Les enjeux de cybersécurité en Arabie saoudite

Variables culturalistes et conceptualisation d'une stratégie nationale

Lucie Le Barreau et Édouard Longeon

Volume 47, numéro 2-3, juin-septembre 2016

Enjeux géostratégiques au Moyen-Orient

URI : <https://id.erudit.org/iderudit/1039541ar>

DOI : <https://doi.org/10.7202/1039541ar>

[Aller au sommaire du numéro](#)

Éditeur(s)

Institut québécois des hautes études internationales

ISSN

0014-2123 (imprimé)

1703-7891 (numérique)

[Découvrir la revue](#)

Citer cet article

Le Barreau, L. & Longeon, É. (2016). Les enjeux de cybersécurité en Arabie saoudite : variables culturalistes et conceptualisation d'une stratégie nationale. *Études internationales*, 47(2-3), 155-175. <https://doi.org/10.7202/1039541ar>

Résumé de l'article

Les enjeux de sécurité au Moyen-Orient sont protéiformes. Partant de la définition de Buzan et Waever, nous entendons démontrer que, face aux menaces portées par le milieu « cyber » contre la sécurité nationale, les États du Moyen-Orient trouvent des réponses conformes à leur identité stratégique traditionnelle. Le cas de l'Arabie saoudite est particulièrement intéressant dans la compréhension des logiques du sous-système régional du golfe Arabo-Persique quant à l'intégration de la variable « cyber » dans la démarche de sécurisation, du fait de sa posture stratégique dominante. Dès lors, deux questions se posent à l'égard de cette analyse : la première relève du volet strictement théorique et interroge la lecture culturaliste des stratégies mises en place devant la montée des enjeux de cybersécurité au Moyen-Orient. La seconde s'intéresse aux dynamiques du complexe régional et aux tensions systémiques procédant de la confrontation entre l'interdépendance des acteurs étatiques et leur recherche de sécurité nationale.

Les enjeux de cybersécurité en Arabie saoudite

Variables culturalistes et conceptualisation d'une stratégie nationale

Lucie LE BARREAU et Édouard LONGEON*

RÉSUMÉ : *Les enjeux de sécurité au Moyen-Orient sont protéiformes. Partant de la définition de Buzan et Wæver, nous entendons démontrer que, face aux menaces portées par le milieu « cyber » contre la sécurité nationale, les États du Moyen-Orient trouvent des réponses conformes à leur identité stratégique traditionnelle. Le cas de l'Arabie saoudite est particulièrement intéressant dans la compréhension des logiques du sous-système régional du golfe Arabo-Persique quant à l'intégration de la variable « cyber » dans la démarche de sécurisation, du fait de sa posture stratégique dominante. Dès lors, deux questions se posent à l'égard de cette analyse : la première relève du volet strictement théorique et interroge la lecture culturaliste des stratégies mises en place devant la montée des enjeux de cybersécurité au Moyen-Orient. La seconde s'intéresse aux dynamiques du complexe régional et aux tensions systémiques procédant de la confrontation entre l'interdépendance des acteurs étatiques et leur recherche de sécurité nationale.*

MOTS-CLÉS : relations internationales, culture stratégique, cyberstratégie, cybersécurité, sécurité, sécurité nationale, risque cybernétique

ABSTRACT : *Security issues in the Middle East are highly variable. Using Buzan and Waever's definition as its starting point, this paper seeks to demonstrate that, in the face of cybersecurity threats to national security, Middle Eastern governments respond according to their traditional strategic identities. The case of Saudi Arabia is particularly helpful in understanding the logic behind the integration of cybersecurity into national security approaches in the Persian/Arabian Gulf regional sub-system due to the country's dominant strategic position. Two questions arise from this analysis : the first is strictly theoretical and queries the culturalist interpretation of the strategies developed in response to growing cybersecurity threats in the Middle East. The second looks at regional subsystem dynamics and the systemic tensions that result when the interdependence of state actors comes into conflict with their search for national security.*

KEYWORDS : International relations, strategic culture, cyberstrategy, cybersecurity, security, national security, cybernetic risk

* Lucie Le Barreau est docteure en science politique et membre du CLESID de l'Université Jean Moulin Lyon 3. Édouard Longeon est consultant Sécurité et Risk Management au sein du cabinet de conseil CGI Business Consulting.

RESUMEN : *Los retos en materia de seguridad en el Oriente Medio son pro-teiformes. Partiendo de la definición de Buzan y Wæver, pretendemos demostrar que, frente a las amenazas que representan los desarrollos del Internet y la informática para la seguridad nacional, los estados del Oriente Medio dan respuestas de acuerdo a su identidad estratégica tradicional. El caso de Arabia Saudita es muy interesante en la comprensión de las lógicas del sub-sistema regional del golfo árabo-pérsico con respecto a la integración de la variable cibernética en el proceso de seguridad, debido a su postura estratégica dominante. Por consiguiente, se plantean dos cuestiones con respecto a este análisis : la primera es del ámbito estrictamente teórico y pone en tela de juicio la lectura culturalista de las estrategias implementadas frente a la escalada de las problemáticas de ciberseguridad en el Oriente Medio. La segunda se interesa por las dinámicas del complejo regional y las tensiones sistémicas derivadas de la confrontación entre la interdependencia de los agentes estatales y su búsqueda de seguridad nacional.*

PALABRAS CLAVE : relaciones internacionales, cultura estratégica, ciberestrategia, ciberseguridad, seguridad, seguridad nacional, riesgo cibernético

À l'heure de l'interconnexion des sociétés, envisager les « enjeux de sécurité » demande qu'on s'intéresse aux nouvelles formes de menaces induites par les réseaux informatiques. En effet, le « risque cybernétique » fait aujourd'hui partie intégrante des contraintes qui pèsent sur les acteurs du système international dans leur processus de conceptualisation de leur sécurité. Les États, en particulier, ne peuvent échapper au processus de formulation d'une stratégie de réponse efficiente, mais également cohérente avec les doctrines déjà à l'œuvre au niveau national. Dès lors, nous entendons démontrer dans cet article la pertinence de l'approche proposée par les variables culturalistes non seulement dans la formation, mais également dans la compréhension de ces « cyberstratégies ».

L'Organisation internationale de normalisation (ISO) propose une approche de la sécurité de l'information servant de base aux développements suivants. Elle considère ainsi que :

La valeur de l'information dépasse les mots, les chiffres et les images : la connaissance, les concepts, les idées et les marques sont des exemples de formes d'information immatérielles. Dans un monde interconnecté, l'information et les processus, systèmes et réseaux qui s'y rattachent, ainsi que le personnel impliqué dans son traitement, ses manipulations et sa protection, sont des actifs précieux pour l'activité d'une organisation, au même titre que d'autres actifs d'entreprise importants, et, par conséquent, ils méritent ou nécessitent d'être protégés contre les divers risques encourus (ISO/CEI 27002).

Il est possible d'associer cette définition à des risques particuliers grâce à la méthode EBIOS (Expression des besoins et identification des objectifs de sécurité) créée par l'ANSSI (Agence nationale de la sécurité des systèmes

d'information). Cette méthode décrit la sécurité de l'information comme étant une « satisfaction des besoins de sécurité des biens essentiels », ces biens considérés comme critiques et nécessaires au bon fonctionnement d'une activité. Pour évaluer un risque cybernétique par la méthode EBIOS, un processus itératif est décliné en plusieurs modules, facilitant l'analyse d'un contexte, l'étude d'événements redoutés, l'étude de scénarios de menaces et la définition de risques et de mesures de sécurité¹.

Nous retiendrons, en définitive, que le risque cybernétique – autrement désigné comme le risque relatif à la sécurité informatique – doit être entendu en termes opérationnels comme « *potential that a threat will exploit a vulnerability of an asset or group of assets and thereby cause harm to the organization* » (ISO/CEI 27000; AFNOR 2013). D'un point de vue plus théorique, nous entendrons le risque cybernétique comme les menaces que font peser sur la sécurité les nouvelles technologies de l'information et de la communication, tant dans leur existence – par exemple l'informatisation constante des données et des processus – que dans l'utilisation qui peut en être faite – par exemple la manipulation comme arme.

Ainsi, parmi les nombreux enjeux de sécurité auxquels le Moyen-Orient doit faire face, on ne peut désormais plus écarter de l'analyse ceux qui relèvent du cyberspace. Concevoir la sécurité comme « la capacité d'une société à conserver son caractère spécifique malgré des conditions changeantes et des menaces réelles ou virtuelles [et qui] concerne la permanence de schémas traditionnels de langage, de culture, d'association, d'identité et de pratiques nationales ou religieuses » (Buzan et Wæver 2003 : 9), c'est admettre que les menaces contre la sécurité ne relèvent plus seulement d'une vision réaliste des relations internationales. Le cyberspace emporte avec lui de nouvelles formes de violence et par conséquent de menace contre la sécurité des États, dans leur individualité, mais également dans leur organisation systémique, régionale ou internationale. Le Moyen-Orient n'échappe pas à cette logique : l'attaque informatique de 2012 sur les infrastructures de Saudi Aramco le prouve bien. La cybersécurité devient donc primordiale pour la sécurité des États. Elle prend place dans un théâtre où les conflits aux frontières sont récurrents, où les résurgences identitaires et religieuses des minorités sont certes maîtrisées par le pouvoir central saoudien, mais où elles restent très vives. Une cyberattaque de cette ampleur ancre la prise en compte d'une nouvelle variable sécuritaire dans le golfe Arabo-Persique : la sécurité informatique.

Nous appuyant sur la définition proposée par Buzan et Wæver, nous entendons démontrer la pertinence des variables culturalistes dans la compréhension de la conceptualisation d'une stratégie nationale efficace face à la montée des

1. D'après la méthode EBIOS, un risque est souvent caractérisé en référence à des événements et des conséquences potentiels ou à une combinaison des deux. Un risque est ainsi souvent exprimé en termes de combinaison des conséquences d'un événement et de sa vraisemblance.

enjeux de cybersécurité. Nous prendrons pour appui le processus s'étant développé en Arabie saoudite. Ce cas est particulièrement intéressant dans la compréhension des logiques du sous-système régional du golfe Arabo-Persique quant à l'intégration de la variable «cyber» dans la démarche de sécurisation. Initiatrice d'un modèle stratégique dominant, conforme aux spécificités culturelles de la région, elle doit aujourd'hui faire face à la montée d'autres acteurs étatiques, tels que les Émirats arabes unis et le Qatar. La question se pose *in fine* de la modélisation de la cyberstratégie saoudienne au sein des dynamiques du complexe régional et des tensions systémiques procédant de la confrontation entre l'interdépendance des acteurs étatiques et leur recherche de sécurité nationale.

La prise en compte des menaces relevant du cyberspace dans la formulation des stratégies nationales de défense est relativement récente. Pour autant, elle constitue un défi majeur pour les gouvernements, puisqu'il s'agit pour eux, désormais, de faire face à de nouvelles formes de violence et d'atteintes à la sécurité. Les stratégies applicables au cyberspace – autrement appelées cyberstratégies – relèvent du savoir classique stratégique détenu par les États et suivent ainsi les schémas habituels dans son processus de création. Pour autant, la spécificité de l'espace informatique – le cyberspace – nécessite l'inclusion de nouvelles variables dans le processus. De fait, si les études théoriques classiques – et en particulier le courant réaliste – montrent bien une prise en compte des intérêts des États, de leurs volontés de puissance, mais aussi de rayonnement au sein du système international, il n'en demeure pas moins que le cyberspace exige une accentuation de ces principes.

Les variables culturalistes, et en particulier le concept de «culture stratégique», identifient ainsi la linguistique, l'histoire, la religion, la construction étatique et les interactions sociales comme opérantes dans le processus de modélisation d'une cyberstratégie. En effet, ces éléments dévoilent des logiques rationnelles et pragmatiques, ontologiquement basées sur la domination d'une structure étatique, un processus perpétuel de mise à jour des capacités de l'État, la résilience de celui-ci vis-à-vis des attaques extérieures et une course à la technologie. Cependant, ces logiques ne peuvent prétendre proposer à elles seules une lecture complète du cyberspace et de ses conséquences sur les enjeux sécuritaires.

I – Les fondements théoriques de l'application des variables culturalistes au risque cybernétique

A — Le cadre géopolitique et géostratégique spécifique d'analyse : le golfe Arabo-Persique

Le Moyen-Orient doit être limité géographiquement aux États situés «sur près de quatre mille kilomètres entre les détroits turcs et la pointe sud de l'Arabie sur

l'Océan indien, ou entre la Vallée du Nil et les confins de l'Afghanistan» (Lacoste 1994 : 677). Cependant, à ces considérations purement spatiales il convient d'ajouter des précisions relatives à la spécificité culturelle et religieuse de cet espace politique. Le concept de « monde arabo-musulman » permet ainsi de mettre en évidence des variables culturalistes, fondées notamment sur la pratique de l'islam (Lacoste 1994).

De manière à pouvoir apporter un moyen de comparaison, les doctrines stratégiques opérant dans les pays qui relèvent du sous-système occidental semblent les plus abouties, sur le plan de la formalisation opérationnelle, mais également quant à la délimitation des buts politiques. Il s'agit par conséquent de s'écarter des études actuelles afin de s'intéresser au complexe régional du Moyen-Orient, et plus spécifiquement au sous-complexe du golfe Arabo-Persique. En effet, ce dernier propose des particularismes culturels rendant difficiles les analyses scientifiques complexes et expliquant le manque de conceptualisation notable en matière de positionnement de ces États dans le domaine du cyberspace.

On tient pour constitutifs de ce sous-complexe régional les États de Bahreïn, du Qatar, de l'Arabie saoudite, des Émirats arabes unis, du Koweït et de l'Iran. Mais on considère Oman comme lié mais non inclusif. S'il est admis que ce pays développe des postures stratégiques cohérentes avec le sous-complexe envisagé, tant en matière d'organisation de sa défense qu'en ce qui concerne les principes de sa politique étrangère, il n'en demeure pas moins que la lecture géopolitique classique qui est la nôtre le distingue du sous-complexe spécifique sélectionné. En effet, malgré sa présence en bordure du Golfe, entendu dans sa réalité géographique, Oman est davantage tourné vers le golfe d'Oman. Cette réalité géographique le pousse à concevoir une dynamique proche de notre cas d'étude, sans en être complètement constitutif. On ne peut à ce titre nier le choix stratégique d'Oman d'incarner une forme de « Suisse arabe » par l'affirmation d'un processus de neutralité – envisagée dans son acception de tiers stratégique au sens de la science politique et de la sociologie politique – et par conséquent de son désir d'émancipation des phénomènes de conflictualité de la région. Ces pays ont longtemps été considérés comme « en voie de développement » dans le domaine des technologies de l'information, alors même que, paradoxalement, cette région est soumise à des tensions cyberstratégiques fortes, notamment du fait de la proximité géographique d'acteurs transnationaux habitués à l'exercice, par exemple depuis 2014 l'organisation État islamique, qui a développé ses principes de communication en s'appuyant sur une très grande maîtrise des outils numériques. En s'appuyant sur les conceptions transnationalistes développées par Keohane et Nye dans les années 1970, on considère que le système international est composé non seulement des États, mais également d'autres acteurs dont la portée d'action dépasse les espaces frontaliers juridiquement reconnus. « La société internationale est composée, outre des rapports

interétatiques, de relations entre diverses formes d'organisations et d'individus [...]. Pour ses tenants les rapports mondiaux ne sont pas internationaux, mais plutôt transnationaux» (Macleod et O'Meara 2010 : 155). Les acteurs transnationaux peuvent donc être envisagés comme un « ensemble hétéroclite constitué par les ONG (organisations non gouvernementales), les firmes multinationales, les opérateurs financiers, les migrants, les terroristes, les trafiquants de drogue, les mafias, et une infinité d'autres acteurs privés » (Cohen 2005).

Ainsi, on note comme postulat empirique initial à cette étude la distinction fondamentale entre les cultures stratégiques des États du golfe Arabo-Persique et ceux d'autres pays situés au Moyen-Orient. Qu'il s'agisse de l'Iran, de la Syrie ou de l'Irak – puissances régionales fondées sur une construction étatique mouvementée mais plus ancienne –, on ne peut que constater qu'au-delà de la proximité culturelle, les ancrages stratégiques divergent. À ce titre, il convient de préciser que l'Iran en tant qu'État-nation détient une antériorité historique, alors que, si le passé de l'Irak est une réalité géographique, l'affirmation de ce pays en tant qu'État-nation est plus récente. Il faut donc distinguer l'ancienneté historique de la nature de l'État. De fait, les États de notre sous-complexe régional spécifique sont plus récents et se sont forgés sur des préceptes culturels fondamentalement centrés sur la domination politique de grandes familles dirigeantes et sur l'appartenance à l'islam. Leur positionnement stratégique est par ailleurs emprunté des dynamiques internationales modernes et, en particulier, des domaines de développement désormais centraux, tels que les économies pétrolière et gazière. Les perspectives de mise en valeur de leur puissance ne passent donc plus exclusivement par une prépondérance diplomatique ou militaire, mais par une volonté d'expansion économique et de contrôle de la finance. Dès lors, les variables explicatives convocables à l'analyse de la culture stratégique de ces États varient, et cela est d'autant plus vrai dans la conceptualisation de leur culture stratégique appliquée particulièrement au cyberspace.

Nous devons par conséquent tenir compte dans notre démonstration de plusieurs phénomènes sociologiques propres au sous-complexe régional du golfe Arabo-Persique, dans une perspective précise de conceptualisation de la culture cyberstratégique de l'Arabie saoudite. Parler d'ancrages stratégiques divergents, c'est admettre que les fondements religieux des cultures des États du Golfe sont eux-mêmes différents. Ainsi, si le phénomène religieux islamique constitue un trait commun, les conceptions de l'islam n'en demeurent pas moins hétéroclites et source de conflit entre groupes représentatifs au sein d'un même État. L'opposition entre chiisme et sunnisme dans les provinces Est et Sud-Ouest de l'Arabie saoudite rendent aussi compte de facteurs conflictuels sur des espaces partagés par plusieurs États, dont le Yémen et les Émirats arabes unis. À une conflictualité théologique inhérente aux populations s'agrègent désormais des conflits de domination territoriale. Cette structure régionale est, de fait, sujette à de nombreuses tensions entre les États qui la composent. Les pratiques sont

comparables mais non identiques, et la rigueur scientifique impose de tenir compte de ces éléments dans la conceptualisation de la cyberstratégie, d'autant plus lorsqu'elle est appliquée à un seul des acteurs en présence. Ainsi, l'Iran s'affirme comme l'une des frontières naturelles du complexe régional, mais elle ne peut pas en être totalement exclue au regard de son rôle de puissance régionale. Selon notre approche, l'Arabie saoudite et les pays du golfe Arabo-Persique se développent entre traditionalisme religieux et modernisme social, proposant une vision hybride entre les différents modèles stratégiques à l'œuvre. Ajoutons que les États comme l'Irak, la Syrie, la Jordanie et Israël représentent des zones de tensions majeures, marquées par des rivalités religieuses intrinsèques et par des interventions étrangères récurrentes, tant militaires qu'humanitaires. Par conséquent, tenter de comprendre les logiques stratégiques inhérentes au Moyen-Orient s'avère théoriquement et empiriquement complexe, et cela nécessite d'envisager chaque État dans sa spécificité nationale sans exclure totalement les contraintes que font peser sur lui le système international et le sous-système régional.

C'est le choix qui a été le nôtre dans le cas de l'Arabie saoudite. Appartenant au golfe Arabo-Persique, cet État est marqué par une hybridité stratégique qui implique une modernisation rapide, d'une part, et la conservation des lignes traditionnelles, culturelles et religieuses, d'autre part. Il fait ainsi partie de ces États ayant décidé de se doter de protections informatiques dès les années 2000, de façon précipitée et en investissant de nombreux moyens techniques, sans pour autant disposer du recul nécessaire quant à la cohabitation du cyberspace et de sa culture politique nationale. Malgré son leadership régional de coopération cybernétique, l'Arabie saoudite n'échappe pas à cette logique de fragmentation, et l'analyse du processus de conceptualisation de sa culture stratégique en matière de cybersécurité met en évidence les failles inhérentes à ce sous-complexe régional, au regard des variables culturalistes.

B — Les fondements des variables culturalistes : culture stratégique et identité stratégique

Le terme « culture stratégique » renvoie à des conceptions et à des domaines multiples.

La référence aux notions de culture stratégique, de sécurité, de guerre ou militaire, ne trouve pas place dans une théorie, mais plutôt dans une série d'approches théoriques – non des moindres aujourd'hui, le social constructivisme, les études critiques et postmodernes de sécurité (Wasinski 2006b : 117).

Il apparaît ainsi que l'étude de ce concept impose une certaine pluridisciplinarité pour offrir toute son envergure analytique. Cet outil de compréhension des postures étatiques est ancien et repose sur la compréhension des « particularités nationales stratégiques historiquement fondées » (Wasinski 2006b : 118). Il

faudra cependant attendre la fin de la crise des études stratégiques des années 1970 pour voir s'affirmer cette notion, sous la plume de Jack Snyder en 1977, quant à la culture stratégique soviétique en matière nucléaire. L'auteur définit alors la culture stratégique comme « la somme totale des idéaux, réponses émotionnelles conditionnées et modèles de comportements habituels que les membres d'une communauté nationale ont stratégiquement acquis au travers de l'instruction ou de l'imitation et qu'ils partagent entre eux par rapport à la stratégie nucléaire » (Wasinski 2006b : 123-124). Dès lors, « la culture stratégique permet de prendre en compte les intentions au travers des discours et de l'expérience historique » (Wasinski 2006b : 123-124). Le débat relatif au concept de culture stratégique a cependant évolué. Colin Gray l'envisage ainsi comme étant :

basé sur l'auto-appréciation d'une expérience historique et du caractère national. [...] Telle qu'il l'envisage, la culture stratégique est un mélange d'histoire, de géographie, de philosophie politique, de culture civique. En fait, Gray présuppose l'existence de cultures stratégiques distinctes. Il les considère comme un environnement qui influence la prise de décision (Wasinski 2006b : 123-124).

La question de la nature et de la proportion de cette influence reste cependant en suspens. Carnes Lord, quant à lui, considère que :

la culture stratégique est composée de la géopolitique, des relations internationales, de la culture politique et de l'idéologie, de la culture militaire (histoire militaire, traditions et éducation des soldats, des relations civils-militaires dans l'organisation bureaucratique et des équipements, armements et technologies disponibles) (Wasinski 2006b : 123-124).

Un tournant est opéré dans la compréhension et l'utilisation du concept avec l'émergence du courant constructiviste dans les théories des relations internationales.

L'idée selon laquelle la réalité est en fait le fruit de constructions intersubjectives était déjà bien implantée dans de nombreuses disciplines, comme la philosophie et la psychologie. Le matérialisme reste pourtant longtemps dominant dans l'étude de la politique internationale (Wasinski 2006b : 127).

In fine, la culture stratégique a traditionnellement été appliquée à des ensembles étatiques. Le postulat initial a été de considérer qu'il existait plusieurs cultures stratégiques selon les types d'États, et que pour en déterminer ses fondements il s'agissait de déterminer les particularismes opérant au sein d'un État envisagé. Le postulat soutenu ici est celui selon lequel les variables culturalistes favorisent la compréhension des schèmes à l'œuvre dans la formulation d'une cyberstratégie. On pourrait dès lors envisager l'identité stratégique de l'Arabie saoudite comme révélatrice de la culture stratégique du système régional duquel elle dépend, le Moyen-Orient. Même si plusieurs États reposant sur un socle

commun de critères peuvent partager la même culture stratégique, il n'en demeure pas moins qu'ils développent des spécificités nationales qui correspondent à des positionnements stratégiques subjectifs au sein d'une catégorie d'États.

Il convient à ce stade de notre démonstration de préciser les variables que nous entendons tirer des «perspectives culturalistes». Cette grille méthodologique s'inscrit ouvertement dans une perspective multidimensionnelle, mais surtout pluridisciplinaire. Ainsi que nous l'avons envisagé précédemment, prenant la mesure de l'étendue du champ d'étude proposé, nous estimons impératif de ne pas limiter les approches nourrissant l'argumentation qui sera la nôtre. À ce titre, nous évoquons les travaux d'Anne-Marie Slaughter, qui a tenté de répondre à la question de la pertinence de cette méthode dans un article publié en 1998. L'auteure développe ainsi deux niveaux d'argumentation venant expliquer ce phénomène analytique.

Pour le premier niveau, l'intérêt dans la collaboration interdisciplinaire peut être compris comme le résultat des réponses données par les membres de chaque discipline aux développements de l'environnement externe qu'ils cherchent à expliquer et former. Pour l'autre niveau, l'intérêt dans la collaboration interdisciplinaire peut être compris en termes de dynamique intellectuelle interne à chaque discipline (Slaughter 1998 : 370).

Les facteurs externes sont au nombre de quatre : la convergence de l'objet d'étude, la globalisation des phénomènes, l'accroissement des institutions supranationales et de leur préférence pour la *soft law* et, enfin, la recherche continue de conformité (Slaughter 1998). Mais ce sont les facteurs internes qui nous apparaissent comme les plus pertinents pour justifier l'emploi de cette méthode dans le cadre de cet article. Ainsi, l'on ne peut nier l'apport du droit, des Relations internationales – notamment dans leur volet théorique – et de la sociologie politique dans la compréhension des phénomènes internationaux et des dynamiques à l'œuvre au sein du système international.

Nous entendons à présent définir les variables que nous incluons dans les perspectives culturalistes :

1. La notion de contrainte au sein du système international à l'aune des théories des relations internationales réalistes et néoréalistes.
2. La notion de contrainte au sein du système régional à l'aune de l'apport de la géopolitique et de la géostratégie.
3. Les théories constructivistes permettant de déterminer le rôle structurant de l'État et donc sa place au sein du système auquel il appartient.
4. La sociologie permettant d'éclairer la nature de l'État et donc de ses contraintes nationales.
5. La stratégie permettant de définir la fonction de l'État et donc ses aspirations politiques.

À cette structuration initiale facilitant la lecture de l'« identité stratégique » d'un État prise dans sa dimension classique, il conviendra de joindre les spécificités liées au domaine d'étude qu'est le cyberspace. Nous ne pouvons notamment pas faire l'économie d'inclure la technologie, fondement même de l'espace qui compose notre champ d'études. Cette variable emporte également avec elle la notion de modernité, opposée dans sa définition initiale à la tradition. Nous verrons que, dans la perspective de construction de sa cyberstratégie, l'Arabie saoudite a la particularité de proposer une lecture combinée de ces deux termes. Elle peut de ce fait bâtir une réponse aux menaces cybernétiques en adéquation avec ses valeurs traditionnelles sans renier les apports techniques et sociologiques de la modernité. On notera la nécessaire adaptation des variables contenues dans une lecture stratégique appliquée au cyberspace.

C — La culture stratégique appliquée au cyberspace : modélisation d'une grille d'analyse spécifique

Pour pouvoir utiliser les approches constructivistes et culturalistes au sein du cyberspace, il convient de rappeler la grille d'analyse établie par Nazli Choucri dans son ouvrage *Cyberpolitics in International Relations* (Choucri 2012). Au terme « cyberstratégie » l'auteure a préféré le mot « cyberpolitique », envisagé au sens de son art et de sa pratique au service des intérêts de l'État. Choucri utilise la « théorie des pressions latérales » pour proposer une interprétation des interactions entre les États au sein du système international. À ce postulat initial, elle associe la « théorie du choix rationnel », qui lui permet de présenter le comportement des individus au sein d'un État et d'ainsi proposer une analyse classique de la définition des intérêts que celui-ci poursuit. Cette approche distingue trois « profils types » d'États, selon trois variables : population, ressources, technologie. Ces dernières proposent une interprétation des décisions politiques dans le domaine du cyberspace grâce à des variables sociales et culturelles. La population ne doit pas être restreinte à une conception quantitative, mais plutôt considérée selon une conception où les changements opérés au sein d'un groupe sociétal sont observés sur un temps donné. Les bouleversements ethniques et sociaux sont ainsi pris en compte pour définir le profil de la population. La variable technologique, pour sa part, n'est pas un fondement classique empirique des capacités techniques de l'État ; elle doit intégrer l'ensemble du processus éducationnel que celui-ci possède, permettant ainsi de désigner la sensibilité de l'acteur au domaine du cyberspace. Enfin, notons l'absence de prise en compte des objectifs politiques *stricto sensu* au sein de cette grille, variable à laquelle l'État est préféré en tant que structure.

On observe ainsi l'abandon de l'inclusion des variables d'analyse classiques tirées d'une vision réaliste ou constructiviste du système international. À l'anarchie du système, impliquant la puissance au service de la survie, et au comportement en tant que processus explicatif de la construction étatique, nous privilégierons l'appel

à de nouveaux schèmes pour comprendre et conceptualiser l'impact des menaces de cybersécurité dans la conceptualisation des stratégies étatiques nationales. À domaine inédit, grille d'analyse inédite, à l'image de celle proposée par Choucri.

Tirant les conclusions épistémologiques qui s'imposent, nous entendons produire ici une démonstration en plusieurs strates : le poids grandissant des cybermenaces sur la sécurité des États ; la nature spécifique des réponses stratégiques formulées dans ce domaine ; la viabilité des variables culturalistes dans la compréhension du processus de conceptualisation des doctrines stratégiques des États. Prenant comme cas d'étude l'Arabie saoudite, il convient de rappeler la spécificité du complexe régional auquel celle-ci appartient – le Moyen-Orient –, mais aussi celle du sous-système dont elle relève – le golfe Arabo-Persique. Nous ne pouvons que constater l'existence de contraintes géostratégiques et géopolitiques propres à ces espaces géographiques et en déduire l'apparition d'une nouvelle strate d'analyse, qui ne remet pas en cause les schèmes utilisés, mais apporte une densité aux variables culturalistes employées.

II – Application empirique des variables culturalistes au risque cybernétique au Moyen-Orient : comprendre la conceptualisation de la cyberstratégie saoudienne

A — Modélisation du risque cybernétique dans le cadre du golfe Arabo-Persique

Pour confronter la notion de « culture stratégique » appliquée au golfe Arabo-Persique et les bases de la conceptualisation d'une stratégie nationale, il est essentiel de comprendre les mécanismes de formulation d'une stratégie afin d'en tirer les enseignements nécessaires à son inclusion dans le champ cybernétique. Ce dernier met en œuvre des contraintes particulières, liées à la nature même de cet environnement, mais ne fait pas table rase des postulats théoriques et doctrinaux initiaux. Au-delà de l'expression des intérêts étatiques et des logiques de puissance réalistes, la stratégie relève donc du champ culturaliste. Ce présupposé signifie concrètement la prise en compte des variables relevant de la « culture stratégique ». Cette dernière notion reste à ce jour contestée dans son épistémologie, puisqu'elle suppose l'intégration de nombreuses données, souvent contradictoires, et toujours subjectives. Elle suppose par conséquent des précautions ontologiques dans son maniement.

Pour appliquer les concepts de culture stratégique au sein du sous-complexe régional du golfe Arabo-Persique, il est nécessaire de s'intéresser à la construction des États qui le composent. La construction de la souveraineté et de l'entité administrative des États du Golfe est fondée sur le principe d'expansions territoriales soutenues par des familles régnantes. Les Matareesh et les Khalifa ont dominé le territoire du Bahreïn dès le XVI^e siècle. Le Qatar voit s'affronter quant à lui les familles Al-Khalifa et Al-Tani pour la prise du pouvoir central. Les

Émirats arabes unis, de leur côté, sont composés de six émirats, dont chacun possède sa propre famille régnante. Ils forment une fédération et entretiennent des relations économiques et politiques autour d'une volonté de collaboration et de survie face aux autres États du golfe Arabo-Persique (Cordeman 1997). L'Arabie saoudite, soumise à des contraintes différentes, a quant à elle été marquée par des conflits tribaux plus importants, et a connu plusieurs phases d'expansion territoriale non comparables à celles observées dans les États voisins.

En plus de ce développement étatique propre à la région, ces États ont entretenu de forts liens diplomatiques avec des puissances occidentales et orientales pour de nombreux aspects liés à la défense de leurs intérêts. Cet historique particulier se ressent encore aujourd'hui dans les relations qu'ont ces États avec leurs homologues occidentaux et orientaux, de même que dans la définition de leurs doctrines stratégiques.

Ces dernières ont été influencées par des conceptions théoriques issues des études occidentales. Les États ont ainsi adopté des principes fondateurs qui ne leur appartenaient pas, rendant compte de certaines lacunes dans le milieu scientifique de la région. Le cyberspace, pour les États du Golfe, représente par conséquent un domaine qui ne leur est pas acquis. *De facto*, le processus de réflexion correspond à l'agrégation de postulats, et non à l'établissement d'une grille d'analyse spécifique. Il faut ajouter que les doctrines occidentales, qui se représentent le cyberspace comme un domaine neutre, ne pouvaient faire référence à des logiques culturalistes. Or, il est plus pertinent pour ces États d'inverser cette logique et d'adopter une approche théorique nouvelle. La conceptualisation d'une cyberstratégie dans les pays du golfe Arabo-Persique intègre par conséquent des variables sociales et culturelles. L'influence de la modernité, exercée à travers la technologie numérique dans une société fondamentalement traditionnelle, pose des barrières quant à la capacité des États de se doter d'une stratégie cohérente. La perception qu'ont ces États du cyberspace est d'autant plus problématique que les influences occidentales ne répondent que partiellement aux contraintes auxquelles ils sont soumis empiriquement. Dès lors, pour comprendre les sources de conceptualisation d'une cyberstratégie appliquée à cet espace arabo-musulman stratégique, il faut saisir les enjeux étatiques et les principes de développement de cet espace. Il s'agit de mettre en lumière les variables que l'Arabie saoudite préconise pour efficacement sécuriser son propre cyberspace avant de projeter sa puissance cybernétique.

B — La culture stratégique appliquée à l'Arabie saoudite : réponse opérationnelle au risque cybernétique

Depuis 2007, l'Arabie saoudite a développé un environnement stratégique face aux menaces de cybersécurité, avec l'élaboration du référentiel stratégique

Developing National Information Security Strategy for the Kingdom of Saudi Arabia (NISS) (Ministry of Communications and Information 2011), certes précaire mais néanmoins existant, en formulant des normes nationales capables d'assurer sa sécurité informatique. Pour autant, l'ambivalence qui règne subsiste de façon permanente. En effet, le pays se prévaut d'une volonté «à double hélice». Si, d'un côté, il privilégie le recours à des ressources externes et à des enseignements occidentaux dans la gestion de ses infrastructures, il n'en demeure pas moins que de l'autre il affiche une volonté entière d'affirmer son autonomie dans l'élaboration de stratégies cohérentes avec ses particularismes. Dès lors, il convient de mettre en parallèle les variables favorisant la mise en place d'une culture stratégique efficace en termes de cybersécurité et les choix opérés par l'Arabie saoudite dans la construction de son savoir opérationnel.

Tenant compte des avancées techniques issues des mathématiques et de l'informatique, mais aussi des approches théoriques issues en particulier des études socioconstructivistes, nous entendons modéliser le processus à l'œuvre dans le cadre spécifique de cet État du sous-complexe régional du golfe Arabo-Persique. Nous devons donc nous interroger sur la mise en place des cyberstratégies au Moyen-Orient face à la montée de nouvelles menaces sécuritaires, mais aussi sur l'impact des particularités locales et l'étendue des contraintes géopolitiques et géostratégiques. Il conviendra ainsi de nous demander si cet espace est soumis à des particularismes tels qu'ils supposent un champ de développement inédit en matière de cybersécurité.

Il faut rappeler à ce titre que la conceptualisation de la culture stratégique appliquée au cyberspace est un domaine d'analyse nouveau, sans doute anticipé. Ses bases permettront néanmoins de considérer que les États développant leur potentiel stratégique dans ce domaine prennent conscience de la nécessaire prise en compte des particularités nationales pour adapter leur «réponse cybernétique» aux enjeux politiques et sociétaux auxquels ils sont confrontés.

La prise en compte de variables issues de la culture stratégique suppose une démonstration d'arguments empiriques nécessaires à la compréhension de cet État particulier qu'est l'Arabie saoudite et de son développement stratégique au sein du cyberspace, en plus de s'inspirer de l'histoire de la construction de l'État.

Rappelons que la création du premier royaume saoudien se fait à travers une alliance entre le réformateur Mohammad ibn Adb al-Wahhab et le chef de clan Mohammad ibn Saoud. La construction du second puis du troisième Royaume d'Arabie saoudite revient à la famille Al-Saoud et au clan guerrier des Almohades (*Al-Muwahhidin*). L'expansion territoriale de la famille régnante s'est ainsi établie sur une colonisation des espaces méridionaux, septentrionaux, orientaux et occidentaux à partir du cœur géographique de l'État, le Nadj, au détriment des autres entités étatiques voisines. La culture saoudienne se fonde alors sur deux axes liés. Le premier axe procède de la forte revendication identitaire du peuple saoudien.

Cet « état d'esprit » spécifique est issu de la *perception*² que ce peuple a de lui-même comme centre du monde arabo-musulman et qui le conduit à développer un attachement narcissique à tout ce qui touche à l'État comme entité souveraine. Le second axe fondateur peut être perçu quant à lui comme la cause du premier, puisqu'il s'agit de la forte présence de la religion de l'islam sur le territoire saoudien et de sa *perception* dans le rapport à l'Autre. Non seulement l'État saoudien possède les deux plus importants lieux saints de l'islam, mais la construction de l'État s'est basée sur les principes de la religion islamique.

Les cultures occidentales placent la rationalité en une valeur indispensable, particulièrement depuis l'Âge de la Raison. La culture traditionnelle saoudienne est aussi capable de faire preuve de rationalité, mais du fait de la prédominance de Dieu dans l'Islam, la détermination des effets de causalités peut changer en fonction du contexte et des visions de chacun (Long et Maisel 2010 : 48).

La relation au divin change profondément les interactions au sein de la société, mais aussi avec les sociétés du sous-complexe régional. L'histoire, la culture et la religion constituent par conséquent les premières variables qu'il convient de convoquer dans le processus de compréhension de l'identité saoudienne, en tant que nation mais également en tant qu'acteur au sein du système. Ces premiers éléments contribuent en particulier à mettre en lumière la place du religieux dans la construction sociétale de l'Arabie saoudite, non seulement en termes d'interactions sociales, mais aussi quant aux répercussions matérielles. Dès lors, la conceptualisation d'une stratégie, cette dernière ayant vocation à défendre les intérêts nationaux, suppose nécessairement la prise en compte de cet élément identitaire et notamment religieux, y compris lorsqu'il s'agit de la formulation d'une cyberstratégie.

La linguistique constitue par ailleurs un élément non négligeable de la définition d'une stratégie applicable au cyberspace. Part essentielle de la culture d'une nation, elle doit être intégrée au processus de conceptualisation. Ainsi, dans le cas de l'Arabie saoudite, la langue arabe, à travers notamment des noms de domaines ou des supports numériques, prend une place essentielle dans l'élaboration d'une cyberstratégie cohérente par l'United Nations Economic and

2. Au sens proposé par Jervis (1976). Si cela ne signifie pas que la perception est la seule variable conduisant à l'élaboration de la conduite politique d'un État, il n'en demeure pas moins qu'elle reste un critère d'évaluation essentiel. Ainsi, Jervis considère que l'approche psychologique et sociologique doit être retenue pour compléter le champ d'exploration théorique classique afin de mettre en exergue la complexité des relations internationales. Ainsi, les contraintes psychologiques qui pèsent sur les États – à la fois au niveau de l'entité et des décideurs politiques – doivent être prises en compte dans l'analyse du processus politique. L'auteur considère ainsi que les perceptions et les « méperceptions » (*misperceptions*) sont les images, croyances ou intentions qui influencent les prises de décision, mais aussi les actions des individus et des États.

Social Commission for Western Asia (ESCWA). Il s'agit là d'un aspect purement technique et mathématique de l'informatique et des réseaux, car il dépend d'un outil de programmation. Néanmoins, les enjeux qui sous-tendent cette logique sont non négligeables pour faire valoir des idées. La langue arabe est représentée à hauteur de 3,6 % pour les communications sur Internet (ESCWA 2013). Cependant, si l'arabe est l'une des dix premières langues utilisées sur Internet, cela ne signifie pas pour autant que des contenus numériques intellectuels en langue arabe sont créés et diffusés, ni que des développeurs utilisent cette langue pour programmer des logiciels. Ce dernier point exige des compétences techniques plus abouties, puisque dans le cyberspace la première langue de programmation est l'anglais.

La nécessité pour les développeurs de posséder leurs propres outils de programmation en arabe conduit à proposer un fondement pratique pour la conceptualisation plus aboutie d'un outil informatique. La langue arabe possède des caractéristiques qu'aucune autre langue ne peut reproduire. La volonté internationale de promouvoir une langue sur le cyberspace sert donc les intérêts de l'Arabie saoudite, qui souhaite affirmer sa position de leader technologique dans le sous-complexe régional du golfe Arabo-Persique. Par son développement technologique rapide et ses partenariats avec les entreprises américaines, elle possède un nombre avantageux d'infrastructures – en matière quantitative mais aussi qualitative – pour le traitement des données, et représente ainsi un nœud de transit pour les informations dématérialisées. Les initiatives internationales servent autant les États de la région que les partenaires occidentaux ou asiatiques, puisque l'Arabie saoudite peut s'appuyer sur des expertises techniques et économiques pour les intégrer dans son cheminement intellectuel de conceptualisation d'une stratégie adaptée aux contraintes du cyberspace.

Déjà évoquée précédemment, la religion constitue également un vecteur essentiel de la spécificité stratégique de l'Arabie saoudite, notamment dans son influence sur le développement de ses infrastructures et de son savoir, parfois contraint par un dogme religieux limitant la diffusion de connaissances non conformes.

Les rapports entre technologies de l'information et de la communication, d'une part, et les principes culturels saoudiens, d'autre part, s'inscrivent textuellement dans les documents officiels de l'État. Les rapports institutionnels font pour la plupart référence à des conceptions de la culture pour l'Arabie saoudite. Le centre de recherche King Abdulaziz City for Science and Technology (KACST) exprime dans ses études la relation entre communication et pèlerinage religieux. Cette interdépendance peut paraître non pertinente comme variable analytique ; elle reste pourtant très présente dans les travaux de développement d'infrastructures. Il s'agit par exemple pour le KACST de rendre possible le déploiement du pèlerinage pour Médine et La Mecque avec l'appui des nouvelles technologies.

«Les applications pour le pèlerinage *Hajj* comptent des bases de données, des modèles de simulation, des systèmes d'information géographique, de même que l'application pour l'identification des fréquences radio pour le contrôle de la population» (King Abdulaziz City for Science and Technology 2008). Cette considération est particulièrement importante, car il s'agit de la première preuve d'une occurrence entre religion/culture et informatique. Pour autant, l'analyse informatique d'un pèlerinage s'inscrit dans la prise en compte de particularités locales religieuses, qui seront adaptées au moyen de la technologie. Cette volonté peut passer par la mise en place d'un système de surveillance et de reconnaissance faciale au bénéfice des autorités chargées de la protection et de la sécurité des populations en pèlerinage. Les doctrines stratégiques institutionnelles font rarement l'état des lieux de procédés à développer à destination des civils et de leur attachement à la religion. Il convient donc de voir dans cet exemple une des premières prémisses de la pensée culturelle dans le cyberspace.

Le document stratégique de référence *NISS Draft 7* pour l'État saoudien, bien que prenant parfois ses sources dans des référentiels internationaux, n'omet pas de mentionner quelques références culturelles et religieuses en son sein :

By the will of Allah, the Saudi economy in 2024 will be a more diversified, prosperous, private-sector driven economy, providing rewarding job opportunities, quality education, excellent health care and necessary skills to ensure the well-being of all citizens while safeguarding Islamic values and the Kingdom's cultural heritage (Ministry of Communications and Information Technology 2011).

Ce passage présente un reflet de la vision à long terme que veut proposer l'Arabie saoudite en matière de sécurité et de progrès social. Cependant, la référence à Allah et aux valeurs de l'islam sont bien ancrées dans le processus d'amélioration de l'État saoudien, qui ne peut faire fi de sa culture, de sa religion et de son passé. Cette citation est elle-même reprise d'un document stratégique de développement économique et social à long terme pour 2024. La présence de ce texte dans un document stratégique, non en préambule ou en citation d'introduction, mais dans un chapitre explicite, assure que, même si l'Arabie saoudite accroît sa sécurité en faisant appel à des connaissances occidentales, elle conserve cet aspect unique à un État religieux qui fait référence à ses croyances dans un document national.

Les éléments clés de la stratégie de l'Arabie saoudite en matière de développement de ses infrastructures numériques portent sur la création d'un corpus réglementaire et législatif pour la régulation du cyberspace. Il s'agit essentiellement d'établir des standards pour un développement cohérent des institutions et de la société civile au regard du cyberspace (Ministry of Communications and Information Technology 2011). Les lois qui ont été édictées sur les pratiques

du cyberspace ne doivent pas être envisagées indépendamment les unes des autres, mais doivent être réinterprétées dans leur globalité pour fonder une conceptualisation d'une cyberstratégie. La loi du 27 mars 2007 sur l'« anticybercriminalité » (The Royal Embassy of Saudi Arabia 2010) reste une pierre angulaire dans le déploiement d'une législation ciblée contre les pratiques criminelles et délictuelles au sein du cyberspace. Cette loi, composée de 16 articles, présente les principales définitions des crimes pouvant être perpétrés dans le cyberspace et les sanctions prévues à l'encontre des individus qui en seraient reconnus coupables. L'Arabie saoudite, en pleine phase de conceptualisation stratégique, utilise par conséquent des acquis législatifs pour constituer la base de futurs projets de loi. Ce qui reste pourtant paradoxal, c'est que, si ce corpus légal s'affirme par l'exhaustivité de son article premier (The Royal Embassy of Saudi Arabia 2010) quant à la définition des termes et des expressions liés à la cybercriminalité, les exemples apportés par les articles suivants ont peu ou pas servi d'appui à la compréhension du cyberspace dans les analyses stratégiques et les documents gouvernementaux.

La présentation de principes stratégiques appliqués à l'Arabie saoudite permet désormais de percevoir la « méthode » de conceptualisation de la stratégie nationale en matière de cybersécurité. Cependant, il n'est pas encore possible de donner une réponse culturaliste à des menaces présentes dans le cyberspace.

Outre la nécessité de produire une stratégie opérationnelle qui puisse répondre aux besoins de sécurité de l'Arabie saoudite, les enjeux de sécurité du pays face aux cyberspaces se complexifient avec l'augmentation des menaces réelles et connues. L'attaque des infrastructures de Saudi Aramco en 2012 représente symboliquement la prise de conscience de l'Arabie saoudite face aux menaces du cyberspace : les cyberattaques sont récurrentes et elles ne viennent pas des acteurs traditionnels.

Rappelons d'abord le contexte : Saudi Aramco a été attaqué en 2012 par le *malware* « Shamoon » (Symantec 2012), spécialement développé pour le cyberespionnage et la destruction d'informations. Ce programme malveillant a infecté près de 30 000 disques de stockage présents au sein des infrastructures de Saudi Aramco, rendant la société inopérante pendant deux semaines. Cette attaque, la plus importante connue à ce jour dans le domaine énergétique, a été revendiquée par plusieurs groupes cyberactivistes, dont chacun aurait apporté son expertise dans le développement de ce *malware* : The Arab Youth Group (Pastebin 2012), The Cutting Sword of Justice (Pastebin 2012b) et un troisième groupe présumé sans dénomination (Pastebin 2012c). Dénoncer l'Iran comme auteur de cette attaque serait sous-estimer la complexité des liens entre les groupes cyberactivistes, dont certains sont capables de développer des armes numériques redoutables, et le soutien d'institutions qui fournissent des moyens considérables à ces groupes, sans jamais reconnaître leurs activités ou une quelconque affiliation.

L'analyse de l'écosystème cybercriminel en Arabie saoudite met en évidence de nouvelles menaces transnationales, à l'image des menaces telles que «Shamoon», qui ne correspondent toutefois pas nécessairement aux traditionnels opposants d'un conflit armé. Par exemple, en juin 2014, un programme malveillant financier de type rançongiciel (*ransomware*), «Svpeng»³, a sévi sur les réseaux saoudiens. Ce type de logiciel ne cible pas spécifiquement une institution au regard de son positionnement politique, stratégique, culturel ou religieux ; il s'agit d'une menace nouvelle qui entraîne la collecte des sommes financières importantes, mais qui se coupe d'une revendication politique ou stratégique classique (*Al Arabiya* 2013).

Dans ce contexte, les autorités saoudiennes ont un vif intérêt à protéger leurs patrimoines et leurs intérêts nationaux sur le territoire. Hormis un arsenal législatif existant et opérationnel, l'Arabie saoudite, dès 2008, a mis sur pied un CERT (Computer Emergency Response Team), un organe indispensable dont le rôle est la prévention et l'alerte de menaces existantes sur le cyberspace. De nombreux États européens, des sociétés privées et des centres de recherche possèdent et développent des CERT, favorisant ainsi un niveau de prévention élevé face aux risques et aux menaces. Le CERT saoudien propose une prévention de type «Honeypot», un système qui laisse un accès réseau et un serveur de données moins protégé que le reste des infrastructures pour agir en tant qu'appât et attirer un ensemble d'attaques malveillantes non encore identifiées sur les réseaux. Cette réponse rend compte d'un élément particulier de notre analyse : l'État peut concevoir, de manière consciente ou inconsciente, une stratégie basée sur la culture stratégique, mais le développement de réponses et de capacités opérationnelles ne peut être culturellement orienté, car il dépend de procédés informatiques et mathématiques qui ne sont pas régis par des principes culturels.

À titre d'exemple concret de ce principe, signalons que le CERT d'Arabie saoudite a élaboré en 2011 un cadre réglementaire de développement de politiques de sécurité de l'information pour les agences gouvernementales (CITC 2011). Ce document s'inspire de méthodes et de référentiels, dont :

- US – National Institute of Standards & Technology NIST PUB 80053 Recommended Security Controls for Federal IS
- Germany – Federal Office for Information Security (BSI) Baseline Protection Manual
- ISO/IEC 27001
- Input for selected Government Agencies
- Saudi Laws

3. <http://cert.sa/index.php> (consulté le 1^{er} juillet 2016).

- Transaction Law
- Crimes Law

On a recours à ces documents dans la construction d'un cadre de références et d'inspirations utiles au développement de bonnes pratiques dans une volonté de sécuriser les informations d'agences gouvernementales. Le CERT saoudien n'impose pas de principes culturels ou religieux, mais cherche à maximiser la sécurité d'agences gouvernementales en bénéficiant d'enseignements internationaux.

La culture stratégique révélatrice des failles dans la conceptualisation des doctrines stratégiques civiles et militaires au Moyen-Orient

À l'issue de cette analyse, on ne peut que constater les nombreux paradoxes sur lesquels repose le développement d'une cyberstratégie efficiente en Arabie saoudite. Ainsi, l'État développe une approche intellectuelle qui met l'accent sur ses particularismes, qu'il transpose dans une vision spécifique du cyberspace et de la cybersécurité. Pour autant, ces avancées doivent être relativisées au regard d'une approche empirique paradoxale.

La gestion managériale présente dans les documents institutionnels *NISS* (Ministry of Communications and Information Technology 2011) pour l'Arabie saoudite met en avant une vision occidentalisée de la gestion des procédures techniques, des fonctionnements en ressources humaines et en management de la sécurité.

Ressemblant fortement aux bonnes pratiques que l'on peut trouver dans les référentiels institutionnels de l'Organisation internationale de normalisation, avec comme exemples la certification ISO/IEC 27001 et le code de bonnes pratiques ISO/IEC 27002, la gestion des risques numériques ne peut pas être exclusivement culturocentrée.

Ce phénomène se précise et devient inhérent à la technologie et au développement de capacités en matière de cybersécurité et de cyberdéfense des États. Pour établir un parallèle avec les conflits armés, les stratégies varient en fonction de la culture, mais les armes et les matériels sont plus ou moins identiques en fonction de l'époque et du niveau de développement technologique. La perception est la même avec la cybersécurité. Hormis le langage informatique utilisé sur les réseaux de communication, il n'existe pas de méthode culturelle pour se protéger de conflits numériques, et les technologies sont communes à un ensemble mondial. Une information nuisible circulera de la même manière sur les réseaux de télécommunications, quelles que soient la religion et la culture de l'État : c'est une donnée virtuelle et numérique. Ce point de vue rationalise l'approche culturaliste pour l'Arabie saoudite dans le sens où elle met en lumière un État en accord avec une base historique, culturelle et religieuse, tout en menant des

travaux de plus en plus importants en faveur d'une technologie numérique sous-tendant les questions sécuritaires à l'œuvre au Moyen-Orient.

En conclusion, l'analyse de la conceptualisation de la cyberstratégie saoudienne met en évidence la pertinence des variables culturalistes. En effet, l'acteur étatique ne peut se départir d'un processus doctrinal ancré dans des variables culturelles historiques, et ce, d'autant moins lorsque le facteur religieux a un impact aussi fort dans la pensée stratégique et institutionnelle. On peut ainsi constater la présence des vecteurs culturalistes dans la démarche des gouvernants et dans leur approche de cette nouvelle menace sécuritaire qui pèse sur leurs populations et leurs systèmes. Si cette grille d'analyse théorique aide à comprendre la formalisation intellectuelle et à mettre en évidence les particularismes nationaux, elle n'en demeure pas moins le seul axe d'analyse. Les éléments théoriques opérationnels tendent ainsi à démontrer l'influence des cultures stratégiques extérieures dominantes du système international – et donc occidentales – dans la formalisation d'une culture stratégique appliquée au cyberespace. Ce phénomène est renforcé par la mondialisation des risques numériques et par leur extension à l'ensemble des acteurs du système. Ces derniers doivent faire face aux mêmes risques et ils tentent aujourd'hui d'y répondre, certes en prenant en compte leurs spécificités nationales, mais aussi en recourant aux outils mis à leur disposition, qui viennent pour l'essentiel, encore aujourd'hui, des pays occidentaux. Tant le savoir que les capacités opérationnelles restent majoritairement l'apanage des États les plus avancés en matière cybernétique, les États-Unis et les pays d'Europe pour ne citer qu'eux. Dès lors, si les variables culturalistes favorisent une meilleure compréhension des schèmes à l'œuvre au Moyen-Orient – et notamment en Arabie saoudite –, il n'en demeure pas moins que l'une des contraintes lourdes reste la réalité technique et opérationnelle en matière de cyberstratégie au niveau du système international.

Lucie LE BARREAU

7357 avenue de chateaubriand
Montréal QC, H2R2L7
Canada

lebarreau.lucie@gmail.com

Édouard LONGEON

Siège CGI France,
Immeuble CB16
17 place des Reflets
92097 Paris la Defense Cedex
France

edouard.longeon@cgi.com

Bibliographie

- AL ARABIYA, 2013, «Middle East in Spotlight amid Escalating Cyber Attacks», *Al Arabiya*, le 19 mai. Page consultée sur Internet (english.alarabiya.net/en/business/technology/2013/05/19/Cyber-security-efforts-can-t-keep-up-with-the-attacks.html) le 1^{er} juillet 2016.
- ASSOCIATION FRANÇAISE DE NORMALISATION (AFNOR), 2013, *Code de bonnes pratiques pour le contrôle de la sécurité de l'information*, normes ISO/CEI 27000 – 27001 – 27002.
- BUZAN Barry et Ole WÆVER, 2003, *Regions and Powers. The Structure of International Security*, Cambridge, Cambridge University Press.
- CHOUCRI Nazli, 2012, *Cyberpolitics in International Relations*, Cambridge, MIT Press.
- COHEN Samy, 2005, «Les États face aux nouveaux acteurs», *Politique internationale*, n° 107, printemps.
- COMMUNICATIONS AND INFORMATION TECHNOLOGY COMMISSION (CITC), 2011, *Information Security Policies and Procedures Development Framework for Government Agencies*, Kingdom of Saudi Arabi, CITC, 1432 AH.
- CORDESMAN Anthony H., 1997, *Bahrain, Oman, Qatar, and the UAE. Challenges of Security*, Boulder, CO, Westview Press.
- JERVIS Robert, 1976, *Perceptions and Misperceptions in International Politics*, Princeton, NJ, Princeton University Press.
- KING ABDULAZIZ CITY FOR SCIENCE AND TECHNOLOGY (KACST), 2008, *Strategic Priorities for Information Technology Program*, Ministry of Economy and Planning, Kingdom of Saudi Arabia.
- LACOSTE Yves (dir.), 1994, *Dictionnaire de géopolitique*, Paris, Flammarion.
- LONG David E. et Sebastian MAISEL, 2010, *The Kingdom of Saudi Arabia*, Gainesville, FL, University Press of Florida.
- MACLEOD Alex et Dan O'MEARA, 2010, *Théories des relations internationales. Contestations et résistances*, Montréal, Athéna.
- MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY, 2011, *Developing National Information Security Strategy for the Kingdom of Saudi Arabia*, NISS Draft 7, Kingdom of Saudi Arabia.
- PASTEBIN, 2012, «Arab Youth Groups», *Pastebin*, le 15 août. Page consultée sur Internet (pastebin.com/PUHqDQnd) le 1^{er} juillet 2016.
- PASTEBIN, 2012b, «Untitled», *Pastebin*, le 15 août. Page consultée sur Internet (<http://pastebin.com/HqAgaQRj>) le 1^{er} juillet 2016.
- PASTEBIN, 2012c, «Saudi Aramco, once again», *Pastebin*, le 22 août. Page consultée sur Internet (pastebin.com/WKSk3pmp) le 1^{er} juillet 2016.
- SLAUGHTER Anne-Marie, 1998, «International Law and International Relations Theory. A New Generation of Interdisciplinary Scholarship», *The American Journal of International Law*, vol. 92, n° 3, juillet : 367-397.
- SYMANTEC, 2012, «The Shamoon Attacks», *Symantec Official Blog*, le 16 août. Page consultée sur Internet (www.symantec.com/connect/blogs/shamoon-attacks) le 1^{er} juillet 2016.
- THE ROYAL EMBASSY OF SAUDI ARABIA, 2010, *Anti-Cyber Crime Law*, Washington, DC, USA, 1-3.
- UNITED NATIONS – ECONOMIC AND SOCIAL COMMISSION FOR WESTERN ASIA (ESCWA), 2013, *Outlook of the Information Society in the Arab Region*, New York, United Nations.
- WASINSKI Christophe, 2006b, «La culture stratégique : évaluation d'un concept et de ses ramifications en relations internationales», *Les Cahiers du RMES*, vol. III, n° 1 : 117-141.