Centre d'étude des crises et conflits internationaux

Xiber-Chine

Puissance digitale en devenir

Orinx Kimberly & Struye de Swielande Tanguy

Juin 2020

Note d'analyse no. 68

Xiber-Chine : Puissance digitale en devenir

Orinx Kimberly & Struye de Swielande Tanguy

Direction :
Tanguy Struye de Swielande

Centre d'étude des crises et conflits internationaux
Université catholique de Louvain
Place Montesquieu 1, bte L2.08.07
1348 Louvain-la-Neuve
Belgique

Photo de couverture : Tanguy Struye de Swielande

A propos des auteurs

Kimberly Orinx, assistante au cadre à l'Université catholique de Louvain, est diplômée d'un master de spécialisation en droit international de l'Université Libre de Bruxelles (ULB) et d'un master en sciences politiques, relations internationales obtenu en co-diplomation entre l'ULB et Tongji University (Shanghai, Chine). Ses recherches doctorales se concentrent principalement sur la Chine et la guerre de l'information et l'environnement informationnel.

Tanguy Struye de Swielande est professeur en relations internationales à l'Université catholique de Louvain et directeur du CECRI. Il est spécialisé dans la géopolitique et politique étrangère des grandes puissances et dans l'analyse de la prise de décision. Il dirige la collection Scène internationale aux presses universitaires de Louvain.

Table des matières

Daniel Coats, directeur américain du renseignement national, déclarait en janvier 2019 que les cyber-opérations menacent non seulement les infrastructures, mais exercent également une pression mentale sur les citoyens américains.[9] En mai 2019, suite à un discours du secrétaire-général de l'OTAN Jens Stoltenberg, l'ambassadeur de la République de Tchéquie affirmait : « plus nos infrastructures critiques seront protégées et résilientes, plus nos ennemis se concentreront sur l'esprit de nos sociétés ». Cette phrase résume assez bien la complexité du cyber. En effet, le cyber, en particulier chinois, pose aujourd'hui cinq défis majeurs : la vulnérabilité des infrastructures et données, la guerre de l'information dans l'environnement informationnel, la cybersouveraineté, les nouvelles technologies, et les matières premières.

1. VULNERABILITE DES INFRASTRUCTURES

Le premier, et probablement le plus connu, concerne la sécurité des infrastructures et par conséquent les dimensions physique (ordinateurs, serveurs, routeurs, etc.) et logistique (softwares, etc.) du cyberespace. Malgré les récents exemples de cyberattaques de type *hard,* les investissements restent, dans un pays comme la Belgique, insuffisants. Les risques que courent les infrastructures de nos ministères et entreprises sont souvent sous-évalués alors qu'une cyberattaque pourrait avoir pour conséquence la paralysie de notre économie. Selon le site *Threatmap checkpoint*, plus de deux millions de cyberattaques sont lancées chaque jour.[1] Des sites internet sont même dédiés à la visualisation en temps réel des cyberattaques mondiales.[2] Bien sûr les États ne sont pas tous visés par des DDoS (*Distributed Denial of Service*). En effet, plusieurs types de cyberattaques existent. Par exemple, les *malwares,* le *phishing,* ou encore les *botnets*. Parmi les cyberattaques les plus connues, notamment pour leur envergure, nous pouvons citer l'Estonie en 2007, la Géorgie en 2008, le virus Stuxnet contre le programme nucléaire iranien en 2010 ou encore le logiciel malveillant WannaCry en mai 2017.[3]

Les exemples récents de cyberattaques au niveau mondial ne manquent pas. En mai 2020, des pirates chinois sont parvenus à accéder aux données de neuf millions de passagers de la compagnie britannique EasyJet. À cette même période, les Américains ont accusé des hackers liés à Pékin de tenter de voler des recherches américaines sur le vaccin contre le coronavirus. Les exemples pour le seul mois de mai 2020 ne s'arrêtent pas là ; les Chinois sont également suspectés d'avoir mené des opérations de *phishing* pour compromettre le gouvernement vietnamien dans le cadre du conflit en mer de Chine du Sud ou encore le fait que des pirates

[1] "Live Cyber Threat Map" https://threatmap.checkpoint.com [dernière consultation 19 mars 2020]

[2] Notamment https://cybermap.kaspersky.com/fr/ ou https://www.deteque.com/live-threat-map/

[3] Il faut toutefois faire attention à différencier les différents types de cyber-opérations qui peuvent avoir lieu. En effet, toute attaque dans le cyberespace n'équivaut pas à un déclenchement d'une cyberguerre.

de l'armée populaire de libération (APL) chinoise aient attaqué des entreprises publiques, des ministères des affaires étrangères et des ministères des sciences et de la technologie dans de nombreux pays comme l'Australie, l'Indonésie, les Philippines, le Vietnam, la Thaïlande, le Myanmar et le Brunei.[4] La Belgique n'est bien sûr pas épargnée par ce genre d'attaques. En novembre 2019, les téléphones et ordinateurs des membres de la mission économique belge en déplacement à Pékin et Shanghai ont été hackés, probablement par des services de sécurité chinois.[5] Si nous revenons en particulier à la Chine le tableau en annexe, loin d'être exhaustif, montre de nombreux exemples de cyber attaques chinoises (certaines effectuées directement par l'APL - Unités 61368 et 61398) D'ailleurs la présidente de la commission européenne Von der Leyen a accusé le 22 juin lors du sommet UE-Chine, la Chine de cyberattaques contre des hôpitaux européens : « Nous avons vu des attaques… sur des systèmes informatiques, sur des hôpitaux, et nous connaissons l'origine des cyberattaques »[6].

Parallèlement, et bien que les cyberattaques de type DDoS, aient tout de même alerté la communauté internationale sur le potentiel du cyberespace, tout un pan du danger est souvent négligé. C'est sur ce dernier que repose les deux défis suivants, souvent sous-estimés alors qu'ils touchent aux fondements de nos démocraties : à savoir la guerre de l'information dans l'environnement informationnel [7] et la logique de la cyber-souveraineté défendue par la Chine.

2. LA GUERRE DE L'INFORMATION

L'information est devenue un moyen pour déstabiliser les pays et en particulier les démocraties, aussi bien par des acteurs externes mais également de plus en plus internes. Pour nos sociétés connectées et considérées comme des « sociétés de l'information », les menaces à l'information sont devenues des menaces à ces sociétés. Bien que la manipulation de l'information ne soit toutefois pas un phénomène nouveau, des pays comme la Russie et la Chine ont pris conscience que la crise de confiance dans les démocraties ainsi que la rapidité de diffusion qu'offrent internet et les réseaux sociaux, ouvraient de nouvelles opportunités. Comme le reconnait le neuroscientifique Giordano, « le cerveau humain est devenu le champ de bataille du XXI[e] siècle ». En s'appuyant sur des failles

[4] Center for strategic & international studies, "Significant Cyber Incidents Since 2006". https://csis-website-prod.s3.amazonaws.com/s3fs-public/200528_Significant_Cyber_Events_List.pdf

[5] Gosset, O., "Les services de sécurité chinois soupçonnés d'être derrière les récentes cyberattaques", *L'Echo*, 25 novembre, 2019.

[6] Cerulus, L., « Von der Leyen calls out China for hitting hospitals with cyberattacks », *Politico*, 22 juin 2020.

[7] Défini par l'armée américaine de la façon suivante : « est composé et agrège de nombreux attributs sociaux, culturels, cognitifs, techniques et physiques qui agissent sur les connaissances, la compréhension, les croyances, les visions du monde et, en fin de compte, les actions d'un individu, d'un groupe, d'un système, d'une communauté ou d'une organisation. [Et] comprend également les systèmes techniques et leur utilisation des données. » (JCOIE, 2018, p.42).

cognitives humaines comme le biais de confirmation (qui fait que nous avons tendance à privilégier les informations confirmant nos hypothèses) ou notre paresse intellectuelle naturelle qui consiste à ne pas exercer notre esprit critique de façon systématique, la manipulation des informations à travers l'environnement informationnel devient un moyen d'influence extrêmement dangereux en raison de la rapidité de diffusion de l'information. Ainsi, ce qui a changé n'est pas la façon dont réagissent nos cerveaux mais bien la quantité d'information à laquelle nous sommes exposés, la vitesse à laquelle elle se propage et la distance devenue quasi-inexistante.

Le déclin du leadership occidental, en particulier moral, la perte de confiance dans les élites politiques, le retour du populisme rendent les populations dans les démocraties vulnérables aux discours alternatifs et par conséquent aux manipulations indirectes via des acteurs internes (partis politiques, mouvements, …) au service de puissances étrangères ou directes de la part de ces dernières. Le défi pour Pékin est d'établir ainsi un discours légitime qui est accepté et partagé par une majorité, facilitant l'établissement d'une « identité commune » en altérant ou en manipulant les préférences[8]. Considérant, selon les études, que par exemple les Américains passent en moyenne plus de 11 heures par jour et les Belges plus de 9 heures à « écouter, regarder, lire, ou globalement interagir avec les médias »,[9] Pékin aurait embauché des « membres du Parti à 50 cents » afin qu'ils postent des commentaires fabriqués de toute pièce, mais comme s'il s'agissait de réelles opinions de citoyens chinois, sur les réseaux sociaux.[10] On a ainsi pu observer des campagnes de désinformation orchestrées par la Chine à l'égard de l'Australie, de la Nouvelle Zélande ou aujourd'hui de façon plus générale dans le contexte du coronavirus.

Les Chinois n'ont ainsi pas hésité à réinventer la narration du coronavirus. La quantité de désinformation concernant la pandémie COVID-19 est telle que l'Organisation Mondiale de la Santé (OMS) a déclaré faire face à une « infodémie ». En plus de venir de citoyens, cette infodémie provient également des Etats lançant des campagnes de manipulation de l'information dont notamment la Chine. « Il est possible que ce soit l'armée américaine qui ait apporté l'épidémie à Wuhan. Les États-Unis doivent être transparents ! Et doivent publier leurs données ! Les États-Unis nous doivent une explication ». Par la publication de ce tweet le 12 mars dernier sur le compte de Zhao Lijian, porte-parole des Affaires étrangères chinoises, ce dernier accuse Washington d'être à l'origine du coronavirus et de l'avoir

[8] Prys, M., « Hegemony, Domination, Detachment: Differences in Regional Powerhood », *International Studies Review*, vol. 12, n°4, 2010, p. 494.

[9] Insikt Group, "Beyond Hybrid War: How China Exploits Social Media to Sway American Opinion", *Recorded Future,* (2019:11. <go.recordedfuture.com/hubfs/reports/cta-2019-0306.pdf> (15 April 2019); « Le Belge passe la moitié de son temps éveillé à consommer des médias », *L'Echo*, 19 mai 2016.

[10] King, G., Pan, J., et Roberts, M.E., "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument", *American Political Science Review.* Vol. 111, n°3, 2017, p. 497.

introduit sur le sol chinois par son armée.[11] Ces accusations n'ont aucun fondement scientifique mais sont populaires dans les cercles conspirationnistes. Dans le journal *La Croix* du 8 mars, un article explique : « Aux yeux du Parti communiste chinois (PCC), que la Chine ait pu être pointée du doigt comme étant la source du coronavirus est inacceptable. Tout ce qui relie la Chine au virus doit être mis en doute et disparaître de tous les livres d'histoire. Ainsi tous les ambassadeurs chinois à l'étranger ont comme impératif de répandre à partir de leur compte Twitter (pourtant interdit en Chine)[12] ou dans les médias étrangers le message suivant : 'Si le coronavirus s'est bien déployé depuis Wuhan, son origine réelle reste inconnue. Nous sommes en train de chercher d'où il vient exactement' ».

Du fait de la (non)gestion de la crise par les autorités chinoises au tout début, Pékin a, dès le départ, perdu le contrôle sur le discours du coronavirus. En recourant aux théories du complot, fake news et autres de façon structurelle, le pouvoir chinois espère tout simplement rétablir ce contrôle[13]. Selon le Professeur Huang, membre du *Global Health at the Washington-based Council on Foreign Relations*: « Il n'est pas surprenant que le gouvernement cherche à contrôler la recherche scientifique connexe afin que les résultats ne remettent pas en cause sa propre narration sur l'origine du virus et la réponse du gouvernement à la crise », poursuivant en disant que « le danger est que lorsque la recherche scientifique est soumise aux besoins des personnes au pouvoir, il sape davantage la crédibilité du discours du gouvernement, rendant les accusations de sous-déclaration et de désinformation plus convaincantes ».[14] Selon Steve Tsang, directeur du *SOAS China Institute* de Londres, « le gouvernement chinois s'est concentré sur la façon dont l'évolution et la gestion du virus sont perçues depuis les premiers jours de l'épidémie ». De plus, « En termes de priorité, le contrôle de la narration est plus important que la santé publique ou les

[11] Ceci forme un parfait exemple de la nouvelle génération de diplomates chinois, appelés *Wolf Warriors* en référence à un film chinois d'action chinois de 2015. Ces diplomates sont très présents sur twitter pour défendre la ligne défendue par le PCC et n'hésite pas recourir aux théories du complot, la propagande …

[12] A ce sujet il est intéressant de suivre le compte twitter de l'ambassade chinoise en France, cette dernière n'hésitant pas à relayer de nombreuses théories du complot, à lancer des fake news afin de redorer l'image de la Chine. Toute réaction négative ou critique aux tweets de l'ambassade est accueillie par de la propagande et/ou des insultes. Certains chercheurs sont même bloqués. De nombreux comptes twitter ont été créés entre décembre 2019 et mars 2020 dans le cadre de cette campagne de désinformation menée par Pékin. Twitter a d'ailleurs fermé 170 000 comptes en juin 2020 « liés à une opération de propagande et de désinformation en ligne soutenue par Pékin »: « La firme américaine a retiré le cœur du réseau, composé de 23 750 comptes Twitter hautement actifs, ainsi que quelque 150 000 comptes périphériques chargés d' 'amplifier' le contenu diffusé par les comptes principaux ». (« Twitter supprime 170 000 comptes diffusant des messages favorables à la Chine », *Le Monde et Reuters*, 12 juin 2020).

[13] Lire également Struye de Swielande, T., "China: From coronavirus to conspiracy virus", *Commentary Paper*, n°65, March 19, 2020 ; Orinx, K., « COVID-19 : un virus au service du digital chinois ? », *Commentary Paper*, n° 67, 31 mars, 2020.

[14] Gan, N., Hu, C., et Watson, I., ''Beijing tightens grip over coronavirus research, amid US-China row on virus origin''. *CNN*, April 13, 2020. https://edition.cnn.com/2020/04/12/asia/china-coronavirus-research-restrictions-intl-hnk/index.html

retombées économiques ». « Cela ne signifie pas que l'économie et la santé publique ne sont pas importantes. Mais la narration est primordiale ».[15]

En outre, au contraire des États-Unis, la Chine axe sa narration sur l'optimisme dans la couverture médiatique de la pandémie. Alors que les médias américains ont tendance à souligner les nouveaux cas d'infections et les tendances des décès, les médias chinois rapportent le nombre de patients guéris et des exemples d'histoires positives. Par exemple, le *China Daily* a publié un article expliquant qu'une femme infectée par le coronavirus avait donné naissance à un bébé en bonne santé (non infecté), tandis que *CNN* a préféré publier l'histoire d'un autre bébé qui était devenu le plus jeune patient atteint du coronavirus.[16] Réalisant une analyse du discours, Molter et son équipe ont découvert que « du 31 décembre 2019 au 16 mars 2020, le terme 'infecté' était couramment utilisé à propos de 'patient' dans les médias américains et chinois. Cependant, au-delà de ce terme commun, il existe des divergences importantes, telles que les médias américains rapportant les patients comme 'malades' ou 'affectés', et les médias chinois mentionnant fréquemment des termes liés au traitement et au rétablissement comme 'traité', 'rétabli', 'ayant pu sortir de l'hôpital', 'guéri'».[17]

Cette volonté de réécrire le discours du coronavirus a un double objectif. En premier lieu, il s'agit de renforcer l'image dans certaines parties du monde déjà très anti-américaines et anti-occidentales (Moyen-Orient, Afrique...) que les États-Unis sont le grand Satan, renforçant ainsi les croyances de ces pays. Dans d'autres parties du monde, un tel discours sèmerait le doute, affaiblissant ainsi l'image des États-Unis. D'autre part, il s'agit de montrer à la population chinoise que le coronavirus est une attaque envers la Chine, renforçant le nationalisme et la fierté chinoise (*rallying around the flag*), ce qui à son tour permet au Parti communiste de se dédouaner de ses responsabilités dans le cas de la gestion de l'épidémie.

En conséquence de toutes ces actions, l'Occident est en train de perdre la guerre de la narration, en particulier sur les réseaux sociaux : vulnérabilité en raison de nos sociétés ouvertes[18] et difficultés à toucher aujourd'hui les sociétés fermées[19]. Comme l'a déclaré le

[15] Kirchgaessner, S., Graham-Harrison, E., et Kuo, L. ''China clamping down on coronavirus research, deleted pages suggest''. *The Guardian*, April 11, 2020. https://www.theguardian.com/world/2020/apr/11/china-clamping-down-on-coronavirus-research-deleted-pages-suggest

[16] Molter, V. ''Pandemics & Propaganda: How Chinese State Media Shapes Conversations on the Coronavirus''. *Stanford Cyber Policy Center, Internet Observatory*, 19 mars, 2020. https://cyber.fsi.stanford.edu/news/chinese-state-media-shapes-coronavirus-convo

[17] *Ibidem*

[18] Plus les activités de désinformation seront un succès, plus elles renforceront les « silos cognitifs » des extrêmes, et donc des partis politiques populistes. Ce qui aura comme conséquence un danger de paralysie politique, économique et social.

[19] Il faut également suivre une évolution inquiétante, à savoir une possible coordination entre la Russie et la Chine dans le domaine cyber. Si actuellement, il n'y a aucune preuve d'une coordination entre Moscou et Pékin dans le cadre de cyberattaques, les choses apparaissent plus complexes au niveau de la guerre de l'information.

colonel Qiao Liang, de l'APL, « La première règle de la guerre sans restriction est qu'il n'y a pas de règles, rien n'est interdit »[20]. Dans ce contexte, l'application de la « force écrasante » sur le « point décisif », telle que déterminée par Antoine-Henri de Jomini, est un bouleversement de la société : la population civile et les élites[21]. Cela concorde avec la pensée de Sun Tzu selon laquelle « vous pouvez être sûr de réussir vos attaques si vous n'attaquez que des endroits qui ne sont pas défendus » [22].

3. LA CYBERSOUVERAINETE

Dans un rapport de 2013 communément appelé « Document n ° 9 » (officiellement intitulé *Communiqué sur l'état actuel de la sphère idéologique*), la République Populaire de Chine (RPC) a affirmé que « la démocratie constitutionnelle occidentale est une tentative de dégrader le leadership actuel et le socialisme avec les caractéristiques chinoises du système de gouvernance » et a affirmé que les valeurs universelles occidentales sont « une tentative d'affaiblir le fondement théorique de la direction du parti »[23]. Le dernier paragraphe du document indique également, « nous devons renforcer la gestion de tous les types et de tous les niveaux de propagande sur le front culturel, perfectionner et mettre en œuvre les systèmes administratifs associés et ne laisser aucune possibilité ni aucun moyen de diffuser des idées ou des points de vue incorrects »[24].

Selon le président de la République populaire de Chine, Xi Jinping, « respecter la cybersouveraineté » implique « respecter le droit de chaque pays de choisir son propre chemin du développement Internet, son propre modèle de gestion Internet, ses propres politiques publiques en matière d'internet, et de participer sur un pied d'égalité à la gouvernance du cyberespace international - en évitant la cyberhégémonie et en évitant toute ingérence dans les affaires intérieures d'autres pays. … [Nous devons] mettre en place un

En effet, lors du COVID-19, on a pu constater que les Chinois relayaient les *fake news* et théories du complot russes et inversement, ce qui entraine un effet multiplicateur. On observe également une volonté chinoise de copier les tactiques russes de la désinformation. Il y a clairement une convergence d'intérêts à court terme pour affaiblir les sociétés occidentales de la part de ces deux grandes puissances.

[20] Liang et Xiangsui, *Unrestricted Warfare*, Beijing, People's Liberation Army Literature and Arts Publishing House, 1999, p. 2.

[21] Greathouse, C.B., "Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?," in *Cyberspace and International Relations: Theories, Prospects, and Challenges*, ed. Jan-Frederik Kremer and Benedikt Müller New York, Springer, 2014, p. 28.

[22] Sun Tzu, *The Art of War*, trans. Lionel Giles, London, Quarto, 2017, p.18.

[23] Document 9: A ChinaFile Translation—How Much is a Hardline Party Directive Shaping China's Current Political Climate?," ChinaFile, 8 November 2013.

[24] *Ibid.*

système de gouvernance multilatéral, démocratique et transparent pour l'Internet mondial »[25].

Dans la déclaration de Xi, le terme clé est « multilatéral ». Contrairement à l'actuelle approche multi-acteurs du cyberespace, qui est « l'implication sur un pied d'égalité de tous les acteurs ayant un intérêt direct dans Internet, y compris les entreprises et la société civile », la Chine défend vigoureusement l'idée opposée, en promouvant la gouvernance d'internet multilatérale ou intergouvernementale qui considère les États comme les principaux décideurs[26]. De plus, la cybersouveraineté a été décrite en 2015 par Xu Lin, chef de l'administration chinoise du cyberespace à l'époque, comme la différence entre l'approche multi-acteurs et l'approche multilatérale.[27]

L'idée sous-jacente derrière la logique de cybersouveraineté est de développer un système internet totalement fermé et contrôlé par les autorités et d'amener une souveraineté étatique dans l'espace cyber, à l'image du fameux ouvrage d'Orwell « 1984 ». Afin de promouvoir son modèle, la Chine organise des conférences, telles que la *World Internet Conference* et des séminaires de plusieurs semaines organisés pour les journalistes et politiques étrangers afin d'encourager les pays à diffuser la vision chinoise et à promouvoir son système de cybersouveraineté.

Ainsi, la Chine défend et promeut de plus en plus son modèle autoritaire et est disposée à exporter un « socialisme à caractéristiques chinoises », proposant ainsi une alternative au modèle libéral. À cette fin, elle renforce son pouvoir discursif en proposant de nouvelles idées, concepts et institutions afin de renforcer le contrôle de la définition des priorités régionales et internationales aux niveaux politique, économique et de la sécurité. C'est ainsi que Pékin persuade d'autres États à adopter sa vision de l'ordre mondial (avec quelques succès déjà dans des régions d'Afrique, d'Asie centrale et du Moyen-Orient). L'« autoritarisme numérique» est ainsi encouragé « comme un moyen pour les gouvernements de contrôler leurs citoyens par le biais de la technologie, inversant le concept d'internet comme moteur de la libération humaine».[28] À travers ce nouveau processus de socialisation, les États s'approprieront les normes imposées par la Chine, dont la source du *leadership* se situera dans les normes et valeurs qu'elle sera parvenue à internationaliser et, dans une certaine

[25] Remarks by H.E. Xi Jinping President of the People's Republic of China at the Opening Ceremony of the Second World Internet Conference, Wuzhen, 16 December 2015.

[26] Raud, M., *China and Cyber: Attitudes, Strategies, Organization,* Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016, p. 15; Gady, F.-S., "The Wuzhen Summit and the Battle over Internet Governance," *The Diplomat* (website), 14 January 2016. https://thediplomat.com/2016/01/the-wuzhen-summit-and-the-battle-over-internet-governance/.

[27] Gady, F.-S., "The Wuzhen Summit and the Battle over Internet Governance", *op. cit.*

[28] Shahbaz, A., "The Rise of Digital Authoritarianism," in *The Rise of Digital Authoritarianism*, New York, Freedom House, October 2018, p. 2.

mesure, à institutionnaliser[29]. Ainsi, en se positionnant ouvertement comme alternative, la Chine attire *de facto* à elle les puissances insatisfaites par l'ordre international, mais ne pouvant pas s'y opposer directement[30].

C'est aussi d'ailleurs un des enjeux de la *Digital Silk Road,* partie intégrante des Nouvelles routes de la Soie chinoise, qui comprend outre cette question de souveraineté, les questions liées à la 5G, les normes de télécommunication de demain et l'intelligence artificielle.

4. LES NOUVELLES TECHNOLOGIES

Facebook, Twitter, Google, Wechat contre Alibaba, Sina Weibo, Baidu et RenRen. Demain, le leadership mondial sera déterminé par la maitrise des technologies avancées (intelligence artificielle -IA, semi-conducteurs, informatique quantique[31], biotechnologie, cyber, 5G…)[32]. L'avantage occidental dans ces domaines se rétrécit rapidement : « Grâce à un marché intérieur protégé, aux transferts de technologie forcés par des sociétés occidentales, à l'espionnage industriel pur et simple et au vol de propriété intellectuelle, la Chine se forge des champions technologiques conçus pour concurrencer et surpasser leurs concurrents internationaux. Grâce à des mandats légaux qui forcent la coopération des entreprises avec les organes de sécurité et de renseignement, les entreprises technologiques chinoises sont les yeux et les oreilles de Pékin dans une économie mondiale numérique. Ce modèle fait appel aux despotes du monde entier, tandis que les prix bon marché plaisent à tout le monde. Ne vous méprenez pas sur les enjeux existentiels de savoir si des sociétés ouvertes ou des régimes autoritaires détermineront le cours de l'avenir technologique ». [33]

[29] Pour plus de détails sur la socialisation lire, Struye, T. et Vandamme, D., « Modernizing Holsti into the 21st Century », in Struye de Swielande, T. et Vandamme, D. (eds.), *Power in the 21st Century. Determinants and Contours*, Presses universitaires de Louvain, Louvain-la-Neuve, 2015; Vandamme, D. et Struye, T., «Global Swing States: Which Leadership Will They Follow? », in Struye de Swielande, T. et Vandamme, D. (eds.), *Power in the 21st Century. Determinants and Contours*, Presses universitaires de Louvain, Louvain-la-Neuve, 2015 ; Struye de Swielande, T., *Duel entre l'aigle et le dragon pour le leadership mondial*, Peter-Lang, Bruxelles, 2015.

[30] Ce n'est pas un hasard si la Chine s'intéresse tant aux organisations régionales et internationales : en y étant fortement active elle y détermine souvent l'agenda et par conséquent les normes et règles de demain. La Chine occupe actuellement la direction de cinq agences des Nations Unies, dont l'Union internationale des télécommunications (UIT), spécialisée dans les technologies de l'information et de la communication. Et quand son influence est trop limitée, la Chine crée de nouvelles institutions ou fora. [Lire à ce sujet, T. Struye, « La grande stratégie chinoise et la BRI », dans *La Chine et les Nouvelles Routes de la Soie : une politique impériale ?* (Direction Tanguy Struye de Swielande & Kimberly Orinx), Coll. Scène internationale, Presses universitaires de Louvain, Louvain-la-Neuve, 2019].

[31] Allison, K. , "Why quantum computing could be a geopolitical time bomb", *GZEROmedia*, November 05, 2019.

[32] Vladimir Poutine (2017): « Le leader en intelligence artificielle dominera le monde ».

[33] Rogers, M. et Nye, G., "Why America must boldly win the technological race against China", *The Hill*, October 21, 2019.

Il s'agit d'être le first mover et la Chine l'a bien compris. La Chine investit massivement dans les nouvelles technologies, l'objectif étant de devenir n°1 en 2030. Cinq entreprises ont été désignées pour mener cette révolution technologique : Baidu, Alibaba, Tencent, iFlytek et SenseTime. Ces sociétés bénéficient d'aides publiques importantes en raison du capitalisme d'Etat et leur lien avec le Parti communiste chinois. D'autant plus qu'il y a une obligation pour les entreprises d'avoir en leur sein une cellule du parti communiste. La question légale se trouve également en lien avec les nouvelles technologies au travers de la *cybersecurity law* entrée en vigueur en Chine dès 2017. Cette loi, qui s'applique à l'ensemble des opérateurs de réseaux et aux entreprises engagées dans les communications, les services d'information, l'énergie, les transports, les services financiers, etc., contraint notamment les entreprises à coopérer avec les services de sécurité chinois et à autoriser l'accès complet aux données à la moindre demande des autorités gouvernementales.[34] Ce qui pourrait donc passer pour un détail au premier abord, puisqu'il s'agit d'une simple loi nationale, peut en réalité avoir un impact sur toute collaboration avec des entreprises chinoises[35].

Toujours dans le domaine légal, une réglementation dans nos sociétés occidentales massive et complexe, et lourde administrativement pourrait également ralentir nos entreprises et les rendre moins compétitives : « la concurrence technologique exige aujourd'hui des réformes allant de politiques d'acquisition et d'achat plus favorables à l'innovation à un soutien accru à la recherche fondamentale. La collaboration entre les laboratoires nationaux et le secteur privé est également impérative, tout comme la coopération avec les partenaires économiques et de sécurité les plus proches ».[36] Cela dit, les sociétés libres encouragent les inventions, les innovations, l'autonomie et l'initiative ce qui est plus complexe dans des sociétés autocratiques telle que la Chine.

Les Chinois déposent, en outre plus de brevets dans les technologies de l'IA, et diplôment trois fois plus d'informaticiens (185 000 contre 65 000) et quatre fois plus d'étudiants STIM (science, technologie, ingénierie et mathématiques) que les États-Unis (1,3 million contre 300 000).[37] Ainsi, les entreprises et organisations chinoises « détiennent près d'un tiers des brevets internationaux dans le domaine de l'intelligence artificielle, représentent plus d'un cinquième des dépenses mondiales de R&D et sont l'auteur de plus d'un cinquième des

[34] Wagner, J. (2017, June 1st). "China's Cybersecurity Law: What You Need to Know". *The Diplomat.* Retrieved from https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/

[35] La société chinoise étant moins individualiste et faisant plus appel au sens de la communauté et de la hiérarchie (Confucianisme, légisme) sera plus loyal au PCC, d'autant plus que le PCC se présente aujourd'hui comme nationaliste et moins comme communiste ; par conséquent, il existe un nationalisme pas seulement top-down, mais également bottom-up.

[36] Rogers, M. et Nye, G., "Why America must boldly win the technological race against China", *The Hill*, October 21, 2019.

[37] Allison, G.*, loc. cit.*

publications mondiales évaluées par des pairs (dont un grand nombre sont co-publiées avec des collaborateurs américains) ».[38]

Les Chinois sont également numéro un en fintech. WeChat Pay de Tencent (pour payer les factures, transférer de l'argent, contracter des emprunts, faire des investissements, faire des dons à des œuvres de bienfaisance et gérer des comptes bancaires) compte neuf cent millions d'utilisateurs chinois, tandis qu'Apple Pay n'en compte que vingt-deux millions aux États-Unis.[39] L'autorité chinoise à travers entre autres son système de crédit social a de plus amassé des mégadonnées, qui seront utiles pour étudier le comportement des consommateurs : le profilage de 1,3 milliards de personnes. Sensetime est l'un des leaders de la reconnaissance faciale ; Hikvision et Dahua Technology contrôlent un tiers du marché mondial des caméras de sécurité ; et Tiandy et Wuhan Guide Infrared, sont spécialisés dans l'imagerie infrarouge et thermique[40]. Comme Allison l'observe dans une société autoritaire comme la société chinoise, la reconnaissance faciale est égale au contrôle et au profit, dans les démocraties, les choses sont plus compliquées : elles ont « concédé la course en raison de préoccupations concernant la vie privée de l'individu ordinaire et de profondes réserves sur la façon dont cette technologie pourrait être déployée »[41].

Dans le but de devenir leader dans le domaine de l'IA d'ici 2030, la Chine a d'ailleurs profité de la situation entourant le coronavirus pour utiliser toutes les avancées déjà réalisées, par exemple au niveau de l'analyse des données, du *machine learning, deep learning,* ou encore dans la reconnaissance faciale, comme arme contre le nouveau Covid. Ainsi, la Chine en a profité pour augmenter la surveillance de sa population suite aux mesures prises pendant la quarantaine imposée suite au coronavirus. Par exemple, des caméras infrarouges ont été posées sur les casques-intelligents de policiers, des systèmes de caméras 'moins futuristes' ont été placés dans les gares et certaines stations de métro permettant ainsi de détecter automatiquement la température corporelle des voyageurs et le système de reconnaissance faciale a été également mis à profit pour vérifier que les gens portaient bien leur masque (port rendu obligatoire en Chine). En mettant en avant sa bonne gestion de la crise et le fait que ses mesures particulièrement restrictives aient fait leurs preuves quant à l'endiguement du virus, la Chine ne peut que mieux vendre son système. La Russie profite d'ailleurs, elle aussi, de la pandémie actuelle pour précipiter l'utilisation en masse de la technologie et de la reconnaissance faciale pour surveiller sa population.[42]

---

[38] Taylor, J., "Need to reimagine strategic narratives about China", *ANU*, December 1, 2019.

[39] Allison, G., *loc. cit.*

[40] *Ibidem.*

[41] *Ibidem.*

[42] Ilyushina, M. "How Russia is using authoritarian tech to curb coronavirus". *CNN*, March 29, 2020 https://edition.cnn.com/2020/03/29/europe/russia-coronavirus-authoritarian-tech-intl/index.html?utm_medium=social&utm_source=fbCNNi&utm_content=2020-03-29T08%3A50%3A38&fbclid=IwAR0BZ3kTpeyea1JNAON9sylXjeqM0mJH3F1F2DnaVjibzCB7cH0tapd5UFE

Enfin, la Chine est devenue également un joueur majeur dans la pose de câbles sous-marins : « Les fournisseurs de télécommunications d'État chinois China Unicom, China Telecom et China Mobile sont propriétaires du nouveau câble SeaMeWe-5 reliant l'Europe, le Moyen-Orient et l'Asie du Sud-Est. China Unicom possède également en partie un câble reliant le Cameroun et le Brésil. Et Huawei Marine Systems - une joint-venture entre Huawei et la société britannique Global Marine Systems - construit de tels câbles à travers l'Afrique »[43]. L'objectif de la Chine n'est pas uniquement de voler les données mais également de dominer la construction et les futures modernisations des infrastructures de communication qui serviront l'e-commerce, l'e-finance…[44].

5. MATIERES PREMIERES

La 5G, les semi-conducteurs, les fermes de stockage de données (datacenters), les ordinateurs quantiques, les téléphones portables, l'IA, les voitures et villes intelligentes[45], les énergies renouvelables (solaire, éoliennes…) tous ont des terres rares dans leurs composantes. La Chine contrôle le marché des terres rares indispensable aux technologies avancées : 80% de la production mondiale et 40% des réserves mondiales[46]. Dès les années nonante la Chine avait compris l'importance des terres rares, ainsi en témoigne les propos de Deng Xiaoping en 1992 : « Le Moyen-Orient a du pétrole et la Chine des terres rares ». Les terres rares comprennent 17 éléments[47]. Bien qu'elles ne soient pas rares, le processus d'extraction est complexe et très polluant et elles sont dispersées en petites quantités dans de nombreuses parties du monde. Le quasi-monopole sur la production des terres rares permet à la Chine de contrôler le marché : réduction des exportations pour exercer des pressions sur certains Etats, diminution des prix afin d'éviter que d'autres mines dans le monde soient rentables… En recourant à ces moyens la Chine fait tout en la matière pour veiller à ce que les autres Etats restent dépendant de la Chine. L'Europe, les Etats-Unis, le Japon… essaient de contrer le monopole chinois en (r)ouvrant des mines (Mountain Pass aux Etats-Unis, Mount Weld en Australie)[48], en promouvant le recyclage (mais qui est quasi inexistant) et en développant des matériaux alternatifs, mais sans grand succès jusqu'à présent. Ces pays ont en outre encore des difficultés à établir des réserves stratégiques de terres rares.

[43] Gorman, L., "A Silicon Curtain is Descending: Technological Perils of the Next 30 Years", German Marshall Fund, 2019, p. 76.

[44] Spengler, "US-China tech war and the US intelligence community", *Asia Times*, July 8, 2019

[45] A ce sujet, le 23 juin 2020, la Chine a finalisé Beidou (GPS chinois) -lequel s'appuiera sur la 5G- en lançant le dernier satellite des 30 nécessaires, renforçant encore plus sa volonté de totale indépendance technologique.

[46] Site le plus important de production : Baotou (Mongolie intérieure), gisement minier de Bayan Obo.

[47] Lanthane, Cérium, Praséodyme, Néodyme, Prométhium, Samarium, Europium, Gadolinium, Terbium, Dysprosium, Holmium, Erbium, Thulium, Yterrbium, Lutécium, Yttrium et Scandium.

[48] Souvent ces mines ne sont pas rentables et referment aussitôt. De plus Pékin entend bien faire main basse sur tous ces gisements étrangers pour un prix très intéressant. Vu que les mines ne sont soit plus exploitées soit exploitées à perte. (Pitron, G., *La guerre de métaux rares*, Les liens qui libèrent, 2018, p.228-229)

Que ce soit pour les terres rares ou d'autres ressources nécessaires pour les nouvelles technologies *lato sensu* (le lithium, le cobalt, le coltan…), mais aussi le pétrole, le charbon, le gaz ou les renouvelables [49] la lutte ne fait que commencer, renforçant le risque de déstabilisation de certaines régions d'Afrique, d'Asie centrale, du Moyen-Orient et d'Amérique latine. L'enjeu est tel que l'exploration et bientôt l'exploitation sous-marine deviendra le nouvel eldorado potentiel[50], sans oublier l'Arctique et l'Antarctique (avec toutes ses conséquences environnementales) – partout les Chinois s'y positionnent comme les pierres sur le *goban* du jeu de Go.

6. CONCLUSION : NECESSITE D'UNE REACTION OCCIDENTALE

A travers cette brève analyse, nous observons que la Chine a une approche holistique par rapport aux nouvelles technologies et leurs enjeux[51]. Nous rejoignons Berard, Fayoll et Pahud qui dans leur ouvrage, *Guerres économiques pour l'intelligence artificielle* démontrent de manière très convaincante que tout est lié et qu'il s'agit pour la Chine de contrôler toute la chaine de valeur : ressources, technologies et usages. Comme les auteurs l'expliquent l'enjeu géoéconomique est double : 1) Conquérir par les ressources : main d'œuvre, matières premières, brevets, moyens financiers et la maitrise des canaux de communication et 2) Séduire par l'influence culturelle, le modèle économique et sociétal, et par la diplomatie[52]. Leur étude démontre en outre que la Chine pourrait bientôt contrôler l'ensemble de la chaine de valeur, que les Etats-Unis sont vulnérables dans le domaine des matières premières devant se reposer sur leurs alliés tels que l'Australie. Quant à l'UE, elle a d'énormes retard sur ses concurrents sur toute la chaine de valeur (mines, investissements insuffisants dans les technologies, pas d'écosystème propre ou cloud)[53].

A travers ces politiques le projet chinois, nous apparait toutefois encore plus ambitieux : la Chine tente non seulement de redéfinir les normes, les règles et standards économiques de demain mais également ceux de la gouvernance en promouvant son modèle de régime autoritaire. Il s'agit ainsi pour la Chine de faire accepter sa place comme légitime en proposant une alternative à l'ordre libéral, qui serait à son image. La mise en place d'un régime international permettrait à la Chine d'introduire des mécanismes d'autorégulation internes

[49] Toutes ces nouvelles technologies sont énergivores.

[50] et probablement la lune dans un futur proche.

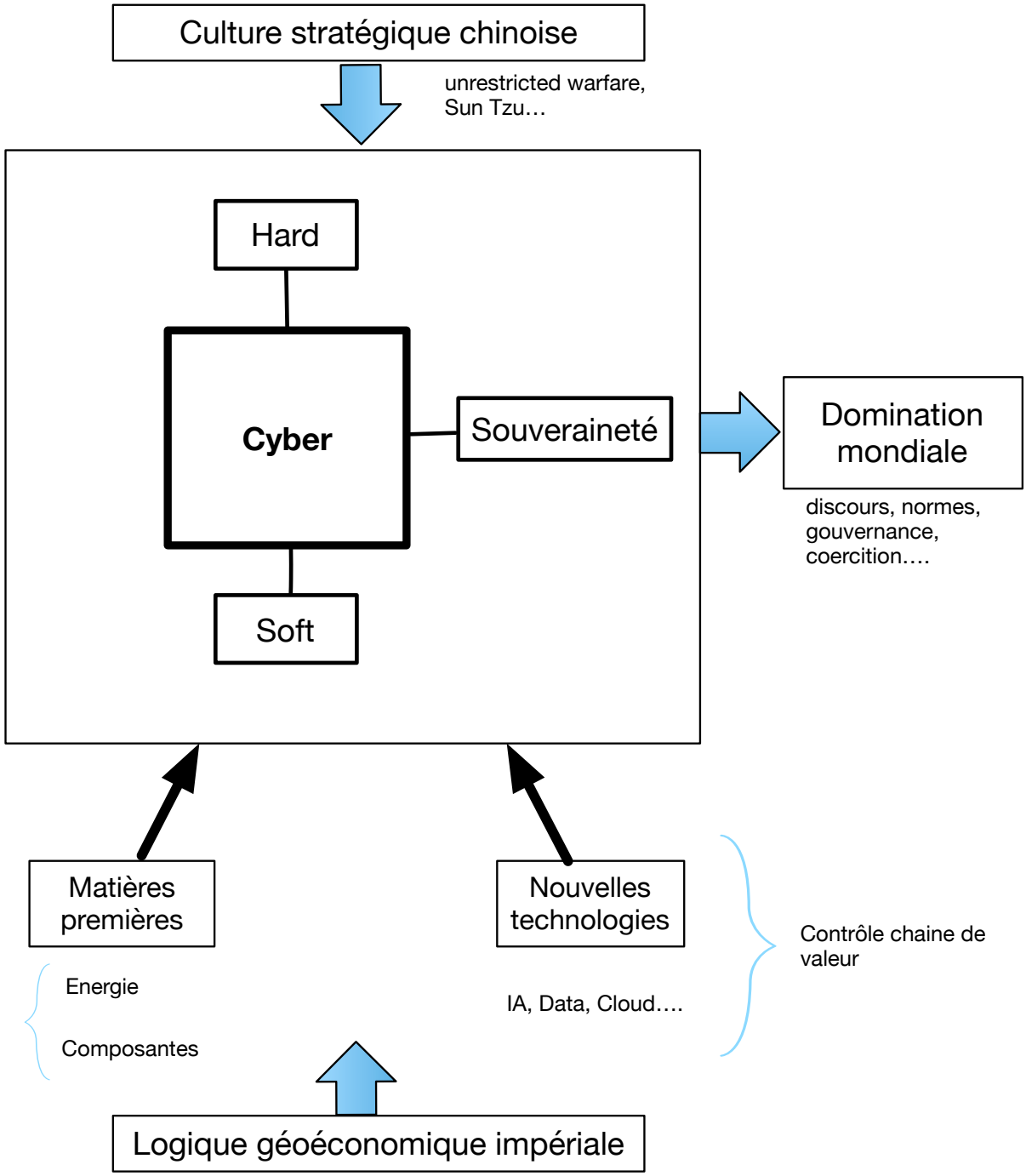
[51] Pour une analyse comparative entre les approches chinoise et américaine/occidentale envers le cyber lire : Orinx, K. et Struye, T., "A Chinese Fox against an American Hedgehog in Cyberspace?", *Military Review*, Vol. 100, n°5, Sept-Oct, 2019.

[52] Berard, B. Fayolle, C., et Pahud, B., *Guerres économiques pour l'intelligence artificielle*, Collection Guerre de l'information, V.A. Editions, 2018, p. 15.

[53] *Ibid.*, p. 258.

au régime réduisant la marge de manœuvre des États qui en sont partie prenante, et délégitimant les États qui ne s'y conformeraient pas.

Figure 1 : Approche holistique du cyber



Par rapport à cette approche holistique chinoise, les pays occidentaux se rendent eux-mêmes vulnérables en adoptant une approche souvent trop cloisonnée et linéaire. Au niveau cyber, Pékin a une vision intégrée, dans une logique de guerre hybride, dont nous ne mesurons pas les conséquences sur nos sociétés démocratiques. D'autant plus que son approche rend la frontière entre paix et guerre extrêmement floue. Face à cela, l'approche occidentale se retrouve limitée tant dans l'aspect offensif que défensif. Or, l'impact sociétal négatif sur nos sociétés démocratiques est colossal et ces dernières ne parviennent pas à trouver des réponses adéquates. Aussi, parait-il urgent de développer une stratégie intégrale et multidimensionnelle au niveau européen et otanien qui prenne en considération les trois défis du cyber *sensu stricto* (hard, soft et cybersouveraineté) : cela demandera des investissements importants de la part des gouvernements (en particulier en matière de défense et de renseignement), de dépasser les clivages bureaucratiques et divisions étatiques. Quelques pistes concrètes sont le développement d'une contre-narration plus agressive et plus ciblée, tenant compte des écosystèmes nationaux, régionaux et systémiques, garantir un internet ouvert, là où il est mis en danger par des puissances telles que la Chine, encourager la collaboration industrielle transatlantique pour être compétitif face à la 5G chinoise, contrer les Nouvelles routes de la Soie, dont la Nouvelle route de la Soie digitale, en continuant à développer la politique européenne de connectivité Europe-Asie lancée en 2018, en incluant outre le Japon, d'autres puissances partageant les mêmes approches normatives. Cette stratégie holistique ne pourra aboutir que si les différents acteurs se parlent et se concertent afin d'utiliser les ressources et les moyens de manière intelligente et efficace.

Mais cela ne suffira pas si nous n'avons pas des politiques plus cohérentes et agressives concernant les métaux précieux et les nouvelles technologies. *Primo*, il faudra éviter, en raison également des conséquences du COVID-19, que la Chine fasse main basse sur les joyaux industriels que ce soit les grandes entreprises minières ou high tech. *Secundo*, il faudra avoir le courage politique d'envisager la réouverture de certaines mines de terres rares afin de ne plus dépendre autant de la Chine et de potentielles intimidations ou chantages. *Tertio*, même si cela a été peu abordé dans cette recherche, continuer à investir dans l'éducation et la R&D, et par conséquent augmenter les budgets de l'éducation afin de former les jeunes aux métiers de demain (géophysiciens, ingénieurs, chimiste, logisticien, programmeurs, électroniciens, mathématiciens, linguistes…). et établir des partenariats privé-public pour créer des chaires sur l'IA, sur l'enjeu des matière premières etc. Enfin, il faudra également investir beaucoup plus dans la prospection stratégique. La cécité politique et stratégique a comme conséquence une vacuité stratégique, compris comme l'incapacité d'anticiper les mouvements, phénomènes, tendances pourtant inévitables. Les décideurs politiques risquent de continuer de nous entraîner dans des politiques réactives et à court terme, avec pour conséquence un affaiblissement généralisé de l'Etat et une situation socio-économique de plus en plus instable : « Il n'est pas de vents favorables pour celui qui ne sait pas où il va » (Sénèque).

Annexe 1: Exemples de cyber attaques contre la Belgique, membres de l'UE (données récoltées par Vincent Gabriel, stagiaire au CECRI de février à mai 2020)

Cyberattaques subies par la Belgique venant de Chine

Où ?	Quoi ?	Source
Attaques régulières contre des ordinateurs belges ayant entrainé une réaction en 2008.	Jo Vandeurzen, alors Ministre de la Justice, affirme avoir des preuves que ces attaques sont liées au Parti Communiste chinois. UK, France, Allemagne, se joignent à cette dénonciation.	GOODIN, D., « India and Belgium decry Chinese cyber attacks » dans *The Register*, 8 mai 2008.
Chine, novembre 2019	La mission belge en déplacement en Chine (Pékin et Shanghai) a été la cible d'une attaque en novembre 2019. Les téléphones et ordinateurs des membres ont été piratés. Il s'agit probablement des services de sécurité chinois.	GOSSET, O., « Les services de sécurité chinois soupçonnés d'être derrière les récentes cyberattaques » dans *L'Echo*, 25 novembre 2019.
	135 attaques par heure ont été enregistrées	BELGA, « La mission économique belge en Chine cible de cyberattaques massives » dans *Le Soir*, 23 novembre 2019.
	Témoignage de Geert Baudewijns, cyber-expert présent.	« Des belges victimes de cyber-attaques en Chine » dans *DataNews*, 25 novembre 2019.

Cyberattaques venant de Chine contre des pays de l'UE

Où ?	Quoi ?	Source
Attaque contre la *House of Commons*, 2006		TIKK, E., "Ten Rues for Cyber Security", https://citizenlab.ca/cybernorms2011/rules.pdf. WARREN, P. (18 Jan 2006) "Smash and grab, the hi-tech way," The Guardian
UK, Novembre 2007	Dénonciation d'attaques contre des secteurs vitaux de l'économie britannique	BALL, D., « China's Cyber Warfare Capabilities" dans *Security Challenges*, vol. 7, n°2, Hiver 2011, p. 89
Cheval de Troie au sein de programmes de la suite Word dans les ordinateurs de plusieurs gouvernementsd ont Allemagne (2007).	Hackage du bureau de Merkel, contenu dans la suite office.	BALL, D., « China's Cyber Warfare Capabilities" dans *Security Challenges*, vol. 7, n°2, Hiver 2011, p. 90. "Espionage Report: Merkel's China Visit Marred by Hacking Allegations," (27 Aug 2007) Spiegel

France, novembre-décembre 2010	Ministère des Finances, environ 150 ordinateurs pénétrés et documents au sujet du G20 consultés. Des traces d'un cheval de Troie ont été retrouvés dans près de 10 000 ordinateurs en mars 2011.	
L'UE au G20 en Russie, 2013.	C'est la compagnie de sécurité américaine FireEye qui a détecté cela. Cela aurait eu lieu lors des réunions du G20 : différents pays ont reçu des mails infectés au sujet d'une intervention américaine en Syrie. Le groupe de hackers est Ke3chang, déjà à l'origine d'un mail lié aux JO de 2012 ou en 2011, avec des photos de nu de Carla.	« Offensive de pirates informatiques chinois contre des diplomates européens » dans *L'Express*, 10 décembre 2013.
Royaume-Uni, entre 2014 et 2017	Plusieurs entreprises ont été attaquées par la campagne Cloud Hopper, par le groupe APT10.	« 'Serious' hack attacks from China targeting UK firms » dans *BBC News*, 3 avril 2017
Allemagne, 2017	L'Allemagne, par son agence de renseignement, accuse la Chine d'utiliser des faux profils linkedin pour recruter des informateurs	« German spy agency warns of Chinese LinkedIn espionage » dans *BBC News,* 10 décembre 2017.
Ecosse, 2017	Cyberattaque contre le parlement écossais	HUTCHEON, P., « China accused of being behind recent cyber attack on Scottish Parliament » dans *The Herald Scotland*, 17 septembre 2017.
Royaume-Uni, à partir d'avril 2017.	Des think tanks britanniques auraient fait l'objet d'attaques chinoises.	CORERA, G., « UK think tanks hacked by groups in China, cyber-security firm says » dans *BBC News*, 26 février 2018.
Communications diplomatiques de l'UE (découvert en décembre 2018)	Le réseau diplomatique aurait été piraté pendant trois ans. Technique similaire à une cellule de l'armée chinoise.	D'ALANÇON, F., « L'Union européenne ciblée par des hackers chinois » dans *La Croix*, 19 décembre 2018.
	Brèche découverte par la compagnie Area 1, les documents interceptés sont des câbles diplomatiques.	« European Union diplomatic communications 'targeted by hackers'" dans *BBC News*, 19 décembre 2018.
	Sont également touchées les Nations Unies, …	JOHN ROBERTS, J. et HACKETT, R., "Chinese Hackers Stole Diplomatic Cables, Report Says. Here's How They Did It" dans *Fortune*, 19 décembre 2018.
Airbus, janvier 2019	« incident de cybersécurité » sans conséquence. Dans le courant de l'année, l'entreprise sera frappée par trois autres attaques d'envergure.	REUTERS, « Airbus a détecté un incident de cybersécurité, pas d'impact » dans *Challenges*, 30 janvier 2019. « Airbus ciblé par une série de cyberattaques, la Chine soupçonnée » dans *Les Echos*, 26 septembre 2019.
Norvège, 2019	Un article paru en février 2019 explique que la Chine (campagne Cloudhopper) a volé les données de Visma, une entreprise de software. Elle a probablement eu lieu en décembre 2018.	STUBBS, J., « China hacked Norway's Visma to steal client secrets: investigators » dans *Reuters*, 6 février 2019.
Attaques contre plusieurs des plus grandes entreprises dans le service de la technologie en juin 2019.	A entrainé une réponse de la Présidence finlandaise de l'Union Européenne	BOFFEY, D., « EU to run war games to prepare for Russian and Chinese cyber-attacks » dans *The Gardian*, 27 juin 2019.
Allemagne, juillet 2019	Plusieurs entreprises (BASF, Siemens, Henkel) victimes de cyberattaques, très probablement venues de Chine, avec le groupe Winnti. Rheinmetall a été attaquée aussi, sans certitude que cela vienne de la Chine	HUMMEL, T., « Shares in Rheinmetall drop after company discloses malware attack » dans *Reuters*, 27 septembre 2019.
France, septembre 2019	Airbus a été la cible d'attaques, notamment contre ses sous-traitants tels qu'Expleo.	

	La cible était des « documents techniques relatifs à la certification des avions du géant européen ». Méthode très proche du groupe APT10, un groupe de hackers.	IZAMBARD, A., « Cyberattaques contre Airbus : pourquoi la Chine est soupçonnée » dans *Challenges*, 27 septembre 2019.
Rolls-Royce	A été la cible des mêmes attaques. On soupçonne des membres de ces entreprises d'avoir collaboré avec les services de renseignement chinois.	
Allemagne, 23 décembre 2019	Un groupe APT20, lié au gouvernement chinois, a vu son activité signalée par Fox-IT, une entreprise de cybersécurité.	MELLO, J., Cyberwarfare Report, vol. 4, n°4 : *Chinese and Iranian Hacking Spikes, Mobile App Spyware* dans *Cybercrime magazine*, https://cybersecurityventures.com/q1-2020-cyberwarfare-report-chinese-and-iranian-hacking-spikes-mobile-app-spyware/

Les recherches du CECRI sont menées au sein de l'Institut de science politique Louvain-Europe (ISPOLE) de l'Université catholique de Louvain. Elles portent sur la géopolitique, la politique étrangère et l'étude des modes de prévention ou de résolution des crises et des conflits.

L'analyse des éléments déclencheurs des conflits et des instruments de leur gestion - sanctions et incitants économiques comme moyens de politique étrangère; crises et interventions humanitaires; rôle de la mémoire dans un processus de réconciliation, par exemple - est combinée à l'étude empirique de différends internationaux et de processus de paix spécifiques.