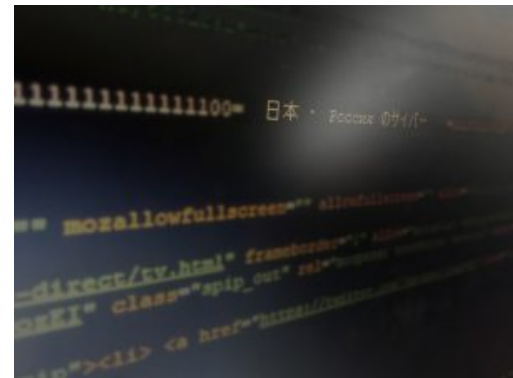


Le Japon 'reboote' ses relations avec la Russie

Description

L'archipel japonais, contraint à l'absence d'armée depuis 1945, ne parviendrait pas à s'inscrire dans le rang des grandes cyber-puissances du fait de son incapacité à assumer un programme de militarisation du cyberspace. Or les pays qui le voient, eux, ne sont pas inactifs en la matière. Parmi eux - la Russie. À la veille des Jeux olympiques de Tokyo, quelles sont les perspectives politiques japonaises en matière cyber face à une prétendue menace russe ?

L'année 2019 a démarré sur les chapeaux de roues : en janvier, le ministère russe des Affaires étrangères a fait savoir que des attaques DDoS [\(1\)](#) venaient d'être perpétrées contre son site internet. Origine première de l'offensive cyber : le Japon ! Un constat laissant pantois au regard d'une situation inverse bien plus fréquente. En effet, Tokyo ne compte plus les cyberattaques russes lancées à l'encontre de l'archipel. Il faut dire qu'à moins de dix mois de l'ouverture des Jeux olympiques, dans le cadre desquels depuis l'organisation de l'événement à Londres en 2012 l'enjeu cyber apparaît crucial, la tension est à son comble [\(2\)](#).



Une activité russe conséquente sur les réseaux japonais

La Russie l'a donc affirmé haut et fort : 77 millions de cyberattaques ont frappé le site de son ministère des Affaires étrangères entre janvier et septembre 2018, dont une majorité provenant de l'archipel.

Ce qui inspire d'emblée quelques commentaires : le nombre avancé par Moscou, établi sur une année, peinerait à atteindre les 120 millions d'attaques. Sur la seule année 2014, le Japon, lui, a fait face à plus de 25 milliards de cyberattaques.

Qui plus est, le NISC (*National center of Incidents readiness and Strategy for Cybersecurity*, organe du gouvernement japonais créé en 2005 et spécialiste en la matière) fait aujourd'hui état d'un constat alarmant : alors que les menaces chinoises et coréennes sur le cyberspace japonais étaient établies de longue date, l'activité russe, loin d'être négligée, n'était pourtant pas celle dénoncée prioritairement par le gouvernement japonais. Jusque récemment du moins. Parce qu'elle semble aujourd'hui profiter du déclin des perspectives chinoises : en 2018, on estime que 20,8 % des tentatives d'intrusion sur les réseaux japonais sont venues de la Fédération de Russie, contre 14,8 % de la Chine [\(3\)](#).

Tout cela invite à relativiser l'existence d'une menace japonaise sur la Russie. D'autant que, si menace il y a eu en 2018, il est fort probable que l'utilisation des réseaux japonais par un pays tiers en soit la cause. Ce genre de comportement est caractéristique de la Corée du Nord, de la Chine mais aussi... de la Russie même qui aurait procédé ainsi en 2007 contre l'Estonie. Le rapport annuel de la société américaine de cybersécurité *CrowdStrike* décrivait en 2018 des stratégies cyber de la Russie concentrées sur le piratage d'entreprises de télécommunications. Tokyo soupçonne d'ailleurs que l'une des cyberattaques « pivots », perpétrée contre le Japon en 2011 et dirigée contre les entreprises MHI et KHI, spécialisées dans le domaine de la défense, serait l'œuvre de la Russie, tant l'espionnage et l'intérêt pour les industries de défense et d'armement sont caractéristiques du pays. En 2018, un groupe nommé Sandworm Team, à l'origine russe assumée sur le terrain ukrainien depuis 2016, aurait attaqué plusieurs entreprises de logistique japonaises, dont Fire Eye. Ces attaques, si elles sont avérées, confirmeraient que les objectifs russes pourraient avoir été étendus au-delà des États issus de l'Union soviétique, induisant un système cyber institutionnalisé et complexe, avec des unités de cyberintelligence spécialisées sur les systèmes de l'Extrême-Orient.

Enfin, à ces attaques s'ajouteraient des activités de déstabilisation sur le Japon portées par différents groupuscules russes, comme des fakes news et des blogs pro-conservateurs propagés sur la toile nipponne en juin 2017, contraignant Yahoo!, qui en était l'hébergeur, à des mesures de répression contre le multicompte, technique privilégiée pour ce mode opératoire.

Tokyo 2020 : l'enjeu en matière de cybersécurité

D'un certain point de vue, ces différentes attaques sont dotées d'une vertu : elles permettent au Japon de s'offrir une répétition générale avant les Jeux olympiques que le pays accueillera à partir du 24 juillet 2020.

D'une part, parce que l'enjeu olympique est devenu, depuis 2012, un défi majeur en matière de cybersécurité : lors des Jeux olympiques d'hiver qui se sont déroulés en Corée du Sud en février 2018, ce sont 600 millions de cyberattaques qui ont été enregistrées d'abord durant la période de préparation, puis 5,5 millions pendant celle couvrant la compétition des JO. La majorité a été identifiée comme étant d'origines russe et nord-coréenne. Depuis les JO de Londres et l'émoi qu'elles avaient suscité alors, la question des cyberattaques, et plus spécifiquement celles de type DDoS, s'affirme comme cruciale pour le pays organisateur.

Il faut, d'autre part, tenir compte du fait que le Japon, nonobstant quelques politiques nationales visant à « revitaliser le pays » en matière cyber, dépend largement des entreprises pour s'affirmer comme une cyberpuissance : en l'absence de cyberarmées offensives, Tokyo doit compter sur une protection assurée majoritairement par les acteurs privés, dont l'entreprise israélienne KELA qui avait d'ailleurs assuré la protection des JO de Rio en 2016. Et cela n'est pas sans conséquences géopolitiques.

Mais, par ailleurs, le Japon s'affirme aussi au niveau international en promouvant des coopérations, dont certaines sont soutenues par la Russie. En effet, cette dernière fut à l'initiative dès 1998 de la création de groupes d'experts (GGE) onusiens, soutenus entre autres par le Japon, qui se sont réunis à quatre reprises. Ce format doit toutefois être relativisé, tant les réglementations qui en sont issues ont été laissées pour lettre morte par la communauté internationale. La perspective d'une coopération cyber russo-japonaise d'ici l'été 2020 peut laisser dubitatif, tant le Japon est avancé dans une coopération sécuritaire soutenue avec les États-Unis, mais aussi parce que la participation russe aux Jeux olympiques semble une nouvelle fois compromise du fait de l'accusation de cyberattaques perpétrées en octobre 2019 par le groupe russe FancyBear contre des institutions sportives et d'antidopage dans le monde, nationales comme internationales. Quoi qu'il en soit du potentiel coopératif de Moscou, la suspension des équipes russes des prochains JO d'été pourrait de fait transformer la Russie en ennemi cyber dont le Japon devra se méfier.

La perspective d'un réchauffement numérique ?

Des perspectives de coopération nippo-russes en la matière ne sont pourtant pas à exclure, à plus long terme. Mais elles doivent être pensées avec prudence. Bien que le Japon privilégie largement son partenariat avec les États-Unis, d'ailleurs réaffirmé avec une « alliance cyber » en avril 2019 établie sur la base du traité de sécurité nippo-américain de 1960 mais aussi dans son *Livre Blanc sur la sécurité en 2019*, Tokyo ne se prive pas d'envisager l'extension de ses partenariats bilatéraux. Il va même jusqu'à inclure des États au potentiel pourtant menaçant, tels que la République tchèque, dans le cadre d'une coopération renforcée avec l'Union européenne. Ces partenariats trouvent leur écho dans des dialogues bilatéraux cyber nippo-russes institués en 2015, renouvelés en 2016⁽⁴⁾ et relancés le 20 novembre 2019 après trois ans de stagnation. Les nombreuses collaborations économiques entre les deux pays et l'Année nippo-russe 2019 n'ont pas été affectées par ces questions de sécurité pourtant si névralgiques pour le Japon et la Russie. Force est de constater en outre que le *Livre Blanc sur la sécurité du Japon en 2019*, bien loin de négliger l'activité de son voisin russe sur son cyberspace, fait en revanche état d'une Chine considérée bien plus menaçante que l'ours russe - ce dernier étant présenté comme une menace essentiellement sur les questions de brouillage électromagnétique.

L'éventualité d'une coopération nippo-russe allant au-delà des traditionnels champs économiques qui lient les deux pays est donc loin d'être absurde. Elle a même suscité un rappel du Japon en l'espèce, qui va jusqu'à esquisser

l'ébauche d'un partenariat : le *Livre Blanc* de 2019 assume le dialogue cyber de 2015 comme pérenne malgré son essoufflement, illustrant la continuité de la politique du Premier ministre Shinzo Abe à vouloir normaliser ses relations avec la Russie. Les Jeux olympiques de 2020 pourraient l'infirmier ou la confirmer du côté russe. La démarche est stratégique pour le Japon parce que sa coopération avec la Russie dans le cyberspace sera inmanquablement comprise comme un risque par la Chine, elle-même désormais perçue comme la prochaine menace cyber du monde occidental au sens large.

Notes :

(1) Attaques par déni de service, *id est* par saturation des réseaux.

(2) Selon le Rapport de gestion des JO 2012, près de 2,3 milliards d'incidents liés au cyberspace avaient été recensés à cette occasion. Le site web officiel des Jeux olympiques de Londres avait été la cible de 212 millions de cyberattaques, dont 11 000 cas d'attaques DDoS.

(3) Franz-Stefan Gady (*in* « Japan: The Reluctant Cyberpower », *Asie. Visions*, n° 91, IFRI, mars 2017) estime qu'en 2014, 40 % de ces attaques étaient d'origine chinoise.

(4) « 2 *Second dialogue cyber nippo-russe* », *in* (*Relations avec la Fédération de Russie*), ministère japonais des Affaires étrangères.

Vignette : © Félix Deramond.

* Félix Deramond est étudiant en Master II Relations internationales à l'INALCO.



[Retour en haut de page](#)

date créée

23/12/2019

Champs de Méta

Auteur-article : Félix Deramond*