La sécurisation des technologies et services de l'information et de la communication (TSIC) dans le contexte des relations sino-américaines en tension : le cas de Huawei et de New IP (2012-2023)

Marilia Ferreira Maciel

Université Bordeaux Montaigne

École Doctorale Montaigne Humanités (ED 480)

THESE DE DOCTORAT EN

« SCIENCES DE L'INFORMATION-COMMUNICATION »

La sécurisation des technologies et services de l'information et de la communication (TSIC) dans le contexte des relations sino-américaines en tension : les cas de Huawei et New IP (2012-2023)

Synthèse

(original en anglais)

Marília FERREIRA MACIEL

Sous la co-direction de Divina FRAU-MEIGS et Mokhtar BEN HENDA

Membres du jury

Mokhtar BEN HENDA, MCF-HDR , Université Bordeaux Montaigne (co-directeur)

Dennis BROEDERS, Professeur, Université de Leiden (Pays-Bas)

Divina FRAU-MEIGS, Professeur, Université Sorbonne Nouvelle (co-directrice)

Julie MOMMÉJA, MCF, Université de Lorraine

Mathieu O'NEIL, Professeur, Université de Canberra (Australie)

Maud QUESSARD, Maître de conférences, IRSEM

Synthèse du volume 1
(original en anglais)

Cette recherche vise à comprendre pourquoi et comment un problème est identifié comme une question de sécurité, ainsi que les effets de ce processus sur les TICS. La sécurisation fait référence à un processus par lequel les problèmes sont définis par des agents de sécurisation comme des menaces existentielles contre un objet de référence, en l'occurrence les protocoles et les normes Internet.

I. L'intérêt du sujet

La convergence actuelle entre les TIC et les préoccupations en matière de sécurité contraste fortement avec l'idée que les TIC constituent une « autoroute de l'information » porteuse d'opportunités économiques, comme l'avait annoncé le président Bill Clinton dans les années 1990. Dans ce contexte, la Chine était un marché prometteur pour les entreprises américaines après la fin de la guerre froide. La coopération sino-américaine a été essentielle pour permettre le développement de l'infrastructure chinoise des TIC et a également apporté des rendements supérieurs à la moyenne aux investisseurs américains, qui ont contribué à la recherche et au développement ainsi qu'à l'innovation aux États-Unis. Toutefois, en moins de deux décennies, les télécommunications et la technologie mobile sont devenues les premiers domaines bien établis de litiges liés aux TIC entre les États-Unis et la Chine.

La théorie de la sécurisation, formulée par l'école d'études de sécurité de Copenhague, cherche à comprendre pourquoi et comment un problème est identifié comme une question de sécurité, ainsi que les effets de ce processus sur la vie et la politique d'une communauté[1]. Selon cette théorie, les menaces pour la sécurité ne sont pas objectives, mais formulées au moyen d'un discours. La sécurisation se réfère à un processus par lequel les questions sont formulées par des agents de sécurisation comme des menaces existentielles contre un objet référent. La conséquence la plus importante de l'identification d'une question de sécurité est qu'elle devient prioritaire et urgente par

[1] T. Balzacq, S. Léonard and J. Ruzicka, "Securitization revisited: theory and cases," *International Relations* 30 4 (2016).

rapport à d'autres questions de l'agenda public, nécessitant des mesures d'urgence et justifiant des actions en dehors des limites normales de la procédure politique [2].

Pour l'école de Copenhague, la sécurisation est donc un processus de « création de sens ancré dans la pratique politique[3] ». Les agents de sécurisation formulent des actes de langage de sécurisation qui ont une force illocutoire. En d'autres termes, dire « sécurité », c'est faire de la sécurité. Grâce aux « actes de langage sécurisants », les menaces sont représentées et reconnues[4]. La théorie de la sécurisation vise à comprendre les actions de sécurisation, sur le plan politique et discursif, afin de pouvoir les désacraliser dans la mesure du possible.

La théorie de la sécurisation s'est développée dans le contexte d'un double processus d'élargissement et d'approfondissement de l'agenda sécuritaire. De nouvelles sources d'insécurité sont apparues ou ont été accentuées en tant qu'externalités négatives produites par l'interdépendance et la mondialisation, telles que la criminalité transnationale organisée, les problèmes environnementaux et les effets en cascade de l'instabilité financière[5]. Le programme des études sur la sécurité internationale a été élargi, représentant une réponse évolutive aux pressions provenant de l'environnement politique mondial. Dans ce contexte, la théorie de la sécurisation a soutenu l'élargissement du champ de la sécurité en allant au-delà d'une approche de la sécurité centrée sur l'État et militarisée, mais a cherché à circonscrire la sécurité à cinq « secteurs de sécurité », dans lesquels les menaces posées à certains objets référents pouvaient être clairement identifiées : militaire, politique, économique, sociétal et environnemental[6].

Buzan et Wæver se sont particulièrement concentrés sur le développement de la théorie de la sécurisation au-dessus de l'État, au niveau du système international. Ils ont inventé le terme de « macro-sécurisation » pour désigner les situations dans lesquelles plusieurs processus de sécurisation sont regroupés sous l'égide d'un ordre supérieur de sécurisation, qui « s'incarne de

[2] B. Buzan, O. Wæver and J. de Wilde, *Security: A New Framework for Analysis* (London: Lynne Rienner Publishers, 1998), 23-4.
[3] J. Nyman, "Securitization" In P. D. Williams and M. McDonald (eds.), *Security Studies: an Introduction* (Abingdon and New York: Routledge, 2018), 100.
[4] M. C. Williams, "Words, Images, Enemies: Securitization and International politics," *International Studies Quarterly* 47 4 (2003).
[5] M. Z. Butler and Z. Wolf, "Introduction: Revisiting securitization and the 'constructivist turn' in security studies" In M.J. Butler (ed.), *Securitization Revisited: Contemporary Applications and Insights* (London and New York: Routledge, 2020).
[6] B. Buzan and L. Hansen, *The Evolution of International Security Studies* (Cambridge: Cambridge University Press, 2009).

manière à incorporer, aligner et classer les sécurisations plus partielles qui lui sont subordonnées[7] ».

Chaque dimension de la sécurité -militaire, politique, économique, sociétale et environnementale- a des objets de référence différents et des manières différentes d'organiser les priorités. Cela signifie que la notion de « menace existentielle » et de « mesures d'urgence » sera différente dans chacun de ces domaines. Les menaces existentielles ne peuvent donc être comprises qu'en fonction de l'objet référent en question.

II. Les questions de recherche

Sur cette toile de fond théorique, la première question principale abordée par cette recherche est de savoir s'il existe un processus continu de sécurisation des TICS dans le contexte des relations sino-américaines. Dans l'affirmative, la première question secondaire est de savoir si ce processus de sécurisation peut être situé dans l'un des secteurs de la sécurité identifiés par l'école de Copenhague, ou si les TICS constituent un nouveau champ de mise en œuvre de la sécurisation. L'hypothèse initiale est que la sécurisation a lieu dans le contexte des TICS et ne peut être placée dans l'un des secteurs existants, ce qui nécessite une adaptation de la théorie de la sécurisation.

Le mouvement de sécurisation est une pratique intersubjective, et la dimension performative de cet acte repose entre la sémantique de l'acte de discours sécurisant et les circonstances contextuelles de l'auditoire[8]. Il existe deux « conditions facilitatrices[9] » qui influencent le succès d'une action de sécurisation : le contexte, qui peut être compris comme des facteurs extérieurs à l'action de sécurisation elle-même, et les structures linguistiques internes du discours de sécurisation, qui doivent suivre ce que Buzan et al. appellent « la grammaire de la sécurité[10] ».

Le contexte de la tendance actuelle à la sécurisation des TICS est l'histoire des relations bilatérales sino-américaines. Selon Shambaugh, les Américains ont une série d'images

[7] B. Buzan and O. Wæver, "Macrosecuritizations and security constellations: reconsidering scale in securitization theories," *Review of International Studies* 35 (2009): 253.
[8] Balzacq, Léonard and Ruzicka, "Securitization revisited," 504.
[9] Buzan, Wæver and Wilde, *Security, 32.*
[10] Buzan, Wæver and Wilde, *Security, 32.*

dichotomiques « amour/haine » de la Chine et pour leur part, les Chinois ont des images tout aussi ambivalentes des États-Unis[11].

L'ambivalence se reflète dans les cycles récurrents d'amitié et d'inimitié qui caractérisent les relations sino-américaines depuis la fin du XIX[e] siècle[12]. L'étude de cette « altérité » mutuelle est importante car elle crée les conditions nécessaires à l'examen des discours amis/ennemis qui font partie de la structuration de la sécurité. Pour réussir, les actes de langage doivent être acceptés par le public, et une menace existentielle crédible sous la forme d'un ennemi est le recours narratif le plus efficace.[13]

Du point de vue de la Chine, les conséquences des guerres de l'opium ont fait naître la crainte d'une menace existentielle et la conviction que l'affaiblissement de la Chine répondait aux intérêts occidentaux. Cette crainte, qui a alimenté les positions anti-impérialistes et anti-hégémoniques de la Chine, a été ramenée à la surface par le pivot américain vers l'Asie. Les perceptions américaines de la Chine ont été forgées sous l'influence significative de la peur de l'Occident à l'égard du « peuple jaune ». La notion de « péril jaune » imminent a traversé les siècles en Occident et s'est incarnée dans différents récits, allant d'une « minorité modèle » représentant une menace pour les emplois américains à une « menace chinoise » liée à la criminalité et au vol de propriété intellectuelle. Au XXI[e] siècle, une version actualisée du « péril jaune », qui met l'accent sur l'utilisation potentiellement abusive de la technologie, fait partie intégrante des relations sino-américaine[14]. Comprendre la façon dont ce thème se métamorphose en différentes variations peut créer les conditions nécessaires à l'examen des discours amis/ennemis et à l'identification des récits de macro-sécurisation qui font partie de la structuration de la sécurité dans le contexte d'un équilibre mondial des pouvoirs.

Le contexte des relations bilatérales facilite l'élaboration de récits de menaces au niveau politique. La deuxième question principale de la recherche est de savoir si un processus de « macro-sécurisation » est en cours dans le contexte des relations sino-américaines et, dans l'affirmative, la deuxième question secondaire vise à identifier les principaux éléments du discours de sécurisation. L'hypothèse est que les récits de macro-sécurisation sont créés à la

[11] D. Shambaugh, *Beautiful Imperialist: China perceives America, 1972-1990* (Princeton: Princeton University Press, 1991), 3.
[12] Shambaugh, *Beautiful Imperialist,* 3.
[13] Huysmans, "The Question of the Limit".
[14] L. Siu and C. Chun, "Yellow Peril and Techno-orientalism in the Time of Covid-19: Racialized Contagion, Scientific Espionage, and Techno-Economic Warfare," *Journal of Asian American Studies* 23 3 (2020).

fois par les États-Unis et par la Chine. Du point de vue des États-Unis, la macro-sécurisation est motivée par la perception d'un équilibre des forces en présence, mais elle est alimentée par des opinions bien ancrées sur le « péril jaune ». Du point de vue de la Chine, elle est motivée par la perception d'une vulnérabilité accrue, mais elle est historiquement alimentée par une position anti-hégémonique.

Afin de comprendre la dynamique de la sécurisation, les chercheurs ont souvent recours à l'application empirique de la théorie de la sécurisation à des questions ou des cas spécifiques[15]. Cette approche est utile car elle fournit à l'analyste des focales théoriques puissantes pour éclairer des événements particuliers, tout en permettant aux événements du cas d'élargir la théorie, d'affiner ses principaux éléments constitutifs et d'identifier les lacunes. Deux cas ont été sélectionnés pour l'analyse. Le premier cas concerne les restrictions imposées par le gouvernement américain en matière de commerce avec Huawei et de déploiement des produits et services de Huawei aux États-Unis. Le deuxième cas est lié à la proposition d'un nouveau protocole Internet (« New IP ») introduite par le gouvernement chinois, Huawei et d'autres entreprises de télécommunications chinoises au sein de l'Union internationale des télécommunications (UIT).

III. La méthodologie et le corpus

L'analyse de la sécurisation dans le contexte des études de cas sélectionnées est basée sur l'analyse qualitative du discours contenu dans un échantillon de documents écrits, afin d'identifier les actes de langage clés. Six éléments caractérisant la sécurisation structurent l'analyse des documents sélectionnés : la menace existentielle ; l'objet référent auquel s'applique la menace ; le geste sécurisant dans l'acte de langage (la grammaire de la sécurité) ; l'acteur sécurisant ; le public du geste sécurisant ; et les mesures adoptées dans le cadre de ce geste.

Une grille de codage a été élaborée pour mettre en corrélation les catégories suivantes : 1) les éléments fournis par la théorie de la sécurisation ; 2) les variables, qui se réfèrent aux manières spécifiques dont ces éléments peuvent apparaître dans le discours ; 3) des exemples tirés des textes analysés, qui montrent comment les éléments et les variables ont pris la forme de discours prononcés, au moyen d'une sélection de citations littérales. Les grandes lignes de la grille se trouvent en annexe I (modèle de grille pour l'analyse du discours).

[15] Balzacq, Léonard and Ruzicka, “Securitization revisited,” 503.

L'échantillon de documents écrits constitue le principal corpus identifié pour la recherche. Étant donné que l'État est le principal responsable de l'usage de la force et du maintien de la sécurité, et qu'il dispose souvent de règles explicites concernant les personnes autorisées à parler en son nom, le gouvernement (autorisé à parler au nom de l'État) est souvent l'un des acteurs les plus efficaces en matière de sécurisation. Dans ce contexte, dans le cas 1 (Huawei), la sélection des documents à analyser met l'accent sur la capture du discours produit par le gouvernement américain. Dans le cas 2 (nouveau protocole IP), la proposition initiale a été présentée conjointement par Huawei, China Mobile, China Unicom et le ministère chinois de l'industrie et des technologies de l'information (MIIT). Bien que le MIIT n'apparaisse pas en tant qu'auteur des documents ultérieurs, la cohérence de fond des documents ultérieurs avec la proposition initiale demeure.

Dans le cas des restrictions imposées à Huawei, quatre documents produits par le gouvernement américain ont été sélectionnés : 1) US House of Representatives Permanent Select Committee on Intelligence "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications" (Rapport d'enquête sur les problèmes de sécurité nationale posés par les télécommunications chinoises aux États-Unis). National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE" (8 octobre 2012) (annexe II) [16] ; 2) le décret 13873, émis par l'ancien président Trump (mai 2019) et confirmé par le président Biden (annexe III) [17] ; 3) les transcriptions de l'audition "Commanding Heights : ensuring U.S. leadership in the critical emerging technologies of the 21st Century", tenue par la commission spéciale de la Chambre des représentants sur le renseignement (US House Select Committee on the Strategic Intelligence) (annexe IV) [18] ; 4) une lettre signée par quatorze présidents de commissions de la Chambre des représentants et adressée à Alan Estevez, sous-secrétaire du ministère américain du commerce (septembre 2023) (Annexe V) [19].

Dans le cas du « New IP », trois documents proposés par des acteurs chinois ont été sélectionnés pour analyse : 1) Huawei Technologies Co. Ltd. (Chine) ; China Mobile

[16] U.S. House of Representatives Permanent Select Committee on Intelligence "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE".
[17] U.S. Executive Office of the President E.O. 13873 of May 15, 2019 "Securing the Information and Communications Technology and Services Supply Chain".
[18] US House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, "Commanding Heights: ensuring U.S. leadership in the critical emerging technologies of the 21st Century," Transcripts from the hearing (26 July 2023).
[19] M. T. McCaul *et. al*., Letter sent to Alan Estevez, Under Secretary U.S. Department of Commerce (14 September 2023).

Communications Corporation ; China Unicom ; Ministère de l'industrie et des technologies de l'information (MIIT), "New IP, Shaping Future Network : Propose de lancer la discussion sur la transformation de la stratégie pour l'UIT-T" (septembre 2019) (Annexe VI)[20] ; 2) Huawei, "A Brief Introduction about New IP Research Initiative", publié en ligne par Huawei (sans date) (Annexe VII) [21] ; 3) "Supporting contribution to the two contributions submitted into the July 2020 SG13 meeting, which propose text amendments to the terms of reference of, respectively, draft questions F and G of SG13 (Q. F/13 et Q.G/13) pour la prochaine période d'étude du SG13" (juillet 2020) soumise par China Telecom, China Mobile et Huawei (Annexe VIII) [22].

La sécurisation est intersubjective, construite entre l'acteur qui sécurise et le public. Hansen affirme que le public n'a pas d'existence a priori, mais qu'il ne peut être défini que dans le contexte d'une relation de communication entre l'acteur qui sécurise et les acteurs auxquels il s'adresse[23]. Dans ce contexte, un échantillon de réactions du public au discours américain (cas 1) et au discours chinois (cas 2) a été sélectionné. Outre la réaction de la Chine au discours américain (cas 1) et la réaction des États-Unis au discours chinois (cas 2), les réactions du secteur des affaires et de la communauté technique -deux acteurs essentiels à l'adoption de pratiques de sécurisation- ont également été prises en compte.

Dans le cas des restrictions imposées à Huawei, dix documents contenant des réactions au discours américain ont été sélectionnés pour analyse : 1) une déclaration de 2019 publiée par l'ancien vice-président exécutif et chef des affaires internationales de la Chambre de commerce des États-Unis, Myron Brilliant, "U.S Chamber Statement on Escalating Tensions in U. S-China Trade" (19 août 2019) (annexe IX) [24] ; 2) "Comments in the Matter of 'Request for Comments on Future Extensions of Temporary General License (TGL)" par GSMA (25 mars 2020) (annexe X) [25] ; 3) Comments from USTelecom - The Broadband Association - on the matter of

[20] Huawei Technologies Co. Ltd. (China); China Mobile Communications Corporation; China Unicom; Ministry of Industry and Information Technology (MIIT) "New IP, Shaping Future Network: Propose to Initiate the Discussion of Strategy Transformation for ITU-T," Proposal to ITU-T TSAG (September, 2019). Available at http://prod-upp-image-read.ft.com/ec34d7aa-70e6-11ea-95fe-fcd274e920ca
[21] Huawei Technologies, "A Brief Introduction about New IP Research Initiative," Huawei United States (no date).
[22] China Telecom, China Mobile, and Huawei, "Supporting contribution to the two contributions submitted into the July 2020 SG13 meeting, which propose text amendments to the terms of reference of, respectively, draft questions F and G of SG13 (Q.F/13 and Q.G/13) for the next study period of SG13," SG13-C996, Virtual meeting (20-31 July 2020).
[23] L. Hansen, *"*The politics of securitization and the Muhammad cartoon crisis: A post-structuralist perspective," *Security Dialogue* 42 (2011): 360.
[24] M Brilliant, "U.S Chamber Statement on Escalating Tensions in U.S-China Trade," U.S. Chamber of Commerce (19 August, 2019).
[25] GSMA, "Comments in the Matter of 'Request for Comments on Future Extensions of Temporary General License (TGL)" (25 March 2020).

Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs (février 2020) (annexe XI) [26] ; 4) "Statement Regarding Engagement with Companies Added to the U.S. Export Administration Regulations (EAR) Entity List in 3GPP Activities" par le 3rd Generation Partnership Project (3GPP) (novembre 2019) (annexe XII) [27] ; 5) un courriel sur la "Compliance with Recent U.S. Export Regulations" envoyé par Jason Livingood au nom du conseil d'administration de l'Internet Engineering Task Force (IETF) LLC (mai 2020) (annexe XIII) [28] ; 6) 1) "Huawei Open Letter" par Ken Hu, vice-président de Huawei Technologies et président de Huawei USA (2011) (annexe XIV) [29] ; 7) "Huawei Statement regarding HPSCI's report," (8 octobre 2012) (annexe XV) [30] ; 8) "Huawei Statement on US Justice Department Indictment" (14 février 2020) (annexe XVI) [31] ; 9) les points de vue exprimés par les porte-parole du ministère chinois des affaires étrangères, Mao Ning[32], Hua Chunying[33] et Wang Wenbin[34], lors de conférences de presse régulières, lorsqu'ils ont été interrogés par les médias (voir annexe XVII) ; 10) la déclaration du ministère des affaires étrangères, intitulée "Reality Check : Falsehoods in US Perceptions of China" , qui aborde la question de Huawei (annexe XVIII) [35].

Dans le contexte de l'affaire du nouveau protocole IP, cinq documents contenant des réactions au discours de la Chine ont été sélectionnés pour analyse : 1) "Proposed Way Forward on Tentative New Questions, Q.F/13 and Q. G/13" (juillet 2020) proposé par les États-Unis (annexe XIX) [36]; 2) "Input on Proposals and Positions for the 2020 World Telecommunication

[26] USTelecom, Comments from USTelecom – The Broadband Association in the matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs (February 2020).
[27] 3rd Generation Partnership Project (3GPP) "Statement Regarding Engagement with Companies Added to the U.S. Export Administration Regulations (EAR) Entity List in 3GPP Activities", SA WG2 Meeting 136 (18 - 22 November, 2019).
[28] J. Livingood, "Compliance with Recent U.S. Export Regulations," IETF LCC Board (30 May 2019).
[29] Ken Hu, Huawei Open Letter (2011).
[30] Huawei, "Huawei Statement regarding HPSCI's report," CNBC (8 October 2012).
[31] Huawei, "Huawei Statement on US Justice Department Indictment" (14 February 2020).
[32] Ministry of Foreign Affairs of the People's Republic of China "Foreign Ministry Spokesperson Mao Ning's Regular Press Conference (20 September, 2023); Ministry of Foreign Affairs of the People's Republic of China Foreign Ministry Spokesperson Mao Ning's Regular Press Conference (31 January 2023); Ministry of Foreign Affairs of the People's Republic of China Foreign Ministry Spokesperson Mao Ning's Regular Press Conference (30 January 2023);
[33] Ministry of Foreign Affairs of the People's Republic of China Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on July 16, 2020 http://mz.china-embassy.gov.cn/por/fyrth/202007/t20200716_6728336.htm
[34] Ministry of Foreign Affairs of the People's Republic of China Foreign Ministry Spokesperson Wang Wenbin's Regular Press Conference (25 September 2023);
[35] Ministry of Foreign Affairs of the People's Republic of China Reality Check: Falsehoods in US Perceptions of China (19 June 2022). Available at: https://www.mfa.gov.cn/eng/wjbxw/202206/t20220619_10706059.html
[36] United States of America, "Proposed Way Forward on Tentative New Questions, Q.F/13 and Q.G/13," SG13-C1057 (20-31 July 2020).

Standardization Assembly", produit par la National Telecommunications and Information Administration (NTIA) du ministère américain du commerce (mai 2020) (annexe XX) [37] ; 3) "Comments of the Telecommunications Industry Association," Before the National Telecommunications and Information Administration in the Matter of Input on Proposals and Positions for the 2020 World Telecommunication Standardization Assembly (8 juin 2020) (annexe XXI) [38] ; 4) "Next Steps for proposed work on 'New IP'" un document introduit conjointement par plusieurs pays européens, la Commission européenne, la GSMA, et le RIPE-NCC (juillet 2020) (annexe XXII) [39] ; 5) "Liaison Statement : Response to LS on New IP, Shaping Future Network" par l'IETF (mars 2020) (annexe XXIII) [40].

IV. L'organisation de la thèse

La recherche est divisée en trois parties. La première partie est consacrée à l'établissement du cadre théorique qui soutient l'enquête et comprend trois chapitres.

Le **chapitre I** est consacré à la notion d' « équilibre » dans les relations internationales. Il montre que différentes manières de conceptualiser l' « équilibre des pouvoirs » -l'une associative et l'autre conflictuelle- sont en concurrence pour devenir le contenu associé à l'expression « équilibre ». La prédominance d'un contenu contradictoire dans les discussions sur l'« équilibre des pouvoirs » dans les relations internationales occidentales trouve son expression la plus connue dans la théorie de l'« équilibre des menaces ». S'appuyant sur la notion occidentale d'un équilibre associatif des pouvoirs, ce chapitre explore la possibilité que le « tournant relationnel » qui s'opère dans les théories des relations internationales occidentales et non occidentales puisse éclairer les discussions sur l' « équilibre », en permettant à l'équilibre entre les pays d'être formulé de manière non conflictuelle. Il examine en particulier la notion

[37] National Telecommunications and Information Administration [NTIA], "Input on Proposals and Positions for the 2020 World Telecommunication Standardization Assembly," Federal Register 85, no. 90 (08 May 2020), 27390. Available at: https://www.govinfo.gov/content/pkg/FR-2020-05-08/pdf/2020-09835.pdf

[38] Telecommunications Industry Association (TIA), "Comments of the Telecommunications Industry Association," Before the National Telecommunications and Information Administration In the Matter of Input on Proposals and Positions for the 2020 World Telecommunication Standardization Assembly (8 June 2020). Available at: https://www.ntia.gov/sites/default/files/publications/tia-06082020_0.pdf

[39] Austria, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, GSMA, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, RIPE-NCC, Romania, Slovakia, Spain, Sweden and United Kingdom, "Next Steps for proposed work on 'New IP'," SG13-C971-R2 (20-31 July 2020).

[40] Internet Engineering Task Force (IETF), "LS on New IP, Shaping Future Network," Liaison Statement between the IETF and the ITU-TSAG (30 March 2020). Available at: https://datatracker.ietf.org/liaison/1677/

d'« équilibre des relations », en identifiant les différences et les similitudes avec la théorie de l'« équilibre des pouvoirs ».

Le **chapitre II** place l'analyse de l'équilibre des pouvoirs dans le cadre d'un ordre mondial interdépendant, en s'appuyant sur la théorie de l'interdépendance développée par Keohane et Nye. Les parties interdépendantes ont une relation permanente entre elles et les caractéristiques de cette relation influenceront fortement la réaction d'un pays à une situation d'interdépendance asymétrique. Elles influenceront également la décision du pays de maintenir ou d'affaiblir les liens structurels avec son environnement. L'État est décomposé en sous-systèmes sociaux - politique, juridique, économique et technique- ce qui permet d'intégrer dans l'analyse la complexité et les arrangements en réseau.

Le **chapitre III** donne un aperçu de la théorie de la sécurisation élaborée dans les années 1990 par l'École de sécurité de Copenhague et la situe dans le contexte plus large des études sur la sécurité internationale. La sécurisation est également analysée du point de vue des théories critiques, qui ont contribué à améliorer et à renforcer les piliers théoriques de la sécurisation. Une perspective relationnelle est utilisée pour critiquer la dyade schmittienne ami/ennemi qui sous-tend la théorie de la sécurisation.

La partie II, organisée en quatre chapitres, se concentre sur l'analyse de deux études de cas et de leur contexte culturel et historique, afin de prendre en compte les facteurs internes et externes, en mettant l'accent sur les actes de langage et les métaphores clés autour des TIC.

Le **chapitre IV** étudie les origines historiques qui influencent les perceptions de la menace mutuelle dans le contexte des relations sino-américaines. La première partie du chapitre se concentre sur la Chine et sur la manière dont la relation bilatérale avec les États-Unis s'est construite sur des bases antagonistes, fondées sur la résistance à l'impérialisme et à l'hégémonie. Cette relation a contribué à forger l'identité moderne de la Chine, non seulement en fournissant un « autre » qui contrastait avec le « soi », mais aussi par l'assimilation des caractéristiques de cet « autre », intégrées dans la quête de développement technologique et de modernisation de la Chine. La deuxième partie du chapitre se concentre sur les perceptions occidentales de la Chine. Ces perceptions ont été réélaborées au fil des ans, mais elles peuvent être reliées à la notion de « péril jaune », profondément enracinée dans un répertoire de croyances déclenchées par un « autre » différent et menaçant.

Le **chapitre V** s'appuie sur les perceptions sino-américaines de l' « autre » et analyse la traduction de ces perceptions en politiques. Il aborde l'adoption d'une position compétitive et antagoniste des États-Unis vis-à-vis de la Chine et la caractérisation de la Chine comme une menace pour les intérêts fondamentaux des États-Unis dans les domaines de la sécurité militaire, économique et politique. La deuxième partie du chapitre adopte le point de vue de la Chine et examine la perception chinoise selon laquelle les États-Unis pourraient représenter une menace pour les intérêts nationaux fondamentaux de la Chine.

Le **chapitre VI** se penche sur le cas de Huawei. Il examine la formation et l'évolution du lien entre Huawei et la sécurité nationale sur la scène politique américaine, ainsi que la manière dont les États-Unis et la Chine sont entrés dans une bataille d' « armes légales[41] », dans laquelle les restrictions à l'exportation jouent un rôle clé. La deuxième partie du chapitre est consacrée à l'analyse du discours sur la base des éléments clés proposés par la théorie de la sécurisation.

Le **chapitre VII** est consacré à l'étude de cas sur la « nouvelle proposition de protocole internet » ou « New IP ». Basé sur l'idée de Lawrence Lessig selon laquelle « le code est loi[42] » et sur les travaux de Martha Finnemore et Kathryn Sikkink sur la diffusion des normes[43], ce chapitre aborde la force normative des protocoles et le rôle des acteurs techniques en tant qu' « entrepreneurs de normes ». Il analyse également les actes de langage produits par les promoteurs du nouveau protocole IP de 2019-2020, ainsi que les réactions à cette proposition.

La partie III, composée d'un seul chapitre interprétatif, tente de répondre aux questions de recherche initiales à travers le prisme des résultats des études de cas et offre quelques perspectives théoriques renouvelées sur la sécurisation.

Le **chapitre VIII** identifie les aspects de la théorie de la sécurisation qui ont été particulièrement utiles dans l'analyse des études de cas, tout en soulignant leurs forces et leurs limites. Il examine les principales conclusions des études de cas, liées à la macro-sécurisation des relations sino-américaines et à la sécurisation des TICS. Il examine si la sécurisation des

[41] Xi Jinping, "Strengthen the Party's leadership in comprehensively governing the country according to law," Qiushi (15 February 2019) [original title: 加强党对全面依法治国的领导] Available at: http://www.qstheory.cn/dukan/qs/2019-02/15/c_1124114454.htm
[42] L. Lessig, *Code: version 2.0*. (New York: Basic Books, 2006).
[43] M. Finnemore and K. Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52 4 (1998).

TICS peut être incluse dans le cadre de la cybersécurité, selon les critères proposés par Hansen et Nissenbaum[44].

V. Les principaux résultats

Les principaux résultats confirment le pouvoir explicatif du processus de sécurisation dans les relations sino-américaines (QR1). Ils montrent également le nouveau processus de macrosécurisation à l'œuvre, la Chine et les États-Unis présentant des discours mondiaux concurrents dans leur lutte systémique pour l'hégémonie dans le domaine des TICS (QR2). L'enjeu particulier des protocoles et des normes Internet à l'œuvre dans les deux études de cas montre l'évolution rapide des relations internationales dans le domaine des TICS.

Trois grandes tendances émergent suite à l'analyse des deux études de cas, mises dans leur contexte historique, géo-politique et juridique dans les chapitres IV à VII, et discutées dans le chapitre VIII.

V.1 Les focales théoriques de la sécurisation : forces et limites

Les études de cas montrent deux types différents mais complémentaires de mesures de sécurisation prises par les États-Unis et la Chine. L'étude de cas consacrée à Huawei montre un processus de sécurisation qui correspond largement à la théorie de la sécurisation élaborée par l'école de Copenhague. Les objets référents ont été clairement identifiés, la « menace existentielle » a été explicitement reconnue et la grammaire de la sécurité a été bien articulée au moyen d'une position d'opposition à un Autre menaçant, qui nécessite l'adoption de mesures urgentes et exceptionnelles. La déclaration d'urgence nationale par le décret 13873 est un acte de langage classique[45]. Comme le prévoit la théorie, une personne habilitée à « parler de sécurité » -le président des États-Unis- prononce un acte illocutoire, établissant ainsi l'état d'urgence national.

Dans l'étude de cas sur Huawei, les approches critiques de la théorie de la sécurisation sont utiles pour expliquer le rôle complémentaire que les pouvoirs législatif et exécutif américains ont joué dans la sécurisation des TIC dans le contexte des relations sino-américaines. Les auditions et les enquêtes du Congrès donnent l'occasion aux membres du Congrès et à certains

[44] L. Hansen and H. Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly* 53 (2009).
[45] Executive Order 13873 of 15 May 2019, Establishing "Securing the Information and Communications Technology and Services Supply Chain".

témoins d'exprimer leurs préoccupations. Le discours qu'ils créent joue un rôle clé dans la formulation de la grammaire de la sécurité qui soutiendra la législation du Congrès et de l'exécutif.

Parallèlement, l'exécutif américain détient un pouvoir important sur la politique étrangère et la sécurité nationale, et décide en dernier ressort d'adopter ou non le récit produit par le Congrès. Les présidents américains Trump et Biden ont utilisé les récits du Congrès comme soutien politique pour déclarer une situation d'urgence nationale en ce qui concerne les TICS. En fin de compte, cette déclaration tire sa force juridique d'une autorisation plus large du Congrès, inscrite dans la NEA et l'IEEPA, qui a accordé à l'exécutif un contrôle exceptionnel sur les transactions économiques internationales privées.

Contrairement à ce que prévoyait l'école de Copenhague, l'étude de cas sur Huawei montre que la sécurisation s'effectue sans rupture totale avec la normalité, mais dans les limites des lois et des procédures établies. La sécurisation ne doit donc pas seulement être comprise comme une politisation extrême qui fait sortir la question de la politique, mais elle peut aussi opérer à la frontière de la politique[46]. Les deux branches du gouvernement américain ont collaboré conjointement pour réglementer l'état d'exceptionnalisme et l'inscrire dans les pratiques adoptées par l'ensemble du gouvernement américain. La lettre des quatorze présidents des commissions de la Chambre des représentants cherche à institutionnaliser l'« exceptionnalisme » en demandant la création d'une autorité de sanction dans le cadre de l'IEEPA, axée sur les entreprises chinoises qui font fi des contrôles technologiques américains[47].

L'étude de cas consacrée au « New IP » révèle les limites de la théorie originale de la sécurisation, l'importance des perspectives ajoutées par les approches critiques de la théorie et les domaines dans lesquels des lacunes théoriques subsistent. Tout d'abord, l'étude de cas révèle comment les perceptions du continuum entre les questions non politisées/politisées/sécurisées peuvent être perturbées dans la pratique, en particulier dans les discussions sur les questions techniques, qui sont souvent étiquetées comme politiquement neutres[48].

La notion de « sécurité intrinsèque » contenue dans la nouvelle proposition de protocole internet montre comment l'association entre les questions techniques et la neutralité peut être

[46] Nyman, "Securitization," 104.
[47] McCaul *et. al*., Letter sent to Alan Estevez, Under Secretary U.S. Department of Commerce
[48] M. Thompson, "The Neutralization of Harmony: The Problem of Technological Neutrality, East and West," *Boston University Journal of Science and Technology Law* 18 2 (2012).

trompeuse. Dans la nouvelle proposition IP, la sécurité serait intégrée dans le code du réseau. Cela montre que les auteurs de la proposition sont conscients du fait que « le code est loi[49] » et qu'il peut être utilisé pour limiter les comportements ou, comme le mentionne la contribution de New IP, « pour renforcer la confiance dans l'infrastructure ». Néanmoins, Huawei nie faire la « politique des protocoles[50] ».

Cette tendance à la neutralité aide à comprendre le fait que le discours de la Chine manque de marqueurs clairs qui indiqueraient un objectif de sécurisation. Son discours ne vise pas à promouvoir une politisation accrue, il représente plutôt une tentative d'esquiver la nature politique des décisions relatives aux protocoles. Cette attitude est similaire aux tendances à la dépolitisation et à l'« innocence artificielle » identifiées par Cath-Speth dans les travaux de l'IETF, caractérisés par « une position délibérément et socialement construite d'irréprochabilité pour les conséquences dans le monde réel des décisions prises dans le contexte du développement de la technologie[51] ». Cette attitude résonne également avec la position déclarée des États-Unis selon laquelle les normes sont « un terrain de jeu neutre ».[52]

La démarche de sécurisation de la Chine ne peut être comprise sans considérer que le code est une loi et que les ingénieurs sont des entrepreneurs de normes. Cela atteste de la nécessité d'élargir la théorie de la sécurisation au-delà de l'acte de langage afin d'accepter différentes manières de promouvoir la sécurisation, y compris par le biais de normes et de protocoles. Les discussions sur la sécurisation favorisée par les algorithmes se sont concentrées sur la manière dont les algorithmes ont facilité l'accomplissement des pratiques de sécurité, telles que la surveillance et la police prédictive[53], mais elles n'ont pas exploré la manière dont l'élaboration de normes et le codage peuvent générer une architecture qui facilite (ou crée un obstacle) à ces utilisations de la technologie axées sur la sécurité.

En plaçant les deux études de cas ensemble sous un angle plus précis, on obtient des indications sur les similitudes et les différences concernant la manière dont les gouvernements, le secteur privé et les acteurs techniques s'engagent dans les principaux éléments de la sécurisation. Dans les deux études de cas, la menace perçue par le pays qui formule l'initiative de sécurisation (les

[49] Lessig, *Code*, 79.
[50] DeNardis, *Protocol Politics.*
[51] Cath-Speth, "Changing Minds and Machines", 18.
[52] The White House, "United States Government National Standards Strategy for Critical and Emerging Technologies".
[53] L. Amoore and R. Raley, "Securing with Algorithms: Knowledge, Decision, Sovereignty," *Security Dialogue* 48 1 (2017).

États-Unis dans le cas de Huawei et la Chine en ce qui concerne le nouveau protocole IP) est rejetée par l'autre pays.

Parallèlement, les États-Unis et la Chine cherchent à redéfinir la menace dans leurs propres termes. Par exemple, dans le cas des restrictions imposées à Huawei, le gouvernement chinois et Huawei réfutent l'idée que l'entreprise représente une menace pour la sécurité nationale des États-Unis, tout en accusant les États-Unis de constituer une menace pour l'ordre économique en adoptant des mesures discriminatoires qui restreignent le commerce et perturbent les chaînes de valeur mondiales. Le MAE chinois souligne en outre la menace que les pratiques hégémoniques des États-Unis font peser sur l'ordre politique international, fondé sur l'égalité souveraine entre les États.

Les perceptions différentes et contradictoires de la source réelle des menaces dans l'affaire Huawei ont incité les deux pays à adopter des approches antagonistes. Dans le cas du « New IP », en revanche, les acteurs chinois n'ont pas adopté de position contradictoire, ce qui corrobore leur intention de ne pas politiser la question et de l'aborder sous l'angle de la neutralité technologique.

Les positions de Huawei et du gouvernement chinois n'ont pas toujours été alignées. L'entreprise a d'abord adopté une approche non contradictoire dans le contexte des restrictions commerciales dont elle faisait l'objet, attribuant les positions américaines à des « perceptions erronées » -qui pouvaient donc être corrigées- et cherchant à établir une « ressemblance mutuelle » avec les États-Unis en affirmant que « Huawei n'est pas différente de n'importe quelle entreprise en démarrage dans la Silicon Valley ». La ressemblance imaginée est un moyen important de gérer les différences dans les relations dans la culture chinoise, en permettant l'émergence d'une identité collective imaginée et en facilitant le développement de relations équilibrées[54]. La Silicon Valley est devenue un symbole important dans l'imagerie américaine, et l'analogie choisie par Huawei l'évoque donc de manière significative.

La publication du rapport 2012 de la HSPCI a modifié le ton conciliant de Huawei. L'entreprise a remplacé les termes « malentendu » et « perception erronée » par des affirmations selon lesquelles des « rumeurs » intentionnelles étaient diffusées à son sujet. Huawei a accusé les États-Unis d'être motivés par un comportement anticoncurrentiel et le protectionnisme, plutôt

[54] Shih et al, *China and International Theory.*

que par des préoccupations de sécurité nationale[55], et a affirmé que « nous devons soupçonner que le seul but d'un tel rapport est d'entraver la concurrence et d'empêcher les entreprises chinoises de TIC d'entrer sur le marché américain[56] ». Le durcissement des mesures américaines a donc été décisif pour faire basculer Huawei dans le camp adverse.

La contribution d'USTelecom résume ce qui semble être un point de vue largement répandu dans le secteur privé : les décisions gouvernementales prises pour protéger la sécurité nationale sont soutenues pour autant qu'il s'agisse de décisions coordonnées qui atténuent l'incertitude et la confusion en adoptant une approche pangouvernementale et qui prennent en compte les points de vue du secteur privé[57].

Dans le cas du nouveau protocole IP, les acteurs privés et techniques occidentaux se sont opposés à tout changement qui affecterait le rôle de l'IETF en tant que « foyer naturel » de l'élaboration des normes Internet, et qui introduirait une « exceptionnalité » dans les discussions relatives à l'IP. Ils ont défendu le rôle central de l'IETF, ses méthodes de travail et son approche évolutive des normes Internet. Les acteurs privés et techniques occidentaux ont adopté une approche comparativement plus conflictuelle à l'égard des acteurs chinois dans l'affaire « New IP », alors que leur position était moins conflictuelle dans l'affaire relative aux restrictions imposées à Huawei. Cela s'explique probablement par les interdépendances complexes entre les États-Unis et la Chine dans le secteur des télécommunications et par la perte d'opportunités commerciales qu'entraîne la limitation des échanges avec Huawei. Dans le contexte du nouveau protocole IP, l'intérêt de ces acteurs occidentaux à maintenir la centralité de TCP/IP et le statu quo des processus d'élaboration des normes est plus clair.

Un point commun entre les deux cas est que Huawei apparaît comme protagoniste. Ce n'est pas un hasard. Huawei est un acteur majeur dans deux couches qui sous-tendent le fonctionnement des TICS, la couche infrastructurelle, composée des télécommunications, des équipements de réseau et des logiciels, et la « couche logique » des protocoles et des normes. En outre, Huawei est devenu un symbole des prouesses technologiques chinoises et de la détermination de la Chine à rattraper et à dépasser l'Occident en termes de modernisation technologique.

[55] Huawei, "Huawei Statement regarding HPSCI's report" *CNBC* (8 October 2012).
[56] Huawei, "Huawei Statement regarding HPSCI's report".
[57] USTelecom, Comments of USTelecom Before the Federal Communications Commission, 9.

Plus profondément, les deux cas sont liés par des objectifs stratégiques symétriquement opposés : préserver ou modifier l'épicentre du désordre technologique dans le domaine des TIC. Cet épicentre a été fixé aux États-Unis par le biais d'une association public-privé entre le gouvernement américain et les pionniers techniques, qui ont promu conjointement l'expansion de l'Internet basé sur le protocole TCP/IP jusqu'aux années 1980, et entre l'administration américaine et le secteur privé dans les années 1990.

Avec le soutien du gouvernement, les champions nationaux chinois ont renforcé leur participation au déploiement de l'infrastructure mondiale. Huawei, en particulier, a commencé à modifier la topologie de l'économie mondiale en réseau. La proposition conjointe du gouvernement chinois, de Huawei et d'autres entreprises chinoises de télécommunications d'abandonner -ou du moins de mettre en veilleuse- les principaux protocoles qui ont défini l'internet (d'un point de vue technique, normatif et historique), représente une pression supplémentaire sur l'épicentre américain.

Dans la première étude de cas, cela est corroboré par le fait qu'au fur et à mesure des discussions sur Huawei, le seuil qui déclencherait une action contre l'entreprise s'est abaissé. Au lieu d'essayer d'affirmer l'existence d'une menace pour la sécurité nationale américaine, comme le suggérait le rapport de 2011, les mesures adoptées par les États-Unis se sont basées sur l'existence d'un risque. S'il existe une possibilité pour le gouvernement chinois d'utiliser à mauvais escient la technologie Huawei, ce risque est devenu suffisant pour justifier le remplacement des équipements Huawei dans les réseaux américains et la restriction des échanges avec l'entreprise. Cette affaire confirme l'importance d'ajouter la notion de risque -des menaces possibles à long terme qui peuvent être atténuées plutôt qu'éliminées[58]- au spectre de l' « exceptionnalisme » qui caractérise la sécurisation.

Dans le cas de « New IP », la proposition a été étiquetée et rejetée comme une tentative chinoise de mettre en œuvre des protocoles à « saveur autoritaire[59] », sans tenir compte du fait que les idées contenues dans la proposition n'étaient ni nouvelles ni exclusivement chinoises, mais pouvaient être retracées dans des projets de recherche sur les « futures architectures internet[60] »

[58] Kirk, “From Threat to Risk?”, 267.
[59] Caiero, McFadden and Taylor, “Standards: the new frontier”, 1.
[60] Pan, Paul and Jain, “A survey of the research on future internet architectures”.

en cours dans plusieurs pays. L'argument des valeurs a servi de substitut aux préoccupations géoéconomiques déclenchées par un changement potentiel de l'épicentre de l'internet.

V.2. Projeter la sécurisation au niveau systémique

V.2.1 la macro-sécurisation de la « menace chinoise »

Buzan et Wæver ont utilisé le concept de « macro-sécurisation » pour désigner un processus global de sécurisation qui « s'intègre de manière à incorporer, aligner et classer les sécurisations plus locales qui lui sont subordonnées[61] ». Selon eux, la principale différence entre la sécurisation et la macrosécurisation est que cette dernière se produit à plus grande échelle, regroupant les sécurisations qui se produisent au niveau des États en une menace plus élevée et plus importante pour l'ordre mondial. Cette menace sert de point de gravité qui galvanise les liens entre les différents secteurs de la sécurité, ainsi que les alliances qui sont formées pour défendre les notions d'idéologie, d'appartenance ou d'identité contre une menace perçue.

Selon Buzan, la guerre froide et la guerre mondiale contre la terreur (Global War on Terror - GWoT) ont été les récits de macro-sécurisation les plus réussis jusqu'à présent en politique internationale. Pendant la guerre froide, le récit anticommuniste a simplifié l'interaction complexe entre les États-Unis et l'Union soviétique « en une histoire simple, bipolaire et classique d'un héros capitaliste et d'un mal communiste[62] ». La menace communiste constituait une « cause commune et un cadre partagé qui sous-tendait le leadership américain sur l'Occident ». Selon Buzan, « Washington se considérait comme le représentant de l'avenir, et donc comme ayant le droit et le devoir de parler et d'agir au nom de l'humanité, et cette prétention était, jusqu'à un certain point, acceptée par une grande partie du reste de l'Occident[63] ».

Après 1989, cependant, les États-Unis ont connu un « déficit de menace[64] » en raison de l'absence d'un point focal autour duquel le récit d'une lutte mondiale pouvait être créé. Dans ce contexte, la « guerre mondiale contre le terrorisme » est apparue comme une macro-sécurisation de la « lutte à somme nulle, à l'échelle mondiale et générationnelle contre les extrémistes idéologiques antilibéraux[65] ». Ce récit a soutenu le leadership unipolaire des États-

[61] Buzan and Wæver, "Macrosecuritizations and security constellations", 253.
[62] Yuan and Fu, "Narrative Framing and the United States' Threat Construction of Rivals", 13.
[63] Buzan ,"Will the 'global war on terrorism'", 1103.
[64] Buzan, "Will the 'global war on terrorism'".
[65] Buzan, "Will the 'global war on terrorism'", 1101.

Unis, lui permettant d'être légitimement exercé[66]. Il a également servi de principe directeur à d'autres dynamiques de sécurisation, liant par exemple la « guerre contre la drogue » et la « guerre contre le terrorisme[67] ».

Bien que le GWoT soit resté une stratégie de sécurisation viable pendant quelques années, Buzan a prédit en 2006 que la « guerre contre le terrorisme » pourrait être remplacée par la « menace chinoise » en tant que récit de macro-sécurisation. En décembre 2017, les États-Unis ont officiellement qualifié la Chine, dans leur stratégie de sécurité nationale, de « puissance révisionniste » qui a l'intention de « façonner un monde contraire aux valeurs et aux intérêts des États-Unis ». Selon la SSN 2022, les démocraties et les autocraties ne sont pas seulement « engagées dans une compétition pour montrer quel système de gouvernance peut le mieux répondre aux besoins de leur peuple et du monde[68] », mais les grandes puissances autocratiques cherchent également à « façonner l'ordre international » dans le but de « créer un monde propice à leur type d'autocratie hautement personnalisé et répressif[69] ». Les documents tels que la stratégie de sécurité nationale ne sont pas seulement des instruments politiques visant à synchroniser les priorités en matière de sécurité dans l'ensemble de l'Union européenne. Il s'agit également d'artefacts de narration, qui rassemblent les discours de sécurisation dans des domaines politiques spécifiques, contribuant ainsi à construire le récit d'un affrontement.

Dans le contexte du Congrès américain, la « China Task Force » et le « Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party » ont joué un rôle important dans la production et l'amplification des récits de macro-sécurisation. Ils ont également joué un rôle dans la continuité des positions réalistes et antagonistes à l'égard de la Chine, malgré la transition politique entre les Républicains et les Démocrates en 2021.

Les principaux éléments qui indiquent une tentative d'interpréter la « menace chinoise » comme un récit de macro-sécurisation ont été bien formulés par le groupe de travail sur la Chine. Le rapport conclut que « les enjeux sont aussi urgents qu'existentiels (...) le PCC est totalement engagé dans une idéologie communiste hostile qui cherche à éliminer toute menace perçue pour sa sécurité -au premier rang desquelles les valeurs qui sous-tendent la société américaine et le

[66] Buzan, "Will the 'global war on terrorism'", 1101.
[67] M-M. Müller, "Enter 9/11: Latin America and the Global War on Terror," *Journal of Latin American Studies* 52 3 (2020); D. Corti and A. Swain, "War on Drugs and War on Terror: Case of Afghanistan," *Peace and Conflict Review* 3 2 (2009).
[68] White House, 2022 *National Security Strategy*, 7.
[69] White House, 2022 *National Security Strategy*, 7-8.

système international construit par les États-Unis[70] ». Il prédit également que « le monde libre se trouve dans un conflit irréconciliable de systèmes avec le PCC[71] ». Dans ce contexte, « s'attaquer à une telle conduite malveillante ne peut plus être l'une des nombreuses priorités de nos gouvernements respectifs, mais plutôt le principe d'organisation du monde libre[72] ».

Outre les menaces qui pèsent sur les États-Unis, les membres du Congrès ont exprimé la crainte que le PCC n'instaure un État policier totalitaire dans le monde[73], représentant une menace plus grande pour la liberté mondiale que l'Union soviétique ne l'a jamais fait[74]. En conséquence, ils perçoivent « une lutte existentielle pour savoir à quoi ressemblera la vie au XXI[e] siècle[75] », qui s'inscrit dans une compétition militaire, technologique et économique, affectant non seulement le peuple américain, mais aussi les démocraties du monde entier[76]. Comme cela a été mentionné lors d'une audition du Comité permanent sur la Chine, du point de vue des autres pays, la formation d'alliances « n'est pas un choix entre Washington et Pékin ; c'est un choix entre la souveraineté et la servitude[77] ». La commission spéciale décrit la menace systémique qui pèse sur l'ordre mondial comme un conflit entre différentes idéologies politiques, ou un affrontement entre démocraties et autocraties.

Cette polarisation schmittienne a conduit à une perception aiguë de la menace et à la promotion d'un état d'exceptionnalisme permanent. Le contrôle des politiques étrangères et de sécurité a été reporté sur l'exécutif, ce qui a permis l'adoption de mesures extraordinaires et urgentes[78]. Parmi les mesures extraordinaires introduites en temps de guerre et dont l'application a été étendue au temps de paix figure la TWEA. La TWEA a été remplacée par la NEA et l'IEEPA, qui ont fourni une justification juridique au décret 13873 sur la « sécurisation de la chaîne

[70] McCaul, China Task Force Report, 1.
[71] McCaul, China Task Force Report, 3.
[72] McCaul, China Task Force Report, 6.
[73] U.S. House of Representatives, Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, Intervention by Congressman Torres at the Hearing on "The Chinese Communist Party's Threat to America" (28 February 2023), 80.
[74] U.S. House of Representatives, Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, Intervention by General McMaster, witness at the hearing "The Chinese Communist Party's Threat to America", 83.
[75] U.S. House of Representatives, Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, Intervention by Chairman Gallagher at the hearing on "The Chinese Communist Party's Threat to America", 3.
[76] U.S. House of Representatives, Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, Intervention by Robert J. Wittman at the hearing on "The Chinese Communist Party's Threat to America", 30.
[77] U.S. House of Representatives, Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, Intervention by General McMaster, witness at the hearing on "The Chinese Communist Party's Threat to America," 45.
[78] Bolton, *The Rise of the American Security State.*

d'approvisionnement des technologies et services de l'information et de la communication », un jalon du processus de sécurisation concernant Huawei.

Comme l'a souligné M. Wæver, toutes les questions sécurisées avec succès ne seront pas nécessairement « militarisées[79] ». Néanmoins, la militarisation de la politique étrangère des États-Unis conduit à une tendance à la militarisation des questions sécurisées, en mettant en avant la « logique de guerre » dans leur discussion[80]. Cela signifie que la logique de guerre et le « mode opérationnel » de la sécurité nationale seront appliqués dans tous les secteurs de la sécurité, même si l'État n'est pas le principal objet de référence d'une menace perçue.

Cela permet d'expliquer l'affirmation selon laquelle « la sécurité économique est la sécurité nationale[81] » et la pression exercée sur le secteur privé américain pour qu'il s'aligne sur les politiques gouvernementales à l'égard de la Chine. Cela éclaire également l'utilisation récurrente de l'IEEPA pour fonder les décisions gouvernementales, montrant que la logique de guerre l'emporte sur la logique d'un ordre économique libre et libéral, qui s'est imposée depuis la fin de la guerre froide. Le puissant récit de macro-sécurisation lié à cette logique concerne le secteur des TICS, car les services internet proposent une architecture déconcentrée et horizontale qui s'apparente à la vision du monde des États-Unis. Dans ce contexte, le macro-récit de la « menace existentielle du communisme » peut s'imposer solidement.

V.2.2. Discours et pratiques contre-hégémoniques de la Chine

La Chine a réagi à la macro-sécurisation encouragée par les États-Unis de deux manières principales. La première consiste en une tentative de renforcement de son contre-récit, d'une manière qui s'aligne étroitement sur le modèle des conceptions réalistes classiques de l'équilibre. La seconde propose une sinisation de la notion de sécurité et la projette au-delà des frontières chinoises.

La perception par la Chine que les États-Unis représentent une menace pour ses intérêts nationaux fondamentaux s'est accompagnée du renforcement d'un discours anti-hégémonique. Après les guerres de l'opium, une position anti-hégémonique est devenue « indélébile dans le psychisme de la plupart des Chinois », servant de « points de référence dans la vision du monde

[79] Wæver, “Securitization and Desecuritization,” 54.
[80] Wæver, “Securitization and Desecuritization,” 54.
[81] White House, Interim National Security Strategy Guidance.

de la Chine moderne[82] ». En outre, le développement du communisme chinois d'inspiration occidentale s'est entremêlé avec l'anti-impérialisme et l'anti-hégémonisme, perpétuant l'antagonisme au-delà de la transition politique vers la République en 1949.

L'analyse effectuée dans l'étude de cas consacrée à Huawei a montré que le discours anti-hégémonique de la Chine a été appliqué de deux manières principales. Premièrement, il s'agit d'un recours pour contrer la perception de la menace par les États-Unis et la renverser. La Chine recadre le discours de manière à identifier les États-Unis comme la véritable source de menace, en qualifiant le comportement du pays de « manœuvre hégémonique ».

Deuxièmement, le discours anti-hégémonique a été utilisé pour créer un récit qui présente les États-Unis comme une menace plus large pour l'ordre international et les intérêts légitimes des autres pays. Ce discours s'adresse à un public mondial et la Chine cherche activement à valider sa perception.

La position de la Chine repose sur des perceptions anti-hégémoniques et révisionnistes qui ont été partagées par un groupe plus large de pays. Comme le rappelle Stuenkel, la montée en puissance de l'ordre libéral après la Seconde Guerre mondiale n'a pas été un transfert volontaire de pouvoir aux États-Unis. Dans ce contexte, « la distinction entre légitimité et coercition est problématique, et (...) la coercition était un élément important de la consolidation de l'ordre libéral[83] ».

L'une des traces les plus visibles du révisionnisme sont les BRICS -formés par le Brésil, la Russie, l'Inde, la Chine et l'Afrique du Sud. Leur alignement n'était pas dirigé contre un pays en particulier, mais en faveur d'un ordre anti-hégémonique et visant à « rétablir un équilibre dans les affaires mondiales[84] ». Cela se ferait non seulement en encourageant la multipolarité, mais aussi en insufflant un programme de réforme dans les relations internationales. Ce programme comprendrait plusieurs actions, telles que la promotion d'un changement dans les accords de gouvernance des mécanismes existants, comme la Banque mondiale et le Fonds monétaire international (FMI), la recherche d'un affaiblissement de la domination du dollar

[82] Shambaugh, *Beautiful Imperialist*, 81.
[83] O. Stuenkel, *Post-Western World: How Emerging Powers Are Remaking Global Order* (Cambridge: Polity Press, 2016), 3.
[84] R. Sakwa, "Stasis and Change: Russia and the Emergence of an Anti-hegemonic World Order," In E. Parlar Dal and E. Erşen (eds.), *Russia in the Changing International System* (Switzerland: Palgrave, 2020).

américain en tant que monnaie de réserve mondiale, et le développement d'un cadre parallèle de financement lié au développement.

Ces dernières années, cependant, la Chine s'est démarquée de ce groupe de pays en adoptant un discours contre-hégémonique, avec un pôle d'opposition clair. Dans ce récit, les États-Unis sont désignés comme l'hégémon -un acteur doté d'une capacité écrasante à façonner le système international par des moyens coercitifs et non coercitifs[85]- qui représente une menace pour la Chine et pour l'ordre international. Bien que le récit soit interprété du point de vue du pays victime, il n'en demeure pas moins contradictoire dans son essence.

L' « équilibre des pouvoirs » est une institution visant à éviter les pratiques hégémoniques d'un pays ayant acquis une position dominante dans le système international et/ou à s'opposer à un pays perçu comme une menace. En dénonçant l'hégémonie, la Chine reconnaît la position dominante des États-Unis. En mettant l'accent sur les menaces que le pays représente pour l'ordre international, la Chine reconnaît la nécessité de pratiques contre-hégémoniques. La construction de ce macro-récit conduit le public vers la notion contradictoire de l'équilibre des pouvoirs. Cette attitude est conforme à l'influence que les approches réalistes des relations internationales ont exercée sur l'establishment politique chinois.

La deuxième réaction de la Chine consiste à adopter des pratiques contre-hégémoniques et axées sur la sécurité au niveau systémique, politiquement guidées par l'idée chinoise de « sécurité globale » et de « sécurité totale ». Sous les gouvernements de Hu Jintao et de Wen Jiabao, l'idée d'une « sécurité nationale globale » (综合国家安全, zonghe guojia anquan) a été introduite. La « sécurité globale » est une expression courante dans le lexique de la sécurité en Asie-Pacifique, inventée par le Japon dans les années 1970. Elle a été largement adaptée et employée par d'autres pays de la région, souvent en mettant l'accent sur l'aspect national de la sécurité nationale[86].

Singapour, par exemple, a adapté le concept de sécurité globale à la notion de « défense totale », parfois appelée « sécurité totale », pour faire référence à la notion selon laquelle « chaque secteur de la société est mobilisé et a un rôle à jouer dans la sécurité de Singapour[87] ». Capie et Evans affirment que « le principe central de la sécurité globale est que la sécurité doit être

[85] Ministry of Foreign Affairs of the People's Republic of China "America's Coercive Diplomacy".
[86] Capie and Evans, *The Asia-Pacific security lexicon*.
[87] Capie and Evans, *The Asia-Pacific security lexicon*, 70.

conçue de manière holistique - pour inclure les menaces militaires et non militaires qui pèsent sur le bien-être général d'un État. Le concept souligne également l'importance des réponses politiques non militaires[88] ».

La mise en œuvre de la sécurité globale par la Chine sous Hu Jintao et Wen Jiabao se distingue par le fait qu'elle met l'accent sur les menaces internes et externes et reconnaît l'impact direct de ces dernières sur la sécurité intérieure de la Chine. Elle reconnaît que les menaces non traditionnelles sont en augmentation et qu'il convient donc d'élargir les domaines de la sécurité[89]. La sécurité globale intègre aussi plus étroitement la sécurité politique, économique, militaire, sociale et culturelle.

Sous la direction de Xi Jinping, l'expression « sécurité nationale totale » (总体国家安 全/zongti guojia anquan) a été adoptée. Selon Nyman, le léger changement de mot est important, puisque le nouveau mot « Zongti » « connote quelque chose qui comprend l'ensemble, ou le total, et pourrait également être traduit par système entier, holistique, ou sécurité nationale totale[90] ». Comme l'ont noté Capie et Evans, la « sécurité holistique » est l'une des caractéristiques définissant la sécurité globale dans la région Asie-Pacifique[91], et l'expression « totale » a déjà été utilisée par Singapour pour faire référence à la « défense totale » et à la « sécurité totale ». Cela suggère que la « sécurité totale » ne doit pas être considérée comme une nouvelle construction, mais comme faisant partie du long développement de la notion de sécurité globale dans la région Asie-Pacifique.

Le changement de terme n'implique pas un changement de nature, mais marque une accélération de l'élargissement et de l'approfondissement de l'agenda de la sécurité en Chine. D'une part, il élargit considérablement le champ des domaines politiques qui devraient être considérés sous l'angle de la sécurité, en précisant que cette liste est « ouverte » et pourrait être encore élargie en fonction de l'environnement de sécurité. D'autre part, elle lie la sécurité de la Chine à la sécurité d'objets référents situés au-dessus de l'État, au niveau du système international.

[88] Capie and Evans, *The Asia-Pacific security lexicon*, 64.
[89] Nyman, "Towards a global security studies".
[90] Nyman, "Towards a global security studies", 687.
[91] Capie and Evans, *The Asia-Pacific security lexicon*, 64.

Le triangle des intérêts nationaux fondamentaux de la Chine reste valable en tant que base de la sécurité nationale de la Chine, avec la stabilité et la sécurité politique au sommet. La stabilité repose sur le développement et la souveraineté, cette dernière étant garantie par une triade plus étroitement articulée (sécurité militaire, sociale et culturelle) qui constitue la « ligne de défense » de la Chine, incarnant les « garanties[92] » de la souveraineté. La « sécurité nationale totale » a commencé à être conceptualisée autour de ces intérêts fondamentaux dans une myriade de nouveaux domaines : sécurité scientifique et technologique, cybersécurité, sécurité de l'information, sécurité écologique, sécurité des ressources, sécurité nucléaire, biosécurité, sécurité spatiale, sécurité polaire, sécurité en haute mer et sécurité des intérêts étrangers[93].

Au niveau systémique, la « sécurité nationale totale » se distingue de la « sécurité globale » en brouillant les lignes de démarcation entre sécurité traditionnelle et non traditionnelle, sécurité intérieure et extérieure, sécurité et développement, et sécurité individuelle et commune[94]. La raison en est que la plupart des menaces actuelles sont non traditionnelles -de la dégradation de l'environnement au trafic de drogue. Elles ont un impact simultané sur plusieurs domaines de la sécurité, ne peuvent être combattues par des mesures prises uniquement à l'intérieur des frontières et ne peuvent être résolues par la seule puissance militaire ou économique. Dans ces domaines, la distinction entre intérieur et extérieur perd de sa pertinence. La sécurité ne doit pas être conçue derrière des frontières rigides, mais être abordée comme des cercles concentriques interdépendants. Le besoin de survie de l'État est satisfait « par un sentiment accru de sécurité relationnelle[95] ».

L'absence d'une division nette entre sécurité intérieure et extérieure ressemble à la logique sous-jacente de la Tianxia chinoise, structurée autour de cercles concentriques -l'individu, la famille, l'État chinois et tous les autres États sous le ciel- dans lesquels il n'y avait pas d'extérieur absolu, mais seulement des degrés relatifs de proximité par rapport au centre[96]. La volonté de s'inspirer de la tradition chinoise transparaît dans les propos de Xi Jinping, révélant une tentative de sinisation du concept de sécurité emprunté à l'Occident. Selon lui, les conditions uniques et l'expérience historique de la Chine requièrent une compréhension de la sécurité nationale

[92] Peng, "Fundamentals to Observe".
[93] K. Drinhausen and H. Legarda, "Confident Paranoia: Xi's 'comprehensive national security' framework shapes China's behavior at home and abroad" *Merics China Monitor* (22 September, 2022).
[94] Nyman, "Towards a global security studies".
[95] Shih and Huang, "Balance of Relationships", 181.
[96] Tingyang, "A Political World Philosophy in Terms of All-Under-Heaven".

différente de celle de l'Occident, appelant à une approche basée sur la sécurité avec des caractéristiques chinoises[97].

Cette façon d'aborder la sécurité remet en question la distinction fondamentale entre l'intérieur et l'extérieur qui sous-tend le concept eurocentrique de la sécurité. Considérer la sécurité comme un continuum rayonnant à partir du centre -la sécurité du peuple- et s'étendant à des cercles concentriques -régionaux et mondiaux- facilite la compréhension de l'affirmation chinoise sur l'importance simultanée et indissociable de l'auto-sécurité et de la sécurité commune.

Cette approche chinoise a deux conséquences importantes. Premièrement, la suppression des divisions entre sécurité intérieure et extérieure permet à la Chine de projeter ses priorités fondamentales dans les relations qu'elle établit avec l'extérieur, dans le prolongement de sa politique intérieure. Comme le reconnaît Yongnian, « l'extension des principes, de la sphère nationale à la sphère internationale, vient "naturellement" dans la pensée chinoise parce que, tout au long de l'histoire, la Chine a compris que les relations extérieures étaient l'expression extérieure des mêmes principes que ceux qui sous-tendaient ses ordres sociaux et politiques intérieurs[98] ».

La projection des priorités nationales fondamentales de la Chine peut être observée dans trois initiatives, l'Initiative de développement mondial (IDM), l'Initiative de sécurité mondiale (ISM) et l'Initiative de civilisation mondiale (ICM). L'IDM vise à favoriser la coopération pour accélérer la mise en œuvre des Objectifs de développement durable à l'horizon 2030. La GSI vise à créer « une nouvelle voie vers la sécurité », à construire « une communauté de sécurité », en intégrant le respect de plusieurs principes, tels que la souveraineté et l'intégrité territoriale, et la résolution pacifique des différends, en privilégiant « le partenariat à l'alliance » et « le gagnant-gagnant au détriment de la somme nulle ». L'ICG vise à promouvoir le respect des différentes civilisations et des valeurs communes de l'humanité. Il encourage le respect de la diversité, y compris des modèles politiques et des idéologies, et l'adoption d'échanges mutuels et de coopération[99]. Dans l'ensemble, ces initiatives ne sont pas seulement une « vision de la

[97] Mentioned by Peng, "Fundamentals to Observe".
[98] Yongnian, "Organizing China's inter-state relations", 294.
[99] CGTN "Full text of Xi Jinping's keynote address at the CPC in Dialogue with World Political Parties High-level Meeting," CGTN (16 March 2023).

Chine qui comprend de mieux en mieux sa propre voie de modernisation, mais aussi une expansion progressive de cette voie[100] ».

Bien que la Chine reconnaisse la nécessité de proposer quelque chose de différent de l'approche réaliste de la sécurité, la nouveauté de cette vision s'estompe au moment où elle s'incarne dans le discours. Le contexte de la « sécurité totale » et des trois initiatives mondiales reflète une dynamique d'équilibre traditionnel dans le contexte de la concurrence entre grandes puissances. Les États-Unis sont toujours présents en tant que pôle opposé dans le discours chinois, en tant qu'adversaire ou « autre » par rapport auquel se construit l'identité de la Chine dans la société mondiale.

Cela révèle une tension dans la conception chinoise de la sécurité, actuellement déchirée entre le réalisme occidental et l'héritage de la pensée traditionnelle chinoise. Dans le domaine de la sécurité, la Chine est toujours à la recherche de sa version hybride de la modernité.

V.3. Le passage de la sécurisation des TSIC (Technologies et Services d'Information et Communication) à celle des TCE (Technologies Critiques et Emergentes)

Le 3 janvier 2023, le département d'État américain a annoncé la création d'un nouveau bureau de l'envoyé spécial pour les technologies critiques et émergentes[101]. Ce bureau vise à renforcer « l'expertise politique, le leadership diplomatique et la direction stratégique[102] », à coordonner la politique étrangère en matière de technologies critiques et émergentes et à impliquer les partenaires étrangers. Cette décision a été adoptée en réponse à l'intensification de la concurrence pour le développement et le déploiement des technologies critiques et émergentes (TCE), qui « remodèlent le monde[103] ». Les considérations stratégiques sur les TCE sont devenues « une partie intégrante de la conduite de la politique étrangère et de la diplomatie des États-Unis[104] ». La concurrence technologique, en particulier dans le contexte plus large des TCE (par rapport aux TICS), est au centre des tensions géopolitiques sino-américaines.

[100] Wang Yingwu, "Implementing the Global Civilization Initiative to Write a New Chapter of World Civilizations," (06 May 2023).
[101] U.S. Department of State, "Establishing the Office of the Special Envoy for Critical and Emerging Technology," Media Note, Office of the Spokesperson (3 January 2023).
[102] U.S. Department of State, "Establishing the Office of the Special Envoy".
[103] U.S. Department of State, "Establishing the Office of the Special Envoy".
[104] U.S. Department of State, "Establishing the Office of the Special Envoy".

L'importance des TCE pour la politique américaine est débattue depuis les années 1980[105]. À l'époque, l'idée sous-jacente était que « certaines technologies ont des propriétés spéciales qui les rendent particulièrement pertinentes pour les intérêts nationaux[106] ». Ces « propriétés spéciales » n'ont pas été précisées, mais les justifications du statut spécial des TCE ont été trouvées soit dans leur importance pour la promotion de la sécurité économique -entendue comme l'amélioration du bien-être humain et de la qualité de vie- soit dans la promotion de la sécurité nationale, puisque les TCE pourraient avoir un impact sur le coût, la précision ou la fiabilité des systèmes d'armement[107].

À l'heure actuelle, l'administration américaine définit les TCE dans une perspective plus étroite et axée sur la sécurité[108]. Les TCE peuvent être considérés comme « un sous-ensemble de technologies avancées qui sont potentiellement importantes pour la sécurité nationale des États-Unis ». Cela signifie que la présence des TCE a été « politisée » dans le cadre des questions de sécurité, ce qui accroît l'importance du sujet. Comme le notent Hansen et Nissenbaum, « constituer quelque chose comme un "problème de sécurité" tout en définissant simultanément quelque chose comme n'en étant pas un a des conséquences significatives dans la mesure où cela confère au "problème" un statut et une priorité que n'ont pas les "problèmes non liés à la sécurité" »[109].

La définition des TCE proposée par l'administration américaine se compose notamment de trois expressions, « avancé », « critique » et « émergent », qui méritent d'être approfondies. Dans le contexte de l'administration américaine, les politiques de promotion des technologies dites « avancées » ont été mises en place à la fin des années 1990 et faisaient référence aux « technologies habilitantes ayant un fort potentiel de retombées économiques pour la nation[110] ». Selon Gartner, les technologies avancées font référence à des technologies immatures qui promettent d'apporter une valeur significative, ou à des technologies relativement matures, mais dont les cas d'utilisation pratique sont encore peu nombreux[111]. Ces technologies sont considérées comme cruciales pour la

[105] B. Bimber and S. A. Popper, "What is Critical technology?," *RAND* DRU-605-CTI (February 1994).
[106] Bimber and Popper, "What is Critical technology?," 1.
[107] Bimber and Popper, "What is Critical technology?," 2.
[108] United States Executive Office of the President, "Critical and Emerging Technologies List Update" (September 2023).
[109] Hansen and Nissenbaum, "Digital Disaster", 1156.
[110] W. H. Schacht, "The Advanced Technology Program," *Congressional Research Service Report* Code 95-36 SPR (June 2005).
[111] Gartner, "Advanced Technology," *Gartner Glossary* (no date).

croissance économique à long terme, mais nécessitent souvent des partenariats public-privé pour être pleinement développées[112].

Dans cette optique, les technologies avancées s'apparentent à la technologie de pointe ou à la haute technologie. Par conséquent, les secteurs spécifiques inclus sous l'étiquette « technologies avancées » changent constamment, parallèlement à l'évolution technologique. Cela explique la pluralité des classifications potentielles des technologies avancées. Du point de vue du commerce américain, l'US Census Bureau fournit une liste de produits de technologie avancée, regroupés en dix catégories, qui sert de cadre à leur classification et à leur évaluation dans les importations et exportations américaines : 1. biotechnologie, 2. sciences de la vie, 3. optoélectronique, 4. information et communications, 5. électronique, 6. fabrication flexible, 7. matériaux avancés, 8. aérospatiale, 9. armement, 10. technologie nucléaire.[113].

L'IA illustre également la manière dont l'infrastructure des TIC est souvent associée à un service ou, de plus en plus, proposée en tant que tel. Ces dernières années, plusieurs fournisseurs de services en nuage ont commencé à proposer l'intelligence artificielle en tant que service. Dans ce cas, des modèles d'apprentissage automatique sont mis à la disposition de l'utilisateur. Les services Google Cloud et IBM Watson proposent une myriade de produits spécifiques, axés sur la reconnaissance de la vision et la compréhension du langage naturel, par exemple ChatGPT. C'est pourquoi le gouvernement américain désigne de plus en plus souvent ce secteur par l'expression « technologies et services de l'information et de la communication » (TSIC), pour faire référence à la technologie, ainsi qu'aux services et applications qui tirent parti de l'infrastructure TIC sous-jacente pour apporter de la valeur et des fonctionnalités aux utilisateurs. Cette évolution renforce le sentiment qu'il existe un nouveau secteur à ajouter à la théorie de la sécurisation.

Les TSIC fournissent l'infrastructure et les applications sur lesquelles se développent de nombreux TCE émergents. Cela signifie que les TSIC constituent une catégorie d'ancrage importante dans les discussions politiques, ainsi qu'un point de contrôle potentiel pour influencer le développement des technologies de l'information et de la communication. L'IA,

[112] United States of America, “Technology for America’s Economic Growth: a New Direction to Build Economic Strength,” Clinton Administration Policy White Paper (22 February, 1993).
[113] U.S. Census Bureau, “Advanced Technology Product (ATP) Code Description.”

par exemple, dépend des micropuces, des normes harmonisées, du traitement et de l'analyse des données et du stockage en nuage pour fonctionner.

Les TSIC sont donc devenues un nouveau champ d'application de la sécurisation, qui pourrait être considéré comme distinct des autres secteurs de la sécurité identifiés par Buzan. Selon Buzan, les préoccupations en matière de sécurité peuvent se situer dans cinq secteurs[114] : militaire, politique, économique, sociétal et environnemental. Les secteurs identifiés par Buzan ne sont pas en nombre fixe, mais pourraient potentiellement s'accroître avec la complexité croissante des interactions mondiales. Ces dernières années, plusieurs domaines ont été considérés comme de nouveaux domaines de sécurité, tels que la santé mondiale, la religion, l'énergie et la cybersécurité[115].

Selon l'école de Copenhague, les secteurs de sécurité sont des focales qui peuvent être utilisées pour aborder les discours sur la sécurité, plutôt que des phénomènes objectivement existants[116]. Ils sont définis par des constitutions particulières d'objets référents et de types de menaces, ainsi que par des formes spécifiques ou des « grammaires » de sécurisation, qui sont utilisées pour lier les objets référents, les menaces et les acteurs de la sécurisation de manière spécifique. Afin d'identifier la présence d'éléments de sécurisation, il est utile de se pencher sur la catégorie « technologie » dans les deux études de cas analysées. La première chose qui ressort est que les menaces liées à la technologie sont liées aux trois objets référents identifiés par la théorie originale de la sécurisation: l'État, l'économie et les valeurs et l'ordre politiques. Selon Hansen et Nissenbaum, la nature transversale des menaces est une conséquence du caractère en réseau des systèmes informatiques - étayés par des logiciels et des protocoles matériels- et de la dépendance de tous les secteurs de la société à l'égard de cette infrastructure[117].

Selon les auteurs, lorsque le discours technique de la « sécurité informatique » (axé sur les moyens techniques d'améliorer la sécurité des machines et de leurs systèmes) a été élargi pour prendre en compte l'impact systémique que ces systèmes interconnectés pourraient provoquer en cas de défaillance, la notion de « cybersécurité » est apparue. La cybersécurité est donc " »a

[114] B. Buzan, *People States and Fear* (Colchester: ECPR Press, 2016).
[115] Balzacq, Léonard and Ruzicka, "Securitization revisited", 503.
[116] Buzan, Wæver and Wilde, *Security, 27.*
[117] Hansen, and Nissenbaum, "Digital Disaster," 1161.

sécurité informatique plus la sécurisation[118] », ce qui a ajouté la dimension de « sécurité nationale » au sujet.

Hansen et Nissenbaum ont soutenu que la cybersécurité devait être considérée comme un domaine distinct de la sécurité. Le travail développé par Hansen et Nissenbaum se distingue cependant par la proposition d'un objet référent spécifique -le réseau- et d'une « grammaire de la sécurité » spécifique qui caractériserait la cybersécurité, la différenciant des autres domaines de sécurité identifiés par l'école de Copenhague. Compte tenu de l'affinité entre les TICS et le domaine de la cybersécurité, il est important d'analyser si le discours relatif aux TICS identifié dans les deux études de cas correspondrait aux éléments spécifiques de sécurisation proposés par Hansen et Nissnbaum.

La conceptualisation du « réseau » en tant qu'objet référent apparaît dans plusieurs extraits de discours, à travers des expressions telles que « réseaux », « systèmes » et « infrastructures critiques ». Les deux expressions les plus récurrentes -« réseaux » et « infrastructures critiques »- fournissent des éléments importants pour comprendre les propriétés particulières et distinctives de cet objet référent. Aradau attire l'attention sur la « matérialité » de l'infrastructure, qui est étroitement liée aux composants physiques et à leur connectivité matérielle[119]. La protection des infrastructures critiques -qui englobent des secteurs tels que l'énergie, les transports, la finance et les systèmes d'approvisionnement en eau, par exemple- est devenue un domaine important dans les discussions sur la cybersécurité, visant à garantir que les opérations considérées comme essentielles pour les sociétés puissent se poursuivre sans interruption indue et que les données cruciales et sensibles soient protégées[120].

Aradau mentionne que les infrastructures d'information critiques -telles que les réseaux de communication, les systèmes d'information gouvernementaux et les systèmes de gestion de l'énergie- présentent une caractéristique importante, puisque ces infrastructures « apparaissent comme un objet dont la matérialité a des effets à la fois habilitants et contraignants sur ce qui peut être dit et fait pour les sécuriser[121] ». Cette caractéristique se révèle dans le cas du nouveau protocole IP. Une modification du protocole IP visant à intégrer la « sécurité intrinsèque » équivaudrait à une « réglementation par le code » de l'architecture de l'internet, limitant les

[118] Hansen, and Nissenbaum, "Digital Disaster," 1160.
[119] C. Aradau, "Security That Matters: Critical Infrastructure and Objects of Protection," *Security Dialogue* 41 5 (2010).
[120] Aradau, "Security That Matters", 492.
[121] Aradau, "Security That Matters", 492.

options techniques et les comportements en amont. Aradau a proposé de « reconceptualiser le rôle et l'agence des objets dans la production de la réalité[122] », ce qui est cohérent avec le « pouvoir normatif » de l'architecture du réseau.

Parallèlement, Hansen et Nissenbaum attirent l'attention sur l'importance de la relation intime entre l'infrastructure physique et les objets référents liés à l'homme qui caractérisent d'autres domaines de la sécurité[123]. L'infrastructure de l'information est critique dans la mesure où elle permet le fonctionnement d'autres infrastructures critiques qui permettent aux constructions humaines -l'État, l'économie, le système politique- de continuer à fonctionner. Ils proposent donc de mettre l'accent sur l'élément humain et non sur les « objets » de l'infrastructure[124].

Les arguments avancés par Aradau et par Hansen et Nissenbaum ne sont pas opposés, mais se complètent. Le « réseau » peut se référer à l'infrastructure des composants physiques interconnectés, mais la même expression peut être utilisée pour faire référence aux réseaux créés par l'interaction sociale. Le « réseau » est un joker qui permet au processus de sécurisation de passer de la couche physique à la couche sociale, du secteur des TIC au secteur des TSIC, et de se concentrer sur le déploiement de l'infrastructure, les nœuds physiques et les goulots d'étranglement, aux relations de pouvoir qui se forment lorsque certains acteurs prennent le contrôle de ces nœuds centraux. Il révèle les liens entre l'infrastructure, les réseaux d'interdépendance et la possibilité de « militariser » l'interdépendance. Le terme « réseaux » est donc un objet de référence adéquat dans le contexte des deux études de cas.

Selon Hansen et Nissenbaum, la « grammaire de la sécurité » spécifique au domaine de la cybersécurité se compose de trois éléments clés : l'hypersécurisation, les pratiques quotidiennes de sécurité et la technification[125]. L'hypersécurisation est une expression inventée par Buzan pour faire référence à l'expansion de la sécurisation au-delà d'un niveau normal de menaces et à une tendance à exagérer les menaces et, par conséquent, leurs contre-mesures[126]. Pour les auteurs, l'hypersécurisation fait référence à « la manière dont le discours sur la cybersécurité s'articule autour de scénarios de cybercatastrophe multidimensionnels qui regroupent une

[122] Aradau, "Security That Matters", 492.
[123] Hansen, and Nissenbaum, "Digital Disaster".
[124] Hansen, and Nissenbaum, "Digital Disaster".
[125] Hansen, and Nissenbaum, "Digital Disaster," 1163-8.
[126] Buzan, "The United States and the Great Powers".

longue liste de menaces graves dans une séquence monumentale en cascade, et au fait qu'aucun de ces scénarios ne s'est produit jusqu'à présent[127] ».

L'analyse d'extraits des documents du corpus révèle que les menaces « monumentales » aux effets « en cascade » font partie intégrante du discours. Dans l'ordre exécutif 13873, le président des États-Unis fait référence aux « effets potentiellement catastrophiques » de l'acquisition sans restriction de TSIC fournis par des adversaires étrangers[128]. L'utilisation d'expressions hyperboliques dans d'autres extraits indique une direction similaire, comme la comparaison de l'insertion de « composants malveillants » avec une « arme redoutable[129] ».

L'effet de cascade apparaît également lorsque l'on considère que les TCE sont des éléments constitutifs des technologies émergentes qui se développent en amont. Comme l'a mentionné le témoin William Evanina, lors de l'audition « Commanding heights », qui s'est tenue devant la commission spéciale sur la concurrence stratégique entre les États-Unis et le Parti communiste chinois, il existe une « menace majeure » liée au fait que « les piles de technologies numériques s'appuient les unes sur les autres », comme les applications d'IA qui sont construites au-dessus de l'infrastructure 5G [de Huawei][130]. Un autre exemple a été fourni par GSMA, qui a critiqué la nouvelle proposition de protocole IP au motif qu'elle introduit des « points de défaillance uniques », qui représentent une vulnérabilité pour l'ensemble du système[131].

Deux des idées centrales associées à l'hypersécurisation, telles que définies par Hansen et Nissenbaum, sont donc présentes dans le discours sur les TSIC dans les deux cas. En outre, leur troisième critère -la référence à des menaces monumentales qui n'ont pas eu lieu- suggère que les risques sont un des principaux moteurs de l'hypersécurisation. Dans l'étude de cas Huawei, l'importance de la logique axée sur le risque dans les discussions politiques est corroborée par l'étude de 2011 de la Commission d'examen de l'économie et de la sécurité des États-Unis et de la Chine[132]. Elle souligne « les problèmes de sécurité potentiels liés au fait que des éléments d'infrastructure passent sous le contrôle d'entités étrangères[133] » et affirme qu' « il n'y a pas

[127]Hansen, and Nissenbaum, "Digital Disaster," 1164.
[128] Executive Order 13873 of 15 May 2019 Establishing "Securing the Information and Communications Technology and Services Supply Chain".
[129] U.S. House of Representatives Permanent Select Committee on Intelligence, "Investigative Report".
[130] US House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, "Commanding Heights".
[131] Austria, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, GSMA, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, RIPE-NCC, Romania, Slovakia, Spain, Sweden and United Kingdom, "Next Steps for proposed work on 'New IP'".
[132] U.S.-China Economic and Security Review Commission "The National Security Implications,"7.
[133] U.S.-China Economic and Security Review Commission "The National Security Implications,"7.

d'études de cas facilement disponibles où cela s'est réellement produit[134] ». Les risques d' «effets catastrophiques » qui n'ont pas eu lieu ont justifié les mesures prises par la suite pour restreindre le commerce avec Huawei et le déploiement d'équipements Huawei aux États-Unis.

La deuxième caractéristique de la « grammaire de la cybersécurité » proposée par Hansen et Nissenbaum est le recours aux pratiques quotidiennes. Il s'agit d'une tentative de lier la sécurisation aux expériences des individus afin de « garantir le partenariat et la conformité de l'individu » avec les mesures de protection de l'objet référent et de « rendre les scénarios d'hypersécurisation plus plausibles en reliant les éléments du scénario de catastrophe à des expériences familières de la vie quotidienne[135] ».

Dans les extraits de discours recueillis pour les études de cas, des références sont faites aux « technologies de la vie quotidienne[136] » et à la possibilité que perdre la compétition avec la CCP signifie une dégradation de ces technologies, parce qu'elles seraient intégrées par un ensemble de valeurs différentes[137] . Le président de la commission spéciale sur la concurrence stratégique entre les États-Unis et le Parti communiste chinois l'a exprimé en termes simples lors de l'audition consacrée aux technologies critiques et émergentes : « Si nous gardons une longueur d'avance, nous pourrons nous assurer que la technologie est au service de l'humanité et non l'inverse. Mais l'inverse est également vrai. Si nous perdons, nous pourrions voir cette technologie avoir un impact sur nos libertés et limiter nos opportunités. Tels sont les enjeux[138] ».

La troisième caractéristique de la « grammaire de la cybersécurité » proposée par Hansen et Nissenbaum est la technification. Selon eux, « l'importance accordée à l'hypothétique dans la cybersécurité crée un espace particulier pour le discours technique et expert[139] ». En conséquence, « la légitimité accordée aux experts et l'autorité épistémique que détiennent les informaticiens leur permettent de jouer le rôle privilégié de ceux qui ont l'autorité de parler de l'inconnu[140] ». Les auteurs soulignent que les acteurs techniques sont placés sous les feux de

[134] U.S.-China Economic and Security Review Commission "The National Security Implications," 23.
[135] Hansen and Nissenbaum, "Digital Disaster," 1165.
[136] U.S. House of Representatives, Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, Intervention by Krishnamoorthi at the Hearing "Commanding Heights", 6.
[137] U.S. House of Representatives, Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, Intervention by Krishnamoorthi at the Hearing "Commanding Heights", 6.
[138] U.S. House of Representatives, Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, Intervention by Krishnamoorthi at the Hearing "Commanding Heights", 7.
[139] Hansen and Nissenbaum, "Digital Disaster," 1166-7.
[140] Hansen and Nissenbaum, "Digital Disaster," 1166-7.

la rampe dans le débat public et deviennent des voix autorisées de la sécurité, remettant en cause le manque de visibilité des « petits riens de la sécurité[141] » des experts en sécurité.

À ce stade, il y a une divergence entre ce qui a été proposé par Hansen et Nissenbaum et ce qui a été observé dans l'une des études de cas. Dans le cas de la proposition relative au nouveau protocole IP, deux organisations techniques ont officiellement contribué par des textes aux discussions sur le nouvel IP au sein de l'UIT, l'IETF et le RIPE-NCC. L'IETF, en particulier, a été considérée comme une voix faisant autorité dans les discussions lorsqu'elle a mentionné que « nous pensons que la création d'un effort de conception de haut en bas pour remplacer en gros la pile de protocoles IP existante serait préjudiciable. Cela créerait très certainement des îlots de réseau, endommagerait l'interconnexion et mettrait en péril l'interopérabilité[142] ». Bien que le cas ne présente pas un échantillon diversifié d'acteurs techniques, leur présence et les arguments techniques avancés dans la discussion sur le « New IP » corroborent les critères de technification.

Dans le cas de Huawei, en revanche, la technification des discussions est remarquablement absente. La commission responsable du rapport du HPSCI, un document qui a établi des paramètres clés pour la sécurisation de la question, se détache du domaine des discussions techniques lorsqu'elle affirme que « l'expertise de la commission ne se prête pas à des examens complets de pièces d'équipement particulières[143] ». L'objectif était plutôt d'évaluer si le gouvernement chinois aurait la possibilité d'exploiter les composants et les systèmes de télécommunications des entreprises chinoises. Parallèlement, de nombreux acteurs qui ont témoigné lors des auditions de la commission spéciale sur la concurrence stratégique entre les États-Unis et le parti communiste chinois appartiennent à l'establishment américain de la sécurité. Lors d'une audition devant la commission du renseignement du Sénat américain, six chefs du renseignement américain ont conseillé aux Américains de ne pas utiliser les produits ou services des entreprises chinoises Huawei ou ZTE[144], ce qui a été largement repris par les médias internationaux.

Ce résultat peut s'expliquer par deux aspects qui semblent liés dans l'affaire Huawei : la militarisation de la politique de sécurité et de la politique étrangère des États-Unis et la macro-

[141] Huysmans, “What's in an act?,” 376.
[142] Liaison Statement: Response to LS on New IP, Shaping Future Network” (IETF, 2020)
[143] U.S. House of Representatives Permanent Select Committee on Intelligence, “Investigative Report,” 11.
[144] U.S. Senate Select Committee on Intelligence, “Open Hearing on World Threats,” (13 February 2018).

sécurisation du récit de la « menace chinoise ». Contrairement à la cybersécurité, qui peut ou non comporter un élément de « politique étrangère », l'affaire Huawei n'a pas seulement un aspect de politique étrangère évident, mais se réfère à un pays étranger considéré comme le principal adversaire des États-Unis et la principale préoccupation du pays en matière de sécurité nationale. Le récit de la macro-sécurisation fournit le cadre dans lequel d'autres récits de sécurisation peuvent se développer. La « menace chinoise » établit une relation ami/ennemi et un récit du « bien contre le mal » qui supplante la nécessité d'arguments techniques pour justifier une menace. Dans l'affaire Huawei, qui a été étroitement liée à la macro-sécurisation, la détechnification (par opposition à la technification) est une caractéristique remarquable.

Malgré les résultats mitigés obtenus par rapport au critère de « technification » proposé par Hansen et Nissenbaum, les éléments de la « grammaire de la cybersécurité » peuvent être utilisés pour analyser les deux études de cas. Ils confirment l'argument présenté par Hansen et Nissenbaum et par d'autres auteurs, selon lequel les domaines de la sécurité initialement présentés par l'école de Copenhague devraient être élargis pour inclure la cybersécurité en tant que secteur dans lequel la sécurisation est mise en œuvre. Cela serait particulièrement important à l'heure actuelle, où les technologies critiques et émergentes sont de plus en plus discutées sous l'angle de la sécurité.

Conclusion

Les deux études de cas ont montré de manière convaincante la façon dont les deux hégémons se disputent le contrôle et la centralité des TSIC, considérés comme les strates inférieures sur lesquelles les technologies critiques et émergentes vont être construites. Le contrôle des nœuds centraux de l'infrastructure physique donne aux pays un avantage concurrentiel, comme l'accès à de plus grands volumes de données, la capacité de tirer parti de l'interdépendance asymétrique et d'influencer le développement des technologies en amont. Le contrôle des normes et des protocoles leur donne accès au marché et leur confère un avantage de pionnier. La possibilité d'influencer et de limiter les choix comportementaux par le biais de protocoles est une caractéristique importante de cet espace en réseau. Les décisions prises au niveau des protocoles peuvent avoir un impact sur la sécurité mondiale. L'adoption potentielle de différents protocoles pourrait créer différents « villages », avec des degrés variables d'interopérabilité entre eux

La fragmentation n'est pas une préoccupation nouvelle. Au lendemain des révélations d'Edward Snowden, ancien employé de l'Agence nationale de sécurité américaine (NSA), sur la

surveillance massive des communications numériques, certains ont prédit que l'internet pourrait se fragmenter. L'expert en sécurité Eugene Kaspersky a affirmé que « l'utopie d'un village numérique mondial sans frontières pourrait toucher à sa fin[145] ». La fragmentation du World Wide Web est déjà en cours, le long des frontières nationales. Ce scénario a conduit à l'organisation de la réunion NETMundial, en 2014, au Brésil, et les forces centrifuges de la fragmentation ont été contrées par un pacte multipartite renouvelé autour des principes clés de la gouvernance de l'internet[146]. Depuis lors, sous l'impulsion de la technologie numérique, le commerce des services a commencé à croître plus rapidement que le commerce des marchandises, devenant le segment le plus dynamique de l'économie mondiale[147]. L'intérêt de maintenir un réseau mondial unifié et non fragmenté entre les démocraties libérales était évident.

Les préoccupations liées à la fragmentation sont aujourd'hui plus graves. D'une part, le problème de la surveillance de masse n'a pas été résolu, comme le montrent les décisions de la Cour européenne des droits de l'homme invalidant le cadre juridique des flux de données transatlantiques entre l'UE et les États-Unis. D'autre part, le pendule de l'élaboration des politiques s'est déplacé de la libéralisation vers un contrôle accru des « flux » qui traversent les frontières, qu'il s'agisse de biens, de services ou de données. Les questions commerciales sont discutées en tandem avec d'autres questions politiques, telles que les normes de travail, les droits de l'homme et la sécurité.

Alors que l'interopérabilité au niveau de l'infrastructure et des protocoles techniques de base de l'internet continue d'être observée, des pressions croissantes de fragmentation s'exercent au niveau de la gouvernance et de l'expérience de l'utilisateur. Du point de vue de la gouvernance, un nombre croissant de questions de politique numérique -des identités numériques aux systèmes de crédit social en passant par les modèles d'IA- sont discutées dans de multiples forums, y compris dans le contexte des accords commerciaux. Les négociations commerciales sont opaques et difficilement accessibles aux acteurs non gouvernementaux. Du point de vue de l'expérience utilisateur, la fragmentation entraîne souvent l'impossibilité d'accéder à certains contenus et services. Ces barrières étaient courantes dans les pays qui ont une tradition de contrôle de l'accès à l'internet, mais elles prolifèrent aujourd'hui partout. En novembre 2023, un

[145] E. Kaspersky, "What will happen if countries carve up the internet?," *The Guardian* (17 December 2013).
[146] M. Maciel, N. Zingales and D. Fink, "The Global Multistakeholder Meeting on the Future of Internet Governance (NETmundial)," NoC Internet Governance Case Studies Series (2015).
[147] World Trade Organization (WTO), "World Trade Report 2019: the future of services trade," World Trade Organization (2019).

juge américain a bloqué une loi de l'État du Montana qui aurait interdit l'accès à TikTok[148]. Les divergences politico-idéologiques entraînent également une fragmentation de la chaîne de valeur, en particulier dans les domaines liés à la technologie, créant des fossés qu'il pourrait être difficile de combler à l'avenir.

En ce qui concerne les recherches futures, il existe plusieurs pistes potentielles pour poursuivre l'étude de la sécurisation des TSIC. Cette recherche en indique trois principales.

Premièrement, l'approche méthodologique développée pour la recherche peut être appliquée pour analyser la sécurisation dans le contexte d'autres cas, tels que les restrictions imposées dans le secteur des semi-conducteurs et les mesures visant à protéger les données personnelles dans le contexte de l'utilisation croissante des plateformes en ligne chinoises et des médias sociaux aux États-Unis. La récente tentative d'interdiction de TikTok dans l'État du Montana montre qu'il s'agit d'une controverse pertinente.

Deuxièmement, une étude comparative pourrait être menée entre la sécurisation des TSIC dans les relations sino-américaines et la manière dont le sujet est traité dans le contexte d'autres relations, telles que l'UE-Chine, par exemple. Une analyse critique du discours pourrait révéler les convergences et les clivages au sein de l'Occident.

Troisièmement, de nouvelles études de cas empiriques dans le domaine de la technologie pourraient contribuer à élargir et à affiner la théorie de la sécurisation. Les deux études de cas couvertes par la recherche -sur les limitations de Huawei et sur New IP- ont montré l'importance de certaines dimensions introduites par les approches critiques de la théorie de la sécurisation. L'une d'entre elles est la notion de risque. L'importance croissante des mesures d'atténuation des risques dans le contexte des stratégies de sécurité économique montre qu'il est nécessaire d'approfondir l'analyse de l'atténuation des risques. Le mariage de la sécurisation et du risque est intéressant. D'une part, il permet de remettre en question la théorie originale de la sécurisation en montrant qu'elle ne nécessite pas toujours une « rupture avec les limites de la procédure normale ». D'autre part, elle permet de placer le risque dans un continuum

[148] K. Paul, "US judge blocks Montana TikTok state ban: 'oversteps state power'," *The Guardian* (30 November 2023).

d'exceptionnalité, en montrant que les mesures d'atténuation du risque et les « petits riens de sécurité[149] » peuvent conduire à une normalisation de l'exceptionnel.

Les études de cas ont également mis en évidence les lacunes de la théorie. Dans le contexte des sociétés numérisées, une gamme de plus en plus vaste d'objets est sous-tendue par la technologie numérique. Cette technologie dépend des spécifications des protocoles et du code source pour fonctionner. Les spécifications des protocoles sont également écrites sous forme de code source afin d'être mises en œuvre. Il existe une lacune dans l'étude de la question de savoir si les langages de programmation peuvent être considérés comme des langages du point de vue de la linguistique (puisqu'ils présentent une syntaxe, une sémantique et une pragmatique et servent à établir la communication entre les ordinateurs, entre l'homme et la machine, et entre les hommes), et si le code source écrit par un programmeur peut être considéré comme un discours doté d'un poids illocutoire, capable de constituer un acte de langage. Cela pourrait ouvrir une voie de recherche innovante sur le thème de la « sécurisation par le protocole ».

La situation actuelle marque un « point d'inflexion », qui ne modifie pas seulement la direction, mais peut également se référer à un moment de changement significatif, au cours duquel des événements émergents et difficiles à prévoir se produisent parce qu'un système se trouve proche de son point critique. Cela signifie que la stabilité et l'instabilité deviennent volatiles. Dans ce scénario, l' « équilibre » doit être compris comme un processus d' « interrelation et d'adaptation » constant, car tout équilibre atteint ne sera rien de plus qu'un état éphémère.

Il pourrait être important, à l'heure actuelle, de promouvoir un grand remaniement des caractéristiques relationnelles que l'on retrouve dans les différentes conceptions de l'« équilibre » à travers le temps -de la notion d'«équilibre actif » que l'on retrouve en Occident au XIII^{e} siècle à la notion d'équilibre en tant que gestion des relations. Même lorsque l'équilibre des pouvoirs est l'approche dominante, chercher à « équilibrer les relations » pourrait être utilisé comme une stratégie auxiliaire pour apaiser la peur et remplacer progressivement l'image menaçante de l'autre par une ressemblance partagée et une identité commune. Si la gestion et l'amélioration des relations deviennent un principe directeur de l'interaction et la base de la (re)définition de l'identité, les idées préconçues sur l'autre peuvent être examinées et les éléments de ressemblance imaginée peuvent être mis en évidence.

[149] Huysmans, “What's in an act?,” 376.

Dans les relations sino-américaines, le lien entre la technologie et la modernité est une source de peur et d'anxiété. La crainte de perdre le contrôle du « sens de la marche » de la modernité perturbe l'Occident, tout comme la crainte de « manquer le train de la modernité » perturbe la Chine. Paradoxalement, le lien entre la technologie et la modernité fournit également un terrain fertile pour la construction d'une « ressemblance imaginaire », comme l'a suggéré Huawei [150]. Le « projet inachevé[151] » de la modernité technologique, incarné par le développement des technologies émergentes dans les années à venir, pourrait potentiellement offrir une « zone d'atterrissage » pour ce grand re-câblage, si le secteur n'était pas plus rapidement déconnecté dans les relations sino-américaines. De ce point de vue, la décision du Royaume-Uni d'impliquer la Chine dans le sommet mondial sur l'IA parrainé par le Royaume-Uni en octobre 2023, appelant à un « engagement plus profond avec Pékin[152] » dans ce domaine, ouvre de nouvelles perspectives pour l'avenir.

Bien que les différends liés à la technologie dans le contexte des relations sino-américaines aient fait la une des journaux, il existe un groupe plus large de « puissances moyennes numériques[153] ». Elles sont non seulement « de plus en plus pressées de déterminer de quel côté elles se situent[154] », mais elles cherchent également à se tailler une place dans l'élaboration de la technologie et de sa gouvernance. Le Brésil en est un exemple. Bien qu'il ne dispose pas de ressources matérielles et techniques suffisantes pour égaler celles des grandes puissances, il a la capacité d'influencer les décisions et d'exercer un leadership et un soft power sur la scène internationale. L'annonce d'un événement NETMundial +10 en 2024 est un exemple de cette proactivité. Tout comme en 2014, l'un des thèmes à l'ordre du jour de l'événement de 2024 est la fragmentation. Dans un scénario géopolitique transformé, les défis et les enjeux découlant des tendances à la fragmentation sont plus importants que jamais et nécessiteront un redémarrage de la gouvernance de l'internet et du multipartenariat, avec une plus grande représentation de la société civile et de sa base, le public oublié.

[150] Huawei, “Huawei Statement regarding HPSCI's report”.
[151] Habermas, “Modernity – an Unfinished Project”.
[152] W. James, “Britain invites China to its global AI summit,” *Reuters* (19 September 2023).
[153] A. Pannier, “Digital Middle Powers and the Global Tech Competition,” In A. Pannier (ed.), *The Technology Policy of Digital Middle Powers* (Paris: IFRI, 2023).
[154] Pannier, “Digital Middle Powers,” 7.