UNIVERSITÉ DU QUÉBEC À MONTRÉAL

NAVIGUER EN EAUX TROUBLES : LES RISQUES LIÉS AUX PROJETS NUMÉRIQUES CHINOIS EN MALAISIE

TRAVAIL DE RECHERCHE DIRIGÉ

PRÉSENTÉ

COMME EXIGENCE PARTIELLE

MAÎTRISE EN SCIENCE POLITIQUE (SANS MÉMOIRE)

PAR

GABRIELLE GENDRON

JUIN 2024

UNIVERSITÉ DU QUÉBEC À MONTRÉAL
Service des bibliothèques

Avertissement

La diffusion de ce document diplômant se fait dans le respect des droits de son auteur, qui a signé le formulaire *Autorisation de reproduire et de diffuser un travail de recherche de cycles supérieurs* (SDU-522 – Rév. 04-2020). Cette autorisation stipule que «conformément à l'article 11 du Règlement no 8 des études de cycles supérieurs, [l'auteur] concède à l'Université du Québec à Montréal une licence non exclusive d'utilisation et de publication de la totalité ou d'une partie importante de [son] travail de recherche pour des fins pédagogiques et non commerciales. Plus précisément, [l'auteur] autorise l'Université du Québec à Montréal à reproduire, diffuser, prêter, distribuer ou vendre des copies de [son] travail de recherche à des fins non commerciales sur quelque support que ce soit, y compris l'Internet. Cette licence et cette autorisation n'entraînent pas une renonciation de [la] part [de l'auteur] à [ses] droits moraux ni à [ses] droits de propriété intellectuelle. Sauf entente contraire, [l'auteur] conserve la liberté de diffuser et de commercialiser ou non ce travail dont [il] possède un exemplaire.»

DÉDICACES

Je dédie ce travail et toutes ces années de travail
à mon grand-père Jacques et à ma grand-mère Hélène,
avec qui j'aurais tant aimé célébrer.

REMERCIEMENTS

Je tiens à exprimer ma profonde gratitude envers ma famille, qui a été mon pilier de soutien tout au long de ces années où j'ai dû jongler entre mes études et mon travail. Votre support indéfectible et vos encouragements constants ont été une source d'inspiration inépuisable, me permettant de persévérer et de réussir dans ces deux aspects importants de ma vie. Votre foi en moi et votre amour inconditionnel ont été le carburant qui a alimenté mon parcours académique. Merci du fond du cœur.

Merci aussi à Louis pour tout.

TABLE DES MATIÈRES

RÉSUMÉ

Résumé

Cette recherche approfondie examine la question de la souveraineté numérique dans le contexte des projets numériques chinois en Malaisie, qui suscitent des préoccupations en matière de souveraineté et de cybersécurité. En utilisant un cadre théorique et méthodologique néoréaliste et critique, et en élargissant la notion de sécurité pour inclure des dimensions économiques, politiques, sociétales et numériques, cette étude met en évidence l'importance que la Chine accorde à la cybersécurité pour sa sécurité nationale. Elle considère également la Malaisie comme un partenaire stratégique en raison de son développement économique et de son potentiel dans le secteur numérique.

L'analyse des initiatives numériques, comme le projet *Alibaba Cloud's ET City Brain*, démontre que l'expansion de l'influence chinoise soulève des préoccupations en matière de souveraineté et de cybersécurité. Ce partenariat entre la Chine et la Malaisie suscite des inquiétudes quant à l'exportation du modèle d'autoritarisme numérique chinois et ses implications pour la cybersécurité en Malaisie. En somme, cette recherche met en lumière les défis et les implications de la croissance de l'influence numérique chinoise en Malaisie.

Mots clés : Souveraineté numérique, cybersécurité, Chine, Malaisie, Routes de la soie, autoritarisme numérique, développement numérique

ABSTRACT

Abstract

This in-depth research examines the issue of digital sovereignty in the context of Chinese digital projects in Malaysia, which raise concerns about sovereignty and cybersecurity. Using a neorealist and critical theoretical and methodological framework, and expanding the notion of security to include economic, political, societal, and digital dimensions, this study highlights the importance China places on cybersecurity for its national security. It also considers Malaysia as a strategic partner due to its economic development and potential in the digital sector.

The analysis of digital initiatives, such as the Alibaba Cloud's ET City Brain project, demonstrates that the expansion of Chinese influence raises concerns about sovereignty and cybersecurity. This partnership between China and Malaysia raises concerns about the export of the Chinese model of digital authoritarianism and its implications for cybersecurity in Malaysia. In sum, this research sheds light on the challenges and implications of the growth of Chinese digital influence in Malaysia.

Keyword : Digital Sovereignty, Cybersecurity, China, Malaysia, Silk Roads, Digital Authoritarianism, Digital Development.

CHAPITRE 1

Introduction à l'étude

La grande renaissance de la Chine, si surprenante fût-elle pendant un certain temps, n'étonne désormais plus personne. Les « trente glorieuses » ont été le théâtre de la transformation fulgurante d'une Chine exsangue à la suite de la Révolution culturelle et depuis 2008 sa montée est saisissante. Après ce que Xi Jinping appelle un « siècle d'humiliation », la Chine se positionne en tant que l'une des principales puissances et reprend une place centrale au sein de la politique mondiale. Ce changement se reflète notamment par trois piliers : les dépenses du gouvernement dans ses capacités militaires, son affirmation dans les institutions internationales et le lancement de l'initiative de la *Belt and Road Initiative* (BRI).

Dévoilé à l'automne 2013 par Xi Jinping lors de visites diplomatiques au Kazakhstan et en Indonésie, le projet de la Ceinture et la route qui était présenté comme étant celui du siècle suscita une vague de protestations dans le reste du monde. En effet, il s'inscrivait dans le sillage du rêve chinois. L'initiative déposait les bases d'une politique séculaire visant notamment à donner à la république une place importante sur la scène internationale. D'une ampleur colossale, le projet présentait deux nouvelles initiatives commerciales et de développement pour la Chine, la ceinture économique de la route de la soie et la route de la soie maritime du XXIe siècle. Ce projet dévoilait une vision à long terme pour des projets de développements d'infrastructures de connectivité et de coopération économique de l'Eurasie. Il couvrait en tout six corridors de développement.

Développés de concert avec la Banque asiatique d'investissement dans les infrastructures (AIIB), ces corridors visent à répondre à un excédent de capacité industrielle et de nouveaux

intérêts financiers, tout en illustrant la volonté d'expansion territoriale du capitalisme chinois. Il est projeté que l'Asie nécessitera 26 billions de dollars d'investissements en infrastructures d'ici 2030 (BAD, 2017) pour faire naître son projet. Il est estimé que les bénéfices découlant de ces investissements permettront non seulement à la Chine de développer à long terme des débouchés pour ses produits, mais également de pallier à court terme la surcapacité industrielle.

Selon un rapport de l'*Office of the Leading Group for the Belt and Road Initiative*, l'initiative ne se limite pas qu'à un aspect économique. Elle témoigne aussi d'une volonté de pérenniser la puissance chinoise et de renouer avec le symbolisme historique de l'ancienne Route de la Soie. L'objectif est de maintenir un système économique mondial ouvert, tout en favorisant un développement diversifié, indépendant et durable. Il y a environ 110 projets recensés qui sont directement ou indirectement liés aux nouvelles routes de la Soie ainsi que plus de 66 institutions et mécanismes qui y sont associés. Ces entités comprennent notamment des organismes politiques, des coopérations multilatérales, des institutions de financement, des plateformes, des groupes de réflexion et des entreprises publiques.

En somme, ces projets proposent une vaste gamme d'éléments, incluant des voies ferrées transcontinentales, des installations portuaires, des pipelines d'énergie et des autoroutes. L'importance du projet est notamment soulignée par le fait qu'il concerne potentiellement plus de 60 pays, dont la population combinée dépasse les 4 milliards d'habitants et dont les marchés représentent actuellement environ un tiers du PIB mondial.

Au fil des dernières années, l'aspiration du Parti communiste chinois (PCC) à s'affirmer dans le domaine numérique est devenue un phénomène complexe qui nécessite une analyse approfondie de ses récentes initiatives numériques. Il a été démontré que la souveraineté numérique

occupe une place centrale dans la vision chinoise de la gouvernance mondiale du cyberespace. La Chine reconnaît effectivement que le rôle et les capacités d'un pays dans cette gouvernance dépendent de son développement national et de sa puissance technologique. Ces capacités constituent les fondements de ce que la Chine considère comme étant le pouvoir dans les discussions sur la gouvernance mondiale de l'Internet[1], c'est ce type de puissance qu'elle s'efforce d'acquérir depuis quelques années.

En effet, selon l'*International Institute for Strategic Studies*, le ministère chinois de la Sécurité d'État est devenu un acteur extrêmement compétent dans le domaine du cyberespace. Il démontre un niveau d'innovation et de sécurité opérationnelle croissant et mène une campagne mondiale de cyberespionnage à des fins économiques, politiques et stratégiques. Cette montée en compétences et capacités en matière de cyberdéfense s'opère notamment à travers le développement d'initiatives numériques dans les pays participants au projet chinois de la *Belt and Road Initiative* (BRI).

En effet, en tant que deuxième économie numérique la plus importante au monde, avec le plus grand nombre d'utilisateurs Internet ainsi que le plus grand volume de ventes en ligne, la Chine développe désormais des projets visant à la positionner en tête du développement des technologies numériques. Les nombreuses initiatives présentées par le volet numérique de la Route de la Soie témoignent ainsi d'une volonté de poursuivre un développement axé sur l'économie

[1] Cuihong, C. (2018). China and global cyber governance: main principles and debates. *Asian Perspective, 42*(4), 650.

numérique, l'intelligence artificielle, les nanotechnologies, l'informatique quantique, le développement de mégadonnées, l'infonuagique et le développement de villes intelligentes[2].

L'affirmation récente du Parti communiste chinois (PCC) dans l'espace numérique suscite des inquiétudes non seulement de la part des autres puissances mondiales, mais aussi des pays bénéficiaires de ces projets numériques. En effet, la Chine a été un acteur majeur dans la vente et l'exportation de technologies de l'information depuis une dizaine d'années, ce qui lui a permis de générer de nouvelles sources de revenus et de données, ainsi que de renforcer sa position stratégique face à l'Occident. L'enjeu ici est que ce volet numérique de la BRI semble présenter des risques en termes de cybersécurité et de souveraineté numérique. Il semble en effet que la Chine exporte à travers celui-ci son modèle de censure et de surveillance, ce qui pourrait être interprété comme une exportation d'autoritarisme numérique, notamment dans le cadre de son partenariat numérique avec la Malaisie.

1.1 Problématisation de la recherche

À la lumière des recherches effectuées, de la définition du sujet et de sa pertinence pour la discipline, il apparaît que la plupart des approches analytiques visant à analyser la « menace » numérique chinoise, et plus spécifiquement son impact en Asie du Sud-Est, présentent certaines lacunes. En outre, il est important de souligner que l'actuelle vision de la « menace chinoise » est principalement construite à partir de la lecture néoréaliste et de celle de l'économie politique internationale. Toutefois, simplement inclure ces approches dans l'analyse serait réducteur et ne rendrait pas compte de manière adéquate des événements. Pour tenter de combler ces lacunes, ce

[2] Shi-Kupfer, K., & Ohlberg, M. (2019). China's digital rise : Challenges for Europe. *Merics papers on China, 7*, 8.

travail aura une approche hybride de l'enjeu, pour tenter de rendre compte de la complexité du phénomène étudié.

De plus, ce travail se positionnera en considérant que le cyberespace est opaque, ce qui permet d'appliquer la notion de territorialisation ainsi que le concept de souveraineté numérique, concept qui se rapproche du modèle chinois. En réponse aux enjeux de la littérature actuelle qui analysent les politiques chinoises dans le domaine de la souveraineté numérique avec une tendance « occidentaliste », ce travail optera pour une lecture hybride du concept, s'inspirant à la fois du concept de Pierre Bellanger et du modèle chinois de souveraineté numérique[34].

Face à cette problématique, cet essai posera la question de recherche suivante : quels sont les impacts du volet numérique des nouvelles routes de la soie sur la souveraineté numérique et la cybersécurité de la Malaisie ?

Cet essai défendra l'idée selon laquelle l'influence croissante de la Chine en Malaisie et dans la région de l'Asie du Sud-Est s'effectue au profit de l'exportation de la puissance chinoise à différents niveaux : économique, numérique, politique et sécuritaire. En d'autres termes, cet essai propose que, matérialisé par les deux projets phares de ce partenariat, le volet numérique des nouvelles Routes de la Soie représente une forte ingérence dans la souveraineté numérique malaisienne, tout en constituant une menace pour la cybersécurité et la confidentialité des données. Les manœuvres du gouvernement chinois inscrivent ainsi le Parti communiste et l'État chinois au

[3] Creemers, R. (2020). China's conception of cyber sovereignty. *Governing cyberspace: Behavior, power and diplomacy*, 110.

[4] Lindsay, J. R., Cheung, T. M., & Reveron, D. S. (2015). *China and cybersecurity: Espionage, strategy, and politics in the digital domain*. Oxford University Press, USA, 113.

sein des sociétés bénéficiaires de ces initiatives. Ce dispositif constitue donc également, à bien des égards, un moyen pour la Chine d'avancer ses objectifs en matière de cyberdéfense.

Finalement, cet essai défend l'idée que l'objectif à long terme de la Chine est de transformer le paysage mondial de la concurrence technologique en définissant et en exportant ses propres normes pour toutes les industries numériques émergentes. Ce processus vise à garantir que les produits et services chinois ne sont pas entravés par les normes établies par d'autres pays. Le renforcement des compétences et des capacités en matière de pouvoir et de souveraineté numérique qui s'effectue par le biais du développement et de la mise en œuvre d'initiatives numériques dans les pays participants à l'initiative chinoise *Belt and Road Initiative* (BRI) pourrait éventuellement conduire à une hégémonie numérique régionale en Asie du Sud-Est.

CHAPITRE 2

Analyse approfondie des approches théoriques pertinentes au sujet

La place de la Chine dans le domaine des relations internationales a considérablement évolué au fil du temps. Autrefois considérée comme une puissance de moindre importance, la Chine semble désormais occuper une position centrale sur la scène internationale. Les premières tentatives de conceptualisation de la Chine dans le contexte des relations internationales ont émergé après la guerre froide. Avec le recul, il est devenu évident que ces théories post-guerre froide étaient largement influencées par l'étude des grandes puissances de l'époque.

Avant cette période, d'autres régions du monde ont été souvent analysées uniquement en fonction de leur relation avec les grandes puissances. Par exemple, après la guerre froide, l'expérience européenne a été projetée sur l'Asie, alimentant des préoccupations quant à une possible course aux armements et une dynamique de politique de puissance dans la région. Cette projection était en grande partie influencée par le concept d'Ernst B. Hass, qui envisageait un avenir où les États asiatiques se livreraient à une dynamique d'équilibre des puissances, justifiée par la recherche de survie à tout prix, une perspective souvent associée aux conflits[5]. L'Asie était perçue comme un terrain propice aux rivalités, en raison des disparités économiques et militaires entre les États de la région après la guerre froide[6]. Cependant, malgré les prédictions selon lesquelles les États asiatiques s'opposeraient à la Chine, prédictions basées sur les postulats précédemment

[5] Haas, E. B. (1953). The balance of power: prescription, concept, or propaganda? *World Politics, 5*(4), 444.
[6] Kang, D. C. (2003). Getting Asia Wrong: The Need for New Analytical Frameworks. *International Security, 27*(4), 60. http://www.jstor.org/stable/4137604

mentionnés, l'Asie semble aujourd'hui plutôt suivre une tendance de *bandwagoning*, où certains États cherchent désormais à s'allier avec la Chine pour assurer leur sécurité.

Dans ces mêmes années, on vit apparaître la théorie de la « menace chinoise » qui devint un concept clé pour définir la Chine tant dans le contexte des relations internationales que pour un public plus large. Selon le chercheur Khalid R. Al-Rodhan, cette théorie repose sur des projections linéaires et des analogies historiques imparfaites, ce qui la rend conceptuellement fallacieuse. La théorie de la « menace chinoise, » notamment formulée par Robert Kagan, décrit l'ascension de la Chine comme un vecteur conduisant à un conflit violent, il se basait notamment sur des exemples historiques de puissances montantes occidentales[7]. Cette théorie reposait donc sur les notions de politique, de puissance, de capacités, et sur des suppositions quant aux intentions de la Chine. Pourtant, la théorie de la « menace chinoise » a largement influencé le discours américain, et ce malgré les avertissements de théoriciens tels que Joseph Nye qui évoquait le risque d'autoréalisation d'une telle prophétie[8].

Enfin, les approches néoréalistes et les approches critiques de la sécurité, majoritairement cadrées sur les travaux de Kenneth Waltz, d'A.F.K. Organski et de Thierry de Balzacq, sont les trois approches préconisées pour cet essai. Ces approches ont été choisies puisque les auteurs font preuve d'une excellente qualité d'analyse et ont contribué à l'élaboration de concepts et de théories qui s'applique à la complexité de la question de recherche. Cette étude s'articule aussi autour de certains concepts chinois, notamment les visions chinoises de la souveraineté numérique et

[7] Kagan, R. (2005). « The Illusion of 'Managing' China, » Washington Post.
[8] Nye, J. (2006). "The Challenge of China," in Stephen Van Evera, ed., How to Make America Safe: New Policies for National Security (Cambridge, Mass.: Tobin Project, 2006), 74.

cyberespace qui sont devenues les pierres angulaires du discours chinois au sein de la gouvernance mondiale du cyberespace[9].

2.1 Les approches néoréalistes en relations internationales

L'approche néoréaliste est une des approches dominantes dans l'étude des relations internationales et celle qui a dominé au lendemain de la Guerre froide dans l'étude de la montée en puissance de la Chine. Le néoréalisme s'inscrit dans la continuité du réalisme classique, mais en mettant davantage l'accent sur la notion de structure, de politique, de puissance et du comportement des États. Ainsi, pour les néoréalistes, le résultat des actions des États dans le système international est distinct de leurs intentions en tant que telles[10]. Ainsi, la notion de structure est la variable indépendante qui explique le comportement des États. Pour les néoréalistes cette structure est l'anarchie, contrairement aux réalistes qui conçoivent l'anarchie comme une simple composante du système international. Les tenants de cette approche affirment que le réalisme est une théorie considérée comme générale tandis que le néoréalisme examine plus en détail le pouvoir dans le système international.

Une des grandes différences entre le réalisme et le néoréalisme est que pour le second, la théorie se concentre sur les capacités tandis que le réalisme explore les États et le système international. Le concept de capacité est particulièrement pertinent dans le cadre de cet essai. Dans l'ouvrage *Theory of International politics*, Waltz stipule que l'utilisation de la puissance se rapporte à appliquer ses capacités dans une tentative de modifier le comportement d'un autre État de

[9] Creemers, R. (2020). China's conception of cyber sovereignty. *Governing cyberspace: Behavior, power and diplomacy*, 107-145.
[10] Waltz, K. N. (1979). *Theory of international politics*. Addison-Wesley Pub. Co.

certaines manières[11]. En ce sens, la répartition des capacités matérielles est ce qui différencie les États des autres. Cette même notion s'applique justement dans le cadre de cet essai, du fait que la Chine développe des capacités technologiques et numériques en Asie du Sud-Est qui affectent sa relation avec les autres États, mais qui affectent aussi l'équilibre des puissances dans la région. L'équilibre des puissances ou la balance des forces se résume à l'impératif suivant : qu'aucun État ne l'emporte en puissance sur la somme des États voisins au sein d'une coalition ; la puissance d'un seul État jamais ne doit excéder celle des autres réunis[12]. Ainsi, dans cette logique d'idée, il est attendu d'un État qu'il ait une politique étrangère et un comportement interne caractérisé par la prudence, la consolidation d'alliances, et des relations bilatérales basées sur les intérêts[13].

Or si Waltz fait valoir les capacités de chaque État, elles déterminent par le fait même si un État est en sécurité dans la mesure ou le suivant le perçoit comme une menace. Cela revient au postulat que l'objectif de tout État est la survie[14]. Dans cette recherche de survie, un État accroît l'insécurité de ses voisins, ce qui peut amener la notion de dilemme de sécurité. Ainsi, cette logique sous-tend que les États sont en perpétuelle insécurité et souhaitent systématiquement acquérir de nouvelles capacités de défenses. Dans le cadre de cet essai, ce genre de comportement est facilement observable, du fait que la Chine qui mène des efforts de développement technologique et numérique engendre des questionnements et des représailles concernant les capacités accrues qu'elle dispose dans le domaine.

[11] Waltz, K. N. (1979). *Theory of international politics*. Addison-Wesley Pub. Co.
[12] Waltz, K. N. (1979). *Theory of international politics*. Addison-Wesley Pub. Co, 117.
[13] Waltz, K. N. (1979). *Theory of international politics*. Addison-Wesley Pub. Co, 120.
[14] Waltz, K. N. (1979). *Theory of international politics*. Addison-Wesley Pub. Co, 131.

De plus, pour les néoréalistes, les capacités permettent aux États d'assurer leur survie. Il y a cinq critères particulièrement étudiés en lien avec la notion de capacités qui sont : (1) la dotation en ressources naturelles, (2) la capacité démographique, (3) la capacité économique, (4) la capacité militaire et (5) la capacité technologique. Cela fait aussi référence à la théorie des gains relatifs, qui chez les néoréalistes entraîne un esprit de concurrence qui rend alors la coopération plus difficile[15].

Pour pousser un peu la réflexion, le dilemme de sécurité et la théorie des gains relatifs soulèvent d'autre questionnement sur le jeu des alliances qui repose sur une double logique de « l'appartenance et de l'inclusion ». Waltz dénote deux types d'alliance ou d'appartenance à un bloc : un État peut décider de rejoindre le bloc dominant pour s'assurer de sa sécurité (*bandwagoning*), ou bien s'allier à une coalition pour contrebalancer l'État le plus puissant (*balancing*).

Le concept de *bandwagoning* est particulièrement intéressant, Kenneth Waltz le théorise comme étant la dynamique d'un État ou un groupe d'États qui, dans l'optique d'assurer leur sécurité, vont s'allier avec un État (ou groupe) plus puissant[16]. Une deuxième définition est pertinente pour cet essai, celle théorisée par Randall L. Schweller qui soutient que les États ont tendance à faire du *bandwagoning* dans l'espoir de réaliser des gains[17]. En effet, dans la pratique, selon Schweller, les États ont des raisons très différentes de choisir l'équilibrage ou le *bandwagoning*. L'objectif de l'équilibrage est l'autopréservation et la protection des valeurs déjà

[15] Mearsheimer, J. J., & Alterman, G. (2001). *The tragedy of great power politics*. WW Norton & Company, 40.
[16] Waltz, K. N. (1979). *Theory of international politics*. Addison-Wesley Pub. Co, 126.

[17] Schweller, R. L. (1994). Bandwagoning for Profit : Bringing the Revisionist State Back In. *International Security, 19*(1), 74. https://doi.org/10.2307/2539149

possédées, tandis que le but du *bandwagoning* est généralement la recherche de quelque chose qui représente une nécessité, par exemple, d'obtenir des valeurs convoitées. En d'autres termes, l'équilibrage est motivé par le désir d'éviter les pertes, tandis que le *bandwagoning* est motivé par l'opportunité d'un gain[18].

Or, Schweller amène un autre point de vue du concept qui semble plus pertinent pour cet essai, celui de *jackal bandwagoning* dont le but primaire est le profit. Plus précisément, les États révisionnistes adhèrent au *bandwagoning* pour partager le butin de la victoire. Puisque les puissances révisionnistes aux visées illimitées ne peuvent pas faire partie d'un groupe (elles sont le groupe), le groupe offensif est fait exclusivement par des agresseurs de moindre importance, qui se nomme des états révisionnistes aux visées limitées. Outre le désir d'acquérir un profit quelconque, la motivation du *jackal bandwagoning* peut également être de garantir sa sécurité face à l'État révisionniste[19]. Schweller explique que les *jackals* sont des États qui sont prêts à payer des coûts élevés pour défendre leurs possessions, mais des coûts encore plus élevés pour étendre leurs bénéfices. Les *jackals* sont donc des puissances insatisfaites, mais qui accordent de la valeur à leurs possessions et, en tant qu'expansionnistes, ont tendance à être averses au risque et opportunistes[20].

[18] Schweller, R. L. (1994). Bandwagoning for Profit : Bringing the Revisionist State Back In. *International Security, 19*(1), 74. https://doi.org/10.2307/2539149.
[19] Schweller, R. L. (1994). Bandwagoning for Profit : Bringing the Revisionist State Back In. *International Security, 19*(1), 93. https://doi.org/10.2307/2539149
[20] Schweller, R. L. (1994). Bandwagoning for Profit : Bringing the Revisionist State Back In. *International Security, 19*(1), 103. https://doi.org/10.2307/2539149

2.2 Théorie de la transition de la puissance

Une théorie pertinente dans le cadre de cet essai est celle qui est née des travaux du réaliste A. F. K. Organski. Il est à l'origine de la théorie sur la transition de la puissance, bien que provenant de l'école réaliste des relations internationales. Le modèle de la transition de la puissance se structure autour du rejet de trois postulats fondamentaux des théories réalistes.

Premièrement, le modèle considère que l'ordre international n'est pas du tout anarchique, mais qu'il est organisé hiérarchiquement d'une manière similaire au système politique national. Deuxièmement, le modèle conçoit les règles régissant le système politique national et international comme fondamentalement similaires. Les nations, comme les groupes politiques dans le système national, sont en constante compétition pour l'obtention de ressources. Troisièmement, la transition de la puissance conçoit la compétition internationale comme étant motivée par les gains nets potentiels qui pourraient résulter d'un conflit ou d'une coopération[21]. Ces trois postulats offrent une compréhension de l'ordre international bien différente des réalistes. La théorie d'Organski repose sur deux postulats fondamentaux, la puissance d'un État provient de son développement interne et comme le développement se fait à un rythme différent, les nations s'élèvent et chutent les unes par rapport aux autres[22].

De plus, Organski propose un point intéressant dans sa théorie de la transition de la puissance, c'est-à-dire que l'industrialisation et la modernisation politique apportent l'accroissement du pouvoir pour une nation. Selon cet énoncé, une nation qui s'industrialise passerait alors par une transition au cours de laquelle elle évolue d'un stade de pouvoir faible à un

[21] Kugler, J. J., & Organski, A. (2011). CHAPTER 7 The Power Transition: A Retrospective and Prospective Evaluation. *Handbook of War Studies*, 172.
[22] Kugler, J., Organski, A., & Midlarsky, M. I. (1989). Handbook of War Studies. In: Unwin Hyman, 339.

stade de pouvoir accru. Or, Organski amène un point particulièrement pertinent quant à la notion de pouvoir qu'il qualifie comme étant relative et non absolue. En effet, ce n'est pas une caractéristique de la nation, mais plutôt une caractéristique de sa relation avec les autres nations[23].

La perception de la hiérarchie qu'offre la théorie de la transition de la puissance donnait déjà un indice en 1989 quant à la position de la Chine au sein de l'ordre international. En effet, selon Organski et Kugler, la paix est assurée dans l'ordre international par la nation dominante avec le soutien des grandes puissances qui sont satisfaites de la répartition des avantages et des règles qui la régissent[24]. Or, les auteurs mentionnent la présence de nations insatisfaites qui sont nommées comme des *challengers,* ce sont les grandes nations qui ont accru leur puissance après l'imposition de l'ordre international existant. En 1989, Organski et Kugler considéraient que l'Union soviétique et la Chine étaient des *challengers* potentiels, mais qu'ils étaient trop en concurrence directe et trop faible par rapport aux États-Unis pour être réellement dommageable[25]. En effet, selon Organski, la probabilité qu'une guerre éclate entre deux grandes puissances, une dominante et l'autre montante, est particulièrement élevée lorsque trois conditions sont réunies : le système international doit connaître des transformations importantes dans la répartition de la puissance ; l'État montant doit atteindre, ou s'approcher de la parité avec l'État dominant, sur le plan de la puissance ; l'État montant doit être insatisfait de l'ordre international imposé par le second, c'est-à-dire qu'il n'accepte plus le statu quo international[26].

[23] Kugler, J., Organski, A., & Midlarsky, M. I. (1989). Handbook of War Studies. In: Unwin Hyman, 359.
[24] Kugler, J. J., & Organski, A. (2011). CHAPTER 7 The Power Transition: A Retrospective and Prospective Evaluation. *Handbook of War Studies*, 173.
[25] Kugler, J., Organski, A., & Midlarsky, M. I. (1989). Handbook of War Studies. In: Unwin Hyman, 359.
[26] Organski, A. F. (1968). World politics. *(No Title)*.

2.3 Approches critiques de la sécurité internationale

Bien que la théorie néoréaliste soit centrale pour cette étude, cet essai soutient aussi que la sécurité doit être étudiée sous d'autres spectres que celui des facteurs militaires. En effet, cet essai s'appuie sur les approches critiques de la sécurité qui permettent l'ajout des dimensions économiques, politiques, sociétales et numériques. Dans cette optique, la théorie de Barry Buzan, Ole Waever et Jaap de Wilde se veut une bonne introduction aux études de sécurité.

Dans leur ouvrage *Security : A new framework for analysis*, les auteurs rejettent de prime abord les arguments des traditionalistes qui, comment mentionné plus haut, se limitent à la sécurité[27]. Ils s'opposent *de facto* à l'idée que le cœur des études de sécurité soit l'usage de la force et qu'un enjeu international trouve sa pertinence dans la guerre. La sécurité est donc ici un concept particulier qui est applicable à un large éventail de questions et qui ne doit pas simplement s'en tenir aux affaires militaires. En effet, les menaces et les vulnérabilités peuvent surgir au travers d'une variété de domaines qu'ils soient militaires et non militaires. Le postulat central des études critiques de la sécurité est donc de rejeter la conception stratocentrée de la sécurité pour élargir le concept.

2.3.1 Concept de la sécurisation

Un concept particulièrement pertinent a émergé des études critiques de la sécurité, notamment pour tenter de combler la question concernant la provenance des menaces et des vulnérabilités hors du domaine militaire. Par conséquent, pour que ces menaces considérées comme non traditionnelles soient perçues comme des questions de sécurités, elles doivent être mises en

[27] Buzan, B., Wæver, O., Wæver, O., & De Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers, 5.

scène par un acteur sécuritaire, comme représentant des menaces existentielles pour un objet de référent. Ce processus de sécurisation permet de générer la mise en place de mesures d'urgence comme celles découlant des études traditionnelles de sécurité[28].

La sécurisation permet ainsi un cadre d'analyse plus large qui offre une vision radicale des études de sécurité, justement par l'exploration de menaces considérées comme non traditionnelles. En effet, le concept de sécurisation se constitue par l'établissement intersubjectif d'une menace dite existentielle dont l'importance est suffisante pour avoir des effets politiques substantiels[29]. Ainsi l'analyse de discours est un exemple intéressant pour illustrer la théorie de la sécurisation, si un discours n'est pas traditionnellement perçu comme une menace, c'est le processus de sécurisation qui en découle et dans lequel le discours est instrumentalisé qui en fait une menace sécuritaire.

L'école de Copenhague considère que le processus de sécurisation comprend cinq étapes : la désignation d'un « objet de référent » à sécuriser ; la définition subjective d'une menace à la survie d'un État grâce à une rhétorique de mise en péril ; l'accomplissement de la sécurisation par une personne ou un groupe de personnes dont on reconnaît l'autorité de sécuriser ; la prise de mesures d'exception pour contrer la nouvelle menace et, finalement, l'acceptation de cette réalité par l'ensemble de la collectivité ou par un groupe particulier d'individus[30]. Sur la scène internationale, la sécurisation se concrétise notamment par la représentation d'un enjeu comme urgent et existentiel, ayant tant d'importance qu'il ne devrait pas être exposé au marchandage

[28] Buzan, B., Wæver, O., Wæver, O., & De Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers, 5.
[29] Buzan, B., Wæver, O., Wæver, O., & De Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers, 25.
[30] Buzan, B., Wæver, O., Wæver, O., & De Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers, 23-36.

normal de la politique, mais devrait être traité de manière décisive par les hauts dirigeants avant les autres questions[31]. Barry Buzan, Ole Weaver et Jaap de Wilde présentent ainsi trois conditions facilitantes pour réussir la sécurisation d'un enjeu : (1) l'exigence de suivre la grammaire de la sécurité, (2) les conditions sociales concernant la position d'autorité de l'acteur de sécurisation — c'est-à-dire la relation entre l'orateur et le public et donc la probabilité que le public accepte les affirmations faites et (3) les caractéristiques des menaces présumées qui facilitent ou entravent la sécurisation[32].

Le politologue Thierry Balzacq de l'école de Paris a lui aussi théorisé le processus de sécurisation. Balzacq considère la sécurisation comme :

> Un assemblage articulé de pratiques à travers lesquelles des artéfacts heuristiques (métaphores, instruments politiques, répertoires d'images, analogies, stéréotypes, émotions, etc.) sont contextuellement mobilisés par un acteur en position d'autorité qui incite l'audience à construire un réseau cohérent d'implications (sensations, pensées et intuitions), à propos de la vulnérabilité critique d'un objet de référence, lequel s'ajuste aux raisons de choix et d'actions de l'acteur, en investissant le sujet de référence d'une aura menaçante, à un point tel qu'une politique ciblée va immédiatement être adoptée pour le bloquer[33]. (Balzacq, 2016)

Balzacq démontre ainsi l'importance des outils utilisés pour modifier la portée et la nature d'une sécurisation, ces instruments façonnent donc les menaces, parce qu'ils incarnent une image très spécifique de la menace[34].

---

[31] Buzan, B., Wæver, O., Wæver, O., & De Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers, 26.

[32] Buzan, B., Wæver, O., Wæver, O., & De Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers, 33.

[33] Balzacq, T. (2016). *Théories de la sécurité*. Presses de Sciences Po. https://doi.org/10.3917/scpo.balza.2016.01,194.

[34] Balzacq, T. (2007). The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies*. *JCMS: Journal of Common Market Studies, 46*(1), 75-100. https://doi.org/10.1111/j.1468-5965.2007.00768.x, 79.

Nous allons adapter la vision de l'acte pragmatique et de la politique du risque, telle que décrite par Balzacq, qui appelle à une action pour protéger un objet de référence contre une menace. Cette adaptation sera intégrée à notre question de recherche, où nous analyserons comment est désignée la « menace » numérique que la Chine impose en Asie du Sud-Est.

2.4 Postulats de bases des concepts chinois

Comme il a été mentionné plus haut, pour cette étude, il est important de prendre en compte les postulats chinois. En effet, ils jouent un rôle assez essentiel en fournissant des informations cruciales sur les motivations et les priorités de la Chine en matière de politique étrangère. La conception chinoise des concepts fondamentaux tels que la souveraineté, la stabilité, la coopération internationale, et d'autres éléments clés est impérative pour déchiffrer la logique qui sous-tend les politiques et les réactions de la Chine face aux événements internationaux. De plus, ces postulats offrent un aperçu des valeurs et des principes qui guident la diplomatie chinoise, contribuant ainsi à une analyse plus approfondie des politiques étrangères chinoises et de leurs implications pour la scène mondiale.

Les postulats de base des concepts chinois en relations internationales se distinguent notablement des postulats occidentaux. Contrairement aux conceptions occidentales, qui insistent sur la promotion de la démocratie et des droits de l'homme, la Chine met en avant le principe de stabilité, préférant souvent des relations pragmatiques avec des régimes plus autoritaires[35]. Quant

[35] Cuihong, C. (2018). China and global cyber governance: main principles and debates. *Asian Perspective*, *42*(4), 648.

à lui, le concept chinois de *win-win* (gagnant-gagnant) se concentre sur la coopération mutuellement bénéfique plutôt que sur la compétition[36].

Pour une mise en contexte plus approfondie du sujet de cette recherche, il est essentiel de prendre en considération les concepts de « souveraineté numérique » et de « cyberespace chinois, » qui occupent une place centrale dans la perspective chinoise des relations internationales, notamment à travers les initiatives numériques associées aux projets du volet numérique des Routes de la Soie. Il convient de noter que ces notions reposent sur des postulats distincts de ceux découlant des théories occidentales. Ces divergences fondamentales soulignent la nécessité impérieuse de comprendre en profondeur les postulats chinois pour mener une analyse plus nuancée des dynamiques mondiales.

2.4.1 Modèle chinois de la souveraineté numérique

Le concept de souveraineté numérique a été popularisé par Pierre Bellanger au début des années 2010, et appelait à une alliance entre les nations européennes pour contrer la domination des États-Unis en matière numérique. L'expression désigne l'application des principes de souveraineté au domaine des technologies de l'information et de la communication[37]. Si le concept est peu employé par les démocraties qui préfèrent l'expression « autonomie stratégique numérique », il trouve sa popularité en Chine et en Russie pour justifier des politiques visant à encourager le développement d'une industrie nationale, mais aussi comme levier pour limiter la liberté d'expression en ligne[38]. Selon Alix Desforges, cet emploi du terme pour traiter des questions

[36] Yi, W. (2015). Toward a new type of international relations of win-win cooperation. *China Int'l Stud., 52*, 7.
[37] Bellanger, P. (2012). De la souveraineté numérique. *Le Débat, n° 170* (3), 149-159. https://doi.org/10.3917/deba.170.0149

[38] Danet, D., & Desforges, A. (2020). Souveraineté numérique et autonomie stratégique en Europe : du concept aux réalités géopolitiques. *Hérodote, N° 177-178* (2), 179-195. https://doi.org/10.3917/her.177.0179, 180.

stratégiques prend son sens du fait que le concept est basé sur la représentation par les acteurs politiques d'une perte de souveraineté de l'État dans l'espace numérique et d'une volonté de réappropriation du cyberespace qui est perçu comme un territoire à conquérir[39]. La révolution numérique vient ainsi bouleverser l'exercice de la souveraineté des États puisqu'elle permet des activités transfrontières et qu'elle offre la possibilité de réaliser des actions à distance sur des réseaux d'autrui.

Or, si le concept est assez récent, la Chine a édifié un principe de souveraineté numérique qui est devenu la pierre angulaire de sa position dans la gouvernance mondiale de l'Internet, c'est d'ailleurs une des lignes directrices de ses politiques numériques nationales. En effet, la souveraineté numérique chinoise s'applique à la fois au niveau domestique, mais aussi pour appuyer son agenda de politique étrangère. Le postulat chinois de la souveraineté numérique au niveau domestique est majoritairement défensif, il sert à protéger l'intégrité politique, sociale et économique de la Chine contre les tentatives de subversion des gouvernements étrangers. Cela s'exprime notamment par la mise en place du système très restrictif du Grand Pare-feu de Chine qui en plus de régir l'accès des citoyens à Internet est aussi un puissant outil de surveillance et de censure pour le ministère de la Sécurité publique de la République populaire de Chine.

Sur la scène internationale, son instrumentalisation permet à la Chine de s'éloigner d'une architecture de gouvernance caractérisée par des normes fortes et des institutions internationales puissantes qui sont en place dans l'optique de favoriser un système westphalien basé sur l'autodétermination nationale et le principe de non-ingérence[40]. En considérant la position de la

[39] Danet, D., & Desforges, A. (2020). Souveraineté numérique et autonomie stratégique en Europe : du concept aux réalités géopolitiques. *Hérodote, N° 177-178* (2), 179-195. https://doi.org/10.3917/her.177.0179, 180.

[40] Creemers, R. (2020). Comment la Chine projette de devenir une cyber-puissance. *Hérodote, N° 177-178* (2), 297 - 311. https://doi.org/10.3917/her.177.0297, 13.

Chine dans le monde numérique actuel, sa propre interprétation de la souveraineté numérique représente donc un enjeu pour l'ordre numérique mondiale. Exclure cette vision de l'analyse serait donc réducteur et ne permettrait pas de comprendre les subtilités associées à la diplomatie numérique chinoise.

2.4.2 Vision chinoise du cyberespace

Le concept de cyberespace est un élément central de cette analyse. Le cyberespace a été de prime abord abordé comme étant un espace sans frontières, sans cadres physiques ni juridiques[41]. Toutefois, l'émergence assez récente des grandes puissances au sein de celui-ci est venue bousculer les notions préétablies, notamment en raison de la nécessité de réglementer ce nouvel espace informel. Le géopolitologue Olivier Kempf soutient que la notion de frontière s'applique au cyberespace. Selon cette affirmation, le cyberespace appartient donc au domaine de la souveraineté, il permet alors la décision de l'État et représente un espace où les États qui en ont la volonté et les capacités peuvent exercer des jeux de pouvoir et de puissance. Cette territorialisation du cyberespace démontre que si désormais ces jeux de pouvoir et de puissance s'exercent hors des territoires classiques de la géopolitique, ils doivent toutefois être analysés sous une loupe géopolitique[42].

Cette vision propose donc un cyberespace qui est un territoire aux frontières poreuses qui permet à la manipulation de l'information, mais aussi, à la défense du secret d'État. Cette manipulation de l'information implique *ipso facto* une cyberdéfense de haute qualité ainsi que des

[41] Kempf, O. (2015). Cyberespace et dynamique des frontières. *Inflexions, N° 30* (3), 141. https://doi.org/10.3917/infle.030.0141.

[42] Kempf, O. (2015). Cyberespace et dynamique des frontières. *Inflexions, N° 30* (3), 144. https://doi.org/10.3917/infle.030.0141.

cyberfrontières de nature opératoire qui garantissent la liberté d'action étatique au sein du cyberespace. En définissant le cyberespace comme étant un territoire, Kempf note deux types de frontières au sein du cyberespace : la frontière opératoire (qui vient garantir la liberté d'action de l'État) et la frontière politique et territoriale (qui vient en second si la liberté d'action est garantie). Kempf rappelle que même si le cyberespace n'a pas la géographie sensible de l'espace terrestre, ses frontières ne sont jamais totalement étanches et que les cyberfrontières sont structurellement poreuses. L'enjeu pour un État consiste donc à les rendre visqueuses dans l'optique de pouvoir en dominer les flux et ainsi conserver une certaine maîtrise de son cyberespace national[43]. Cette opération est bien illustrée par le gouvernement chinois qui a mis en place une cybermuraille sur les couches sémantique, logicielle et physique du cyberespace.

Ce travail aborde donc une vision du cyberespace comme étant opaque, où autant l'individu que l'État peut y agir en étant camouflé et ainsi appliquer la stratégie de l'innatribution qui permet de garder son anonymat au sein du cyberespace[44]. Cette affirmation se positionne dans une notion de territorialisation du cyberespace qui ne fait pas le consensus en relations internationales, notamment par la complexité de ses frontières, c'est néanmoins une lecture territoriale qui sera faite par cet essai.

[43] Kempf, O. (2015). Cyberespace et dynamique des frontières. *Inflexions, N° 30* (3), 146. https://doi.org/10.3917/infle.030.0141.

[44] Kempf, O. (2015). Cyberespace et dynamique des frontières. *Inflexions, N° 30* (3), 146. https://doi.org/10.3917/infle.030.0141.

CHAPITRE 3

Étude de cas : La présence chinoise en Malaisie

Cette étude tente donc d'évaluer les impacts du volet numérique des nouvelles routes de la soie sur la souveraineté numérique et la cybersécurité de la Malaisie. Ceci est possible en analysant le partenariat numérique et les deux projets phares entre la Chine et la Malaise, soit, la zone de libre-échange[45] et la ville intelligente E.T City Brain[46]. Ces deux projets ont été choisis puisqu'ils sont au cœur de la relation sino-malaisienne et s'inscrivent dans le projet de développement numérique chinois en Asie du Sud-Est. Puisque les projets sont spécifiques au partenariat avec la Malaisie, il s'agit d'une étude de cas simple. Elle se positionne au sein d'une population plus large, car elle s'inscrit dans une population de pays situés en Asie du Sud-Est participant aux initiatives numériques de la route de la soie. Il est important de noter que la zone de libre-échange numérique avec la Malaisie fut mise en service en novembre 2017, toutefois, les premiers documents en provenance du groupe Alibaba et de la Malaysian Digital Economy Corporation (MDEC) ont fait surface en 2016. Le projet des routes de la soie, quant à lui, fut dévoilé à l'automne 2013 par Xi Jinping lors de visites au Kazakhstan et en Indonésie.

[45] La zone de libre-échange numérique de la Malaisie a été mise en service en novembre 2017 dans l'optique de faire de la Malaisie un centre de logistique pour les marchés mondiaux en offrant des opportunités pour les entreprises de la Malaisie et des autres pays de l'ASEAN.

[46] Le E.T City Brain est une plateforme d'intelligence artificielle élaborée par Alibaba Cloud, spécifiquement conçue pour soutenir les administrations municipales dans la gestion efficace des défis liés à la circulation, à la sécurité et à l'infrastructure urbaine. Cette plateforme exploite des données en temps réel et des algorithmes d'analyse avancés afin d'optimiser les opérations urbaines et d'améliorer la qualité de vie des citoyens.

3.1 Expansion du pouvoir numérique chinois en Malaisie

L'ouverture de la zone de libre-échange numérique représente un engrenage de zones physiques et virtuelles visant à aider les petites ou moyennes entreprises (PME) à tirer parti de la convergence de la croissance exponentielle de l'économie d'Internet et des activités de commerce électronique transfrontalier. Diverses initiatives ont été entreprises par le groupe Alibaba en Malaisie afin de mettre en place une telle infrastructure technologique commerciale mondiale inclusive pour les PME locales, notamment la création du premier centre régional d'*e fulfillment* d'Alibaba dans le parc DFTZ de KLIA Aeropolis et l'établissement du centre de données Internet d'Alibaba Cloud en Malaisie — la première plateforme publique mondiale de cloud computing en Malaisie.

Le projet d'Alibaba Cloud's ET city brain, fera de Kuala Lumpur en Malaisie la seule ville hors Chine à essayer le projet. Alibaba Cloud's ET city brain est un système très complexe qui a effectivement prouvé son utilité en Chine, il fonctionne par une immense collecte de donnée qui transite dans les systèmes de traitement de données du groupe Alibaba. C'est ce transit qui pose une ambivalence face au projet, notamment puisqu'il implique possiblement une utilisation de ces données par le gouvernement chinois. Ces projets accentuent l'influence du groupe Alibaba en Malaisie et dans la région de l'Asie du Sud-Est, influence qui s'effectue au profit de l'exportation de la puissance chinoise au niveau économique, numérique, politique et sécuritaire.

Il est important aussi de mentionner que du fait du manque d'accès au processus décisionnel de la politique économique étrangère chinoise (p. ex. accès aux discussions entre décideurs, aux énoncés de politiques à l'interne, aux rapports de comités consultatifs informels sur la politique économique) cette approche méthodologique comporte des limites explicatives.

3.2 L'exploitation du cyberespace par la Chine

Au cœur même de ce partenariat entre les deux pays se trouve le concept de la cybersécurité. Bien que le concept fût utilisé en premier par des informaticiens et des programmeurs, la cybersécurité a, depuis, dépassé la conception technique de la sécurité informatique, de par ses répercussions dans la société. Ce sont les études de sécurité qui ont principalement conceptualisé la notion de sécurité mobilisée dans le discours politique.

L'École de Copenhague a notamment traité de la cybersécurité comme étant un exemple de tentative de sécurisation. En effet, il est ici important de théoriser la cybersécurité comme un secteur imbriqué aux secteurs militaires, politique, environnemental, sociétal, économique et religieux[47]. En effet, pour appuyer leurs arguments, les auteurs citent le fait que l'ampleur potentielle des cybermenaces rejoint des secteurs et des objets d'ordre physiques tels que des transformateurs électriques, des trains, des pompes de pipeline, des cuves de produits chimiques et des radars ». De facto, la sécurisation du cyberespace se fait dans l'optique de cibler ce qui pourrait compromettre par exemple, les systèmes et les réseaux de manière à rendre les communications et la distribution d'énergie électrique difficiles ou impossibles, à perturber le transport et l'expédition, à empêcher les transactions financières et à entraîner le vol de grandes quantités d'argent[48].

On voit ici que le discours sur la cybersécurité progresse à travers des secteurs et des distinctions jugées cruciales pour les études de sécurité : entre sécurité individuelle et collective, entre autorités publiques et institutions privées, et entre sécurité économique et sécurité politico-

[47] Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly, 53*(4), 1156.

[48] Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly, 53*(4), 1161.

militaire. En juxtaposant cette notion de cybersécurité au développement du volet digital de la route de la soie, il est impossible de faire abstraction du niveau politique que prend cette sécurisation.

En effet, pour mieux comprendre l'étendue des répercussions d'un contrôle sur la cybersécurité, il est important de définir la place que prend la cybersécurité au niveau politique. Au niveau politique, cette cybersécurité s'explique par l'intrication des enjeux économiques (escroquerie, espionnage) et sécuritaires (protection des opérateurs d'importance vitale/OIV[49]), cela correspond à une représentation de la cybersécurité comme un bien public, comme étant l'affaire de tous. C'est ainsi qu'une idée d'action s'est répandue dans les discours politiques : en plus d'assurer la sécurité de ses propres systèmes d'information (SSI), l'État doit assurer à tous les citoyens la liberté d'utiliser les réseaux informatiques et garantir la protection de son économie et de son territoire[50]. De plus, la réglementation de plus en plus restrictive d'Internet démontre que la Chine érige désormais la cybersécurité au rang de priorité nationale, cette focalisation sur la cybersécurité est très présente au sein de son programme politique concernant le volet digital des routes de la soie[51].

Dans le cas de la Chine, la conception de la cybersécurité est une notion définie par les officiels chinois comme un ensemble de technologies et de procédures conçues pour protéger de nombreux domaines des menaces issues d'Internet : l'intégrité politique et idéologique, les données, la technologie, les applications, l'économie et les flux de communications. La Chine accorde une

[49] Un opérateur d'importance vitale (OIV) est une organisation identifiée par l'État comme ayant des activités indispensables ou dangereuses pour la population.

[50] d'Elia, D. (2014). La cybersécurité : de la représentation d'un bien public à la nécessité d'une offre souveraine. *Sécurité et stratégie* (4), 72-80.

[51] Yuen, S. (2015). Devenir une cyber-puissance. Le renforcement de la politique de cybersécurité chinoise et ses conséquences. *Perspectives chinoises, 2015* (2015/2), 55-61.

grande importance à cette question de cybersécurité. En effet, la phrase *sans cybersécurité il n'y a pas de sécurité nationale* est utilisée de façon constante dans les discours concernant la sécurité nationale ainsi que dans les quotidiens chinois[52].

Parallèlement, il est possible d'analyser que les stratégies digitales démontrées par le gouvernement chinois ne sont pas seulement conçues pour garantir la survie du régime et protéger la sécurité nationale, mais elles ont également pour objectif de protéger et favoriser le développement de l'économie nationale — et en particulier des industries technologiques chinoises. En effet, nombreuses sont celles qui vont s'implanter dans la région Asie-Pacifique. Xi Jiping, vise ainsi à ce que la chine « devienne un leader mondial en matière d'innovation », tout en construisant une « Chine numérique et une société intelligente », la cyberpuissance de la Chine constitue donc une composante essentielle de sa puissance nationale globale et est intrinsèquement liée à la compréhension de la portée de ses actions sur la région de l'Asie-Pacifique.

Le gouvernement a d'ailleurs déposé les bases de sa politique séculaire lors d'un discours prononcé par Xi Jinping au 19e Congrès national du Parti communiste de Chine lors du 18 octobre 2017, nommé *Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era*.

> Nous devrions nous efforcer d'atteindre les domaines scientifiques et technologiques de pointe, de renforcer la recherche fondamentale et de réaliser des percées majeures dans la recherche fondamentale pionnière et les innovations originales et novatrices. Nous renforcerons la recherche fondamentale en sciences appliquées, lancerons de grands projets nationaux en science et technologie et donnerons la priorité à l'innovation dans les technologies génériques clés, les technologies de pointe à la frontière, les technologies d'ingénierie modernes et les technologies de rupture. Ces efforts contribueront grandement à renforcer la force de la Chine dans les domaines de la science et de la technologie, de la qualité des produits, de l'aérospatiale, du

[52] « Meiyou wangluo anquan jiu meiyou guojia anquan » (Sans cybersécurité, il n'y a pas de sécurité nationale), Quotidien du peuple, 18 mai 2014, disponible sur http://politics.people.com.cn/n/ 2014/0518/c1001-25030371.html

> cyberespace et des transports, ainsi qu'à bâtir une Chine numérique et une société intelligente[53]. (Jinping, 2017)

Les ambitions du président de la République populaire de Chine sont indéniables : la Chine aspire à devenir la première puissance technologique mondiale. Depuis plusieurs années, elle a su exploiter le potentiel de transformation économique de l'Internet, tout en préservant jusqu'à présent sa stabilité politique. Cette combinaison fait d'elle une force redoutable sur la scène internationale.

De plus en plus, il semble que la Chine cherche activement à promouvoir ce que Xi Jinping a appelé un « programme chinois », qui pourrait avoir des implications inquiétantes pour la gouvernance démocratique dans le monde entier. Par exemple, l'administration du cyberespace de la Chine[54] a organisé un séminaire pour les pays participants à l'initiative chinoise *Belt and Road Initiative* (BRI) qui a mis en évidence le potentiel d'outils tels que les « systèmes de gestion de l'opinion publique à base de données volumineuse », renforçant ainsi la portée de son *soft power*[55] auprès des régions convoitées.

On voit donc, depuis quelques années, une augmentation de l'importance accordée au potentiel stratégique du cyberespace ainsi qu'une fusion du domaine militaire à celui du cyberespace en Chine. En effet, lors de la Conférence nationale sur la cybersécurité et l'informatisation en avril 2018, Xi Jinping a souligné le dynamisme de la fusion militaire et civile au sein du domaine de la cybersécurité et de l'informatisation, appelant la Chine à instrumentaliser la transformation des technologies de l'information et celle des affaires militaires. Exhortant ainsi

[53] Jinping, X. (2017). *Secure a decisive victory in building a moderately prosperous society in all respects and strive for the great success of socialism with Chinese characteristics for a new era, vol. 18*. (Ma traduction)
[54] *Office of the Central Cyberspace Affairs Commission*.
[55] *Concept tiré de* Joseph S. Nye, Jr., Soft Power : The Means to Success in World Politics, New York, Public Affairs, 2004, particulièrement le chapitre 1.

la Chine à créer une structure de développement complète, multidomaine et intrinsèquement liée au développement du marché[56]. La Chine reconnaît ainsi que l'espace et le cyberespace sont désormais des domaines et stratégies essentiels pour les futurs conflits.

S'imposant ainsi comme une nouvelle menace et loin de s'en cacher, dans la publication de son livre blanc sur la défense nationale de 2015, la Chine appelle à une mobilisation dans l'optique d'accélérer le développement d'une cyberforce et de renforcer ses capacités en matière de cyberdéfense[57]. Ce renforcement de compétences et de capacité en matière de cyberdéfense s'effectue au travers du développement et à l'implantation d'initiatives de nature numérique dans les pays participants à l'initiative chinoise *Belt and Road Initiative* (BRI). La Malaisie, comme terrain d'expérimentation pour la première zone de libre-échange numérique et d'implantation de la première ville intelligente hors chine, représente à la fois des stratégies économiques, mais aussi, une volonté d'imposer un contrôle qui passe par le numérique.

3.2.1.1 La Malaisie : Un terrain stratégique pour les aspirations numériques de la Chine

L'intérêt de la Chine envers la Malaisie représente un choix hautement stratégique pour le développement du pays. En effet, le pays présente plusieurs caractéristiques bénéfiques à l'expansion de la Chine en Asie du Sud-Est. Il y a eu plusieurs vagues de développement économique en Malaisie qui ont commencées lorsque l'impérialisme britannique qui est venu inscrire la Malaisie dans les marchés mondiaux de matières premières comme l'étain et le caoutchouc, dont le marché et la transformation étaient majoritairement financés sur la base de

[56] Xi, J. (2018). Xi Jinping's April 20 speech at the national cybersecurity and information work conference. *New America*.

[57] China, Ministry of National Defense, '2015 White Paper: China's Military Strategy', May 2015, available at http://eng.mod.gov.cn/Database/WhitePapers

capitaux essentiellement privés, anglais, mais aussi hollandais et français. Sachant que la population malaisienne était peu nombreuse, le système économique capitaliste entraîna une forte immigration chinoise et indienne vers la fin du 19e siècle[58]. Obtenant son indépendance en 1957, la Malaisie continua son expansion économique jusqu'au début des années 1990 en bénéficiant d'un afflux massif de capitaux étrangers, croissance qui fut durement touchée par la crise monétaire de 1997. Le pays adopta alors une politique économique protectionniste et vit son économie croître de plus de 8 % en 2014, contrairement aux économies indonésiennes et thaïlandaises. Depuis, la Malaisie est considérée comme un pays en expansion économique, elle se positionne au troisième rang comme destination préférée des multinationales et des sociétés technologiques du monde entier.

La Malaisie agit désormais en tant que carrefour économique entre l'Inde et la Chine, elle est au centre géographique de l'Association des nations de l'Asie du Sud-Est (ANASE). Le pays représente un partenaire commercial fiable pour les exportateurs chinois dans le climat mondial actuel, mais aussi, la porte d'entrée idéale pour avoir de l'influence envers l'ANASE. De plus, le lien économique entre les deux pays est fort, la Chine reste le plus grand partenaire commercial du pays. En effet, un total de 4,4 milliards de RM (1 077 115 611,49 USD) a été investi par la Chine, ce qui en fait la deuxième source d'investissement manufacturier approuvé en Malaisie.

L'économie numérique est un pilier essentiel de la croissance malaisienne et continue d'évoluer et de stimuler l'économie nationale. La Malaisie valorise fortement le développement de son économie numérique. Fahmi Fadzil, le ministre malaisien des Communications et du Multimédia, a annoncé en mai 2023 que l'économie numérique devrait représenter environ 25,5 %

[58] Alary, P., & Lafaye de Micheaux, E. (2013). L'économie politique de l'Asie : état des lieux et perspectives de recherche pour l'Asie du Sud-Est. Introduction. *Revue de la régulation. Capitalisme, institutions, pouvoirs* (13), 98

du Produit intérieur brut (PIB) de la Malaisie d'ici 2025. En 2023, la Malaisie a enregistré une hausse considérable des investissements dans l'économie numérique, avec une croissance de 289 % par rapport à l'année précédente. Cela équivaut à peu près à un total de 6 milliards de dollars US[59]. La Malaisie est donc déjà un sol propice à l'expansion de l'économie numérique. Bien que leurs infrastructures ne soient pas aussi avancées que celles de la Chine, les fondations nécessaires à cette croissance sont déjà en place.

En effet, la Malaisie a opéré un virage vers l'industrie numérique, motivée par une vision politique qui visait une augmentation significative de la productivité grâce à la transition vers le numérique. Différents ministères et agences publics assistent le secteur privé dans cette transformation vers le numérique. La *Malaysian Digital Economy Corporation* (MDEC), qui relève du ministère des Communications et du Multimédia, est la principale agence chargée de créer un cadre global propice à la numérisation. La *Malaysian Digital Economy Corporation* (MDEC) concentre ses efforts sur quatre piliers stratégiques : stimuler l'investissement, promouvoir des champions locaux de la technologie sur la scène régionale et mondiale, créer des écosystèmes d'innovation propices aux *start-ups* et populariser le numérique au sein de la population. En 2022, le total des exportations de haute technologie de la Malaisie s'élevait à 66,21 milliards de dollars US[60].

[59] MDEC. (2023, 26 octobre). MDX2023: Celebrating the Growth of Malaysia's Digital Economy. *Forbes*. https://www.forbes.com/sites/malaysia-digital-economy-corporation/2023/10/26/mdx2023-celebrating-the-growth-of-malaysias-digital-economy/?sh=4893380028c2

[60] The World Bank. (2022). High-technology exports (current US$) – Singapore, Malaysia, Thaildan, Indonesia. *United Nations, Comtrade database through the WITS platform*. https://data.worldbank.org/indicator/TX.VAL.TECH.CD?locations=SG-MY-TH-ID

Par voie conséquente, le pivot vers la Malaisie est motivé par le fait que le pays représente un marché très important pour Alibaba et Lazada[61], c'est la région la plus payante dans l'ANASE pour le commerce électronique, en effet, la proportion d'internautes au sein de l'ANASE a doublé en cinq ans ; en 2022 leur nombre a atteint 516,5 millions, représentant un immense marché pour la Chine[62]. Cette proportion d'internautes est d'autant plus pertinente puisqu'actuellement, il est rapporté que neuf entreprises sur dix en Malaisie sont des petites et moyennes entreprises (PME), dont 28 % ont apparemment une présence en ligne et 15 % d'entre elles utilisent Internet pour des exportations[63]. L'objectif spécifique d'exportation pour les PME est de 38 milliards USD d'ici 2025. S'il est atteint, cela fera de la Malaisie la première plateforme de transbordement d'Asie.

3.3 Le partenariat Sino-Malaisien : Un jeu risqué

En développant son aspect numérique des routes de la soie, la Chine s'engage dans une compétition technologique stratégique avec les États-Unis. Cela soulève la question de savoir si elle exporte son modèle d'autoritarisme numérique à l'échelle mondiale. En effet, dans la volonté de réaliser des progrès technologiques rapides, le gouvernement chinois semble motivé par plusieurs raisons : la nécessité de générer une nouvelle croissance économique par la modernisation industrielle et la promotion de modèles commerciaux novateurs ; l'objectif de renforcer l'autonomie en matière d'innovation et d'intégration civile-militaire, et l'objectif d'étendre

[61] Alibaba et Lazada sont deux grandes plateformes de commerce électronique qui opère principalement dans les pays d'Asie du Sud-Est.

[62] Statista. (2022). Nombre d'utilisateurs d'Internet dans le monde en 2022, par région (en millions). https://fr.statista.com/statistiques/564020/nombre-d-utilisateurs-d-internet-dans-le-monde-en-par-region/

[63] Yean, T. S. (2018). The Digital Free Trade Zone (DFTZ): Putting Malaysia's SMEs onto the Digital Silk Road.

l'influence mondiale de la Chine en développant l'utilisation des produits chinois pour les infrastructures numériques, les télécommunications et le commerce électronique[64].

Renforçant son pouvoir d'action et d'exportation, la Chine bénéficie d'avantages structurels pour faire avancer ses projets, Pékin canalise des quantités massives de capitaux par le biais de fonds d'orientation de l'État dans les technologies émergentes et dissuade les concurrents étrangers d'entrer sur le marché intérieur pour protéger les entreprises nationales de la concurrence. De plus, la Chine se bat maintenant pour devenir un chef de file mondial dans des technologies comme la 5G, l'Intelligence artificielle, l'informatique quantique et les chaînes de blocs.

De plus, la Chine exporte maintenant son modèle numérique et ses normes vers les pays qui bénéficient des routes de la soie. Depuis l'annonce du projet, de nombreux responsables chinois ont organisé des formations sur les nouveaux médias et/ou la gestion de l'information avec des représentants de 36 des 65 pays évalués. Ces pays incluent l'Arabie saoudite, les Émirats arabes unis, l'Égypte, la Jordanie, le Liban, la Libye, le Maroc, l'Ouganda, la Tanzanie, les Philippines, le Vietnam et la Thaïlande. On observe un partage des normes numériques strictes de la Chine, où par exemple, une censure importante est appliquée à l'accès à Internet et un contrôle rigoureux est exercé sur la navigation sur Internet.

On observe une augmentation de la désinformation et de la propagande diffusées en ligne, ainsi qu'une collecte incessante de données personnelles qui remet en question les notions traditionnelles de la vie privée. Un nombre croissant de pays se dirige vers l'autoritarisme numérique en adoptant le modèle chinois de censure étendue et de systèmes de surveillance

[64] Shi-Kupfer, K., & Ohlberg, M. (2019). China's digital rise: Challenges for Europe. *Merics papers on China, 7,* 14.

automatisés, y compris la Malaisie si les projets aboutissent. Xi Jinping propose ainsi un modèle de gouvernance du pays, y compris sa gestion de l'Internet, comme « une nouvelle option pour les autres pays et nations qui souhaitent accélérer leur développement tout en préservant leur indépendance ». Mais plutôt que de simplement montrer l'exemple, Beijing a pris des mesures significatives cette année pour établir ses normes et ses pratiques à l'échelle mondiale, exportant de facto son autoritarisme numérique[65].

Lorsque l'on parle d'autoritarisme numérique, on fait référence à un régime qui s'attache à la suppression de ces dimensions : limitation de la participation politique et non-possibilité de contestation par la société ou ses institutions représentatives (partis, associations, syndicats, etc.) des décisions essentielles qui sont prises par un petit groupe restreint. Il ne saurait cependant les annihiler, à l'instar du régime totalitaire, autour d'une idéologie englobante et d'une transformation radicale de la société, dont il n'a pas les moyens, même si la rhétorique ou l'appétence en ont parfois été présentes dans un certain nombre de cas. L'autoritarisme est essentiellement un système de contrôle[66].

Ce concept incite à envisager la possibilité d'un contrôle numérique à l'échelle régionale. Certains perçoivent le projet du volet digital de la route de la soie comme une initiative davantage nationale qu'internationale à certains égards, visant à établir une hégémonie régionale de nature digitale. Il semble que la Chine se protège considérablement de l'influence extérieure afin de poursuivre sa vision de la cybergouvernance, de la gestion sociale et du contrôle. Il est donc crucial

[65] Shahbaz, A. (2018). Freedom on the net 2018: The rise of digital authoritarianism. Washington, DC : Freedom House.

[66] Droz-Vincent, P. (2004). Quel avenir pour l'autoritarisme dans le monde arabe ? *Revue française de science politique, 54* (6), 945-979.

de ne pas percevoir les ambitions numériques de la Chine comme étant de simples exercices économiques ou civils. Elles associent des objectifs économiques à des objectifs normatifs et sécuritaires, manifestant une volonté d'accroître son pouvoir discursif en façonnant des normes et des standards mondiaux basés sur les normes et standards chinois[67]. Les ambitions numériques de la Chine ont un impact bien au-delà de ses frontières géographiques ; ses produits et services numériques sont déjà en train de conquérir les marchés mondiaux et ceux de la région de l'Asie du Sud-Est.

La Chine cherche également à se doter d'une infrastructure numérique mondiale de diverses manières, notamment en étant à l'avant-garde des initiatives internationales en matière d'infrastructure, de commerce électronique et de collaboration en matière de recherche. Si la Chine parvient à imposer ses normes et standards numériques dans la région de l'Asie du Sud-Est, et à exercer un contrôle strict sur le commerce électronique et les développements technologiques, y compris la collecte de données et la surveillance, le Parti communiste chinois pourrait exercer un contrôle hégémonique sur la région. Il est très probable que cette hypothèse se concrétise, notamment parce que les technologies présentées par le volet numérique de la route de la soie sont conçues pour compléter l'infrastructure physique de la ceinture et de la route. Elles introduisent également des normes techniques communes dans les pays participants, dont la majorité sont des économies émergentes qui ne disposent pas d'infrastructures Internet de base. Cela facilite l'implantation des politiques et initiatives numériques chinoises.

[67] Shi-Kupfer, K., & Ohlberg, M. (2019). China's digital rise : Challenges for Europe. *Merics papers on China*, *7*, 14.

En outre, le gouvernement chinois présente ce volet numérique comme un moyen de renforcer la connectivité pour faciliter l'échange d'informations, une « coopération mutuellement bénéfique et gagnant-gagnant ». Cependant, les implications géopolitiques sont trop importantes pour se limiter à une coopération gagnant-gagnant si les gouvernements étrangers permettent aux entreprises technologiques chinoises, qui ont des liens étroits avec l'État, d'installer des systèmes de communication de données complexes. Ce transfert de données équivaut à un transfert de renseignements de nature intelligente, militaire, économique, sociologique et politique. L'accès à ces données amplifie le pouvoir d'action de la Chine, rendant l'hypothèse d'un contrôle strict sur la région de l'Asie du Sud-Est à la fois plausible et menaçante.

CONCLUSION

Après avoir analysé l'aspect numérique des routes de la soie, et plus spécifiquement le cas de la Malaisie où la Chine envisage de mettre en œuvre plusieurs projets, les informations recueillies nous permettent de répondre à la question de recherche posée au début de ce travail : quels sont les impacts de l'aspect numérique des nouvelles routes de la soie sur la souveraineté numérique et la cybersécurité de la Malaisie ?

Il est juste de dire que l'aspect numérique des nouvelles routes de la soie représente une ingérence significative dans la cybersouveraineté malaisienne, ainsi qu'une menace pour la cybersécurité. Les initiatives du gouvernement chinois visent à intégrer le Parti communiste et l'État chinois parmi les bénéficiaires des projets de la Ceinture et de la Route. En effet, l'influence croissante du groupe Alibaba en Malaisie, et plus largement dans la région de l'Asie du Sud-Est contribue à l'exportation de la puissance chinoise sur les plans économique, numérique, politique et sécuritaire. Il est important de noter que les entreprises numériques chinoises (Alibaba, Taobao, Huawei) sont, par conséquent, liées soit au Parti communiste, soit à des institutions d'État. Leurs projets sont probablement en accord avec des stratégies plus larges élaborées par les dirigeants chinois.

Ce dispositif est aussi, à bien des égards, un moyen pour la Chine d'avancer ses objectifs en matière de cyberdéfense. L'objectif à long terme de la Chine est de changer le paysage mondial de la concurrence technologique en définissant et en exportant ses propres normes pour toutes les industries émergentes, ce qui permettra de s'assurer que les produits et services chinois ne sont pas entravés par les normes établies par un autre pays. La Chine reconnaît effectivement que

l'espace et le cyberespace sont désormais des domaines stratégiques essentiels pour les futurs conflits[68].

La Malaisie, en tant que terrain d'expérimentation pour la première zone de libre-échange numérique et pour l'implantation de la première ville intelligente en dehors de la Chine, incarne à la fois des stratégies économiques et des stratégies de développement de la puissance. Il est important de noter que cette zone de libre-échange numérique, en plus d'ouvrir la Malaisie au marché chinois et à ses 500 millions de consommateurs, crée une dépendance au marché chinois que la Malaisie ne peut se permettre de contester. Étant le premier partenaire commercial de la Malaise et avec un volume total de commerce entre les deux pays s'établissant en 2017 à 67,5 milliards de dollars américains et représentant 16,4 % du commerce extérieur de la Malaisie, contester ce partenariat et la dépendance inévitable résulterait à un immense déficit économique pour la Malaisie.

Il existe donc de nombreux avantages à permettre à Alibaba de s'implanter sur le territoire, notamment celui de la survie économique du pays. Cela est vrai même si les préoccupations de la Malaisie concernant l'ouverture d'une zone de libre-échange numérique incluent la présence croissante de travailleurs étrangers et d'expatriés chinois dans le pays, l'éviction des petites et moyennes entreprises locales et les risques économiques relativement élevés des mégaprojets. Cela vient faire un lien avec le concept de *bandwagonning* de Waltz.

De plus, le projet phare du partenariat entre Alibaba et la Malaisie, à savoir l'implantation de la première Alibaba Cloud's ET City Brain à Kuala Lumpur, représente une menace sérieuse

[68] China, Ministry of National Defense. (2015), '2015 White Paper: China's Military Strategy'. http://eng.mod.gov.cn/Database/WhitePapers.

pour la perte de la cybersouveraineté malaisienne au profit d'une hégémonie numérique chinoise. En effet, l'aspect des villes intelligentes soulève des enjeux en matière de cybersécurité et de cybersouveraineté. La Chine semble exporter son modèle de censure et de surveillance, ce qui équivaut à l'exportation d'un autoritarisme numérique via Alibaba Cloud et son système de surveillance. L'implantation des villes intelligentes ouvre la porte à une ingérence numérique de la Chine en Malaisie, notamment par la collecte de données et l'implantation des systèmes de surveillance chinois. Ce qui devrait être contrôlé par la Malaisie tombe entre les mains de la Chine, entraînant une perte de la cybersouveraineté malaisienne.

Il est important de noter que la Chine fait des efforts très limités pour établir un régime de protection des données et aucun régime ne couvre actuellement les abus ou la collecte non contrôlée de données par les acteurs gouvernementaux. La protection des citoyens contre les excès du gouvernement n'est pas — et ne peut pas être — discutée dans le climat politique actuel de la Chine. Par conséquent, les données collectées auprès de la population malaisienne ne bénéficient d'aucune protection et sont libres d'utilisation une fois qu'elles sont stockées dans les centres de données d'Alibaba en Chine. L'utilisation de ces données peut servir à sécuriser des enjeux politiques et sécuritaires, en facilitant la compréhension du climat politique et sécuritaire en Malaisie.

L'enjeu ici est que l'accès libre et le contrôle libre de Kuala Lumpur représentent un danger pour la cybersécurité, et dans le cas analysé, il pose la question d'une perte de la cybersouveraineté malaisienne au profit d'une hégémonie numérique chinoise. Bien qu'il s'agisse d'une violation de la cybersouveraineté malaisienne, la Malaisie n'est pas en mesure de contester cette ingérence chinoise si elle tient à la viabilité de son régime économique. Il est fort plausible que la Malaisie

soit un succès pour la Chine, ce qui pourrait entraîner une volonté d'exportation numérique vers les pays voisins.

RÉFÉRENCES

Alary, P., & Lafaye de Micheaux, E. (2013). L'économie politique de l'Asie : état des lieux et perspectives de recherche pour l'Asie du Sud-Est. Introduction. *Revue de la régulation. Capitalisme, institutions, pouvoirs* (13).

Balzacq, T. (2007). The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies*. JCMS : Journal of Common Market Studies, 46(1), 75-100. https://doi.org/10.1111/j.1468-5965.2007.00768.x

Balzacq, T. (2016). Théories de la sécurité. Presses de Sciences Po. https://doi.org/10.3917/scpo.balza.2016.01

Bellanger, P. (2012). De la souveraineté numérique. Le Débat, n° 170 (3), 149-159. https://doi.org/10.3917/deba.170.0149

Buzan, B., Wæver, O., Wæver, O., & De Wilde, J. (1998). Security: A new framework for analysis. Lynne Rienner Publishers.

China, Ministry of National Defense. (201). '2015 White Paper: China's Military Strategy'. http://eng.mod.gov.cn/Database/WhitePapers

Creemers, R. (2020). China's conception of cyber sovereignty. Governing cyberspace: Behavior, power and diplomacy, 107-145.

Creemers, R. (2020). Comment la Chine projette de devenir une cyber-puissance. *Hérodote, N° 177-178* (2), 297-311. https://doi.org/10.3917/her.177.0297

Xi, J. (2018). Xi Jinping's April 20 speech at the national cybersecurity and information work conference. *New America*.

Cuihong, C. (2018). China and global cyber governance: main principles and debates. Asian Perspective, 42 (4), 647-662.

Danet, D., & Desforges, A. (2020). Souveraineté numérique et autonomie stratégique en Europe : du concept aux réalités géopolitiques. Hérodote, N° 177-178 (2), 179-195. https://doi.org/10.3917/her.177.0179

d'Elia, D. (2014). La cybersécurité : de la représentation d'un bien public à la nécessité d'une offre souveraine. *Sécurité et stratégie* (4), 72-80.

Droz-Vincent, P. (2004). Quel avenir pour l'autoritarisme dans le monde arabe ? [What Is the Future of Authoritarianism in the Arab World?]. Revue française de science politique, 54 (6), 945-979. doi : 10.3917/rfsp.546.0945

Haas, E. B. (1953). The balance of power: prescription, concept, or propaganda? *World Politics, 5*(4), 442-477.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. International studies quarterly, 53(4), 1155-1175.

Kagan, R. (2005). « The Illusion of 'Managing' China, » Washington Post.

Kang, D. C. (2003). Getting Asia Wrong: The Need for New Analytical Frameworks. International Security, 27(4), 57-85. http://www.jstor.org/stable/4137604

Kempf, O. (2015). Cyberespace et dynamique des frontières. Inflexions, N° 30 (3), 141-149. https://doi.org/10.3917/infle.030.0141

Kugler, J. J., & Organski, A. (2011). CHAPTER 7 The Power Transition: A Retrospective and Prospective Evaluation. Handbook of War Studies.

Lindsay, J. R., Cheung, T. M., & Reveron, D. S. (2015). China and cybersecurity: Espionage, strategy, and politics in the digital domain. Oxford University Press, USA.

MDEC. (2023, 26 octobre). MDX2023: Celebrating the Growth of Malaysia's Digital Economy. Forbes. https://www.forbes.com/sites/malaysia-digital-economy-corporation/2023/10/26/mdx2023-celebrating-the-growth-of-malaysias-digital-economy/?sh=4893380028c2

Mearsheimer, J. J., & Alterman, G. (2001). The tragedy of great power politics. WW Norton & Company.

Nye, J. S. (2004). *Soft power: The means to success in world politics*. Public affairs.

Organski, A. F. (1968). World politics. (No Title).

Polyakova, A., & Meserole, C. (2019). Exporting digital authoritarianism: The Russian and Chinese models. Policy Brief, Democracy and Disorder Series (Washington, DC : Brookings, 2019), 1-22.

Shahbaz, A. (2018). Freedom on the net 2018: The rise of digital authoritarianism. Washington, DC : Freedom House. Retrieved February, 28, 2019.

Schweller, R. L. (1994). Bandwagoning for Profit : Bringing the Revisionist State Back In. International Security, 19(1), 72. https://doi.org/10.2307/2539149

Shi-Kupfer, K., & Ohlberg, M. (2019). China's digital rise: Challenges for Europe. Merics papers on China, 7, 14.

The World Bank. (2022). High-technology exports (current US$) – Singapore, Malaysia, Thaildan, Indonesia. *United Nations, Comtrade database through the WITS platform*. https://data.worldbank.org/indicator/TX.VAL.TECH.CD?locations=SG-MY-TH-ID

Statista. (2022). Nombre d'utilisateurs d'Internet dans le monde en 2022, par région (en millions). https://fr.statista.com/statistiques/564020/nombre-d-utilisateurs-d-internet-dans-le-monde-en-par-region/

Waltz, K. N. (1979). Theory of international politics. Addison-Wesley Pub. Co.

Yean, T. S. (2018). The Digital Free Trade Zone (DFTZ): Putting Malaysia's SMEs onto the Digital Silk Road.

Yi, W. (2015). Toward a new type of international relations of win-win cooperation. China Int'l Stud., 52, 5.

Yuen, S. (2015). Devenir une cyber-puissance. Le renforcement de la politique de cybersécurité chinoise et ses conséquences. Perspectives chinoises, 2015 (2015/2), 55-61.

BIBLIOGRAPHIE

Akdag, Y. (2018). The Likelihood of Cyberwar between the United States and China: A Neorealism and Power Transition Theory Perspective. Journal of Chinese Political Science, 24(2), 225-247. https://doi.org/10.1007/s11366-018-9565-4

Allan, B. B., Vucetic, S., & Hopf, T. (2018). The Distribution of Identity and the Future of International Order: China's Hegemonic Prospects. International Organization, 72(4), 839-869. https://doi.org/10.1017/s0020818318000267

Balding, C. (2020). Chinese Open Source Data Collection, Big Data, And Private Enterprise Work For State Intelligence and Security: The Case of Shenzhen Zhenhua. Big Data, And Private Enterprise Work For State Intelligence and Security: The Case of Shenzhen Zhenhua (September 13, 2020).

Bodurtha, M., Forough, M., Ghiasy, R., & van der Lugt, S. (2021). The Digital Silk Road: Perspectives From Affected Countries.

Burgers, T., & Robinson, D. R. S. (2016). Networked Authoritarianism Is on the Rise. Sicherheit und Frieden (S+F) / Security and Peace, 34(4), 248-252. http://www.jstor.org/stable/26429018

Carrai, M. A. (2020). Chinese Political Nostalgia and Xi Jinping's Dream of Great Rejuvenation. International Journal of Asian Studies, 18(1), 7-25. https://doi.org/10.1017/s1479591420000406

Cattaruzza, A. (2019). La numérisation du champ de bataille. In Géopolitique des données numériques (pp. 137-145). Le Cavalier Bleu. https://www.cairn.info/geopolitique-des-donnees-numeriques--9791031803487-page-137.htm

Chambers, M. (2005). China and Southeast Asia: Creating a Win-win Neighborhood. China's "Good Neighbor" Diplomacy: A Wolf in Sheep's Clothing, 16-22.

Chaponnière, J.-R., & Lautier, M. (2016). L'intégration économique régionale en Asie du Sud-Est : une dynamique impulsée de l'extérieur. Mondes en développement (3), 113-130.

Cheney, C. (2019). China's Digital Silk Road: strategic technological competition and exporting political illiberalism. Council on Foreign Relations [Em linha],(26 Set. 2019). [Consult. 4 ago. 2020]. Disponível em WWW:< URL: https://www. cfr. org/blog/chinas-digital-silk-road-strategic-technological-competition-and-exporting-political.

Chun, W. H. K. (2008). Control and freedom: Power and paranoia in the age of fiber optics. mit Press.

Côté, D., & Martel, S. (2014). La Chine et l'Asie du Sud-Est : une relation ambivalente. Monde chinois, N° 38-39 (2), 48-65. https://doi.org/10.3917/mochi.038.0048

Danner, L. K., & Martín, F. E. (2019). China's hegemonic intentions and trajectory: Will it opt for benevolent, coercive, or Dutch-style hegemony? Asia & the Pacific Policy Studies, 6(2), 186-207. https://doi.org/10.1002/app5.273

de Lespinois, J. (2019). Le cyberespace : assurer la supériorité numérique des armées. Stratégique, N° 120 (3), 189-193. https://doi.org/10.3917/strat.120.0189

Deler, J.-P. (2010). Mutations économiques et recompositions territoriales en Asie du Sud et du Sud-Est : Introduction [Economic Transformations and Territorial Reconstructions in South and Southeast Asia: An Introduction]. Annales de géographie, n° 671-672 (1), 4-6. https://doi.org/10.3917/ag.671.0004

Douay, N., & Henriot, C. (2016). La Chine à l'heure des villes intelligentes. L'Information géographique, Vol. 80 (3), 89-102. https://doi.org/10.3917/lig.803.0089

Douzet, F. (2014). La géopolitique pour comprendre le cyberespace [Understanding Cyberspace with Geopolitics]. Hérodote, n° 152-153 (1), 3-21. https://doi.org/10.3917/her.152.0003

Douzet, F. (2020). Du cyberespace à la datasphère. Enjeux stratégiques de la révolution numérique. Hérodote, N° 177-178 (2), 3-15. https://doi.org/10.3917/her.177.0003

El Kadi, T. H. (2019). The promise and peril of the digital silk road. Chatham House: The Royal Institute of International Affairs, 6.

Erie, M. S., & Streinz, T. (2021). The Beijing Effect: China's' Digital Silk Road'as Transnational Data Governance. New York University Journal of International Law and Politics (JILP), Forthcoming.

Fang, B., Fang, & Zhang. (2018). Cyberspace sovereignty. Springer.

Fu, T. (2019). China's personal information protection in a data-driven economy: A privacy policy study of Alibaba, Baidu and Tencent. Global Media and Communication, 15(2), 195-213. https://doi.org/10.1177/1742766519846644

Gomez, M. (2013). Awaken the cyber dragon: China's cyber strategy and its impact on asean. Journal of Communication and Computer, 10, 796-805.

Ha, H. T. (2021). Un même lit, mais des rêves différents pour la Chine et l'ANASE1. Rédaction et administration, 28, 65.

Hache, E., & Mérigot, K. (2017). Géoéconomie des infrastructures portuaires de la route de la soie maritime. Revue internationale et stratégique (3), 85-94.

Han, D. (2017). The market value of who we are: the flow of personal data and its regulation in China. Media and Communication, 5(2), 21-30.

Hao, C. J. (2019). All may not be smooth along China's Digital Silk Road. Lowy Institute, Interpreter, August, 20.

Hemmings, J. (2020). Reconstructing Order: The Geopolitical Risks in China's Digital Silk Road. Asia Policy, 15(1), 5-21. https://doi.org/10.1353/asp.2020.0002

Hou, R. (2017). Neoliberal governance or digitalized autocracy? The rising market for online opinion surveillance in China. Surveillance & Society, 15(3/4), 418-424.

Huang, P., & Rioux, M. (2015). Gouvernance de l'Internet — vers l'émergence d'une cyberpuissance chinoise ? Monde chinois, N° 41 (1), 79-94. https://doi.org/10.3917/mochi.041.0079

Hugon, P. (2001). L'Asie de l'est après la crise : entre la mondialisation et la régionalisation. Mondes en développement (2001/1), 117-127.

Ikenberry, G. J. (1998). Institutions, strategic restraint, and the persistence of American postwar order. International Security, 23(3), 43-78.

Ikenberry, G. J. (2008). The Rise of China and the Future of the West: Can the Liberal System Survive? Foreign Affairs, 87(1), 23-37. http://www.jstor.org.proxy.bibliotheques.uqam.ca/stable/20020265

Ikenberry, G. J. (2016). Between the Eagle and the Dragon: America, China, and Middle State Strategies in East Asia. Political Science Quarterly, 131(1), 9-43. http://www.jstor.org.proxy.bibliotheques.uqam.ca/stable/43828766

Inkster, N. (2015). The Chinese Intelligence Agencies: Evolution and Empowerment in Cyberspace.". China and cybersecurity: Espionage, strategy, and politics in the digital domain, 29-50.

Irvine, R. (1982). The formative years of ASEAN: 1967–1975. In Understanding ASEAN (pp. 8-36). Springer.

Keohane, R. (1984). After hegemony: Cooperation and discord in the World political economy Princeton. Press, Princeton.

Kim, W., & Gates, S. (2015). Power transition theory and the rise of China. International Area Studies Review, 18(3), 219-226. https://doi.org/10.1177/2233865915598545

Kitchin, R., Coletta, C., Evans, L., Heaphy, L., & MacDonncha, D. (2017). Smart cities, epistemic communities, advocacy coalitions and thelast mile'problem. It-Information Technology, 59(6), 275-284.

Kokas, A. (2018). Platform patrol: China, the United States, and the global battle for data security. The Journal of Asian Studies, 77(4), 923-933.

Krause, K. (2003). Approche critique et constructiviste des études de sécurité. Annuaire français des relations internationales, 4, 600-612.

Lemke, D., & Tammen, R. L. (2010). Power Transition Theory and the Rise of China. International Interactions, 29 (4), 269-271. https://doi.org/10.1080/714950651

Lewis, D. (2017). China's global Internet ambitions : finding roots in ASEAN. Institute of Chinese Studies: Occasional Paper, 14.

Lilkov, D. (2020). Made in China: Tackling Digital Authoritarianism. European View, 19(1), 110-110.

Lincot, E. (2019). Les nouvelles routes de la soie du numérique et le défi de l'intelligence artificielle. Nectart, N° 9 (2), 146-153. https://doi.org/10.3917/nect.009.0146

Lindsay, J. R. (2015). The Impact of China on Cybersecurity: Fiction and Friction. International Security, 39(3), 7-47. https://doi.org/10.1162/ISEC_a_00189

Liu, M., & Tsai, K. S. (2020). Structural Power, Hegemony, and State Capitalism: Limits to China's Global Economic Power. Politics & Society, 49(2), 235-267. https://doi.org/10.1177/0032329220950234

Ly, B., & Tan, A. W. K. (2020). Challenge and perspective for Digital Silk Road. Cogent Business & Management, 7(1), 1804180. https://doi.org/10.1080/23311975.2020.1804180

MacKinnon, R. (2011). Liberation Technology: China's « Networked Authoritarianism ». Journal of Democracy, 22(2), 32-46. https://doi.org/10.1353/jod.2011.0033

Macleod, A. (2004). Les études de sécurité : du constructivisme dominant au constructivisme critique. Cultures & conflits (54), 13-51. https://doi.org/10.4000/conflits.1526

Macleod, A., Masson, I., & Morin, D. (2004). Identité nationale, sécurité et la théorie des relations internationales. Études internationales, 35 (1), 7-24. https://doi.org/10.7202/008445ar

Michelino, A. (2022). Rivalité entre grandes puissances, politique de puissance et coercition au 21e siècle.

Naughton, B. (2020). Chinese Industrial Policy and the Digital Silk Road: The Case of Alibaba in Malaysia. Asia Policy, 15(1), 23-39. https://doi.org/10.1353/asp.2020.0006

Noesselt, N. (2015). Revisiting the Debate on Constructing a Theory of International Relations with Chinese Characteristics. The China Quarterly, 222, 430-448. https://doi.org/10.1017/s0305741015000387

Oreglia, E., Ren, H., & Liao, C.-C. (2021). The Puzzle of the Digital Silk Road. Digital Silk Road in Central Asia: Present and Future, 1.

Owen, J. M. (2018). Ikenberry, international relations theory, and the rise of China. The British Journal of Politics and International Relations, 21(1), 55-62. https://doi.org/10.1177/1369148118791979

Piccone, T. (2018). Democracy and Digital Technology. SUR-Int'l J. on Hum Rts., 27, 29.

Puig, E. (2004). L'ordre et la menace : analyse critique du discours de la menace chinoise en Relations internationales. Revue internationale et stratégique, n° 54 (2), 119-130. https://doi.org/10.3917/ris.054.0119

Qiang, X. (2019). The road to digital unfreedom: President Xi's surveillance state. Journal of Democracy, 30(1), 53-67.

Qiang, X. (2021). Chinese Digital Authoritarianism and Its Global Impact. Digital Activism and Authoritarian Adaptation in the Middle East, 35.

Samaan, J.-L. (2011). Une géographie américaine de la menace chinoise. Hérodote, n° 140 (1), 103-122. https://doi.org/10.3917/her.140.0103

Schia, N., & Gjesvik, L. (2017). China's cyber sovereignty (Policy Brief). https://doi.org/10.13140/RG.2.2.30512.15360

Schmidt, B. (2018). Hegemony: A conceptual and theoretical analysis. Dialogue of civilizations Research Institute, 15.

Schneider, J. (2019). The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war. Journal of Strategic Studies, 42(6), 841-863. https://doi.org/10.1080/01402390.2019.1627209

Schwarck, E. (2018). Intelligence and informatization: the rise of the Ministry of Public Security in intelligence work in China. The China Journal, 80(1), 1-23.

Shah, A. R. (2021). Revisiting China Threat: The US' Securitization of the 'Belt and Road Initiative'. Chinese Political Science Review, 8(1), 84-104. https://doi.org/10.1007/s41111-021-00179-0

Shen, Y. (2016). Cyber Sovereignty and the Governance of Global Cyberspace. Chinese Political Science Review, 1(1), 81-93. https://doi.org/10.1007/s41111-016-0002-6

Sinpeng, A. (2019). Digital media, political authoritarianism, and Internet controls in Southeast Asia. Media, Culture & Society, 42(1), 25-39. https://doi.org/10.1177/0163443719884052

Song, W. (2015). Securitization of the" China Threat" discourse: A poststructuralist account. China Review, 15(1), 145-169.

Stryker, C. (2021). Digital Silk Road and Surveillance Technology in Central Asia. Digital Silk Road in Central Asia: Present and Future, 17.

Stuart-Fox, M. (2004). Southeast Asia and China: The role of history and culture in shaping future relations. Contemporary Southeast Asia: A Journal of International and Strategic Affairs, 26(1), 116-139.

Taidong, Z., & Qi, X. (2020). The Digital Silk Road and Southeast Asian Countries. The Fourth Industrial Revolution and the Future of Work: Implications for, 132.

Tan, D., & Grillot, C. (2018). L'Asie du Sud-Est dans le « siècle chinois » : Cambodge, Laos et Vietnam. Institut de recherche sur l'Asie du Sud-Est contemporaine.

Tertrais, H. (2009). Fin de guerre au Vietnam et construction de l'Asie [The End of the Vietnam War and the Construction of Asia]. Bulletin de l'Institut Pierre Renouvin, N° 29 (1), 169-177. https://doi.org/10.3917/bipr.029.0169

Thornton, P. M. (2010). Censorship and surveillance in Chinese cyberspace: Beyond the great firewall. Chinese politics: State, society and the market, 179-198.

Triolo, P., Allison, K., Brown, C., & Broderick, K. (2020). The Digital Silk Road: Expanding China's Digital Footprint. Eurasia Group, 8.

Vanolo, A. (2013). Smartmentality: The Smart City as Disciplinary Strategy. Urban Studies, 51(5), 883-898. https://doi.org/10.1177/0042098013494427

Ventre, D. (2015). Cybersécurité : perspectives chinoises. Revue Défense Nationale, N° 785 (10), 93-97. https://doi.org/10.3917/rdna.785.0093

Vila Seoane, M. F. (2019). Alibaba's discourse for the digital Silk Road: the electronic World Trade Platform and 'inclusive globalization'. Chinese Journal of Communication, 13(1), 68-83. https://doi.org/10.1080/17544750.2019.1606838

Villasenor, J. (2011). Recording everything: Digital storage as an enabler of authoritarian governments. Center for Technology Innovation at Brookings.

Waltz, K. N. (2000). Structural Realism after the Cold War. International Security, 25(1), 5-41. http://www.jstor.org.proxy.bibliotheques.uqam.ca/stable/2626772

Xinning, S. (2001). Building International Relations Theory with Chinese Characteristics. Journal of Contemporary China, 10(26), 61-74. https://doi.org/10.1080/10670560125339

Yang, F., & Xu, J. (2018). Privacy concerns in China's smart city campaign: The deficit of China's Cybersecurity Law. Asia & the Pacific Policy Studies, 5(3), 533-543. https://doi.org/10.1002/app5.246

Yecies, B., Keane, M., Yu, H., Zhao, E. J., Zhong, P. Y., Leong, S., & Wu, H. (2019). The cultural power metric: Toward a reputational analysis of China's soft power in the Asia-Pacific. Global Media and China, 4(2), 203-219. https://doi.org/10.1177/2059436419849724

Yu, H. (2017). Networking China: The Digital Transformation of the Chinese Economy Yu Hong Urbana, Chicago and Springfield: University of Illinois Press, 2017 225 pp. $28,00 ISBN 978-0-252-08239-9. The China Quarterly, 231, 817-819.

Zeng, J. (2016). China's date with big data: will it strengthen or threaten authoritarian rule? International Affairs, 92(6), 1443-1462. https://doi.org/10.1111/1468-2346.12750

Zeng, J., Stevens, T., & Chen, Y. (2017). China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of “Internet Sovereignty”. Politics & Policy, 45(3), 432-464. https://doi.org/10.1111/polp.12202

Zenglein, M. J., & Holzmann, A. (2019). Evolving made in China 2025. Merics papers on China(8), 78.

Zhao, X., Xu, X., Nai, H., Zhou, C., Hu, Z., Zhang, Y., & Jiang, H. (2018). Analysis of behavioral differentiation in smart cities based on mobile users’ usage detail record data. International Journal of Distributed Sensor Networks, 14(4), 155014771877008. https://doi.org/10.1177/1550147718770087