Les évolutions des postures cyber : comment la Chine, la Russie, les États-Unis et l'Union européenne voient le monde

Par Rayna STAMBOLIYSKA
Fondatrice et directrice générale de RS Strategy

Certaines avancées technologiques sont si importantes qu'elles fracturent notre compréhension du monde. Les experts et les décideurs politiques commencent à disséquer, même si c'est parfois timidement, les conséquences potentielles de l'ajout de nouvelles technologies peu familières, avancées et potentiellement dévastatrices à la boîte à outils des puissances adverses. Dans ce contexte, les postures de cybersécurité présentent un attrait particulier. Ces postures permettent de mieux appréhender les changements stratégiques en cours chez les principaux acteurs de l'échiquier géopolitique. Ainsi, nous examinons la Chine, la Russie, les États-Unis et l'UE par le prisme de leurs postures cyber où se reflètent les visions civilisationnelles qui déterminent les actions à venir de ces acteurs. Ces stratégies reflètent les perspectives à long terme de ces acteurs, offrant ainsi un aperçu de leurs motivations et des éventuels angles morts à prendre en compte.

« Tous les 18 mois, le coefficient de QI nécessaire pour détruire le monde baisse d'un point »[1]. Comment penser sa place dans le monde face à la diversification des menaces et des acteurs capables de les matérialiser ?

Certaines avancées technologiques sont si importantes qu'elles fracturent notre compréhension du monde. Une telle rupture s'est produite avec la bombe nucléaire ; son avènement a transformé la conception de la guerre et de la puissance. Aujourd'hui, les progrès rapides des technologies recèlent le même potentiel, qu'il s'agisse de ciblage publicitaire, de ChatGPT ou encore d'informatique quantique. Les experts et les décideurs politiques commencent à disséquer, même si c'est parfois timidement, les conséquences potentielles de l'ajout de nouvelles technologies peu familières, avancées et potentiellement dévastatrices à la boîte à outils des puissances adverses.

Dans ce contexte, les postures de cybersécurité présentent un attrait particulier. Dans sa compréhension générique, il s'agit d'appréhender quels risques numériques pèsent sur les actifs stratégiques pour les en protéger. Si on adopte la définition la plus stricte, la posture cyber désigne la robustesse des approches de prévention et d'atténuation des cybermenaces, ainsi que la capacité d'agir avant, pendant et après un incident.

[1] Il s'agit de la « loi de Moore pour la science folle » (*Moore law for mad science*), un concept créé et popularisé par l'écrivain américain Eliezer Yudkowsky, http://web.archive.org/web/20071027141829/ ; http://www.acceleratingfuture.com/people-blog/?p=209

La posture cyber repose sur des politiques et procédures organisant les utilisations de logiciels, du matériel, des services, des réseaux et des informations. Il s'agit donc d'un concept dynamique en ce qu'il traduit l'existant ; il permet également une vision longitudinale qui soutient la prise de décision face à l'évolution des menaces et de l'appétence au risque.

Généralement appliquée dans le contexte d'une organisation, la notion de posture cyber peut être utilement mobilisée pour apprécier les principales tendances de gestion des risques. Ainsi, la posture cyber peut aider à comprendre des changements stratégiques le long d'un spectre qui comprend les opérations défensives et offensives, la dissuasion et la résilience. Une telle cartographie est également pertinente lorsqu'on souhaite projeter les lignes de démarcation face à la multiplication d'acteurs pouvant mobiliser des technologies actuelles et émergentes, qu'il s'agisse de leur consommation ou de leur production.

La technologie comme déterminant géopolitique dans un monde incertain

Lorsque le politologue américain Francis Fukuyama annonçait sa grandiloquente « fin de l'histoire », la puissance de créer des tensions et de parer les dangers était l'apanage quasi-exclusif des États. La proclamation aux allures de prophétie se voulait une assurance face à l'incertitude se déployant avec la fin de l'URSS : le modèle civilisationnel occidental de démocratie et de prospérité économique allait submerger le reste de la planète et confirmer l'idée selon laquelle l'essor économique mène inéluctablement à une gouvernance démocratique. La candeur de la vision selon laquelle l'émergence de classes moyennes aisées mènerait à la compétition de valeurs politiques et, de là, au pluralisme politique avait de quoi interpeller.

Quelques trois décennies plus tard, la Chine et la Russie témoignent de l'inanité de cette prédiction. Ni l'une ni l'autre n'a vu se développer un pluralisme politique viable avec son essor économique. Plus encore, chacune a su promouvoir et asseoir sa vision civilisationnelle, qu'il s'agisse de relations extérieures ou de critères pour jauger de la légitimité de ses têtes dirigeantes. Ces trois décennies ont démontré que le modèle occidental a une alternative viable : non seulement un régime autoritaire peut créer de la stabilité, mais il permet également l'innovation et l'émergence de *leaders* technologiques globaux.

Le développement concomitant du numérique a contribué à l'émergence d'innovations et accéléré la mise sur le marché de technologies de rupture. Les ruptures sous-entendues concernent les modifications profondes des comportements individuels et des interactions sociétales, bien plus significatives qu'une prouesse technologique spécifique. Aux côtés des puissances étatiques se sont rangés des acteurs transnationaux, non étatiques et privés, disposant de moyens d'action parfois spectaculaires. Pendant presque aussi longtemps que trois décennies, le numérique était un sujet d'expertise et d'ingénierie, avant de devenir un levier économique. Son rang d'objet politique est récent, la pandémie de Covid-19 ayant significativement accéléré cette reconnaissance. La tech est devenue politique, et, avec ce devenir, le numérique s'est retrouvé mobilisé pour soutenir des visions civilisationnelles distinctes.

La démocratisation de la destruction

Cette « montée en rang » n'est ni facilement acceptable par tous ni facilement gérable. Avec la porosité exceptionnelle des sociétés au numérique est venue une évolution des risques et une fragmentation des acteurs, donc des responsabilités.

Beaucoup plus prégnant aujourd'hui est le constat que l'accès à des technologies puissantes est possible avec un coût d'entrée souvent risible. La diversité des acteurs et des usages combinée à l'absence de débat public sérieux sur l'impact de la technologie sur le tissu sociétal et sur les individus créent ce que Timothy Shoup et August Leo Liljenberg (2023) du Copenhagen Institute for Futures Studies (CIFS) appellent la « démocratisation de la destruction »[2]. En associant ces deux termes, ils soulignent que la prolifération de technologies (notamment émergentes) diverses change la donne ; elle permet à des acteurs non étatiques, à des groupes de plus en plus petits et même à des individus, d'exercer et de projeter leur pouvoir pour faire des choses que seuls les États-nations (souvent de grands États-nations politiquement puissants, économiquement prospères et éduqués) pouvaient faire auparavant.

En effet, la barrière à l'utilisation de nombreux outils technologiques est extrêmement basse. Ce que la notion de « démocratisation de la destruction » projette est l'abaissement des seuils nécessaires à la mobilisation d'un outil complexe et multifonction. Ainsi, le premier seuil est la capacité cognitive de comprendre l'outil et ce qu'il peut faire. Le deuxième est la capacité à accéder à l'information et à comprendre comment l'outil fonctionne. Enfin, le troisième est le seuil de compétence, c'est-à-dire la manière dont la personne transforme son savoir en savoir-faire. Par conséquent, il est possible d'affecter une population significative avec un outil *a priori* anodin et avec un coût de mobilisation faible. Cette situation diffère profondément des dégâts provoqués par une bombe nucléaire : s'il est vrai qu'une population significative en serait affectée, l'outil n'a rien d'anodin et son coût de mobilisation est extrêmement important.

C'est sur cette toile de fond que se joue le déploiement des visions civilisationnelles des principaux pôles de puissance (géo)politique, à savoir l'UE, les États-Unis, la Chine et la Russie. Ce qui interpelle, c'est l'inscription de ces valeurs dans les postures de cybersécurité de ces entités.

La posture cyber : quand la vision civilisationnelle devient réalité opérationnelle

Alors que la Russie et la Chine ont revendiqué assez tôt une vision civilisationnelle dans la gestion du technologique, les États-Unis ont assigné ce volet au militaire et l'UE a privilégié le dénominateur commun économique. Pour la Russie et la Chine, le numérique (et plus largement, le technologique) ont toujours été un moyen de projeter leur puissance et leur vision du monde. En revanche, c'est avec une certaine surprise qu'on découvre, en mars 2023 l'alignement de partenariats avec « des pays qui partagent nos valeurs » annoncé par le Président américain Joe Biden dans la publication de la nouvelle stratégie cyber américaine[3], et en avril 2023 l'annonce d'un *Cyber Solidarity Act* européen par les commissaires Thierry Breton (au marché intérieur) et Margaritis Schinas (à la promotion du mode de vie européen)[4] sur fond d'une recherche d'autonomie

[2] SHOUP T. & LILJENBERG A.L. (2023), "Destruction democratized", in *Farsight: A world pulled apart?*, CIFS, https://cifs.dk/p/a-world-pulled-apart

[3] THE WHITE HOUSE (2023), "Fact sheet: Biden-Harris administration announces national cybersecurity strategy", https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

[4] Adoption of the Cyber Package proposals: Closing statements by Margaritis Schinas and Thierry Breton (2023), https://multimedia.europarl.europa.eu/en/video/adoption-of-the-cyber-package-proposals-closing-statements-by-margaritis-schinas-vice-president-of-the-european-commission-and-by-thierry-breton-european-commissioner-for-internal-market_I239958

stratégique[5]. Alors, que disent les postures cyber de ces quatre grands acteurs de leurs projections dans le monde et possibles interactions futures ?

Les tendances d'évolution des postures cyber des quatre grands acteurs (Chine, États-Unis, Russie, UE) indiquent naturellement des divergences dans la façon d'appréhender les risques. Ainsi, l'UE fait office d'exception dans sa timidité à mobiliser des opérations cyber offensives (ou, comme elles sont souvent appelées en référence aux postures américaine et chinoise, des « actions de défense proactive »). En effet, pour l'instant, l'UE reste partagée sur l'emploi de capacités cyber offensives. La résolution du Parlement européen sur l'état des capacités de cyberdéfense de l'UE, adoptée en octobre 2021, reconnaît que « dans une certaine mesure, la cyberdéfense est plus efficace si elle contient également des moyens et des mesures offensifs »[6]. Bien que cela n'équivaille pas automatiquement à un changement fondamental dans la position défensive européenne, il y a une évolution dans l'approche de cette question. De même, la recherche d'une approche harmonisée de la mise en œuvre de l'autonomie stratégique est un véritable différenciant européen. Enfin, la « troisième voie » européenne[7] – le réglementaire – s'affirme, avec une intensification des textes normatifs affectant des producteurs technologiques non européens (RGPD, *Cyber Resilience Act*, etc.).

Une autre divergence notable, cette fois lorsqu'on met en parallèle la Chine et la Russie, est l'appréhension du contrôle de l'information. Ces deux acteurs ont placé ce qu'on pourrait appeler une souveraineté informationnelle au cœur de leurs postures cyber. En effet, la maîtrise des contenus est érigée en doctrine aussi bien en Russie[8] qu'en Chine[9] ; dans les deux cas, il s'agit de garantir une vision civilisationnelle unifiée et univoque. Cependant, là où la Russie passe de contrôle informationnel à une « guerre des mentalités », la Chine adopte une démarche diplomatique techniciste et une défense proactive holistique. Dans

[5] Apparu officiellement en 2013 (https://data.consilium.europa.eu/doc/document/ST-217-2013-INIT/fr/pdf), le concept d'autonomie stratégique est devenu central dans la vision du monde de l'UE : il est expressément consacré dans la stratégie globale de l'UE en 2016 (https://data.consilium.europa.eu/doc/document/ST-10715-2016-INIT/fr/pdf ; le document de référence sur les orientations européennes de sécurité et de défense). La pandémie de Covid ayant laissé des traces indélébiles dans nos sociétés, l'autonomie stratégique embrasse depuis fin 2020 (https://www.consilium.europa.eu/media/45918/021020-euco-final-conclusions-fr.pdf) l'ensemble du marché unique, de la politique industrielle, de l'espace et du numérique, notamment en ce que ce dernier est aussi la source de nouveaux risques. En raison de l'interdépendance des économies mondiales, le commerce, la santé ou encore l'énergie sont également concernés. Plus généralement, tous les secteurs dont les chaînes d'approvisionnement dépassent les frontières européennes et sont donc vulnérables aux tensions géopolitiques sont dans le giron de l'autonomie stratégique.

[6] European Parliament resolution of 7 October 2021 on the state of EU cyber defence capabilities (2020/2256(INI)).

[7] FRADIN L. (2020), « L'UE post-Covid : une troisième voie face à la Chine et aux États-Unis », *Le Grand Continent*, https://legrandcontinent.eu/fr/2020/06/18/lue-post-covid-une-troisieme-voie-face-a-la-chine-et-aux-etats-unis/

[8] Dans les versions antérieures des documents stratégiques russes, l'approche de sécurité était énoncée comme faisant obstacle aux « menaces contre les droits et libertés constitutionnels de l'homme et du citoyen dans le domaine de la vie spirituelle et des activités d'information, de la conscience individuelle, collective et publique » se matérialisant par « l'utilisation illégale de moyens spéciaux d'influencer la conscience individuelle, collective et publique » (Doctrine pour la sécurité de l'information de la Fédération de Russie, 9 septembre 2000, https://base.garant.ru/182535/). L'hostilité (perçue et réelle) de l'Occident à l'égard de la Russie s'est également manifestée en matière de souveraineté culturelle, conduisant le même document à identifier « l'application des technologies de l'information dans l'intérêt de la préservation des valeurs culturelles, historiques, cultuelles et morales du peuple multinational de la Fédération de Russie » comme un intérêt national à sauvegarder par le truchement de la sécurité de l'information.

[9] RAUD M. (2018), "China and cyber: Attitudes, strategies, organisation", NATO CCD COE, https://ccdcoe.org/library/publications/china-and-cyber-attitudes-strategies-organisation

ce contexte, la posture cyber de la Chine prend davantage les allures d'une image en miroir des postures occidentales. La Russie continue sa trajectoire de modulation informationnelle en codifiant dans ses doctrines depuis 2016 la « guerre des mentalités » qui vise à modifier « la conscience, la vision du monde, les objectifs, les valeurs et les priorités d'une société »[10] adverse, c'est-à-dire les fondements de sa civilisation.

Outre ces divergences, les tendances d'évolution des postures cyber de ces quatre acteurs font aussi état de beaucoup de similitudes. Tel est notamment le cas dans les approches occidentales de contrôle de l'information : tout en dénonçant les approches chinoise et russe, l'UE et les États-Unis ont également tendance à déployer des moyens pour localiser et exploiter le transit d'informations. Même s'il ne s'agit pas tant de façonner les contenus, l'effort pour héberger des données sur les territoires respectifs et à ne pas permettre de main mise sur des informations jugées stratégiques est prééminent depuis quelques années.

Il est notable de constater que la Chine, la Russie et les États-Unis redoublent d'effort pour équilibrer les opérations cyber défensives et offensives dans un processus continu de préparation-détection-atténuation-réponse-résilience. En témoignent les doctrines respectives, notamment américaine et chinoise, articulées autour de concepts tels que « défense active », voire « défense proactive ». La « défense active » côté russe existe de longue date ; elle se retrouve également dans la « guerre des mentalités » : l'effort de transformer et modeler les fondations civiques et culturelles adverses peut se matérialiser par la prise de contrôle de la narration adverse pour en influencer le comportement. La Chine de son côté enrichit sa boîte à outils conceptuelle en développant la « défense proactive » dans une « fusion civil-militaire »[11]. Ainsi, la distinction entre temps de paix et temps de guerre s'efface pour laisser place à un continuum où le processus continu peut se déployer quel que soit le niveau de conflictualité. Enfin, l'approche proactive américaine est articulée autour des notions de « défense en avant » et « engagement persistant »[12] où on retrouve l'aspect longitudinal de la conflictualité. Par ailleurs, les efforts des États-Unis en faveur d'une plus grande intégration entre les secteurs public et privé reflètent certains aspects de la « fusion civil-militaire » chinoise, qui cherche à structurer une approche holistique renforçant les capacités défensives et offensives.

Ce tour d'horizon des tendances suggère que la Chine, les États-Unis et la Russie assument un comportement de plus en plus préventif et conflictuel dans le cyberespace, tout en se considérant mutuellement comme des adversaires potentiels. L'UE devra prestement formuler une position afin de mieux gérer ses réponses, compte tenu notamment de la diversité des positions des États membres et de sa recherche d'une déclinaison réalisable d'autonomie stratégique.

[10] ИЛЬНИЦКИЙ А.М. (2021), МЕНТАЛЬНАЯ ВОЙНА РОССИИ (La guerre russe des mentalités), ministère de la Défense de la Fédération de Russie, https://vm.ric.mil.ru/Stati/item/336904/

[11] US DEPARTMENT OF DEFENSE (2022), "Military and security developments involving the People's Republic of China", Annual report to Congress, https://media.defense.gov/2022/nov/29/2003122279/-1/-1/1/2022-military-and-security-developments-involving-the-peoples-republic-of-china.pdf

[12] US DEPARTMENT OF DEFENSE (2018), "Fact Sheet: 2018 DoD cyber strategy and cyber posture review", https://media.defense.gov/2018/Sep/18/2002041659/-1/-1/1/factsheet_for_strategy_and_cpr_final.pdf