Note n° 10/22

16 mars 2022

Valérie Niquet
Maître de recherche
Fondation pour la recherche stratégique

Visions françaises et japonaises des nouveaux défis dans le contexte de la guerre en Ukraine : mer, espace et cyberespace

Les défis posés à la sécurité des espaces communs sur mer, dans l'espace et dans l'espace cybernétique sont au cœur des enjeux de défense auxquels fait face l'ordre libéral international[1]. Ce sont également des éléments importants dans les stratégies pour l'Indo-Pacifique publiées à Paris d'abord, puis à Bruxelles et dans le dialogue stratégique qui s'est développé entre la France et le Japon.

La guerre en Ukraine décuple ces défis en raison des répercussions sur les équilibres stratégiques en Asie, mais aussi du fait de l'importance de ces domaines, notamment l'espace et le cyberespace, dans les formes nouvelles de guerre. Ces formes nouvelles de la guerre s'ajoutent aux formes très traditionnelles – guerre de position, guerre de siège – que nous observons sur le terrain en Ukraine.

La dimension maritime

Alors que les tensions maritimes sont très présentes en Asie face à une Chine qui n'hésite pas à recourir à la coercition pour changer le *statu quo*, l'expérience de la Russie dans le conflit ukrainien est observée avec attention par les pays de la région. Moscou a mobilisé des bâtiments de sa

[1] Cette note a été rédigée à partir de la web conférence du programme Japon de la FRS *France and Japan Visions on Security Challenges in Global Commons: Sea, Space, Cyber*, 8 mars 2022.

flotte du Nord pour renforcer ses capacités en Mer noire et en Méditerranée. La Russie fait toutefois face à une difficulté liée à une configuration historique. C'est celle du contrôle des détroits par la Turquie qui interdit le passage des bâtiments de guerre. Les croiseurs russes en Méditerranée ne peuvent regagner les ports de la mer Noire. Ils ne peuvent pas non plus recevoir de renforts. La question logistique se pose sur terre pour la Russie mais aussi sur mer, les 46 bâtiments russes en Méditerranée étant coupés de leur source de ravitaillement.

Ces difficultés de la Russie sont observées par la Chine. En mer de Chine, la première chaîne d'îles, qui s'étend de la Corée au nord aux Philippines au Sud en passant par l'archipel japonais et Taïwan puis se prolonge jusqu'au détroit de Malacca, limite les capacités de sorties des forces navales chinoises vers le Pacifique occidental. Les bâtiments chinois, et tout particulièrement les sous-marins, ne peuvent emprunter que trois détroits (Bashi, Lombok, et Mindanao) pour accéder à l'océan Pacifique et l'océan Indien. En cas de conflit, la liberté de passage ne serait pas assurée, affaiblissant considérablement les positions chinoises. Tels sont les éléments que le Japon et les pays riverains en Asie doivent analyser et prendre en compte dans l'hypothèse d'un conflit dans le détroit de Taïwan.

La dimension spatiale

Depuis 1998, le Japon a rompu le tabou pesant sur l'usage strictement pacifique de l'espace en se dotant de satellites d'observation militaire. Le tir d'un missile nord-coréen Taepodong, qui a survolé le territoire japonais, revendiqué comme un essai de lanceur de satellite, a mis en évidence la nécessité pour Tokyo de se doter d'une capacité d'observation et d'évaluation autonome, y compris des États-Unis.

Depuis, d'autres activités spatiales ont été menées au service de la défense du pays. La JAXA a développé un radar SSA (*Space Situational Awareness*) qui doit être déployé en 2022 et permettra d'observer des débris d'une dimension de 10 cm, mais aussi tout objet dans l'espace, y compris les satellites chinois, même si l'enjeu principal demeure la sécurité des satellites, et non la capacité de mener des activités hostiles. Il s'agit de pouvoir répondre aux capacités chinoises de frappes anti-satellites. L'objectif, pour le Japon, est d'anticiper et de se doter des moyens de poursuivre ses missions spatiales en cas de destruction de satellites, en utilisant des solutions de secours mobilisant les capacités civiles ou le soutien des pays alliés. Les enjeux liés au spatial seront au cœur de la nouvelle Stratégie de sécurité nationale qui doit être publiée à la fin de l'année 2022, et du programme de défense qui l'accompagne (*National Defense Program Guidelines*).

La dimension spatiale de la sécurité a également pris une importance considérable pour le Japon du point de vue du concept d'Indo-Pacifique libre et ouvert. L'ambition est d'imposer des normes d'utilisation de l'espace fondées sur des valeurs communes respectant les règles du droit international. Cette dimension se retrouve dans les domaines de compétence élargis du Quad (Australie, États-Unis, Inde, Japon). Dans ce cadre, les satellites peuvent être utilisés à la fois pour des missions d'observation liées à la sécurité militaire, mais aussi pour améliorer la résilience des pays concernés face aux catastrophes naturelles. L'esprit de cette coopération se veut inclusif, et la Chine n'en est pas exclue *a priori*, mais sa participation est soumise à l'acceptation et au respect de normes communes. La dimension de la transparence est essentielle pour garantir la sécurité dans l'espace.

La dimension cyber

La dimension cyber est au cœur de la sécurité informationnelle, qui joue un rôle majeur dans les conflits contemporains. Même en temps de paix, les opérations offensives sont constantes. La guerre en Ukraine soulève plusieurs questions en la matière. La Russie pourrait lancer une offensive contre les infrastructures critiques, accroître la désorganisation de la réponse militaire et les mouvements de panique avec un effet domino sur les pays voisins.

Au quinzième jour de guerre, contrairement aux attentes, on n'a toutefois pas constaté d'offensive majeure dans le domaine cyber de la part de la Russie. Durant les premiers jours, les attaques contre les installations gouvernementales et militaires ukrainiennes n'ont augmenté que de 196 %, ce qui est peu par rapport aux capacités de nuisance dont dispose la Russie.

Plusieurs explications peuvent être avancées. La vénalité des groupes de hackers russes indépendants les rend plus difficiles à mobiliser, conséquence des sanctions financières qui frappent très durement la Russie et ses réseaux de financement à l'étranger. Un autre élément est la sous-estimation de la capacité de résistance de l'Ukraine, et la prolongation imprévue des opérations.

Par ailleurs, la Russie, qui a l'ambition de contrôler une partie du territoire ukrainien, ne peut par conséquent détruire les infrastructures dont elle a besoin, y compris les infrastructures de communication, vitales pour la poursuite des opérations.

En revanche, les risques contre les chaînes d'approvisionnement ne sont pas négligeables, au travers notamment de *ransomware* opportunistes qui se développent dans l'ombre de la guerre en Ukraine, en exploitant, par exemple, les appels aux dons et à la solidarité internationale.

Les entreprises japonaises, et plus particulièrement les PME, demeurent vulnérables à ce type d'opérations. La guerre en Ukraine impose de revoir tous les plans de continuité en situation de stress cyber, ainsi que la résilience des chaînes de communication et d'approvisionnement à tous les niveaux.

Ceci d'autant plus que les menaces se déplacent vers les technologies opérationnelles (OT) et les systèmes de contrôle industriel. Ces systèmes sont d'autant plus vulnérables qu'ils n'étaient pas initialement conçus pour être résilients. Par ailleurs, en ce qui concerne les chaînes d'approvisionnement, les attaques ciblées contre des entreprises non critiques peuvent permettre de pénétrer par des voies détournées des systèmes mieux protégés. C'est le cas notamment des champs d'éoliennes, cibles d'attaques récentes, à la fois plus vulnérables et directement reliées aux réseaux de distribution d'électricité.

La prise de conscience et la préparation de tous les acteurs, ainsi que les investissements dans l'après-5G, dont dépend l'Internet des Objets, sont critiques pour assurer la résilience de nos sociétés. C'est aussi l'une des leçons de la guerre en Ukraine. L'Asie n'est pas à l'abri d'un conflit armé, et la Chine a également fait des opérations cyber un élément clef de ses capacités de disruption.

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

WWW.FRSTRATEGIE.ORG

ISSN : 2273-4643