Black swans, red herrings :
Analyse infocindynique d'un scénario de bifurcation des cyber-luttes

Pascal COHET [†]

Résumé

Un scénario d'émergence de cyber-conflit est proposé, à partir d'un élément réel -un déficit nomique : l'inintelligibilité du droit de la communication, contrevenant à un objectif à valeur constitutionnelle- et de deux éléments fictifs : d'une part une opération d'influence menée par une grande puissance sous couvert de son secret défense afin d'obtenir la signature d'un traité international favorisant ses intérêts économiques, et d'autre part une procédure judiciaire à l'encontre d'une cyber-ONG menant des actions de contre-influence s'opposant à la signature de ce traité. Ce scénario explore les possibles conséquences vicariantes d'une hypothétique décision de justice à l'encontre d'un acteur non étatique, et suggère une importante vulnérabilité, en particulier dans un contexte de restriction du budget de la défense limitant la capacité de protection des opérateurs d'importance vitale.

Précisions liminaires : choix lexicaux

Comme le remarquait Atkinson, le préfixe « cyber- » est fréquemment utilisé sans discernement comme synonyme d'Internet[1] ; par ailleurs un lien conceptuel véritablement pertinent avec les travaux de Norbert Wiener est difficilement justifiable à ce jour, même s'il pourrait -par convergence- le devenir avec le développement des systèmes cyber-physiques (CPS), si jamais le choix conceptuel initial -basé sur des considérations économiques[2]- de les déployer sur l'actuelle infrastructure IP devait être maintenu malgré les incommensurables vulnérabilités que cela génèrerait. Quoi qu'il en soit, puisqu'il s'agit ici de décrire un scénario de « cyber-affrontement », l'usage de ce préfixe est conservé, conformément à un usage internationalement établi dans les milieux de la défense.

Le mot « risque » n'est pas utilisé ici au sens de l'ISO 31000 : « *effect of uncertainty on objectives* », en particulier parce que le domaine de la sécurité concerne aussi le plus grand nombre, qui pourrait trouver cette définition absconse. Le sens adopté ici est donc : « *possibilité ou probabilité de survenance d'un dommage* », le mot probabilité étant entendu au sens large[3], et restant inclusivement compatible avec sa signification mathématique, pour les cas éventuels où cette dernière trouverait à s'appliquer rigoureusement en pratique. Pour cette même raison, le sens retenu écarte celui de « *risque positif* », qui pourrait mener à des confusions dommageables entre risques et opportunités.

S'agissant d' « information », l'infocindynique s'intéresse en premier lieu à l'information signifiante : à l'aspect sémantique de l'information, soit, très exactement, ce à quoi Shannon a explicitement indiqué que sa théorie ne s'applique pas[4], dès l'introduction de son article séminal sur la théorie mathématique de la *communication*[5]. Le sens retenu ici est (approché par) : « *ce qu'il est possible d'extraire de données grâce à des connaissances* », et n'est pas restreint au seul cas des informations décrivant des faits objectifs réels et avérés comme c'est le cas dans les théories véridicalistes.

Le terme « déontologique » qualifiant initialement l'aspect des règles, lois et règlements de l'hyperespace cindynique est remplacé par le terme « nomique » par l'infocindynique, pour deux raisons : Primo, généralement, un code de déontologie est un ensemble de règles qu'un acteur s'impose librement à lui-même, processus dans lequel le législateur n'a pas à intervenir, par définition. Secundo, parce que l'infocindynique est conçue comme un noyau descriptionnel conceptuellement et intentionnellement perfectible, destiné à être librement étendu de façon spécifique et adaptée par les utilisateurs via la méthode de conceptualisation relativisée[6] (MCR). Le terme grec νόμος, englobant toutes formes de règles, lois, coutumes, permet ainsi de préparer une analyse -au sens MCR- de l'aspect nomique en sous-apsects, comme par exemple : les lois, les règlements intérieurs, les normes, les procédures, les codes de déontologie ou les chartes éthiques, dont les relations peuvent être déficitaires au sens cindynique.

[†] IFREI- Institut de Formation et Recherche sur l'Environnement Informationnel.

Hic poenus non optime graece, sed tamen libere respondisse fertur, multos se deliros senes saepe vidisse, sed qui magis quam Phormio deliraret vidisse neminem.
Cicéron (De oratore.[7])

Introduction

Dans un article récent[8], Elisabeth Paté-Cornell met en lumière l'usage parfois abusif de la métaphore du cygne noir (black swan), servant d'excuse à une absence de gestion pro-active des risques. Pour sa part, l'infocindynique, qui s'intéresse aussi, en particulier, aux TIC et aux systèmes cyber-physiques, permet de modéliser la création de vulnérabilité inhérente aux processus d'innovation, conséquence de l'impéritie fondamentale des experts face à des périls émergents : il est évident que toute création de technologie (comme toute innovation financière) par un acteur crée immédiatement un déficit épistémique (en l'espèce, une lacune) chez les autres acteurs ne la maîtrisant pas encore, donc de la vulnérabilité. Elle crée aussi de facto souvent un déficit nomique puisqu'aucune loi ne l'a anticipée, déficit nomique que le législateur aura du mal à combler dès lors qu'il est lui aussi atteint de déficit épistémique, ce qui mène dynamiquement au phénomène de la dialectique réglementaire, bien connu dans les milieux de l'économie (ex : succession des accords Bâle[9]).

Parallèlement, une compréhension superficielle des cindyniques mène parfois le néophyte à considérer qu'elles ne s'appliquent qu'ex-post, et omettent la gestion ex-ante[10], la notion de déficit étant souvent perçue de façon restrictive comme : ce qu'il faut changer aux organisations *à la suite* d'un dommage afin qu'il ne se reproduise plus. La définition même de la vulnérabilité d'une situation pourrait apparaître comme quasi-tautologique puisqu'elle est définie comme la propension d'une situation à générer des dommages, et décrite comme une fonction -en particulier- des déficits, eux-mêmes décrits comme générateurs de danger. Pour autant, cela signifie simplement que l'analyste a la capacité de recenser et évaluer les déficits (des acteurs) d'une situation, et ce aussi bien 'ex-post', que 'ex-ante'. Dans le cas ex-ante, et concernant les processus d'innovation, l'approche fréquentielle semble peu réaliste : l'intérêt des cindyniques, basées sur une approche propensionniste, devient alors évident. L'infocindynique étend cette approche aux situations multi-polaires ou conflictuelles, en relativisant les observations et estimations, et en raisonnant en termes de *champs de propensions*, c'est-à-dire -comme le conçoit Karl Popper[11]- de *champs de forces* concurrentes. Cette extension permet en particulier une application au domaine de la cyber-défense, ce qui était *conceptuellement impossible* avec les descriptions cindyniques initiales, ne serait-ce que parce qu'en pratique elles supposaient l'existence d'un unique acteur chef de projet conduisant un unique opérateur de transformation intentionnel, et ne décrivaient pas le cas des situations à plusieurs opérateurs de transformations intentionnels concurrents conduits par des acteurs dont les volontés s'affrontent.

Au-delà de sa valeur d'exemple applicatif, le scénario proposé ici a principalement pour objectif d'exposer une modélisation infocindynique *ex-ante* d'une situation conflictuelle et la possibilité de prévoir des risques émergents : Le plus souvent, les cygnes noirs ne sont effectivement pas nécessairement une fatalité, *à condition* de se donner les moyens d'étudier à temps les transformations silencieuses opérées (veille) ou qui pourraient être opérées (scénarisation) à un instant donné. Ces deux activités, veille ou scénarisation prospective, ne sont pas exclusives l'une de l'autre dès lors que l'on raisonne en termes de théorie du chaos : si la veille permet d'avoir une certaine vision d'une transformation en cours (à condition de détecter les signaux faibles pertinents, i.e. ceux concernant un changement, une modification de régime permanent), elle ne permet pas à elle seule la pleine prise en compte de l'impondérable « battement d'aile d'un papillon », de l'événement d'apparence anodine qui modifiera radicalement les opérateurs de (contre-)transformations intentionnels mis en œuvre.

Situation initiale (actuelle) réelle : déficits, blocages, et disjonctions

Les sciences du danger modélisent les acteurs d'une situation cindynique selon cinq aspects : statistique (données, informations brutes, faits, histoire), épistémique (modèles, savoirs, connaissances), téléologique (buts, objectifs, finalités), nomique (lois, règlements intérieurs, codes de déontologie) et axiologique

(valeurs). La vue sur un acteur est ainsi un espace à cinq dimensions (d'où le terme 'hyperespace') dans lequel l'analyste va rechercher les déficits, dans le but de les corriger pour diminuer la vulnérabilité de la situation i.e. sa propension à générer des dommages : Il n'est pas inutile de rappeler que par nature, un cinquième de l'analyse scientifique du danger consiste donc à recenser les pathologies nomiques (donc, en particulier des lois, de leur production, et des usages qu'en feront les juges), génératrices de danger (cindynogènes). Du fait de son but cindynolitique, la présente analyse tend *in fine* à conforter l'autorité de la justice dont les acteurs ne peuvent cependant scientifiquement pas être analysés autrement que comme les autres acteurs[12].

Ainsi, la vulnérabilité de la situation cindynique *réelle* de départ du scénario envisagé provient d'un déficit de la loi en matière de communication, ayant incité le Conseil d'Etat à étudier un projet de codification du droit de la communication[13], projet présenté par Thomas Andrieu[14] au Ministère de la Culture lors du colloque « convergence numérique- convergence juridique » du 28 novembre 2006. En substance, au fil des ans, la multiplication des textes et l'accumulation de la jurisprudence font qu'en pratique seul un spécialiste de ce domaine du droit est apte à le comprendre et l'utiliser de façon effective. Autrement dit la loi est devenue en pratique inintelligible pour le non spécialiste (a minima, selon le Conseil d'Etat, sa clarté et son intelligibilité sont grandement améliorables), ce qui pose problème dès lors que l'intelligibilité de la loi est un objectif à valeur constitutionnelle.

D'un point de vue cindynique, les acteurs concernés par ce problème peuvent plus précisément être caractérisés par trois déficits qui se sont développés : un déficit nomique (une accumulation disjointe de textes *in fine* peu claire ou intelligible), un déficit statistique (la non connaissance de la jurisprudence accumulée), et un déficit épistémique (l'absence des connaissances spécialisées nécessaires à la maîtrise des textes et de la jurisprudence). Ce cas de figure est un exemple type des raisons qui ont mené l'infocindynique à adopter une représentation en « plum blossom » (*Figure 2*) de l'hyperespace du danger, différente de la représentation initiale en « H » des cindyniques (*Figure 1*).

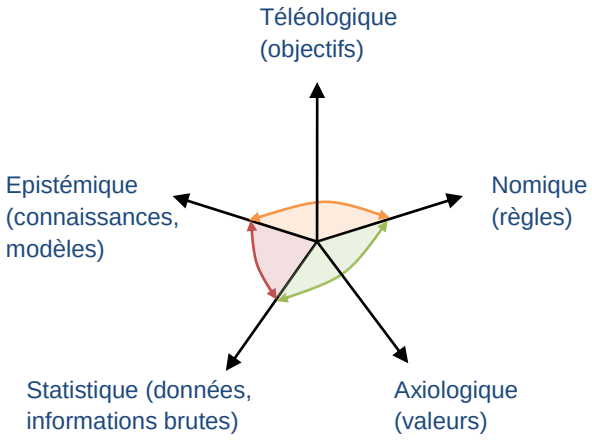

Figure 2 : Hyperespace infocindynique

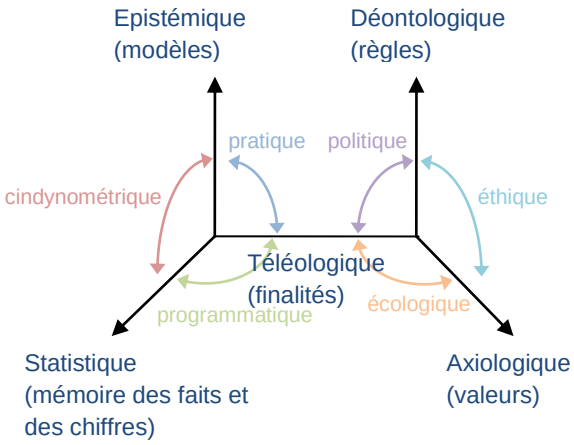

Figure 1 : Hyperespace cindynique

Historiquement, la représentation en « H » de l'hyperespace cindynique trouve son origine dans la mise en évidence, dans un premier temps d'un espace à trois dimensions construit sur les axes (ou aspects) données, modèles, et objectifs (espace praxique), puis dans un second temps d'un autre espace construit sur les aspects objectifs, lois et valeurs (espace ontologique généralisé), mis en évidence par des études post-accidentelles ayant fait apparaître le rôle non négligeable des facteurs règlementaires et axiologiques. L'axe objectifs, commun au deux espaces, permettait de les relier, d'où la notion de « passerelle téléologique ».

Cette représentation en H fait apparaître des plans construits sur chaque paire d'axes de l'hyperespace : il convient de noter que la notion de plan ne doit pas être interprétée au sens géométrique. Il ne s'agit pas de munir chaque axe d'une distance qui permettrait de définir la position d'un point sur chaque plan : un plan construit sur deux aspects est le 'lieu' des relations pertinentes existant, ou devant exister, ou qui ne

devraient pas exister entre des éléments de ces aspects. Les pathologies de ces relations, constituant des déficits, sources de vulnérabilité, sont en particulier les disjonctions et les blocages, deux notions parfois insuffisamment distinguées. Les disjonctions de deux axes correspondent à une « *incohérence manifeste entre deux espaces ou entre deux axes* »[15], par exemple une absence de régulation ou de lien causal, ou la présence d'une régulation ou d'un lien causal inadapté ou cindynogène. Un exemple est celui des zoonoses[16] : lors de la mise en évidence du prion, il existe des réglementations qui encadrent les pratiques des éleveurs, mais aucune ne prohibe l'utilisation des farines animales ; du point de vue de la problématique de l'encéphalopathie spongiforme, les objectifs -ou comportements- des éleveurs britanniques sont disjoints d'une réglementation qui en pratique ignore purement et simplement cette problématique. Un autre exemple de disjonction téléologique/nomique pourrait être celui d'une procédure décrochage imposant à un pilote la pleine puissance des moteurs, alors que les nacelles des moteurs de son appareil sont situés sous le centre de gravité et que cette augmentation de poussée provoquerait un couple à cabrer entrant en conflit avec l'objectif -vital- du pilote qui est de restaurer ou préserver la portance. Dans le plan cindynométrique, un exemple de disjonction statistique/épistémique est celui des données qui alimentent le modèle d'un simulateur de vol : si des données de comportement réel en vol d'un appareil sont indisponibles (par exemple celles concernant son comportement en cas de perte de portance) il peut être tentant de leur substituer des données théoriques : la conséquence directe est qu'il est alors possible de douter du bien fondé de l'entraînement au décrochage sur simulateur.

Les blocages, ou plus exactement les blocages de *régulation*, correspondent à l'*arrêt* d'une régulation (censée être cindynolytique) entre deux axes, par exemple entre des objectifs décidés, donc -à terme- des comportements, et une réglementation : autrement dit, *il existe* une « *cohérence manifeste entre deux espaces ou entre deux axes* », *mais* une relation pertinente initialement existante entre ces deux axes disparaît à un moment donné. Il convient de plus de remarquer qu'un blocage n'est pas nécessairement cindynogène et *peut* même au contraire être cindynolytique : en cas de décrochage *ou* d'approche de décrochage, un pilote *aurait* sans doute eu intérêt, contrairement à la procédure initialement en vigueur, à appliquer la puissance *ad hoc* et donner un ordre à piquer de façon à réduire son angle d'attaque et récupérer de la portance[17]. Autrement dit, un blocage de régulation *peut* permettre de contrer l'effet cindynogène -voire létal- d'une disjonction (en l'espèce : d'une régulation cindynogène générée par un déficit nomique).

La notion de blocage permet ainsi de mieux cerner la notion d'hyperespace : ce dernier est parfois appréhendé comme « statique » alors qu'il représente le *fonctionnement* d'une organisation à un instant donné, donc une dynamique, tout comme une fonction de transfert représente le fonctionnement dynamique d'un système, même si cette fonction peut apparaître comme « statique ». Le blocage d'une régulation entre deux axes est bien un déficit qui entache le fonctionnement dynamique d'une organisation, lequel est représenté par l'hyperespace cindynique, qui relève de la cindynique dite « statique » uniquement par opposition à la *cindynamique*, qui elle concerne les *transformations* (opérateurs de transformation intentionnels ou catastrophiques), c'est-à-dire les *changements de fonctionnements*.

La représentation en « plum blossom » de l'hyperespace infocindynique permet de faire apparaître des disjonctions et blocages dans les quatre nouveaux plans qu'elle introduit : nomique/épistémique, nomique/statistique, axiologique/épistémique, axiologique/statistique. Cette évolution du modèle de l'hyperespace cindynique reste parfaitement orthodoxe, dans la mesure où Georges-Yves Kervern avait lui-même clairement mentionné dès 1995 les disjonctions épistémique/axiologique[18]. Ces nouveaux plans permettent la prise en compte de phénomènes cindyniques importants, comme celui de la neutralité axiologique (plan axiologique/épistémique), fondamental pour la question de la scientificité des sciences économiques[19], ou encore, dans le plan épistémique/nomique : le problème du déficit épistémique du législateur, ou du négociateur d'un traité international, qui peine parfois à comprendre les articles ou amendements qui lui sont soumis, ou qui les comprend trop tard, ou encore, dans le cas envisagé ici, de celui du public qui ne dispose pas de la somme de connaissances nécessaires en pratique au respect de la loi existante (blocage de régulation téléologique/nomique par lacunes statistiques ou épistémiques -elles-mêmes générées par l'évolution des textes et de la jurisprudence- soit, dans l'hyperespace infocindynique : des disjonctions nomique/épistémique et nomique/statistique).

Le droit applicable à la communication, en particulier dans le domaine des TIC, est ainsi entaché de nombreux déficits. Outre le manque de clarté des textes évoqué par le Conseil d'Etat, leur adaptation au monde actuel réel est discutée : c'est par exemple le cas du plaquage de l'ancienne notion de directeur de la publication aux entités s'exprimant sur Internet ; cette notion, réaliste pour des topologies d'acteurs pyramidales, c'est-à-dire pour des hiérarchies classiques, est vue comme un archaïsme topologique, souvent perçu comme médiéval, voire comme une fiction juridique, dans le cyber-espace où de telles topologies n'existent souvent tout simplement pas. Il est par exemple éclairant de se poser la simple question de la désignation du « directeur de la publication » de l'entité Anonymous… L'implémentation de cette notion à l'occasion de la transposition de la directive 2000/31CE apparaît comme un déficit particulier : une *éminence*, c'est-à-dire le contraire d'une lacune (soit : la présence d'un élément cindynogène sur un axe). Dynamiquement, le flou des textes mène aussi à la dérive de certaines notions, comme celle d'hébergeur, qui, en l'absence d'une définition claire, s'écarte progressivement et considérablement si ce n'est de l'intention du législateur, du moins de celle des rédacteurs des amendements. De même, s'agissant d'intention du législateur, en raison du flou rédactionnel, le sens initial particulièrement restrictif du « manifestement illicite », connu des acteurs historiques du processus législatif, et re-précisé par le secrétaire général du Conseil Constitutionnel le 15 juin 2004[20] lors de la publication de la décision 2004-496 DC du 10 juin 2004[21], tend à tomber dans l'oubli (soit : l'apparition de lacunes statistiques ou épistémiques), y compris chez certains acteurs juridiques, et ce malgré son importance fondamentale.

Comme mentionné précédemment, l'évolution concrète de ce droit a mené chez de nombreux acteurs à la création en creux de déficits *de facto* sous forme de lacunes épistémiques et statistiques, donc des disjonctions épistémique/nomique et statistique/nomique : La conséquence pratique est la nécessité pour les acteurs de s'adjoindre *a priori* les services de juristes spécialisés, d'où une *fracture juridique*, une inégalité manifestement évidente et incontestable entre d'une part les acteurs de type économique, politique, ou institutionnel qui ont les moyens de payer de tels services, et d'autre part les acteurs individuels ou associatifs qui ne les ont pas. S'il est considéré que la constitution pose l'égalité de tous devant la loi comme principe, le problème de ces déficits s'inverse : il ne s'agit plus de *lacunes* épistémiques et statistiques qu'il conviendrait en théorie de combler (tâche incombant au justiciable), mais de la présence d'*éminences* épistémiques et statistiques qu'il convient en pratique de supprimer (tâche incombant au législateur), ce qui est en fait l'objectif du projet de codification proposé il y a quelques années par le Conseil d'Etat dans un contexte de prise de conscience de l'importance des phénomènes de convergence et des risques juridiques qui en découlent.

Pour l'instant, les acteurs ne disposant pas de juristes spécialisés ont le choix entre : soit ne pas prendre de risques, et donc se censurer (auto-censure par précaution, ou '*chilling effect'*), soit prendre des risques, et là, la question à se poser désormais est celle des conséquences globales de la matérialisation non improbable de certains de ces risques, et en particulier de celles qui impacteront la cyber-défense et les opérateurs d'importance vitale (OIV).

Scénario de bifurcation

Le problème fondamental du stratège est de reconnaître la nature du problème auquel il est confronté.
Hervé Coutau-Bégarie[22]

Comment arriver à se convaincre que ces modèles hallucinatoires qui nous font face en tant qu''objets' avec tant d'extériorité et tant d'acuité de présence, ne sont qu'une sorte d'hologrammes de marionnettes liées par mille ficelles à notre corps-et-esprit ?
Mioara Mugur-Schächter

A des fins prospectives, préventives ou cindynolytiques, il est possible de spéculer le scénario fictif suivant : Une grande puissance tente d'imposer un traité international favorisant ses intérêts économiques, en masquant le contenu du projet de traité par son secret défense. La manœuvre consiste à élaborer une première version du traité et à la négocier avec un nombre initialement restreint de pays choisis pour leur alignement, puis à intégrer progressivement d'autres pays de moins en moins alignés, mais qui devront finir

par adhérer au traité du fait des adhésions précédentes, et ce malgré la diminution de leur marge de négociation au fur et à mesure de ce processus d'expansion.

Cette tentative provoque la réaction de cyber-activistes qui considèrent cette opération de transformation comme une menace pour les libertés civiles, et une tentative de contournement du processus parlementaire. Des opérations de contre-influence et d'*agitprop* (d'un point de vue cindynique, un opérateur de contre-transformation) sont donc initiées, ciblant en particulier le parlement européen dont il est souhaité qu'il fasse avorter le projet de traité.

Dans le cadre de ces opérations, en l'état de la clarté et de l'intelligibilité du droit existant, et ne disposant pas des conseils d'un juriste spécialisé, un cyber-activiste prend le risque de publier un billet sur le site d'une cyber-ONG 'de fait', c'est-à-dire ne disposant pas d'une forme juridique, et dont les règles élémentaires de sécurité imposent *ab initio* le pseudonymat aux participants. S'estimant lésé par ce billet, un acteur institutionnel dépose une plainte. Les enquêteurs butent sur l'efficacité de la défense en profondeur de la cyber-ONG et ne parviennent pas à récupérer la moindre IP exploitable. A défaut, le propriétaire du nom de domaine est identifié, et un juge décide de le poursuivre en tant que directeur de la publication en dehors de tout fondement réel. Par précaution, la cyber-ONG se voit contrainte de décider de suspendre toute activité publique, et ne peut plus participer au débat démocratique tant que le jugement n'a pas eu lieu. Puis, contre toute attente, malgré les pronostics des juristes spécialisés, le juge finit par condamner le propriétaire du nom de domaine.

Cette hypothèse d'école mène à conjecturer un spectre de situations dans lequel nombre d'acteurs-observateurs, dont en particulier *un certain nombre* de cyber-activistes vont *estimer* que loin d'être un événement anodin, un tel jugement, au-delà de sa simple iniquité, est de nature à bouleverser les modalités des luttes pour les libertés civiles. Il est possible d'envisager que ce bouleversement mène, entre autres, à des menaces sérieuses sur les opérateurs d'importance vitale, par ailleurs aujourd'hui vulnérables.

其政悶悶，其民淳淳；其政察察，其民缺缺。
治大國若烹小鮮。
Lao Tseu

Concernant le plaignant, dont l'objectif est initialement la protection de sa réputation, la conséquence quasi-mécanique de la décision de justice est que cette réputation sera in fine considérablement plus attaquée, avec en particulier des publications hostiles décuplées en dehors du territoire national, donc hors d'atteinte de la moindre action effective, et d'ampleur rendant vaine toute tentative d'offuscation. Sur internet, ce pharmakon, appelé dans ce cas 'effet Streisand', est en effet devenu, si ce n'est une tradition, du moins un réflexe spontané et constant très largement répandu. Par manque de culture infocindynique, ce risque 'certain' est trop souvent insuffisamment pris en compte, par exemple récemment par des personnels de la DCRI ayant tenté de faire dépublier un article Wikipédia : ce qui est incompris, c'est que le plus souvent ce n'est pas tant la demande de retrait d'un contenu en elle-même qui provoque l'effet Streisand que la façon de le demander. Si cette façon est a priori abrupte, l'effet Streisand est garanti : il s'agit là clairement d'une riposte à un geste considéré comme formellement hostile[23]. Une part importante de ce risque pourrait ainsi être mitigée facilement par des demandes de retrait plus urbaines, non génératrices de rapports de forces. Pour autant, cela ne doit par ailleurs pas occulter la nécessité d'une réflexion plus générale sur la légitimité d'hypothétiques tendances à tenter de noircir des sources ouvertes par le secret défense, éventuellement par connexité.

Concernant les opérateurs d'importance vitale et les agents chargés de renforcer leur sécurité, outre l'état actuel de leur organisation ou leur niveau de sécurité réel, deux facteurs extérieurs déterminent leur vulnérabilité dans la situation conjecturée[24] : d'une part le nombre d'acteurs individuels potentiellement concernés par la décision de justice et effectivement informés de cette décision, et d'autre part la perception qu'ils en auront (et, plus précisément, dans le spectre de situations, leur prospective, c'est-à-dire leur *estimation* de la situation idéale, par rapport à leur *observation* de la situation réelle, i.e. leur perspective).

The acceptance that is secured may be the « I do » shotgun wedding, but acceptance there must be.
Herbert Simon[25]

Des sources ouvertes institutionnelles mentionnent, de façon récurrente, si ce n'est le mauvais état, du moins la perfectibilité de la cyber-sécurité des opérateurs d'importance vitale, et font apparaître une certaine inertie face aux transformations prophylactiques souhaitées par l'agence idoine[26] qui -quantitativement- constituent, il est vrai, un programme particulièrement vaste. Cette inertie pose la question endémique de l'*autorité* de l'acteur conduisant un opérateur de transformation, et si autorité théorique il y a, de son autorité effective. C'est typiquement une des raisons qui ont mené l'infocindynique à faire évoluer les descriptions cindyniques, et à compléter le concept de situation cindynique par celui de *spectre* de situations[27](ou 'méta'-situation), en prenant en compte la relativité de l'observation et de l'analyse des situations, et leur multi-polarité factuelle. Un problème récurrent lors de tout *changement* est en effet celui de l'efficacité de l'opérateur de transformation intentionnel, qui se heurte à un phénomène de *friction cindynique*[28], définie par l'écart entre la prospective d'un acteur à un instant t correspondant au début de la mise en œuvre effective d'un opérateur de transformation -quel qu'il soit, ou quelle que soit sa finalité-, et sa perspective à un instant ultérieur $t+\Delta t$, rendant compte de la progression effective de l'opérateur, cette friction venant limiter la *puissance* de l'acteur, définie comme sa capacité à imposer sa prospective. La relativisation des acteurs-observateurs permet ainsi plus finement de mettre en évidence la présence simultanée de multiples opérateurs de transformation (ou de *contre*-transformation, en réaction à un opérateur de transformation tiers, ou 'conformation') résultant des différences de prospectives (i.e. des divergences) entre acteurs, ce qui revient à décrire un *champ de propension*s. Ces divergences correspondent aux différents facteurs menant à des inerties plus ou moins passives ou homéostasiques pouvant s'opposer à l'opérateur de transformation intentionnel mis en œuvre par un acteur en situation de conduite du projet (par exemple : une agence devant opérer un opérateur de transformation sur des opérateurs tiers). L'analyse infocindynique permet ainsi -et c'est un de ses objectifs majeurs- d'améliorer l'efficacité ou l'efficience des opérations de prévention ou sécurisation, quelles qu'elles soient. Quoi qu'il en soit, le fait notable est que des failles existent, et qu'elles risquent de perdurer ou de se renouveler : autant d'opportunités pour des opérations offensives[29].

Concernant le cyber-activisme, un facteur important est l'ampleur de la base concernée. La majeure partie des cyber-luttes repose en fait principalement sur les trois *risques infocindyniques primaires*, qui sont des risques de flux informationnels : *ouverture* (risque sur la confidentialité), *fermeture* (risque sur l'émission et l'accès à l'information), et *toxicité* (manipulation, désinformation…). D'un point de vue opérationnel, la matérialisation de ces risques primaires correspond à des *déficits cindynamiques cindynogènes*, affectant le fonctionnement des acteurs, aussi bien, d'ailleurs, que les changements de fonctionnement (les opérateurs de transformation intentionnels). Le fait important est qu'il s'agit là de problématiques extrêmement simples, échappant aux clivages axiologiques communs (politiques, idéologiques, …) ce qui génère un très large consensus, donc une large population *convergente* (i.e. dont les divergences prospectives sont faibles ou nulles).

En situation multi-polaire, les problématiques d'ouverture et de fermeture de l'information mènent à une lutte de détermination ou de positionnement de *frontière* entre l'information ouverte et l'information fermée, posant la question de l'*horogénèse* informationnelle, ce qui est par exemple bien illustré par la position émise par le secrétaire général du SGDSN[30] sur l'affaire Wikileaks. Il convient aussi de prendre en compte l'*axiome de relativité* de la perception du risque (d'importance fondamentale, et justifiant par ailleurs le concept ultérieur de spectre de situations introduit par l'infocindynique) : pour le cyber-activisme -dont l'activité revient *dans les faits* à de la gestion de risques- le risque considéré est bien celui de la création ou de l'existence de règles, technologies, et usages dangereux, alors que pour ses antagonistes, le risque considéré est celui porté par ces règles, technologies, et usages, qui existent ou dont ils promeuvent la création. Par exemple, s'agissant de risque d'ouverture, le

cyber-activisme considère comme un risque la vente d'un système de surveillance des populations (comme le système Eagle[31], vendu à la Jamahiriya de Mouammar Kadhafi par une ex-filiale du groupe Bull[32]), là où d'autres considèrent éventuellement les risques liés aux usages qui pourraient en être faits *après* cette vente (arrestations, torture). Un autre exemple pourrait être celui de la mention d'une ethnie sur une carte d'identité : soit on peut considérer qu'une telle mention ne doit pas exister, soit on peut considérer qu'elle peut exister mais qu'il ne faut pas s'en servir à des fins illégales. Dans le cas du Rwanda, cette différence de perception du risque mène *in fine* à une différence de quelques centaines de milliers de morts. Dans le cyber-espace, cette relativité de perception des risques est, avec la question de l'horogénèse informationnelle, une des principales causes de confrontation entre cyber-activisme d'une part, et pouvoirs antagonistes (exécutif, législatif, et économiques) d'autre part.

Le même principe de relativisation de la perception peut aussi s'appliquer à l'éventuel déploiement d'une infrastructure de routage IP par DPI, où à l'utilisation de l'infrastructure IP par les CPS, ouvrant la porte à de nouveaux risques matériels majeurs, d'ailleurs préfigurés par Stuxnet[33]. Quoi qu'il en soit, la simplicité, l'évidence manifeste, et le faible nombre des problématiques concernées génèrent une base convergente dont l'unité de mesure adaptée est sans doute le million d'individus. La question suivante est l'estimation du nombre d'acteurs concernés par la décision de justice conjecturée : l'exemple choisi ici n'est pas tout à fait arbitraire, puisqu'en réalité une condamnation de propriétaire de nom de domaine a effectivement eu lieu il y a une dizaine d'année, ce qui permet de disposer d'une indication : Le fait historique significatif est que cette condamnation d'un intermédiaire technique avait provoqué l'une des plus grandes manifestations du cyber-espace, avec une opération de blackout ayant mené à la fermeture de 90% des forums communautaires puis à une mobilisation massive et durable à l'encontre de la transposition de la directive 2000/31CE.

> *Dovete adunque sapere come sono due generazioni di combattere: l'una con le leggi, l'altra con le forze. Quel primo è degli uomini; quel secondo è delle bestie; ma perchè il primo spesse volte non basta, bisogna ricorrere al secondo.*
> Machiavel

Au-delà de ces aspects quantitatifs se pose la question de la *perception* par cette base de la décision conjecturée, et de ses conséquences. Une majorité d'acteurs de cette base estimeront que la condamnation d'un propriétaire de nom de domaine pour un billet litigieux publié par un tiers est inique. Cela étant, ce problème ne doit pas masquer un problème plus lourd de conséquences : la condamnation ne vise pas tant le propriétaire du nom de domaine que le nom de domaine lui-même, donc la cyber-ONG utilisant ce nom de domaine. Dans le principe, il pourra être estimé que c'est la possession même d'un nom de domaine par une ONG qui est visée, donc son accès au débat démocratique, et son existence même : dans le cyber-espace, tout leader stratégique a une conscience très claire de l'importance *vitale* (du contrôle) de son nom de domaine. La question alors posée est celle du bilan risques/opportunités du dialogue démocratique en tant que *moyen* d'atteindre des *objectifs* et, partant, celle des moyens en général et de leur légalité formelle, posant *ipso facto* la question de l'extension du nombre de *dimensions* de confrontation envisageables : tout se passe comme si la décision conjecturée provoquait -ou favorisait- une mutation de la forme des cyber-luttes, en faisant conjoncturellement apparaître à certains acteurs le débat démocratique légal comme un cul-de-sac évolutif momentané. Cette dernière perception pourrait de plus être renforcée par le constat suivant : entre la condamnation d'un propriétaire de nom de domaine il y a dix ans et aujourd'hui, il n'y a pas de différence, hormis, cependant, une dizaine d'années au cours desquelles le débat démocratique a été utilisé comme moyen de lutte, *justement*, en particulier, pour empêcher que des intermédiaires techniques puissent être condamnés pour des actions ayant été menées par des tiers. Il est alors probable qu'un nombre non négligeable d'acteurs estiment ce moyen obsolète, tout en ne renonçant pas à poursuivre leurs objectifs.

> 以正治國，以奇用兵，以無事取天下
> Lao Tseu[34]

D'un point de vue infocindynique, le phénomène prévisible est ainsi celui d'une augmentation des déficits perçus et d'une augmentation des divergences par rapport à un pouvoir ou un ordre établi, soit deux facteurs d'augmentation d'un *potentiel insurrectionnel*[35]. Un phénomène connexe prévisible, déterminant pour la topologie des réseaux effectifs d'acteurs émergents, est celui d'une clusterisation du cyber-activisme liée à

l'apparition de divergences entre acteurs optant pour des moyens non conventionnels, et ceux les refusant. Cependant, les divergences de ces deux clusters ne portant que sur les moyens, et leurs finalités restant identiques, que leurs actions soient coordonnées *ou non,* (un avantage supplémentaire sur l'adversaire commun étant d'ailleurs la difficulté pour lui de lever cette *ambigüité*) elles sont complémentaires, les acteurs conventionnels bénéficiant d'une manière ou d'une autre des actions non conventionnelles.

The target of all human conflict, the battleground of all conflict resolution, is the human mind. Neocortical warfare uses language, images and information to assault the mind, hurt morale and change the will.
Szafranski.

Au sein du cyber-activisme la culture stratégique conventionnelle reste du domaine de l'exception ; cependant, la 'complexification des structures par le bruit'[36] explique l'émergence d'un art opératif de plus en plus complexe. Ce mode d'émergence a un impact sur l'analyse stratégique des acteurs :

Lors de l'analyse d'une situation conflictuelle, la phase de cartographie des acteurs mène à tenter de déceler et identifier le ou les stratèges, ce qui pourrait faire apparaître un premier problème : s'il a pu y avoir dans le passé des cyber-activistes assurant cette fonction de façon coordonnée, et donc un système téléologique, cela pourrait ne plus être le cas. Et dans cette hypothèse, il pourrait s'avérer paradoxalement que cela soit en fait un avantage : supposons par exemple qu'il ait été délibérément décidé d'abandonner ce type de fonctionnement. La réflexion sous-jacente à une telle défection stratégique intentionnelle étant d'une part que l'adversaire perdrait alors son temps à essayer de découvrir quelque chose qui n'existe pas, et d'autre part que l'opinion publique est suffisamment largement sensibilisée (i.e. ne présente plus de lacunes épistémiques, statistiques, ou axiologiques) pour que quoi qu'il arrive, de multiples initiatives soient prises systématiquement de façon autonome, et que leur nombre soit un gage supplémentaire de puissance effective. En termes hayekiens, cela revient à laisser émerger un ordre spontané (cosmos : κόσμος) après avoir créé les conditions de son apparition (chaos : χάος), autrement dit, à substituer un système a-téléologique, auto-organisateur, à un système téléologique. La cible de cette stratégie a-téléologique est bien conceptuellement et délibérément la pensée même des stratèges adverses. Une piste ayant pu mener à cette décision pourrait trouver son origine dans la pensée de Sun Tzu pour qui l'attaque suprême consiste à attaquer le plan de l'ennemi : il peut être pensé qu'alors la défense suprême consiste à ne pas avoir de plan.

En réalité, il s'agit là d'une description schématique préalable, qui doit être dépassée et détaillée : la distinction entre système téléologiques et a-téléologiques est en pratique un *faux* problème, puisque *in fine,* un système auto-organisateur fait finalement progressivement émerger des acteurs organisés, c'est-à-dire des systèmes on ne peut plus téléologiques en pratique : un ordre spontané est *aussi* un ordre. De même, une absence de plan (ou de dispositif) laisse émerger une multitude de plans (ou de dispositifs). Les seules questions véritablement intéressantes sont alors : la topologie et la légitimité des puissances émergentes[37], la difficulté pour le stratège adverse à prévoir la stratégie de l'autre puisqu'elle émerge -dialectiquement- au fur et à mesure de l'évolution d'une situation (du processus démiurgique), et l'atomisation des acteurs émergents, donc des stratégies émergentes, qui vise à submerger la réflexion du stratège adverse. L'art suprême pourrait ainsi consister non pas à attaquer le plan de l'adversaire, mais à attaquer la 'rationalité', les capacités rationnelles, du stratège adverse, soit, d'un point de vue infocindynique : son plan cindynométrique (S,E) et donc son espace praxique (S,E,T), avec pour effet majeur recherché une dislocation de son hyperespace. Finalement, le fait remarquable est le suivant : que ce système (chaotique et, partant, auto-organisateur) ait été instauré sciemment ou pas ne change rien puisque *in fine* l'effet disloquant sur le stratège adverse reste le même. Autrement dit, pour un stratège, être la cible commune de l'ensemble d'un système dit 'a-téléologique' est peut-être une des pires situations qui soit.

强调的是以偏修正
Qiao & Wang[38]

If you squeeze a balloon in one part, it bulges out in another
William Lawrence[39]

Une façon d'aborder cette situation est de penser en termes de dimensions possibles du conflit, d'observer les dimensions utilisées, et d'essayer de prévoir l'émergence de l'usage de dimensions nouvelles, en particulier par l'étude de l'évolution des facteurs bloquant ou favorisant l'usage d'une dimension. A ce jour, le cyber-activisme utilise essentiellement des dimensions informationnelles : envers la base (mobilisation), envers les médias (effets de leviers), envers des acteurs tiers ou antagonistes (influence et communication

offensive). La lutte informatique offensive (LIO) est rarement utilisée, si ce n'est pour des attaques de type déni de service qui occasionnent peu (ou pas) de dommages et ont en revanche de bons effets informationnels. La dimension des savoirs est sous-utilisée, et les actions juridiques restent exceptionnelles en mode offensif, étant plus liées à des considérations consuméristes. Hormis le cas -discuté- des dénis de service, les usages conventionnels -y compris les divulgations de type Wikileaks- restent donc légaux, la régulation fixant ainsi les dimensions de l'espace des confrontations.

Or la décision conjecturée provoque un *blocage de régulation* pour *une part* des acteurs y percevant un barrage par dissuasion aux usages légaux dans une situation marquée par des déficits nomiques non résolus, et ouvre *ipso facto* la porte à l'usage d'autres dimensions, dont en particulier : la LIO. Tout se passe comme si un stratège avait raisonné en termes d'ultraguerre[40] ou de full dimensional operations : la décision conjecturée agit *de facto* comme un facteur de vicariance, déplaçant la fonction de lutte vers un nouvel espace, ou, plus globalement, étendant les dimensions de l'espace conventionnel, et permettant de nouvelles actions ou combinaisons (intentionnelles, tacites, ou fortuites) d'actions.

Etant donnés les antagonistes naturels du cyber-activisme, il est raisonnable de penser que les cibles privilégiées seront, en première intention, les opérateurs d'importance vitale, dont les vulnérabilités semblent relativement durables et autorisent différentes actions ou dommages offrant un bon effet de levier sur les pouvoirs antagonistes : pénétration de systèmes, acquisition de données confidentielles divulgables ou négociables ou permettant le blackmailing, éventuellement sabotage. Les attaques de type déni de service présentant un plus faible rapport opportunités/risques devraient en revanche tendre à être délaissées par les acteurs expérimentés. Les OIV sont ainsi des cibles intermédiaires servant des opérateurs de conformation, qui visent *in fine* à imposer une prospective aux cibles finales.

Ich sehe, daß es sich nicht geändert hat; und sehe es doch anders.
Diese Erfahrung nenne ich « das Bemerken eines Aspekts »
Wittgenstein

Les OIV ne sont que des moyens, tout comme la plupart des dénis de services qui n'ont en fait qu'un but informationnel : ces constats évidents mènent à concevoir une forme d'attrition dont le principe, déjà exposé[41], repose sur la gestion de la furtivité. En règle générale, la logique veut que l'attaquant cherche à maximiser sa furtivité lors de la pénétration d'un système. La logique paradoxale[42] de la guerre suggère donc *a contrario* que cela puisse ne pas être le cas. L'intérêt qu'a un attaquant à être suffisamment non furtif lors de la pénétration d'un OIV est trivial : cette attaque sert d'appeau, attirant l'attention des agents défenseurs, pendant qu'une attaque réelle et furtive a lieu ailleurs. Le point de départ est donc la création de fausses pistes (red herrings), la cible réelle de l'attaque non furtive est l'attention de l'agent défenseur.

Viennent ensuite des aspects quantitatifs : plus l'attaque non furtive dure longtemps, plus elle consomme de processus cognitif d'agent défenseur. La multiplication de pénétrations non furtives durables permet d'augmenter le nombre d'agents défenseurs ciblés, jusqu'à atteindre la limite des effectifs de leur agence. Dans ce système de crise permanente assurée par la persistance des attaques, c'est bien l'agence qui devient la cible réelle des attaques informatiques apparentes sur les OIV, l'objectif étant de saturer l'ensemble de ses ressources cognitives, qui ne peuvent pas être revues à la hausse en raison des restrictions du budget de la défense. Ce qui apparaît comme des attaques informatiques plus ou moins aléatoires est en réalité une guerre d'attrition cognitive. Une fois l'agence saturée par les attaques non furtives, les attaques furtives sont grandement facilitées, tant que la saturation est maintenue.

Une autre dimension peut aussi être introduite pour compléter le dispositif : en répartissant judicieusement les attaques non furtives sur des dates ou plages horaires non conventionnelles, les processus affectifs ou émotionnels peuvent être ciblés, du fait de l'augmentation prévisible des astreintes imposées aux effectifs, augmentant la pénibilité des postes (donc le coût salarial, d'où un impact possible sur les recrutements), ce qui est susceptible de générer des désordres organisationnels internes (dissonances, déficits, et divergences). Là encore, l'effet majeur recherché est celui d'une dislocation de l'espace praxique.

Du point de vue du défenseur, la perception de la situation par les agents est impactée par un brouillard d'ambigüités difficilement gérable. Ils peuvent éventuellement déceler une attaque qui se voulait furtive : ils sont en réalité incapables de distinguer une attaque d'intention furtive d'une attaque d'intention non furtive, ce qui crée pour eux de l'ambigüité. Autrement dit, le contrôle strict de la furtivité importe peu pour l'attaquant, dans la mesure de la fongibilité des cibles OIV réelles. De plus, l'agent défenseur est bien souvent incapable d'*attribuer* l'attaque, qui pourrait très bien être menée par un acteur économique, une puissance étrangère, un acteur non-étatique, ou encore un réseau maffieux, ce qui génère des ambigüités supplémentaires. Une des conséquences, ajoutant à l'asymétrie de la situation, est que le défenseur est cantonné dans des réactions purement défensives excluant toute réaction offensive : dans ce cas, le débat actuel sur le concept de légitime défense pouvant justifier des frappes cybernétiques[43] ne présente donc pas d'intérêt, sauf à attirer l'attention sur l'extrême dangerosité de ce concept en présence d'attaquants utilisant par exemple à dessein des IP extrême-orientales.

Conclusion

Pour les cindyniques, l'ontologie du danger est caractérisée en particulier par une cible du danger aisément identifiable puisqu'il s'agit de l'acteur subissant un dommage, et une source de danger plus délicate à appréhender : d'un point de vue cindynique, c'est la situation, dans son ensemble, i.e. avec ses déficits et dissonances, qui est cette source de danger[44]. D'un point de vue infocindynique, c'est l'ensemble du spectre de situations, avec donc -en plus- ses divergences et disparités, facteurs de conflictualité, qui est la source du danger.

Cette identification systémique de la source du danger est fondamentale : dans le scénario de cyber-guerre d'attrition envisagé ici, une fois la confrontation engagée, les agents en situation de défense des opérateurs d'importance vitale pourraient être rapidement saturés, en particulier dans un contexte de restriction budgétaire -donc d'effectifs- et pour une durée d'autant plus longue que les cyber-attaquants feront l'effort de maintenir une bonne sécurité opérationnelle et que les entités offensives seront efficacement disjointes et diversifiées. Etant donnée la limitation des effectifs de la cyber-défense, il est suggéré que la solution la plus réaliste est la prévention, passant par une opération de transformation intentionnelle sur les sources cindyniques : les déficits nomiques, et le contrôle de l'aléa juridique déclencheur de possibles processus de radicalisation.

P. Cohet.
V1b -Draft-3 mai 2013
Version temporaire susceptible de modifications.

[1] « *Cyber- is frequently used uncritically as a synonym for the Internet*.»
S. Reay Atkinson. *Cyber-: Envisaging New Frontiers of Possibility*. Unpublished, Advanced Research and Assessment Group, Occasional Series 03/09, Defence Academy of the United Kingdom.

[2] « *It appears that there is always a gap between how new systems are expected to operate and how they do operate in reality. The reason is that the vision of the market stakeholders is different from the vision of academic researchers, as the former do not care about optimized efficiency, but rather reduce the time-to-market and cost of real products. Hence, it can be easily noticed that, in practical terms, the modeling paradigm is to quickly design, implement and put-into-market simple solutions that (1) just work, (2) fulfill basic requirements and (3) can be patched to plug new functionalities or to improve their behaviors. Therefore, it seems that rethinking the current computation foundations to build large-scale CPS is not pragmatic. Instead, it seems that it is more natural to take profit from the legacy infrastructure to achieve the large-scale CPS objectives.* »

A. Koubâa, B. Andersson. *A Vision of Cyber-Physical Internet*. In : Proc. of the Workshop of Real-Time Networks (RTN 2009), ECRTS 2009, Juillet 2009. http://www.dei.isep.ipp.pt/~akoubaa/publications/AK-BA-RTN09-CRC.pdf

[3] Probable = « *Qu'il est raisonnable de supposer, de conjecturer ; qui risque fort de se produire.* »
Dictionnaire de l'Académie française, 9ème édition. http://www.cnrtl.fr/definition/academie9/probable

[4] « *La théorie de Shannon occulte délibérément et radicalement les contenus d'information, précisément, portés par les 'messages' considérés : seuls les contenus de signes constituant les 'messages' sont pris en considération (les alphabets, les codages, les longueurs mises en jeu). Il en va de même pour le contenu d'information de la loi de probabilité sur les signes de la source S.* ***Dans ces conditions, dénommer la théorie de Shannon 'théorie de l'information' est proprement induire du*** **contre-*sens.*** »
M. Mugur-Schächter. *Sur le tissage des connaissances*. Lavoisier, Paris 2006.

[5] « *The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point. Frequently the messages have meaning; that is they refer to or are correlated according to some system with certain physical or conceptual entities.* ***These semantic aspects of communication are irrelevant to the engineering problem.*** »
C.E. Shannon. *A Mathematical Theory of Communication*, Reprinted with corrections from The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, October, 1948.
http://cm.bell-labs.com/cm/ms/what/shannonday/shannon1948.pdf

[6] M. Mugur-Schächter. *Sur le tissage des connaissances.* Lavoisier, Paris 2006.

[7] « *Il est rapporté que le carthaginois répondit, si ce n'est dans un très bon grec, du moins librement, qu'il avait souvent vu de nombreux vieillards délirer, mais qu'il n'en avait vu aucun délirer autant que Phormion*. » Hannibal, commentaire sur Phormion. Cicéron, *De oratore, livre 2*. http://la.wikisource.org/wiki/De_oratore/Liber_II

[8] Elisabeth Paté-Cornell. *On "Black swans" and "Perfect storms": Risk analysis and management when statistics are not enough*.
Stanford University, December, 2011.
http://www.stanford.edu/dept/MSandE/cgi-bin/people/faculty/mep/pdfs/MEP.%20black%20swans%20and%20perfect%20storms.Rev5.Dec.2011.pdf

[9] A. Lenoir. *Comprendre la crise et prévoir la prochaine*. L'Harmattan, Paris, 2012

[10] Constat du GTR Cindyniques de l'Institut pour la Maîtrise du Risque, dirigé par Guy Planchette. Janvier 2013.

[11] K. Popper. *Un univers de propensions*. L'éclat, Combas, 1992.

[12] Les activités des acteurs scientifiques et des acteurs juridiques sont parfois sources de frictions, à titre d'exemple, dans l'affaire du séisme de l'Aquila, Jean-Paul Montagner commentait la décision de la justice italienne : « *Je ne m'y attendais pas du tout, je pensais naïvement que l'intelligence et le bon sens allaient triompher. Ce verdict est proprement hallucinant! Avec ce genre de logique, il faudrait intenter un procès à George Bush pour ne pas avoir pu empêcher l'attentat du 11 septembre et attaquer tous les chirurgiens de la planète qui n'ont pu sauver tous leurs malades. Les faits sont pourtants simples: on est encore incapables de prévoir les séismes*. »
http://www.lefigaro.fr/sciences/2012/10/22/01008-20121022ARTFIG00457-seisme-de-l-aquila-le-proces-de-scientifiques-inquietant.php
On peut aussi noter l'étude de Danziger et al. sur les facteurs humains impactant les décisions de justice :
Danziger S., Levav J., Avnaim-Pesso L. (2011). *Extraneous factors in judicial decisions*. Proceedings of the National Academy of Sciences of the United States of America. 108, 6889–6892.
http://www.pnas.org/content/108/17/6889.full.pdf http://www.ncbi.nlm.nih.gov/pubmed/21482790

[13] http://www.conseil-etat.fr/fr/rapports-et-etudes/-inventaire-methodique-et-codification-du.html

[14] « *Le Premier ministre a demandé au Conseil d'État de procéder à un inventaire méthodique du droit de la communication en vue d'une reprise du travail de codification. Existe-t-il, au-delà du droit des médias, qui est l'acception la plus courante du droit de la communication, un champ inexploré qui mériterait d'être codifié ? Pour répondre à cette question, il fallait faire deux choses: 1) réaliser un inventaire aussi large que possible du droit de l'information et de la communication, sans a priori sur le périmètre optimal d'un Code; 2) se demander en quoi la codification,* ***outre une meilleure accessibilité et intelligibilité des textes****, pouvait apporter des éléments éclairants sur le fond et, ainsi que les rapporteurs en ont très vite eu le sentiment, si la convergence numérique» ne rendait pas plus urgente une telle codification.* »[…]
« *Le second scénario proposé par le Conseil d'État réunit dans un même Code droit des médias et droit des communications électroniques, ainsi que les dispositions autonomes de la loi du 21 juin 2004 pour la confiance dans l'économie numérique.[…]* ***La clarté et l'intelligibilité du droit en vigueur dans les deux domaines seraient grandement améliorée par une codification commune***. »
L'étude du Conseil d'État: «Inventaire méthodique et codification du droit de la communication» par Thomas Andrieu, Auditeur au Conseil d'État, In : Conseil d'Etat. *Legicom N°40, Convergence numérique, convergence juridique? Actes du colloque du Conseil d'Etat du 28 novembre 2006*. Paris : Victoires éditions, 2007.

[15] G.Y. Kervern, P. Boulenger . *Cindyniques, Concepts et mode d'emploi*. Economica, Paris, 2007.

[16] J.L. Nicolet, G.Y. Kervern. *Cindynique de l'interface homme-animal et notamment des zoonoses*. Atelier AMRAE Cindyniques appliquées, janvier 2001.

[17] Cf Nouvelle procédure générique «Stall Warning or Aerodynamic Stall Recovery Procedure »
J. Rosay. *What is stall ? How a pilot should react in front of a stall situation*. Airbus Safety Magazine, Janvier 2011.
http://ebookbrowse.com/airbus-safety-first-mag-january-2011-pdf-d75431071

[18]Dans la liste des déficits systémiques cindynogènes (DSC), le DSC15 était décrit comme : « *disjonction entre le cognitif et l'éthique (science sans consience)* » même s'il était noté d T/T sans doute en raison de la forme en « H » de l'hyperespace. In : G.Y. Kervern. *Eléments fondamentaux des cindyniques*. Economica, Paris, 1995.
Le même DSC15 a été renuméroté DSC16 par la suite : « *DSC16 d A/E disjonction axiologique/épistémique* », avec cette fois la notation plus cohérente d A/E au lieu de d T/T. In : G.Y. Kervern, P. Boulenger. *Cindyniques, Concepts et mode d'emploi*. Economica, Paris, 2007.

[19] P. Cohet. *Approche infocindynique des crises financières et économiques : Lutte cognitive, étiologie des situations ante-crises et opérateurs de transformation pré-catastrophique*. IFREI, mai 2012.
http://www.ifrei.org/tiki-download_file.php?fileId=35

[20] Le triptyque de contenus visés était : le racisme et la xénophobie, le négationnisme, et la pédophilie. cf. /ex. : « *Cette interprétation a été pourtant contredite par le secrétaire général du Conseil, qui s'exprimait lors d'une explication de texte pour la presse, le 15 juin. Ce haut fonctionnaire avait alors considéré que le terme "manifestement" se rapportait à des cas d'illégalité flagrants, comme des propos ouvertements racistes ou xénophobes, ou encore des images pédophiles.* » J. Thorel. *LCEN: le Snep désapprouve en partie l'avis du Conseil constitutionnel*. Zdnet, 22 juin 2004.
http://www.zdnet.fr/actualites/lcen-le-snep-desapprouve-en-partie-l-avis-du-conseil-constitutionnel-39157926.htm
et : « *Selon l'explication du Conseil en conférence de presse, cela désigne avant tout les contenus incitant à la haine raciale ou à caractère pédophile.* » E. Dumout, J. Thorel. *Lcen : le Conseil constitutionnel censure l'amendement Devedjian*. Zdnet, 15 juin 2004.
http://www.zdnet.fr/actualites/lcen-le-conseil-constitutionnel-censure-l-amendement-devedjian-39157007.htm

[21] http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2004/2004-496-dc/decision-n-2004-496-dc-du-10-juin-2004.901.html

[22] H. Coutau-Bégarie. *Bréviaire stratégique*. Argos, Paris, 2013.

[23] « *Wikipédia n'a pas pour vocation de diffuser des informations illégales, bien au contraire. Mais quand Wikimedia Foundation a demandé un document légal fournissant un cadre juridique à la suppression d'un contenu s'appuyant sur un reportage vidéo, la DCRI a failli à fournir un tel document.* C'est la méthode brutale utilisée envers un administrateur de Wikipédia que nous dénonçons, *et non la protection du secret défense.*
À chaque sollicitation des forces de l'ordre, nous avons toujours répondu présent, avons consacré des heures à expliquer le fonctionnement de Wikipédia. Pourtant aujourd'hui c'est une méthode de pression qui a été utilisée, au lieu de celle du droit. »
P. Col. *Affaire DCRI / Wikipedia : interview exclusive de Christophe Henner, vice-président de Wikimedia France : Comment devenir la risée du monde entier ? Demandez à la DCRI*. Zdnet, 7 avril 2013.
http://www.zdnet.fr/actualites/affaire-dcri-wikipedia-interview-exclusive-de-christophe-henner-vice-president-de-wikimedia-france-39789081.htm

[24] La vulnérabilité d'une situation cindynique est sa propension à générer des dommages : il s'agit de la vulnérabilité de la situation, mais pas de la vulnérabilité d'un acteur. Il est cependant possible de définir la vulnérabilité cindynique d'un acteur comme étant la propension de la situation à générer des dommages impactant cet acteur. Cet aspect est *relativisé* dans l'approche multi-polaire par les spectres de situation.

[25]H. Simon. *Authority*, in : C. Arensberg. *Research in Industrial Human Relations : A Critical Appraisal*. Harper & Brothers publishers, New York, 1957.

[26] « *Si j'en reviens à l'année dernière, j'étais intervenu sur le thème de l'hygiène informatique, du retour aux bases. Je voudrais bien vous dire que tout le monde s'y est mis. Mais évidemment vous ne me croiriez pas, et vous auriez raison*. » Discours de Patrick Pailloux, directeur général de l'Agence nationale de la sécurité des systèmes d'information lors des Assises de la sécurité 2012 . SGDSN-ANSSI.
http://www.ssi.gouv.fr/IMG/pdf/Discours_Patrick_Pailloux-_Assises_2012.pdf

[27] P. Cohet. Extension du concept vulnérabilité/résilience : Opérateurs de conformation, conflictualité et conciliance des méta-situations infocindyniques. IFREI, Juin 2011.
http://www.ifrei.org/tiki-download_file.php?fileId=31

[28] Cf « friction d'innovation » in : P. Cohet. *Infocindynique et environnement informationnel.* IFREI, novembre 2010.
http://www.ifrei.org/tiki-download_file.php?fileId=29

[29] « *Le développement rapide des infrastructures numériques ne s'est pas toujours accompagné d'un effort parallèle de protection, de sorte que les agressions de nature cybernétique sont relativement faciles à mettre en oeuvre et peu coûteuses.* »
Livre Blanc Défense et Sécurité nationale 2013.
Version en ligne : http://www.elysee.fr/assets/pdf/Livre-blanc-sur-la-Defense-et-la-Securite-nationale.pdf

[30] « *Sur le plan juridique, on peut dès à présent penser que plusieurs gouvernements, au premier rang desquels le gouvernement américain, vont chercher à explorer des voies législatives ou réglementaires pour lutter à l'avenir contre la diffusion d'informations de cette nature depuis leur territoire. L'affaire révèle la tension entre une exigence croissante d'information, facilitée par les nouveaux outils de communication et les possibilités offertes par Internet d'une information quasi instantanée, de portée potentiellement mondiale, et la nécessité persistante pour les autorités publiques de protéger les informations confidentielles relevant de la sécurité de l'Etat. C'est une question essentielle, qui touche directement au fonctionnement de nos sociétés démocratiques modernes, et pour laquelle seule une approche équilibrée, soucieuse tant du droit à l'information des citoyens que de l'intérêt supérieur de l'Etat, semble pouvoir apporter une réponse.* »
SGDSN. *Ce que révèle vraiment WikiLeaks*. 15 février 2011.
http://www.sgdsn.gouv.fr/site_article108.html

[31] « *Un juge français va pouvoir enquêter pour déterminer si la société d'électronique Amesys, une filiale du groupe français Bull, s'est rendue complice de torture en Lybie en fournissant du matériel de surveillance de communications en 2007 au régime de l'ex-dirigeant libyen Mouammar Kadhafi.* »
F. Alexandre. *La société Amesys soupçonnée de complicité de torture en Libye*. RFI, 16 janvier 2013.
http://www.rfi.fr/france/20130116-amesys-soupconnee-complicite-torture-libye-surveillance-communications-bull
[32] «*Le Groupe Bull a signé un accord d'exclusivité pour négocier la cession des activités de sa filiale Amesys relatives au logiciel Eagle, destiné à construire des bases de données dans le cadre d'interception légale sur internet.*
Cette activité n'est pas stratégique pour le Groupe Bull qui souhaite se concentrer sur son expertise en matière de systèmes critiques électroniques et en particulier sur les domaines concernant la protection des personnes et du territoire. L'activité cédée représente moins de 0,5% du chiffre d'affaires du Groupe Bull. »
http://www.wcm.bull.com/internet/pr/new_rend.jsp?DocId=717953&lang=fr
[33] « *STUXNET : une « arme informatique » des Etats-Unis dirigée contre le programme nucléaire militaire iranien ?*
Le virus informatique STUXNET a été découvert en juin 2010 par la société biélorusse spécialisée dans les produits de sécurité informatique VirusBlokAda.
Les autorités iraniennes révèlent alors qu'elles ont été victimes d'une vaste attaque informatique visant leurs installations nucléaires. STUXNET aurait, en effet, endommagé le réacteur de la centrale nucléaire de Busher et détruit un millier de centrifugeuses du site d'enrichissement d'uranium de Natanz. Selon certaines sources, cette attaque aurait permis de retarder de six mois à deux ans, le programme nucléaire militaire de l'Iran.
Décrit à l'époque comme « l'arme cybernétique la plus sophistiquée jamais déployée » ou comme une « cyber arme de destruction massive » STUXNET est un virus informatique qui a été calibré pour s'attaquer à un logiciel informatique bien spécifique, mis au point par Siemens et utilisé dans différentes installations industrielles. Il s'agit de ce que les spécialistes appellent un SCADA (Supervisory, control and data acquisition), c'est-à-dire un système de contrôle et de supervision de processus industriels, utilisé dans des domaines tels que la distribution d'énergie ou la régulation des transports. »
La cyberdéfense : un enjeu mondial, une priorité nationale. Rapport d'information n° 681 (2011-2012) de M. Jean-Marie BOCKEL, fait au nom de la commission des affaires étrangères, de la défense et des forces armées, déposé le 18 juillet 2012.
http://www.senat.fr/rap/r11-681/r11-681_mono.html
[34] Dao De Jing 57 : 以正治國，以奇用兵，以無事取天下.
« *Rule a kingdom by the normal* [正]. *Fight a battle by (abnormal)* [奇] *tactics of surprise. Win the world by doing nothing* » .
Traduction : Lin Yutang. *The wisdom of LaoTse*. The modern library, New York 1948.
[35] cf fig. 11 : Potentiel insurrectionnel : fonction des déficits et divergences : $\Pi(\Delta, \nabla)$.
P. Cohet. *Approche infocindynique des crises financières et économiques : Lutte cognitive, étiologie des situations ante-crises et opérateurs de transformation pré-catastrophique*. IFREI, mai 2012.
http://www.ifrei.org/tiki-download_file.php?fileId=35
[36] H. Atlan. *Entre le cristal et la fumée. Essai sur l'organisation du vivant*. Editions du Seuil, Paris, 1986.
[37] « *Le choix du terme mythologique 'cosmos' (κόσμος) par Hayek pour désigner l'ordre spontané endogène pouvant émerger des systèmes auto-organisateurs est tout sauf anodin. Sous le cosmos, se cache le chaos : c'est bien du 'chaos' (χάος), transformé par un 'démiurge' (δημιοργός) que naît le cosmos. La 'main invisible' du démiurge est en pratique le processus de sélection naturelle permettant de créer l'ordre spontané à partir du chaos. De fait, le chaos a-téléologique est nécessaire à ce processus, qui permet à un certain nombre d'acteurs de s'organiser -de façon téléologique- et de gagner en puissance, et autorise même l'émergence de néo-pouvoirs dont la puissance est telle qu'elle peut supplanter et menacer celles des démocraties et des pouvoirs étatiques : Dès lors, le problème n'est pas tant celui de la distinction entre systèmes téléologiques ou non, que celui, topologique et stratégique, d'une redistribution de puissance entre acteurs téléologiques organisés (donc caractérisés par un ordre 'construit', correspondant -de facto- au 'taxis' hayékien, à un changement de topologie de puissance près).* »
P. Cohet. *Approche infocindynique des crises financières et économiques : Lutte cognitive, étiologie des situations ante-crises et opérateurs de transformation pré-catastrophique*. IFREI, mai 2012.
http://www.ifrei.org/tiki-download_file.php?fileId=35
[38] « *the emphasis is on using the side element* [偏] *for modifying* [修] *the* [正] *principal element* »
Unrestricted warfare : China's master plan to destroy America By Liang Qiao, Al Santoli(sic), *Xiangsui Wang.* Pan American Publishing Company, Panama City 2002. Traduction CIA/FBIS.
[39] W. Lawrence, International Crisis Group. http://www.guardian.co.uk/world/2013/apr/28/libya-mali-islamist-violence-tripoli
[40] P. Cohet. *Cindyniques et Art de la guerre, Infocindynique et Ultraguerre : La convergence cachée des sciences du danger et de la pensée stratégique chinoise*. IFREI, Août 2011.
http://www.ifrei.org/tiki-download_file.php?fileId=32
[41] P. Cohet. *Risques et menaces informationnels, efficience organisationnelle et opérationnelle.* Non publié, Colloque Intelligence économique, Willaya d'Oran, janvier 2012 .
[42] « *The large claim I advance here is that strategy does not merely entail this or that paradoxical proposition, blatantly contradictory and yet thought valid, but rather that* the entire realm of strategy is pervaded by a paradoxical logic *very different from the ordinary "linear" logic by which we live in all other spheres of life.* »
E. Luttwak. *Strategy : the logic of war an peace*. The Belknap Press of Harvard University Press, Cambridge, Massachusetts, 2003.
[43] « *Des questions aujourd'hui ouvertes méritent qu'une réflexion internationale plus poussée soit engagée au sein des Nations unies : comment interpréter la légitime défense de l'article 51 de la Charte de l'ONU face à des cyberattaques, ou face à des*

actions terroristes menées notamment par des groupes non-étatiques à partir d'États trop faibles pour contrôler effectivement leur territoire ? »
Livre Blanc Défense et Sécurité nationale 2013.
Version en ligne : http://www.elysee.fr/assets/pdf/Livre-blanc-sur-la-Defense-et-la-Securite-nationale.pdf

[44] « *On peut penser que la source c'est moi, c'est l'autre, c'est la nature des choses, c'est la Nature, c'est la Culture. La première tâche est donc de repérer les rhétoriques de légitimation, d'imputatio,n d'accusation, de disculpation, de consolation qui sont à l'oeuvre dans les différentes postures face au danger. Pour les cindyniciens, le concept de propension -au sens de Karl Popper- est assez vite venu prendre place sur les chemins de l'intelligibilité. De potentiel, le danger devient réel ; on dit qu'il se «matérialise». La propension du danger à se matérialiser est une fonction de la situation cindynique.* ***Cette situation est la source du danger.*** »
G.Y. Kervern. *Emergence et histoire des cindyniques. Déconstruction de la destruction*. Cerisy 2005.
et : G.Y. Kervern, P. Boulenger . *Cindyniques, Concepts et mode d'emploi*. Economica, Paris, 2007.