Institut français d'Analyse stratégique (IFAS)

—

Programme de Recherche 2013

Section 1

Orientations générales de l'IFAS

L'IFAS a été créé en 2001 par François Géré dans le but de réunir au sein d'une même équipe des compétences dans les domaines extrêmement variés qui sont aujourd'hui concernés par la stratégie et de façon générale par les questions de défense : relations internationales, sciences humaines et politiques, technologies des armements. Notre démarche consiste à intégrer domaines flous et sciences dures et de croiser les approches macrostratégiques (dimension globale des affrontements) et microstratégiques (particularités régionales des affrontements).

Les principaux domaines de recherche comportent :

- L'analyse des affrontements actuels, notamment guerrillas et terrorismes ;
- Le rôle du nucléaire dans le monde, civil et militaire ; dimension énergétique, stratégies, prolifération, risque terroriste, etc.
- Le triangle stratégique CHINE-Etats-Unis-Union européenne ;
- Le rôle stratégique des technologies de l'information et de la communication, en temps de paix, de crise et de guerre. mais aussi informatique, science de l'Internet, sécurité des Systèmes d'information, économie politique.

Section 2

Le domaine des études de Cyberstratégie

En raison de l'évolution accélérée de ce dernier domaine, il occupe désormais un espace tout particulier dans les travaux et recherches de l'IFAS.

On en trouvera ci-dessous les points saillants et les principales orientations de recherche.

Comme toute association à but de recherche scientifique, l'IFAS dispose de membres correspondants dans divers pays : Etats-Unis, Chine, Russie, Israël...

L'IFAS participe aux différents programmes d'études de l'UE et de l'OTAN.

La dernière section du présent document présente brièvement les membres de l'équipe, dont on trouvera sur le site de l'IFAS (http://www.strato-analyse.org/fr/spip.php?rubrique2) une présentation plus complète.

2.1 Organisation et géographie du Cyberespace

L'organisation spatiale et topologique de l'Internet, ainsi que le découpage de ses territoires entre puissances, sont des éléments de compréhension des conflits qui s'y déroulent. Nous travaillons avec le Professeur Kavé Salamatian, de l'Université de Savoie, qui a un cursus de recherche sur le sujet, ainsi qu'avec Michel Volle.

Nous avons mis en ligne quelques textes sur le sujet :

http://www.strato-analyse.org/fr/spip.php?article221
http://www.strato-analyse.org/fr/spip.php?article222
http://kave.salamatian.org/wordpress/?p=6

L'Internet est constitué de 5 000 et quelques réseaux qui communiquent entre eux de plein droit, c'est-à-dire qui ne sont pas juste les clients d'un autre réseau. À l'intérieur d'un réseau, son propriétaire (en général un fournisseur d'accès ou FAI) fixe les règles de fonctionnement auxquelles ses clients doivent obéir. On peut considérer l'Internet comme un continent dont ces réseaux seraient les États, qui auraient entre eux des frontières, dont le franchissement obéit à des règles déterminées par des *accords de transit* entre FAI. Ces accords sont instanciés dans des *routeurs*, c'est-à-dire des ordinateurs spécialisés connectés simultanément à plusieurs réseaux et capables de faire passer des données d'un réseau à un autre, selon des règles qui dans la cas considéré ici sont formulées selon la syntaxe du protocole *Border Gateway Protocol* (BGP).

Il y a entre réseaux une hiérarchie : les réseaux d'envergure internationale (le *tier 1*) peuvent conclure des accords de transit sur un pied d'égalité *(peering)* avec tous les autres opérateurs, cependant que les plus petits doivent acheter à un de ces grands opérateurs leur accès au réseau mondial, leur *connectivité*.

Les données circulent dans les fibres optiques de l'Internet à une vitesse proche de celle de la lumière, les distances physiques peuvent donc être considérées comme nulles, et on accordera plus d'importance à une distance mesurée en nombre de routeurs ou en nombre de réseaux à franchir entre deux points.

C'est l'étude de ces relations entre réseaux, de leur topologie et des rapports de puissance qui s'y établissent qui constitue l'objet de la cybergéographie.

2.2 Droit et économie

L'informatique et l'Internet remettent en cause notre compréhension de l'économie, parce que « l'informatisation bouleverse depuis 1975 le système productif en faisant émerger une *iconomie* qui, s'appuyant sur les rendements d'échelle croissants qui se diffusent à partir de la microélectronique, du logiciel et de l'Internet, transforme la nature des produits, la façon de produire et de commercialiser, les compétences, les organisations, la structure du marché, la forme de la concurrence et jusqu'aux préférences des consommateurs. » (Michel Volle[1]).

L'émergence de l'iconomie est une révolution industrielle, la troisième après celle de la fin du XVIII^{e} siècle (vapeur, mécanique, chimie) et celle de la fin du XIX^{e} siècle (électricité et moteur à explosion). Cette révolution peut remettre en cause tous les rapports de force entre nations, et les États qui n'en tireront pas les conséquences seront condamnés au déclin et à la dépendance.

Dans cette perspective, le contrôle des points d'échange entre réseaux (*Internet Exchange Points*, IXP) est aussi important que l'était celui des Dardanelles et du canal de Suez au temps de la seconde révolution industrielle. Pour analyser ces phénomènes, il faut réunir la compréhension économique du marché des connexions, la compréhension politique des

1 http://michelvolle.blogspot.fr/2012/12/de-leconomie-liconomie-opportunites-et.html

postures des États, la compréhension technique des protocoles du réseau, la compréhension géographique de son organisation topologique. Michel Volle est le précurseur de ce domaine de recherche.

2.3 Sécurité, liberté et prospérité

Internet, l'individu, l'État

L'usage de l'Internet est aujourd'hui répandu dans toutes les couches de la population ou presque, y compris dans les pays peu prospères. Il en résulte des bouleversements qui posent des problèmes inédits dans les sphères de la culture, du droit, de la police et de la défense. En témoignent en France les controverses soulevées par la création de la Hadopi par la loi Création et Internet, les conflits d'intérêt entre Free et Google ou entre Google et les entreprises de presse, et de façon générale tout ce qui a trait à la propriété intellectuelle, dont la législation actuelle demande notoirement une mise à jour. Aux États-Unis des problèmes analogues sont soulevés par les projets de loi (rejetés pour l'instant) SOPA *(Stop Online Piracy Act)* et PIPA *(Protect IP Act)*.

La protection de la vie privée est un autre sujet, dès lors que les systèmes de géolocalisation des téléphones portables permettent de suivre mètre par mètre les déplacements des individus, et que la mise en réseau de toutes les banques de données permet des recoupements de données personnelles, y compris biologiques et thérapeutiques, dont aucune dictature du siècle dernier n'aurait rêvé. Plus largement, c'est la démocratie qui est remise en question et dont certaines modalités doivent être redéfinies.

La localisation territoriale des données et de leurs traitements dans l'Internet devient de plus en plus difficile, surtout depuis la généralisation de l'informatique en nuage *(Cloud Computing)*, qui permet la migration de machines virtuelles et leur multiplication sans tenir compte des frontières, et sans préjudice du changement de régime législatif lors de leur franchissement. L'idée de Kavé Salamatian selon laquelle l'Internet devrait être défini comme un espace extra-territorial réglementé par une agence spécialisée de l'ONU semble alors s'imposer, mais restent à préciser les termes et les modalités de son application.

Ces sujets soulèvent la question de la gestion des identités dans le cyberespace : signature électronique, certificats, séquestre de clés. Des solutions techniques existent, qui ne sont pas à l'abri de toute critique, par exemple depuis la compromission d'autorités de certification reconnues telles que DigiNotar et GlobalSign. Et l'aspect technique n'est pas le plus important, l'acceptabilité de l'anonymat des transactions et de la navigation est l'objet de vigoureuses controverses, tout autant que celle de l'obligation de s'identifier.

Ces questions nécessitent l'intervention de chercheurs en sciences sociales, juridiques et économiques, en renfort des informaticiens et des stratèges.

2.4 Vers des cyberguerres ?

S'il est clair que le cyberespace, défini comme l'ensemble des données accessibles par l'Internet et des flux de leurs circulations, est à la fois un enjeu de conflits et le lieu potentiel d'actes agressifs commis au cours d'un conflit,

Si l'accord est à peu près unanime autour de l'idée qu'une offensive qui aurait lieu exclusivement dans le cyberespace ne saurait, du moins aujourd'hui, obtenir un résultat stratégique décisif tel que l'anéantissement des capacités (militaires ?) de l'adversaire, de nombreuses questions restent ouvertes :

- si la nécessité de capacités défensives est une évidence, un État démocratique doit-il développer des capacités offensives dans le cyberespace ? La création de capacités défensives dignes de ce nom est-elle possible en l'absence de compétences offensives ?

- si l'attribution à son auteur d'un acte d'agression cyber se heurte à des difficultés nombreuses et sévères, jusqu'à quel point peuvent-elles être surmontées, en d'autres termes, quel taux de succès peut-on espérer pour l'attribution ?
- en étroite corrélation avec le point précédent : quelles sont les voies possibles pour développer une stratégie de cyberdissuasion ?
- question classique de stratégie, à poser désormais dans le contexte cyber : l'avantage est-il à la défensive ou à l'offensive ?
- la riposte à une agression cyber doit-elle rester dans le cyberespace, ou se déployer par des moyens plus classiques ? et si l'on accepte la seconde alternative, comment déterminer les seuils de déclenchement des différents niveaux de riposte ?

Par ailleurs, comme il est inévitable dès lorsqu'existe une situation d'affrontement, on ne saurait se confiner aux « simples » conflits inter étatiques transfrontaliers. Il convient d'envisager les formes « inférieures » mais parfois excessivement meurtrières telles que les guerres civiles, les insurrections ou subversions avec leurs modes d'action tels que la guerrilla et le terrorisme. Le cyber terrorisme souvent évoqué, jamais sérieusement pratiqué jusqu'à présent, du moins à une échelle de haute létalité, finira sans doute par se frayer une voie spectaculaire. D'ores et déjà l'extorsion de fonds n'a plus besoin de recourir au kidnapping.

Dans les cas de soulèvements politiques intérieurs, l'usage de l'ensemble des réseaux sociaux constitue désormais un mode d'action fondamental tant pour l'organisation des manifestations que pour leur répression et pour assurer la diffusion hors des frontières de l'existence de l'affrontement interne (Iran 2009, Syrie depuis 2010).

L'ensemble de ces formes d'affrontement, les modes d'action et les instruments utilisés de manière classique ou novatrice, ne font à ce jour, l'objet d'aucune régulation internationale. La convention de Budapest de 2001 n'est ni universelle, ni contraignante pour les parties.

Tel est l'objet de la cyberdiplomatie.

2.5 *Cyberdiplomatie* : diplomatie et droit international

On introduit ici la catégorie de *Cyberdiplomatie* comme composante de la Cyberstratégie.

Ce champ de recherches se constitue comme résultante de l'analyse du jeu des grands acteurs, du positionnement de leurs intérêts d'où procèdent des alliances et de leur position respective au sein de la communauté des Nations.

L'objectif de la cyberdiplomatie est de parvenir à des accords de principe mais plus encore à des résultats concrets, à savoir : conclure des accords de bonne conduite pour adopter des normes de comportement coopératif entre États qui n'entretiennent pas toujours des relations de confiance. Ce domaine inclura donc l'étude de la mise en place et du développement de l'activité diplomatique des parties : les propositions de législation aux Nations Unies faites par différents États, notamment par la Russie, les offres de dialogue bilatéral, avec ou sans conditions préalables (tentatives pour le moment infructueuses américano-chinoises). Elle étudie le rôle des organisations internationales. Elle prend en compte les discussions, concertations et agréments au sein des différentes organisations internationales (UE, OTAN, Organisation de Coopération de Shanghaï). Elle évalue, en fonction des propositions formulées, leur niveau de compatibilité et estime leurs chances de succès.

Droit et dispositions réglementaires au plan international

Il n'est de diplomatie efficace que celle qui parvient à des traités et à des dispositions normatives auxquelles les Etats acceptent de souscrire. Quelles sont aujourd'hui les réponses

apportées par le droit international public et privé aux enjeux du fonctionnement « normal » du cyberespace ? On examine les différents cas de figure en situation de tension, de crise et d'affrontement pouvant aller jusqu'au recours à la force armée dont on aura à considérer la légitimité, ou, au contraire, l'arbitraire et l'illégalité.

Un droit international se construit autour du cyberespace. Il aura à se fonder sur des définitions : **qu'est-ce qu'une arme** dans le cyberespace, un procédé hostile, une agression, une attaque ?

Comment faire fonctionner le principe de légitime défense ?

Une diplomatie adaptée au cyberespace fait déjà l'objet d'initiatives multiples, bien peu coordonnées. Elle se cherchera encore longtemps. Elle comporte potentiellement des accords bilatéraux, multilatéraux, des règles de comportements, des normes (par exemple le cyber espionnage bouscule la tradition établie par agréments tacites entre services). Qu'en est-il, par exemple, de la **neutralité** au regard d'un domaine par définition déterritorialisé ?

Que deviennent les notions traditionnelles de *jus ad bellum* et de *jus in bello* ? Quel est leur degré de pertinence par rapport au cyberespace ?

Cet aspect sera traité en relation étroite avec le domaine de recherche 2.3 consacré à la sécurité humaine et à la garantie des libertés indivuelles.

Section 3

L'équipe

L'Institut français d'Analyse stratégique (IFAS) est *une structure interdisciplinaire* qui réunit des spécialistes de stratégie et de relations internationales, d'informatique et de réseaux de données, d'économie et de science des organisations, de systèmes d'information et de droit.

- François Géré, directeur de recherche en stratégie et relations internationales, président de l'IFAS (http://www.strato-analyse.org/fr/) ; auteur de nombreux ouvrages et articles sur la prolifération et la dissuasion nucléaires, la guerre psychologique, le terrorisme ;
- Michel Volle, économiste et statisticien, un des fondateurs de l'école française d'analyse des données, coprésident de l'Institut Xerfi (http://institutxerfi.org/), spécialiste des Systèmes d'information ; auteur de nombreux ouvrages et articles, ainsi que d'un site Web (http://volle.com/) et d'un blog (http://michelvolle.blogspot.fr/) ;
- Kavé Salamatian, professeur d'université en informatique et réseaux (université de Savoie), membre correspondant de l'Académie des Sciences de Chine, consultant pour de grands opérateurs et équipementiers (Cisco, Huaweï...) ; auteur de nombreux articles scientifiques (http://kave.salamatian.org/wordpress/?p=10) ;
- Hervé Schauer a créé en 1989 son propre cabinet de sécurité des systèmes d'information, HSC, qui conseille les plus grandes entreprises françaises et européennes ; il est un expert de réputation internationale, auteur de nombreux articles et ouvrages de référence, dont on trouvera la liste sur le site du cabinet HSC, http://www.hsc.fr/ ;
- Laurent Bloch a dirigé les équipes informatiques de l'Ined, du Cnam, de l'Institut Pasteur, avant d'être responsable de la sécurité des systèmes d'information (RSSI) de l'Inserm, puis directeur des systèmes d'information (DSI) de l'Université

Paris-Dauphine ; auteur de plusieurs ouvrages de référence et d'un site Web (http://www.laurentbloch.org/MySpip3/) consacré aux Systèmes d'information, à leur technique et à leur sécurité ;

- Olivier Danino, en cours de thèse de doctorat sous la direction de François Géré, a publié plusieurs articles remarqués, notamment sur la configuration géopolitique et stratégique du Moyen-Orient ;
- Lars Wedin, breveté d'études militaires supérieures du Collège de Défense à Stockholm et de l'École Supérieure de Guerre navale à Paris, auteur d'ouvrages et d'articles, notamment sur la guerre navale ;
- Thierry Widemann, historien spécialisé en histoire militaire comparée de l'Antiquité et du XVIIIème siècle, spécialiste de théorie stratégique ;
- David Rigoulet-Roze, titulaire de diplômes de Sciences politiques, de Relations internationale et de Géopolitique, auteur d'ouvrages et d'articles principalement consacrés à la situation géopolitique du Moyen-Orient moderne et contemporain ;
- Philippe Wodka-Gallien, diplômé de l'IEP, auteur de nombreux articles, notamment sur l'utilisation des technologies de pointe à des fins militaires.