Le concept de guerre sociétale : mutation des *political & information warfares*

Abstract (English version)

This article describes the contemporary levers of societal shaping and destabilization induced by information & political warfares' operations. The described mechanisms are largely based on the methodologies implemented for, on the one hand, military influence operations and, on the other hand, disinformation operations that have targeted electoral systems in the past years.

It therefore tackle specific mechanisms related to : psychological operations, cyber actions, psycho-cognitive and socio-economic individuals targeting, as well as methods of institutions' delegitimization and actors' radicalization. By putting into perspective these vectors of destabilization with the Russian and American doctrines of both civil and military influence, the analysis concludes to the existence of a new type of low intensity conflictuality : the societal warfare. The distinctiveness of societal warfare does not lie in the assets that are deployed, but rather in the mechanisms used for and by the destabilization of the societal chessboard.

The societal warfare is characterized by a diffuse and subversive conflictuality, with a singular temporality, and coming under more sociological approaches. In doing so, classic approaches of intelligence and counter-interference only imperfectly detect the destabilizing potential of this type of attack. The nature of societal modeling mechanisms is more in line with the traditions of public relations, strategic communication and market shaping. Contemporaneous military operations would benefit from this civilian legacy.

Societal warfare is therefore likely to be a spreading mode of conflict, used by secret services, political groups, radicalized communities as well as rogue-like companies. To protect society from a manipulated alteration of its social pact, it is necessary to build an informational resilience on a societal scale.

The last part of the article makes the following recommendations : a strengthening of the « influence » specialty in the intelligence and counter-interference ecosystem (3.1), an adaptation of civic education to the new citizenship challenges (3.2), and the development of companies' societal resilience capacities (3.3).

Avant-propos

Le modèle sociétal occidental est régulièrement mis à l'épreuve, et serait entré en crise. Derrière ce constat se cachent des mécanismes précis de déstabilisation reposant sur la diffusion d'informations fausses ou manipulées et des actions d'influence. Cette

conflictualité de basse intensité s'est renouvelée pour cibler avec précision les ancrages fondamentaux de nos sociétés.

En se plaçant sur l'échiquier sociétal, les actions de déstabilisation vont davantage tirer profit des contradictions internes du modèle ciblé. L'exploitation de ces vulnérabilités a été facilité par le rôle fondamental de l'information, des médias et du numérique dans les sociétés post-modernes. A cela s'est ajouté le profilage de masse, permis par la captation de plus en plus importante d'informations personnelles et l'amélioration croissante des capacités d'analyse. La communication digitale, l'e-influence et l'ingénierie sociale ne sont plus l'apanage des directions marketing et communications des entreprises. Partis politiques, organisations non-gouvernementales, associations, groupes autonomes s'affrontent pour modéliser l'espace sociétal. Si les interactions de ces acteurs étaient initialement perçues comme un signe de démocratisation de la société, elles peuvent aujourd'hui constituer un signal faible de la déstabilisation de l'État ou de la fracturation de la Société. Cette guerre sociétale n'est évidemment pas exempte d'une exploitation plus ou moins marquée par des services clandestins à des fins d'ingérence et de guerre économique.

L'application de la dialectique militaire aux affrontements sociétaux offre des grilles d'analyse particulièrement adaptées à l'étude des rapports de force et jeux d'influence à l'œuvre dans les stratégies de déstabilisation. Si les armées ont depuis longtemps recours à des techniques de guerre sociétale, la ruse ou la déception ne leur étant pas étrangères, la guerre sociétale se démarque par l'utilisation de moyens non militaires (s'inscrivant dans le continuum *hybrid - non linear - political warfare*), alliant les techniques classiques de la guerre informationnelle et des opérations psychologiques, augmentées par des actions numériques.

Le concept de guerre sociétale permet d'établir la jonction entre les conflits de très faible intensité et l'affrontement des acteurs sociétaux. La contre-ingérence et la contre-influence répondent à des impératifs de sécurité nationale obligeant à la mise en place de priorités. La guerre sociétale tire justement parti de cette situation et parie sur l'incapacité de l'État à mettre de lui-même en place une résilience sociétale. Cette approche holistique est d'autant plus difficile à concevoir qu'elle suppose un décloisonnement des silos traditionnels et une autonomisation de la société civile.

Dans ce contexte, une première étape de conceptualisation (1) et de description des mécanismes de la guerre sociétale (2) permettra d'identifier des stratégies de construction d'une résilience sociétale (3).

1. Conceptualisation de la guerre sociétale

La guerre sociétale est une nouvelle guerre du temps de paix (1.1) dont l'objet est spécifiquement de saper les fondements sociétaux d'un État ou d'une communauté cible (1.2) en reprenant des modes opératoires de basse intensité (1.3).

1.1. Un nouvel exemple de guerre non linéaire : temporalité et logique d'échiquier

La guerre sociétale, une guerre perpétuelle ?

L'acception la plus communément partagée de la guerre est celle d'une période de conflictualité armée entre États. A la fin du XXe siècle, les conflits évoluèrent et les doctrines militaires se sont articulées autour de nouveaux concepts : les guerres asymétriques, les guerres hybrides et enfin les guerres non linéaires. Les concepts d'hybridation et de dé-linéarisation traduisent non seulement une diversification des modalités d'actions mais également un effacement des frontières temporelles. La Russie a exploré ce nouveau champ de conflictualité pour l'intégrer dans sa stratégie d'influence en Europe [1], et l'a étendu à l'ensemble des théâtres d'opérations contemporains (Syrie, Afrique centrale, Arc Sahélo-Saharien, Venezuela).

Sur le champ temporel, la guerre sociétale s'inscrit dans la tradition des guerres du temps de paix à l'image de la guerre économique, de la guerre informationnelle et de la guerre politique. Ces types de conflictualités sont évidemment présents dans le temps de guerre, mais ils se singularisent par leur continuation dans le temps de paix. Il en résulte un stress chronique des États et des Sociétés qui ne sont structurellement pas construites de façon à résister perpétuellement. Cette permanence de la menace sociétale nécessite l'édification d'une résilience spécifique.

Enfin, l'adaptation des stratégies de résilience interroge également celle des politiques de sécurité nationale. L'approche classique de la guerre privilégie une résilience active, répondant à des attaques circonscrites dans le temps. Mais s'agissant d'une menace perpétuelle, mobilisant qui plus est des vulnérabilités difficilement identifiables, une résilience passive soutenue par une veille plus performante semble plus adéquate.

L'échiquier sociétal, du vecteur au théâtre de déstabilisation

La guerre sociétale participe du phénomène d'hybridation de la guerre, visant à mobiliser tous les moyens possibles pour atteindre l'état final recherché. Cette globalisation à l'échelle sociétale du phénomène guerrier avait inspiré en 2005 au Lieutenant-Colonel MONNERAT de l'armée suisse la formule de « *guerres sociétales* » : *« De ce fait, la guerre est devenue plus que totale : elle est désormais sociétale. Ce sont toutes les ressources non plus des seules nations, mais bien celles des sociétés, des collectivités organisées autour d'une identité commune, qui sont engagées ou visées. La guerre classique entre formations militaires est devenue une exception, une entreprise bien trop risquée pour être acceptée autrement qu'en dernier ressort, et dont le plus souvent aucun vainqueur n'émerge. La conquête du territoire, mode opératoire classique des guerres, est presque entièrement supplantée par celle des marchés et des esprits »* [2]. Sans entrer dans une logique d'échiquier qui pousse à singulariser la conflictualité sociétale, le Lieutenant-Colonel MONNERAT avait dès la première décennie du XXIe siècle relevé l'importance des opérations psychologiques (PsyOps) et leur introduction dans la sphère socio-économique. L'hybridation n'était plus uniquement une utilisation de moyens civils, elle induisait un renouvellement des opérations militaires d'influence. Pourtant la réalité de l'apport stratégique de l'hybridation et de la

globalisation du champ de bataille est questionnée. Le Dr. Christopher PAUL, expert en sciences sociales de la RAND Corporation et analyste comportemental pour le *U.S. Departement of Defense*, critiquera d'ailleurs avec pertinence cette approche dans son article « *Confessions of a hybrid warfare skeptic* » [3]. En effet, la planification militaire n'a pas attendu la doctrine du XXIe siècle pour comprendre l'intérêt de l'hybridation de la guerre. Il n'en reste pas moins que cet effort de conceptualisation permet de recentrer l'institution militaire sur la conflictualité de basse intensité en ce qu'elle joue un rôle toujours plus central dans les conflits du XXI^{e} siècle. Peut-être sera-t-il nécessaire d'opérer une bascule paradigmatique dans laquelle l'influence militaire sera au cœur de la planification stratégique, et les autres capacités ne seront déployées qu'en soutien. Ce faisant, les armées ont cherché à s'adapter pour développer les opérations militaires d'influence (OMI) : création de parcours spécialisés (PsyOps et Influence), diversification des unités, renforcement capacitaire dans le cyberespace, et plus récemment aux États-Unis un renouveau des opérations d'influence en dehors du cyberespace [4].

L'hybridation et la dé-linéarisation de la guerre ne sont pas pour autant les piliers de la guerre sociétale. Son intérêt porte sur la diversification des modes opératoires et ses conséquences sur les interactions intra-civiles. A l'image de la guerre économique, les relations de puissance n'opposent pas nécessairement des acteurs étatiques. La théorie des échiquiers permet de souligner la singularité de la guerre sociétale et de détecter les opérations d'influence qu'elle génère. Dans le prolongement de la pensée socio-économique de Max WEBER, M. Christian HARBULOT identifie trois échiquiers : étatique, économique et sociétal. Ces échiquiers permettent une ventilation des acteurs interagissant ensemble, à la fois en intra-échiquier et en inter-échiquier. La complexité vient de ce que chaque échiquier répond à une normativité qui lui est propre. La guerre sociétale vise essentiellement à théoriser les mécanismes conflictuels propres à la déstabilisation par l'échiquier sociétal.

De l'hybridation de la guerre aux guerres politiques et sociétales

Cette guerre ne poursuit pas nécessairement des objectifs militaires et se veut proche de la *Political Warfare* décrite par le Pr. Mark GALEOTTI [5] dont le but est de perturber le processus décisionnel d'un État cible afin d'altérer ses capacités défensives et prédictives. La guerre sociétale s'attache davantage à la re-modélisation de l'environnement sociétal d'une cible. Il s'agit moins d'une atteinte à son processus décisionnel que d'une réduction de son influence dans son propre cercle de confiance. Les opérations de guerre sociétale interviennent souvent en soutien de la guerre politique sans pour autant coïncider avec elle. Les exemples de guerres politiques présentés par le Pr. Mark GALEOTTI (op. cit.) révèlent des marqueurs de conflictualité sociétale et renforcent l'idée d'une complémentarité opérationnelle.

1.2. Conflictualité diffuse et travail de sape des fondements sociétaux

L'objet de la guerre sociétale n'est pas cinétique par nature. La guerre sociétale relève d'une conflictualité à la fois de diffuse et de basse intensité, visant à saper les fondements

sociétaux et à déstabiliser une cible par la redéfinition de son environnement sociétal. Le processus de transformation est long et implique une modification du référentiel de valeur des groupes humains ciblés, voire de l'ensemble du « contrat social » au sens rousseauiste [6]. L'ancrage cognitif est profond et ses effets participent d'une modification collective des perceptions ou des comportements.

Les opérations de guerre sociétale ont ainsi une temporalité beaucoup plus longue. Cette lenteur de mise en œuvre en fait justement un instrument particulièrement subversif. La subtilité des variations du référentiel sociétal permet de passer sous le seuil de sensibilité des services de contre-ingérence et réduit la capacité de réponse étatique. Il s'agit, selon une métaphore de Christian HARBULOT, de « *construire une jungle cognitive pour atteindre les lignes de fractures de l'adversaire* ».

L'apport stratégique étasunien (stratégie du fort) : les tactiques de modélisations sociétales et de nation shaping

L'intérêt des processus de modélisation avait déjà été souligné par Edward BERNAYS et Noam CHOMSKY lorsqu'ils développèrent respectivement les techniques américaines de relations publiques et *market shaping* (guerre économique) [7] et par fabrication du consentement collectif (guerre de l'information) [8]. Cette tradition américaine de modélisation environnementale pourrait avoir facilité leurs politiques de *nation building*. A cet égard, le plan Marshall constituait une formidable opération de guerre économique et sociétale, structurant durablement les sociétés européennes et implantant une dépendance stratégique toujours active. L'exemple du *nation building* (*nation shaping* serait plus approprié) est d'autant plus intéressant que la mise sous dépendance et la reconfiguration sociétale ont eu des externalités positives notables pour les cibles. Outre l'impérieux besoin de reconstruction des nations européennes au sortir de la Seconde Guerre mondiale, la sociétalisation de cette opération d'influence pourrait avoir contribuer à son acceptabilité. Il n'en reste pas moins que les stratégies de reconstruction ou de modélisation ne sont pas anodines. Le « *Beginner's Guide to Nation-building* » publié par la RAND Corporation [9] illustre l'ambiguïté que peuvent avoir les opérations de guerre sociétale. Ce mode opératoire étatsunien se distingue ainsi par une convergence des objectifs opérationnels de mise en dépendance stratégique et de stabilisation de la cible. D'où l'idée d'une stratégie relevant davantage d'une modélisation que d'une déstabilisation.

La réponse stratégique russe (stratégie du faible) : les tactiques de disruption et de déstabilisation sociétale

A l'inverse, la stratégie de guerre sociétale la plus courante réside dans le déploiement d'un processus de déstabilisation. Celui-ci prend la forme d'une délégitimation des autorités ciblées, d'une fracturation du sentiment d'appartenance à une communauté nationale, et de l'exacerbation du « *narcissisme de la petite différence* » selon la formule de Sigmund FREUD [10]. Les doctrines russes de la Maskarovia (маскировка / mascarade : utilisation de la ruse pour tromper l'adversaire) [11], Primakov et Guerasimov (utilisation de vecteurs non militaires pour atteindre l'état final recherché en temps de guerre ou de paix) [12] s'inscrivent dans cette logique déstabilisatrice.

Un paradoxe de la pensée doctrinale russe réside justement dans cette tradition de la démilitarisation des guerres. Inverser la grille de lecture de la traduction russe met en évidence une faiblesse conceptuelle de l'influence militaire russe : la Russie a un penchant pour la militarisation des conflictualités civiles. Alors que les stratèges occidentaux, et notamment otaniens, voyaient dans les doctrines russes une innovation subversive majeure. En matière de guerre sociétale, le tropisme militariste russe apparait au contraire comme une faiblesse idéologique.

Un certain nombre de facteurs expliquent cette tendance, notamment le poids historique de l'institution militaire russe et des services spécialisés, l'importance du complexe militaro-industriel dans l'échiquier économique russe, mais également l'intégration des stratégies du faible au fort dans sa volonté de puissance. Ainsi la Russie appréhende essentiellement les rapports de force sous l'angle de l'échiquier étatique, et va tendanciellement militariser ses interactions sur les autres échiquiers liés à ses intérêts vitaux. La Russie en est ainsi venue à accumuler une forte expérience des guerres politiques et sociétales (*Political and Societal Warfare*), mais tout en les militarisant à outrance.

Décorrélation de la guerre sociétale et des ingérences étrangères : l'approche sociologique

Or, la guerre sociétale innove justement par sa capacité à être conduite par des organismes qui ne sont ni militaires, ni étatiques, ni clandestins. En instituant l'hybridation comme référentiel stratégique, c'est justement l'importance des acteurs civils qui s'estompe. Les acteurs mobilisés peuvent être identiques à ceux de la guerre hybride, mais il n'y a pas nécessairement d'ingérence étatique. Si les associations, *think tanks* et organisations non gouvernementales sont traditionnellement instrumentalisés dans des conflits interétatiques, l'échiquier sociétal peut être le théâtre de ses propres antagonismes.

L'instrumentalisation des acteurs sociétaux n'est pas un critère essentiel de la guerre sociétale mais une donnée offrant des clefs de compréhension. N'importe quelle communauté peut avoir un intérêt à redéfinir les normes, coutumes et habitus d'une Société, en d'autres termes les Institutions telles que conceptualisées par Emile DURKHEIM [13]. Contrairement à la guerre de l'information ou la guerre politique, où l'opinion et le processus décisionnel sont respectivement attaqués ou tout simplement sous influence, dans la guerre sociétale la cible est soit une Institution au sens sociologique, soit une valeur. Si le point de départ peut être provoqué par un conflit non linéaire, la guerre sociétale comporte un potentiel auto-réalisateur. L'instabilité sociétale en Turquie, en Chine et au Venezuela pourrait relever de cette logique. L'ingérence étrangère, directe ou indirecte, n'est pas un élément constitutif de la guerre sociétale, mais davantage un émulateur.

Les contradictions internes des modèles sociétaux peuvent être soulevées par des acteurs nationaux autonomes. On retrouve les mécanismes classiques de la contestation politique et sociale (rôle des partis politiques et syndicats). Mais c'est avec la conceptualisation des « nouveaux mouvements sociaux » que les sociologues français vont pressentir l'importance du potentiel déstabilisateur de l'échiquier sociétal [14]. Se pose alors la question de distinguer la guerre sociétale de la contestation socio-politique. Trois facteurs seraient à cet

égard pertinents : le refus de se placer dans un processus de régulation étatique de cette conflictualité, le glissement des modes d'action vers des actions d'influence, une radicalisation des acteurs au potentiel cinétique. Cette expertise française constitue un avantage comparatif sur les approches anglo-saxonnes (tropisme neuroscientifique), russes (hybridation) et germanique (influence économique).

Quelles conséquences opérationnelles pour la planification stratégique militaire ?

La contextualisation sociologique n'est évidemment pas une innovation. La planification des opérations psychologiques inclut cette dimension. La compréhension du facteur humain suppose à la fois une analyse psycho-cognitive et une analyse socio-économique. Les avancées notables de la neuropsychologie dans l'étude de la radicalisation et des adhésions émergentistes, analysées par Yannick BRESSAN [15], invitent à poursuivre l'analyse des facteurs exogènes impactant l'humain (c'est-à-dire des facteurs sociétaux). Pour autant, le facteur sociétal est très souvent minoré dans les actions d'influence. Cela s'explique en grande partie par la temporalité et les injonctions opérationnelles. La redéfinition d'une Institution telle que la Religion, l'Etat, le Travail, la Solidarité, *etc.*, s'incorpore difficilement dans une planification stratégique standard. Bien que la doctrine française d'« approche globale » [16] s'inscrive dans cette vision stratégique holistique, celle-ci ne répond qu'imparfaitement aux enjeux de la guerre sociétale. L'approche globale est une méthode de gestion de projet interministérielle visant à coordonner les acteurs étatiques et à concentrer leurs moyens, mais pas un outil d'orchestration des actions en fonction d'un état final recherché. Or, cette approche par effet est une spécificité de la planification stratégique militaire, dite approche « EBO » (*effect based operations*) [17].

La perspective historique semblerait inscrire la guerre sociétale dans un horizon temporel d'un à deux siècles. Pourtant, les acteurs non étatiques, notamment les entreprises, ont appris à considérablement réduire la durée des actions d'influence sociétale. La médiatisation, l'accroissement du rôle de l'information et l'accélération de sa diffusion n'ont pas uniquement servi la guerre de l'information et la modification des opinions publiques, mais elles ont également permis d'élargir la nature des actions d'influence en réduisant considérablement la durée nécessaire pour provoquer un changement du référentiel sociétal. Ce délai s'est raccourci malgré un accroissement exponentiel de la quantité d'information créées. Alors que la guerre sociétale était historiquement le signe de bascules civilisationnelles, elle est aujourd'hui un outil d'influence activable dans une perspective stratégique pluri-annualisée. Cela a permis la naissance de nouveaux acteurs, notamment les entreprises et organisations non gouvernementales, dont l'émergence a été facilitée par l'étroitesse des liens entre la guerre sociétale, la guerre de l'information, la communication stratégique et plus récemment la cyber-influence.

1.3. Des modes opératoires de basse intensité alliant influence, guerre de l'information et actions numériques

L'information joue un rôle central dans la guerre sociétale de sorte que l'on pourrait considérer qu'il s'agit d'une mutation de la guerre de l'information induite par l'accélération des sociétés. Dans le contexte spécifique de la guerre sociétale, l'information est relayée au rang de vecteur et non plus d'objectif. Guerre de l'information par le contenu, propagande, désinformation, infobésité et manipulation font partie intégrante de la guerre sociétale. L'ensemble des techniques visant à modifier la perception ou le comportement d'un individu sont utilisées dans la guerre sociétale mais l'état final recherché étant la modification d'une institution sociétale, cette altération doit perdurer dans le temps.

Le renforcement du vecteur numérique dans les actions d'influence, d'ingérence ou de déstabilisation

Le développement du cyberespace a renforcé la portée opérationnelle de la guerre sociétale contemporaine. Ainsi les belligérants ont systématisé le recours aux actions numériques d'influence pour modifier la perception de groupes cibles. Le cyberespace étant un lieu privilégié de circulation de l'information dans lequel les mécanismes d'autodéfense cognitive sont amoindris, celui-ci est un théâtre de plus en plus propice aux actions d'influence [18]. Les États font toutefois preuve d'une grande discrétion en la matière.

S'agissant du dispositif français, la quantité d'informations disponibles en source ouverte s'est accrue depuis 2019. Le Ministère des forces armées a augmenté ses recrutements et les fiches de poste mentionnent la « lutte informatique défensive » (LID), la « lutte informatique offensive » mais surtout la « lutte informatique d'influence » (L2I), à l'image des CYBER COMMAND britanniques et américains [19]. Le renforcement de la réflexion doctrinale en la matière constitue un autre signal d'accroissement d'intérêt du MINARM pour les actions d'influence dans le cyberespace [20].

La digitalisation des actions d'influence a marqué un tournant de l'hybridation de la guerre et a plus spécialement dynamisé les actions de guerre politique. L'exemple des ingérences russes dans les processus électoraux occidentaux (2016 : Brexit [21] et élection présidentielle américaine [22] ; 2017 : élection présidentielle française [23] ; 2019 : élections européennes [24] et élection présidentielle ukrainienne [25]) et africains (2018 : élection présidentielle malgache [26] ; 2019 : élection présidentielle sud-africaine [27]) a dévoilé la professionnalisation des services d'influence numérique et leur capacité à créer des écosystèmes de déstabilisation informationnelle. Le modèle d'ingérence électorale russe présente d'ailleurs des *patterns* de glissement d'une guerre politique vers une guerre sociétale.

L'une des pierres angulaires de la méthodologie de déstabilisation politique réside dans la combinaison entre la désinformation et le contrôle réflexif [28] ce qui relevait déjà de l'héritage soviétique de la *Maskarovia* comme le soulignait le Major Christian KAMPHUIS (op. cit.) et a été intégré dans la guerre non linéaire [29]. L'intérêt de la démarche russe a été d'ajouter à cette tradition une couche logique pour créer les premières actions numériques d'influence [30]. Déjà depuis les années 2000, le croisement de la sociologie et des neurosciences cognitives a fait émerger de nouvelles disciplines. L'application de la neuroscience aux sciences criminelles avait ouvert la voie au profilage et à l'identification

des schémas comportementaux, tandis que son application aux sciences économiques a produit le neuromarketing. Mais c'est dans le domaine des sciences politiques et de l'influence que leur apport aura été le plus impactant. Les sciences cognitives permettent une forte amélioration du ciblage. C'est justement cet élément qui a fait le succès d'*Aggregate IQ* et de *Cambridge Analytica*. En automatisant le ciblage grâce à de l'analyse *big data* et l'implémentation d'intelligences artificielles, ces entreprises auront interpellé les stratèges sur l'importance des capacités de calcul. Si la Russie avait démontré le potentiel disruptif de la désinformation, les États-Unis ont transposé la course aux actions d'influence numérique sur le théâtre technologique : captation des données et capacité d'analyse. Ce faisant, la mobilisation des supercalculateurs dans les prochaines campagnes d'influence sera le prochain bond technologique dans les actions d'ingérence et de déstabilisation.

La sociétalisation des actions d'influence

La lutte informatique d'influence n'en est encore qu'au stade artisanal et a vocation à sensiblement accroitre son potentiel déstabilisateur. Deux facteurs plaident pour une hausse de la menace : d'une part, la course technologique et la facilité à industrialiser le ciblage et l'orchestration des campagnes d'influence et, d'autre part, le glissement des actions numériques des *information & political warfares* vers la guerre sociétale. La première hypothèse participe du continuum Data, Intelligence artificielle, *New Space* et recherche quantique. Mais la seconde posera de nouveaux défis de résilience à l'ensemble des acteurs (États, mais aussi entreprises, organisation non gouvernementales et communautés). Les ingérences russes dans le mouvement des gilets jaunes auront marqué un tournant [31], soulevant plus généralement le problème de la désinformation sur l'échiquier sociétal [32]. Contrairement à l'accoutumée, les actions numériques russes ne se cantonnent plus à une disruption politique mais ont évolué en une déstabilisation sociétale.

Dans ce cadre le contrôle réflexif perd de son importance. Le mythe de la programmation est un biais d'analyse répandu dans les doctrines russes et américaines. Leurs courants neuroscientifiques partagent une confiance déraisonnée dans les *patterns*. Mais en matière de guerre Sociétale, autant le ciblage et les liens de causalité sont précis, autant la prédictibilité des effets reste relative. On peut ainsi considérer que l'échiquier sociétal est davantage soumis à des modélisations chaotiques au sens mathématique. En effet, l'échiquier sociétal se caractérise par une plus forte « entropie informationnelle », le distinguant ainsi des échiquiers étatique et économique. Les actions d'influence et la guerre de l'information se sont mécaniquement adaptées à cet environnement en ciblant les espaces informationnels autonomes [33].

La vulnérabilité des acteurs économiques face à la subversivité de la guerre sociétale

Si les services clandestins ont un savoir-faire historique dans la mise en place et l'orchestration d'espaces informationnels autonomes, ceci n'est pas le cas des entreprises, des organisations non gouvernementales ou des administrations publiques intermédiaires (collectivités territoriales en premier lieu). La sphère économique souffre d'une ignorance de la dimension subversive de la guerre sociétale et tend à l'analyser sous l'angle des stratégies

de communication, des affaires publiques ou de la sécurité. Or une campagne de contre-influence sociétale répond à une méthodologie particulière. Fort heureusement, la tendance actuelle dans les investissements technologiques en *web-influence* permettent d'améliorer le seuil de détection de ce type de déstabilisation par les victimes. Si les entreprises sont pour l'instant peu génératrices de guerre sociétale, cette tendance risque de s'accentuer. Le phénomène de radicalisation des acteurs non gouvernementaux et non économiques impacte d'ores et déjà l'échiquier économique. A titre illustratif, l'instrumentalisation du véganisme par l'industrie américaine de synthétisation de la viande constitue un cas de sociétalisation de la guerre économique [34].

2. Analyse des mécanismes fondamentaux de la Guerre sociétale

La guerre sociétale repose sur trois mécanismes fondamentaux : l'altération du rapport individuel au réel (2.1), l'implantation d'un processus de délégitimation de l'autorité (2.2) et l'accentuation des radicalisations (2.3). La guerre sociétale aura ainsi hérité des stratagèmes déceptifs des opérations psychologiques.

2.1. L'altération du rapport individuel au réel

L'information et les médias étant un vecteur privilégié de la guerre sociétale, l'une des étapes essentielles de déstabilisation est celle de l'altération du rapport au réel des groupes cibles. La désinformation va progressivement déconnecter l'information du réel et faire perdre à la donnée sa valeur objective. Durant cette phase, les individus cibles vont progressivement réécrire leur référentiel pour passer d'une confrontation du réel à l'expérience d'une vérité. En inondant le théâtre sociétal de fausses informations, les individus ciblés sont amenés à considérer que toute information est égale par ailleurs. Cela va faciliter la mise en place d'effets de vérité, eux-mêmes renforcés par le biais cognitif de confirmation, qui va lui-même être alimenté par le processus de radicalisation. L'effet est double : le processus de radicalisation permet l'émergence des thèses complotistes mais également de fragiliser les actions de déconstruction de la fausse information. La rapidité de ce processus est proportionnelle au degré d'autonomie de l'espace informationnel créée et au degré de résilience informationnelle et cognitive de la société.

La seconde étape vise à déplacer le terrain d'évaluation individuelle de l'information de la vérité à la légitimité. L'individu ne raisonne plus en termes de véracité de l'information mais en termes de légitimité du vecteur. La grille d'analyse informationnelle bascule du contenu de l'information vers son contenant. L'encerclement cognitif de la cible peut s'installer et les contre-mesures rationnelles (*fact checking)* vont perdre en efficacité. Il est ainsi primordial de reconnaitre les signes d'encerclement cognitifs suffisamment en amont, et donc d'optimiser la veille des acteurs sociétaux.

L'automatisation de ce processus constitue un avantage comparatif non négligeable mais elle se heurte à deux limites. La première est constitutive du vecteur informationnel. La qualification de la portée d'une attaque informationnelle est nécessairement subjective. Il est plus simple de détecter sa propagation que de percevoir le potentiel déstabilisateur

d'une information. La surveillance systématisée des médias et réseaux sociaux induit donc un retard de prise en charge. La seconde limite est liée à la migration des agents déstabilisateurs vers des espaces informationnels autonomes et clandestins.

La capacité déstabilisatrice de la guerre sociétale provient pour partie de la capacité des orchestrateurs à constituer des communautés clandestines dans la société civile. A ce stade, la veille numérique perd en effectivité pour détecter les cellules déstabilisatrices, et dépend de plus en plus d'autre sources de renseignement, qu'il soit humain (HUMINT), électromagnétique (SIGINT) ou géographique (GEOINT), mais également d'une approche davantage holistique : l'*Activity Based Intelligence* (IBA) [35]. L'étape suivante vise à paralyser les capacités de contre-influence informationnelle en créer un processus de délégitimation de l'autorité.

2.2. L'implantation d'un processus de délégitimation de l'autorité

L'offensive sociétale atteint un seuil déstabilisateur critique lorsque la légitimité des acteurs véhiculant une démonstration rationnelle et argumentée est déconstruite. Les autorités publiques sont régulièrement la cible de tentatives de délégitimation, ce qui peut constituer un signal d'ingérence.

La dimension sociétale étend les cibles de délégitimation à tout acteur faisant autorité et diffusant un contre-discours dérangeant les agents déstabilisateurs. Ordres professionnels, syndicats, organisations non gouvernementales, sont autant de sources d'autorité au sens sociologique. Ce processus est d'autant plus pernicieux qu'il a tendance à se produire par agrégation successive pour aboutir à une délégitimation des principaux acteurs de l'échiquier sociétal. Ce phénomène renforce d'ailleurs l'encerclement cognitif des cibles.

Dans ce nouveau type de guerre de l'information, l'individu n'a plus nécessairement besoin d'adhérer à une opinion. Il suffit à l'agent déstabilisateur de faire adhérer l'individu au processus de délégitimation. C'est ce que M. Christian HARBULOT nomma le « *passage de la Fabrique du consentement à la Fabrique de l'illégitimité* » en référence à l'ouvrage d'Edward HERMAN et Noam CHOMSKY (op. cit). Or, l'environnement informationnel numérique dans lequel nous évoluons a facilité la mise en place des processus de délégitimation. L'infobésité accélère le processus d'altération du rapport individuel au réel et les boucles informationnelles causées par les algorithmes favorisent la création d'encerclements cognitifs.

L'enjeu de la guerre sociétale est d'induire une modification comportementale déstabilisatrice à l'échelle collective du fait d'une attaque initialement informationnelle. En matière sociétale, la déstabilisation a tendance à prendre la forme de troubles à l'ordre public, quand bien même les autorités publiques n'étaient initialement pas ciblées par le processus de délégitimation.

A ce stade, l'action d'influence va évoluer d'un ciblage individuel avec ancrage communautaire à une extension à l'ensemble de la sphère sociétale. L'échiquier sociétal a,

de manière contre-intuitive, une tendance à essouffler l'action du fait de l'entropie informationnelle. Pour passer de l'attaque informationnelle à l'attaque sociétale, les agents déstabilisateurs vont alors accentuer la radicalisation des acteurs pour consolider et exploiter la ligne de fracture sociétale.

2.3. L'accentuation des radicalisations

La radicalisation constitue un mécanisme d'augmentation des clivages et soustrait à l'individu sa capacité à trouver un compromis. A l'échelle individuelle, la radicalisation suscite une augmentation de l'intensité des conflits et facilite le passage à l'acte. A l'échelle collective, cette propension au passage à l'acte est rendue d'autant plus forte par la polarisation de groupe [36]. Le ciblage des candidats à la radicalisation est une donnée essentielle du phénomène de radicalisation [37] et explique l'efficacité des espaces informationnels autonomes en matière de guerre sociétale. Mais c'est sous l'angle de ses effets, notamment de la modification comportementale par l'information, que la radicalisation va amplifier la guerre sociétale.

En outre, la radicalisation est un phénomène protéiforme qui s'est diversifié au XXIe siècle pour prendre des formes de plus en plus sociétales. Historiquement très présents dans les domaines politiques et religieux, les formes de radicalisation se sont progressivement répandues dans les domaines sociaux, écologiques, genristes et complotistes. Par ailleurs, la radicalisation n'aboutit pas nécessairement au basculement dans le terrorisme. La radicalisation connaît une gradation de son intensité, et n'atteint pas nécessairement un seuil cinétique. Néanmoins, le potentiel déstabilisateur de la radicalisation débute à de très faibles intensités à l'image du processus de délégitimation de l'autorité.

La qualité d'une attaque sociétale résidera justement dans la capacité à mobiliser le maximum de formes de radicalisation possibles en restant sous le seuil de détection des Institutions publiques pour créer une « floraison cinétique ». Plus cette floraison cinétique est fulgurante, moins la remédiation informationnelle devient pertinente, du moins jusqu'à la phase de stabilisation du conflit. Si cette attaque avait agrégé différents types de radicalisation de manière autonome, la crise serait d'autant plus complexe à résoudre. La force d'une attaque sur plusieurs fronts sociétaux réside dans l'affaiblissement des possibilités de remédiation informationnelle de la cible. La communication de crise de la cible aura bien du mal à trouver un axe unique de défense. Les causes étant différentes selon les types de radicalisation, il n'est généralement pas possible de trouver un dénominateur commun permettant d'affaiblir l'ensemble de l'attaque informationnelle. Or, une communication dissonante, spécialisée par communauté radicalisée, risque justement d'attiser les autres fronts informationnels. A l'inverse, si l'attaque est coordonnée, une réponse de type « *divide et impera* » [38] serait la plus adaptée. L'atomisation des pôles de radicalité, leur autonomisation d'objectifs et de ressorts de mobilisation, va atténuer l'efficacité du contre-discours. En matière de guerre sociétale, la communication stratégique repose sur une capacité d'analyse et de profilage accrue ainsi que sur une défense en profondeur

La propension de la guerre sociétale à s'appuyer sur les mouvements radicalisés conduit à repenser la stratégie défensive. L'effort principal doit résider dans une résilience informationnelle étendue à l'ensemble de la société. Ce n'est qu'à titre exceptionnel que la gestion de crise et la communication stratégique ont vocation à intervenir. Pour autant, l'absence de stratégie au niveau étatique tend à faire reposer la protection sociétale sur les acteurs non étatiques. Ce transfert de responsabilité, illustré par les politiques RSE et la construction progressive de leur opposabilité en justice [39], revient à faire peser cette charge défensive sur les entreprises. Pour autant, l'État à un rôle fondamental à jouer en matière de guerre sociétale, justement parce qu'il dispose des moyens légitimes de création d'une résilience cognitive et informationnelle à l'échelle sociétale.

3. Stratégie défensive de construction d'une résilience sociétale et informationnelle

La stratégie de défense repose à la fois sur la construction d'une résilience informationnelle dans l'ensemble de la société et sur un réarmement cognitif des individus. La guerre sociétale emprunte l'essentiel de ses modes opératoires aux opérations d'influence. Il convient donc de diffuser des logiques de contre-influence dans l'ensemble de la société. Le premier levier réside dans un renouvellement de la coopération publique en matière d'influence et de contre-ingérence (3.1). Le second vise à diffuser dans le corps social les compétences nécessaires pour résister à la diffusion d'informations fausses ou manipulées. A ce titre, l'éducation nationale (3.2) et les entreprises (3.3) disposent de solides acquis exploitables.

3.1. Renouveler la coopération publique en matière d'influence et de contre-ingérence

Qu'il s'agisse des relations trans-ministérielles, de la coopération avec les entités décentralisées, ou des relations avec l'Union européenne (UE), les problématiques d'influence et de contre-ingérence invitent à approfondir la coopération publique en lien avec la société civile.

L'Union européenne : le choix de la communication stratégique

La résilience informationnelle est devenue un enjeu de résistance à la *political warfare* conduite par la Russie en Europe. L'Union européenne s'est emparée de la question au point de créé en 2015 une *task force* dédiée à la lutte contre la désinformation, pudiquement nommée « *East StratCom* ». Cette cellule est rattachée au « *Service européen pour l'action extérieure (SEAE) afin de répondre aux campagnes de désinformation menées par la Russie* » [40]. Ce même communiqué de presse rappelle l'existence d'une coopération avec le Groupe des régulateurs européens des services de médias audiovisuels (ERGA) créé en 2014, l'adoption d'un « *plan d'action contre la désinformation* » et d'un « *code de bonne conduite* ».

Les missions de la *East StratCom* s'inscrivent dans la lignée des affaires publiques auxquelles s'ajoutent l'analyse et la déconstruction des opérations de désinformation orchestrées par la Russie [41]. La production d'un contre-discours didactique est essentielle dans le processus de réarmement cognitif des sociétés européennes. Toutefois, cette cellule n'est pas pour autant un service spécialisé dans la contre-ingérence et les actions d'influence à l'échelle européenne. Ce type de capacité relèverait de la politique européenne de sécurité, avec une mise en œuvre par les Etats membres. Pour gagner en effectivité, la résilience informationnelle européenne pourrait se baser sur une coopération entre les différents services nationaux de contre-ingérence et leurs homologues spécialisés dans les actions d'influence. A cela pourrait s'ajouter la production d'un fond doctrinal commun à l'ensemble de l'Union européenne. Le Collège du renseignement en Europe, créé le 5 mars 2019 [42], pourrait prendre une part active dans l'édification d'une doctrine européenne de contre-ingérence.

En se concentrant sur la désinformation, l'Union européenne ferme toutefois les yeux sur la problématique de l'influence des Etats-Unis et de la Chine dans le processus décisionnel européen. Le *monitoring* des dépenses de lobbying par des acteurs non européens, ainsi que la cartographie de leur *think tanks* et autres organisations non gouvernementales auraient dû alerter les institutions européennes. Certes, il ne faut pas perdre de vue la spécificité de ces deux problématiques. Une ingérence par mobilisation d'actions clandestines n'est pas comparable à l'utilisation d'actions d'influence légales. Mais il n'en reste pas moins que ces deux modes d'actions contribuent à la modélisation de la société européenne et à l'accentuation des guerres économiques et sociétales. Être conscient de cette situation ne doit pas pour autant atténuer notre propre responsabilité. N'oublions pas que l'Union européenne ne dispose pas de souveraineté propre : ce sont en réalité les Etats membres qui ont fait le choix de ne pas résister aux influences extérieures. Dans une perspective d'autonomisation stratégique de l'Europe, cette vulnérabilité n'est pas anodine. Qu'il s'agisse de la création de dépendance stratégique durable ou de déstabilisation sociétale, quels que soient les modes opératoires, l'état final recherché par les puissances étrangères n'est certainement pas un renforcement de l'autonomie stratégique européenne. Le Député Arnaud DANJEAN, rapporteur de la commission des affaires étrangères, a d'ailleurs rappelé l'importance de créer cette autonomie stratégique pour l'Europe dans un monde multipolaire [43].

Développement de la coopération entre services d'influence et de contre-ingérence

En matière d'influence, la dissociation entre les actions offensives et la contre-ingérence n'est pas évidente. La séparation organique des services s'intègre dans la logique de distinction entre actions extérieure et sécurité intérieure. Mais du point de vue des compétences nécessaires aux agents, le référentiel pédagogique de l'influence et de la contre-ingérence est beaucoup plus similaire qu'il n'y parait. Ce faisant, une coopération accrue notamment en matière de préparation opérationnelle et de formation initiale serait opportune. D'autant plus que les services compétents en matière d'influence et de contre-ingérence relèvent traditionnellement en France du premier cercle de la communauté du renseignement [44]. Ce rattachement organique s'est accentué avec la réforme de la

communauté du renseignement depuis 2009 [45], ainsi qu'avec la création en 2010 de l'Académie du renseignement [46]. Il en résulte la diffusion d'un socle commun de compétences au sein des services français de renseignement, d'influence et de contre-ingérence. Or, les approches méthodologiques du renseignement répondent davantage au référentiel de compétences de la contre-ingérence que de l'influence.

Il n'en reste pas moins que cet écosystème est propice à l'émergence d'une spécialisation des agents dans l'influence, les opérations psychologiques et les actions numériques. Cette spécialisation se justifie par la complexification des techniques d'influence, sollicitant de plus en plus les neurosciences, la psychologie, la sociologie et la cyber-influence. La valorisation de cette spécialité et la facilitation de passerelles interministérielles pour diversifier la carrière des agents, à l'image du cycle américain du renseignement, participerait d'un renforcement capacitaire à moindre coût. Permettre une passerelle entre les services d'influence à visée offensive et les services de contre-ingérence accompagnerait la diversification capacitaire de l'Etat français. Par ailleurs, force est de constater que le militaires, policiers et gendarmes ont des approches différentes de l'environnement numérique. Il serait d'ailleurs envisageable de capitaliser sur cette diversité culturelle par des exercices communs de préparation opérationnelle et la production de RETEX Influence/Contre-ingérence. Deux modes de coopérations opérationnelles seraient envisageables, voire complémentaires : des actions bilatérales interservices d'une part, et des actions centralisées auprès de l'Académie du renseignement d'autre part.

S'agissant de la coordination interservices, celle-ci relevant de la compétence du Premier ministre, elle devrait être assurée par le Secrétariat général de la défense et de la sécurité nationale (SGDSN). La création d'un service spécialisé au sein du SGDSN pourrait être bénéfique tant l'influence et la contre-ingérence sont liés à la communauté française du renseignement. Par ailleurs, le SGDSN pourrait, ce faisant, accompagner le Ministère de l'Europe et des Affaires étrangères (MEAE) dans ses discussions avec la *Task force East StratCom* du SEAE.

Penser la résilience sociétale dans la trans-ministérialité : une mission pour les HFDS ?

Soutenir le développement de l'influence et de la contre-ingérence au sein de la communauté du renseignement n'est pas en soi constitutif d'une résilience informationnelle. La diffusion de cette culture aux autres ministères et leur sensibilisation à la déstabilisation informationnelle sont une autre piste à explorer. Le réseau des hauts fonctionnaires de défense et de sécurité (HFDS) s'y prête particulièrement [47]. Outre la protection du secret de la défense nationale, de la cyber, et de la sécurité économique, les HFDS pourraient mobiliser leurs ministères sur les enjeux de résilience informationnelle et sociétale. La prise en compte de cette menace de faible intensité par les HFDS serait l'occasion de repenser la communication stratégique de leurs ministères pour inclure la surveillance et la lutte contre la désinformation. Cette sensibilisation est d'autant plus importante que les signaux de déstabilisation sont particulièrement faibles et une grille de lecture centrée sur les logiques de renseignement et de contre-ingérence intègre imparfaitement les vulnérabilités sociétales. Cette approche souligne par ailleurs l'apport

stratégique des directions de la communication et des affaires publiques, ainsi que l'opportunité de renforcer leur partenariat avec leur HFDS ministériel respectif.

Résilience sociétale et collectivités territoriales : vers une diffusion de l'intelligence territoriale ?

La nature de la guerre sociétale fait des collectivités territoriales l'échelon de représentation de l'autorité publique le plus exposé à la déstabilisation sociétale. Les collectivités ont des moyens très limités de détection des espaces informationnels autonomes, ne disposent que rarement de moyens de communication stratégique, et ont une vulnérabilité accrue du fait de leur lien avec l'environnement sociétal. Les collectivités territoriales ont donc tout intérêt à diversifier leurs interactions avec l'échiquier sociétal.

A l'inverse les agents déstabilisateurs ont tout intérêt à cibler les collectivités territoriales pour provoquer ne défaillance voire une corruption de l'autorité publique. Dans ce contexte les collectivités territoriales perdent leur fonction régulatrice, et participent au contraire à la déstabilisation de leur environnement sociétal. C'est ce que l'on peut observer sur le territoire national dans les communes où le crime organisé et les cellules radicalisés ont soutenus les élus locaux. Résoudre cette incompatibilité ne peut se faire en uniquement par une approche sécuritaire. Des actions de modélisation sociétale, et non pas uniquement développement socio-économique, sont nécessaires.

Par ailleurs, sur des territoires moins exposés, le développement d'une résilience sociétale peut au contraire accroitre les bénéfices d'une bonne gouvernance déjà installée. L'approche sociétale va alors pousser à développer tant l'intelligence territoriale que la réflexivité territoriale [48]. Le développement des *smart cities* participe de cette synergie en intégrant une approche spatiale, des enjeux d'influence numérique, et en modifiant la perception et le comportement des administrés.

3.2. L'éducation des jeunes générations au décryptage des informations fausses ou manipulées

Quelle éducation civique à l'ère du numérique et des attaques informationnelles ?

L'enseignement de l'éducation civique est une étape fondamentale de la construction de l'identité citoyenne. Traditionnellement centrée sur la transmission du référentiel de valeur de l'Etat de droit et du modèle républicain, elle véhicule la notion moderne de démocratie.

L'éducation civique a évolué en 2015 en « Education civique et morale » (EMC), à la suite de l'entrée en application de la loi d'orientation et de programmation pour la refondation de l'École de la République du 8 juillet 2013 [49]. L'ancrage moral de la nouvelle éducation civique revêt un sens particulier dans la France du début du XXI^{e} siècle. La radicalisation religieuse est depuis une vingtaine d'année un défi majeur pour la Sécurité nationale contemporaine. La vague d'attentats terroristes islamiste a dévoilé le potentiel cinétique d'une transformation sociétale. Ainsi, il importait de refonder une concorde, un socle de

valeurs communes, capable de transcender les identités religieuses en cours de radicalisation. La substitution d'un enseignement d'une morale laïque à l'échelle nationale devait lutter contre la radicalisation et le communautarisme. Ainsi l'évolution de l'éducation civique en EMC, marqua l'intérêt opérationnel de l'éducation civique. Si la guerre sociétale peut sembler abstraite et difficilement palpable, l'analyse du processus de radicalisation islamique sur les 30 dernières années souligne l'impérieuse nécessité de prendre ce type de conflictualité en compte. Cela est aujourd'hui renforcé par la diversification des types de radicalisation.

Cet exemple souligne la flexibilité et l'utilité opérationnelle de l'éducation civique dans une stratégie de défense sociétale. Le vecteur contemporain de déstabilisation n'est plus seulement religieux, mais également informationnel. Les ingérences répétées dans les processus électoraux, le rôle des *Data Driven Campaigns*, de la collecte de données personnelles, et le recours massif à la désinformation, sont autant de nouveaux enjeux auquel l'éducation civique doit préparer nos futurs citoyens.

Les affaires *Aggregate IQ* [50] et *Cambridge Analytica* [51] auront dévoilé au grand public comment l'utilisation des méthodologies relevant des opérations psychologiques pouvait altérer le processus démocratique. L'éducation civique doit aujourd'hui s'adapter aux effets de la numérisation de la société.

L'éducation aux médias et à l'information (EMI) : un vecteur stratégique de résilience sociétale sous-exploité

L'édification d'une résilience informationnelle à l'échelle sociétale est un processus long mais redoutable. Long parce que la sensibilisation de l'ensemble des acteurs ne dépend pas uniquement de politiques publiques. Redoutable par la diversité des externalités positives qu'il produit et notamment sur la gouvernance : développement de capacité d'analyse, adhésion au modèle de l'Etat de droit, stabilisation de la société et renforcement du pacte social. A l'image de l'écologie, concentrer l'effort sur certaines générations s'avère particulièrement efficace, notamment lorsqu'il s'agit des plus jeunes (élèves de primaire et de secondaire).

L'éducation nationale est un levier particulièrement adapté dans cette tâche. Les programmes d'éducation aux médias et à l'information (EMI) s'inscrivent d'ores et déjà dans cette perspective. L'EMI permet entre autres « *aux élèves d'apprendre à lire, à décrypter l'information et l'image, à aiguiser leur esprit critique, à se forger une opinion, compétences essentielles pour exercer une citoyenneté éclairée et responsable en démocratie* » [52]. Cet enseignement répond parfaitement aux enjeux de l'éducation civique à l'ère numérique.

Une démarche pédagogique par pallier alliant sensibilisation à l'intox en primaire, intégration des problématiques de citoyenneté (*Fake news* et Démocratie) et de la vie privée (*Privacy* et collecte de données personnelles) à partir du collège, avec éventuellement une mise en perspective avec les enjeux internationaux à partir du lycée (intox, propagande et manipulation dans l'Histoire et les relations internationales) pourrait facilement se construire. Le Centre de Liaison de l'Enseignement et des Médias d'Information (CLEMI),

créé dès 1982, centralise d'importantes ressources pédagogiques et a récemment publié son référentiel de formation des enseignants [53].

L'impérieuse nécessité de procéder à la généralisation de l'enseignement de l'éducation aux médias et à l'information

Le savoir-faire français en matière d'EMI a d'ailleurs été reconnu par l'UNESCO en 2017 (remise du *Global Media and Information Literacy Award* à l'institutrice Rose-Marie FARINELLA, anciennement journaliste [54]) et par le Parlement européen. Malgré la qualité des initiatives individuelles d'enseignants et le perfectionnement des ressources pédagogiques, l'enseignement de l'EMI n'est toujours pas généralisé sur le territoire national. Sont en cause : une insuffisance du vivier d'enseignants du primaire et du secondaire formés à l'EMI, une absence de l'EMI dans la formation initiale et continue des enseignants, et un manque d'ambition du rôle pédagogique des documentalistes.

Alors que l'Europe subit de plein fouet les campagnes de désinformation des puissances étrangères, au point de créer une Task Force *East StratCom*, la généralisation de l'enseignement aux médias et à l'information tarde. Certes, les moyens ne sont pas infinis et le Ministère de l'Education nationale a toujours eu raison d'insister sur les fondamentaux. Mais à l'heure où le cyberespace informationnel devient un vecteur majeur de déstabilisation de nos sociétés, les priorités doivent s'ajuster.

Si le Ministère de l'éducation nationale pourrait être tenté d'y voir un énième centre de coût, force est de constater que l'EMI est également un formidable outil de diplomatie d'influence. Le savoir-faire de la poignée d'enseignants qui se sont investis dans l'EMI est déjà reconnu par les organisations internationales, s'exporte en Afrique et dans la Péninsule arabique. Plus encore, la diffusion de l'EMI participe indirectement à celle de la francophonie. En spécialisant son enseignement en fonction des spécificités linguistiques, de la culture de l'oralité, de la place des différents médias dans la société, l'EMI participe au rayonnement culturel français. A ce titre, l'Education nationale pourrait en la matière trouver des alliés auprès du MEAE et du Ministère de la Culture. Une initiative conjointe de ces différents ministères auprès de l'Organisation Internationale de la Francophonie pourrait à la fois participer au rayonnement de l'influence française et à la diffusion de l'EMI dans l'ensemble des pays francophones.

3.3. La résilience sociétale des entreprises par l'intelligence économique et les politiques RSE

Les entreprises se distinguent dans la guerre sociétale par une meilleure capacité d'adaptation à l'évolution de leur environnement. Les *business* et *market intelligences* ont fourni aux entreprises des capacités d'observation et d'analyse de leur environnement. L'intelligence économique (IE), dans son acception française [55], participe de la construction d'une résilience sociétale des entreprises. Encore faudrait-il que celle-ci pénètre davantage le tissu des PME. Fédérations professionnelles, chambres consulaires et service économique des Régions ont un rôle particulier à jouer dans l'accompagnement des

PME. Enfin, s'agissant des entreprises plus matures sur les questions d'intelligence économique, la responsabilité sociale et environnementale des entreprises (RSE) constitue un gisement de résilience sociétale exploitable.

Une stratégie spécifique pour les PME fondée sur la sensibilisation et le regroupement

La sensibilisation et l'accès des PME à l'intelligence économique a depuis ses débuts fait face à un certain scepticisme, bien que son utilité ne soit pas remise en cause[56]. Les dirigeants de PME perçoivent l'IE comme un centre de coût au retour sur investissement difficile à évaluer et qui ferait double emploi avec la fonction commerciale. La fonction IE leur apparait comme une dépense somptuaire. Le biais des coûts irrécupérables [57] joue d'ailleurs en défaveur d'une réforme organisationnelle des PME.

Pour autant, le développement de la fonction IE participe de deux logiques : l'optimisation des coûts et le *business development*. Les outils et méthodes mobilisés par l'IE accroissent l'interopérabilité des fonctions métiers de l'entreprise et contribuent à faire du *knowledge management* un outil d'aide à la décision stratégique. Dans cette optique, l'IE intervient comme vecteur de rationalisation des processus et de concentration des moyens. Le retour sur investissement est donc directement quantifiable. Sans compter que l'IE participe du renforcement sécuritaire de l'entreprise, tout en accroissant son agilité, ainsi qu'une meilleure intégration des personnels à leur tour mobilisés autour de la pérennité de leur entreprise. Rares sont les leviers d'optimisation qui transforment la sécurité et la sûreté en vecteurs de souplesse tout en faisant muter un centre de coûts en gisement de croissance.

La guerre sociétale accentue la nécessité d'une résilience des entreprises. Par sa transversalité et sa proximité avec la stratégie et la sûreté-sécurité, l'IE est un vecteur sous-exploité par les PME. Mais outre la résilience, c'est également l'influence de l'entreprise dans son environnement sociétal qui est en jeu. L'ancrage territorial est une nécessité pour les PME. La co-construction avec les autorités publiques d'une intelligence territoriale permet de réduire le risque de déstabilisation sociétale tout en renforçant l'influence de l'entreprise. Or, dans une économie fortement polarisée (taille d'entreprises, répartition territoriale, accès aux financements), le développement des capacités d'influence des PME est un enjeu majeur de stabilisation sociétale. Les externalités négatives issues de la croissance d'une entreprise sont moins importantes lorsqu'il s'agit de PME. Il peut d'ailleurs être opportun de repenser les interactions entre PME et Grandes entreprises pour améliorer leur impact sociétal et créer une coopération symbiotique. L'apport stratégique de l'IE aux PME est tel que même sa mutualisation reste préférable à son absence. L'externalisation de cette compétence a un groupement d'entreprise apparait comme une solution temporaire efficace. Bien entendu, le caractère stratégique des échanges demande la mise en place d'un protocole renforcé. Cette démarche conduit généralement l'entreprise à repenser son écosystème de confiance. C'est ce renouvellement de la pensée stratégique de l'entreprise qui va justement contribuer à la résilience sociétale des entreprises et des territoires.

L'utilisation stratégique des politiques RSE aux fins de résilience

L'investissement des entreprises dans les politiques de RSE a longtemps été motivé par les obligations réglementaires issues de la *compliance,* les politiques achats des clients stratégiques et le gain d'image associé. La réflexion sur la fonction sociétale de l'entreprise qu'induisent les politiques de RSE en font un vecteur naturel de résilience [58], ainsi qu'un atout compétitif en terme de concurrence et de construction d'écosystèmes de confiance.

Les entreprises n'ont pas tardé à faire de la RSE un outil opérationnel d'influence. La RSE offre au même titre que les relations publiques une faculté de modélisation de l'environnement sociétal. Si l'éthique est une valeur cardinale de la RSE, elle permet à la fois de jouer sur les perceptions et de modifier le comportement des acteurs sociétaux, notamment autour des grands enjeux climatiques ou de sécurité économique (approvisionnement stratégique de l'entreprise), de production décarbonée et d'économie circulaire. Qui plus est, plus les politiques RSE sont en adéquation avec le référentiel de valeurs de l'échiquier sociétal, plus leur potentiel inductif sera important.

Après la guerre économique, la guerre sociétale renouvelle l'importance des approches transdisciplinaires ou généralistes au sein des entreprises. L'exploitation de ce pôle de conflictualité de basse intensité va accentuer la fracture entre les entreprises qui ont développé leur agilité et résilience, et celles n'ayant pu ou vu l'intérêt stratégique de cette lame de fond. La déstabilisation des entreprises par une modification de l'échiquier sociétal tend à se généraliser et n'est plus l'exclusivité des services clandestins. Les capacités étatiques à réagir au niveau sociétal sont toutefois relativement faibles. L'efficacité de la normativité juridique, instrument privilégié de l'action publique, est moindre lorsqu'il s'agit de répondre à une déstabilisation sociétale. Ainsi les entreprises ont tout intérêt à créer des boucles de rétroaction rapide dans leur environnement sociétal.

Nicolas ZUBINSKI

Eléments bibliographiques

[1] Tad A. Schnaufer II, « *Redefining Hybrid Warfare: Russia's Non-linear War against the West* », 2017, Journal of Strategic Security, Volume 10 N°1 art.3, disponible sur www.scholarcommons.usf.edu

[2] LCL Ludovic MONNERAT (Département fédéral de la défense suisse), « Les guerres sociétales », 6 août 2005, www.ludovicmonnerat.com, disponible sur www.ludovicmonnerat.com

[3] Dr. Christopher PAUL, « *Confessions of a hybrid warfare skeptic* », 2016, Small Wars Journal, disponible sur www.smallwarsjournal.com

[4] Patrick TUCKER, « *Should the US Have a Secretary For Influence Operations ?* », 22 février 2020, DefenseOne, disponible sur www.defenseone.com

[5] Pr. Mark GALEOTTI, « *Russian Political War : Moving Beyond the Hybrid* », 2019, Routledge : Taylor & Francis Group

[6] Jean-Jacques ROUSSEAU, « *Du contrat social ou Principes du droit politique* », 1er édition 1762, Marc Michel Rey

[7] Edward BERNAYS, « *Propaganda - Comment manipuler l'opinion en Démocratie* », 1er édition 1928

[8] Edward Herman et Noam Chomsky, « *La Fabrication du consentement : De la propagande médiatique en démocratie* », 1er édition 1988

[9] James DOBBINS, Seth G. JONES, Keith CRANE, Beth Cole DE GRASSE, « *The Beginner's Guide to Nation-Building* », 2007, RAND Corporation, National Security Research Division, disponible sur www.rand.org

[10] Edmund Freud, « *Le Malaise dans la culture* », 1930

[11] Major Christian KAMPHUIS (Royal Netherlands Army), « *Reflexive Control : The relevance of a 50-year-old Russian theory regarding perception control* », 21 juin 2018, Militaire Spectator, disponible sur www.militairespectator.nl
[12] Général et Chef d'état-major Valéri GUÉRASSIMOV (Ministère de la Défense de la Fédération de Russie), « ЦЕННОСТЬ НАУКИ В ПРЕДВИДЕНИИ » (Value of science in forecast), Военно-промышленный курьер (Military-Industrial Kurier), 27 février 2017, disponible sur www.vpk-news.ru
[13] Émile DURKHIEM, « Les règles de la méthode sociologique », Revue Philosophique, 1894
[14] Danielo MARTUCCELLI, « *Michel Foucault et les impasses de l'ordre social* », automne 2006, Revue Sociologie et sociétés, disponible sur www.erudit.org
[15] Yannick BRESSAN, « *La particule fondamentale de l'être* », Mjw Fedition, 18 février 2019
[16] Jean-Claude MALLET, « Défense et Sécurité nationale : le Livre blanc », Présidence de la République et Ministère de la défense, éd. Odile Jacob : La Documentation française, Juin 2008, 402 pages, disponible sur www.ladocumentationfrancaise.fr
[17] Philippe COQUET, « *Opérations basées sur les effets : rationalité et réalité* », Octobre 2007, IFRI, Laboratoire de Recherche sur la Défense (LRD), disponible sur www.ifri.org
[18] Brad BOYD et Herbert LIN, « Affecting the Cognitive Dimension of the Information Envionment through Cyber-Enabled Information Operations », 2019, Journal of Information Warfare (JIW), disponible sur www.jinfowar.com
[19] Intelligence ONLINE, « *Paris veut son armée de cyber-influenceurs* », 13 mars 2019, Intelligence ONLINE, disponible sur www.intelligenceonline.fr
[20] LCL Julien CHEIZE, « Les enjeux du cyberespace pour l'armée de Terre », 21 mars 2020, Centre de doctrine et d'enseignement du commandement (CEDC), disponible sur www.penseemiliterre.fr
[21] Parlement britannique, House of Commons, HC 1791, « *Disinformation and fake news: Final Report* », 18 février 2019, disponible sur www.sanef.org.za
[22] Special Councel Robert S. MUELLER III « *Report On The investigation Into Russian Interference In The 2016 Presidential Election* », Mars 2019, US Departement of Justice, version intégrale et originale disponible sur www.justice.gov
[23] Martin UNTERSINGER, « *Les preuves de l'ingérence russe dans la campagne de Macron en 2017* », 6 décembre 2019, Lemonde.fr, disponible sur www.lemonde.fr
[24] Parlement européen, « Lutte de l'UE contre les fausses informations et l'ingérence électorale étrangère », 10 octobre 2019, Communiqué de presse, disponible sur www.europarl.europa.eu
[25] Pavel POLITUK, « *Exclusive: Ukraine says it sees surge in cyber attacks targeting election* », 25 janvier 2019, Reuters, disponible sur www.reuters.com
[26] Michael SCHWIRTZ et Gaelle BORGIA, « *How Russia Meddles Abraod for Profit : Cash, Trolls ans a Cult Leaser* », 11 novembre 2019, New York Times, disponible sur www.nytimes.com
[27] Ferial HAFFAJEE, « *Exclusive: Did Putin's 'Chef' attempt to interfere in South African election?* », 7 mai 2019, Daily Maverick, disponible sur www.dailymaverick.co.za
[28] Annie KOWALEWSKI, « *Disinformation and Reflexive Control: The New Cold War* », 1er février 2017, Georgetown Security Studies Review, disponible sur www.georgetownsecuritystudiesreview.org
[29] Margarita LEVIN JAITHER et Major Harry KANTOLA, « Applying Principles of Reflexive Control in Information and Cyber Operations », 2016, Journal of Information Warfare (JIW), disponible sur www.jinfowar.com
[30] Dr. Can KASAPOGLU, « Russia's Renewed Military Thinking : Non-Linear Warfare and Refexive Control », Novembre 2015, OTAN - NATO Defense College, Rome, disponible sur www.ndc.nato.int
[31] Marina ALCARAZ, « Gilet Jaunes : La Russie accusée d'envenimer la situation », 9 décembre 2018, Les Echos, disponible sur www.lesechos.fr
[32] Marion CANDAU, « les Gilets jaunes noyés sous les infox sur facebook », 13 mars 2019, Euractiv, disponible sur www.euractiv.fr
[33] Jean-Michel BARBIER, Laurence BAULT, Clément CHEVIGNON et Fabien RENAUDIN, *« Les Espaces Informationnels Autonomes à l'ère du numérique* », Février 2020, Centre de réflexion sur la guerre économique, École de Guerre Économique, disponible sur www.infoguerre.fr
[34] Olivier MERY, « *Les menées offensives sur la viande artificielle : comment les investisseurs créent le futur eldorado* », 4 février 2019, Centre de réflexion sur la guerre économique, École de Guerre Économique, disponible sur www.infoguerre.fr
[35] Jean-Philippe MORISSEAU, « La révolution dataculturelle du renseignement », 4 octobre 2019, Geointblog, disponible sur www.geointblog.wordpress.com

[36] Benoit TESTÉ, « *Polarisation de groupe et norme d'internalité : le rôle de l'engagement collectif dans l'attribution de valeur sociale* », 1999, Université Rennes 2
[37] Yannick BRESSAN, « Radicalisation, renseignement, individus toxiques », 7 juin 2018, Broché
[38] Locution attribuée à Phillipe II de Macédoine (-382 à -336 av. J.-C.)
[39] Isabelle CADET, « *Aspects juridiques de la responsabilité sociale* », I2D, disponible sur www.cairn.info
[40] Commission européenne, « Code de bonnes pratiques contre la désinformation, un an après: les plateformes en ligne soumettent leurs rapports d'autoévaluation », communiqué de presse du 29 octobre 2019, disponible sur www.ec.europa.eu
[41] Service européen pour l'action extérieure (SEAE), Est StratCom, « Questions and Answers about the East StratCom Task Force », 5 décembre 2018, SEAE, disponible sur www.eeas.europa.eu
[42] Collège du Renseignement en Europe, « *Lettre d'intention* », 26 février 2020, disponible sur www.intelligence-college-europe.org
[43] Arnaud DANJEAN, Rapporteur de la Commission affaires étrangères, Parlement européen, « *Projet de rapport sur la mise en œuvre de la politique de sécurité et de défense commune - rapport annuel* », 21 octobre 2019, Parlement européen, disponible sur www.europarl.europa.eu
[44] Commission nationale de contrôle des techniques de renseignement (CNCTR), *« Le cadre légal du renseignement* », juillet 2018, disponible sur www.cnctr.fr
[45] Académie du renseignement, « *La coordination nationale du renseignement et de la lutte contre le terrorisme* », octobre 2015, disponible sur www.academie-renseignement.gouv.fr
[46] Décret n° 2010-800 du 13 juillet 2010 portant création de l'académie du renseignement, disponible sur www.legifrance.gouv.fr
[47] Décret n° 2019-206 du 20 mars 2019 relatif à la gouvernance de la politique de sécurité économique, disponible sur www.legifrance.gouv.fr
[48] Patrice MELÉ, « *Identifier un régime de territorialité réflexive* », 2009, Martin Vanier, Territoires, territorialité, territorialisation ; controverses et perspectives, Presse Universitaire de France, disponible sur www.halshs.archives-ouvertes.fr
[49] Loi n° 2013-595 du 8 juillet 2013 d'orientation et de programmation pour la refondation de l'école de la République, disponible sur www.legifrance.gouv.fr
[50] Carole CADWALLADR, « *Aggregate IQ : the obscure Canadian tech firm and the Brexit data riddle* », 31 mars 2018, The Guardian, disponible sur www.theguardian.com
[51] Thomas HUCHON, Documentaire, « Scandale Cambridge Analytica : nouvelles révélations », Avril 2020, Spicee, disponible sur www.spicee.com
[52] Ministère de l'Education nationale, de l'Enseignement supérieure et la Recherche, Infographie, « Le parcours citoyen : De l'École élémentaire à la terminale, apprendre les valeurs de la République », *26 Août 2014,* Ministère de l'Education nationale, de l'Enseignement supérieure et la Recherche, disponible sur www.gouvernement.fr
[53] Centre pour l'Education aux Médias et à l'Information (CLEMI), « *Référentiel enseignant.e.s et formateurs/formatrices CLEMI* », Avril 2020, disponible sur www.clemi.fr
[54] UNESCO, « *2017 Global Media and Information Literacy Award: Organizations in four countries recognized* », 6 novembre 2017, UNESCO, disponible sur www.en.unesco.org
[55] Sous la direction d'Henri MATRE, Philippe CLERC, Christian HARBULOT, Philippe BAUMARD, Bernard FLEURY, Didier VIOLLE, Commissariat Général du Plan, « Rapport du Groupe Intelligence économique et stratégie des entreprises », février 1994, La Documentation Française, disponible sur www.vie-publique.fr
[56] Philippe CALLOT, « *Intelligence Economique et PME* », 2006, La Revue des Sciences de Gestion, disponible sur www.cairn.info
[57] Hal R. ARKES & Catherine BLUMER, « *The Psychologie of Sunk Cost* », 1985, Organizational behavior and human decision processes, disponible sur www.communicationcache.com
[58] Bénédicte DAUDÉ et Christine NOËL-LEMAÎTRE, « *La responsabilité sociale de l'entreprise analysée selon le paradigme de la complexité* », 2006, Management & Avenir, disponible sur www.cairn.info