ;URL (Uniform Resource Locator) chaîne de caractères pour identifier une ressource sur Internet.

Les différentes strates opérationnelles se retrouvent dans les procédés de collecte du renseignement et d'analyse des cybermenaces.

Le renseignement conduit à l'action ; il en est de même en cybersécurité. Dans la lutte contre les menaces qui ciblent les systèmes numériques, la connaissance est un maillon essentiel de la sécurité globale cyber-physique.

OpenCTI est une plateforme initialement développée par l'ANSSI pour contextualiser les menaces cyber

Appréhender le risque biologique au XXIème siècle : quelles menaces, quels enjeux ?

Par le Chef de bataillon Louis FATZ, stagiaire EMSST 2024-2025,
Master Risques Sanitaires NRBCe

En 2020, la pandémie de Covid-19 a rappelé à l'humanité sa vulnérabilité face à l'émergence de nouvelles maladies. Sous le prisme militaire, cette prise de conscience permet de considérer l'ampleur que peut prendre la menace biologique dans un conflit. En effet, une force exposée à un risque biologique, de façon intentionnelle ou non[3], perdrait rapidement sa liberté d'action et ainsi l'ascendant sur un ennemi mieux préparé. Comment donc anticiper cet éventuel danger ? Ce risque se traduit par l'utilisation d'agents biologiques pathogènes qui regroupent tous les micro-organismes (bactéries, champignons, parasites, virus) capables de provoquer une infection ou une toxicité. Mais un agent biologique seul (comme une bactérie capable de donner la peste par exemple) ne constitue pas pour autant une arme biologique. Il faut également que celui qui envisage de l'utiliser dispose de connaissances spécifiques, de moyens de production et de stockage. Il devra également être capable de vectoriser cet agent mais aussi de pouvoir cibler d'éventuels objectifs en fonction de ses ambitions. Une prise en compte plus efficace de la menace biologique nécessite donc une plus large connaissance des agents biologiques et une meilleure anticipation des intentions dans ce domaine de nos adversaires pour pouvoir être ainsi capable de préparer au plus tôt des contre-mesures efficaces.

➢ Les armes biologiques, une technique de guerre vieille comme le monde

Le risque biologique n'est pas nouveau. Depuis l'Antiquité, l'homme a eu recours à des armes biologiques pour combattre ses ennemis. Ainsi, à l'ère néolithique déjà, les chasseurs utilisaient des poisons d'origine biologique (comme le curare ou d'autres toxines d'amphibiens) pour accroitre la létalité de leurs flèches. De même, à de nombreuses reprises dans l'Histoire, un opposant a utilisé des cadavres pour

[3] Le danger biologique peut-être classé en trois catégories. Il peut être d'origine naturelle et regroupe alors les maladies émergentes naturelles (comme la fièvre jaune, causée par son virus, transmis par les moustiques) ou les maladies infectieuses ré-émergentes comme la peste dont la première pandémie est datée du VIème siècle et qui a sévi à Madagascar en 2017. Le danger biologique peut également être d'origine accidentelle ou non intentionnelle comme l'épidémie de fièvre aphteuse au Royaume-Uni en 2007 causée chez le bétail par une fuite d'un laboratoire de recherche ayant entraîné des pertes agricoles importantes et des mesures de quarantaine strictes. Enfin, il peut être intentionnel et résulter de l'emploi délibéré d'un acteur (étatique ou non) comme l'attaque menée par la secte Aum Shinrikyo au Japon1993 avec des spores d'anthrax et de la toxine botulique.

transmettre des maladies à ses ennemis. Ainsi, le siège de Caffa en 1347, mené par les Mongols contre cette ville portuaire génoise en Crimée, est souvent cité comme un exemple précoce de guerre biologique. Les Mongols, touchés par la peste bubonique, auraient catapulté des cadavres infectés par-dessus les murailles, contaminant les habitants. Les marchands génois, fuyant la ville, auraient ensuite ramené la peste en Europe, contribuant à la pandémie dévastatrice de peste noire qui a suivi.

Peste à Caffa 1347

D'autres exemples d'utilisation d'armes biologiques au cours des siècles illustrent l'importance de l'immunité développée par certaines populations par rapport à d'autres plus naïves face à l'agent disséminé. Ainsi, en 1736, les Britanniques offrirent aux indiens d'Amérique des couvertures préalablement utilisées par des sujets contaminés par la variole. Les autochtones n'ayant aucune immunité contre cette maladie, sont décimés par des épidémies de variole et exterminés lors des guerres coloniales qui marquent le XVIII^{ème} siècle sur le nouveau continent.

Pendant la 1ère guerre mondiale, les Allemands ont eu recours à des bactéries[4] pour contaminer la nourriture des animaux des forces alliés (ciblant principalement les chevaux). Ces procédés eurent des impacts significatifs sur les mouvements des troupes françaises sur le front et mettent donc en exergue le pouvoir incapacitant des agents biologiques sur l'environnement des soldats. Avant la mise en place de législations[5] pour réguler l'emploi de telles armes, quelques États cherchèrent à développer des programmes biologiques entre les deux guerres pour ainsi acquérir une supériorité par rapport à leurs adversaires dans ce champ d'affrontement spécifique. Si la France abandonne son programme en 1940, d'autres pays alliés le poursuivent pendant la 2ème guerre mondiale comme la Grande-Bretagne qui mènent des essais de bombes chargées de spores de charbon sur l'île de Gruinard en 1942. Du coté des puissances de l'Axe, les Japonais sont responsables du programme biologique entre deux guerres le plus avancé : ils auront mené plusieurs expérimentations sur des êtres humains dans l'unité 731, détruite immédiatement après l'envoi de la première bombe atomique et l'invasion de la Mandchourie par l'URSS en 1945.

Unité 731 1945

- **Une menace toujours prégnante et de nouvelles perceptives**

[4] Plus précisément, les Allemands utilisèrent une bactérie nommée *Burkholderia mallei* à l'origine de la maladie de la morve, transmissible des chevaux à l'homme par simple inhalation d'aérosols émanant de l'animal contaminé. La létalité chez l'homme due à cette maladie est de 40%.

[5] Le Protocole de Genève de 1925 interdit l'usage des armes chimiques et biologiques en guerre, mais pas leur développement ou stockage. La Convention d'interdiction des armes biologiques et des toxines (CIABT) de 1972 interdit la recherche, la production et le stockage d'armes biologiques, afin d'éliminer leur utilisation potentielle.

Plus récemment, entre 1991 et 1995, l'Irak a développé un programme biologique secret incluant la production d'armes à base d'agents comme l'anthrax et la toxine botulique. Après la guerre du Golfe, la mission UNSCOM (Commission spéciale des Nations Unies) fut créée pour inspecter et démanteler ces capacités d'armes de destruction massive.

Dans les années 2000, le danger biologique se caractérise par l'émergence du bioterrorisme et l'utilisation par des acteurs non étatiques d'agents biologiques pour servir des objectifs bien particuliers. En effet, grâce aux progrès technologiques et scientifiques des dernières décennies, ces agents sont de plus en faciles à produire, à stocker et à vectoriser. Ainsi en 2001, plusieurs lettres contenant des spores de *Bacillus Anthracis* (responsable de la maladie du charbon) sont envoyées à certaines autorités américaines. Cet attentat biologique, non revendiqué à ce jour[6], contamine 23 personnes, occasionne 5 décès et nécessite la mise sous traitement prophylactique de plus de 30.000 personnes. Au-delà de ce bilan, il mobilise le FBI pendant de longs mois d'enquête et contribue à plusieurs milliers de fausses alertes partout dans le monde (dont plus de 4.000 en France), perturbant largement les forces de sécurité de nombreux pays. Vingt ans plus tard, cette menace du bioterrorisme est toujours d'actualité.

Lettres contaminées à l'anthrax 2001

Mais surtout, l'expansion de la biologie de synthèse, la multiplication des laboratoires de sécurité biologique dans le monde depuis la fin du Covid-19 et la désinhibition manifeste de certains États sur un recours aux armes biologiques, rendent crédible la prolifération de ces arsenaux dans le monde. En effet, tous ces facteurs pourraient permettre de détourner les agents biologiques que nous connaissons déjà en accroissant par exemple la virulence d'un agent infectieux ou en lui permettant d'acquérir une résistance à des moyens de prévention ou de traitement. Nous pourrions imaginer également la construction d'un agent infectieux aux propriétés inconnues, d'un agent infectieux éradiqué ou disparu ou encore la synthèse d'une nouvelle toxine. De même, la création d'un agent capable d'altérer la capacité de résistance d'une population à un agent infectieux ainsi que l'amélioration de la stabilité dans l'environnement ou l'accroissement de la contagiosité d'un agent biologique sont parfaitement


Characterization of the Reconstructed 1918 Spanish Influenza Pandemic Virus

Terrence M. Tumpey,[1]* Christopher F. Basler,[2] Patricia V. Aguilar,[2] Hui Zeng,[1] Alicia Solórzano,[2] David E. Swayne,[4] Nancy J. Cox,[1] Jacqueline M. Katz,[1] Jeffery K. Taubenberger,[3] Peter Palese,[2] Adolfo García-Sastre[2]

Publication sur la synthèse du virus de la grippe espagnole de 1918

[6] Le principal suspect, Bruce Ivins, était un microbiologiste travaillant dans un laboratoire militaire américain spécialisé dans les armes biologiques. Il a été identifié par le FBI après une longue enquête, mais il s'est suicidé en 2008 avant d'être officiellement inculpé.

envisageables dans le futur tout comme la diminution de la sensibilité d'un agent biologique aux méthodes de diagnostic et de détection déjà utilisées.

En définitive, toutes ces prévisions et ces scénarios nous imposent de nous préparer face à cette menace bien spécifique mais toujours d'actualité. Pour cela, il nous faudra être toujours renseigné sur les activités de nos potentiels adversaires dans le domaine. C'est pourquoi la Red Team Défense a pris en compte dans ses travaux prospectifs la dimension portée par le risque de guerre biologique dans le futur. Ce scénario de guerre biologique explore les conséquences des avancées biotechnologiques dans un futur proche et nous permettent d'appréhender cette menace pour nous y préparer.

Les pièges invisibles d'une décision

Par le Chef de bataillon Nicolas VANLOO, stagiaire EMSST 2024-2025,
Mastère spécialisé en management des risques à l'ENSAM

Selon KAHNEMAN (2011, *Thinking, Fast and Slow*), « Le mot illusion évoque l'idée d'illusion d'optique, parce que nous connaissons tous ces images trompeuses. Mais les illusions ne sont pas cantonnées au domaine de la vision ; la mémoire aussi y est sujette, tout comme la pensée, de manière plus générale. ».

S'engager dans des raisonnements réfléchis et analytiques demande des ressources importantes en mémoire de travail, pour retenir, analyser, manipuler et traiter les données reçues. Cependant, notre inclination naturelle est davantage d'utiliser le « système 1 » de notre cerveau, qui est rapide et intuitif, plutôt que le « système 2 », qui demande plus d'effort cognitif et d'énergie.

Les biais cognitifs sont ainsi des raccourcis de jugement particulièrement fréquents lors de l'utilisation du système 1 de notre cerveau, qui peuvent mener à des décisions irrationnelles face à des incertitudes. Ce domaine fait l'objet de nombreuses études qui militent sur l'aspect particulièrement prévisible et systématique de ces comportements, qui sont par conséquent instrumentalisables à des fins d'influence ou de manipulation.

En utilisant des techniques de désinformation, de tromperie et d'influence, un adversaire peut se servir des biais cognitifs pour orienter l'interprétation du renseignement recueilli et induire en erreur les analystes et les décideurs. Souvent, l'erreur ne provient pas d'une manipulation de l'ennemi, mais plutôt de biais intrinsèque au fonctionnement de notre cerveau.

Basé sur les enseignements dispensés par l'École nationale supérieure d'arts et métiers (ENSAM), cet article explore certains biais cognitifs que nous pourrions retrouver dans le domaine du renseignement en opération et propose des stratégies pour les contrer.

➢ Biais dans la collecte du renseignement

• *Biais de disponibilité*

Le biais de disponibilité se produit lorsque l'on juge la probabilité d'un évènement en fonction de la facilité avec laquelle des exemples viennent à notre esprit ou lorsque l'on donne trop de poids aux informations qui nous parviennent. Cela peut fausser le jugement en rendant certains risques ou opportunités plus probables qu'ils ne le sont réellement.

Un adversaire peut ainsi mettre en scène des évènements marquants ou médiatisés dans le but d'influencer la perception de la menace, orienter les analystes vers une surévaluation de certains types d'attaque et ainsi détourner l'attention des véritables objectifs stratégiques de l'ennemi. La bataille de Hattin au cours des Croisades (1187) illustre ce biais. Les forces croisées, menées par le roi Guy de LUSIGNAN, y ont subi une défaite décisive face aux armées de SALADIN, principalement à cause d'une

mauvaise interprétation des renseignements recueillis et d'une évaluation hâtive de la situation qui les a conduits dans un piège, entraînant inéluctablement leur défaite.

Pour se prémunir contre ce type de manipulation, il est essentiel de diversifier les sources de renseignement et ne pas se focaliser uniquement sur les évènements récents.

- ***Biais de rétrospection***

Le biais de rétrospection est la tendance à voir des évènements passés comme étant plus prévisibles qu'ils ne l'étaient avant qu'ils ne se produisent, sans tenir compte des incertitudes du moment. Cela peut fausser la nouvelle prise de décision en créant un faux sentiment de sécurité. Cependant, ce biais de rétrospection se manifeste principalement lors du jugement des actions entreprises.

L'incident de My Lai durant la guerre du Vietnam, illustre ce biais. Les soldats américains ont tué un grand nombre de civils vietnamiens dans le village de My Lai, en réponse à des soupçons de soutien aux forces ennemies. Après que les détails de cette action aient été révélés au public en 1969, les médias ont largement couvert l'affaire, alimentant un sentiment croissant de désillusion envers la guerre et conduisant à des critiques acerbes sur la compétence des commandants militaires. Les opinions publiques ont alors été influencées par une vision simplifiée des évènements, souvent déformée par le biais de rétrospection, où les actions et les décisions des chefs militaires étaient jugées uniquement sur la base des conséquences catastrophiques qui avaient suivi.

Pour atténuer ce biais, il est essentiel de mener une analyse post-mortem objective des projets ayant échoué, en considérant tous les aspects du problème. Il convient donc d'archiver les données apportées par les services de renseignement pour comprendre les incertitudes auxquelles les décideurs ont dû faire face.

- **Biais dans l'évaluation des incertitudes**

- ***Biais de confirmation***

Peter WASON, psychologue britannique connu pour ses recherches sur le raisonnement, met en lumière le biais de confirmation à travers un casse-tête appelé « la tâche de sélection » (1966). Il souligne l'erreur systématique consistant à chercher à confirmer une hypothèse ou une croyance *a priori*, plutôt qu'à la réfuter.

Les sites en ligne sur l'actualité capitalisent sur ce biais en personnalisant le flux d'articles en fonction des lectures antérieures et des sujets d'intérêt de chaque utilisateur. Un décideur peut également y succomber lorsqu'il accorde inconsciemment plus d'importance aux données recueillies par le renseignement qui sont en phase avec ses croyances préexistantes sur un sujet, qu'à ceux qui s'y opposent. Un ennemi peut également fournir délibérément des informations pour entretenir des scénarios fallacieux afin de dissimiler ses véritables intentions.

Par conséquent, pour contrer ce biais, il est recommandé de rechercher les arguments allant à l'encontre du schéma de manœuvre envisagé, plutôt que de

chercher à le confirmer et de réfléchir sur les raisons pour lesquelles la décision que l'on s'apprête à prendre pourrait se solder par un échec.

➢ Biais dans le processus de prise de décision

- ***Biais d'optimisme et de supériorité***

Le biais d'optimisme consiste à croire que l'on a moins de chances d'éprouver des difficultés que nos pairs. Il se combine très bien avec le biais de supériorité qui est l'idée retenue que l'on se situe au-dessus de la moyenne. Cela peut mener à une mauvaise évaluation des objectifs à atteindre et sous-estimer les délais nécessaires.

Le biais de supériorité a conduit à une erreur stratégique majeure lors de l'opération Market Garden, en septembre 1944. Cette opération alliée, conçue par le Maréchal britannique Bernard MONTGOMERY, visait à pénétrer rapidement en Allemagne en prenant le contrôle d'une série de ponts aux Pays-Bas. Le renseignement allié avait relevé que les forces allemandes dans la région étaient plus importantes et mieux organisées que prévu. Cependant, les commandants alliés, y compris MONTGOMERY, biaisés par les récents succès de la campagne de Normandie, ont choisi de ne pas tenir compte de ces informations, engendrant *in fine* l'échec de l'opération.

Pour contrer ce biais, il est recommandé entre autres d'impliquer les parties prenantes dans le processus décisionnel pour obtenir et confronter des perspectives différentes. Il est également nécessaire de maintenir une vision réaliste de ses capacités ainsi que de celles de l'ennemi et d'ajuster les stratégies en conséquence.

- ***Biais des coûts irrécupérables***

Il est difficile d'admettre en public ou en privé que l'on s'est trompé dans l'investissement d'un projet et qu'il conviendrait de l'arrêter malgré les sommes déjà versées, même si elles sont désormais « irrécupérables ». Persister sur un projet pour ne pas gâcher l'argent déjà investi, tel est le biais des coûts irrécupérables qui amène à dépenser toujours plus pour rentabiliser les dépenses passées. Il est d'autant plus fort lorsque le décideur qui peut mettre un terme à cet enlisement est aussi responsable de la dépense initiale.

Ainsi, lors de la bataille de Stalingrad, HITLER et son haut commandement ont refusé de reconnaître l'échec indéniable de l'opération en cours et ont persisté à envoyer de nouvelles troupes et du ravitaillement dans une ville déjà encerclée par les Soviétiques. Cette décision illustre comment le biais des coûts irrécupérables peut pousser à maintenir une stratégie perdante, malgré les signes évidents d'une défaite imminente.

Ainsi, pour prendre une décision rationnelle, il est recommandé de comparer les bénéfices attendus avec les coûts futurs, sur lesquels on peut réellement agir et faire abstraction des investissements passés. Il convient également de dédramatiser le changement de stratégie bien que cela puisse être extrêmement difficile selon le contexte.

➢ Conclusion

La liste des biais de raisonnement cités *supra* n'est pas exhaustive. La littérature psychologique recense plus de 200 biais cognitifs. Comprendre leur fonctionnement constitue une première étape vers une prise de décision plus éclairée.

En outre, en adoptant des pratiques qui favorisent la réflexion critique, la diversité des sources de renseignement et une analyse rigoureuse des données recueillies, il est possible de réduire leur impact.

Il convient également de noter que les biais cognitifs peuvent servir d'outils puissants pour manipuler un adversaire et compromettre sa stratégie, comme l'histoire l'a maintes fois illustré.

L’ordre serré, un catalyseur de cohésion ?

Par le Capitaine Ludovic MARTEL, stagiaire EMSST 2024-2025, Université des sciences du sport

Ceux qui ont revêtu l’uniforme le savent bien : les premiers pas dans l’armée ou au sein d’une unité à vocation militaire (gendarmerie, police, sapeurs-pompiers) s’effectuent généralement en cadence, en groupe et sous les ordres d’un chef, souvent avant même d’avoir pu tenir entre leurs mains l’arme de dotation.

L’OS, pour « ordre serré », est véritablement l’une des principales singularités militaires, après le maniement des armes. Son origine remonte à la Grèce antique, où il désignait la manière de rassembler les soldats en unité constituée durant une bataille ou lors des déplacements. L’intérêt de l’ordre serré était d’abord tactique. En effet, les Grecs, grâce à leur formation en phalange, ont été à l’initiative de ce regroupement de soldats, les lances pointées en avant et les boucliers orientés d’un côté, protégeant ainsi le flanc de l’unité.

Si ce « bloc » combine à la fois force de frappe et protection, il stimule également un aspect moins tangible du champ de bataille : le courage. Comme l’explique Arthur Boucher[7] : « … ce qui domine dans la tactique grecque, c’est la préoccupation d’organiser la bravoure. Cette idée engendre la file, qui permet d’utiliser la bravoure des plus braves et d’en donner à ceux qui peuvent ne pas en avoir. […] La file se prête avec la plus grande facilité à toutes les formations que peut avoir à prendre une troupe créée exclusivement pour le combat, le soldat n’ayant jamais qu’à suivre les traces de celui qui est devant lui ».

Repris par les Macédoniens et les légions romaines, l’ordre serré a été régulièrement adapté à chaque époque et à chaque peuple guerrier, avec succès. Son intérêt tactique atteint son paroxysme avec l’apparition des premières armes à feu. Le manque de puissance et de précision des fusils de l’époque étaient compensés par le volume et la synchronisation des tirs, avant que le choc du corps à corps ne devienne, avant l’amélioration des fusils et munitions au XIX^{ème} siècle, la phase déterminante d’une bataille. L’ordre « Serrez le rang !» visait ainsi à éviter toute dislocation de la troupe et à maintenir les moins braves dans les rangs[8].

Aujourd’hui, avec l’avancée technologique des systèmes d’armement, l’ordre serré n’a plus sa place sur le champ de bataille et rendrait n’importe quelle armée vulnérable au feu ennemi. Pourtant, cet exercice continue d’être enseigné et plébiscité par le commandement militaire. De nombreuses vertus lui sont encore attribuées, telles que le renforcement de la discipline, de la rigueur, de l’esthétique et de la cohésion des soldats.
Si la discipline et la rigueur se conçoivent assez aisément à travers le respect des ordres et des postures imposées par l’ordre serré, ainsi que l’esthétique mise en avant

[7] « La tactique grecque à l’origine de l’histoire militaire ». 1912, Boucher A. Revue des études Grecques
[8] De guerre et de grâce : le pas cadencé dans l’armée française de la seconde moitié du XVIII^{ème} siècle (1750-1791). 2015, Arnaud Guinier, p15-26, e-Phaïstos – Revue d’histoire des techniques.

lors des cérémonies et parades militaires ; la cohésion, quant à elle, est plus difficile à interpréter.

Pourquoi une troupe qui marche en cadence développerait-elle son esprit de cohésion ?

En 1521, Machiavel fut l'un des premiers grands théoriciens de la guerre à appeler les troupes à marcher au « *son du tambourin* », afin de synchroniser leur rythme avec celui-ci. Cependant, ce sont les Prussiens qui instaurèrent cette pratique en imposant à leurs armées de marcher d'un pas ne dépassant pas 60 centimètres, ce qui favorisait une synchronisation des mouvements et évitait de heurter le talon du soldat qui le précédait.

À la même époque, en France, c'est le Maréchal de Saxe qui initia la marche au pas cadencé pour améliorer « *la manœuvre des troupes et la psychologie des hommes* ».
Il ajoutait également : « *ils sont unis, se sentent plus forts, et si l'un tombe, on resserre les rangs, et le groupe poursuit son avance. Les chants et la musique militaire n'ont pas d'autre rôle : améliorer la cohésion et le mouvement des armées, redonner de l'élan au soldat, réduire la sensation de fatigue*. »
Le pas du soldat a également fait l'objet d'une ordonnance en 1788 afin de formaliser celui-ci.
Les chefs militaires de l'époque perçoivent donc, sans réellement comprendre, que l'ordre serré et la synchronisation que cela induit entre les hommes, auraient un effet favorable sur la cohésion et performance au combat.

Plus récemment, une étude[9] menée en 2014 par Daniel Fessler et Colon Holbrook de l'université de Los Angeles a mis en lumière l'influence de la synchronisation sur les perceptions des membres d'un groupe. Après avoir comparé deux groupes d'individus, dont l'un marchait au pas tandis que l'autre ne le faisait pas, les chercheurs ont constaté que la synchronisation des pas influençait la manière dont les membres percevaient l'environnement. En effet, le groupe qui avait synchronisé ses pas avait tendance à minimiser les caractéristiques physiques (tailles, corpulence, etc.) d'une personne aux traits agressifs présentée sur une photo, la rendant moins menaçante.

Daniel Fessler a conclu son étude de la manière suivante : « *Nous avons constaté que lorsque des hommes marchent en synchronisation avec d'autres, ils pensent qu'un ennemi potentiel est plus petit et moins redoutable physiquement et donc moins intimidant que quand ils marchent simplement* ». L'étude a également souligné que le sentiment d'appartenance ou de lien social était plus fort chez les individus qui avait synchronisé leurs pas.

Par ailleurs, une étude[10] d'Ilanit Gordon publiée en 2020, s'est s'intéressée aux paramètres physiologiques de la cohésion, en mettant en évidence les liens qui peuvent exister entre la synchronisation des variabilités cardiaques des individus, leur cohésion et leur performance sur une tâche impliquant de la coopération. Pour cela,

[9] « Entrer dans la bataille : marcher de manière synchronisée diminue la perception de redoutabilité d'un adversaire chez l'homme ». 2014, D.M.T Fessler and C. Holbrook. *Lettres biologiques*
[10] « Physiologique et comportemental : la synchronie prédit la cohésion et la performance du groupe ». 2020. I. Gordon & al.

l'étude a identifié 41 groupes de 3 individus pour lesquels on a créé, dans un cas, des conditions favorables de synchronisation mais pas dans l'autre. Les chercheurs ont alors tenté de mesurer le degré de cohésion sociale et opératoire qu'il en découlait, tout en l'associant à la variabilité cardiaque observée durant l'expérience.
Les résultats mettent clairement en évidence que les groupes dont le rythme cardiaque était le mieux synchronisé ont montré une cohésion et une performance de groupe plus forte que les autres.

Cependant, on ne sait pas encore dans quel ordre s'enchaîne ces adaptations. Est-ce le fait d'avoir un rythme cardiaque synchronisé qui favorise la cohésion ou l'inverse ? C'est pourquoi, il faut peut-être considérer la synchronisation cardiaque comme un déterminant physiologique synonyme de la cohésion.

Mais, en quoi l'ordre serré induirait de telles synchronisations ? Sachant que la cadence du pas dans l'armée française est de 120 par minute et que la fréquence cardiaque d'un individu en train de marcher oscille entre 105 et 135 battements par minute, on obtient alors une superposition de ces deux rythmes qui peuvent, avec le temps, tendre à se synchroniser. L'ordre serré, au même titre que les percussions de l'expérimentation de I. Gordon, pourraient réunir les conditions propices au développement de la cohésion au sein du groupe.

Une étude analysant le rythme cardiaque des militaires durant un défilé permettrait de tester cette hypothèse. Néanmoins, même sans une telle validation, ne pouvons-nous pas déjà affirmer qu'à l'heure où des séminaires et des séances de « team building » promus par les experts en management, sont largement utilisés pour renforcer la cohésion des groupes, les armées possèdent, avec l'ordre serré, un catalyseur de cohésion à la fois puissant et unique ?