Note n°05/23

13 février 2023

Valérie Niquet

Maître de recherche, Fondation pour la recherche stratégique

Cybersécurité : le grand bond en avant du Japon

Introduction

La dimension cyber est au cœur de la réflexion stratégique au Japon[1]. Au mois de décembre 2022, la Stratégie de sécurité nationale (NSS) et la Stratégie de défense nationale (NDS) sont venues compléter et approfondir la stratégie de cybersécurité initialement publiée en 2015 et actualisée en 2018. Ce document consacré à la sécurité cyber du Japon définissait de grands principes généraux tels que la libre circulation de l'information, le respect du droit, l'ouverture, l'autonomie et la coopération entre organisations[2].

L'accent mis sur la dimension cyber dans les deux textes fondamentaux démontre une prise de conscience des autorités japonaises devant la complexité des défis auquel le Japon – comme d'autres grandes démocraties – fait face en la matière, mais aussi les difficultés à élaborer et à mettre en œuvre une réponse adéquate dans un laps de temps limité.

La perception des menaces auxquelles le Japon doit se préparer s'est considérablement assombrie depuis la première Stratégie de sécurité nationale, publiée en 2013[3]. L'environnement de sécurité du Japon est désormais décrit comme « *le plus sévère et le plus complexe depuis la Seconde Guerre mondiale* ». Les rivalités géopolitiques globales, en particulier la montée des tensions entre la Chine et les Etats-Unis, la poursuite du développement des capacités nucléaires et balistiques de la Corée du Nord, mais surtout la montée en puissance d'une Chine agressive,

[1] Cette note a été rédigée dans le prolongement du séminaire « Cyber Security: Common Challenges to Europe and Japan in Post Ukraine War Context » qui s'est tenu en ligne le 5 décembre 2022 (replay ici).
[2] *Cybersecurity Strategy*, 4 septembre 2015.
[3] Texte en anglais ici.

accusée de vouloir modifier le *statu quo* en utilisant la force et des moyens coercitifs de guerre hybride, sont au cœur de ces inquiétudes croissantes[4]. L'invasion de l'Ukraine par la Russie a joué le rôle de signal d'alarme, faisant craindre une offensive similaire de la part de la République populaire de Chine (RPC) dans le détroit de Taïwan.

Dans ce contexte, les menaces de type hybride occupent une place croissante avec les opérations de zones grises, aux confins du civil et du militaire, que ce soit sur mer ou dans le domaine cyber. La menace cybernétique globale, qui pèse aussi sur l'archipel, est considérable. Comme d'autres Etats, démocratiques ou non, le Japon subit plusieurs centaines d'attaques cybernétiques par an. Au cours du premier trimestre 2022, 114 attaques ont été officiellement répertoriées par l'Agence de police nationale, soit une augmentation de 87 % par rapport à l'année précédente. 59 de ces attaques ont touché les petites et moyennes entreprises (PME) et 36 les grandes entreprises ; parfois, comme pour l'entreprise Toyota, par l'intermédiaire d'un sous-traitant (Kojima). L'essentiel des attaques sont des opérations de *phishing*, de fraude, de vol d'identité et de crimes financiers mais aussi des attaques de *malware*, des refus de service (*denial of service*) et des modifications de sites internet (*website defacement*). Les infrastructures de santé, comme en France, sont particulièrement vulnérables avec un incident majeur dans un hôpital d'Osaka au mois d'octobre 2022[5]. Selon les chiffres de la police, 70 % de ces attaques proviendraient des Etats-Unis, du Royaume-Uni, de Chine et de Russie[6]. En dépit de ces attributions diverses, difficiles à confirmer, la Chine est considérée par Tokyo comme la menace principale, notamment en ce qui concerne le vol de données technologiques civiles ou militaires.

Dans le domaine plus strictement militaire, ce sont les méthodes de la guerre qui ont changé. Aux formes traditionnelles de guerre et d'invasion du territoire national se sont ajoutées de nouvelles formes de guerre hybride, de guerre de l'information, de guerre asymétrique. Les capacités spatiales, électromagnétiques et cyber sont utilisées et leur potentiel est démultiplié par le recours aux technologies de l'intelligence artificielle (IA) particulièrement développées en Chine[8]. Les limites entre guerre et paix s'effacent, entre systèmes défensifs et offensifs, y compris dans le cyber. Par ailleurs, les difficultés d'attribution, avec le recours à des groupes qui agissent pour eux-mêmes comme des pirates, ou pour le compte d'Etats comme des corsaires, viennent renforcer ce phénomène de dilution de la guerre et de la paix. Dans le domaine cyber, les menaces en temps de paix sont d'autant plus sérieuses qu'elles touchent à la vie quotidienne des citoyens et aux infrastructures critiques comme les hôpitaux ou les infrastructures énergétiques. Elles sont également majeures pour la préservation des capacités de défense dans la guerre moderne. Elles touchent à la guerre de l'information et aux opérations d'influence et de déstabilisation, en soutien ou non à des opérations militaires. Dans le domaine civil comme dans le domaine militaire, les risques augmentent avec la digitalisation croissante – et indispensable – des capacités.

Des systèmes vulnérables

Le 1er septembre 2021, sous la pression de la crise de la Covid-19, le gouvernement japonais a mis en place une Agence de la digitalisation, dont 150 employés sur 500 viennent du secteur privé. Cette rupture avec les pratiques habituelles de l'administration, ainsi que le poids accordé aux menaces cyber dans les deux stratégies de sécurité et de défense publiées au mois de décembre 2022, sont le signe de la prise de conscience au plus haut niveau des limites et des vulnérabilités de l'Etat et du pays en matière de sécurité cyber.

[4] *National Security Strategy*, 16 décembre 2022, texte en anglais ici.
[5] « Ransomware Attack Halt Service at Osaka Hospital », *The Asahi Shimbun,* 1er novembre 2022.
[6] « Japan Saw a 87% Increase in Ransomware Attacks in First Half of 2022 », *Japan Times,* 15 septembre 2022.
[7] *National Defense Strategy*, 16 décembre 2022, texte en anglais ici.

En dépit de son statut de troisième puissance économique mondiale, et de son image de puissance d'innovation héritée des années 1970-1980, le Japon, en 2022, se situait au 29ème rang sur 63 pays en matière de compétitivité digitale, en recul d'un point par rapport à l'année précédente selon l'*IMD World Digital Competitiveness Ranking*[8]. La prise de conscience du retard et des conséquences de ce retard en matière de sécurité est récente, notamment en raison d'un système de responsabilité qui privilégie encore les hommes d'âge mûr souffrant souvent d'illectronisme et insuffisamment conscients de ces enjeux.

Au niveau institutionnel, les responsabilités ont longtemps été dispersées entre plusieurs organisations, sans véritable communication ou cohérence dans les objectifs et les missions. L'agence de digitalisation (*Digital Agency*) a été mise en place le 1er septembre 2021 pour répondre aux défis révélés par la pandémie de Covid. L'agence est responsable de la digitalisation et de la rationalisation des moyens utilisés par les institutions officielles au niveau du gouvernement central comme au niveau local, mais elle n'est pas en charge de la cyber-sécurité. Le *Cyber Security Headquarter*, inauguré en 2015 dans le prolongement de l'adoption de la loi fondamentale sur la cybersécurité, est placé sous la direction du Secrétariat général du cabinet du Premier ministre. Il est chargé de la coordination et des réactions d'urgence en matière de cybersécurité. Le NSCI (*National center of Incident Readiness and Strategy for Cyber Security*) qui a succédé (2015) au *National Information Security center* (2005) est le bras opérationnel du *Cyber Security Headquarter,* chargé de formuler la politique en matière de cybersécurité, et de mobiliser l'ensemble des ressources du public et du privé. Enfin, les Forces d'autodéfense (SDF) ne sont responsables que de leur propre cybersécurité et ne peuvent intervenir pour les autres organisations. Par ailleurs, au sein des SDF, chaque arme contrôle ses propres capacités[9].

Dans la société, en dépit d'une volonté exprimée depuis 2015, le Japon demeure très en retard en matière de digitalisation que ce soit au niveau des institutions gouvernementales, des administrations centrales ou locales, de l'accès au service ou du secteur privé[10]. La volonté de rationalisation ne s'est pas encore traduite par une harmonisation des systèmes et des logiciels utilisés. L'architecture des sites internet, y compris ceux des plus grandes universités, est souvent obsolète. Dans les entreprises privées, si des progrès sont indéniables dans les très grands groupes, c'est beaucoup moins le cas, y compris en ce qui concerne la prise de conscience des enjeux de sécurité, dans les PME, dont le tissu est particulièrement dense dans l'archipel. Par ailleurs, même si la digitalisation existe, elle n'a généralement pas entraîné de transformation majeure dans les modes de gestion[11].

C'est pour remédier à ces lacunes et répondre à ces défis que le Japon met aujourd'hui l'accent sur la dimension cyber de la sécurité.

La place du cyber dans la Stratégie de sécurité nationale et la Stratégie de défense nationale

Les deux documents publiés par le Japon au mois de décembre 2022 mettent l'accent sur le développement de la cybersécurité, par une augmentation considérable des capacités du Japon en la matière et une réforme de l'architecture de défense pour une meilleure prise en compte

[8] World Digital Competitiveness Ranking 2022, consulté le 25 janvier 2022. En Asie, la Corée se situe au 8ème rang, Taïwan au 10ème, la Chine au 17ème.
[9] Kazuto Suzuki, intervention lors du séminaire « Cyber Security: Common Challenges to Europe and Japan in Post Ukraine War Context » (voir note 1).
[10] Lena Broeckaert, *Digital Transformation in Japan,* EU Japan Center for Industrial Cooperation, février 2022.
[11] *Ibid.*

de cette dimension. Il s'agit également d'accroître la prise de conscience des enjeux, d'améliorer les capacités de réponse de tous les organismes gouvernementaux (ministères, forces d'autodéfense, police, etc.) et de veiller à la protection des technologies sensibles dans les secteurs civils et militaires.

Répondre aux nouvelles méthodes de la guerre hybride, dont le cyber fait partie, est présenté comme un défi majeur pour les futures capacités de défense du pays. Le renforcement de l'architecture de défense doit mobiliser tous les aspects de la puissance, militaire mais aussi scientifique, technologique, civile, etc., et cette ambition s'applique tout particulièrement au domaine cyber[12].

Ainsi, dans la Stratégie de sécurité nationale, le mot « cyber » est mentionné 29 fois pour un texte de 36 pages. La cybersécurité fait l'objet d'une partie spécifique intitulée *Improve Response Capabilities in the Field of Cyber Security*[13]. Dans la Stratégie de défense, l'occurrence est de 41 fois pour un texte de 38 pages[14]. S'il n'y a pas de section spécifique, le cyber s'impose dans tous les domaines. La dimension cyber de la défense et de la sécurité prend donc pour le Japon une importance croissante, globalisante, qui se traduit dans la définition d'objectifs très élargis et la recherche de moyens nouveaux.

Une réflexion élargie et des moyens diversifiés

Le premier de ces moyens est la rationalisation et le renforcement des institutions en charge de la cybersécurité. La Stratégie de sécurité nationale prône la restructuration du NCIS, transformé en une organisation nouvelle pour coordonner l'ensemble des politiques en matière de sécurité et prendre en charge toutes les dimensions de la cyberdéfense nationale[15].

Le document *Defense of Japan 2022* mentionne également l'établissement d'une unité de défense cybernétique (*cyber defense unit*) installée au mois de mars 2021 au quartier général du ministère de la Défense à Tokyo. Cette unité est responsable de la défense cybernétique de l'ensemble des forces qui disposent aussi de leurs propres unités de défense cybernétique[16].

Au niveau conceptuel, on assiste à une évolution semblable à celle que l'on constate dans le domaine des missiles, avec une réflexion approfondie sur les capacités de frappe préemptive[17]. La réflexion intègre désormais le concept de défense active appliquée au cyber. L'objectif, pour renforcer les capacités contre les attaques cyber, est d'adopter une posture de défense « avancée » permettant l'évaluation en continu du risque sur les systèmes d'information critiques. Dans cet objectif, les forces d'autodéfense doivent se doter des moyens « *de pénétrer, de perturber ou de neutraliser l'utilisation, par un adversaire, du domaine cyber* »[18]. Il s'agit de surveiller de potentiels attaquants et d'être capable de contre-hacker leur système, qu'il s'agisse d'acteurs privés ou étatiques[19]. Il s'agit également, selon le document du ministère de la Défense, de se doter des capacités de surveiller et d'évaluer en continu le système informationnel de toutes les agences gouvernementales, de mener toute action nécessaire pour détecter les

[12] *National Security Strategy*, *op. cit.*
[13] *Idem.*
[14] *National Defense Strategy*, *op. cit.*
[15] *National Defense Strategy*, *op. cit.*
[16] *Defense of Japan 2022*, consulté le 15 janvier 2023 ; « Japan's SDF Launches New Cyber Defense Unit », 17 mars 2022.
[17] Mari Yamaguchi, « Japan Declares Plans to Have Preemptive Strike Capabilities and Cruise Missiles », *Japan Today,* 17 décembre 2022.
[18] *National Defense Strategy, op. cit.*
[19] « Japan to Upgrade Cyber Defense Allowing Preemptive Measures », *Nikkei Asia,* 11 décembre 2022.

serveurs – y compris privés – susceptibles d'être attaqués en utilisant les informations fournies par les pourvoyeurs de services de télécommunication. En cas d'attaque, le partage des informations entre entités privées et organisations gouvernementales doit également être renforcé[20].

Cette capacité de mobiliser une cyberdéfense active pour éliminer à l'avance la possibilité d'une attaque cybernétique « sérieuse » doit pouvoir s'exercer même si cette attaque cybernétique n'est pas assimilée à une attaque armée. Une attaque cybernétique « sérieuse » étant définie comme une attaque contre les organisations gouvernementales ou des infrastructures critiques[21].

Le Japon a également l'ambition de développer ses capacités en prenant en compte la dimension cognitive et celle de la guerre de l'information – qui s'appuie aussi sur les ressources du cyber et de l'intelligence artificielle – auxquelles sont confrontées les démocraties. En la matière, la menace la plus importante provient – dans le cas du Japon – de la Chine, qui a mis la manipulation de l'information et la supériorité en matière informationnelle dans tous les domaines au cœur de sa réflexion stratégique dans un contexte de guerre asymétrique. Face à cette offensive, les capacités de résistance mais aussi de « contre-information » doivent être renforcées à tous les niveaux de l'administration[22].

Au niveau opérationnel, et partant d'un niveau très modeste, les forces d'autodéfense veulent établir à l'horizon 2027 une posture de cybersécurité capable de protéger les opérations de contrôle et de commandement et les systèmes prioritaires soumis à une attaque cybernétique tout en appuyant les capacités de défense cybernétique de l'industrie de défense. A l'horizon 2030, l'objectif est de pouvoir accomplir toutes les missions dans les conditions d'une attaque cybernétique tout en renforçant la capacité des forces d'autodéfense à assurer la défense cybernétique d'entités qui lui sont extérieures[23].

Il s'agit également pour les forces japonaises d'intégrer les capacités des trois domaines de l'espace, du cyber et de l'électromagnétisme pour créer des synergies favorables à une meilleure réponse, l'ambition officielle étant d'atteindre un niveau de capacité de réponse « *supérieur ou meilleur que celui des pays occidentaux* »[24].

En termes de personnel, l'objectif est de renforcer les unités spécialisées des forces d'autodéfense pour atteindre 5 000 hommes à l'horizon 2027. En 2022, l'effectif de l'unité de défense cybernétique créée au mois de mars était de 540 hommes, 890 en comptant l'ensemble du personnel affecté à d'autres armes[25]. La création d'un enseignement cyber spécialisé intégré à l'enseignement technique supérieur des forces terrestres d'autodéfense est également prévu, ainsi que la multiplication des exercices, y compris avec l'OTAN. Du 13 au 16 avril 2021, une équipe des forces d'autodéfense a participé pour la première fois aux exercices Lock Shield organisés par le Cooperative Cyber Defense Center of Excellence (CCDCE) de l'OTAN[26]. Le Japon

[20] *National Security Strategy*, *op. cit.*
[21] *Idem.*
[22] *National Defense Strategy*, *op. cit.*
[23] *Idem.*
[24] *Idem.*
[25] « Japan Plans to Boost Cyber Defense Personnel by Fiscal 2027 », *Japan Times,* 30 octobre 2022.
[26] Voir site du ministère de la Défense.

a également participé à distance aux exercices au mois de juin 2022, en équipe avec le Royaume-Uni[27]. Il s'agit pour l'archipel de mieux évaluer ses capacités et de se situer par rapport à celles des trente pays impliqués, avec un retard estimé à une dizaine d'années par rapport aux autres grandes démocraties[28].

La montée en puissance des ressources humaines qualifiées se heurte toutefois au faible niveau de digitalisation et de compétence de la société. En matière d'innovation, le tissu de *start ups* demeure très insuffisant dans l'archipel, peu favorisé par les offres de financement, traditionnellement tournées vers les très grandes entreprises. Ces dernières ont longtemps été la principale source d'innovation, notamment dans le domaine automobile ou celui de l'électronique grand public, mais c'est beaucoup moins le cas – pour le moment – dans le domaine cyber[29].

Dans la population en général, en 2015, seuls 46 % de la génération des 16-25 ans avaient la capacité de résoudre des problèmes dans un environnement technologique complexe. Ce taux n'était que de 10 % pour la génération des 55-65 ans, qui est celle de l'encadrement à tous les niveaux[30]. De même, le taux d'utilisation des services informatiques de l'administration n'est que de 7,9 % alors que la moyenne des pays de l'OCDE est de 63,3 %. Enfin, si 91,5 % des entreprises au Japon ont une forme de présence sur internet, seuls 30 % des employés peu qualifiés formés en interne sont préparés à mettre en œuvre la transformation digitale dans laquelle le Japon veut s'engager[31].

Tous ces éléments, qui s'expliquent aussi par le vieillissement de la population, une hiérarchie encore très marquée par la gérontocratie, une utilisation essentiellement ludique ou consommatrice d'internet à partir d'un téléphone portable ou d'une console de jeu, limitent les capacités de recrutement de personnel qualifié dans les entreprises privées mais aussi dans l'administration et pour couvrir les besoins des forces d'autodéfense.

Renforcer la coopération internationale

Les deux documents stratégiques publiés au mois de décembre 2022 soulignent également la nécessité pour le Japon, dans son adaptation aux nouvelles formes de guerre, y compris dans le cyber, de coopérer plus étroitement avec « *ses alliés, les pays qui partagent les mêmes valeurs et d'autres* »[32]. En ce qui concerne les alliés, ce sont les Etats-Unis qui sont au premier rang, dans le cyber comme dans d'autres domaines. Mais la coopération internationale et la mise en place de « partenariats digitaux » avec d'autres puissances comme la France dans l'espace Indo-Pacifique pourrait aussi permettre d'améliorer la surveillance des activités illicites déstabilisatrices dans le domaine maritime, et la surveillance des câbles sous-marins. Plus globalement des actions communes peuvent être menées en s'appuyant sur la collaboration dans le domaine cybernétique dans le cadre de la lutte contre le changement climatique[33].

---

[27] Koichiro Komiyama, « JPCERT/CC Participated in the Locked Shield 2022 », JPCERT/CC Eyes, 1er juin 2022. Le commentateur note la nécessité pour l'équipe japonaise de communiquer en anglais.
[28] Les exercices *Lock Shield* sont organisés depuis 2010. La France y occupe régulièrement la première ou la seconde places dans plusieurs catégories.
[29] Lena Broeckaert, *op. cit.*
[30] OECD, Going Digital Toolkit.
[31] *Ibid.*
[32] *National Defense Strategy, op. cit.*
[33] Kazuto Suzuki (voir note 1).

Le Japon a également financé en 2018 un centre de *capacity building* dans le domaine cyber avec l'ASEAN, l'objectif étant de former 700 professionnels en quatre ans. Le centre, qui fait aussi partie de l'offensive diplomatique du Japon en direction des pays d'Asie du Sud-Est pour contrer l'influence de la Chine, offre une série de cours qui portent sur les *malwares*, le *hacking* ou l'entraînement aux exercices de cyberdéfense[34].

Sur la scène internationale, le domaine cybernétique constitue en effet pour le Japon, comme le désarmement nucléaire, une niche de politique étrangère avec le lancement du concept de *data free flow with trust* (DFFT) en 2019 à l'occasion du sommet du G20 d'Osaka. Il s'agit d'encourager la libre circulation des données publiques entre partenaires de confiance tels que les Etats-Unis, l'Union européenne ou l'Inde, tout en contrôlant la diffusion ou le vol d'informations sensibles – informations personnelles, technologiques et tout type d'information nuisant à la sécurité du pays. Le concept DFFT se veut une réponse au modèle chinois autoritaire de contrôle de l'information par la censure et d'exploitation des failles de l'adversaire, notamment en ce qui concerne le vol de propriété intellectuelle[35]. Toutefois, le niveau encore insuffisant du Japon en matière de sécurité et de protection des données peut freiner la mise en place de cette liberté totale de circulation des données entre « alliés de confiance »[36].

Conclusion

Depuis 2015 et l'adoption de la première *Cyber Security Strategy,* le Japon a donc accompli des avancées significatives en matière de cybersécurité, notamment dans la prise de conscience et la définition des objectifs au travers des deux textes fondamentaux consacrés à la sécurité et à la défense nationale publiés en décembre 2022. En 2015, la perspective des Jeux olympiques de 2020 a joué un rôle moteur dans cette prise de conscience et la mise en place d'institutions consacrées à la cybersécurité. A partir de 2020, la pandémie de Covid-19 et les besoins de dématérialisation qu'elle a entraînés ont considérablement accéléré l'impulsion initiale. La montée en puissance technologique de la Chine dans le domaine de l'intelligence artificielle et l'agressivité revendiquée de sa stratégie extérieure ont également joué un rôle majeur. Au sein du groupe des démocraties avancées, le Japon ne peut se laisser distancer, sous peine d'apparaître comme un maillon faible dans un secteur stratégique pour la sécurité des données et les combats futurs.

Pourtant, les obstacles sont encore importants, difficiles à écarter et de plusieurs ordres. Comme nous l'avons vu, le faible niveau de digitalisation d'une société vieillissante peut être une forme de protection « négative » mais est aussi une source de vulnérabilité aux opérations de pénétration ou d'influence. La méfiance de la population face aux risques d'intrusion des autorités dans leur volonté d'atteindre une libre circulation des données et d'obtenir une collaboration plus étroite entre entreprises privées et organisations gouvernementales limite les progrès possibles. Ainsi, en dépit de pressions croissantes, les Japonais demeurent réticents à utiliser le numéro d'identification universel *My Number*, pour le moment toujours facultatif, notamment en raison de la mauvaise protection des données au niveau des administrations locales.

[34] Voir le site du Centre.
[35] *Idem.*
[36] De même, le faible niveau de protection du secret au Japon, en dépit de l'adoption, en 2013, de l'*Act of protection of special designated secrets*, et l'absence de service de renseignement centralisé rendent peu probable l'intégration de l'archipel au groupe très fermé des *Five Eyes.*

Mais les obstacles se situent également au niveau politique et législatif. Si les partis politiques de gouvernement s'accordent sur la nécessité d'améliorer les capacités du Japon en matière de cybersécurité, les questions budgétaires de financement des objectifs énoncés ne sont pas résolues. Au sein même du PLD (Parti libéral démocrate) au pouvoir, des divisions existent sur les méthodes de financement, qui passeraient notamment par l'augmentation des impôts. La question recoupe celle de l'augmentation du budget de la défense, qui devrait atteindre 2 % du PIB en 2027. En dépit des annonces, aucun calendrier précis n'a été présenté pour le financement d'un budget dont une partie concerne la cybersécurité[37].

Les questions budgétaires touchent également au fonctionnement en silos étanches des institutions gouvernementales, civiles et militaires, concernées par les questions de cybersécurité. Si l'ambition est de renforcer le partage d'information, une meilleure coopération et la rationalisation des organisations, la défense de chaque territoire administratif pèse sur la mise en œuvre des objectifs proclamés. Par ailleurs, le ministère de la Défense est très loin d'être le plus puissant pour s'imposer à ses partenaires, y compris au nom de l'amélioration des capacités globales en matière de cybersécurité.

Enfin, la mise en œuvre des mesures annoncées impose une révision du cadre législatif et constitutionnel du Japon. Au niveau constitutionnel, l'article 21 de la Constitution garantit la protection des communications privées. Il interdit de surveiller les échanges et d'identifier la source d'une attaque possible et rend difficile la mise en œuvre du concept de défense active et d'attaque préemptive en matière de sécurité[38]. En dehors du cadre d'une situation d'urgence avec mobilisation des forces, il est également impossible aux forces d'autodéfense d'imposer leur aide et le partage des informations aux entreprises privées[39]. A un autre niveau, le concept de défense active appliqué au cyber, avec la mise en œuvre d'une capacité de surveillance ou de contre-mesures préemptives (intrusion et contre-*hacking*), est mis en cause au nom du respect du caractère exclusivement défensif de la politique de défense du Japon ; au risque de ralentir ou de compromettre les évolutions destinées à mieux répondre aux menaces auxquelles l'archipel est confronté[40].

Sans réforme constitutionnelle et législative, le Japon ne pourra pas mettre en œuvre les objectifs énoncés en matière de cybersécurité. Par ailleurs, l'acceptation de ces évolutions par l'opinion publique est également un facteur d'autant plus important que les moyens d'action de l'Exécutif contre la volonté du Parlement, et donc de l'opinion publique, demeurent limités. Un des obstacles en matière d'acceptabilité de ces évolutions demeure le niveau peu élevé de protection des données privées et la faiblesse de la législation. A ce titre, un dialogue accru avec l'Union européenne, qui a mis en place en 2018 la *General Data Protection Regulation* (GDPR), une des régulations les plus sévères en matière de protection des données, pourrait s'avérer très positif. En France, la Loi informatique et liberté, qui date de 1978 et a été actualisée en 2019 pour intégrer les dispositions prévues par la GDPR, constitue aussi un modèle dont le Japon pourrait s'inspirer dans sa marche vers la mise en œuvre d'un système de cybersécurité à la fois performant, sûr et équitable[41].

[37] Isabelle Reynolds, « Japan PM Kishida Faces Call for Election Over Defense Tax Hike », 30 janvier 2023.
[38] Kazuto Suzuki (voir note 1).
[39] *National Defense Policy*, *op. cit.*
[40] Daisuke Akimoto, « Exploiting Japan's Policy Debate on Strike Capability », *The Diplomat,* 7 août 2020.
[41] Kazuto Suzuki (voir note 1).

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

WWW.FRSTRATEGIE.ORG

ISSN : 2273-4643