Cybersécurité et cyberdéfense chinoise : évolutions

Monsieur Daniel Ventre
Ingénieur au CNRS, chercheur au CESDIP (Centre de Recherches Sociologiques du Droit et des Institutions Pénales)[1]

L'essentiel de la connaissance qui nous parvient sur les pratiques, politiques et stratégies chinoises en matière de cybersécurité et défense trouve son origine dans un discours anglo-saxon dominé par la perspective américaine, grande productrice de rapports, études et discours sur le sujet. Les entreprises de cybersécurité (Mandiant, Novetta Solutions…), les médias, les responsables ou ex-responsables d'agences du gouvernement, mais encore le monde de la recherche académique, les think tanks, traitent de la question depuis le début des années 2000[2]. La Chine communique également, que ce soit par les médias, par des publications officielles, par des discours, sur sa vision de la cybersécurité et son analyse des défis que pose le cyberespace à la société et à la sécurité. Sur ces bases, essayons d'identifier quelles ont été au cours des deux dernières décennies les principales évolutions de la cybersécurité/cyberdéfense chinoise, ou du moins l'idée que l'on s'en fait.

Une « menace » exprimée en de nouveaux termes

La récente cyberstratégie publiée par le Département de la Défense américain (avril 2015)[3] considère la Chine comme une pièce maîtresse, si ce n'est « la » pièce maîtresse, dans l'environnement de la cybermenace. Cette considération n'a guère été modifiée au fil des ans**, la Chine constituant toujours une menace** en raison de ses développements capacitaires et de ses

1. L'auteur est également Titulaire de la Chaire Cybersécurité et Cyberdéfense (Ecoles de Saint-Cyr Coëtquidan/Sogeti/Thales), chargé de cours à Telecom ParisTech, Directeur de la collection Cybercriminalité et Cyberconflit aux éditions Hermes Lavoisier. Il a publié une dizaine d'ouvrages sur le cyberconflit et la guerre d et l'information.
2. Un recensement des sources et des diverses approches proposées par chacune d'entre elles est proposée dans : Daniel Ventre, Discourse Regarding China : Cyberspace and Cybersecurity, Chapitre 8, pp.199-282, *in* Daniel Ventre (Edit.), Chinese Cybersecurity and Defense, Wiley ISTE, juillet 2014.
3. U.S. Department of Defense, The DoD Cyber Strategy, 2015, 42 pages, Washington, http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

orientations stratégiques dans le cyberespace, lesquels sont confirmés par une démonstration d'efficacité soutenue, si l'on s'en réfère aux multiples opérations de cyberattaques dont le pays est crédité depuis les années 1990.

La manière de qualifier les hackers chinois en 2015 diffère de celle des années 1990-2000. On insistait alors davantage sur les hackers « patriotes », « nationalistes », « hacktivistes » qui, motivés par des sentiments patriotiques, agissaient soit d'initiative, soit de concert avec les acteurs étatiques. Il était fréquent d'évoquer les opérations de ces hackers (défigurations de sites massives, intrusions dans des serveurs étatiques) qui venaient s'inscrire dans des contextes de crises sino-japonaise ou sino-américaine. Désormais les hackers désignés sont avant tout ceux des services de renseignement militaires chinois. L'implication de Pékin dans les perturbations planétaires du réseau est sans détour dénoncée. Or le fait d'avoir déporté l'attention vers les pratiques étatiques, ne signifie pas que les communautés de hackers-citoyens ou cybercriminels n'existent plus ou qu'elles sont moins actives qu'auparavant.

Les États-Unis semblent avoir trouvé la grille de lecture qui leur faisait défaut dans les années 2000. Ayant jusqu'alors critiqué les stratégies chinoises de cyberdéfense pour leur opacité, hésité entre qualifier la cyber-puissance chinoise de menace guerrière/conquérante, de menace économique ou cybercriminelle, les États-Unis pointent aujourd'hui principalement le doigt sur la « menace économique » que constituent les pratiques de cyberespionnage menées par l'armée chinoise. Les autorités américaines voient essentiellement la Chine comme un voleur de propriété intellectuelle, vols commis par les renseignements militaires chinois au profit de leurs industries civiles et militaires, et bien sûr au détriment de la compétitivité américaine. Le cyberespionnage relèverait donc ainsi essentiellement de la guerre économique.

Les **menaces de conflits interétatiques** régionaux impliquant la Chine, dans lesquels on trouvera toujours désormais une dimension cybernétique, n'ont guère régressé. Si la menace d'attaque contre Taïwan, mobilisant une stratégie de guerre de l'information et de cyberdéfense, n'est pas écartée, la question apparaît cependant moins soulignée dans les analyses stratégiques américaines. Cette menace n'est plus aussi systématiquement mise en avant qu'elle l'était au cours des années 2000. D'autres crises perdurent toutefois : en attestent les récentes tensions territoriales entre la Chine et le Japon (îles …), les tensions entre la Chine et l'Inde.

Les États-Unis, mais aussi l'ensemble des pays qui s'affichent en victimes des pratiques agressives chinoises (intrusions dans les systèmes industriels et étatiques, APT), peinent à entamer un dialogue constructif avec la Chine, à **trouver de véritables mesures dissuasives**. Les poursuites engagées en mai 2014 contre quelques officiers de l'armée chinoise accusés de cyberespionnage économique, ne sont probablement pas de nature à altérer la détermination des agresseurs et à faire office de menace dissuasive. La Chine, face aux accusations répétées, maintient sa position, réfutant systématiquement son implication.

Sur le **plan intérieur,** mais avec de fortes connexions internationales, on constate que les efforts de domination de l'espace informationnel par les autorités de Pékin n'ont guère contribué à la réduction des violences et des revendications (Xinjiang, Tibet). Les opérations dans l'espace informationnel, les mesures prises dans le cyberespace (influence, contrôle, surveillance, censure, blocage d'applications, coupure des communications) n'ont pas contribué à pacifier les régions touchées par ces crises.

La cybersécurité est certainement l'un des enjeux majeurs de la société chinoise moderne. **Mais le pays doit faire face à d'autres défis sécuritaires énormes**, tout aussi urgents, voire prioritaires. Les conditions du développement économique, de la course effrénée au rendement, à la croissance, à l'enrichissement, ont eu des conséquences majeures sur la société : pollution environnementale, climat, sécurité sanitaire, sont au rang des priorités vitales. La société de l'Internet, des nouvelles technologies de l'information, aura contribué à la destruction environnementale. La Chine est parmi les nations les plus touchées par le phénomène.

La Chine, devenue un acteur global dans le cyberespace

Sur le plan industriel, la Chine a acquis des compétences dont elle ne disposait pas dans les années 1990. Elle ne se contente plus d'acquérir des technologies étrangères comme ce pouvait être le cas, elle ne se contente pas d'être l'usine du monde : elle est devenue force créatrice, a amélioré son processus de recherche et de développement, créé des *clusters* industriels partout dans le pays, et est en mesure d'exporter ses technologies, de gagner des parts de marchés importantes, de racheter des entreprises étrangères. La Chine tente d'imposer ses solutions. Sans doute pour lui barrer la route (pour des raisons évidentes de luttes pour des parts de marchés), tout autant que pour

répondre à de vrais enjeux de sécurité nationale, nombre d'États se sont opposés à l'accès à des marchés nationaux par les entreprises chinoises. À la détermination de conquête économique chinoise, les États opposent des barrières justifiées par la sécurité nationale, et la nécessité de technologies « souveraines ». De son côté la Chine impose elle aussi de fortes contraintes aux entreprises étrangères présentes sur son territoire (telle que l'obligation d'utiliser des systèmes de sécurisation – crypto – approuvés par Pékin, interdiction faite aux banques chinoises d'adopter des systèmes et applications chinois)[4] Ainsi Huawei s'est-elle vue dans de nombreux pays les portes des marchés étatiques sur des segments définis comme sensibles/vitaux. Le marché chinois lui-même s'est considérablement transformé : le web 2.0 chinois dispose désormais de ses industries nationales, avec des leaders comme Baidu (moteur de recherche), Weibo (équivalent chinois de Twitter). **La Chine est devenue un acteur global,** en ce sens qu'elle dispose désormais de capacités industrielles pour couvrir les trois couches du cyberespace (couche 1 : créer des infrastructures, développer du *hardware*, en industrialiser la production ; couche 2 : créer, développer, imposer commercialement des applications logicielles, y compris dans le web 2.0 ; couche 3 : créer, développer des plates-formes de réseaux sociaux, créer du contenu, permettre la croissance de cette couche informationnelle), et que cette maîtrise s'étend bien au-delà de son seul cadre national, en conquérant des parts de marchés jusque-là dominées par des entreprises occidentales ou japonaises. Cette force industrielle, et les perspectives ouvertes par la R&D, soutenues par une planification politique, ouvrent des perspectives pour les développements à venir : internet des objets, villes intelligentes, *big data*, mais encore renforcement du caractère « national », « souverain » des solutions adoptées par la sphère chinoise. **Le tout confère à la Chine une puissance réelle et un pouvoir d'influence sur la configuration du cyberespace** aujourd'hui déjà, et plus encore dans les prochaines années. Cette puissance contribue à l'évolution des rapports de force sur la scène internationale et à la capacité d'influence de la Chine.

La Chine a tenté d'exploiter le contexte de tensions internationales consécutif aux révélations d'E. Snowden sur les pratiques de surveillance, pour influencer les perceptions à son égard. Les révélations de Snowden ont suscité de l'indignation, des interrogations sur les pratiques des États démocratiques (surveillance), sur le sens des relations de confiance entre États. Les critiques traditionnellement formulées à l'encontre de la Chine se sont vues retournées contre le « modèle » que souhaitait représenter l'Amérique :

4. US voices concern over China's banking technology restrictions, RT.com, 27 mars 2015, http://rt.com/business/244589-usa-china-wto-cybersecurity/

responsable de cyberattaques, d'intrusions dans les serveurs étatiques des puissances étrangères y compris alliées, vols de données, espionnage politique et économique, surveillance des citoyens. Cette similitude entre les pratiques des États (même si les États-Unis légitiment leurs pratiques par des motivations se distinguant de celles de la Chine) contribue peut-être à **relativiser la nature de la « menace » chinoise.** Les autorités de Pékin en tous cas ont joué de cette situation pour se défendre des accusations portées à leur encontre par Washington et nombre d'autres puissances. Au lendemain des accusations visant ses officiers militaires pour cyberespionnage, Pékin accusait Washington d'hypocrisie, rappelant que les États-Unis maîtrisent l'essentiel des technologies et possèdent les infrastructures clefs pour conduire des opérations de cybersurveillance (espionnage) massive planétaire visant gouvernements, entreprises, populations[5].

Les enjeux du cyberespace sont devenus l'objet de **discussions officielles aux plus hauts niveaux** entre la Chine et de nombreux pays : ainsi les autorités américaines et chinoises s'entretiennent-elles sur le cyberespace (Sino-U.S. Cybersecurity Dialogue[6], Cyber Working Group), sur la nécessité de définir des règles de sécurité dans le cyberespace (visant par exemple à éviter tout risque d'erreur d'interprétation, qui pourrait déboucher sur une escalade de la violence entre les États). Ces échanges sont suspendus à la qualité des relations diplomatiques : le dialogue au sein du Cyber Working Group a été suspendu par la Chine en mai 2014. La Chine veut plus largement imposer sa voix à l'échelle internationale, se dit ouverte aux dialogues bilatéraux[7] sur les enjeux de normalisation et de gouvernance du cyberespace, l'un de ses leitmotivs étant la défense de la souveraineté. Elle est pour cela présente dans les instances de normalisation (UIT), et formalise des accords avec des partenaires étrangers (elle a par exemple signé en mai 2015 un accord avec la Russie, surnommé par les médias « Pacte Cyber »[8]).

---

5. Ben Knight, US goes after China over cyber attacks, 20 mai 2014, http://www.dw.de/us-goes-after-china-over-cyber-attacks/a-17648859

6. Bilateral Discussions on Cooperation in Cybersecurity China Institute of Contemporary International Relations (CICIR) - Center for Strategic and International Studies (CSIS) , Juin 2012, http://csis.org/files/attachments/120615_JointStatement_CICIR.pdf

7. China to deepen int'l cooperation on cyber security, CCTV.com, 10 février 2015, http://english.cntv.cn/2015/02/10/VIDE1423536244824155.shtml

8. Alexandra Kulikova, China-Russia cyber-security pact: should the U.S. be concerned?, Russia Direct, 21 mai 2015, http://www.russia-direct.org/analysis/china-russia-cyber-security-pact-should-us-be-concerned . Une traduction en anglais de l'accord est propose sur le site csistech.com : http://www.csistech.org/blog/2015/5/11/sino-russian-cybersecurity-agreement-2015