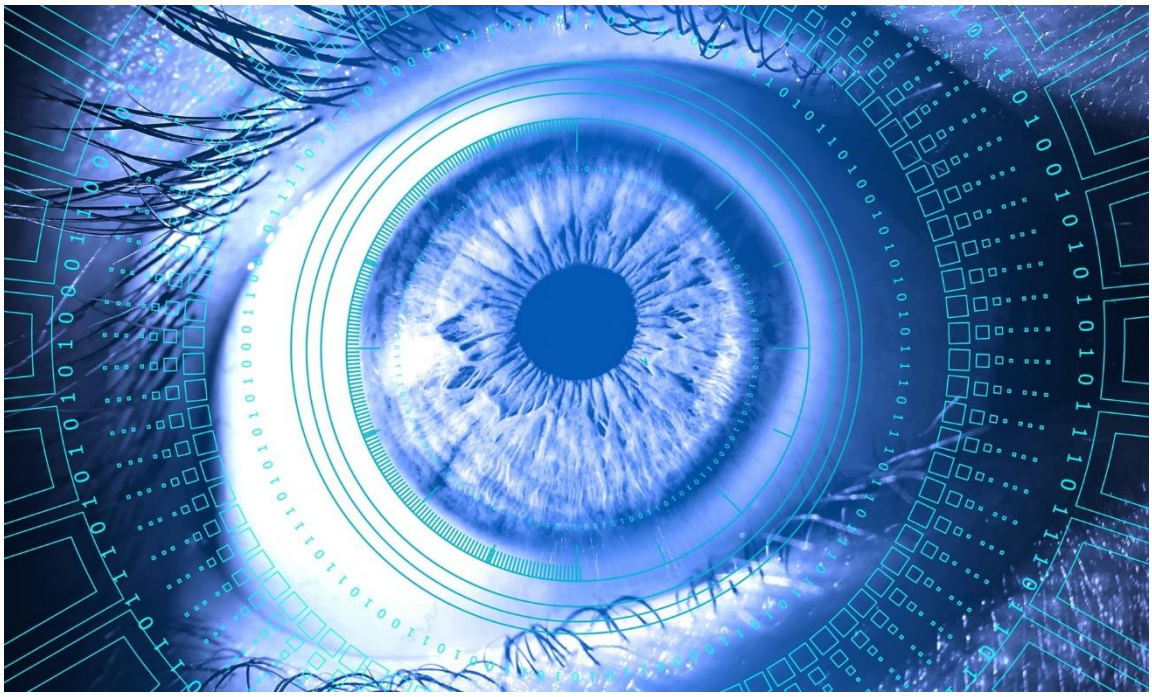
Les Espaces Informationnels Autonomes à l'ère du numérique



« Une grande civilisation n'est conquise de l'extérieur que si elle s'est détruite de l'intérieur. »
Will & Ariel Durant, L'Histoire de la Civilisation 1935 - 1975

Jean-Michel BARBIER
Laurence BAULT
Clément CHEVIGNON
Fabien RENAUDIN

Table des matières

DES ESPACES AUTONOMES A L'ÈRE DE L'INFORMATION 5

Définitions 5

« Espace » 5

« Autonome » 6

« Espace autonome » 6

« Informationnel » 7

« Espace informationnel » 8

« Espace informationnel autonome » 8

Espace informationnel autonome : Principe de fonctionnement 8

Le contexte de Guerre Économique 8

Du besoin de création jusqu'à l'entretien de la raison d'être de l'EIA. 9

Quelle méthode d'analyse appliquer pour comprendre un Espace Informationnel Autonome ? 10

Méthode d'observation 10

Méthode d'analyse structuraliste et organisationnelle 11

Méthode d'analyse systémique 11

Principe et fonctionnement d'un espace informationnel 11

Mise en garde 11

Au cœur de chaque fruit un noyau ou des pépins 12

…en quête de légitimité 13

APPROPRIATION DU NOUVEL ESPACE INFORMATIONNEL 15

Les approches offensives de l'espace informationnel 15

CARTOGRAPHIE D'UN E.I.A 22

L'identité d'un Espace Informationnel Autonome 22

La vision de l'EIA : 22

La gouvernance et structure d'un EIA : 23

Les ressources 26

L'image de « marque » ou son marketing 26

Les effets recherchés au sein d'un EIA 27

Définir la cible en fonction de l'effet majeur recherché 27

Les armes de la guerre de l'information au service des EIA 28

Les objectifs tactiques et l'effet recherché 28

Les actions au sein d'un EIA. 30

Agir « contre » l'information : saboter la chaine de production 31

Agir « pour l'information » : l'espionnage _____ 33
Agir « par l'information » : la subversion _____ 34
Exploiter les biais cognitifs pour influencer _____ 38
Les fondamentaux de l'influence : De nos failles cognitives _____ 39

CONCLUSION _____ ***43***

Introduction

L'amalgame trop souvent fait entre informations, données, savoirs, connaissances, réalités, opinions, vérités, etc., limite l'approche scientifique dans notre rapport à la surabondance informationnelle. Notre rapport à l'information associé aux mécanismes de simplification cognitifs exacerbés par les nouveaux médias numériques permet à de nombreux acteurs d'exercer un poids sensible sur l'interprétation de l'histoire et le déroulement de certains évènements. Au croisement des stratégies d'influence, de guerres informationnelles, de manipulations, de propagande et de techniques de détournement d'usage (hacking), les espaces informationnels autonomes (ci-après dénommés EIA) sont peu connus, mal définis et souffrent de l'absence d'analyse académique.

Pourtant, les activités qui s'y déroulent ont des conséquences réelles sur le quotidien des français. La tentative d'affaiblissement et de discrédit faite à l'encontre du marché de la viande (1er marché agroalimentaire français) en est un exemple, alors que les impacts potentiels sont de nature à menacer toute la filière.

Les contraintes temporelles liées à notre formation ne nous permettent pas de traiter le sujet de manière exhaustive. Nous tenterons ainsi d'éclairer le lecteur sur ce qu'est un espace informationnel autonome et comment l'analyser en proposant une grille de lecture.

Dans un premier temps, nous présenterons ce qu'est un espace autonome. Puis nous introduirons la notion d'espace informationnel. Cette première partie nous apportera les définitions nécessaires à la compréhension du fonctionnement de base d'un **espace informationnel autonome**. Nous proposerons dans cette partie un moyen d'illustrer l'évolution d'un espace autonome dans le temps afin de permettre une analyse graphique de celui-ci.

Ensuite, nous aborderons l'impact du numérique dans les espaces informationnels en commençant par l'évolution des moyens de communication jusqu'à l'arrivée des nouvelles technologies de l'information. Dans cette deuxième partie, nous chercherons aussi à identifier les différentes approches des espaces informationnels selon les principales puissances. Nous nous attacherons à identifier les différences et les particularités que nous pouvons trouver selon les cultures, et apporterons des éléments qui permettront de caractériser un espace informationnel autonome.

Enfin, nous proposerons une première grille de lecture permettant de détecter et d'identifier un EIA. Cette grille qui est une première (aucun outil proche n'a été trouvé dans la littérature) a été conçue de manière à permettre à la fois l'identification et les tactiques employées par un espace informationnel afin de pouvoir être intégrées à une méthodologie de résolution de crise puis d'analyse de crise. En effet, le gain de puissance discret, et l'attaque par surprise sont des caractéristiques communes à la plupart des espaces, c'est donc souvent lors d'une crise qu'on le rencontre pour la première fois.

DES ESPACES AUTONOMES A L'ÈRE DE L'INFORMATION

La notion d'Espaces Informationnels Autonomes est peu connue et souvent mal abordée, car imbriquée dans des concepts fourre-tout tels que les groupes de pression ou les réseaux d'informations. Si l'on utilise les termes « Espaces Informationnels Autonomes » comme mots-clés sur les moteurs de recherche les plus populaires, nous sommes redirigés vers des pages web qui informent sur les centres de documentation… Et ce n'est là qu'une partie de notre sujet, dont le cadre est bien plus vaste.
L'objectif de cette partie est donc de proposer un cadre de lecture commun qui sera utile à la bonne compréhension du lecteur.

Un rapide rappel sur ce qu'est la guerre économique et ses principales composantes nous donnera une idée du contexte dans lequel s'inscrit la conquête des espaces que nous souhaitons aborder. Ce contexte nous permettra de définir les termes et les concepts qui seront abordés tout au long de cette analyse. Qu'est-ce qu'un espace informationnel ? Dans quelle mesure est-il autonome et qu'entendons-nous par informationnel ? De quelle manière un groupe d'individus peut-il se créer et mettre en œuvre un plan d'influence ou de propagande dans un but précis en neutralisant ses opposants ? Comment celui-ci disparaît-il ou reste-t-il intouchable en se prémunissant de toute accusation ?

Définitions

Afin d'appréhender le concept d'espace autonome, il paraît indispensable dans un premier temps de définir chaque terme indépendamment et de préciser de ce que nous entendons par « espace », puis « autonome » pour enfin comprendre ce que l'on entend par « espace autonome ». La notion « informationnelle » sera ensuite adjointe au concept d'espaces autonomes.

« Espace »

Un espace peut correspondre à une étendue, qui peut être mobile. Cette étendue finie implique donc un espace intérieur, un espace extérieur et une frontière qui les sépare.
Le Larousse définit un espace comme « une propriété particulière d'un objet qui fait que celui-ci occupe une certaine étendue, un certain volume au sein d'une étendue, d'un volume nécessairement plus grand que lui et qui peut être mesurée ». Cette définition est large et peut regrouper des notions très différentes en fonction du contexte où elle est utilisée.
Toujours d'après le Larousse, une étendue est la « dimension de quelque chose considéré dans l'espace qu'il occupe ».
Ainsi, un espace fait référence à l'étendue ou à la surface qu'il occupe. Cette dimension n'est pas forcément figée, elle peut évoluer au fil du temps, du contexte et de ses besoins. Elle peut alors se développer et croître ou au contraire se rétracter. Elle peut en outre, se déplacer dans un univers plus grand qu'elle, sans pour autant changer de taille.
Cette étendue est elle-même caractérisée par deux notions indissociables et antagonistes. Pour exister, un espace doit forcément déterminer une structure intérieure et une structure extérieure.
La structure intérieure regroupe des individus qui se rassemblent autour d'un intérêt commun. Cet intérêt peut prendre différents aspects idéologiques, économiques, politiques ou sociétaux…
À l'opposé, la structure extérieure de cet espace représente généralement le reste du monde comprenant à la fois les éléments inertes, les opposants et les cibles éventuelles. Ces deux

espaces sont séparés par une frontière qui est fixe en temps de paix et qui disparaît en période de conflit. Dans un contexte de guerre, les frontières deviennent des fronts qui se déplacent soit dans leurs propres espaces, soit sur celui de leurs adversaires.
Ainsi, en cas de guerre informationnelle, ce même principe s'applique : il s'agit d'installer ses forces, ses idées sur le théâtre d'opérations (politique, culturel, sociétal) de son adversaire ou de son concurrent.

« Autonome »

Pour bien comprendre ce que l'on entend du terme autonome, il convient encore une fois de se référer à sa définition. Le dictionnaire Larousse nous propose : « qui jouit de l'autonomie : un territoire autonome ». Cette définition n'est pas suffisante il convient donc de définir le concept « d'autonomie ». Toujours d'après le Larousse, le mot autonomie fait référence à la : « situation juridique d'une collectivité susceptible de déterminer elle-même tout ou partie de règles de droit qui la régissent ». Dans le cadre des espaces autonomes, la notion juridique introduite dans la définition est à prendre avec prudence, car certains espaces recherchent justement de s'affranchir du juridique. Il semble donc plus pertinent pour comprendre la notion d'autonomie, d'insister sur d'autres aspects qui vont nous permettre de caractériser le terme « autonome ». Pour cela, nous estimons qu'il est nécessaire de comprendre réellement le sens des mots « collectivité » et celui de « déterminer ».
En effet, le mot collectivité représente une caractéristique importante, car il permet d'aborder « le liant » qui maintient un espace cohérent. D'après le Larousse, une collectivité est : « un groupe de personnes, généralement assez étendu, que réunissent un intérêt commun, une organisation commune ou des sentiments communs ».

Le verbe déterminer est aussi à souligner, car il signifie : « Établir quelque chose, le définir avec suffisamment de précision au terme d'une recherche, d'une réflexion, d'une analyse ». Le mot règles correspond, toujours selon le Larousse à « une prescription, de l'ordre de la pensée ou de l'action, qui s'impose à quelqu'un dans un cas donné ».

Ainsi, « autonome » correspond dans le cas de notre étude à un groupe de personnes qui se réunissent dans un intérêt commun et qui sont susceptibles d'établir eux-mêmes leurs propres prescriptions.

« Espace autonome »

Compte tenu des précisions que nous venons d'établir sur les termes « espace » et « autonome ». Un espace autonome est une étendue qui peut être mobile et est caractérisée par trois sous-ensembles : un intérieur, une frontière et un extérieur. L'intérieur correspond au rassemblement d'un groupe de personnes lié par des intérêts communs et bénéficiant de la capacité d'établir eux-mêmes leurs propres règles.

Un élément de comparaison utile pour mieux cerner ce que nous entendons par espace autonome se trouve dans la description qui est faite des Zones Autonomes Temporaires TAZ (H. BEY, 1991). En effet, pour Hakim BEY, ces zones autonomes temporaires n'existent que tant qu'elles restent invisibles des pouvoirs de contrainte ; « La TAZ est comme une insurrection sans engagement direct contre l'État, une opération de guérilla qui libère une zone (de terrain, de temps, d'imagination), puis se dissout, avant que l'État ne l'écrase, pour se reformer ailleurs dans le temps ou l'espace ».

« Informationnel »

La définition du Larousse de l'adjectif informationnel est la suivante : « *relatif à l'information, à sa théorie* ». Bien que très courte, cette approche nous pousse à mieux appréhender le concept « d'information ». Il existe plusieurs définitions du mot information.

La première est la suivante : l' « ac*tion d'informer quelqu'un, un groupe, de le tenir au courant des évènements* ». Cette approche nous permet de comprendre que cette information s'adresse à un groupe d'individu afin de le tenir au courant de quelque chose. Néanmoins, le mot « informer » de cette proposition de définition mérite aussi une description exacte. Toujours d'après le Larousse, le verbe informer signifie : « *faire savoir quelque chose à quelqu'un, le porter à sa connaissance, le lui apporter* ».
Nous pouvons donc définir « l'information » comme étant une action de donner ou de transmettre un savoir, ou de la porter à la connaissance d'un groupe d'individu.
De même, en informatique, le Larousse nous propose la définition d'une information comme étant un « *élément de connaissance susceptible d'être représenté à l'aide de conventions pour être conservé, traité ou communiqué* ». Cette définition nous apporte une notion nouvelle, celle de la mise en forme proprement dite de cette information. Elle peut être conservée, c'est-à-dire stockée, mais elle peut être aussi analysée et transmise.

Une définition alternative du Larousse nous permet d'avancer dans notre démarche de compréhension du sujet. Une information correspond également à « *tout évènement, tout fait, tout jugement porté à la connaissance d'un public plus ou moins large, sous forme d'images, de textes, de discours, de sons* ». Celle-ci vient appuyer et même compléter celle du domaine informatique.

Ainsi, si nous souhaitons faire une définition synthétique, une information est un élément qui est porté à la connaissance d'un groupe d'individus sous différentes formes, supports, *médium*. Dans notre approche, nous prenons cette information comme étant une notion et une connaissance immatérielle, mise à la disposition ou transmise à un groupe d'individus. Néanmoins, cette approche peut se révéler assez réductrice. En effet, nous devons prendre en compte cette notion de l'information à travers le prisme de caractéristiques indispensables à sa compréhension. Il s'agit de :

- Son caractère social : une information est toujours une relation entre un contenu et une personne ;
- Son caractère contextualisé : une même information n'aura pas la même signification en fonction du contexte de sa transmission et de sa réception. Il s'agit du concept de temporalité, de localisation et d'individus recevant cette information ;
- Sa dimension matérielle : l'impact d'une information reste étroitement lié à sa mise forme, son message et aussi de son vecteur de diffusion, le *médium*.[1]

Nous venons de caractériser la notion d'information pour bien appréhender la définition exacte de l'adjectif informationnel. Cependant, nous devons aussi associer cette notion au concept « d'espace » afin de bien comprendre leur association à un EIA.

[1] Théories de Shannon et de Léon Brillouin.

« Espace informationnel »

Ce que nous venons de décrire sur les notions « espace » et « informationnel » nous permet de suggérer qu'un espace informationnel est un lieu public qui peut être à la fois physique et dématérialisé, c'est-à-dire virtuel. Sa raison d'être est de mettre à disposition des ressources informationnelles. Ainsi, il est le lieu de la production, de la conservation du traitement et de la diffusion des informations. Néanmoins, pour que cette mise à disposition et cet échange de l'information se produisent, ils doivent être intégrés dans un réseau et dans un espace informationnel.

Ainsi, un espace informationnel est un environnement ouvert qui peut être physique ou virtuel. Il permet la conservation et la diffusion d'informations sur différents supports. Il peut servir, à la fois, de source d'information, mais constitue aussi un environnement permettant de recueillir, d'analyser, d'élaborer et d'échanger des informations.

« Espace informationnel autonome »

La notion d'espace informationnel autonome (EIA) est une approche récente[2] employée par les milieux spécialisés dans les enjeux de stratégie d'influence et d'intelligence économique, cette notion n'a pourtant pas encore été définie. Cette absence crée une certaine zone de floue, voire même d'incompréhension. Notre approche se propose d'éclairer le lecteur sur cette représentation et les enjeux qui en résultent au sein des domaines économiques, sociétaux et politiques.

Ainsi, un espace informationnel autonome (EIA) est la fusion d'un espace informationnel et d'un espace autonome. De ce fait, grâce à l'approche conduite précédemment pour expliciter ces notions, nous pouvons proposer la définition suivante pour un EIA.

Un espace informationnel autonome est une étendue, physique ou virtuelle, qui n'est pas figée et qui est caractérisée par trois sous-ensembles (un intérieur, une frontière et un extérieur). Le cœur de cet EIA correspond au rassemblement d'un groupe de personnes liées par des intérêts communs et qui bénéficient de la capacité d'établir eux-mêmes leurs propres règles. Ce même EIA permet la conservation et la diffusion d'informations sur différents supports. Il peut servir, à la fois, de source d'information, mais aussi d'un environnement permettant de recueillir, d'analyser, d'élaborer et d'échanger des informations.

Espace informationnel autonome : Principe de fonctionnement

Le contexte de Guerre Économique

Le concept de guerre économique a été créé en 1971 par Bernard Esambert et redéfini par Christian Harbulot et le rapport intelligence économique et stratégie des entreprises – Rapport Marte (H. Martre, 1994). L'origine du concept de guerre économique serait née au XVIe siècle, dans le débat religieux au sein de l'Église Catholique qui devait se positionner par rapport à la Guerre. « *Il s'agit de l'expression majeure des rapports de forces non militaires entre puissances (États, blocs, territoires, groupe de personnes)* »[3].

La guerre économique comprend donc les aspects usuels de la compétition mercantile, mais élargit le conflit au niveau des économies des États et des instances supra-étatiques afin de gagner en puissance et en suprématie. Elle se déroule sur trois théâtres principaux :

- La compétition économique entre les entreprises ou les États, dont les principaux leviers sont décrits dans « *The competitive advantage of nations* » (M.E. Porter, 1990), ouvrage qui a

[2] Atlantico, « Bombarder l'EI en Syrie ne suffira pas, il faudra aussi le faire reculer sur un autre territoire ou il est solidement implanté : les réseaux sociaux. » ; 6 Avril 2016.
[3] Cercle Henry Lagrange – La guerre économique : Définition et application (entretien avec Christian Harbulot) 2016.

ensuite été adapté par le même auteur pour les entreprises (théorie des cinq forces) et qui est désormais complété par la théorie de la création de valeur partagée avec la participation de Mark.R. Kramer dans « *Strategy and Society : The link between Competitive Advantage and Corporate Social Responsibility » (M. E. Porter & M. R. Kramer, 2006)*.

- La manipulation des règles juridiques et normatives ; sujet repris par de nombreuses publications qui traitent de l'accaparement des normes et du contrôle des marchés par la prise davantage sur les limites exigibles, le « benchmark », par les consommateurs ;
- La guerre de l'information par le contenu qui peut prendre différentes formes comme l'atteinte à la réputation ou la manipulation du ressenti par la population ou celle du contexte, afin de mettre en difficulté l'adversaire.

Nous nous intéresserons en particulier à ce dernier théâtre de la guerre de l'information par le contenu qui vise à la fois à maitriser le contexte et donc à influencer la perception du marché, sans pour autant revendiquer sa volonté de conquête. Et par conquête, nous entendons l'accroissement de puissance par l'augmentation de richesse, d'espace marchant, de création de dépendance de l'autre sur un plan durable.

Maintenant que le contexte est établi, nous pouvons aborder le cas particulier des Espaces Informationnels Autonomes.

Du besoin de création jusqu'à l'entretien de la raison d'être de l'EIA.

Prenons l'exemple d'un service de recherche et développement d'une entreprise privée en concurrence avec ses pairs ; l'espace de réflexion, d'expérimentation et de mise au point d'un produit doit se faire dans la discrétion afin de garantir la primauté de l'innovation. Ce besoin de « protection du secret » peut être de n'importe quelle nature (isolement des personnels, des lieux, contrôles d'accès, cloisonnement[4]). À l'opposé, le besoin de connaître sa concurrence et son marché nécessite une veille qui représente une menace pour qui organise une telle gestion du secret.

Dans le cas de notre étude, ce besoin va plus loin, l'objectif premier n'étant pas forcément d'adresser une offre à un marché, mais plutôt de gagner des points de pouvoir ou de puissance sur un marché existant ou en devenir.

On trouvera donc des groupes informationnels qui auront pour objectif de mieux connaître les évolutions d'un secteur et qui travailleront à la fois leur forme et leur réseau pour s'approprier ce secteur et les acteurs qui le composent.

Par exemple dans le secteur du latex, composant essentiel des pneus, des relations entre concurrents avec la participation d'ONG ont eu lieu afin de mieux appréhender l'augmentation future de ces marchés (causé par l'augmentation du niveau de vie général et l'émergence d'une classe moyenne en Asie). Ce groupe informationnel a su trouver son autonomie sur différents plans avec le support des principaux producteurs de pneumatiques qui ont apporté une aide financière, des informations techniques et du temps d'une part, et le WWF qui a apporté les savoir-faire et les relais de son réseau et a permis la mise en commun des réflexions sur la problématique avec d'autres ONG. En découlera par la suite une plateforme pour le latex naturel durable qui acte l'association de ses membres d'une part, et qui occupe la position légitime d'émetteur de « recommandations » et d'éditeur de la « conformité » sur la filière.

4 Arrêté du 30 novembre 2011 qui approuve l'instruction interministérielle n°1300 sur la protection du secret de la défense nationale.

L'originalité de cet exemple se trouve dans l'initiative, par le secteur privé qui a pris le problème en amont (du fait des cycles longs des plantations d'hévéas sources de latex) et dans la sollicitation des parties prenantes par le recours aux ONG environnementales et sociales.
De cette manière, les producteurs de pneus ont innové et se prémunissent d'attaques informationnelles, du moins pour un temps en apportant une illustration concrète de la création d'un espace d'information en quête d'autonomie sur son secteur marchand. Cette création d'un avantage concurrentiel *stricto sensu* reprend les trois axes majeurs de la guerre économique que sont :

- La sécurisation de la compétition économique par l'entente et la coopétition face à d'éventuelles forces disruptives qui viendraient tenter d'accaparer le marché du pneumatique ;
- La sécurisation de la décision relative à la normalisation, par la mise en place d'un espace d'échange autonome qui est force de proposition et qui a pris les devants sur les instances normatives traditionnelles ;
- La sécurisation de l'image et de la parole (guerre de l'information par le contenu) en prenant l'initiative sur la définition des problématiques, la publication des méthodologies de résolutions et de l'expression de l'union consensuelle entre compétiteurs, Société Civile.

Il convient d'admettre que l'ambition de cet espace est principalement de sécuriser le développement d'une filière en prenant l'initiative de l'action sur un territoire vierge. Ce n'est pas toujours le cas et les ambitions des EIA qui peuvent avoir des objectifs de déstabilisation lorsque le territoire informationnel est déjà occupé.

Quelle méthode d'analyse appliquer pour comprendre un Espace Informationnel Autonome ?

Cette question mérite d'être posée afin de se prémunir des biais inhérents à chacune des différentes méthodes d'analyse à notre disposition.

Méthode d'observation

Pour décrire un Espace Informationnel Autonome (EIA), connaître ses composants ainsi que les sujets avec lesquels cet espace interagit, nous ferons appel à l'analyse descriptive qui se contente de décrire les parties en lice.
Une illustration simpliste, mais néanmoins utile consiste à se représenter deux ensembles, deux espaces (A et B) qui ont une limite commune. Cette limite joue le rôle de frontière, et lorsque l'un ou l'autre des espaces souhaite déplacer cette frontière, il y a conflit.
Ces conflits peuvent se matérialiser par la guerre militaire ou par la recherche de puissance *par* la guerre économique. Ainsi un espace cherchera à prendre l'ascendant sur l'autre soit en captant la puissance d'un autre espace par la recherche d'alliés pour renforcer sa puissance propre, soit en appauvrissant l'espace adverse *par* des techniques subversives ou d'encerclement cognitif, afin d'inverser le rapport de force.

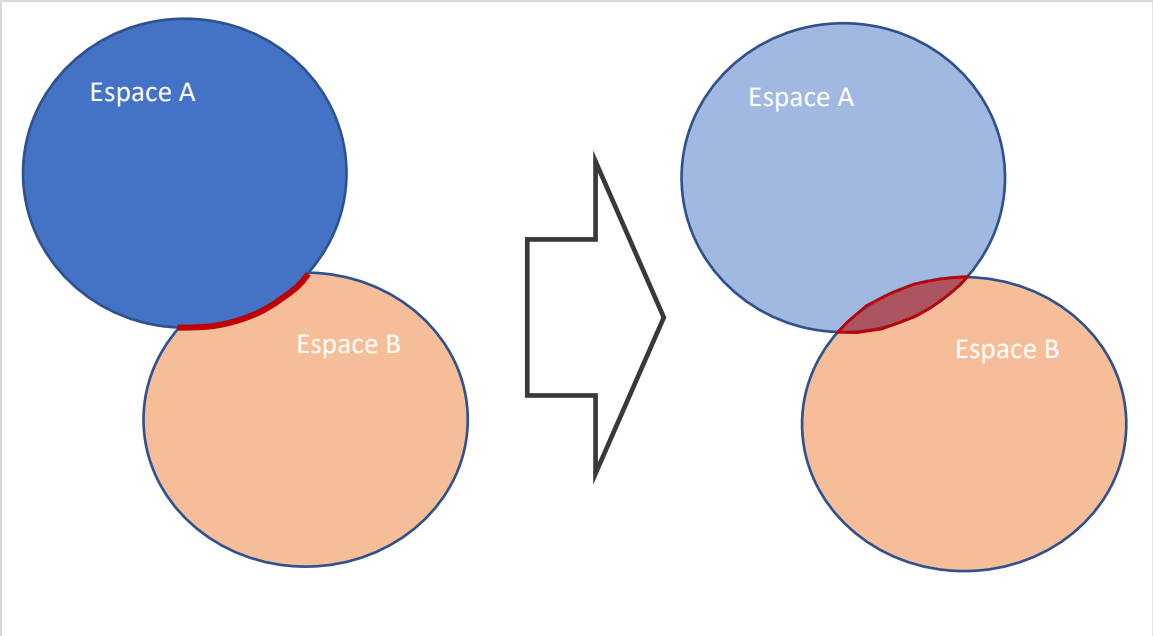


Figure 1 : Passage d'un état stable avec une frontière, à un état de conflit la frontière devient front.

Méthode d'analyse structuraliste et organisationnelle

Avec l'appui de l'analyse descriptive qui permet de porter une première observation et de clarifier certains termes, nous pouvons ensuite aborder le fonctionnement interne d'un espace, sur la base des éléments repris dans la littérature, ainsi que ceux que nous avons recueillis lors d'entretiens. Étant donné que les espaces informationnels autonomes ont en leur sein une partie « cachée », qui leur garantit une certaine invisibilité, il est impossible d'en faire le diagnostic organisationnel complet (Planification / Gestion / Ressources). En revanche, nous pouvons sur la base des retours d'expérience de cas passés, proposer une typologie structuraliste de ces espaces (Lévi-Strauss, 1950) et apporter par la même occasion des éléments permettant d'ouvrir le champ d'investigation.

Méthode d'analyse systémique

Après avoir identifié les éléments constitutifs types de ces espaces informationnels autonomes, ainsi que leurs organisations internes, il devient possible d'aborder leur interaction avec le monde extérieur. Pour cela, il est nécessaire dans un premier temps de faire état des différentes typologies de cibles, pour ensuite prendre en compte les interactions multiples entre les espaces informationnels autonomes et ces cibles. L'approche structuraliste présente un intérêt dans le périmètre d'un scénario d'attaque particulier, mais demeure incomplète lorsque l'on souhaite aborder les espaces informationnels autonomes par leurs interactions multiples avec le monde extérieur.

Principe et fonctionnement d'un espace informationnel

Mise en garde

Si la notion de guerre de l'information par le contenu commence à émerger auprès du public, en particulier avec l'arrivée des fake-news[5] (fausses nouvelles) et de l'industrialisation de la manipulation des masses avec le scandale de Cambridge Analytica ; la notion d'espace informationnel autonome reste peu connue.

5 Bien que le terme fake-news est le plus communément admis, nous préférons la notion de désinformation qui nous semble plus en accord avec les objectifs visés.

En effet, à chaque nouvelle annonce de manipulation ou de propagande s'en suit une chasse au responsable, le plus souvent sur le plan juridique sans vraiment s'intéresser à la cause racine de cette manipulation. Cette quête est conduite en mettant le spectateur dans une position d'opérateur, le média prend le rôle de décodeur qui permettra au spectateur de distiller quelques informations et d'arriver à ses propres conclusions. On recherche pour le compte du spectateur qui a fauté, le média (publiques ou privés) décrypte l'information pour vous et illustre le tout avec force d'images et d'émotion. L'analyse est donc tronquée dans le meilleur des cas, ou orientée dans le pire des cas.
De plus, faute de temps et d'attention, nous ne pouvons-nous appuyer essentiellement que sur des faits désignés, plus ou moins tangibles, mais chargés émotionnellement. Il est donc dans ce cas bien plus commode de se focaliser sur les contenants en les désignant (un groupe de « casseurs » sur tel édifice, une attaque cyber sur telle cible, un mouvement politique avec tel leader…) plutôt que des contenus…
Puis, tout s'arrête une fois le responsable désigné ou lorsqu'un autre scandale plus grisant plus populaire se présente : le spectateur s'ennuie vite, il faut le rassasier.

Au cœur de chaque fruit un noyau ou des pépins

L'analyse de la structure d'un espace informationnel doit se conduire par étape, comme étant confronté à un sujet inhabituel. La recherche des émotions ne doit pas dépasser la mesure et la prudence vis-à-vis du cœur du sujet ou du noyau. Car il y a toujours un noyau, un centre plus ou moins dur, plus ou moins mou quand il ne s'agit pas de pépins.
Cette analogie nous permet de commencer à distinguer trois types structurels d'espace informationnels :

- ***Les espaces à noyau dur*** **:** Assez facilement identifiables et difficiles à pénétrer, ils sont typiques des espaces tenus par un état ou une structure suffisamment puissante qui gouverne et agit avec des intermédiaires maitrisés (services ou filiales). La gouvernance vue de l'extérieur est plutôt pyramidale.

- ***Les espaces à noyau mou*** : Moins identifiables, car uniques, mais ouverts à des associations qui viennent peu à peu se cristalliser autour du noyau et servir d'intermédiaire, de médiateur ou de bras armés. Ces « associés » n'ont cependant pas assez de puissance pour prendre des initiatives et restent aux ordres du noyau.

- ***Les espaces à pépins*** : Difficilement identifiables, car du point de vue de l'analyste, il est délicat de savoir exactement combien et quelle forme ont ces « pépins » qui agissent à la fois ensemble et pour eux même, sans qu'il n'y ait de structure de gouvernance clairement établie. C'est une constellation d'intérêts divers et de réseaux différents, avec au moins un objectif commun.

- Enfin, nous devons aussi aborder les espaces informationnels sans noyau, qui s'apparentent plutôt à un groupement d'intérêt qui se focalise essentiellement sur la collecte d'information portant sur un sujet donné et qui échange sur ce sujet sans chercher à interagir au-delà du groupe.

…en quête de légitimité

Lorsqu'un espace informationnel autonome souhaite interagir avec son environnement, il doit se présenter de manière légitime (Éthos) afin de justifier son intervention et d'avoir un message qui porte.

Si cette légitimité est mise à mal du fait de l'historique, du positionnement ou des relations de l'émetteur des messages, le risque de voir un effet contre-productif en boomerang est réel et ce risque doit être exclu.

Par exemple, dans le cadre du réchauffement climatique, le GIEC détient la légitimité scientifique (composé d'experts dans le domaine) et politique, car ce groupe est mandaté par l'ONU. Mais si l'on prend la même problématique au travers du prisme sociétal, nous pouvons identifie la personne publique de Greta THUNBERG qui se représente comme légitime en tant qu'enfant emprunteuse d'une planète « malade » et héritière d'un système qui en est la cause. Sans aller plus loin dans les détails, nous identifions ici deux espaces qui se considèrent légitimes et qui se chevauchent sur la thématique environnementale.

Cette légitimité joue le rôle de point d'ancrage et la structure même du cœur de l'EIA (centralisé dans un noyau ou prenant la forme d'un collectif) doit être en cohérence avec la vision de cet espace. C'est cela qui va jouer le rôle d'aimant et provoquer l'adhésion et donc l'engagement des membres.

Pour illustrer ce propos, nous pouvons utiliser le disque (voir schéma ci-dessous) comme représentation des individus du groupe et les limites au sein desquelles ils se cantonnent (règles et objectifs du groupe). Les engagements évoluant on peut tout à fait observer un individu (point rouge) qui reste sur ses positions (attitude et opinion propre) et qui appartient à un groupe dont l'identité et les engagements évoluent dans le temps.

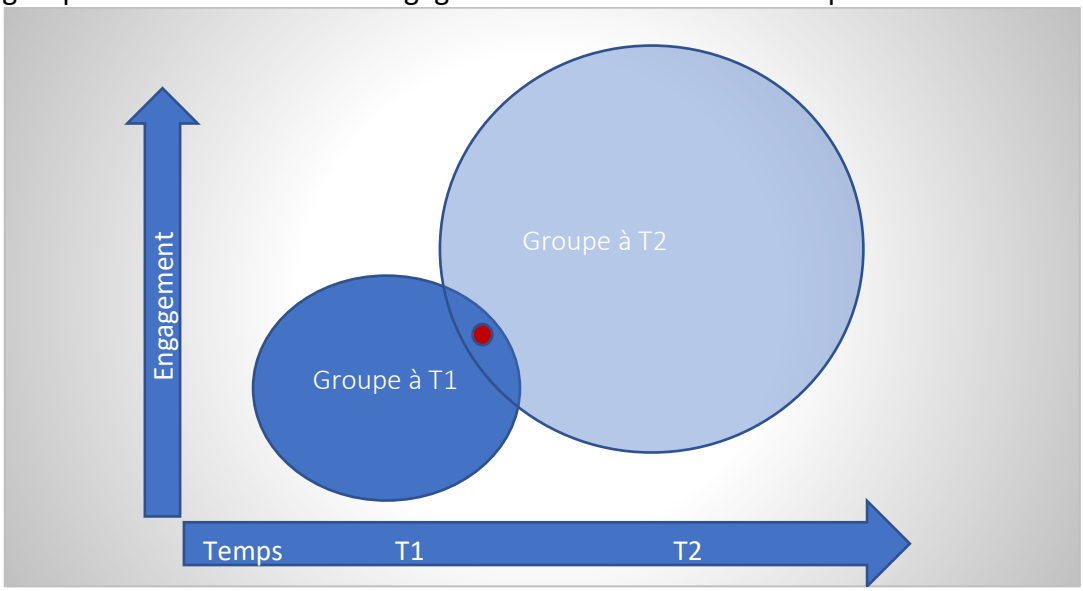


Figure 2- Modélisation de l'évolution d'un groupe Informationnel dans le temps. Le point rouge représente un individu dont l'engagement reste le même entre T1 et T2.

On peut observer ici que dans le temps de T1 à T2 :

- Le groupe a augmenté en nombre (diamètre du cercle),
- L'engagement du groupe (axe vertical) a évolué, mais celui de l'individu reste le même
- L'individu qui pouvait être perçu comme un élément marginal avec un engagement fort à T1 est désormais toujours parti du groupe, mais son engagement par rapport au

groupe est devenu moyen à modéré. Il est possible que cet individu ne se soit pas rendu compte de ces changements.

- De nouveaux adhérents encore plus engagés ont été recrutés
- Le groupe a généralement augmenté en nombre ainsi qu'au niveau de son engagement et les plus modérés à T1 sont devenus plus engagés ou ont quitté le groupe.

APPROPRIATION DU NOUVEL ESPACE INFORMATIONNEL

De véritables affrontements par le contenu se font jour, mêlant manifestations physiques, productions de chercheurs, bruits et rebonds sur les médias numériques tels que Facebook et Twitter. Les techniques pouvant être utilisées pour alimenter un débat public de manière transparente et non faussée sont les mêmes utilisées pour influencer une cible par du contenu modelé spécifiquement pour cet objectif.

Les approches offensives de l'espace informationnel

L'approche américaine : ascendance technologique et sabotage de l'opinion

Précurseurs en 1995 d'une forme de conflit lié à l'information, la RAND Corporation, avait théorisé la militarisation du cyberespace avec le concept de « Netwar » de John Arquilla et David Ronfeld[6]. Cette acception de « guerre des réseaux » faisait « référence aux conflits liés à l'information au plus haut niveau, entre nations ou sociétés ». Il s'agissait d'essayer de perturber ou d'endommager ce qu'une population cible sait ou pense savoir sur elle-même et sur le monde qui l'entoure. Une guerre par les réseaux peut se concentrer sur l'opinion publique ou l'opinion de l'élite, ou les deux. Il peut s'agir de diplomatie, de propagande et de campagnes psychologiques, de subversion politique et culturelle, de tromperie ou d'ingérence dans les médias locaux, d'infiltration des réseaux informatiques et des bases de données, et d'efforts visant à promouvoir les mouvements dissidents ou d'opposition sur les réseaux informatiques[7]. Néanmoins, la stratégie américaine a donné la primauté à la maitrise des infrastructures et à l'utilisation de cet avantage pour essayer de « tout surveiller, tout analyser afin de tout savoir »[8] à travers l'installation d'implants à l'échelle mondiale sur des systèmes informatiques. Ce programme d'infiltration dirigé par la NSA a été révélé par les fuites de documents classifiés de Chelsea Manning en 2010 puis Edward SNOWDEN à partir de 2013. Elles auront un impact sur la perception de la menace et remettront en question la supériorité morale dont se prévalaient les États-Unis.

La feuille de route dictée par Obama en 2012 intégrait la possibilité de conduire des opérations cyber offensives et cyber défensives ayant pour objectif « de manipuler, perturber, bloquer, dégrader ou détruire des ordinateurs, systèmes d'information, de télécommunications, des infrastructures réelles ou virtuelles contrôlées par des ordinateurs ou des systèmes d'information, ou de l'info stockée dans ces systèmes »[9].

Néanmoins, à la suite des manipulations de la campagne présidentielle de 2016, il n'y aurait pas eu de représailles.

Avec l'arrivée de Donald Trump à la Maison-Blanche, est officialisée une « National Cyber Streategy of the United State of America » (de septembre 2018). Ce document est composé de 4 piliers. Le premier pointe la protection du peuple américain, de la patrie et du mode vie américain. Le quatrième nommé « Advance American Influence » précise entre autres, les actions prioritaires parmi lesquelles la nécessité de faire adopter mondialement les bonnes

6 Arquilla, John and David Ronfeldt, eds., "Networks and Netwars: The Future of Terror, Crime, and Militancy". Santa Monica, CA: Rand Corporation, 2001.
7 Jonathan Zittrain (2017) "Netwar": The unwelcome militarization of the Internet has arrived, Bulletin of the Atomic Scientists, 73:5, 300-304
8 Gergorin, J-L. et Isaac-Dognin, L., *Cyber*, (2018). Paris, Les Editions du Cerf, 2018, p211.
9 Ibid

pratiques en cybersécurité[10], sous-entendu les pratiques édictées par les Etats-Unis d'Amérique. Nous y retrouvons également des principes tels que le besoin d'être « leader » en cybersécurité afin de maintenir la capacité d'influence américaine contre les compétiteurs mondiaux. Il s'y ajoute le principe que la liberté de l'Internet aux États-Unis est étroitement liée à la sécurité nationale.

Objective : Preserve the long-term openness, interoperability, security, and reliability of the Internet, which supports and is reinforced by United States interests.[11]

En 2007, Frank Hoffman, définissait « guerre hybride » comme « un éventail complet de méthodes d'affrontement, soit des capacités conventionnelles, des tactiques et des formations irrégulières, des actes terroristes, y compris des attaques aveugles et de la coercition, ainsi que des troubles d'ordre criminel ». Hoffman ajoute que la guerre hybride « peut être menée aussi bien par les forces de l'État que par différents acteurs non étatiques ».
En parallèle des activités cyber, concept de base des échanges informationnels, la USIA[12] (United States Information Agency) et ses activités se voient revalorisées depuis le 11 septembre 2001, mais surtout depuis l'élection du Président B. OBAMA. C'est sous la coupe d'Hilary Clinton, en 2009 que le programme « Civil Society 2.0 » obtient la mission de renforcer les liens avec la société civile afin de pouvoir bénéficier de son leadership (promouvoir la création d'ONG…). Les États-Unis rentrent dans l'ère de la diplomatie 2.0.[13] : « *En soutenant les révolutions arabes ou en épaulant les cyberactivistes du monde entier via Twitter, Alec Ross et Jared Cohen auraient contribué à l'avènement d'une nouvelle diplomatie…* ».
Comme le rappelle également les auteurs du rapport « *Les puissances étrangères développent des actions de soft Power en France : État des lieux et proposition d'une grille de lecture* [14]», l'administration OBAMA a multiplié les actions de soft Power (ils ont 8/10 des sites les plus visités sur Internet) essaimant les différents programmes dédiés aux futurs décideurs, aux étudiants, et aux artistes sur le territoire français.
Le partenariat entre le gouvernement américain et les acteurs du secteur privé se font également sur les couches informationnelles grâce à Twitter, Facebook, mais également des sites web tels que https://movements.org qui proposent son aide pour lancer une campagne politique.

L'approche chinoise : le contrôle par la maîtrise

Comme nous le verrons ci-dessous, dès ses prémisses, le Web a été vu par les dirigeants chinois comme un appareil médiatique complémentaire de propagande dans la sphère virtuelle. Depuis les années 90, la diplomatie chinoise s'appuie sur plusieurs piliers destinés à promouvoir la vision d'une Chine attractive, dotée d'un modèle de développement qui a fait

---

10 National Cyber Strategy of the United States of América – September 2018, « Promote and Maintain markets for united states ingenuity worldwide » … Finally, the United States will work with international partners, government, industry, civil society, Technologists, and academics to improve the adoption and awareness of cybersecurity best practices worldwide.
11 National Cyber Strategy of the United States of América – September 2018.
Traduit par les auteurs : « Préserver l'ouverture, l'interopérabilité, la sécurité et la fiabilité à long terme de l'Internet, qui soutient et est renforcé par les intérêts américains ».
12 USIA, créé le 3 août 1953, Stratégies d'influence et guerres de l'information, Maud QUESSARD (IRSEM).
13 Ibid, équipe de bloggeur, twitter au sein de la Maison Blanche.
14 Rapport de MSIE 29 de novembre 2018, Bruno GOUTARD, Leila SARFATI GHILAS, Nawfal BAKHAT, sous la supervision de Christian Harbulot.

ses preuves. Le développement d'un narratif autour de la culture classique et traditionnelle, l'extension de l'apprentissage de la langue chinoise à travers le monde, le financement des grands programmes d'infrastructure, couplés aux réalisations technologiques et à la mise en place de grands médias, soutiennent cette omniprésence et cette représentation.

Apparaissant déjà dans les années 90, la guerre de l'information et le principe des opérations non cinétiques vont être développés de manière plus intensive à partir des années 2000. Le terrain des idées et de l'influence va être investi plus clairement, à travers plusieurs réformes et textes de loi.

Ces derniers vont préciser les intentions du pays en plaçant la sécurité nationale comme objectif prioritaire unifiant la réponse face aux menaces internes ou externes. Le concept des « Trois guerres » détaille une approche mêlant :

- Des opérations psychologiques avec pour objectifs d'intimider et de provoquer le mécontentement et la dissidence chez l'adversaire ;
- Une guerre de l'opinion publique utilisant toutes les formes d'influence s'appuyant sur l'ensemble des différents types de médias (nouveaux ou plus traditionnels) pour convaincre de la pertinence des politiques et des intentions chinoises ;
- Enfin la guerre juridique qui s'efforce d'utiliser les régimes légaux existants pour limiter et contester les moyens d'action des adversaires et maximiser les atouts de la Chine.

En 2013, un rapport du Comité central du Parti, le Document n°9, liste les poisons qui doivent être combattus « la démocratie constitutionnelle occidentale, les valeurs universelles, la société civile, le néolibéralisme, le journalisme à l'occidentale, le nihilisme historique, et la critique du socialisme chinois », constituant ainsi le programme de Xi Jinping sur le terrain de l'idéologie. En 2015, la loi sur la sécurité nationale reconnait que la lutte dans le « monde des idées » est un enjeu de la sécurité du pays et de la stabilité du régime, et confirme ainsi sa priorité.

Cette volonté politique volontariste vise à maitriser les 3 couches et à faire de la sécurité nationale l'affaire de tous comme stipulé dans la loi sur le renseignement national. Toute organisation se doit de collaborer aux missions de renseignement national .

Convaincue de la force de son modèle (« dictature de marché libérale ») et forte de la maîtrise de son économie et de sa propagande, la Chine a voulu assoir sa domination sur toutes les composantes de l'espace numérique à ses propres conditions pour assurer sa souveraineté sans faille sur cet espace en réalisant des investissements massifs. Pour les dirigeants chinois, la sécurité numérique et la sécurité nationale sont intimement liées. Le principe que suit la Chine est que « plus on se numérise, plus on se vulnérabilise, mais qu'en même temps, pour prétendre au statut de superpuissance il faut se numériser. » Les entreprises ayant émergé sur les vingt dernières années répondent à cet impératif en devenant des champions nationaux puis mondiaux rivalisant avec les précurseurs américains. Ces acteurs ont bénéficié du régime autoritaire et de la restriction généralisée organisée avec le « bouclier doré » (ou Great Firewall) afin de trier les informations qui peuvent entrer dans le pays, mais aussi le blocage de sites web, d'applications et les restrictions de certains contenus spécifiques. Les entreprises du secteur commercial comme Alibaba, Baidu, Tencent, Xiaomi ont profité d'un marché réservé pour se développer et atteindre une taille critique suffisante pour peser à l'international.

À l'instar des infrastructures systèmes et réseaux, la couche logicielle est occupée par des applications chinoises, versions miroirs, mais locales des équivalents de Facebook ou Google, assurant un contrôle des contenus et constituant une vaste ressource de données des citoyens. De même, la Chine investit massivement dans la technologie 5G (les perspectives

sont de 200 milliards de dollars d'ici à 2025) et représente aujourd'hui le 2e acteur en termes de stockage de données derrière les États-Unis. Cette capacité d'accès à la donnée contribue à la création d'un socle de souveraineté dans le cyberespace.

Enfin, le volet informationnel est également organisé autour de grandes entreprises d'État véhiculant l'information à destination de la population chinoise, en Chine, mais également à travers le monde, et relayant le narratif dicté par le PCC (Parti communiste chinois). Le gouvernement dispose de chaines de télévision, de stations de radio et d'instituts culturels pour mettre en place cette présence au niveau informationnel voulu dans la loi de 2015. La China Global Television Network (CGTN) diffuse dans le monde entier en anglais et prend la suite des dépêches et informations relayées par l'agence de presse Xinhua présente à travers 170 bureaux dans le monde et publiant des contenus en 18 langues. L'agence reflète l'agenda du gouvernement en matière de traitement de l'information, passe sous silence des dissidences et a investi dans l'intelligence artificielle destinée à améliorer le niveau de précision des informations de la rédaction. Ce que va permettre également la technologie est un changement d'échelle grâce à l'automatisation des processus, une concurrence pour les agences n'ayant recours qu'à des journalistes. Ces capacités activables sont à mettre en rapport avec le poids des agences de presse et leur pouvoir de prescripteur dans la fixation de l'ordre du jour médiatique et d'une tonalité liée aux informations relayées et traitées.

En matière de cyberespace, des troupes spécialisées de l'Armée Populaire de Libération (APL) sont investies très tôt et à grande échelle dans les opérations offensives cyber afin de pénétrer les entreprises et institutions étrangères. Pékin est ainsi en mesure de récolter des informations stratégiques directement derrière les lignes adverses, ou de neutraliser opérationnellement les capacités militaires ou commerciales de leurs cibles.

À cela s'ajoute, les 829 millions d'internautes chinois (environ 40 % des utilisateurs asiatiques) constituant une large ressource d'influenceurs plus ou moins actifs à travers les réseaux sociaux principalement. Depuis 2007, le recrutement à grande échelle de commentateurs du web a été institutionnalisé afin de guider l'opinion publique en ligne. Ces commentateurs permettent au régime de conduire des campagnes ininterrompues d'astroturfing ou de censure inversée. La fuite d'un document en 2016 a permis une analyse systématique des contenus postés en ligne : 448 millions de posts ou commentaires sur les médias sociaux par an seraient fabriqués par le gouvernement. L'étude de contenu révèle que les commentateurs ont pour but de s'insérer dans le débat pour soutenir et animer des discussions positives en évitant les sujets trop sensibles ou amenant une controverse. Les chercheurs ne notent pas de soutien explicite à l'action du gouvernement ou de représailles à des critiques formulées à l'encontre de ce dernier. En revanche, cette activité doit servir selon eux à détourner les conversations de la négativité générale, à déterminer les questionnements liés directement au gouvernement et/ou celles qui pourraient dégénérer en action collective. La maitrise des actions et de la population se ferait donc par la distraction, premier objectif de cette armée des réseaux sociaux. Cette stratégie met en lumière la volonté d'embarquer la population, mais également les internautes reliés aux réseaux chinois dans la vision d'une Chine leader d'une société connectée et en pleine expansion.

L'approche russe de l'espace informationnel

L'arrivée au pouvoir de Vladimir Poutine en 2000 marque la mise en place d'une affirmation de puissance à l'international et de souveraineté sur son territoire dans laquelle le monde numérique joue un rôle à la fois offensif et défensif. L'utilisation du numérique, comprenant des éléments informationnels et informatiques, dans la politique internationale russe

s'explique en réaction à « une politique de cloisonnement fondée sur la « pression politique, économique, militaire et informationnelle » dirigée par les puissances occidentales et notamment les États-Unis, afin de protéger le pays des agressions étrangères et ainsi tenter de contrebalancer « le rapport de force perçu comme défavorable »[15] par rapport à l'Occident. Les évolutions des années 90, avec l'intégration des anciennes républiques soviétiques à l'OTAN, l'impossibilité de protéger ses alliés[16] et le conflit en Tchétchénie, mettent en exergue la volonté d'indépendance de certaines régions et participent à la vision d'une Russie encerclée. En plus de ces déconvenues s'ajoutent la perception que « l'empire anglo-américain jouit d'un avantage [en matière de guerre de l'information] depuis l'effondrement de l'URSS »[17].

Ainsi, le pays doit faire face à des menaces contre la sécurité nationale en représailles d'une « politique étrangère et intérieure indépendante [qui a] suscité de la résistance de la part des États-Unis et de leurs alliés, qui cherchent à conserver leur domination dans les affaires internationales ». En effet, les révolutions dites de couleurs (Géorgie en 2003, Ukraine en 2004, Kirghizistan en 2005) et les printemps arabes à partir de 2010 utilisant l'essor des réseaux sociaux pour soutenir et organiser les mouvements insurrectionnels sont perçus par Moscou comme « des outils de déstabilisation échappant à tout contrôle étatique ». Utilisés sans distinctions entre les utilisateurs ni limites, ces canaux permettent ainsi de diffuser massivement des informations orientées, avec le risque de manipulation associé.

La Russie parle d'espace informationnel pour désigner le cyberespace[18], donnant ainsi la primauté à la couche sémantique, l'aspect technologique n'étant vu que comme l'une des composantes de la sécurité de l'information, mais n'est pas considérée comme le plus important. Bien que mentionné dans la doctrine militaire de la Fédération de Russie de 2010 par la définition faite de sphère informationnelle (voir encart et extrait de l'article 41 encadré), ce texte porte principalement sur l'amélioration des systèmes d'information et sa protection.

Définition de sphère informationnelle :

Ensemble des données, d'infrastructures de l'information, les entités impliquées dans la collecte, la création, la diffusion et l'utilisation des systèmes d'information et de contrôle rencontrés dans les relations publiques. Elle influe activement sur la société et ses composantes politiques, économiques, militaires et d'autres secteurs.

41. Les tâches qui consistent à équiper les forces armées et les autres troupes en armes, en équipements militaires et spéciaux:

a) équipement complexe (rééquipement) en armes modernes, équipements militaires et spéciaux de forces nucléaires stratégiques, de formations et d'unités militaires en état de préparation permanente de forces générales, d'unités antiterroristes, d'unités de génie militaire et d'unités militaires de construction de routes, ainsi que leur maintien en état de marche, assurer leur utilisation au combat;

b) la création d'armes multifonctionnelles (polyvalentes), d'équipements militaires et spéciaux utilisant des composants normalisés;

c) le développement des forces et des moyens de la guerre de l'information;

d) une amélioration qualitative des moyens d'échange d'informations fondée sur l'utilisation des technologies modernes et des normes internationales, ainsi qu'un seul champ d'information sur les forces armées et d'autres troupes dans le cadre de l'espace informationnel de la Fédération de Russie;

Figure 3 Doctrine militaire 2012 Fédération de Russie

Ce n'est que dans le texte de 2012 que le cyber est clairement pris en compte[19]. Il est complété par texte majeur[20] dans les mois qui suivent sa parution et portant sur l'espace informationnel

15 Gergorin, J-L. et Isaac-Dognin, ibid, p174.
16 Gergorin, J-L. et Isaac-Dognin, ibid, p35.
17 Nocetti, J., « Guerre de l'information : le web russe dans le conflit en Ukraine Russie »., Nei. Reports, n° 20, septembre 2015.
18 Mazucchi, N., *Audition sur la souveraineté numérique dans les relations internationales au Sénat* , 23 mai 2019.
19 Nocetti, J., Guerre de l'information : le web russe dans le conflit en Ukraine Russie. Nei.Reports, n° 20, septembre (2015), accessible.
20 Les visées conceptuelles des forces armées dans l'espace informationnel.

en tant que tel[21]. Internet est identifié comme un « nouveau terrain d'action militaire … Les trois couches classiques du cyberespace sont réunies en une seule… » La définition donnée de la guerre informationnelle n'en est pas moins intéressante : « *Confrontation entre deux ou plusieurs États dans l'espace de l'information pour endommager les systèmes d'information, les processus et les ressources, et d'autres structures critiques, affaiblissant les systèmes politiques économiques et sociaux ;* ***action psychologique massive envers la population pour déstabiliser la société et l'État****, ainsi qu'une influence forçant l'État visé à prendre des mesures dans l'intérêt de la partie adverse*[22] »

En 2013, la publication d'un article du Général Gerasimov, chef d'état-major de l'armée russe, analysant les conflits au XXIe siècle et notamment l'approche occidentale, marque un tournant dans l'observation de l'approche soviétique. Ce texte est perçu par certains comme une approche descriptive de la stratégie militaire russe, « la doctrine Gerasimov », et éclaire sur la vision soviétique d'appréhender et de mener des conflits : « Les règles mêmes de la guerre ont changé. L'utilisation des moyens non militaires pour atteindre des objectifs politiques et stratégiques a cru, et dans bien des cas leur efficacité a surpassé celle de l'utilisation des armes »[23]. Dans ce cadre, « l'espace informationnel offre de larges capacités asymétriques pour réduire la capacité de combat de l'ennemi[24] » et doit être utilisé de manière extensive par le Kremlin. La mainmise du pouvoir sur les médias traditionnels et la mise en conformité des applications stockant des données avec les prérequis russes de vérification d'identité, complètent le contrôle de l'information voulu par Vladimir POUTINE.

L'utilisation de l'espace informationnel comme espace de guerre est une réalité dans l'histoire et l'idéologie du pays. La stratégie d'influence ne se limite néanmoins pas aux périodes de conflits, et doit pouvoir se poursuivre en temps de paix[25].

Venant en écho à la doctrine Gerasimov, le concept de contrôle réflexif issu de la recherche militaire soviétique des années 70 et défini par Timothy Thomas comme « un moyen de faire entendre à un partenaire ou à un adversaire des informations préparées spécifiquement, pour l'amener à prendre volontairement une décision préalablement établie et souhaitée par l'initiateur de l'action »[26]. Ceci suppose la connaissance des leviers cognitifs des individus ciblés ainsi que le contexte dans lequel ils évoluent afin d'influer sur leurs décisions. L'émergence des technologies de communication va permettre une application à plus large échelle d'opérations de subversion et de désinformation.[27]

Les élections présidentielles américaines de 2016 seront symptomatiques du changement d'échelle de la stratégie russe. L'utilisation d'attaques informatiques et informationnelles avec le recours d'usines à trolls est représentative de la nouvelle stratégie russe d'occupation du cyberespace. La déstabilisation de la candidate CLINTON, la mise en doute des méfiances à l'égard des médias et leur polarisation sur des sujets dictés par des révélations résultant d'ingérences de hackers, a ébranlé la confiance dans le bon déroulement du processus de l'élection. Le doute et la confusion ont été instillés tant dans le système politique que médiatique américain[28].

---

21 , Yannick Harrel, *La Cyberstratégie russe*, Paris, Nuvis,2013.
22 Ibid.
23 Gergorin, J-L. et Isaac-Dognin, L., Cyber, Paris, Les Editions du Cerf, 2018, p184.
24 Ibid.
25 Nocetti, J., « Guerre de l'information : le web russe dans le conflit en Ukraine Russie », Nei.Reports, n° 20, septembre 2015.
26 Shemayev, V., Cognitive approach to modeling reflexive control in socio-economic systems, Information & Security, An International Journal, Vol.22, 2007, 28-37. Accessible http://connections-qj.org/system/files/22.04_Shemayev.pdf
27 Marangé, C. « Les stratégies et les pratiques d'influence de la Russie », IRSEM, mars 2017.
28 J-B. Jeangène-Vilmer, « Les manipulations de l'information », IRSEM, 2018.

L'approche française : les strates technologiques

La voie française vers une prise de conscience d'une stratégie de sécurité informatique fut concentrée sur les éléments techniques et les questions de protection des systèmes. Le rapport Romani et le livre blanc sur la défense et la sécurité nationale de 2008 marquent les premières décisions d'une politique remettant les questions numériques au premier plan. Les faiblesses de la France face à des attaques informatiques, l'absence d'une autorité en charge de détecter les menaces y sont notamment relevées[29].

De ces différents constats sera créée l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) en 2009 qui aura la charge de la défense des systèmes d'information et de coordonner les actions nécessaires à la sécurisation des réseaux.

En 2014, le Pacte de Défense Cyber trace les grandes lignes d'une action venant renforcer la doctrine autour de la protection et du développement d'une capacité de réponse aux crises pour être mieux préparé et plus résilient.

Bien que le Rapport Marini appelât déjà à un « partenariat avec le secteur privé [pour] contribuer au soutien à la base industrielle et technologique en matière de produits sécurisés », le besoin d'un secteur privé innovant et fort est toujours en question et le financement des entreprises avec le fléchage de flux d'investissements ne soutient pas la comparaison face aux acteurs américains ou chinois[30].

La Loi de programmation militaire 2019-2029 constitue une avancée dans la reconnaissance de la menace cyber comme permanente et susceptible de concerner tous les domaines de l'espace numérique, y compris celui de l'influence. La ministre des Armées a par ailleurs souligné l'utilisation de l'arme cyber à des fins offensives « isolément ou en appui des moyens conventionnels ». Ces capacités offensives sont sous la direction du Président de la République en tant que Chef des Armées. Il n'a toutefois pas été fait mention aussi nette d'un besoin d'agir au service des intérêts économiques des entreprises françaises, telle que ce l'on pourrait voir aux États-Unis. Il faut se tourner vers le Chapitre 1.c de la récente « Stratégie Nationale du Renseignement» de juillet 2019 (CNRLCT) pour fixer le cadre de « la défense et la promotion de notre économie ». Toutefois, bien que les textes présentent les concepts de LID (Lutte informatique défensive) et de LIO (Lutte Informatique Offensive) qui concernent plus les couches techniques du cyberespace, il n'est pas fait « officiellement » mention de luttes informationnelles offensives, ce qui laisserait penser un écart important entre ce qui est fait ou est assumé en France par rapport aux autres puissances internationales.

29 Rapport Romani, Cyberdéfense : un enjeu de sécurité nationale, 2008.
30 Thierry Breton, Audition au Sénat

Cartographie d'un E.I.A.

La compréhension de ce qu'est un EIA et ses différentes approches par les grandes puissances mondiales, ne répond pas aux questions les plus pragmatiques de l'identification de celui-ci, ni même de sa catégorisation. Les grilles de lectures habituelles proposées dans les ouvrages de management tendent à dire qu'un rapport de force entre organisations ne peut qu'être concurrentiel. Elles ne permettent donc pas de faire un état des lieux des frictions générées par l'opposition de deux EIA. Il faut donc s'extraire des grilles de lectures habituelles pour analyser d'autres réalités telles qu'une guerre informationnelle, afin d'aborder une riposte à cette dernière. Comprendre l'origine de l'attaque et les techniques utilisées par la partie adverse est essentiel pour mieux parer les coups.

Le sujet n'étant pas la globalité d'un espace autonome, mais bien sa composante informationnelle.
Nous retenons 3 thèmes pour regrouper les critères de cette grille :

L'identité d'un Espace Informationnel Autonome

L'identité d'un EIA se caractérise par sa raison d'être ou plus exactement la vision qu'il porte, la gouvernance, les ressources dont il dispose et l'image qu'il se donne.

La vision de l'EIA :

L'EIA porte une vision de rupture en contradiction avec l'activité de l'entité visée. Comprendre sa raison d'être peut nous permettre de mesurer sa vraisemblance. L'EIA sera alors identifiable comme étant une source de menace potentielle.
Pour bien cerner et comprendre l'identité même d'un espace informationnel autonome, il est nécessaire de rechercher et de définir les items suivants :

- Sa raison d'être, son type de gouvernance et sa structure ;
- Connaître son mode de financement et ses ressources ;
- La façon dont il assure sa promotion (son marketing) s'il existe ;
- Son périmètre géographique d'intervention.
  L'identité d'un EIA est avant tout définie par son objectif, ou en d'autres termes, par sa raison d'être. Afin d'en faciliter la compréhension, nous proposons de la décomposer en quatre sous-items :
- Environnement de cet espace ;
- Vision à long terme ;
- Cause supportée ;
- Cause à abolir.
  Par exemple, l'association L214 intervient sur le domaine économique de l'agroalimentaire avec comme objectif de mettre fin à la souffrance animale en

supportant la réduction de la consommation de viande et en dénonçant les pratiques générant de la souffrance animale.

La gouvernance et structure d'un EIA :

La deuxième caractéristique d'un EIA correspond à l'appréhension de sa gouvernance, ainsi qu'à la description de sa structure hiérarchique. Pour bien comprendre son organisation, nous proposons de décliner cette caractéristique en quatre sous-domaines. Chaque sous-domaine est susceptible d'apporter, des informations sur cet espace informationnel autonome. Les sous-domaines que nous avons identifiés comme étant pertinents sont les suivants :

- Le type d'organisation ;
- Les cercles d'influences ;
- Présence d'une structure juridique ;
- Existence de « martyrs ».

▪ *Type d'organisation :*

Dans ce premier sous-domaine, il s'agit d'identifier le mode d'organisation de l'EIA qui peut être de plusieurs types. Il est soit hiérarchique ou participatif, soit centralisé ou décentralisé. Ce critère d'évaluation est plus ou moins difficile à identifier en fonction de la structure de l'EIA (noyaux durs, mous, pépins – cf. plus haut)

Exemple 1 : une structure nébuleuse et sans leader déclaré telle que celle de la ZAD de Notre-Dame-des-Landes assure une certaine forme de survie en cas de neutralisation d'une partie des membres. Son organisation n'est pas hiérarchique. Elle est participative.

Exemple 2 : l'EIA L214 est composé de l'association L214, d'une multitude d'association et de partenaires. Elle n'est pas unique. Il existe l'association dite principale qui définit les actions et qui gère les campagnes de communication. Et il existe différentes associations locales qui sont subordonnées à la structure mère. Néanmoins, son organisation est très hiérarchique.

▪ *Cercles d'influence*

Il existe plusieurs cercles concentriques d'influence gravitant autour d'un EIA. Le premier cercle, le plus central, représente ceux qui vivent de l'EIA. Il est généralement composé des meneurs de la première heure du mouvement, des ambassadeurs et des influenceurs. Le second cercle est constitué de ceux qui bénéficient de l'EIA. Il s'agit généralement des personnes dont le rôle est de convaincre. Il regroupe les membres actifs tels que des scientifiques ou des personnalités publiques prêtant leur image et donnant ainsi une résonance et une crédibilité à la cause. Ils ont un rôle de prescription pour l'EIA. Enfin, un troisième cercle rassemble les sympathisants aux idées fondatrices de l'EIA ou ceux qui en parlent pour servir leur intérêt propre plutôt que servir la cause de l'EIA.

Figure 4 Illustration des cercles d'influence d'un EIA avec L214

- *Existence d'une structure juridique (oui ou non) :*

Le cinquième sous-domaine correspond à l'existence d'une structure juridique. Si une telle structure est en place, elle peut nous permettre de nous procurer des renseignements utiles. Par exemple, la structure mère de L214 est une association de type loi 1908. Il peut être pertinent de se poser la question de savoir pourquoi L214 a préféré ce type de régime plutôt que celui plus usité de loi 1901. Créée en 2008, l'association de droit 1901 L214 a changé de statut en 2015 pour passer sous le régime de la loi dite 1908 pour devenir une association de droit local alsacien mosellan.

	Alsace – Moselle	**Reste de la France**
Loi	1908 – Article 21 à 79 du Code civil local	Loi du 1er juillet 1901
Nombre minimum de membres fondateurs	7	2
But	But lucratif possible	But non lucratif exclusivement
Déclaration	Inscription au tribunal d'instance	Déclaration en préfecture
Publication de l'annonce	Journal local	Journal officiel
Capacité juridique	Capacité juridique étendue	Capacité juridique limitée

Figure 5 : comparaison loi associative 1901 et 1908

Les deux principales différences entre la loi 1901 et la loi 1908 se trouvent au niveau de leur but et de leur capacité juridique. En effet, le régime de la loi 1908 est à but lucratif. Ainsi, il est possible de faire des bénéfices qui reviendront aux membres. De même, les capacités juridiques sont beaucoup plus importantes avec la loi 1908. Elle autorise notamment la fusion d'associations entre elles. Subséquemment, on peut s'interroger sur ce changement de statut juridique réalisé juste deux ans avant que l'association L214 ne reçoive 1.14 million d'euros de la fondation Open Philanthropy Project[31].

- *Existence de martyrs :*

Le quatrième et dernier sous-domaine correspond à la présence ou non de « martyrs » à la cause. Ces « martyrs » ont un rôle très important lorsqu'ils existent. En effet, ils peuvent permettre de rallier plus de sympathisants du troisième cercle d'influence à la cause de l'EIA. Dans le cas de L214, les martyrs sont les animaux. Le mouvement des gilets-jaunes (en France courant 2018-2019) s'est également vu avoir plusieurs « martyrs » dont les images ont été associées par les organisateurs aux « gueules cassées » de la Première Guerre mondiale afin de parfaire leur communication. (Voir illustration ci-contre représentant le portrait du ministre de l'intérieur Christophe Castaner réalisé à l'aide de portraits de gilets-jaunes ayant été blessés).

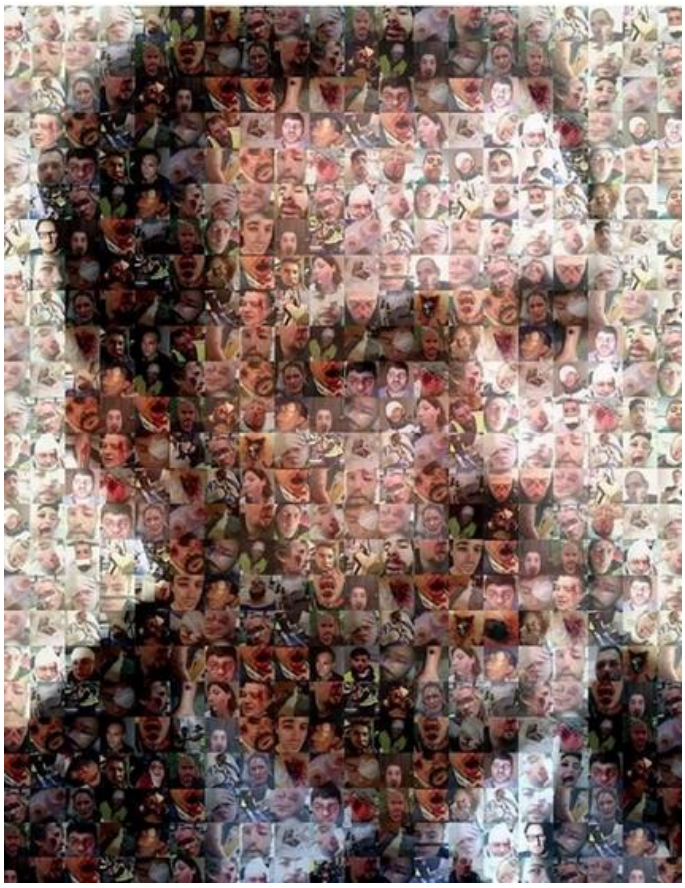


Figure 6 Campagne d'affichage des Gilets jaunes

[31] L'Opinion.

Les ressources

La troisième caractéristique identifiable de la carte d'identité d'un EIA est celle définie par ses ressources. Pour bien l'appréhender, nous avons établi 3 sous-domaines :

- Autonomie de subsistance ;
- Mode de financement ;
- Moyens physiques.
-

▪ *Autonomie de subsistance*

Par autonomie de subsistance, nous nous référons à une notion d'existence en autarcie. Pour cet exemple, le mode de fonctionnement qui peut être observé à travers la ZAD de Notre-Dame-Des-Landes est pertinent.

▪ *Mode de financement*

Le deuxième sous-domaine correspond aux différents modes de financement d'un EIA. En effet, cette information est très importante à connaitre. Savoir d'où proviennent les capitaux peut permettre éventuellement de découvrir qui se cache derrière l'EIA, ou qui réalise des opérations de guerre informationnelle, donc de connaître l'adversaire.
Dans le cas de L214, outre les dons et les cotisations des membres, nous savons qu'elle a reçu en 2017 la somme de 1.14 million d'euros de la fondation Open Philanthropy Project. Or cette fondation finance aussi des sociétés américaines développant des projets de viande artificielle[32]. Il s'agit là d'un faisceau d'indices laissant supposer un acte de guerre économique. Celui-ci ayant pour objectif de déstabiliser la filaire viande française au profit des entreprises financées par l'OPP.

▪ *Moyens physiques*

Le troisième sous-domaine permet d'identifier les éventuels biens matériels appartenant à l'EIA. Cela peut aller du simple local à des immeubles ou des entrepôts.
Concernant L214, nous n'avons pas identifié de biens fonciers ni de moyens physiques pertinents.

L'image de « marque » ou son marketing

La quatrième caractéristique de la carte d'identité d'une EIA correspond à son image de marque, ou plutôt à ses signes distinctifs facilement identifiables, les médias, les prospectus… Nous pouvons regrouper dans cette rubrique son logo, son slogan éventuel et tous les autres signes de communication. Connaître ces éléments permet l'identification des différentes ramifications de l'EIA, les membres et les sympathisants à la cause.
Les slogans et ses logos de L214 ont toujours bien été mis en avant à chaque opération dite « coup de poing » dans les abattoirs pratiquant des méthodes répréhensibles et contraires à l'éthique. D'ailleurs, toutes les nouvelles campagnes de communication sont maintenant toujours lancées sur les chaines de médias télévisuels.

32 Listée en tant qu'investisseur d'Impossible Foods.

Les effets recherchés au sein d'un EIA

En raison de leur nature agrégée d'individus proches d'un point de vue idéologique, les objectifs que l'on peut trouver au sein des EIA sont le plus souvent d'ordre politique et stratégique. C'est d'abord une lutte pour modifier un pan de la société qui est désigné comme le mal absolu. On retrouve par exemple dans les groupes d'ultragauches un sentiment commun de détestation de l'ordre établi par la finance (le pouvoir du capital) qui est identifiée et qui est présentée comme la source de tous les maux d'une part, et le discours fédérateur et rassembleur de la classe prolétarienne qui subit et doit réagir d'autre part. Cependant, si le discours ou la communication sont volontairement simples et directs, le contexte est complexe et la stratégie souvent nébuleuse. Nous allons tenter d'identifier et de définir les principaux points communs aux EIA en termes d'objectifs.

Définir la cible en fonction de l'effet majeur recherché

Si du point de vue stratégique l'effet recherché relève plus de l'idéologie et d'un mal-être commun aux individus qui composent un espace informationnel autonome, les batailles et la désignation des cibles et des tactiques suivent des règles plus simples et plus directes. Le choix des batailles est fonction du contexte et les étapes de ce choix sont bien décrites dans l'ouvrage de S. Popovic, moteur de l'EIA Otpor, « *Blueprint for revolution* [33]».

Dans cet ouvrage, l'auteur relate différentes interventions de présentation et de formation à la résistance non violente. Il y précise que les batailles ne peuvent aller directement à l'encontre du pouvoir en place qui possède une force de contrainte colossale face à une minorité d'opposants.

Dans un premier temps, il faut s'affranchir de l'idée que cela ne peut pas arriver, puis voir grand, mais commencer petit, et peu à peu apporter une vision pour demain, s'appuyer sur les piliers de son propre pouvoir et saper ceux de l'ennemi pour en rire jusqu'à la victoire tout en retournant l'oppression contre elle-même. Tout ceci dans un esprit de démonstration de l'unité du peuple finement planifiée.

Ainsi l'espace créé parvient à accomplir les deux principaux objectifs visés que sont :

1. Renverser ce qui est désigné comme oppresseur ;
2. Maintenir sa cohésion et grossir pour atteindre la masse suffisante à l'achèvement du premier objectif.

On notera que ces deux objectifs sont relativement proches de ceux que l'on peut appliquer à chacun de nous et qui sont : se nourrir et s'informer. Ces deux objectifs stratégiques ne peuvent évoluer l'un sans l'autre, car sans augmentation du nombre de partisans, de membres, de figures ; il n'y a pas de nourriture (tant matérielle qu'intellectuelle) et sans avancées évidentes contre l'ennemi désigné, il y a une perte de moral et un risque de désengagement.

La désignation de la cible est donc un point central, car il faut une cible qui évoque à toute la population (membres de l'EIA et forces de l'ordre inclus) une injustice, afin d'obtenir l'adhésion du plus grand nombre. Puis, petite victoire après petite victoire, démunir l'adversaire et le rendre à la fois impuissant et ridicule.

33 S. Popovic, *Comment faire tomber un dictateur quand on est seul, tout petit et sans armes*, Paris, Payot & Rivages 2015.

Les armes de la guerre de l'information au service des EIA

Dans le discours des EIA, on retrouve tout l'arsenal de la guerre économique et de la guerre de l'information par le contenu qui est utilisé soit pour attirer des membres soit pour désigner la cible et peu à peu l'encercler.

Les principaux arguments avancés sont les suivants :

- **La peur de la pénurie** : qui en fonction du contexte peut s'apparenter à :
  - La famine ;
  - La perte d'emplois ;
  - La perte de droits fondamentaux au profit de l'oppresseur.
  -
- **La perte de puissance financière** :
  - Faire perdre des parts de marché pour faire basculer l'oppresseur ;
  - La perte de souveraineté (qui peut être à la fois un moteur du rassemblement et/ou spécifiant un ennemi) ;
  - Désignation des corrompus.
  -
- **Contrôle de la chaine logistique** : tant à l'amont qu'à l'aval par :
  - Le sabotage et les actions de ralentissement de l'outil de production ;
  - Le boycott de produit désigné.
  -
- **Changement culturel** : Prospective de rupture et insinuation d'une modification des modes de vie forcés. C'est un des arguments particulièrement utilisés pour soutenir des changements de mode de vie afin de réduire l'impact humain sur le climat. C'est une approche qui se rattache à la maitrise du discours moralisateur et qui permet de justifier à la fois le rassemblement et la désignation du mal.
-
- **Faire évoluer les modèles d'affaire**s : par exemple :
  - Soutenir l'inversion du rapport de force entre actionnaires (incarnation du capital) et ouvriers / salariés ;
  - Insister sur la dimension novatrice d'une approche du commerce populaire (airbnb, UBER) en insistant sur les avantages pour le consommateur et en minimisant la précarité générée sur les prestataires de services. Argument très courant dans le secteur des nouvelles technologies.
  -

Les objectifs tactiques et l'effet recherché

À chaque effet recherché son objectif tactique. Nous présentons ici quelques exemples d'objectifs tactiques qui, une fois atteints et combinés, deviennent un encerclement et permettent d'obtenir une position dominante sur tout un secteur, voir même un pays. Il est important de préciser ici que ces objectifs tactiques et les méthodologies d'encerclement sont aussi applicables par les États pour le maintien des autorités de contraintes en place et le maintien de leur souveraineté. On retrouve de manière générale les tactiques suivantes :

- **Identifier une cible « personnifiée »** : pour peu que l'effet recherché soit intimement lié à un secteur particulier, la tactique de la personnification d'une cible (viser une personne ou un profil type de personne en lieu et place d'un système). Cette méthode permet de simplifier le travail de critique du secteur en utilisant des traits de personnalité ou de la vie privée d'individus qui sont ensuite présentés comme inhérents à ce secteur.

- **Identifier la cause de l'irritant** : cette tactique est très souvent employée par les médias pilotés par des États, par les partis politiques et les groupes d'influence qui cherchent à fournir la démonstration de la raison du mal-être et du malaise vécu par la population. En faisant ce travail en lieu et place des individus, un EIA s'octroie les faveurs de ceux qui n'ont pas le temps de faire l'analyse comparée et manipule la vérité pour mieux peser et atteindre l'effet recherché.

- **Agir sur le spectre émotionnel** : connue plus communément dans le secteur du marketing, et plus particulièrement du neuro-marketing, cette tactique de manipulation fait agir par réaction. C'est une manipulation de l'expérience et du contexte qui va agir sur la partie reptilienne du cerveau et utiliser un processus de décision basé sur nos instincts plutôt que sur notre raisonnement (lobe frontal). Cette tactique se fondera donc particulièrement sur des arguments générateurs de peur du manque, qu'ils soient d'ordre alimentaire, reproductif ou territorial. C'est une des raisons pour lesquelles on observe une « sexualisation » latente dans les publicités.

- **Agir sur le spectre réglementaire et juridique** : afin de maintenir sa puissance et de garder l'ascendant sur les autres espaces (groupes supra-étatiques, États, groupes privés) l'action de manipulation de la décision par le biais de réseaux d'influence et de lobbying permet de neutraliser momentanément l'adversaire.

- **Agir sur le contenu et la verbalisation des normes** : cette approche inhérente à la guerre économique vise à influencer les commissions normatives ainsi que les groupes de travaux sur les évolutions des contenus des normes. C'est une tactique qui est proche de l'action sur le spectre réglementaire, mais qui est plus complète, car elle permet d'aller jusqu'à la formulation du texte normatif. Ainsi la maitrise des points de détails des normes ou le blocage du processus de validation d'une commission permet de maintenir sa puissance ou de gagner du temps pour se mettre à niveau.

- **Avoir la main sur les savoirs scientifiques** : les articles et publications scientifiques constituent le socle de la démarche et de la réflexion scientifique. Dans un monde de plus en plus complexe, avec des capacités de mesure et d'analyse très pointues, il est impossible de ne pas prendre en compte les avancées de la science en faisant référence à ces publications. Cependant, en imposant un comité de relecture (qui fera en fait office de censure) ou en biaisant la démarche scientifique par le financement de recherches sous condition de résultats imposés, un EIA gagne la maitrise des données de base maitrise le contexte et manipule les décisions.

- **Rester invisible et agir dans l'ombre** : dans bien des cas, l'invisibilité est un impératif majeur de l'EIA qui lui permet de quérir de l'information, de l'analyser et de la manipuler pour ensuite la déverser par des canaux officiels sans être identifié. Cette tactique fait appel à l'utilisation de faux profils au niveau individuel, mais elle peut aussi motiver, dans le cas de manipulation à grande ampleur, la création d'organisations et d'acteurs de la société civile qui pourront se présenter sous une identité totalement fabriquée. De ce fait ces avatars d'EIA pourront manipuler l'information sans éveiller de soupçons et pénétrer des milieux qui leur seraient inaccessibles si leur volonté réelle était dévoilée.

- **Tuer la réputation** : en tuant la réputation d'un individu ou d'une organisation, on décrédibilise tous ces arguments ainsi que sa vision. Les attaques peuvent porter sur divers aspects de la cible et chercheront à mettre la cible dans une position intenable qui l'obligera à mobiliser ses ressources pour recouvrir sa réputation plutôt que de continuer à agir dans son domaine et donc de laisser la place à l'EIA qui l'attaque.

- **Agir sur les moyens de communication de l'adversaire** : Tactique de subversion par l'accaparement des sujets et parfois même des canaux de communication de l'adversaire pour le « noyer » dans un flot de contenu et de doutes. C'est une tactique de sape sur l'adversaire qui vise à le ralentir.

Les actions au sein d'un EIA.

Que la guerre soit cinétique ou informationnelle, nous retrouvons des concepts tels que le « théâtre d'opération » (ici l'espace) et les effets recherchés (voir section précédente). Ils peuvent être de plusieurs natures et s'alimentent mutuellement afin d'atteindre un objectif stratégique.

Figure 7 EIA, Interactions et effets recherchés

Pour les atteindre, plusieurs actions peuvent être menées. Celles-ci peuvent être regroupées en 3 familles :

- Les actions **contre** l'information : le sabotage ;
- Les actions **pour** l'information : l'espionnage ;
- Les actions **par** l'information : la subversion.

Bien qu'utilisable dans tout type d'espace, nous les aborderons ici à travers un prisme de lecture « cyber ». Nous pouvons ainsi faire un lien entre ces trois familles et les strates du cyberespace présentées dans la seconde partie de ce document. (Voir schéma ci-contre)

Dans le cadre de la grille d'analyse d'un EIA, il nous semble structurant d'identifier rapidement l'existence d'actions du type espionnage ou sabotage. La complexité de mise en œuvre de celles-ci indiquera l'ampleur des moyens (financiers, techniques …) disponibles de l'attaquant ainsi que de ses motivations.
Les propos qui suivent aborderont ces trois familles en donnant des exemples d'actions.

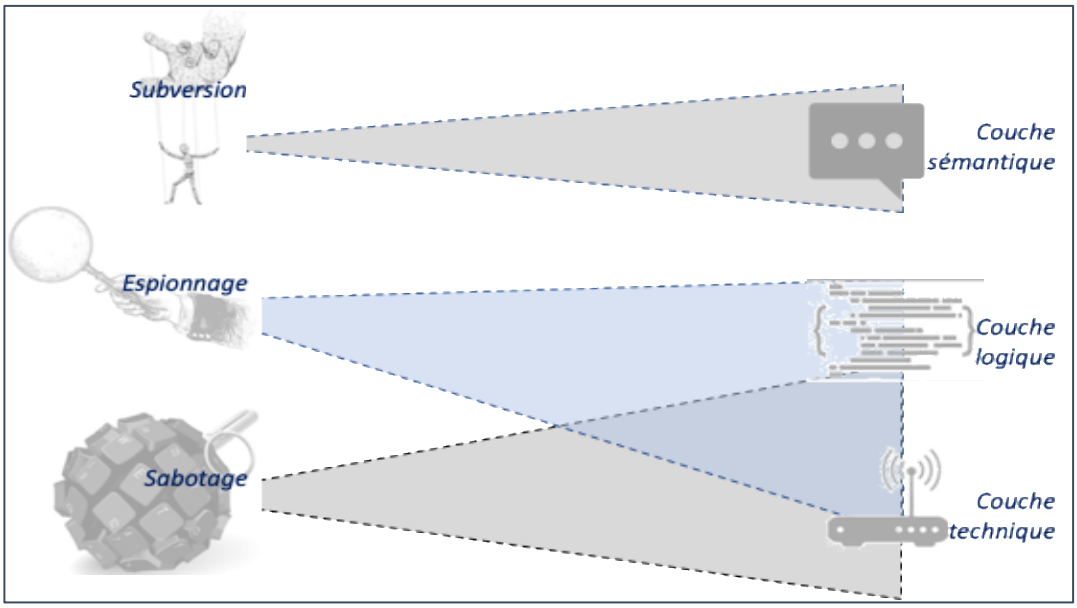


Figure 8 les différents types d'attaque selon les couches visées

Agir « contre » l'information : saboter la chaine de production

- *Attaquer les infrastructures informatiques*

Les actions de sabotage (au sens de destruction physique) interviendront principalement sur les couches techniques et logiques du cyberespace. Nous retrouverons de manière la plus visible des attaques de type DDOS (Distributed Deny of Service) qui ont pour effet recherché la saturation des ressources de l'infrastructure de l'entreprise ciblée ; et ceci, jusqu'à les rendre inutilisables. Par exemple, l'hébergeur français OVH a subi une attaque de ce type fin 2016, perturbant fortement les services fournis à ses clients particuliers et entreprises.

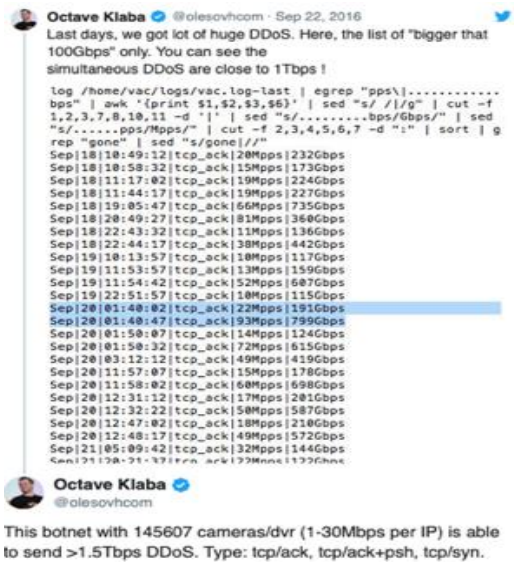


Figure 9 Tweet d'Octave KLABA, CEO d'OVH

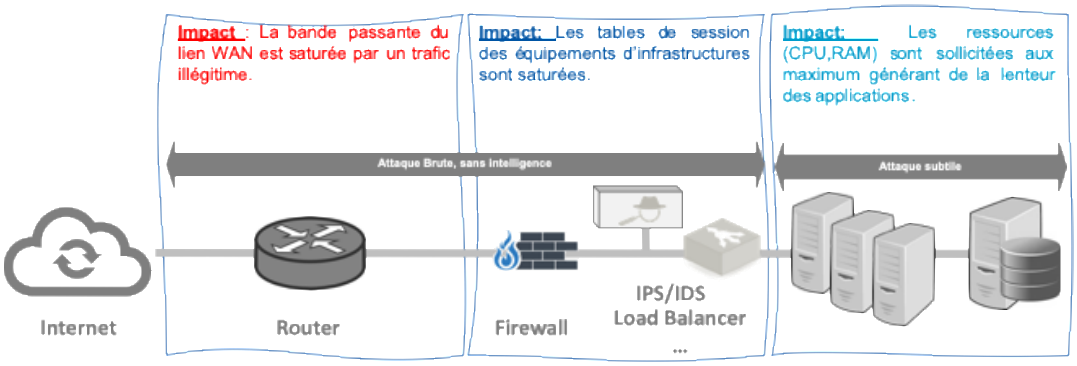


Figure 10 les différents types d'attaque DDOS

Dans la catégorie des attaques « destructrices », le DDOS partage le podium avec les rançongiciels. Ces codes malveillants rendent les systèmes d'informations inutilisables (en chiffrant les fichiers du système d'information de l'entreprise) jusqu'à ce que l'organisation touchée paye une rançon. L'effet de cette dernière dépend cependant de « l'honnêteté » de l'attaquant. Par exemple, en mai 2017, « Wannacry » était le premier rançongiciels réellement médiatique. Renault et bien d'autres entreprises ont été gravement touchées. L'usine de Douai (59) a dû stopper la production et mettre le personnel au chômage technique pendant plusieurs jours. Quelques mois plus tard, Saint-Gobain et Auchan ont été touchés par « Notpetia ». Cette attaque ciblait les organisations ukrainiennes par l'intermédiaire de « MeDoc », un logiciel réputé licite dont une mise à jour s'est trouvée infectée par un cryptovirus. Plus d'un million d'ordinateurs ont été neutralisés en Ukraine.

Figure 11 Exemple d'écran d'une attaque Rançongiciel

- *Intimider les acteurs de la chaine de production*

L'arrêt d'une chaîne de production ne passe pas obligatoirement par de la destruction. Exercer une pression sur les fournisseurs ou partenaires de l'entreprise ciblée peut également avoir un effet ravageur. Par exemple, dans le cadre de « l'appel d'offre concernant le suivi des mesures compensatoires pour la déserte routière du futur Aéroport Grand Ouest », l'une des associations « anti » aéroport a fait parvenir aux entreprises soumissionnaires « potentielles », un courrier menaçant. L'extrait ci-dessous en donne le ton :

> *« Si nous vous faisons parvenir ce courrier, c'est dans la louable intention de vous mettre en garde des risques encourus par l'entreprise qui décrochera ce marché. Vous ignorez peut-être les pertes dont les autres entreprises liées à ce projet furent précédemment l'objet. Celles qui ont travaillé sur le terrain, à la ZAD, furent confrontées à de multiples interruptions de travail, dégradations, harcèlements téléphoniques… Les pertes et dégâts matériels infligés sont à anticiper, car ils ont de graves conséquences économiques et ne se limitent pas au périmètre de la ZAD. Chaque local, siège social, où qu'il soit, est une cible potentielle. Sans parler de la mise*

à mal de l'image de marque des entreprises concernées. Certaines ont renoncé à leur contrat. Les travaux sur place sont au point mort. »

L'impact a été immédiat et a causé un grand retard sur les travaux prévus. Le site internet https://adopteunsoustraitant.noblogs.org a été mis en ligne afin d'identifier plus facilement les entreprises participant au projet. L'effet pour ces cibles collatérales est immédiat. Peu d'entrepreneurs veulent prendre le risque de mettre leur activité ou leur collaborateur en danger.

Chupin épisode 2

Chupin encore! Ci-dessous un texte publié sur indymedia nantes:

Action directe contre l'aéroport! Nous aussi on adopte Chupin, sous traitant.

Cher Chupin

depuis qu'on a appris ton engagement dans le projet d'aéroport de Notre-Dame-des-Landes, on s'inquiète beaucoup pour toi.
On a vu que des gens te l'ont déjà dit, on voulait insister.

Figure 12 Extrait

- *Bloquer la production par le juridique*

Bien qu'il ne s'agisse pas d'un sabotage « destructeur », l'utilisation de l'arme juridique peut se trouver encore plus puissante pour saboter une chaîne de production. Les lenteurs administratives et les interprétations des textes sont autant d'éléments aggravants (ou arrangeants suivant les parties).
L'exemple des réponses juridiques formulées par les opposants de l'aéroport à Notre-Dame-Des-Landes illustre parfaitement ce type d'actions. L'un des dossiers est parfaitement illustré par Frédéric Beniada et Marc Bouchery dans leur ouvrage[34] consacré à cet espace autonome. Les opposants au projet se sont associés aux élus écologistes du parlement européen. C'est grâce à une pétition (déclarée recevable par la commission) où chaque citoyen européen peut faire valoir son point de vue que les opposants ont pu bloquer le projet en dénonçant une non-conformité avec le droit européen. Ceci alors même que la commission s'était déjà prononcée négativement en 2010 sur ce sujet.
Ce type d'action a également été intensément utilisé par Greenpeace lors de l'appel d'offre européen lancé par la France et concernant le désamiantage et le démantèlement de l'ancien porte-avion « le Clémenceau »[35]. Nombreux rebondissement reposant sur une base juridique, tel que des annulations de contrats pourtant signés et des débats sur la nature de la coque (déchet de guerre ou matériel de guerre), ont bloqué le lancement des travaux.

Agir « pour l'information » : l'espionnage

- *Collecter de l'information par le cyber*

Les actions d'espionnage consistent à acquérir du renseignement, idéalement sans être repéré par les équipes de défense de l'organisation ciblée. Par exemple, entre 2014 et 2015,

34 Frédéric Beniada et Marc Bouchery, « Aéroport de Notre-Dame-Des-Landes – Autopsie d'un Déni démocratique », 2019.
35« Le Bilan de l'affaire de l'ex-Clémenceau », Rapport de l'école de Guerre économique, Novembre 2009, MSIE9.

l'OPM[36], l'agence fédérale de ressources humaines pour le gouvernement américain, a été infiltré. Les attaquants ont pu extraire des millions de données personnelles d'Américains. Cela incluait les formulaires SF86 (le formulaire SF86 contient les données personnelles telles qu'adresses, dates de naissance, mais également préférences sexuelles, race, empreintes digitales, rémunérations, dettes, et habilitations …). La motivation d'une telle attaque pourrait être la déstabilisation politique, l'espionnage ou même le chantage dans l'objectif d'atteindre d'autre cible. Un groupe d'attaquants supposés chinois nommé « DEEP-PANDA » est soupçonné d'être l'instigateur.
Cette attaque a exploité les vulnérabilités du système d'information se trouvant sur ce que nous identifions comme la couche logique. (Accès à une vulnérabilité LSASS par Mimikatz et utilisation de prestataires mal maîtrisés).

- *Collecter de l'information et la diffuser*

L214 a également mis en œuvre des procédés de collecte d'informations dans un objectif de création de contenu. Les membres de l'association posent des équipements de captation dans les endroits les plus stratégiques. Pour ce faire, ils s'introduisent illégalement dans les locaux ciblés ou se font passer pour des candidats à l'embauche, ce qui leur permet de visiter les sites en plein jour.

Figure 13 Vidéo-choc d'abattoir par Konbini et repris par L214

Il existe de nombreuses vidéos sur YouTube explicitant les défaillances rencontrées et les atteintes contre les animaux. Les informations collectées et présentées ont pour but de générer des émotions d'effarements de la part de l'opinion publique.

Agir « par l'information » : la subversion

- *Avant tout, se rendre légitime*

L'un des éléments clés pour peser dans un espace informationnel autonome est le poids représenté par les parties dans « le cœur et les esprits [37]» des partisans de la cause ou des opposants. Se rendre légitime au sein de l'EIA est le moyen d'assoir son action pour mettre

36 Office Personnel Management.
37 Expression reprise de Maud Quessard, lors d'un interview, auteure de Stratégies d'influence et guerres de l'information, 2019.

sous pression sa cible. Cela passe par un plan de communication marketing plus traditionnel incluant, la présence sur les réseaux sociaux, l'utilisation et la production de « contenu de référence » est la base... » Le choix de l'irritant, la cause profonde à défendre sont ainsi une clé pour clarifier la position tenue.

« Dans ce conflit, la question n'est pas la représentativité de l'adversaire, mais sa capacité à faire adhérer le public à sa cause »[38]
Christine Roguet, chercheur à l'IFPI

Comme le montre le rapport de l'EGE « comment perdre une guerre économique : l'exemple de la filaire viande », L214 et ses fondateurs ne sont pas apparus au hasard d'un blog ou d'un twitter. Brigitte GOTHIERE et Sébastien ARSAC[39] ont très tôt activement participé aux cahiers antispécistes et continus encore à ce jour.
L'objectif à rechercher n'est pas de convaincre immédiatement l'ensemble de la population, mais bien de consolider le premier cercle et constituer le second. Des chercheurs de l'université de Pennsylvanie et de l'université de Londres ont cherché à déterminer quelle devait être la masse critique d'un groupe soutenant un point de vue minoritaire, pour renverser une opinion faisant consensus. Résultat : Il apparaît ainsi que si la minorité dépasse le seuil des 25 %, elle peut entraîner la majorité à rejoindre son point de vue.

« Choisissez des batailles assez importantes pour compter, mais assez petites pour les gagner[40] *»*
Jonathan Kozol

- *Construire du contenu médiatique pour décrédibiliser*

Gagner une course revient à confronter deux réalités :

- Le gagnant a été meilleur que le perdant ;
- Le perdant a été moins bon que le gagnant.

La guerre informationnelle se gagne en surclassant son adversaire. Cela peut se faire de deux manières opposables. Construire un discours et une image forte ayant acquis à sa cause l'ensemble des masses, ou décrédibiliser l'adversaire afin de réduire son attrait au sein de ses propres troupes et ainsi réduire son pouvoir d'influence.

« Avec deux lignes de l'écriture d'un homme, on peut faire le procès du plus innocent », Cardinal Richelieu

Pour ce faire, un plan de communication spécifique peut être construit. Par exemple, pendant les affrontements de la ZAD de Notre-Dame-des-Landes, deux types d'actions ont pu être mises en avant :

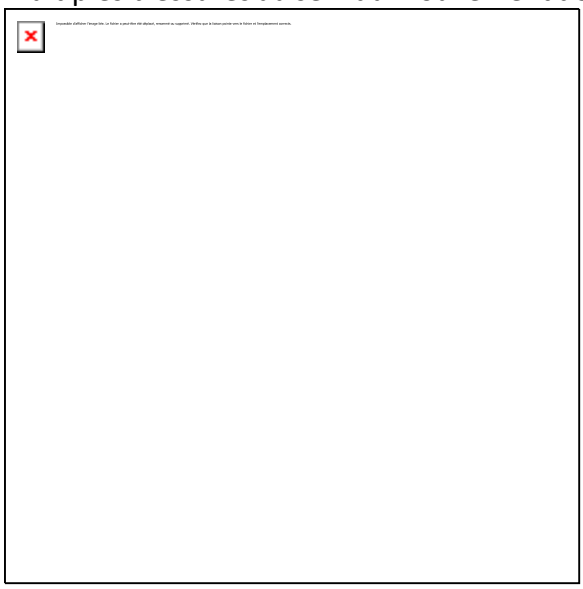
- Des affrontements violents ;

38 EGE, « comment perdre une guerre économique : l'exemple de la filaire viande », promotion MSIE 27, Janvier 2018.
39 Membres fondateurs de L214.
40 Citation reprise de « Comment faire tomber un dictateur quand on est seul, tout petit, et sans armes », Srdja Popovic, p55.

- Des « méthodes douces.

Figure 14 photo de Zadistes à Notre Dame des Landes

Cette dernière a été nommée ainsi par les journalistes couvrant l'évènement. Elle consistait à avancer « presque nu et en rampant » vers le front des forces de l'ordre. Se faisant ils rendaient les zadistes sympathiques aux yeux de l'opinion, car prêts à défendre une cause quoiqu'il en coûte[41]. Ce qui par débordement (voir le biais cognitif « effet halo » décrit plus bas) rendait la cause défendue louable, quelle qu'elle soit. Cependant, le second effet de cette mise en scène est encore plus puissant dans l'opinion publique. Elle ridiculisait les forces de l'ordre obligées de prendre le rôle de Goliath contre David. Ils placent ainsi les forces de l'ordre dans le rôle du « dictat » bien armé qui n'hésite pas à s'en prendre aux plus faibles. Les multiples blessures au sein du mouvement des Gilets-Jaunes reprennent le même mécanisme.



41 Frédéric Beniada et Marc Bouchery, Autopsie d'un Déni démocratique : p53 : « Les forces de l'ordre reçoivent, du haut des cabanes construites dans les arbres, des sacs d'urine et d'excréments ; des « cacatov » qui feront école par la suite comme projectiles lancés sur les forces de l'ordre dans des manifestations. « C'est immonde » confie l'un des gendarmes mobiles présents sur place. En parallèle des opposants n'hésitent pas à ramper dans la boue entre les forces de l'ordre, à témoigner en caleçon pour les hommes et seins à l'air pour les femmes devant les journalistes ».

S'ajoute à cela que « jouer sur la surprise, le rire, la colère, les croyances, les émotions, les indignations, les outrances, c'est associer au message une prime de viralité qui lui garantira d'être partagé, souvent même avant d'avoir été lu.[42] »

Figure 15 Banderole choc lors de manifestation des gilets jaunes

42 Bruno Patino, *La civilisation du poisson rouge,* Paris, Grasset, 2019.

Exploiter les biais cognitifs pour influencer

Sommes-nous otages d'affrontements informationnels à cause de failles cognitives ? Si oui, comment exploiter ces dernières ? Comment explique-t-on que lorsque deux phénomènes arrivent ensemble, on a l'impression qu'ils sont liés ? Quelles règles régissent nos modes de communication, véritables serrures permettant d'ouvrir une porte béante vers nos vulnérabilités cognitives. Schopenhauer[43] s'interroge sur « la médiocrité naturelle de l'espèce humaine » et de sa « vanité innée qui accompagne un besoin de bavardage » ?
Nous aborderons ces thèmes dans les lignes qui suivent en abordant succinctement le concept de vérité puis en listant quelques biais cognitifs régulièrement exploités pour nous convaincre, nous persuader, nous influencer, voir nous manipuler.

- *À travers le rapport à la vérité*

Dans une confrontation d'opinions entre deux parties, il est naturel d'attendre que l'argumentation et la critique mutuelle fassent émerger une vérité. Cela laisse un champ immense de possibilités à explorer pour l'ensemble des participants qui prennent comme postulat de départ que leur thèse est leur vérité et que toute autre affirmation ne serait au mieux qu'une erreur de la partie adverse. L'abandon de sa thèse n'est alors pas une option envisageable. Pour Arthur Schopenhauer, « la vérité objective d'une proposition et la validité de celle-ci sur le plan de l'approbation des opposants et des auditeurs sont deux choses bien distinctes[44] ». Il n'existe donc pas une seule vérité, mais plutôt des opinions, des convictions à faire évoluer, jusqu'à les faire converger. Pour le Robert, la vérité est « ce à quoi l'esprit peut et doit donner son assentiment, par suite d'un rapport de conformité avec l'objet de pensée, d'une cohérence interne de la pensée »[45]. Le Larousse nous indique qu'elle est une « adéquation entre la réalité et l'homme qui la pense », mais également une « idée, proposition qui emporte l'assentiment général ou s'accorde avec le sentiment que quelqu'un a de la réalité ». La vérité n'est donc pas unique. Il faut l'accoucher[46] par une « joute intellectuelle »[47].

La réalité, c'est ce qui continue d'exister lorsque l'on cesse d'y croire.
Philip K. Dick, 1978

Déjà Aristote répète que l'on « traite philosophiquement les thèses en fonction de la vérité, et dialectiquement en fonction de l'apparence ou de l'appropriation de l'opinion des autres »[48], là où Schopenhauer rappelle que « celui qui sort vainqueur de débat doit bien souvent sa victoire non pas tant à la justesse de son jugement quand il soutient sa thèse, qu'à l'astuce et à l'adresse avec lesquelles il l'a défendue ». Il convient donc de définir que la vérité peut-être appelée comme telle quand l'affirmation qui la compose s'appuie sur un

[43] Arthur Schopenhauer, L'art d'avoir toujours raison.
[44] Ibid.
45 Dictionnaire Le Robert
46 Mayeuthique de Socrate
47 Arthur Schopenhauer, ibid.
48 Aristote (Topiques, 1, chap.12)

raisonnement prenant comme matière première des preuves acceptées par tous les opposants[49].

…dans les règles de ce combat, on ne doit pas tenir compte de la vérité objective parce qu'on ignore la plupart du temps où elle se trouve…
Arthur SCHOPENHAUER

Les fondamentaux de l'influence : De nos failles cognitives

Les travaux rendant compte des réflexes génétiques ou culturels déterminant des modes de fonctionnement d'un homme soumis à son propre logiciel sont nombreux. Ils prennent leur source dans la structuration même de notre cerveau plus que dans l'éducation que nous recevons de nos parents ou notre environnement. Ces programmes fortement enfouis dans notre cortex et grâce à qui l'homme a survécu sont exploitables par ceux qui en connaissent le mode d'emploi.

Par exemple, les comportements automatiques qui ont pour premier objectif de gagner du temps et de l'énergie mentale sont soumis à des évènements déclencheurs.

Les raisons de cette optimisation nous plongent insidieusement dans une paresse intellectuelle qui pousse chacun d'entre nous à trouver les solutions les moins contraignantes. C'est ce qui pousse Neil Postman à écrire déjà en 1985 « Bien que j'estime que l'ordinateur soit une technologie grandement surestimée … ils s'en serviront comme on leur dira, à savoir sans réfléchir »[50].

Plusieurs mécanismes existent et sont régulièrement exploités par les communicants, les commerciaux, et une grande partie des professionnels ayant pour objectif de convaincre. Ces armes non létales associées aux « comportements irraisonnés des foules[51]» peuvent également servir à atteindre une cible sur un théâtre d'opération non concurrentiel et dans une guerre économique. Des chercheurs de l'université de Pennsylvanie et de l'université de Londres ont cherché à déterminer quelle devait être la masse critique d'un groupe soutenant un point de vue minoritaire, pour renverser une opinion faisant consensus. Résultat : si la minorité dépasse le seuil des 25 %, elle peut entraîner la majorité à rejoindre son point de vue.

Aujourd'hui, par rapport à nos ancêtres, nous avons gagné 3h37 de vie par jour, ce qui est colossal, et ce chiffre-là, 3h37, correspond exactement au temps passé devant la télévision. C'est-à-dire que l'espérance de vie qu'ils ont gagnée, ils le perdent à devenir con ! C'est extraordinaire, oui extraordinaire !
Michel Serres, 15/03/2013

49 Arthur Schopenhauer, ibid, « On peut en effet avoir objectivement raison quant au débat lui-même tout en ayant tort aux yeux des personnes présentes, et parfois même à ses propres yeux. »
50 Neil Postman, *Se distraire à en mourir*, Paris, Fayard, 2011.
51 Gustave Lebon, « Psychologie des foules », Paris, 1895.

Le principe de perception contrasté[52]

Le principe de perception contrastée consiste à changer le référentiel qui nous permet de juger d'une nouvelle situation qui se présente à nous.
Le choix que nous faisons est réalisé au regard d'une expérience passée ou simultanée. Ainsi nous pouvons définir si l'option proposée est acceptable. C'est ce qui nous permet de dire qu'un bien que nous désirions acquérir est « une affaire », est trop cher, ou que sa qualité est meilleure ou moindre.
Lorsque l'adéquation entre le besoin du client et le produit proposé n'est pas optimale, il faut donc préparer le terrain en présentant un bien de qualité médiocre et trop cher, qui ne pourra être accepté. Il sera ensuite plus facile de faire admettre que tous les autres produits perçus comme ayant un rapport qualité/prix acceptable sont au-delà des exigences espérées par l'acquéreur.
Le principe de perception *contrastée* consiste donc à changer le référentiel qui nous permet de juger d'une nouvelle situation qui se présente à nous.

La réciprocité

La règle de la réciprocité consiste à créer le sentiment d'une dette qui devra être payée. C'est ce mécanisme qui explique que l'on s'efforce à envoyer des cadeaux aux amis qui nous en auraient offert un pour un anniversaire par exemple. Ou encore, cette habitude de ne pas venir « les mains vides » lorsque nous sommes invités à un repas. « Le fait de recevoir crée une dette ; d'où le double sens du mot obligé[53] ». Deux définitions sont intéressantes à rappeler.

52 Robert Cialdini, n'identifie pas le principe de contraste comme une catégorie en tant que telle dans son ouvrage, mais s'y réfère en introduction pour mettre en évidence les comportements automatiques.
53 Robert B. Cialdini, *Influence & Manipulation*, Pocket, Paris, 2014.

- Obligé : Personne à qui on a rendu service, qui est lié par la reconnaissance à quelqu'un : Il est mon obligé en cette affaire ;
- Redevable : "Nous vous serions obligés de bien vouloir nous transmettre ces données".

Également connus des ONG, nous pouvons retrouver l'application de cette règle dans leurs communications. Au-delà de l'émotion et de la réalité du terrain, quel occidental, directement visé ou non, ne sait jamais senti concerné par cette accroche :

« Tandis que des millions de personnes ne mangent pas à leur faim, 672 millions d'autres sont obèses, et 1,3 milliard sont en surpoids. Nous avons le pouvoir de changer les choses ***».***

Ou encore, dans le tract des « Anonymes des colis du cœur » : ***« Manger est un besoin essentiel pour tous, donnez à ceux qui n'ont pas cette chance ».***

Figure 16 Exemple de communication basée sur la réciprocité

Engagement et cohérence

Lorsque nous prenons un engagement vis-à-vis de quelqu'un et dans un contexte donné, les décisions suivantes mettront nos sentiments et nos opinions en cohérence avec la première. « Une fois notre opinion faite sur une question quelconque, la cohérence obstinée nous offre un luxe bien agréable : nous n'avons plus à réfléchir sur la question »[54] . Utilisée par l'armée chinoise, cette technique s'est montrée fortement efficace pour endoctriner les soldats américains au Vietnam.

L'engagement cohérence est particulièrement puissant s'il est écrit et s'il est public : « Nous restons fidèles à nos choix si nous les avons exprimés publiquement ». Cette spécificité en fait un biais très pertinent dans le cadre des réseaux sociaux qui se transforment ainsi en vaste chambre d'écho.

La preuve sociale

La preuve sociale, ou l'influence sociale est un biais de conformité. Il s'agit de la tendance à croire qu'un comportement est approprié à partir du moment où d'autres l'adoptent. Nous cherchons à confirmer qu'un autre ferait la même chose à notre place. Il dénote un manque de confiance en nous.

54 Influence & Manipulation, ibid.

- « 95% des gens sont des imitateurs de nature et 5% des innovateurs »[55]
  Il s'agit d'un des biais les plus utilisés dans les réseaux sociaux.

Le biais de confirmation

Nous nous entourons au quotidien des personnes qui nous ressemblent, avec qui nous partageons les mêmes activités, et laissons peu de temps pour ce qui n'entre pas dans notre bulle de confort. Nous suivons les comptes Twitter des personnes dont les publications nous intéressent. Nous avons des points communs avec nos amis Facebook, et Google sait ce que nous avons l'habitude de rechercher.
Les algorithmes de ces plateformes publicitaires cachées sous des moteurs de recherches ou des réseaux sociaux nous encouragent à continuer dans les voies que nous arpentons en minimisant les contenus qui pourraient nous offrir d'autres réflexions. Comme le rappel Caroline Faillet, « l'individu face à la rumeur aura davantage tendance à rechercher les phénomènes qui semblent confirmer plutôt que ceux qui pourraient l'infirmer[56] ». Les fonctions de « Like », « j'aime », et autre mises en valeur de contenu permettent ainsi aux auteurs de contenus de bénéficier d'une audience rapide.

La fonction Google Suggest permet d'avoir des suggestions de saisie sur la requête en cours.

Figure 17 Le moteur de google suggest en action

L'effet halo

Il s'agit de la tendance à juger une caractéristique de quelqu'un sur la base d'une autre, qu'elle soit liée ou non. Par exemple, estimer qu'une personne experte dans un domaine de compétence l'est également dans un autre complètement étranger au premier.

Il existe encore bien d'autre biais que nous n'abordons pas ici, tel que l'aisance cognitive (impact le sentiment que l'on a à propos d'une information en fonction de l'aisance avec laquelle nous l'avons traitée) ; biais de croyance (tendance à juger de la logique d'un argument par la croyance en la vérité ou la fausseté de la conclusion. La croyance remplace la logique) …

55 Influence & Manipulation, Ibid.
56 Caroline FAILLET, *L'art de la guerre digitale*, Paris, Dunod,2016, p127.

Conclusion

La guerre économique est une lutte pour la suprématie se matérialisant de plusieurs manières. La lutte informationnelle est une partie intégrante de cette guerre et s'incarne à travers ce que nous avons identifié et défini comme des Espaces Informationnels Autonomes (EIA).
L'existence de zones d'autonomie temporaires "à l'intersection de plusieurs forces"[57] n'est pas nouvelle. Il s'agit de poches de résistance animées par des logiques d'occupation de terrain (physique et cognitifs) et destinées à faire pression sur des élites, des gouvernants, des incarnations du pouvoir, des idées. La ZAD de Notre-Dame des Landes en est un bon exemple, facile à représenter. Cette zone s'incarnait dans l'occupation concrète et physique du territoire, mais également dans son combat pour offrir un mode de société alternatif à celui régi par l'échange marchand (à confirmer).

L'information est alors une donnée clé lorsqu'il s'agit de gagner l'opinion et de renverser les logiques de pouvoir. Dans cette lutte, la manipulation de l'information s'inscrit alors dans la stratégie de conquête.
Les développements de la technologie ayant mené à la création d'un cyberespace omniprésent, transcendant les géographies, ont permis l'émergence de nombreux EIA. Ces zones autrefois ardues à créer et à maintenir, nécessitant une forte implication de ses membres et des ressources continues, sont désormais actives à une toute autre échelle. La technologie a agi comme un levier sur la taille et le nombre d'EIA. Ces espaces utilisent aujourd'hui la mobilisation d'individus à travers des communautés d'intérêts par le réseau virtuel créé par l'Internet et celui, plus concret, de ses membres dans leurs existences hors-lignes. Les sujets soulevés peuvent ainsi prendre une ampleur de nature à remettre en question des pratiques ou des états de fait.
Ils sont à la fois mis en œuvre par des états, des entreprises, des groupes d'intérêt ou des individus et prennent ainsi toute leur place dans une étude liée aux pratiques de la guerre économique.

57 Hakim BEY,*TAZ, Zone autonome temporaire*, Paris, édition L'éclat, 2000.