LA CYBERPUISSANCE CHINOISE

Illusion ou réalité ?

RÉDIGÉ PAR

Maxime Boury
Margaux Collot
Tiphaine Dieudonné
Bastien Humbert
Téo Lacharmoise
Arnaud Sers
Mélanie Y Breh Hwing

EGE

5 juin 2022

SOMMAIRE

EXECUTIVE SUMMARY

Le travail de recherche sur la cyberpuissance chinoise, réalisé par les étudiants de la quatrième promotion en Risques, Sûreté Internationale et Cybersécurité de l'École de Guerre Économique, décrit les différents outils dont dispose l'État chinois, et ceux qu'il développe, pour remplir son ambition : s'affirmer comme une grande puissance dans le champ cybernétique. L'objectif est de proposer une grille de lecture critique pour comprendre au mieux les connexions et interactions entre les intérêts économiques, politiques et militaires liés à la notion de numérique et du cyber en Chine.

La Chine veut depuis longtemps garder ses prérogatives en matière de contrôle de l'information pour légitimer le pouvoir politique. Le gouvernement chinois étend depuis 2015 les buts de sa stratégie cyber. Il applique un contrôle de l'information, auquel s'ajoute premièrement la volonté d'influer sur l'architecture du cyberespace, notamment par le levier normatif ; puis la volonté de contrer les autres puissances mondiales (notamment les États-Unis) et enfin la volonté de défendre les intérêts économiques et militaires chinois. La politique cyber chinoise évolue en fonction de la géopolitique mondiale et part d'une position défensive sous Hu Jintao puis voit dans l'affaire Snowden un point de bascule. Sous Xi Jinping depuis 2013, la Chine développe une politique cyber active. Elle vise à gagner en autonomie vis-à-vis des américains, à défendre les intérêts nationaux par l'utilisation des moyens cyber et enfin à encourager l'innovation nationale.

La Chine met alors ostensiblement en place un nouveau type de modèle, qui surpasse le cadre du numérique pour s'étendre à des questions de modèle de société. Parmi les objectifs du gouvernement, on retrouve donc la mise en place d'un cadre normatif, qui expose le contexte doctrinal et l'accompagnement juridique du domaine cyber de la Chine. Pour cela, le PCC a peu à peu pris conscience de l'importance du numérique ces dernières années. Le pays est d'ailleurs passé à une stratégie de défense active afin de répondre au mieux à ce nouvel enjeu cyber. Ensuite, le développement économique du pays et notamment des entreprises est rendu possible grâce à l'absence d'un cadre législatif international clair dans le domaine cyber. Les entreprises chinoises peuvent ainsi librement se servir du numérique comme d'une arme face à leurs compétiteurs. De plus, cet aspect économique permet de

servir les intérêts politiques du gouvernement chinois, qui souhaite aller vers une souveraineté numérique de la Chine. À cela s'ajoutent également le rôle des universités chinoises et de la R&D qui permettent d'affirmer les aspirations d'hégémonie chinoise en termes d'innovation. Enfin, le numérique chinois sert un objectif de maintien de la stabilité du pays et de contrôle de la population, qui passe par la diffusion d'un modèle politique à travers le monde et la montée en puissance militaire. La Chine se base effectivement sur une interdépendance entre le civil et le militaire. La chaîne de commandement et les motivations en matière de cyberdéfense du pays sont complexes. Il existe de multiples unités et opérations des autorités chinoises pour s'approprier les technologies étrangères. Celles-ci ont été impactées au fil du temps par les réformes successives de l'APL pour s'adapter aux nouveaux enjeux cyber. Plus qu'une simple affirmation de souveraineté, c'est une volonté ferme de projection de cyberpuissance qu'effectue la Chine.

GLOSSAIRE

3/PLA : PLA General Staff Department's Third Department

4/PLA : PLA General Staff Department's Fourth Department

AIEA : Agence internationale de l'énergie atomique

BAT : Bureau des Affaires Taïwanaises

BATXH : Baidu Alibaba Tencent Xiaomi Huawei

BM : Banque Mondiale

BPC : Banque populaire de Chine

BPF : Berkeley Packet Filter

BRI : Banque des règlements internationaux

C4ISR : Space-based command, control, communications, computers, intelligence, surveillance, and reconnaissance

CAS : Chinese Academy of Science

CAC : Cyber Administration of China

CCAC : Commission centrale pour la cybersécurité et l'informatisation

CCDI : Commission Centrale d'Inspection de la Discipline

CERT : Computer emergency response team

CETC : China Electronic Technology Corporation

CGAP : Consultative Group to Assist the Poor

CIPS : China International Payments System

CMC : Commission Militaire Centrale

CMI : Civil–Military Integration

CNE : Computer Network Exploitation

CNNIC : China Internet Network Information Center

CNO : Computer Network Operation

CNUDCI : Commission des Nations unies pour le droit commercial international

CPA : Cour permanente d'arbitrage

CSIRT : Computer Security and Incident Response Team

DIA : Defense Intelligence Agency

DOD : Department Of Defense

DSR : Digital Silk Road

EW : Electronic Warfare
FBI : Federal Bureau of Investigation
FIRST : Forum of Incident Response and Security Teams

FMI : Fonds Monétaire Internationale

FSS : Force de Soutien Stratégique

GGE : Group of Governmental Experts

GSD : General Staff Department

GRU : *Glavnoïé Razvédyvatel'noïé Oupravlénié*

IA : Intelligence Artificielle

IAD : Information Analysis and Dissemination

ICANN : Internet Corporation for Assigned Names and Numbers

ICE : Immigration and Customs Enforcement

IGF/FGI : Internet Governance Forum / Forum sur la gouvernance de l'Internet

IoT : Internet Of Things

IS&T : Information Systems and Technology

IRSEM : Institut de Recherche Stratégique de l'Ecole Militaire

IW : Information Warfare
JLSF : Joint Logistics Support Force

MASINT : Measurement and Signatures Intelligence

MSE/MSS : Ministère de la Sécurité d'Etat

MSP/MPS : Ministère de la Sécurité Publique

NCCST (Taïwan) : National Center for Cyber Security Technology / Centre National pour la Technologie de la Cybersécurité

NCPH : Network Crack Program Hacker

NICST (Taïwan) : National Information and Communication Security Taskforce / Groupe de Travail National sur la Sécurité de l'Information et de la Communication

NIJC *:* National Informatization Joint Conférence

NIP: National Information Policy

NSA : National Security Agency

NSB (Taïwan) : National Security Bureau / Bureau de la Sécurité Nationale

NSD : Network Systems Department

NTIC : Nouvelles Technologies de l'Information et de la Communication

OFAC : Office of Foreign Assets Control

OGI *:* Open Government Initiative

OMC : Organisation mondiale du commerce

OPM : Office of Personal Management

PAPL : People's Armed Police

PCC : Parti Communiste Chinois

PLA / APL : People's Liberation Army / Armée Populaire de Libération

PLASSF : People's Liberation Army Strategic Support Force / Force de Soutien Stratégique de l'Armée Populaire de Libération

PLAN : People's Liberation Army Navy

PRC / RPC : République populaire de Chine

RMB : Renminbi

SCS : Système de Crédit Social chinois

SILG : State Informatization Leading Group

SSD : *Space Systems Department*

SWIFT : Society for Worldwide Interbank Financial Telecommunication

TNP : Traité sur la non-prolifération des armes nucléaires

TSMC : Semiconductor Manufacturing Company Ltd

VPN : Virtual Private Network

UEFI : Unified Extensible Firmware Interface

UIT : Union internationale des télécommunications

ZES : Zones Économiques Spéciales

INTRODUCTION

« La sécurité d'Internet et l'informatisation sont une problématique stratégique majeure concernant la sécurité, le développement du pays ainsi que la vie et le travail de la population [....] Des efforts doivent être fait pour faire de notre pays une cyberpuissance »[1]

Xi Jinping, 2014, Discours auprès du Groupe Central pour la Cybersécurité et l'Informatisation.

Depuis le début des années 90 et l'avènement d'Internet, la technologie et le numérique sont au cœur des projets de réformes chinois. Dans son discours auprès du Groupe Central pour la Cybersécurité et l'Informatisation, Xi Jinping, secrétaire général du Parti Communiste Chinois (PCC) depuis 2013, appelle même à faire de la Chine une cyberpuissance.

La cyberpuissance n'a pas qu'une seule définition mais elle peut s'entendre comme dépendante "des ressources qui caractérisent le domaine du cyberespace. Cela inclut d'une part, l'Internet et ses instruments tels que les ordinateurs en réseau, les intranets, les technologies cellulaires, les communications spatiales et, d'autre part, les compétences humaines. C'est la faculté, à l'aide de ces instruments du pouvoir, « d'utiliser le cyberespace pour créer des avantages et influencer les événements dans d'autres environnements opérationnels »"[2]

L'économie du pays est, avec les évolutions du numérique, rapidement passée d'un modèle d'exportation de biens de consommation à un modèle d'économie de technologie de pointe. Identifié dès les années 1980 comme un moteur de croissance et d'autonomie stratégique, le secteur des nouvelles technologies témoigne de cette montée en puissance du pays, aussi bien d'un point de vue économique, militaire que d'influence.

[1] Panda A. (2014) Xi Jinping: China Should Become a 'Cyber Power' Xi Jinping has great ambitions for China in cyberspace.*The Diplomat.* https://thediplomat.com/2014/03/xi-jinping-china-should-become-a-cyber-power/ "*Internet security and informatization is a major strategic issue concerning a country's security and development as well as people's life and work [...] Efforts should be made to build our country into a cyber power*"

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

Pensé dans les hautes sphères du PCC, le développement du secteur numérique et de sa cyberpuissance ne peut se concevoir indépendamment des pouvoirs politiques du pays et ne résulte pas tant d'une évolution naturelle des choses que d'un plan méticuleusement préparé.
Servant des objectifs larges comme le maintien de la stabilité du pays et du PCC, la diffusion d'un modèle politique à travers le monde (en compétition avec les démocraties libérales) ou la montée en puissance militaire (pour la reconquête de Taïwan et la sécurisation des routes commerciales), le numérique chinois peut s'appuyer sur un arsenal normatif indépendant, une large autonomie stratégique et des ressources numériques importantes.
Avec son milliard d'internautes pour un taux de pénétration de 72 %, le pays rassemble plus d'utilisateurs d'internet que l'Europe et les États-Unis réunis. Avec son *armée des 50 centimes*, la Chine emploie des milliers d'internautes défendant quotidiennement le modèle politique. Intégrant les nouveaux enjeux du numérique, l'APL (Armée Populaire de Libération) pense et conceptualise la guerre numérique, du téléphone aux satellites. Gagnant toujours plus en autonomie stratégique et forçant les GAFAM à se plier à ses règles, la Chine propose un modèle alternatif, dépassant largement le cadre du numérique pour s'étendre à des questions de modèle de société.

Dès lors, comment la Chine met-elle en ordre de bataille sa stratégie de cyberpuissance et quels sont les objectifs défendus?

La première partie de ce travail reviendra sur le contexte doctrinal et le cadre normatif du pays. Elle abordera la prise de conscience progressive du PCC quant à l'importance du numérique dans la société chinoise vu comme un réel enjeu de puissance. Il s'agira d'étudier les discours mais également les doctrines, ces dernières étant particulièrement importantes pour comprendre comment pense la Chine. Une partie sera consacrée à l'étude du cadre normatif et doctrinal militaire, le PCC entendant bien se hisser comme puissance cyber de premier plan à l'aide d'une stratégie de "défense active". La première partie se concluera sur l'absence de cadre législatif dans le domaine cyber, donnant une porte ouverte aux entreprises chinoises (comme aux autres) à utiliser le numérique comme arme économique. Ainsi, cette partie permettra de mieux comprendre les corrélations entre enjeux politiques et doctrinaux d'un côté, stratégie militaire et concrétisation économique de l'autre.
La seconde partie du travail traitera d'abord de la puissance chinoise dans le numérique d'un point de vue économique (et devant servir des objectifs politiques) et abordera différents thèmes, comme les BATX, la route de la soie numérique ou encore la quête de souveraineté numérique de la Chine.

Dans un second temps, la puissance des universités technologiques chinoises et l'importance de la R&D seront traitées. Enfin, nous verrons comment cette puissance dans le numérique sert un objectif de contrôle de la population et de maintien du régime.

Si la première partie de ce travail abordait les discours, politiques, lois et doctrines chinoises dans le secteur du numérique et que la deuxième se concentrait sur les réalisations économiques et sociales, la dernière partie reviendra sur la montée en puissance du pays dans le numérique d'un point de vue militaire.

Reposant sur une interdépendance entre le civil et le militaire, la puissance cyber de la Chine est difficile à appréhender tant elle est complexe. Le but de cette dernière partie sera donc de tenter de démêler la chaîne de commandement cyber du pays et d'en comprendre les motivations. Ainsi, elle décrira les différentes unités impliquées, les réformes successives de l'APL pour s'adapter aux nouveaux enjeux cyber et les opérations connues (ou soupçonnées) des autorités chinoises pour accaparer des technologies étrangères.

Le sujet du numérique en Chine étant vaste et complexe, ce travail ne prétend pas couvrir l'intégralité du sujet mais souhaite proposer une grille de lecture pour mieux comprendre l'interconnexion entre les intérêts économiques, politiques et militaires dans le pays liés à la notion de numérique, et surtout de cyberpuissance, en Chine.

Chapitre 1 : La quête de cyberpuissance de la République Populaire de Chine: contexte doctrinale et cadre normatif

Xi Jinping l'a annoncé, il veut faire de la Chine une cyberpuissance. Cette ambition n'est pas tout à fait nouvelle et remonte déjà, dans une moindre mesure, au début des années 1990-2000 A travers ses plans quinquennaux, discours, nombreuses agences liées au PCC, la Chine œuvre pour tisser un maillage numérique dans le but de se trouver dans une situation de puissance incontestable et incontestée. Il s'agira d'étudier le contexte doctrinal et les discours qui entourent l'évolution de la prise en compte du numérique en Chine, qui, d'une économie de l'information se transforme en une économie de l'informatisation. Il faudra alors s'attarder sur le cadrage normatif de ce que l'on appelle la « guerre informatisée » (信息化作战), nouveau terrain d'affrontement moderne et outil de puissance du Parti Communiste Chinois (PCC) pour avoir un ascendant militaire sur ses voisins. Il sera par la suite utile de s'attarder sur sa position à l'internationale dans la formulation d'un cadre normatif international que la Chine voudrait globaliser.

Avant d'aborder le chapitre, il est important de pointer un aspect particulier quant aux sources de ce travail:

Bien que la Chine publie des textes traitant de stratégie, il existe peu de documents autoritaires, les analyses se reposent donc autant que faire se peut sur des textes ayant une valeur institutionnelle, mais cela n'est pas toujours possible, notamment sur la déclinaison opérationnelle des concepts stratégiques, ce qui est également souligné par Jon R. Lindsay dans l'introduction de China and Cybersecurity , Espionage, Strategy, and Politics in the Digital Domain.

Dans une autre mesure, les textes publiés par le régime ou des experts sont régulièrement rédigés en mandarin, cependant le manque d'expertise dans cette langue par une partie des experts font que les textes sont parfois inutilisés et ignorés, compliquant le traitement du sujet.

I) Cadrer l’utilisation et le développement du numérique pour atteindre un statut de cyberpuissance: un réel enjeu de puissance

Depuis les débuts d’Internet en Chine, le paysage numérique à bien évolué. Alors qu’elle était en retard au début des années 90-2000, la Chine a vraisemblablement su se saisir de la question du numérique, cadrer comme un enjeu de puissance non négligeable pas seulement d’un point de vue technique et militaire mais également commercial et économique. La Chine comprend l’intérêt du cyberespace et il s’agira ici de faire un état des lieux du cadre normatif, doctrinal et conceptuel qui entoure la montée en puissance de la Chine dans ce domaine. Elle a fait le choix de devenir une société de l’informatisation, terminologie qu’il faudra expliquer.

A) L’économie de l’information et les débuts d’Internet

Dès l’introduction d’internet en 1994, des réflexions commencent à être menées sur le sujet mais il faut attendre les années 2000 pour que soit réellement formalisées ces politiques. Le terme de société d'information, explicité plus longuement dans la suite de l’argumentaire, n’est formulé qu’à partir des années 2000. Il s'agit en fait ici d'étudier ce qui a conduit à cette prise de conscience dans les années 1990 de la nécessité pour la Chine de miser sur le numérique, tout en faisant face à des problématiques internes issues des politiques du régime commmuniste depuis 1949. .

1) 1949 - 1978 : La chape de plomb de Mao Zedong, frein aux avancées futures

Remonter aussi loin chronologiquement peut paraître surprenant lorsque l’on fait le choix d’étudier l’évolution d’Internet et du numérique en Chine. En 1949, il n’y avait rien de tout cela. Pour autant, les profondes modifications engendrées par le régime dictatorial de Mao Zedong ont participé au retard de la Chine dans le domaine du numérique. Il s’agira de s’y arrêter brièvement pour expliquer de quelle manière.

De 1949 à 1966, le Parti communiste chinois, sous l’influence de Mao, supprime les valeurs premières de la société de l'information, c'est-à-dire l’échange libre d'idées et d'informations.

Cette période est marquée dès 1958 par ce que Mao a appelé le « Grand Bond En Avant » qui a causé une famine et plusieurs milliers de morts en 3 ans.
Il n'est pas possible alors de parler de société de l'information dans les années 1960-1970, dans un pays dominé par un mode de vie rurale et le développement de l'industrie lourde, la population étant pour sa part majoritairement illettrée. L'année 1966 marque la date de la révolution prolétarienne initiée par Mao et qui voit une répression des intellectuels chinois, obligés d'adopter un mode de vie rurale. Cette répression marque une incompatibilité entre régime social totalitaire et développement d'une société de l'information, qui restera en toile de fond jusque dans les années 1990-2000.

2) 1978 : Deng Xiaoping et l'économie de l'information

La mort de Mao en 1976 constitue un premier tournant et un moyen de renverser l'idéologie anti-information et anti-sciences de Mao. L'arrivée de Deng Xiaoping au pouvoir en 1978 marque une période de réforme et d'ouverture à la technologie.
Le PCC lance dès 1979 la politique des « 4 Modernisations » dans les domaines de l'agriculture, de l'industrie , de la science et technologie et de la défense nationale. Pour autant, cela ne veut pas dire qu'il y a une libéralisation des échanges et du partage de l'information. La ligne politique reste la méfiance vis-à-vis de l'Ouest (idée politique et produits).
L'industrie électronique se développe dès 1983 parce que la Chine en fait une priorité, bien qu'il y ait encore très peu d'ordinateurs disponibles (mis à part à Hong-Kong et Taiwan). 1983 marque aussi la première révolution de l'information et avec elle l'arrivée d'informations venues de l'Ouest qui risquent d'ébranler le PCC.

C'est le début d'une économie de l'information sans liberté de l'information. La même année, le concept d' économie de l'information ouverte est adopté par le Parti communiste chinois. Il n'en reste pas moins que le contrôle des masses reste une priorité. Le cloisonnement des échanges et cette volonté appuyée de censure sous-tendent encore l'évolution des politiques numériques : la Chine est aujourd'hui à la pointe de la censure et du contrôle d'Internet. Les évènements sur la place Tiananmen à Beijing en 1989 donnent lieu à une campagne de propagande massive rendue plus facile parce que le Parti contrôle la télévision et donc l'information. Le PCC tire des leçons de cette situation : l'information est dangereuse et doit être cadrée, contrôlée.

3) La société de l'information et la lente prise en compte de l'importance d'Internet dans les années 1990

Les dix ans qui suivent permettent à l'innovation de se développer. On passe d'une économie de l'information à une société de l'information avancée, une société de l'informatisation qui s'appuie sur l'industrialisation. L'informatisation c'est "tout ce qui est relié au développement de la cyber en tant que transformation globale d'une société industrielle à une société de l'information"[3]

En 1992, le PCC décide de faire du concept de l'économie de l'information un « objectif important. »[4] En 1994, le PCC met en place une *National Informatization Joint Conférence* (NIJC) et une *Informatization Expert Team* afin de faire un premier pas vers l'accès à Internet. Les deux rencontres entre Jiang Zemin et Bill Gates en 1995, montrent un changement de paradigme : alors que la Chine se refusait à accepter des produits de l'étranger, elle voit la nécessité de coopérer (bien qu'elle prône tout de même une voie chinoise, notamment en terme de production technologique) pour avancer ses pions sur l'échiquier de l'informatisation. Jiang Zemin en 1996 lors d'une adresse au Parti Communiste déclare que saisir la dominance de l'information "*deviendrait un point d'attention dans les conflits*". [5]

Le développement d'Internet pose également la question du contrôle des réseaux, des informations partagées… Des projets sont rapidement mis en place dans le sens du contrôle et de la censure : La loi de 1994 "Regulation for the Protection of Computer Information System" (中华人民共和国计算机信息系统安全保护条例) donne le ton puisqu'elle révèle les intentions chinoises de contrôle du cyberespace. Depuis, la Chine s'efforce de maintenir Internet sous contrôle. Le contrôle du contenu devient également important et le Conseil d'Etat publie "Implementation Measures for Enforcing the Temporary Decree on the Management of Computer Information Network International Connectivity in the People's Republic of China" en Février 1996. "L'utilisation d'Internet pour produire un contenu

[3] Vidal, R. (2008). Les systèmes d'information et les technologies de l'information et de la communication: Enjeux et outils de la responsabilité sociale de l'entreprise dans une perspective de contribution à la soutenabilité. *La Revue des Sciences de Gestion*, 231-232, 137-150. https://doi.org/10.3917/rsg.231.0137
[4] Austin G. (2014) Cyber Policy in China. *China Today*.
[5] *Ibid*

délétère et obscène qui pourrait porter atteinte à la RPC est interdite"[6]. La définition de "délétère" était bien entendu laissée à l'appréciation du gouvernement. En 1998, le gouvernement met en place le pilote du projet *Golden Shield,* aussi dit Bouclier Doré (金盾工程) pour monitorer tous les réseaux et ordinateurs en Chine à des fins de contrôle politique, prévention de crime et protection de la moralité. Il ne sera mis en place définitivement qu'en 2006 et sera abordé plus en détail ultérieurement.
La protestation des Falun Gong de 1999 accentue l'importance du contrôle de la société de l'information. Cette protestation est vite réprimée mais le PCC se rend d'autant plus compte des capacités informationnelles du mouvement, Internet ayant joué un rôle dans le rassemblement des 1000 protestants. [7]

En résumé, à la fin des années 1990, la société de l'information comme idée était clairement dans les esprits des leaders du Parti mais ceux-ci ne l'avaient pas utilisé comme outil politique. Ils n'utilisent alors que les termes d'économie de la connaissance ou économie de l'information.

La trajectoire de l'informatisation de la Chine n'a cependant pas été sans encombre. Les politiques développées se sont parfois retrouvées ralenties voire stoppées par des conflits internes au Parti. Ce qui, dans le même temps, a permis à d'autres pays d'avancer et de devenir des sociétés d'informatisation plus avancées.

[6]Lorci, E. (2021). The Chinese Model of Cyber Sovereignty: Main Principles and Implementations. *Uluslararası İlişkiler Çalışmaları Dergisi University*
Studies https://dergipark.org.tr/en/pub/jirs/issue/68261/1064082 "The use of the Internet to produce harmful and obscène content that could harm the People's Republic of China is forbidden"
[7]*Ibid*

B) Une transformation politique, légale et réglementaire : vers une société de l'informatisation

1) Hu Jintao min et le changement de cap: la société de l'informatisation, nouveau cheval de bataille

Le Politburo détermine en 2000 que la société de l'information serait le but principal des politiques.[8] Le but était de faire un « bond en avant » en utilisant la technologie de l'information pour arriver à une productivité sociale.

La Chine se rend compte qu'elle aura, dans 10 ans, plus d'utilisateurs d'Internet que les États-Unis et s'inquiète de la dissémination de l'information et du monopole qu'elle perdra. Le but défendu par la Chine est de devenir une société de l'information et non plus simplement une économie de l'information, pousse le parti à modifier le State Informatization Leading Group, SILG (国家 信息化领导小组) afin de la politiser davantage.

À partir de 2001 et jusqu'en 2003, le gouvernement tente d'être plus transparent sans vraiment vouloir l'être en réalité. Il devra s'y résoudre partiellement quand, en 2004, le Politburo approuve la première mesure politique, dédiée exclusivement à la promotion d'un développement plus rapide des ressources d'information, qui tiendraient au courant des décisions politiques et aideraient à développer les intérêts économiques du secteur privé.

Les leaders tentent également de cadrer la nouvelle liberté de l'information comme étant liée à la démocratie socialiste avec des caractéristiques chinoises.

En 2005, 14 ministères et agences dont la sécurité publique et le ministère de l'information et du commerce publient des régulations sur les services liés à l'information et à Internet. Dès 2006, des plateformes Internet pour maximiser les échanges d'informations et le networking social du même acabit que ceux des pays développés sont en place.

[8]Austin G. (2014) Cyber Policy in China. *China Today*.

C'est en 2006 qu'une stratégie nationale est pensée et qu'un portail centralisé ww.gov.cn est établi. Son contenu était censé être managé par Xinhua.net, le bras armé de l'Internet officiel des journalistes d'État. En 2007, la Chine publie une régulation sur le *Open Government Initiative,* OGI (中华人民共和国政府信息公开条例) pour que les citoyens puissent légalement sauvegarder des informations gouvernementales ou au sujet de personnes morales et autres organisations. Le but étant d'augmenter la transparence du travail du gouvernement.

Il faut attendre 2010 pour que la Chine sorte un Livre Blanc de la Défense sur Internet. La motivation première était de définir des valeurs publiques autour de l'utilisation d'Internet. Ce papier affirme la liberté de parole, la supervision démocratique des politiques gouvernementales et le droit constitutionnel des citoyens.[9]

2) Penser le changement : La National Information Policy (NIP) de 2006

En 2006, un second plan est décidé, le NIP, à objectif 2020. Il est approuvé dès novembre 2005 par le SILG, présidé par le premier ministre et incluant le Politburo du PCC. Le programme du NIP comporte plusieurs points résumés ci-dessous[10] :

- Promouvoir la société de l'information ;
- Promouvoir l'économie de l'information ;
- Renforcer le développement et l'utilisation des ressources liées à l'information ;
- Implémenter un e-gouvernement ;
- Construire une culture Internet avancée ;
- Améliorer l'intégration des structures liées à l'informatisation ;
- Améliorer la compétitivité de l'industrie des technologies de l'information ;
- Construire un système de sécurité de l'information nationale ;
- Améliorer les capacités nationales en créant un vivier de personnels IT ;
- Améliorer les politiques et la recherche ;
- Améliorer les investissements et le financement des politiques liées à l'information ;
- Promouvoir un système juridique propre à l'IT ;
- Renforcer les échanges et la coopération internationale dans le domaine de l'IT ;

[9] Austin G. (2014) Cyber Policy in China. *China Today*.
[10] Ibid.

- Améliorer la promotion de l'informatisation.

Le rapport de la Chinese Academy of Science, la CAS (中国科学院) [11], paru en 2011, souligne l'importance des transformations sociales et politiques voulues par le gouvernement ou tout du moins envisagées, tout en jugeant les apports du NIP, appelant à aller encore plus loin dans la définition d'objectifs. Le CAS est un think tank chinois créé en 1977 par le gouvernement. Après avoir pris le parti des dissidents lors des événements de la place Tiananmen, le pouvoir s'est saisi de l'Académie pour en remanier le système et y placer uniquement des chercheurs dont les vues coïncident avec celles du PCC. Elle est ainsi devenue un outil pour créer des chercheurs et participer aux innovations futures. Elle publie le rapport A Roadmap to 2050 concernant le développement de la société de l'information et de l'informatisation, et plus particulièrement l'*Information Systems and Technology* (IS&T)[12]

Elle définit plusieurs axes d'amélioration dans le domaine du numérique et de l'informatisation qui doivent être : orienté utilisateur, omniprésente (ubiquitous), offrir un accès pratique à l'information, donner les moyens aux individus de coopérer davantage et plus efficacement, créer des opportunités pour améliorer la qualité de vie, être vue comme un phénomène global et pas simplement technologique, opérer en toute liberté, avoir des caractéristiques chinoises pour développer un contenu en chinois, remplir les critères de sécurité nationale. Le schéma ci-dessous définit les grandes aspirations pour être une société de l'information développée[13].

Le plan est ambitieux, il détaille 40 ans d'évolution pour atteindre une société de l'information complète. Il argue que en termes de progrès des technologies du réseau d'information, le développement de l'information doit se diviser en deux phases (illustrées sur le schéma ci-dessous) : la e-société (société de l'information qui doit être établie à objectif 2020) et la u-société (le U ayant trois significations : universel, orientés utilisateurs (*user-oriented*) et omniprésente (*ubiquitous*).

[11] Li, G. (Ed.). (2011). Information Science & Technology in China: A Roadmap to 2050. *Chinese Academy of Sciences* doi:10.1007/978-3-642-19071-1
[12] Ibid.
[13] Li, G. (Ed.). (2011). Information Science & Technology in China: A Roadmap to 2050. *Op. Cit.*

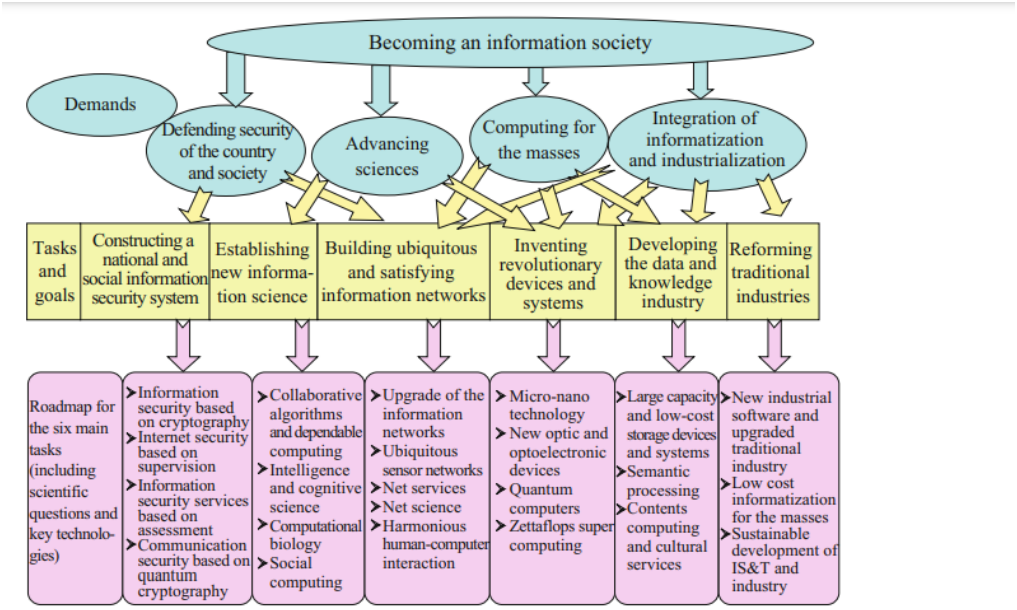


Figure 3-2 Framework for the IS&T development roadmap

Il est néanmoins à relativiser. Il s'agit d'un plan, d'un idéal, qui décrit la volonté de mieux se saisir du sujet du numérique qui est prégnant dans les années 2000. Cela permet tout du moins de réaliser l'ampleur des transformations à entreprendre.

3) Contrôle de l'information et propagande : le Golden Shield ou Great Firewall

D'un point de vue du contrôle intérieur de l'usage d'Internet, la censure et la propagande chinoises sont particulièrement ingénieuses. Il faut rappeler que les politiques décrétées par le PCC ont pour but la continuité d'existence et la légitimation du Parti. C'est ce qui explique en partie la volonté de développer des politiques qui contrôlent voire cadenassent Internet. L'objectif est bien de faire en sorte que l'autorité du PCC ne soit pas remise en cause, tout en profitant des retombées économiques liées à la globalisation d'Internet et des nouvelles technologies.

Comme il l'a été défini précédemment, le contrôle d'Internet était déjà une question qui préoccupait le Parti dans les années 1990, et elle le reste sous Hu Jintao. Le Ministère de l'Industrie de l'Information (précurseur du Ministère de l'Industrie et des Technologies de l'Information créé en 2008) publie une notice officielle en juin 2005 demandant à tous ceux qui possèdent un site internet hébergé en Chine de s'enregistrer auprès des autorités. 1000 sites sont fermés à cette occasion[14]. Les régulations du cyberespace sont strictes et les contrevenants punis : c'est le cas de Google qui est banni en août 2002 parce qu'il refusait de

[14] Lorci, E. (2021). The Chinese Model of Cyber Sovereignty: Main Principles and Implementations. *Op. cit.*

mettre le filtre requis par le gouvernement chinois. Google accepte finalement mais est de nouveau interdit en 2010. Pour contrôler le contenu, le gouvernement s'appuie sur une stratégie simple : le blocage.

C'est la motivation derrière le projet du « *Great Firewall* »[15] à l'Ouest, un système développé de blocage et de filtrage, mis en place en 2006. C'est, en d'autres termes, l'implémentation technologique de régulations législatives pour contrôler Internet.
Le *Great Firewall* a d'abord bloqué des domaines spécifiques, des noms et adresses IP chinoises, identifiant ceux qui contreviennent aux règles. Le gouvernement central demande même l'installation de programmes d'espionnage dans les cybercafés, où les utilisateurs devaient même s'enregistrer avec une carte d'identité avant d'accéder aux machines. Le Great Firewall a, dans un deuxième temps, filtré par mot-clé les recherches. En d'autres termes, la recherche de certains mots « sensibles » déconnecte automatiquement l'utilisateur. Dans un troisième temps, il s'est agi de bloquer les fournisseurs de VPN (*Virtual Private Network*) puis vient ensuite le cadrage législatif qui pénalise les contrevenants.[16]

Le contrôle d'Internet et la dictature de l'information sont donc une haute priorité. Ils ont dû s'adapter après chaque innovation en termes d'échange d'informations. Par exemple, Weibo remplace Twitter en Chine à partir de 2010 pour assurer à la Chine une mainmise sur les réseaux sociaux.

C) Le tournant discursif: l'arrivée au pouvoir de Xi Jinping et l'accroissement de l'importance du cyber dans le cadre national

« Les forces de l'Ouest Anti-Chine ont constamment et vainement tenté d'utiliser Internet pour renverser la Chine …. Que nous puissions rester camper sur nos positions et remporter cette batailles au sujet d'internet a un lien direct sur l'idéologie et la sécurité politique de notre pays »[17] L'arrivée au pouvoir de Xi Jinping modifie le rapport au

[15]Griffiths J. (2019) The Great Firewall of China, *ZED*
[16] Chandel, S., Zang J., Yu Y., Sun J., and Zhipeng Z. (2020). 'The Golden Shield Project of China: A Decade Later An in-depth study of the Great Firewall,' 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery https://www.researchgate.net/publication/338361425_The_Golden_Shield_Project_of_China_A_Decade_Later-An_in-Depth_Study_of_the_Great_Firewall
[17] Xi Jinping (2013 Aout), Discours à la Conférence de la Propagande Nationale et du Travail Idéologique (ideology work) : *« Western anti-China forces have constantly and vainly tried to exploit the internet to"topple*

numérique puisque le nouveau secrétaire général du PCC entend bien faire de la Chine une cyberpuissance.

1) L'arrivée de Xi Jinping au pouvoir: La première pierre à l'édification de la cyberpuissance

Pour édifier sa cyberpuissance, Xi Jinping s'appuie sur plusieurs nouveaux organes et agences qu'il met en place ainsi que sur ces discours, qui enjoignent à faire de la Chine une cyberpuissance.

D'abord, en 2014, le PCC créé la CAC (Cyber Admnistration of China) 中华人民共和国国家互联网信息办公室) qui est sous le contrôle direct de la Commission centrale pour la cybersécurité et l'informatisation (CCAC) (Zhōngyāng Wǎngluò Ānquán Hé Xìnxī Huà Wěiyuánhuì [中央网络安全和信息化委员会]) présidée par Xi Jinping (dont les prérogatives concernent les thématiques liées au numérique) elle-même rattachée au Comité Central du Parti. Elle est chargée de la coordination des politiques publiques numériques du pays, de la diplomatie numérique mais également des questions d'ordre sécuritaire, de la protection des données et du contrôle d'Internet et des contenus.

De nombreux discours, politiques, lois et règlements ont depuis lors été produits pour renforcer l'objectif affiché de Xi Jinping : renforcer l'innovation, limiter sa dépendance technologique, surtout américaine, développer une économie autour du numérique, contrôler Internet, les réseaux, les contenus, rendre l'usage de la technologie plus systématique tout en empêchant des dissidents de l'utiliser contre la Chine.[18]

À la suite du 19ème Congrès du Parti Communiste de 2015, XI Jinping revient sur sa conception du cyberespace qui doit guider le gouvernement sur l'élaboration de stratégies liées au numérique. Il évoque les quatre principes « pour une transformation globale du système de gouvernance d'Internet et cinq propositions « pour construire une communauté de destins partagés dans le cyberespace », décrites dans le tableau ci-dessous[19] :

China' … Whether we can stand our ground and win this battle over the internet has a direct bearing on our country's ideological and political security."

[18] Creemers, R. (2020). Comment la Chine projette de devenir une cyberpuissance. *Hérodote*, 177-178, 297-311. https://doi.org/10.3917/her.177.0297

[19] Kania E., Sacks S., Triolo P., and Webster G. (2017, Septembre 25) China's Strategic Thinking on Building Power in Cyberspace, A Top Party Journal's Timely Explanation Translated. *New America.* https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/

Five Propositions	五点主张, wǔdiǎn zhǔzhāng	The Five Propositions were paired with the Four Principles in Xi's December 2015 speech, which was seminal for today's official rhetoric and approach on cyberspace. They are: 1) Accelerate the construction of a global network infrastructure, and stimulating interconnection and interactivity. 2) Build shared platforms for online cultural interaction, and stimulating exchange and mutual learning. 3) Promote innovation and development in the online economy, and stimulating common flourishing. 4) Guarantee cybersecurity and stimulate orderly development. 5) Build the Internet governance system, and stimulate fairness and justice.
Four Principles	四项原则, sìxiàng yuánzé	The Four Principles were paired with the Five Propositions in Xi's December 2015 speech, which was seminal for today's official rhetoric and approach on cyberspace. They are: 1) Respect for cyber sovereignty. 2) Safeguarding peace and security. 3) Stimulating open cooperation. 4) Building a good order.

2) Assurer le contrôle du cyberespace interne : du Great Firewall à la Loi sur la Cybersécurité de 2017

Les politiques liées au *Great Firewall* continuent à être mises en place par le Parti. Une des parties du projet interdisait l'usage de certains VPN. Voyant que les utilisateurs faisaient usage de VPN pour contourner le Great Firewall, le CPP s'empare du sujet et promulgue une série de lois pénalisant l'utilisation de VPN. La première est promulguée en janvier par le Ministère de l'Industrie et des Technologies de l'Information sous le nom de « *Notice on Clearing Up and Regulating the Internet Access Service Market* ». Le tableau suivant présente la série de lois et évènements relatifs à ce sujet :

TABLE 3 THE DEVELOPMENT OF CYBER LAWS FOR VPNS IN CHINA

Time	Development
January 22, 2017	the Chinese Ministry of Industry and Information Technology (MIIT) announced a "Notice on Clearing Up and Regulating the Internet Access Service Market" [6]
January 2017 - March 2018	A large amount of Taobao shops were shut & the VPN applications were removed from iPhone market [40]
December 2017	Xiangyang, the VPN service provider, was sentenced to jail for being guilty [39]
October 2018	Dai Mou has been sentenced to three years in jail and a fine for selling and using VPN services.[38]

L'une des étapes les plus importantes dans la surveillance du contenu Internet est la Loi sur la Cybersécurité (中华人民共和国网络安全法) de 2017. Les entreprises du numérique, opérant en Chine, ont alors une responsabilité vis-à-vis des activités cyber de leurs clients : toutes les entreprises doivent surveiller l'activité des utilisateurs et rapporter aux autorités tout comportement illégal. Internet est devenu un outil de management de la société. Après l'entrée en vigueur de cette loi, 6000 sites ont été

fermés en 2018 et 733 en 2019 ; 7 millions d'informations retirées d'internet, 9328 applications mobiles retirées.[20]

3) Building Digital China : le 14ème plan quinquennal (2021)

La nouvelle stratégie affichée lors de la présentation du 14ème plan quinquennal de 2021 est celle de Building Digital China (建设数字中国),[21] Le plan reprend des éléments de langage, utilisés dans les plans précédents : il s'agit d'un choix stratégique pour l'avenir, pour accélérer les transformations technologiques et sociétales afin d'atteindre le rêve chinois du rajeunissement (*rejuvenation*) de la nation, pour promouvoir la modernisation de la gouvernance…

Le maître mot est à l'innovation, à la poursuite de la modernisation technologique. Deux concepts clés ressortent « la circulation duale » (双循环) et la « vision 2035 » (年远景目标). Le concept de « circulation duale » tient d'une stratégie basée sur le développement et l'expansion du marché interne. Elle tient, en revanche, moins d'une intégration internationale. La vision 2035 quant à elle veut jouer un rôle dans la définition des standards des futures évolutions technologiques pour parvenir à faire de la Chine une autarcie technologique (*technological autarchy*).[22]

Cette stratégie est donc une décision avisée de la part de Xi Jinping dans la continuité de sa volonté de transformer la Chine en une cyberpuissance. Elle fait, en effet, suite au 13ème plan quinquennal que la CCAC estime être un succès dans son rapport de 2020.[23]

Ce 14ème plan est lié à la personne même de Xi Jinping, dont les origines sont décrites et vues comme une sorte de récit populaire lorsqu'on le lit dans les sources chinoises.[24] Lorsqu'il est gouverneur de la province de Fujian, Xi Jinping remarque que celle-ci n'est pas

---

[20] Lorci, E. (2021). The Chinese Model of Cyber Sovereignty: Main Principles and Implementations. *Uluslararası İlişkiler Çalışmaları Dergisi University*

[21]加快数字化发展 来源(2021, Janvier 25)《求是》https://theory.gmw.cn/2021-01/25/content_34569312.htm

[22] Gatti B. (2020 17 Décembre) The 14th Five-Year Plan: a high-speed roadmap for China, *EIAS*, https://eias.org/publications/op-ed/the-14th-five-year-plan-a-high-speed-roadmap-for-china/

[23] The Cyberspace Administration of China (2020) released the "Digital China Development Report (2020). *Cac.gov.cn* http://www.cac.gov.cn/2021-06/28/c_1626464503226700.htm

[24]数字福建是数字中国的思想源头. [Digital Fujian is the ideological source of Digital China (2018, avril 23)] *Guangming Daily*. http://news.sina.com.cn/o/2018-04-23/doc-ifznefkh9862417.shtml

suffisamment équipée en technologie et a donc des difficultés pour implémenter un système de communication efficace. “Le camarade Xi Jinping, alors Gouverneur de la Province de Fujian, avec une vision stratégique, planifie de manière exhaustive et ouvre la voie scientifiquement au développement de l'informatisation, proposant clairement ‘digitalisation, réseautage, visualisation et intelligence.’”[25] Cet épisode s’inscrit dans une sorte de mythe autour du nouveau plan puisque, nommé “Digital Fujian”, il a évolué pendant 20 ans avant d’émerger à nouveau pour servir de vision au Parti : “une arme aiguisée qui augmente le pouvoir de la nation (augmentation la compétitivité nationale) et une pluie de printemps qui bénéficie au peuple (augmentation de l’efficience opérationnelle de la société”)[26]

Pendant la pandémie, Xi Jinping en profite pour accélérer sa stratégie, sans se faire remarquer par le reste du monde alors trop occupé. Incluse dans sa stratégie *Building Digital China*, la construction du réseau 5G a été accélérée[27] dans le cadre de la campagne *New Type Infrastructure* (新型基础设施) dont le but est de moderniser les infrastructures digitales. Ce plan, met en exergue les efforts réalisés par la Chine pour avoir une position dominante dans la « Quatrième Révolution Industrielle » autour de la gestion de la data (définie en 2015 lors du Forum Économique Mondiale)[28] Le plan Building China repose sur cinq aspects: digital economy, e-government, digital culture, smart society, and digital ecology.
Difficile pour l’instant de mesurer le succès de la stratégie.

Le 19ème Congrès du PCC évoque la notion de « société intelligente » (智慧社会的美好愿景) [29] dès 2018 pour faire suite à la société de l’informatisation évoquée précédemment. Ses caractéristiques sont les suivantes : réseau d’information omniprésent,

[25] *Ibid*
[26]Dorman D. (2022, Mars 28) China’s Plan For Digital Dominance. *War on The Rocks.* https://warontherocks.com/2022/03/chinas-plan-for-digital-dominance/ “*a sharp weapon that empowers the nation (improved national competitiveness) and a spring rain that benefits the people (improved operating efficiency of society*)”
[27]Dorman D. (2020, Novembre) Making The Most Of It, Part Ii: Xi Jinping Leverages Coronavirus “War Without Smoke” To Spur Digital Transformation, Test National Defense Mobilization. *Security Nexus Perspectives.* https://apcss.org/wp-content/uploads/2020/11/Dorman_Making-the-Most-of-It-Part-II-final.pdf
[28] Doshi, R. (2020, juillet 31). The United States, China, and the contest for the Fourth Industrial Revolution. *Brookings.* https://www.brookings.edu/testimonies/the-united-states-china-and-the-contest-for-the-fourth-industrial-revolution/
[29]Shan Zhiguang S. (2018, Décembre 2) A beautiful vision for a smart society: People's Daily Online http://theory.people.com.cn/n1/2018/1202/c40531-30436566.html

planning et management informatisés, infrastructures intelligentes, services publics inclusifs, gouvernance social améliorée, développement industriel du digital and un processus décisionnel gouvernemental basé sur des données scientifiques.[30]

Peut-être que le succès de cette stratégie mise en œuvre par Xi Jinping peut être jaugée au regard de de sa capacité à promouvoir la notion de « société intelligente » sur la scène internationale. Cette stratégie devra montrer la puissance chinoise dans tous les domaines stratégiques du numérique dont celui de la défense et de la sécurité nationale. Toute cette stratégie est sous-tendue par un autre aspect, celui de la sûreté de la Chine.

II) Discours et positionnements autour de la stratégie chinoise de guerre informatique : un nouveau terrain d'affrontement contemporain

Le positionnement militaire de la Chine apparaît pour les chercheurs étrangers comme très ambigu, du point de vue des discours et des actes. D'une part, la Chine se positionne comme une puissance ne souhaitant que défendre ses intérêts et non se battre, et de l'autre elle augmente ses capacités cyber dans un but qu'elle qualifie de défense active. La Chine entend ainsi développer sa supériorité informationnelle défensive mais également offensive. Cette stratégie découle des objectifs affichés du PCC de maintenir l'unité et la stabilité du pays tout en accroissant sa puissance (au sens économique, influence, technologique et militaire).

A) Concepts généraux de la cyberstratégie chinoise : nécessaire informatisation et "guerre informatique"

1) La tradition chinoise de l'art de la guerre appliquée à la « guerre informatique »

La Chine a une longue tradition stratégique qui imbibe les discours et les prises de position du PCC. Le rôle de l'information, de l'intelligence, de la connaissance de son

[30]Ibid "*Ubiquitous information networks, informatized planning and management, intelligent infrastructure, inclusive public services, refined social governance, digital industrial development, and scientific government decision-making.*"

ennemi est le noyau de la guerre. La prévalence de l'information dans la guerre est résumée par Sun Tsu : "Connais l'adversaire et surtout connais-toi toi-même et tu seras invincible."[31] La maîtrise de l'information dans un théâtre d'affrontement est déterminante. L'avènement d'internet, des réseaux sociaux, l'interconnexion des réseaux, la rapidité de circulation de l'information et des innovations technologiques toujours plus poussées, fait prendre à cette collecte d'information une tout autre dimension. Cet héritage stratégique peut être imputé à Deng Xiaoping qui met l'information au centre de sa stratégie lorsqu'il modernise l'armée dans les années 1980.

La meilleure façon de gagner sans livrer bataille, dit encore Sun Tsu, est de décourager l'adversaire de se battre. Parce qu'elle ne peut pas affronter les Etats-Unis de manière frontale, la Chine développe cette stratégie, cette idée de victoire sans combat. Encore une fois cette conception se base sur les préceptes issus de Sun Tsu : "Parvenir à battre son adversaire sans l'avoir affronté est la meilleure conduite." Enfin, l'art de la guerre pour Sun Tsu est également basé sur la tromperie, stratégie qui peut se mettre en place dans le cyberespace : manipulation de l'information, difficulté pour remonter aux auteurs d'une attaque et évaluer les capacités cyber des adversaires, espionnage….

2) L'épineuse question de Taïwan : propice à une volonté d'augmenter ses capacités militaires et cyber

Pour bien comprendre la stratégie chinoise, il s'agit d'abord de l'ancrer dans son contexte géopolitique avant de s'intéresser plus spécifiquement aux théories qui l'entoure. Pour la Chine, la Sécurité nationale est un facteur déterminant pour la prospérité du pays et pour que l'économie et le développement social soient stables. C'est avec ce contexte international bien particulier que la stratégie chinoise s'articule en premier lieu autour de la mitigation de ses ennemis. Un second axe se situe autour d'une recherche de la paix, ou tout du moins du statu quo afin de pouvoir se développer au niveau économique notamment dans le domaine clef de l'informatisation. On la définira comme " l'application de technologies de l'information avancées sur tous les aspects d'opérations militaires, particulièrement en soutien au capacités de commandement, de contrôle, de communication, liées aux ordinateurs, d'intelligence, de surveillance et de reconnaissance (C4ISR)"[32]

[31]Sun Tsu, (s.d) L'art de la guerre.

[32] Campbell C. (2021, juin 4) China's Military: The People's Liberation Army, *PLA.* https://sgp.fas.org/crs/row/R46808.pdf

C’est bien entendu la question de Taïwan qui se trouve au cœur des plans militaires de la Chine. Bien qu’en 1995 Jiang Zemin, alors premier secrétaire du PCC, déclare que “les chinois ne devraient pas combattre des chinois”[33], cela n’empêche pas le PCC d’émettre l’hypothèse de menacer militairement Taïwan.

Quand le président de Taïwan Lee Teng-hui obtient un visa et se rend aux Etats-Unis en juin 1995, la situation dégénère et se transforme en crise, la Chine se sentant menacée. Entre 1995 et 1996 la Chine, sous couvert d’exercices militaires, envoie des missiles de portée moyenne vers Taiwan, qui ne touchent pas l’île, en signe de menace contre Taiwan et les Etats-Unis. La situation politique avec Taïwan se détériore tandis que le candidat pro-indépendance Chen Shui-Bian gagne l'élection présidentielle le 18 mars 2000. Dans le même temps, cette élection attise des divergences d'opinions avec les États-Unis. Le contexte reste tendu, d’autant que la stratégie de la Chine est articulée autour de cette peur d’une contre-attaque des Etats-Unis. La Chine se sait surclassée.

3) Le concept d’informatisation appliqué à la stratégie de sécurité nationale

D’abord, il faut bien comprendre ce qu’informatisation signifie pour la People’s Liberation Army, (PLA) (中国人民解放军). Il faut la différencier de la conception de l’Ouest. L’informatisation pour la PLA “décrit le processus de se mouvoir vers une plus grande collecte, systématisation, distribution et utilisation de l’information. [...] A n'importe quel niveau, le terme “informatisation” peut se référer à un processus de décentralisation organique (comme les “conditions informatisées que la PLA doit prendre en compte pour gagner des guerres locales) à un processus intentionnel direct (l’informatisation des armes et équipements) ou dans certains cas à des actions prises par un acteur pour s’adapter ou se préparer à des tendance de l’informatisation qu’elle ne peut pas contrôler." [34]

“the application of advanced information technology across all aspects of military operations, particularly in support of command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) capabilities”

[33] SCOBELL, A. (2000). Show of Force: Chinese Soldiers, Statesmen, and the 1995-1996 Taiwan Strait Crisis. *Political Science Quarterly*, 115(2), 227–246. doi:10.2307/2657901 *“Chinese shouldn’t fight Chinese”*

[34] Kamphausen R., Lai D. et Tanner T. (2014, Avril 1) Assessing The People’s Liberation Army In The Hu Jintao Era, *Strategic Studies Institute, US Army War College* https://www.jstor.org/stable/resrep11946.9?seq=12 *“describes the process of moving toward greater collection, systematization, distribution and utilization of information. […] at any given level, the term “informatization” can refer to an organic decentralized process (such as the “informatized conditions” under which the PLA are instructed to prepare to win local wars) to an intentional directed process (the informatization of weapons and equipment) or in some cases to actions taken by an actor to adapt or prepare for informatization trends beyond its control.”*

Outre la situation avec Taïwan, plusieurs éléments font comprendre à la Chine que le futur de sa stratégie de Sécurité nationale se trouve dans les nouvelles technologies, notamment dans la guerre de l'information. D'abord, l'opération *Desert Storm* de 1991 menée par les USA en Irak démontre à la Chine l'importance croissante de la technologie dans la Défense nationale et dans la guerre. C'est ensuite le bombardement de l'ambassade de Chine à Belgrade par les États-Unis en 1999 suivi l'invasion de l'Afghanistan par les Etats-Unis en 2001 qui participent un peu plus à cet accroissement d'intérêt. La propension d'utilisation des systèmes informatisés, d'appareils dans l'espace et une collecte d'information efficace ont participé de sa supériorité sur le terrain d'affrontement.[35]

L'informatisation de la société devient un but à atteindre comme cela a déjà pu être souligné.

La conception de la guerre évolue donc à l'aune de l'ère de l'informatisation. Dès 1995, le PCC prend conscience du potentiel du cyberespace. Le major Général Wang Pufeng, directeur du département Stratégie de l'Académie des Sciences militaires de Pékin expliquait que l'objectif découlant de l'avènement d'Internet serait la formation de personnels à la guerre de l'information. Le stratège chinois Wei Jincheng rédige en 1996 Une nouvelle forme de guerre populaire, reprenant les termes de Mao. Il y écrit qu'Internet ouvrait la possibilité d'une « nouvelle forme de guerre ouverte via internet […] où n'importe qui comprenant les ordinateurs deviendrait des combattants et où le pays ennemi pourrait recevoir un coup paralysant en étant incapable de dire s'il s'agit d'une mauvaise blague ou d'une attaque de son ennemi. »[36]
L'ouvrage « La guerre hors limite », qui s'appuie sur l'expérience de la guerre du Golfe et la supériorité informationnelle des américain, insiste sur la nécessité de préparer une « guerre non-conventionnelle » diffuse et permanente (y compris en temps de paix). Il ajoute que ce type de guerre peut se greffer à la guerre plus « traditionnelle »[37].

L'informatisation est alors vue comme la prochaine composante majeure des guerres futures. La Chine doit s'armer sur ce front pour développer sa puissance. Le discours du secrétaire général du Parti communiste Jiang Zemin en 2000 lors d'un discours à la Commission

[35]de Durand, É. (2003). « Révolution dans les affaires militaires »: « Révolution » ou « transformation » ?. *Hérodote*, 109, 57-70. https://doi.org/10.3917/her.109.0057
[36] Fravel, M. T. (2020). Active Defense : China's Military Strategy Since 1949. Princeton University Press.
[37]*Ibid*

Militaire Centrale (CMC [中央军事委员会])[38] le prouve. Il argue que la Chine n'est pas en mesure de combattre dans des guerres informatisées parce qu'elle est trop faible. Le pays se doit de se positionner dans cette sphère et exercer sa souveraineté sur ses propres informations pour exercer une véritable souveraineté territoriale. Frédérick Douzet souligne que « La stratégie chinoise est ainsi focalisée sur l'acquisition d'une suprématie informationnelle au service des conflits modernes, par tous les moyens possibles. »[39]

En 2002, Jiang Zemin s'adressant de nouveau à la CMC déclare que l'informatisation est le cœur du changement et identifie 3 tendances : (1) les armes et les équipements informatisés déterminerait les capacités de combat militaire ; (2) le rôle des frappes de dissuasion (ciblants un ennemi, la défense aérienne et d'autres systèmes) deviendrait plus important ; (3) « confrontations among systems will become the basic future of battlefield confrontations » ; (4) L'espace est devenu « the new strategic high ground »[40]. Contrairement à de nombreuses perceptions, il n'y a pas, dans cette conception, de différences entre les intrusions dans les réseaux, la guerre informationnelle ou les actes de guerre électromagnétique (brouillage). Tout est considéré comme un même ensemble, permettant une suprématie informationnelle, de son système de C4ISR sur celui adverse.

B) Théories appliquées à la stratégie de « guerre informatisée » en Chine

La stratégie chinoise doit s'étudier au prisme de sa relation avec les Etats-Unis. Si le régime chinois choisit une approche dite "asymétrique"[41] dans le domaine militaire numérique c'est pour contrer la supériorité des Etats-Unis. La stratégie de l'asymétrie se définit par des attaques pour exploiter au mieux les ressources du cyberespace ainsi que par le recueil (légal et illégal) d'information stratégique, de tout type (scientifiques, technologiques, économiques et politiques). Cette stratégie s'appuie sur la PLA (*People's Liberation Army)* qui se compose de quatre sous ensemble, pas tous impliqués dans cette stratégie: PLA Army, *PLA Navy, PLA Air Force, et PLA Rocket Force.* Depuis 2015, elle se compose également de la *Joint Logistics Support Force* (JLSF) et de la *PLA Strategic Support Force* (PLASSF

[38]*Ibid*
[39] Douzet, F. (2014). L'art de la guerre revisité. Cyberstratégie et cybermenace chinoises. *Hérodote*, 152-153, 161-173. https://doi.org/10.3917/her.152.0161
[40]Fravel T. (2020) Military Strategy Since 1949, *op.cit*.
[41]Clerot Fabienne & Mayor Victoire, « Jeu de Go dans le Cyberespace », Revue Internationale et Stratégique, 2012/3, N°87, 2012, p. 11

[zhanlüe zhiyuan budui, 战略支援部队].) qui sera abordée ultérieurement. La PLA représente le bras armé du PCC.

1) Théories appliquées à la guerre informatique

a) Le principe de la coercition

Un principe clef de la doctrine chinoise sur le cyber est la stratégie de coercition (*weishe 威慑*), qui date du début des années 2000, défendant un objectif d'évitement des conflits.

L'Académie des Sciences Militaires Chinoises (中国人民解放军军事科学院) voit cette stratégie comme un moyen, pour un pays ou une organisation politique, de faire montre de ses capacités à utiliser sa puissance pour forcer l'adversaire à rendre les armes afin qu'il n'ose ni attaquer, ni faire une démonstration de sa propre puissance militaire. Pour résumer, c'est une manière de soumettre l'ennemi sans se battre. La Chine définit deux types de coercition qu'elle met en totale opposition, ce qui lui sert à légitimer sa position dans le domaine de la guerre informatique. La première, offensive, caractérise les pays expansionnistes de l'Ouest en ce qu'ils cherchent à obtenir des avantages et des gains sur leurs voisins de manière illégitime . Il est évident que la Chine vise en premier lieu les Etats-Unis. La seconde, défensive, caractérise une stratégie de dissuasion basée sur la notion de défense de ses propres intérêts afin d'assurer une stabilité au sein du pays, une intégrité territoriale, et prévenir toute dissidence interne et externe. C'est bien entendu d'elle-même dont la Chine parle. Elle appuie son discours sur la dichotomie entre illégitimité et légitimité des intérêts. Pour la Chine, il est tout à fait légitime pour le pays de vouloir défendre son territoire à travers une coercition défensive. Jiang Zemin argue que "China never invades other countries it also never allows other nations to invade its sovereign territory and sea interests"[42]

[42]Feng Y. (2000) The Construction and Use of New China's Defense Deterrent Force, *Journal of PLA Nanjing Institute of Politics.*

b) Stratégie de Défense active

La stratégie militaire chinoise s'appuie sur le principe de "Défense active", définie depuis 1949 par Mao Zedong. On entend par là les capacités chinoises à utiliser l'information comme moyen de repousser les attaques ennemies tout en menant une stratégie de dissuasion active. Mais cette stratégie chinoise apparaît néanmoins offensive à travers la PLA a ce titre, les auteurs de "The Science of Campaigns" jugent que l'APL doit "continuer dans sa position de défense active, tout en essayant de saisir l'initiative en frappant le premier" mais également qu'il était nécessaire que la doctrine de l'APL soit tournée vers l'offensive.
Le chapitre 3 de ce mémoire s'attachera à étayer ce constat.

Une stratégie offensive active permet l'idée d'affaiblir les capacités de son adversaire tandis que les opérations d'information défensives ne font que repousser les attaques sans affaiblir les forces de l'adversaire. Pour la Chine, seules les opérations d'information offensives permettent d'atteindre une réelle supériorité informationnelle.
Comme on l'a vu plus haut, la notion de « whoever strikes first prevails »[43] est forte dans la doctrine chinoise. C'est en fait pour d'une part éviter qu'un futur ennemi que l'on imagine plus fort riposte et d'autre part que l'ennemi n'attaque pas en premier, ce qui mettrait la Chine dans une position de faiblesse, avec une possibilité de ne jamais pouvoir reprendre l'initiative ce qu'on retrouve évoqué dans certains textes chinois, "Gagner la maîtrise en frappant le premier" C'est pourquoi la doctrine de l'APL sur les opérations informationnelles est axée sur "l'offensive active" car il estimé que contrairement aux opérations traditionnelles qui peuvent réduire la puissance de feu de l'adversaire, les affrontements informationnels peuvent repousser directement ces attaques. L'ouvrage cité de La science des Campagnes de 2006 confirme ainsi l'attention portée aux systèmes informatiques, jugés comme point de gravité des armées modernes.

2) L'application de ces théories d'un point de vue politique

a) Les années 1990 : la formalisation de l'Information Warfare (IW) et de l'Electronic Warfare (EW)

[43]Zhang Y. [张玉良] (2006). ed., The Science of Campaigns [战役学], 2nd ed., Beijing: National Defense *University Press*

Il faut s'arrêter brièvement sur la décennie 1990, puisqu'elle permet de mettre en place deux entités qui vont avoir une importance particulière pour l'élaboration de stratégie cyber liée à l'IW et à l'EW. C'est à travers elles que la Chine formalise sa double stratégie de défense active et d'offensive active.

La PLA voit dès le début des années 90 l'importance de la technologie et de l'électronique dans les conflits futurs. Durant cette décennie, la PLA établit la PLA General Staff Department's Third Department (3/PLA) et la PLA General Staff Department's Fourth Department (4/PLA). Ces deux départements dépendent du General Staff Departement (GSD), subordonné directement au CMC. Le GSD donne des prérogatives liées, pour la 3/PLA, aux guerres de l'information (travaux d'intelligence et de collecte d'information, SIGINT) et liées, pour la 4/PLA, aux guerres électroniques (et pas encore électromagnétiques).[44]

b) Les années 2000 : Livre Blanc de la Défense et « agencification »

Dès 2002, comme mentionné auparavant, Jiang Zemin alors président du CMC explique que la Chine est trop faible pour s'engager dans une guerre informatisée. Il veut, par ces mots, enjoindre le pays à développer ses compétences dans le domaine[45]. Impossible d'être exhaustif sur tous les discours, agences créés en rapport avec l'informatisation, prise de position… Il s'agira plutôt de donner des traits globaux pour comprendre l'évolution des discours entourant l'aspect militaire de l'informatisation de la société à partir des années 2000.

Ce renouveau transparaît dans la doctrine dite Information Warfare and Electronic Warfare (INEW) puis modifiée pour signifier Integrated Network Electronic Warfare.[46]

Cette doctrine est majoritairement portée par les travaux de Dai Qinming, dont le travail séminal date de 1999, et est nommé On Integrating Network Warfare and Electronic Warfare. Il y milite pour une intégration plus grande entre la guerre informationnelle et la guerre électronique. Son travail semble avoir été reconnu, car il a été porté à la tête du 4eme

[44]Krekel B., Adams P. et Bakos G. (2021, Mars 7) Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage, *Northrop Grumman*. https://www.uscc.gov/sites/default/files/Research/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf

[45] Austin G. (2014) Cyber Policy in China. *Op. cit.*

[46] Deepak S. (Avril 2010) Integrated Network Electronic Warfare: China's New Concept of Information Warfare Jounal of Defense Studies https://idsa.in/system/files/jds_4_2_dsharma.pdf

département du General Staff Department (GSD). Le but recherché serait donc de consolider l'autorité organisationnelle de la guerre de l'information sur les intrusions de réseaux informatiques.[47]

Cette doctrine se rapproche de la doctrine de combat radio électronique poursuivie par l'URSS lors de la guerre froide, ce qui semble cohérent avec la vision de la cybernétique russe historique. Il est difficile d'estimer le lien de parenté mais cette doctrine n'était sûrement pas inconnue au camp chinois lors de l'élaboration de la doctrine INEW. Explicitée très succinctement, la doctrine chinoise revient à combiner la guerre électronique (brouillage etc) et des frappes de précision en ajoutant des intrusions informatiques et des attaques kinétiques sur des systèmes spatiaux, en vue d'obtenir une supériorité, voire une hégémonie sur l'information, en bref cibler tout ce qui s'apparente à des systèmes C4ISR. Elle vient irriguer tous les champs, tant stratégiques qu'opérationnels ou tactiques.[48]

Ainsi à partir de 2003, les leaders du PCC comprennent que l'informatisation doit transformer profondément leur conception des affaires militaires. C'est parce que les opérations d'information de la part de leurs adversaires deviennent à cette période monnaie courante. La prise en compte de cet aspect a été tardive, puisqu'il a fallu attendre les années 2000. On peut aller plus loin et dire qu'il a fallu attendre Xi Jinping et les réformes de 2014 , évoquées ultérieurement, pour qu'un réel changement s'opère. La priorité a été d'abord donnée aux capacités de cyber-espionnage, l'informatisation des capacités militaires quant à elle était vue comme plus secondaire jusqu'en 2007.[49] On notera que les sources publiques disponibles concernant le sujet de l'informatisation militaire sont très édulcorées, rendant parfois difficile l'appréciation de la stratégie chinoise.

Le discours de Jiang Zemin de 2002, déjà évoqué, pointe du doigt les aspects de la PLA qui devraient être réformés, notamment dans le domaine du commandement et du contrôle et des opérations interarmées. Pour lui, cette volonté d'augmenter les capacités militaires informatiques chinoises se situe dans la continuité de la position défensive de la Chine. En 2003, la CMC promulgue une modification dans la doctrine officielle de la PLA. Elle y définit un peu plus l'entrée de l'informatisation dans la PLA.

---

[47] Wortzel L. (2014, Mars) The Chinese People's Liberation Army and Information Warfare. *US Army War College.* https://publications.armywarcollege.edu/pubs/2263.pdf

[48] *Ibid*

[49] Austin G. (2014) Cyber Policy in China. Op.cit.

On retrouve cette notion dans le Livre Blanc de la Défense de 2004 qui contient une section entière sur la nécessité d'augmenter la prise en compte de l'information. La doctrine de la PLA se retrouve modifiée pour se concentrer sur « gagner les guerres locales dans des conditions informatisées »[50] au regard des guerres du Kosovo (1999) et d'Irak (2003)

En décembre 2006, la politique militaire liée à l'informatisation prend une tournure plus sophistiquée, un plan est même établi de 2006-2020, le NIP, dont il a été question plus haut. Jiang Zemin évoque la nécessité de complémenter les outils de dissuasion nucléaire par des outils de dissuasion liés à l'information. Dans le Livre Blanc de la Défense de la même année, apparait l'importance d'adopter une posture *défensive* contre les opérations d'information des autres États. Le CMC établi un « joint operational command system, training system and support system"[51] pour combattre dans les guerres informatisées.
Un changement majeur survient avec le White Paper de 2008. Là où la guerre informatisée ne prenait en compte que les ordinateurs, la transmission de code, le réseau informatique, la guerre de l'information doit quant à elle prendre en compte l'intégralité du spectre électromagnétique. La définition est donc élargie.

Le terme d'informatisation devient indissociable de la PLA avec le Livre Blanc de la Défense de 2010 qui établit que les avancées vers l'informatisation de la société sont aujourd'hui irréversibles. C'est également dans ce document qu'est souligné l'importance de la *cybersécurité* dans la Défense nationale de la Chine[52]. En complément de cette doctrine, le *General Staff Departement* (GSD) crée une «*information warfare base* » dédiée aux activités cybernétiques et à la cyberdéfense. Traditionnellement, les prérogatives données à cette nouvelle organisation tombaient sous la juridiction des 3/PLA et 4/PLA.
En 2011, la PLA consolide sa doctrine de « Integrated Warfare Network » : "the use of electronic warfare computer network operations and kinetic strikes to disrupt battlefield information systems especially through joint operation"[53]. Dans le même temps en 2011 le GS Headquarter transforme son département de la communication en département de l'information et ordonne l'établissement d'unités parallèles

[50]Douzet, F. (2014). L'art de la guerre revisité. Cyberstratégie et cybermenace chinoises. *Hérodote*, 152-153, 161-173. https://doi.org/10.3917/her.152.0161
[51]Austin G. (2014) Cyber Policy In China, *China Today*
[52]Office of the Secretary of Defense. (2013) Annual Report To Congress Military and Security Developments Involving the People's Republic of China
[53]Austin G. (2014) Cyber Policy In China, *op.cit.*

On le voit à travers l'évolution du contenu des Livres Blancs de la Défense, pour la PLA la guerre de l'information devient une priorité opérationnelle et pas seulement un but stratégique global.

Le rapport de 2013 du Pentagone au Congrès américain[54] sur les capacités militaires de la Chine voit que le pays acquiert des capacités dans le cyberespace : "Beijing investit dans les programmes et armes militaires conçus pour augmenter la puissance de projection et des opérations dans des domaines émergents comme la cyber, l'espace et la guerre électronique."[55] Le rapport note que la Chine considère la guerre électronique comme la quatrième dimension d'un combat, au même titre que les forces aériennes, maritimes et terrestres. Le rapport note enfin que la Chine « continue de faire de progrès sur les systèmes de commande, de communication et de systèmes de contrôle"

Toute cette stratégie est soutenue par des agences et des départements liés à la guerre informatique. Les cyber-offensives, sont par exemple, la prérogative de la 4/PLA évoquée plus haut. Dans le même temps, la 3/PLA poursuit ses opérations de SIGINT. Le chapitre 3 de ce mémoire s'attachera à développer plus précisément ces structures et stratégies.

Au printemps 2013, Xi Jinping accède au pouvoir en tant que premier secrétaire du Parti Communiste.

3) Xi Jinping et le rêve de faire de la Chine une cyberpuissance d'ordre militaire: dominer l'espace cyber

L'année 2013 marque un véritable tournant pour la Chine de deux manières différentes. D'abord, l'affaire Snowden révèle les limites des capacités de cyberdéfense chinoise. Ensuite, 2013 marque l'arrivée de Xi Jinping au poste de secrétaire général du PCC. En 2014 il déclare lors de son premier discours d'envergure vouloir faire de la Chine une cyberpuissance. Dans le même discours il déclame "sans la cybersécurité [ou la sécurité du

[54]Office of the Secretary of Defense. (2013) Annual Report To Congress Military and Security Developments Involving the People's Republic of China

[55]*Ibid "Beijing is investing in military programs and weapons designed to improve extended-range power projection and operations in emerging domains such as cyber, space, and electronic warfare"*

réseau], il n'y aura pas de sécurité nationale."[56], ajoutant que la "cybersécurité et l'informatisation sont les deux ailes d'un seul corps et les deux roues d'un moteur […] Ils doivent être planifiés, déployés, avancés et implémentés de manière unifiée »[57] Il souligne aussi la nécessité de réduire la dépendance chinoise aux technologies étrangères tout en augmentant les capacités d'innovation technologiques locales.

À cette occasion et plus tout à fait comme en 2004, la doctrine de la PLA est modifiée et appuie sur la notion d'informatisation pour "gagner des guerres locales informatisées "[58]. Cet ajustement tient lieu d'orientation pour les grandes réformes organisationnelles qui vont suivre en 2015 et 2016. Une autre initiative est lancée lorsque Xi Jinping et le CMC publient "Opinion on Further Strengthening Military Information Security Work" en 2014, listant les directives liées à la sécurité de l'information pour l'armée.

a) Livre Blanc de la Défense (2015)

Il faut attendre le Livre Blanc de la Défense de 2015 pour avoir une première stratégie militaire sur l'informatisation : "L'espace et le cyberespace sont les nouveaux points de commandement de la compétition internationale en matière de sécurité. [...] La forme de la guerre accélère son évolution vers l'informatisation. Les grandes puissances mondiales ajustent activement leurs stratégies de sécurité nationale et leurs politiques de défense, et accélèrent la transformation de leur armée et la restructuration de leurs forces." [59] Le Livre Blanc de la Défense de 2015 met en avant la volonté de la Chine de montée en capacité, surtout en termes de projection de puissance mais également en temps que puissance coercitive. Il appelle la Chine à "expédier le développement de la force cyber" (*expedite the development of a cyber force*) et à améliorer ses capacités en termes de "connaissance de la situation dans le cyberespace " (*cyberspace situation awareness*) et de "cyberdéfense". Cela permettra d' "'endiguer les cybercrises majeures, d'assurer la sécurité des réseaux et des

[56]Picarsic N., Ferguson J., De La Bruyère E. et Doshi R. (2021, Avril) China As A"Cyber Great Power"Beijing's Two Voices In Telecommunications, F*oreignPolicies at Brookings: "*without cyber [or network] security, there will be no national security"

[57]*Ibid* "Cybersecurity and informatization are two wings of one body, and two wheels of one engine[…] They must be planned, deployed, advanced, and implemented in a unified manner

[58]Douzet, F. (2014). L'art de la guerre revisité. Cyberstratégie et cybermenace chinoises. *Op.cit.*

[59]*In* Blessing J. and Austin G. (2022, Février) Assessing military cyber maturity: strategy, institutions and capability, *The International Institute for Strategic Studies*

"outer space and cyberspace are the new commanding heights of international security competition. […] The form of war is accelerating its evolution to informationization. World major powers are actively adjusting their national security strategies and defense policies, and speeding up their military transformation and force restructuring"

informations au niveau national et de maintenir la sécurité nationale et la stabilité sociale"[60] Xi Jinping introduit 3 nouveaux organes à travers ce Livre Blanc de la Défense : la PLA *Rocket Force*, la PLA *Strategic Support Force*, et l'*Army Leadership Organ.*

b) La PLASSF (2015)

La PLASSF est créée en 2015 à travers le Livre Blanc de la Défense dans le but de servir de soutien aux opérations militaires et de créer des synergies entre des informations et les capacités militaires afin de mener des opérations stratégiques décisives[61]. Sa création répond en effet à un besoin de rassembler guerre et support informationnel. Ce changement, cette centralisation au final, devrait permettre à la PLA d'être plus efficace et donc d'accroître sa supériorité. Le premier commandant de la SSF, le General Gao Jin met en avant l'importance du soutien à l'information : "le soutien à la sauvegarde et à l'élévation d'un "parapluie d'information" [xinxi yusan, 信息雨伞] pour le système militaire, qui sera intégré aux actions de nos forces terrestres, maritimes et aériennes et de nos forces de fusée tout au long d'une opération, [et] sera la force clé pour la victoire dans la guerre."[62]

Le directeur adjoint du 54ème Institut de Recherche de la SSF Lü Yueguang déclare même que les challenges liés à "l'intégration des systèmes de systèmes à dominante informationnelle" vont devenir "une exigence fondamentale pour les futures opérations conjointes."

c) La fusion civilo-militaire (2015)

[60]The State Council Information Office of the People's Republic of China (Mai 2015) Defense White Paper. *Xinhua* http://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm "*stem major cyber crises, ensure national network and information security, and maintain national security and social stability*"

[61]Costello J. and McReynolds J. (2018 Octobre) China's Strategic Support Force: A Force for a New Era. *China Strategic Perspectives.* https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf

[62]*Ibid "support for safeguarding and raising up an 'information umbrella' [xinxi yusan, 信息雨伞] for the military system, which will be integrated with the actions of our land, sea, and air forces and rocket forces throughout an entire operation, [and] will be the key force for victory in war."* https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf

La Chine entend développer une stratégie de fusion civilo-militaire. Ce concept a émergé dans les récentes années au sein des débats internationaux, sa théorisation dont la date est compliquée à déterminer (on estime la retrouver dans les années 1980), devient un terme utilisé par une source autoritaire en 2007. Lors de son discours, Hu Jintao, lors du 17eme congrès du parti, incite urgemment le pays à "prendre la voie d'une fusion civilo-militaire avec des caractéristiques chinoises", se rapprochant de ce qui était à l'époque nommé comme l'intégration civilo-militaire (junmin jiehe, 军民结合), ouvrant ensuite la voie à ce que Xi Jinping renomme la fusion civilo-militaire: (junmin ronghe, 军民融合).[63]

S'invitant de plus en plus dans les publications chinoises, à l'instar de ce qu'il se passe au niveau international, cette notion prend une importance grandissante dans la doctrine chinoise, bien qu'encore en mutation et pas forcément encore clairement définie.[64]

En effet la fusion que cette stratégie vise à créer n'est pour l'instant qu'une aspiration, rendant le reflet des réalités du terrain différente que ce qui devrait être réalisé par la doctrine.C'est donc un sujet infiniment complexe et différent en fonction de l'angle duquel on l'analyse. Le concept même de fusion civilo-militaire, de part son évolution sémantique est donc un concept créé par Xi. Sous sa direction le PCC instaure une nouvelle commission, qu'il dirigera, la Commission Centrale du Développement de la Fusion Civilo-Militaire, qui se déclinera en partie en Centre d'Innovation et Fusion civilo-militaire en cybersécurité (网络空间安全军民融合穿心中心), qui sera conduite par Qihoo 360, entreprise au coeur de la stratégie de sécurité informatique chinoise dans le but, là encore, d'améliorer les capacités numériques de la chine, dans le prolongement de sa poursuite de capacités de défense active.[65]

---

[63] By Fritz A. (2019, Aout 2) China's Evolving Conception of Civil-Military Collaboration. *Center for Strategic and International Studies* https://www.csis.org/blogs/trustee-china-hand/chinas-evolving-conception-civil-military-collaboration

[64] Kania E. et Lorand L.(2021 janvier) Myths and Realities of China's Military-Civil Fusion Strategy. *Center for a New American Security* https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Myths-and-Realities-of-China%E2%80%99s-Military-Civil-Fusion-Strategy_FINAL-min.pdf?mtime=20210127133521&focal=none

[65] Kania E. (2018, Mars 16) China's quest for political control and military supremacy in the cyber domain Australien Strategic Policy Institute https://www.aspistrategist.org.au/chinas-quest-political-control-military-supremacy-cyber-domain/

Cette stratégie se retrouve dans L'ouvrage *Science of Military Strategy* (SMS) de 2015, où il est expliqué que "Compte tenu des limites ambiguës entre le temps de paix et le temps de guerre en matière de contre-mesures cybernétiques et de la difficulté à distinguer les attaques militaires et civiles, il faut persister dans l'intégration de la paix et de la guerre [et] dans l'intégration militaro-civile ; en temps de paix, utiliser les civils pour cacher les militaires ; en temps de guerre, les militaires et le peuple, mains jointes, attaquent ensemble."[66] Le PCC instaure une nouvelle commission, dirigée par Xi Jinping la *Central Military–Civil Fusion Development Commission*. Celle-ci crée le *Cyberspace Security Military–Civil Fusion Innovation Centre* dans le but, encore une fois, d'améliorer les capacités de cyber défense de la Chine.

A l'occasion de la *National Cyber Security and Informatization Work Conference*[67] en 2018, Xi Jinping souligne l'importance de cette fusion, en soulignant la relation privilégiée entre le "marché et le champ de bataille", tout en "promouvant la création d'une structure de développement multifactorielle, multidomaine et hautement efficace pour l'intégration militaro-civile."[68]

d) Discours successifs, conférences et Livre Blanc de la Défense post 2015

Les adresses successives du PCC et de Xi Jinping vont dans le même sens : faire de la Chine une cyberpuissance. Les discours maintiennent ce but. Dans son discours de 2018 à la *National CyberSecurity and Informatization Work Conference*, il réitère ses propos de 2015 : "sans cybersécurité, pas de Sécurité nationale."

En 2019, la Chine maintient cette attitude, dans son Livre Blanc de la Défense : "La ligne directrice stratégique militaire pour une nouvelle ère adhère aux principes de défense, d'autodéfense et de réaction après une attaque, et adopte la défense active. Elle s'en tient à la

---

[66]China, Academy of Military Science, *Science of Military Strategy*. "*In light of the ambiguous boundaries between peacetime and wartime in cyber countermeasures, and the characteristic that military and civilian attacks are hard to distinguish, persist in the integration of peace and war [and] in military–civil integration; in peacetime, use civilians to hide the military; in wartime, the military and the people, hands joined, attack together*"

[67]IISS (2019, Mai) Chapter Five: China's cyber power in a new *In* Asia Pacific Regional Security Assessment, 77-99https://www.iiss.org/publications/strategic-dossiers/asiapacific-regional-security-assessment-2019/rsa19-07-chapter-5

[68]Creemers R., Triolo P., and Webster G. (2018, Avril 30)Translation: Xi Jinping's April 20 Speech at the National Cybersecurity and Informatization Work Conference. *New America.*https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/ *"market and the battlefield', tout en "promot[ing] the creation of a full-factor, multi-domain, and highly efficient development structure for military–civil integration*"

position selon laquelle "nous n'attaquerons pas à moins d'être attaqués, mais nous contre-attaquerons sûrement si nous sommes attaqués"[69]
En 2021, un nouveau plan est publié pour la montée en puissance des industries domestiques de la cybersécurité, secteur sur lequel s'appuie largement les opérations cyber militaires. [70]

En définitive, la Chine ne veut pas de la militarisation du cyberespace, qui affecterait la paix et la stabilité du pays. Elle revendique malgré tout son droit à accroître ses capacités de cyberdéfense. [71] On notera que les documents émis par le gouvernement mentionnent peu la stratégie militaire numérique, souvent inclue dans un spectre plus large.
Analyser les prises de position liées à cette volonté de cyberpuissance chinoise n'est pas aisé mais on l'aura vu, avec l'accès au pouvoir de Xi Jinping, tout semble s'accélérer. Il s'agira par la suite de voir si ces déclarations ont un réel poids et un réel impact, notamment en termes offensif et défensif. A-t-on affaire à de "beaux discours" ou à des discours ancrés dans une réalité qui fait que la Chine à tous les facettes d'une cyberpuissance ?

Il faudra aussi s'attacher à éclairer un point qui n'a été que peu abordé jusque-là, l'inclusion de la Chine dans le cadre de la gouvernance du numérique dans la sphère internationale. Parce qu'elle est devenue un acteur incontournable du numérique et parce que sa stratégie de défense passive s'appuie sur la position chinoise défendue auprès des autres nations, il nous sera utile de voir à quel point la Chine peut se targuer d'être hégémonique au-delà de son territoire.

III) L'absence d'une gouvernance internationale du numérique définie : une porte ouverte à la cyber-hégémonie chinoise

Malgré plusieurs tentatives d'instauration d'un cadre normatif international sur la gouvernance d'Internet, cette absence formelle est une véritable aubaine laissée au géant

[69] PRC State Council Information Office(2019, Juillet) China's National Defense in the New Era. "*The military strategic guideline for a new era adheres to the principles of defense, self defense, and post-strike response, and adopts active defense. It keeps to the stance that "we will not attack unless we are attacked, but we will surely counterattack if we are attacked*"
[70] Blessing J. and Austin G. (2022, Février) Assessing military cyber maturity: strategy, institutions and capability, *The International Institute for Strategic Studies*
[71] Creemers, R. (2020). Comment la Chine projette de devenir une cyberpuissance. *Hérodote*, 177-178, 297-311. https://doi.org/10.3917/her.177.0297

chinois dont la stratégie de cybergouvernance est axée sur la défense de sa souveraineté nationale.

A) Les tentatives fragiles d'instauration d'un cadre normatif international sur la gouvernance du numérique : faire face au sacro-saint principe de souveraineté des États

Véritable enjeu d'avenir au cœur des relations internationales, le cyberespace est aujourd'hui une préoccupation majeure. Les tensions croissantes entre puissances ont mis en lumière les lacunes normatives en matière de régulation et de réglementation. En ce sens, il n'existe d'ailleurs pas de définition unique du cyberespace. Si certains le définissent comme un synonyme d'Internet, d'autres lui confèrent un sens plus opérationnel[72]. Il est à la fois un domaine, un environnement, un moyen et de plus en plus un théâtre d'opérations.

Pourtant, encore aujourd'hui, la gouvernance internationale d'Internet n'est toujours pas un acquis. La conception westphalienne du système international, conçue à travers la notion de frontières et de souveraineté territoriale des Etats, ne s'imbrique pas réellement dans celle du cyberespace qui en est dépourvu. Par conséquent, la mise en place d'un cadre normatif international se veut plus complexe et a fortiori, dans un contexte international divisé par les enjeux de puissance. A ce titre, les ambitions souverainistes de la Chine sur le cyberespace n'y contribuent pas.

1) Une incapacité à organiser une coopération internationale efficiente

Si aucun cadre international normatif précis n'a été défini, qu'en est-il vraiment de la coopération internationale en matière de gouvernance d'Internet

a) Panorama des acteurs de la coopération internationale

Parmi les acteurs classiques de cette coopération, figurent les institutions onusiennes à l'instar de l'*Internet Governance Forum* (IGF)[73] ou de l'Union internationale des

[72] Desforges, A. (2014). Les représentations du cyberespace : un outil géopolitique. *Hérodote*, 152-153, 67-81. https://doi.org/10.3917/her.152.0067.

[73] *Site officiel de l'Organisation des Nations Unies* - Département des affaires économiques et sociales. UN.org. https://publicadministration.un.org/fr/internetgovernance

Télécommunications (UIT)[74]. Pour sa part, l'IGF est un forum de discussions qui rassemble plusieurs groupes d'intervenants dans le but d'échanger sur les bonnes pratiques liées à la gouvernance d'Internet, tout en prenant en compte les risques et défis liés. De son côté, l'UIT s'intéresse à des sujets plus techniques liés spécifiquement aux télécommunications, à l'instar du standard sans fil 5G. Également, des groupes de travail intergouvernementaux (GGE) ont été mis en place[75] dans le cadre onusien depuis 2019 relative à la définition du cyberespace[76]. Enfin, à cela s'ajoutent des organisations internationales dont les domaines d'activité gravitent, directement ou indirectement, autour d'Internet. C'est le cas par exemple de l'Organisation mondiale du Commerce (OMC)[77].

En ce sens, la Commission des Nations Unies pour le Droit Commercial International (CNUDCI), a même contribué à l'élaboration de normes spécifiques, en matière de commerce électronique[78] ou d'utilisation des communications électroniques dans les contrats internationaux[79], inspirant de ce fait certaines législations nationales (Australie, France, Russie ou Chine).

Enfin, parmi les acteurs non-onusiens de cette coopération internationale figure notamment l'ICANN (Internet Corporation for Assigned Names and Numbers)[80], une organisation à but non lucratif dont le but est de rassembler des participants du monde entier et ainsi de discuter de sécurité et d'interopérabilité d'Internet (ex : attribution des adresses internet au niveau mondial). Également, il est essentiel d'évoquer les CSIRT, pour *Computer Security Incident Response Team*, soit équipe de réponse aux crises informatiques, présents dans le monde entier. Il s'agit globalement de structures d'alerte et d'assistance chargées à la fois d'anticiper les menaces potentielles et de répondre à celles en cours, pour le compte d'entreprises ou encore d'administrations. Dès 1990, la création d'une enceinte internationale regroupant tous les CSIRT et visant à les faire interagir a été actée sous l'égide du *Forum of incident response*

---

[74] *Site officiel de l'Union Internationale des Télécommunications*. ITU.org. https://www.itu.int/fr/Pages/default.aspx

[75] Résolution 73/266 de l'Assemblée générale des Nations Unies, *Advancing responsible State behaviour in cyberspace in the context of international security*, A/RES/73/266 (22 décembre 2018). https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/465/01/PDF/N1846501.pdf?OpenElement.

[76] *Group of Governmental Experts – UNODA*. (2019). ONU.org. https://www.un.org/disarmament/fr/group-of-governmental-experts/

[77] *Site officiel de l'Organisation mondiale du commerce*. OMC.org. https://www.wto.org/indexfr.htm

[78] *Loi type de la CNUDCI sur le commerce électronique - Commission des Nations Unies pour le droit commercial international*. (1996). UN.org. https://uncitral.un.org/fr/texts/ecommerce/modellaw/electronic_commerce

[79] *Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux (New York, 2005) | Commission des Nations Unies pour le droit commercial international*. (2005). UN.org. https://uncitral.un.org/fr/texts/ecommerce/conventions/electronic_communications

[80] *Site officiel de l'Internet Corporation for Assigned Names and Numbers*. ICANN.org. https://www.icann.org/fr

and security teams (FIRST). Aujourd'hui, le FIRST regroupe près de 627 entités à travers le Monde[81] dans le but de coopérer au niveau international sur les questions de cybersécurité. Une fois par an, une conférence annuelle internationale est organisée afin de traiter des incidents de sécurité et de partager les expertises sur le sujet.

Pour faire suite à la présentation des différents acteurs influents de la coopération en matière de gouvernance internationale d'Internet, il s'agira de s'intéresser aux causes de l'incapacité à instaurer un cadre normatif international ainsi qu'au rôle joué par la Chine dans la coopération internationale mise en place.

b) La place de la Chine dans le dialogue international sur la gouvernance d'Internet

Avant l'émergence d'Internet sur son territoire, la Chine demeurait largement absente du dialogue international lié au cyberespace. Manque d'expertise sur les questions numériques[82] ou raisons politiques[83]? Il semblerait que ces deux raisons y aient contribué, à son détriment. Pour autant, depuis quelques années seulement, la Chine adopte une position plus proactive dans les discussions. En effet, le discours de Xi Jinping lors de la Conférence mondiale sur l'Internet en 2015 a clairement redessiné les contours de la stratégie chinoise du contrôle du cyberespace et de sa place dans la gouvernance mondiale liée. Ce discours demeure encore aujourd'hui le fondement de la politique étrangère chinoise en matière de numérique.

Petit à petit, Xi Jinping réussit à faire de la Chine une puissance influente dans la sphère de la coopération internationale sur le cyberespace. Pour y parvenir, il défend largement les intérêts de sécurité nationale et s'appuie sur un sentiment croissant de défiance à l'égard de la prééminence des Etats-Unis dans les discussions sur la cybergouvernance internationale. En 2012, des débats au sein de l'UIT ont mené au vote d'un document critiquant la gouvernance actuelle d'Internet. Parmi les votants en faveur, près de 89 pays dont la Chine. En outre, la fin de la mainmise américaine sur l'ICANN, en 2016, a aisément contribué à redonner à la Chine une place plus visible sur cette question. En revanche, la fin de cette mainmise ne marque ni

---

[81] *FIRST - Forum of Incident Response and Security Teams*. FIRST.org. https://www.first.org/

[82] *Exemple en ce sens* : lors de la première série de négociations du Groupe d'experts gouvernementaux sur la cybersécurité (GGE) de l'ONU, la délégation chinoise était constituée de représentants du ministère du Commerce, connaissant peu les questions de droit international.

[83] *Exemple en ce sens* : La Chine boycotte le Comité consultatif des gouvernements de l'ICANN entre 2001 et 2009 en raison du statut politique accordé à Taiwan et de la structure multipartite de l'institution.

la fin de l'influence américaine sur l'organisation ni son rattachement au système multilatéral onusien.

Force est de constater, encore aujourd'hui, que la Chine ne réussit pas à rassembler de soutiens suffisamment importants pour influer sur la gouvernance du cyberespace, tant sa vision de celle-ci est peu convaincante. A titre d'exemple, la Conférence mondiale sur l'Internet organisée par la Chine et en Chine depuis 2013 ne suscite pas l'intérêt des dirigeants étrangers. L'Initiative Wuzhen, présentée en 2015 lors de la 3ème édition, a permis à la Chine de présenter son projet de *Digital Silk Road* (DSR), angle technologique de la Belt and Road Initiative. Les soutiens à ce projet n'ont pas été à la hauteur des attentes de Pékin, dont seulement sept pays[84] ont rejoint formellement l'accord de coopération. Accord dont le respect et les modalités d'application ne sont pas garantis.

Pour le PCC, l'objectif prioritaire de la Chine est la reconnaissance de son « *huayuquan* » (话语权) , qui peut être traduit comme son « droit à prendre la parole ». Pour le pays ayant la plus importante population connectée au Monde, sa place dans la cybergouvernance devrait être mieux représentée, selon lui. Pour renforcer le poids de ses arguments, elle entend bien mener des actions conjointes avec la Russie pour choisir le vocabulaire utilisé durant les négociations sur le cyberespace. Ce fut le cas, en 2009 au sein de l'Assemblée générale des Nations Unies, lors de leur proposition de discussions visant à instaurer un code de conduite dans le cyberespace. Malgré un faible succès, les deux puissances maintiennent leur position en développant toute une stratégie dédiée à peser dans la gouvernance mondiale.

D'une manière générale, au sein des discussions internationales, deux conceptions de la gouvernance cyber sont défendues[85]. La première, celle des pays dits « libéraux » comme la Suède, est attachée à défendre Internet comme un espace de liberté, ne considérant pas comme nécessaire toute forme de réglementation du cyberespace. La deuxième, celle de la Chine et de la Russie, fait la promotion de règles contraignantes pour les États dans le cyberespace afin d'assurer la sécurité des systèmes d'information mais aussi réglementer le contenu des informations.

[84] Parmi eux, l'Arabie saoudite, l'Égypte, la Turquie, la Thaïlande, le Laos, la Serbie et les Émirats arabes unis.
[85] Bockel, J. M. (2012). *La cyberdéfense : un enjeu mondial, une priorité nationale*. Site officiel du Sénat. https://www.senat.fr/rap/r11-681/r11-68113.html

En ce sens, en 2010, le Secrétaire général de l'UIT évoque notamment l'idée d'un traité international interdisant la cyberguerre[86]. Une idée soutenue par la Chine et la Russie et bon nombre de pays en développement, qui souhaitent utiliser l'UIT comme enceinte permettant de diffuser leur approche de la cybergouvernance d'Internet. De leur côté, les pays dits « libéraux », qui ne souhaitent pas de traité contraignant sur la cybersécurité, plaident en faveur d'une aide de l'UIT au développement de solutions nationales, en particulier dans les pays en développement. L'installation, ou la multiplication de CSIRT en serait un des angles principaux. Par conséquent, les difficultés d'instauration d'un cadre normatif international de la cybergouvernance sont ici plus aisément perceptibles.

Outre les considérations politiques ou purement cyber, le talon d'Achille de la Chine demeure l'image qu'elle renvoie sur la scène internationale. La violente répression dans le Xinjiang, les mystères autour de l'installation des systèmes 5G par Huawei[87] ou encore le flou lié à l'origine de la pandémie de Covid-19, ne contribuent pas à faire d'elle un acteur fiable pour la majorité des États. A cela s'ajoute le non-respect des décisions internationales la condamnant, à l'instar de celle rendue par la Cour Permanente d'Arbitrage (CPA) en 2016 relative à son différend avec les Philippines sur la mer de Chine méridionale[88]. Elle se défend en expliquant que la juridiction n'a pas compétence dans cette affaire, alors même qu'elle demeure partie aux traités constitutifs. Il est ainsi plus difficile, pour les autres acteurs de la scène internationale, de croire en la bonne foi d'une Chine qui souhaite instaurer un cadre juridique contraignant sur la cybergouvernance mais qui ne se plie pas à la justice internationale. Est-ce pour autant à dire que l'incapacité à instaurer un cadre normatif international de cybergouvernance ne relève que de la méfiance des autres États envers la stratégie de la Chine ?

---

[86] Ibid.

[87] Hérard, P. (2021, 24 décembre). *Réseaux 5G : des problèmes et des inconnues à tous les étages*. TV5MONDE.https://information.tv5monde.com/info/reseaux-5g-des-problemes-et-des-inconnues-tous-les-etages-302251

[88] *PCA Press Release : The South China Sea Arbitration (The Republic of the Philippines v. The People's Republic of China)*. (2016). CPA.org. https://pca-cpa.org/fr/news/pca-press-release-the-south-china-sea-arbitration-the-republic-of-the-philippines-v-the-peoples-republic-of-china/

c) Les faiblesses structurelles du cadre de coopération internationale

Le format multi-acteurs de la coopération internationale en matière de cybergouvernance demeure paradoxalement sa principale faiblesse actuelle. Tout d'abord, le cadre onusien à travers les GGE ne permet pas de créer un cadre normatif international[89]. En effet, les divergences de conception du cyberespace entre les États et l'absence de pouvoir contraignant des résolutions de l'Assemblée générale des Nations Unies, contrairement à celles du Conseil de sécurité, en sont les principales causes. De la même façon, des entités telles que l'ICANN, dont la mission principale est la gestion de l'infrastructure Internet ou le FGI, qui n'est qu'une enceinte de discussions, ne peuvent outrepasser ou étendre leur compétence initiale. En effet, comme le mentionne Bertrand de la Chapelle dans son ouvrage, le FGI est « *un outil de decision-shaping et non de decision-making* »[90], en ce sens qu'il n'a pas pour vocation d'élaborer un régime normatif mais d'intervenir en amont d'une enceinte de décisions. De son côté, l'ICANN ne peut étendre la compétence qui lui a été attribuée initialement pour traiter de la gouvernance des usages d'Internet. Ces deux entités sont des laboratoires mais ne permettent pas d'entrevoir un cadre précis de cybergouvernance. Dès lors, comment imaginer un cadre d'élaboration de règles et régimes spécifiques ainsi qu'un organe veillant à la mise en œuvre et au respect de ceux-ci ?

Bien que le format multi-acteurs permet un échange diversifié, au-delà du système traditionnel entre acteurs étatiques, les limites sont naturellement visibles. Chacun cherchant à défendre une vision qui lui est propre, avec plus ou moins de pouvoir dans l'enceinte de discussions. Dans un contexte comme celui-ci, difficile de définir et d'établir des règles communes pour régir la gouvernance et l'usage d'Internet.

De plus, dans la prise en compte de certains enjeux de la gouvernance, à savoir ceux liés à la cyberguerre, certaines difficultés juridiques persistent. Par exemple, dans le cas de l'élaboration d'un traité international sur la cybersécurité, quel organe se chargerait de contrôler l'utilisation de capacités offensives et d'en sanctionner les éventuelles utilisations non autorisées ? Peut-on raisonnablement songer à instaurer un cadre similaire à celui du

[89] Bannelier-Christakis, K. (2017, 1 décembre). *Cyber-sécurité et régulation internationale : Quel forum après l'échec du GGE de l'ONU ?* Archive ouverte HAL. https://hal.archives-ouvertes.fr/hal-02055599/

[90] de La Chapelle, B. (2012). Gouvernance Internet : tensions actuelles et futurs possibles. *Politique étrangère*, , 249-261. https://doi.org/10.3917/pe.122.0249.

Traité de non-prolifération des armes nucléaires (TNP)[91], dont l'organe de régulation est l'Agence internationale de l'énergie atomique (AIEA)[92]?

Cependant, les difficultés d'élaboration d'un cadre international de la cybergouvernance sont-elles uniquement liées à des faiblesses structurelles? A l'absence d'une structure contraignante sur la cybergouvernance, s'ajoute le contexte de tensions internationales croissantes, qui fait ressortir des fragilités liées à la réaffirmation de la souveraineté étatique sur le sujet, avec pour chef de file la Chine.

2) Une défense chinoise ardue du principe de souveraineté nationale sur la gouvernance d'Internet

Au-delà de la simple défense du principe de souveraineté nationale, la Chine défend aujourd'hui celui de cyber-souveraineté[93], comme pierre angulaire de la politique numérique du PCC. A l'intérieur du pays, le *Cyberspace Administration of China* se charge d'administrer le cyberespace en Chine, sous le contrôle personnel du président Jinping. Déja en 2010, dans son Livre blanc sur l'Internet du futur, la Chine exposait clairement sa vision de la gouvernance du cyberespace dans son territoire *« à l'intérieur du territoire chinois, l'Internet est sous la juridiction de la souveraineté chinoise »*[94]. Et, l'arrivée au pouvoir de Xi Jinping en 2013 ne fera que confirmer cette vision de la souveraineté numérique, notamment lors de la Conférence mondiale de l'Internet en Chine en 2015[95], en déclarant *« Nous devons respecter le droit de chaque pays de choisir son propre modèle de cybergouvernance, sa propre politique à l'égard d'Internet »*.

a) La cyber-souveraineté au service du PCC dans son opposition avec les États-Unis

Historiquement, cette stratégie s'est construite via l'opposition marquée entre Pékin et Washington. En 2011, la publication par la Maison Blanche de sa vision libérale de la

---

[91] *Treaty on the Non-Proliferation of Nuclear Weapons - IAEA*. (1970). AIEA.org. https://www.iaea.org/publications/documents/infcircs/treaty-non-proliferation-nuclear-weapons

[92] *Site officiel de l'Agence internationale de l'énergie atomique*. AIEA.org. https://www.iaea.org/

[93] Ici les termes *cyber-souveraineté* et *souveraineté numérique* sont utilisés similairement.

[94] Richeri, G. (2018). L'Internet en Chine, entre État et opinion publique. *Les Enjeux de l'information et de la communication*, 19(1), 21-33. https://doi.org/10.3917/enic.024.0021

[95] Lemaître, F. (2021, 7 avril). *Le « modèle chinois » de souveraineté d'Internet gagne du terrain*. Le Monde.fr. https://www.lemonde.fr/international/article/2021/04/07/le-modele-chinois-de-souverainete-d-internet-gagne-du-terrain_6075852_3210.html

gouvernance du cyberespace[96] n'a pas été perçue d'un très bon œil par la Chine, qui y a vu une extension de son hégémonie dans le domaine numérique. Il faut dire que jusqu'aux années 2010, la Chine ne pouvait raisonnablement pas se permettre une confrontation directe avec les Etats-Unis. Ne serait-ce qu'à cause de leur interdépendance économique et a fortiori, de la supériorité militaire conventionnelle de ceux-ci.

Xi Jinping marque un tournant stratégique lors de son arrivée au pouvoir. Pour lui, la Chine doit s'affirmer comme première puissance mondiale, et ce, pas uniquement sur le domaine économique. Puisque les capacités militaires conventionnelles de la Chine ne sont pas à la hauteur de celles des Etats-Unis, Pékin se tourne alors vers les technologies militaires. La stratégie est alors duale : défendre sa souveraineté et poursuivre ses ambitions de puissance.

D'une manière générale, pour faire écho aux précédents développements, l'élaboration de la cyberstratégie chinoise est à la fois fondée sur la pensée militaire chinoise (*weishe*) mais avec des adaptations plus modernes pour faire face au géant américain. Les ambitions de puissance de la Chine dans le cyberespace sont inévitablement liées à la conception du cyberespace défendue par les américains. Évidemment, des conceptions plus subjectives à la Chine entrent en jeu dans sa stratégie de cybergouvernance.

b) Les limites de la conception chinoise de la souveraineté numérique

Dans la conception essentielle de la cyber-souveraineté, il y a cette idée selon laquelle chaque Etat doit être en mesure de décider seul de la réglementation de son propre cyberespace. La transposition de la notion de souveraineté étatique sur celle du cyberespace ne semble a priori pas poser de problème.

La Chine considère largement la notion de souveraineté étatique à la fois comme de l'autodétermination mais également comme l'autorité suprême de l'État face aux acteurs non étatiques. Cette prédominance de l'État est perceptible dans la stratégie diplomatique chinoise, à l'instar de la nomination d'un coordinateur dédié à la cybersécurité au sein du département de contrôle des armements du Ministère des Affaires étrangères[97]. Celui-ci étant chargé de mener les discussions sur le sujet, à la fois en bilatéral avec les autres États mais aussi en multilatéral, par exemple dans l'enceinte des Nations Unies.

---

[96] Kolton, M. (2017). Interpreting China's Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence. *The Cyber Defense Review*, Vol. 2, N°1, p. 129. https://cyberdefensereview.army.mil.

[97] Bockel, J. M. (2012). *La cyberdéfense : un enjeu mondial, une priorité nationale*. Site officiel du Sénat. https://www.senat.fr/rap/r11-681/r11-68113.html

En outre, l'État doit être le seul habilité à contrôler ce qui se passe sur le territoire national, notamment l'usage d'Internet qui en est fait. Outre la simple capacité à définir des règles d'usage applicables au cyberespace, c'est la bonne application et la conduite des individus et entreprises qui y sont contrôlées. A ce titre, la Grande muraille pare-feu chinoise (Great Firewall of China)[98] est l'illustration parfaite de la vision de la souveraineté numérique qu'entretient la Chine.

Néanmoins, le point d'orgue de la contradiction juridique demeure la question de la souveraineté territoriale, dans un cyberespace dépourvu de frontières physiques. En pratique, si un bureau d'enregistrement[99] basé sur le territoire d'un État X procède à l'enregistrement du nom de domaine d'un site étranger, la cyber-souveraineté territoriale de l'État s'étend hors de ses frontières. A titre d'exemple, ce fut le cas pour le site espagnol *rojadirecta.com* en 2011[100], dont le nom de domaine avait été acquis par un bureau d'enregistrement américain, qui a fait l'objet d'une saisie par le département *Homeland Security* de l'*Immigration and Customs Enforcement* (ICE).

De cette façon, considérer qu'une loi nationale ou une décision de justice s'appliquent au contenu d'un site étranger, simplement car l'enregistrement du nom de domaine est réalisé à l'étranger, occasionnerait forcément des conflits de lois ou des conflits de juridictions en droit international privé. En effet, cela obligerait toute plateforme web à se conformer dès sa création à plus d'une centaine de législations nationales, avec une possibilité de contradiction entre elles voire même de règles spécifiques édictées au niveau infranational pour les systèmes fédéraux.

Par conséquent, la limite principale du concept de souveraineté numérique demeure l'aspect territorial. La souveraineté numérique territoriale se modulant ainsi en fonction de l'implantation des bureaux d'enregistrement dans le pays, plus un pays en est doté plus sa souveraineté numérique est importante et vice-versa. En ce sens, faut-il considérer qu'ils constituent une nouvelle « géographie du cyberespace »?

---

[98] Pedroletti, B. (2010, 12 octobre). *La grande muraille virtuelle de Chine*. Le Monde.fr. https://www.lemonde.fr/asie-pacifique/article/2010/10/11/archive-la-grande-muraille-virtuelle-de-chine_1424220_3216.html

[99] Les *registrars* assurent la distribution, auprès des utilisateurs finaux, des noms de domaine de second niveau gérés par les registres. Plusieurs centaines de *registrars* à travers le monde assurent ainsi la mise à disposition des noms en *.com, .org, .net* ou de certaines extensions pays.

[100] Le Monde. (2012, août 31). *Fin de blocage des noms de domaine de Rojadirecta*. Le Monde.fr. https://www.lemonde.fr/technologies/article/2012/08/31/fin-de-blocage-des-noms-de-domaine-de-rojadirecta_1754045_651865.html

B) Mise en place d'un système de monnaie numérique nationale : faire entrer le régalien dans le cyberespace

Pan entier d'un des domaines régaliens de l'État, la politique monétaire est l'expression de sa puissance aussi bien en interne qu'à l'internationale. En ce sens, la monnaie chinoise - le yuan[101] - ne parvient toujours pas à se hisser au niveau du dollar dans le système financier international. Et pour cause, depuis la fin du système de Bretton Woods en 1971 et la fin de la convertibilité en dollar-or, les États-Unis règnent d'une main de maître sur le système financier international grâce notamment au Fonds Monétaire International (FMI) et à la Banque mondiale (BM). Malgré un développement économique fulgurant depuis le début des années 2000[102], la République populaire de Chine peine à imposer le yuan comme monnaie d'échange à l'international. Aujourd'hui, dans sa stratégie de cyberpuissance, comment la Chine peut-elle espérer s'imposer en tant que telle sur l'aspect monétaire?

La mise en place de sa propre monnaie numérique, gérée par le gouvernement chinois, est un premier pas dans sa stratégie de cyberpuissance, à la fois pour contourner le système américain (B) mais aussi pour contrôler sa population (A).

1) Le yuan numérique comme outil de contrôle de la population et des transactions

a) Contrôler les transactions pour mieux contrôler la population

L'Etat chinois entend bien conserver en son sein le pouvoir de contrôler les transactions financières pour contrôler les dépenses de sa population. En effet, la Chine compte également reprendre en main ses géants locaux à l'instar d'Alibaba et Tencent qui possèdent les deux applications de paiement les plus utilisées en Chine : AliPay et WeChat Pay. Elle souhaite pouvoir contrôler leurs activités, au même titre que ceux des particuliers, en témoigne la récente amende infligée par l'État chinois à son géant Alibaba[103]. Pas question pour le PCC de laisser à ces géants du numérique les plein pouvoirs sur le contrôle de

[101] En ce sens, par souci de simplification, l'utilisation de « yuan » sera préférée à « renminbi ». Yeung, K. (2020, 15 décembre). *China's yuan vs renminbi : what's the difference?* South China Morning Post. https://www.scmp.com/economy/china-economy/article/3109065/chinas-yuan-vs-renminbi-whats-difference

[102] Mistral, J. (2021). *Guerre et paix entre les monnaies - Économie et géopolitique au XXIe siècle*. Gallimard.

[103] Leplâtre, S. (2021, 12 avril). *L'amende de 2,3 milliards d'euros infligée à Alibaba, signe de la reprise en main des géants de la tech par Pékin*. Le Monde.fr. https://www.lemonde.fr/economie/article/2021/04/11/alibaba-mis-a-l-amende-par-pekin-qui-accentue-la-reprise-en-main-de-la-tech-chinoise_6076382_3234.html

l'argent. Et pour cause, un rapport publié en 2017 par le think tank indépendant CGAP (*Consultative Group to Assist the Poor*)[104] montre que les deux applications de paiement mobile détiennent 92% des parts de marché puisque la plupart des utilisateurs souscrivent aux deux solutions. Ce qui n'est pas étonnant lorsqu'il s'agit de constater le nombre d'utilisateurs de paiement mobile en Chine, qui s'élève à plus de 500 millions, selon l'organisme public *China Internet Network Information Center* (CNNIC)[105]. Également, grâce à une surveillance accrue de ses géants technologiques, la Chine veut supplanter, sinon compléter les services de paiements AliPay et WeChat. La monnaie « physique » s'éteint progressivement dans les grandes villes chinoises, ce qui pousse la Chine à s'immiscer dans ce marché.

A posteriori, cela ne semble pas être une source d'inquiétude pour la Chine qui y voit là une opportunité de contrôle supplémentaire. En effet, l'argent physique est plus difficilement traçable, il est impossible de contrôler en temps réel et au yuan près ce qui est dépensé par un particulier. D'où cette volonté d'introduire sa propre monnaie numérique : le e-yuan. Avec une valeur identique à celle d'un billet papier, le e-yuan est simplement son équivalent numérique. Le lancement effectif de sa monnaie en 2020[106], précédé du dépôt par la RPC d'une centaine de brevets[107], lui laisse entrevoir doucement les portes du contrôle massif des dépenses de la population du pays.

Outre la simplicité d'utilisation qu'elle avance - un téléphone portable et l'application de la Banque centrale suffisent pour régler - l'absence de frais générés par ces paiements est un avantage indéniable aussi bien pour les consommateurs que pour les commerçants, contrairement aux applications privées qui en prélèvent[108]. Pour la population qui utilise les solutions de paiement mobile, cela ne constitue qu'une autre application à télécharger. Mais ce portefeuille numérique créé et détenu par le gouvernement chinois sera un véritable outil de pointe pour contrôler les transactions et éventuellement infliger des sanctions à ceux qui ne dépenseraient pas l'argent comme bon lui semble. Contrairement aux cryptomonnaies, le e-yuan ne protège pas l'anonymat de l'utilisateur.

---

[104] Aveni, T., & Roest, J. (2017). *Chine - Alipay et WeChat Pay : atteindre les utilisateurs ruraux*. CGAP. https://www.cgap.org/sites/default/files/Brief-Chinas-Alipay-and-WeChat-Pay-Dec-2017-French.pdf

[105] Ibid

[106] *Triennial Central Bank Survey of Foreign Exchange and Over-the-counter (OTC) Derivatives Markets in 2019*. (2019, 16 septembre). BIS.org. https://www.bis.org/statistics/rpfx19.htm

[107] Courrier International. (2021, 23 janvier). Monnaie. Le yuan numérique, un outil de contrôle pour la Chine. https://www.courrierinternational.com/article/monnaie-le-yuan-numerique-un-outil-de-controle-pour-la-chine

[108] André, D. (2021, 8 mai). *La Chine teste le e-yuan, une monnaie numérique*. Franceinfo. https://www.francetvinfo.fr/monde/chine/la-chine-teste-le-e-yuan-une-monnaie-numerique_4615889.html

En ce sens, l'autre positionnement de la Chine en faveur de sa propre monnaie numérique est l'annihilation progressive des paiements en crypto-monnaies qui persistent. L'anonymat, qui est le principal attrait des particuliers pour ce genre d'actifs.

b) En finir avec les crypto-monnaies

Effectivement, un autre intérêt de la Chine à développer sa propre monnaie numérique est de réduire l'intérêt de la population pour les crypto-monnaies. Malgré l'interdiction progressive de la fabrication et l'utilisation de crypto-monnaies en Chine[109], les transactions entre les personnes s'opèrent dans l'ombre. En septembre 2021, la Banque populaire de Chine (BPC) a déclaré dans un communiqué que *« toutes les activités commerciales liées aux crypto-monnaies étaient illégales »*[110]. Cette action a, en outre, eu pour conséquence de faire baisser la valeur des crypto-monnaies les plus plébiscitées, à l'instar du Bitcoin qui a plongé de 6,2% ou de l'Ethereum à hauteur de 10,7% en une journée, selon les données de Bloomberg[111]. Cette volonté d'annihiler la circulation de crypto-monnaies est évidemment liée à l'essence même d'une crypto-monnaie, destinée à s'affranchir des banques centrales.

2) Le yuan numérique comme outil de contournement du système financier international

a) S'extraire d'un système financier dominé par le dollar

L'importance d'une monnaie sur le plan international se mesure à la place qu'elle prend dans les réserves de change officielles détenues par les banques centrales, dont les données recueillies par le FMI contiennent quasiment 95% des réserves de change mondiales[112]. Sans surprise, le dollar s'inscrit en tête du classement de ces réserves de change

[109] Capital.fr. (2022, 28 janvier). *Le Bitcoin plonge, la Chine interdit l'industrie des cryptomonnaies*. https://www.capital.fr/crypto/interdiction-de-lindustrie-des-cryptomonnaies-en-chine-les-fermetures-dentreprises-se-succedent-1407034

[110] Shawn Deng and Chris Liakos, CNN Business. (2021, 24 septembre). *Bitcoin plummets after China intensifies cryptocurrency crackdown*. CNN. https://edition.cnn.com/2021/09/24/investing/china-cryptocurrency-ban/index.html

[111] *cf note 34*

[112] Prasad, E. « Has the dollar lost ground as the dominant international currency? », *Global Economy and Development at Brookings*, Brookings, 20 septembre 2019 (www.brookings.edu/ research/has-the-dollar-lost-ground-as-the-dominant-international-currency).

détenues par diverses banques centrales avec 61,8% selon les chiffres du FMI en 2019[113]. A côté, le yuan n'apparaît qu'en 5ème position avec quasiment 2%[114]. Par ailleurs, dans l'enquête menée en 2019 par la Banque des règlements internationaux (BRI), le dollar est également la devise la plus échangée dans le monde à hauteur de 88% des transactions enregistrées contre 4,3% pour le yuan en huitième position[115]. Dès lors, comment la Chine peut-elle espérer imposer le yuan dans le système financier international ?

Depuis 2014, la Chine développe sa propre monnaie numérique nationale et est même le premier pays à l'avoir lancé lors de phases de tests en 2020[116]. Son objectif, à moyen terme, est de marquer la fin de la prééminence du dollar américain dans les transactions internationales.

Première étape, le lancement de son système de paiement interbancaire transfrontalier en 2015, le *China International Payment System* (CIPS)[117] qui a pour vocation de lever tout obstacle à l'internationalisation du yuan. En effet, l'un des principaux obstacles demeure à nouveau américain via le principal système de paiement interbancaire mondial SWIFT (*Society for Worldwide Interbank Financial Telecommunication)* qui capte la majeure partie des transactions mondiales. Afin d'inciter à opter pour CIPS, la Chine garantit une réduction des frais de transactions ainsi que des délais de traitement[118]. En effet, avant l'instauration de ce système, les transactions transfrontalières effectuées en yuan devaient transiter par d'autres établissements habilités ou bien encore une banque continentale affiliée à ces établissements. Mais, le nouveau système CIPS permet aux entreprises localisées hors de Chine de pouvoir traiter directement avec les entreprises chinoises, notamment dans le cadre du projet des Nouvelles routes de la soie de la Chine.

---

[113] Arslanalp, S., Simpson-Bell, C. (2021, 5 mai). *La part du dollar dans les réserves de change mondiales atteint son niveau le plus faible en 25 ans*. FMI. https://www.imf.org/fr/News/Articles/2021/05/05/blog-us-dollar-share-of-global-foreign-exchange-reserves-drops-to-25-year-low

[114] Ibid

[115] *cf note 31*

[116] Fouquet, C. (2022, 7 janvier). *La Chine accélère le déploiement de son yuan numérique*. Les Echos. https://www.lesechos.fr/finance-marches/marches-financiers/la-chine-accelere-le-deploiement-de-son-yuan-numerique-1376805

[117] *The Chartered Institute of Procurement and Supply*. CIPS.org. https://www.cips.org/

[118] Chen, M. K. G. Q. (2015, 9 mars). *Ultimes préparatifs pour le système chinois de paiements internationaux*. Reuters.com. https://www.reuters.com/article/chine-paiements-yuan-idFRL5N0WB1CG20150309

Pour autant, Pékin a compris qu'il serait très difficile de concurrencer le système SWIFT. En conséquence, et a priori paradoxalement, elle a choisi de s'allier avec lui pour déployer sa monnaie numérique via l'entreprise pékinoise *Finance Gateway Information Service* créée en janvier 2021. Les parts de l'entreprise sont divisées entre l'actionnaire majoritaire SWIFT à hauteur de 55% , la People's Bank of China (PBOC) à 34%, le CIPS à 5% et enfin un service interne et un institut de recherche de la PBOC qui se partagent les 6% restants. Dans un premier temps, la stratégie de la Chine n'est pas de s'émanciper totalement du système SWIFT, mais d'y introduire sa monnaie numérique pour démocratiser son existence. Ainsi, elle pourra, au moment opportun, adopter une stratégie offensive de repli vers son système CIPS.

Autre problématique, la mise en place de ce système concurrent CIPS est une véritable aubaine pour la Chine dans sa stratégie de détournement du système financier dominé par les États-Unis. En effet, les sanctions américaines touchant plusieurs États du Monde à l'instar de l'Iran ou la Russie pourront ainsi être contournées puisqu'aucun contrôle de la part de l'OFAC (*Office of Foreign Assets Control*) ne sera réalisé sans transaction en dollars. A ce titre, depuis la mise en place des sanctions américaines en 2014 pour faire suite à l'annexion de la Crimée par la Russie, le commerce entre Pékin et Moscou a augmenté de 50%[119]. La Chine est ainsi devenue la première destination pour les exportations russes. La situation actuelle en Ukraine, et les sanctions américaines adoptées contre la Russie notamment sur le réseau SWIFT, est une porte ouverte laissée à la Chine pour introduire son modèle. Le développement de ce système est évidemment inquiétant pour Washington, dont la domination sur les transactions transfrontalières s'en verrait affaiblie.

b) Ouvrir la voie à un nouvel écosystème financier

L'introduction de la monnaie numérique chinoise ne permettra de rivaliser de manière imminente avec le dollar dans les transactions financières, néanmoins son objectif est de croître, en particulier en marge du système financier international. Autre avantage de ce nouvel écosystème financier dominé par la monnaie nationale numérique, les banques centrales pourraient baisser leurs taux d'intérêt en-deçà de zéro, ce qui constitue une stratégie

[119] Leblanc, C. (2022, 3 mars). *Russie : contre Swift, l'alternative chinoise passe par Cips et le e-yuan.* l'Opinion.https://www.lopinion.fr/international/swift-cips-yuan-numerique-pekin-alternative-financier-domine-par-occident

d’investissement indéniable et a fortiori garantit à la Chine de détenir des créances de toute part. Le contrôle de l’État sur la monnaie sera total puisque toutes les transactions seront suivies en temps réel et dépourvues de toute surveillance de la part des institutions financières internationales telles que le FMI ou la BM. L’État chinois aura donc un quasi « droit de vie et de mort » sur sa monnaie nationale. A sa guise, la banque centrale pourra émettre de la monnaie mais aussi décider de la péremption de celle-ci. Un système aussi innovant qu’inquiétant, d’autant que la Chine devance largement les autres puissances sur cette question. Son leadership technologique est sans aucun doute la caractéristique qui lui permet d’influencer sur les marchés et de se hisser comme cyberpuissance à terme.

Mais la Chine a d’autres ambitions pour se positionner comme cyberpuissance sur la scène internationale, en témoignent le contrôle ardu qu’elle exerce sur l’économie du pays.

Chapitre 2 : Développer l'écosystème cyber chinois pour une hégémonie économique

Le contrôle et la souveraineté financière que la Chine exerce sur le pays lui permettent de développer son écosystème économique, de manière et surpasser les marchés étrangers. Afin d'affirmer cette hégémonie économique, on constate que la Chine possède à son actifs des réalisations, mais également des ambitions tels que les routes de la soie du numérique, la diffusion de l'accès à internet à toute la population, mais aussi l'utilisation des BATX comme outils de puissances.

De plus, la Chine a souvent été considérée comme l'usine du monde. Elle a gardé l'image d'un pays qui fabrique et recopie les créations de ses voisins. Cependant, son développement passe également par sa recherche et à sa capacité d'innover de nouveaux produits. C'est dans le domaine du digital qu'elle arrive à prospérer grâce à sa jeune population impliquée dans les domaines, ses universités spécialisées à la recherche de l'excellence, enfin ses entreprises qui orientent leur croissance économique dans la numérisation. Ses nombreux axes sont poussés par le gouvernement, connaissant pleinement les enjeux du cyber.

Cette connaissance des enjeux cyber est d'ailleurs utilisée par le PCC afin d'influencer le reste du monde et sa population. Les nouvelles technologies permettent effectivement au Parti de mettre en place des mesures plus ou moins incitatives pour faire adhérer ses citoyens à son idéologie. Ces mesures font partie intégrante de la stratégie chinoise en matière de guerre de l'information.

I) Conquête de marchés : Diffusion à l'extérieur et implantation à l'intérieur.

A) La mise en place de l'écosystème numérique par l'expérimentation

1) Les Zones Économiques Spéciales

Théorisées à partir des années 70, les **zones économiques spéciales** (**ZES**) sont des régions dans lesquelles les lois économiques sont plus avantageuses pour les entreprises, que celles pratiquées dans le reste du pays. Ce dispositif qui offre une combinaison d'incitations fiscales, de droits de douanes favorables, des procédures douanières simplifiées et réglementations limitées a retenu l'attention de nombreux États. En Chine, les ZES ont fait figure de zones d'expérimentations de mesures libérales avant que ces expériences ne soient étendues à l'ensemble du pays.

En Chine comme ailleurs, c'est d'abord à travers le développement des ZES que s'est conçue la diffusion nationale du numérique. Mais après les expérimentations des années 90, l'accès à internet s'est démocratisé grâce à différents plans. Que ce soit avec les villages Taobao ou la "Go west policy", le régime s'est employé à utiliser le numérique comme facteur de réduction des inégalités et de décentralisation.

a) Les ZES et les premières expérimentations du numérique chinois.

Les Zones Économiques Spéciales, ou ZES (经济特区) sont des zones définies par le régime et bénéficiant d'un statut juridique particulier devant les rendre plus attrayantes pour les investissements étrangers et leurs savoir-faire.

Voyant le jour dès 1979 et d'abord limités aux provinces du Guangdong et du Fujian dans le Sud de la Chine, elles connaissent sous le gouvernement de Deng Xiaoping un développement très rapide, particulièrement à Shenzhen., qui passe en 35 ans d'un petit village à une métropole de 10 millions d'habitants. Le principe même des ZES est d'expérimenter des tentatives de libéralisation de l'économie avant de les étendre au reste du pays.

Les premières ZES chinoises se sont concentrées sur la fabrication et l'exportation des produits de base (comme les vêtements) avant de remonter la chaîne de valeur et de se reconvertir vers une production plus sophistiquée.

En 1984, quatorze villes côtières, dont Canton et Shanghai, sont autorisées à créer leurs propres ZES, ouvertes aux investissements étrangers. C'est le début de l'industrialisation de la Chine, tournée vers la production de biens de consommation destinés à l'exportation, et de l'insertion massive de lu pays dans l'économie globale.

Dans l'article de Michel Roy intitulé *Shenzhen: une zone économique spéciale en Chine populaire*[120], l'auteur reprend les propos de Liang Xiang, maire de Shenzhen entre 1980 et 1988 qui décrit les ZES comme un ensemble de politiques visant à favoriser les capitaux étrangers à investir en Chine afin d'acquérir de nouvelles compétences techniques et de nouveaux équipements plus modernes.

En pratique, les ZES offrent des allégements fiscaux et administratifs pour les entreprises étrangères à condition de transférer à la Chine de nouvelles technologies. Contrairement au reste du pays, l'État simplifie les formalités pour faciliter l'entrée dans le marché chinois. Les entreprises technologiques de pointe, dont le montant des investissements dépasse 5 millions de dollars, peuvent bénéficier d'une réduction fiscale pouvant aller jusqu'à 50 %.

En engageant des réformes d'abord limitées à des zones bien définies, Deng Xiaoping a pris le temps d'analyser les forces et les faiblesses du capitalisme occidental. En son temps, le petit timonier[121] recommandait de s'appuyer sur "les pierres du gué pour traverser la rivière"[122] (摸着石头过河) et ainsi d'injecter du pragmatisme et de l'expertise là où le militant communiste rouge devait remplacer l'expert durant la révolution culturelle. Il considérait ainsi que les systèmes politiques devaient évoluer pour correspondre aux besoins de la population. Peu importe la couleur du chat du moment qu'il attrape la souris[123]...

---

[120]Roy, M. (2016, 26 avril). *Shenzhen : une zone économique spéciale en Chine populaire*. Persée. https://www.persee.fr/doc/receo_0338-0599_1983_num_14_3_2451

[121] C'est le surnom donné à Deng Xiaoping, alors que Mao Zedong était le grand timonier.

[122] S'exprimant souvent sous forme de d'images, Deng Xiaoping veut ici exprimer l'idée que le pragmatisme économique est plus efficace que l'idéologie. Girardot, P. E. (2009). *TRAVERSER LA RIVIÈRE EN TÂTONNANT PIERRE À PIERRE - 摸着石头过河.* Nouvelles du Monde. https://www.lajauneetlarouge.com/wp-content/uploads/2014/10/698-page-058-061.pdf

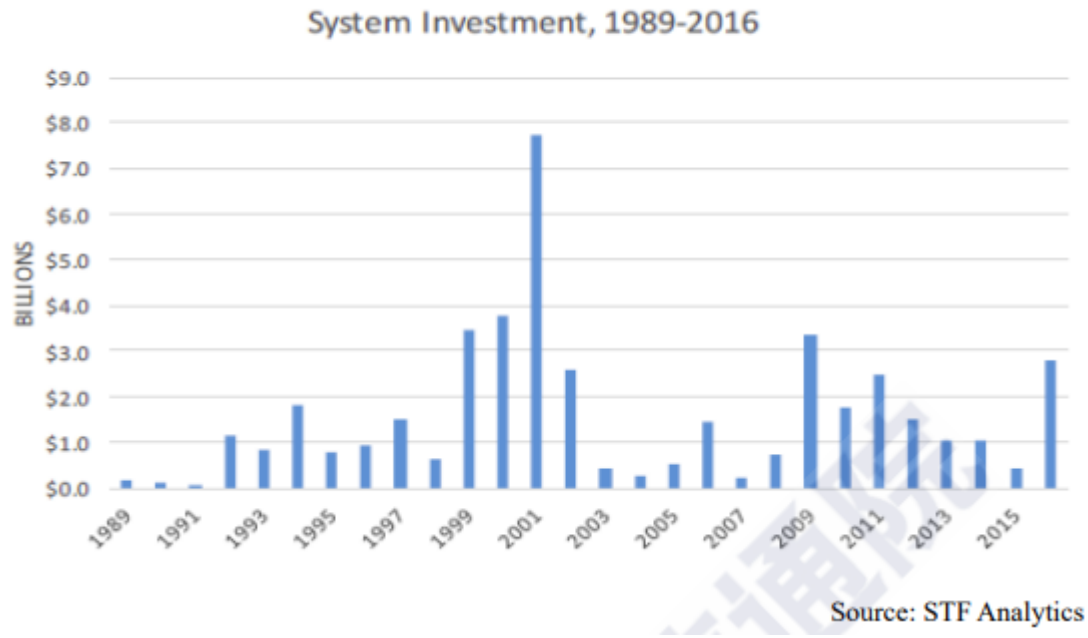
[123] 不管黑猫白猫，捉到老鼠就是好猫 en chinois est un slogan prononcé par Deng Xiaoping en 1971 montrant que peu importe l'idéologie ou la nationalité des entrepreneurs et des investisseurs pourvu qu'ils contibuent au développement économique de la Chine.

À cette vision prudente de petits pas succède celle incarnée par Xi Jinping, qui pense l'accélération économique du pays comme une véritable rupture de l'ordre économique mondiale.

Dans ce contexte de transformations économiques profondes des années 80, 90, les télécommunications et l'industrie du numérique sont dès l'origine identifiées par le régime comme des domaines stratégiques prioritaires. De lourds investissements sont alors consentis pour développer la téléphonie mobile, ainsi que le réseau internet. Entre 1997 et 2009, c'est 4,3 milliards de yuans qui sont investis dans la construction d'infrastructures Internet pour un réseau de 8 268 millions de kilomètres de câbles optiques, favorisant l'apparition de géants des télécoms comme China Telecom, China Unicom ou China Mobile, pour plus de 500 millions de consommateurs en 2012. En 2016, la Chine regroupait plus de 750 millions d'internautes (l'équivalent de la population européenne).

Evolution des investissements dans les câbles Internet en Chine entre 1989-2016[124]

Figure 1-1 Submarine cable system investment (1989-2016)



Ainsi, avec les ZES, la stratégie chinoise n'est plus de rattraper le niveau de développement numérique des pays occidentaux, mais de devenir pionnière dans les technologies de pointe.

Dans le discours officiel, Internet est un élément déterminant pour le retour de la Chine comme première puissance mondiale. Dès 2001, dans le Quotidien du peuple, le régime

[124] China Academy of Information and Communications. (2018). *White Paper on China International Optical Cable Interconnection*. CAICT. http://www.caict.ac.cn/english/

annonçait que “le degré de développement des technologies de l’information et des réseaux est devenu un instrument important pour mesurer le niveau de modernisation d’un pays et sa puissance globale”[125].

Concrètement et dès le début du web chinois, par des mesures de censure vis-à-vis de la population et un arsenal législatif contraignants contre les entreprises étrangères, constituant un dilemme pour ces dernières, devant choisir entre se soumettre aux règles de la censure et l’accès au marché chinois.

Assumant cette posture d’un contrôle d’internet pour des raisons de souveraineté, le régime déclare ainsi dans le *white paper*[126] de 2010 : “*Le gouvernement chinois croit qu’internet est un équipement d’infrastructure important pour la nation. Sur le territoire chinois, Internet est sous la juridiction de la souveraineté chinoise. La souveraineté de la Chine sur Internet doit être respectée et protégée* “.

Avec les ZES, le régime chinois développe ainsi ses futurs géants du numérique en revendiquant dès le début une mainmise sur le secteur des nouvelles technologies de l’information et de la communication (NTIC), identifiés comme stratégiques. La construction d’une économie socialiste de marché par ces expérimentations permet alors de développer des pôles d’activités numériques dans les grandes métropoles, constituant un maillage des infrastructures centralisé.

b) Le “go west Policy” et les village Taobao

En parallèle du développement des ZES. Avec sa politique du *Go West Strategy* (西部大开发) qui couvre 6 provinces[127], 3 régions autonomes[128] et la municipalité autonome de Chongging dans le Sichuan, le régime veut réduire les inégalités croissantes entre les régions côtières du Sud et l’intérieur des terres.

Sur ces régions couvrant 70 % du territoire pour 30% de la population, les investissements se concentrent d’abord sur les grandes infrastructures, (comme des ensembles de gazoducs, le chemin de fer reliant Lhassa au Tibet ou de grands barrages, notamment dans le Sichuan),

[125] Boschet, A., Chimenti, J., Mera Leal, N. et Duval, T. (2019) *Chine Digitale Dragon Hacker de puissance.* Editions VA. Editions-Collection Guerre de l’information, page 18

[126] White paper on the Internet in China (15 juin 2019), disponible ici : Full Text: White paper on the Internet in China[7]- Chinadaily.com.cn

[127] Sichuan, Guizhou, Yunnan, Shaanxi, Gansu et Qinghai

[128] Tibet, Xinjiang et le Ningxia

cette politique comporte un volet sur le numérique visant à diluer la concentration des entreprises technologiques après avoir créé un vivier de talents dans la première phase des ZES. Des villes comme Chongjing ou Changdu attirent des entreprises comme Lenovo, Foxconn, Intel ou Honda, qui profitent des réductions fiscales faites aux entreprises travaillant dans le numérique et du réseau de câble optiques qui double dans les régions concernées.

Le concept des villages *TaoBao (淘宝网)* traduit la volonté du régime d'encourager toujours plus l'économie numérique à se diffuser à l'intérieur du pays et dans les campagnes. Le nom TaoBao vient de l'entreprise TaoBao.com, du groupe Alibaba. Le terme n'est donc pas officiel, mais correspond à la diffusion d'internet et de ses possibilités commerciales, particulièrement au niveau du E-Commerce en dehors des grandes métropoles.
Ainsi, la croissance de Taobao.com a créé de nouveaux pôles numériques et de production de service, regroupant un grand nombre de commerçants en ligne, vivant dans un village, faisant des affaires principalement sur TaoBao.com et réalisant des économies d'échelle par leur regroupement.
Alors qu'en 2009, seuls trois villages en Chine étaient défini comme un village TaoBao, on en compte plus de 2500[129] en 2019 répartis sur 24 régions relevant du gouvernement central et des régions autonomes.
Ici les villageois sont acculturés au numérique et encouragés par le PCC local à créer au moins 3 sites par villages.

À travers les ZES, la politique du GO west et les villages TaoBao, on peut voir que le régime chinois veut développer un large tissu d'entreprises du numérique présent sur tout le territoire.
En plus d'être présenté comme un outil efficace pour réduire les inégalités entre les régions, cette politique permet à la Chine de décentraliser l'activité économique, trop longtemps concentrée sur les côtes.

[129] Lulu, F. (2019). *Taobao Villages - The Emergence of a New Pattern of Rural Ecommerce in China and its Social Implications*. Friedrich Ebert Stiftung. http://library.fes.de/pdf-files/bueros/indonesien/15198-20180218.pdf

2) Les batxh comme outil de puissance

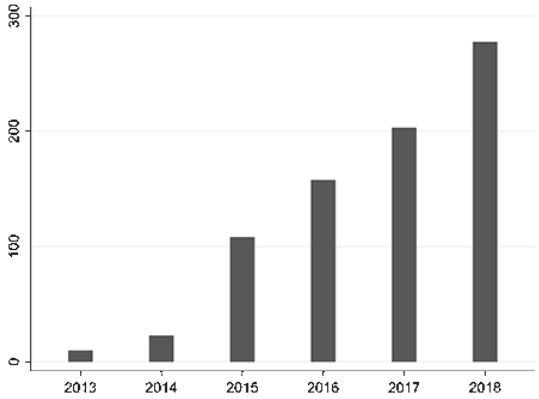
a) Alibaba et Tencent, exemples d'outils de puissances sous le contrôle de Beijing pour développer des activités stratégiques comme l'IA, la 5G ou le Cloud.

Cette diffusion de l'activité en ligne sur l'ensemble du territoire a permis de réaliser des économies d'échelle et d'atteindre un marché encore à développer dans les campagnes.
Au niveau national et dès 2018, 70 % des paiements quotidiens[130] se font déjà par téléphone, écartant les paiements traditionnels comme Mastercard.
Profitant de cette diffusion des paiements par téléphone et de l'e-commerce, des entreprises comme Alipay ou Wechat Pay connaissent des succès fulgurants pour plus de 700 millions de clients à travers le pays. En 2017, les transactions effectuées depuis des téléphones ont ainsi dépassé les 10 000 milliards d'euros sur l'année.

Ces dernières années, on a assisté à une expansion rapide des activités de paiement mobile en Chine, en termes d'utilisateurs actifs, de nombre de transactions et de valeur des transactions. Le nombre d'utilisateurs actifs d'Alipay est passé d'un peu plus de 100 millions en 2013 à 900 millions en 2018, et celui de WeChat Pay est passé d'environ 350 millions à 1,1 milliard. La valeur totale des transactions a bondi de 14,5 trillions de RMB en 2013 à 277,4 trillions de RMB en 2018, enregistrant un taux de croissance annuel de 80 %.
Le nombre de transactions de paiement mobile a atteint 60,5 milliards en 2018, soit une hausse de 61 % par rapport à l'année précédente. La part du paiement mobile dans la valeur totale des paiements scripturaux est passée de moins de 1 pour cent en 2013 à 7,4 pour cent en 2018, et la part du paiement mobile dans le nombre total de transactions de paiement scripturales est passée de 3,3 pour cent en 2013 à 27,3 pour cent en 2018.
Certaines plateformes de paiement mobile ont également évolué vers de grands écosystèmes, couvrant un large éventail d'activités telles que le financement, la gestion financière, la référence de crédit et le big data (ici on pense à Wechat ou Alipay).

[130] Yiping Huang, Xue Wang et Xun Wang Mobile Payment in China: Practice and Its Effects (Octobre 2021) Mobile Payment in China: Practice and Its Effects* | Asian Economic Papers | MIT Press

Évolution de la valeur totale des transactions par paiement mobile entre 2013 et 2018.[131]



À l'international, les BATX (Baidu, Alibaba, Tencent, Xiaomi) mènent leur politique d'internationalisation[132]. Lancée par le gouvernement chinois à la fin des années 1990, elle doit jouer un rôle majeur pour aider les industriels à s'insérer dans la mondialisation. Les géants du numérique, qui ont pris le temps de se développer à l'ombre de l'État chinois, partent à la conquête de la planète.

La première étape de leur stratégie a consisté à s'emparer de leurs concurrents régionaux. En quelques années, ils ont pris le contrôle de plusieurs leaders numériques asiatiques, aidés en cela par les diasporas chinoises implantées dans ces pays.

C'est le cas de Go-Jek, la licorne indonésienne spécialiste des scooters à partager rachetée par Tencent, ou de la start-up singapourienne d'e-commerce Lazada, désormais propriété d'Alibaba. Les BATX se sont même emparés d'actifs stratégiques dans ces pays, à l'instar des 10 % de la poste singapourienne acquis par Alibaba en 2014. *« Les BATX ont profité de la frilosité des investisseurs asiatiques pour le numérique, et de la passivité des Gafam, pour mettre ces pays en coupe réglée »*, explique Martin Pasquier, directeur général de *Innovation is everywhere*[133], basé à Singapour.

Les BATX ont également investi dans la production de contenus. Ainsi, Tencent, très présent dans les jeux vidéo en Chine, a misé dans ce secteur en Thaïlande, à Singapour et même en

[131] Idem.

[132] La Go Out Policy ou stratégie de mondialisation (en chinois, 走出去战略) est la stratégie actuelle de la République populaire de Chine pour encourager ses entreprises à investir à l'étranger.

[133] Martin Pasquier, directeur général de *Innovation is everywhere*, dans un article de Florent Detroy *Les BATX sous l'empire du milieu.* (Janvier 2018) Magazine-deciedeurs.com Les BATX, sous l'empire du Milieu - Magazine Decideurs (magazine-decideurs.com)

Finlande, avec le rachat de Supercell, l'éditeur du jeu Clash of Clans. Xiaomi, le constructeur de smartphones, a appliqué une stratégie similaire en Inde, en rachetant une société de diffusion de contenus audio et vidéo. Plus récemment, les géants chinois de la tech ont mené une offensive remarquée sur le marché américain. Alibaba a investi dans divers films hollywoodiens, dont le dernier épisode de la saga *Mission : Impossible-Rogue Nation*, tandis que Tencent devrait financer le prochain film Avatar 2, de James Cameron, le réalisateur de *Titanic*[134]. Les stratégies de ces acteurs sont claires, s'imposer sur tous les marchés du numérique de manière verticale afin de commercialiser autant les supports que les contenus diffusés. Les BATX visent également l'excellence technologique, avec pour horizon de s'emparer du leadership mondial.

La victoire du programme d'intelligence artificielle AlphaGo, développé par Google, contre le champion du monde coréen Lee Sedol en 2016, a créé un électrochoc en Chine[135] et fait figure d'un match entre les technologies occidentales et la culture chinoise.

La prise de conscience du potentiel de l'IA a amené le gouvernement chinois à en faire une priorité nationale. L'année suivante, Pékin publie son « Plan de développement de la prochaine génération d'intelligence artificielle »[136].

Étalé sur trois ans, il doit permettre à la Chine de devenir le leader technologique mondial en 2025, en particulier grâce à la construction d'un parc technologique dédié à l'IA. Les géants du numérique sont ici aux avant-postes. Jack Ma, le dirigeant d'Alibaba, annonce dans la foulée un investissement de 13 milliards de dollars dans l'IA. Baidu, quant à lui, a inauguré un institut du deep learning dès 2013 et Tencent travaille sur le secteur dans son centre de la Silicon Valley.

Cette stratégie a rapidement produit des résultats. Aujourd'hui, les avancées de la Chine sur l'IA talonnent, si ce n'est dépassent, celles des géants américains. Par exemple, la reconnaissance d'images de Baidu atteint 95,4 % de précision, contre 95,2 % pour celle de Google[137]. Les BATX poussent même leur avantage en investissant dans le hardware pour l'intelligence artificielle.

---

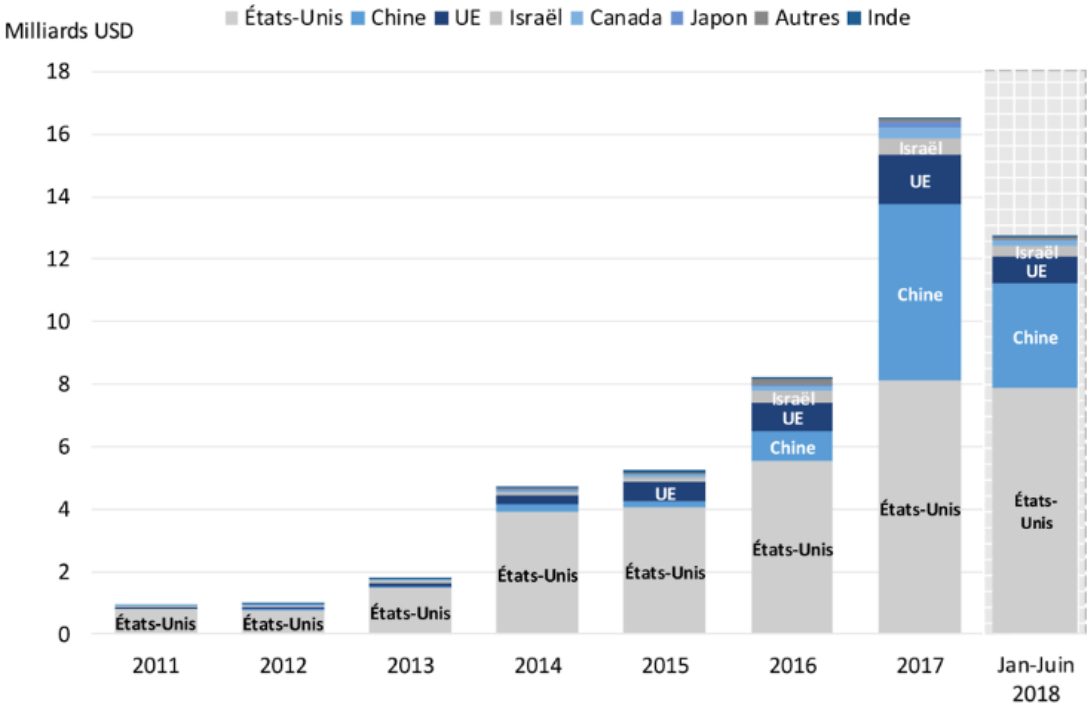
134 G.E *Avatar 2: Made in China ?* The Economist Avatar 2: Made in China? | The Economist

135 Yifu Dong, AlphaGo and the Clash of Civilizations. (18 mars 2016) foreignpolicy.com AlphaGo and the Clash of Civilizations – Foreign Policy

136 Frédéric Schaeffert La Chine prete à tout pour etre le leader mondial de l'IA. (19 février 2020) Lesechos.frLa Chine prête à tout pour être le leader mondial de l'IA | Les Echos

137 Guillame Champeau Google battu par le Chinois Baidu sur la reconnaissance d'images. (15 mai 2015) Numera.fr Google battu par le Chinois Baidu sur la reconnaissance d'images - Numerama

En 2017, Alibaba entre au capital de la start-up chinoise Cambricon, qui développe des puces spécialement conçues pour les applications IA, et qui se pose en rivale de l'américaine Nvidia. En 2018, l'entreprise de Jack Ma investit dans le hongkongais SenseTime, spécialiste de la reconnaissance faciale valorisé plus de 3 milliards de dollars.



Note : Les estimations pour 2018 pourraient être sous-évaluées, certaines données pouvant être manquantes du fait des délais de déclaration (voir Encadré 2.1. Note méthodologique).

Source : Estimations de l'OCDE d'après Crunchbase (juillet 2018), www.crunchbase.com.

Part des investissements dans l'IA entre 2011 et 2018 par région[138]

La Chine réussit également à faire émerger quelques-unes des pépites les plus en vue du secteur. C'est le cas de iFlytek, une start-up basée à Hefei, devenue un des leaders mondiaux de la reconnaissance vocale. Elle se targue d'être capable d'isoler et retranscrire une voix parmi vingt autres lors d'une conversation. Le succès est tel que la Chine devient un partenaire essentiel pour les pépites occidentales. Dans la médecine connectée par exemple, des pépites anglaises font désormais appel à Tencent pour intégrer de l'IA à leurs dispositifs médicaux. Et les Gafam multiplient les investissements en Chine. Depuis 2017, Microsoft et Amazon ont annoncé ouvrir des centres de recherche en IA à Shanghai.

[138] Estimation de l'OCDE. Venture Capital Investments in artificial intelligence analysing in VC in A.I companies from 2012 through 2021. (septembre 2021) Venture Capital Investments in Artificial Intelligence (oecd-ilibrary.org)

Dans la compétition mondiale autour de l'IA, les géants chinois bénéficient d'un atout majeur, l'accès quasi illimité aux données des utilisateurs. Grâce au modèle économique construit autour des écosystèmes des géants, ces acteurs ont accès à toutes les données de leurs clients et peuvent les croiser. Par exemple, Tencent a développé Webank (première banque en ligne privée du pays), lui permettant de croiser les données bancaires avec celles de son application Wechat.
Au même titre que les grands GAFAM qui ont profité d'un soutien politique et financier depuis leurs débuts de la part de Washington, les BATX doivent beaucoup au régime communiste de Beijing.

C'est grâce aux investissements publics dans les infrastructures numériques lancés dès les années 1990 que ces géants ont pu prendre leur essor. Au début des années 2000, l'informatique devient une des priorités des Plans quinquennaux. Et l'État n'hésite pas à évincer les acteurs occidentaux du marché chinois, à l'image de Google, Yahoo ou encore Facebook, pour protéger ses ouailles. Mais ces acteurs jouissent encore d'une relative indépendance politique. Le ton change radicalement lorsque l'informatique devient un enjeu de compétitivité internationale.
Dès son arrivée à la tête de l'État chinois en 2012, Xi Jinping délaisse la stratégie du profil bas sur la scène internationale et assume les ambitions mondiales de son pays. Son objectif, le hisser au rang de première puissance mondiale. Pour y arriver, la Chine a besoin du leadership technologique. Pékin lance ainsi Made in China 2025, un vaste plan de montée en gamme de son industrie. Les robots, les réseaux mobiles ou encore les technologies de big data deviennent alors des priorités stratégiques. À partir de 2016 et le choc AlphaGo, l'intelligence artificielle s'impose pour Pékin comme le mètre étalon de sa puissance internationale.

La compétition mondiale qui s'est accélérée ces dernières années autour de l'IA s'explique par le rôle central que cette technologie va tenir dans nombre de secteurs d'avenir. C'est le cas de la voiture autonome. Le moteur de recherche Baidu s'est d'ailleurs associé aux constructeurs chinois JAC, BAIC et Chery pour lancer ses propres modèles cette année. Plus stratégique encore, l'IA sera une arme militaire déterminante sur les champs de bataille de

demain. Le *South China Morning Post*[139], qui appartient depuis 2015 à Alibaba, a récemment dévoilé que les technologies d'intelligence artificielle avaient été intégrées dans les sous-marins nucléaires chinois.

On le voit, depuis 2010, l'IA rassemble les acteurs de l'économie, le pouvoir politique et même l'armée populaire de libération. Identifiée comme levier de croissance à l'horizon 2030, l'IA chinoise repose sur 4 priorités[140]:

- Créer un écosystème de données riches,
- encourager l'adoption de l'IA dans le maximum de secteur pour multiplier les données exploitables.
- Développer les ressources humaines et les compétences en IA,
- développer un système éducatif répondant aux nouveaux enjeux du XXIe siècle.

Dans ce sens, en 2017, la Chine dévoile son plan de développement de l'IA reposant sur une collaboration étroite entre l'État, l'APL et les géants du numérique chinois. En plus des initiatives du régime, de nombreuses régions et villes investissent dans l'IA (par exemple, Shenzhen propose une subvention d'un million de dollars à tout projet relatif à l'IA qui s'implante dans la région). Ainsi, en 2018, les régions disposent de 445 milliards de dollars à injecter dans l'IA à l'échelon régional.

Concrètement, et s'inscrivant dans le plan *Ambition 2030*, c'est à cette période que Baidu créé son Institut de Deep learning à Beijing, son Laboratoire d'innovation pour les véhicules autonomes et son Laboratoire national d'ingénierie des systèmes et logiciels Big Data, en collaboration avec la très prestigieuse université Tsinghua. D'autres projets en IA sont dans le même temps confiés à d'autres géants, comme Tencent, qui doit développer l'imagerie médicale, Alibaba qui réfléchit sur les smart cities et iFlytek qui doit travailler sur la reconnaissance vocale.

C'est donc par une coopération public- privée que doit se comprendre l'émergence de l'IA (et du numérique au sens large) en Chine. Alors que les entreprises américaines sont encore à l'origine de la plupart des recherches dans le secteur, la Chine a aujourd'hui toutes les cartes en mains pour devenir leader dans ce secteur déterminant la puissance future d'une nation.

---

[139] Stephen Cheng *China's plan to use artificial intelligence to boost the thinking skills of nuclear submarine commanders.* (février 2018). Southchinamorning*post.com* China's plan to use artificial intelligence to boost the thinking skills of nuclear submarine commanders | South China Morning Post (scmp.com)

[140]Sophie-Charlotte Fischer *Intelligence artificielle: Les ambitions de la Chine.* (Février 2018) Center for Security Studies (CSS) de l'ETH Zurich CSSAnalyse220-FR.pdf (ethz.ch)

b) Huawei comme instrument d'une stratégie de conquête et d'influence.

Si le régime chinois a su porter ses grands géants du numérique en créant des monopoles en interne, la plus grande réussite du régime reste l'entreprise Huawei, vu par les dirigeants du parti comme un véritable instrument de domination, sortant largement du cadre commerciale.

Huawei Technologies est le leader mondial de l'électronique grand public et des équipements télécoms. Accordant une grande importance à l'innovation, le groupe réinvestit 12% de son chiffre d'affaires dans la R&D (pour 5% chez Apple et 6% chez Google). En 2017, Apple, Samsung et Huawei se partagent plus de 50% des ventes de smartphones à travers le monde. Au sein de Huawei, 62 000 chercheurs sont employés uniquement au sein des 23 centres de R&D du groupe en Chine (plus 5 aux États-Unis).

Fin 2017, le groupe avait déposé 64 000 brevets sur le territoire national et 48 000 en dehors de son territoire.

Sous l'angle sensible des câbles optiques, Huawei est le 5e fournisseur de câbles sous-marins, après les États-Unis, la France, la Finlande, le Japon et le Royaume Unis, faisant de la firme à la fleur le premier fournisseur de câble sous-marins privé.

Et c'est bien ce qui inquiète les occidentaux à partir de 2018. Alors que les réseaux de 5G commencent à être déployés à travers le monde, Huawei est pris en otage dans la guerre économique et technologique que se livrent chinois et américains. Ainsi, alors que le groupe profitait de son avance technologique dans la 5G (notamment face aux concurrents américains que sont Cisco ou Juniper Networks) pour pouvoir proposer aux pays de l'UE ses services à un coût très compétitif, l'internationalisation du groupe connaît un coup de frein suite au début de la guerre commerciale en 2018, qui se voit écarté de tous les appels d'offres des réseaux 5G en Europe.

B) La puissance cyber à l'international, quand les intérêts diplomatiques dictent une politique économique

La Chine s'efforce de devenir un leader dans l'établissement de normes internationales, et la route de la soie numérique, qui fait partie de l'initiative "Belt and Road" de la Chine visant à étendre son infrastructure et ses marchés mondiaux, est essentielle pour

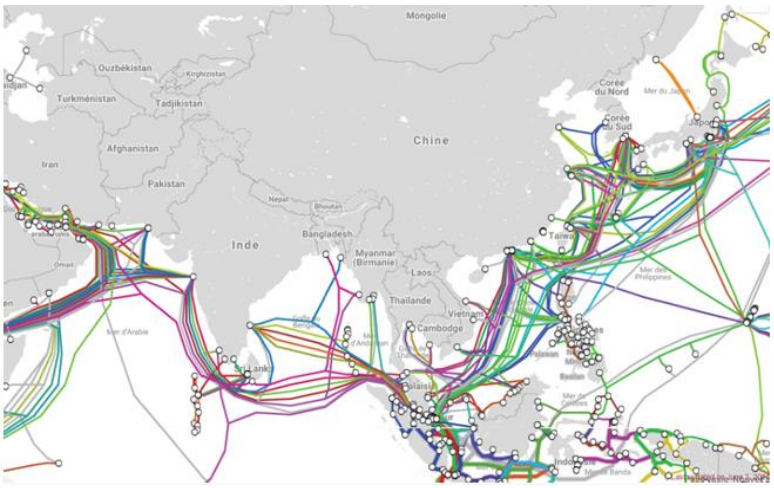
atteindre cet objectif. Toutefois, la Chine doit faire face à une forte concurrence pour gagner en influence au sein des organismes internationaux de normalisation, qui sont dominés par l'Union européenne et les États-Unis.

Répondant à des impératifs de continuité dans la chaîne d'approvisionnement du pays, les nouvelles routes de la soie ont un volet politique affirmé et visent à étendre le modèle de socialisme de marché à travers le monde.
Si les infrastructures occupent le principal poste de dépense, notamment à travers l'Asie centrale, les routes de la soie ne peuvent se concevoir sans étudier leurs volets digitaux et numériques. Certes, la BRI s'est progressivement étendue à des secteurs technologiques comme le 5G, l'internet des objets, l'IA, le big data et les villes intelligentes.
Si officiellement les nouvelles routes de la soie sont lancées à partir de 2015, la route de la soie numérique est lancée en 2017, devenant un élément central au sein de la BRI.

1) La nouvelle route de la soie numérique.

La DSR (Digital silk Road) vise à améliorer la connectivité numérique dans les pays participants, la Chine étant le principal moteur du processus. Au niveau macro, le DSR concerne le développement et l'interopérabilité des infrastructures numériques essentielles, telles que les câbles de données terrestres et sous-marins, les réseaux cellulaires 5G, les centres de stockage de données et les systèmes mondiaux de navigation par satellite (la Chine a achevé le lancement de son système mondial de satellites, BeiDou, qui, dans certaines régions, est plus précis que le gps américain ou le Galileo européen).

Carte des câbles optiques sous-marins s'inscrivant dans la DRI.[141]



En Asie, le Pakistan, le Laos, Brunei et la Thaïlande figurent parmi les pays qui ont adopté BeiDou, et l'utilisation de ce système se développe en Asie occidentale (Moyen-Orient) et en Afrique. Au niveau local, la DSR favorise la connectivité entre les entreprises et les consommateurs locaux et entre les entreprises et les consommateurs. Il s'agit par exemple de plateformes et d'applications de commerce électronique, de services de taxi, de fintech (technologie financière) et d'edtech (technologie de l'éducation), ainsi que de matériel comme des routeurs, des smartphones et des PC.

Les investissements des entreprises chinoises à l'étranger ont couvert de nombreux secteurs de l'économie numérique, comme la 5G et l'IoT (internet des objets, la domotique), la reconnaissance faciale ou la surveillance.
On peut le voir dans les secteurs favorisés, la DSR est plus qu'un simple projet d'infrastructure et est vue comme une proposition d'un ordre numérique chinois moins centré sur les États-Unis.

La DSR s'inscrit alors parfaitement dans les objectifs nationaux ambitieux des autorités chinoises, tels que "Made in China 2025" et "China Standards 2035". Ces initiatives visent à renforcer les capacités nationales de la Chine en matière d'innovation technologique, de production et de transactions. À leur tour, ces objectifs s'inscrivent dans une vision globale du

[141] Carte consultable sur le site de l'observatoire Français des Nouvelles routes de la soie. Route de la soie numérique - Géostratégie des câbles sous-marins - Observatoire Français des Nouvelles Routes de la Soie (observatoirenrs.com)

gouvernement chinois visant à assurer la primauté de la technologie et une plus grande autonomie dans l'ordre numérique mondial.

Derrière de simples câbles sous-marins se cachent des préoccupations géopolitiques pour les États, qui perçoivent de plus en plus l'espace numérique, et ses infrastructures physiques, comme un nouveau lieu d'affrontement, de concurrences et de menaces entre États. En quelques années, le système de câbles sous-marins s'est donc considérablement complexifié, sans que soit pensée une gouvernance mondiale sur cette question.

Le gouvernement chinois cherche à réduire la dépendance vulnérable du pays à l'égard des autres leaders technologiques, en particulier les États-Unis, le Japon et certains États européens. La DSR aide les géants chinois de la technologie et les plus petits acteurs à stimuler leurs ventes et leur savoir-faire local et à prendre pied sur les marchés étrangers - souvent avec l'aide de la politique du gouvernement chinois.
L'objectif visé étant de mettre fin à la situation de quasi-monopole des géants américain dans ce secteur stratégique.

En effet, un petit nombre d'acteurs dirige le monde de la technologie, et les géants américains de la technologie Alphabet (Google), Intel, Amazon, Cisco et Facebook en particulier ont un monopole quasi mondial dans leurs domaines respectifs. Par exemple, à la fin de 2018, les fournisseurs de contenu tels que Microsoft, Facebook et Amazon possédaient ou louaient plus de la moitié de la bande passante des câbles sous-marins.
Ces câbles transportent près de 98 % du trafic international de données internet et de téléphonie. Une telle domination n'est pas saine et plusieurs acteurs, dont l'UE et l'Australie, ont pris des mesures pour freiner l'emprise de ces géants de la technologie.

La DSR se concentre souvent sur les participants à la BRI[142] et les économies en développement, mais sa portée ne se limite pas à ces acteurs. Parmi les principaux bénéficiaires des investissements du DSR figurent même de grandes économies européennes comme l'Allemagne et l'Italie[143]. En Europe, les projets se concentrent sur les réseaux 5G, la fintech et les technologies des villes intelligentes. Grâce à des accords de partenariat public-privé chinois compétitifs, la DSR catalyse un monde plus numérisé, de la Serbie au Mexique

[142] Acronyme de la Belt and Road Initiative
[143] Richard Ghuasy et Rajeshwari Krishnamurthy *China's Digital Silk Road and the global Digital Order.* (février 2021) Thediplomat.com China's Digital Silk Road and the Global Digital Order – The Diplomat

en passant par le Myanmar. Un monde plus numérisé n'est pas exclusivement bénéfique à la Chine et aux entreprises chinoises. En effet, la numérisation du DSR, si elle s'accompagnait d'une croissance économique, pourrait offrir une multitude d'opportunités d'investissement et de vente pour les entreprises technologiques et non technologiques non chinoises.

Ici, la DSR a deux implications stratégiques importantes et de grande portée. Tout d'abord, la Chine peut construire et offrir des solutions numériques qui sont presque entièrement fabriquées sur place.
Deuxièmement, la DSR peut aider la Chine à définir des normes pour l'infrastructure numérique et les technologies de nouvelle génération telles que l'intelligence artificielle, la robotique, l'internet des objets, la blockchain, l'informatique sans serveur, etc.

Le gouvernement chinois applique des restrictions strictes au cyberespace en Chine. Il n'hésite pas non plus à surveiller de près ses net-citoyens dans un "intranet" national considérablement fermé.
Certes, la Chine n'est certainement pas le seul pays à avoir une vision restrictive de la gouvernance numérique, et différents pays appliquent différents types et niveaux de restrictions sur le cyberespace. Des pays comme Singapour et l'Inde ont tendance à appliquer des contrôles sur le contenu également, et l'UE, par exemple, réglemente de plus en plus le contenu.
La DSR sert clairement un objectif plus large de réduction de la fracture numérique mondiale. Il remet par ailleurs en question la domination actuelle du système de valeurs numériques des États-Unis et la part de marché dominante de ses entreprises technologiques. Ainsi, la DSR représente à la fois des partenaires sérieux dans la transformation numérique pour les pays qui ont besoin de produits et de services numériques à des prix compétitifs, et une concurrence pour les leaders technologiques existants.

2) Les autres succès chinois dans le numérique

Dans le numérique comme dans le reste de l’économie, la Chine réaffirme et n’ambitionne rien de moins que la première place.

Même si le rattrapage avec les Etats-Unis est encore loin dans certains secteurs comme dans la défense, la Chine connaît des succès dans différentes industries de pointe identifiées comme déterminantes pour la seconde moitié du XXIème siècle.

Portés par des grandes entreprises au rayonnement globale et par un soutien politique au niveau du PCC, l'informatique quantique et les technologies de surveillance sont deux secteurs déterminants pour le futur où la Chine fait la course en tête.

Avec la fin de la loi Moore (postulant que la puissance de calcul de nos ordinateurs double tous les 18 mois) qui pourrait arriver dès 2030, l'informatique quantique pourrait se révéler être une technologie de rupture, proposant en théorie de changer de paradigme et de multiplier presque à l'infini nos puissances de calcul informatiques, permettant l'optimisation de processus industriels dans de nombreux domaines et posant de nombreuses questions en matière de sécurité informatique et de souveraineté nationale.
Appelé à révolutionner l'informatique d'ici à 20 ans, les applications de la physique quantique dans l'informatique restent cependant encore à leurs balbutiements, mais font l'objet d'investissements massifs à travers le monde, révélant leurs natures stratégiques. Chinois principalement vers Huawei et Tencent, américains à travers les entreprises de la Silicon Valley, et même européens, notamment via des instituts de recherche (comme l'institut Fraunhofer en Allemagne, qui propose le premier ordinateur quantique sur le sol européen ou le CEA en France avec son ordinateur quantique EXA1,développé en collaboration avec Atos) ou de grands groupes (Atos, Thales) ou des start-up (Pasqal,C12 Quantum...).
En annonçant en 2019 avoir atteint "la suprématie quantique"[144], Google propose un prototype
d'ordinateur quantique permettant de résoudre en 3 minutes un calcul là où il aurait fallu 10 000 ans à un ordinateur classique. De même, l'université des sciences et technologies de Chine annonce en 2020 que son ordinateur quantique a été capable d'accomplir en 200 secondes une tâche là où il aurait fallu 200 millions d'années à un superordinateur classique.

Bien qu'encore au stade de la R&D, l'informatique quantique pourrait ainsi révolutionner de nombreux domaines largement au-delà de l'informatique, comme la recherche, la simulation climatique, les communications, la cryptographie, l'agriculture, l'optimisation énergétique et

[144]Anthony Cobinne, Pourquoi Google annonce avoir atteint la suprématie quantique ? (Juin 2019) Forbes.fr Pourquoi Google Annonce Avoir Atteint La Suprématie Quantique - Forbes France

industrielle et le trafic automobile. Dans la santé par exemple, des vaccins pourraient voir le jour en quelques semaines grâce à la puissance de simulation du quantique là où il faut des années aujourd'hui. Avec les voitures connectées, les déplacements seront optimisés afin d'éviter les embouteillages. Mais de manière plus sensible, l'algorithme quantique de Shore pourrait casser en quelques minutes toutes les communications chiffrées, exposant le secret défense, les données bancaires ou encore les portefeuilles de cryptomonnaie.

Globalement, une étude de Boston Consulting Group montre que l'informatique quantique pourrait accroître de 450 à 850 milliards de dollars par an, les bénéfices d'exploitation de ses utilisateurs d'ici à 2050[145].

Comprenant l'importance stratégique de ce domaine, c'est la Chine qui fait la course en tête en termes d'investissement avec 10 milliards, principalement vers Huawei, suivit de près par les leaders de la tech américaine comme Google, IBM, Intel ou Microsoft. Mais là où l'UE a abandonné toutes ses ambitions souveraines en matière de cloud et d'applications internet, elle ambitionne dans l'informatique quantique rien d'autre que la première place.

Certes, l'UE va investir 8 milliards d'euros d'ici 2027 (dont 2,6 milliards venant d'Allemagne et 1, 8 milliards de France, avec le Plan Quantique annoncé en janvier 2021 par le Président E.Macron), l'équivalent de l'enveloppe américaine et à peine moins que la chinoise (dont les chiffres sont sujets à caution) pour développer ses forces, notamment à travers des grands groupes comme Atos ou Thales, mais aussi grâce à des start-up à la pointe de la recherche comme Pasqal, Quandela ou encore C12 Quantum Electronics. L'idée de ces investissements étant d'acquérir les compétences et la maîtrise de cette technologie pour dominer le marché le jour où l'ordinateur quantique BtoB sera prêt.

Ainsi, derrière la maîtrise de ce marché encore en développement découle des enjeux de compétitivité économique et de souveraineté nationale allant bien au-delà du secteur informatique et qui permettra à la nation leader d'avoir un avantage décisif pour la seconde moitié du XXIe siècle.

Au côté de l'informatique quantique, on peut trouver les technologies de surveillance du régime chinois.

Plus qu'un succès commercial, l'analyse de ce secteur permet de mieux comprendre les sous-entendus de cette politique d'internationalisation des géants du numérique chinois. Après

[145]Selon une étude de Boston Consulting Group par Jean François Bobier, Matt Langione, Edward Tao et Antoine Gourévitch *The Path to building quantum advantage.* (21 juillet 2021) bcg.com The Path to Building Quantum Advantage | BCG

avoir connu une croissance rapide dans leur pays, les géants chinois de la surveillance visent à dominer les marchés mondiaux. Ensemble, Hikvision (caméras affichées ci-dessus) et Dahua fournissent près de 40 % des caméras de surveillance dans le monde. Seule la Chine dispose d'entreprises compétitives à chaque étape du processus de surveillance, de la fabrication des caméras à la formation de l'IA en passant par le déploiement des analyses.

La technologie de surveillance chinoise est utilisée dans plus de quatre-vingts pays, sur tous les continents à l'exception de l'Australie et de l'Antarctique. Sous Xi Jinping, la Chine a mis en place un État de surveillance d'une ampleur et d'une ambition immenses, axé sur la prévention et le contrôle des risques pour la stabilité sociale et le pouvoir du PCC, la technologie étant l'outil clé pour atteindre les objectifs de prévention du régime.
Au cours de la dernière décennie, les technologies chinoises de surveillance et de maintien de l'ordre chinoises se sont également "mondialisées" et sont désormais utilisées dans plus de 80 pays dans le monde.

Carte du monde montrant les pays ayant adoptés des solutions de surveillance chinoise pour la sécurité publique en 2019[146]

Le développement des technologies de surveillance et de maintien de l'ordre de la Chine a déjà eu des conséquences mondiales. En effet, la Chine a exporté des plates-formes de surveillance destinées à être utilisées pour le maintien de l'ordre et le contrôle interne.

Ici, on peut s'interroger sur la dynamique de cette expansion commerciale, qui vise non plus à développer l'offre chinoise à travers le monde, mais bien à défendre un système politique ne respectant pas les libertés individuelles définis par l'occident et défendant des régimes

[146]Sheena Chestnut Greitens *China surveillance state at home and abroad.* (Janvier 2020) Université du Texas à Austin Sheena-Greitens_Chinas-Surveillance-State-at-Home-Abroad_Final.pdf (cpb-us-w2.wpmucdn.com)

politiques autocratiques. Ici comme dans d'autres secteurs de la tech chinoise, les succès économiques et commerciaux de l'empire du milieu doivent se comprendre au regard d'une politique plus large visant à répandre à travers le monde son régime politique au détriment des démocraties libérales.

C) La guerre commerciale et technologique Etats-Unis/Chine.

1) Une guerre transpartisane aux États-Unis préfigurant un mur de fer numérique entre deux mondes.

S'il y a bien un domaine où l'administration démocrate de Joe Biden poursuit la politique initiée par Donald Trump, c'est bien dans la guerre commerciale et technologique engagée contre la Chine par les États-Unis et ses alliés proches.
Alors que la guerre en Ukraine occupe l'actualité et fait croire à une nouvelle guerre froide entre l'Otan (qui dépense plus de 1000 milliards dans ses forces armées) et la Russie (avec des dépenses militaires s'élevant en 2020 à 64 milliards de dollars), le véritable conflit pour le leadership mondial se déroule dans le Pacifique et remplace tank et missiles par des contrôles d'exportation et des tentatives d'isolement diplomatique et commerciales.

Le président Joe Biden a inversé un certain nombre de politiques de l'administration Trump au cours de sa première année de mandat, mais il a laissé en place des tarifs douaniers sur 350 milliards de dollars de marchandises chinoises qui avaient été imposés par l'administration de son prédécesseur.

Certains de ces tarifs, qui sont payés par les importateurs américains, sont en place depuis près de quatre ans. La guerre commerciale de l'ancien président Donald Trump avec la Chine a commencé en 2018 lorsqu'il a imposé des droits de douane sur 50 milliards de dollars de produits fabriqués en Chine. Au cours de l'année suivante, il a ajouté des droits de douane sur davantage d'articles après que Pékin ait riposté en ordonnant des droits de douane sur certains produits fabriqués aux États-Unis.

Après des mois d'escalade, Trump et le président chinois Xi Jinping ont conclu une trêve au début de 2020, en signant ce que l'on appelle l'accord de phase 1[147]. La Chine a accepté d'augmenter ses achats de biens et de produits agricoles américains, se fixant l'objectif ambitieux d'acheter 200 milliards de dollars de plus qu'avant le début de la guerre commerciale.

Les États-Unis ont cherché à contenir l'ascension de la Chine en tant que puissance technologique, en interdisant le réseau 5G de Huawei[148] aux États-Unis et en interdisant aux entreprises américaines de fournir des logiciels et des composants aux entreprises technologiques chinoises.

L'année dernière, l'administration Trump a également décidé d'interdire TikTok aux États-Unis, craignant que l'application ne vole les données personnelles des utilisateurs pour le compte du régime communiste de Pékin. Dans un article du New York Times[149], Apjit Walia, responsable mondial de la stratégie technologique de la Deutsche Bank parle d'un nouveau rideau de fer numérique entre la Chine et l'Occident. Mais les analystes préviennent que ces escarmouches ne font qu'aggraver le "rideau de fer numérique" qui se dresse entre la Chine et l'Occident. Selon lui, le monde est en train de se diviser en deux écosystèmes technologiques concurrents et mutuellement exclusifs, chacun disposant de ses propres plateformes Internet, matérielles, financières et de communication.

Qu'il s'agisse de la façon dont vous calculez par ordinateur, de la façon dont vous communiquez avec les téléphones portables et de tout ce qui tourne autour de l'électronique, vous commencez à avoir deux normes qui s'opposent. En 2019, Mark Zuckerberg, le patron de Facebook, est revenu au sein de l'université de Georgetown sur le doublement d'internet, où la Chine développe un monde en ligne très différent de celui de l'internet occidental, où l'empire du milieu véhicule ses propres valeurs grâce à ses propres plateformes numériques sous contrôle du régime. "La Chine est en train de construire son propre internet axé sur des valeurs différentes, et exporte désormais sa vision de l'internet dans d'autres pays", a ainsi déclaré Mark Zuckerberg[150].

---

[147] Anne Corpet *La Chine et les Etats-Unis signent la phase 1 de leur accord commercial.* (15 Janvier 2020) RFI.fr La Chine et les États-Unis signent la phase 1 de leur accord commercial (rfi.fr)

[148]Samina Hassan *Why did Huawei get banned by the US ?* (24 mai 2019) the planetoday.com Why did Huawei get banned by the US? - Complete details

[149]Interview de Apjit Walia par Shira Ovide *A capitalist fix to the digital divide.* (22 septembre 2020) nytimes.com A Capitalist Fix to the Digital Divide - The New York Times (nytimes.com)

[150]Ryan Brown *Mark Zuckerberg warns about China's "dangerous" approach to internet.* (18 mars 2020) cnbc.com Mark Zuckerberg warns about China's 'dangerous' approach to internet (cnbc.com)

La plateforme de médias sociaux chinoise WeChat, le marché en ligne Alibaba et le moteur de recherche Baidu ont créé un cyberespace distinct de celui dominé par les titans technologiques américains tels que Facebook, Amazon et Google. Ainsi, pour des raisons de stabilité intérieure et de souveraineté numérique, l'internet chinoise se sépare progressivement du reste du réseaux. Des plateformes comme Facebook et Google ont été interdites, le gouvernement communiste créant un "marché protégé" pour les entreprises technologiques chinoises qui se soumettraient plus volontiers aux exigences politiques de Pékin.

La construction par la Chine de son propre écosystème technologique n'a fait que se poursuivre, s'étendant au-delà des plateformes internet aux systèmes d'exploitation, aux architectures de processeurs, aux réseaux de communication par satellite et aux systèmes de paiement, avec une faible interopérabilité avec les équivalents occidentaux.

Les sanctions de l'administration Trump ont peut-être nuit aux activités de Huawei dans le domaine des smartphones en empêchant le fabricant de téléphones chinois d'accéder au système d'exploitation (OS) mobile Android de Google, mais elles ont aussi obligé Huawei à se concentrer sur le développement de son propre OS Harmony et à sortir les microprocesseurs américains du processus de fabrication des téléphones Huawei.

Ainsi, la fracture numérique croissante pourrait bientôt pousser les entreprises et même les nations à choisir un système - ou à supporter le coût d'être à cheval sur deux régimes technologiques.

2) Contrôle des exportations du côté américain puis chinois

L'Export *Administration Regulation* (EAR) sont les règles par lesquelles le Bureau de l'industrie et de la sécurité (BIS) du ministère américain du Commerce réglemente et contrôle les exportations de marchandises en provenance des États-Unis. Si le domaine militaire est couvert par l'USML[151], l'EAR est l'outil qu'utilisent les États-Unis contre la Chine pour empêcher les exportations dans des secteurs sensibles, et plus particulièrement dans le domaine des nouvelles technologies. Ici, le département de justice américain a dressé une

[151]La United States Munitions List (USML) est une liste d'articles, de services et de technologies connexes désignés comme étant liés à la défense et à l'espace par le gouvernement fédéral des États-Unis. De ce fait, ces articles ne sont pas exportables à l'international par les entreprises américaines. Ici, la liste : United States Munitions List - Wikipedia

liste d'entreprises chinoises ayant des liens trop étroits avec le gouvernement chinois et avec qui le commerce est interdit pour les Américains.
Consultable en ligne, la liste des entreprises chinoises soumissent à l'EAR cible particulièrement les entreprises du numérique[152].

Concrètement, le texte empêche les investissements américains de soutenir le complexe militaro-industriel chinois, ainsi que les programmes de recherche et de développement dans les domaines de l'armée, du renseignement et de la sécurité, et c'est en utilisant ce texte que Google a sorti Android des téléphones Huawei (donnant un accélérateur au développement d'Harmony OS, le système d'exploitation de Huawei).

3) Des sanctions américaines poussant la Chine vers une plus grande résilience.

Comme on a pu le voir, la guerre technologique engagée par Donald Trump et poursuivie par Joe Biden visait à déstabiliser les géants du numérique chinois et leurs politiques d'internationalisation pour freiner la diffusion du modèle d'internet chinois.
Bien qu'efficace à court terme si on regarde le chiffre d'affaires de Huawei qui s'est effondré[153] et le bannissement de la société chinoise dans les réseaux 5G d'Europe occidentale[154] (au profit de constructeurs américains, comme Ericsson[155]), on peut s'interroger sur les résultats à long terme de cette politique, particulièrement au regard de l'autonomisation croissante du numérique chinois vis-à-vis des États-Unis.
Si le développement d'Harmony OS pour remplacer Android sur les téléphones de Huawei a été très médiatisé dans le courant de 2020, un décret chinois passé relativement inaperçu en 2019 (et réédité après le Covid en 2022) est une révolution dans le secteur et constitue une preuve de plus que le monde du numérique se double, avec d'un côté les géants et normes occidentales (surtout américains) et de l'autre le monde numérique chinois qui s'émancipe toujours plus du monopole américain.

---

[152] Ainsi le 4 juin 2021, l'administration de Joe Biden publie une liste de 59 entreprises chinoises du monde de la tech qui seront sous le contrôle de l'EAR.Reuters.com : Biden bans investment in 59 Chinese defense and tech firms - Nikkei Asia (4 juin 2021)

[153] Evelyne Cheng, Huawei expects 2021 revenue to drop by 28,9 % as sanctions drag on. (30 decembre 2021) cnbc.com Huawei expects 2021 revenue to drop by 28.9% as sanctions drag on (cnbc.com)

[154] France 24 EU issues strict 5G rules, stops short at Huawei ban (29 janvier 2020) france24.com EU issues strict 5G rules, stops short at Huawei ban (france24.com)

[155] Nicolas Rolander Ericsson Reports Profit, Market Share gains after Huawei Ban (21 octobre 2020) Bloomberg.com Ericsson Reports Profit, Market Share Gains After Huawei Ban - Bloomberg

Ainsi, en mai 2022[156] la Chine a ordonné aux agences du gouvernement central et aux sociétés soutenues par l'État de remplacer les ordinateurs personnels de marque étrangère par des alternatives nationales dans un délai de deux ans, marquant ainsi l'un des efforts les plus agressifs déployés jusqu'à présent par Pékin pour éradiquer les technologies étrangères clés au sein de ses organes les plus sensibles (pour rappel, cette décision date de 2019[157] , mais a connu un coup d'arrêt avec le covid.
L'objectif ici étant de remplacer pas moins de 70 millions de PC sous Windows au niveau local et central et ainsi de remplacer les technologies importées par des solutions locales pour réduire la dépendance de la Chine à l'égard des constructeurs américains.

Ici encore, on peut souligner la volonté du régime chinois de se déconnecter du réseau informatique américain et de gagner toujours plus en autonomie et en souveraineté numérique alors que les révélations de Snowden ont mis en évidence l'espionnage systématique des grandes entreprises étrangères par la NSA utilisant un service numérique américain (ou utilisant le dollar pour leurs transactions internationales)

L'écosystème numérique chinois s'efforce donc de gagner en souveraineté depuis plus d'une décennie. Tendant à couvrir tous les secteurs du numérique, de la téléphonie mobile à la connectivité par satellite, il connaît néanmoins des limites, particulièrement au regard de la géopolitique de la région.

Dans un rapport du faible au fort où le faible identifie un élément clé dans la chaîne de valeur du numérique, la République de Chine, ou Taïwan à trouver dans les semi-conducteurs un levier de puissance que la RPC n'arrive toujours pas à maîtriser malgré de lourds investissements.
Alors que les semi-conducteurs sont indispensables dans tous les systèmes informatiques du monde, le secteur est dans une situation d'offre limitée pour une demande toujours croissante. En dominant la fabrication des semi-conducteurs les plus avancés, le géant Taiwan Semiconductor Manufacturing Company Ltd (TSMC) s'est emparé d'une technologie cruciale pour les appareils et les armes numériques de pointe d'aujourd'hui et de demain. Ainsi, TSMC

[156] Équipe de rédaction de Bloomerg.com, avec l'aide de Yanping Li et Yuan Gao China orders government, state firms to replace foreign computers. (6 mai 2022). Bloomerg.com China Orders Government, State Firms to Replace Foreign Computers - Bloomberg
[157] Arjun Kharpal *China reportedly orders state offices to remove foreign tech* (9 decembre 2019) cnbc.com China reportedly orders state offices to remove foreign tech (cnbc.com)

représente plus de 90 % de la production mondiale de ces puces, se rendant indispensable non seulement pour la Chine, mais aussi pour les États-Unis.
Alors que le processus de fabrication d'un semi-conducteur n'est maîtrisé que par une poignée d'entreprises à travers le monde, Américains comme Chinois tentent de résoudre cette rupture dans la chaîne de valeur du numérique.
Washington a persuadé TSMC d'ouvrir une usine en Arizona nécessitant 12 milliards de dollars d'investissement qui fabriquera des semi-conducteurs de pointe et s'apprête à dépenser des milliards pour reconstruire son industrie nationale des puces[158].

Pékin dépense également beaucoup, mais son industrie des puces accuse un retard d'une dizaine d'années sur celle de Taïwan dans de nombreux domaines clés. Pour pallier ce retard technique, la Chine n'hésite plus à tenter de débaucher les ingénieurs taïwanais, mais sans beaucoup de succès jusqu'à présent[159].

Cette dépendance des deux superpuissances vis-à-vis de Taiwan doit se lire à travers la grille de lecture de la région, qui fait de l'île pour le régime chinois un territoire séparatiste, promis à être reconquis par tous les moyens, et un territoire stratégique à défendre pour maintenir la crédibilité américaine.
Certes, alors que le statu quo reste l'unique solution raisonnable, les tensions sont croissantes sur la question. On peut penser à la loi du régime chinois qu'y s'autorise à attaquer par la force Taiwan si l'ile demande à être reconnu à l'ONU, ou aux déclarations récentes du président Joe Biden[160], qui promet de défendre l'île militairement (et ne pas renouvellement l'erreur de l'Ukraine)

[158] Reuters.com *TSMC says it has begun construction at its Arizona chip factory site.* (2 juin 2021) reuters.com TSMC says has begun construction at its Arizona chip factory site | Reuters
[159] Durier, P.M. *Intrigue dans le détroit de Formose autour de la loyauté des ingénieurs taïwanais dans le domaine des semi-conducteurs.* (14 avril 2022) Portail-ie.fr Intrigue dans le détroit de Formose autour de la loyauté des ingénieurs taiwanais dans le domaine des semi-conducteurs | Portail de l'IE (portail-ie.fr)
[160] Sam Meredith Biden says U.S willing to use force to defend Taiwan - prompting China backlash. (23 mai 2022) cnbc.com Biden says U.S. willing to use force to defend Taiwan — prompting China backlash (cnbc.com)

II) La Recherche et le Développement digital, moteur stratégique de l'expansion cyber chinois

La recherche et développement exponentiel de la Chine est dû principalement au soutien du gouvernement. Xi Jinping lors d'une intervention dans une usine intelligente annonce : "L*'innovation ne peut pas être tenue par les autres, en particulier quand il s'agit des technologies clés et les technologies de base. Nous ne pouvons compter que sur nos efforts. Sinon nous resterons que des suiveurs*"[161]. L'innovation technologique est au cœur des ambitions chinoises. Elle est un facteur clé pour saisir l'importance de son développement dans le milieu du cyber. Dans cette partie, il s'agira de montrer que les différentes innovations menées par ses entreprises, ses universités et sa population, poussées par les exigences du Parti Communiste Chinois, font partie des piliers de son développement cyber.)

A) La Chine, contrainte de tout miser sur son innovation afin de s'affirmer dans le cyberespace mondial

1) Une main d'œuvre bon marché, moteur de la production digitale chinoise

Il est important de souligner que la Chine n'était pas destinée à avoir un niveau de recherche et développement aussi avancé qu'aujourd'hui. Après la Seconde Guerre mondiale et de son sous-développement, le pays s'est retrouvé avec une très grande main d'œuvre bon marché. Le gouvernement s'est donc tourné vers un développement qui cible la production d'innovations d'autres pays. L'exemple d'Apple est le plus frappant : Sur les 30 pays où ses appareils technologiques ont été fabriqués en 2020, six représentaient plus de 80 % de la production annuelle. La Chine a contribué à hauteur de 42 %, suivie du Japon (16 %), des États-Unis (9 %), de Taïwan (6 %), de la Corée du Sud (5 %) et du Vietnam (4 %).[162] La Chine affirme sa position de leader dans les chaînes d'approvisionnement et de production dans beaucoup d'entreprises technologiques. Cette politique a permis à un pays qui avait raté

[161] CGTN Français, "La Chine resplendissante - Technologie et innovation", *Youtube* *https://www.youtube.com/watch?v=SGK0eTyWKVQ*

[162] GobalData, "Apple diversifie sa chaîne d'approvisionnement mais maintient la Chine au centre", *Verdict*, https://www.verdict.co.uk/apple-supply-chain-china/

la révolution industrielle d'absorber les avancées manufacturières les plus modernes au monde en seulement une décennie ou deux de part :

- l'immense infrastructure industrielle du pays,
- la disponibilité d'une main-d'œuvre nombreuse, abordable et qualifiée ;
- le faible coût de production par rapport à la plupart des autres pays ;
- la capacité des fabricants chinois à automatiser les lignes de production.

À juste titre, la Chine a acquis une réputation de copieur mondial.[163]

2) Une population jeune formée au digital

Depuis 1979, la politique de l'enfant unique est conçu pour réduire un taux de natalité en dessous du niveau de remplacement[164]. Cette politique connaît un succès, seulement, le pays manque aujourd'hui de main d'œuvre pour assurer un bon maintien de sa production. La main d'œuvre baby boomer est en voie de disparition. Selon son bureau national des statistiques[165], la Chine comptera 81 millions de personnes en âge de travailler de moins en 2030 qu'en 2015 ; après 2030, cette population devrait diminuer en moyenne de 7,6 millions par an. Cette diminution du nombre de main d'œuvre et une population vieillissante, la Chine se tourne vers une nouvelle orientation qui mise sur l'innovation.

C'est un pari réussi : en 2015, huit des 10 entreprises qui avaient atteint une valorisation de 1 milliard de dollars dans les plus brefs délais étaient chinoises et six de ces huit ont été fondé en 2014[166]. La Chine, même si elle a un comportement imitateur au niveau des nouvelles technologies, a une redoutable capacité d'adaptation qui en devient une force économique gigantesque au niveau mondial. Cette habileté s'explique par l'implication de la jeune population chinoise dans les nouvelles technologies : une volonté de pénétration et une adoption pour l'univers digital bien plus intéressé.

Pour illustrer cette représentation, l'exemple du paiement mobile est révélateur : cette technologie est arrivée en même temps en Chine et aux États-Unis à partir de 2019. Apple annonce que 383 millions de téléphones dans le monde avaient activé Apple Pay, mais à ce

---

163 Zak Dychtwald, (2021) "China's New Innovation Advantage", *Harvard business review*, https://hbr.org/2021/05/chinas-new-innovation-advantage

164 I.Attané, (2016), "La fin de l'enfant unique en Chine ?", *Cairn*, https://www.cairn.info/revue-population-et-societes-2016-7-page-1.htm

165 (2018) " Répartition de la population en Chine en 2018, par groupe d'âge", *Statista*, https://fr.statista.com/statistiques/666288/repartition-population-par-groupe-d-age-chine/

166 Zak Dychtwald, (2021) "China's New Innovation Advantage", Harvard business review, https://hbr.org/2021/05/chinas-new-innovation-advantage

moment-là, seuls 24 % des propriétaires d'iPhone aux États-Unis avaient déjà utilisé cette technologie. Et ce n'est que cette année-là qu'Apple Pay a dépassé l'application mobile Starbucks, utilisée uniquement dans les magasins Starbucks, en tant qu'application de paiement mobile la plus utilisée aux États-Unis. En Chine, le paiement mobile s'est passé bien différemment : l'application WeChat Pay c'est 84 % de pénétration du marché parmi les utilisateurs de smartphones. (L'application est seulement disponible pour les utilisateurs de WeChat qui compte 1,2 milliard d'utilisateurs actifs par mois.)[167] Ce type de pénétration explique pourquoi en 2018, WeChat Pay a effectué 1,2 milliard de transactions par jour, alors qu'Apple Pay en a effectué un milliard par mois. Mais cela s'explique également par l'accord du gouvernement pour les deux entreprises de créer des licences bancaires : (AliPay pour Alibaba et WeChat Pay pour Tencent). [168]Se soutient à clairement fait décoller ses deux géants du numérique.

En outre, la Chine a su rebondir et surmonter parfaitement son image de simple producteur mondial et imitateur des technologies créée par la forte main-d'œuvre du baby-boom. La jeune population chinoise, grâce à une politique forte, s'est foncièrement adapté au milieu digital dans son quotidien. L'univers cyber n'est pas indifférent, connaissant très bien les enjeux et la complexité de ce domaine. Un atout considérable pour la Chine sur le moyen et long terme dans un monde de plus en plus digitalisé. L'adoption du milieu digital par la population passe par deux domaines : la recherche universitaire et les entreprises. Ces derniers s'avèrent crucial pour le développement technologique et cyber chinois. Quels sont les moyens mis en œuvre ?

[167] Anonyme, (2020). "La Chine, nouvel eldorado de la distribution digitale", ESCP business School, https://escp.eu/fr/news/la-chine-nouvel-eldorado-de-la-distribution-digitale

[168] Zak Dychtwald, (2021) "China's New Innovation Advantage", *Harvard business review*, https://hbr.org/2021/05/chinas-new-innovation-advantage

B) La recherche universitaire : un impact considérable dans le développement cyber chinois

1) Une orientation concentrée sur la recherche et le développement digital

Comme vu précédemment, le gouvernement chinois souhaite digitaliser sa population. Cela se reflète également dans les universités où l'objectif est de développer l'éducation politique et idéologique par des moyens numériques.[169]

Lexis Nexis a publié un classement de 20 universités chinoises les plus innovantes en fonction de leurs brevets. Dans ces universités, 18 ont leurs principaux domaines de recherche dans la nouvelle technologie et le digital (les deux autres sont dans le domaine de la biologie et de l'énergie). 8 couvrent l'informatique numérique et le traitement des données.[170]

	Owner	Top Research Area by Patent Asset Index™
1	Tsinghua University	Electronic communication (H04L 12)
2	Zhejiang University	Microscopic and hyperspectral image technologies (G01N 21)
3	South China University of Technology	Text, object and face recognition (G06K 9)
4	Southeast University	Construction technologies (E04B 1)
5	Harbin Institute of Technology	Digital computing and data processing (G06F 17)
6	Tianjin University	Microscopic and hyperspectral image technologies (G01N 21)
7	Shanghai Jiao Tong University	Digital computing and data processing (G06F 17)
8	Huazhong University of Science & Technology	Digital computing and data processing (G06F 17)
9	Beihang University	Digital computing and data processing (G06F 17)
10	Xi'an Jiaotong University	Digital computing and data processing (G06F 17)
11	Jiangsu University	Technologies for the treatment of water (C02F 1)
12	UESTC	Text, object and face recognition (G06K 9)
13	Beijing University of Technology	Building technologies (E04B 1)
14	Central South University	Electrode technologies (H01M 4)
15	CUMT	Drawing off gas (E21F 7)
16	Shandong University	Digital computing and data processing (G06F 17)
17	Jiangnan University	Cultivation and transformation of micro-organisms (C12R 1)
18	Peking University	Digital computing and data processing (G06F 17)
19	Hohai University	Digital computing and data processing (G06F 17)
20	Xidian University	Text, object and face recognition (G06K 9)

Top research areas of the top 20 most innovative Chinese universities by Patent Asset Index™ as of October 15, 2018.
Source: PatentSight Business Intelligence Platform www.patentsight.com

Cette liste nous apprend que la Chine mène une quête sur les brevets technologiques : en termes d'indice des actifs en matière de brevets, l'Université Tsinghua se classe au premier

[169] Distance Education, (2019) "Digital transformation in higher education: critiquing the five-year development plans (2016-2020) of 75 Chinese universities" Taylor and Francis Online https://www.tandfonline.com/doi/abs/10.1080/01587919.2019.1680272

[170] LexisNexis PatentSight team, (2018), "The Top 20 Most Innovative Chinese Universities", *PatentSight IP Analytics Blog,* https://www.patentsight.com/en/ip-analytics-blog/the-top-20-most-innovative-chinese-universities

rang parmi de nombreuses universités chinoises ayant la plus forte force et influence mondiales en matière d'innovation technologique. Elle possède un portefeuille de 27 411 brevets actifs dans le monde. Avec plus de dix pour cent de leur indice des actifs qui couvre les technologies de communication électrique. D'autres domaines technologiques forts qui comprennent de la nanotechnologie y sont également. Elle est classée 65 parmi les 100 propriétaires de brevets les plus solides au monde, plus élevée que Dell Technologies ou Amazon. [171]

2) Mais également sur l'ouverture et le partage des connaissances

Sur le site de l'université de Tsinghua, ils insistent sur le fait que la connaissance dans le domaine digital doit être partagée en accueillant tous les étudiants étrangers. D'ailleurs, le gouvernement chinois propose de multiples bourses qui montent jusqu'à plus de 40 000 euros.[172] "Tsinghua s'engage à former des citoyens du monde qui prospéreront dans le monde d'aujourd'hui et deviendront les leaders de demain. Grâce à la poursuite de l'éducation et de la recherche au plus haut niveau d'excellence, Tsinghua développe des solutions innovantes qui aideront à résoudre les problèmes urgents en Chine et dans le monde."[173]
De même pour l'université de l'UESTC (12e sur le classement) qui partage un message intéressant du président de l'école Zeng Yong : "Nous espérons que les étudiants internationaux apprendront à s'adapter à l'environnement chinois, [...] à découvrir le développement de la Chine. Nous espérons que vous pourrez développer vos compétences en communication interculturelle par l'échange [...] de devenir des ambassadeurs amicaux entre la Chine et d'autres pays du monde. Nous espérons également que [...] vous deveniez des leaders académiques et techniques dans les domaines de l'information électronique, de l'informatique, de la gestion et d'autres domaines professionnels, et contribuerez au développement de votre patrie et du monde entier."[174] Outre le fait du partage des connaissances dans le domaine du numérique, les universités chinoises se rejoignent sur un autre point : celui du développement pour l'intérêt du pays. En d'autres termes, les étudiants,

[171] LexisNexis PatentSight team, (2018), "The Top 20 Most Innovative Chinese Universities", *PatentSight IP Analytics Blog*, https://www.patentsight.com/en/ip-analytics-blog/the-top-20-most-innovative-chinese-universities
[172]Anonyme. "Study in China" *Study portal master*, https://www.mastersportal.com/study-options/270156099/cyber-security-china.html
[173]Anonyme. "General information", *Tsinghua university*, https://www.tsinghua.edu.cn/en/About/General_Information.htm
[174] Anonyme. Zeng Yong, "Message from president" *University of electronic science and technology of China*, https://en.uestc.edu.cn/About_UESTC/Message_from_the_President.htm

qu'ils soient chinois ou étrangers, doivent tout d'abord porter attention aux intérêts chinois. Par conséquent, il est indéniable que cette production de connaissance doit d'abord servir les intérêts (ici cyber) de la Chine. Un dernier exemple avec l'Université de Zhejang (2e du classement) : "Tout en renforçant la construction de sa propre culture, ZZU souligne également son rôle sociétal de guide culturel, s'efforçant d'apporter de nouvelles contributions à l'héritage et à l'innovation de la civilisation chinoise. "[175]

3) L'Université cyber et d'ingénierie du Sud-Est (Zhengzhou University) au cœur de la stratégie de développement cyber chinois

Les universités qui touchent particulièrement le domaine du cyber sont nombreuses. L'école de cyber et d'ingénierie de l'Université du Sud-Est est un très bon exemple de ce que la Chine veut transmettre en matière de cyber. Lors de son ouverture, le directeur de l'école Zhang Guangjun s'est exprimé sur l'orientation de développement de l'université. Tout d'abord, l'école doit servir l'intérêt national du pays : "Nous devons élargir l'horizon et servir la stratégie nationale. Il a souligné que dans la nouvelle ère, nous devrions être conscients que c'était une responsabilité politique [...] assurer une gestion réussie de l'École de cyberscience et d'ingénierie". L'école met l'accent sur le développement de la cybersécurité en se mettant comme objectif de construire le « Projet de démonstration dans la construction d'un institut de cybersécurité de première classe » [...] C'est le succès et l'excellence que nous recherchons. [...] Ce développement doit servir les intérêts de la nation chinoise et aux exigences de la construction d'un institut national de cybersécurité. Pour cela, une compétition avec les meilleurs sur le domaine est nécessaire : " Nous devons nous efforcer de constituer une équipe d'enseignants de premier ordre, de cultiver des talents de premier ordre" Enfin, l'université veut globaliser la cybersécurité sur l'ensemble du territoire : "Dans le même temps, nous devons conduire et stimuler la construction et le développement de la discipline nationale de la cybersécurité. " Cet exemple prouve bien la volonté d'un développement et une extension du domaine cyber dans tous les milieux.

L'université fait partie du cœur de l'innovation digitale chinois, elle attire les chercheurs de la planète dans tous les domaines avec une volonté d'extension sur l'ensemble du territoire

[175]Anonyme. "About ZUU, introduction" *Zenhgzou university,* http://english.zzu.edu.cn/About_ZZU/Introduction.htm

chinois. Ces recherches universitaires alimentent l'industrie chinoise qui se digitalise de plus en plus afin d'augmenter sa productivité.

C) L'essor de la digitalisation dans les industries chinoises

1) Des changements conséquents pour répondre aux nouveaux enjeux économiques.

Selon certaines estimations, la cybersécurité en Chine pourrait atteindre 345,4 milliards de dollars en 2026 (comparé à 25,8 milliards de dollars en 2020). Dans ce nombre, on retrouve des entreprises digitales chinoises comme celle de la télécommunication qui devront, d'ici à 2023, consacrer 10% de leurs dépenses dans une mise à jour sur la sécurité et le niveau informatique. [176]

Pour la Chine, l'enjeu est capital pour sa stratégie économique. Elle commence par les universités, où le nombre de travailleurs dans les domaines augmentent afin de subvenir aux attentes des entreprises.[177] Pour prendre un exemple, le marché de détail connaît une numérisation grandissante : les canaux de ventes canaux s'étendent sur de courtes vidéos sur internet, les réseaux sociaux comme Douyin (la version chinoise de Tiktok) et Bilibili, ainsi que sur d'autres services à forte teneur en contenu comme Toutiao. Les panneaux d'affichage numérique, le mobile, les sites web et la télévision. Les transactions se font plus rapidement et directement. Enfin, les chaînes d'approvisionnement devront devenir plus agiles grâce au BigData et l'automatisation pour répondre à la demande de plus en plus fréquentes et diversifiées, ainsi qu'un algorithme développé pour mieux prévoir les tendances de consommation et les sources de demande.[178] Des entreprises étrangères devraient s'intéresser à ce modèle même si elles ne sont pas implantées en Chine. En effet, les industries chinoises

[176] B. TERRASSON, (2021) "La Chine prépare un plan sur trois ans pour stimuler son secteur de la cybersécurité" *Siècle Digital*, https://siecledigital.fr/2021/07/15/chine-plan-cybersecurite/

[177] McKinsey Global institute, (2014) "McKinsey Global InstituteChina's digital transformation : The Internet's impact on productivity and growth" McKinsey and Company https://www.mckinsey.com/~/media/mckinsey/industries/technology%20media%20and%20telecommunications/high%20tech/our%20insights/chinas%20digital%20transformation/mgi%20china%20digital%20full%20report.pdf

[178] L. Bu ,V. Chung , N. Leung , K. Wei Wang , B. Xia, C. Xia, (2021) "The Future of Digital Innovation in China: Megatrends Shaping One of the World's Fastest Evolving Digital Ecosystems", McKinsey and Company, https://www.mckinsey.com/featured-insights/china/the-future-of-digital-innovation-in-china-megatrends-shaping-one-of-the-worlds-fastest-evolving-digital-ecosystems

ont un écosystème numérique innovant et très développé qui leur permettent un avantage face à un monde de plus en plus numérisé.[179]

L'adoption en Chine du cyber en entreprise offre une très bonne dynamique. Une dynamique qui s'oriente vers un modèle de croissance économique basé sur la productivité, mais aussi sur l'innovation. Elle permet aussi de rationaliser les opérations d'entreprises en, par exemple, automatisant les procédures entre toutes les entreprises chinoises afin de créer un écosystème numérique large et efficace au sein du pays.[180] La technologie numérique est alors cruciale pour la modernisation des industries traditionnelles chinoises. Elle crée aussi de nouvelles entreprises et de nouveaux métiers très spécifiques dans le domaine du numérique. L'explosion d'internet dans le monde a permis d'abaisser les barrières sur le marché. Le développement des sites web, des réseaux sociaux est alors décisif pour attirer et créer de la nouvelle demande. Enfin, on constate une intensification de la concurrence entre les entreprises, accélérant, de surcroît, la croissance des industries les plus innovantes. Tous ces facteurs permettent à la Chine d'avoir une position de plus en plus dominante dans le cyberespace mondial.

2) L'adoption des nouvelles technologies qui passe par une sécurisation des entreprises

Le développement industriel numérique n'est pas seulement synonyme de croissance économique et d'innovation. Le gouvernement chinois cherche par ailleurs à protéger ses entreprises des menaces extérieures. Comme vu avec les télécommunications, les entreprises chinoises vont devoir mettre un budget concernant la sécurité de leurs donnée, d'après Ivan Platonov, analyste chez EqualOcean : "il est crucial de développer une stratégie globale qui incitera les entreprises du pays à augmenter leurs dépenses en matière de sécurité des données." [181] Le ministère chinois de l'Industrie et de la technologie s'attend à ce que le secteur représente plus de 38,6 milliards de dollars US d'ici à 2023. De plus, rajoute que

[179]Anonyme, (2020) "Les capacité d'innovation croissante de la Chine" CGTN Français https://www.youtube.com/watch?v=n0HHMb6kPKo

[180] R. Creemers, (2020), "Comment la Chine projette de devenir une cyberpuissance", Cairn.info, https://doc-center.ocg.msf.org/doc_num.php?explnum_id=4298

[181] M. BORAK, (2021), "China drafts three-year plan to boost its cybersecurity industry amid increasing concerns for data safety", South China Morning Post, https://www.scmp.com/tech/policy/article/3140963/china-drafts-three-year-plan-boost-its-cybersecurity-industry-amid

“Sans cybersécurité, nous ne pouvons garantir ni la sécurité nationale, ni la stabilité économique et sociale, ni les intérêts du peuple. Nous devons acquérir une solide compréhension de la cybersécurité et renforcer la cybersécurité et la protection des infrastructures d'information.”[182]

La Chine veut clairement se positionner en tant que leader dans l’innovation numérique qui attire le monde entier. Elle s’est donnée les conditions nécessaires pour donner naissance à l'écosystème numérique avec en premier temps, une vaste base de consommateurs numériques, puis une pression intense pour atteindre rapidement l'échelle, enfin un écosystème numérique qui favorise l'innovation et la formation rôle du gouvernement.[183] Elle souhaite attirer le monde entier en promouvant une collaboration entre entreprises, centres de recherches et universités internationales. Cependant, cette dynamique garde toujours un aspect conservateur de la culture et la vision chinoise : la Chine veut être la première et être dominante sur ses pays voisins. Un renversement des rapports de force est déjà en marche.

III) Le numérique, bras armé de la stratégie d’influence chinoise

Afin d’imposer son hégémonie, la Chine mène aujourd’hui une conquête des marchés étrangers et est en compétition avec le reste du monde. Cependant, ce n’est pas la seule bataille que mène la Chine.

En effet, l’État chinois pratique aujourd’hui une politique d’influence. Elle est dirigée vers la population chinoise, mais aussi vers les pays du reste du monde. Il s’agit d’une stratégie globale et nationale, qui s’inscrit dans un modèle beaucoup plus ambitieux, touchant différents domaines, que ce soit la politique, le droit, l’économie ou la citoyenneté. Pour mettre en place cette guerre d’influence, le Parti Communiste chinois exerce un contrôle accru sur ses entreprises et sa population. De plus, il pousse ses citoyens et les citoyens

[182] Xi Jinping The Governance of China III “Enhance Cyber Capabilities Through Innovation”, Quishi, http://en.qstheory.cn/2022-04/25/c_744275.htm

[183] L. Bu ,V. Chung , N. Leung , K. Wei Wang , B. Xia, C. Xia, (2021) “The Future of Digital Innovation in China: Megatrends Shaping One of the World’s Fastest Evolving Digital Ecosystems”, McKinsey and Company, https://www.mckinsey.com/featured-insights/china/the-future-of-digital-innovation-in-china-megatrends-shaping-one-of-the-worlds-fastest-evolving-digital-ecosystems

étrangers à adhérer consciemment et inconsciemment à son idéologie. Cette stratégie d'influence externe et interne est majoritairement possible aujourd'hui grâce à l'utilisation des nouvelles technologies. Le numérique permet à la Chine de mener une guerre de l'information et surtout de désinformation. Cela passe par le web et les réseaux sociaux, qui sont des vitrines des idées du Parti.

Cependant, il faut se demander si cette tactique novatrice sert vraiment les intérêts chinois. En effet, cette stratégie peut sembler quelque peu paradoxale. Comme le citait Jean-Baptiste Jeangène Vilmer et Paul Charon en parlant du PCC dans la synthèse de l'IRSEM[184] : « Il est plus sûr d'être craint que d'être aimé », Le Prince de Machiavel.[185]

A) Une stratégie d'influence extérieure

Afin de montrer sa puissance, la Chine mène une politique d'influence extérieure qui se trouve être une stratégie globale et agressive. Il s'agit d'une véritable guerre de l'information, qui passe par un contrôle total des organismes chinois.

1) Une stratégie globale et agressive

Le modèle chinois voulait auparavant renvoyer une image positive au reste du monde. Il voulait représenter un modèle de bienveillance, de traditions et de puissance. Cependant depuis 2003 la Chine a basculé vers une stratégie visant à séduire, infiltrer et contraindre. Elle applique une tactique dite des « Trois Guerres »[186] Il s'agit d'une guerre politico-juridique et psychologique, qui influence l'opinion publique (médiatique), en utilisant principalement le vecteur cyber afin de « vaincre sans combattre »[187] .

[184] Irsem (2021) LES OPÉRATIONS D'INFLUENCE CHINOISES. https://www.irsem.fr/rapport.html
[185] Poujade, O. (2021b, septembre 20). La stratégie d'influence chinoise : Un réseau tentaculaire qui veut désormais s'imposer au reste du monde. Radio France. https://www.radiofrance.fr/franceculture/la-strategie-d-influence-chinoise-un-reseau-tentaculaire-qui-veut-desormais-s-imposer-au-reste-du-monde-7980973
[186] Ibid.
[187] Cf note de bas de page 184.

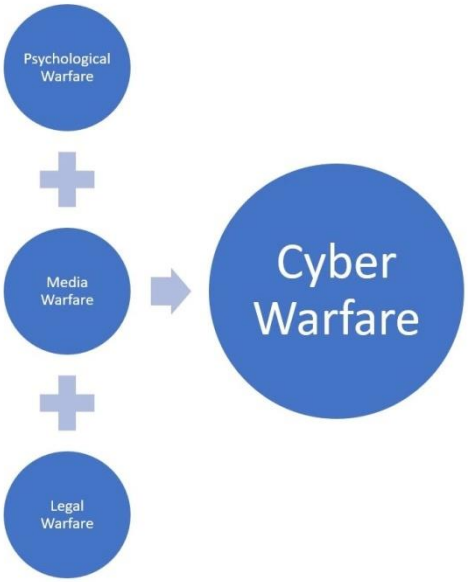


Figure: Warfare tools of CMC
Compiled by @saikirankannan

Elle se base notamment sur une guerre du droit ou « lawfare » en mettant en place des mesures coercitives ; mais aussi sur des mesures plus actives. Il est alors question de désinformation, de sabotage, de contrefaçon, d'opération de déstabilisation de gouvernements étrangers, d'opération de discrédit, de création de structure de dîtes de façade ou bien même de citoyens payés pour servir les intérêts du régime.

Ce choix de stratégie national se veut beaucoup plus agressif et offensif que le précédent, ce qui a conduit la Chine à être comparée à la Russie. On parle de « russianisation ». Le rapport de l'IRSEM, rédigé en 2021, parle à ce propos de la stratégie adoptée par Pékin afin d'imposer sa vision du monde. On y apprend que l'APL est chargé d'une manipulation de l'information, qui touche différents domaines qui seront étudiés dans le chapitre sur la guerre d'influence. A travers ces différents domaines, l'APL vise les Etats-Unis, mais également Taïwan, Singapour, la Suède, la France, le Canada et la Nouvelle-Calédonie parmi d'autres.

2) Un contrôle total

Ces opérations d'influence passent par le contrôle des entreprises et notamment par la collecte de leurs données. Pour le moment et officiellement, l'État chinois n'a pas accès aux données de ses entreprises privées. Cependant, il utilise aujourd'hui à sa guise les bases de données de ses entreprises publiques et semi-publiques. De plus, des opérations d'espionnage

permettent à la Chine de contrôler une partie des données des entreprises à l'étranger et le déploiement de sociétés comme les BATXH dans le monde entier permet d'affirmer ce contrôle. Ces bases de données sont d'ailleurs qualifiées de « techno-autoritaristes » dans la synthèse de l'IRSEM, car elles servent les opérations d'influence étrangères.

Par ailleurs, la Chine effectue une lente pénétration des organismes et crée petit à petit une dépendance économique qui lui permet de mettre en place certaines mesures politiques et une diplomatie punitive. Cela comprend des mesures comme l'embargo, le refus d'accès au marché chinois, le tourisme contingenté, les sanctions économiques, le boycottage ou la censure par exemple. Cela lui permet de contrôler indirectement ces entreprises, afin de stopper toutes formes d'actions qui ne seraient pas en adéquation avec les intérêts du Parti. L'exemple de Jack Ma Didi, ancien dirigeant d'Alibaba, va même plus loin. L'homme d'affaires chinois a disparu pendant plusieurs mois après avoir quitté ses fonctions. On peut se demander jusqu'où le PCC a pu aller pour asseoir son contrôle sur l'entreprise Alibaba.

3) Une guerre d'influence

L'histoire de Jack Ma Didi montre bien que la Chine contrôle l'information et que la lumière ne sera jamais faite sur ce qu'il s'est vraiment passé. En effet, le PCC mène une véritable guerre d'influence.

Cette propagande de terrain passe notamment par le contrôle des diasporas, afin d'éviter que les Chinois à l'étranger soient une menace pour le Parti et qu'ils propagent une image de la Chine non conforme à son idéologie. Pour cela le PCC pratique une répression qui va au-delà des frontières nationales. Selon l'ONG Freedom House, il s'agit du contrôle de diasporas « la plus sophistiquée, globale et complète dans le monde ».

L'Etat chinois se sert aussi des hauts postes de l'ONU qu'occupent ses citoyens. Cela lui permet d'influencer de l'intérieur les politiques des pays étrangers en utilisant la diplomatie, la corruption, des pressions économiques et politiques ou la cooptation. Les opérations d'influences clandestines et d'ingérences étrangères sont effectivement monnaie courante. Notamment dans la compétition entre la Chine et les Etats-Unis, mais également entre la Chine et Taïwan.

De plus, les think tanks, les universités et instituts Confucius, les touristes chinois et les influenceurs permettent eux aussi de propager les idéologies du Parti. De même que certains

groupes indépendantistes, que l'on retrouve par exemple en Nouvelle Calédonie, ou les groupes pacifistes comme No Cold War[188]

L'importation et l'exportation des technologies fait également partie de cette stratégie d'influence. L'importation des technologies, par exemple via les universités étrangères, est le fruit de surveillance des campus étrangers et du travail des chercheurs chinois répartis dans de nombreuses universités à l'étranger via des programmes de recherche conjoints. Ces importations concernent d'ailleurs et souvent des technologies de surveillance ou la fabrication d'armes de destruction massive. Il y a eu plusieurs cas de ce genre découverts en 2020 et 2021 selon la synthèse de l'IRSEM[189].
Enfin, la culture et les médias représentent une grande partie de cette stratégie. A ce titre, la Chine a investi depuis 2008 plus de 1,3 milliards d'euros dans ses médias nationaux et transnationaux, afin de développer son contrôle de l'image. En effet, on retrouve des émissions chinoises sur différents continents et dans de nombreuses langues. En ce qui concerne la culture, la Chine fait souvent pression sur les productions culturelles nationales et même étrangères, qui par crainte des répercussions possibles, censurent leurs productions.

4) Les limites de cette stratégie extérieure

Pour le moment, cette stratégie ne s'étend qu'à certaines régions, même si le but de la Chine et d'affirmer son hégémonie sur le monde. La Chine concentre pour l'instant ses efforts vers Taïwan et Hong Kong, qui font office de lieux d'expérimentations. On a pu constater un exemple de ces entraînements en 2018 lors des élections municipales à Taïwan, ou encore en 2019 lors de la crise de Hong Kong. Les prochaines cibles sont les voisins australiens et néo-zélandais.

Aussi, de plus en plus de puissances étrangères ont pris conscience de ce phénomène et n'hésitent plus à répliquer. C'est par exemple le cas de la société taïwanaise Team T5, créée en 2014 par le chercheur en sécurité Sung-Tin Tsai, et qui surveille attentivement les opérations d'influence chinoise. (intelligence.co…)[190]. Cette société travaille notamment en collaboration avec l'Australie, pays de plus en plus touchés par les opérations chinoises.

[188] Irsem (2021) LES OPÉRATIONS D'INFLUENCE CHINOISES. https://www.irsem.fr/rapport.html
[189] Ibid.
[190] TAIWAN : TeamT5, de la menace cyber chinoise à la contre-influence - 18/03/2022. (2022, mars 18). Intelligence Online. https://www.intelligenceonline.fr/surveillance--interception/2022/03/18/teamt5-de-la-menace-cyber-chinoise-a-la-contre-influence,109761129-gra

B) Une stratégie d'influence intérieur

La démonstration de la puissance chinoise passe par l'influence étrangère, mais également par une guerre de l'information interne. En effet, le PCC exerce un contrôle strict de la population. Il passe pour cela par des incitations négatives et positives, afin de faire adhérer ou de contraindre les citoyens à son idéologie.

1) Un contrôle de la population

Cette stratégie d'influence chinoise est également intérieure. Elle vise effectivement la population. En ce sens des mesures ont été prises pour surveiller et influencer les citoyens chinois, notamment depuis 2000 avec une réglementation de l'utilisation des données[191]. Un contrôle social a aussi été mis en place en 1990. Ce contrôle est rendu possible grâce aux nouvelles technologies pour espionner la population et façonner les comportements.

Le contrôle social fonctionne entre autres grâce à une technologie d'intelligence artificielle qui peut effectuer une reconnaissance faciale. Cependant ce contrôle de la population passe aussi par du traçage de téléphone, de pass de transport et par la collecte de données des entreprises publiques et semi-publiques.

Ce contrôle fonctionne comme un permis à points pour les citoyens, avec des catégories qui donnent des avantages pour les comportements jugés conformes aux yeux du Parti. Les comportements non-conformes sont quant à eux dévalorisés. Ce système fonctionne avec ce que l'on appelle le crédit social chinois le SCS. Il est par exemple possible pour les citoyens de Shangaï de consulter leur crédit social sur une application, Honest Shangaï, qui évalue leurs points sur la base de : leur casier judiciaire, leurs impôts et leur statut professionnel. Ce système de notation existe aussi à Pékin, où une liste noire des citoyens ayant un mauvais comportement a même été mise en place. L'objectif du PCC étant officiellement de garantir la sécurité de sa population et de favoriser la citoyenneté.

Toutefois, ces mesures s'apparentent plus à de la surveillance de masse qu'à de la bienveillance du gouvernement vis-à-vis de ses citoyens. En effet, le contrôle social permet au gouvernement chinois de surveiller tous les faits et gestes de sa population. Les caméras installées permettent par exemple de surveiller les lieux publics, comme les rues ou les gares.

[191] Le contrôle social chinois : Le numérique pour surveiller la population. (2020, décembre 17). Aleteia. https://fr.aleteia.org/2020/12/17/le-controle-social-chinois-le-numerique-pour-surveiller-la-population/

En 2019, on ne compte d'ailleurs pas moins de 200 millions de caméras de surveillance installées en Chine[192]. La reconnaissance faciale permet aussi aux citoyens chinois d'ouvrir leur porte ou de payer dans les commerces. Cela peut permettre de fournir des données réutilisables contre eux. Le Parti utilise d'ailleurs des bases de données qui lui permettent d'effectuer un fichage de la population. De cette façon, les citoyens en marge de la société, qui pratiquent une religion différente par exemple, sont réprimés. C'est le cas des musulmans ouïghours, qui subissent une répression, sous prétexte de lutte contre la radicalisation. Cette forme de surveillance de masse à également pu être utilisée et observée avec la crise du au Covid-19 depuis 2020. Dans n'importe quel cas de figure, les citoyens qui ne respectent pas les règles imposées par le gouvernement se voient privés de certains de leurs droits civiques. Il peut leur être refusé de faire un emprunt, de prendre les transports en commun ou d'être membre du PCC par exemple.

2) Incitations négatives

Le contrôle social peut revêtir un aspect positif qui encourage les citoyens chinois à bien agir en les récompensant, mais aussi un aspect négatif et répressif, par exemple avec la dévalorisation du crédit social chinois lorsqu'une infraction a été commise.

Cela fait partie intégrante de la stratégie chinoise de contrôle de la population. Concernant les incitations négatives, le parti cherche à se faire craindre. Il prône notamment la délation, par exemple dans la ville de Rongcheng qui attribue des points bonus à ceux qui dénoncent les personnes opposées au régime. Il faut cependant rappeler qu'une personne opposée au régime peut tout simplement être une personne ayant une religion différente. Ces personnes-là peuvent d'ailleurs être qualifiées de terroristes au sens chinois du terme, et sont alors placée dans la catégorie d'alerte C se trouvant juste avant la catégorie dans laquelle se trouve les criminels[193]. De plus, l'affichage public des personnes ayant de mauvais scores sur le crédit social, participe à alimenter la crainte de la population vis-à-vis du Parti. De même que les messages automatiques diffusés sur la ligne de téléphone des citoyens lorsque ceux-ci sont appelés. En effet, un message est laissé à leur interlocuteur juste avant la communication, leur demandant de les encourager à mieux agir ou leur disant de se méfier de cette personne. Enfin, ces mesures répressives se retrouvent également dans les entreprises chinoises. C'est

[192] *Promesse de la technologie—Faits marquants de DEF CON China 1.0*. (2019, juin 5). The Cloudflare Blog. http://blog.cloudflare.com/fr-fr/technologys-promise-def-con-china-1-0-highlights-fr-fr/

[193] *Le contrôle social chinois : Le numérique pour surveiller la population*. (2020, décembre 17). Aleteia. https://fr.aleteia.org/2020/12/17/le-controle-social-chinois-le-numerique-pour-surveiller-la-populatio

par exemple le cas de Baidu, entreprise qui a relevé la faille Log4j et qui a été de ce fait sanctionnée par le gouvernement chinois, car cela ne diffusait pas une bonne image de la Chine. En effet, cela montrait que la Chine pouvait également être sujette aux cyberattaques.

3) Incitations positives

Cependant, il existe également un grand nombre d'incitations positives qui permettent de guider l'opinion publique de la population chinoise, mais aussi des pays étrangers. Le but étant de les faire aller dans le sens du Parti et d'adopter ses idéologies.

Comme déjà mentionné, il existe les mesures incitatives liées au contrôle social, qui prône des valeurs telles que la solidarité et la civilité. On retrouve aussi l'utilisation de la culture et des médias qui façonne l'imaginaire chinoise et permet de mener une véritable lutte psychologique qui idéalise le PCC.

Par ailleurs on retrouve également des événements qui permettent de montrer le savoir-faire des Chinois. C'est par exemple le cas de la Tianfu Cup, contre-projet de l'américaine Pwn20wn créé en 2015. Cette compétition permet aux hackers chinois de montrer leurs compétences et de se confronter à d'autres hackers, car ils avaient avant cela interdiction de participer à des compétitions de hacking étrangères[194].

La Def Con Asia va dans le même sens que la Tianfu Cup. Il s'agit ici d'une conférence internationale de sécurité, lancée depuis 2018 en Chine. Cette conférence permet au gouvernement chinois de montrer son soft power, son savoir-faire en matière de cybersécurité et d'innovation au reste du monde.

C) Une nouvelle forme de propagande

Il est effectivement constaté que la Chine exerce une nouvelle forme de propagande, beaucoup plus agressive. Cependant, on peut surtout remarquer que le gouvernement s'appuie de plus en plus sur les nouvelles technologies pour propager ses idées et contrôler son image.

[194] Promesse de la technologie—Faits marquants de DEF CON China 1.0. (2019, juin 5). The Cloudflare Blog. http://blog.cloudflare.com/fr-fr/technologys-promise-def-con-china-1-0-highlights-fr-fr/

1) Une guerre de la désinformation

Cependant, le gouvernement chinois ne passe pas que par le soft power pour affirmer sa puissance mondiale. La Chine, et plus précisément l'APL, mène effectivement une guerre de l'information et surtout de la désinformation, qui passe notamment par les médias et les réseaux sociaux. La propagande manipule pour cela de fausses identités pour redorer l'image de la Chine et dévaloriser l'image de ses concurrents, qui se trouvent souvent être des démocratie libérales[195]. Ces démocraties en viennent même souvent à s'auto-censurer pour ne pas aller contre le PCC et par crainte de représailles. Les accusations contre les Etats-Unis en février 2020, affirmant qu'ils étaient responsables de la crise du Covid-19, est un exemple de cette guerre de la désinformation menée par la Chine. Un autre exemple de cette guerre est l'affaire Larry Romanoff. Il s'agit d'un Canadien qui a été utilisé par le gouvernement chinois pour écrire des articles complotistes sur les Etats-Unis et la pandémie du Covid-19[196]. Des moyens traditionnels sont donc utilisés pour diffuser la propagande du PCC, cependant des cyber techniques sont maintenant utilisées et donnent à cette propagande une nouvelle forme encore plus dangereuse.

2) Le web, vitrine de la propagande chinoise

En effet, la Chine utilise désormais des outils numériques de plus en plus répandus et efficaces. Le web est notamment devenu la vitrine de la propagande chinoise, propagande menée par l'APL, l'unité 61070 et plus précisément la base 311, qui est le centre d'opération de l'influence chinoise[197].

Pour mettre en œuvre cette stratégie, une « armée » a même été créée, elle se fait appeler «l'armée des 50 centimes ». Elle est constituée de citoyens chinois, qui sont payés pour publier du contenu soutenant le régime sur Internet. Ce contenu est publié sous la forme de fermes de contenus, de comptes, de pages, grâce notamment à des influenceurs. Le but est de faire penser au public qu'il s'agit d'initiatives populaires et spontanées. En 2019, YouTube, Twitter et Facebook tirent d'ailleurs la sonnette d'alarme et identifient les campagnes chinoises circulent sur leurs réseaux.

---

[195] Irsem (2021) LES OPÉRATIONS D'INFLUENCE CHINOISES. https://www.irsem.fr/rapport.html

[196] Poujade, O. (2021b, septembre 20). La stratégie d'influence chinoise : Un réseau tentaculaire qui veut désormais s'imposer au reste du monde. Radio France. https://www.radiofrance.fr/franceculture/la-strategie-d-influence-chinoise-un-reseau-tentaculaire-qui-veut-desormais-s-imposer-au-reste-du-monde-7980973

[197] Ibid.

L'astroturfing est également une des méthodes qui a vu le jour sur les réseaux chinois. Cette méthode consiste à avoir une place importante sur les réseaux et à inonder ceux-ci de messages soutenant les idées du Parti. Cette technique essaye également de faire passer ces messages comme étant authentiques et soutenant spontanément le régime, afin de stopper les discours étant contre les idées du PCC. Selon le rapport IRSEM 22 millions de citoyens seraient rémunérés pour effectuer cette tâche, d'où l'utilisation du terme « idiots utiles »[198].
La stratégie des loups guerriers peut également être mentionnée. Il s'agit d'une stratégie chinoise, agressive représentée par la glorification du trolling. Elle se base effectivement sur le harcèlement et la désinformation. Cette stratégie est appliquée par ce que l'on appelle des « loups guerriers » qui diffusent un discours agressif et violent sur les réseaux du monde entier, en réponse à des propos négatifs sur la Chine[199].

Concernant les réseaux sociaux, le gouvernement chinois exerce également une large politique de contrôle et une stratégie d'influence interne et externe. Certains réseaux sociaux, comme Facebook, sont d'ailleurs interdits en Chine et d'autres, comme Baidu, les remplacent ou sont plus commercialisés. Comme c'est le cas de Tik Tok, qui possède un véritable enjeu d'influence pour le PCC.

Les réseaux sociaux chinois sont des véritables lieux de lutte informationnelle. On y retrouve des faux comptes visant à contrôler l'opinion publique chinoise et étrangère. De fausses photos de profils sont même utilisées. Celles-ci sont créées grâce à l'intelligence artificielle. Ce pan de la stratégie d'influence de la Chine est décrit comme étant une stratégie d'influence « ouverte » par le rapport de l'IRSEM[200]. On y pratique la dissuasion et la guerre psychologique.

La Chine mène une grande campagne de séduction et d'influence au sein de son pays et à l'étranger. Cependant, cette stratégie se veut de plus en plus agressive et se rapproche du modèle russe. On parle désormais de guerre qui est menée sur divers fronts, économique, politique, sociale et éducationnel. Le numérique, ainsi que le cyber permettent au gouvernement chinois de contrôler ses entreprises, ses écoles, son image et sa population, mais aussi de montrer une partie de sa puissance.

Le pays a eu quelques réussites notamment tactiques, toutefois et de manière plus globale cette stratégie a montré ses limites. En effet, cette stratégie demande beaucoup de

198 Irsem (2021) LES OPÉRATIONS D'INFLUENCE CHINOISES. https://www.irsem.fr/rapport.html
199 Ibid.
200 Ibidem.

moyens et de temps et comme dans tous les autres pays les filières de la cyber et des nouvelles technologies rencontrent des problématiques de recrutement. L'isolement et le cloisonnement du pays n'aident pas non plus à améliorer l'image de la Chine, qui souffre depuis l'arrivée de Xi Jinping d'une image négative. Cette image négative de la Chine hyper-contrôlée et agressive a notamment été exacerbée depuis 2020 à cause de la crise du Covid-2019. La stratégie du Parti entre crainte et adoration renvoie une mauvaise image au reste du monde, qui voit la Chine comme un pays autoritaire. Cette vision de la Chine est même de plus en plus partagée par les chinois eux-mêmes.

Chapitre 3 - Projections militaires et para-militaires dans le cyber-espace

Le Parti Communiste Chinois considère, dans la lignée clausewitzienne[201], que « la guerre n'est que la continuité de la politique par d'autres moyens ».
Parce que sa victoire n'est pas encore assurée dans les espaces terrestres, aériens et maritimes, le PCC préfère l'éviter pour l'instant, n'ayant pas encore suffisamment dépassé le seuil critique de supériorité militaire face aux USA, leur principal adversaire d'aujourd'hui, et ennemi de demain.
Le cyberespace est en cela le lieu de prédilection d'un affrontement larvé et d'un espionnage intense pour l'Armée Populaire de Libération, qui peut, si elle le souhaite, mener des attaques dévastatrices sur des systèmes d'informations ciblés, tout en niant en être à l'origine.

C'est d'ailleurs ce qu'exposait le Général Fang Fengshui, chef d'État-Major de l'APL, à son homologue américain Martin E. Dempsey, lors de sa visite en Chine en 2013[202] :

"Une cyber-attaque majeure peut-être aussi dévastatrice qu'une bombe nucléaire, et n'importe qui peut lancer les attaques, depuis l'endroit où il vit, depuis son propre pays, depuis un autre pays" sans que l'on puisse toujours formellement l'identifier, tout au plus le soupçonner. C'est aussi le principe sous-jacent à la dissuasion nucléaire sous-marine, à laquelle la Chine a fini par adhérer. Le parallèle entre les évolutions doctrinales de la Marine chinoise[203] et celles de sa composante de cyber-guerre sont d'ailleurs frappantes : mise à disposition d'unités civiles "accréditées" par les militaires, tels les garde-côtes pour l'une, et les techniciens informatiques du Ministère de la Sécurité de l'État pour l'autre, création de milices civiles aux caractéristiques parfois para-militaires pour l'une et l'autre, utilisation de la dissuasion, etc.

[201] Meilinger, P. S. (2010). China and Clausewitz. Science Applications International Corporation.
[202] Maurer, T. (2018). Cyber mercenaries : The state, hackers, and power.
[203] Luo, S., & Panter, J. G. (2021). *China's Maritime Militia and Fishing Fleets*. Army University Press. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2021/Panter-Maritime-Militia/

De plus l'APL a su se saisir, particulièrement depuis la fin des années 90, des imbrications civilo-militaires et académico-militaires à son avantage direct, multipliant les partenariats et la supervision au sein des entreprises et universités. La décision en 2013 d'une vague de réformes successives[204] quant à sa structuration a fini par lui donner une capacité d'affirmation de cyberpuissance qu'elle met au profit d'un PCC toujours plus agressif au sein des rapports économiques internationaux, accentuant les crispations étrangères contre lui.
Cela ne signifie pas pour autant que les forces armées chinoises ne connaissent pas des facteurs d'affaiblissement relatifs en leur sein même, freinant leur efficience. L'arrestation du même Général Fang Fengshui pour corruption[205] en est une illustration.

La cyber-menace des opérations de l'APL demeurent cependant une problématique majeure pour les adversaires du PCC, inscrite dans une militarisation modernisée plus large.

Dans un rapport de la Defense Intelligence Agency (DIA, Agence du Renseignement de la Défense US), de 2021, le Department of Defense des USA (DOD) disait[206] à propos de la Chine :
"Reconnaissant que les opérations conjointes, les flux d'informations et la prise de décision rapide sont essentiels dans la guerre moderne, la République Populaire de Chine continue d'accorder une grande priorité à la modernisation de la capacité de l'APL à commander des opérations interarmées complexes sur des champs de bataille proches et éloignés. La RPC cherche à améliorer les systèmes de commandement et de contrôle interarmées de l'APL ; les systèmes logistiques conjoints; et les systèmes de commande, contrôle, communications, ordinateurs, renseignement, surveillance et reconnaissance (C4ISR). La RPC modernise, diversifie et étend également ses forces nucléaires, ainsi que l'approfondissement de l'interopérabilité et de l'intégration de l'APL avec les forces paramilitaires et forces de la milice".

[204] Col. Shukla, A. (2017). Chinese Military Reform, 2013-2030. IPCS | Institute Of Peace and Conflict Studies. http://www.ipcs.org/comm_select.php?articleNo=5361
[205] BBC News. (2019, 20 février). Fang Fenghui : China's ex-top general jailed for life. https://www.bbc.com/news/world-asia-china-47306275
[206] Office of the Secretary of Defense. (2021). Military and Security Developments Involving the People's Republic of China. Annual Report to Congress.

I) Organisation et structures

Pour analyser, la projection de force dans le cyberespace qu'applique la Chine, il faut se concentrer en premier temps dans les différentes structures mises en place pour gérer les différents concepts doctrinaux relatifs à la guerre informationnelle. Ces structures mouvantes, qui ont connu plusieurs changements majeurs, témoignent des changements doctrinaux qui ont pu avoir lieu, et des différentes mesures entreprises par le PCC pour reprendre contrôle des armées ou résoudre des problèmes identifiés.

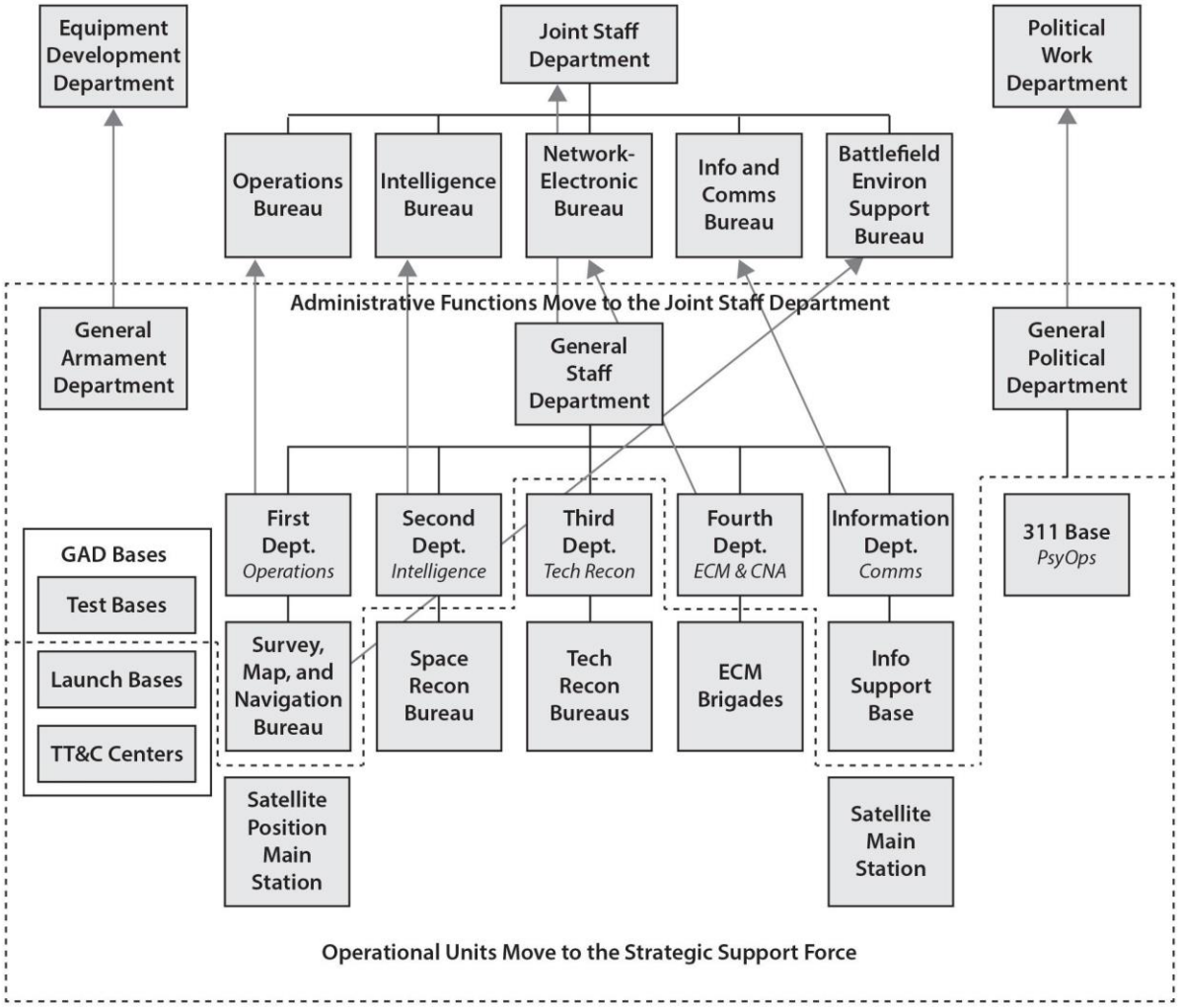
A) Pré-réforme

Tout d'abord, il sera abordé l'élément historique de l'armée populaire de libération, première concentration des forces de guerre électronique et de guerre informatique.
Il s'agit du General Staff Department, ou GSD (Zongcanmou Bu, 中国人民解放军总参谋部) , qui est un des quatre départements généraux, directement sous la direction et le contrôle d'un des organes de commandement les plus élevés en Chine, la Commission Militaire Centrale.
La présentation des éléments qui en sera faite servira principalement à permettre une meilleure compréhension des différentes réformes de ces dernières années. Ainsi, il ne sera pas présenté l'ensemble des éléments techniques du GSD.

1) Le General Staff Department (GSD), introduction à la structure de support informatique, dont dépendent les opérations numériques.

Au sein du GSD, on retrouve une majorité d'officiers de l'armée de terre chinoise, on peut par exemple citer que jusqu'en 1998, les officiers de la marine ou armée de l'air chinoise qui y étaient affectés devaient porter des uniformes de l'armée de terre. Cela était dû aussi à la confusion qui était faite entre les missions du GSD, qui était à la fois organisme aux missions générales comme de renseignement, mais aussi qui était l'équivalent de l'État-major de l'armée de terre chinoise.

Figure 1. Pre-Reform Locations of Major SSF Components



Key: ECM: electronic countermeasures; GAD: General Armament Department; PsyOps: psychological operations; TT&C: telemetry, tracking, and control; GPD: General Political

Les troisièmes et quatrième départements s'occupent du renseignement électromagnétique au sens large, et comprennent donc la composante d'attaque informatique, qui se rapproche doctrinalement de ce que les Américains qualifient de Computer Network Exploitation (exploitation de réseaux informatique) et de Computer Network Operation (opération au sein de réseaux informatique) cela comprend également les opérations de Computer Network Defense, défense de réseaux informatiques, qui ne sera cependant pas abordé dans cette partie. Ces départements s'insèrent donc directement dans la stratégie numérique militaire chinoise, devenant les organismes de référence de l'armée, et notamment à travers les concepts de « reconnaissance technique » (技术侦察), fondation de la doctrine de guerre informatisée déjà évoquée.

On les retrouve intégrés, comme les autres départements, directement sous le commandement du département général et du département politique.

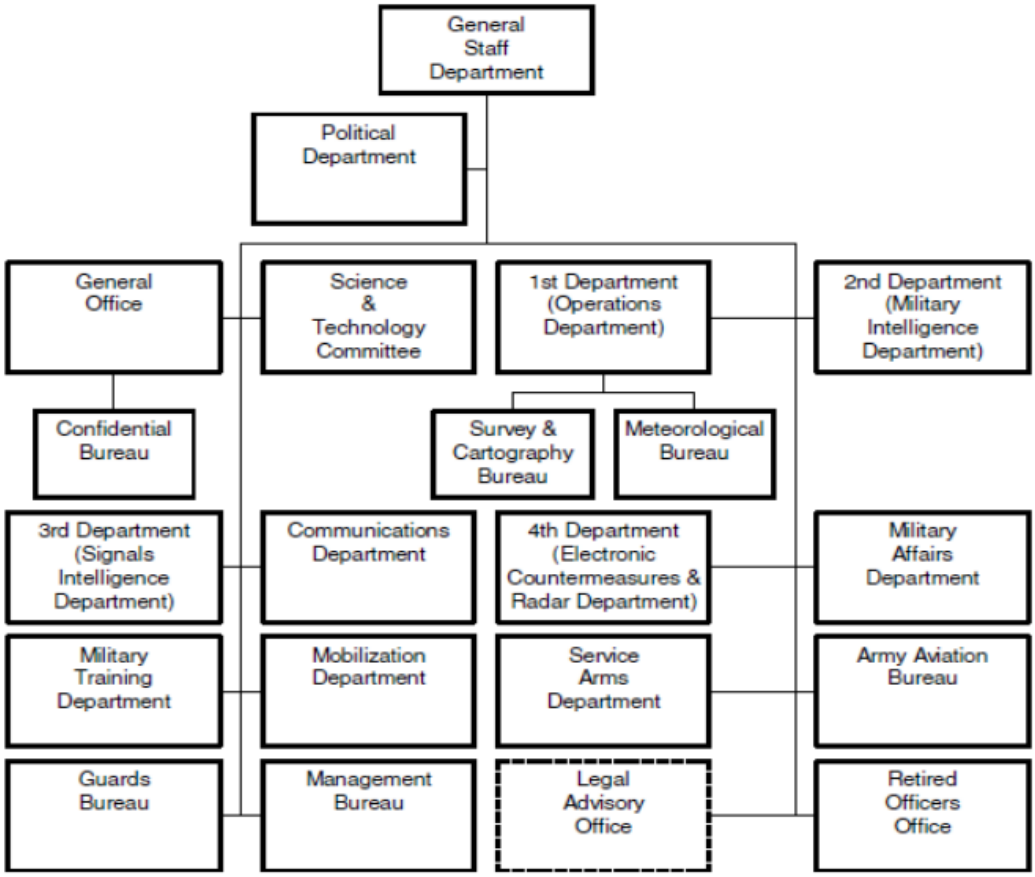


Figure 1: General Staff Department of the People's Liberation Army[51]

2) Le département technique, 3eme département du GSD, concepts généraux

Le département technique du GSD, couramment appelé Troisième Département, qui a été évoqué, semble être détenteur d'une vaste infrastructure de contrôle des flux depuis des sites de collection en Chine, depuis les ambassades, voire même potentiellement à terme depuis des systèmes satellitaires.[207]

Ses origines historiques (datant de 1930, où il était alors connu comme le Second Bureau de la Commission Militaire Centrale) lui lèguent des missions de collecte de l'information, de traduction et de déchiffrement/chiffrement, et font donc de lui un organisme possédant une grande compétence et expérience dans ces milieux, et est qualifié par les chercheurs de

[207] Kevin Pollpeter et Kenneth W.Allen (2017) *The PLA as Organization v2.0* https://apps.dtic.mil/sti/pdfs/AD1082742.pdf

l'institut Projet2049 travaillant sur la Chine, de « plus grand employeur de linguistes expérimentés en Chine » [208]

Il semblerait qu'en sus de ses activités de renseignement électromagnétique «traditionnelles» pour les raisons évoquées, il a hérité des activités d'intrusion informatique, servant d'exécutif national pour les opérations numériques, confirmé par l'intrusion GhostNet, opération massive d'espionnage informatique, ciblant les institutions tibétaines sur une période de 10 mois.[209]

Il gère donc certes la partie offensive, mais également la partie défensive, devant prévenir un accès illégitime aux réseaux comportant des informations sensibles de l'APL.

Actuellement, un rapport non confirmé indique que le Troisième Département aurait 130 000 personnels. Il semble aussi y avoir 12 bureaux opérationnels qui seront décrits succinctement et trois instituts de recherche.

Il paraît ainsi naturel, au vu de ses moyens et missions héritées, que le GSD soit au moins alerté des intrusions sur le sol national et des opérations numériques offensives réalisées par la Chine.

À noter, il est très peu probable qu'un département du GSD (Troisième ou Quatrième) en charge de la défense n'ait aucun lien avec la partie offensive, notamment en reprenant les dires chinois tels que "sans connaissance de l'offensive, on ne sait pas défendre". À ce titre, les opérations numériques sont souvent évoquées comme « attaques et défense d'un réseau » (网络功防)

3) Organisation du département technique

Pour traiter des opérations numériques militaires chinoises, il semble important de s'attarder sur le département technique du GSD, qui pourrait être grossièrement comparé à la NSA en tant qu'organisme de renseignement technique, duquel découle son nom de département technique au sein du GSD.

---

[208] Stokes, M. A., Lin, J., & Russell Hsiao, L. C. (2011). *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*. Project 2049 Institute. https://project2049.net/wp-content/uploads/2018/05/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf

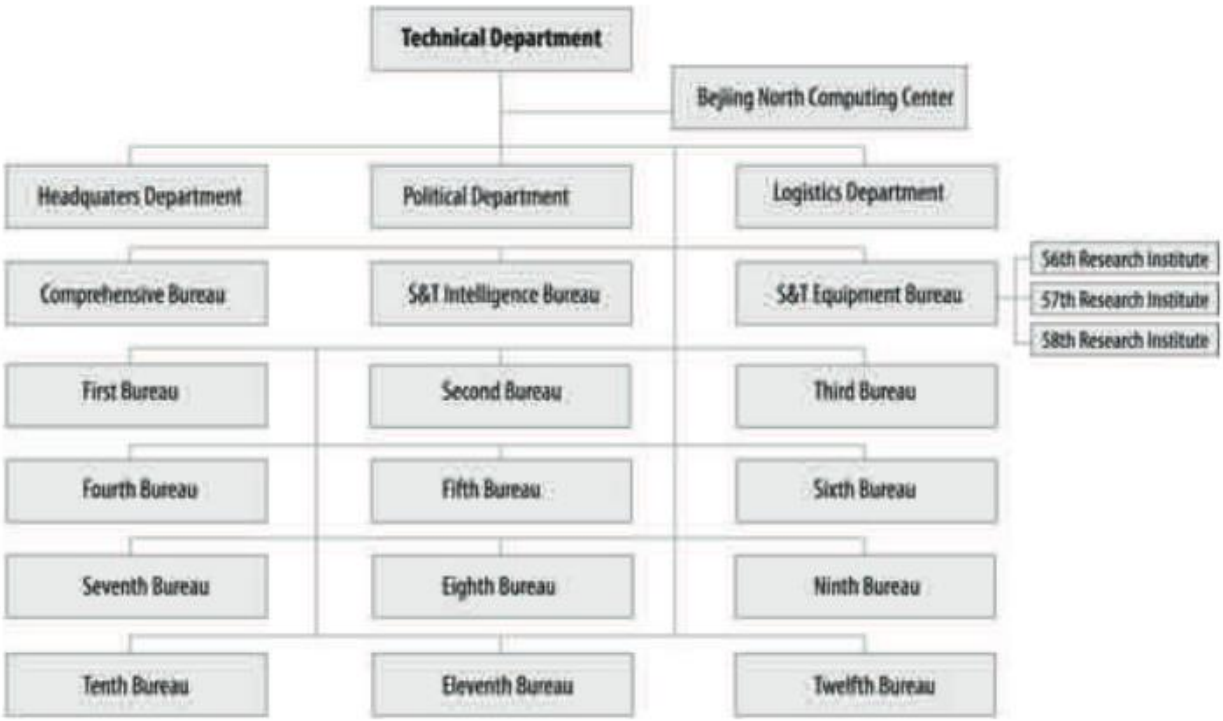
[209] Anonyme. (2009). *Tracking GhostNet : Investigating a Cyber Espionage Network*. Information Warfare Monitor. http://www.nartv.org/mirror/ghostnet.pdf

Lors de la présentation du département technique, un point sera réalisé ici uniquement sur la partie technique, et non pas sur les spécificités chinoises, telles que le département politique. D'autres informations sont disponibles, en majorité publiées par l'institut project2049, qui s'est attardé à deux reprises sur le GSD, une fois lors d'une présentation générale[210], une autre fois en se focalisant sur le département technique. [211]

Cette partie technique se représente donc majoritairement par les différents bureaux, et quelques autres services que sont les instituts de recherche.

Une vue d'ensemble nous est proposée par Kevin Pollpeter et Kenneth W. Allen, présentée ci-dessous[212]

Figure 6: GSD Technical Department



[210] Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao (2011, novembre 11) The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure. Project 2049 Institute https://project2049.net/wp-content/uploads/2018/05/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf

[211] *Ibid*

[212] Pollpeter K. et Allen W. (2017) The Pla as organisation v.2 Defense Group Inc. https://apps.dtic.mil/sti/pdfs/AD1082742.pdf

4) Présentation des bureaux

Les douze bureaux présents possèdent des attributions différentes. L'institut Project2049 a essayé dans les rapports cités de les estimer, en fonction des travaux publiés, et souvent, en fonction de la spécialité des linguistes identifiés.

Dénomination	Attribution
Premier Bureau (unité 61786)	Son rôle exact est inconnu, on sait cependant qu'il a participé au programme national 863.
Second Bureau (unité 61398)	Ce bureau cible principalement les Etats-Unis et le Canada sur des sujets politiques, économiques et militaires
Troisième Bureau (unité 61785)	Il s'occuperait des émissions radio "en ligne de vue", donc ce qui serait de la radio haute fréquence. Cela consisterait aussi dans les normes TEMPEST, d'émission électromagnétique menant à une fuite de l'information.
Quatrième Bureau (unité 61419)	Il est concentré sur la Corée, ce qui a été identifié par la présence de linguistes.
Cinquième Bureau (unité 61565)	Son attribution semble être la Russie, là encore dû à la présence de linguistes spécialisés en Russe
Sixième Bureau (unité 61726)	Son rôle est inconnu, mais une de ses sous-unités a une mission d'entraînement.

Septième Bureau (unité 61580)	Il possède des traducteurs anglophones, et a publié sur l'attaque et la défense de réseau. Cependant dans la formulation de Project2049, il ne semble pas avoir un rôle particulièrement opérationnel.
Huitième Bureau (unité 61046)	Il cible l'Europe, là encore dû aux linguistes présents. Il pourrait cependant également cibler l'Amérique Latine ou des parties de l'Afrique.
Neuvième Bureau (sans matricule officiel)	Aucune définition du rôle potentiel n'est donné, il est uniquement connu des recherches sur les bases de données et de l'encodage et traitement de vidéo/audio
Dixième Bureau (unité 61886)	Ses missions sont concentrées sur l'Asie centrale et la Russie, mais serait plus de la télémétrie (MASINT dans la définition américaine) et de renseignement électromagnétique.
Onzième Bureau (unité 61672)	Il est également fait état d'une mission centrée autour de la Russie, mais la différence avec le Cinquième Bureau est inconnue.
Douzième Bureau (unité 61486)	Son rôle est centré sur les communications satellites, et il est connu un lien avec le second bureau.

On retrouve dans l'organigramme un bureau d'équipement logiciel et technologique, il coordonne la liaison avec des équipementiers Shanghaiens, et pourrait donc servir de dépôt matériel dans la région de l'Est.

5) Les bureaux de recherche technique et les régions militaires.

En plus de ces bureaux, il existe plusieurs Bureaux de Recherche Technique (TRB), ces derniers servant visiblement à la reconnaissance, à la recherche et à l'analyse technique. Les bureaux opérationnels, qui sont séparés des TRB, étant sous la direction des régions militaires et d'autres services. Ils sont au nombre de cinq, trois pour l'armée de l'air et deux pour la marine.
Ils sont peu documentés et donc ne seront pas abordés, et on se concentrera uniquement sur une description des TRB.

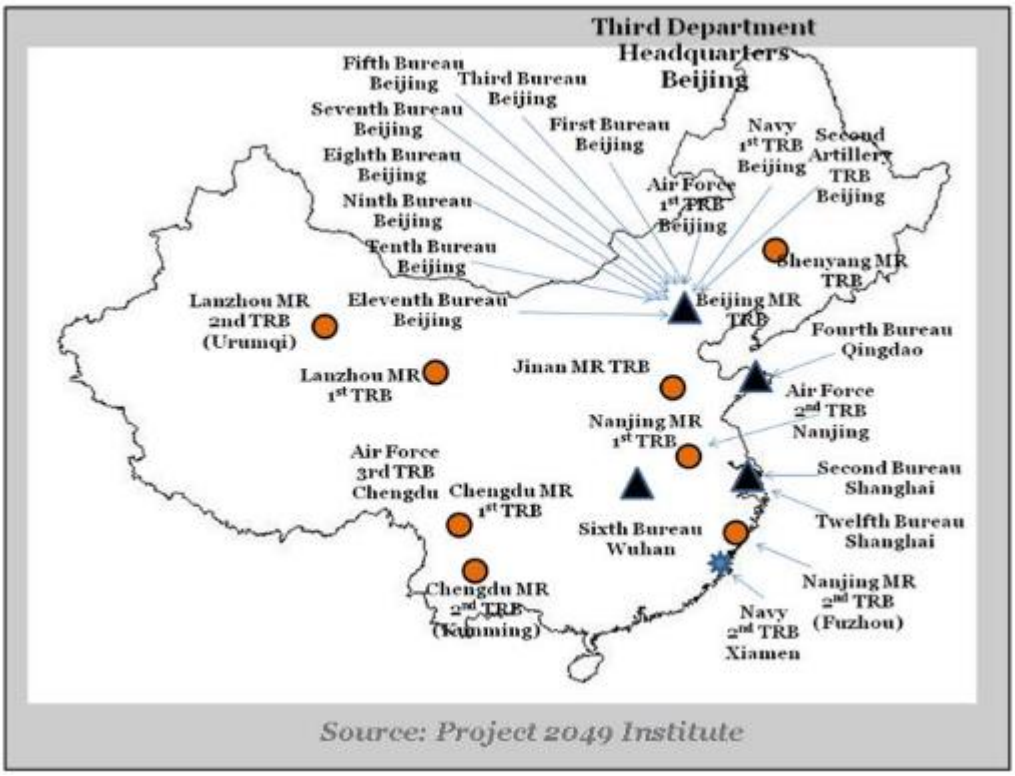
Au niveau général, en termes de formation, les linguistes du Troisième Département et bureaux associés (comme les TRB), sont formés à l'université des langues étrangères de l'Armée Populaire de Libération (解放军洛阳外语学院]), basée à LuoYang. Ils sont ensuite, une fois diplômés, envoyés en entraînement technique spécifique, dans les bureaux cités précédemment.
Quant aux personnels techniques, ils sont formés à l'Université d'Ingénierie de l'Information de l'Armée Populaire de Libération (解放军信息工程 大 学).

Les TRBs des régions militaires sont :

. Région militaire de Beijing, aussi dénommé unité 66407, il semble détenir une expertise linguistique en russe de par la présence de nombreux linguistes russophones.
. Région militaire de Chengdu, aussi dénommé unité 75770, semble étudier les virus et la surveillance réseau, au vu des publications de certains membres rattachés au TRB de cette région militaire.
. Région militaire de Jinan, unité 72959, supervise un ensemble d'environ 670 techniciens et semble être spécialisé sur la Corée et Japon majoritairement, là encore au vues des linguistes rattachés.
. Région militaire de Lanzhou, unité 68002 , il semble contrôler et surveiller par du renseignement électromagnétique les frontières chinoises, au nord à l'ouest et au sud.

. Région militaire de Nanjing, unité 73610. Un de ses TRB semble être spécialisé sur la région de Taïwan.
. Région militaire de Shenyang, unité 65016. Il semble orienté sur la Russie, la Corée, et le Japon.

Là encore, l'institut Project2049 propose une carte de résumé des différents éléments cités, présentée ci-dessous.



6) Le 4eme Département.

Le 4eme département, bien que plus discret, semble également jouer un rôle dans les intrusions informatiques de l'armée chinoise. Il est donc difficile de ne pas le mentionner, même brièvement.
Il supervise en effet le 54ème Institut de Recherche, qui fournit un support en ingénierie et, par exemple, détient quelques liens avec l'entreprise *China Electronic Technology Corporation* (CETC) et ses entités. On y retrouve également, le 29ème Institut de Recherche, le 36ème Institut de Recherche ou encore le 38ème Institut de Recherche.

Ce 54ème Institut de Recherche revient d'ailleurs dans une enquête du FBI et est incriminé pour une intrusion sur des entreprises américaines, ce qui confirmerait un rôle du Quatrième Département dans les intrusions informatiques chinoises.
Pour autant, son rôle exact est difficile à déterminer, de même les sources traitant son sujet sont en général anciennes, ce qui implique que son fonctionnement pourrait être différent de celui qu'il occupait en 2015.

7) Remarques générales sur le GSD.

Le GSD en plus de sa position doctrinale comme acteur important de la communauté du renseignement chinois, possède également un réel impact en pratique.
Par exemple, l'officier de renseignement chinois le plus haut gradé ; soit le responsable des affaires étrangères et du renseignement du GSD, participe au processus politique en dehors de la chaîne de commandement de l'Armée Populaire de Libération, en siégeant au petit groupe de décision sur les affaires étrangères, Taïwan, Hong Kong et Macao. [213]

Il est important de préciser que l'armée chinoise repose en partie sur des milices, bien que leur rôle ne soit qu'explicité plus tard, à tel point qu'elles sont parfois qualifiées de troisième grand corps militaire chinois, derrière l'APL et la police armée (PAPL).
Ainsi, celles en lien avec l'attaque et la défense de réseau informatique devraient être liées au 3eme ou 4eme Département du GSD. Cependant, ce lien n'est pas connu exactement, ni n'est connu le degré de contrôle exact entre ces Départements et les milices.
Mais les milices et le département technique du GSD et le Quatrième Département du GSD sont bel et bien liés, car le district militaire du Sichuan a appelé en 2004 à ce que les milices jouent un rôle plus important dans la guerre informationnelle.
Cependant, cette structure autour du GSD est dépréciée et a subi de multiples réformes depuis 2015, proposant une restructuration totale de l'organisation de l'APL autour des notions de guerre informationnelle.

[213]Mattis P (2015 Decembre 29) China's military intelligence system is changing. *War on the Rocks* https://warontherocks.com/2015/12/chinas-military-intelligence-system-is-changing/

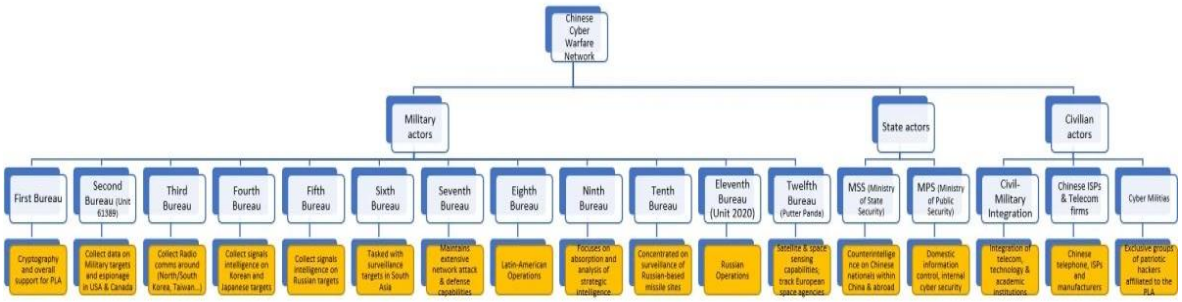


Figure: Chinese network forces
Compiled by @saikirankannan

B) Post-réforme

En novembre 2013, le Comité Central du PCC tenait une assemblée générale sous forme de réunion plénière, annonçant une série de réformes concernant l'APL.

D'abord, une restructuration des zones de défense pour lutter contre le "factionnalisme militaire"[214], passant de 7 Régions Militaires à 5 "Régions de Guerre" ("战区") ou "Théâtre d'Opérations", avec un commandement régional interarmées, toujours contrôlé par un commandant militaire et un commissaire politique. Cette centralisation des commandements de chaque branche devait permettre de simplifier les aléas bureaucratiques[215], dont le PCC avait très bien conscience, et elle s'accompagnait d'une lutte généralisée contre la corruption, déjà mentionnée plus-haut. Elle entraînait avec elle des restructurations supplémentaires propres à chaque force et unité,et étalées sur des années (la force aérienne ne commencera à adopter ces nouvelles mesures qu'en 2017)[216].

Ensuite, les 4 Départements de l'APL étaient morcelés en une quinzaine de structures spécifiques et dédiées à des missions particulières, toutes sous la direction directe et commune de la Commission Militaire Centrale (CMC). La CMC avait d'ailleurs émis un rapport dans ce sens, intitulé "Opinion de la Commission Militaire Centrale sur l'approfondissement de la réforme de la Défense Nationale et des Forces Armées"

[214] Military Regions / Military Area Commands. (s. d.). GlobalSecurity.org. https://www.globalsecurity.org/military/world/china/mr.htm

[215] Lampton, D. M., & Lieberthal, K. G. (2018). Bureaucracy, Politics, and Decision Making in Post-Mao China. *University of California Press.*

[216] Allen, K. W., Mulvaney, B. S., & Char, J. (2020). *Ongoing organizational reforms of the People's Liberation Army Air Force*. Journal of Strategic Studies. https://www.tandfonline.com/doi/abs/10.1080/01402390.2020.1730818

(“中央军委关于深化国防和军队 改革的意见”), explicitant que les réformes n'étaient pas seulement nécessaires pour l’APL , mais pour la Chine toute entière, afin de devenir “un pays socialiste moderne d’ici 2049”.

Enfin, de nouveaux services, ou forces (à comprendre comme “armée”) étaient créés. Le Second Corps d’Artillerie devenait la Force des Fusées de l’APL (中国人民解放军火箭军), regroupant les unités opérant les missiles balistiques (courte et moyenne portée, ainsi qu’intermédiaire) mais aussi les missiles de croisières (longue portée) et surtout les missiles nucléaires, faisant de la Chine le pays à l’arsenal de missiles le plus important au monde[217]. Cette force devenait donc celle des frappes de saturation, pouvant “damner le terrain” à de futures opérations terrestres.

Figure: Inauguration of PLASSF (Strategic Support Force)
Source: Ministry of Defence, China

[217] *Missiles of China | Missile Threat*. (2021). CSIS Missile Defense Project. https://missilethreat.csis.org/country/china/

Cependant, le fait le plus marquant de cette réforme était celle de la création, en 2015, de la Force de Soutien Stratégique de l'APL ("中国人民解放军战略支援部队"), PLASSF en anglais, devenant la cinquième branche des forces armées chinoises (en plus des 3 éléments traditionnels et de la Force des Fusées).

Figure: PLASSF insignia
Source: PLA

1) Création réussie de la Force de Soutien Stratégique de l'Armée Populaire de Libération (PLASSF).

La création de la PLASSF est particulièrement marquante, en ce qu'elle regroupe l'ensemble des nouveaux champs de bataille du 21ème siècle : spatial, électro-magnétique, informationnel et surtout cybernétique (mais aussi psychologique). La République Populaire de Chine devient par la même occasion l'un des premiers pays au monde a pleinement intégré ces nouveaux champs dans une structure dédiée, au sein de ses forces armées.

Cette nouvelle structure a permis de centraliser les dynamiques de *Civil-Military Integration*, ou Intégration Civilo-Militaire (CMI) entre l'APL et ses partenaires et sous-traitants privés, point qui sera développé plus en aval.

Elle a surtout permis d'élaborer une doctrine stratégique sur l'utilisation du vecteur cyber (et spatial) comme supplétif pré-opérationnel et opérationnel pour des guerres de nature cinétique.

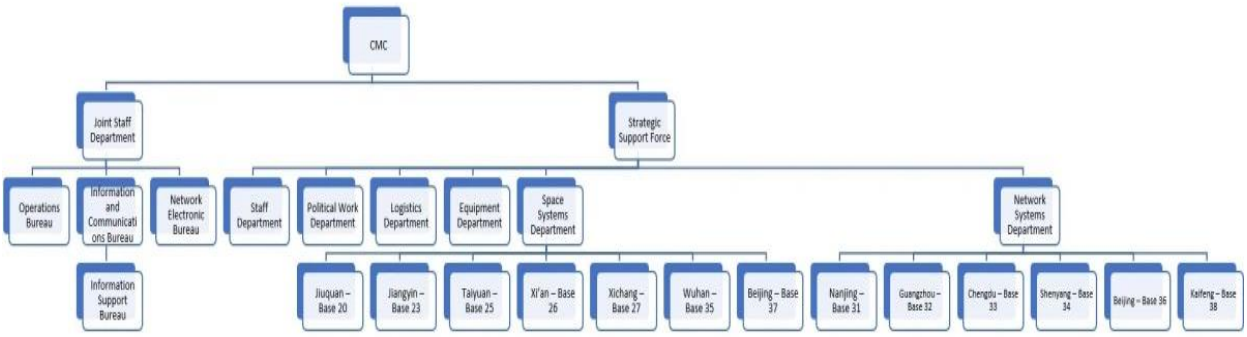


Figure: Organisational and functional chart of PLA Joint Staff Department cyber warfare capabilities and PLA Strategic Support Force (PLASSF)
Source: Compiled by @saikirankannan

Ces guerres, dans les domaines aériens, maritimes, et terrestres, à travers lesquelles la PLASSF devra appuyer les forces engagées, sont appelées "Campagnes conjointes" (联合战役) ou "Opérations conjointes" (联合作战) et les 5 principales[218] sont :

- Joint Firepower Strike Operations against Large Island / Opérations conjointes de frappe de puissance de feu contre une grande île (大型岛屿联合火力突击作战)
- Joint Blockade Operations against Large Island / Opérations conjointes de blocus contre une grande île (大型岛屿联合封锁作战)
- Joint Attack Operations against Large Island / Opérations d'attaque conjointes contre une grande île (大型岛屿联合进攻作战)
- Joint Anti-Air Raid Operations / Opérations conjointes de raid anti-aérien (联合反空袭作战)
- Joint Border Area Operations / Opérations conjointes de zone frontalière (边境地区联合作战)

[218] Easton, I. (2019). *China's Top Five War Plans*. Project 2049 Institute. https://project2049.net/wp-content/uploads/2019/01/Chinas-Top-Five-War-Plans_Ian_Easton_Project2049.pdf

On notera l'ambiguïté du théâtre d'opération que serait "*une* grande île", ou potentiellement, selon la traduction, "*la* grande île", appellation indirecte de Taïwan.

Hors, dans le manuel militaire de 2014, post-réformes, intitulé *Informatized Army Operations* [信息化陆军作战], de la *National Defense University Press* chinoise, il est explicité que dans ces perspectives d'opérations, le cyber est vu à la fois comme un outil et un espace, dont les applications ne sont plus seulement limitées à la collecte d'informations propre au renseignement, mais aussi à l'attaque à travers des cyber-opérations incapacitantes pour l'infrastructure des systèmes d'informations adverses (civiles et militaires, notamment radars), en particulier via le pré-positionnement, que l'on développera plus tard.

Cette crainte de possibles cyber-attaques de la PLASSF contre les infrastructures taïwanaises est d'ailleurs mise en avant par le *National Information and Communication Security Taskforce* de Taïwan (NICST) et sa branche cyber, le *National Center for Cyber Security Technology* (NCCST), à travers un rapport de 2018[219]. Dans ce rapport, il est estimé que l'année précédente, en 2017, 360 cyber-attaques sur des systèmes d'informations gouvernementaux avaient réussies, dont au moins 288 sont directement imputables aux forces armées chinoises. La même année, Taïwan s'inspirait de la PLASSF et créait le *Information, Communications and Electronic Force Command* (Commandement de l'Information, des Communications et de l'Électronique) comme quatrième force à part entière de son armée.

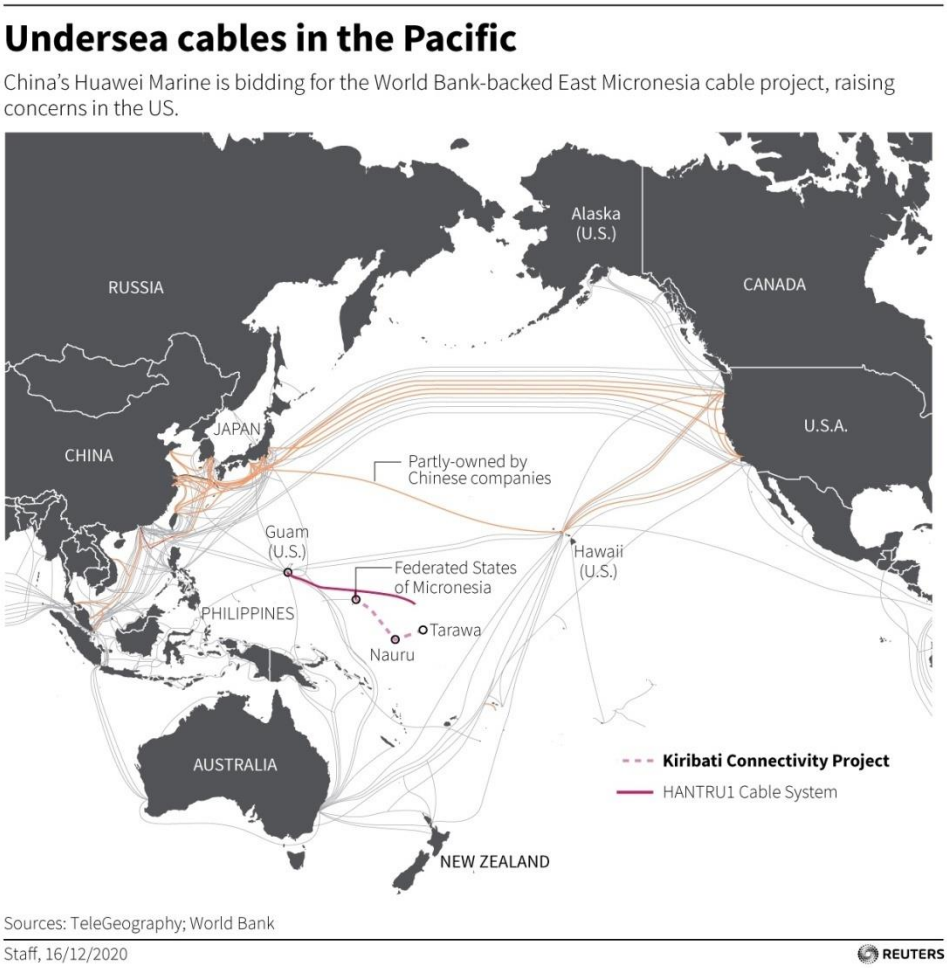
Les applications cyber-offensives de la PLASSF sont donc largement considérées comme une réussite des réformes post-2013 conduites par le PCC, inspirant d'autres pays à reproduire une organisation structurelle assez semblable.
Et c'est à travers une répartition géographique, au sein du territoire chinois, des unités et des tâches, que la PLASSF opère avec succès.

2) Les unités connues (et pas toujours reconnues) et tactiques de la PLASSF.

Si le cyber-espionnage est parfois davantage du ressort de forces de guerre cinétique, comme c'est le cas avec la PLAN (Force Navale) soupçonnée d'espionner certains câbles

[219] Pryor, C. D. (2019). *Taiwan's Cybersecurity Landscape and Opportunities for Regional Partnership*. CSIS.

sous-marins[220](la Chine en possède même certains reliant le Japon et Hawaï), la PLASSF parvient néanmoins presque à monopoliser le leadership des opérations cybernétiques, alors qu'elle dispose d'un nombre assez limité[221] d'unités spécialisées et assignées selon des missions plus codifiées qu'avant la réforme générale de 2013[222].



Début 2021, le général Li Fengbiao était le commandant général de la PLASSF. Le lieutenant-général Shang Hong celui du *Space Systems Department* (SSD) et le lieutenant-général Ju Qiansheng celui du *Network Systems Department* (NSD). Ce dernier est d'ailleurs

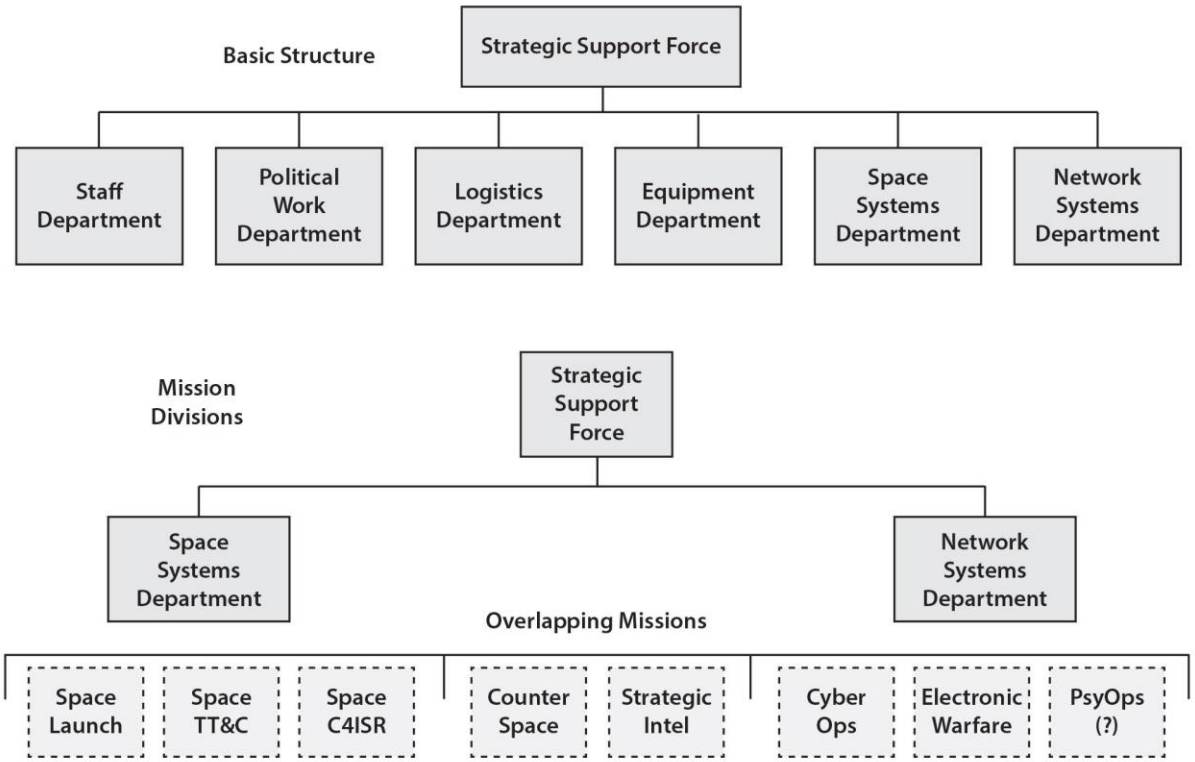
[220] Burdette, L. (2021). *Leveraging Submarine Cables for Political Gain : U.S. Responses to Chinese Strategy*. Journal of Public and International Affairs. https://jpia.princeton.edu/news/leveraging-submarine-cables-political-gain-us-responses-chinese-strategy

[221] Shakarian, P., Shakarian, J., & Ruef, A. (2013). *Introduction to Cyber-Warfare A Multidisciplinary Approach*. Elsevier Science & Technology Books.

[222] Andress, J., & Winterfeld, S. (2014). *Cyber Warfare : Techniques, Tactics and Tools for Security Practitioners. Second Edition*. Elsevier Science & Technology Books.

un élève issu de l'Université de Xidian, classée parmi les meilleures au monde pour… les sciences informatiques. Courant 2021, il deviendra le commandant général de la PLASSF, avec le général Li Wei pour commissaire politique.
Le SSD et le NSD constituent les deux services opérationnels de la PLASSF.

Figure 2. Overall Structure of the SSF



Key: PsyOps: psychological operations; TT&C: telemetry, tracking, and control.

C'est donc sur le *Network Systems Department* qu'il faut s'attarder, puisqu'il est responsable de mener la guerre de l'information avec un ensemble de missions comprenant la cyberguerre, la reconnaissance technique, la guerre électronique, et la guerre psychologique. De ce qui est connu, c'est-à-dire assez peu, le *Network Systems Department* possède au moins 5 bases de "reconnaissances techniques" tournées vers des régions du monde spécifiques :

- Unité 61726 : Ciblant Taïwan.
- Unité 61786 : Focus sur la Russie et l'Asie-Centrale.
- Unité 61486 : Renseignement sur l'Europe et l'Amérique du Nord.
- Unité 61398 : Assez secrète, et non-reconnue par Pékin. Elle est probablement l'APT1 déjà existante depuis 2006.

- Unité 61195[223] : Idem.
- D'autres unités sont suspectées d'exister; Unité 61419[224], Unité 78020, Unité 65017 …

Figure 5. Timeline of PLA Unit 61398's CNE Incidents from 2006–2013

Source: "APT 1: Exposing One of China's Cyber Espionage Units," Mandiant (February 2013), 20, http://intelreport.mandiant.com/.

Certaines unités n'ont effectivement pas d'existence officielle. C'est le cas de la base 311. Comme le précisent également les chercheurs de l'IRSEM, P. Charon et J-B. Jeangène Vilmer dans *Les opérations d'influence chinoises, un moment machiavélien*, : "Plus précisément, le principal acteur identifié dans ce domaine [la guerre d'influence] est la base 311, qui a son quartier général dans la ville de Fuzhou, et qui est dédiée à l'application de la stratégie des « Trois Guerres ». Elle gère aussi des entreprises de médias qui servent de couvertures civiles et un faux hôtel qui est en réalité un centre de formation.". Cette stratégie militaire des Trois Guerres, c'est celle du contrôle de l'information à 3 dimensions : médiatique, juridique et psychologique, dans le but de tromper l'adversaire, mais aussi de manipuler l'observateur-témoin, telle la communauté internationale, en un mot, la désinformation.

On trouve également au sein du NSD :

- Le 58ème Institut de Recherche de Pékin.
- Le 57ème Institut de Recherche de Chengdu[225].
- Le 56ème Institut de Recherche de Wuxi.

[223] Fraser, N., & Vanderlee, K. (2019). *Achievement Unlocked : Chinese Cyber Espionage Evolves To Support Higher Level Missions*. FIREEYE. https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf

[224] INSIKT GROUP. (2021). *China's PLA Unit 61419 Purchasing Foreign Antivirus Products, Likely for Exploitation*. Recorded Future. https://www.recordedfuture.com/china-pla-unit-purchasing-antivirus-exploitation

[225] Fraser, N., & Vanderlee, K. (2019). *Achievement Unlocked : Chinese Cyber Espionage Evolves To Support Higher Level Missions*. FIREEYE. https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf

- Ainsi qu'un ensemble de bases militaires annexes aux fonctions diverses, d'appui opérationnel et de soutien logistique.

Cependant, l'information sur la structuration des différentes unités orientées cyber demeure très limitée, en comparaison des renseignements disponibles sur l'organisation pré-réforme. C'est d'ailleurs là l'une des réussites du PCC, que d'être parvenu à augmenter la capacité de force de cyber-frappe, tout en maintenant grandement confidentielles les unités agissant pour mener ces opérations. En parallèle, la PLASSF forme intensément de nouvelles générations aux problématiques informatiques et spatiales au sein de ses écoles.

Figure: PLASSF INFORMATION ENGINEERING UNIVERSITY
Source: PROJECT2049
Compiled by @saikirankannan

En terme de *Computer Network Operations* (CNO), ou Opérations de Réseaux Informatiques, l'APL a identifié 5 principales procédures et modalités :

Table 2. China's Computer Network Operations (CNO) Strategy Deconstructed

Core Concept	Description	Why?
1. DEFENSE FIRST	CND is the top priority. Once secure, develop "tactical counteroffensives"	*Because United States conducts high-volume CNE operations on Chinese servers*
2. PREEMPTIVE STRIKE ALWAYS	Use preemptive CNA to exploit an adversary's technological vulnerabilities (damaging their ability to respond) or to create more favorable conditions for offensive cyber operations	*Because China faces more technologically savvy adversaries (the United States) in cyber warfare and preemptive strike levels the playing field*
3. COMPUTER NETWORK ATTACK AS AN UNCONVENTIONAL WARFARE METHOD	CNA is used as an unconventional cyber method in the pre-stages of conflict to gain an advantage, but not for ongoing operations	*Because it helps China conduct quick decisive cyber actions in the case that an adversary cuts off China's access to the adversarial networks or fixes their network vulnerabilities*
4. PREEMPTIVE CNA FOR INFORMATION OPERATIONS	Use CNA to win in information warfare and limit or altogether eliminate the possibility of conventional war	*Because China's ability to monitor and conduct information campaigns is highly effective, China can use this skill in cyberspace to prevent war*
5. EXPLOIT AN ADVERSARIAL DEPENDENCE ON INFORMATION TECHNOLOGY IN C4I	Develop Command, Control, Communications, Computers, and Intelligence (C4I) capabilities that do not rely solely on information technology	*Because China believes it is not as technologically dependent as other countries (the United States)*

Adapted from: James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," in *Beyond the Strait: PLA Missions Other Than Taiwan,* ed. Roy Kamphausen, David Lai, and Andrew Scobell (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2009), 259–60, 266, 269; Kevin Pollpeter, "Chinese Writings on Cyberwarfare and Coercion," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (New York: Oxford University Press), 141–42, 145.

Ce qui découle plus largement des nouvelles modalités induites par les réformes du PCC, c'est la naissance en 2019 de la notion d' *"intelligentization"*, et le concept inhérent d'

"*intelligentized warfare*"[226] (智能化战争, guerre intelligentisée) émanant des forces armées chinoises à travers les nouvelles recherches conjointes de la PLASSF et des universités qu'elle parraine. Ce projet futur de l'utilisation poussée de l'Intelligence Artificielle au profit de la recherche puis du traitement de l'information à des fins d'applications dans la guerre cognitique, placent les adversaires du PCC devant un nouveau levier de puissance politico-militaire, face auquel peu de pays étrangers se sont jusqu'à présent préparés.

Dans un rapport de 2021 rédigé par B. Claverie, B. Prébot, N. Buchler et F. Du Cluzel pour l'OTAN[227], les auteurs expliquent en effet :

"Si la culture stratégique chinoise est plus adaptée à la guerre cognitive, l'Occident a facilité la politique chinoise à deux niveaux : l'état de nos démocraties et la culture stratégique occidentale dépassée.

La polarisation au sein des démocraties est une bénédiction pour Pékin. Les gens sont plus susceptibles de regarder les informations qui confirment leur idéologie, plutôt que des informations contradictoires. Les développements technologiques ont amplifié l'importance des informations et des données dans notre environnement de sécurité. L'information est une ressource qui est et sera de plus en plus utilisée pour déstabiliser les pays, en particulier les démocraties.".

II) Caractéristiques des opérations

Les opérations numériques sont partie intégrante de la stratégie chinoise, abordées plusieurs fois par Pékin dans ses stratégies, elles sont en grande partie responsables de la projection de force de la Chine ressentie par les autres pays. Qu'elles soient actives ou passives, les caractéristiques classiques d'une opération permettent de transposer des réflexions de pays autres sur les actions entreprises par le pays du milieu, pour analyser le déclinement stratégique au niveau opérationnel et confirmer les objectifs recherchés par la Chine.

En effet, les opérations s'inscrivent dans un contexte, et ne peuvent être abstraite des différentes stratégies, comme l'IDAR mentionnée précédemment ou encore du droit

[226] Pomerleau, M. (2020). *China moves toward new 'intelligentized' approach to warfare, says Pentagon*. C4ISRNet. https://www.c4isrnet.com/battlefield-tech/2020/09/01/china-moves-toward-new-intelligentized-approach-to-warfare-says-pentagon/

[227] Claverie, B., Prébot, B., Buchler, N., & Du Cluzel, F. (2021). *Cognitive Warfare - La Guerre Cognitique*. NATO-CSO-STO.

international, même si ce dernier n'est pas forcément contraignant, la position d'un pays sur ses questions, vue au prisme de ses actions peut être plus parlant que l'analyse de ses textes doctrinaux.

De même, les différentes actions ouvrent des problématiques qui leurs sont propre, et qui se manifestent après ces dernières, comme la nécessité du traitement de l'information obtenu lors d'opérations numériques, et donc le besoin d'analystes, qui peut être un point d'étranglement, plus encore que l'absence de capacités offensives.

A) Ciblage et pré-opération, volonté stratégique

Toute opération numérique nécessite en amont une phase de ciblage qui déterminera la cible. Celle-ci, primordiale d'un point de vue tant stratégique qu'opérationnel ou tactique, incite à s'attarder sur les opérations des groupes attaquants attribuées à la Chine, pour tenter de déterminer les motivations possibles poursuivies par le Parti Communiste lors de ses opérations numériques.

Une des premières boussoles du PCC est son plan quinquennal, le five year plan, où sont établies des priorités selon les domaines, en fonction des avancements technologiques réalisés et des besoins les plus urgents. Il permet d'orienter les investissements et les actions sur un plan global. Une partie des efforts fournis par la Chine pour atteindre les objectifs fixés par le plan quinquennal se traduit donc en recherches d'informations technologiques, par voie légale ou illégale, ces dernières étant souvent collectées par les groupes d'attaquants liés à l'État chinois. Les secteurs où l'on retrouve de l'espionnage économique mené par des acteurs de la menace chinoise sont si régulièrement inscrits au plan quinquennal, qu'il est estimé exister un lien entre le *five year plan* et des campagnes menées. [228] [229] [230]

1) Le vol des technologies, arme de contournement des sanctions

[228] Emilio Iasiello (2017, septembre) *La stratégie des «Trois guerres » de la Chine ou comment atténuer les retombées du cyberespionnage.* ASPJ Afrique & Francophonie. https://www.airuniversity.af.edu/Portals/10/ASPJ_French/journals_F/Volume-08_Issue-4/iasiello_f.pdf

[229] Health Sector cybersecurity coordination center, office of information security. Department of Health & and human service USA. (06/2021) *China's 14th Five-Year Plan and the Healthcare and Public Health Sector* https://www.hhs.gov/sites/default/files/china-fyp-hph-tlp-white.pdf

[230] F.Plan, V.Cannon et J.Oleavy (08/2021) *APT41: A dual espionage and cyber crime operation. APT41: A Dual Espionage and Cyber Crime Operation | Mandiant*

Cet espionnage permet également de contourner les différentes sanctions visant la Chine, à l'instar de ce que peut faire la Corée du Nord vis-à-vis des sanctions financières et autres embargos. Ainsi, préalablement aux opérations, peut être entrepris un ciblage sur des technologies clés, manquantes encore à la Chine, qu'elle ne peut obtenir par voie conventionnelle.

En effet, par exemple depuis la répression des manifestations de la place Tiananmen, l'Europe et les États-Unis restreignent l'export de technologie lié à l'armement vers la Chine. [231]

Les différentes sanctions économiques et restrictions diverses, accrues et diversifiées lors du mandat de Donald Trump, pourraient potentiellement pousser la Chine, en cas d'impossibilité d'import de matériel ou de propriété intellectuelle, à simplement voler les technologies voulues, chose qui lui est déjà reprochée.

On pourra distinguer plusieurs cas d'espionnage, l'un, abordé ultérieurement, directement étatique, et réalisé par les renseignements chinois et l'autre par de l'espionnage industriel privé, revendu par la suite au Parti Communiste. Cette dernière opération n'est évidemment pas à considérer comme entreprise menée indépendamment, bien qu'issue d'un espionnage par un particulier, mais comme découlant de la volonté du Parti comme le démontre les financements accordés par ce dernier.

On retrouve aussi d'autres cas [232] comme l'espionnage visant Airbus, où, bien que l'attaquant soit relativement sophistiqué (utilisation de 0-day par exemple), il n'était pas suffisamment mature, ni pour être considéré par les chercheurs comme provenant d'un État, ni comme pouvant être sponsorisé par un. [233]

Cela représente un troisième cas, où des attaques opportunistes sont acceptées tacitement par l'État chinois. Elles peuvent être considérées comme une aggravation de la tendance à l'espionnage que peut avoir la Chine, en ouvrant la possibilité aux acteurs privés de prendre des initiatives tant qu'elles sont dans l'intérêt du PCC.

---

[231] M. Pemberton et R.Stohl (2006 novembre) *Wrangling over arms sales to China*, Institut for policy studies https://ips-dc.org/wrangling_over_arms_sales_to_china/

[232] Airbus Defence &Space (2014) *The eye of the tiger* sur archive.org https://web.archive.org/web/20140809013259/https://bbuseruploads.s3.amazonaws.com/cybertools/whitepapers/downloads/Pitty%20Tiger%20Final%20Report.pdf?Signature=OJ2d54rxyligtoMeHrs2A/s1jT0=&Expires=1407549773&AWSAccessKeyId=0EMWEFSGA12Z1HF1TZ82

[233] Cette campagne n'a pas été directement attribuée à une institution gouvernementale chinoise, mais a été très probablement opérée par des ressortissants chinois, soit avec un probable accord tacite des autorités.

Les différents secteurs visés permettent donc un contournement plus simple des sanctions déclarées par la communauté internationale ou certains acteurs isolés. Un parallèle peut être réalisé avec les sanctions apparues sous l'ère Trump, avec de nombreuses restrictions autour de secteurs considérés comme clé ou souverain par la Chine. Parmi eux, on peut cibler les télécommunications avec les sanctions spectaculaires contre Huawei.

2) Les problématiques juridiques liés à la conception d'opérations d'intrusions

Lorsque l'on étudie les intrusions liées à la Chine, il ne semble pas, dans la phase de ciblage, que le pays prenne autant de précautions que ses homologues, comme on pourra le voir plus tard avec l'utilisation absolument indiscriminée de vulnérabilités ou encore lors du déploiement de ransomware après une opération d'espionnage compromise par une détection, ce qui a valu en partie le nom de DoubleDragon au groupe APT41.[234] De plus, on sait qu'une utilisation opportuniste des capacités offensives d'un État peut avoir de nombreux aspects négatifs, parfois dramatiques.

Outre l'interdiction d'utiliser des armes indiscriminées dans le droit international humanitaire, un malware peut avoir des conséquences non prévues lourdes de conséquences. C'est le cas de NotPetya, qui débuta par une infection de M.E Docs solution commerciale très prisée en Ukraine, et qui, très probablement, ciblait l'Ukraine, mais dont les dégâts se répandirent bien au-delà des seules frontières de ce pays, provoquant jusqu'à dix milliards de dollars de dommages. [235]

Ce genre de comportement semblent être proscrit, au moins pour les Etats-Unis, lorsque l'on voit les différents mécanismes de ciblage du malware Stuxnet, qui ne pouvait s'activer que sur la centrale de Natanz, allant jusqu'à utiliser des sources humaines, dans le but d'obtenir des informations discriminantes sur cette centrale, et éviter qu'il ne se déclenche sur une autre.[236]

---

[234] (2021 janvier) *Apt41 (double dragon): A Dual Espionage and cyber crime operation* https://www.mandiant.com/resources/report-apt41-double-dragon-a-dual-espionage-and-cyber-crime-operation

[235] MIKE MCQUADE (2018 aout) *The untold Strory of NotPetya, the Most devastating Cyberattack in Histor*y. wired.com https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[236]Pierluigi Paganini (2019 novembre) *The role of a secret Dutch mole in the US-Isreali Stuxnet attack on Iran*. securityaffairs.com https://securityaffairs.co/wordpress/90698/cyber-warfare-2/dutch-mole-stuxnet-attack.html

Cette préoccupation est source de débat régulier auprès des chercheurs [237] [238] et semble être toujours prise en compte lors des opérations américaines, même hors opérations de renseignement comme cela a été observé lors de l'opération *Glowing Symphony*, les parties prenantes définissant des plans de notification, une liste des missions à accomplir, [239] et un processus complet d'autorisation. [240]
Cela permet aussi une meilleure prise en compte des risques, notamment au niveau du droit international, afin d'éviter de considérer une action numérique comme un acte de guerre, car réalisée par des militaires. Cela est malheureusement à nuancer, des lignes rouges pouvant être franchies même par des acteurs civils. [241]

Cependant, ce manque de considération ouvre la voie pour la Chine à des structures plus innovantes et souples, primordial lors de la constitution d'opérations informationnelles comme on a pu le voir avec G*uccifer 2.0* où la flexibilité du renseignement militaire Russe le GRU a permis en quelques heures de réorienter l'opération entièrement. [242]
À noter, comme déjà expliqué, il est possible que les événements traités ne soient qu'isolés et issus d'erreurs au sein de la conception des opérations numériques, avec une réelle volonté de prendre en compte les problématiques éthiques et juridiques. Mais en l'absence même de reconnaissance de tout acte offensif dans l'espace numérique, et sans doctrine ni textes reconnus comme officiels en la matière, il n'est pas possible de tirer une autre conclusion au vu des quelques éléments en source ouverte.

Cette absence de considération, notamment juridique, permet également une tolérance à l'échec et au risque plus important. Cette tolérance semble en effet assez élevée, même pour

[237] Steven M.Bellovin et Susan Landau (2017, mars) *Limiting the undesired impact of cyber weapons: technical requirements and policy implications* Journal of Cybersecurity https://academic.oup.com/cybersecurity/article/3/1/59/3097802?login=false
[238] Max Sweet (2022 mai) *The extra Mile: What it takes to be a Responsible power*. lawfareblog.com https://www.lawfareblog.com/going-extra-mile-what-it-takes-be-responsible-cyber-power
[239] Anonyme. (2016, 4 novembre). *Department of Defense, « Agreed Operation Glowing Symphony Notification Plan » , November 4 2016, Top Secret. | National Security Archive*. NSA. https://nsarchive.gwu.edu/document/16747-department-defense-agreed-operation-glowing
[240] Anonyme. (2016b, novembre 8). *USSTRATCOM, Subj : FRAGORD 06 to USSTRATCOM OPORD 8000–17 : Authorization to Conduct Operation GLOWING SYMPHONY, November 8 2016, Secret. | National Security Archive*. NSA. https://nsarchive.gwu.edu/document/16749-usstratcom-subj-fragord-06-usstratcom-opord
[241] Nye, J. S. (2021, 8 juillet). *Will Biden's red lines change Russia's behaviour in cyberspace?* The Strategist. https://www.aspistrategist.org.au/will-bidens-red-lines-change-russias-behaviour-in-cyberspace/
[242] Poulsen, K., & Ackerman, S. (2018, 25 octobre). *EXCLUSIVE : 'Lone DNC Hacker' Guccifer 2.0 Slipped Up and Revealed He Was a Russian Intelligence Officer*. The Daily Beast. https://www.thedailybeast.com/exclusive-lone-dnc-hacker-guccifer-20-slipped-up-and-revealed-he-was-a-russian-intelligence-officer

les groupes institutionnels, au vu des pratiques de sécurité des opérations des acteurs de la menace chinoise. Cela est visible à travers l'échange édifiant entre Intrusion Truth, un collectif anonyme réalisant des investigations reliant des intrusions informatique passées à des instituts chinois, et le compte Ren Yuntao sur Twitter [243], où un supposé membre des renseignements chinois, incriminé par le groupe Intrusion Truth, comme participant à des attaques illégales sur des territoires étrangers, a créé un compte dont le pseudonyme était son nom et son prénom, pour répondre au groupe, en leurs demandant si c'était lui qu'ils cherchaient. On pense aussi aux différents serveurs africains envoyant directement leurs données à Shangaï, sans aucune mesure d'anonymisation employée. [244]

3) La recherche de données à caractère personnelle, sacerdoce des opérations

Malgré les différentes opérations d'espionnage que nous avons vu précédemment, il serait faux de dire que la Chine ne réalise que de l'espionnage économique. Comme tout État, une partie des opérations concerne la récolte de renseignements politiques.

En 2014, survient l'intrusion de l'Office of Personal Management (OPM), l'agence américaine qui gère les applications des habilitations de sécurité de toutes les institutions. [245] Ainsi, les données personnelles des personnes habilitées, celles en cours d'habilitation, et les informations sur les familles, amis et autres personnes dont il est nécessaire de parler lors du processus d'habilitation, se virent exfiltrées. [246]

D'autres sociétés impliquées dans le processus, USIS et KeyPoint, qui réalisaient une partie des enquêtes de sécurité, ont également été compromises , ouvrant l'accès illégitime à 22 Millions de dossiers SF-86 (dossiers servant à l'obtention des habilitations) de personnels du

[243] Anonyme, I. (2021b, septembre 10). *Hello Lionel Richie*. Intrusion Truth. https://intrusiontruth.wordpress.com/2021/09/20/hello-lionel-richie/

[244] Kadiri, G., & Tilouine, J. (2018, 27 janvier). *A Addis-Abeba, le siège de l'Union africaine espionné par Pékin*. Le Monde.fr. https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html

[245] Stecklow, S. A. H. (2019, 24 décembre). *Exclusive : Malware broker behind U.S. hacks is now teaching computer skills in China*. Reuters. https://www.reuters.com/article/us-china-usa-cyber-exclusive-idUSKBN1YS0UI

[246] Anonyme. (2019b, octobre 31). *Why the OPM Hack Is Far Worse Than You Imagine*. Lawfare. https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine

gouvernement américain. [247] Sans que ces opérations ne soient directement liées, elles témoignent pour autant, d'un certain objectif, celui d'obtenir des données personnelles. [248]

Les intrusions continuèrent, toujours à la recherche de données personnelles, comme l'opération ciblant Equifax, attribuée également à des chercheurs du 54ème Institut de Recherche, avec cette fois-ci, environ 145 millions de victimes. [249]

De même lié au hack de l'OPM [250] , on retrouve l'intrusion au sein de la société Anthem [251] , où environ 80 Millions de dossiers ont été exfiltrés, par des attaquants liés à la Chine, les différentes affaires d'exploitation et de vol de données continuent donc. [252] [253] [254]

Ces centaines de millions, voire milliards de dossiers comportant des informations personnelles permettent à la Chine de constituer de grandes bases de données, servant ensuite à traquer des agents sous couverture, en recoupant déplacements, salaires, etc, permettant un gain politique. [255]

Dans cette collecte d'informations s'insère également l'espionnage politique visant l'intérieur du pays avec un contrôle des cinq poisons et des trois forces du mal, ou toute autre structure critique envers la Chine. [256]

---

[247] Nakashima, E. (2015, 10 juillet). *Hacks of OPM databases compromised 22.1 million people, federal authorities say*. Washington Post. https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/

[248] Nakashima, E. (2014). *Un sous-traitant du DHS subit une grave violation informatique, selon les responsables*. Washington Post. https://www.washingtonpost.com/world/national-security/dhs-contractor-suffers-major-computer-breach-officials-say/2014/08/06/8ed131b4-1d89-11e4-ae54-0cfe1f974f8a_story.html

[249] Anonyme. (2020a, février 13). *Chinese Military Personnel Charged with Computer Fraud, Economic*. DOJ. https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking

[250] Anonyme. (2015a). *The Anthem Hack : All Roads Lead to China - ThreatConnect | Risk-Threat-Response*. Threat Connect. https://perma.cc/ZNQ5-325G

[251] Anonyme. (2019b, mai 9). *Member of Sophisticated China-Based Hacking Group Indicted for Series*. DOJ. https://www.justice.gov/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including

[252] Harwell, D., & Nakashima, E. (2015, 6 février). *Experts warn that Anthem hack may foreshadow a larger attack*. Washington Post. https://www.washingtonpost.com/business/economy/investigators-suspect-china-may-be-responsible-for-hack-of-anthem/2015/02/05/25fbb36e-ad56-11e4-9c91-e9d2f9fde644_story.html?itid=lk_inline_manual

[253] Anonyme. (2021b, novembre 16). *APT 10 GROUP*. Federal Bureau of Investigation. https://www.fbi.gov/wanted/cyber/apt-10-group

[254] Anonyme. (s. d.). *U.S. Department of Health & Human Services - Office for Civil Rights*. Département Américain de La Santé et Des Services Sociaux. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=2AA5AC876FA56C6924880A515E58025A.ajp13w

[255] Cf note de bas de page 253.

[256] Perlroth, N. (2021, 21 juillet). *Chinese Hackers Infiltrate New York Times Computers*. The New York Times. https://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html

Après s'être attardé sur certains éléments constitutifs d'une opération numérique réalisés en amont de celle ci, il est possible de traiter de leur déroulement et des problématiques qui y sont liés.

B) Opérations et Post-opérations

1) Opération numérique, l'exemple du secteur aéronautique.

Selon certaines sources, les premières opérations numériques d'espionnage sur ce secteur commencent dès 2003, à travers le programme *Titan Rain*, qui visait à subtiliser des secrets industriels américains. Plusieurs cibles sont aujourd'hui connues, comme Lockheed Martin, contractant majeur de l'armée américaine, ciblé par l'opération. Cette dernière était d'une telle ampleur qu'elle a entraîné une réponse de la NSA, qui a entrepris de traquer les opérateurs jusqu'à arriver à la 3/PLA, Troisième Département de l'État-major général de l'armée chinoise. Pour réaliser cette opération, la NSA a utilisé de nombreux moyens pour retrouver les serveurs de commande et contrôle des différents implants, faisant même intervenir l'unité opérant les *Tailored Access Operation*, ou « TAO » pour de la collecte active. [257] Au final l'identité du probable chef de l'opération chinoise a été découverte, permettant une confirmation de la nationalité du groupe d'attaquant.

Ces intrusions dans le secteur aéronautique continuent, avec d'autres opérations, ciblant toujours du matériel militaire, comme le C-17, avion de transport de matériel de l'armée américaine ou encore le F-22, avion de chasse furtif développé par Lockheed Martin ainsi que d'autres technologies américaines clefs.

Ainsi Su Bin, propriétaire de « Beijing Lode Technology Company Ltd », vit une plainte déposée contre lui en 2014, par le *Department of Justice* américain. La plainte a mené à un procès, ce qui a nécessité son extradition en 2016 vers les Etats-Unis, où il plaide coupable. [258]

Les faits reconnus par Su Bin montrent un début des accès illégaux au sein de systèmes d'information d'entreprises américaines dès octobre 2008, et continueront jusqu'en mai 2014 dans le but de voler de la propriété intellectuelle d'entreprises américaines.

---

[257] Anonyme. (2010). *(S//REL)BYZANTINE HADES : An Evolution of Collection*. NSA. https://www.eff.org/files/2015/02/03/20150117-spiegel-byzantine_hades_-_nsa_research_on_targets_of_chinese_network_exploitation_tools.pdf

[258] United States District Court, Central District of California, *United States of America v. Su Bin*. Criminal Complaint. 27 juin 2014. https://www.exportlawblog.com/docs/us_v_su_complaint.pdf

Des informations exfiltrées sont envoyées par mail, visiblement pour un gain financier. En effet d'après le rapport d'enquête du FBI, Su aurait spécifiquement chercher à réaliser un profit sur le transfert des documents.

De plus, il est insensé de concevoir les opérations de renseignement comme des vases clos. Loin de se limiter à des opérations numériques effectuées par des acteurs étatiques ou de la sphère civile, il est également possible d'utiliser des capteurs humains en combinaison. En effet, plus de 2000 investigations sur du contre-espionnage concernant la Chine sont en cours menées par le FBI, [259] et il serait très étonnant de ne pas voir fait état de tentatives de renseignement humain, qu'elles soient à des fins politiques ou économiques, couplées à du numérique.

Une des opérations publiques attribuées à la Chine visait là encore l'aéronautique, révélée lors de l'investigation de la société Crowdstrike sur l'acteur « Turbine Panda ».[260]

Inséré dans la stratégie chinoise, l'élaboration d'un moyen courrier, le C919 est considéré comme un besoin stratégique, afin de pouvoir, à terme, rivaliser avec le duopole occidental actuel.

L'étendue du vol technologique dont est issu cet avion, rend compliqué de le considérer comme une construction indigène chinoise. Cela étant, on peut observer l'importance que ces opérations semblaient avoir, lorsque l'on étudie les différents moyens de renseignement humain mis en place, pour aider les opérations cyber en cours, avec des ressources mobilisées sur plusieurs années.

Cet épisode permet d'illustrer ce qui était le Second Département de l'État-major général de l'armée chinoise, responsable du renseignement humain, qui comptait 50 000 personnes en 2010

2) Une recherche de donnée s'insérant dans une logique de contrôle

Cette institutionnalisation des intrusions et des recherches d'information dépasse largement le cadre des seules opérations numériques et s'insère pleinement dans une large

[259] Anonyme. (2020, 21 juillet). *The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States*. Federal Bureau of Investigation. https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states

[260] Anonyme. (2019). *INTELLIGENCE REPORT : HUGE FAN OF YOUR WORK : How TURBINE PANDA and China's Top Spies Enabled Beijing to Cut Corners on the C919 Passenger Jet*. CrowdStrike. https://passle-net.s3.amazonaws.com/Passle/5c752afb989b6e0f5cda12f4/MediaLibrary/Document/2019-10-18-10-42-26-646-huge-fan-of-your-work-intelligence-report.pdf

campagne visant à instaurer la peur pour quiconque critiquera le régime de Pékin, la phase de collecte et de traitement n'étant plus qu'un élément constitutif de cette stratégie.

Comme il a été évoqué, la recherche de données à caractère personnel est un des éléments les plus constitutifs des attaques informatiques chinoises. Cela se retrouve par exemple lors des célèbres « retours involontaires » [261] ou encore par l'utilisation des réseaux sociaux pour traquer les dissidents et faire pression sur les membres de la famille restés en Chine continentale. [262] Cette traque des ressortissants nationaux des réseaux sociaux internationaux, jusqu'alors une action non réalisée publiquement, mènent les polices à appeler les personnes directement à leur domicile, en leur expliquant leur mauvais comportement et en appliquant des pressions.

Ces "attaques" variées font partie intégrante du contrôle de l'information voulu par le régime, au même titre que les censures sur les réseaux sociaux chinois (Weibo, Douban, etc), les nouvelles technologies de l'information et de la communication étant vues comme une menace si non contrôlées par l'État. Il est également recherché une instauration d'un climat de tension, menant à une autocensure, beaucoup plus simple à gérer pour le régime de Pékin, à l'instar des différentes procédures baillons qui ont été réalisées ces dernières années contre des chercheurs en relations internationales ou encore des journalistes.

Outre la dissidence, cette institutionnalisation se retrouve dans les relations internationales, où la Chine cible sans réel discernement les pays, [263] tant qu'elle a une information à obtenir. Ainsi, on observe des attaques récurrentes sur les pays de l'initiative des routes de la soie (一带一路) en général lors d'événements comme une signature des contrats. [264]

Ces pays insérés dans un projet important pour Pékin, pourraient être insérés dans le ciblage en cercle concentriques, en devenant des laboratoires pour tester les attaques. [265]

---

[261] Anonyme. (2022, 18 janvier). *Involuntary Returns – report exposes long-arm policing overseas*. Safeguard Defenders.https://safeguarddefenders.com/en/blog/involuntary-returns-report-exposes-long-arm-policing-overseas

[262] Xiao, M., & Mozur, P. (2022, 1 janvier). *Chinese Police Hunt Overseas Critics With Advanced Tech*. The New York Times. https://www.nytimes.com/2021/12/31/technology/china-internet-police-twitter.html

[263] Anonyme. (2022a). *Space Pirates : analyse des outils et connexions d'un nouveau groupe de hackers*. Positive Technologies. https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/space-pirates-tools-and-connections

[264] Anonyme. (2018). *Chinese Cyberespionage Originating From Tsinghua University Infrastructure*. Insikt Group. https://go.recordedfuture.com/hubfs/reports/cta-2018-0816.pdf

[265] Charon, P., & Jeangène Vilmer, J. B. (2021). *Les opérations d'influence chinoises*. IRSEM. https://www.irsem.fr/rapport.html Sans que ce rapport ne traite des opérations d'intrusion dans les réseaux, il y décrit cette stratégie en cercle concentriques.

3) Nécessité de traitement des informations collectées, une intégration au sein de la doctrine d'assimilation

Malgré tous les moyens qui peuvent être mis en place pour de la collecte d'information, une utilisation de moyens étatiques à des fins d'espionnage économique nécessite une mise en commun des informations collectées et des passerelles d'échanges vers le monde civil, et de mécanisme de dé-classification de la donnée, sans quoi toute opération devient inutile, constat assez largement partagé par les différentes communauté du renseignement, avec des méthodes diverses pour palier un fonctionnement en silo trop important, comme avec les centres de fusions américains, qui ne porteraient cependant pas satisfaction en l'état actuel des choses. [266] [267]

Pour résoudre les problématiques d'analyse massive des données et décloisonnement de l'information autant entre les entités que du monde militaire vers le monde civil, des moyens importants sont déployés par la RPC. Des centres de diffusions (IAD), sont déployés à travers la Chine. Leur nombre est cependant difficile à déterminer. Un discours de 2006 évoque 400 centres et environ 50000 personnels. [268]

De même il existe sûrement des centres de fusion, lieux où sont mêlées des informations du secteur public et du secteur privé, permettant un décloisonnement et un endroit privilégié pour blanchir des information obtenues lors d'opérations de renseignement.[269] Cela confère un avantage stratégique direct à la Chine, en lui donnant des manières simples de déclassifier de l'information et ainsi faciliter la dissémination du renseignement acquis. Ici, cependant le terme de fusion center est peut être trompeur, car nous n'avons pas connaissance de leur fonctionnement interne, et bien que le terme soit couramment employé, il n'est pas possible de les considérer comme totalement équivalents, en l'absence d'indices crédibles.

Dans cette lignée de partage de connaissance et d'expertise, dans leur livre, William C. Hannas, James Mulvenon, and Anna B évoquent l'existence d'un département chargé de la

[266] Sanchez, J. (2012). *Notre panoptique brisé : un rapport du Sénat conclut que les centres de fusion sont chers et inutiles*. CATO Institute. https://www.cato.org/blog/our-broken-panopticon-senate-report-finds-fusion-centers-expensive-useless

[267] Patel, F., Levinson-Waldman, R., & Panduranga, H. (2022). *A Course Correction for Homeland Security Curbing Counterterrorism Abuses*. Brennan Center for Justice. https://www.brennancenter.org/media/9444/download

[268] Hannas, W. C., Mulvenon, J., & Puglisi, A. B. (2013). *Chinese Industrial Espionage*. Google Books. https://www.google.com/books/edition/_/sWcolDneRrMC

[269] W.E.T.R.O.O.P.E.R.S. (2017, 5 avril). *TR17 - Surprise Bitches ! - The Grugq*. YouTube. https://www.youtube.com/watch?t=2129&v=wP2J9aYM6Oo&feature=youtu.be

rétro-conception de technologies, appelé officiellement le Centre de Transfert National de Technologie de la Chine, avec un début de ses opérations dès septembre 2001, et inséré dans les politiques officielles vers décembre 2007, dans le plan de transfert et de promotion national technologique, permettant là encore de bénéficier d'une aide supplémentaire dans le traitement de l'information collectées en opération, voire d'un département pouvant aider à la planification des opérations illégales de collecte du renseignement. [270]

Outre l'information obtenue de manière illégale lors d'opérations numériques par des services étatiques, il est important de ne pas négliger l'importance de la collecte, et surtout d'analyse en sources ouvertes, permettant de former des analystes en renseignement qui seront compétent pour recevoir de la donnée classifiées en plus d'avoir un réservoir disponible si une information doit être traitée.

De même, chaque année,d'après le directeur du système de librairie numérique de l'industrie du logiciel et de la technologie de la Défense nationale (国防科技工业数字图书馆系统), sont commandés 17 000 périodiques en langues étrangères, avec en prime 127 bases de données, ouvrant ainsi 20 000 journaux et plus de 3000 journaux rétrospectifs. [271]

Pour cela plus de 100 000 travailleurs du renseignement étaient mobilisés, au début du 21eme siècle, un bon important depuis le dernier chiffre public, qui était de 60 000 personnes, chiffre donné par Miao Qihao en 1985.

Outre cette masse d'analystes, on retrouve également une aide étrangère, aidant à ce que la Chine considère comme du "transfert technologique". Par exemple au sein de l'Administration d'Etat d'affaires aux experts étrangers (国家外国专家局, SAFEA), on retrouve des recrutements d'experts étrangers possédant des connaissances dans des domaines sensibles, qui sans forcément s'insérer dans une logique de renseignement, peuvent aider au traitement de l'information à leur insu. Ils peuvent cependant également donner un complément d'information et s'insérer alors dans une logique d'espionnage, comme il a été le cas pour Noshir Gowadia, accusé d'avoir fait fuiter des

[270] Philipp, J. (2015, 14 septembre). *EXCLUSIVE : How Hacking and Espionage Fuel China's Growth*. The Epoch Times. https://web.archive.org/web/20160413012341/http://www.theepochtimes.com/n3/1737917-investigative-report-china-theft-incorporated/

[271] Hannas, W. C., & Chang, H. M. (2021). *China's STI Operations - MONITORING FOREIGN SCIENCE AND TECHNOLOGY THROUGH OPEN SOURCES*. CSET. https://cset.georgetown.edu/wp-content/uploads/CSET-Chinas-STI-Operations.pdf

éléments classifiés sur le bombardier B-2 à la Chine, il aurait rencontré à de multiples occasions des représentants du SAFEA, pour leur donner lesdits documents. [272]
A titre d'exemple l'armée de terre française en 2021, comptait 130 000 personnes dont 25 000 réservistes, ce qui rapporterait le nombre d'analystes servant au traitement de l'information récoltées (par tous les capteurs) à l'ensemble de l'armée de terre, démontrant la capacité importante du traitement du renseignement vis à vis d'autres pays comme la France.[273]

Tous ces éléments montrent donc une vraie volonté de la Chine de poursuivre sa captation technologique au sein de son programme de transfert, répondant à sa doctrine "IDAR".
Cependant il est compliqué d'estimer la réussite que les différents programmes peuvent avoir, là encore, en tant que domaine régalien, très peu d'informations sont disponibles et la Chine publie peu d'informations officielles rendant l'analyse plus complexe. Ainsi il est impossible de se prononcer sur les centres de fusions, critiqués aux Etats-Unis, mais qui pourrait mieux fonctionner dans leur version chinoise.

On observe aussi une vraie volonté de transmettre l'information vers le monde civil, en permettant une déclassification de l'information, et en impliquant les acteurs hors armée (ministères, entreprises ….) dans ce processus de décision des cibles mais également de traitement de l'information de tous types. C'est pourquoi il est nécessaire d'observer l'application de la doctrine de fusion civilo-militaire, voire uniquement du comportement de la sphère civile au opérations numériques chinoises.

III) Fusion civilo-militaire et cyber-mercenariat

La Chine possède plusieurs acteurs militaires, regroupés autour de la force de support stratégique de l'armée populaire de libération. Cependant, nombre de capacités sont détenues par le secteur privé, il a déjà été observé des groupes liés au secteur privé réalisant des attaques pour le gouvernement chinois.

---

[272] Anonyme. (2011). *Hawaii Man Sentenced to 32 Years in Prison for Providing Defense Information and Services to People's Republic of China*. FBI. https://archives.fbi.gov/archives/honolulu/press-releases/2011/hn012511.htm

[273] Anonyme. (2022). *2021-2022 : l'armée de Terre en chiffres*. Defense.gouv. https://www.defense.gouv.fr/actualites/2021-2022-larmee-terre-chiffres

Ainsi, en revenant sur les bases de la doctrine de fusion civilo-militaire défendue par Xi Jinping, on observe une importance, peut être croissante d'entreprises diverses réalisant une partie du travail de l'armée, comme la recherche de vulnérabilité à exploiter lors des opérations. De même un contrôle accru sur les possibilités qu'ont les acteurs privés à disposer de leurs recherches est voulu pour ne pas laisser échapper ces ressources jugées comme stratégiques. Cela mène ainsi à mutualiser des capacités, soit en employant directement des acteurs de la société civile comme milices, dans la continuité de ce qui étaient les milices de la dynastie Qing, la théorie de la guerre populaire développée par Mao ou alors en mobilisant les entreprises pour une aide ponctuelle aux opérations, par exemple dans une logique de réduction des coûts.

A) Acteurs privés

Comme évoqué précédemment, un des éléments doctrinaux de la Chine est le concept de fusion civilo-militaire (军民融合).

Ainsi, plusieurs mesures sont mises en place afin de contraindre le secteur civil à contribuer à la vision stratégique du Parti Communiste, dont celle de l'APL, qui est sous sa direction directe.

L'utilisation de sociétés de sécurité informatique offensives, sert de substitut, palliatif ou d'écran aux services étatiques, et est un point non négligeable de la stratégie du Parti Communiste Chinois.

1) Les entreprises privées, fer de lance de l'APL

Ainsi dès le début des années 2000, des sociétés proposent, à titre privé, des services d'intrusion au sens large (développement de code d'exploitation, de logiciels malveillants).[274] Cela semble également cohérent au vu des dates auxquelles apparaissent les premiers cas d'espionnage industriel supposés étatiques opérés par la Chine.

Dans le même temps, le PCC cherche à canaliser ses talents provenant de la sphère civile afin de monter en compétence sur le plan militaire. Ainsi de nombreuses entreprises se retrouvent

[274] Keizer, G. (2010, 6 décembre). *Chinese firm hired Blaster hacking group, says U.S. cable*. Computerworld.https://www.computerworld.com/article/2514740/chinese-firm-hired-blaster-hacking-group--says-u-s--cable.html

dans des affaires d'espionnage manifestement en étant liées (sous les ordres ou en lien) avec une partie de l'armée populaire de libération. [275]

Se développent alors des pratiques presque mafieuses. A titre d'exemple, au cours de discussions, un membre du groupe fait explicitement état de pratiques criminelles, visiblement en lien avec l'État. Par la même occasion, il essaye de dissuader un de ses associé de cibler la Chine, en évoquant directement le responsable du Ministère de la Sécurité Publique, et arguant être proche du Ministère. Cela confirme la relation de proximité entre milieux criminels et l'État. Cette même personne, poursuivie par le FBI, continua à exploiter des vulnérabilités, surement à titre privé afin de déployer des ransomwares, tout en étant protégé par sa relation avec le Ministère.[276] Outre le Ministère de la Sécurité Publique, l'État dans son ensemble semble maintenir une confiance envers ces acteurs criminels issus de la société civile, en leur permettant de participer à des projets confidentiels, hors du champ de la sécurité offensive, comme le design d'application. [277]

On assiste ainsi à l'apparition/la création de nombreuses sociétés locales, portée par cette volonté de fusion civilo-militaire. [278] Ces entreprises sont plus ou moins proches du Parti, on y trouve même des contractants des services de renseignement (hors renseignement militaire, BoyuSec était contractant pour le ministère de la sécurité d'état) possédant quelques contrats avec le secteur privé, tel Boyusec. [279]

Le Parti développe alors progressivement une réelle expertise dans divers champs du numérique, ce qui est confirmé par l'article de Margin, où l'on retrouve de nombreuses sociétés faisant de la recherche de vulnérabilité. [280]

---

[275] United States District Court, District of Columbia, United States of America v. Jiang Lizhi, Qian Chuan, Fu Qiang. Criminal Case. 27 juin 2014. https://www.justice.gov/opa/press-release/file/1317206/download

[276] Anonyme. (2022a). *APT41, A DUAL ESPIONAGE AND CYBER CRIME OPERATION*. Mandiant. https://www.mandiant.com/sites/default/files/2022-02/rt-apt41-dual-operation.pdf

[277] Cf note de bas de page 278.

[278] The Diplomat. (2019, 24 septembre). *Expanding Cyber Demands Embolden China's Homegrown Cybersecurity Darlings*. https://thediplomat.com/2019/09/expanding-cyber-demands-embolden-chinas-homegrown-cybersecurity-darlings/

[279] Recorded Future. (2017, 17 mai). *Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3*. https://web.archive.org/web/20170517234328/https://www.recordedfuture.com/chinese-mss-behind-apt3/

[280] Anonyme. (2022c). *The Chinese Private Sector Cyber Landscape*. (C) Margin Research. All Rights Reserved. https://margin.re/media/the-private-sector-chinese-offensive-cyber-landscape.aspx

Figure: Cyber Monitoring platform demo of 360 Enterprise Security Group in Beijing
Source: People's Daily Online

Ces sociétés, quelque soit leur domaine d'activité, intéressent également les agences étrangères, comme le témoigne la fuite d'information Vault7 [281], avec les nombreuses vulnérabilités que la NSA possédait sur les différents équipements de sécurité chinois[10] (exemple : pare-feu de la société TopSec).

Outre les sociétés privées qui fleurissent sur le sol chinois, on remarque aussi une "weaponization" de la diaspora et des entreprises qui en sont issues. En effet, on trouve de nombreuses sociétés hors de la Chine continentale, qui servent en réalité de relais aux services d'État ou qui mènent directement des attaques pour le compte du Parti Communiste Chinois.. Le PCC n'hésite pas à faire appel à des ressortissants présents à l'étranger pour coordonner des attaques, y compris sensibles. Ces pratiques, bien qu'il soit difficile d'en estimer le nombre, semblent idéologiquement se rapprocher de la notion de « front uni » développé par la Chine, "front uni" qui semble s'étendre sous Xi Jinping. [11]

Un rapport du *Department of Justice* américain livre en 2014 une vue directe au sein de ces opérations, en relatant le cas de Su Bin, impliqué dans des affaires d'espionnage pour le compte du PCC. Le Parti qui le financera directement, à hauteur de respectivement 350 000£

[281] Anonyme. (s. d.-a). *NSA / CIA*. NSA/CIA. https://www.mpauli.de/nsa-cia.html

pour les diverses infrastructures (noms de domaine, serveurs …), mises en place pour les campagnes d'espionnages et 660 000$ (6.8 Millions RMB et 3.5 Millions RMB équivalent 2011) uniquement pour celles utilisées dans le cadre de la campagne visant à voler les données relatives au projet du C-17 américain.

2) Les opérations numériques, des coûts à réduire.

Cette externalisation permet donc à la Chine de diminuer ses coûts qui peuvent rapidement atteindre des sommes colossales, en finançant uniquement une partie des infrastructures. Il est aussi logique, afin de passer à l'échelle d'opérations ciblant un grand nombre de personnes, d'industries ou d'organisations, que les coûts soient mutualisés avec la sphère civile, que ce soient les implants, utilisés par les groupes d'attaques, les infrastructures ou potentiellement même des compétences autres. [282]

Par exemple, PlugX est un malware apparu publiquement au début de l'année 2008 selon TrendMicro, entreprise de sécurité japonaise. [283]

Depuis son apparition, elle est connue comme servant à plusieurs groupes de menace attribués à la Chine. Dès 2008, des relations fortes étaient faites entre Poison Ivy (autre malware commun à des acteurs attribués à la chine) et PlugX. Il est donc possible de supposer que dès le départ, cet implant a été mutualisé par des groupes chinois. Son évolution depuis lors implique un intérêt continu par cette même communauté sinophone, comme le montre l'implémentation de nouvelles fonctionnalités en 2012 décrite par le CERT national Japonais[284] ou encore une seconde version apparue courant 2014 documentée par Airbus [285]

Il est à noter qu'une fuite de code (constructeur de code) en 2014, reportée par là encore par Airbus[286] permet à toutes les personnes l'ayant récupérée de construire leurs implants PlugX, et donc, depuis lors, il est compliqué d'attribuer systématiquement PlugX à un acteur chinois,

---

[282] Grugq, T. T. (2018, 14 juin). *Cyber : Ignore the Penetration Testers - thaddeus t. grugq*. Medium. https://medium.com/@thegrugq/cyber-ignore-the-penetration-testers-900e76a49500

[283] Ibid.

[284] Anonyme. (2015b, janvier 29). *JPCERT/CC Blog : Analysis of a Recent PlugX Variant - "P2P PlugX"*. PlugX. https://web.archive.org/web/20150222181334/http://blog.jpcert.or.jp/.s/2015/01/analysis-of-a-r-ff05.html

[285] Perigaud, F. (2014, 29 janvier). *PlugX « v2 » : meet « SController »*. Airbus D&S CyberSecurity Blog. https://web.archive.org/web/20141105025231/http://blog.airbuscybersecurity.com/post/2014/01/PlugX-v2%3A-meet-SController

[286] Anonyme, A. C. (2022, 9 mars). *Latest changes in PlugX*. Airbus CyberSecurity. https://airbus-cyber-security.com/latest-changes-plugx/

c'est potentiellement cette raison qui a mené au constat de CrowdStrike en 2014, qui qualifie PlugX de malware le plus utilisé de l'année. [287]

Depuis 2015, cependant apparaît un second malware, qui semblerait t'il depuis 2017, est utilisé par l'acteur Bronze Atlas (dénomination Secureworks, un autre nom connu est APT41).
Son nom, ShadowPad, est dès 2019, repris par des acteurs toujours attribués à la Chine. Dans plusieurs rapports, des liens entre les codes de PlugX et ShadowPad sont mentionnés, à tel point qu'en 2020, l'éditeur d'antivirus Dr Web conclut dans un de ses rapports que ShadowPad n'est qu'une évolution de PlugX.[288]
De manière intéressante SentinelOne, lors de ses investigations, pense avoir identifié les auteurs, et estime également que le modèle entrepreneurial poursuivi est de vendre ShadowPad à des acteurs de manière privé, sous forme de « Malware-as-a-service ». Cela a visiblement eu un impact fort, à tel point que depuis son introduction, la réduction des coûts, de développement et de maintenance des implants notamment pour les acteurs de la menace a mené à plusieurs à abandonner leurs backdoors et à adopter ShadowPad.[289]

Nous avons donc bien affaire ici à une volonté de mutualisation de certaines de ses capacités pour réduire au maximum le coût des intrusions, pour éviter des dépenses inutiles. Cependant, cela rend les familles de malware de plus en plus intriquées, et augmente la mutualisation des capacités entre les acteurs, rendant les attributions des campagnes plus compliquées, supprimant des éléments discriminants.[290]

Dans cette même lignée, il a été aussi été rapporté que des unités de l'APL n'hésitent pas à impliquer des sociétés étrangères. On peut citer par exemple le cas de Sea Gamer Mall,

---

[287] Anonyme. (2014). *Global Threat Intel Report*. CrowdStrike. https://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf
[288] Anonyme. (2020a). *Study of the ShadowPad APT backdoor and its relation to PlugX*. Doctor Web. https://st.drweb.com/static/new-www/news/2020/october/Study_of_the_ShadowPad_APT_backdoor_and_its_relation_to_PlugX_en.pdf
[289] Hsieh, Y. (2021, 2 septembre). *ShadowPad | A Masterpiece of Privately Sold Malware in Chinese Espionage - SentinelLabs*. SentinelOne. https://web.archive.org/web/20210904104753/https://www.sentinelone.com/labs/shadowpad-a-masterpiece-of-privately-sold-malware-in-chinese-espionage/
[290] Yeh, S., & Chang, L. (2022). *THE NEXT-GEN PLUGX/SHADOWPAD? A DIVE INTO THE EMERGING CHINA-NEXUS MODULAR TROJAN, PANGOLIN8RAT*. TeamT5. https://i.blackhat.com/Asia-22/Thursday-Materials/AS-22-LeonSilvia-NextGenPlugXShadowPad.pdf

compagnie malaisienne, qui a reconnu l'implication de deux de ses employés dans une campagne liée à APT 41, acteur de la menace attribué à la Chine. [291]

Cette volonté de réduction des coûts pousse parfois même à la collaboration avec des entreprise privées qui collaborent également avec des acteurs aux intérêts antagonistes. C'est le cas de COSEINC, une société singapourienne, [292] qui coopérait avec la société Qihoo 360, à qui ils ont vendu la conférence Syscan, [293] conférence notoire dans la recherche de vulnérabilité aidant ainsi au repérage des profils intéressants, comme des participants à la conférence faisant de la recherche de vulnérabilité, ou encore en permettant un certain contrôle des informations divulguées lors de ces conférences. Cela est cependant à nuancer, certaines sociétés ne semblant travailler avec la Chine que de manière occasionnelle, comme c'est le cas pour COSEINC, qui pouvait vendre des 0-days à des sociétés européennes.

Il est cependant important de nuancer la partie de réduction des coûts, en effet, en présentant certains cas où des malware ont été créés pour cibler des réseaux spécifiques, montrant que si la situation le nécessite, il existe des malware sur mesure sortant de cette logique de mutualisation des coûts.

A noter, les données forensic d'intrusion des groupes étant rarement publiques, car dévoilant souvent des secrets d'entreprises, on étudiera ici uniquement les malware divulgués et dont des rapports d'analyses publiques sont disponibles, ce qui limite fortement l'analyse au vu des différentes organisations pouvant exister au sein d'un groupe de menace (comme un groupe de développeurs de malwares pour plusieurs groupes distincts et ne communiquant pas, réalisant des intrusions).

En effet, force est de constater également une grande expertise technique de la part de certains acteurs de la menace. Le premier malware que nous aborderons est le malware ciblant le composant UEFI des ordinateurs. L'UEFI pour *Unified Extensible Firmware Interface*, est un composant primordial, permettant, pour simplifier, de démarrer l'ordinateur en réalisant le lien entre le micrologiciel des composants et le système d'exploitation (Windows/Linux ….).

---

[291] Star, T. (2020, 17 septembre). *Malaysia's SEA Gamer Mall confirms two top staff members charged by US in hacking scam*. South China Morning Post. https://www.scmp.com/news/asia/southeast-asia/article/3101937/malaysias-sea-gamer-mall-confirms-two-top-staff-members

[292] Anonyme. (2015b). *WikiLeaks - The Hackingteam Archives*. WikiLeaks. https://wikileaks.org/hackingteam/emails/emailid/695766

[293] Tsyrklevitch, V. (2015, 22 juillet). *Hacking Team : a zero-day market case study*. Tsyrklevich.net. https://tsyrklevich.net/2015/07/22/hacking-team-0day-market/

Initié avant le système d'exploitation, les outils de sécurité n'ont souvent pas la capacité d'inspection de ce composant ci, dû à leur fonctionnement au niveau du système d'exploitation ou du code utilisateur (Kernel-land/User-land). Cependant les différentes contraintes (taille de code, complexité nécessitant des compétences particulières …) font que ces implants ne sont que rarement utilisés, et généralement sur des cibles spécifiques.
C'est ainsi qu'est apparu début 2022, le module MoonBounce, utilisé par l'acteur de la menace APT41, attribué à la chine, ciblant UEFI. [294]
Kaspersky, la société l'ayant découvert, souligne d'ailleurs la technicité de MoonBounce, le comparant aux deux autres bootkit ciblant les micrologiciels, Lojax et MosaicRegressor, démontrant la compétence des auteurs. De plus, dans la campagne étudiée par l'éditeur d'antivirus, ce malware était couplé à d'autres, qui communiquaient avec la même infrastructure. Les autres malwares, déjà connus, étaient lors de leur découverte, également considérés comme des outils de grande qualité nécessitant des gens expérimentés pour les développer. [295]

Cette capacité à réaliser des malwares par des acteurs liés à l'écosystème de la menace chinois se retrouve aussi dans la porte dérobée Daxin.
Daxin, découvert par Symantec, est une porte dérobée fonctionnant au niveau du système d'exploitation Windows (Kernel-Land), qui, même si plus complexe à rendre portable entre les différentes versions. A sa découverte, elle est qualifiée par Symantec comme malware le plus complexe lié aux groupes de menace chinois qu'ils ont découvert jusqu'alors. [296]
Cependant, toutes les fonctionnalités sont loin de toutes être novatrice (le Hook NDIS, sans que la notion soit développée, elle est déjà mentionnée lors d'une conférence, la Black Hat, en 2006[297]), il est donc important de préciser que c'est plus la qualité et les efforts de développement de ce malware qui semblent impressionner Symantec. [298]

---

[294] Lechtik, M. (2022, 26 janvier). *MoonBounce : the dark side of UEFI firmware*. Securelist. https://securelist.com/moonbounce-the-dark-side-of-uefi-firmware/105468/
[295] Hiroaki, H., & Lee, T. (2021). *Earth Baku Returns : Uncovering the Upgraded Toolset Behind the APT Group's New Cyberespionage Campaign*. Security News. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/earth-baku-returns?utm_source=trendmicroresearch&utm_medium=smk&utm_campaign=0821_EarthBaku1
[296] Anonyme. (2022b). *Daxin : Stealthy Backdoor Designed for Attacks Against Hardened Networks*. Symantec Blogs. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/daxin-backdoor-espionage
[297] Tereshkin, A. (2006). *Rootkits : Attacking Personal Firewalls*. Codedgers. https://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Tereshkin.pdf
[298] Cf note de bas de page 299.

Ensuite, au vu des différentes attentions aux fonctionnalités réseau, il est plutôt clair que cet outil est réalisé pour des cibles particulières, qui présentent un bon niveau de sécurité et où il est compliqué d'être persistant ou de se latéraliser. [299]
C'est donc un un malware sophistiqué, spécialisé pour des réseaux durs d'accès, confirmant là encore la possibilité de l'écosystème chinois de réaliser des malwares spécifiques à certains réseaux, ne s'insérant donc pas dans la logique de mutualisation des capacités pour réduire les coûts.

Cela se confirme par d'autres malwares, comme BPFDoor, malware découvert en mai 2022, permet par l'accès au composant Berkeley Packet Filter, BPF, de créer une porte dérobée passive, ne réagissant donc qu'au contact par l'attaquant de la porte dérobée. Ce fonctionnement permet une discrétion accrue, et est confirmée par la structure et les différentes implémentations de fonctions compliquant la détection de BPFDoor.
Ces différentes protections vis-à-vis d'une potentielle détection se confirment par la durée pendant laquelle le malware a existé sans être découvert, 5 ans, ce qui est particulièrement long pour une porte dérobée.
De plus, on voit que BPFDoor était conçu pour cibler des infrastructures particulières, en effet, l'existence de versions pour Solaris SPARC, système plutôt exotique, implique des opérations ciblées sur des zones spécifiques d'entreprises ou administrations.
L'administration de ces implants, réalisés depuis des routeurs compromis, ajoute un élément de preuve dans la volonté d'anonymisation forte des attaquants, la compromission de routeurs rendant en général, plus compliqué le fait de remonter les traces, car ils sont souvent mal configurés pour garder les logs de sécurité et donc aussi souvent plus compliqués à investiguer.
A ce jour, il est impossible de déterminer comment s'insère cette logique de mutualisation des coûts. Ils pourraient être autant privatisés, pour ne pas payer à plein temps des experts en développement de malware, intégrant ainsi uniquement les coûts de maintenance, ou bien être réalisés entièrement en interne, ce qui néanmoins augmenterait les coûts d'exploitation. Les deux cas sont possibles et dépendent de l'orientation et des dynamiques de l'APL au sujet de ses opérations, et de ce qu'elle estime comme primordial pour ses opérations numériques (volonté de contrôle total de toute la chaîne, intégration du civil dans le militaire ou réduction des coûts).

[299] Ibid.

Cette problématique des coûts et de volonté de contrôle ruisselle finalement vers le domaine juridique. En effet une politisation des actes civils en devient obligatoire émane de cette volonté stratégique

3) La politisation de la sphère sécuritaire numérique, une évolution portée par des contraintes juridiques. Le cas des 0-days

Une 0-day est une vulnérabilité inconnue de l'éditeur de solution qui affecte un de ses produits et permet une atteinte non légitime à la confidentialité, intégrité ou la disponibilité des données, comme par exemple par de l'exécution arbitraire de code sur une machine distante, permettant à un attaquant potentiel d'exécuter du code, comme s'il en était propriétaire. Ce sous groupe de 0-days, permettant une exécution de code à distance, est donc un outil privilégié pour des groupes de menaces voulant s'introduire dans un réseau.
Il complique également la détection, de nombreux équipements ou solutions de sécurité n'étant pas conçus ou configurés pour détecter des comportements anormaux que causent les 0-days.
Cet avantage est utilisé par la Chine lors de ses opérations, en effet bien qu'il soit compliqué de comparer l'utilisation que font les différents pays de 0-day dans leurs opérations, on observe clairement dans les opérations numériques chinoise une propension à utiliser des 0-days sur des cibles variées.
Ainsi dès 2006, des officiels du Ministère de la Défense Nationale taïwanais reportent une utilisation de 13 0-day utilisée par l'Armée Populaire de Libération chinoise, ici la majorité semblait cibler des applications Microsoft. [300]

Cette volonté stratégique se retrouve également dans le domaine juridique, où par exemple, de récentes obligations légales restreignent la liberté des sociétés, notamment sur la remontée de vulnérabilités. la Chine force les personnes (physiques ou morales) à ne pas divulguer les vulnérabilités trouvées à l'éditeur pour qu'elles puissent être corrigées, et oblige à les remonter directement au Parti, qui en aura donc la propriété, supposément pour mieux gérer les risques liés à la divulgation au niveau national.
Cette raison avancée par le parti communiste chinois contredit cependant plusieurs voix influentes du milieux de la sécurité informatique, qui militaient déjà en faveur de mesures

[300] Tkacik, J. (2008). *Trojan Dragon : China's Cyber Threat*. The Heritage Foundation. https://www.heritage.org/asia/report/trojan-dragon-chinas-cyber-threat#_ftn28

similaires, comme Zhou Hongyi[301] alors président du groupe 360, dont fait partie Qihoo 360, une des entreprises de sécurité informatique les plus influentes en chine.
Il s'insurgeait contre les compétitions qui visent à remonter les vulnérabilités inconnues par les éditeurs tel que pwn2own. Dans une interview , il parle des vulnérabilités comme d'une « ressource stratégique » (战略资源), en arguant que, de fait, elles doivent rester en Chine, pour développer un avantage stratégique. On voit alors une contradiction complète avec la raison donnée par le Parti dans son explication sur les raisons d'interdiction de divulguer les vulnérabilités découvertes directement aux éditeurs.

D'autres mesures s'imbriquent dans l'évolution juridique chinoise, et montrent une réelle volonté de contrôle de l'ensemble des acteurs réalisant de la recherche de vulnérabilité.
La Chine va par exemple interdire aux ressortissants de participer aux épreuves internationales de sécurité informatique, [302] bien qu'il soit encore complexe d'évaluer ce qui est entendu par la législation chinoise comme épreuve internationale de sécurité informatique. Pour l'instant il semble sûr que l'épreuve pwn2own en fasse partie, comme le montre la création de la Tianfu Cup énoncé précédemment. [303] De même, la création de la conférence DefCon China cherche à résoudre l'impossibilité pour les ressortissants chinois d'obtenir des visas pour se rendre aux US pour la DefCon, conférence extrêmement reconnu dans le domaine de la sécurité informatique, ce qui a été confirmé par le créateur originel de la DefCon, Jeff Moss, au moins en tant que solution temporaire. [304]
On retrouve également une utilisation directe de ces vulnérabilités par le Parti Communiste. Ces mesures semblent donc théorisées comme une coercition de la société civile afin d'en tirer un gain stratégique. En effet, des vulnérabilités remontées lors de la Tianfu Cup se sont retrouvées utilisées dans des campagnes ciblant la minorité ouïghour. [305] L'utilisation de ces vulnérabilités laissent peu de doute quant à l'identité de l'attaquant étant donné que seuls le chercheur, le PCC et l'éditeur ont connaissance de la manière de l'exploiter.

---

[301] Anonyme, S. M. (2017, 12 septembre). 周鸿祎 ：马云提新零售 我想了几个月想到了"大安全". 新浪移动_手机新浪网. https://tech.sina.cn/i/gn/2017-09-12/detail-ifykusey8931658.d.html?vt=4

[302] Yang, Y. (2018, 14 mai). *Chinese hackers defy government warnings at Beijing Def Con*. Financial Times. https://www.ft.com/content/f03995de-5711-11e8-bdb7-f6677d2e1ce8

[303] Anonyme. (s. d.-b). *Tianfu Cup International Cybersecurity Contest*. 品牌策划 ： 神州互动. http://www.tianfucup.com/en

[304] Tangent, T. D. (2019). *DEF CON® China 1.0 Hacking Conference - Speakers*. DefCon.Org. https://defcon.org/html/dc-china-1/dc-cn-1-speakers.html

[305] Beer, I. (2022, 5 juin). *A very deep dive into iOS Exploit chains found in the wild*. ProjectZero.https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html

On retrouve également certaines universités qui se targuent de fournir directement l'APL en vulnérabilités. C'est le cas par exemple de l'université du Sichuan, qui s'en vantait sur sa page d'accueil, montrant un engagement de tous les acteurs de la société civile dans la poursuite d'un but stratégique de l'armée populaire.[306]

Ces différentes éléments remettent donc bien en cause les raisons données par le Parti, et permettent d'argumenter en faveur d'une vraie stratégie offensive poursuivie par le PCC au sujet des vulnérabilités, en plus d'une réelle intégration civilo-militaire dans un domaine précis, celui de la recherche de vulnérabilité.

Cela permet aussi d'argumenter une évolution doctrinale, le pays devenant plus assertif quant à ses capacités, en développant notamment des opérations pouvant presque être attribuées publiquement sans une grande expertise.[307]

Pour conclure sur les 0-days il est intéressant de constater que depuis un certain temps, les 0-days semblent être décloisonnées et partagées par des groupes reliés à la Chine.

Par exemple, une récente faille touchant Microsoft Exchange, service mail proposé par l'éditeur de solution américain, plébiscité par un grand nombre d'entreprises, fut utilisée par plusieurs groupes attribués à la Chine. L'exploitation concomitante par plusieurs groupes d'une vulnérabilité inconnue du grand public laisse peu de place au doute quant à la coopération entre les groupes. [308]

Une précision sur la structure des groupes s'avère obligatoire ici. Il est compliqué d'être absolument certain quant à la structure de ces groupes, bien qu'ils soient rapportés comme distincts par plusieurs entreprises ou gouvernements. Cette séparation se fait en général sur les actes d'intrusions, qui peuvent être menés en effet par des groupes de personnes différentes. En revanche, il est très compliqué d'obtenir une visibilité sur les fonctions dites

---

306 Sichuan University. (2021). *National Cybersecurity Talent Base*. Sichuan University. https://perma.cc/SQ3K-LZKQ

307 Cela diffère donc des précédentes compétitions telles que la topsec, qui aurait ouvert la voie à des opérations sur des pays étrangers, sous forme de capture the flag étudiant, événement visant à réaliser des challenges de sécurité avec des applications et infrastructures vulnérables fictives (voir en ce sens : Nakashima, E. (2015a). *Security firm finds link between China and Anthem hack - The Washington Post*. Perma.Cc. https://perma.cc/37P3-3PSJ ou encore la robot hacking game, (voir en ce sens : Cary, D. (2022, 4 avril). *Robot Hacking Games*. Center for Security and Emerging Technology. https://cset.georgetown.edu/publication/robot-hacking-games/ compétition s'inspirant du Darpa cyber grand challenge, visant à fournir des outils permettant une identification voire exploitation automatique de vulnérabilités informatiques. Ces opérations bien que sûrement utilisées à des fins offensives, n'ont jamais été revendiquées comme des volontés de développer des capacités étatiques nouvelles.

308 Faou, M., Tartare, M., & Dupuy, T. (2021, 12 mai). *Exchange servers under siege from at least 10 APT groups*. WeLiveSecurity. https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

“support” comme la recherche de vulnérabilité ou le développement de maliciels, qui peuvent être partagées entre groupes. Cela remettrait donc en cause le “partage” de vulnérabilité, qui serait existant “de facto” par cette mutualisation, le décloisonnement cité n’existant alors pas le cas échéant.

Nous avons ainsi pu voir l’intégration entre des composantes civiles et militaires chinoises, qui suivent une volonté de fusion des deux mondes, afin de pouvoir maximiser les capacités opérationnelles du parti communiste.

Cependant, nous avons survolé une partie importante de la composante militaire, qui sont les milices, rapidement abordées précédemment. Considéré comme une partie à part entière, au même titre que la police, il est important de s’y attarder, afin de voir l’évolution de son rôle dans les attaques informatiques.

B) L’évolution des milices

Le concept même de milices au service de l’État remonte à la dynastie Qing. Les empereurs, peinant à assurer la gestion intérieure de leur empire grandissant et dans le même temps d’en défendre les frontières, décidèrent de confier certaines missions de police mais aussi d’espionnage et de sabotage à des bandits qui sévissaient dans les villes et surtout dans les campagnes et zones montagneuses[309].

La question de l’utilisation de “cybermercenaires” comme proxies au service de l’État chinois est apparue dès le commencement d’Internet, et a connu 3 phases principales de configuration et reconfiguration, dépendant des présidences successives du Secrétaire Général du PCC.

Une véritable doctrine, propre à l’utilisation et à l’encadrement des cybermercenaires, a été développée par et pour l’APL au sein de l’Académie des Sciences Militaires[310].

Il faut s’attarder un instant sur la nature de cette structure, loin d’être anodine. De son nom complet, l’Académie des Sciences Militaires de l’Armée Populaire de Libération de Chine constitue l'institut de recherche de plus haut niveau au sein de l’APL, think-tank militaire et stratégique à part entière[311].

Établie en 1958, avec son siège Pékin, l’Académie a été la source principale des recommandations faites au PCC quant à l’utilisation offensive des hackers dans le champ

[309] McCord, E. A. (1988). Militia and Local Militarization in Late Qing and Early Republican China. *Modern China*, *14*(2), 156–187.
[310] T. Maurer, (2018) Cyber Mercenaries, The State, Hackers, and Power, *Cambridge University Press*.
[311] *Ibidem.*

cyber, dépassant même ses prérogatives et n'hésitant pas à faire des suggestions quant à leur apport potentiel dans les opérations intérieures (Golden Shield[312]).

Le président de l'Académie, le lieutenant général Yang Xuejun, a pris son commandement depuis juin 2017, assisté par le commissaire politique, le lieutenant général Fang Xiang. L'Académie collabore directement avec la Commission Militaire Centrale du PCC et l'État-Major de l'APL.

Parmi les travaux publiés par l'Académie, ayant trait à notre sujet, on notera notamment "La Science de la Stratégie Militaire[313]", ouvrage doctrinal décennal, ou encore "Localiser le potentiel militaire dans les capacités civiles[314]", document classé dans le dixième plan quinquennal de l'APL, ou enfin "La fusion civilo-militaire[315]", du rapport du onzième plan quinquennal, avec une approche étendue au secteur industriel, et pas seulement aux hackers.

Il faut donc identifier les 3 périodes d'évolution doctrinale majeure pour saisir tout l'intérêt stratégique des cyber mercenaires.

1) 1994 - 2003 : Apparition des premiers groupes hackers et le laissez-faire tacite

D'abord la période de 1994 à 2003, sous la présidence de Jiang Zemin, voit l'apparition des premiers hackers chinois. Le PCC les considère comme des éléments sociétaux néfastes, et les réprime pendant quelques années. En 1997, le premier réseau majeur de hackers apparaît, sous le nom de Green Army[316]. Très vite cependant, un sentiment patriotique fort et prégnant se développe dans la communauté hacker chinoise, donnant naissance en 1998 à la Red Hacker Alliance (dont fera partie la Green Army), en réaction à de violents mouvements socio-politiques antichinois en Indonésie, et résultera en plusieurs attaques simultanées de type spam, DDoS et défacements de sites[317].

Le PCC finit par voir l'intérêt, pour l'instant tactique, de tels groupes volontaristes, qui lui évitent de devoir se positionner frontalement diplomatiquement. Un laissez-faire généralisé envers ces groupes de hackers est tacitement accepté. De nouveaux groupes patriotes

---

312 *Ibidem.*

313 Kumar, M. (2015). *China Finally Admits It Has Army of Hackers*. The Hacker News. https://thehackernews.com/2015/03/china-cyber-army.html.

314 T. Maurer, (2018) Cyber Mercenaries, The State, Hackers, and Power, *Cambridge University Press*.

315 *Ibidem.*

316 Kumar, M. (2015). *China Finally Admits It Has Army of Hackers*. The Hacker News. https://thehackernews.com/2015/03/china-cyber-army.html

317 T. Maurer, (2018) Cyber Mercenaries, The State, Hackers, and Power, *Cambridge University Press*.

émergent donc, tel la Honker Union of China (60 000 membres sur les forums, et 20 000 sur la mailing list), puis la China Eagle Union, fondée en 2000[318], et qui allant encore plus loin exige de ses membres le serment suivant "Je jure solennellement de placer les intérêts de la nation chinoise au-dessus de tout autre chose. Je suis prêt à faire tout en mon pouvoir pour faire s'élever la nation chinoise"[319].

Le contraste entre les hackers chinois, patriotes, et leurs homologues occidentaux, généralement plus critiques et défiants envers leurs États respectifs, tient notamment du fait que les hackers chinois, en tant qu'étudiants dans des universités comme celle Jiaotong à Shanghai, entretiennent des liens étroits avec l'APL, et plus spécifiquement, à l'époque, avec la 3ème Direction[320].

Peu à peu le PCC, prenant conscience de l'énorme potentiel de ses talentueux hackers, se mit à émettre des notifications d'arrestations envers plusieurs hackers, non pour les emprisonner, mais pour utiliser leurs services. Ce fut le cas en 2001[321], lorsqu'après la mort d'un pilote de chasse chinois ayant percuté un avion de reconnaissance de l'USAF, un groupe de hacker (peut-être sous les ordres de Pékin) décida d'une cyber-action punitive contre des cibles US. Le gouvernement chinois finit même par assumer cette nouvelle approche pro-active, quand il refusa à plusieurs reprises de donner suite à des demandes du Japon de fermer des sites de hackers basés en Chine, sous prétexte qu'il ne peuvent le faire "contre des sites patriotiques"[322].

Alors que dès 1999 l'APL évoquait l'idée d'une "Force du Net" composée de "Guerriers de l'Information", il fut décidé en 2002 de donner accès aux hackers à des formations au sein du 4ème Département.

L'objectif était double : D'abord se créer une force vive pour les "futures guerres des réseaux informatiques"[323] à venir. Dans la pure logique de Sun-Tzu, la guerre informatisée avait elle aussi besoin de transformer des paysans en soldats, ou des hackers indépendants en hackers

---

[318] Belk, R., & Noyes, M. (2012). *On the Use of Offensive Cyber Capabilities : A Policy Analysis on Offensive US Cyber Policy*. Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/use-offensive-cyber-capabilities-policy-analysis-offensive-us-cyber-policy.

[319] T. Maurer, (2018) Cyber Mercenaries, The State, Hackers, and Power, *Cambridge University Press*.

[320] *Ibidem.*

[321] Zarate, J. C. (2015). *The Cyber Financial Wars on the Horizon : The Convergence of Financial and Cyber Warfare and the Need for a 21st Century National Security Response*. The Aspen Institute. https://www.aspeninstitute.org/wp-content/uploads/2016/05/Cyber_Financial_Wars.pdf

[322] T. Maurer, (2018) Cyber Mercenaries, The State, Hackers, and Power, *Cambridge University Press*.

[323] *Ibidem.*

d'État. Il fallait donc s'assurer de ressources humaines continues en provenance de la société civile, en faisant miroiter les ressources techniques et logistiques mises à leur disposition.
Ensuite, cela permettait de garder ces hackers, de plus en plus nombreux et influents au sein de la population (adulés comme "nouveaux héros patriotes"[324]). Le PCC considérait que ces éléments, lorsqu'incontrôlés, pouvaient se retourner contre lui : quand les problèmes extérieurs ne seraient plus suffisamment une source de mobilisation, rien ne garantissait que les problèmes intérieurs ne deviennent une nouvelle source d'attaque, cette fois contre l'État. Enfin les hackers étaient aussi considérés comme trop audacieux dans leur volontarisme patriotique.
Effectivement, constatant la faiblesse générale de la sécurité des réseaux informatiques gouvernementaux, plusieurs groupes s'étaient proposé d'aider le PCC à l'améliorer[325]. Ce dernier, déclinant leur offre, avait alors subi une vague d'attaques visant à démontrer cette faiblesse. Une initiative supplémentaire que le Parti n'avait pas appréciée. C'est dans ce contexte que le leader de la Green Army avait d'ailleurs été arrêté. Un statu-quo de tolérance et coopération entre hackers et PCC était donc de mise, qui serait rapidement délaissé au profit d'une capitalisation totale du dernier sur les premiers.

2) 2003 - 2013 : Soutien étatique et supervision générale

De 2003 à 2013, Hu Jintao et le PCC encouragent une formalisation puis une organisation, ou orchestration, des cyber-milices. On estime d'ailleurs que 36% des milices actuelles furent créées entre 2004 et 2006[326]. Des programmes officiels d'études et de financement apparaissent dans une dizaine d'universités (50 aujourd'hui), parrainés par l'APL ou le Ministère de la Sécurité d'État, et rencontrent un succès certain.
Le nombre de hackers à l'époque avoisine les 1 million selon des sources chinoises[327], les 300 000 selon Taïwan. Lorsque l'on demande alors aux élèves de primaire ce qu'ils pensent

[324] Belk, R., & Noyes, M. (2012). *On the Use of Offensive Cyber Capabilities : A Policy Analysis on Offensive US Cyber Policy*. Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/use-offensive-cyber-capabilities-policy-analysis-offensive-us-cyber-policy
[325] T. Maurer, (2018) Cyber Mercenaries, The State, Hackers, and Power, *Cambridge University Press*.
[326] Belk, R., & Noyes, M. (2012). *On the Use of Offensive Cyber Capabilities : A Policy Analysis on Offensive US Cyber Policy*. Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/use-offensive-cyber-capabilities-policy-analysis-offensive-us-cyber-policy
[327] *Ibidem.*

des hackers, 43% les “adorent” et 33%[328] veulent également devenir hackers. Leur popularité est totale.

L’Académie des Sciences Militaires est en charge de la supervision générale et du recrutement[329]. Pour ce faire, elle lance des compétitions de hacking. Elle crée également ses premières unités de guerre de l’information. Parallèlement, le Ministère de la Sécurité Publique poste des offres de recrutement sur des forums tels Xfocus ou EvilOctal de 2007 à 2008[330]. Cette période coïncide avec la diffusion plus large des premiers témoignages de hackings[331] par des entités étatiques, et non plus par des éléments civils indépendants.

Dans le même temps, le PCC se refuse à toute coopération internationale en matière de répression des crimes informatiques, mais aussi à toute forme de coopération universitaire et scientifique en la matière. Le cyber devient un enjeu d’État.
Illustrant l’agressivité accrue de ces groupes formés, parrainés et encadrés par l’État, le NCPH (Network Crack Program Hacker), composé d’au moins 7 étudiants chinois, parvient en 2006 à s’introduire dans plusieurs agences gouvernementales des USA, y compris le Pentagone[332]. Quelques années plus tard, l’un des membres fondateurs du groupe, Tan Dailin, aussi connu sous l’alias “Wicked Rose”, reconnaîtra avoir agi sous les ordres de commandements militaires régionaux, celui de Sichuan puis de Chengdu[333]. Parallèlement, il percevait de l’argent d’une société privée anonyme, lui permettant de faire ces opérations sur son temps de cours à l’université, une pratique déjà abordée en amont.

Les cyber-opérations des milices de l’APL sont alors grossièrement divisées entre CyberDéfense et CyberAttaque. Et, bien qu’agissant sous les ordres de l’APL, plusieurs milices sont placées au sein de sociétés “privées”, souvent elle-mêmes créées par l’État, tel le

[328] T. Maurer, (2018) Cyber Mercenaries, The State, Hackers, and Power, *Cambridge University Press*.
[329] *Ibidem.*
[330] *Ibidem.*
[331] Belk, R., & Noyes, M. (2012). *On the Use of Offensive Cyber Capabilities : A Policy Analysis on Offensive US Cyber Policy*. Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/use-offensive-cyber-capabilities-policy-analysis-offensive-us-cyber-policy
[332] T. Maurer, (2018) Cyber Mercenaries, The State, Hackers, and Power, *Cambridge University Press*.
[333] *Ibidem.*

groupe Nanhao[334]. Les employés les plus jeunes (généralement moins de 30 ans) rendent régulièrement des services à l'APL, tout en travaillant officiellement pour l'entreprise à laquelle ils sont rattachés. De même que les étudiants encore à l'université sont rattachés à des classes spécifiques, mais reçoivent régulièrement des commandes pour des opérations ciblées. Ce sera le cas avec l'opération Aurora, avec pour cible, entre autres, Google[335]. Encore une fois, l'Université Jiaotong sera au cœur de l'attaque.

Ces attaques, de par leur nature, deviennent donc plus offensives et intrusives. Alors qu'elles se limitaient à des effacements de sites Web et des DDoS lors de la période précédente, sous Hu Jintao on voit augmenter le nombre de vols de données, sur des cibles toujours plus audacieuses.

Seule la règle première des hackers chinois continue d'être appliquée, à savoir ne pas hacker chez soi. Et lorsque certains y dérogent, le PCC punit immédiatement, dissuadant d'autres tentatives de cyber-aventurisme intérieur. Ce sera le cas de Wicked Rose quelques années après son coup d'éclat lors d'Aurora, qui sera arrêté et condamné à plusieurs années de prison ferme pour avoir pour des activités "cybercriminelles" visant des entreprises chinoises[336].

3) 2013 - 2022: Renforcement du contrôle et spécialisation

La période actuelle, dernier volet de cette réorganisation, commence donc en 2013 lorsque Xi Jinping devient le nouveau chef d'État chinois. Deux éléments circonstanciels majeurs sont alors observables : tout d'abord qu'en 10 ans, la part de la population chinoise ayant accès à Internet est passée de 10%, en 2003, à 50%, en 2013[337].

Ensuite, qu'à l'inverse de ses prédécesseurs, Xi Jinping ne semble pas vouloir lutter contre la corruption pendant seulement 1 an ou 2 dans une logique politicienne, mais va en faire une lutte continuelle contre ce qu'il estime être un fléau systémique en Chine[338]. Ce combat anti-corruption va s'étendre jusque dans des cercles généralement intouchables, les hautes sphères politiques et économiques. Le cyber n'est pas exempté[339].

---

[334] Zarate, J. C. (2015). *The Cyber Financial Wars on the Horizon : The Convergence of Financial and Cyber Warfare and the Need for a 21st Century National Security Response*. The Aspen Institute. https://www.aspeninstitute.org/wp-content/uploads/2016/05/Cyber_Financial_Wars.pdf

[335] T. Maurer, (2018) Cyber Mercenaries, The State, Hackers, and Power, *Cambridge University Press.*

[336] *Ibidem.*

[337] *Ibidem.*

[338] *Ibidem.*.

[339] O'Connor, T. (2011). The Jester Dynamic : A Lesson In Assymetric Unmanaged Cyber Warfare. *GIAC.*

Cela va permettre à Xin Jinping de s'assurer d'une efficience accrue des différentes milices sous le contrôle resserré du PCC.

En 2014, Xin Jinping crée un "Groupe Dirigeant Centralisé pour la Cybersécurité et l'Informatisation" au sein du comité central du PCC, chargé de superviser l'ensemble des activités cyber et les directions politiques à leur donner. Une des pistes de réflexion envisagée est alors la possibilité d'une utilisation dévastatrice des réseaux sociaux dans la diffusion d'informations confidentielles, comme c'était le cas pour l'affaire Snowden en 2013. Ce groupe réfléchit donc aux moyens de se prémunir d'une telle possibilité en interne, tout en pouvant l'exploiter en externe. Ce Groupe sera plus tard renommé Commission Centrale des Affaires de Cyberespace (CCAC) avec un plus grand focus sur la surveillance et l'anti-dissidence intérieure.

C'est à la même époque que les premiers manuels doctrinaux de l'Académie sont diffusés publiquement. Pour la première fois, l'APL assume pleinement et ouvertement ses

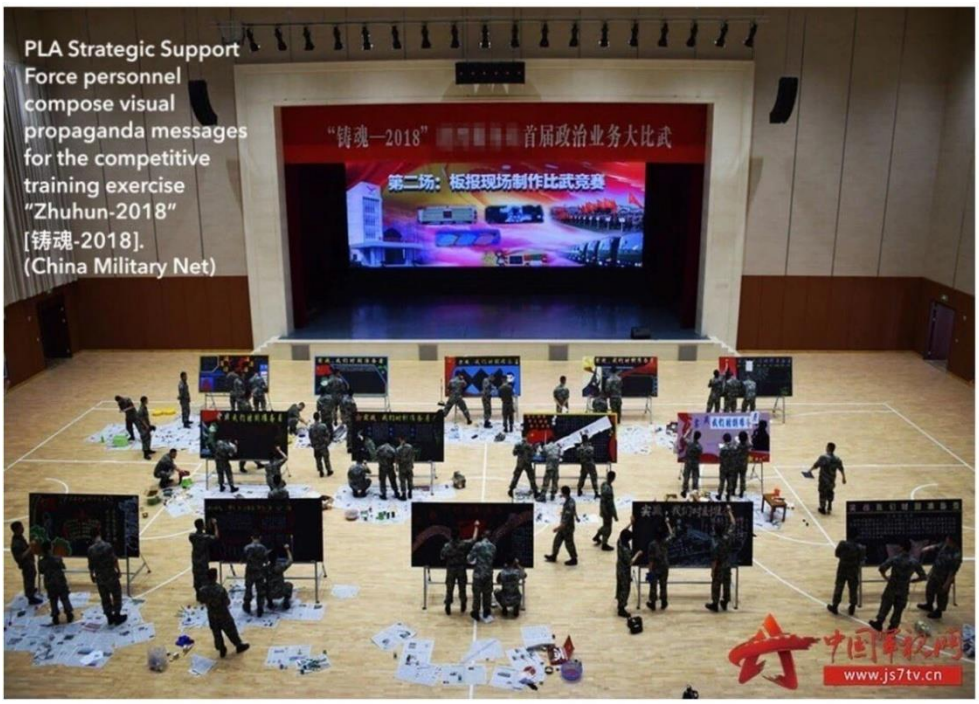


Figure: PLASSF (Strategic Support Force)
Source: Ministry of Defence, China

manœuvres cybernétiques.

Mais il est également décidé de déléguer certaines tâches à des milices spécifiques, qui seront alors réparties en 3 grands ensembles avec des niveaux d'autonomie différents[340] :

Les forces professionnelles de guerre de réseau.

Elles sont constituées d'unités opérationnelles des forces armées, employées pour mener des attaques-réseaux extérieures et de la défense infrastructure réseaux intérieure.

Figure: PLASSF (Strategic Support Force)
Source: Ministry of Defence, China

- Les forces autorisées.

Ce sont des forces étatiques organisées localement, et autorisées par les forces armées (parfois sous leur supervision relative) à participer à la cyber-guerre. Elles sont généralement intégrées à des services et directions spécifiques au sein de Ministères, principalement le Ministère de la Sécurité d'État (MSS), le Ministère de la Sécurité Publique (MPS), et dans une moindre mesure de l'Administration du Cyberespace de Chine (CAC), cette dernière dépendant directement du CCAC et chargée de l'application pratique de ses orientations, sorte d'ANSSI chinoise.

[340] T. Maurer, (2018) Cyber Mercenaries, The State, Hackers, and Power, *Cambridge University Press.*

S'il est vrai que le MSS a quelques prérogatives concernant le renseignement extérieur, ce n'est pas le cas du MPS et encore moins du CAC, qui peuvent néanmoins servir de supplétifs à l'APL pour des opérations particulières. Cependant, leur rôle est avant tout tourné vers la sécurité intérieure, au sens chinois du terme, recouvrant donc largement les opérations de surveillance et répression, influence et propagande, etc.

- Les forces civiles.

Ces dernières sont des forces non-gouvernementales menant spontanément des cyber-opérations offensives ou défensives dans et pour l'intérêt général de la RPC, avec l'assentiment du PCC. Elles peuvent être mobilisées dans le cas de besoins particuliers pour certaines cyber-opérations. Elles sont finalement les héritières idéologiques et structurelles des premières cyber-milices.

Cette restructuration s'accompagne également d'un cyber-contrôle intérieur renforcé suite aux printemps arabes. Craignant une contagion, à juste titre puisque quelques révoltes apparaissent sur son territoire, Pékin décide de formuler de nouvelles interdictions et obligations quant à l'utilisation d'Internet. Pour les appliquer, le PCC se sert des cyber-mercenaires / cyber-miliciens pour assurer une veille accrue et des rapports quotidiens auprès des Ministères concernés[341]. Fort du succès général de cette restructuration, la Chine ira même jusqu'à envoyer des conseillers en Iran pour l'aider à créer le Réseau d'Information National, un intranet iranien dont le développement commencé en 2013 sera achevé en 2016.
Il faut toutefois relever une exception notable à la protection des ses hackers qu'applique en général le PCC[342]. Lors de la visite de Xi Jinping aux USA en 2015, la Chine consent à arrêter les responsables des attaques contre le Bureau de Gestion du Personnel US, dans l'affaire déjà évoquée en amont. Ce geste diplomatique provoquera une certaine confusion au sein du PCC et plus largement en Chine, et demeurera donc un cas assez isolé.

En effet, si la Chine tente un apaisement avec les USA à partir de 2013, sous la volonté commune d'Obama et de XI Jinping, en diminuant d'abord son espionnage économique, et en arrêtant ensuite certains de ses hackers, cette période finit après l'élection de Donald Trump. Alors que la création de la Force de Soutien Stratégique pouvait apparaître comme un

[341] *Ibidem.*
[342] Raud, M. (2016). *China and Cyber : Attitudes, Strategies, Organisation*. NATO-CCDCOE. https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf

choix de centralisation et de contrôle des diverses cyber-forces, elle devient finalement une nouvelle arme offensive contre les adversaires de la Chine, servant d'organisation-parapluie aux différentes milices.

Les récentes attaques contre Microsoft Exchange et même contre le FBI démontrent sans ambiguïtés le retour de l'agressivité chinoise dans le cyberespace[343].
Néanmoins, le choix du PCC de tant vouloir incorporer ou superviser ces milices démontre également sa méfiance quant à leur existence même, et son incapacité à contrôler la venue de nouveaux hackers. Les cyber-milices civiles ne représentent finalement que moins d'un pour cent du total des milices chinoises (alors qu'on retrouve environ 10 000 000 de personnes, toutes milices confondues[344]), une grande partie des hackers demeurent donc indépendants du PCC. Parallèlement, la cybercriminalité intérieure continue d'exister : un frein à l'expansion de la cyberpuissance chinoise, corrélé à un ensemble de limites plus larges.

IV) Défis et menaces, les freins aux velléités cyber-offensives chinoises

Malgré ses capacités avérées en termes de cyber-opérations, la Chine se voit contrainte et limitée dans la potentialité d'accroître sa puissance plus encore, et ce pour deux raisons principales.
D'abord parce qu'elle conserve des manques importants dans son industrie numérique, et que, malgré une jeunesse patriote et talentueuse[345], elle ne parvient pas encore à être entièrement indépendante sur le terrain cybernétique. C'est sans compter sur les difficultés répétées d'une cohésion d'État en la matière.
Ensuite, parce que l'audace et la ténacité répétées de ces attaques ont fini par engendrer une hostilité croissante à son égard, de la part de concurrents et adversaires internationaux qui, encore soucieux du Droit et de "jouer dans les règles" n'ont pas appliquer de manière systémique de telles politiques d'offensivité numérique. Cela ne signifie pas pour autant que

[343] *Ibidem.*
[344] T. Maurer, (2018) Cyber Mercenaries, The State, Hackers, and Power, *Cambridge University Press.*
[345] Raud, M. (2016). *China and Cyber : Attitudes, Strategies, Organisation*. NATO-CCDCOE. https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf

d'autres États ne seraient pas en mesure de rendre la pareille à la Chine, et c'est pour l'instant sur les terrains médiatiques et juridiques que s'observe cette réaction internationale.

A) Limites endogènes

Il serait hasardeux de voir le PCC comme une machine de guerre sans contradictions intérieures. Les rouages du système d'organisation touchant au cyber ont tendance à s'enrayer dès lors qu'il s'agit de diviser le pouvoir pour mieux gérer les applications propres au champ cybernétique. C'est là une forme de corruption qui parfois n'est pas tant de nature économique mais davantage fondée sur les rivalités et le monopole politique. Les divers responsables de commissions au sein du PCC se sont déjà par deux fois opposés à Xi Jinping[346] quant à la création d'un Conseil de Sécurité Nationale sur le modèle américain.

Il faut ajouter à cela l'incapacité latente de la Chine à produire certains composants électroniques spécifiques mais pourtant stratégiques : un exemple marquant est l'utilisation à 80% de technologies étrangère[347]s pour ses systèmes de contrôle industriels. Un pourcentage à la hausse.

Ce retard technique, qui tend à décroître tant grâce à la recherche qu'à l'espionnage industriel massif, est toutefois corrélé à la corruption latente au sein du PCC.

1) Corruption intérieure et divergences

En effet, les jeux de pouvoir et de rivalités, endémiques à un parti unique, freinent les capacités de développement chinois en matière de cyberpuissance. Contrairement à une certaine image faussée, Xi Jinping n'a pas encore totalement les pleins pouvoirs. C'est là le paradoxe structurel même du PCC : son secrétaire général le dirige, et par extension gouverne l'État chinois, mais n'en demeure pas moins élu par le Comité Central du Parti. Hors, si le secrétaire général peut orienter une certaine ligne politique, il doit néanmoins appliquer les décisions collégiales prises par ce même comité qui l'a élu. Cependant, les récentes réformes institutionnelles prises au cours des derniers congrès du PCC tendent à renforcer le monopole du pouvoir pour Xi Jinping[348]. De plus, cumulant plusieurs fonctions dirigeantes au sein

[346] T. Maurer, (2018) Cyber Mercenaries, The State, Hackers, and Power, *Cambridge University Press.*
[347] *Ibidem.*
[348] Al Jazeera. (2021). *China : Communist Party passes resolution on history to elevate Xi*. https://www.aljazeera.com/news/2021/11/11/china-communist-party-passes-resolution-on-history-to-elevate-xi

d'autres comités ou commissions, Xi Jinping, et plus largement les leaders du PCC, sont soumis aux guerres d'influence entre et au sein de ces comités et commissions. Déjà par deux fois, le prédécesseur de Xi Jinping, Hu Jintao, avait tenté de modeler une nouvelle agence de coordination du renseignement et de sécurité, sans succès[349]. Confronté à la levée de boucliers de plusieurs membres éminents du Parti, craignant de perdre leur pouvoir au sein d'entités séparées et disparates, Hu Jintao avait dû renoncer. Si le nouveau sécrétaire général a fini par créer la *Commission Centrale pour la Sécurité Nationale*, il a dû le faire aux dépends de la sécurité extérieure, cette commission ne se focalisant que sur les 3 Grands Maux intérieurs (terrorisme, séparatisme, extrêmisme religieux). Pour temporiser et trouver une solution par intérim, Xi Jinping est obligé de recourir à d'énièmes manoeuvres politiques, comme par exemple la nomination de Lu Wei, ancien chef adjoint du *Département de la Propagande du Comité Central* du PCC, à la tête du *Groupe Dirigeant Centralisé pour la Cybersécurité et l'Informatisation*[350]. Cette nomination souligne l'approche toujours concentrée sur la sécurité de l'information et la priorité au contenu, permettant de donner au Groupe le prisme que devrait avoir une agence centralisée, avec une approche élargie au renseignement extérieur.

Le constat semble néanmoins à nuancer tant l'emprise de Xi Jinping semble se renforcer autour du contrôle de l'APL [351], ce qui est confirmé par plusieurs analystes, certains mettant justement en lumière le regain de contrôle de Xi vis à vis de Hu, réputé pour mal contrôler l'APL[352].

De même, il est indéniable de constater que la corruption est un mal identifié par le Parti qui cherche à la traiter, elle est même définie comme une des plus grandes menaces pour la Chine en particulier depuis Xi.

Ainsi lorsque Xi Jinping déclare qu'il n'épargnera « ni les tigres ni les mouches », on constate une réelle volonté de lutte contre ce phénomène endémique, qui inspire les pires

---

[349] T. Maurer, (2018) Cyber Mercenaries, The State, Hackers, and Power, *Cambridge University Press.*

[350] *Ibidem.*

[351] Anonyme. (s. d.-a). *ICS- Institute of Chinese Studies : « China's military reforms to tighten Xi Jinping's grip on PLA »*. Institute of Chinese studies. https://www.icsin.org/chinas-military-reforms-to-tighten-xi-jinpings-grip-on-pla

[352] Zhen, L. (2018, 20 juillet). *Chinese military overhaul to tighten Xi Jinping's grip on armed forces, say analysts*. South China Morning Post. https://www.scmp.com/news/china/diplomacy-defence/article/1900493/chinese-military-overhaul-tighten-xi-jinpings-grip

craintes du Parti, notamment sur la notion de décadence, la notion de déclin étant chère aux cadres du Parti. [353]

Cette corruption touche évidemment les armées, on note souvent le cas des généraux Guo Boxiong et Xu Caihou, parmi les premiers à être visés dans les campagnes anti-corruption menées par Xi Jinping. Cela diminue grandement l'efficacité des structures existantes menant des opérations, et laisse supposer des débordements résultant de cette corruption. Même si cela est compliqué à prouver, il est probable que certains débordements constatés lors d'opérations, puissent être attribués au moins en partie à de la corruption, comme par exemple lors d'actes visiblement incontrôlés menant à des séries d'exploitations de vulnérabilités sans but stratégique apparent. [354]
Au même titre, on retrouve des purges au sein des instances de renseignement chinois, confirmant l'étendu du problème, touchant toutes les sphères gouvernementales. [355]

Dans le registre de la réponse à ce mal, on constate des mesures encore imparfaites et très souvent menées pour des raisons politiques, même dans le cas des deux généraux cités, qui étaient cependant incontestablement corrompus. [356]

Cependant, on observe une volonté du parti communiste d'améliorer et de dépolitiser, dans une certaine mesure, les procédures anti-coruption. La récente réforme de la Commission Centrale d'Inspection de la Discipline (CCDI) s'inscrit dans le cadre de ces améliorations. Elle se place depuis lors sous la responsabilité de la Commission Nationale de Supervision. Cela la ramène sous le coup de la loi, alors qu'elle ne l'était pas, et pouvait donc réaliser des enquêtes extra-légales. [357] C'est peut être une des raisons pour laquelle des méthodes, comme la double désignation ont été supprimées, et va donc peut être permettre de réduire la dimension politique des enquêtes, en créant une certaine standardisation des procédures, qui n'était pas forcément respectées

[353] Courmont, B. (2016). *La lutte anticorruption en Chine : « la chasse aux tigres et aux renards »*. Cairn.info.https://www.cairn.info/revue-internationale-et-strategique-2016-1-page-131.htm
[354] Ibid.
[355] The Economist. (2021, 4 mars). *China's domestic-security agencies are undergoing a massive purge*.https://www.economist.com/china/2021/03/01/chinas-domestic-security-agencies-are-undergoing-a-massive-purge
[356] Lowsen, B. (2016, 16 juin). *The True Crimes of Chinese PLA General Guo Boxiong*. The Diplomat. https://thediplomat.com/2016/06/the-true-crimes-of-chinese-pla-general-guo-boxiong/
[357] The Economist. (2021b, juin 29).*The anti-graft unit of China's Communist Party has grown in power*.https://www.economist.com/china/2021/06/12/the-anti-graft-unit-of-chinas-communist-party-has-grown-in-power

Mais la corruption des élites chinoises n'est pas la seule vulnérabilité intérieure du Parti. Plusieurs cadres et officiers issus des Ministères, face à l'agressivité croissante du gouvernement envers les autres pays mais également envers sa propre population, ont fait défection. Ces transfuges ont fait pour certains le choix, dévastateur en termes de guerre d'image, de médiatiser leur trahison, intervenant dans les universités ou s'improvisant consultants à l'occasion, pour des services étatiques. C'est le cas notamment de Li Fengzhi[358], officier de renseignement du Ministère de la Sécurité d'État, passé aux USA en 2004, et qui révèlera d'ailleurs que "Pékin place des espions dans les agences de presse chinoises, telles que Xinhua[359], dans le but avoué de glaner des informations auprès de politiciens de haut niveau" dans des pays étrangers, utilisant certains de ces journalistes pour du "sexpionnage", comme le cas probable du Secrétaire Parlementaire Dechert au Canada en 2011[360], dont l'affaire supposée avec une journaliste chinoise très proche du gouvernement avait fait grand bruit.

Ce genre de témoignage affaibli la crédibilité et l'herméticité du PCC. Mais à travers ces campagnes anti-corruption, Xi Jinping muselle les velléités dissidentes internes au Parti. Cela n'empêche cependant pas certains citoyens chinois de parvenir à parfois contester l'information officielle.

Le dernier en date, assez médiatisé, a été celui du Docteur Li Wenliang[361], qui début 2020 témoignait sur WeChat de la propagation du Coronavirus. Le PCC, fidèle à sa stratégie de prioriser le prisme du contenu avant le contenant, avait alors supprimé ses différents posts et commentaires, avant de lui interdire l'accès aux réseaux sociaux, et de finalement l'arrêter. Il avait été accusé de "perturbation de l'ordre social"[362] en répandant de fausses rumeurs. Son témoignage avait néanmoins fait de lui un héros à l'extérieur mais aussi à l'intérieur du pays,

---

358 *Ex-Chinese spy says politicians are targets*. (2011). CTVNews. https://www.ctvnews.ca/ex-chinese-spy-says-politicians-are-targets-1.733398

359 Carlson, K. B. (2012, 22 août). *China's state-run news agency being used to monitor critics in Canada : reporter*. National Post. https://nationalpost.com/news/canada/notes-going-to-china-not-public-canadian-speaks-out-about-split-with-xinhua-news-agency

360 Chase, S. (2011). *Chinese ex-spy warns Canada about how Beijing targets politicians*. The Globe and Mail. https://www.theglobeandmail.com/news/politics/chinese-ex-spy-warns-canada-about-how-beijing-targets-politicians/article547580/

361 FranceInfo avec AFP. (2020). *"Il a donné l'alerte au prix de sa vie" : comment Li Wenliang, le médecin chinois qui a tenté de prévenir le monde sur le coronavirus, est devenu un héros national*. FranceInfo. https://www.francetvinfo.fr/sante/maladie/coronavirus/il-a-donne-l-alerte-au-prix-de-sa-vie-comment-li-wenliang-le-medecin-chinois-qui-a-tente-de-prevenir-le-monde-sur-le-coronavirus-est-devenu-un-heros-national_3816463.html

362 Ibidem.

obligeant le PCC a assurer une cyber-quarantaine des citoyens tentés de suivre son exemple. Car si la télévision, à l'instar de CCTV, reprenait le discours officiel d'accusations dès le lendemain de l'arrestation de Li Wenliang, ce n'était pas le cas des réseaux sociaux, où une nette mise en doute de la transparence des autorités se répandait dangereusement pour le PCC.

Les discordances de la cyber-gestion au sein du gouvernement amène alors à des informations contradictoires entre les ministères et les régions. Le PCC sera finalement obligé de reconnaître l'existence même, puis la propagation, du virus. Quand au docteur, et à ses collègues lanceurs d'alerte comme lui, ils seront même réhabilités par la Cour Suprême, fait extrêmement rare en Chine, participant un peu plus à la décrédibilisation du Parti, et devenant un des sujets de discussions majeurs sur les réseaux sociaux suite à la mort de Li Wenliang, ayant lui-même contracté le Coronavirus. Les réactions des chinois auront été particulièrement virulentes : "Que tous ces fonctionnaires qui s'engraissent avec l'argent public périssent sous la neige"[363] pouvait-on alors lire sur WeChat. Autant de commentaires rapidement effacés par la censure, quelque peu prise au dépourvu face au nombre croissant de critiques de l'État.

Dans cette continuité de problèmes posés par la société civile, on retrouve certains groupes de hacker chinois non inféodés à Pékin. Ces groupes, hostiles vis-à-vis du PCC, se servent de leurs compétences pour nuire aux intérêts chinois. C'est par exemple le cas du groupe rendu célèbre en 1998, nommé Honk Kong Blondes qui avait comme activité principale d'exfiltrer les activistes chinois des Droits de l'Homme en dehors du territoire continental, pour fuir la répression. [364]

2) Le manque de moyens et de compétences : la prédation vers l'extérieur

C'est un fait dont le PCC prend de plus en plus la mesure, à savoir que sa population est ultra-connectée, sa jeunesse en particulier. Malgré l'ampleur de ses moyens de surveillance, le gouvernement est confronté à son impossibilité de suivre numériquement

[363] *Coronavirus : colère en Chine après la mort d'un médecin lanceur d'alerte*. (2020). TV5MONDE. https://information.tv5monde.com/info/coronavirus-colere-en-chine-apres-la-mort-d-un-medecin-lanceur-d-alerte-345563

[364] Ruffin, O. (2020, 14 janvier). *Blondie Wong And The Hong Kong Blondes - Emerging Networks*. Medium. https://medium.com/emerging-networks/blondie-wong-and-the-hong-kong-blondes-9886609dd34b

l'ensemble de ses très nombreux citoyens, bien qu'essayant[365], tout en espionnant à l'extérieur du territoire. Malgré ses innovations numériques et sa formation croissante en cybernétique à travers ses universités, la Chine conserve quelques carences dans plusieurs domaines scientifiques, industriels et plus généralement académiques. Récemment, elle s'est même retrouvée être cette fois la cible d'une fuite massive de données sur ses propres citoyens[366].

Le manque de certains matériels indigènes dans le domaine numérique, préalablement évoqué, a naturellement conduit la Chine a se procurer des composants chez ses adversaires, USA en premier lieu. En 2018, c'était entre 20 et 30 millions d'ordinateurs américains qui étaient utilisés au sein de l'administration chinoise. La décision gouvernementale, qui devait être confidentielle, précisait que le remplacement de l'ensemble des ces machines publiques devrait se faire entre 2020 et 2022… Un objectif qui ne semble pas encore complété, et qui même si l'était, ne change pas le fait que Lenovo, le nouveau fournisseur d'ordinateurs racheté par la Chine, et donc choisi par le PCC, continue d'être dépendant du système d'exploitation Windows.

Pour contrer ses carences, le PCC cherche aussi à savoir ce que pense l'adversaire, et comment il réfléchit. Cette logique s'inscrit dans la stratégie plus large de "réparation", où comment piller les ressources intellectuelles aux anciennes puissances ayant elles-mêmes dépouillé la Chine. Ce n'est donc pas par hasard que le gouvernement encourage ses chercheurs et étudiants à voyager à l'étranger, à y suivre des cursus, et démarche des écoles et instituts pour nouer des partenariats, particulièrement dans les pays occidentaux.
La Chine est en effet encore dépendante de la R&D extérieure sur certains domaines de pointe. Plusieurs universités ont fait les frais de ce flirt académique intéressé, dont en voici quelques unes :

[365] Chansoria, D. M. (2021). *'Sharp Eyes' : Communist China Spies on Its Citizens at Home and Abroad*. JAPAN Forward. https://japan-forward.com/sharp-eyes-communist-china-spies-on-its-citizens-at-home-and-abroad/
[366] Abbas, H. (2020). *'Country Of Spies' : Why China Runs The Risk Of Being Called The Hub Of Espionage After 'Data Leak' ?* Latest Asian, Middle-East, EurAsian, Indian News. https://eurasiantimes.com/country-of-spies-why-china-runs-the-risk-of-being-called-the-hub-of-espionage-after-data-leak/

. L'Université de Canterbury[367] en Nouvelle-Zélande, qui a signé un accord de coopération en 2018 avec l'Institut de Technologie de Harbin, connu pour être l'une des antichambres des cyber-opérations et de l'étude des "sciences dures" de l'APL. Les USA ont d'ailleurs classé l'Institut dans leur liste noire et se refusent à présent à tout partenariat avec.

. Mines ParisTech[368], dont l'accord avec l'Université de Shangaï mais surtout de Jiaotong en 2021 a été la raison d'une nouvelle mise en garde de la part de la DGSI ("Flash ingérence économique"). Comme déjà mentionné, l'Université de Jiaotong est au cœur des formations de l'APL dans le domaine de la cyberguerre. La DGSI a d'ailleurs mentionné plusieurs exemples concrets d'espionnage chinois dans le monde de la recherche, comme le cas de cette étudiante se laissant enfermer dans les bureaux informatiques de son école la nuit…

. Un total de 22 universités américaines maintenaient encore, début 2022, des accords de coopération avec des universités ou instituts chinois considérés comme partie intégrante de la "stratégie de fusion civilo-militaire de l'Administration d'État de la Science, de la Technologie et de l'Industrie pour la Défense Nationale (SASTIND)", selon les mots du Sénateur Marco Rubio, auteur d'une lettre ouverte de mise en garde à l'ensemble de ces universités américaines[369]. A ce titre, l'Australian Strategic Policy Institute (ASPI) maintient une base de données des universités chinoises proches de l'APL, en les déclinant par domaine, comme par exemple dans le domaine cyber. [370]

Il faut rappeler que la *Loi sur le Renseignement National de la Chine* adoptée en 2017 oblige désormais l'ensemble des citoyens et des entreprises voyageant à l'étranger, ou y étant implantés, à effectuer un travail de renseignement extérieur et de rapport au Guoanbu (Ministère de la Sécurité d'État). Dans ce cadre, le *SASTIND* fait office de façade au renseignement universitaire et technologique. C'est également cette administration qui se charge de démarcher des professeurs émérites à venir faire des conférences sur le sol chinois,

---

[367] Van Beynen, M. (2020). *University of Canterbury collaborating with Institute linked to Chinese military*. Stuff. https://www.stuff.co.nz/national/122196854/university-of-canterbury-collaborating-with-institute-linked-to-chinese-military

[368] Guibert, N., & Nevé, S. L. (2021). *Un partenariat passé entre ParisTech et une université chinoise inquiète les services de sécurité français*. Le Monde.fr. https://www.lemonde.fr/societe/article/2021/09/15/un-partenariat-passe-entre-paristech-et-une-universite-chinoise-inquiete-les-services-de-securite-francais_6094764_3224.html

[369] Rubio, M. (2022). *Rubio Calls for End to U.S-China University Partnerships that Support the Development of Chinese Military Technologies*. U.S. Senator for Florida, Marco Rubio. https://www.rubio.senate.gov/public/index.cfm/2022/2/rubio-calls-for-end-to-u-s-china-university-partnerships-that-support-the-development-of-chinese-military-technologies

[370] Anonyme. (s. d.). *Please Wait. . . | Cloudflare*. UniTracker. https://unitracker.aspi.org.au/topics/cyber/

à travers le *Thousand Talent Plan*, pour former de futurs élèves et professeurs, voire même à se transférer définitivement en Chine. Cette stratégie chinoise est dûe à l'incapacité du pays à produire des recherches dans certains domaines, qui en conséquence pratique la "captation" : enlever un atout (académique) à l'adversaire, le prendre pour soi et en faire usage ("remodeler"). La Chine se voit comme le pays du milieu, le "Zhong guo", devant attirer à elle les forces vives de l'ennemi[371].

C'est là le paradigme du renseignement chinois, envoyer des étudiants et futurs professeurs se former dans de prestigieuses écoles occidentales, notamment en sciences informatiques, avant de les faire revenir au pays, ou directement puiser dans les professeurs étrangers. Le succès de cette stratégie double, aura permis aux universités chinoises une certaine spécialisation dans des domaines encore nouveaux pour elle, comme l'Institut de Shenzhen pour la Technologie Avancée qui a créé 5 facultés : Département d'informatique et d'ingénierie, Département des sciences et technologies de l'intelligence, Département de robotique et d'automatisation, Département de génie électronique et électrique, Département de biologie computationnelle et informatique de la santé, et qui demeure avide de faire venir davantage d'étrangers encore.

Malgré tous ces efforts, et malgré les différentes réformes qu'a subi l'APL, comme la création de sa Force de Soutien Stratégique, des problématiques de recrutement subsistent, propre aux armées chinoises.

Cette dynamique s'inscrit d'abord dans le contexte historique de lutte entre le secteur privé et public pour la captation de talents, provenant de multiples facteurs comme la rigidité du système, le fait que certaines universités sont plus prisées que d'autres, réduisant le nombre des candidats pouvant être retenus. [372] Ensuite, l'APL a développé une mauvaise image durant l'ère de Hu Jintao, le département technique du GSD par exemple, était bien moins attractif pour les étudiants que d'autres endroits du secteur civil ou que d'autres ministères, tel le Ministère de la Sécurité d'État.

Ainsi des mesures pour recruter des personnels issus du monde civil ont été mises en place, le recrutement de civils ayant directement comme fonction l'encadrement, ou du recrutement direct en tant qu'officiers non commissionnés, pour des spécialités, ayant au moins été

---

[371] Wu, F., Su, J., & Zeng, J. (2021). *How Does the Chinese Government Select and Funding High-Level Talents ? An Empirical Study Based on the Resumes of Talents*. Frontiers. https://www.frontiersin.org/articles/10.3389/fpsyg.2021.687447/full

[372] Kamphausen, R. D. (2021). *THE PEOPLE OF THE PLA 2.0*. US Army War College Press. https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1940&context=monographs

facilité lors des réformes. Autre fait marquant, un renouveau de l'organisation des civils au sein des départements techniques de l'APL, apparu à l'été 2018, cherche à lutter contre les inégalités que subissent les membres de l'APL vis-à-vis du personnel d'autres ministères, le rendant donc plus compétitif. Cela est corroboré par des reportages chinois, le système ayant été en partie remodélisé pour attirer des talents.

De même un système a été mis en place pour que le personnel hautement qualifié puisse gagner un solde supplémentaire après la réussite d'un examen particulier strict. Selon une source de l'auteur, les TRB's que nous avons évoqués précédemment offriraient également des bonus de solde annuel, et ce pour augmenter les motivations financières à rejoindre l'APL. D'autres mesures financières ont pu être mises en place.

Cependant les problématiques restent inchangées, le secteur civil s'adaptant et augmentant les salaires (bien qu'on retrouve des primes très importantes dans le secteur public), et le secteur public possédant ses problématiques propres, comme la protection du secret national.

Mais cette force centrifuge, d'espionnage envers les pays occidentaux, et centripète, de captation de savoirs-faire, n'est pas sans parfois échouer et provoquer des réactions étrangères de défense, voire de contre-attaques.

B) Réactions exogènes

À mesure que les hackers chinois ciblent l'économie adverse, c'est-à-dire principalement des pays occidentaux, ces derniers voient naître en leur sein des réactions de plus en plus virulentes divergeant des pratiques habituellement jugées comme acceptables ou non dans le milieu de l'espionnage.

De condamnations en délations, ces différentes enquêtes anonymes contre les auteurs de cyber-attaques ont conduit certains États, les USA en premier lieu, à prendre la problématique en mains, et à judiciariser certains de ces cyber-attaquants , une première dans l'histoire du cyber-espionnage mondial.

1) Des attaques identifiées et la montée d'une condamnation internationale.

Le PCC, de par son approche fortement décomplexée à cibler tous ses adversaires mais aussi partenaires, en tout temps, a fini par briser le mythe un peu naïf d'une Chine

“usine du monde” bien pratique, ne recherchant pas l’hégémonie, comme le prétendait Deng Xiaoping à la tribune de l’ONU en 1974[373].

Certaines de ses cyberattaques ont dépassé la seule collecte d’informations générales, puisque ciblées sur des programmes de Défense, elles ont permis d’alimenter la recherche et le développement de nouveaux systèmes d’armement : le cas le plus emblématique est l’infiltration, pendant des années, du programme F-35 de Lockheed Martin.

Seulement, la paternité d’une cyber-attaque est toujours complexe et parfois hasardeuse à déterminer publiquement, et sur la majorité de ces attaques, seulement une infime partie peuvent être publiquement imputables à la Chine. D’autres ont pu être identifiées plus clairement et contrecarrées à quelques reprises.

C’est ainsi le cas de l’opération Aurora, une attaque répétée et simultanée, durant l’année 2009, qui toucha une trentaine de grandes entreprises américaines, à commencer par Google, qui communiqua sur l’affaire en 2010. La société McAfee, spécialisée en cybersécurité, apporta son aide et expertise pour finalement remonter jusqu’à la cellule APT17[374], aussi connue comme le Elderwood Project ou Elderwood Group ou encore Beijing Group, et dont les liens supposés avec l’APL furent d’autant plus probables qu’aucune arrestation ne fut menée, ni conclusion d’enquête rendue par le PCC.

L’attaque fut un succès, au moins pendant quelques mois, avant d’être jugulée. Elle conduisit à une réaction diplomatique virulente, Google menaçant de se retirer du territoire chinois et le gouvernement US la condamnant, sans ambiguïté quant aux auteurs à l’origine de cette attaque. L’expression “Root out China” se développa alors pour désigner la riposte contre la nébuleuse hackeuse chinoise, aux connections gouvernementales sans équivoque.

L’entreprise russe SafenSoft décrit ainsi la stratégie des assaillants à l’époque[375] :

Dans son traité L'art de la guerre, l'éminent ancien théoricien militaire Sun Tzu a écrit : "Ne comptez pas sur l'ennemi qui ne vient pas, mais comptez sur notre préparation contre lui". Il est important de comprendre : Le paradigme même de la sécurité de l'information a changé. A l'heure où les hackers découvrent de nouvelles vulnérabilités, inventent des outils d'intrusion

[373] *Never Seek Hegemony : China's Voice at the UN General Assembly*. (2021). Global Times. https://www.globaltimes.cn/page/202107/1227967.shtml

[374] *MVISION Insights : Winnti Group Targeting Universities In Hong Kong*. (2020). McAfee. https://kc.mcafee.com/corporate/index?page=content&id=KB92731&locale=en_US

[375] *The Elderwood Project : the art of war*. (2012). Proactive protection of the computer against malicious software, ATM protection, data leakage prevention. http://www.safensoft.com/archiv/p/773/1733/

et d'espionnage toujours plus sophistiqués, les agents antiviraux, en effet, sont restés bloqués dans le passé. Le concept même de base de données de signatures antivirus a été créé à une époque où la sécurité informationnelle ne connaissait pas des termes tels que des attaques ciblées (Advanced persistent Threat - APT), une vulnérabilité zero-day, une porte dérobée, un cheval de Troie, etc. Les éditeurs d'antivirus modernes sont trop grands pour saisir leur propre maladresse. Ils sont trop lents à répondre aux nouveaux défis, trop peu attentifs à l'élaboration de nouvelles stratégies de sécurité.".

La temporalité des cyber-attaques n'est pas hasardeuse. Il est facile d'observer une corrélation entre l'actualité géopolitique et celles-ci.
Entre la semaine précédant l'invasion de l'Ukraine par la Russie, et la mi-mars, le nombre de cyber-attaques provenant d'IP chinoises a augmenté de 72% à travers le monde, 116% envers les pays de l'OTAN, avec des disparités importantes entre ces derniers. La France a par exemple subi une hausse de 122%, et le Danemark 281%[376].
S'il n'est pas possible de clairement les imputer au gouvernement chinois, plusieurs hypothèses probables émergent cependant de ces données d'attaques :

. Les hackers étrangers ont tendance à privilégier des pays où il est facile, peu coûteux, et opportun en termes de traçabilité, de gérer un service informatique.
. Les hackers chinois ont, par opportunisme circonstanciel, choisi d'attaquer alors que la situation déjà tendue et confuse le permettait plus facilement.
. Les attaques ont été pilotées par un acteur étatique, chinois ou étranger, mais avec un laissez-faire voire la bénédiction du PCC, autant par opportunisme que pour analyser les défenses et réactions de l'OTAN en cas de crise.

Quels que soient les auteurs, une telle hausse d'attaques dirigées n'a pu se faire sans que le PCC ne le sache. Des attaques ciblées et vraisemblablement coordonnées qui ne sont pas sans rappeler celles de 2021 contre les serveurs de Microsoft Exchange. Dans une déclaration commune[377], les membres de l'OTAN, de l'Union européenne, de l'Australie, de la Nouvelle-

[376] *Cyber Attacks on NATO Countries Surge by 116% - Check Point Software*. (2022). Check Point Software. https://blog.checkpoint.com/2022/03/21/cyber-attacks-from-chinese-ips-on-nato-countries-surge-by-116/
[377] Wilkie, C. (2021). *U.S., NATO and EU to blame China for cyberattack on Microsoft Exchange servers*. CNBC.https://www.cnbc.com/2021/07/19/nato-and-eu-launch-a-cyber-security-alliance-to-confront-chinese-cyberattacks.html

Zélande et du Japon avaient appelé à une coopération sans précédent pour affronter la menace grandissante posée par les cyberattaques “parrainées” par l'État chinois.

Cependant, certains analystes anonymes, issus d’États ciblés par les hackers chinois, prennent l’initiative de la contre-attaque, au-moins médiatiquement, considérant que ces-dits États ne sont pas assez offensifs dans leurs réactions. C’est ainsi que l’on retrouve le collectif *Intrusion Truth*, dont les membres sont suspectés provenir de services de renseignement, ou d’en être des anciens (probablement US), et qui n’hésitent plus à partager publiquement le résultat de leurs cyber-enquêtes, en identifiant les collectifs et parfois même les individus derrière les attaques.

C’est ainsi que plusieurs officiers de l’État chinois ont été dénoncés en 2017 pour leur appartenance à APT3 (se révélant être la société Boyusec, “prestataire” du MSS), et de nouveaux en 2018 pour APT10.

En 2019, c’est au tour de APT17, précédemment mentionné, de voir plusieurs de ses membres révélés au grand public. L’un d’eux : Guo Lin (郭林), ou Mister Guo[378], officier de la branche cyber du MSS, le Centre d'Évaluation de la Sécurité des Technologies de l'Information Chinois (CNITSEC). Après avoir brillamment étudié les sciences informatiques à l’université de Nanjing, il avait publié un essai : “Méthode de classification des attaques basées sur la multi-dimensions” (基于多维角度的攻击分类方法). Mais en enquêtant davantage, Intrusion Truth s’est aperçu que Guo Lin était également le dirigeant de quatre société spécialisées, sans surprise, en informatique. Deux autres hackers seront identifiés, l’ensemble du groupe opérant depuis Jinan. [379]

Si le collectif a réussi plusieurs fois à identifier aussi précisément les hackers, c’est que l’État chinois fait preuve d’une certaine négligence sur la sécurité opérationnelle (OpSec) de ses agents, les laissant parfois créer des comptes avec leur propre identité, numéro, carte

[378] *Who is Mr Guo ?* (2019). Intrusion Truth. https://intrusiontruth.wordpress.com/2019/07/17/who-is-mr-guo/

[379] *APT17 is run by the Jinan bureau of the Chinese Ministry of State Security*. (2019). Intrusion Truth. https://intrusiontruth.wordpress.com/2019/07/24/apt17-is-run-by-the-jinan-bureau-of-the-chinese-ministry-of-state-security/

bancaire, et n'encadre pas toujours suffisamment les procédures de sûreté générale de ceux-ci[380].

Ainsi, en remontant les trajets Uber d'un officier du MSS, *Intrusion Truth* était parvenu à identifier son rôle au sein d'une APT.

Dans une interview, le collectif déclare : "Nous voulons que les hackers chinois ouvrent les yeux et réalisent à quel point leur gouvernement se soucie peu d'eux. À tout moment, leurs officiers traitants du MSS pourraient faire d'eux des boucs émissaires en tant que criminels afin de faire ce que la Chine s'efforce de réaliser : protéger l'État.".

Si les initiatives de *Intrusion Truth* n'entraînèrent pas immédiatement d'autres répercussions, la corroboration de leurs recherches et conclusions par des sociétés de cybersécurité privées finit par pousser l'US Justice Department, via le FBI, a ouvrir plusieurs enquêtes[381].

2) Une riposte étatique : les contre-attaques de services étrangers.

En effet, la liste des personnes recherchées pour des actes de cybercriminalité du FBI affiche désormais les profils de plusieurs agents d'État chinois ou coréens, ou encore de hackers russes et iraniens, aux allégeances parfois incertaines.

Le directeur du FBI, Christopher Wray, déclarait ainsi : "La plus grande menace à long terme pour l'information et la propriété intellectuelle de notre nation, ainsi que pour notre vitalité économique, est la menace de contre-espionnage et d'espionnage économique de la Chine.".

On trouve donc une trentaine de citoyens de la RPC, avec pour la quasi-totalité une à plusieurs photos accompagnant l'avis de recherche, ainsi que des accusations éminemment explicites sur leur implication au sein de services étatiques chinois. Une page propre à la "menace chinoise" a même été créée pour recenser l'ensembles des profils originaires de PRC recherchés[382]. 'est le cas pour un certain Zhu Hua travaillant pour "Huaying Haitai

---

[380] WEareTROOPERS. (2017). *TR17 - Surprise Bitches ! - The Grugq* [Vidéo]. YouTube. https://www.youtube.com/watch?v=wP2J9aYM6Oo

[381] Culafi, A. (2020). *CrowdStrike founder : China hacking indictments are working*. SearchSecurity. https://www.techtarget.com/searchsecurity/news/252479273/CrowdStrike-founder-China-hacking-indictments-are-working

[382] FBI. (2022). *The China Threat - Wanted by the FBI*. https://www.fbi.gov/investigate/counterintelligence/the-china-threat

Science and Technology Development Company située à Tianjin, en Chine, et ayant agi en association avec le Bureau de la Sécurité de l'État de Tianjin du Ministère chinois de la Sécurité d'État", ou encore un Sun Kailiang ayant été "officier du Troisième Département de la RPC du département d'État-Major Général de l'Armée Populaire de Libération (3PLA), deuxième bureau, troisième bureau, indicatif de couverture d'unité militaire (MUCD) 61398, à un moment donné au cours de l'enquête".

WANTED BY THE FBI

SUN KAILIANG

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

Aliases: Sun Kai Liang, Jack Sun

DETAILS

On May 1, 2014, a grand jury in the Western District of Pennsylvania indicted five members of the People's Liberation Army (PLA) of the People's Republic of China (PRC) for 31 criminal counts, including: conspiring to commit computer fraud; accessing a computer without authorization for the purpose of commercial advantage and private financial gain; damaging computers through the transmission of code and commands; aggravated identity theft; economic espionage; and theft of trade secrets.

The subjects, including Sun Kailiang, were officers of the PRC's Third Department of the General Staff Department of the People's Liberation Army (3PLA), Second Bureau, Third Office, Military Unit Cover Designator (MUCD) 61398, at some point during the investigation. The activities executed by each of these individuals allegedly involved in the conspiracy varied according to his specialties. Each provided his individual expertise to an alleged conspiracy to penetrate the computer networks of six American companies while those companies were engaged in negotiations or joint ventures or were pursuing legal action with, or against, state-owned enterprises in China. They then used their illegal access to allegedly steal proprietary information including, for instance, e-mail exchanges among company employees and trade secrets related to technical specifications for nuclear plant designs. Sun, who held the rank of captain during the early stages of the investigation, was observed both sending malicious e-mails and controlling victim computers.

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Pittsburgh

Malgré les demandes d'extradition répétées de l'administration US, la Chine s'est bien-sûr toujours refusée à coopérer quand il s'agissait de hackers à son service. Néanmoins, cette liste illustre le changement d'attitude progressif des États sur la question des cyber-attaques.

La nature même de *Intrusion Truth* peut laisser supposer que le collectif n'est peut-être pas composé "d'anciens" si anciens que ça, mais bien de techniciens et analystes encore au service d'agences comme la NSA et agissant sous les directives du gouvernement US, adoptant par-là même la stratégie de dissimulation que le PCC utilise avec ses propres hackers.

Moins agressive, et plus lente à réagir au niveau institutionnel, de par une culture du renseignement bien différente de ses partenaires anglo-saxons, la France a néanmoins commencé à communiquer sur la problématique.
Les bulletins de suivi de la DGSI, déjà mentionnés, se font plus réguliers et n'hésitent pas à donner des exemples explicites d'actes d'espionnage chinois. Mais le plus marquant fut cette note d'alerte conjointe, comme n'est pas coutume, entre la DGSE et la DGSI, émise en 2018, et diffusée à tous les ministères. Les deux services de renseignement mettent alors en garde contre le cyber-espionnage via les réseaux sociaux professionnels, LinkedIn en premier lieu. Les chiffres sont parlants : environ 500 sock puppets (ou faux-profils) sur LinkedIn seraient tenus par des agents du MSS, à destination du recrutement de sources françaises, et ce à travers une quinzaine de sociétés-écrans. Ce serait plus de 4000 citoyens français qui auraient été approchés par ce biais, pour des offres de recrutement ou des échanges et invitations en Chine, tous frais payés. Presque la moitié d'entre eux seraient des fonctionnaires, les autres des employés de grandes entreprises ou d'entreprises stratégiques[383].
Néanmoins là encore, un certain sentiment d'impuissance relative a pu conduire les services français à rompre certains codes de conduite, dans le but d'alerter une opinion plus large à la menace réelle du PCC en France.
Ce n'est donc pas un hasard si certaines informations ont fuitées dans la presse concernant "l'annexe" de l'Ambassade de Chine en France, au 145 Rue du Lieutenant Petit Le Roy à Chevilly-Larue dans le Val-de-Marne. Ces deux bâtiments, aux massives antennes satellitaires sur le toit de l'un d'eux, sont suspectés de servir de centre d'écoute opéré par l'ex-3 PLA, (Troisième Direction de l'APL) pour l'interception, la communication et la transmission de SIGINT.

[383] Girard, E. (2022). *LinkedIn, DGSE, offres faramineuses... Comment la Chine nous espionne*. LExpress.fr. https://www.lexpress.fr/actualite/societe/linkedin-dgse-offres-faramineuses-comment-la-chine-nous-espionne_2170186.html

Une prise de conscience française grandissante donc, et récemment formalisée dans le rapport précédemment cité : "*Les opérations d'influence chinoises : Un moment machiavélien*" par J-B. Jeangène Vilmer et P. Charon, chercheurs à l'IRSEM.

Mais certaines contre-attaques dépassent même les théâtres d'affrontement médiatique et juridique. Si l'espionnage chinois est de plus en plus connu, certains pays n'hésitent pas à agressivement espionner la Chine en retour. L'accord de coopération stratégique UKUSA et ses *Five Eyes*, réunissant la communauté du renseignement des 5 principaux pays anglo-saxons, a pour première cible la Chine. Cet espionnage décomplexé est déjà ancien, et a pu donner lieu à un ensemble d'opérations, dont en voici quelques exemples :

- Dès 1995, les USA et l'Australie avaient mis en place des moyens d'interceptions (dont une petite antenne) dans les fondations mêmes de la nouvelle ambassade chinoise à Canberra durant sa construction[384].
- Déjà en 1999, la NSA avait 3 stations d'interceptions-transmissions ayant un focus sur la Chine, et situées Geraldton en Australie, Waihopai en Nouvelle-Zélande, et sur la base militaire de Yakima sur la côte Ouest des USA. Le nombre de stations a depuis augmenté, mais le phénomène n'est donc pas nouveau.
- La Chine, à la fin des années 90, confie son système de guidage de missiles et communications satellitaires à … Loral Corp. et Hughes Electronics, deux sociétés aérospatiales américaines. Si l'affaire avait alors enragé quelques politiciens, la NSA, elle, ne s'en était jamais plainte[385].

Il faut enfin rappeler qu'en terme de renseignements humain (HUMINT), les USA ne sont pas en reste. Entre 2015 et 2017, ce sont vraisemblablement une vingtaine de citoyens chinois, sources pour les services américains, qui ont été emprisonnés ou exécutés par le PCC[386].

Quant à Taïwan, cible récurrente des cyber-attaques chinoises, l'État a fini par se doter de services spécialisés dans la cyber-défense, avec notamment le *National Information and*

[384] Windrem, R. (1999). *When it comes to spying, U.S. is as insatiable as China*. Intelligence Resource Program. https://irp.fas.org/news/1999/06/990602-275397.htm
[385] *Ibidem.*
[386] Jennings, R. (2019). *Trump Secret Service USB OpSec FAIL : 'Spy' Story Gets Weirder*. Security Boulevard. https://securityboulevard.com/2019/04/trump-secret-service-usb-opsec-fail-spy-story-gets-weirder/

Communication Security Taskforce de Taïwan (NICST, Groupe de Travail National sur la Sécurité de l'Information et de la Communication) et sa branche cyber, le *National Center for Cyber Security Technology* (NCCST, Centre National la Technologie de la Cybersécurité), qui déclarent :

"Promouvoir un système de défense conjointe au niveau national et établir un mécanisme de partage d'informations sur la cybersécurité en exploitant le National- Information Sharing and Analysis Center (N-ISAC, Centre National de Partage et d'Analyse d'Informations), la National-Computer Emergency Response Team (N-CERT, Équipe Nationale d'Intervention d'Urgence Informatique) et le National-Security Operation Center (N-SOC, Centre d'Opérations de Sécurité Nationale)."
Une décision motivée par les 100 000 attaques informatiques mensuelles que connaît Taïwan ces dernières années, d'après le National Security Bureau[387] (NSB). La présidente de l'île, Tsai Ing-wen, déclarait ainsi dès son premier mandat : "Cybersecurity is national security" ("La cybersécurité est la Sécurité nationale").

Un espionnage et un accroissement de la cyber-défense à double-sens donc, entre chinois et occidentaux, dont les règles semblent tomber une à une face à une Chine irrespectueuse de ces-dites règles, mais innovante et tenace dans sa stratégie, et qui place ses adversaires dans l'obligation de réagir en s'adaptant à son niveau, ou de subir indéfiniment sa voracité informationnelle.

L'analyse globale des cyber-opérations de l'APL et des milices et sociétés civiles sous son contrôle permettent d'identifier 3 domaines-cibles récurrents des attaques qu'elle mène :

- Diplomatique, servant autant à la collecte d'informations que "la collecte d'humains" à travers la compromission des atouts identifiés.
- Économique, avec une intention particulière portée aux innovations scientifiques et à la R&D industrielle.
- Militaire, aussi bien pour espionner les dispositifs ennemis que dérober ses projets. Les USA les premiers ont fait les frais de ce pillage informationnel.

[387] Kitchen, K., & Drexel, B. (2022). *Securing Taiwan Requires Immediate Unprecedented Cyber Action*. Lawfare. https://www.lawfareblog.com/securing-taiwan-requires-immediate-unprecedented-cyber-action

Voici donc 3 exemples-types d'attaques[388] :

Table 3. Chinese Government-sponsored Cyberattacks and their Origins

Target	Exploited Technology or Information	Year of Attack	Cyber Operation Name	PRC-Attributed Entity	Target Category
U.S. OPM	Current, former, and future federal employee background information	2015	N/A	Inconclusive	**Diplomatic**
Avago Technologies & Skyworks Solutions	Cellular technology	2015	N/A	Chinese Tianjin Professors and Chinese nationals	**Economic**
ASEAN nations and countries involved in the South China Sea	Classified and sensitive government and military operations and developmental information	2010 - 2015	*Naikon APT*	PLA Unit 78020	**Military**

Le rapport de *Mandiant* de 2013[389] (PLA) a fait l'effet d'une petite bombe dans la communauté cyber, exposant clairement l'ampleur des cyber-opérations chinoises à travers le prisme d'une seule de ses unités opérationnelles, considérée comme la première *APT*. Jusqu'à 11 plateformes américaines auraient été ciblées par elle. Le vol continue de données a fait de la *Big Data* une ressource numérique à part entière, la plus précieuse exploitable par l'APL.

Alors que cette dernière accroît sa flotte, devenant la première marine au monde en termes de navires, développe des missiles hypersoniques, construit des avions furtifs étrangement similaires à ceux des USA, et projette des ambitions spatiales inenvisageables pour ses adversaires, il convient de s'interroger sur la dangerosité que représenteraient en plus des cyber-opérations en cas de conflit ouvert.

Une telle situation géopolitique n'est en effet pas à exclure, alors que la montée des tensions en Mer de Chine débouche sur ce que certains qualifient déjà de conflit larvé.

Alors que le PCC n'hésite déjà plus à recourir contre ses concurrents à des procédés s'inscrivant en-dehors des codes, traditionnellement acceptés, des relations internationales, il

[388] Ellis, J. M. (2010). CHINESE CYBER ESPIONAGE : A COMPLEMENTARY METHOD TO AID PLA MODERNIZATION. *NAVAL POSTGRADUATE SCHOOL*. https://www.hsdl.org/?view&did=790444

[389] *APT1 : Exposing One of China's Cyber Espionage Units | Mandiant*. (2013). Mandiant. https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units

est envisageable qu'un prétexte d'exacerbation des tensions avec ses adversaires fasse basculer les cyber-opérations de ses forces armées dans une logique de saturation des réseaux de l'ennemi. Une menace contre laquelle il semble difficile de se préserver.

CONCLUSION

Il s'agissait tout au long de ce travail d'identifier les axes de puissance de la Chine dans sa stratégie cyber. Finalement, la question était de savoir si la volonté affichée de Xi Jinping en 2014 de faire de la Chine une cyberpuissance est un objectif atteignable, voire partiellement déjà atteint. Également, la manière dont le PCC a opéré depuis les années 1990 et l'avènement d'Internet, et opère actuellement pour l'atteindre.

Émanant d'une prise en compte dans les années 1990 de l'importance de la technologie et de l'informatique, la Chine décide d'élaborer des doctrines pour mieux contrôler le déploiement d'Internet et des nouvelles technologies. En effet, le régime reste totalitaire et l'arrivée d'Internet risque de mettre le PCC dans une situation d'affaiblissement si trop de voix critiques venaient à se rassembler. Les événements de la place Tiananmen étant encore bien ancrés dans la mémoire collective du PCC. De sa volonté de légitimer le Parti, et surtout d'atteindre une stabilité sociale chère au PCC, celui-ci a rendu stratégique le numérique basé sur « l'informatisation », portant notamment sur l'amélioration de l'industrie numérique, des capacités technologiques, de la gouvernance via le numérique, et la « cybersécurité qui porte sur la disponibilité du réseau mais également sur sa sécurité » (davantage du PCC que de la population). D'un point de vue intérieur, la Chine montre de réels progrès dans sa stratégie de cyberpuissance : infrastructures, connectivité (déploiement de la 5G), nouvelles technologies (IA), entreprises, contrôle de la population (au sens de prouesse technique)… La Chine parvient donc petit à petit à produire ses propres technologies sur son sol.

Son opposition permanente à l'adversaire américain a également joué sur la définition de sa stratégie, puisqu'elle se place en opposition et surtout dans un but défensif face aux États-Unis. La stratégie de cyberpuissance chinoise peut-être vue en quelque sorte comme une réaction à l'hégémonie américaine. Les capacités cyber de la Chine dans le domaine militaire ont quant à elles été analysées pour montrer leur caractère réellement offensif. Bien qu'elle défende une vision de défense active, l'offensive active est également une solution utilisée. Malgré tout, il est difficile d'attribuer les attaques à la Chine, et c'est sur cette notion que le pays s'appuie pour réaliser ses opérations cybermilitaires en presque toute impunité. Après tout, si une attaque est pleinement réussie, elle ne devrait pas être imputable à son commanditaire.

Malgré les avancées numériques, et la volonté de la Chine de rentrer dans une société de l'intelligence (axée sur la data) depuis 2018, on pourra noter que le pays souffre de problématiques qui freinent son expansion numérique : sa rivalité avec les États-Unis et surtout la crainte qu'ils lui inspire (la poussant à produire des doctrines et stratégie *en réponse* à l'adversaire) montre que sa place n'est pas hégémonique. D'autres facteurs s'ajoutent à cela : la corruption, le manque de moyen, la fuite des cerveaux, le manque de personnel compétents, une condamnation internationale croissante des agissements chinois, et des contre-attaques des services étrangers.

La stratégie chinoise pour devenir une cyberpuissance est en marche, mais n'est pas encore entièrement accomplie. Elle en a les caractéristiques, s'équipe, s'arme même, mais les freins à cette expansion sont nombreux. En substance, on pourra qualifier la Chine de puissance cyber, puisqu'elle fait du numérique une arme économique, militaire, sociale et politique éminemment sophistiquée. Quant à sa position de cyberpuissance, loin d'être hégémonique, elle s'affirme néanmoins plus distinctement dans ses ambitions projetées dans ce nouveau champ de conflictualités qu'est le cyberespace.

BIBLIOGRAPHIE

Chapitre 1 : La quête de cyberpuissance de la République Populaire de Chine : contexte doctrinale et cadre normatif

- Anonyme, 数字福建是数字中国的思想源头. [Digital Fujian is the ideological source of Digital China (2018, avril 23)] *Guangming Daily*. http://news.sina.com.cn/o/2018-04-23/doc-ifznefkh9862417.shtml
- Austin G. (2014) Cyber Policy in China. *China Today*.
- Blessing J. and Austin G. (2022, Février) Assessing military cyber maturity: strategy, institutions and capability, *The International Institute for Strategic Studies*
- Boniface P. Sun (2019) L'Art de la guerre De Sun Tzu à Xi Jinping, *Ekho*.
- Campbell, C. (2021, Juin 4) China's Military : The People's Liberation Army (PLA) *Congressional Research Service*.
- Chandel, S., Jingji, Z., Yunnan, Y., Jingyao, S., & Zhipeng, Z. (2019). The Golden Shield Project of China : A Decade Later—An in-Depth Study of the Great Firewall. 111-119. https://doi.org/10.1109/CyberC.2019.00027
- Clerot Fabienne & Mayor Victoire, « Jeu de Go dans le Cyberespace », Revue Internationale et Stratégique, 2012/3, N°87, 2012, p. 11
- Costello J. and McReynolds J. (2018 Octobre) China's Strategic Support Force: A Force for a New Era. *China Strategic Perspectives*
- Creemers, R. (2020). Comment la Chine projette de devenir une cyberpuissance. *Hérodote*, 177-178, 297-311. https://doi.org/10.3917/her.177.0297
- Creemers R., Triolo P., and Webster G. (2018, Avril 30)Translation: Xi Jinping's April 20 Speech at the National Cybersecurity and Informatization Work Conference. *New America.*https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/
- Dorman D. (2020, Novembre) Making The Most Of It, Part Ii: Xi Jinping Leverages Coronavirus "War Without Smoke" To Spur Digital Transformation, Test National Defense Mobilization. *Security Nexus Perspectives.* https://apcss.org/wp-content/uploads/2020/11/Dorman_Making-the-Most-of-It-Part-II-final.pdf
- Dorman D. (2022, Mars 28) China's Plan For Digital Dominance. *War on The Rocks.* https://warontherocks.com/2022/03/chinas-plan-for-digital-dominance/

- Doshi, R. (2020, juillet 31). The United States, China, and the contest for the Fourth Industrial Revolution. *Brookings.* https://www.brookings.edu/testimonies/the-united-states-china-and-the-contest-for-the-fourth-industrial-revolution/

- Douzet, F. (2014). L'art de la guerre revisité. Cyberstratégie et cybermenace chinoises. *Herodote*, 152153(1), 161-173.

- de Durand, É. (2003). « Révolution dans les affaires militaires »: « Révolution » ou « transformation » ?. *Hérodote*, 109, 57-70. https://doi.org/10.3917/her.109.0057

- Evans, R. (2021, septembre 18). Chine : Quelle stratégie dans et pour le cyberespace ? *Hypothèses - Questions Géopolitiques*. https://geopolri.hypotheses.org/2690#_ftn32

- Feng Y. (2000) The Construction and Use of New China's Defense Deterrent Force, *Journal of PLA Nanjing Institute of Politics.*

- Fravel, M. T. (2020a). Active Defense : China's Military Strategy Since 1949. *Princeton University Press*.

- Griffiths J. (2019) The Great Firewall of China, *ZED*

- Grumbach, S. (2014). I. La Chine au cœur de la société de l'information. Dans : Marianne Bastid-Bruguière éd., Une autre émergence: Puissance technique et ressorts culturels en Inde et en Chine (pp. 13-45). Paris: Hermann. https://www.cairn.info/une-autre-emergence-2014--9782705688820-page-13.htm?ref=doi

- Harrell P., Rosenberg E. and Saravalle E.(2018, juin 12) China's Use of Coercive Economic Measures. *CNAS.* //www.cnas.org/publications/reports/chinas-use-of-coercive-economic-measures

- IISS (2019, Mai) Chapter Five: China's cyber power in a new *In Asia Pacific Regional Security Assessment*, 77-99 2019era. https://www.iiss.org/publications/strategic-dossiers/asiapacific-regional-security-assessment-2019/rsa19-07-chapter-5

- Kania E., Sacks S., Triolo P., and Webster G. (2017, Septembre 25) China's Strategic Thinking on Building Power in Cyberspace, A Top Party Journal's Timely Explanation Translated. *New America*. https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/

- Kamphausen R., Lai D. et Tanner T. (2014, Avril 1) Assessing The People's Liberation Army In The Hu Jintao Era, *Strategic Studies Institute, US Army War College* https://www.jstor.org/stable/resrep11946.9?seq=12

- Krekel B., Adams P. et Bakos G. (2021, Mars 7) Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage, *Northrop Grumman*. https://www.uscc.gov/sites/default/files/Research/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf

- Li, G. (Éd.). (2011a). Information Science & Technology in China : A Roadmap to 2050. *Springer Berlin Heidelberg.* https://doi.org/10.1007/978-3-642-19071-1

- Lorci, E. (2021). The Chinese Model of Cyber Sovereignty: Main Principles and Implementations. *Uluslararası İlişkiler Çalışmaları Dergisi University* Studies https://dergipark.org.tr/en/pub/jirs/issue/68261/1064082
- McReynolds, J., & Mulvenon, J. (2014). The Role Of Informatization In The People's Liberation Army Under Hu Jintao (Assessing The People's Liberation Army In The Hu Jintao Era, p. 207-256). *Strategic Studies Institute, US Army War College*. https://www.jstor.org/stable/resrep11946.9
- Office of the Secretary of Defense. (2013) Annual Report To Congress Military and Security Developments Involving the People's Republic of China
- Picarsic N., Ferguson J., De La Bruyère E. et Doshi R. (2021, Avril) China As A"Cyber Great Power"Beijing's Two Voices In Telecommunications, F*oreign Policies at Brookings:*
- PRC State Council Information Office(2019, Juillet) China's National Defense in the New Era
- Raud M. (2016). NATO Cooperative Cyber Defence Centre of Excellence, China and Cyber : Attitudes, Strategies, Organisation. *Unclassified, National Security Archives* https://nsarchive.gwu.edu/document/22256-document-10-mikk-raud-nato-cooperative-cyber
- Scobell, A. (2000a). Show of Force : Chinese Soldiers, Statesmen, and the 1995-1996 Taiwan Strait Crisis. *Political Science Quarterly*, 115(2), 227-246. https://doi.org/10.2307/2657901
- Shan Zhiguang S. (2018, Décembre 2) A beautiful vision for a smart society. *People's Daily Online* http://theory.people.com.cn/n1/2018/1202/c40531-30436566.html
- Sleeboom-Faulkner M. (2007 Mars) Regulating Intellectual Life in China : The Case of the Chinese Academy of Social Sciences. *The China Quarterly* https://www.jstor.org/stable/20192737
- Gatti B. (2020 17 Décembre) The 14th Five-Year Plan: a high-speed roadmap for China, *EIAS,* https://eias.org/publications/op-ed/the-14th-five-year-plan-a-high-speed-roadmap-for-china/
- The Cyberspace Administration of China (2020) released the "Digital China Development Report (2020). *Cac.gov.cn* http://www.cac.gov.cn/2021-06/28/c_1626464503226700.htm
- The State Council Information Office of the People's Republic of China (Mai 2015) Defense White Paper. *Xinhua* http://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm
- Xi Jinping (2013 Aout), Discours à la Conférence de la Propagande Nationale et du Travail Idéologique
- Xingrui M. 加快数字化发展 来源 [Développement] (2021, Janvier 25)《求是》https://theory.gmw.cn/2021-01/25/content_34569312.htm

- Yang, Y. E. (2021). China's Strategic Narratives in Global Governance Reform under Xi Jinping. *Journal of Contemporary China,* 30(128), 299-313. https://doi.org/10.1080/10670564.2020.1790904
- Yunzhu, Y. (1995). The Evolution of Military Doctrine of the Chinese PLA from 1985 to 1995. *Korean Journal of Defense Analysis*, 7(2), 57-80. https://doi.org/10.1080/10163279509464306
- Yau H. (2021 Août) Fragmenting Cyberspace and Constructing Cyber Norms : China's Efforts to Reshape Global Cyber Governance - *Contemporary Chinese Political Economy and Strategic Relations, suppl. Special Issue* https://www.proquest.com/openview/e606e5cd6a5663c304e050e9f6fe5fb3/1?pq-origsite=gscholar&cbl=2042768
- Zhang Y. [张玉良] (2006). ed., The Science of Campaigns [战役学], 2nd ed., *Beijing: National Defense University Press*
- Yuen, S. (2015, 15 juin). *Devenir une cyberpuissance*. Journals OpenEdition. https://journals.openedition.org/perspectiveschinoises/7106
- Harrel, Y. (2021, 19 juillet). *Comparatif des cyberpuissances : Etats-Unis, Chine, Russie*. Conflits : Revue de Géopolitique. https://www.revueconflits.com/comparatif-cyberpuissances/
- Anonyme. (2021). *Cyber Capabilities and National Power : A Net Assessment*. IISS. https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power
- de La Coste, P. (2006). La gouvernance internationale de l'Internet. *Politique étrangère*, 507-518. https://doi.org/10.3917/pe.063.0507
- de La Chapelle, B. (2012). Gouvernance Internet : tensions actuelles et futurs possibles. *Politique étrangère*, , 249-261. https://doi.org/10.3917/pe.122.0249
- Meneut, E. (2021). *LA CYBERSÉCURITÉ GLOBALE ET LA GUERRE FROIDE 2.0*. IRIS.org. https://www.iris-france.org/wp-content/uploads/2021/09/Asia-Focus-166.pdf
- Anonyme. (2017, 2 mai). *Quel cadre juridique international pour le numérique ?* usine-digitale.fr.https://www.usine-digitale.fr/article/quel-cadre-juridique-international-pour-le-numerique.N534374
- Desforges, A. (2014). *Les représentations du cyberespace : un outil géopolitique*. Cairn.info. https://www.cairn.info/revue-herodote-2014-1-page-67.htm
- Fonteneau, A. (2021, 24 décembre). *Une conférence mondiale sur l'internet s'ouvre en Chine, pays de la censure*. TV5MONDE. https://information.tv5monde.com/info/une-conference-mondiale-sur-l-internet-s-ouvre-en-chine-pays-de-la-censure-207084
- Anonyme. (2022, 1 février). *Digital Report 2021 : les dernières données de notre état des lieux du digital dans le monde.* We Are Social France. https://wearesocial.com/fr/blog/2021/01/digital-report-2021-les-dernieres-donnees-de-notre-etat-des-lieux-du-digital-dans-le-monde/

- Arsène, S. (2019). *La Chine et le contrôle d'Internet. Une cybersouveraineté ambivalente*. Centre Thucydide. https://hal.archives-ouvertes.fr/hal-02166585/document
- Richeri, G. (2018). L'Internet en Chine, entre État et opinion publique. *Les Enjeux de l'information et de la communication*, 19(1), 21-33. https://www.cairn.info/revue-les-enjeux-de-l-information-et-de-la-communication-2018-1-page-21.htm
- Aït-Kacimi, N. (2021, 30 juin). *Le e-yuan, l'anti-bitcoin au service de l'hégémonie de Pékin*. Les Echos. https://www.lesechos.fr/idees-debats/editos-analyses/le-e-yuan-lanti-bitcoin-au-service-de-lhegemonie-de-pekin-1328168
- Areddy, J. T. (2021, 24 octobre). *La Chine, première grande économie à créer sa monnaie numérique*. l'Opinion. https://www.lopinion.fr/international/la-chine-premiere-grande-economie-a-creer-sa-monnaie-numerique
- Luccisan, G. (2021, 4 juin). *Le Digital Yuan : remise en question chinoise de l'ordre monétaire mondial ?* Ecole de Guerre Economique. https://www.ege.fr/infoguerre/le-digital-yuan-remise-en-question-chinoise-de-lordre-monetaire-mondial
- Nicolas, F. (2020). *Dollar contre renminbi : chronique (prématurée) d'un déclin annoncé*. IFRI.org. https://www.ifri.org/sites/default/files/atoms/files/dollar_contre_renminbi_chronique_prematuree_dun_declin_annonce.pdf
- Anonyme. (2020, 11 février). *75 ans de Bretton Woods : pourquoi rien n'a (jamais) marché comme prévu*. Banque de France. https://blocnotesdeleco.banque-france.fr/billet-de-blog/75-ans-de-bretton-woods-pourquoi-rien-na-jamais-marche-comme-prevu
- Chen, M. K. G. Q. (2015b, mars 9). *Ultimes préparatifs pour le système chinois de paiements internationaux*. Reuters. https://www.reuters.com/article/chine-paiements-yuan-idFRL5N0WB1CG20150309
- Cimino, V. (2022, 8 avril). *Pékin s'associe à SWIFT pour accélérer le déploiement international du yuan numérique*. Siècle Digital. https://siecledigital.fr/2021/02/08/pekin-swift-yuan-numerique/
- Anonyme. (2021b). *Focus sur les start-up de l'X dédiées aux crypto-actifs et à la blockchain en pleine Bitcoin-mania | FX-Conseil*. Portail Polytechnique. https://portail.polytechnique.edu/fxconseil/fr/focus-sur-les-start-de-lx-dediees-aux-crypto-actifs-et-la-blockchain-en-pleine-bitcoin-mania
- Aveni, T., & Roest, J. (2017). *Chine - Alipay et WeChat Pay : atteindre les utilisateurs ruraux*. CGAP. https://www.cgap.org/sites/default/files/Brief-Chinas-Alipay-and-WeChat-Pay-Dec-2017-French.pdf
- Courrier International. (2021b, septembre 24). *Finance. Non au bitcoin : la Chine déclare "illégales" toutes les transactions en cryptomonnaies*. https://www.courrierinternational.com/article/finance-non-au-bitcoin-la-chine-declare-illegales-toutes-les-transactions-en-cryptomonnaies

- Anonyme, F. (2021, 24 septembre). *La Chine juge illégales les transactions financières en cryptomonnaies*. France 24. https://www.france24.com/fr/%C3%A9co-tech/20210924-la-chine-juge-ill%C3%A9gales-les-transactions-financi%C3%A8res-en-cryptomonnaie

Chapitre 2 : Développer l'écosystème cyber chinois pour une hégémonie économique

- Roy, M. (2016, 26 avril). *Shenzhen : une zone économique spéciale en Chine populaire*. Persée. https://www.persee.fr/doc/receo_0338-0599_1983_num_14_3_2451
- Girardot, P. E. (2009). *TRAVERSER LA RIVIÈRE EN TÂTONNANT PIERRE À PIERRE - 摸着石头过河.* Nouvelles du Monde. https://www.lajauneetlarouge.com/wp-content/uploads/2014/10/698-page-058-061.pdf
- China Academy of Information and Communications. (2018). *White Paper on China International Optical Cable Interconnection*. CAICT. http://www.caict.ac.cn/english/
- Boschet, A., Chimenti, J., Mera Leal, N. et Duval, T. (2019) *Chine Digitale Dragon Hacker de puissance*. Editions VA. Editions-Collection Guerre de l'information.
- Lulu, F. (2019). *Taobao Villages - The Emergence of a New Pattern of Rural Ecommerce in China and its Social Implications*. Friedrich Ebert Stiftung. http://library.fes.de/pdf-files/bueros/indonesien/15198-20180218.pdf
- Huang, Y., & Wang, X. (2020, 1 octobre). *Mobile Payment in China : Practice and Its Effects**. MIT Press. https://direct.mit.edu/asep/article/19/3/1/93345/Mobile-Payment-in-China-Practice-and-Its-Effects
- Anonyme. (2019, 28 janvier). *Les BATX, sous l'empire du Milieu*. Décideurs Magazine. https://www.magazine-decideurs.com/news/les-batx-sous-l-empire-du-milieu
- The Economist. (2012, 24 avril). *Avatar 2 : Made in China?* https://www.economist.com/analects/2012/04/24/avatar-2-made-in-china
- Dong, Y. (2016, 18 mars). *AlphaGo and the Clash of Civilizations*. Foreign Policy. https://foreignpolicy.com/2016/03/18/china-go-chess-west-east-technology-artificial-intelligence-google/#:%7E:text=The%20historic%20match%20attracted%20wide,Western%20technology%20and%20Eastern%20culture.
- Schaeffer, F. (2020, 20 février). *La Chine prête à tout pour être le leader mondial de l'IA*. Les Echos.https://www.lesechos.fr/tech-medias/intelligence-artificielle/la-chine-prete-a-tout-pour-etre-le-leader-mondial-de-lia-1173173
- Champeau, G. (2015, 15 mai). *Google battu par le Chinois Baidu sur la reconnaissance d'images*. Numerama. https://www.numerama.com/sciences/33099-google-battu-par-le-chinois-baidu-sur-la-reconnaissance-d-images.html

- Anonyme. (2021). *OECD Digital Economy Papers*. OECD iLibrary. https://www.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-papers_20716826
- Chen, S. (2018, 6 février). *China's plan to use artificial intelligence to boost the thinking skills of nuclear submarine commanders*. South China Morning Post. https://www.scmp.com/news/china/society/article/2131127/chinas-plan-use-artificial-intelligence-boost-thinking-skills
- Fischer, S.C. *Intelligence artificielle: Les ambitions de la Chine.* (Février 2018) Center for Security Studies (CSS) de l'ETH Zurich. CSSAnalyse220-FR.pdf (ethz.ch)
- Salah, R. (2021, 20 octobre). *Route de la soie numérique – Géostratégie des câbles sous-marins*. Observatoire Français des Nouvelles Routes de la Soie. https://observatoirenrs.com/2021/10/06/route-de-la-soie-numerique-chine/
- Ghiasy, R., & Krishnamurthy, R. (2021, 14 avril). *China's Digital Silk Road and the Global Digital Order*. The Diplomat. https://thediplomat.com/2021/04/chinas-digital-silk-road-and-the-global-digital-order/
- Cobinne, A. (2020, 16 avril). *Pourquoi Google Annonce Avoir Atteint La Suprématie Quantique*. Forbes France. https://www.forbes.fr/technologie/pourquoi-google-annonce-avoir-atteint-la-suprematie-quantique/
- Bobier, J., Langione, M., Tao, E., & Gourévitch, A. (2022, 9 mai). *What Happens When 'If' Turns to 'When' in Quantum Computing?* France FR. https://www.bcg.com/fr-fr/publications/2021/building-quantum-advantage
- Chestnut Greitens, S. *China surveillance state at home and abroad.* (Janvier 2020) Université du Texas à Austin Sheena-Greitens_Chinas-Surveillance-State-at-Home-Abroad_Final.pdf (cpb-us-w2.wpmucdn.com)
- Corpet, A. *La Chine et les Etats-Unis signent la phase 1 de leur accord commercial.* (15 Janvier 2020) RFI.fr La Chine et les États-Unis signent la phase 1 de leur accord commercial (rfi.fr)
- Hassan, S.*Why did Huawei get banned by the US ?* (24 mai 2019) the planetoday.com Why did Huawei get banned by the US? - Complete details
- Ovide, S. *A capitalist fix to the digital divide.* (22 septembre 2020) NYTimes.com A Capitalist Fix to the Digital Divide - The New York Times (nytimes.com)
- Brown, R. *Mark Zuckerberg warns about China's "dangerous" approach to internet.* (18 mars 2020) CNBC.com Mark Zuckerberg warns about China's 'dangerous' approach to internet (cnbc.com)
- Cheng, E. *Huawei expects 2021 revenue to drop by 28,9 % as sanctions drag on.* (30 decembre 2021) CNBC.com Huawei expects 2021 revenue to drop by 28.9% as sanctions drag on (cnbc.com)
- Rolander, N. *Ericsson Reports Profit, Market Share gains after Huawei Ban* (21 octobre 2020) Bloomberg.com Ericsson Reports Profit, Market Share Gains After Huawei Ban - Bloomberg

- Yanping L. et Yuan G. *China orders government, state firms to replace foreign computers.* (6 mai 2022). Bloomerg.com China Orders Government, State Firms to Replace Foreign Computers - Bloomberg
- Kharpal, A. *China reportedly orders state offices to remove foreign tech* (9 decembre 2019) CNBC.com China reportedly orders state offices to remove foreign tech (cnbc.com)
- Anonyme. *TSMC says has begun construction at its Arizona chip factory site.* (2 juin 2021) Reuters.com TSMC says has begun construction at its Arizona chip factory site | Reuters
- Durier, P.M. *Intrigue dans le détroit de Formose autour de la loyauté des ingénieurs taïwanais dans le domaine des semi-conducteurs.* (14 avril 2022) Portail-ie.fr Intrigue dans le détroit de Formose autour de la loyauté des ingénieurs taiwanais dans le domaine des semi-conducteurs | Portail de l'IE (portail-ie.fr)
- Meredith, S. *Biden says U.S willing to use force to defend Taiwan - prompting China backlash.* (23 mai 2022) CNBC.com Biden says U.S. willing to use force to defend Taiwan — prompting China backlash (cnbc.com)
- Anonyme. Chine, l'empire du contrôle. (2020, février 19). *Le Monde.fr*. https://www.lemonde.fr/idees/article/2020/02/19/chine-l-empire-du-controle_6030084_3232.html
- Anonyme. Comment la Chine durcit sa guerre d'influence pour démontrer sa puissance. (2021, septembre 3). *Le Monde.fr*. https://www.lemonde.fr/international/article/2021/09/03/la-chine-durcit-sa-guerre-d-influence-a-l-echelle-planetaire_6093206_3210.html
- Anonyme. *DEF CON® China Hacking Conference*. (s. d.). https://defcon.org/html/defcon-china/dc-cn-index.html
- Defranoux, L. (s. d.). *Opérations d'influence : Les «Trois Guerres» du Parti communiste chinois*. Libération. https://www.liberation.fr/international/asie-pacifique/operations-dinfluence-les-trois-guerres-du-parti-communiste-chinois-20210921_BVEZX45WV5GRZDWJITVOFQLU6E/
- Charon, P., & Jeangène Vilmer, J. B. (2021). *Les opérations d'influence chinoises*. IRSEM. https://www.irsem.fr/rapport.html
- Noe, J.B. *Le contrôle social chinois : Le numérique pour surveiller la population*. (2020, décembre 17). Aleteia. https://fr.aleteia.org/2020/12/17/le-controle-social-chinois-le-numerique-pour-surveiller-la-population/
- Yan, C. *LE MOT DE LA SEMAINE. "Mianzi" : La Face*. (2009, juin 11). Courrier international. https://www.courrierinternational.com/article/2008/07/31/mianzi-la-face
- Anonyme. Les nouvelles technologies au service du contrôle social en Chine. (2019, octobre 16). *Rotek*. https://rotek.fr/nouvelles-technologies-au-service-controle-social-chine/
- Anonyme. *Manipulation, fake news, Covid : Comment la Chine mène une guerre d'influence mondiale*. (s. d.). ladepeche.fr. https://www.ladepeche.fr/2021/09/20/manipulation-fake-news-covid-comment-la-chine-mene-une-guerre-dinfluence-mondiale-9802154.php

- Marc. (s. d.). TianfuCup : Les experts en sécurité piratent près de 2 millions de dollars américains | - Le media 05. https://www.lemedia05.com/tianfucup-les-experts-en-securite-piratent-pres-de-2-millions-de-dollars-americains/

- Poujade, O. (2021a, septembre 20). *Armée de trolls, « loups guerriers », web vitrines : Plongée dans la nouvelle cyberpropagande chinoise*. Radio France. https://www.radiofrance.fr/franceculture/armee-de-trolls-loups-guerriers-web-vitrines-plongee-dans-la-nouvelle-cyberpropagande-chinoise-5843664

- Poujade, O. (2021b, septembre 20). *La stratégie d'influence chinoise : Un réseau tentaculaire qui veut désormais s'imposer au reste du monde*. Radio France. https://www.radiofrance.fr/franceculture/la-strategie-d-influence-chinoise-un-reseau-tentaculaire-qui-veut-desormais-s-imposer-au-reste-du-monde-7980973

- *Promesse de la technologie—Faits marquants de DEF CON China 1.0*. (2019, juin 5). The Cloudflare Blog. http://blog.cloudflare.com/fr-fr/technologys-promise-def-con-china-1-0-highlights-fr-fr/

- *TAIWAN : TeamT5, de la menace cyber chinoise à la contre-influence - 18/03/2022*. (2022, mars 18). Intelligence Online. https://www.intelligenceonline.fr/surveillance--interception/2022/03/18/teamt5-de-la-menace-cyber-chinoise-a-la-contre-influence,109761129-gra

- L. Bu ,V. Chung , N. Leung , K. Wei Wang , B. Xia, C. Xia, (2021) "The Future of Digital Innovation in China: Megatrends Shaping One of the World's Fastest Evolving Digital Ecosystems", *McKinsey and Company*, https://www.mckinsey.com/featured-insights/china/the-future-of-digital-innovation-in-china-megatrends-shaping-one-of-the-worlds-fastest-evolving-digital-ecosystems

- Xi Jinping The Governance of China III "Enhance Cyber Capabilities Through Innovation", *Quishi*, http://en.qstheory.cn/2022-04/25/c_744275.htm

- M. BORAK, (2021), "China drafts three-year plan to boost its cybersecurity industry amid increasing concerns for data safety", *South China Morning Post*, https://www.scmp.com/tech/policy/article/3140963/china-drafts-three-year-plan-boost-its-cybersecurity-industry-amid

- R. Creemers, (2020), "Comment la Chine projette de devenir une cyberpuissance", *Cairn.info*, https://doc-center.ocg.msf.org/doc_num.php?explnum_id=4298

- Anonyme. (2020) "Les capacités d'innovation croissante de la Chine" *CGTN Français* https://www.youtube.com/watch?v=n0HHMb6kPKo

- L. Bu ,V. Chung , N. Leung , K. Wei Wang , B. Xia, C. Xia, (2021) "The Future of Digital Innovation in China: Megatrends Shaping One of the World's Fastest Evolving Digital Ecosystems", *McKinsey and Company*, https://www.mckinsey.com/featured-insights/china/the-future-of-digital-innovation-in-china-megatrends-shaping-one-of-the-worlds-fastest-evolving-digital-ecosystems

- McKinsey Global institute, (2014) "McKinsey Global InstituteChina's digital transformation : The Internet's impact on productivity and growth" *McKinsey and Company*

https://www.mckinsey.com/~/media/mckinsey/industries/technology%20media%20and%20telecommunications/high%20tech/our%20insights/chinas%20digital%20transformation/mgi%20china%20digital%20full%20report.pdf

- B. TERRASSON, (2021) "La Chine prépare un plan sur trois ans pour stimuler son secteur de la cybersécurité" *Siècle Digital*, https://siecledigital.fr/2021/07/15/chine-plan-cybersecurite/
- "About ZUU, introduction" *Zenhgzou university*, http://english.zzu.edu.cn/About_ZZU/Introduction.htm
- Zeng Yong, "Message from president" *University of electronic science and technology of China*, https://en.uestc.edu.cn/About_UESTC/Message_from_the_President.htm
- "General information", *Tsinghua university*, https://www.tsinghua.edu.cn/en/About/General_Information.htm
- "Study in China" *Study portal master*, https://www.mastersportal.com/study-options/270156099/cyber-security-china.html
- LexisNexis PatentSight team, (2018), "The Top 20 Most Innovative Chinese Universities", *PatentSight IP Analytics Blog*, https://www.patentsight.com/en/ip-analytics-blog/the-top-20-most-innovative-chinese-universities
- LexisNexis PatentSight team, (2018), "The Top 20 Most Innovative Chinese Universities", *PatentSight IP Analytics Blog*, https://www.patentsight.com/en/ip-analytics-blog/the-top-20-most-innovative-chinese-universities
- Distance Education, (2019) "Digital transformation in higher education: critiquing the five-year development plans (2016-2020) of 75 Chinese universities" *Taylor and Francis Online* *https://www.tandfonline.com/doi/abs/10.1080/01587919.2019.1680272*
- Zak Dychtwald, (2021) "China's New Innovation Advantage", *Harvard business review*, https://hbr.org/2021/05/chinas-new-innovation-advantage
- "La Chine, nouvel eldorado de la distribution digitale", *ESCP business School*, https://escp.eu/fr/news/la-chine-nouvel-eldorado-de-la-distribution-digitale
- (2018) " Répartition de la population en Chine en 2018, par groupe d'âge", *Statista*, https://fr.statista.com/statistiques/666288/repartition-population-par-groupe-d-age-chine/
- I.Attané, (2016), "La fin de l'enfant unique en Chine ?", *Cairn*, https://www.cairn.info/revue-population-et-societes-2016-7-page-1.htm
- GobalData, "Apple diversifie sa chaîne d'approvisionnement mais maintient la Chine au centre", *Verdict*, https://www.verdict.co.uk/apple-supply-chain-china/
- CGTN Français, "La Chine resplendissante - Technologie et innovation", *Youtube* *https://www.youtube.com/watch?v=SGK0eTyWKVQ*

Chapitre 3 : Projections militaires et para-militaires dans le cyber-espace

- Ellis, J. M. (2010). CHINESE CYBER ESPIONAGE : A COMPLEMENTARY METHOD TO AID PLA MODERNIZATION. *NAVAL POSTGRADUATE SCHOOL*. https://www.hsdl.org/?view&did=790444
- APT1 : Exposing One of China's Cyber Espionage Units | Mandiant. (2013). Mandiant. https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units
- Abbas, H. (2020). *'Country Of Spies' : Why China Runs The Risk Of Being Called The Hub Of Espionage After 'Data Leak' ?* Latest Asian, Middle-East, EurAsian, Indian News. https://eurasiantimes.com/country-of-spies-why-china-runs-the-risk-of-being-called-the-hub-of-espionage-after-data-leak/
- Al Jazeera. (2021). *China : Communist Party passes resolution on history to elevate Xi*. https://www.aljazeera.com/news/2021/11/11/china-communist-party-passes-resolution-on-history-to-elevate-xi
- Belk, R., & Noyes, M. (2012). *On the Use of Offensive Cyber Capabilities : A Policy Analysis on Offensive US Cyber Policy*. Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/use-offensive-cyber-capabilities-policy-analysis-offensive-us-cyber-policy
- Carlson, K. B. (2012, 22 août). *China's state-run news agency being used to monitor critics in Canada : reporter*. National Post. https://nationalpost.com/news/canada/notes-going-to-china-not-public-canadian-speaks-out-about-split-with-xinhua-news-agency
- Chansoria, D. M. (2021). *'Sharp Eyes' : Communist China Spies on Its Citizens at Home and Abroad*. JAPAN Forward. https://japan-forward.com/sharp-eyes-communist-china-spies-on-its-citizens-at-home-and-abroad/
- Chase, S. (2011). *Chinese ex-spy warns Canada about how Beijing targets politicians*. The Globe and Mail. https://www.theglobeandmail.com/news/politics/chinese-ex-spy-warns-canada-about-how-beijing-targets-politicians/article547580/
- Claverie, B., Prébot, B., Buchler, N., & Du Cluzel, F. (2021). *Cognitive Warfare - La Guerre Cognitique*. NATO-CSO-STO.
- *Coronavirus : colère en Chine après la mort d'un médecin lanceur d'alerte*. (2020). TV5MONDE.https://information.tv5monde.com/info/coronavirus-colere-en-chine-apres-la-mort-d-un-medecin-lanceur-d-alerte-345563
- *Ex-Chinese spy says politicians are targets*. (2011). CTVNews. https://www.ctvnews.ca/ex-chinese-spy-says-politicians-are-targets-1.733398
- FranceInfo avec AFP. (2020). *"Il a donné l'alerte au prix de sa vie" : comment Li Wenliang, le médecin chinois qui a tenté de prévenir le monde sur le coronavirus, est devenu un héros national*. FranceInfo. https://www.francetvinfo.fr/sante/maladie/coronavirus/il-a-donne-l-

alerte-au-prix-de-sa-vie-comment-li-wenliang-le-medecin-chinois-qui-a-tente-de-prevenir-le-monde-sur-le-coronavirus-est-devenu-un-heros-national_3816463.html

- Guibert, N., & Nevé, S. L. (2021). *Un partenariat passé entre ParisTech et une université chinoise inquiète les services de sécurité français*. Le Monde.fr. https://www.lemonde.fr/societe/article/2021/09/15/un-partenariat-passe-entre-paristech-et-une-universite-chinoise-inquiete-les-services-de-securite-francais_6094764_3224.html

- Kumar, M. (2015). *China Finally Admits It Has Army of Hackers*. The Hacker News. https://thehackernews.com/2015/03/china-cyber-army.html

- McCord, E. A. (1988). Militia and Local Militarization in Late Qing and Early Republican China. *Modern China*, *14*(2), 156–187.

- *Never Seek Hegemony : China's Voice at the UN General Assembly*. (2021). Global Times. https://www.globaltimes.cn/page/202107/1227967.shtml

- O'Connor, T. (2011). The Jester Dynamic : A Lesson In Assymetric Unmanaged Cyber Warfare. *GIAC*.

- Raud, M. (2016). *China and Cyber : Attitudes, Strategies, Organisation*. NATO-CCDCOE. https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf

- Rubio, M. (2022). *Rubio Calls for End to U.S-China University Partnerships that Support the Development of Chinese Military Technologies*. U.S. Senator for Florida, Marco Rubio. https://www.rubio.senate.gov/public/index.cfm/2022/2/rubio-calls-for-end-to-u-s-china-university-partnerships-that-support-the-development-of-chinese-military-technologies

- Van Beynen, M. (2020). *University of Canterbury collaborating with Institute linked to Chinese military*. Stuff. https://www.stuff.co.nz/national/122196854/university-of-canterbury-collaborating-with-institute-linked-to-chinese-military

- Wu, F., Su, J., & Zeng, J. (2021). *How Does the Chinese Government Select and Funding High-Level Talents ? An Empirical Study Based on the Resumes of Talents*. Frontiers. https://www.frontiersin.org/articles/10.3389/fpsyg.2021.687447/full

- Zarate, J. C. (2015). *The Cyber Financial Wars on the Horizon : The Convergence of Financial and Cyber Warfare and the Need for a 21st Century National Security Response*. The Aspen Institute. https://www.aspeninstitute.org/wp-content/uploads/2016/05/Cyber_Financial_Wars.pdf

- Allen, K. W., Mulvaney, B. S., & Char, J. (2020). *Ongoing organizational reforms of the People's Liberation Army Air Force*. Journal of Strategic Studies. https://www.tandfonline.com/doi/abs/10.1080/01402390.2020.1730818

- Andress, J., & Winterfeld, S. (2014). *Cyber Warfare : Techniques, Tactics and Tools for Security Practitioners. Second Edition*. Elsevier Science & ; Technology Books.

- BBC News. (2019, 20 février). *Fang Fenghui : China's ex-top general jailed for life*. https://www.bbc.com/news/world-asia-china-47306275

- Burdette, L. (2021). *Leveraging Submarine Cables for Political Gain : U.S. Responses to Chinese Strategy*. Journal of Public and International Affairs. https://jpia.princeton.edu/news/leveraging-submarine-cables-political-gain-us-responses-chinese-strategy
- Col. Shukla, A. (2017). *Chinese Military Reform, 2013-2030*. IPCS | Institute Of Peace and Conflict Studies. http://www.ipcs.org/comm_select.php?articleNo=5361
- Easton, I. (2019). *China's Top Five War Plans*. Project 2049 Institute. https://project2049.net/wp-content/uploads/2019/01/Chinas-Top-Five-War-Plans_Ian_Easton_Project2049.pdf
- Fraser, N., & Vanderlee, K. (2019). *Achievement Unlocked : Chinese Cyber Espionage Evolves To Support Higher Level Missions*. FIREEYE. https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
- Glaser, B. S., & Funaiole, M. P. (2020). *Perspectives on Taiwan : Insights from the 2019 Taiwan-U. S. Policy Program*. Rowman & Littlefield Publishers, Incorporated.
- INSIKT GROUP. (2021). *China's PLA Unit 61419 Purchasing Foreign Antivirus Products, Likely for Exploitation*. Recorded Future. https://www.recordedfuture.com/china-pla-unit-purchasing-antivirus-exploitation
- Lampton, D. M., & Lieberthal, K. G. (2018). *Bureaucracy, Politics, and Decision Making in Post-Mao China*. University of California Press.
- Luo, S., & Panter, J. G. (2021). *China's Maritime Militia and Fishing Fleets*. Army University Press. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2021/Panter-Maritime-Militia/
- Maurer, T. (2018). *Cyber mercenaries : The state, hackers, and power*.
- Meilinger, P. S. (2010). *China and Clausewitz*. Science Applications International Corporation.
- *Military Regions / Military Area Commands*. (s. d.). GlobalSecurity.org. https://www.globalsecurity.org/military/world/china/mr.htm
- *Missiles of China | Missile Threat*. (2021). CSIS Missile Defense Project. https://missilethreat.csis.org/country/china/
- Office of the Secretary of Defense. (2021). Military and Security Developments Involving the People's Republic of China. *Annual Report to Congress*.
- *Perspectives on Taiwan : Insights from the 2018 Taiwan-U.S. Policy Program*. (2019). Center for Strategic & International Studies.
- Pomerleau, M. (2020). *China moves toward new 'intelligentized' approach to warfare, says Pentagon*. C4ISRNet. https://www.c4isrnet.com/battlefield-tech/2020/09/01/china-moves-toward-new-intelligentized-approach-to-warfare-says-pentagon/

- Pryor, C. D. (2019). *Taiwan's Cybersecurity Landscape and Opportunities for Regional Partnership*. CSIS.
- Shakarian, P., Shakarian, J., & Ruef, A. (2013). *Introduction to Cyber-Warfare A Multidisciplinary Approach*. Elsevier Science & ; Technology Books.
- *APT17 is run by the Jinan bureau of the Chinese Ministry of State Security*. (2019). Intrusion Truth. https://intrusiontruth.wordpress.com/2019/07/24/apt17-is-run-by-the-jinan-bureau-of-the-chinese-ministry-of-state-security/
- Culafi, A. (2020). *CrowdStrike founder : China hacking indictments are working*. SearchSecurity. https://www.techtarget.com/searchsecurity/news/252479273/CrowdStrike-founder-China-hacking-indictments-are-working
- *Cyber Attacks on NATO Countries Surge by 116% - Check Point Software*. (2022). Check Point Software. https://blog.checkpoint.com/2022/03/21/cyber-attacks-from-chinese-ips-on-nato-countries-surge-by-116/
- *The Elderwood Project : the art of war*. (2012). Proactive protection of the computer against malicious software, ATM protection, data leakage prevention. http://www.safensoft.com/archiv/p/773/1733/
- Girard, E. (2022). *LinkedIn, DGSE, offres faramineuses... Comment la Chine nous espionne*. LExpress.fr. https://www.lexpress.fr/actualite/societe/linkedin-dgse-offres-faramineuses-comment-la-chine-nous-espionne_2170186.html
- Jennings, R. (2019). *Trump Secret Service USB OpSec FAIL : 'Spy' Story Gets Weirder*. Security Boulevard. https://securityboulevard.com/2019/04/trump-secret-service-usb-opsec-fail-spy-story-gets-weirder/
- Kitchen, K., & Drexel, B. (2022). *Securing Taiwan Requires Immediate Unprecedented Cyber Action*. Lawfare. https://www.lawfareblog.com/securing-taiwan-requires-immediate-unprecedented-cyber-action
- *MVISION Insights : Winnti Group Targeting Universities In Hong Kong*. (2020). McAfee. https://kc.mcafee.com/corporate/index?page=content&id=KB92731&locale=en_US
- WEareTROOPERS. (2017). *TR17 - Surprise Bitches ! - The Grugq* [Vidéo]. YouTube. https://www.youtube.com/watch?v=wP2J9aYM6Oo
- *Who is Mr Guo ?* (2019). Intrusion Truth. https://intrusiontruth.wordpress.com/2019/07/17/who-is-mr-guo/
- Wilkie, C. (2021). *U.S., NATO and EU to blame China for cyberattack on Microsoft Exchange servers*. CNBC. https://www.cnbc.com/2021/07/19/nato-and-eu-launch-a-cyber-security-alliance-to-confront-chinese-cyberattacks.html
- Windrem, R. (1999). *When it comes to spying, U.S. is as insatiable as China*. Intelligence Resource Program. https://irp.fas.org/news/1999/06/990602-275397.htm
- FBI. (2022). The China Threat - Wanted by the FBI. https://www.fbi.gov/investigate/counterintelligence/the-china-threat

- T. Maurer, (2018) Cyber Mercenaries, The State, Hackers, and Power, Cambridge University Press.
- Sun Tzu, Xīn Shìjiè, The Art of (Informationized) War: Updating The Oldest Military Treatise In The World, publié indépendamment.
- Zhengrong C., Longhai S., and Yin Y., (2014) eds., Informatized Army Operations [信息化陆军作战], *National Defense University Press,* 109–314
- Wenxian, Y(2009), ed., Course Book on Joint Campaigns and Information Operations [联合战役信息作战教程], *National Defense University Press,*, 271–326;
- Zhengrong C., Runbo W., et Jianjun S., (2008) eds., Informatized Joint Operations [信息化联合作战], *Liberation Army Press,*, 145–323
- Anonyme, (2020, décembre 18). China « plots to use underwater cable network » to plunder secrets from West. *The Sun.* https://www.thesun.co.uk/news/13517388/china-spying-beijing-underwater-cable-secrets-west/
- Anonyme, (2011, décembre 1). 行政院全球資訊網https://nicst.ey.gov.tw/en/FD815304EBFFE6FC/639d32e8-2a07-40da-b033-bc6c95d015ce
- Anonyme, 30% of Global Cyber Attacks Originate from China. Is Beijing the Ultimate Virtual-threat Plotter? (2021, mars 5). News18. https://www.news18.com/news/india/30-of-global-cyber-attacks-originate-from-china-is-china-the-ultimate-virtual-threat-plotter-3502994.html
- P. J. C. L. 23 octobre 2018, M. L. 11 D. 2018. (2018, octobre 23). Espionnage : Comment la Chine tente de recruter des Français. *leparisien.fr*. https://www.leparisien.fr/international/espionnage-comment-la-chine-tente-de-recruter-des-francais-23-10-2018-7925739.php
- About NCCST - National Center for Cyber Security Technology. (2022).https://www.nccst.nat.gov.tw/About?lang=en
- Allen, K. W., Mulvaney, B. S., & Char, J. (2021). Ongoing organizational reforms of the People's Liberation Army Air Force. *Journal of Strategic Studies*, 44(2), 184-217. https://doi.org/10.1080/01402390.2020.1730818
- Ankel, S. (s. d.). China accused of planning to exploit undersea cable networks to spy on other countries, report says. *Business Insider*. https://www.businessinsider.com/china-accused-of-wanting-steal-data-using-undersea-cable-networks-2020-12
- Antoine, I. (2021, octobre 25). Ingérences étrangères : La DGSI change de braquet. *Challenges.* https://www.challenges.fr/entreprise/defense/ingerences-etrangeres-dans-la-recherche-comment-dgsi-a-change-de-braquet_785913
- Antoine Izambard sur Twitter. (s. d.). *Twitter*.https://twitter.com/a_izambard/status/1453252520629964803

- APT17, Deputy Dog, Group G0025 | MITRE ATT&CK. (2020). https://attack.mitre.org/groups/G0025/
- Barrett, J., & Tian, Y. L. (2021, juin 18). EXCLUSIVE Pacific undersea cable project sinks after U.S. warns against Chinese bid. *Reuters.* https://www.reuters.com/world/asia-pacific/exclusive-pacific-undersea-cable-project-sinks-after-us-warns-against-chinese-2021-06-18/
- Burke, E., Gunness, K., Cooper, C., & Cozad, M. (2020). People's Liberation Army Operational Concepts. *RAND Corporation.* https://doi.org/10.7249/RRA394-1
- Burton, R. (s. d.). The People's Liberation Army Strategic Support Force. 14. China. *National Defense University Press.* https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1748555/chinas-strategic-support-force-a-force-for-a-new-era/
- Anonyme, (s. d.). China cyber attacks : The current threat landscape, *ironnet.com.* https://www.ironnet.com/blog/china-cyber-attacks-the-current-threat-landscape
- Anonyme, (s. d.).China Spying on Undersea Internet Cables. *Schneier on Security.* https://www.schneier.com/blog/archives/2019/04/china_spying_on.html
- Anonyme, (2018, octobre 4).China Used a Tiny Chip in a Hack That Infiltrated U.S. Companies. Bloomberg.Com. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies
- Nouwens M. et Legarda H. (s. d.).China's pursuit of advanced dual-use technologies IISS. https://www.iiss.org/blogs/research-paper/2018/12/emerging-technology-dominance
- Herard P. (2019, décembre 12) Chine : Le gouvernement veut remplacer les ordinateurs et logiciels étrangers dans son administration. *TV5MONDE.* https://information.tv5monde.com/info/chine-le-gouvernement-veut-remplacer-les-ordinateurs-et-logiciels-etrangers-dans-son
- Costello, J., & McReynolds, J. (s. d.). CHINA STRATEGIC PERSPECTIVES 13. 84.
- Critical Node : Taiwan's Cyber Defense and Chinese Cyber-Espionage. *Jamestown.* https://jamestown.org/program/critical-node-taiwans-cyber-defense-and-chinese-cyber-espionage/
- Anonyme, (2022, mars 21). Cyber Attacks on NATO Countries Surge by 116%. *Check Point Software.*https://blog.checkpoint.com/2022/03/21/cyber-attacks-from-chinese-ips-on-nato-countries-surge-by-116/
- Anonyme. (2022, mars 22).Cyber-attacks against NATO countries from Chinese IP addresses double. *Digit.* https://www.digit.fyi/cyberattacks-against-nato-chinese-ip-double/
- FBI, (s. d.).Cyber's Most Wanted. *Federal Bureau of Investigation.* https://www.fbi.gov/wanted/cyber
- Cornevin C. et Chichizola J. (2018, octobre 22). Espionnage chinois : La note d'alerte des services secrets français.LEFIGARO.

https://www.lefigaro.fr/international/2018/10/22/01003-20181022ARTFIG00305-espionnage-chinois-la-note-d-alerte-des-services-secrets.php

- Faligot, R. (2022). Les Services secrets chinois : De Mao au Covid-19. *Nouveau Monde Editions.*
- Garafola, C. L. (2016, septembre 23). PLA Reforms and Their Ramifications. https://www.rand.org/blog/2016/09/pla-reforms-and-their-ramifications.html
- Brostra R. Guoanbu, (2018, décembre 26) la puissance du renseignement chinois.. Le Temps. https://www.letemps.ch/monde/guoanbu-puissance-renseignement-chinois
- Hjortdal, M. (2011). China's Use of Cyber Warfare : Espionage Meets Strategic Deterrence. Journal of Strategic Security, 4(2), 1-24.
- Burdette L. (2021, mai 5) Leveraging Submarine Cables for Political Gain : U.S. Responses to Chinese Strategy. . Journal of Public and International Affairs.https://jpia.princeton.edu/news/leveraging-submarine-cables-political-gain-us-responses-chinese-strategy
- Lieberthal, K., & Singer, P. (2012). *Cybersecurity and U.S.-China Relations*. Brookings - China Center. https://www.brookings.edu/wp-content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf
- Mazzetti, M., Goldman, A., Schmidt, M. S., & Apuzzo, M. (2017, mai 20). Killing C.I.A. Informants, China Crippled U.S. Spying Operations. The New York Times. https://www.nytimes.com/2017/05/20/world/asia/china-cia-spies-espionage.html
- McCord, E. A. (1988). Militia and Local Militarization in Late Qing and Early Republican China : The Case of Hunan. *Modern China,* 14(2), 156-187.
- Ministry of National Defense launches new cybersecurity command—New Southbound Policy Portal. (s. d.). *New Southbound Policy.* https://nspp.mofa.gov.tw/nsppe/nspp.mofa.gov.tw/nsppe/content_tt.php?unit=2&post=117794
- Koichiro T. (2022, avril 13) New Tech, New Concepts : China's Plans for AI and Cognitive Warfare. *War on the Rocks.* https://warontherocks.com/2022/04/new-tech-new-concepts-chinas-plans-for-ai-and-cognitive-warfare/
- Orinx, K., & truye de Swielande, T. (2022). *China and Cognitive Warfare : Why Is the West Losing ?* HAL. https://hal.archives-ouvertes.fr/hal-03635930/document
- PLA Strategic Support Force. (2016, décembre 18). *China Defence Today.* https://sinodefence.wordpress.com/pla-strategic-support-force/
- Pomerleau, M. (2020, septembre 1). China moves toward new 'intelligentized' approach to warfare, says Pentagon. *C4ISRNet.* https://www.c4isrnet.com/battlefield-tech/2020/09/01/china-moves-toward-new-intelligentized-approach-to-warfare-says-pentagon/

- Private Sector, & Iasiello, E. (2016). China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities. *Journal of Strategic Security*, 9(2), 47-71. https://doi.org/10.5038/1944-0472.9.2.1489

- Pryor, C. D., Garcia-Millan, T., Gelman, J., Madan, T., Moore, S., Pryor, C., Reijula, L., Smolinske, N., Tensley, B., Weatherby, C., & Yang, J. (2019). Taiwan's Cybersecurity Landscape and Opportunities for Regional Partnership (Perspectives on Taiwan, p. 10-15). *Center for Strategic and International Studies* (CSIS). https://www.jstor.org/stable/resrep22549.5

- Rogin, J. (s. d.). The top 10 Chinese cyber attacks (that we know of). *Foreign Policy*. https://foreignpolicy.com/2010/01/22/the-top-10-chinese-cyber-attacks-that-we-know-of/

- Securing Taiwan Requires Immediate Unprecedented Cyber Action. (2022, janvier 13). *Lawfare*.https://www.lawfareblog.com/securing-taiwan-requires-immediate-unprecedented-cyber-action

- Gouvernement canadien (2018, mai 10). La Loi sur le renseignement national de la Chine et l'avenir des rivalités avec le pays sur le plan du renseignement. *Canada.ca* https://www.canada.ca/fr/service-renseignement-securite/organisation/publications/la-chine-a-lere-de-la-rivalite-strategique/la-loi-sur-le-renseignement-national-de-la-chine-et-lavenir-des-rivalites-avec-le-pays-sur-le-plan-du-renseignement.html

- Anonyme, (2022 Mai) Significant Cyber Incidents | Center for Strategic and International Studies.https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

- Steinke, M. (s. d.). Survival : Global Politics and Strategy Chinese Intelligence in the Cyber Age. https://www.academia.edu/10282732/Survival_Global_Politics_and_Strategy_Chinese_Intelligence_in_the_Cyber_Age_PLEASE_SCROLL_DOWN_FOR_ARTICLE

- Chang Y. (2021 mai 5),Taiwan's president announces new cybersecurity unit. *Taiwan News*.https://www.taiwannews.com.tw/en/news/4194694

- FBI. (s. d.) The China Threat. [Folder]. *Federal Bureau of Investigation.* https://www.fbi.gov/investigate/counterintelligence/the-china-threat

- Corcoran M. (2013, novembre 8).The Chinese Embassy bugging controversy. *ABC News.* https://www.abc.net.au/news/2013-11-08/the-chinese-embassy-bugging-controversy/5079148

- The Elderwood Project : The art of war. (s. d.).http://www.safensoft.com/archiv/p/773/1733/

- Anonyme, (s. d.)Tsai inaugurates National Communications and Cyber Security Center in Taipei—New Southbound Policy Portal . *New Southbound Policy.* https://nspp.mofa.gov.tw/nsppe/nspp.mofa.gov.tw/nsppe/content_tt.php?unit=6&post=145563

- US, D. D., The Conversation. (s. d.). How the Chinese Cyberthreat Has Evolved. *Scientific American.*https://www.scientificamerican.com/article/how-the-chinese-cyberthreat-has-evolved/

- USC US China Institute (2021, November 2) U.S. Dept. Of Defense, Military and Security Developments Involving the People's Republic of China 2021. *US-China Institute.* https://china.usc.edu/us-dept-defense-military-and-security-developments-involving-peoples-republic-china-2021-november-2
- Windrem R. (s. d.) When it comes to spying, U.S. is as insatiable as China.. https://irp.fas.org/news/1999/06/990602-275397.htm
- Chang Y. (2019, juillet 17) Who is Mr Guo? *Intrusion Truth.* https://intrusiontruth.wordpress.com/2019/07/17/who-is-mr-guo/
- Wilkie, C. (2021, juillet 19). U.S., NATO and EU to blame China for cyberattack on Microsoft Exchange servers. *CNBC.* https://www.cnbc.com/2021/07/19/nato-and-eu-launch-a-cyber-security-alliance-to-confront-chinese-cyberattacks.html
- Yasuyuki, S. (2022). The PLA's Pursuit of Enhanced Joint Operations Capabilities. *NIDS.*
- Zetter, K. (2022, mars 29). Unmasking China's State Hackers [Substack newsletter]. *Zero Day*. https://zetter.substack.com/p/unmasking-chinas-state-hackers
- 战略支援部队—中华人民共和国国防部. (s. d.). http://www.mod.gov.cn/power/node_47605.htm
- 新时代的中国国防_白皮书_中国政府网. (s. d.). http://www.gov.cn/zhengce/2019-07/24/content_5414325.htm
- 習近平通令透露的軍事機密（文：孫嘉業） (10:18)—20160825—文摘. (s. d.). 明報新聞網 - 即時新聞 instant news. https://news.mingpao.com/ins/%e6%96%87%e6%91%98/article/20160825/s00022/1472091515819/%e7%bf%92%e8%bf%91%e5%b9%b3%e9%80%9a%e4%bb%a4%e9%80%8f%e9%9c%b2%e7%9a%84%e8%bb%8d%e4%ba%8b%e6%a9%9f%e5%af%86%ef%bc%88%e6%96%87-%e5%ad%ab%e5%98%89%e6%a5%ad%ef%bc%89
- 自由時報電子報. (2015, mars 9). 中國對台網攻大本營 藏身武漢大學—焦點. 自由時報電子報. https://news.ltn.com.tw/news/focus/paper/861206
- Pollpeter, K., & Allen, K. W. *The PLA as Organization v2.0*. DGI Group. https://apps.dtic.mil/sti/pdfs/AD1082742.pdf
- Anonyme. (2015, 21 mars). 第99"虎"落马警示了啥？ - 中国网传媒经济频道. Media China.https://web.archive.org/web/20150416074510/http://media.china.com.cn/cmjujiao/2015-03-21/396575.html
- Stokes, M. A., Lin, J., & Russell Hsiao, L. C. (2011). *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*. Project 2049 Institute. https://project2049.net/wp-content/uploads/2018/05/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf

- Anonyme. (2009). *Tracking GhostNet : Investigating a Cyber Espionage Network*. Information Warfare Monitor. http://www.nartv.org/mirror/ghostnet.pdf
- Mattis, P. (2015, 29 décembre). *China's Military Intelligence System is Changing*. War on the Rocks. https://warontherocks.com/2015/12/chinas-military-intelligence-system-is-changing/
- IASIELLO, Emilio, « China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities », Journal of Strategic Security 9, n° 2, 2016, pp. 45-69. DOI : http://dx.doi.org/10.5038/1944-0472.9.2.1489
- Anonyme. (2021). *China's 14th Five-Year Plan and the Healthcare and Public Health Sector*. HHS Cybersecurity Program. https://www.hhs.gov/sites/default/files/china-fyp-hph-tlp-white.pdf
- Fraser, N., Plan, F., O'leary, J., Cannon, V., Leong, R., Perez, D., & Shen, C. (2019). *APT41 : A Dual Espionage and Cyber Crime Operation | Mandiant*. Mandiant. https://www.mandiant.com/resources/apt41-dual-espionage-and-cyber-crime-operation
- Anonyme. (2010). *(S//REL)BYZANTINE HADES : An Evolution of Collection*. NSA. https://www.eff.org/files/2015/02/03/20150117-spiegel-byzantine_hades_-_nsa_research_on_targets_of_chinese_network_exploitation_tools.pdf
- United States District Court, Central District of California, *United States of America v. Su Bin*. Criminal Complaint. 27 juin 2014. https://www.exportlawblog.com/docs/us_v_su_complaint.pdf
- Anonyme. (2020, 21 juillet). *The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States*. Federal Bureau of Investigation. https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states
- Anonyme. (2019). *INTELLIGENCE REPORT : HUGE FAN OF YOUR WORK : How TURBINE PANDA and China's Top Spies Enabled Beijing to Cut Corners on the C919 Passenger Jet*. CrowdStrike. https://passle-net.s3.amazonaws.com/Passle/5c752afb989b6e0f5cda12f4/MediaLibrary/Document/2019-10-18-10-42-26-646-huge-fan-of-your-work-intelligence-report.pdf
- Pemberton, M., & Stohl, R. (2014, 25 juin). *Wrangling Over Arms Sales to China*. Institute for Policy Studies. https://ips-dc.org/wrangling_over_arms_sales_to_china/
- Fontarensky, I., Perigaud, F., Mouchoux, R., Pernet, C., & Bizeul, D. (2014). *The Eye of the Tiger*. Airbus Defence & Space. https://web.archive.org/web/20140809013259/https://bbuseruploads.s3.amazonaws.com/cybertools/whitepapers/downloads/Pitty%20Tiger%20Final%20Report.pdf?Signature=OJ2d54rxyligtoMeHrs2A/s1jT0=&Expires=1407549773&AWSAccessKeyId=0EMWEFSGA12Z1HF1TZ82
- Greenberg, A. (2018, août 22). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

- Paganini, P. (2019, 2 septembre). *The role of a secret Dutch mole in the US-Israeli Stuxnet attack on Iran*. Security Affairs. https://securityaffairs.co/wordpress/90698/cyber-warfare-2/dutch-mole-stuxnet-attack.html

- Bellovin, S. M., Landau, S., & Lin, H. S. (2017, 31 mars). *Limiting the undesired impact of cyber weapons : technical requirements and policy implications*. OUP Academic. https://academic.oup.com/cybersecurity/article/3/1/59/3097802?login=false

- Smeets, M. (2022, 13 mai). *Going the Extra Mile : What It Takes to Be a Responsible Cyber Power*. Lawfare. https://www.lawfareblog.com/going-extra-mile-what-it-takes-be-responsible-cyber-power

- Anonyme. (2016, 4 novembre). *Department of Defense, « Agreed Operation Glowing Symphony Notification Plan » , November 4 2016, Top Secret. | National Security Archive*. National Security Archive. https://nsarchive.gwu.edu/document/16747-department-defense-agreed-operation-glowing

- Anonyme. (2016b, novembre 8). *USSTRATCOM, Subj : FRAGORD 06 to USSTRATCOM OPORD 8000–17 : Authorization to Conduct Operation GLOWING SYMPHONY, November 8 2016, Secret. | National Security Archive*. National Security Archive. https://nsarchive.gwu.edu/document/16749-usstratcom-subj-fragord-06-usstratcom-opord

- Nye, J. S. (2021, 8 juillet). *Will Biden's red lines change Russia's behaviour in cyberspace?* The Strategist. https://www.aspistrategist.org.au/will-bidens-red-lines-change-russias-behaviour-in-cyberspace/

- Poulsen, K., & Ackerman, S. (2018, 25 octobre). *EXCLUSIVE : 'Lone DNC Hacker' Guccifer 2.0 Slipped Up and Revealed He Was a Russian Intelligence Officer*. The Daily Beast. https://www.thedailybeast.com/exclusive-lone-dnc-hacker-guccifer-20-slipped-up-and-revealed-he-was-a-russian-intelligence-officer

- Anonyme, I. (2021b, septembre 10). *Hello Lionel Richie*. Intrusion Truth. https://intrusiontruth.wordpress.com/2021/09/20/hello-lionel-richie/

- Kadiri, G., & Tilouine, J. (2018, 27 janvier). *A Addis-Abeba, le siège de l'Union africaine espionné par Pékin*. Le Monde.fr. https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html

- Stecklow, S. A. H. (2019, 24 décembre). *Exclusive : Malware broker behind U.S. hacks is now teaching computer skills in China*. Reuters. https://www.reuters.com/article/us-china-usa-cyber-exclusive-idUSKBN1YS0UI

- Anonyme. (2019b, octobre 31). *Why the OPM Hack Is Far Worse Than You Imagine*. Lawfare. https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine

- Nakashima, E. (2015, 10 juillet). *Hacks of OPM databases compromised 22.1 million people, federal authorities say*. Washington Post. https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/

- Nakashima, E. (2014). *Un sous-traitant du DHS subit une grave violation informatique, selon les responsables*. Washington Post. https://www.washingtonpost.com/world/national-security/dhs-contractor-suffers-major-computer-breach-officials-say/2014/08/06/8ed131b4-1d89-11e4-ae54-0cfe1f974f8a_story.html

- Anonyme. (2020a, février 13). *Chinese Military Personnel Charged with Computer Fraud, Economic*. DOJ. https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking

- Anonyme. (2015a). *The Anthem Hack : All Roads Lead to China - ThreatConnect | Risk-Threat-Response*. Threat Connect. https://perma.cc/ZNQ5-325G

- Anonyme. (2019b, mai 9). *Member of Sophisticated China-Based Hacking Group Indicted for Series*. DOJ. https://www.justice.gov/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including

- Harwell, D., & Nakashima, E. (2015, 6 février). *Experts warn that Anthem hack may foreshadow a larger attack*. Washington Post. https://www.washingtonpost.com/business/economy/investigators-suspect-china-may-be-responsible-for-hack-of-anthem/2015/02/05/25fbb36e-ad56-11e4-9c91-e9d2f9fde644_story.html?itid=lk_inline_manual

- Anonyme. (2021b, novembre 16). *APT 10 GROUP*. Federal Bureau of Investigation. https://www.fbi.gov/wanted/cyber/apt-10-group

- Anonyme. (s. d.). *U.S. Department of Health & Human Services - Office for Civil Rights*. Département Américain de La Santé et Des Services Sociaux. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=2AA5AC876FA56C6924880A515E58025A.ajp13w

- Perlroth, N. (2021, 21 juillet). *Chinese Hackers Infiltrate New York Times Computers*. The New York Times. https://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html

- Anonyme. (2022, 18 janvier). *Involuntary Returns – report exposes long-arm policing overseas*. Safeguard Defenders. https://safeguarddefenders.com/en/blog/involuntary-returns-report-exposes-long-arm-policing-overseas

- Xiao, M., & Mozur, P. (2022, 1 janvier). *Chinese Police Hunt Overseas Critics With Advanced Tech*. The New York Times. https://www.nytimes.com/2021/12/31/technology/china-internet-police-twitter.html

- Anonyme. (2022a). *Space Pirates : analyse des outils et connexions d'un nouveau groupe de hackers*. Positive Technologies. https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/space-pirates-tools-and-connections/

- Anonyme. (2018). *Chinese Cyberespionage Originating From Tsinghua University Infrastructure*. Insikt Group. https://go.recordedfuture.com/hubfs/reports/cta-2018-0816.pdf

- Charon, P., & Jeangène Vilmer, J. B. (2021). *Les opérations d'influence chinoises*. IRSEM. https://www.irsem.fr/rapport.html

- Keizer, G. (2010, 6 décembre). *Chinese firm hired Blaster hacking group, says U.S. cable*. Computerworld.https://www.computerworld.com/article/2514740/chinese-firm-hired-blaster-hacking-group--says-u-s--cable.html
- United States District Court, District of Columbia, United States of America v. Jiang Lizhi, Qian Chuan, Fu Qiang. Criminal Case. 27 juin 2014. https://www.justice.gov/opa/press-release/file/1317206/download
- Anonyme. (2022a). *APT41, A DUAL ESPIONAGE AND CYBER CRIME OPERATION*. Mandiant. https://www.mandiant.com/sites/default/files/2022-02/rt-apt41-dual-operation.pdf
- The Diplomat. (2019, 24 septembre). *Expanding Cyber Demands Embolden China's Homegrown Cybersecurity Darlings*. https://thediplomat.com/2019/09/expanding-cyber-demands-embolden-chinas-homegrown-cybersecurity-darlings/
- Recorded Future. (2017, 17 mai). *Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3*. https://web.archive.org/web/20170517234328/https://www.recordedfuture.com/chinese-mss-behind-apt3/
- Anonyme. (2022c). *The Chinese Private Sector Cyber Landscape*. (C) Margin Research. All Rights Reserved. https://margin.re/media/the-private-sector-chinese-offensive-cyber-landscape.aspx
- Anonyme. (s. d.-a). *NSA / CIA*. NSA/CIA. https://www.mpauli.de/nsa-cia.html
- Grugq, T. T. (2018, 14 juin). *Cyber : Ignore the Penetration Testers - thaddeus t. grugq*. Medium. https://medium.com/@thegrugq/cyber-ignore-the-penetration-testers-900e76a49500
- Paz, R. D. (2013). *PlugX : New Tool For a Not So New Campaign | Malware Blog | Trend Micro*. PlugX. https://web.archive.org/web/20130305040841/https://blog.trendmicro.com/trendlabs-security-intelligence/plugx-new-tool-for-a-not-so-new-campaign/
- Anonyme. (2015b, janvier 29). *JPCERT/CC Blog : Analysis of a Recent PlugX Variant - "P2P PlugX"*. PlugX. https://web.archive.org/web/20150222181334/http://blog.jpcert.or.jp/.s/2015/01/analysis-of-a-r-ff05.html
- Perigaud, F. (2014, 29 janvier). *PlugX « v2 » : meet « SController »*. Airbus D&S CyberSecurity Blog. https://web.archive.org/web/20141105025231/http://blog.airbuscybersecurity.com/post/2014/01/PlugX-v2%3A-meet-SController
- Anonyme, A. C. (2022, 9 mars). *Latest changes in PlugX*. Airbus CyberSecurity. https://airbus-cyber-security.com/latest-changes-plugx/
- Anonyme. (2014). *Global Threat Intel Report*. CrowdStrike. https://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf
- Anonyme. (2020a). *Study of the ShadowPad APT backdoor and its relation to PlugX*. Doctor Web. https://st.drweb.com/static/new-

www/news/2020/october/Study_of_the_ShadowPad_APT_backdoor_and_its_relation_to_PlugX_en.pdf

- Hsieh, Y. (2021, 2 septembre). *ShadowPad | A Masterpiece of Privately Sold Malware in Chinese Espionage - SentinelLabs*. SentinelOne. https://web.archive.org/web/20210904104753/https://www.sentinelone.com/labs/shadowpad-a-masterpiece-of-privately-sold-malware-in-chinese-espionage/

- Hannas, W. C., Mulvenon, J., & Puglisi, A. B. (2013). *Chinese Industrial Espionage*. Google Books. https://www.google.com/books/edition/_/sWcolDneRrMC

- Yeh, S., & Chang, L. (2022). *THE NEXT-GEN PLUGX/SHADOWPAD? A DIVE INTO THE EMERGING CHINA-NEXUS MODULAR TROJAN, PANGOLIN8RAT*. TeamT5. https://i.blackhat.com/Asia-22/Thursday-Materials/AS-22-LeonSilvia-NextGenPlugXShadowPad.pdf

- Star, T. (2020, 17 septembre). *Malaysia's SEA Gamer Mall confirms two top staff members charged by US in hacking scam*. South China Morning Post. https://www.scmp.com/news/asia/southeast-asia/article/3101937/malaysias-sea-gamer-mall-confirms-two-top-staff-members

- Anonyme. (2015b). *WikiLeaks - The Hackingteam Archives*. WikiLeaks. https://wikileaks.org/hackingteam/emails/emailid/695766

- Tsyrklevitch, V. (2015, 22 juillet). *Hacking Team : a zero-day market case study*. Tsyrklevich.net. https://tsyrklevich.net/2015/07/22/hacking-team-0day-market/

- Lechtik, M. (2022, 26 janvier). *MoonBounce : the dark side of UEFI firmware*. Securelist. https://securelist.com/moonbounce-the-dark-side-of-uefi-firmware/105468/

- Hiroaki, H., & Lee, T. (2021). *Earth Baku Returns : Uncovering the Upgraded Toolset Behind the APT Group's New Cyberespionage Campaign*. Security News. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/earth-baku-returns?utm_source=trendmicroresearch&utm_medium=smk&utm_campaign=0821_EarthBaku1

- Anonyme. (2022b). *Daxin : Stealthy Backdoor Designed for Attacks Against Hardened Networks*. Symantec Blogs. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/daxin-backdoor-espionage

- Tereshkin, A. (2006). *Rootkits : Attacking Personal Firewalls*. Codedgers. https://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Tereshkin.pdf

- Tkacik, J. (2008). *Trojan Dragon : China's Cyber Threat*. The Heritage Foundation. https://www.heritage.org/asia/report/trojan-dragon-chinas-cyber-threat#_ftn28

- Anonyme, S. M. (2017, 12 septembre). 周鸿祎 : 马云提新零售我想了几个月想到了"大安全". 新浪移动_手机新浪网. https://tech.sina.cn/i/gn/2017-09-12/detail-ifykusey8931658.d.html?vt=4

- Yang, Y. (2018, 14 mai). *Chinese hackers defy government warnings at Beijing Def Con*. Financial Times. https://www.ft.com/content/f03995de-5711-11e8-bdb7-f6677d2e1ce8
- Anonyme. (s. d.-b). *Tianfu Cup International Cybersecurity Contest*. 品牌策划：神州互动. http://www.tianfucup.com/en
- Tangent, T. D. (2019). *DEF CON® China 1.0 Hacking Conference - Speakers*. DefCon.Org. https://defcon.org/html/dc-china-1/dc-cn-1-speakers.html
- Beer, I. (2022, 5 juin). *A very deep dive into iOS Exploit chains found in the wild*. ProjectZero.https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html
- Sichuan University. (2021). *National Cybersecurity Talent Base*. Sichuan University. https://perma.cc/SQ3K-LZKQ
- Nakashima, E. (2015a). *Security firm finds link between China and Anthem hack - The Washington Post*. Perma.Cc. https://perma.cc/37P3-3PSJ
- Cary, D. (2022, 4 avril). *Robot Hacking Games*. Center for Security and Emerging Technology. https://cset.georgetown.edu/publication/robot-hacking-games/
- Faou, M., Tartare, M., & Dupuy, T. (2021, 12 mai). *Exchange servers under siege from at least 10 APT groups*. WeLiveSecurity. https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/
- Lindsay, J. R., Cheung, T. M., & Reveron, D. S. (2015). *China and Cybersecurity*. Google Books. https://books.google.fr/books?id=dgN1BgAAQBAJ&pg
- W.E.T.R.O.O.P.E.R.S. (2017, 5 avril). *TR17 - Surprise Bitches ! - The Grugq*. YouTube. https://www.youtube.com/watch?t=2129&v=wP2J9aYM6Oo&feature=youtu.be
- Philipp, J. (2015, 14 septembre). *EXCLUSIVE : How Hacking and Espionage Fuel China's Growth*. The Epoch Times. https://web.archive.org/web/20160413012341/http://www.theepochtimes.com/n3/1737917-investigative-report-china-theft-incorporated/
- Hannas, W. C., & Chang, H. M. (2021). *China's STI Operations - MONITORING FOREIGN SCIENCE AND TECHNOLOGY THROUGH OPEN SOURCES*. CSET. https://cset.georgetown.edu/wp-content/uploads/CSET-Chinas-STI-Operations.pdf
- Courmont, B. (2016). *La lutte anticorruption en Chine : « la chasse aux tigres et aux renards »*. Cairn.info.https://www.cairn.info/revue-internationale-et-strategique-2016-1-page-131.htm
- Zhen, L. (2018, 20 juillet). *Chinese military overhaul to tighten Xi Jinping's grip on armed forces, say analysts*. South China Morning Post. https://www.scmp.com/news/china/diplomacy-defence/article/1900493/chinese-military-overhaul-tighten-xi-jinpings-grip

- The Economist. (2021, 4 mars). *China's domestic-security agencies are undergoing a massive purge*.https://www.economist.com/china/2021/03/01/chinas-domestic-security-agencies-are-undergoing-a-massive-purge
- The Economist. (2021b, juin 29).*The anti-graft unit of China's Communist Party has grown in power*.https://www.economist.com/china/2021/06/12/the-anti-graft-unit-of-chinas-communist-party-has-grown-in-power
- Kamphausen, R. D. (2021). *THE PEOPLE OF THE PLA 2.0*. US Army War College Press. https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1940&context=monographs
- Anonyme. (s. d.-a). *ICS- Institute of Chinese Studies : « China's military reforms to tighten Xi Jinping's grip on PLA »*. Institute of Chinese studies. https://www.icsin.org/chinas-military-reforms-to-tighten-xi-jinpings-grip-on-pla
- Lowsen, B. (2016, 16 juin). *The True Crimes of Chinese PLA General Guo Boxiong*. The Diplomat. https://thediplomat.com/2016/06/the-true-crimes-of-chinese-pla-general-guo-boxiong/
- Sanchez, J. (2012). *Notre panoptique brisé : un rapport du Sénat conclut que les centres de fusion sont chers et inutiles*. CATO Institute. https://www.cato.org/blog/our-broken-panopticon-senate-report-finds-fusion-centers-expensive-useless
- Anonyme. (2022a). *APT41, A DUAL ESPIONAGE AND CYBER CRIME OPERATION*. Mandiant. https://www.mandiant.com/sites/default/files/2022-02/rt-apt41-dual-operation.pdf
- Patel, F., Levinson-Waldman, R., & Panduranga, H. (2022). *A Course Correction for Homeland Security Curbing Counterterrorism Abuses*. Brennan Center for Justice. https://www.brennancenter.org/media/9444/download
- Anonyme. (2011). *Hawaii Man Sentenced to 32 Years in Prison for Providing Defense Information and Services to People's Republic of China*. FBI. https://archives.fbi.gov/archives/honolulu/press-releases/2011/hn012511.htm
- Ruffin, O. (2020, 14 janvier). *Blondie Wong And The Hong Kong Blondes - Emerging Networks*. Medium. https://medium.com/emerging-networks/blondie-wong-and-the-hong-kong-blondes-9886609dd34b
- Anonyme. (s. d.). *Please Wait . . . | Cloudflare*. UniTracker. https://unitracker.aspi.org.au/topics/cyber/
- Anonyme. (2022). *2021-2022 : l'armée de Terre en chiffres*. Defense.gouv. https://www.defense.gouv.fr/actualites/2021-2022-larmee-terre-chiffres