L'IMPACT DE L'INTELLIGENCE ARTIFICIELLE DANS LA GUERRE DE L'INFORMATION

MEMOIRE DE FIN D'ETUDE 2017-2019

L'IMPACT DE L'INTELLIGENCE ARTIFICIELLE DANS LA GUERRE DE L'INFORMATION

Table Des Matières

I. Introduction

L'intelligence Artificielle fait partie des sujets actuels, on ne peut le nier.À la télévision, dans les publicités, les oeuvres de fictions et la bouche de chacun, tout le monde en parle. Moi même, été un grand passionné de science-fiction (tout particulièrement de l'univers *Ghost In The Shell*, qui met en action plusieurs intelligences artificielles) , je n'ai pu résister à ma curiosité sur le sujet bien longtemps. A mon sens, il semblait inévitable que mon mémoire parle de ce sujet. Bien évidemment, en s'y intéressant, on peut très vite saisir l'importance des données et de l'information dans un système d'IA.

La guerre de l'information ne fait pas partie des sujets actuels. C'est une forme de conflit aussi vieille que les premiers conflits existants, mais elle a été remise en avant avec l'arrivée de l'informatique. De part mon métier que j'ai choisi de faire aujourd'hui, l'informatique et l'information font parties intégrante de ma vie. Je peux voir facilement l'importance que à cette dernière. Difficile alors de ne pas se poser la question de ce qu'il pourrait se passer pour l'IA quand on l'utilisera afin de traiter les informations et communications.

Mes premières recherches se sont concentrées sur l'impact de l'intelligence artificielle sur la guerre de l'information(ou infowar) afin de savoir si cette question avait au moins un intérêt à être soulevée, et si il existait des éléments de réponses qui pouvaient m'orienter dans mes recherches.

Le sujet, bien que abordé, ne l'est que rarement en profondeur. Je prend par exemple la comparaison issu de l'ouvrage RIS 110 – ÉTÉ 2018, présentant les technologies dans le monde de la géopolitique, qui associe l'intelligence artificielle à une arme nucléaire dans un cadre de gestion de l'information, sans réellement expliquer pourquoi, ni dans quel mesure. A ce jour, je n'ai pas trouvé de document pouvant m'indiquer l'impact que à l'utilisation d'un système d'intelligence artificielle dans le big data, par exemple, dans le jeu de chat et de la souris que est l'infowar.

Prenant conscience des difficultés que je rencontrais afin de trouver des ressources satisfaisantes pour m'aider à comprendre que seront les impacts, j'ai décidé de séparer la problématique deux thèmes. D'un côté, l'intelligence artificielle et de l'autre, la guerre de l'information. Afin de pouvoir correctement répondre à ma problématique, je pense que il est important d'essayer de comprendre les deux parties séparément, avant de les mettre en lumière l'une de l'autre.

Que ce que l'intelligence artificielle?Pourquoi et comment effectuons nous des recherches dans ce domaine, sur quel principe elle c'est conçu, que sont ces objectifs et problèmes?
Que ce que la guerre de l'information? Pourquoi est elle utilisé? Comment? qui sont ces acteurs?Que sont ces outils?dans quel domaine elle s'applique?
Finalement, que pourrai-je en conclure en ayant accumulé suffisamment de connaissance dans ces deux domaines?

Ce mémoire sera donc construit en trois parties.

La première sera etat de l'art sur l'intelligence artificielle. Un tour de quelque pages sera fait sur son origine, afin de savoir pourquoi elle est née et sur quel principe elle est basée.
Nous verrons la différence entre une IA faible et IA forte. Cela permettra de tuer dans l'oeuf quelques fausses idées qu'il existe sur l'intelligence artificielle et appuyé sur le fait que l'IA dont nous parlons et utilisons actuellement est l'IA faible. Les objectifs de l'IA seront définit ensuite au travers des trois domaines de tâches.

Finalement, nous allons voir ce qui se cache derrière les termes "d'intelligence artificielle". les différents types d'algorithme et modèle, puis la donnée en elle même. Un zoom sera fait sur les lacs de données, les réseaux neuronaux et l'apprentissage profond, qui sont des technologies très utilisés aujourd'hui.

La deuxième partie sera concentrée sur la guerre de l'information.Une petite précision sera fait sur la notion de "Guerre", puis on définit aussitôt ce qu'est "l'information". On parlera des acteurs de ce genre de conflit ainsi que les méthodes et techniques utilisés. On conclura sur quelques exemples de guerre d'informations entre différents acteurs.

Finalement, la dernière sera à la fois le fin de l'état de l'art, mais la résultante de mes recherches afin de définir l'impact des technologies de l'intelligence artificielle dans la guerre de l'information. Maintenant que IA et infoguerre sont deux domaines un peu moins opaques, on va définir une suite de domaines, comme le big data, la prise de décision, ou le langage naturel, et voir ce qui est utilisé en terme d'IA dans ces derniers.

Puis nous allons définir un cadre, une guerre d'information, afin d'examiner comment l'IA peut y avoir un impact.

Mot clé:

intelligence artificielle, l'information,guerre de l'information,big data,lacs de données
réseaux neuronaux,apprentissage profond

II. Introduction

Artificial intelligence is one of the current topics, it can not be denied.At television, in commercials, works of fiction and in the mouth of everyone, everybody speaks about it.Myself was a big fan of science fiction (especially the *Ghost In The Shell* universe, which puts into action several artificial intelligences), I could not stop my curiosity on this subject for a long time. In my opinion, it seemed inevitable that my dissertation speaks of this subject. Of course, by focusing on it, one can quickly grasp the importance of data and information in an AI system.

The information war is not one of the current topics. This is a form of conflict who are old as the first existing conflicts, but it has been brought forward with the advent of IT science. Because of my job that I chose to do today, computers and information are an integral part of my life. I can easily see the importance of it. Difficult then not to ask the question of what could happen to the AI when it will be used to process information and communications.

My first research focused on the impact of artificial intelligence on information warfare (or infowar) to find out if this question had at least an interest to be raised, and if there were some elements of answers that could guide me in my research.

The subject, although approached, is only rarely in depth. I take for example the comparison from the book RIS 110 - SUMMER 2018, presenting technologies in the world of geopolitics, which combines artificial intelligence with a nuclear weapon in an information management framework, without really explaining why, or to what extent. To date, I have not found a document that can tell me the impact of using an artificial intelligence system in big data, for example, in the game of cat and mouse that is the infowar.

Recognizing the difficulties I had in finding satisfactory resources to help me understand what the impacts will be, I decided to separate the problematic in two themes. On the one hand, artificial intelligence and on the other, the infowar. In order to be able to answer my problem correctly, I think it is important to try to understand the two parts separately, before highlighting them.

What is artificial intelligence? why and how do we conduct research in this area? what principle is it designed for? what are these objectives and problems?
What is the information war? Why is it used? How? Who are these actors? What are these tools? In what area does it apply?
Finally, what can I conclude by having accumulated enough knowledge in these two areas?

This thesis will be built in three parts.
The first will be state of the art on artificial intelligence. Some pages will be done on its origin, to know why it was born and on what principle it is based.
We will see the difference between a weak AI and a strong AI. This will kill some of the false ideas that exist on artificial intelligence and support the fact that the AI we are talking about and using now is weak AI. The objectives of the AI will then be defined through the three task areas.

Finally, let's see what lies behind the terms "artificial intelligence". the different types of algorithm and model, then the data itself. A zoom will be made on data lakes, neural networks and deep learning, which are technologies widely used today.

The second part will be focused on the information war. A small precision will be made on the notion of "War", then we immediately define what "information". We will discuss the actors of this kind of conflict as well as the methods and techniques used. We will conclude on some examples of infowar between different actors.

Finally, the last part will be both the end of the state of the art, and the result of my research to define the impact of artificial intelligence technologies in the information war.
Now that AI and infowar are two domains a little more understood, we will define a series of domains, such as big data, decision-making, or natural language, and see what is used in terms of AI in these last ones.

Then we will define a framework, an information war, to examine how the AI can impact.

keyword:

artificial intelligence, information, information warfare, big data, data lakes neural networks, deep learning

III. Les technologies de l'intelligence artificielle

A. Que ce que l'intelligence artificielle?

Selon Marvin Minsky, l'un des pionniers de l'intelligence artificielle(I.A), nous pouvons la définir comme "*la construction de programmes informatiques qui s'adonnent à des tâches qui sont pour l'instant, accomplis de façon plus satisfaisante par des être humains car elles demandent des processus mentaux de haut niveau tels que: l'apprentissage par la perception, l'organisation de la mémoire et le raisonnement critique.*"

De manière générale, Il s'agit du domaine d'étude cherchant à utiliser un ensemble de processus et algorithmes puisant dans d'autres domaines dans le but de créer une machine qui puisse se rapprocher d'une forme d'intelligence biologique (une intelligence humaine, en d'autre terme).Pour ceci,le système va permettre à un programme d'utiliser une méthode d'apprentissage (un algorithme d'apprentissage, comme l'apprentissage machine et l'apprentissage profond) pour s'entraîner avec un ensemble de jeu de données. L'I.A a ainsi puisé dans de nombreux domaines, que l'on peut regrouper ainsi:

- **les sciences informatiques**

Certains langage de programmation sont très largement utilisés dans la conception des différents composants de l'I.A, comme Python, par exemple. Mais des domaines comme le Big Data (données numériques devenu tellement importantes en quantité que il en devient difficile d'en effectué une analyse efficace par nos propres capacités humaines ou par des outils informatiques classiques),ou tout simplement les questions d'optimisation et d'efficacité de stockage et de vitesse d'accès aux données sont des éléments importants, tout particulièrement quand l'information est une composante capitale pour l'I.A.

- **la robotique**

En se basant sur la théorie de la cognition incarnée, ou "*embodied cognition*", qui décrit que de nombreux aspects des capacités cognitives sont construitent à partir de l'entièreté du corps d'un organisme (comme le mouvement, la perception et la visualisation), humain ou autres, des chercheurs en robotique on développer un système d'apprentissage pour la machine afin qu'elle puisse accumuler des connaissances au travers d'exploration et d'interaction autonome de leur environnement.

- **les sciences humaines**

La technologie des réseaux de neurones artificielles est un modèle simplifié du fonctionnement d'un cerveau humain, par exemple. Mais de manière plus générale, le domaine de l'I.A cherche à reproduire une intelligence biologique, et prend régulièrement comme exemple l'être humain. Des domaines comme la psychologie ou la linguistique peuvent être largement utilisé dans le cas de la conception d'une intelligence artificielle capable de communiquer et représenter des émotions humaines. Un exemple est **Sophia**, le robot créé par l'entreprise Hongkongaise Hanson Robotics, utilisant les technologie de Alphabet et la reconnaissance faciale afin de nourrir son

intelligence artificielle pour permettre de simuler des conversations et adapter son ton et ses expressions faciales selon ce qui est dit.

- **les mathématiques**

Les mathématiques sont au coeur de l'intelligence artificielle. Utilisé dans quasiment tous les domaines de l'I.A, on peut les retrouvés dans les calculs de taux d'erreurs, les fonction linéaire dans les réseaux de neurones ou pour effectuer des prédictions. Les mathématiques et statistiques sont à la base de l'I.A.

- **Information engineering** (que l'on peut traduire par "Gestion de l'information"):

Il s'agit d'un domaine qui étudie la génération, distribution et l'analyse de tout ce qui se rapproche de l'information (de la données brut au "*savoir*") dans un système. On l'utilise dans le cas de machine learning, par exemple, mais aussi dans la détection d'éléments sur une image.

1. Historique

Bien que l'objectif de ce mémoire n'est pas de faire un état de l'art détaillé sur l'historique de l'IA, il est cependant important d'avoir une vue générale de son histoire, afin de comprendre d'où nous vient ce domaine, et les nombreux principes, réflexions, légendes et fictions qui sont à la base de l'intelligence artificielle.

Si les principes et réflexions sont là pour offrir une base à ce qui sera plus tard le domaine académique de l'intelligence artificielle, ce fut d'abord par les légendes et fictions que naîtra l'intelligence artificielle,ainsi que les termes que nous association à ce domaine.

a) La fiction

Le principe d'entité artificiel capable d'imiter ou de posséder une intelligence biologique n'est pas une notion moderne. Elle existe depuis au moins l'antiquité, début du développement de l'écriture. c'est par ailleurs cette absence d'écrit qui rend difficile de remonter plus loin.

La mythologie de la grèce antique a été l'une des premières à explorer la notion de vie mécanique doté d'une intelligence quasi humaine, au travers du dieu Héphaïstos, artisan et maître du feu. Les sources antiques, tel que l'iliade, lui attribue de nombreuse créations d'automate capable d'imiter la vie. Nous pouvons citer, comme exemple:

- les 6 automates, servantes d'or, capable de réflexion. Créée afin de l'assister dans ces travaux, elles ont été conçu pour imiter une intelligence humaine.*(Iliade, chant 18,page 418-419);*

- Talos, colosse de métal qu'il a crée pour Minos ou Europe (les sources divergent sur ce point) afin de protéger la Crète;

- De nombreux automates conçu en se basant non pas sur l'humain, mais sur la vie animales. Trois chiens, un pour Zeus, deux pour garder le palais d'Alkinoos, ou encore un aigle, toujours pour Zeus.

- ❏ Mais aussi un certains nombres d'objets du quotidien capable d'agir d'eux même, comme les soufflets de sa forge, qui semble pouvoir travailler de manière autonome.

C'est de ces légendes que est née le terme d'automates, issu du latin "*automatê",* voulant dire "de soi même".

Le terme de robot, lui, est issu de la pièce de théâtre tchèque de Karel Čapek, **R.U.R**, ou "*Rossum's Universal Robots*". Cette pièce nous présentes des androïdes, crée par l'homme et capable de réflexion. Ainsi, robot est dérivé de "*robota"*, que l'on peut traduire par "travaux forcés*".*

b) le raisonnement formel, de l'antiquité à Dartmouth

Mais c'est aussi durant l'antiquité que est aussi née l'un des principes qui sera le fondement de l'intelligence artificielle, et qui permettra, en 1956, de considérer cette dernière comme une discipline académique.

Le raisonnement formel, issu de la réflection de plusieurs philosophes (Aristote, qui proposa un raisonnement formel du syllogisme dans son ouvrage "*Premiers Analytiques*", Euclide, dont son étude "*Elements*" est un modèle de raisonnement formel sur la géométrie et la théorie des nombres, ou al-Khwārizmī, qui a donné naissance à l'algèbre et aux principe d'algorithme), est la théorie que le processus de réflexion humaine peut être mécanisé.

Ce principe fut régulièrement étudié et à évolué au cours de l'histoire. Le Philosophe Ramon Llull à développé plusieurs machines fonctionnant sur des opérateurs logiques, combinant plusieurs vérités basiques et avérés afin d'essayer de produire toutes les connaissances possible (*The Art and Logic of Ramón Llull: A User's Guide*, Brill, 2007). Ces instruments et réflexions, nommés *Ars magna,* ont une grande influence sur Gottfried Leibniz , philosophe et mathématicien. Ce fut lui, avec Thomas Hobbes et René Descartes, qui explora le raisonnement formel au travers de l'algèbre et des mathématiques. Au travers de leur travaux, ils commençaient à structurer ce qui deviendra plus tard l'hypothèse du raisonnement formel par système de symbole physique, ou *physical symbol system hypothesis*(PSSH).

Avec l'arrivé des travaux de George Boole et Gottlob Frege (respectivement *The Laws of Thought*,1854 et *Begriffsschrift,*1879*,* deux livres sur la logique et le système formel) les fondations du **PSSH** ont été mise en place. Cela fut suivi par *Principia Mathematica,*1913 de Bertrand Russell et Alfred North Whitecard, qui se sont basés sur les travaux de G.Frege pour présenter un traitement plus formel et organisé des fondations mathématiques. Ce dernier livre fut alors la motivation pour David Hilbert de poser la question "*Est ce que tous les raisonnements mathématiques peuvent être formalisés*?".

La réponse fut donné par Kurt Gödel,Alan Turing et Alonzo Church, au travers de *Gödel's incompleteness theorems,*1931 (deux théorèmes de logique mathématiques montrant les limitations de toute systèmes formel axiomatique, un axiom étant un postulat que l'on considère comme vrai afin de permettre l'avancement d'un raisonnement et d'argumentation), **la machine de turing** (qui est, à sa base, un modèle mathématique permettant à une machine de manipuler des symboles selon une table de règle) et la **thèse de Church-Turing** (il s'agit d'une hypothèse qui déclare que une fonction

utilisant des nombres naturels est manipulable par un être humain suivant une algorithme, seulement si cette fonction peut être manipulé par la machine de Turing).

Ces travaux ont permis de voir que n'importe dispositif mécanique peut imiter n'importe quel processus de déduction mathématique, avec comme exemple la **machine de turing**, dispositif mécanique pouvant manipuler des symboles abstrait, concrétisant le **PSSH**.

Allen Newell et Hebert A. Simon dans "*Computer Science as Empirical Inquiry:Symbol and Search*", 1976, ont formulés le **PSSH** ainsi:

"*A physical symbol system has the necessary and sufficient means for general intelligent action*."

Selon cette hypothèse,l'esprit humain fonctionne par manipulation de symbole, ou paternes, qu'il combine en structures, ou expressions, afin de pouvoir les manipuler et produire de nouvelles structures.
Or, avec **la machine de turing**, nous avons pu voir que un dispositif mécanique peut aussi manipuler des symboles.(les chiffres et opérateurs sont les symboles, les expressions sont les équations qui sont une combinaisons de ces symboles et les manipulations sont effectuées selon une table de règle). Si nous suivons cette hypothèse, une machine peut être intelligente.

Bien entendu, cette hypothèse peut être mettre en doute, comme la fait Hans Moravec,membre de l'institut de robotique de l'université de Carnegie Mellon. Dans son article *Mind Children*, 1988, paru dans le Harvard University Press,il écrira ce qui deviendra le **paradoxe de Moravec**:

"il est comparativement plus simple de créer des ordinateurs capable d'effectuer des performance d'adulte sur des tests d'intelligences ou jouant aux échecs, et difficile voir impossible de leur donner des compétences d'un enfant de un an quand il s'agit de perception ou de mobilité".

Basé sur le **PSSH**, un séminaire de deux mois réunissant 21 mathématiciens et scientifiques autour de l'intelligence artificielle, nommée le "*Dartmouth Summer Resarch Project on Artificial Intelligence*", fut organisé en 1956 au collège de Dartmouth.L'objectif était une discussion autour des sujets se rattachant à l'intelligence artificielle à l'époque:

- ❏ l'ordinateur
- ❏ le traitement automatique du langage naturel
- ❏ les réseaux de neurones
- ❏ la théorie du calcul
- ❏ la philosophie de l'abstraction
- ❏ la créativité

dans l'objectif de faire une avance dans ce domaine. (" *A proposal for the dartmouth summer research project on artificial intelligence*",1955). Cela a permis de considérer le domaine de l'intelligence artificielle comme une discipline académique à part entière, ouvrant alors sur les premières recherches et travaux officiels de l'intelligence artificielle.

c) Les premiers pas de la discipline...

Suite au **séminaire de Dartmouth**, de nombreuses recherches ont été effectuées. A.Newell et H.Simon, durant une rencontre en 1957, on prédit qu'une machine suffisamment intelligente pour être championne d'échec serait construite dans environ 10 ans ("*Artificial Intelligence: A Modern Approach*,2009", de Stuart J. Russell et Peter Norvig).Si il y a bien eu une machine devenue championne d'échec (**deep blue**, conçu par IBM), cela est arrivé 40 ans après.

En premier lieu, Arthur Samuel, professeur au MIT, à conçu en 1952 des programmes pouvant jouer au échec niveau amateur.
Ces programmes ont été conçu pour but de démentir l'idée que un ordinateur peut uniquement faire ce qu'on lui dit de faire: ces derniers ont rapidement appris à mieux jouer que leur créateur.
En voyant que, en 1952, la mémoire d'un ordinateur était très limitée, il a développé ses programmes autour d'une fonction de score, qui mesure le pourcentage de chance de chacun des joueurs de gagner à chaque position, prenant en compte le nombre de pièce de chacun des joueurs, la position du roi, et la position des pièces proches du bord adverses pouvant être promu. ("*Some studies in machine learning using the game of checkers",*2000, de A.Samuel).
Avec cette fonction, les programmes possèdent aussi une fonction de "*rote learning*", qui permets à une machine d'apprendre, en gardant un historique des calculs et résultats, afin de les comparer avec les nouveaux résultats. Cette fonction de "*rote learning*" est utilisé dans le cadre du "*machine learning*", ou **apprentissage par la machine**.

John McCarthy, alors professeur assistant à Dartmouth en 1956,parti pour le MIT. La bas, il fit deux cruciales contributions au domaine de l'I.A en une seule année, 1958:

- La première fut la création du langage **LISP**, qui fut pour les trentes années qui ont suivi le langage de programmation dominant pour l'intelligence artificielle.

- Un article se nommant "*Programs with Common Sense*", décrivant un programme hypothétique, **Advice Taker**, qui peut être vu comme le premier système d'intelligence artificielle forte.
  Advice Taker, selon son créateur, posséderait une suite d'information basiques, de fond, que tous connaisse ou que nous assumons tous être vrai (des axioms) , afin de pouvoir résoudre différents type de problèmes. Cependant, l'autre partie de ce programme hypothétique est sa capacité à accepter de nouvelles vérités afin de développer des compétences dans d'autres domaines, sans devoir être reprogrammé.
  L'idée de donner des informations basiques et de axioms sera nommé plus tard les **connaissances du sens commun**("*Commonsense Reasoning and Commonsense Knowledge in Artificial Intelligence"*,2015, par Ernest Davis et Gary Marcus), et sera une des branches de l'intelligence artificiel, avec son lot de problématique qui seront abordés plus loin.

L'année suivante, H.Simon et A.Newell on mis en place le **General Problem Solver**, ou **G.P.S.** Très proche dans sa réalisation de l'**Advice Taker**, il à été construit afin d'imiter le processus de résolution de problème d'un être humain.
Bien que il était limité à la fois en terme de connaissance qu'il possédait et de puzzle que il pouvait résoudre **(G.P.S** ne pouvait résoudre que les problèmes,puzzle et jeu possèdent des règles clairement défini, tel que de la géométrie ou jeu d'échecs), dû à une limitation des capacités de mémoire de la

machine, un examen approfondi a permis de voir que l'ordre et la nature des sous-objectifs que le programme se fixait afin de résoudre un problème était similaire à la manière que à un être humain à résoudre le même problème.

Pour cela, la méthodologie était la suivante:

- ❏ présenter à **G.P.S** à problème.
- ❏ **G.P.S** va diviser l'objectif en sous objectifs.
- ❏ Il va tenter de résoudre chacun de ses sous objectifs les un après les autres, en s'aidant des connaissances qu'il possède (dans un cas de problème de calcul, il va par exemple appliquer des règles basique comme: "transformer un objet en un autre","réduire la différence entre deux objets","appliquer un opérateur entre deux objets" et les tables d'addition ou de soustractions")
- ❏ demander à un être humain de résoudre la même tâche en détaillant son processus.
- ❏ comparer les résultats.

"Human Problem Solving",1972 de A.Newell et H.Simon nous présente un exemple du processus de résolution de problème de **G.P.S**, dans le cas du problème de logique suivant,tel que :**L1= R*(-P => Q) vers L2=(Q ∨ P)*R.**

voici la résolution du problème par **G.P.S**:

- ❏ Objectif 1: Transformer L1 en LO
- ❏ Objectif 2: Reduire la différence entre L1 et L0
- ❏ Objectif 3 appliquer R1 à L1
- ❏ Objectif 4: Transformer L1 vers la condition (R1)
- ❏ Produit de L2(-P=>Q)*R
- ❏ Objectif 5:Transformer L2 en L0
- ❏ Objectif 6: Réduire la différence entre droite(L2) et droite(L0)
- ❏ Objectif 7: Appliquer R5 à gauche(L2)
- ❏ Objectif 8: Transformer Gauche(L2) en condition (R5)
- ❏ Objectif 9: Réduire la différence entre droite(L2) et condition(5)
- ❏ Rejeter: Nullement plus simple que objectif 6
- ❏ Objectif 10: Appliquer R6 to gauche(L2)
- ❏ objectif 11: Transformer gauche(L2) en condition(R5)
- ❏ Produit de L3:(P ∨ Q) *R
- ❏ Objectif 12: Transformer L3 en L0
- ❏ Objectif 13: Réduire la différence entre gauche(L3) et gauche(L0)
- ❏ Objectif 14:Appliquer R1 à gauche(L3)
- ❏ objectif 15: transformer gauche(L3) en condition(R1)
- ❏ Produit L4:(Q∨P)*R
- ❏ Objectif 16: Transformer L4 en L0

Une année juste après, en 1960, Herbert Gelernter, employé d'IBM après l'obtention de son doctorat en informatique à l'Université de Rochester en 1957, avec l'aide de Nathaniel Rochester, membre d'IBM qui avait pris en charge les différents projets d'intelligence artificielle dans l'entreprise,il a conçu le **Geometry Therorem Prover**, la troisième I.A jamais créée.

A l'inverse des deux précédentes, qui fonctionnait avec des problèmes ou jeux tournant autour de logique formel simple, le **G.T.P** permets de prouver des théorèmes géométriques plus complexe. ("*Realization of a geometry-theorem proving machine*",1959, de Herbert Gelernter)

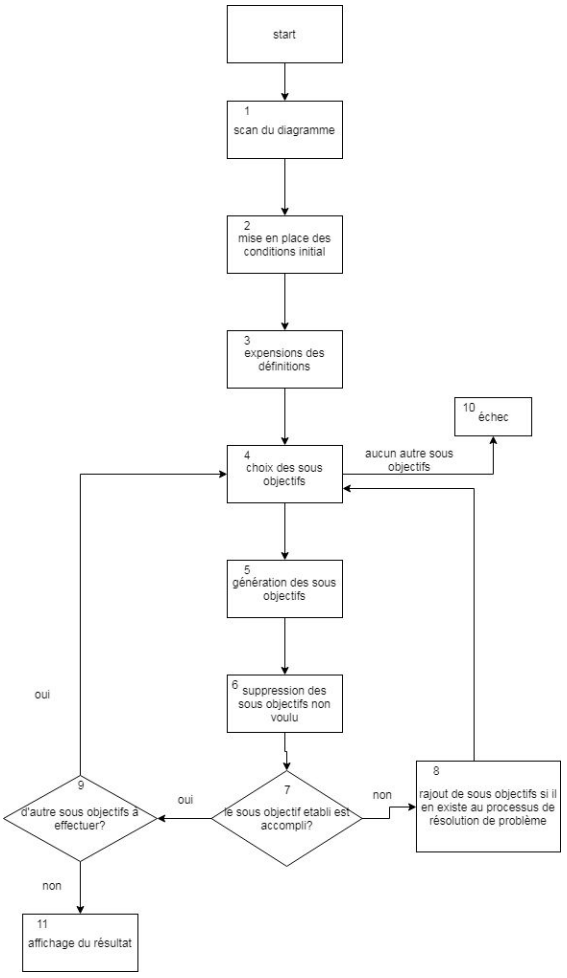
Le **G.T.P** fonctionne sur trois ordinateurs IBM 704, ou chacun aura un rôle clairement défini. Selon H.Gelernter: "*Le G.T.P est en réalité un état de configuration particulier de l'IBM 704 plutôt que un long et complexe programme écrit pour l'ordinateur*" (*Realization of a geometry-theorem proving machine*,1959).

Les trois rôles sont donc:

- **L'ordinateur de syntaxe:**
  Ce charge de faire les manipulation du système formel.

- **l'ordinateur de diagramme:**
  Il possède une représentation des théorèmes qui seront établi avec une série de routines, permettant d'obtenir un diagramme des théorèmes claire.

- **l'ordinateur heuristique:**
  Sa principale fonction est de comparer les résultats généré par l'ordinateur de syntaxe avec leur interprétation dans le diagramme de l'ordinateur de diagramme et rejeter celle qui ne correspond pas. Il effectue aussi l'organisation du processus de recherche de preuve.
  Le processus de l'ordinateur heuristique est le suivant:



(fig.1:diagramme simplifié du processus du G.T.P)

1. le diagramme est scanné pour construire trois listes. Une pour les segments,une pour les angles et une pour les triangles de la figure géométrique pour laquelle on cherche à appliquer le théorème. Chaque élément de chaque liste est accompagné d'une sous liste décrivant les caractéristique de l'élément.

2. La configuration initiale du système est mise en place, avec les prémices de la liste des formules déjà établie, et la conclusion du processus (plus aucun objectif ou sous objectifs)

3. définitions des prédicats non primitifs de chaque prémices sont ajouter à la liste des formules établie.

4. un sous objectif est défini et choisi.

5. les axioms et théorèmes appropriés sont sélectionnés, permettant de définir une suite de nouveaux sous objectifs sont défini.

6. les sous objectifs qui ne sont pas valide sont rejetés.

7. Si l'un des sous objectifs établi est valide, on passe à l'étape 9, sinon, on passe à l'étape 8.

8. Si il est possible, on rajoute des sous objectifs non redondant.

9. Si le sous objectif est valide, il est ajouter à la liste des formules établi. Si il n'y pas aucun autre sous objectifs à accomplir, on passe à l'étape 11.

10. Si les sous objectifs sont impossible à accomplir, le processus est en échec.

11. affichage du résultat.

Finalement, l'une des dernières avancé durant cette période pris la forme de **Shakey**, Robot construit par l'institut de recherche Stanford entre 1966 et 1972. Conçu avec comme objectif de pouvoir avoir une reflection sur ses propres actions et analyser les ordres données pour les découper en sous objectifs.

Créer avec le langage **LISP**, il possédait comme programme le **S.T.R.I.P.S** ("*stanford Research institute problem solver"*), et est l'intégration du raisonnement formel pour une activité physique.

d) ...et son premier hiver

Malgré les avancés entre 1957 et 1972, le domaine de l'IA à commencé à rencontrer de sérieuses difficultés en fin 1973, début 1974:

- **les capacités des ordinateurs de l'époque:**

A cette période, nous rentrons dans la **quatrième génération d'ordinateurs**. Les premiers microprocesseurs venait d'apparaître (les trois premiers sont apparu en 1971: TMS 1000 de Texas Instruments, Intel 4004 de Intel et AL1, de Four-Phase Systems).
Assez limité dans le ressources en terme de vitesse, ils ne permettaient pas de pouvoir construire des systèmes d'intelligence artificielle réellement utile: a titre d'exemple, le microprocesseur Intel 8080, apparu le premier avril 1974, avait une vitesse d'horloge de 2 Mhz et 0,64 millions d'instructions à la secondes (a titre d'exemple, un processeur intel G3220,apparu en septembre 2013, à une fréquence de 3 Ghz).

Les développements étaient alors fait sur des mainframes, comme **l'IBM 7094**. (" *IBM's Early Computers*", Harles J. Bashe,Lyle R. Johnson,John H. Palmer,Emerson W. Pugh, 1986).

Le premier **micro ordinateur**, ancêtre de l'ordinateur de maisons, l**'Altair 8800**, à été conçu en 1974 pour apparaître début 1975 dans les domiciles. Fonctionnant sous Altair DOS, il possédait un processeur Intel 8080, 256 bytes de mémoire.

Les capacités physiques des machines étant limités,de nombreux problèmes qui causèrent l'hiver de l'IA viennent de là: les travaux de Ross Quillian, par exemple, sur le travail du langage naturel ne pouvait fonctionner que sur un dictionnaire de vingt mots. ("*AI: The Tumultuous Search for Artificial Intelligence"*,1993 par Daniel Crevier). Bien que le **G.T.P** contourne le soucis en utilisant trois ordinateurs, chacun ayant son rôle, le résultat était moins conséquent par rapport à la quantité de ressources déployée.

- **gestion de l'information:**

Selon Pamela McCorduck dans "*machines Who Think*",2004, l'un des nombreux soucis rencontrés était la quantité massive d'informations que un système d'IA pour la **reconnaissance d'images** ou l**e langage naturel** à besoin de connaître sur le monde en général (des **connaissances du sens commun**). Et, en 1974, personne ne pouvait construire une base de données assez large pour contenir toutes les informations nécessaires (problèmes de limitation matériel, et la notion de base de données relationnel existait en théorie, grâce au travail de Edgar Codd, dans son papier "*A relational Model of Data for Large Shared Data Banks*", 1970).

- **Critiques:**

L'une des premières critiques est le **paradoxe de Moravec**, qui à été cité plus haut, sur le raisonnement formel.

Le **perceptron**, le type de **réseaux neuronaux virtuels** le plus utilisés à ce moment, créer par Frank Rosenblatt au laboratoire aéronautique de Cornell, a été le sujet du livre "*Perceptrons*", 1969, écrit par M.Minsky et Seymour Papert.
Celui ci mettait en lumière les sévères limitations des **perceptrons**, et provoqua une perte d'intérêt violente sur cette technologie: peu ou plus de recherche n'a été effectué sur le domaine des réseaux neuronaux pendant 10 ans. ("*AI: The Tumultuous Search for Artificial Intelligence*",1993, Daniel Crevier).

Le nombres très importants d'étapes pour prouver le plus simple des théorèmes ou résoudre un problème de logique de **G.T.P** et **G.P.S** ont été aussi mis en avant.

Finalement,Hubert Dreyfus, Professeur de philosophie à l'université de californie, a émis quelque critiques concernant le raisonnement formel.

Dans son livre "*what computers can't do*",1972, il identifie les quatres hypothèses qui ont été effectué par les chercheurs en I.A, ainsi que le problème d'intuition.

➢ *Hypothèse biologique*

Au début du domaine de la neurologie, nous sommes arrivés à la réalisation que les neurones sont fonctione avec des impulsions "*tout ou rien*". Plusieurs chercheurs, comme Walter Pitts et Warren McCulloch, on assumée que le fonctionnement d'un neurone marche de la même manière qu'une porte booléenne, et que un circuit électronique pourrait fonctionner de la même manière. Ce qui a suivi fut le **PSSH**.

H.Dreyfus nota que l'action et le timing des impulsions est plus proche d'un composant analogue que d'un système digital.

➢ *Hypothèse Psychologique*

Toujours sur l'idée du **PSSH**, les chercheurs ont assumé que l'esprit peut être vu comme un système fonctionnant avec des informations et des règles formel.

Selon lui, tant bien même que nous utilisons un système semblable, nous le combinons avec un bagage inconscient de **connaissance de sens commun**. Sans ce bagage, les symboles que notre

pensée manipule n'a plus aucun sens. Du point de vue de Dreyfus, le sens commun n'est pas implémenté dans l'esprit de manière explicite et avec des explications.

➢ *Hypothèse Épistémologique (l'étude des connaissances)*

La critique, ici, est plus d'ordre philosophique et est issu d'une différence de point de vue entre J.McCarthy, qui pense qu'un dispositif manipulant et traitant des symboles peut représenter toute les connaissances, et Dreyfus, qui pense qu'il n'y pas de justification concernant cette hypothèse, si l'on considère que la connaissance n'est pas symbolique.

➢ *hypothèse Ontologique* (domaine philosophique qui s'interroge sur le sens du mot "être")

Toujours dans le domaine de la philosophie, les chercheurs assume souvent que tout ce qui existe peut être défini et expliqué par des symboles et théories scientifiques, par une forme de logique,de langage ou de mathématiques.
Il souligne que cette hypothèse est fausse, nous pouvons alors nous demander ce que nous savons, et en quoi une I.A peut nous aider (si tout n'est pas symboles ou mathématiques, une I.A ne pourra manipuler ce genre de connaissances comme elle a été construit.)

➢ *L'intuition, ou le problème du "savoir quelque chose et savoir comment"*

Dans "*Mind Over Machine*",1986, Dreyfus analyse la différence entre la connaissance et la manière de l'exploiter d'un être humain et celle d'un programme, qui est censé imiter l'humain.
Il présente alors deux principes: "*Knowing-that*" (**savoir quelque chose**) et *"Knowing-How*" **(savoir comment**).

"*Knowing-that*" est notre capacité à savoir prendre du recul face à un problème qui nécessite de la réflection. A ce moment, nous manipulons des symboles en utilisant notre logique. C'est, à ces yeux, ce que les programmes de A.Newell et H.Simon, par exemple, on réussi à imiter.

"*Knowing-How*" est notre manière de réagir et d'agir quand nous agissons normalement, voir par réflexe.
Nous agissons alors sans utiliser une forme consciente de raisonnement par symbole,et notre processus de réflexion atteint directement la réponse appropriée. Quand nous prenons la route du travail que nous arpentons depuis une année, par exemple. Nous effectuons le trajet par instinct. Le "*Knowing-How*" est notre intuition suffisamment exercée si bien que, face à une situation, une réflexion nous n'est même plus nécessaire.

Selon Dreyfus, notre sens de la situation (qui est un ensemble de connaissance inconsciente) n'est pas stocké dans cerveau de manière symbolique. Il conclut que les I.A tel que présent dans les années 70 et 80, ne peuvent capturer le "*Knowing-How*".

- **Complexité en temps:**

Richard Karp, s'appuyant sur le théorème de Stephan Cook, à conçu l'article "*Reducibility Among Combinatorial Problem*s" en 1972. Ce dernier nous présente vingt-un types de problèmes qui ne peuvent être résolu dans un **temps qui était exponentiel par rapport à la tailles des données d'entrées**. Trouver donc une solution optimal à ces problèmes demandait un temps de calcul immense, sauf si le problème est en lui même trivial (si la quantité de données en entrée est minime). Les solutions utilisé dans les systèmes d'intelligence artificielle, alors limité technologiquement, ne

pouvaient être utiliser pour résoudre l'un de vingt-un types de problèmes, sauf si celui qui est présenté n'utilise qu'une petite quantité de données.

Ces différentes difficultés et critiques ont causé une avancée minime dans l'intelligence artificielle. Les différentes organisations finançant la recherche, comme le DARPA ou IBM, on fini par couper les fond.

Le document "*Developments in Artificial Intelligence*", de l'académie national des sciences, médecine et ingénierie (NRC) démontre par exemple une dépense de vingt millions de dollars avant de constater que les avancements n'étaient pas suffisant pour justifier des dépenses supplémentaires.

Cette perte d'intérêt des différentes organisations envers la recherche d'intelligence artificielle provoqua un hiver dans le domaine de l'intelligence artificielle.

H.Moravec blâma cette crise dans les espérances trop hautes de ces collègues (on peut reprendre l'exemple de la prédiction de A.Newell et H.Simon). ("*AI: The Tumultuous Search for Artificial Intelligence*",1993)

e) L'IA devient une industrie

Malgré la frustration dû à un manque d'avancé significatif début 1974,un projet datant de 1965, l**es systèmes experts**, permis au domaine de l'intelligence artificielle de revenir au devant de la scène.

Issu de Edward Feigenbaum, responsable du projet "Stanford Heuristic Programming Project", ce projet cherchait à identifier les domaines d'études où l'expertise est à la fois capitale et complexe.

E.Feigenbaum c'est basé sur l'idée que **la manière de fonctionner des systèmes intelligents se base plus sur les connaissances qu'elle possède plutôt que sur un processus formel** (*Building Expert Systems,1983)*.
Les différences entre les systèmes expert et les systèmes d'IA précédemment cité sont multiples:

- **Leur objectifs:**

Là où les précédentes IA avaient pour but d'accumuler un certains nombre de connaissances afin de pouvoir résoudre des problèmes de tous types et assez générals, les systèmes experts cherche à émuler les capacités à prendre des décisions d'un expert humain dans un domaines.

- **le langage de développement:**

Les systèmes d'IA générales ont été développer en Lisp, là ou les systèmes experts ont été créés surtout en Prolog (langage conçu par le groupe dirigé par Alain Colmerauer, à l'université d'Aix-Marseille).

- **le fonctionnement:**

le développement des IA générales étaient faite au travers d'un code structuré procéduralement, là où les systèmes experts se base sur des règles de condition types "If-Then". De plus ces derniers ne possède pas de systèmes leur permettant d'apprendre de manière autonome depuis des données extérieur, ce qui peut soulever le questionnement de savoir si un système expert est

réellement une intelligence artificielle (“*Siri, Siri, in my hand: Who’s the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence”,*2018 de Andreas Kaplan et Michael Haenlein*).*les systèmes experts sont divisés en deux parties:

➢ *La base de connaissances*

Il s’agit d’une base de données représentants les faits et règles auquel sont régi le domaine du système experts.

➢ *le moteur d’inférence*

Ce moteur va appliquer les règles sur les connaissances déjà présente dans la base de connaissances pour déduire de nouveaux faits.

En 1980 est donc apparu le premier succès commercial des systèmes experts, au travers de **R1**, ou **XCON**. Celui ci à été crée suite à une demande du “Digitial Equipment Corporation” (DEC) et conçu par John P. McDermott, de l'université de Carnegie-Mellon.

R1 à été conçu dans le but d’aider à paramétrer les commandes pour de nouveaux systèmes d’ordinateurs et à permis à DEC d’économiser entre 25 et 30 millions de dollars par ans.

Cela causa un intérêt tel que entre 1980 et 1988, DEC à créer une branche concentré sur l’IA qui avait déployé environ 40 système experts (*Artificial-Intelligence-A Modern Approch,3rd Edition,2016*), DuPont (conglomérat d’entreprise de chimie et métaux lourd) en possédait une centaine et de nombreuses entreprises comme Symbolics (constructeur de matériels informatique et industriel) ou Intellicorp (développeur de logiciel) ont créé une industrie autour des systèmes experts (développement du programmes, ou création de matériel optimisé).

En parallèle du développement de l'industrie de systèmes experts au Etats-Unis et en Europe, Le Japon lança le projet *“Cinquième génération”*, un plan débloquant des fonds de 850 dollars pour la recherche d’intelligence artificielle.L’objectif est,à nouveau, la création de programmes et machines se rapprochant d’une intelligence biologique.

Cela provoque une réponse du reste du monde.Les états unis créèrent le “*Microelectronics and computer technology Corporation*”, ou MMC, afin d’ouvrir des fond pour les projets dans l’intelligence artificielle et le royaume-unis lança le **projet Alvey**, avec comme fond 350 millions de dollars. la DARPA réagit elle aussi en investissant dans le “S*trategic Computing Initiative*”.

f) les réseaux de neurones se réinvente

Cette réouverture de fond pour les recherches dans le domaine de l'intelligence artificielle a permis d’aborder la technologie des réseaux de neurones sous de nouveaux angles.

En 1982,le physicien **John Joseph Hopfield** réussi à créer une nouvelle forme de réseau neuronaux, capable d’apprendre et traiter les données de manière différentes des précédents réseaux de neurones.

En parallèle, **Geoffrey Hinton** et **David Rumelhart**, tous deux professeur à l’université de Carnegie Mellon, remis en avant une méthode d’apprentissage pour entraîner les réseaux de neurones, la

rétropropagation du gradient, méthode encore utilisé dans le cadre d'apprentissage supervisé d'un réseau de neurones.

Cela donna un regain d'intérêt pour le domaine des réseaux de neurones artificielles, qui fut finalement un élément très largement utilisé en 1986 pour les programmes comme la reconnaissance de voix ou d'images.

g) L'intelligence artificiel adopte une approche scientifique

Paul R.Cohen, professeur à l'université de l'Arizona, publia en 1995 un article nommé : "*Empirical Methods for Artificial Intelligence*", présentant l'adoption d'une méthodologie plus scientifique dans la recherche de l'IA, fin 1986, début 1987.

Plutôt que se basés sur des intuitions pour créer de nouvelles théories et mettre en place des systèmes d'IA qui, bien que fonctionnel, sont plus des exemples conçu pour résoudre des problèmes peu concret, il a été adopté une nouvelle manière d'aborder les recherches.
Une hypothèse, pour être désormais accepté, doit être accompagné de **théorèmes rigoureux**, et à du être expérimenter sur **problèmes et applications réel**, afin d'apporter des **preuves solides.**

Cela à permis de plus facilement organiser les recherches et d'effectuer des avancés dans un certains nombres d'applications et sous-domaines de l'IA, comme la r**econnaissance de voix** et les r**éseaux de neurones**. La reconnaissance de voix a adopté une approche basé sur les **modèles cachés de Markov**, qui utilise des théories mathématiques afin que des chercheurs puisse se commencer leur recherche sur des résultats ayant été soumis à plusieurs années d'expérimentations et de tests rigoureux. Cette approche a aussi été accompagné de long processus d'entraînements avec une grande masse de données de langage et de parole afin d'assurer une performance certaines.
Les **réseaux de neurones artificielles** vont désormais de paire avec le domaine des statistiques afin de s'assurer d'une méthodologie et de développement sûr pour permettre aux chercheurs de pouvoir se concentrer sur des principes mathématiques et effectuer des tests et entraînements sur des problèmes pratiques.

Judea Pearl, Membre de l'université de californie, sorti le livre "*Probabilistic Reasoning in Intelligent Systems*" en 1988, ouvrant le domaine de la **probabilité** et à la **théorie de décision** au domaine de l'intelligence artificielle et créa la notion de r**éseau bayésien**, permettant de représenter de manière efficace et avec raisonnement, des **connaissances incertaines**.
Cette approche permis de résoudre de nombreux problèmes concernant les probabilités dans les raisonnements des précédents systèmes d'intelligence artificielle.
J.Pearl, Eric Horvitz et David Heckerman, continuant sur la lignée d'une approche plus organisée et scientifique, proposèrent alors l'idée de concentrer les recherches de l'IA sur des **systèmes normatifs**, fonctionnant en accord avec les lois de la **théorie de décision** plutôt que chercher à imiter le processus de réflexion d'un être humain. (*Horvitz and Heckerman*, 1986)

h) les vastes étendues de données

Pendant ces cinquantes premières années de recherches dans l'intelligence artificielle,les principales études se sont focalisés sur les algorithmes utilisés, et bien que ces études ont permis de faire avancer le domaine afin de permettre la création de technologies et d'algorithme solides, l'un des nombreux problèmes rencontrés à la base de l'intelligence artificielle n'avait pas encore été la cible de l'intérêt des chercheurs.

En 1995, l'intelligence artificielle est désormais équipé d'une méthodologie rigoureuse et puissant sa manière de faire dans les domaines scientifiques, et l'avancé de l'informatique permets désormais d'avoir des ordinateurs possédant des ressources suffisantes pour permettre le développement d'un système d'IA efficace et pouvant se consacrer sur des problèmes concret (Internet était née et d'accès public, les postes fixes sont devenu suffisamment abordable pour que une famille puisse en posséder un, et Windows 95 venait d'être sorti).

Reste alors le problèmes des données et informations servant de base pour l'entraînement et l'apprentissage des programmes.
Le travail de David Yarowsky, professeur de l'université de Hopkins, "*Unsupervised word sense disambiguation rivaling supervised method*s", 1995, fut pivot pour la prise de conscience de cette difficulté.Dans le cadre d'un système d'IA se concentrant sur l'utilisation de mots (reconnaissance vocale ou de texte, par exemple), Le mot "*plant*", en anglais, dans une phrase, **signifie t il une plante ou une usine**? Les précédents essais se reposaient sur des exemples où les mots étaient **étiquetés à la main** afin que le programme sache quel sens utilisés, associé à des **algorithmes d'apprentissage artificiel**.

D.Yarowsky montre dans son document que cette tâche peut théoriquement être effectué avec une **précision d'environ 96%** (le taux d'erreur du programme sur l'utilisation correct du terme est donc de 4%). A la place d'étiqueter des exemples, si nous possédons un très grand corpus de textes d'entraînement, nous pouvons simplement **étiqueter des exemples** du corpus et lancer un apprentissage de motifs ou paternes aidant à étiqueter de nouveaux exemples. Cela sous entend cependant que nous possédons une vaste masse de données pouvant nous servir de base à l'entraînement.

Comme exemple, on peut citer les travaux de James Hays et Alexei A.Efros, dans leur papier "*Scene Completion Using Millions of Photographs*". Ils présentent un algorithme qui, si on souhaite combler des trous dans une photographie numérique, va rechercher le motif dont nous avons besoin dans une collection de photos.
Cette algorithme aura une mauvaise performance quand il utilise une collection de dix milles photos. Cependant, quand le catalogue d'images monte à deux millions de photos, les performances de l'algorithme augmente de manière significative.

2. IA forte et IA faible

Le domaine de l'intelligence artificielle à donc comme objectif général de créer une IA qui est capable d'imiter une intelligence biologique. Cependant, comme nous avons pu voir dans son histoire, chacune des tentatives pour atteindre ces objectifs ont échoué à des niveaux différents, et les chercheurs sont peu à peu passer à la création de système plus spécialisé, cherchant à effectué une seule tâche.

Cette dernière reste toujours du domaine de l'intelligence artificielle. Bien que spécialisé dans une tâche, elle doit malgré tout passer par une plus ou moins longue séance d'apprentissage et d'entraînement et est capable de sortir des résultats qui sont en dehors de leur programmation. Simplement, elles sont entrainés pour répondre à une tâche spécifique, avec le type de jeu de données correspondant.Jouer au échec, comme **DeepBlue**, ou jouer une faction spécifique dans le jeu Starcraft,effectué par **AlphaStar**.
Leur limitation se trouve justement dans le jeu de données et leur temps d'apprentissage. Si, par exemple,on souhaite que **DeepBlue** joue désormais au jeu de dames, il faudra lui fournir un jeu de données correspondant et recommencer le processus d'apprentissage et d'entraînement. Nous sommes donc loin d'une forme d'intelligence générale.
Ce type d'IA sont nommées les **IA faibles**, en contraste aux **IA fortes** (celle capable d'imiter l'intelligence biologique).

Ce mémoire va se focaliser principalement sur l'IA faible, dû au fait que elle celle actuellement utilisés dans la totalité des applications utilisant de l'intelligence artificielle, et que, comme il sera vu par la suite, la seule qu'il à été possible de créer avec succès.
Cependant, afin de faire un état de l'art complet, et de bien comprendre ce que n'est pas l'intelligence artificielle de nos jours, les prochaines pages vont décrire un peu plus en détails ce qu'est l'IA forte.

a) l'IA forte

L'IA forte, ou **l'intelligence artificielle générale** ("artificial general intelligence",AGI), est l'objectif principal des recherches dans ce domaine, et elle est sujet à de nombreuses recherches. Des entreprises comme DeepMind,OpenAI ou GoodAI concentre de nombreuses recherches dessus.(*A Survey of Artificial General Intelligence Projects for Ethics, Risk, and Policy*,Seth Baum,2017)

Elle est, par ailleurs, la forme d'IA qui est la plus représentée dans la fiction (skynet, de la licence "*terminator*" ou le puppet master et les tachikomas dans la licence "*ghost in the shell*".)

Cependant, définir ce qu'on pourrait qualifier d'AGI est encore aujourd'hui sujet à débat, malgré les nombreuses recherches consacré à son sujet et sa représentation dans de nombreuses oeuvres de fiction.

Certain chercheurs parle d'IA forte quand il s'agit de la capacité d'un programme ou d'une machine d'effectuer toute forme de tâches nécessitant les capacités intellectuels d'un être humain adultes. Ray Kurzweil,créateur de l'entreprise "*Kurzweil Applied Intelligence*" et "*Kurzweil Educational Systems*", deux entreprises cherchant à développer des systèmes de **reconnaissances de voix** et actuellement chef de projet à Google pour tout ce qui concerne le machine learning, décrit dans "*The*

singularity is Near",2005 l'**AGI** comme "*une machine possédant toutes les capacités d'une intelligence humaine*".

D'autre considère que une IA forte posséderai une conscience et une capacité de pensée, de la même manière qu'un être humain. S.Russell et P.Norvig la défini ainsi: "*L'affirmation selon laquelle les machines pourraient éventuellement agir intelligemment (ou peut-être mieux, agir comme si elles étaient intelligentes) est appelée l'hypothèse de l'IA faible par les philosophes, et l'affirmation selon laquelle les machines qui le font réfléchissent réellement (par opposition à la pensée simulée) est appelée l'hypothèse de l'IA forte*".
Ce point de vue peut soulevé la question de ce qu'est ce que on nomme "*conscience*" et de la possibilité ou non de la simuler pour une machine (ce qui donnera suite à de nombreuses recherches pour finalement créer le domaine d'étude de la **conscience artificielle**.)

Cependant, la majorité des chercheurs sont au moins d'accord sur un ensemble de prérequis que une IA devra avoir pour être considéré comme potentiellement une AGI.("*Artificial Intelligence:Structures and Strategies for Complex Problem Solving*",George Luger,William Stubblefield,2004):

- **Etre capable de réfléchir:**
  Résoudre des puzzles, faire preuve de stratégie et de prendre des décisions avec des données incomplètes ou incertaines.

- **Posséder des connaissances:**
  En plus d'être capable d'utiliser les connaissances du sens commun (de faire preuve de bon sens, en d'autres termes), mais être aussi capable d'organiser et utiliser les connaissances qu'elle a acquise, pour pouvoir apprendre plus rapidement de nouveaux sujets en effectuant du recoupement d'informations(Si elle a appris à jouer au jeux d'échec, elle devra utiliser ces connaissances pour comprendre et maîtriser plus rapidement le jeu de shogi, qui se rapproche des échecs)

- **Planifier:**
  Face à un problème, elle devra être capable de découper le problème en tâche et sous tâches afin de planifier ces actions.

- **Apprendre:**
  L'apprentissage reste le coeur de l'IA.

- **Communication en langage "naturel":**
  Savoir utiliser une langue, comme l'anglais, pour pouvoir communiquer et engager une discussion avec un être humain.

- **Utiliser l'ensemble de ces compétences pour atteindre un but:**
  A l'inverse d'une IA faible, elle doit être capable d'utiliser l'ensemble des compétences précédemment cité afin d'atteindre un objectif. Un exemple simple serait de préparer un café pour quelqu'un:

➢ *Possession de connaissances*

Savoir ce que c'est, qu'un café, du sucre, un verre ou une tasse, et être capable de les reconnaître. Avoir aussi une idée, même incomplète, des différentes tâches nécessaires pour le faire.

➢ *Capable de réfléchir*

Réussir à trouver les ustensiles et ingrédients nécessaires pour le faire. Adapter sa planification incomplète de tâches par rapport à ce que elle à trouver. (J'ai un verre, du sucre,une cuillère, du café en grain et une bouilloire. Je dois d'abord faire chauffer l'eau, connaitre la quantité de café et de sucre à mettre, versé l'eau chaude et mélanger le tout avec la cuillère)

➢ *Apprendre*

Si elle ne sais pas comment fonctionne les ustensiles, il faut qu'elle apprenne à les utiliser (Je sais qu'il s'agit d'une bouilloire, mais comment fonctionne t elle? dois je appuyer sur un bouton? Celui du dessus ou du dessous?)

➢ *Communication en langage "naturel"*

Demander si la personne veut du sucre, deux ou trois cuillères de café.

afin de permettre de déterminer si l'IA que l'on souhaite tester possède les prérequis afin d'être qualifié d'AGI, ils à été créer de multiples tests au fur à mesure du temps. Les plus connu sont:

- **Le test de turing(**Allan Turing**):**
  Une machine et un humain discute avec une deuxième personne, qui ne sais pas lequels des deux est la machine et l'être humain.
  Il doit donc évaluer qui est qui au travers de la discussion, et l'IA doit réussir à le tromper.

- **le test du café(**Steve Wozniak**):**
  Il s'agit du test que il a été décrit plus haut. Une machine doit réussir à faire un café.

- **le test du passage de diplôme (**Ben Goertzel**):**
  L'IA suis les mêmes cours que des étudiants, et doit réussir à obtenir son diplôme.

- **le test du miroir(**Tanvir Zawad**):**
  Pour ce test, l'IA doit réussir à faire la différence entre un objet et son reflet.

Finalement, il n'existe pas, à ce jour, d'IA que l'on peut qualifié d'AGI. L'un des soucis majeur de sa réalisation est la difficulté qu'ont les chercheurs à définir ce qu'est une AGI.
Ensuite, la notion de IA forte est souvent associé à l'utilisation d'une multitude de technologies et d'applications qui sont habituellement utilisés de manière séparés par des IA faible, plus spécialisés. Si on reprend le test du café, l'AGI devra donc comporter l'utilisation d'un corps robotique lui permettant de manipuler les objets (nous parlons alors du domaine de l'IA se nommant la cognition incarnée), la capacité d'utiliser une reconnaissance d'images, ainsi que la compréhension et l'utilisation d'un langage naturel, la capacité d'apprendre de nouvelles notions face à un imprévu et de pouvoir planifier un ensemble d'étapes à partir de données incomplète.
Ce problème se nomme le **IA-Complete** (ou **AI-hard**). ("*Turing Test as a Defining Feature of AI-Completeness*",Roman V. Yampolskiy,2012).

b) l'IA faible

L'IA faible, aussi appelée **IA restreinte** ("*Narrow AI*") est une forme d'intelligence artificielle concentré sur une seule tâche, et est actuellement celle qui est utilisée aujourd'hui.

Il s'agit de la combinaison de l'utilisation de technologies comme les **réseaux de neurones**,**l'apprentissage profond** et **l'apprentissage machine** (qui sont les trois technologies actuellement les plus utilisés dans le cadre de l'intelligence artificielle) afin de permettre à un programme d'être entraîné et d'apprendre à partir d'un jeu de données afin d'accomplir une tâche spécifique.

Comme cité plus haut, **l'IA faible** sera le sujet principal de l'état de l'art de l'intelligence artificielle de ce mémoire. La suite va donc décrire plus en détails ces objectifs, les problèmes rencontrés ainsi que son fonctionnement.

3. Les tâches et domaines de l'IA

Si les **objectifs primaires** de l'intelligence artificielle est de créer une AGI,permettre de simplifier certaines tâches complexes pour l'être humain, ou laisser une IA en effectuer certaines pour obtenir un gain d'efficacité, définir plus en détails les objectifs des différentes recherches dans ce domaines va en réalité **dépendre de la nature de l'entreprise** qui les effectue et le **domaine sur lequel on souhaite utiliser l'IA**.

Si nous prenons par exemple les entreprises DarkTrace et Boston Dynamics, deux entreprises effectuant des recherches dans l'intelligence artificielle, les objectifs sont différents, du au domaine dans lequel est utilisé l'IA et la nature de l'entreprise.

Darktrace est une société de sécurité informatique utilisant activement l'IA pour améliorer leur système de sécurité et leur temps de réponse. Leur recherche dans ce domaine est surtout dans l'objectif de traiter plus rapidement et facilement des données afin de pouvoir réagir efficacement à de potentiels menaces.

Boston Dynamics est une entreprise spécialisée dans la conception en robotique. L'utilisation de l'intelligence artificielle est principalement pour permettre à leur création de pouvoir s'adapter à leur environnement.

Dans les deux cas, l'utilisation de **réseaux de neurones**, associé à de **l'apprentissage profond** est présent. Cependant, là où Boston Dynamics effectue leur recherche sur un système d'IA fonctionnant avec de la **cognition incarnée** afin de permettre à un robot de pouvoir se déplacer correctement dans une multitude d'environnement, incorporant un ensemble de senseur, Darktrace focalise leur études sur du traitement de quantité massive de données (du **big data**), afin que leur système puisse répondre efficacement en cas de menaces.

Il est donc plus aisé de définir les objectifs des recherches d'IA en abordant les différents champs d'études. . Bien que ils peuvent se regroupés afin de résoudre un problème ou effectuer une tâche spécifique (si nous reprenons le cas de boston dynamics, on retrouve la vision numérique associé au

mouvement pour permettre à un robot d'ouvrir une porte, par exemple),nous pouvons les diviser en trois domaines de sous-tâches.

a) sous-tâches mondaines

Il va s'agir de l'ensemble d'actions que une personne fait naturellement ou qui est de **l'ordre du normal**. Paradoxalement (et selon le **paradoxe de moravec**) , il s'agit des sous-tâches que un système d'IA à le plus de difficulté à accomplir, alors ques les sous-tâches formelles et expertes, qui sont les plus complexes à effectuer pour un être humain, sont les plus simples à effectuer pour le système.

L'objectif de ces recherches est de lui permettre de gérer des actions et tâches qu'un être humain peut faire de lui même. On retrouve donc:

- **Perception**

Ils s'agit des tâches touchant la perception du monde que peut avoir un ordinateur, tel que la vue ou le son. Nous retrouvons donc la **reconnaissance de la parole** et celle de **la voix**, ainsi que la **vision numérique.**

La reconnaissance de la parole et celle de la voix sont deux technologies très lié mais ayant des objectifs différents.
La reconnaissance de la parole va chercher à comprendre ce qui est dit, et son entraînement nécessite que la machine puisse traduire le son produit en fréquence, puis en binaire (pour simplifier le processus de traitement) avant que les données passe par réseau de neurones pour permettre d'être comparé à sa base de données contenant les mots utilisés afin d'en connaître la définition la plus probable suivant la phrase complète, en utilisant du traitement de langage naturel. (*Connectionist Temporal Classification: Labelling Unsegmented Sequence Data with Recurrent Neural Networks,*2012,Alex Graves,Santiago Fernandez,Faustino Gomez,Jurgen Schmidhuber). Un exemple d'utilisation de cette technologie sont les **assistants vocales** (google home ou amazon echo).

La reconnaissance de la voix à pour objectif de pouvoir associé une voix à une personne. Si elle aussi analyse la fréquence du son de la voix ainsi que ces paternes, elle nécessite d'être entraîné avec un seul interlocuteur afin qu'elle puisse nourrir sa base de données pour pouvoir comparer la voix qu'elle capte et les données qu'elle possède. Cela permet d'identifier le locuteur.

C'est deux technologies se base donc énormément sur la **linguistique**,le **big data** et le **génie électrique.**

L'analyse et la compréhension des images fonctionne avec l**a vision numérique**.Par rapport à la tâche que l'on cherche a effectuer au travers de la vision numérique (reconnaissance de visage, traque de mouvement ou restauration d'image,lecture de texte manuscrit ou de code comme un QR code), elle va chercher à extraire les données intéressantes d'images ou de vidéos afin de pouvoir les analyser et traiter.
Si il est possible d'effectuer de la vision numérique sans avoir besoin d'apprentissage machine et de réseaux de neurones, dans le cadre d'un système ayant besoin d'informations sur l'environnement qui l'entoure ou issu de multiple flux vidéos, la vision est capitale.

Par exemple, les robots devant se déplacer dans un environnement de manière autonome auront besoin de senseurs visuel, et donc de **vision numérique**.
Un autre exemple hypothétique de l'utilisation de la **vision numérique** serait l'utilisation de multiples caméras fonctionnant sur un système peu ou pas supervisé ayant comme but d'effectuer une reconnaissance faciale et de mouvement pour attribuer des points aux personnes reconnu selon leur actions.

- **Langage naturel**

L'une des grandes difficultés concernant **l'interface homme-machine** est le langage. Si un ordinateur peut gérer avec facilité des données structurés et standardisés, le **langage humain** suit des **règles abstraites**, n'étant pas structurés. C'est ce qu'on appelle **le langage naturel**. Si nous arrivons à comprendre le sens d'une phrase, un système d'IA, malgré sa capacité à utiliser la reconnaissance de la parole, ne pourra pas comprendre le sens de la phrase, tout particulièrement quand un mot, selon la phrase, peut avoir une **définition différente**.

le traitement automatique du langage naturel à donc été créé pour permettre un programme ou une application de comprendre le langage naturel. Ce traitement regroupe plusieurs axes de recherches, comme **l'analyse syntaxique**,ou **la sémantique**, afin qu'un programme puisse comprendre ce qu'il lit.

Avec ceci, il existe aussi le domaine de **génération de langage naturel**, qui va chercher, à partir du langage naturel qu'il a appris à comprendre, à **générer des textes compréhensible par l'homme** et qui ont un sens.

Un exemple d'utilisation de **traitement automatique du langage naturel** est l'application de traduction de Google ("*Google's Neural Machine Translation System: Bridging the Gap between Human and Machine Translation*",2018). La traduction fonctionne avec un système d'**apprentissage profond** et **réseau de neurones**, nommé "*Neural Machine Translation"*.

- **bon sens**

Le bon sens, ou **sens commun**, du point de vue des recherches dans l'intelligence artificielle peut se diviser en deux parties: **Posséder les connaissances** du sens commun (exemple: un oiseau vole) et effectuer un **raisonnement** avec ces connaissances (exemple: un oiseau vole, le pigeon vole, donc le pigeon est un oiseau). Il s'agit respectivement les **connaissances du sens commun** et le **raisonnement du sens commun**.

Les connaissances du sens commun sont donc un ensemble de données simple et considérer comme vrai. Cette ensemble de données peut être incomplet,mais va permettre au système de pouvoir effectuer un raisonnement basé sur de nouvelles données qu'il va récupérer,issu d'une situation commune, en les associant aux données déjà présente pour effectuer **une présomption.**

Il s'agit d'une des taches sur lequel les chercheurs en IA ont le plus de difficulté. Une grande partie des données du sens commun sont compréhensible de manière instinctive pour un être humain mais sont trop **abstraite** pour une machine.

- **Mouvement**

Dans le cadre de l'utilisation de système d'IA dans la robotique, **le mouvement** fait parti des tâches à effectuer. Le robot,équipé de senseur, doit pouvoir se d**éplacer de manière autonome**. Si une partie de cette tâche viens de la construction physique du robot, le programme doit pouvoir utiliser son "*corps*" physique afin d'atteindre l'objectif qui lui a été assigné, sans avoir les tâches à effectuer pour y arriver.

b) sous-tâches formelles

Il va s'agir de l'ensemble des tâches nécessitant une **logique** et de la **réflexion**, sans que cela soit nécessairement spécialisé dans un domaine spécifique.Souvent des problèmes et tâches assez générales, comme effectuer un calcul, ou jouer à un jeu de logique. A l'inverse des tâches mondaines, cela fait partie des tâches les plus "*simples*" pour une système d'IA à apprendre et effectué, dû à leur **nature formelles** et suivant des **règles explicite** et clair, comme les règles d'opération en mathématiques.

- **mathématiques et géométrie**

Le *Geometry Therorem Prover* est un exemple d'un système d'intelligence artificielle utilisé dans le cadre des **mathématiques et de la géométrie**. Il va s'agir d'utilisation d'un algorithme afin de tester, effectuer, prouver ou résoudre des **problèmes mathématiques ou géométrique**. Le but en soit n'est pas simplement de pouvoir résoudre des problèmes, mais de pouvoir offrir un support capable d'effectuer des tâches mathématiques pour des domaines plus experts.

- **jeu**

Les jeux, comme **les échecs ou le go,** sont des problèmes à la fois **simple** à saisir du fait de leur **nombres de règles** permettant de facilement déterminer comment ils fonctionnent à leur base et **complexe** du fait qu'il existe de **multiples possibilités de résolutions**,dépendant de nombreuses variables, rendant leur s**olutions complexes à obtenir**. Du point de vue du domaine de l'I.A, ce nombre de possibilités peut rendre **le temps de résolution** du problème très long, tout particulièrement si le jeu requiert d'avoir un opposant. Pour résoudre alors le problème, l'intelligence artificielle va devoir adopter les **différentes possibilités** à une variable sur lequel elle n'a aucun contrôle: un adversaire qui va lui aussi adopter sa stratégie.

Ce défi entraîne alors le programme à adopter un **plan à long terme**, ayant comme objectif de gagner la partie. Cette **planification** peut être modifié pour s'adapter à la stratégie adverse. Il faut alors que le programme redéfinissent son plan, les solutions disponibles et celle qui ne le sont plus.

En d'autre termes, les jeux vont **entraîner** un algorithme à apprendre **des règles prédéfinies**, évaluer les **possibilités de solutions** face au problème présenté,prendre une décision basé sur l**es informations** qui lui sont présentés et adopter une **planification** selon les nouvelles informations qu'elle reçoit suite à sa décision , tout en cherchant à prendre le moins de temps possible entre chaque décision.

l'autre partie de l'intérêt de faire jouer un programme d'intelligence artificielle à un jeu et **l'apprentissage de ce jeu**. **Connaître les règles d'un jeu** et **savoir y jouer** sont deux choses différentes, et un algorithme doit passer par une phase d'apprentissage. ("*Artificial Intelligence and Games*",2018,Georgios N.Yannakakis et Julian Togelius)

Par exemple,*AlphaGo*, intelligence artificielle créé par DeepMind capable de jouer au jeu de go.Il à commencé son apprentissage en imitant des mouvements effectués par des joueurs experts, puis à jour contre lui même durant quelques millions de parties pour s'améliorer, utilisant de l'apprentissage machine.

- **logique**

La notion de logique se dérive en multiples types. De la **logique classique**, qui fonctionne par un système de "vrai" et "faux", à la **logique booléenne**,qui utilise des mathématiques pour interpréter la logique(les AND,OR,NOR,NAND sont de la logique booléenne).

Celle qui intéresse la recherche dans l'intelligence artificielle est la **logique floue**, ou "*fuzzy logic*". Cette forme de logique est utilisé dans la vie de tous les jours, et représente la **variation** se situant entre les valeurs "1" (vrai) et "0" (faux), quand nous manipulons des **données imprécise**, incomplète ou non numérique.
Dans ce cas, l'intelligence artificielle s'entraîner à résoudre des problèmes en ayant des jeu de données floue, lui permettant par la suite de pouvoir gérer des informations incertaines et incomplètes, comme des informations issu des connaissances du sens commun. ("*Fuzzy Logic in Artificial Intelligence",*1997,Erich P. Klement,Wolfgang Slany).

c) tâches expertes

Comme le nom l'indique, il va s'agir des tâches qui vont être **spécialisé dans un domaine spécifique**, comme un diagnostic médical (le "*Beth Israel Deaconess Medical Center",* situé à l'école médicinal de harvard utilise un système d'IA afin de les aider à diagnostiquer des cancers du sein). Ils a donc autant de **tâches expertes** que il de **domaines** où l'IA est utilisés. Un exemple sont les **systèmes experts**, qui sont conçu pour effectuer ces tâches. Ils sont le résultat des précédentes sous-tâches ci-dessus concentrées autour d'un domaine spécifique.

B. Son fonctionnement

Comment fonctionne une intelligence artificielle? Ils existe de **multiples approches** et **techniques** afin de concevoir un programme possédant la capacité "*d'apprendre*".

De manière général, une IA va être découpé en **trois parties**.
La première est le **programme**. Il va s'agir du code qui va définir la ou les **tâches finales** à effectuer, comme l'interprétation d'un texte ou la reconnaissance d'image.
Ensuite viens le **modèle**. Il va s'agir du **cerveau du programme**. C'est une structure, un "*framework*", qui va être mis en place afin de permettre à un ou **plusieurs algorithmes d'apprendre**, retenir les **informations** et effectuer des **tâches**.
Finalement, il y a **l'algorithme**. Il va permettre au modèle **d'apprendre**. C'est à dire que c'est l'algorithme qui va effectuer la tâche de **traiter les données** afin de générer une suite de **règles générales** que le modèle va utiliser pour prendre une **décision** selon les nouvelles données qu'il reçoit, et modifier, ajouter ou supprimer des règles si besoin.

Les **données,**bien que n'appartenant pas à l'architecture même, sont une composante essentielle pour permettre au modèle de **s'entraîner et apprendre**.

Le domaine de l'apprentissage d'un programme à partir de données se nomme le *"machine learning"*, ou **apprentissage machine**,et constitue le coeur du domaine de l'IA.

Dans cette partie, je vais expliquer plus en détails ce qu'est l'a**pprentissage machine**, en présentant les **différents types d'algorithmes et modèles**. Puis je m'arrêterai plus en détail sur l'algorithme le plus utilisé actuellement, le *"deep learning"*, ainsi que son modèle associé,nommée *"neuronal network"*.
Ils sont actuellement les plus représentatifs des algorithmes et modèles utilisés, les plus connus, et permettra de pouvoir expliquer plus en détail le fonctionnement d'un algorithme et d'un modèle par l'exemple.

Finalement, je présenterai un type de **gestion de données**, le **lac de données**, qui est actuellement très utilisé dans le cadre de l'apprentissage machine.

1. l'apprentissage machine

De manière générale,**l'apprentissage machine**, ou "*machine learning*" va être l'utilisation de **modèles statistiques**, d'**algorithmes et de données** afin que programme accompli une tâche sans qu'il soit nécessaire qu'il possède les instructions explicites.

L'**apprentissage machine** est l'utilisation de **modèles mathématiques de statistique** et d'un **algorithme** afin qu'un programme puisse recevoir des données et effectuer des tâches et actions qu'il devra apprendre de lui même à faire.

Quelque soit le ou les types d'algorithmes utilisés ou de modèle, le fonctionnement dans sa globalité reste similaire.Le programme va recevoir en premier lieu des **données d'entraînement**, sur lequel il va **former une fonction**(une représentation généralisée des paternes perçu dans le jeu de données) que nous allons utiliser dans un modèle en se basant sur les paternes qu'il va percevoir dans les données reçu.

Les différents types d'algorithmes peuvent et **sont régulièrement utilisés ensemble**.
Si, pour une question de clarté et compréhension, un découpage par type à été fait dans ce mémoire,de nombreux systèmes utilise plusieurs algorithmes en même temps afin d'accomplir efficacement leur tâche. *AlphaGo* et ses successeurs (*AlphaGo Zero* et *AlphaZero*) , par exemple, utilisent comme algorithme un mélange entre de l'**apprentissage profond** et de l'**apprentissage par renforcement**.

Si il est cependant parfaitement possible de n'utiliser que un seul algorithme à la fois (de nombreuses fonction d'anti spam fonctionne uniquement avec de l'apprentissage supervisé), il est régulièrement associé l'**apprentissage profond** (qui fonctionne en utilisant comme modèle les réseaux de neurones artificielle) avec un autre type d'algorithme.

a) Les types algorithmes d'apprentissages

- **Apprentissage supervisé**

Cette apprentissage va fonctionner avec un jeu de données qui est **annoté** ou **labellisé**, c'est à dire que ces méta-données (ces caractéristiques) possède une **description de la donnée**. Ce jeu va être diviser en deux: Une partie pour **entraîner l'algorithme** et le reste pour définir ce que souhaite obtenir comme **sortie**. Par exemple, si j'ai comme jeu de données "2+2=4", "2+2" va servir à l'entraînement et sera mis de paire avec "4", qui sera le résultat attendu.
Il va donc définir sa **fonction** en se basant sur cette **entraînement**, qui sera associé avec un niveau de précision. Ce dernier nous permets de savoir le **taux d'erreur** de l'algorithme avec le jeu de données fourni et de décider si la fonction peut être utilisable ou si il est nécessaire d'effectuer des modifications supplémentaires.

En d'autres termes, il s'agit d'un **apprentissage par l'exemple**.

Ce type d'algorithme, bien que le plus simple à mettre en place, possède un certain nombre de **limitations**. Le premier étant la **nature des données** en elle même, qui sont annotés. Cela provient régulièrement d'un travail en amont d'une ou plusieurs personnes ayant rendu les données lisibles pour ce types d'algorithmes. Cela veut aussi dire que pour chaque données récupérées, il faut récupérer aussi le résultat.

Finalement, il existe le **compromis entre le biais et la variance**.
Le biais est une erreur que effectue l'algorithme quand il sort un résultat faux en s'entraînant avec le jeu de données d'apprentissage. un taux de biais trop élevé peut signifier que il n'arrive pas à trouver de fonction entre les données en entrée et les données que il est sensé avoir en sorti.
La variance est l'inverse. C'est quand l'algorithme, pour définir sa fonction, à pris en compte des données considérées comme du **bruit** (des données qui sont des anomalies exceptionnelles dans le jeu de données). La précision de l'algorithme est donc maximal (100%) avec le jeu de données d'entraînement que nous lui avons fourni, mais sera incapable d'appliquer la fonction établie quand il faudra effectuer une prédiction ou prendre une décision face à de nouvelles données.

En d'autre termes, le **compromis biais-variance** est un compromis entre un **algorithme trop souple**, ce qui l'empêche de trouver des paternes lui permettant de définir une fonction, ou **trop rigide**, ce qui l'empêche de réagir correctement face à une situation qui ne correspond pas à l'exactitude de son entraînement. Il est donc important de trouver un **juste compromis** entre le biais et la variance.

- **apprentissage non supervisé**

Ce type d'algorithme est l'inverse de l'**apprentissage supervisé**. Les données utilisés pour l'entraînement ne sont pas **labellisés**. A la place, il va chercher à lui même **classifié** les données en analysant les **ressemblances et différences** entre chaque données afin d'établir une possible relation. Une fois que il a trouvé cette possible relation, il va tenter de créer la fonction à utiliser pour le modèle.

Il s'agit d'un type d'apprentissage qui cherche à se rapprocher le plus possible des **capacités de réflexions d'un être humain**, tout particulièrement la capacité à organiser des informations et des

données pour permettre d'en établir la relation et définir les paternes. Il est cependant très difficile de mesurer un **taux de pourcentage de précision** de l'algorithme, du à la nature des données. La mise en place d'un apprentissage de ce type va demander beaucoup de **tâtonnement et de test**.

- **Apprentissage par renforcement**

L'**apprentissage par renforcement** ce vois beaucoup dans le monde des automates et de la **robotique**. Il s'agit de l'apprentissage par l'**exploration et l'exploitation** de l'environnement immédiat.
Ce type d'apprentissage ne fonctionne pas avec un jeu de données qui servira d'apprentissage, mais avec un ensemble d'actions possible à effectuer dans un environnement défini, et une fonction de récompense, basé sur le **processus de décision de Markov**.

Au début de l'apprentissage, il va être défini un ensemble de **premières actions possibles** ainsi qu'un objectif à atteindre. **La fonction de récompense** va être défini par rapport à cette objectif, au nombre d'actions précédemment effectué, le temps pris et, dans le cas d'un système mécanisé, l'énergie coûté.

L'automate va commencer son **apprentissage étape par étape**, en effectuant une action qui obtiendra une **valeur de récompense**, permettant de connaître quel action priorisée par rapport à une autre. L'action suivante va obtenir **une nouvelle récompense**, et il va obtenir deux valeurs différentes:

- Une qui sera la récompense de l'action prise;
- une autre qui sera la valeur de l'ensemble des actions prises jusqu'à maintenant.

La fonction de réponse est différente selon **l'objectif** que l'on souhaite accomplir. Si, par exemple, il faut un automate capable d'atteindre un point B partant d'un point A en moins de temps possible, la **fonction de récompense** sera très différente pour celle d'un automate ayant la même tâche, mais devant le faire en utilisant le moins d'énergie possible.

Finalement, il existe aussi une notion de **regret** dans les algorithmes d'**apprentissage par renforcement**, permettant de faire la différence entre **comportement optimal** et **comportement performant**:

- *performant*: l'automate va effectuer ces actions uniquement en se basant sur les récompenses associés et va chercher à avec le niveau maximum de récompense à court termes. (Si j'ai une action qui vaut 4 de récompense, et une autre qui vaut 5, je vais choisir l'action à 5)

- *optimal*: L'automate va raisonner par rapport au résultat et conséquences de ces actions, cherchant à maximiser ses résultats par rapport à l'ensemble de ces actions. En d'autre termes, il va réfléchir à long terme.

Le **regret** est donc ici une mesure qui va **diminuer la récompense** gagnée par action selon si l'automate se contente d'agir uniquement **selon son algorithme** (performant), ou si **il réfléchi** par rapport à l'ensemble des actions que il va entreprendre (optimal).

- **Apprentissage par transfert**

Nouveau type d'apprentissage, l'**apprentissage par transfert** est encore sujet à de nombreuses recherche, bien qu'il soit utiliser dans certains système. Le "*Cancer Genome Atlas Program*" utilise par exemple un algorithme de transfert pour la découverte, diagnostic et traitement de certains type de cancer.

Il répond à la problématique du manque de **transfert de connaissance** d'un système d'IA entre deux domaines. Quand nous devons utiliser un algorithme d'apprentissage, il va apprendre pour **un domaine spécifique**. **La connaissance accumulée** dans ce domaine ne peut pas être reporté dans l'apprentissage d'un autre domaine, forçant à recommencer un nouveau apprentissage.

Dans l'apprentissage machine, au travers d'un jeu de données, l'algorithme va générer une fonction issu des paternes qu'il découvre et l'apprendre au modèle. l'apprentissage par transfert va commencer l'apprentissage du **nouveau modèle en utilisant les paternes** précédemment découvert pour une nouvelle tâche. Cela peut permettre de résoudre des **problèmes concret complexes** plus facilement,géré des données n'étant peu ou pas labellisés, et avancé sur l'objectif d'arriver à une AGI.

Cependant, ce type d'algorithme présente encore **quelques défis**. Le **transfert de connaissances** peut amener à une **perte de performance générale** du système, dû à l'apprentissage et l'utilisation de la mauvaise connaissance dans un domaine qui n'en a pas besoin (un exemple par exagération serait d'utiliser le savoir de casser une planche en voulant ouvrir une porte. Même si l'objectif d'ouvrir la porte est bien atteint, en brisant la porte en deux, la performance n'est pas bonne.).
L'autre challenge est **le transfert de trop de connaissances inutiles**. Dans ce cas, le modèle est surchargé de données (les connaissances reste des données, avec une taille).

2. les modèles

Un modèle est un système qui va se servir des **données traités** fourni par l'algorithme pour accumuler des connaissances et les manipuler. Quand nous entraînons un système d'IA, nous entraînons le modèle qui le compose. Il est en quelque sorte le cerveau de l'IA.

a) Les types de modèles

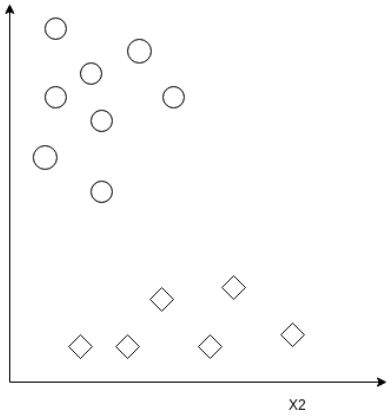
- **Vecteur de support**

Aussi appelé **séparateurs à vaste marge**, il s'agit d'un type modèle utilisé pour **l'apprentissage supervisé** conçu pour résoudre les problèmes d'analyse **statistique discriminante** (utiliser pour décrire,expliquer et prédire l'appartenance à des groupes pour des paternes issu des observations des données) et de **régression** (utilisé pour déterminé et analysé la relation d'une donnée avec les autres).

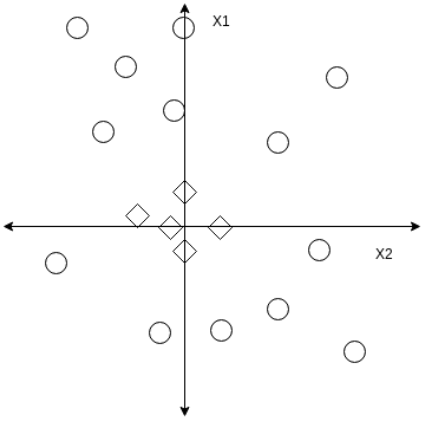
Son fonctionnement est basé sur un système de **classifieurs linéaires**. En d'autre termes, les données qui vont passer par le **vecteur de support** vont être **classés dans différents groupes** selon la **labellisation** de la donnée. Il est donc conçu pour manipuler des **données labellisés**, d'où son utilisation dans de l'**apprentissage supervisé**.

Quand il y a organisé les données dans différentes classes, il va pouvoir ensuite définir un **paterne**, qui va être représenter par un **vecteur**.

Prenons par exemple un ensemble de données qui peuvent être organisés en **deux classes différentes**, représenté respectivement par des **cercles et losanges**. le vecteur de support va les organiser sur un **plan en deux dimensions**. Nous pouvons arriver devant deux cas de figures. Le premier cas va avoir un **séparateur dit linéaire**. Le second aura un **séparateur non-linéaire**, le cercle unité.

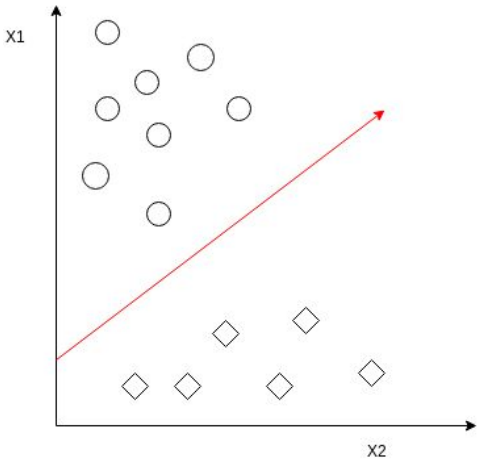


(fig.2 Cas de figure 1)

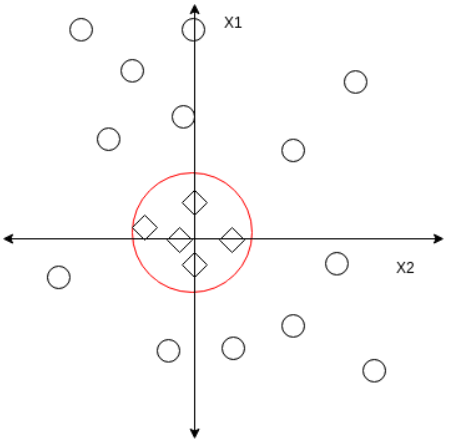


(fig.3 Cas de figure 2)

Dans les deux cas, le modèle par **vecteur de support** va créer un vecteur qui va faire la séparation entre les jeux de données:

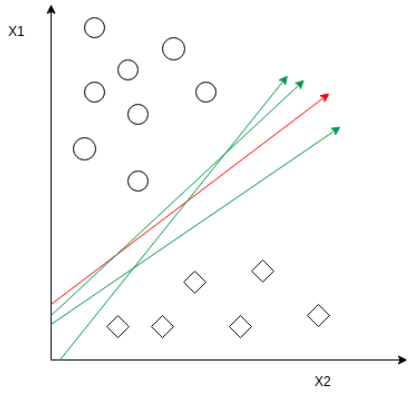


(fig.4 Cas de figure 1 avec séparateur)



(fig.5 cas de figure 2 avec séparateur)

Dans les **premier cas,** les données sont **linéairement séparable**. Le modèle de support de vecteur va alors proposer une **séparatrice linéaire** qui va découper les deux groupes. mais ce n'est pas le seul séparateur possible:



(fig.6 cas de figure 1 avec différents séparateurs)

Les **différents séparateurs** possèderont les **mêmes performances** quand il s'agira d'effectuer un **apprentissage**, mais n'auront pas la même **efficacité** quant à leur **généralisation de paternes**, qui reste l'objectif final du modèle. Afin d'obtenir une **performance optimal**, le chercheur va travailler sur la distance entre **les points les plus proches du séparateur**. Cette distance ce nomme **la marge**, et les points les plus proches sont **les supports de vecteurs**.
L'objectif est donc de trouver **la marge optimal** entre les **supports de vecteurs** et le séparateur afin de trouver le juste milieu.

Le **cas numéro 2** est un **cas de transformation simple**, qui arrive quand les données ne sont pas **linéairement séparable**.
Le chercheur va alors manipuler la dimension utilisé par le modèle de **vecteur de support**, en le passant sur un **plan en trois dimensions**, par exemple. Ici, nous sommes passé de **coordonnées cartésiennes en deux dimensions**, qui est le **plan par défaut**, à un plan en deux dimensions utilisant des **coordonnées polaires**. Autrement dit, nous sommes passé d'un plan utilisant des **coordonnées X1 et X2** à un plan utilisant des **angles comme coordonnées**.

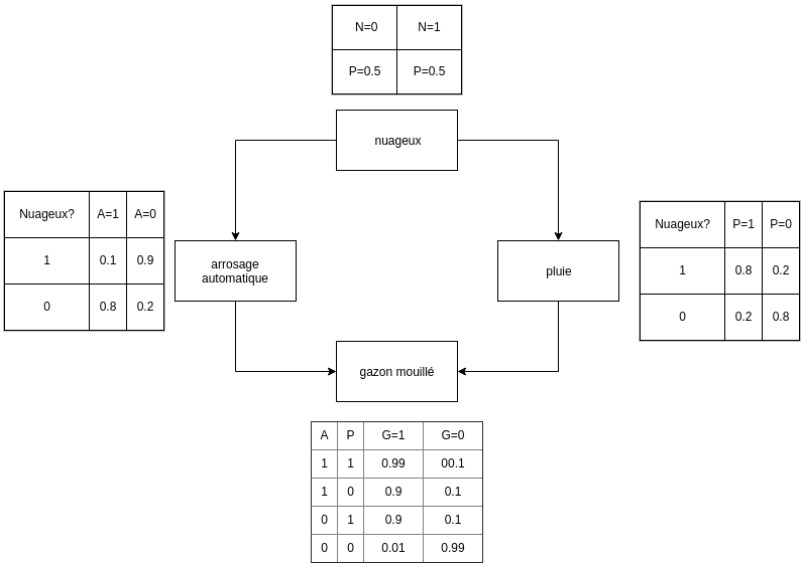
- **Réseau Bayésien**

Les **réseaux bayésiens** sont des **graphes orientés**. C'est à dire que il fonctionne avec un **système de noeud**, représentant une **donnée** ou l'effet que peut avoir **l'association de deux données** sous forme de **variables**, et de **flèches** qui vont faire **le lien avec ces données**.
chaque **noeud** va avoir **deux états**, 0 (qui peut se traduire par un **état inactif**, ou non présent) ou 1 (**actif** ou présent), et, selon l'état, va avoir une **interaction différente** avec la variable auquel il est associé via la flèche.

A chaqu'un de ces **noeuds** sera associée une **table de probabilité**, qui va donnée **la probabilité** qu'un noeud soit à un ou zéro selon **l'état du noeud précédent**.

Supposons que nous voulons savoir **la probabilité** qu'un gazon soit arrosé selon un temps nuageux et que le gazon soit équipé d'un arroseur automatique.

Le réseaux bayésien se présentera ainsi:



(fig.7 schéma d'un réseau bayésien)

Il y aura quatre noeuds: **nuageux,pluie,arrosage automatique,gazon mouillé.** A chaque noeud sera associé une **table de pourcentage**.

Ce type de modèle peut être utilisée pour les **différents types d'apprentissages** (**supervisé,non supervisé,renforcement et profond**). La **période d'apprentissage** va alors se concentrer sur la **construction du modèle** afin qu'il puisse créer les **noeuds**, leur **relation**, ainsi que les **tables de pourcentage.** Ils sont surtout utilisés dans le cas où le domaine ou les tâches nécessite de percevoir les **relations** entre **plusieurs événements** afin d'en déduire une **conséquence** (appelé en logique **l'inférence**) comme dans le domaine médical ("*Bayesian Networks in Medicine : a Model-based Approach to Medical Decision Making*",Lucas Peter,2001) ou dans la reconnaissance de voix ("*Speech recognition with mixtures of bayesian networks*",Microsoft Corporation,2002).

3. réseau de neurones artificiels

a) description

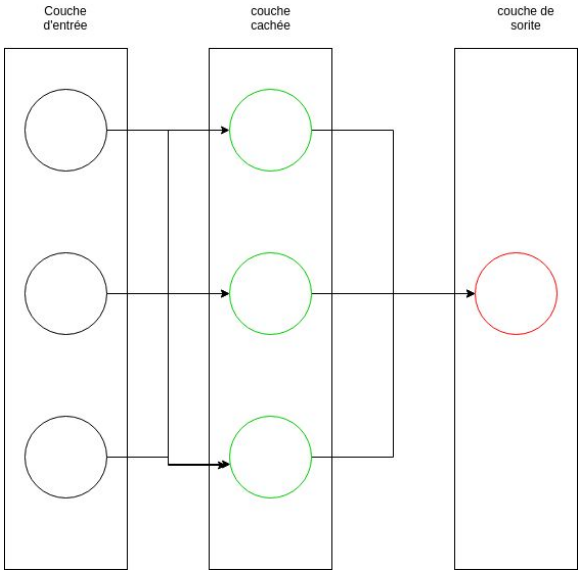
les **réseaux de neurones artificiels** sont des modèles inspirés par les **réseaux de neurones biologiques**. Ce type de modèle **apprends lui aussi par l'exemple**, de même manière que l'**apprentissage supervisé**. En examinant un ensemble de **données similaires et labellisés**, il va déterminer **les paternes caractéristiques** et tenter de les appliquer sur les **nouvelles données** qu'il reçoit. Son fonctionnement est basé sur un principe de **statistique** et de **probabilité**.
Par exemple, dans un cadre bancaire,après avoir été entraîné avec un jeu de données suffisant concernant les clients actuels de la banque, il répondra pour un nouveau client 1 si il s'agit d'un bon client, -1 si il va s'agir d'un mauvais client, 0 si le modèle ne peut pas répondre à la question, ou 0.7 si il n'est pas sûr de soi.

Le réseau de neurones possède un **système de décision intégré**, permettant de confronter ces connaissances avec les situations qu'il rencontre. A l'inverse de d'autre modèle d'apprentissage, qui utilise une **logique algorithmique**, suivant une suite de règle leur permettant de définir ce qu'ils vont apprendre face au problèmes rencontrés,**le système de déduction** d'un réseau de neurones va

examiner le **nombre de fois** qu'il rencontre une **situation similaire** et **la complexité** de l'événement par rapport à l'objectif à atteindre.

De même manière que son inspiration,il va posséder un ensemble de **neurones artificiels** (un ensemble de noeuds), lié par des **synapses** qui va transmettre un signal entre chaque noeud.

Le réseaux est organisé en **couches**, avec une **couche d'entrée** en première,une **couche de sortie** en dernière et un ensemble de **couches intermédiaires**, appelées les **couches cachés**.
Les neurones de la **couche d'entrée** va recevoir des données, qu'ils vont les transformer en des **signaux numériques**, l'envoyant aux neurones de la **couche suivante** , qui vont à leur tour effectuer une **transformation**. Chaque synapses va posséder un **poid**, une **valeur numérique** permettant de définir la **force du signal**, qui changera au fur et à mesure de l'apprentissage.

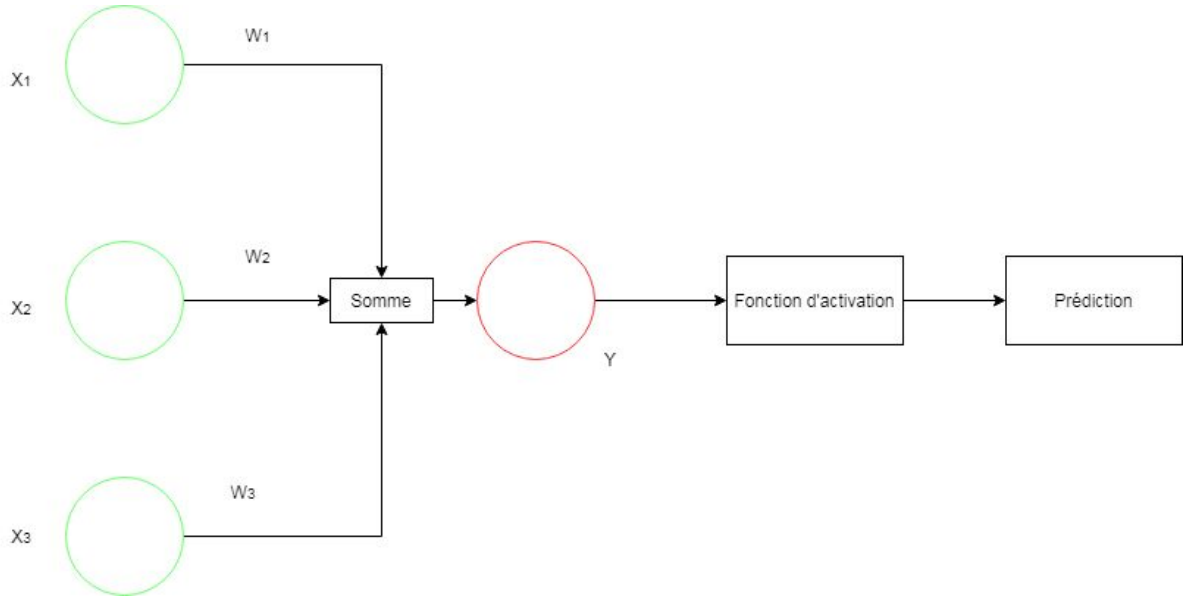


(fig.8 schéma simplifié d'un réseau de neurones à une couche cachée)

Un réseau de neurones peut ne pas posséder de couche intermédiaire.On parle alors de **perceptron**.
Dans le cas d'un réseau de neurones à plusieurs couches, nous parlons de **perceptron multi-couche**, ou **MLP** pour "*Multilayer perceptron*".

b) architecture

Pour correctement comprendre un MLP, il faut commencer par le **perceptron**.
Le modèle le plus simple est composé de **deux couches**, entrée et sortie. Celle d'entrée va posséder un ensemble d'**unités**, de neurones, X_i, où chaque individu i va recevoir les **variables d'entrées**, les données à traiter.
La sortie possède une **seule unité**, Y, qui va recevoir la **somme des signaux des unités** X_i qui lui sont reliée. Chaque signal, avant d'en faire la **somme**, va être multiplié par **le poid** W_p qui lui est associé.Il s'agit de la **fonction de sortie**.
Une fois cette **somme reçue**, la couche de sortie va la faire passer par une **fonction d'activation**, qui va permettre d'effectuer la **prédiction** ou la **décision**.



(fig.9 schéma simplifié d'un perceptron)

Selon la nature du problème pour lequel nous utilisons le perceptron, la **fonction d'activation** va être différente. Un **problème de régression** (un cas où nous effectuons une prédiction), la fonction sera différente que dans un cas de **classification binaire** (un cas où le modèle devra prendre un décision pour classer une **donnée d'entrée** dans **deux classes** différentes.Classer un client dans la catégorie "Bon client" ou "Mauvais client", par exemple.

Dans le cas d'un problème nécessitant nécessitant une classement dans **différentes classes** (une **classification multi-classe**), nous allons posséder Y_i unités de sorties, i étant le nombre de classes. Chaque neurones X_i sera liés aux différentes unités de sorties et chaque lien synaptique aura un poid. Chaque sortie aura sa propre **fonction d'activation.**

Si nous prenons l'exemple d'une architecture MLP dites "*feed-forward*" (**connexions unilatérales** des premières couches vers les dernières)il sera donc créé des **couches intermédiaires** (des **couches cachées**) entre la **couche d'entrée** et la **couche de sortie**. Chaque **unités d'une couche est connectée** à toutes les **unités de la couche qui la suit**, et chaque **sortie** d'une **couche intermédiaire** est une nouvelle **représentation des données**.

La couche d'entrée considère **la couche intermédiaire** qui la suit comme une **couche de sortie**, si bien que le calcul reste le même que avec un **perceptron** (sommes des signaux qui ont été au préalable multiplié par le poid W_p)
Cependant,La **sortie** d'un neurone h d'une **couche cachée** est calculé en appliquant la fonction d'activation du neurone h à la **combinaison linéaire des entrées**.
En d'autre termes, quand un neurone d'une **couche intermédiaire** va envoyer un **signal de sortie**, il va à être appliqué une **fonction d'activation** sur l'ensemble des signaux d'entrée du neurones avant d'envoyer le **signal résultant aux neurones suivants.**

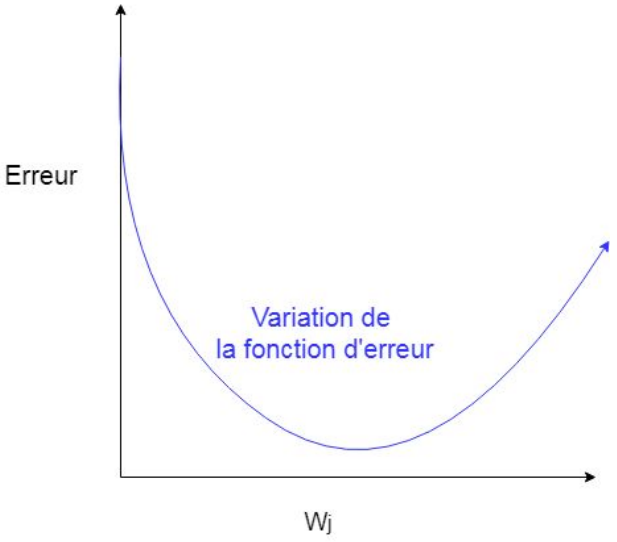
Finalement, la sortie de la couche de sortie est fait de la même manière. Elle va appliquer **la fonction d'activation** du/des neurone(s) de sortie sur **la combinaison linéaire des sorties** de la dernière couche intermédiaire.

Il existe d**'autre types d'architecture**, comme **le réseau de neurones convolutifs**,**linéaire adaptatif** ou **la machine de Boltzmann restreinte**. Certaines sont utilisées pour de **l'apprentissage non supervisé**, **supervisé, multi-couche** ou simplement de type **perceptron**.

c) apprentissage

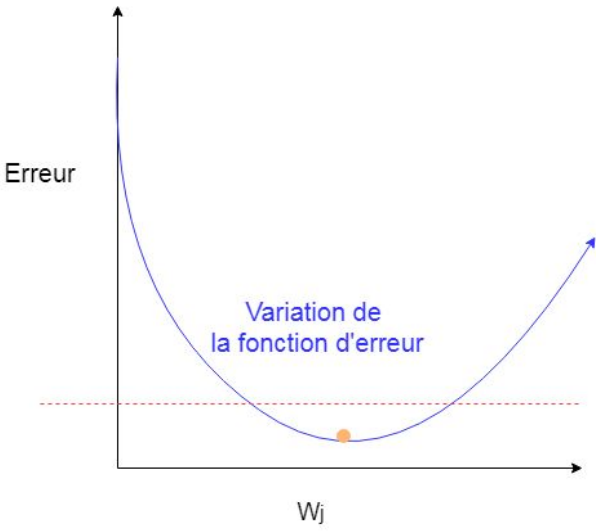
De même manière, pour saisir l'apprentissage d'un MLP, le plus simple est de commencer par un **perceptron**.
L'apprentissage s'effectue sur les **poids des connexions**. Ce sont ces valeurs qui vont être altérées afin de **minimiser les erreurs d'apprentissage** sur le jeu de données d'entraînement. En premier lieu, il s'agit d'un **processus itératif**. Après chaque tour avec le jeu de données, le modèle va ajuster le poid, en utilisant **l'algorithme de gradient**.

Cette algorithme va nous donner un plan en deux dimensions:



(fig.10 Schéma d'une courbe de gradient)

L'ordonnée correspond au **taux d'erreur**, **l'abscisse** est **la valeur des poids** et **la courbe** correspond à la **variation de la fonction d'erreur** (que le chercheur défini selon le but du modèle). l'objectif est alors de réussir à atteindre une **valeur minimum optimale** de la fonction, qui aura alors comme gradient une valeur se rapprochant de zéro, zéro signifiant que le modèle a réussi à trouver la valeur optimal pour le poid.



(fig.11 schéma de la recherche de la valeur minimum. plus nous arrivons proche d'un gradient à zéro, en dessous de la ligne rouge, plus nous sommes proche de la valeur optimale,qui est représenté par le point orange.En dessus de la ligne , augmentons notre taux d'erreurs.)

Pour cela, le **réseau de neurones** va commencer à changer aléatoirement les poids initiaux. A chaque tour, il va augmenter ou diminuer les poids selon ces observations, jusqu'à arriver à un gradient suffisamment proche de zéro ou que il accompli le nombre d'itérations fixé.

Un **MLP** va lui aussi se baser sur le principe de l'itération de l'**algorithme du gradient**, à la différence que il devra être effectué pour chacune des **connexions inter couches** (chacunes ayant des poids différents), augmentant **le temps de calcul** et le **risque d'erreur**.

Afin de simplifier le calcul, le modèle va utiliser l'idée de la **rétropropagation des erreurs**. Il s'agit du fait de décomposer l'erreur grâce au **théorème de dérivation des fonctions composées**.

Plus simplement, la mise à jour des poids va se faire en alternant une **phase montante** dans laquelle les sorties des **couches intermédiaires** sont mise à jour et une **phase descendante** dans laquelle le **gradient de l'erreur** par rapport aux poids d'une couche est calculé à l'aide du **gradient de l'erreur** des poids de la couche supérieure. La mise à jour des poids se fait à cette phase.

d) problèmes des réseaux de neurones

les **réseaux de neurones**, bien que très utilisés dans les différents types d'apprentissage et dans plusieurs domaines **(classification**, **reconnaissance de motif**, **estimations boursières** ou autres), rencontre encore des limitations et des problèmes.

- *Vision limité*: On entend par là l'**opacité d'un réseaux de neurones**. Plus celui ci commence à être **complexe**, plus il devient difficile de **comprendre le processus de réflexions**. Les calculs, comme ceux de la **rétropropagation**, deviennent alors très difficile à comprendre, donnant une sensation de **boite noir**.

- *Surapprentissage*: Aussi appelé **saturation** dans le cas des **réseaux de neurones**, il s'agit d'un modèle ayant comme sortie 0 ou 1 quelque soit l'entraînement qu'il reçoit. Un

changement dans le jeu de données ne donne alors plus **aucun résultat** en sortie, et le réseau n'arrive plus à apprendre.

- *instabilité du gradient*: dans le cas d'un **MLP**, les **couches basses** peuvent prendre une valeur de **gradients trop grandes** ou **trop petites**, rendant **le gradient des couches supérieurs faux**.

4. apprentissage profond

l'**apprentissage profond**, ou "*deep learning*", est un type d'**apprentissage machine supervisée** ou non, basé sur les **modèles de réseaux de neurones**. Il est utilisé pour permettre la **modélisation de données à haute abstraction** (représentation de données abstraite cherchant à les simplifier pour en permettre leur manipulation. Un signal sonore, visuel, des symboles écrit sur du papier, par exemple.)

Ces techniques vont extraire et transformer des c**aractéristiques de données** afin de pouvoir construire des **représentations du réel** et de faire apprendre au modèle utilisé **la manipulation des données non labellisés** associés.

Avec l'**apprentissage profond**, chaque couche du **réseau de neurones** va transformer les d**onnées d'entrée** en des données de plus en plus **abstraites**. Par exemple, dans le cadre d'une rec**onnaissance d'image**, la première couche va recevoir une **matrice de pixels** représentant l'image. Elle va définir les bords, puis envoyer les données à la seconde couche, qui va définir les bordures d'un visage. La troisième va permettre de reconnaître les détails généraux de ce visage (nez, bouche, yeux), puis la quatrième va reconnaître que l'image possède un visage.

Cette algorithme va chercher à définir le niveau d'abstraction de la données que chaque couche du réseau de neurones va effectué (dans notre précédent exemple, la troisième couche aurai pu définir tout de suite qu'il y a un visage sur l'image.). Cependant, **le besoin de régler le niveau d'abstraction** de chaque couche à la main peut se faire sentir, en ajoutant plus de **couches au réseaux**, par exemple. Ce niveau d'abstraction et le nombre de couches qui vont être défini font partie du **CAP**, ou "*credit assignement path*".

l'utilisation d'**apprentissage profond** implique que l'architecture du modèle qu'il l'utilise soit construit avec une méthode dite "*d'algorithme glouton*", ou chaque couches va chercher à obtenir le meilleur résultat localement, indépendamment du résultat globale.

5. lac de données

la définition la plus simple du **lac de données** : un **lac de données** est une **méthode de stockage de données** structurée ou non qui est actuellement utilisé dans le domaine de la **mégadonnées**, ou *"big data"*.
Concrètement, il va s'agit d'une **architecture mis en place** afin de stocker des i**mmenses quantités de données de toute formes et de toutes sources**. Elles peuvent être **structurées** (des données issu d'une base de données relationnelles), **semi-structurées** (tableurs, csv, journaux de logs, fichiers JSON) ou **non structurées** (email, fichiers textes, pdf, images et vidéos). L'objectif principal étant de

pouvoir stocker et préparer une **potentielle utilisation** de ces données (tout particulièrement les non-structurées) de manière efficace.

Pour comprendre pourquoi nous parlons de **stockage de données non structurés** efficace, une comparaison entre une **base de données** et un **lac de données** est possible.

Une **base de données,** tout particulièrement si elle est **relationnelle**, ne peut contenir des d**onnées non structurées**, comme des fichiers textes, si un processus de préparation doit être fait. Le risque de **perdre des données** et **le temps et le coût** de cette transformation, tout particulièrement par rapport à **leur utilisation ou non utilisation** sont important. **l'efficacité est donc moindre**. Le **lac de données** ne présente pas ce désavantage. Il va contenir les données sans les modifier et les garder en mémoire de sorte à ce que leur accès soit rapide.

Le lac de données est donc utilisée pour de **l'exploration de données** et **de texte**,par exemple.Mais effectué une **analyse et un traitement efficace** du contenu d'un **lac de données** afin d'en pouvoir en sortir un résultat intéressant n'est pas chose aisée. Comme dit précédemment, le lac possède une **quantité importante d'information** (on compte en **tera-octets**, avec des offres qui propose des emplacements de stockage à tailles croissante afin de pouvoir stocker de nouvelles données, comme Azure data lake, une offre de stockage pour les lac de données de microsoft. A titre d'idée, un tera-octets fait environ 125 clés usb de 8 giga-octets), qui peuvent être de toute formes. Difficilement **exploitable** pour un être humain, et même avec des **outils adaptés** *(*HDInsight,Azure Data Lake Analytics,Elastic Search ou DynamoDB pour ne citer que eux comme exemple).

l'intérêt des **lac de données** dans le domaine de **l'intelligence artificielle** est justement la **donnée**. Un algorithme d'**apprentissage machine** peut puiser dans un lac de données afin d'apprendre, que cela soit des **données labellisés** (les données structurées) ou non (les données non structurées).

Pareillement, une fois l'apprentissage finit, l'utilisation du système d'IA dans le cadre du l**ac de données** va permettre de faciliter le **traitement et l'analyse de son contenu**. Dans ce cas, l'IA va être utilisé dans du **big data**.

C. Les défis et difficultés actuels

Le domaine de l'intelligence artificielle, malgré les nombreuses avancées qu'elle a rencontrées sur ces dernières années, n'est pas exempt de **difficultés et de challenges**. Dû à sa nature **pluridisciplinaire** (les mathématiques, les neurosciences, les technologies de l'informatique,etc….), elle va nécessairement faire face au problèmes associés à ces disciplines. Cependant, elle possède son propre lot de **défis et de limitation**, que l'on peut séparer en deux parties.
Les **problèmes d'ordre technologique ou technique** sont ceux que l'on rencontre quand il s'agit du système d'IA en lui même. Des problèmes de malfunction, par exemple, ou la nature des données qui nous servent à les entraîner.
Les problèmes humains sont ceux qui sont associés avec notre comportements par rapport à l'intelligence artificielle et la limitation de nos connaissances sur certains sujets. Les attentes concernant l'intelligence artificielle(qui fut en partie la cause de l'**hiver** du domaine entre 1974 et 1980), ou des q**uestionnements d'éthique**,peuvent être des difficultés ou du moins des raisons d'un ralentissements des recherche de l'IA.

1. techniques

a) overfitting et underfitting

Un système d'**intelligence artificielle** est, à son coeur, un ensemble de programmes, algorithmes et infrastructure matériel. Il peut être donc lui aussi soumis à des problèmes, comme des dysfonctionnements.
Cependant, l'apprentissage en lui même peut faire face à des problèmes quand il s'entraîne avec des données,quel que soit le modèle et la méthode d'apprentissage. Il s'agit de *"l'overfitting"*(**sur-apprentissage**) et *"L'underfitting"* (**sous-apprentissage**).

le **sur-apprentissage** est l'**incapacité** à créer des **paternes** assez généraux pour pouvoir être appliqués à de nouvelle données. En d'autre termes, le système d'IA a appris par coeur les données d'apprentissage et est incapable d'appliquer ces connaissances à de nouvelles informations si elles ne sont pas exactement les mêmes que celle issu du jeu d'apprentissage.
Par exemple, plutôt que d'apprendre que l'équation de 2+2 est l'addition de plusieurs chiffres, quelque qui soit (générer un paterne), elle a appris que 2+2 valait 4. Si elle se retrouve face à une équation autre, elle ne pourra pas appliquée le paterne appris.

le **sous-apprentissage** est l'inverse. Malgré le jeu de données d'apprentissage, elle ne peut pas générer les paternes.

b) les données

Les données sont un élément capital pour l'intelligence artificielle. C'est ce qui va lui permettre d'apprendre, et donc de la rendre utile. Sans données,l'IA est donc incapable de faire quoi ce soit, qu'importe le modèle et l'algorithme utilisé. Au delà de la **quantité massive d'informations** nécessaire selon l'objectif que l'on souhaite atteindre, il y a aussi la question de la **qualité** de la donnée en soi, sa **labellisation** selon le type d'apprentissage effectué et l'existence ou non de la **quantité de données** nécessaire pour certains domaines.

La qualité de la donnée concerne sa justesse et sa précision. Si nous possédons un jeu de données incorrect ou trop imprécis, l'apprentissage sera faussé.

Selon le type d'apprentissage, il est nécessaire que les **données soient labellisés**. Il n'est pas nécessairement possible d'en trouver une quantité suivante naturellement pour permettre un apprentissage. Cela signifie qu'il faut donc **labellisés les données manuellement**.

Finalement, certains domaines ne possède pas nécessairement le nombre d'informations nécessaire pour permettre un **apprentissage efficace**. Dans la cas de la médecine, par exemple. Si l'objectif est la découverte et l'étude d'une nouvelle forme de maladie, il est nécessaire d'avoir des patients atteint de cette maladie. Le problème vient alors d'une **question d'éthique**, où les chercheurs ne vont pas demandés à ce que des personnes soient atteint de manière volontaire à cette maladie pour permettre d'effectuer un apprentissage correct.

c) l'apprentissage spécialisé

En 2017, Google créa l'architecture *MultiModel* ("*One model to learn them all*",Google,2017), modèle permettant à une architecture de pouvoir manipuler **8 tâches différentes** issu de différents domaines (l**e langage naturel**,**la reconnaissance d'image** et l**a reconnaissance de parole**), offrant une avancée significative dans la recherche d'une IA capable de travailler dans plusieurs domaines différents.
Cependant, bien que proposant une bonne performance, cette architecture nécessite une quantité importante de jeu de données (pour quatres domaines différents),et rencontre le même problème que les tentatives précédentes d'IA générale. Si les **performances sont bonnes**, elles le sont moins qu'une **IA spécialisée**, tout particulièrement en rapport au données nécessaire.
Bien que, grâce à l'architecture *MultiModel*, il a été prouvé que il est possible de gérer plusieurs tâches de différents domaines, la problématique d'une IA générale suffisamment performante pour résoudre des problèmes réel reste présente, et il est toujours plus simple et efficace d'effectuer un apprentissage focalisé sur un domaine.

2. humains

a) les attentes

le manque de compréhension de ce qu'on entend derrière la notion d'intelligence artificielle,le fait que à nos jours, ils existent une surreprésentation de cette notion, que cela soit utiliser comme argument de vente (l'entreprise chinoise Huawei a basé une partie de la promotion de son téléphone portable Mate 20 pro sur l'intégration d'une intelligence artificielle) ou dans la fiction (on retrouve l'intelligence artificielle dans les films Alita:Battle Angel,Upgrade ou la licence Blade Runner) peut générer une attente trop importante par rapport à ce domaine,malgré le fait que le domaine de l'IA possède des limitations.

Cela peut créer la même situation que en 1974: beaucoup d'attentes, qui peut potentiellement créer une lassitude où une désintérêt si ces attentes ne sont pas rencontrer assez tôt, pouvant repartir sur un nouvelle hiver.

b) l'éthique

De nombreux questionnements d'**ordre éthiques** et **philosophiques** tourne autour du domaine de l'intelligence artificielle. Des hypothèses concernant un potentiel risque pour l'humanité,la création d'une superintelligence,l'absence de morale ou d'empathie d'une IA ou le potentiel remplacement d'être humain pour certain type de travail ont permis de créer un nouveau domaine: l'éthique de l'intelligence artificielle. Ce dernier effectue des recherches sur les questions de l'ordre de l'éthique de l'IA afin de proposer une direction morale au recheche technique. L'entreprise GoodAI, par exemple, en a fait son objectif.

D. Conclusion

Dans cette première partie de l'état de l'art, il a été expliquée ce qu'est l'intelligence artificielle. Cela permet de définir un peu plus précisément la première partie de la problématique, en prenant conscience de son fonctionnement, ces limitations et ces domaines d'applications.
Il devient alors clair que, même si un système d'IA peut être efficace, il ne peut l'être que dans une **suite de tâches spécifiques**. Elle est limitée par les **données utilisées** pour son apprentissage, et son efficacité dépendra d'un grand nombres de facteurs, que cela soit la quantité et justesse de ces données, mais aussi l'**utilisation du bon algorithme** et modèle par rapport à l'objectif que l'on souhaite accomplir, l'entraînement qu'elle a subi et les situations auquelle elle fait face.

Ce domaine n'est donc pas magique ou capable de tout faire. une IA ne permets que de mettre en lumière des paternes dans un ensemble de données afin d'effectuer une décision ou une prédiction. Elle répond à une logique, qui ne peut tout prévoir,et le risque d'erreur est toujours présent. De même manière que toutes formes de technologies, elle n'est qu'un outil pouvant remplacer efficacement l'accomplissement de tâches que les chercheurs peuvent eux mêmes comprendre et découper en une suite d'actions logiques afin d'aider un être humain, comme devenir un outil d'aide à la décision. Cependant, la décision finale reste celle de l'opérateur qui l'utilise.

IV. la guerre de l'information

A. définition de la guerre de l'information

Dans cette seconde partie de l'état de l'art, il sera présenté **la guerre de l'information** (ou *infowar*), ces **acteurs**, **méthodes et techniques**. Une définition de l'**information**, qui est le nerf de guerre de ce domaine sera donnée, et finalement, quelques exemples de guerre d'information entre les différents acteurs sera présentés.

En premier lieu, il est important de signaler que la définition de guerre selon le dictionnaire larousse est "**un conflit entre état**". Cependant, l'*infowar*, bien que portant ce terme de "*guerre*", dépasse cette définition, et peut se dérouler entre **groupe d'influences**, ou **entre entreprises**. De même manière, une **guerre de l'information** peut s'effectuer alors que aucun conflit armée n'est présent.

Ceci étant signalée,l'institut pour l'étude avancée sur la guerre de l'information défini l'*infowar* comme: "*la guerre de l'information consiste en l'utilisation offensive et défensive d'information et de systèmes d'information afin d'exploiter,altérer ou de détruire les informations et les systèmes d'information de l'adversaire, tout en protégeant les siens. Des actions de ce type sont destinées à obtenir des avantages sur des adversaires militaires ou commerciaux*".

La guerre de l'information, bien que présente depuis les premiers conflits armées dans l'histoire (des auteurs comme Sun Tzu ou Miyamoto Musashi, deux philosophe et stratège respectivement Chinois et Japonais, cite régulièrement des techniques de désinformation et de tromperie dans leur livre "*l'art de la guerre*" et "*le livre des cinq roue*"), est devenu beaucoup plus présente avec l'**apparition de l'informatique**, qui permets de t**ransmettre et manipuler** de la **donnée** en un **temps réduit**, voir proche de zéro.
Il est admis de manière générale qu'elle fonctionne en **deux niveaux**:

- *Psychologique*: Toute **techniques psychologiques**,**médiatiques**,**diplomatiques et militaires** destinées à **influencer le mode de pensée** d'un opposant, que celui-ci soit un chef militaire ou une population entière. Par exemple, l'opération Fortitude durant la seconde guerre mondiale. Il s'agissait de la création de fausses unités au nord et au sud du Royaume-Uni afin de tromper l'Axe que le débarquement aurait lieux en Norvège ou dans le Pas de Calais.

- *Technologique*: les attaques contre des **infrastructures d'information civiles ou militaires**. Il est alors sujet de **piratage informatiques**, **déchiffrage de codes**, **interruption des flux de données**, i**ntrusion dans des systèmes d'information** voir leur **destruction physique**.

Si les deux niveaux sont séparés pour une question de clarté, il est important de garder en tête qu'ils fonctionnent de paire. Une attaque technologique peut être faite afin d'offrir une possibilité d'attaque psychologique, et vice-versa.

Ensuite, une **guerre de l'information** n'est pas nécessairement présente uniquement en temps de guerre. Toute entité **possédant,manipulant et nécessitant des informations**,étant d'en une situation où elle a un adversaire (que cela soit une entreprise concurrente, une population ou un état) peut participer à une **infoguerre**. On peut citer par exemple **la guerre industrielle**, qui est effectué autant pendant une période de conflit ouvert, mais aussi de temps de paix.

Si l'objectif principal de la **guerre de l'information** est l'obtention et la protection d'un avantage face à un adversaire, il est possible de déterminer **quatre manières**, quatre sous-objectifs, afin d'y arriver:

- *l'exploitation et l'obtention d'information*
- *l'intoxication d'informations*
- *l'interruption et/ou la destruction de l'information*
- *protection de l'information*

L'exploitation et l'obtention de l'information à pour but d'obtenir des données afin de les utiliser. Il va s'agir de piratage de système d'exploitation, de vol de documents,etc…
L'intoxication d'informations est l'utilisation volontaire d'information fausses, que cela soit pour induire l'adversaire en erreur, corrompre leur système d'information ou propager une idée et faire changer un opinion. La propagande ou l'insertion de fausse données dans un système d'information sont des exemples.
L'interruption et la destruction concerne les actions effectuées afin de paralyser un flux d'information, voir le détruire. Une surcharge de données dans tous les canaux d'entrée du système, ou la destruction physique du système, par exemple.
Finalement, **la protection de l'information,** qui va chercher à empêcher les objectifs ci dessus. Chiffrer nos données, fonctionner en boucle fermée, etc…

La guerre de l'information peut être donc résumée ainsi: *Savoir,empêcher l'autre de savoir, convaincre et tromper.*

1. Que ce que l'information

a) définition générale

Avant d'aller plus loin, il est bon de pouvoir définir ce qu'il a derrière **le terme** "*d'information*", afin d'éviter de fausse idée ou des incompréhension.
Comme de nombreux sujets, la définition du concept "*d'information*" va dépendre du domaine dans lequel il va être utilisé. De manière générale, on détermine l'information comme le message à transmettre , et les symboles qui vont le composer(les données du message).

A ceci s'attache d'autres principes, comme celui du **sens de l'information** (une suite de la lettre "A" dans un message écrit n'est pas nécessairement considéré comme une information,car n'ayant pas de sens. On parle alors de **néguentropie**),la **pertinence du message** ou la possibilité qu'il est un effet, et donc d'engendrer ou non une action.

la définition de l'**information** peut alors correspondre plus à une **connaissance** (une suite de données étant assemblées pour permettre d'avoir un sens) utilisant un support, qui peut être mis en présence d'une entité capable de l'interpréter et l'utiliser pour atteindre un objectif.

On fait donc une **distinction entre l'information**, qui est une **connaissance interprétable** pouvant être utilisé, et la **communication**, qui est l'information sujet à une interprétation et transmise.

La notion d'**information** est étudiée dans différents domaines, comme la finance ou la philosophie, est sa définition va varier selon le contexte et le domaine qu'il l'utilise. Cependant, dans le cadre de la guerre de l'information, deux théories sont mise en pratique, celle de la décision et celle de l'information.

Les prochains points qui vont suivre vont étudier un plus en détails ces deux théories.

b) selon la théorie de la décision

La **théorie de la décision** est l'étude du processus de **prise de décision** d'une entité selon les informations qu'il possède, et le résultat de ces décisions afin de permettre de trouver le choix optimal.

Pour cette théorie, l'information est toute donnée qui est de nature à **entraîner ou modifier une décision**, que cela soit une information vrai,fausse ou biaisées. Dans le cas contraire, on parle de **bruit** (une information qui n'a pas de données pertinentes).

c) selon la théorie de l'information

La théorie de l'information,aussi appelée la **théorie de l'information de shannon**, est une théorie cherchant à quantifier le niveau d'une information d'un ensemble de message selon une **distribution statistique**. Il existe d'autres formes de théorie de l'information, comme **la théorie algorithmique de l'information**.

Dans ce cas, l'information est une **mesure quantifiable**, défini par la **complexité du moyen de la fabriquer** (la suite de chiffre allant de 1 à 100 est un simple à réaliser, par exemple), le couple "*message+récepteur*" (si le message est écrit en allemand et que le récepteur n'a aucune connaissance dans cette langue, la valeur de l'information est nulle), et le **contexte associé** (si Fenrir est un chien, la phrase "*Fenrir est un chien*" à plus d'information que "*Fenrir est un quadrupède*". Avec la première, nous savons que Fenrir est un chien, et donc qu'il s'agit d'un animal canin quadrupède, sauf amputation. La deuxième ne permets pas de faire ce lien).

Cette mesure se nomme l'entropie de shannon, qui correspond à la quantité d'information d'un message.

B. Fonctionnement

La guerre de l'information est un domaine de stratégie en soit. Elle possède ses propres rouages, **méthodes**, et **acteurs**. Comme dit précédemment, bien que le terme de guerre soit présent dans l'**infoguerre**, elle dépasse le cadre d'une lutte entre deux états, et peut être effectué entre plusieurs entitées différentes.

Le conflit entre les sociétés Coca-Cola et Pepsi,appelé **la Guerre du cola**, par exemple, est un cas de **guerre d'information**, toute proportion gardée, entre **deux entreprises**. On peut aussi citer l'exemple

du cas du **printemps arabe**, où l**es gouvernements** ont cherchés à contrôler **le flux d'information** des réseaux sociaux alors que ceux-ci servaient de **plateforme d'échange d'information** entre les utilisateurs (**une guerre d'information** entre un gouvernement et son peuple par tentative d'interruption d'un système de communication) ou la perte de la quasi-totalité du trafic internet et téléphonique en Birmanie, toujours durant le printemps arabe.
Dans ce dernier cas, nous sommes toujours dans une interruption du **système d'information** venant du gouvernement vers son peuple, mais aussi dans une **guerre d'information** entre un pays et le reste du monde. Aucune information sortante, impossible donc de savoir ce qui se passe.

le théâtre d'opération étant différent d'un conflit "*classique*", les méthodes pour parvenir à atteindre l'objectif fixé changent.
Censure (la censure des image en URSS, qui supprima toute personnalité ne correspondant pas à des critères) , **attaque informatique** (l'exercice "*Eligible Receiver*",organisé par l'ensemble des services de renseignements américain, à fait affronter la "*NSA Red Team*" à l'infrastructure et les services de renseignement. La "*Red Team*" ont pu, par exemple,accéder et modifier des e-mails ou perturbés le service téléphonique.) ou **propagande** (la propagande nazie, passant par le cinéma, les affiches,le sport ou le contrôle de la radio allemande) deviennent les outils et méthodes pour cette forme de conflit. A nouveau, si **les différentes méthodes**, dans un objectif de clarté, sont séparés, elles sont en **réalité utilisée ensemble**. Utiliser de la **désinformation** pour effectuer une **subversion** en utilisant les **informations** obtenus via une **action de surveillance électronique**, par exemple.

1. Ces acteurs

Cette première partie va présenter les acteurs d'une guerre de l'information, leur impacts et rôles.

a) états et gouvernements

Bien que l**'infoguerre** dépasse l'affrontement classique entre deux pays (ou plus) , ces derniers n'en reste pas moins des acteurs majeurs.
En premier lieu, il faut se rappeler que chaque états possède ses **propres services de renseignements**: Le Mossad et le Shin Bet pour Israël, la DGSI et DGSE en France ou le CSIS au Canada, par exemple. Ces **agences gouvernementales** ont comme **responsabilité la collecte, analyse et exploitation de l'information** pour différent objectifs (**militaire**, **sécurité nationale**, **application de la loi**).

Mais il peut aussi avoir des **tensions politiques** entre deux pays (**intérêts différents**, **confrontation d'idéologie**) qui peut entraîner une **guerre d'information** entre eux, cherchant à discréditer l'autre (**propagande**, utilisation de vecteurs comme les médias pour censurer ou déformer des informations, discours publique de figure d'autorités) et à avoir un coup d'avance (un **avantage**). A ce titre, **l'infoguerre** devient alors un outil pour le domaine de la **géopolitique**.

Cependant, les états sont aussi des **acteurs majeurs** par le fait qu'ils peuvent contribuer à d'autres acteurs de la guerre d'informations, financièrement, par partenariat, ou par la création d'une demande d'un service ou d'un bien de la part de l'état vers un des acteurs. Pour reprendre l'Allemagne Nazie, les **journaux** d'avis contraire au gouvernement en place sont censurés et les autres sont fortement conseiller de se calquer à l'idéologie du moment, comme le journal Der Stürmer et Signal.

En Ukraine, l'entreprise **Burson Cohn & Wolfe**, travaillant dans la **communication** et les **relations publiques**, à été embauché en 2012 par le parti Ukrainien "Le Partie des Régions". L'objectif de ce contrat était d'aider le Partie des Régions à communiquer ces activités et leur position sur le cas "*Yulia Tymoshenko*" (Madame Tymoshenko étant accusée d'activités criminelles).

b) groupe d'influence

Un **groupe d'influence** est toute organisation ayant comme but d'**influencer**, directement ou non, des décisions ou un opinion. Ils sont naturellement enclin à participer à la **guerre de l'information**, cherchant à influencer l'opinion du public.

Ces groupes peuvent s'organiser de multiples manières. De simple groupe pacifique, comme les "*thinks tanks*", ou **laboratoires d'idées**, qui élabore des études et de propositions, souvent ciblant les domaines politique et économique, aux groupe plus virulent, comme le **Djihadisme**,qui c'est servi de **Internet** pour lancer des **campagnes de propagandes**, et dans de multiple langues (Français,Espagnol, ou Anglais). Autrement dit, Ce dernier cas utilise largement l'**aspect psychologique** de l'infoguerre pour justifier leur actes et convaincre la population de les rejoindre.

Mais un **groupe d'influence** ne verse pas uniquement dans les **actions psychologiques**.
Par exemple, en novembre 1998, un groupe de **pirate informatique** a pris comme cible un se**rveur web en Albanie** appartenant alors à l'OTAN, faisant passer comme un avertissement: ce groupe avaient comme volonté d'attaquer les systèmes d'informations de l'OTAN.
L'alliance a alors temporairement fermé tout accès au serveur web pendant 2 jours.

Il est aussi possible de citer le cas chinois d'octobre 1998. La naissance d'un nouveau site web chinois soulignant leur efforts en faveurs des droits de l'homme à provoquer la réaction d'un autre **groupe de pirates informatiques**.La page d'acceuil à alors été remplacé par un message condamnant Pékin pour ces violations de ces mêmes droits de l'homme.

Ces groupes ne sont donc pas associé à un état, et possèdent **des objectifs** et **des moyens** qui leurs sont propre. Loin d'avoir des **outils ou du financement** comme on peut en trouver chez c**ertaines organisations gouvernementales**, il ne reste pas moins qu'ils sont malgré tout capable de pouvoir se lancer de cette forme de conflit, et effectuer des actions qui ont des répercussions.

C'est par ailleurs pour cette raison qu'il a été souligné plusieurs fois dans ce mémoire que une **guerre d'information** dépasse la notion de conflit entre états. L'apparition de l'**informatique** (et des **technologie de communication** de manière générale), et tout particulièrement depuis que ce domaine est devenu libre d'accès ont permis à tous , pour peu que certains disposent des connaissances (souvent aussi accessible sur internet), de pouvoir participer à l'infoguerre.

c) entreprise et société

Pour reprendre un exemple cité plus haut, **la guerre du Cola** à confronter les entreprises Coca et Pepsi dans une escalation de programmes publicitaires visuels et comparatives afin de discréditer l'autre et convaincre l'opinion publique que leur "camp" était le meilleur.

(fig.12 un exemple de la guerre de cola. A gauche,Pepsi et à droite,Coca-Cola)

Ces campagnes publicitaires, si elles ne sont pas techniquement de la **propagande**, ont malgré tout comme objectif de **changer l'opinion générale d'un public** afin de prendre l'avantage sur l'autre, en passant par des **systèmes d'informations**. On reste sur une idée de **guerre d'information**, toute proportion gardée.

De manière générale, **l'infoguerre** entre sociétés passe entre autres par des campagnes publicitaires: **la guerre du Cola** (Pepsi et Coca-Cola) ou **les publicités comparatives** entre les chaînes de **restauration rapides** McDo,Burger King et Wendy's. Mais elles peuvent aussi y être engagé par d'autres activités, comme de **la veille** (collecte d'information), de la **protection d'information et d'influence** (propagation d'information traitée pouvant bénéficier une stratégie). On parle alors "*d'intelligence économique*", qui se place dans un cadre légal, et donc effectué par des moyens légaux. Si les actions sorte du système légal, il s'agit "*d'espionnage industriel*".

Cependant, ce n'est pas le seul cadre où une entreprise peut être actrice d'une **guerre de l'information**.
La société Thales, par exemple. Elle propose de multiples services et outils tournant autour de **l'information et des systèmes associés**. (**développement de drones aériens**, **communications radios**,**interception et exploitation de signaux électronique**, **sécurité informatique ou big data**).
Un autre exemple de même nature, il existe les sociétés General Dynamics, ou United Technologies qui produisent le même genre de service.

L'entreprise n'est alors plus une **actrice directe de l'infoguerre**, mais propose ses services ou biens afin de fournir **un autre acteur**.

d) peuple

Il est entendu par "*peuple*" **toute population** de gens ne faisant pas partie des **autres acteurs**, comme un **gouvernement ou une entreprise**.
Le peuple d'un état est souvent sujet à **la guerre de l'information**. que cela soit en tant que **participant** ou simple "*victime*". Le cas,par exemple, du **Printemps Arabe** à présentée différentes forme de **guerre d'information** entre le **peuple d'un état** et son **gouvernement**.**La guerre du Cola**, citée plus haut, à comme **objectif de convaincre les gens**. De manière générale, quand l'objectif va être de **convaincre ou influencer** l'opinion publique, le peuple sera concerné.

C. ces méthodes et techniques

Comme dit précédemment, il se dégage généralement **deux axes** dans le cadre de l'**infoguerre**. **L'aspect psychologique** et **l'aspect technologique**. Les deux sont complémentaires et utiliser ensemble. Cependant, pour une question de clarté, il va être aborder les méthodes et techniques de chacun des deux axes séparément.Les méthodes se basant très fortement sur un **comportement humain** seront donc dans l'axe psychologique de la guerre de l'information. Ceux nécessitant principalement un **vecteur technologique** seront dans l'axe technologique.

1. aspect psychologique

a) désinformation

Sun Tzu, auteur du livre "*l'art de la guerre*", donne comme définition de la désinformation comme l'acte de duper: "*la guerre à le mensonge pour fondement et le profit pour ressort*" (chapitre 7).Ce même livre fut l'un des premier ouvrage connu à donner les principes de la désinformation, alors principalement appliqué en temps de guerre.

on peut ainsi lire les **quatres fondements suivants**:

- ❏ Discréditer tout ce qui a de bien dans le pays adverse.
- ❏ Impliquer les représentants des couches dirigeants du pays adverse dans des entreprises illégales. Ébranler leur réputation et livrez les le moment venu au dédain de leur concitoyens.
- ❏ Répandez la discorde et les querelles entre les citoyens du pays adverse.
- ❏ Exciter les plus jeunes contre les plus vieux. Ridiculisez les traditions de vos adversaires.

On peut la définir plus en détail par l'acte de diffuser délibérément une **information fausse**,une **information déformé**, ou une information vraie mais présenté d'une manière spécifique afin de f**ausser une décision**, **manipuler une opinion** ou **déformer** une vérité.
C'est ici qu'on retrouve les actions comme la **propagande**,la **censure** ou l'**usage de faux documents**. L'**opération Fortitude**, par exemple, est un cas de **désinformation**, où une information à été construite de toute pièce et diffuser de sorte à ce qu'elle soit visible afin de fausser **le processus de décision** de l'ennemi.

L'objectif ici est donc l'insertion de **données volontairement fausses**, mais **suffisamment crédible** pour ne pas lever de suspicion, dans un **système d'information** adverse tout en permettant de diriger ou pousser la ou les cibles dans une situation qui sera profitable.

Il est important de faire la **différence** entre des actes comme de la **publicité**, qui va chercher surtout a, du moins à leur base, **suscité un intérêt** afin de pousser les un public cible à adopter à un comportement (acheter un produit, suivre une personnalité…) en mettant en avant les avantages du produit et de la **désinformation**.
Si la ligne est fine entre, par exemple, **publicité** et **propagande** (dans les deux cas, on cherche à modifier l'opinion ou le comportement, et elles vont souvent se basés sur les mêmes leviers psychologiques pour y arriver), la **différence** tient dans leur **utilisation** et la **réglementation**:
La **publicité** cherche plus à **convaincre** de faire le choix de ce produit pour les avantages qu'il présente, la **propagande** est plus souvent utilisé pour convaincre le public ciblé **qu'il n'a pas le choix** et qu'il s'agit de **la seule solution possible**, ou que le choix qui a été fait pour lui est le meilleur.
la **publicité** est soumis à des **lois**, afin d'éviter des abus et de tomber dans de la **propagande** (la publicité pour des produits alcoolisés est soumise à la loi Evin, qui lutte contre le tabagisme et l'alcoolisme, par exemple).

La **désinformation** donc un acte qui utilise largement les différents **vecteurs technologiques**, mais cherche surtout à effectuer un **poid** dans **l'esprit humain**. Une rumeur peut très rapidement se répandre comme une traîné de poudre sur un réseau social (surtout si on souhaite qu'elle se répande et que on sais où la diffuser pour optimiser sa communication), mais elle n'a que comme cible un groupe plus ou moins larges de personnes.

Elle autant **pratiquée** en temps de **guerre** que de **paix**, et si les préceptes de la désinformation de "l'art de la guerre" étaient surtout centré sur un conflit ouvert entre deux nations, ils ont été aussi appliqués dans des **guerres commerciales** ou en **marketing**. Le schéma d'un acte de désinformation est alors plus ou moins le même, bien que il doit s'adapter au **contexte social**, **politique** et **technique**.

Un client va effectuer une demande, **financer** et **majeur bénéficiaire** de l'action. Ce client peut être une personne individuel, une société ou un état. Dans la majorité des cas, le client va préférer rester en retrait, ne souhaitant pas que **l'acte soit associé à son nom**. Il va donc passer par un **intermédiaire**.

Ce dernier va être **l'agent**. C'est donc lui qui va **gérer et concevoir** l'opération de désinformation, et, si jamais elle échoue, va être pris comme responsable. L'agent va donc étudier **les leviers psychologiques** qu'il va devoir utiliser pour mener l'action à bien, en prenant en compte le c**ontexte politique et sociale**, et la **population ciblée**. Une fois les leviers choisis, il choisit le t**hème et le support** qu'il compte utiliser afin d'optimiser la **diffusion du message** et la **crédibilité** de ce dernier.
Ici, deux choses sont à signaler:

- **Le message et sa crédibilité:**

dans les deux cas, avoir les **bonnes informations** et **bonnes données** sont des **éléments importants** afin de s'assurer d'un **message efficace et crédible**. Cela peut donc nécessité une **action de fouille**, comme l'utilisation d'un **lac de données** pour trouver une information utile, ou/et, dans certains cas, de **l'espionnage** si nous souhaitons effectuer une action de d**ésinformation offensive**: attribuée des **crimes à un état**, par exemple. Durant le *procès de Nuremberg*, L'URSS a accusée la mort d'officiers polonais à la Wehrmacht (l'armée du IIIème Reich), elle a produit un ensemble de fausse preuves, en se basant sur les procédés de la Wehrmacht pour les construire. Finalement,le 26 novembre 2010, La Russie reconnaît la mort des officiers comme étant de la responsabilité de L'URSS.

- **Les leviers psychologiques:**

On entend par "*leviers psychologiques*" les différentes **méthodes** qui vont être utilisés durant la **conception du message** pour provoquer les réactions voulus: Faire naître **le doute**, **la peur**, ou une trop **grande confiance**, par exemple.

Cela peut aller de l'utilisation des couleurs, la mise en forme du message, à son champ lexical, dans le cas de **propagande**.
Si on reprend l'exemple des mort d'officiers polonais: Les cadavres (environ 4 500 corps d'officiers polonais) ont été mis dans des charniers dans la forêt de Katyn. La Wehrmacht les découvrit en août 1941, alors qu'elle commençait à pénétrer dans le territoire de l'URSS. Signal,alors hebdomadaire de l'allemagne Nazie, publia de nombreuses photos de l'exhumation des corps pour exploiter les sentiments associés à cette macabre découverte afin de justifier le conflit entre le IIIème reich et l'URSS.
A nouveau dans le livre de "*l'art de la guerre*", Sun Tzu conseille de repérer les espions ennemis et les garder en vie: "*vous devez supposer que l'ennemi aura aussi les siens. Si vous venez à les découvrir, gardez-vous bien de les faire mettre à mort ; leurs jours doivent vous être infiniment précieux. Les espions des ennemis vous serviront efficacement, si vous mesurez tellement vos démarches, vos paroles et toutes vos actions, qu'ils ne puissent jamais donner que de faux avis a ceux qui les ont envoyés.*" dans cette exemple, la **désinformation** effectuée va mettre en place un **levier psychologique** qui sera plus proche d'un faux "*persona*" (un persona est un concept de **psychologie** qui désigne le comportement adopté par un individu face à un autre ou à la société. Il s'agit d'une sorte de "*masque social*") afin de **fausser les rapports de l'espion**. En d'autre terme, on insère des **données fausses**, construite de toute pièce, afin de **tromper l'espion**, rendant son **rapport faux**, et poussant l'ennemi à adopter un comportement qui nous avantage.

Finalement, l'opération de désinformation va utiliser des **relais** afin de diffuser le message. Il va s'agir des systèmes d'information utilisés. Par des **réseaux sociaux**, **journaux**, **radios** ou **télévision**, par exemple. Le message, si il est correctement construit, va être repris, amplifié et transmis sur ces **relais**, et même repris sur d'autres. Par exemple, une rumeur lancée sur les réseaux sociaux (facebook, twitter, etc…), qui va être repris par les utilisateurs, amplifiés, pour finir par apparaître en tant que articles sur les sites internet des médias.

b) subversion

La définition du concept de **"subversion**" ne fait pas partie de celle qui sont universellement acceptée, si bien que il en existe plusieurs:

"*la subversion est la dégradation ou la dissociation des loyautés de groupes politiques et sociaux importants au sein de l'état ciblé, et de leur transfert, dans les conditions optimales, vers les symboles et groupes de l'agresseur*"("*The Strategy of Subversion: Manipulating the Politics of Other Nations"*,Paul W. Blackstock,1964)

"*Subversion-Actions visant à miner la force militaire,économique,psychologique et/ou politique ainsi que le moral d'une autorité dirigeante*"("*Dictionary of Military and Associated Terms*",département de la défense américaine)

"*La subversion est une activité destructive et agressive visant à détruire un pays, nation ou une zone géographique de votre ennemi en démoralisant les valeurs culturels et changeant la perception de la réalité de la population*"("*Soviet Subversion of Western Society"*,*Yuri Bezmenov(Ex-KGB)*,1983)

Cependant, **l'idée** qui se retrouve dans les différentes définitions est l'**objectif d'affaiblissement** d'un ou plusieurs **pouvoirs d'un état** (ou du moins, d'un regroupement organisé d'un grand nombre de personnes ayant une hiérarchie et des valeurs ou culture commune) et de la **démoralisation des membres** de cette état (ou groupe).

Il va s'agir d'une méthode souvent utilisé en cas d**'asymétrie des rapports de force** (un petit groupe d'influence entrant en conflit avec un gouvernement, par exemple), et elle va **agir sur l'opinion** par effet de "*pourrissement*" (entendre par là que la subversion va chercher à noircir l'opinion vers la force au pouvoir, le "*pourrir*").
En d'autres termes. **Le pratiquant de la subversion** (ou l'**agent subversif**) va tenter de faire naître une forme de **discorde** entre les membres du groupe ciblé, en visant les différents éléments qui le compose et qui sera jugé comme "*pilier*",comme l'**autorité**, **la culture** ou **les valeurs de la cible**. Les objectifs sont de **diviser**, **diminuer le morale et la confiance**, et **convaincre** que le pratiquant est de **bonne foi**, en appelant à la justice et la liberté.

La subversion va donc utiliser des **mécontements** déjà présent dans le groupe,les **problèmes** existants ainsi que de la **psychologie sociale** pour **diviser un groupe** et le **détruire** (ou du moins le diminuer) de l'intérieur. En cela, elle est considérée comme **agressive et non constructive**, à la différence d'une révolution, qui cherche à mettre en place un nouveau système. Il est possible de considérer l**a subversion** comme une forme d'application du "*diviser pour mieux régner*".
C'est pour cette raison que elle est utilisée quand les forces en présences sont asymétrique. Face à entité plus forte, un groupe va chercher à créer la discorde en son sein.

Pour arriver à ceci, le processus reste très proche de celui de la **désinformation**, si ce n'est que l'objectif n'est pas de **tromper un adversaire**, mais de **diviser un groupe**. Posséder les **bons renseignements**, voir créer des i**nformations fausses mais crédibles**, utiliser les systèmes de communications de masse pour **atteindre individuellement et simultanément**, et la création de **message** faisant appel au **sentiments** et à l'**irrationalité** reste les éléments centraux d'une opération de subversion.

L'agent subversif, une fois qu'il aura commencé son opération, va pouvoir **utiliser toute critique** ou **action** envers lui à son avantage, en les diabolisant. Il exploite les **idéaux et valeurs** (universels ou celle qui sont déjà présente dans le groupe) à son **avantage**, pour remettre en doute chacune des **décisions** et **actions** des "*piliers*" de la cible. Une tentative de destruction de ces affiches sera associé à de la censure, les avis contraire au siens seront répété et déformé.

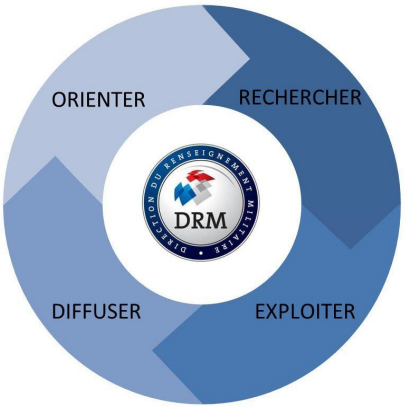
c) renseignement

On parle de **renseignement** pour définir l'ensemble des **activités consacrées** au traitement des **informations**, et, par extension, l'ensemble des **organismes** qui se consacrent à ces **activités**.Il va s'agir d'une des activités principales dans la **guerre de l'information**. Difficile d'effectuer une action de désinformation efficace sans savoir sur quelle information se baser, quelle point faible exploité ou comment est organiser l'acteur.

Une **activité de renseignement** est souvent issu d'un **besoin**. Face à une situation, avant d'effectuer une décision ou simplement pour s'assurer que l'organisation fonctionne correctement, il y a un besoin d'informations pertinente, d'où la présence, par exemple, des multiples organismes gouvernementaux de renseignements.
Ce besoin est donc autant présent en l'absence de conflit (il s'agit alors de rester au courant de ce qui se passe autour de soi pour prendre les meilleurs décisions possible), que en cas de tension ou de conflit (savoir comment fonctionne l'autre, ces prochaines actions ou ces objectifs.).

L'activité de prise de **renseignement** possède son propre cycle, appelé communément "*le cycle du renseignement*". Il peut varier entre pays et organisme, mais on retrouve cinq étapes:

- ❏ L'expression du besoin de renseignement par l'établissement d'un plan définissant ce qu'il faut surveiller.
- ❏ La collecte des informations.
- ❏ Le traitement des informations brutes. On évalue leur perterniences, on les regroupes et recoupe entre elles et avec les informations déjà connu.
- ❏ L'analyse, ou on transforme les informations en renseignements exploitables.
- ❏ la diffusion des renseignements. Souvent sous forme de rapport quotidiennes, on va chercher à équilibrer la quantité de données avec la qualité de celle ci.



(fig 12, exemple du cycle de renseignement. Issu du site www.defense.gouv.fr, concernant le fonctionnement de la direction du renseignement militaire)

L'activité du renseignement va donc chercher **l'information**. Pour cela, elle possède différentes sources:

- **Sources libres**

Il va s'agir de toutes les **informations** qui sont disponibles dans **l'espace public**. On retrouve donc les journaux, site web, documents universitaires, livres,etc…
L'obtention de l'information à partir de sources libres **la plus simple à effectuer**, mais est aussi la plus complexe à analyser dû à sa nature. En plus de la **quantité importante** d'informations brutes facile à trouver, une attention particulière doit être présente dans son analyse, afin de s'assurer de la **pertinence des données obtenues**,et de leur **fiabilité**.

La tâche de r**ecoupage** entre elles en devient plus importante, afin de s'assurer du minimum de contradiction entre les différentes sources pour déterminer les données fiables.

Les sources libres servent surtout de **première recherche** afin de s'orienter et de se documenter sur des sujets ou des événements inopinés. L'avantage, en plus de leur quantité, et la diversité des sources, permettant d'avoir des perceptions différentes, et **orienter les collecte suivantes**. Elles permettent aussi de se constituer un ensemble de fond **documentaire rapidement**, effectuer une **veille efficace**, pour peu qu'il à été défini des secteurs de vigilance et des sources libres fiable. Par exemple, il est possible de se baser sur des sources libres pour obtenir la cartographie d'une zone, l'ethnie et langue d'une population ou les infrastructures public au alentour.

- **Sources humaine**

Toutes les informations issu d'un **individu**. Cela concerne les simples questions posé à un habitant, un interrogatoire,les remontés d'informations issu d'individu sur la zone concerné, l'avis d'un spécialiste sur un sujet spécifique ou un rapport.

C'est dans ce genre de source que on retrouve les tâches comme l'**espionnage** ou la **reconnaissance de terrain** d'un éclaireur militaire. Selon le type de sources humaines, la collecte peut faire face à plusieurs **problèmes**: la **coopération** de l'individu,sa **connaissance**,sa **fiabilité** et celle de l'**information obtenu**.

Si on prend un exemple simplifié. Demander à un habitant d'une ville où se trouve la station essence la plus proche. On peut s'attendre à ce que l'habitant nous donne l'information de bonne volonté (**coopération**), connais bien la ville (**connaissance**), soit en état de nous répondre (**fiabilité de l'individu**) et ne se trompe pas (**fiabilité de l'information**).

En prenant l'exemple inverse, si les informations sont issu d'un interrogatoire d'un prisonnier de guerre, il est possible qu'il refuse de répondre (**aucune coopération**), ne connaisse pas la réponse à la question (**aucune connaissance**), soit trop désorienté (**peu fiable**) ou possède des informations qui sont volontairement fausse (l'**information n'est pas fiable**).

A ces premiers **problèmes** peuvent aussi s'ajouter les **risques** dans le cas d'un contexte tendu, voir de guerre ouverte. Un **individu** s'introduisant dans un **environnement inconnu** peut prendre du temps,et doit faire attention à ces actions au risques de faire face à de la méfiance et des soupçons. L'agent, alors présent dans l'environnement, peut courir un risque physique évident, en plus d'un risque diplomatique. Finalement, il peut obtenir des informations fausses, volontairement laisser à sa disposition afin que son rapport soit faux.

Cependant, une **source humaine** à aussi **ces avantages**. Les informations peuvent être **rapide à obtenir** (il est plus parfois plus simple de simplement poser la question à une personne maitrisant le sujet), et un individu reste capable d'**agir en autonomie**, **interpréter** et **analyser les informations obtenues** et s'**adapter en conséquences**.

- **source technologique**

Toutes les **sources d'informations** issu de **signaux électromagnétiques**, **systèmes d'informations électroniqu**es, les **informations visuels obtenues par moyens techniques** (video surveillance, image satellite) et les **données mesurables** (énergétiques,sons, mouvements, etc…). Selon le domaines, il existe différents types d'activités de renseignements: militaires, économiques, de sécurité, informatiques,etc...

d) gestion de la perception

Mao TseTung, ou Mao Zedong, Chef militaire chinois ayant participé à la guerre sino-japonaise(1937-1945), à déclarer "*dans le but de d'obtenir la victoire, nous devons faire de notre mieux pour sceller les yeux et les oreilles de l'ennemi, le rendant aveugle et sourd, et créer la confusion dans l'esprit des commandants ennemis, les rendant fou.*"("*on the protracted war"*,1938).

Cette déclaration est ce qui se rapproche plus de la **gestion de la perception** dans le domaine de l**'infoguerre**. L'objectif n'est pas de manipuler l'information en elle même, mais la **perception** que l'ennemi en a, afin qu'il n'y prête pas attention, ou à l'inverse, se concentre sur une information vraie, mais sans intérêt.

Supposons qu'un groupe A possède une source d'information qui lui donne un avantage sur le groupe B. Si B souhaite limiter cette avantage, il peut essayer de manipuler la perception de l'importance de la source de A. B va alors chercher à manipuler la manière de voir la source de A. Pour cela, B va devoir connaître le processus de perception de A, et donc connaître les paternes associé à la perception d'un élément.

Cette manipulation peut se présenter sous la forme d'un attaque de envers la **perception** d'un adversaire, en brouillant volontairement **les paternes** afin qu'il soit incapable de trouver une logique, ou à l'inverse, **créer volontairement des paternes** pour tromper l'adversaire et le forcer à réagir d'une certaine manière.

2. aspect technologique

a) C4ISR

C4ISR est un raccourci effectué pour représenter un ensemble de fonctions militaires. Les **quatres C** ("*Computerized Command,Control,Communications*"), **le renseignement militaire** ("*Intelligence*"), **la Surveillance** et **la Reconnaissance**. Il s'agit des **systèmes**, **procédures** et **techniques** utilisées pour **collecter** et **diffuser** l'**information**, diviser en plusieurs domaines qui travaille en synergie afin de diffuser efficacement l'information sur un théâtre d'opération.

Le "*Computerized Command and Control*" n'a pas une définition précise qui est accepté de tous, mais on considère généralement qu'il s'agit du domaine dont sont issu les ordres et d'où sont issu les décisions.
Les communications est le domaine de la transmission d'information.
Le renseignement militaire fait référence au domaine du traitement de l'information utile concernant la mission, ou pouvant servir l'organisation effectué pour accomplir l'objectif.

La surveillance est l'observation des activités et comportements des forces en présence de différentes manières afin de les donner au renseignement.
La reconnaissance, domaine différent de la surveillance, est l'utilisation de personnel ou d'équipement dans les zones inconnues pour obtenir des renseignements.

L'objectif final d'un système **C4ISR** est de permettre d'**améliorer la conscience de l'environnement** et de **la situation d'une opération**, afin d'offrir l'i**nformation pertinente** rapidement pour prendre **les meilleurs décisions**.

Ce genre de système nécessite des **senseurs**, **ordinateurs** et **système de communication** capable de collecter les renseignements des différentes zones, qui peuvent être autant terrestre, aérienne ou maritime.À ceci, elle peut être aussi récupérer les images satellites de l'environnement.

Il s'agit d'un **centre de commandement**, devant gérer de multitude d'informations qui peuvent être cruciale pour les futurs décisions. Dans le cadre d'une guerre de l'information, il s'agit d'une cible de choix si nous souhaitons perturbé le système de communication adverse.

b) Informatique

Comme dit plus haut, **la guerre de l'information** est revenu au devant de la scène grâce à l'émergence de l'**informatique**.
Nombreux s**ystèmes d'information** se base sur de l'informatique, si bien que une guerre de l'information va aussi se dérouler via un tel support. A ce titre, de nombreuses actions autant pour **obtenir l'information** (piratage d'une boîte mail, par exemple), **détruire un système** (Virus, attaque par dénis de services, destruction physique), **prendre le contrôle d'un système** (obtenir les mots de passes administrateur ou Root selon la nature du système) que pour **protéger le système** (mise en place de par-feu, détecteur d'intrusion) ou **protéger l'information** (chiffrement) sont effectués autour des systèmes d'information.

Cette forme de guerre de l'information (appelé "*cyberguerre*") est d'autant plus dangereuse qu'elle efface la l**imite géographique** et est **facile d'accès**. Un pirate informatique possédant les connaissances suffisantes pourra facilement trouver les outils nécessaires sur Internet pour se construire une boîte à outil, l'utiliser de n'importe où et rendre complexe la détection de l'origine de son attaque, voir même de l'attaque en elle même, avant qu'elle puisse atteindre son objectif où effectué des dommages.

Si il existe des multitudes de manière de prendre d'assaut un système d'information informatisé (déni de service,la virologie,qui possède en elle même différentes formes de virus, détournement, exploitation de vulnérabilité d'un système ou logiciel, "*man in the middle*", etc...) on peut les catégoriser en quatre types:

- **Attaque à l'aide de données:**

Insertion de données corrompu ou mal formé pour provoquer le mauvais fonctionnement du système (le "*Ping of death*", par exemple. On peut aussi mettre la virologie dans ce type d'attaque).

- **les attaques à l'aide logiciels:**

Chargement de logiciels dans des systèmes qui vont entraîner leur mise hors service ou effectuer des fonctions différentes de celles auxquelles ils sont destinées (un ordinateur zombie, par exemple)

- **prise de contrôle:**

La prise de contrôle de la totalité ou d'une partie du système pour pouvoir manipuler son fonctionnement, voler des ressources ou des données, ou causer d'autre forme de dommage (vol du mot de passe administrateur, "*brut force*").

- **l'écoute:**

La mise en place d'un agent afin d'écouter les communications dans le système. Sans nécessairement en prendre le contrôle, les informations qui transite dans le système sont surveiller et récupérer (détournement).

A ceci, on peut rajouter les attaques physiques, qui consiste la destruction physique de l'équipement composant le système d'information.

D. exemple de guerre d'information

Pour finir cette état de l'art sur la guerre de l'information, quelques exemples vont être présentés afin de pouvoir se représenter concrètement ce qu'est une une guerre de l'information. Pour cela,il sera présenter des situations issu de la seconde guerre mondiale et de la guerre froide.

1. seconde guerre mondiale

La seconde guerre mondiale fut l'un des premiers conflits où l'information fut aussi capitale et utilisé. Cela peut s'expliquer par le fait de la présence de la Résistance, s'engageant alors dans un conflit asymétrique où elle était en position de faiblesse, mais aussi par l'opération "*Bodygard*", ou ENIGMA.

a) La résistance

En premier lieu, la communication entre résistants. Dû à leur situation, ils se devaient à la plus grande prudence, si bien que toute potentielles informations se devait d'être codé. Cela leur permettait d'utiliser des systèmes de communications public (comme la radio), en faisant passer des messages aux allures innocentes qui se relevait être un message codé.

Ensuite, de nombreuses actions étaient effectué autour de l'information. L'espionnage était de mise, et les Alliées utilisaient régulièrement la Résistance pour obtenir des informations concernant les mouvements de troupes, l'emplacement de ressources ou d'infrastructure stratégiques, ou la présence de personnalité importante de l'armée allemande.

Lors du débarquement en Normandie, de nombreux système de communications Allemand furent saboter, voir détruit par les résistants.

b) Enigma

Enigma est un système de chiffrement utilisé par les systèmes de communication allemandes pour chiffrer les messages. Réputée inviolable, cela n'a pas empêcher une équipe de mathématiciens britanniques, notamment Alan Turing, aidé par le service de renseignement français ayant récupéré la documentation de la machine, de réussir à déchiffrer les messages, offrant un avantage en terme d'information non négligeable.

c) opération "Bodygard"

Cette opération a été mis en place par les alliés durant la seconde guerre mondiale, dans l'objectif de tromper le haut commandement de l'Axe concernant le jour et l'endroit du "*D-Day*", et à constituer à de multiple sous-opération de duperie. Nous pouvons retrouver les opérations "*Fortitude*", "*Ironside*", "*Graffham*", "*Royal Flush*", "*Zeppelin*" et "*Copperhead*". Chacun de ces différents plans avaient comme objectifs de tromper l'ennemis sur de multiple détails. "*Fortitude"* devait fausser la taille des forces alliées pour faire croire à une invasion sur le Pas de Calais et la Norvège.
"*Irionside"* fut lancé après l'interception de communication indiquant que le commandement allemand craignait une attaque vers Bordeaux. Les alliées ont décidé d'utiliser ces craintes à leur avantage, et mis en place trois agents doubles ("*Tate*","*Bronx*" et "*Garbo*") afin d'appuyer ses craintes.
"*Graffham"* et *"Royal Flush"* avaient comme objectif de faire croire que les Alliées tissaient des liens politiques avec la Suède, en préparation de l'invasion depuis la Norvège.
"*Zeppelin*" possédait le même objectif que "*Fortitude"*, mais pour la Crête et la Roumanie. Cette opération à simuler de faux exercices et communication radio afin de faire croire à l'existence de la neuvième,dixième et douzième armée.
Finalement, l'opération *"Copperhead"* fut la dernière effectuée, un jour avant le "*D-Day"*. L'objectif était de tromper le haut commandement Allemand sur la position de Bernard MontGomery, alors l'un des commandants les plus connu des Alliées. Pour cela, l'acteur Clifton James, qui possédait une ressemblance frappante avec le commandant, joue le rôle de ce dernier et fit plusieurs apparitions publique à Gibraltar et dans l'Afrique du Nord, laissant penser à une attaque via la Méditerranée.

2. guerre froide

La guerre froide c'est fait confronté les deux superpuissance issu de la seconde guerre mondiale, entre les Etats-unis et l'URSS. L'affrontement, dans le cadre de la guerre de l'information, c'est fait à coup de propagande et d'espionnage.

E. conclusion

Dans cette seconde partie de l'état de l'art, nous avons pu voir un peu plus en détail ce qu'était **la guerre de l'information**, son **fonctionnement** et **ces acteurs**. Si elle est issu d'ancienne stratégie de guerre, son **évolution** à accompagner celle des **technologies**, si bien qu'elle en devient **indissociable**. Elle exploite de nombreux **ressorts psychologiques** et **technologiques**, mais possède un nerf de guerre très commun à l'intelligence artificielle, la donnée, qui sera transformée en information ou renseignement.

L'objectif de l'**infoguerre** reste et restera toujours de **tromper son adversaire**, afin d'en obtenir un avantage. Cependant, si on parle de "*guerre*", il ne faut pas oublier qu'elle dépasse cette notion de conflit entre état. Une infoguerre peut être effectué entre différents acteurs, et ces derniers peuvent participer de manière différentes.

VI. Bibliographie

A. documents

- *Iliade*, chant 18,page 418-419
- *The Art and Logic of Ramón Llull: A User's Guide*, Brill, 2007
- *The Laws of Thought,*1854
- *Computer Science as Empirical Inquiry:Symbol and Search*, 1976
- *Mind Children*, 1988
- *A proposal for the dartmouth summer research project on artificial intelligence*,1955
- *Artificial Intelligence: A Modern Approach,2009*, Stuart J. Russell et Peter Norvig
- *Some studies in machine learning using the game of checkers*,2000, A.Samuel
- *Commonsense Reasoning and Commonsense Knowledge in Artificial Intelligence*,2015, Ernest Davis et Gary Marcus
- *Human Problem Solving*,1972,A.Newell et H.Simon
- *Realization of a geometry-theorem proving machine*,1959, de Herbert Gelernter
- *IBM's Early Computers*, Harles J. Bashe,Lyle R. Johnson,John H. Palmer,Emerson W. Pugh, 1986
- *AI: The Tumultuous Search for Artificial Intelligence*,1993 par Daniel Crevier
- *machines Who Think*,2004
- *A relational Model of Data for Large Shared Data Banks*, 1970
- *Perceptrons*, 1969
- *what computers can't do*,1972
- *Reducibility Among Combinatorial Problems*,1972
- *Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence*,2018 de Andreas Kaplan et Michael Haenlein
- *Artificial-Intelligence-A Modern Approch*,3rd Edition,2016
- *Empirical Methods for Artificial Intelligence*,1995
- *Probabilistic Reasoning in Intelligent Systems*,1988
- *Unsupervised word sense disambiguation rivaling supervised methods*,1995
- *A Survey of Artificial General Intelligence Projects for Ethics, Risk, and Policy*,Seth Baum,2017
- *Artificial Intelligence:Structures and Strategies for Complex Problem Solving",George Luger,William Stubblefield*,2004
- *Turing Test as a Defining Feature of AI-Completeness*,Roman V. Yampolskiy,2012
- *Connectionist Temporal Classification: Labelling Unsegmented Sequence Data with Recurrent Neural Networks*,2012,Alex Graves,Santiago Fernandez,Faustino Gomez,Jurgen Schmidhuber
- *Google's Neural Machine Translation System: Bridging the Gap between Human and Machine Translation*,2018
- *Artificial Intelligence and Games*,2018,Georgios N.Yannakakis et Julian Togelius
- *Fuzzy Logic in Artificial Intelligence*,1997,Erich P. Klement,Wolfgang Slany

- *Bayesian Networks in Medicine : a Model-based Approach to Medical Decision Making*,Lucas Peter,2001
- *Speech recognition with mixtures of bayesian networks*,Microsoft Corporation,2002
- *La guerre de l'information I,*Lieutenant Paul Scimar
- *La guerre de l'information II,*Lieutenant Paul Scimar
- *L'art de la guerre*, Sun Tzu

B. Site Internet

- https://www.academia.edu/38587573/What_the_Near_Future_of_Artificial_Intelligence_Could_Be
- https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/what-ai-can-and-cant-do-yet-for-your-business
- https://www.theverge.com/2016/10/10/13224930/ai-deep-learning-limitations-drawbacks
- https://medium.com/@InDataLabs/3-major-problems-of-artificial-intelligence-implementation-into-commercial-projects-6ead79e97088
- https://towardsdatascience.com/the-real-reason-ai-is-difficult-10b64a230c5e
- https://www.academia.edu/11981255/ARTIFICIAL_INTELLIGENCE_Lecture_Note_1_INTRODUCTION
- https://fr.scribd.com/document/61928377/Ai-Mundane-Task
- https://openclassrooms.com/fr/courses/4470406-utilisez-des-modeles-supervises-non-lineaires/4732186-empilez-les-perceptrons
- https://blogs.oracle.com/bigdata/machine-learning-data-lake
- https://solutionsreview.com/data-management/4-data-lake-tools-vendors-to-watch-in-2018/
- https://blogs.oracle.com/bigdata/data-lake-database-data-warehouse-difference
- https://blogs.oracle.com/bigdata/whats-a-data-lake
- https://azure.microsoft.com/fr-fr/blog/the-intelligent-data-lake/
- https://medium.com/datadriveninvestor/getting-ready-for-ai-a-data-lake-or-a-big-swamp-273b0c6ebb6e
- https://www.zdnet.com/article/why-ai-machine-learning-is-driving-data-lakes-to-data-hubs/
- https://www.lebigdata.fr/intelligence-artificielle-et-big-data
- https://www.goodai.com/about
- https://consumer.huawei.com/en/campaign/ai-for-good/
- https://www.bbntimes.com/en/companies/6-challenges-of-artificial-intelligence
- https://www.mckinsey.com/featured-insights/artificial-intelligence/the-promise-and-challenge-of-the-age-of-artificial-intelligence
- https://futureoflife.org/background/benefits-risks-of-artificial-intelligence/?cn-reloaded=1
- https://infoguerre.fr/2018/05/traiter-de-guerre-de-linformation-opposant-russie-a-loccident/
- https://web.archive.org/web/20100612060533/http://ausairpower.net/Deception-IWC6-05-Slides.pdf
- https://upload.wikimedia.org/wikipedia/commons/3/38/Deception%2C_Disinformation%2C_and_Strategic_Communications.pdf
- https://fas.org/irp/eprint/gough.pdf
- https://www.psychologicalscience.org/publications/journals/pspi/psychopathy.html
- https://www.merriam-webster.com/dictionary/manipulate
- https://en.wikipedia.org/wiki/Psychological_manipulation
- https://en.wikipedia.org/wiki/Mass_communication

- https://web.archive.org/web/20140106052052/https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/eyes_wide_open_v1.pdf
- https://www.mi5.gov.uk/what-we-do
- http://www.cyber-police.org/
- http://www.infosentinel.com/
- http://www.journal.forces.gc.ca/vo3/no1/doc/53-64-eng.pdf
- https://www.thalesgroup.com/fr/worldwide/defense/global-activities-defence-land-forces/c4isr
- https://infoguerre.fr/2001/11/les-principes-de-la-guerre-de-l-information/
- https://armeeinformationstpe.wordpress.com/category/i-2-a-propagande-censure-et-desinformation/
- https://blogs.mediapart.fr/ewoillez/blog/101117/puissance-et-dangers-de-la-desinformation
- https://reseauinternational.net/sun-tzu-et-lart-de-mener-une-guerre-commerciale/
- https://fr.wikipedia.org/wiki/Massacre_de_Katy
- https://www.leretourauxsources.com/blog/la-subversion-roger-mucchielli-n710
- https://www.cairn.info/revue-hermes-la-revue-2016-3-page-80.htm#
- https://www.monde-diplomatique.fr/1961/11/A/24504
- http://media.leeds.ac.uk/papers/pmt/exhibits/746/Friman(1999)PW.pdf