Note n°12/21

25 mars 2021

Valérie Niquet
Maître de recherche, Fondation pour la recherche stratégique

FONDATION pour la RECHERCHE STRATÉGIQUE

Covid-19 et défis de sécurité dans le cyberespace

Cet article a été rédigé à la suite du webinaire du programme Japon « Digital security challenges in the context of Covid-19 » organisé le 26 mars 2021.

La question de la digitalisation et de la sûreté des systèmes informatiques en temps de Covid pose des problèmes d'ordre divers. Les cas de la France et du Japon présentent des similitudes, d'ailleurs communes à toutes les sociétés démocratiques ouvertes. La France et le Japon font également face à des défis de natures différentes, mais qu'il est vital de prendre en compte, y compris par un échange d'informations et d'expérience entre pays partageant les mêmes valeurs.

Au Japon, contrairement à l'image que l'on peut en avoir en Occident, le défi a d'abord été, notamment au niveau des administrations et des petites et moyennes entreprises, ainsi que dans la population en général, celui de la digitalisation de la société. Le télétravail a révélé un système obsolète en période de crise, fondé sur le présentiel, les réunions en face-à-face et une confiance encore très massive dans le document papier. Un système très hiérarchisé fondé sur l'ancienneté, où les dirigeants d'entreprises, les hauts fonctionnaires et les cadres plus âgés ne maîtrisent pas les technologies et parfois ne les utilisent pas eux-mêmes, a aggravé ces limites.

L'autre défi est celui de la sécurité et de la solidité des systèmes, alors que la digitalisation, le e-commerce et le télétravail ont connu une accélération rapide à la faveur de la pandémie de Covid-19 dans une population qui n'y était pas préparée. Le secteur financier a été la cible d'attaques et les menaces sur des infrastructures sensibles n'ont pas disparu. Paradoxalement, c'est le faible niveau de digitalisation de nombreuses PME qui a joué le rôle de bouclier contre ces attaques.

Face à ces menaces, la prise de conscience et la réponse institutionnelle demeurent limitées, même si elles ont beaucoup progressé. Au sein du Cabinet, le *National Center for Incident Readiness and Strategy for Cyber Security* a pour mission essentielle d'améliorer la sécurité des organisations gouvernementales. Les structures en charge de la cybersécurité sont éclatées entre plusieurs institutions, le Cabinet du Premier ministre, le ministère de l'Economie, le ministère de l'Intérieur et la Police nationale. Le *Computer Emergency Response Team Coordination Center* a permis une prise de conscience et un meilleur échange d'informations, y compris avec d'autres partenaires en Asie et dans le monde, mais avec un résultat concret encore limité.

La France, de son côté, est confrontée à des enjeux qui sont ceux de la couverture de l'ensemble de la population par des réseaux performants. La France a également été confrontée au cours des derniers mois à des attaques massives qui ont notamment touché les hôpitaux, soumis à de fortes tensions en raison de la pandémie de Covid-19. Les industries sensibles en période de pandémie, comme les grandes entreprises pharmaceutiques, en France comme au Japon, ont également été la cible d'offensives.

Quelles normes dans un monde digitalisé ? Le concept de *Data Free Flow with Trust* (DFFT)

Lors du sommet du G20 de 2019 qui s'est tenu à Osaka, le Japon a soutenu une initiative appelée « Osaka track » qui aborde la question des normes et de la transparence des échanges en matière digitale. En période de crise comme celle de la pandémie de Covid-19, il s'agit aussi de répondre aux Etats qui exploitent la digitalisation des sociétés démocratiques libérales pour mener une forme de « guerre cybernétique » de désinformation et de propagande.

L'objectif est de renforcer le système de normes défendu par les sociétés libérales démocratiques. Il s'inscrit dans le contexte d'un conflit idéologique entre régimes autoritaires (Russie) ou totalitaires (Chine, Corée du Nord) et régimes démocratiques libéraux et ouverts. La question de la vulnérabilité de ces derniers aux attaques en provenance de Russie, de Chine ou de Corée du Nord constitue un défi majeur de sécurité, que l'épidémie de Covid-19 a renforcé. Pour la République populaire de Chine en effet, l'espace cyber est intégré au concept plus large de « guerre de l'information », et constitue un élément essentiel, dans les dimensions défensive et offensive, de la guerre hybride du faible au fort théorisée par Pékin.

Répondre à ce type de menaces impose aux sociétés démocratiques d'intégrer des menaces et des modes de conflit fondés sur l'exploitation des « zones grises » auxquels elles étaient moins préparées, particulièrement depuis la disparition de l'URSS et la fin de la Guerre froide[1]. Lors du forum économique de Davos de 2019, le Premier ministre Shinzo Abe avait introduit le concept de *Data Free Flow with Trust* (DFFT), qui prolonge, dans le domaine digital, le principe de « qualité des infrastructures » que le Japon met en avant face aux projets chinois de « nouvelles routes de la soie ».

Le concept a été repris lors de la réunion du G20 d'Osaka, avec la volonté de répondre, par un modèle ouvert, fondé sur la confiance, la transparence et le respect des règles de droit, aux initiatives russes et chinoises de régulation du cyberespace. Pour Pékin et Moscou, l'objectif

[1] Valérie Niquet, *La pensée stratégique chinoise*, Economica, Paris, 1997.

premier demeure la non-ingérence et le contrôle de l'information entrante, assimilée à une menace contre les régimes en place, même si, dans ce domaine, le régime chinois est beaucoup plus fermé que le russe. En 2011, Pékin et Moscou avaient soumis à l'ONU une proposition de « code de conduite international pour la sécurité informatique ».

L'objectif de l'initiative soutenue par le Japon est également de soutenir la coopération pour faciliter, tout en en régulant l'usage, la circulation d'informations et de données en impliquant les gouvernements mais aussi les entreprises. La pandémie de Covid-19 et l'explosion de l'utilisation des *big data* et de l'intelligence artificielle ont rendu plus urgente encore cette réflexion.

Le concept de DFFT peut apparaître comme encore vague, mais son imprécision répond aussi au flou des menaces dans le cyberespace, qui peuvent prendre de multiples formes. L'objectif est de préserver la circulation de l'information, tout en protégeant les sociétés et les institutions d'opérations offensives hostiles : actions d'influence politique, fausses informations, vol de propriété intellectuelle, espionnage, chantage, pressions diverses, qu'elles soient d'origine étatique, privée ou mixte.

Constituant, comme l'espace et l'espace maritime, un bien commun essentiel au fonctionnement des sociétés, mais aussi une source de vulnérabilités inédites, le cyberespace est ainsi devenu, pour le Japon comme pour ses partenaires, un sujet majeur d'échanges et de coopération, et un marqueur de la volonté d'engagement dans un système global libre et ouvert.

Les opinions exprimées ici n'engagent que la responsabilité de leur auteur.

WWW.FRSTRATEGIE.ORG

4 BIS RUE DES PÂTURES 75016 PARIS TÉL : 01 43 13 77 77 FAX 01 43 13 77 78

ISSN : 2273-4643