La balkanisation du web : chance ou risque pour l'Europe ?

DELEGATION AUX AFFAIRES STRATEGIQUES
MINISTERE DE LA DEFENSE

La Délégation aux Affaires Stratégiques propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation.

Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la DAS a confié au Centre de Recherche des Ecoles de Coëtquidan, à l'Université Paris 8, à l'Institut Français de géopolitique de Paris et à l'Ecole Normale Supérieure de Paris cette étude sur le thème « La balkanisation du web : chance ou risque pour l'Europe », sous le numéro de marché 2013 1050 096 274.

Ministère de la défense

Délégation aux Affaires Stratégiques

Sous-direction Politique et Prospective de Défense

14 rue St Dominique

75700 PARIS SP 07

La balkanisation du web : chance ou risque pour l'Europe ?

Etude « La balkanisation du web : chance ou risque pour l'Europe » réalisée avec le soutien de la Direction aux Affaires Stratégiques

Septembre 2014

Etude réalisée par :

- Amaël Cattaruzza, CREC Saint Cyr
- Didier Danet, CREC Saint Cyr
- Alix Desforges, Institut Français de Géopolitique, Université Paris 8
- Frédérick Douzet, Institut Français de Géopolitique, Université Paris 8
- David Naccache, Département d'informatique, Ecole Normale Supérieure

Avec les contributions de :

- Jérémy Robine, Institut Français de Géopolitique, Université Paris 8 (réalisation des cartes)
- Kevin Limonier, Institut Français de Géopolitique, Université Paris 8 (étude de cas Russie)
- Jean-Sylvestre Mongrenier, Institut Français de Géopolitique, Université Paris 8 (enjeux de souveraineté et sécurité)
- Philippe Boulanger, Institut Français de Géopolitique, Université Paris 8 (étude de cas sur les pays du Golfe)
- Danilo d'Elia, Institut Français de Géopolitique, Université Paris 8 (enjeux économiques et industriels)
- Vincent Joubert, Institut Français de Géopolitique, Université Paris 8 (enjeux de souveraineté et de sécurité)
- Eric Laurent-Ricard, Département d'informatique, Ecole Normale Supérieure (solutions techniques)

SOMMAIRE

Introduction générale

Depuis les révélations de l'affaire Snowden et de programmes d'écoutes et de surveillance de grande ampleur mise en place par la NSA, les débats sur ce que certains appellent la souveraineté numérique ont ré-émergé et se sont multipliés. De la même manière les discours sur les risques de la fragmentation de l'Internet se sont amplifiés et se sont diffusés rapidement par le biais de la presse, des journaux ainsi que sur le web. Ainsi, le 6 février 2014, l'un des fondateurs du Web, Tim Berner-Lee intervenait dans la revue *Wired* en dénonçant les dangers qui pèsent sur la toile du futur : la cybercriminalité, les corporations économiques dominantes qui cherchent à miner le libre jeu du marché et le poids des gouvernements qui cherchent de façon technique ou juridique à prendre le contrôle de l'Internet[1]. Il dénonçait en particulier les programmes de surveillance américains et britanniques qui, en sapant la confiance des usagers, engendre, selon lui, la « *balkanisation du web* »[2]. D'après un panel d'experts interrogés par le Pew Research Center, la « balkanisation de l'Internet » résultant de l'action des Etats-nation constituerait même la principale menace qui pèse sur le futur de l'Internet[3].

L'usage du terme « balkanisation » doit retenir toute notre attention, compte tenu de sa signification implicite. Par « balkanisation », on entend historiquement l'idée du morcellement territorial d'une entité politique en plusieurs Etats concurrents. Le mot renvoie aujourd'hui très fortement à l'éclatement sanglant de la Yougoslavie du début des années 1990. Il s'agit ici pour Tim Berner-Lee de désigner une menace, cette notion supposant déjà une forme de condamnation. Nous avons affaire à une représentation, une manière subjective d'interpréter le monde, dont nous devons analyser à la fois les différents contenus implicites, et les acteurs qui en sont à l'origine. En géopolitique, les représentations ne sont pas neutres, elles ont une fonction dans les conflits, elles influencent et servent les décisions et stratégies des acteurs.

L'usage du terme « balkanisation » doit donc être étudié en soi. L'apparition de ce terme remonte à la fin de Première Guerre mondiale, date à laquelle il désignait le morcellement de l'Europe centrale et orientale (en particulier des Empires ottomans et austro-hongrois). Les travaux de Maria Todorova ont montré comment ce mot est, dès l'origine,

[1] http://www.wired.co.uk/news/archive/2014-02/06/tim-berners-lee-reclaim-the-web
[2] *Ibid.*
[3] http://www.pewinternet.org/2014/07/03/net-threats/

chargé d'une signification péjorative, supposant, en plus de la fragmentation territoriale, une régression politique vers une forme de tribalisme, voire de barbarie[4]. En désignant les Balkans comme une région intrinsèquement vouée au morcellement, et aux « haines endémiques », les Européens se déchargeaient de leur propre responsabilité dans l'apparition des crises qui ont conduit à la Première guerre mondiale (guerres balkaniques de 1912-1913, assassinat de l'archiduc François-Ferdinand le 28 juin 1914). Ainsi, l'expression « balkanisation », si son usage s'est banalisé depuis les conflits yougoslaves des années 1990, n'est pas neutre et renvoie à tout un imaginaire de la violence et du chaos politique. Elle semble présupposer une fragmentation sans fin du monde, une « prolifération étatique », aboutissant à des Etats fermés sur eux-mêmes, conduisant soit à des systèmes autoritaires, soit à des Etats non-fonctionnels (image de la « zone grise », mal contrôlée par les Etats, et des trafics qu'elle engendre). Aussi, la notion de « balkanisation » appliquée au cyberespace, au web ou à l'Internet —définis plus bas— produit-elle au moins deux effets. Elle conduit tout d'abord à considérer tous les processus ainsi désignés comme une menace et à considérer la « balkanisation » dans le sens avant tout politique d'un morcellement par les Etats. Elle coupe le pied ensuite à toute tentative de débats sur le réel danger de ces phénomènes qui relèvent en fait davantage de l'expression de rapports de force. L'expression de « balkanisation de l'Internet » doit donc être utilisée avec prudence, car elle soulève plus de problèmes qu'elle n'en résout. Elle s'insère dans un ensemble idéologique plus large, mobilisé en fonction des intérêts des acteurs soit pour assurer le maintien d'un rapport de force favorable, soit pour en créer un.

De fait, les discours utilisant la notion de « balkanisation » appliqués tantôt au cyberespace, tantôt au Web, tantôt à l'Internet, tantôt aux trois sont bien antérieurs à l'affaire Snowden. Le premier usage identifié de cette expression remonte à 1995, époque où le terme était fréquemment utilisé dans la presse internationale pour qualifier les événements en ex-Yougoslavie. On retrouve le terme dans l'ouvrage du *designer* indépendant américain David Siegel, qui diffuse sur l'Internet un texte intitulé « La balkanisation du Web ». Dans ce petit essai sur la construction et le *design* de sites en langage HTML, le terme de « balkanisation » est utilisé dans un sens très technique. Il ne s'agit pas de parler des différents pays et de leurs enjeux politiques, mais plutôt des limites du premier langage HTML, et des clivages qui s'ensuivent, notamment entre Netscape et Internet Explorer, les deux navigateurs étant dans les années 1990 en partie incompatibles l'un avec l'autre (un site ne pouvait s'afficher que sur l'un ou l'autre des navigateurs). Balkanisation s'entend ici comme un synonyme de

[4] Voir Maria Todorova, *Imagining the Balkans*, Oxford University Press, 1997

fragmentation, le contenu de l'Internet visible par l'usager étant partiellement dépendant du navigateur utilisé. Apparaît déjà une tension entre l'idée d'un cyberespace « universel » d'un côté, et l'émergence de plusieurs cyberespaces distincts de l'autre. Remarquons ici que ce sens technique est encore en usage aujourd'hui, certains acteurs voyant par exemple dans les versions mobile des sites à destination des smartphones, une nouvelle forme de fragmentation du Web.

Plus récemment, l'expression est de nouveau employée dans un sens beaucoup plus politique, et appliquée cette fois-ci à l'Internet dans son ensemble, à l'initiative d'universitaires américains comme Tim Wu et Jack Goldsmith. Tous deux professeurs de droit (respectivement à Columbia et Harvard), ils publient en 2006 l'ouvrage *Who controls the Internet ?*, dans lequel ils s'interrogent sur la tension existant entre l'Internet, en tant qu'outil de communication global, et les gouvernements nationaux qui cherchent à en prendre le contrôle. Selon eux, des puissances comme les Etats-Unis, la Chine ou l'Europe « *utilisent leur pouvoir de coercition pour établir différentes visions de ce que Internet devrait être* » (Goldsmith, Wu, 2006, p.184). L'avenir imposerait donc aux différents Etats de choisir leur « *modèle d'Internet* », en fonction de leurs valeurs et de leur régime politique, dans une gamme de propositions allant du modèle américain d'un Internet libre et sans entrave au modèle chinois d'un Internet sous contrôle politique. A terme, les auteurs décrivent la perspective d'un Internet territorialisé et morcelé en autant de cyberespaces que d'États. Dans cet esprit, Tim Wu, qui est également l'un des pères de l'expression de « neutralité du Web » en 2003, n'hésitait pas à parler dès 2005 de « balkanisation » possible de l'Internet, décrivant le contrôle politique pratiqué en Chine de manière très négative, ce que l'on peut interpréter comme une nouvelle occurrence du discours sur la « menace chinoise », qui imprègne à la même époque les milieux stratégiques américains[5]. Ce type de discours sur cette menace, auquel concourt l'expression de « balkanisation » de l'Internet du moins à l'origine, est concomitant d'un basculement géostratégique de la politique extérieure américaine vers l'Asie.

Remarquons le caractère très large et polymorphe de cette expression, qui peut s'appliquer tant à la couche matérielle qu'aux couches logique et sémantique du cyberespace

[5] Cette attention spécifique à la Chine se traduit par l'émergence de nouvelles expressions géopolitiques, comme celle de la « stratégie du collier de perles », apparue au début des années 2000 aux Etats-Unis et désignant un réseau de facilités logistiques et d'investissements portuaires financé par la Chine, courant du golfe Arabo-persique jusqu'à la mer de Chine méridionale. Cette représentation américaine identifie derrière ces investissements une stratégie chinoise planifiée, visant à sécuriser ses routes d'approvisionnement énergétiques, ce qui a toujours été démenti par la Chine.

et qui intègre à la fois des aspects techniques et politiques, mais aussi juridiques et économiques. Elle désigne en fait des phénomènes très larges et très disparates, qui vont du contrôle étatique (souvent évoqué par le biais de la sécurité nationale) à la volonté des Etats de créer leurs propres infrastructures nationales (comme dans le débats sur les *clouds* souverains), en passant par les difficultés de définition de juridictions dans le cyberespace ou encore la volonté d'introduire dans les noms de domaines différents alphabets nationaux (cyrillique ou chinois en particulier). L'ensemble de ces processus est décrit sous le même terme, celui de « balkanisation ». Dans le même esprit est apparue ces dernières années l'expression de « *splinternet* » (de l'anglais « *to splinter* », scinder ou fendre), dont la définition proposée sur le Wikipédia anglophone est elle aussi très large : « *Le splinternet (ou cyberbalkanisation ou balkanisation de l'Internet) décrit l'Internet comme la fragmentation et la division en raison de divers facteurs : technologiques, commerciaux, politiques, nationalistes, religieux et de divers intérêts* »[6].

Ainsi, l'aspect malléable de l'expression permet finalement, sous le couvert d'une formule se présentant comme « neutre » et objective, de qualifier un ensemble très étendu de pratiques et de processus très divers. Elle couvre sous le même vocable des débats aussi divers que le filtrage, la segmentation et la fragmentation potentielle résultant des politiques de sécurité nationale ; le maintien de l'opérabilité et d'un fichier racine commun ; les conflits autour des juridictions et l'application de la loi américaine dans le cyberespace via le principe d'extra-territorialité ; le contrôle national des contenus et des usages dans le cyberespace ; le modèle de gouvernance multi-parties prenantes par opposition à la montée en puissance d'un modèle intergouvernemental ; les pressions commerciales qui cloisonnent les contenus numériques via les algorithmes sélectifs, les systèmes d'exploitation mobiles ou les *app stores* exclusifs.

On notera que le concept est particulièrement mobilisé dès lors qu'il s'agit de remettre en question la suprématie de la première puissance mondiale dans le domaine. Cependant, la force de ce concept créé aux Etats-Unis est qu'il s'est rapidement diffusé de par le monde (plus particulièrement en Europe), par médias interposés, et qu'il est repris aujourd'hui par des acteurs ne participant pas directement aux intérêts américains.

Aussi, dans un souci d'explicitation des enjeux et problématiques que recouvre le concept, le terme « balkanisation » ne sera-t-il utilisé dans ce rapport que pour désigner l'ensemble des représentations évoquées ci-dessus et non comme un concept opératoire. Les

[6] http://en.wikipedia.org/wiki/Splinternet

termes de fragmentation technique, politique, économique et juridique seront préférés afin de décrire la complexité des processus à l'œuvre.

Ces remarques préliminaires sont importantes, car ce discours de la « balkanisation de l'Internet » s'inscrit dans un contexte géopolitique particulier. De fait, l'affaire Snowden a servi de catalyseur à des tendances de fond qui ont émergé au début des années 2000, et qui dépassent largement le domaine du cyberespace. Pour rester très schématique en introduction, nous pouvons distinguer huit orientations stratégiques majeures qui expliquent l'apparition de ce discours :

Première orientation : la remise en cause de la suprématie des Etats-Unis, qui s'attaque à la vision d'un monde structuré autour de l'hyperpuissance américaine et basé essentiellement sur l'idéologie de la démocratie libérale considérée comme à vocation universelle. Cette remise en cause générale se répercute y compris dans le cyberespace.

Deuxième orientation : la fin d'un monde unipolaire avec la montée en puissance des pays émergents, dont le Brésil, la Russie, l'Inde, la Chine, l'Afrique du Sud, (BRICS). Cette ascension de puissances émergentes engendre aux Etats-Unis la crainte d'une perte de puissance et d'une potentielle menace que ces pays pourraient représenter contre les intérêts américains dans le monde. Cette crainte s'accompagne de discours stratégiques plus ou moins alarmistes, en particulier vis-à-vis de la Chine considérée comme particulièrement offensive. Cette représentation de la menace chinoise est particulièrement perceptible dans les discours américains touchant au cyberespace.

Troisième orientation : la reprise en main par les Etats du cyberespace. Celle-ci est particulièrement visible dans le domaine militaire (multiplication rapide des doctrines militaires autour des questions de cyberdéfense, généralisation et banalisation des stratégies offensives), et dans le domaine de la sécurité (multiplication des agences de sécurité, création de cellules spécifiques au sein des polices et des douanes nationales, etc.).

Quatrième orientation : la dynamique de prolifération de lois et régulations visant à défendre son propre cyberespace et à remettre en place un contrôle aux frontières. Ainsi, des appareils législatifs complexes autour de l'Internet sont apparus au niveau juridique, tant à l'échelle des Etats qu'à celle d'organisations régionales comme l'Union européenne.

Cinquième orientation : la dynamique de globalisation du réseau. L'Internet est de moins en moins américano-centré. Le nombre d'utilisateurs est en constante augmentation à l'échelle du monde et de ce fait apparaissent sur le cyberespace de nouvelles langues, de

nouvelles pratiques et tout un ensemble de nouvelles communautés qui diversifient la toile et affaiblissent d'autant l'influence culturelle américaine en son sein.

Sixième orientation : l'omniprésence de la technologie et l'accroissement de la surveillance généralisée. La technologie s'est aujourd'hui insérée dans toutes les sphères privées et publiques de la vie quotidienne des individus et des organisations. Les informations ainsi générées sont innombrables et profitent aux puissances ayant les moyens d'instaurer une surveillance systématique de ces données. Or, au lendemain de l'affaire Snowden, ce constat, qui restait encore pour certains de l'ordre d'une hypothèse exagérée, voire paranoïaque, est aujourd'hui de notoriété publique. S'instaure donc un climat de méfiance générale vis-à-vis des réseaux interconnectés et de leurs usages par les Etats.

Septième orientation : le renforcement du pouvoir des géants économiques (Google, Amazon, Facebook, Apple, IBM, etc.) à travers diverses dynamiques, comme la généralisation du *cloud computing* et de l'Internet mobile. Ces phénomènes induisent un risque de fragmentation, tant au niveau de l'offre, que du contenu.

Huitième orientation : la fin des illusions d'un monde Internet idéalisé entièrement connecté, globalisé et pacifié. Celle-ci ci s'explique par deux facteurs. Tout d'abord, la permanence des conflits dans le monde est toujours d'actualité malgré les progrès constants des nouvelles technologies de l'information et de la communication (NTIC). Ensuite, le cyberespace a perdu aujourd'hui auprès des internautes son image de "neutralité" et d'espace de liberté, tandis que les pressions politiques et économiques s'accentuent en son sein. Ainsi, la monétisation de l'Internet offre un exemple de la fin de l'idée d'une information accessible à tous.

De fait, ces différentes tendances de fond entraînent une série de prises de conscience au sein des Etats et de leur population. Ainsi, les pratiques étatiques de surveillance se voient remises en cause du fait même de leur banalisation et de l'ampleur considérable prise par le phénomène. Les enjeux géopolitiques et stratégiques du cyberespace sont de plus en plus pris en considérations par les gouvernements nationaux. En Europe particulièrement, les différentes administrations s'interrogent sur le retard pris en termes économiques et politiques sur ces questions et sur la dépendance qui en résulte à l'égard des firmes américaines.

Enfin, un débat international émerge et se structure autour du thème de la gouvernance de l'Internet. La suprématie américaine dans le cyberespace est systématiquement remise en question. La polémique autour de l'*Internet Corporation for Assigned Names and Numbers*

(ICANN) offre un parfait exemple de cette contestation. L'organisation a un pouvoir de gouvernance primordial, puisque les Etats-Unis lui ont transféré la gestion de l'attribution des noms de domaines en 1998, y compris les noms de domaines à vocation régionale et nationale (ccTLDs), tout en conservant un contrôle final par le Département du Commerce, aujourd'hui remis en question comme nous le verrons. Si l'organisation se veut neutre, son attachement géographique, politique et juridique à l'administration américaine est ainsi indéniable. Or, cette contestation autour de la gouvernance se renforce depuis l'affaire Snowden autour du thème de la surveillance, un lien discursif étant quelquefois établi entre l'influence américaine sur l'ICANN et les programmes de la NSA.

Toutefois, les enjeux de gouvernance dépassent la simple question de la suprématie américaine. L'augmentation du nombre d'internautes entraîne de nouveaux défis et impose de repenser les cadres de la gouvernance pour assurer la transition vers trois milliards d'utilisateurs. Il devient de fait important de penser un système permettant d'assurer la coexistence pacifique de tous, y compris les nouveaux entrants dans le cyberespace. En termes de sécurité, cela implique également de nouveaux enjeux, comme la nécessité de redéfinir les cadres de la gouvernance de l'Internet et sur l'Internet, et de fixer dans la concertation des « règles du jeu » mondial pour assurer la sécurité collective.

Finalement, un clivage apparaît, que nous pouvons évoquer ici de manière très schématique, entre les partisans d'un Internet libre, ouvert, global, bénéficiant de facto aux Etats-Unis, du fait de leur prédominance économique, politique et technique dans ce secteur, et ceux qui remettent en cause ce modèle, évoquant l'idée d'une régulation politique ou même d'un contrôle à l'échelle des Etats, ou des organisations régionales. Deux approches contradictoires mais qui peuvent être promues par les mêmes acteurs en fonction des enjeux. La diffusion rapide de l'expression de « balkanisation de l'Internet » à l'échelle mondiale s'inscrit dans le cadre de ce débat. Or, qu'est-ce que la « balkanisation » dans ce contexte ? Si nous avons bien défini l'origine américaine de cette représentation, et son caractère instrumental chez les partisans d'une vision libérale de l'Internet, sa circulation de par le monde implique une réappropriation du concept par différents acteurs locaux non américains. Par conséquent, si l'expression de « balkanisation de l'Internet » peut avoir été pensée comme péjorative et menaçante par ses concepteurs, celle-ci n'a pas forcément la même signification pour tous ses usagers. Comprenons bien : dans les rivalités de pouvoir au sein et autour du cyberespace, les processus désignés et dénoncés sous l'appellation de « balkanisation » par certains acteurs peuvent être désirés, revendiqués et vus comme de nouvelles opportunités par

d'autres. Cette question de la signification des représentations géopolitiques en fonction des acteurs, en l'occurrence celle de balkanisation, sera donc également au cœur de notre étude.

A l'image du concept de balkanisation, il n'est pas inutile de revenir sur les définitions des termes cyberespace, web et Internet. L'Internet est le « réseau mondial associant des ressources de télécommunication et des ordinateurs serveurs et clients, destiné à l'échange de messages électroniques, d'informations multimédias et de fichiers. Il fonctionne en utilisant un protocole commun qui permet l'acheminement de proche en proche de messages découpés en paquets indépendants »[7]. Le web est l'une des applications de l'Internet qui consiste à l'aide d'un navigateur à accéder aux pages consultables sur les sites Internet. Les définitions de web et de l'Internet font l'objet d'un consensus, mais la situation est relativement différente en ce qui concerne le terme cyberespace. Reflétant les préoccupations, intérêts et stratégies des différents acteurs, on constate la multiplication des définitions du terme.

Dans le cadre de cette étude, on adoptera la définition a minima suivante : « le cyberespace, c'est à la fois l'Internet et l' « espace » qu'il génère : un espace intangible dans lequel s'opèrent des échanges déterritorialisés entre des citoyens de toutes nations, à une vitesse instantanée qui abolit toute notion de distance »[8]. Une conception aujourd'hui largement diffusée consiste à décrire le cyberespace comme constitué de plusieurs couches, en utilisant ici une métaphore géologique. Le nombre de couches distinguées varie d'ailleurs en fonction des auteurs, allant de 3 à 5, voire 7. Nous pouvons rappeler ici la théorie des 3 couches du cyberspace, car elle permet de mieux qualifier cet « espace », et de voir en quoi celui-ci peut être affecté par des frontières physiques, ou virtuelles. Le cyberespace serait donc composé de 3 couches superposées :

- une couche matérielle constituée par tous les périphériques d'accès et les infrastructures nécessaires à son fonctionnement chez les fournisseurs de connexions. C'est l'aspect physique d'Internet avec ses serveurs, ses câbles sous marins, ses satellites, ses fermes de données, etc.

- une couche logicielle constituée de strates, de langage machine et de protocole qui permet aux ordinateurs de communiquer les uns avec les autres, et d'échanger en des temps record de gros paquets de données. Cette couche comprendrait aussi les applications les

[7] Source : France Terme
[8] Frédérick Douzet, « La géopolitique pour comprendre le cyberespace », in Cyberespace : enjeux géopolitiques, *Hérodote*, n°152-153, pp. 3-21

programmes plus accessibles et conviviaux qui permettent aux internautes d'utiliser au quotidien leur machine, sans avoir besoin d'un savoir technologique avancé. Cette couche est la cible des attaques les plus fréquentes (virus, hacking, cheval de Troie, etc.).

- enfin, une couche sémantique ou cognitive qui est plus spécifiquement en rapport avec le contenu informationnel. En clair, l'ensemble des messages qui passe par l'Internet. Cette couche est donc le lieu des interactions sociales et des échanges d'information.

Sans changer cette structure de base, certains auteurs complexifient cette approche en distinguant d'autres « couches ». Il est ainsi possible de dissocier au sein de la couche logicielle :

- une couche de « l'infrastructure logique », qui « comprend tous les services qui permettent d'assurer la transmission des données entre deux points du réseau », et qui repose sur un langage commun (protocole TCP/IP) et sur des services comme le routage, le nommage, ou l'adressage (Douzet, 2014, p.6)

- une couche des applications, qui permet « à tout un chacun d'utiliser l'Internet sans rien connaître à la programmation informatique (Web, e-mail, réseaux sociaux, moteurs de recherche, etc.) » (Douzet, 2014, p.7).

Tout l'intérêt de cette conceptualisation théorique du cyberespace pour notre recherche sur les frontières est de nous fournir une dimension géographique plus concrète de l'Internet.

Dans ce contexte, le but de cette étude est d'évaluer la pertinence de ce discours en analysant la réalité des différents processus techniques, économiques, politiques, culturels qu'il désigne. Pour ce faire, le travail ici proposé s'articule autour d'une méthode multiscalaire, alternant des analyses à petites échelles, fournissant une vision globale des dynamiques à l'œuvre, et des approches plus focalisées, microscalaires ou thématiques (rapports de terrain, études de cas), donnant un éclairage local et régional permettant d'aborder le point de vue des différents acteurs impliqués. Si une territorialisation du cyberespace est aujourd'hui indéniablement à l'œuvre, celle-ci n'est pas forcément en-soi une menace, comme le sous-entend l'expression de balkanisation, et peut même au contraire être considérée comme une nouvelle opportunité d'expression pour les ensembles régionaux

encore plus ou moins sous dépendance américaine. Ce cadre étant posé, il s'agira donc pour nous de s'intéresser aux perspectives que ces processus ouvrent pour l'Europe[9].

La territorialisation du cyberespace ouvre la possibilité pour une organisation régionale comme l'Union européenne de promouvoir un modèle de l'Internet défendant les valeurs européennes : celles de la paix et de la prospérité. A rebours des rivalités émergentes, l'Europe peut porter le message d'une coexistence pacifique possible dans le cyberespace. Bien que le discours puisse paraître simple, il est important de réfléchir à l'application d'un tel modèle dans différents domaines. Quelle politique adopter pour l'Europe en terme législatif ? En terme industriel ? En terme stratégique et de sécurité ? En clair, il s'agit ici de s'interroger sur les enjeux de la « balkanisation » du cyberspace pour l'Europe, ainsi que sur la question : quelle Europe dans le cyberespace ? L'Union Européenne à 28 est-elle l'échelle pertinente pour penser une politique commune dans ce domaine ?

Pour répondre à ces questions, il s'agira tout d'abord d'évaluer la réalité de ces processus de territorialisation de l'Internet, à tous les niveaux : politiques, techniques, économiques, culturels, ce que nous aborderons dans la première partie. Puis, il faudra s'interroger sur ce que représente réellement cette balkanisation pour l'Europe, ce que nous ferons en deuxième partie. Quelle est la part du risque et de la menace ? Quels sont les enjeux pour l'Europe ? Enfin, quelle est la part de la chance et de l'opportunité ? La troisième partie explorera des pistes de réflexion stratégique pour l'Europe.

[9] Par Europe, nous entendons ici essentiellement l'Europe politique (Europe des 28) et non pas géographique. Toutefois, les stratégies européennes autour de l'Internet étant au mieux en cours de définition, ou au pire inexistantes ou sans impacts réels (comme dans le domaine industriel), nous nous intéresserons à l'échelle étatique, certains pays européens étant plus avancés que d'autres dans la mise en place d'une politique concernant le cyberspace (France, Allemagne, Espagne, Grande-Bretagne, Estonie entre autres).