ASSEMBLEE PARLEMENTAIRE DE L'OTAN

COMMISSION SUR LA DÉMOCRATIE ET LA SÉCURITÉ (CDS)

RENFORCER LA RÉSILIENCE DES SOCIÉTÉS ALLIÉES GRÂCE À LA PRÉPARATION DU SECTEUR CIVIL

Projet de rapport général

Joëlle GARRIAUD-MAYLAM (France)
Rapporteure générale

011 CDS 21 F rév. 1 | Original : français | 30 juillet 2021

Fondée en 1955, l'Assemblée parlementaire de l'OTAN est une organisation interparlementaire consultative qui est institutionnellement séparée de l'OTAN. Tant qu'il n'est pas adopté par les membres de la commission sur la démocratie et la sécurité, le présent document de travail représente seulement le point de vue du de la rapporteure générale. Il est basé sur des informations provenant de sources accessibles au public ou de réunions tenues dans le cadre de l'AP-OTAN - lesquelles sont toutes non classifiées.

TABLE DES MATIÈRES

SYNTHÈSE

La pandémie de Covid-19 a douloureusement démontré l'importance pour les sociétés alliées de renforcer leur préparation et leur capacité de réponse aux crises. Consolider notre résilience par la préparation du secteur civil apparaît ainsi plus essentiel que jamais face à la complexification de l'environnement sécuritaire et la multiplication des menaces militaires et non-militaires affectant l'ensemble de nos sociétés.

Malgré des efforts substantiels réalisés par l'OTAN et les pays alliés au cours des deux dernières décennies, des vulnérabilités persistent dans ce domaine. Lors du sommet de l'OTAN en juin 2021, les chefs d'État et de gouvernement se sont engagés à continuer de renforcer la résilience nationale et collective des pays alliés. Ce projet de rapport offre des pistes de réflexion pour avancer dans cette direction et développer au sein de l'Alliance une approche pansociétale de la résilience, dans laquelle l'ensemble des acteurs civils et militaires fonctionneraient en plus grande complémentarité. Il suggère notamment de s'inspirer des succès acquis par plusieurs états membres et pays partenaires. Enfin, il émet des recommandations visant à permettre de renforcer la capacité de nos sociétés à faire face aux risques présents et futurs.

Ce projet de rapport sera présenté et examiné par la commission sur la démocratie et la sécurité (CDS) en vue de son adoption à la prochaine session annuelle de l'Assemblée parlementaire de l'OTAN.

I. INTRODUCTION

1. En 2020, le déclenchement de la pandémie de Covid-19 et ses répercussions dans les domaines sanitaire, politique, économique, sociétal et sécuritaire ont douloureusement rappelé la nécessité pour les gouvernements et les sociétés alliés de renforcer leur préparation et leur capacité à répondre à tous les types de crises, qu'il s'agisse de menaces militaires, de catastrophes naturelles ou de risques épidémiologiques. Nombre de gouvernements avaient, en effet, identifié le déclenchement d'une pandémie comme un risque potentiel. Pour autant, bien peu avaient fait de la préparation à une telle menace une priorité. La réponse des sociétés alliées n'a donc pas été suffisamment efficace. Elle a notamment été marquée par l'adoption de réflexes contreproductifs par la population, une communication parfois hasardeuse des autorités, un manque dommageable de coordination entre les différents éléments du secteur civil et les autorités, des insuffisances flagrantes dans la coopération multilatérale et internationale et des interruptions fréquentes de chaînes d'approvisionnement. Ces manquements, combinés à la dissémination de désinformation par des acteurs hostiles, ont mis à l'épreuve les fondements démocratiques des systèmes et institutions alliés.

2. Les difficultés rencontrées dans les réponses apportées à la pandémie font de la nécessité d'adopter une approche pansociétale de la résilience l'une des premières leçons à tirer de cette crise. Afin de faire face à la crise sanitaire actuelle, mais aussi aux chocs et défis futurs, il est essentiel que les acteurs civils et militaires fonctionnent en complémentarité. Ces préoccupations ne sont néanmoins pas nouvelles. Dès la création de l'Alliance et durant la guerre froide, les pays alliés ont mis en place ou consolidé des politiques de renforcement de la résilience par la préparation du secteur civil. Ces efforts étaient soutenus et financés à l'échelle nationale comme otanienne. Néanmoins, l'effacement progressif de la menace soviétique a temporairement fait perdre de leur importance à ces concepts dans les politiques de sécurité de l'Alliance.

3. Aujourd'hui, les Alliés font face à un environnement sécuritaire de plus en plus complexe et diversifié. Dans ce contexte, la notion de résilience par la préparation du secteur civil revient au cœur des préoccupations liées à la défense et à la réponse aux crises. Lors du sommet de Varsovie en 2016, les chefs d'État et de gouvernement alliés ont adopté un *Engagement en faveur d'une meilleure résilience*. Au sommet de juin 2021, ils ont renouvelé et consolidé cet engagement en approuvant un *Engagement renforcé en faveur d'une meilleure résilience*. Ils y déclarent que « la résilience nationale et collective est un élément primordial pour une dissuasion et une défense crédibles ainsi que pour la bonne exécution des tâches fondamentales de l'Alliance, et qu'elle est vitale dans les efforts que nous déployons pour protéger nos sociétés, nos populations et nos valeurs communes ». L'OTAN reconnaît ainsi, d'une part, que la capacité et les actions militaires de l'Alliance dépendent désormais en grande partie du soutien, de l'expertise et des infrastructures du secteur civil. D'autre part, elle constate que les menaces sécuritaires auxquelles elle est confrontée ne sont plus toutes d'ordre militaire et tendent à affecter l'ensemble des éléments des sociétés alliés ; en cela, elles requièrent une combinaison de réponses militaires et civiles.

4. Relever les défis posés par les menaces présentes et futures nécessite un changement de culture encore plus profond au sein de l'Alliance. Les pays membres doivent, tout en maintenant leurs engagements visant à renforcer leur capacité militaire (et notamment celui de consacrer 2 % de leur PIB aux dépenses de défense), donner un rôle plus central aux acteurs civils qui contribuent à la résilience de nos sociétés face aux crises. Le secteur privé, les autorités nationales et locales, et surtout les citoyens eux-mêmes, doivent être reconnus comme des acteurs à part entière de la sécurité des États membres. La résilience de notre

Source: Centre d'excellence sur la cooperation civilo-militaire (CIMIC)

Alliance dépend à la fois d'une meilleure préparation de ces différents acteurs civils aux risques présents et futurs et d'une coopération efficace et approfondie entre eux et avec les forces armées.

5. Il convient ici de définir les concepts de résilience et préparation du secteur civil. La notion de **résilience** est définie par l'OTAN comme l'aptitude d'une société à résister à un choc majeur comme une catastrophe naturelle, une défaillance d'infrastructures critiques ou une attaque armée, et à s'en remettre aisément et rapidement (OTAN, 2018). Une société résiliente est donc une cible moins attrayante pour des acteurs extérieurs malintentionnés, ce qui réduit son exposition aux attaques, qu'elles soient classiques ou non, et donc sa vulnérabilité. Une telle société est aussi plus à même de rebondir après une catastrophe naturelle de grande ampleur. Le développement de cette capacité suppose l'interaction cohérente et la préparation des acteurs civils et militaires en amont des crises.

6. La **préparation du secteur civil**, quant à elle, est définie par l'OTAN comme la « capacité d'assurer la continuité des fonctions de base de l'État en situation d'urgence ou en cas de catastrophe naturelle, que ce soit en temps de paix ou en période de crise » (OTAN, 2020). Elle comprend, d'une part la protection civile, c'est-à-dire la résilience du secteur civil en cas de guerre ou de menace de guerre, et d'autre part la préparation aux crises, que l'on définira ici comme la capacité de la société à prévenir et à gérer une crise en temps de paix.

7. Ces dernières années, un nombre croissant d'États ont mis l'accent sur la notion de résilience pansociétale comme objectif de leurs stratégies de sécurité et de gestion des crises. En particulier, dans certains États membres de l'OTAN, tels que l'Estonie et la Norvège ; pays partenaires, comme la Finlande, Israël, la Suède, et la Suisse ; ou bien d'autres États, comme Singapour, le développement de la résilience par la préparation du secteur civil constitue un aspect central des politiques dites de « **défense totale** ». La défense totale décrit une approche de la sécurité impliquant l'ensemble de la société à travers une collaboration institutionnalisée, sous le contrôle démocratique des autorités politiques, entre ces dernières, les forces armées, les administrations civiles, le secteur privé, et le public. Elle vise à dissuader un ennemi potentiel en augmentant le coût d'une attaque et en réduisant ses chances de succès.

II. L'ÉVOLUTION PARALLÈLE DE L'ENVIRONNEMENT SÉCURITAIRE ET DES POLITIQUES DE LA RÉSILIENCE

A. LA PRÉPARATION DU SECTEUR CIVIL AU CŒUR DES DOCTRINES DE DÉFENSE PENDANT LA GUERRE FROIDE

8. Durant la guerre froide, les autorités nationales des pays alliés ont développé des politiques de « défense civile » (ou « plans d'urgence dans le domaine civil ») visant à accroître la résilience des sociétés par la préparation du secteur civil. Ces efforts avaient principalement pour objectif de renforcer la capacité des autorités locales à faire face à une crise et celle des citoyens à subvenir à leurs besoins par eux-mêmes, au cas où les autorités gouvernementales seraient temporairement dans l'incapacité d'intervenir.

9. Ces efforts se sont matérialisés sous différentes formes, telles que la construction d'abris antiatomiques, l'élaboration de plans d'évacuation massive, la constitution de groupes locaux de protection civile et la création d'agences gouvernementales spécialisées. Ils incluaient également la mise en place de programmes d'éducation du public, notamment à travers la diffusion dans les écoles de vidéos d'information et la distribution au sein de la population de brochures sur les réactions à adopter en cas d'urgence, comme cela a été par exemple fait massivement en Suède.

10. Les efforts de préparation du secteur civil n'étaient pas limités aux pays de l'Alliance pendant la guerre froide. Ils étaient aussi perçus comme une préoccupation d'importance stratégique de l'autre côté du rideau de fer. L'Union soviétique organisait ainsi fréquemment de vastes programmes

de préparation de sa population aux situations d'urgence. Ceux-ci incluaient notamment des formations obligatoires pour le grand public, des exercices et alertes périodiques et la large diffusion d'informations sur le rôle de la population en cas de crise.

B. ÉVOLUTION ET ESSOUFLEMENT DES EFFORTS DE RENFORCEMENT DE LA RÉSILIENCE PENDANT LES ANNÉES 1990

11. La fin de la guerre froide et la disparition de la menace soviétique ont entrainé un relâchement des efforts dans le domaine de la résilience par la préparation du secteur civil dans les années 1990, tant au niveau national qu'otanien. La probabilité d'une attaque militaire conventionnelle contre le territoire des pays de l'OTAN était désormais perçue comme faible. De plus, la multiplication des crises au-delà de ses frontières a poussé l'OTAN à se concentrer sur des opérations « hors zone ».

12. En conséquence, les investissements dans ce domaine ont diminué drastiquement. Cela s'est notamment traduit par une privatisation progressive et une externalisation de tâches et d'infrastructures militaires. Pendant la guerre froide, les efforts étatiques en matière de renforcement de la résilience étaient facilités par le fait que de nombreux moyens civils, cruciaux en cas de crise, étaient sous contrôle étatique et pouvaient donc, le cas échéant, être rapidement mis au service de la défense. À partir des années 1990, ces ressources civiles, au rôle essentiel dans la résilience d'une nation, telles que les infrastructures énergétiques et les réseaux de transports, deviennent principalement exploitées par des acteurs commerciaux. Ainsi, d'après l'OTAN, environ 90 % du transport militaire impliqué lors d'opérations militaires de grande envergure est aujourd'hui réalisé par le secteur commercial. De même, en moyenne, plus de 30 % des communications par satellite utilisées à des fins de défense sont fournies par le secteur privé (OTAN, 2018).

13. Les programmes de renforcement de la résilience par la préparation du secteur civil ayant perduré durant les années 1990 ont ensuite changé d'objectifs. L'accent s'est déplacé de la capacité de la société à faire face à une attaque militaire à sa capacité à réagir en cas de catastrophe naturelle. Par exemple, en Norvège, la politique de défense totale qui avait été en vigueur durant la guerre froide a été revue et recentrée sur la préparation aux crises en temps de paix (Wither, 2020). Cette évolution a notamment permis d'adopter une approche plus intégrée de la préparation du secteur civil, fondée sur le fait que les procédures en termes d'évacuation, de communication, et de survie sont largement partagées, que la menace soit d'ordre militaire ou non.

C. UN REGAIN D'INTÉRÊT POUR LES POLITIQUES DE LA RÉSILIENCE PAR LA PRÉPARATION DU SECTEUR CIVIL FACE À LA MULTIPLICATION DES RISQUES SOCIÉTAUX

14. L'émergence de la menace non-conventionnelle posée par le terrorisme international à l'intérieur des frontières de l'OTAN, particulièrement à partir des attaques du 11 septembre 2001, a entrainé un regain d'intérêt pour les politiques de renforcement de la résilience par la préparation du secteur civil. Le défi terroriste et la menace de prolifération d'armes de destruction massive ont influencé les stratégies de préparation. Ces dernières ont ainsi vu leur champ s'élargir à une large variété de menaces, y compris les armes chimiques, biologiques, radiologiques et nucléaires (CBRN) et les attaques contre les infrastructures critiques.

15. Depuis lors, la complexification croissante de l'environnement sécuritaire n'a fait que renforcer cette tendance. L'OTAN fait aujourd'hui face à un large éventail de risques qui tend à s'accroître. Il va d'un potentiel conflit interétatique conventionnel aux menaces posées par des acteurs non-étatiques, en passant par le danger posé par les catastrophes naturelles, ou encore par la pandémie actuelle de Covid-19. Depuis 2014, le recours par la Russie à la guerre hybride, parce qu'elle vise précisément à exploiter les vulnérabilités d'une société pour la fragiliser, a aussi poussé les Alliés à repenser leur approche de la résilience (Gjørv, 2020). L'augmentation du nombre et de l'impact des cyberattaques affecte aussi de plus en plus la capacité des États à assurer la continuité

des services publics et à gérer une crise. Durant la pandémie de Covid-19, en mai 2021, une cyberattaque contre les services de santé irlandais a, par exemple, forcé les autorités à mettre à l'arrêt pendant plusieurs semaines une large partie du système informatique dont ces derniers dépendent pour répondre à l'urgence sanitaire (Perlroth et Satariano, 2021). D'autres cyberattaques, comme WannaCry en 2017 et SolarWinds en 2020 ont similairement mis en lumière le risque croissant pour nos sociétés que pose l'exploitation de cybervulnérabilités par des acteurs malintentionnés. Par ailleurs, la menace grandissante que fait aujourd'hui peser le changement climatique sur la résilience de nos sociétés, en exaltant les risques préexistants est de plus en plus prise en compte par l'OTAN (Oppenheimer, 2020; Hill & Martinez-Diaz, 2020). Ces différents facteurs menacent des rouages essentiels du fonctionnement de nos sociétés tels que les communications, les transports, les systèmes de santé, l'approvisionnement en nourriture, en eau, et en énergie, sans oublier la continuité des pouvoirs et services publics.

16. Face à ces risques, au cours des deux dernières décennies, les Alliés ont partiellement pris conscience de la nécessité de venir compléter leurs capacités de défense en développant la résilience de leur société et en préparant leur secteur civil. En conséquence, ils ont adopté des mesures concrètes à cet effet à l'échelle nationale et otanienne. Pour autant, comme en atteste la pandémie actuelle, des efforts plus conséquents restent indispensables.

III. VERS UNE APPROCHE PANSOCIÉTALE DE LA PLANIFICATION ET DE LA GESTION DES RISQUES SÉCURITAIRES

A. LE RÔLE DES ACTEURS CIVILS DANS LA PRÉPARATION ET LA RÉPONSE AUX CRISES

Les autorités nationales et locales

17. Les autorités nationales et locales sont responsables du développement de la résilience sociétale. Premièrement, elles mettent en place le cadre législatif et institutionnel qui sous-tend la réponse aux crises. Elles développent notamment des plans d'urgence et des outils d'alerte précoce. Elles mettent aussi en place les systèmes leur permettant de se coordonner. De plus, les parlements élaborent, avant le déclenchement d'une crise, la législation permettant aux autorités d'agir en réponse à une menace. Ils veillent aussi à ce qu'un financement approprié soit attribué à des domaines clés tels que la protection des infrastructures critiques et le maintien de stocks de biens essentiels ou d'urgence. À cet égard, il est important de rappeler la nécessité d'accroître la participation des femmes au sein des autorités nationales et locales afin de garantir que leurs contributions et besoins soient bien intégrés dans les efforts de renforcement de la résilience.

18. Deuxièmement, les autorités nationales et locales aident les autres acteurs civils à se doter des capacités leur permettant de faire face à une crise, notamment dans le cas où la continuité du gouvernement ou sa communication ne sauraient être assurées. La population, en particulier, doit être informée à l'avance des mesures à prendre dans un tel cas. En Norvège par exemple, la direction de la protection civile a envoyé en 2018 à tous les ménages une brochure contenant des instructions sur les mesures à adopter en cas d'interruption temporaire des services publics essentiels en situation d'urgence, allant d'un conflit militaire à une catastrophe naturelle (Wither, 2020). En Lituanie, en 2015, le ministère de la défense et le service des sapeurs-pompiers ont élaboré conjointement un manuel sur la réponse aux situations de crise (Flanagan, Osburg, Binnendijk, Kepe, & Radin, 2019). D'autres Alliés, comme la Lettonie et l'Estonie, ont développé des brochures similaires.

19. Enfin, lorsqu'une crise frappe un pays, les autorités doivent prendre les décisions nécessaires en vue de la résoudre, les communiquer et les appliquer. Cela s'adresse évidemment à l'exécutif, mais aussi au corps législatif qui doit pouvoir continuer à fonctionner même en cas de crise. Au début

de la pandémie, les parlements alliés ont dû interrompre brièvement leurs travaux. Néanmoins, ils ont rapidement su faire preuve d'innovation et de flexibilité afin d'adapter le processus parlementaire à la situation sanitaire (Cartier, Richard, & Toulemonde, 2020). Les leçons de cette période difficile, pour les assemblées parlementaires, doivent être tirées afin de renforcer la résilience aux chocs de nos institutions démocratiques. Prendre, communiquer et appliquer les décisions nécessaires en cas de crise nécessite par ailleurs la mise en place de processus efficaces fondés sur des données et des informations probantes, ainsi que l'adoption d'une communication transparente et stratégique permettant aux autorités de gagner la confiance de la population et partant, son adhésion à leurs actions. Le rôle primordial de ces deux aspects dans le développement d'une réponse pansociétale efficace face à une crise a été amplement démontré lors de la pandémie de Covid-19, notamment en raison de la prolifération de désinformation qui l'a accompagnée. Il en ressort que se préparer, en amont d'une crise, à combattre la désinformation et la propagande en établissant la confiance de la population dans les actions des autorités, ainsi que dans les informations qu'elles fournissent, est un aspect clé de la préparation du secteur civil.

Le secteur privé

20. Le secteur privé représente à la fois une force et une vulnérabilité pour la résilience d'une nation. En effet, les entreprises privées sont sources d'efficacité et d'innovation, deux qualités nécessaires pour faire face aux crises. Néanmoins, leurs décisions sont fondées sur la recherche de profits, pas sur la résilience, ce qui les rend moins résistantes aux perturbations. La crise de la Covid-19 l'a démontré. D'une part, les entreprises pharmaceutiques ont su développer des vaccins novateurs contre le coronavirus en un temps record, qui devraient permettre de mettre un terme à cette crise. D'autre part, la diminution des transports et la fermeture des usines ont perturbé les chaînes d'approvisionnement et causé des goulots d'étranglement. On en a vu l'impact dans l'incapacité des pays alliés, au début de la crise, à obtenir des masques et autres équipements de protection individuelle dont la fabrication était dominée par des entreprises chinoises (Bradsher, 2020). Les chaînes d'approvisionnement alimentaire alliées et mondiales ont également été touchées pendant cette crise.

21. Pour mieux faire face aux menaces et chocs, il est donc crucial, premièrement, d'intégrer le secteur privé dans les efforts de renforcement de la résilience en amont des crises afin de maximiser sa contribution potentielle le cas échéant. En effet, il joue un rôle central dans la fourniture de biens nécessaires et dans le fonctionnement d'infrastructures essentielles dont dépendent les forces armées pour mener à bien leur mission de défense, mais aussi plus généralement au sein de la société pour faire face à une crise. Les plans d'urgence en place dans ce secteur doivent être améliorés, en coopération avec les autres acteurs, pour lui permettre de faire face à des catastrophes ou menaces de grande envergure pouvant potentiellement avoir un impact majeur sur la société tout entière.

22. Deuxièmement, au-delà de leur contribution à la résilience sociétale, les entreprises doivent s'assurer qu'elles sont elles-mêmes résilientes aux crises. C'est particulièrement le cas face aux cybermenaces, qui peuvent complètement remettre en cause leur capacité à fonctionner. Par exemple, en mai 2021, une cyberattaque a paralysé le principal opérateur privé américain d'oléoducs, Colonial Pipeline. Cette attaque a engendré des difficultés d'approvisionnement en carburant sur la côte Est des États-Unis pendant plusieurs jours. Un groupe criminel de piratage informatique, nommé Darkside et possiblement implanté en Russie, en serait à l'origine. Après cette attaque, les autorités américaines ont pris des mesures afin de renforcer la résilience des entreprises du pays aux cyberattaques. Elles ont publié des directives obligeant, entre autres, les exploitants de gazoducs et d'oléoducs à les informer lorsqu'ils sont la cible de cyberattaques et à désigner un responsable de la cybersécurité au sein de leur entreprise (Nakashima et Aratani, 2021).

23. Les risques associés à l'interconnexion entre secteurs ont ainsi été amplifiés par le rôle de plus en plus central joué par l'internet et les technologies de l'information dans le fonctionnement de

nos sociétés. L'ensemble des secteurs économiques en dépendent, de même que le fonctionnement des infrastructures critiques qui les soutiennent. Les débats actuels parmi les Alliés sur la sécurité de la 5G démontrent l'importance de telles infrastructures critiques sur la résilience des sociétés alliées.

24. En devenant de plus en plus complexes, intégrées et interdépendantes, nos sociétés ont développé des vulnérabilités croissantes que des acteurs malveillants cherchent à exploiter. Une défaillance dans un domaine économique peut causer des perturbations en cascade dans d'autres domaines, avec des conséquences graves pour l'ensemble de la société concernée (Schaake, 2020). En 2017, la cyberattaque NotPetya, lancée par des pirates informatiques russes, l'a démontré en paralysant des millions d'ordinateurs à travers le monde, dont environ la moitié en Ukraine. Dans ce pays, cette attaque a causé des perturbations conséquentes en effaçant les données d'ordinateurs appartenant à des banques, des entreprises du secteur de l'énergie, des hauts fonctionnaires ainsi que d'un aéroport (Perlroth, Scott, & Frenkel, 2017). En 2020, ce sont les chercheurs et compagnies impliqués dans le développement et la distribution de vaccins contre la Covid-19 qui ont été confrontés à des cyberattaques, notamment d'origine russe (Kuchler & Murphy, 2020; Sabbagh & Roth, 2020).

25. Troisièmement, il convient de mieux contrôler et défendre la capacité des entreprises à participer à la réponse aux crises. L'augmentation des investissements étrangers directs dans des secteurs stratégiques du secteur privé allié, notamment en Europe, par la Chine depuis la crise de 2008-2009, est une source d'inquiétude quant à la capacité de résilience des pays membres. Par exemple, des groupes chinois ont investi dans le port commercial du Pirée, en Grèce, ainsi que dans les aéroports de Londres Heathrow, Francfort Hahn, ou encore Tirana et Ljubljana. Ces investissements s'étendent aussi au secteur de l'énergie, comme le projet de construction de la centrale nucléaire Hinkley Point C à Somerset, au Royaume-Uni (Le Corre, 2018). L'augmentation de ces investissements dans plusieurs pays alliés interroge sur la capacité de ces derniers à contrôler et à utiliser ces infrastructures en cas de crise grave. Les gouvernements alliés doivent donc se concerter avec le secteur privé pour évaluer les vulnérabilités de ce dernier, et mettre en place des mesures correctives et des plans alternatifs.

La population civile

26. La population civile est probablement l'acteur le plus crucial, et le plus souvent négligé, en matière de résilience. Elle est la cible, voire la victime principale, de la majorité des menaces auxquelles font face les pays alliés. Néanmoins, si elle y est adéquatement préparée, elle constitue aussi la première ligne de défense face à ces mêmes menaces. La crise de la Covid-19 l'a montré. L'efficacité de la réponse au coronavirus dépend, en effet, au premier chef de l'acception et du respect par les citoyens des mesures adoptées par leurs autorités.

27. Il est donc essentiel de placer les citoyens au cœur des efforts de développement de la résilience. Ils doivent être formés à faire face à une crise de son début jusqu'à sa résolution et ce, y compris si les autorités ne sont pas en mesure d'apporter leur soutien habituel. Les autorités doivent promouvoir les connaissances et capacités nécessaires à cet effet au sein de la population en amont des crises. Par exemple, la brochure susmentionnée distribuée à la population par les autorités norvégiennes comprend des informations sur les stocks alimentaires de base, les lignes de communication d'urgence et la formation aux premiers secours. D'autres pays ont développé de telles brochures et il serait souhaitable que l'ensemble des Alliés suivent ces exemples. De même, le système éducatif doit participer à la formation des jeunes, filles comme garçons, à la réponse aux crises. Ces efforts doivent, entre autres, viser à développer la capacité des jeunes à détecter la désinformation qui mine la capacité de réaction des autorités et la confiance des citoyens en ces dernières en cas d'urgence. Les défis liés à la désinformation pendant la pandémie de Covid-19 ont rendu ce besoin évident.

28. Enfin, il est fondamental de générer parmi la population civile une volonté de protéger et de défendre les principes démocratiques qui forment les fondements de nos sociétés alliées. Les chocs sécuritaires peuvent être sources de remise en cause de ces derniers, de polarisation politique et de tensions sociales, comme cela a été le cas dans le cadre de la pandémie. À travers le développement de stratégies de communication plus inclusives et avec l'implication du système éducatif, les autorités doivent donc sans cesse réaffirmer et réaffermir le lien qui unit les citoyens aux valeurs et institutions démocratiques.

B. L'IMPORTANCE DE LA COORDINATION DES ACTEURS DU SECTEUR CIVIL ENTRE EUX ET AVEC LES FORCES ARMÉES DANS LA PRÉPARATION ET LA RÉPONSE AUX CRISES

29. Les forces armées restent évidemment les premières garantes de l'intégrité territoriale, de la dissuasion et de la défense alliées. Néanmoins, la diversification des risques et des vulnérabilités auxquels elles sont confrontées et leur dépendance croissante vis-à-vis du secteur civil nécessitent qu'elles s'engagent pleinement dans une approche pansociétale de la sécurité. En effet, une réponse efficace à une crise est aujourd'hui impossible sans l'implication combinée et coordonnée des secteurs militaire et civil.

30. La pandémie de Covid-19 a montré l'impact positif que peut avoir une coopération accrue entre le secteur civil et les forces armées face à une crise grave, y compris de nature non militaire. L'intervention des forces armées en soutien des structures civiles, notamment dans le domaine médical et dans celui de la logistique, a été l'un des rares points positifs dans la réponse à la pandémie. En Allemagne, par exemple, quelque 15 000 militaires ont participé à l'administration de tests, aux efforts pour retracer les chaînes de contamination ou à la fourniture d'équipement médical d'urgence. De même, au Royaume-Uni, environ 3 000 militaires ont été déployés en novembre 2020 pour aider les autorités civiles à effectuer des tests et répondre aux besoins logistiques. Au vu de son succès, cette coopération entre de multiples acteurs des secteurs civil et militaire, allant de l'armée à la police, en passant par les autorités nationales et locales, les instituts de recherche, le secteur privé et la société civile, dans la réponse à une crise de nature non-militaire devra absolument être formalisée et pérennisée à l'avenir.

31. Pour s'assurer que la coopération civilo-militaire soit efficace lorsqu'une crise se déclenche, il est en effet nécessaire d'institutionnaliser et d'opérationnaliser les relations entre les acteurs militaires et civils en amont des crises. Cela passe par l'organisation d'exercices permettant de tester les mécanismes de complémentarité et d'interaction entre ces acteurs en cas de crise. Des pays alliés organisent régulièrement des exercices à cet effet. Par exemple, la Lettonie a pris des mesures supplémentaires ces dernières années pour améliorer la coordination des efforts de tous ses ministères en vue de contribuer à la défense nationale et a mené des exercices périodiques pour en tester l'efficacité. La Lituanie a aussi organisé des exercices de grande échelle impliquant des institutions civiles et basés sur des scénarios de menaces non-conventionnelles. Par ailleurs, depuis 2013, ce pays organise chaque année l'exercice *Flaming Sword* visant à préparer ses forces armées et différentes autorités publiques à faire face ensemble à des menaces hybrides (Flanagan, Osburg, Binnendijk, Kepe, & Radin, 2019).

32. Malgré ces exemples positifs d'intégration et de coordination entre les secteurs civil et militaire en amont des crises, beaucoup reste à faire pour améliorer la coopération civilo-militaire dans les efforts de développement de la résilience parmi les Alliés. Cela nécessite la mise en place d'accords de coopération, de protocoles de préparation et de réaction, de formations, ainsi que la tenue d'exercices plus complets, impliquant secteurs civil et militaire, dans l'ensemble des pays de l'OTAN. Il conviendrait notamment de généraliser les bonnes pratiques déjà développées par les États alliés et les pays partenaires, et notamment par les quatre États étudiés au chapitre V.

IV. LE RÔLE DE L'OTAN EN MATIÈRE DE RÉSILIENCE ET DE PRÉPARATION DU SECTEUR CIVIL

A. LA RÉSILIENCE COMME ÉLÉMENT CRUCIAL DE LA SÉCURITÉ ALLIÉE DEPUIS LA CRÉATION DE L'OTAN

33. La résilience et la préparation civile ne sont pas seulement des ambitions, mais représentent aussi une obligation pour les Alliés. Des éléments à la base de la notion de résilience peuvent déjà être discernés dans le Traité de l'Atlantique Nord. Son article 3 déclare en effet que : « les parties, agissant individuellement et conjointement, d'une manière continue et effective, par le développement de leurs propres moyens et en se prêtant mutuellement assistance, maintiendront et accroîtront leur capacité individuelle et collective de résistance à une attaque armée ». Les États membres considèrent donc la résilience comme dépendant à la fois de la capacité militaire de l'Alliance, de l'état de préparation du secteur civil de chacun d'entre eux, et de la coordination et de l'intégration de ces deux éléments. En effet, des États bien préparés à répondre à tout type d'attaque ou de crise sont moins susceptibles d'être attaqués. En ce sens, l'article 5 ayant trait à la défense collective et l'article 3 concernant la résilience sont étroitement liés l'un à l'autre.

34. Bien que le développement de la résilience et la préparation du secteur civil soient des prérogatives nationales, depuis sa création, l'OTAN a développé dans ce domaine des capacités, connaissances, structures, et partenariats dont bénéficie l'ensemble des Alliés. L'OTAN joue aussi un rôle crucial dans la coordination des efforts nationaux et dans la mise en place d'objectifs et de références communs sur le sujet. En cela, elle rend l'action des États membres plus cohérente et efficace.

B. L'ÉVOLUTION RÉCENTE DE L'APPROCHE DE LA RÉSILIENCE PAR L'OTAN ET LA CRÉATION DES EXIGENCES DE BASE

35. Le besoin de résilience s'est progressivement étendu au-delà de la seule réponse à une attaque armée telle qu'envisagée par le Traité. D'une part, les catastrophes naturelles peuvent gravement affecter le fonctionnement des sociétés alliées. D'autre part, de nouveaux risques, comme les menaces hybrides ou les cyberattaques, peuvent ne plus atteindre le seuil d'une attaque armée, mais présentent toujours une menace pour la sécurité des Alliés. Pour cette raison, lors du sommet de Varsovie de 2016, les chefs d'État et de gouvernement de l'OTAN ont adopté un Engagement en faveur d'une meilleure résilience. Dans ce texte, ils notent que la résilience face aux nouveaux défis militaires et non-militaires commande aux Alliés de « maintenir et protéger les capacités civiles critiques, en plus des capacités militaires et à l'appui de celles-ci, et œuvrer au sein du secteur civil dans son ensemble, ainsi qu'avec le secteur privé », ainsi que de coopérer avec d'autres organisations internationales, notamment l'Union Européenne (UE), et les pays partenaires.

36. Lors de ce même sommet, sur la base d'une première évaluation (menée la même année) des capacités nationales en matière de résilience, les Alliés ont défini sept exigences de base dans ce domaine. Elles permettent de mesurer et de guider leurs efforts nationaux en faveur du développement de leur propre capacité et donc, par extension, de celle de l'Alliance entière. Elles concernent :

1. La garantie de la continuité des pouvoirs publics et des services publics essentiels et de leur capacité à prendre des décisions, à les communiquer et à les faire appliquer en période de crise ;
2. La résilience des approvisionnements énergétiques en mettant en place des plans et réseaux de secours ;
3. L'aptitude à gérer efficacement des mouvements incontrôlés de personnes ;

4. La résilience des ressources en nourriture et en eau en s'assurant que celles-ci soient protégées contre les perturbations et le sabotage ;
5. L'aptitude à gérer un grand nombre de victimes en veillant à ce que les systèmes de santé civils puissent faire face et que des fournitures médicales soient disponibles ;
6. La résilience des systèmes de communication civils, tels que les réseaux informatiques et de télécommunications, même en cas de crise ;
7. Le fonctionnement des systèmes de transport en veillant à ce que les forces de l'OTAN puissent se déplacer rapidement à travers le territoire de l'Alliance et que les services civils puissent utiliser ces réseaux, même en période de crise (OTAN, 2018).

37. Une seconde évaluation de la capacité de résilience de chaque Allié a été menée en 2018 sur la base de ces exigences. Elle a montré que, si le niveau de résilience et de préparation du secteur civil est élevé dans l'Alliance, des efforts supplémentaires sont nécessaires dans certains domaines.

38. En 2019, les dirigeants de l'OTAN ont souligné la nécessité de renforcer la résilience des infrastructures critiques et des systèmes de communication. À cette fin, les ministres alliés de la défense ont mis à jour la sixième exigence en soulignant la nécessité de disposer d'un réseau 5G fiable et d'options efficaces pour le rétablir si besoin. Ils ont aussi indiqué que les autorités nationales doivent bénéficier d'un accès prioritaire à ces réseaux en temps de crise et que les risques auxquels ces systèmes font face doivent faire l'objet d'évaluations approfondies et régulières.

39. Le renforcement de la résilience nationale et collective de l'Alliance a été l'un des thèmes centraux du sommet de l'OTAN en juin 2021. Les chefs d'État et de gouvernement y ont adopté l'agenda OTAN 2030, proposé par le secrétaire général, qui met en avant la nécessité d'accroître la capacité de l'Alliance à faire face aux crises futures. Ils ont, par ailleurs, agréé un Plan d'action sur le changement climatique et la sécurité. Ils y notent que le changement climatique met « à l'épreuve la résilience de nos installations militaires et de nos infrastructures critiques » et déclarent que « l'OTAN intégrera des considérations relatives au changement climatique dans les travaux qu'elle mène concernant la résilience, la préparation du secteur civil », entre autres.

40. Les dirigeants des pays de l'OTAN ont aussi approuvé à cette occasion un *Engagement renforcé en faveur d'une meilleure résilience* qui décrit plus en détail les mesures que l'Alliance compte prendre au cours des prochaines années dans ce domaine. Conformément à l'Article 3 du Traité de Washington, les Alliés s'y engagent à adopter une approche plus globale et mieux coordonnée de la résilience et de la préparation du secteur civil. Ils élaboreront prochainement une proposition en vue d'établir, d'évaluer et de revoir les exigences de base en matière de résilience, et d'en assurer le suivi. Ils ont l'intention de tirer les leçons de la pandémie afin de mieux répondre aux crises futures, notamment en renforçant la coopération civilo-militaire. Ils souhaitent intensifier leurs efforts pour sécuriser les chaînes d'approvisionnement, les infrastructures critiques et les systèmes de communication, pour assurer leur sécurité énergétique et pour renforcer leur capacité à faire face aux catastrophes naturelles. Ils s'engagent aussi à impliquer dans ces efforts les différents acteurs du secteur civil, ainsi que les pays partenaires et les organisations internationales concernées, notamment l'UE. Cet engagement renforcé rappelle enfin que la résilience de l'Alliance est intrinsèquement liée à l'attachement commun des États membres aux valeurs démocratiques qui sont au fondement de l'OTAN.

41. La Rapporteure prend note avec satisfaction de ce renforcement de l'engagement des Alliés en faveur de la résilience et de la préparation du secteur civil. Elle appelle les chefs d'État et de gouvernement à continuer de placer la résilience, y compris démocratique, au cœur des discussions sur le futur de l'OTAN dans le cadre du processus OTAN 2030 et de la révision du concept stratégique.

C. LES STRUCTURES ET EXERCICES DE L'OTAN AU SERVICE DE LA RÉSILIENCE

42. L'OTAN a développé des structures lui permettant de remplir sa mission de coordination et de soutien auprès des États membres dans le domaine de la résilience par la préparation du secteur civil. Créé dans les années 1950, le Comité pour l'étude des plans d'urgence dans le domaine civil (CEPC) est le principal organe consultatif en matière de préparation du secteur civil et rend compte directement au Conseil de l'Atlantique Nord. Il coordonne la planification des pays membres et leur fournit une expertise dans des domaines variés. Il peut aussi, à la demande d'un pays allié, déployer des équipes consultatives de soutien pour aider ce dernier à identifier les domaines dans lesquels il peut améliorer sa résilience, ainsi que des équipes de réaction rapide en cas de crise.

43. Le CEPC supervise plusieurs bureaux et comités d'étude techniques chargés d'élaborer des procédures communes aux Alliés pour faire face à des situations de crise. Ils rassemblent des experts des gouvernements nationaux et de l'industrie ainsi que des représentants militaires. Ils élaborent des plans d'urgence dans des domaines tels que la protection civile, les transports, les ressources industrielles, les communications, la santé publique, ainsi que l'alimentation, et l'eau. Par ailleurs, le CEPC a mis en place en 2020 un processus pour tirer les leçons de la pandémie. Il vise à aider les autorités nationales à améliorer leur niveau de préparation et de résilience.

44. Le CEPC supervise aussi les activités du centre euro-atlantique de coordination des réactions en cas de catastrophe (EADRCC). En cas de crise, l'EADRCC joue un rôle de partage des informations et de coordination des efforts et des capacités de secours parmi les États membres et les pays partenaires, ainsi que dans les pays où l'OTAN est engagée militairement. Il joue actuellement un rôle, bien que limité, dans la gestion des efforts d'assistance et de secours en réponse à la pandémie de Covid-19, notamment en coordonnant le transport et la fourniture d'équipements médicaux. Qui plus est, il conduit chaque année des exercices afin de renforcer la coordination et la préparation des autorités nationales.

45. Par ailleurs, le Programme pour la science au service de la paix et de la sécurité (SPS) favorise le dialogue et la coopération pratique entre les États membres et les pays partenaires dans le domaine de la résilience à travers des activités axées sur la recherche, l'innovation technologique, et l'échange de connaissances scientifiques.

46. L'OTAN mène aussi des exercices permettant d'opérationnaliser la coopération et l'interaction entre secteurs civil et militaire parmi les Alliés. Par exemple, l'exercice *Trident Juncture*, auquel 31 pays ont participé en 2018 en Norvège, a permis à ce pays d'exercer son approche de la résilience dans le cadre de son concept de « défense totale », d'évaluer l'état de préparation de la société et d'identifier les vulnérabilités restantes. Dans le cadre de cet exercice, le plus grand organisé par l'OTAN depuis la fin de la guerre froide, les forces armées norvégiennes ont coopéré étroitement avec la Direction de la protection civile. Son scénario faisait intervenir des sociétés privées de transport, des médias, des représentants politiques et économiques et des organisations non gouvernementales et internationales. En outre, il faisait appel à différentes capacités du secteur civil essentielles dans le renforcement de la résilience sociétale, comme la logistique, la cyberdéfense, la communication stratégique et la protection des civils. De même, l'exercice multinational *Defender-Europe 20*, dirigé par les États-Unis et mené entre janvier et mars 2020, a permis de tester la coopération civilo-militaire et la facilitation (c'est-à-dire la capacité « de mettre en place les arrangements et les infrastructures nécessaires aux mouvements d'unités, le plus rapidement possible et partout où il le faut »), deux éléments cruciaux de la résilience, dans le cadre d'un large déploiement de forces entre les deux rives de l'Atlantique et en Europe continentale (Thomas, Williams, & Dyakova, 2020).

47. Bien que ne faisant pas partie intégrante de l'OTAN, plusieurs centres d'excellence homologués par l'Alliance lui apportent leur expertise dans des domaines liés à la résilience et à la préparation du secteur civil. On citera en particulier les centres d'excellence pour la coopération

civilo-militaire, pour la communication stratégique, pour la cyberdéfense coopérative, pour la gestion de crise en cas de catastrophe et pour la défense contre le terrorisme.

48. En mai 2021, un centre euro-atlantique pour la résilience (E-ARC) a été inauguré en Roumanie. Le centre, qui n'est pas non plus une structure otanienne, constitue une institution internationale d'échange dans le domaine de la résilience. Son travail s'organise autour de trois piliers : l'atténuation des risques grâce à l'anticipation et l'adaptation, le développement d'outils analytiques et de bonnes pratiques, et la coopération en matière d'éducation, de formation et d'exercices conjoints. La portée de ses travaux est large, incluant notamment la résilience sociétale, la résilience dans le domaine des technologies émergentes, la résilience des systèmes de communication, la résilience face aux crises complexes, le maintien de la continuité du gouvernement et des services essentiels, la résilience des infrastructures de transport, et la résilience des États voisins de l'OTAN et de l'UE face aux tentatives de déstabilisation par des acteurs étatiques et non-étatiques. Le centre collaborera pleinement avec des représentants du secteur privé, des universités, des centres de recherche internationaux et de la société civile dans ses activités futures. Pour le moment, l'E-ARC fonctionne en tant qu'entité nationale placée sous l'égide du ministère roumain des affaires étrangères. À l'avenir, il a vocation à devenir un centre international, similaire structurellement au centre d'excellence européen pour la lutte contre les menaces hybrides, auquel se joindront des experts des États membres et partenaires de l'OTAN et de l'UE.

D. L'IMPORTANCE DE LA COOPÉRATION AVEC LES PAYS PARTENAIRES ET L'UNION EUROPÉENNE POUR RENFORCER LA RÉSILIENCE COMMUNE

49. Du fait de la digitalisation et de l'intégration sans cesse croissantes de nos sociétés, la vulnérabilité a perdu son sens géographique. Un évènement à l'extérieur des frontières de l'OTAN peut rapidement se transformer en crise sécuritaire pour l'Alliance tout entière, comme l'a démontré la propagation du coronavirus lors des premiers mois de 2020. Ainsi, coopérer étroitement avec ses partenaires dans le domaine de la résilience permet, d'une part, à l'Alliance de les soutenir et d'accroître la stabilité de son voisinage. D'autre part, cela est aussi un moyen pour l'OTAN de renforcer sa propre résilience en échangeant avec eux sur les meilleures pratiques qu'ils ont développées, y compris dans des domaines dans lesquels les Alliés peuvent encore progresser. Ce besoin a été mis en évidence par la pandémie de Covid-19, à laquelle un certain nombre de pays, notamment en Asie et en Océanie ont su répondre avec bien plus d'efficacité (The Economist, 2020).

50. L'OTAN a développé des relations approfondies avec certains pays partenaires dans le domaine de la résilience en amont des crises. Par exemple, en février 2019, elle a déployé une équipe d'experts en préparation du secteur civil en soutien à l'Ukraine. L'OTAN a également mis en place en 2019 un projet conjoint avec les Nations unies de trois ans pour aider la Jordanie à rehausser sa préparation face à la menace posée par les armes CBRN (UNOCT, 2019).

51. Elle coopère également étroitement avec la Suède et la Finlande sur les menaces hybrides, en organisant des consultations, des formations et des exercices conjoints (OTAN, 2019). Par ailleurs, elle contribue aussi activement à la réponse aux crises dans les pays partenaires. Durant la pandémie, elle apporte son soutien à de nombreux pays partenaires en distribuant des fournitures médicales et alimentaires. De même, en juin 2020, l'EADRCC a coordonné la réponse alliée face à de graves inondations ayant affecté l'Ukraine.

52. Le renforcement de la résilience est aussi un élément central des efforts de coopération et de coordination entre l'OTAN et l'UE. Les deux organisations ont adopté une déclaration conjointe et des propositions communes en 2016, qui font explicitement référence au renforcement de la résilience. Elles y affirment leur intention d'intensifier les contacts entre leurs personnels dans ce domaine, de renforcer la cohérence entre leurs plans et politiques respectifs et d'être prêtes à

déployer de manière coordonnée des experts pour assister leurs États membres à améliorer leur résilience, soit dans la phase précédant une crise soit en réponse à une crise. Ces dernières années, l'OTAN et l'UE ont traduit ces engagements en coopérations concrètes, notamment dans les domaines de la cybersécurité et de la défense, et dans la lutte contre les menaces hybrides.

53. Dans leur communiqué publié après le sommet de l'OTAN de juin 2021, les chefs d'États et de gouvernements alliés ont réaffirmé l'importance de la coopération avec les pays partenaires de l'Alliance et d'autres organisations internationales, dont l'UE, en matière de résilience.

V. ÉTUDES DE CAS DE QUATRE ÉTATS MEMBRES ET PAYS PARTENAIRES

A. ESTONIE : UN PAYS EN AVANCE DANS LA RÉSILIENCE AUX CYBERMENACES

54. Les États baltes sont confrontés à divers défis posés par la Russie, notamment des menaces hybrides, des cyberattaques, des campagnes de propagande et de désinformation, des pressions économiques, des opérations de renseignement, ainsi qu'une forte présence militaire près de leurs frontières. L'Estonie a fait l'amère expérience de l'impact potentiel de ces risques. À partir d'avril 2007, pendant plusieurs mois, le pays a été confronté à une cyberattaque d'un niveau sans précédent, lancée selon les autorités, depuis la Russie. Des attaques par déni de service ont affecté le fonctionnement des sites Internet des autorités du pays, des agences de presse, des fournisseurs de services Internet, des grandes banques, et de petites entreprises, entre autres. Ces attaques ont provoqué des perturbations graves pour la société estonienne qui ont eu un coût de plusieurs milliards d'euros (Tamkin, 2017). Elles ont fait évoluer le degré de réflexion sur la résilience et la préparation du secteur civil en Estonie.

55. De 1993 à 2010, le concept de sécurité nationale du pays était fondé sur les principes de défense totale et de défense territoriale. Néanmoins, en réponse à l'évolution de l'environnement sécuritaire, et notamment aux attaques de 2007, les autorités ont mis à jour le concept de sécurité nationale et la stratégie de défense nationale, respectivement en 2010 et 2011. Ces deux documents ont reconnu que les menaces auxquelles était confronté le pays, notamment dans le domaine cyber, n'appelaient plus nécessairement une réponse principalement militaire comme préconisé par les stratégies et concepts précédents. Au contraire, ils recommandaient désormais l'utilisation intégrée d'un large éventail de moyens militaires et non militaires.

56. En particulier, après les attaques de 2007, le pays a fait de la résilience de la société entière face aux cybermenaces une priorité. Comme précisé lors d'une visite virtuelle de l'AP-OTAN le 22 avril 2021, 99% des services publics dans le pays sont accessibles en ligne et l'Estonie est devenue en 2015 le premier pays à adopter le vote électronique (en 2019, lors des élections législatives, 43% des électeurs y ont recouru). Cela fait de l'Estonie une référence mondiale dans le domaine numérique. Néanmoins, cette digitalisation croissante expose aussi particulièrement le pays aux cyberattaques et accroît leur impact potentiel sur l'ensemble de la société estonienne. L'un des objectifs centraux de la stratégie estonienne de cybersécurité pour 2019-2022 est donc d'investir dans une « société numérique durable reposant sur une forte résilience technologique et une préparation aux situations d'urgence » (Ministère estonien des affaires économiques et des communications, 2019). Le pays a adopté une approche intersectorielle de la cybergouvernance et de la cyberdéfense, facilitée par un Conseil de cybersécurité placé sous l'autorité directe du gouvernement. Une Autorité des systèmes d'information et un cybercommandement ont été créés, respectivement au sein des ministères de l'économie et des forces armées. Enfin, l'Estonie accueille le centre d'excellence pour la cyberdéfense coopérative, accrédité par l'OTAN, et organise les exercices *Locked Shields* et *Crossed Swords* de l'OTAN (Kohler, 2020). Les efforts réalisés dans le domaine de la cyberrésilience font de l'Estonie un exemple pour les autres Alliés dans ce domaine.

57. Les actions illégales et illégitimes de la Russie depuis 2014 ont contribué à un nouvel examen de la politique estonienne de sécurité. En 2017, le concept de sécurité nationale a été à nouveau actualisé et se base désormais sur le concept de « défense intégrée et sécurité totale ». Il promeut une approche de la sécurité incluant l'ensemble de la société et comprend six piliers : la défense militaire, le soutien civil à la défense militaire, l'action internationale, la sécurité intérieure, le maintien du fonctionnement de l'État et de la société et la défense psychologique. Le modèle estonien donne un rôle important à chaque acteur de la société. La gestion des risques est fortement décentralisée mais rendue efficace par un niveau élevé de coordination entre les différents secteurs. Par ailleurs, l'Estonie bénéficie de l'expertise de la Ligue de défense, une organisation de défense nationale volontaire, organisée militairement et subordonnée au commandement des forces de défense. Ses 16 000 membres soutiennent les forces armées estoniennes dans diverses tâches. Ils forment aussi la population à la défense et à la résilience sur le plan national. La capacité de résilience et de coordination de l'ensemble des acteurs des secteurs civil et militaire est testée lors d'exercices annuels. L'exercice *Siil*, notamment, met à l'épreuve la capacité de coopération des forces armées avec la police, les gardes-frontières, le conseil de secours, et la Ligue de défense (Flanagan, Osburg, Binnendijk, Kepe, & Radin, 2019).

58. Dans le cadre de leurs efforts pour améliorer la résilience de la société estonienne aux cyberattaques, les autorités ont également développé des solutions technologiques innovatrices. Les citoyens et résidents estoniens obtiennent notamment une carte d'identité électronique leur permettant de prouver leur identité lorsqu'ils voyagent, de se connecter à leurs comptes bancaires, de signer des documents électroniquement, de voter en ligne, d'accéder à leurs dossiers médicaux, de déclarer et de payer leurs impôts, etc. L'Estonie a aussi développé une infrastructure numérique, nommée X-Road, permettant aux citoyens et aux services publics estoniens d'échanger des données de manière sûre. Son fonctionnement n'autorise le partage de chaque catégorie d'informations qu'avec une agence déterminée. Ainsi, si un serveur était piraté, seule une seule catégorie de données serait compromise. Cette compartimentation rend le système plus résilient face aux cybermenaces. Le réseau X-Road met aussi l'accent sur la transparence en indiquant aux citoyens quelles agences publiques ont accédé à leurs données et pour quelle raison. Enfin, afin d'assurer la continuité de ces services publics digitaux en cas de choc majeur affectant le pays, l'Estonie a établi en 2017 une ambassade numérique au Luxembourg faisant office de serveur de sauvegarde en dehors des frontières nationales. Une copie des données les plus critiques et confidentielles des citoyens et résidents y est conservée. Elle complète les serveurs de sauvegarde de données situés sur le territoire estonien. Ces solutions permettent de renforcer la sécurité et l'efficacité des services publics tout en augmentant la confiance de la population dans la bonne gestion de leurs données (Visite virtuelle de l'AP-OTAN en Estonie, 2021).

B. FINLANDE : UN MODÈLE D'APPROCHE PANSOCIÉTALE DE LA SÉCURITÉ

59. En tant que pays non aligné ayant une longue frontière terrestre avec l'Union soviétique, face à qui elle a dû se battre en 1939-1940 pour conserver son indépendance, la Finlande a adopté une doctrine de défense totale largement fondée sur la préparation du secteur civil et la dissuasion par la résilience lors de la guerre froide (Wither, 2020). Après la fin de cette dernière, contrairement à certains de ses voisins, la Finlande est restée fidèle au concept de mobilisation de l'ensemble de la société dans le cadre d'efforts de défense totale. La dernière « Stratégie de sécurité pour la société », adoptée en 2017, a ainsi pour objectif d'assurer le maintien des fonctions vitales de la société en cas de crise et donne des directives claires à chaque secteur de la société sur son rôle dans la préparation et la réponse aux risques. Sa mise en œuvre est appuyée par des stratégies spécifiques pour certaines branches administratives, et des stratégies intersectorielles et thématiques, telles que la stratégie de cybersécurité.

60. La stratégie de sécurité pour la société « est basée sur le principe de la sécurité globale dans laquelle les fonctions vitales de la société sont conjointement garanties par les autorités, les opérateurs commerciaux, les organisations et les citoyens » (Comité de sécurité de Finlande, 2017). Bien entendu, les forces armées sont au cœur du concept de sécurité globale, notamment grâce au service national obligatoire. Néanmoins, l'ensemble de la société est impliqué dans la sécurité du pays (Salonius-Pasternak, 2018). La préparation, l'opérationnalisation et la mise en place de cette sécurité globale sont gérés par le Comité de sécurité qui coordonne les activités des ministères et assiste le gouvernement dans ce domaine. Il est composé d'une vingtaine de hauts fonctionnaires et d'experts des autorités nationales ainsi que, fait intéressant, du secteur privé.

61. La stratégie met particulièrement l'accent sur la « résilience psychologique », qu'elle définit comme « la capacité des individus, de la société et de la nation à résister aux pressions résultant de situations de crise et à se remettre de leurs impacts ». En cas de crise, la résilience psychologique est considérée comme un facteur critique pour maintenir la volonté du peuple finlandais de défendre son pays (Comité de sécurité de Finlande, 2017). Son rôle est crucial pour déjouer les campagnes de propagande et de désinformation qui sont, selon une évaluation menée en 2018 par les autorités finlandaises, l'un des principaux facteurs de risques pour la résilience du pays, avec les attaques terroristes et les perturbations causées par le changement climatique.

62. Cette même évaluation identifiait d'autres risques pouvant affecter la stabilité de la société comme une grave perturbation économique, une attaque militaire ou encore l'immigration à grande échelle (Ministère de l'intérieur de la Finlande, 2018). Pour faire face à ces risques divers d'origine anthropique ou naturelle mettant au défi la résilience de sa société, la Finlande a développé une stratégie de coopération à l'échelle internationale. En particulier, elle coopère avec l'OTAN et l'UE et accueille notamment le centre européen d'excellence pour la lutte contre les menaces hybrides, affilié aux deux organisations. À l'échelle nationale, elle a acquis une expertise importante dans la planification, les exercices et le développement de ressources. Le pays stocke notamment de la nourriture, du carburant, du fourrage et des équipements pour la défense civile et, selon les chiffres officiels, compte 45 000 abris de défense civile pouvant accueillir jusqu'à 3,6 millions de ses citoyens.

C. SUÈDE : RETOUR VERS LA DÉFENSE TOTALE

63. Contrairement à la Finlande, la Suède a abandonné son approche globale de la sécurité après la guerre froide. Jusqu'au milieu des années 1980, la Suède s'appuyait sur d'importantes forces armées et sur un vaste plan de stockage de produits essentiels. Au cours des années 2000, face à l'évolution des menaces auxquelles était confronté le pays, le budget de défense a été fortement réduit, les infrastructures nécessaires pour soutenir la défense nationale ont été en grande partie privatisées ou démantelées, le système de préparation aux crises a été largement décentralisé et les stocks d'urgence vendus ou détruits (Wither, 2020; Salonius-Pasternak, 2018). La conscription obligatoire a aussi été abandonnée en 2010.

64. La résurgence de la menace russe à partir de 2014 a entrainé un regain d'intérêt pour les politiques de résilience par la préparation civile et pour une approche pansociétale de la sécurité. La Suède a lancé un important effort de réforme et de reconstruction de ses systèmes de défense, de protection civile et de préparation aux crises. En 2015, un projet de loi sur la défense nationale a ré-adopté le concept de « défense totale ». Sa mise en place et son opérationnalisation dépendent d'une commission de la défense créée à cette occasion (von Sydow, 2018). En 2017, la Suède a réintroduit la conscription obligatoire et a organisé son plus grand exercice de défense nationale depuis des décennies, Aurora-17. Des membres des forces armées suédoises et étrangères, mais aussi de la garde nationale, de la police et des services sociaux y ont pris part.

65. Cette même année, la commission de la défense a publié un rapport intitulé « La résilience - le concept de défense totale et le développement de la défense civile 2021-2025 ». Le rapport identifie les attaques militaires ou hybrides, notamment cyber, comme les principaux risques auxquels le pays est confronté. Il affirme que face à ces menaces, « le Parlement, le gouvernement, les autorités publiques, les municipalités, les entreprises privées, les organisations de défense volontaires ainsi que la population font tous partie de la défense totale ». Il déclare que le développement d'une stratégie de défense totale doit permettre de doter les acteurs du secteur civil « d'une capacité à résister à des perturbations graves dans le fonctionnement de la société suédoise pendant trois mois ». Concernant la population, il ajoute que « chaque individu doit se tenir prêt à se charger de ses provisions de base et de ses soins pendant une semaine sans soutien public » (Commission de défense, 2017). En décembre 2020, le parlement suédois a adopté une nouvelle loi sur la défense totale qui maintient pour les années à venir la priorité accordée au renforcement des capacités de défense et à l'approfondissement de la coopération internationale, notamment avec la Finlande.

66. La coordination entre les secteurs et les niveaux de gouvernement de la prévention, de la préparation et de la réponse aux situations d'urgence en temps de paix est la responsabilité de l'agence des urgences civiles (MSB). Celle-ci propose aux acteurs privés, aux autorités publiques et aux particuliers des formations et des exercices sur la résilience par la préparation du secteur civil. En 2018, elle a aussi distribué à chaque ménage une brochure d'information expliquant le concept de défense totale ainsi que le rôle de chaque acteur dans le renforcement de la résilience, et notamment celui de chaque individu dans la préparation à diverses situations d'urgence.

67. La conception suédoise de la sécurité accorde une place centrale au respect des valeurs démocratiques et à la protection des droits fondamentaux et de l'État de droit. Or, comme dans d'autres démocraties, des acteurs malveillants internes et externes tentent de déstabiliser les institutions suédoises et de remettre en cause les principes libéraux sur lesquels elles fondent leurs actions, notamment en diffusant de la désinformation au sein de la population. Face à cette menace, l'agence a accru ses efforts dans le domaine de l'analyse de la désinformation et de la réponse à cette dernière. Comme mentionné par deux représentants de l'agence lors de la réunion de notre commission à la session de printemps virtuelle de l'AP-OTAN en Suède, la MSB a, par exemple, depuis 2017, formé 18 000 fonctionnaires à identifier et à contrer les campagnes de désinformation. Néanmoins, la lutte contre la désinformation et le renforcement de la résilience psychologique devraient en grande partie devenir la responsabilité d'une nouvelle agence à l'avenir. En effet, le concept de défense totale repose fortement sur la volonté de la population de défendre son pays en temps de guerre, et sur son engagement dans les efforts de développement de la résilience en temps de paix. Reconnaissant cette corrélation, le gouvernement suédois a annoncé en 2018 la création d'une Autorité de défense psychologique d'ici à 2022.

68. Afin de mieux opérationnaliser les politiques de résilience et de préparation des secteurs militaire et civil aux crises, la Suède mène régulièrement des exercices. En particulier, un exercice nommé « Défense totale 2020 » a débuté en 2019 et se termine en 2021. Dirigé par les forces armées et la MSB, l'exercice rassemble plus de 60 agences gouvernementales ainsi que des autorités locales, des organisations bénévoles et d'autres acteurs du secteur civil. Il se concentre sur le maintien des services vitaux pour la société en cas de crise ou de guerre, le fonctionnement et l'interaction des chaînes de commandement militaire et civile, l'analyse et la compréhension de la situation par les acteurs civils et leur coopération entre eux et avec le secteur militaire, ainsi que la coordination de la communication adressée à la population.

69. Les partenariats jouent aussi un rôle important dans les politiques suédoises de défense totale et de renforcement de la résilience. La Suède coopère ainsi étroitement avec ses voisins nordiques, et particulièrement la Finlande. Une loi a d'ailleurs été adoptée en octobre 2020 par le parlement suédois afin de renforcer le soutien militaire opérationnel entre les deux pays. Le Danemark, la Finlande, l'Islande, la Norvège et la Suède coopèrent également dans le contexte de

« la coopération Haga » établie en 2009 et ayant pour objectif de renforcer la protection et la préparation civiles.

70. L'exemple suédois montre bien que construire ou reconstruire un système de défense totale, et notamment une capacité de résilience par la préparation civile, nécessite un engagement politique et citoyen fort, des moyens importants et du temps, ainsi que le développement de partenariats tangibles.

D. JAPON : UN EXEMPLE DANS LE DOMAINE DE LA RÉSILIENCE FACE AUX CATASTROPHES NATURELLES

71. Le Japon est un exemple à l'échelle mondiale dans le domaine de la résilience face aux catastrophes naturelles. En effet, étant régulièrement frappée par des séismes, tsunamis et autres inondations, la société japonaise a dû apprendre à vivre avec ce type de risques. En particulier, le 11 mars 2011, un séisme au large de la côte pacifique du Tōhoku a déclenché un tsunami qui a, à son tour, provoqué un accident à la centrale nucléaire de Fukushima Daiichi. Cette catastrophe naturelle a causé la mort de près de 20 000 personnes, en a blessé environ 6 000 et a nécessité l'évacuation et le déplacement d'environ 470 000 habitants (Agence japonaise de reconstruction, 2021). Les dégâts économiques qu'elle a engendrés ont été estimés à environ 210 milliards de dollars (OCDE, 2019). Au regard de ces chiffres et face à la forte probabilité (estimée de 70 à 80%) d'un séisme majeur à venir dans les trois prochaines décennies (OCDE, 2019), le renforcement de la résilience nationale face aux catastrophes naturelles est une priorité pour le Japon.

72. À la suite de cette catastrophe, le pays a encore développé sa capacité et ses connaissances, pourtant déjà très avancées, dans les domaines de l'anticipation du risque et de la résilience par la préparation du secteur civil. Le pays a tiré des leçons cruciales de la catastrophe de 2011 et de ses conséquences. Ces leçons ont été incorporées dans une loi sur la résilience nationale en 2013, dont découle un plan fondamental (adopté en 2014 et actualisé en 2018), ainsi qu'un plan d'action (Bureau japonais de la promotion de la résilience nationale, 2015). Le plan fondamental se décline autour de quatre axes principaux : 1) prévenir les pertes humaines par tous les moyens ; 2) éviter la défaillance de l'administration ainsi que des systèmes sociaux et économiques ; 3) atténuer les dommages engendrés aux biens et aux installations ; et 4) permettre une reconstruction rapide après une catastrophe naturelle.

73. Par ailleurs, l'approche japonaise en matière de résilience se fonde sur plusieurs principes directeurs. Premièrement, elle repose sur le principe de subsidiarité. L'ensemble des autorités locales doivent élaborer leur propre plan fondamental pour la résilience dans le cadre de leurs juridictions respectives (OCDE, 2019). L'anticipation des crises et leur gestion est ainsi largement déléguée aux autorités locales. Le Bureau du Cabinet assure néanmoins la supervision et la coordination de ces efforts. En cas d'effondrement des structures de décision et des chaînes de communication locale, comme ce fut le cas dans certaines municipalités affectées en 2011, le gouvernement a d'ailleurs la possibilité de reprendre rapidement le contrôle sur la gestion de la réponse.

74. Deuxièmement, la stratégie japonaise dans ce domaine est basée sur l'étroite coopération entre les autorités et le secteur privé. Ce dernier est en effet incité à contribuer à la préparation et à la résilience de la population en proposant des programmes éducatifs et de formation sur les gestes à adopter face aux catastrophes naturelles. En outre, l'utilisation des compétences et des équipements privés en cas de crise est explicitement encouragée par le plan fondamental pour la résilience nationale.

75. Troisièmement, la politique japonaise de résilience s'appuie sur une forte coopération entre le secteur civil et les forces japonaises d'autodéfense. En amont des crises, les forces armées sont consultées dans le développement des plans fondamentaux et améliorent leur coordination avec les

autorités locales dans le cadre d'exercices réguliers. En cas de crise majeure, les forces armées sont ainsi en mesure de réagir rapidement et efficacement en appui des autorités nationales et locales. Afin d'assurer une communication efficace entre ces différents éléments, des officiers retraités des forces armées travaillent au sein des administrations préfectorales et municipales à travers le pays (Wambach, 2012).

76. Enfin, la forte capacité de résilience du Japon face aux catastrophes naturelles est le résultat d'efforts en matière de renforcement de la préparation de la population à ces dernières. Des exercices de préparation aux tremblements de terre et à d'autres catastrophes naturelles sont régulièrement organisés dans l'ensemble des écoles du pays. Les connaissances et capacités acquises à travers ces formations sur les gestes à adopter en cas d'urgence ont notamment permis de sauver de nombreuses vies lors de la catastrophe de 2011 (Wambach, 2012).

VI. CONCLUSIONS ET RECOMMANDATIONS

77. L'environnement sécuritaire contemporain se caractérise par une multiplication des menaces militaires et non-militaires ayant un impact sur l'ensemble de nos sociétés. Elles affectent notamment le secteur civil et en tout premier lieu la population. Il est donc nécessaire pour l'Alliance d'adopter une approche pansociétale de la résilience dans laquelle l'ensemble des acteurs civils et militaires fonctionnent en complémentarité et sont en mesure de répondre efficacement à toute crise, quelle qu'en soit la nature. Après une perte d'intérêt pour les politiques relatives à la résilience et à la préparation du secteur civil à l'issue de la guerre froide, l'OTAN et les pays alliés ont fait des efforts substantiels dans ces domaines au cours des deux dernières décennies. La pandémie de Covid-19 a, à nouveau, souligné l'importance de renforcer la capacité des sociétés alliées à faire face à tout type de crise. Lors du sommet de l'OTAN en juin 2021, les représentants des États membres ont donné une nouvelle impulsion aux efforts alliés en ce sens. Beaucoup reste néanmoins à faire afin de renforcer la capacité de l'Alliance et de nos sociétés à faire face aux risques actuels et futurs. Pour ce faire, il conviendrait de :

1. ***Se donner les moyens de nos ambitions :*** Développer la résilience requiert des investissements. Les pays membres et l'OTAN, à leur niveau respectif, doivent donc veiller à renforcer leur expertise, à développer leurs structures et à mettre à disposition des ressources financières et humaines suffisantes, en plus des moyens nécessaires à la tenue de l'engagement de consacrer 2% du PIB aux dépenses de défense, pour atteindre les objectifs que se sont fixés les Alliés eu égard au renforcement de la résilience de nos sociétés.

2. ***Identifier les vulnérabilités et évaluer les capacités :*** Les États membres doivent procéder régulièrement, individuellement et collectivement, à des évaluations critiques de leurs vulnérabilités et de leurs capacités. Pour rendre ce processus plus aisé, l'OTAN doit réviser et développer des exigences de base pour la résilience nationale plus facilement mesurables. Lors du sommet de juin 2021, les dirigeants alliés ont avancé dans cette direction en annonçant l'élaboration à venir d'une proposition visant à établir, évaluer et réviser ces exigences et à développer le suivi régulier de leur mise en application. Ces évolutions devraient permettre aux Alliés de mieux quantifier leur progrès et de pouvoir se comparer.

3. ***Faciliter l'échange de bonnes pratiques*** : Il est crucial, tout en respectant les spécificités et la responsabilité nationales, de mieux disséminer les leçons apprises et l'expertise développée par certains États membres et pays partenaires dans des domaines précis : par exemple, l'Estonie concernant les cybermenaces, la Finlande sur la mise en place d'une approche pansociétale de la résilience, la Suède au sujet des avantages et des défis de la défense totale, et le Japon dans l'anticipation et la réponse aux catastrophes naturelles. Un échange plus approfondi entre Alliés et partenaires permettrait de répliquer ces pratiques dans d'autres pays alliés et partenaires. Le rôle de coordination et d'échange du centre euro-atlantique de

coordination des réactions en cas de catastrophe concernant les efforts nationaux de préparation et de réponse aux crises mériterait, à cet égard, d'être renforcé.

4. ***Adopter une approche plus globale et intégrée de la planification et de la gestion des crises*** *:* Face à un éventail de risques qui tend à croître et qui appelle des réponses militaires et non-militaires, il apparaît nécessaire de renforcer la coopération en amont des crises entre les forces armées, d'une part, et les autorités nationales et locales, le secteur privé et la population, d'autre part. Cette coopération doit notamment s'exprimer dans la mise en place de systèmes d'alerte précoce et le développement de plans d'urgence afin de garantir une réponse rapide et efficace en cas de crise.

5. ***Tester nos capacités pour mieux les renforcer :*** Il est nécessaire d'organiser plus d'exercices, à la fois à l'échelle nationale mais aussi à celle de l'OTAN, pour exercer, opérationnaliser et améliorer les plans d'urgence en amont des crises. Ils doivent :

   a. Inclure tous les secteurs de la société et tenir compte de leur interdépendance croissante ainsi que de l'impact négatif et du risque de réaction en chaîne que peut engendrer la défaillance d'un acteur vis-à-vis des autres.
   b. Se baser sur des scénarios prenant en compte des menaces traditionnelles comme un conflit armé, ainsi que des risques non-militaires comme les catastrophes naturelles ou une pandémie, et des menaces hybrides (désinformation, cyberattaques, etc.).
   c. Tester nos systèmes jusqu'au point de rupture pour permettre aux différents acteurs des secteurs civil et militaire d'identifier et de réduire leurs vulnérabilités.

6. ***Améliorer la communication et la sensibilisation du secteur civil et des populations sur l'importance et les bénéfices de la résilience afin de créer un état d'esprit de résilience :*** Accroître la résilience des sociétés alliées requiert la participation et la coopération de tous les acteurs des secteurs civil et militaire aux efforts en ce sens. Il est donc nécessaire que les États membres et l'OTAN élaborent activement une politique de sensibilisation commune à l'adresse des citoyens et des acteurs des secteurs civil et militaire sur la nécessité et les bénéfices de la résilience. De même, les Alliés doivent promouvoir l'enseignement de la résilience dans leurs systèmes éducatif et universitaire.

7. ***Développer les efforts de planification au sein du secteur privé :*** La pandémie de Covid-19 a montré à quel point il est crucial, pour le secteur privé en coopération avec les forces armées et les autorités, de mieux anticiper les crises et de s'y préparer en mettant en place des stratégies visant à :

   a. Garantir le développement de plans alternatifs pouvant être activés aux fins de maintenir des services essentiels à la population ou aux forces armées dans le cadre de leur réponse en cas de crise ;
   b. Limiter les interconnexions non nécessaires entre infrastructures essentielles et dans les chaînes d'approvisionnement, et s'assurer que celles qui sont nécessaires soient identifiées à l'avance et remplaçables afin de minimiser les risques de défaillances en cascade en cas de crise.

8. ***Instaurer et renforcer des mécanismes d'évaluation des investissements étrangers :*** De tels outils sont nécessaires pour s'assurer que les infrastructures essentielles puissent être mises au service de la sécurité et de la défense nationales des pays alliés, et de leurs forces armées, en cas de crise.

9. ***Renforcer la résilience démocratique de nos sociétés :*** La pandémie de Covid-19 a été instrumentalisée par des acteurs malveillants internes et externes cherchant à remettre en cause les valeurs et principes fondamentaux de nos démocraties. Afin d'assurer la capacité

de nos sociétés à mieux se défendre contre de telles attaques en période de paix, de crise ou de conflit, il est nécessaire d'intégrer la protection des principes et institutions démocratiques au sein de l'Alliance parmi les exigences de base en matière de résilience. Le lien intrinsèque entre la défense des valeurs démocratiques et le renforcement de la résilience des pays alliés est d'ailleurs explicitement reconnu dans l'*Engagement renforcé en faveur d'une meilleure résilience* adopté par les dirigeants des pays de l'OTAN lors du sommet de juin 2021. Les Alliés doivent, par ailleurs, traduire de manière concrète l'engagement en faveur de ces valeurs qui ont été réaffirmées lors du sommet et forment le socle de nos sociétés. Pour ce faire, comme suggéré par le président de l'Assemblée parlementaire de l'OTAN, Gerald E. Connolly, il conviendrait de créer un centre pour la résilience démocratique ayant pour rôle, au sein de l'OTAN, de soutenir les pays alliés dans le renforcement de leurs système et institutions démocratiques. Ce centre mènerait des recherches et fournirait des conseils et une assistance aux États membres dans les domaines, entre autres, de l'intégrité et la sécurité des élections, l'indépendance judiciaire, la liberté de la presse et la lutte contre la désinformation (Connolly, 2019; Groupe d'experts de l'OTAN, 2020). Les Alliés doivent aussi continuer d'apporter leur soutien au développement du centre euro-atlantique pour la résilience, inauguré en mai 2021 en Roumanie. La suggestion de créer un centre pour la résilience démocratique au sein de l'OTAN et le développement du E-ARC sont, en effet, complémentaires et ne doivent pas être opposés. Le premier doit se focaliser sur l'opérationnalisation en interne de l'assistance en réponse aux menaces dirigées contre les valeurs démocratiques, tandis que le second joue un rôle d'analyse, d'échange, de formation et de coopération (y compris avec des partenaires extérieurs à l'organisation, notamment les pays voisins et l'UE).

10. ***Accroître la participation des femmes et mieux intégrer la dimension du genre dans les politiques de la résilience :*** Comme la réponse à la pandémie l'a de nouveau démontré, les femmes jouent un rôle crucial dans la résilience de nos sociétés. Il est donc essentiel d'accroître leur participation dans les instances politiques et institutions sécuritaires chargées de l'anticipation des crises, ainsi que de la préparation et de la réponse à ces dernières. Par ailleurs, la dimension du genre doit être mieux intégrée dans l'ensemble des phases de la gestion de crise. Il est nécessaire que les besoins et apports spécifiques des femmes soient pris en compte dès la préparation en amont d'une crise, dans la réponse apportée à celle-ci, mais aussi dans le travail de réhabilitation et de reconstruction qui la suit.

11. ***Approfondir la coopération entre l'OTAN et l'UE :*** Un renforcement de cette coopération doit permettre aux deux organisations de mieux identifier les menaces et les vulnérabilités communes et partager leurs meilleures pratiques. Par ailleurs, l'OTAN et l'UE doivent renforcer leurs efforts pour distinguer les domaines dans lesquels leur travail de développement de la résilience se chevauchent et ceux dans lesquels une coopération plus poussée pourrait apporter une valeur ajoutée. Cela devrait permettre d'utiliser de manière plus efficace et cohérente les compétences et les capacités des deux organisations.

12. ***Développer les partenariats existants et en créer de nouveaux*** : Les Alliés doivent accroître leurs liens avec leurs partenaires ayant acquis des connaissances et des capacités dans la résilience face à divers types de crises potentielles. Il serait souhaitable aussi de renforcer les relations avec des pays avec lesquels aucun partenariat n'a encore été formalisé mais dont les Alliés ont beaucoup à apprendre comme certains pays d'Asie et d'Océanie qui ont fait montre d'une exceptionnelle capacité de résilience durant la crise de la Covid-19.

13. ***Tirer les leçons de la pandémie de Covid-19 et se préparer aux futures crises dues au changement climatique :*** Le processus mis en place au sein du CEPC afin de tirer les leçons de la pandémie dans le domaine de la préparation du secteur civil et de la résilience doit permettre de recueillir les meilleures pratiques mises en place à l'échelle nationale et de faciliter leur diffusion aux autres États membres et partenaires. Ce processus mériterait d'être

maintenu, institutionnalisé, et élargi au-delà de la pandémie. Il pourrait ainsi servir de forum d'échange d'idées et de meilleures pratiques concernant la planification et la gestion par l'OTAN des menaces non-militaires, telles que les pandémies mais aussi le changement climatique. Cela permettra de répondre plus efficacement et de manière plus coordonnée aux futures crises. Par ailleurs, les Alliés doivent soutenir l'élaboration à venir d'un traité international sur la prévention des pandémies et la préparation à celles-ci dans le cadre de l'OMS. Un tel traité permettrait en effet d'accroitre la coopération dans le domaine de la préparation et la réaction aux urgences sanitaires, et ainsi de renforcer la sécurité sanitaire mondiale.

14. ***Continuer à placer la résilience au cœur de la réflexion sur le futur de l'Alliance :*** Le renforcement de la résilience des sociétés alliées a été l'un des thèmes les plus amplement abordés par les chefs d'État et de gouvernement lors du sommet de l'OTAN en juin 2021. Il est aussi un élément central de l'agenda OTAN 2030 proposé par le secrétaire général de l'OTAN et approuvé par les dirigeants nationaux à cette occasion. Il est crucial que ce sujet continue d'occuper une place majeure dans les discussions, au sein de l'OTAN et de l'Assemblée parlementaire de l'OTAN, sur la révision du concept stratégique et sur l'avenir de l'Alliance en vue du prochain sommet des chefs d'État et de gouvernement en 2022.

BIBLIOGRAPHIE

Abi-Habib, M. (2018, December 18). *China's 'Belt and Road' Plan in Pakistan Takes a Military Turn*. Retrieved from The New York Times: https://www.nytimes.com/2018/12/19/world/asia/pakistan-china-belt-road-military.html

Agence japonaise de reconstruction. (2021). *reconstruction.go.jp*. Retrieved 29 janvier, 2021, from www.reconstruction.go.jp/english/topics/GEJE/

Albert, E. (2018, February 9). *China's Big Bet on Soft Power*. Retrieved from Council on Foreign Relations: https://www.cfr.org/backgrounder/chinas-big-bet-soft-power

Albert, E. (2019, June 25). *The China–North Korea Relationship*. Retrieved from Council on Foreign Relations: https://www.cfr.org/backgrounder/china-north-korea-relationship

Allen, G. C. (2019, February 6). *Understanding China's AI Strategy*. Retrieved from CNAS: https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy

Apuzzo, M. (2020, April 30). *Top E.U. Diplomat Says Disinformation Report Was Not Watered Down for China*. Retrieved from The New York Times: https://www.nytimes.com/2020/04/30/world/europe/coronavirus-china-eu-disinformation.html

Auerswald, D. (2019, May 24). *China's Multifaceted Arctic Strategy*. Retrieved from War on the Rocks: https://warontherocks.com/2019/05/chinas-multifaceted-arctic-strategy/

Austin, G. (2020, January 20). *Can there be any winners in the US–China 'tech war'?* Retrieved from IISS: https://www.iiss.org/blogs/analysis/2020/01/csfc-any-winners-in-the-us-china-tech-war

BBC. (2017). *bbc.com*. Retrieved 29 janvier, 2021, from www.bbc.com/news/technology-41753022

Belkin, P. (2020, April 1). *NATO: Key Issues Following the 2019 Leaders' Meeting*. Retrieved from Congressional Research Service: https://crsreports.congress.gov/product/pdf/R/R46066

Bennhold, K., & Ewing, J. (2020, January 16). *In Huawei Battle, China Threatens Germany 'Where It Hurts': Automakers*. Retrieved from The New York Times: https://www.nytimes.com/2020/01/16/world/europe/huawei-germany-china-5g-automakers.html

Bradsher, K. (2020). *nytimes.com*. Retrieved 29 janvier, 2021, from www.nytimes.com/2020/07/05/business/china-medical-supplies.html.

Brautigam, D. (2020). A critical look at Chinese 'debt-trap diplomacy': the rise of a meme. *Area Development and Policy*, 1-14.

Brennan, D. (2019, December 17). *Will China Be NATO's Next Challenge? Alliance Eyes Beijing's Rise While Mired in Infighting*. Retrieved from Newsweek: https://www.newsweek.com/china-nato-next-challenge-alliance-eyes-beijing-rise-battling-infighting-1477669

Bugajski, J. (2019, April 30). *China's Eurasian Ambitions*. Retrieved from CEPA: https://www.cepa.org/chinas-eurasian-ambitions

Bureau japonais de la promotion de la résilience nationale. (2015). *cas.go.jp*. Retrieved 29 janvier, 2021, from www.cas.go.jp/jp/seisaku/kokudo_kyoujinka/en/e01_panf.pdf

BusinessEurope. (2020, January). *The EU and China: Addressing the Systemic Challenge*. Retrieved from BusinessEurope: https://www.businesseurope.eu/sites/buseur/files/media/reports_and_studies/the_eu_and_china_full_february_2020_version_for_screen.pdf

Carlson, B. (2018, November). *Vostok-2018: Another Sign of Strengthening Russia-China Ties*. Retrieved from SWP: https://www.swp-berlin.org/en/publication/vostok-2018-another-sign-of-strengthening-russia-china-ties/

Cartier, E., Richard, B., & Toulemonde, G. (2020). Retrieved from Fondation Robert Schuman: https://www.robert-schuman.eu/en/doc/ouvrages/FRS_Parliament.pdf

Chad, B. P. (2020, January 21). *Unappreciated hazards of the US-China phase one deal*. Retrieved from Peterson Institute for International Economics: https://www.piie.com/blogs/trade-and-investment-policy-watch/unappreciated-hazards-us-china-phase-one-deal

Chun, Z. (2020, January 10). *China's "Arctic Silk Road"*. Retrieved from Maritime Executive: https://www.maritime-executive.com/editorials/china-s-arctic-silk-road

Comité de sécurité de Finlande. (2017). *turvallisuuskomitea.fi*. Retrieved 29 janvier, 2021, from turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf

Commission de défense. (2017). *The total defence concept and the development of civil defence 2021-2025* . Retrieved from https://www.government.se/4afeb9/globalassets/government/dokument/forsvarsdepartementet/resilience---report-summary---20171220ny.pdf

Connolly, G. (2019). *nato-pa.int*. Retrieved 29 janvier, 2021, from www.nato-pa.int/download-file?filename=%2Fsites%2Fdefault%2Ffiles%2F2019-11%2FRAPPORT%20146%20PCTR%2019%20F%20rev.%201%20fin%20-%2070%20ANS%20DE%20L%27OTAN%20-%20POURQUOI%20L%E2%80%99ALLIANCE%20DEMEURE%20T%20ELLE%20INDISPENSABLE.pdf

Cook, S. (2020). *Beijing's Global Megaphone: The Expansion of Chinese Communist Party Media Influence since 2017*. Retrieved from Freedom House: https://freedomhouse.org/report/special-reports/beijings-global-megaphone-china-communist-party-media-influence-abroad

Creemers, R., Webster, G., Triolo, P., Tai, K., Laskai, L., & Coplin, A. (2018, May 31). *Lexicon: Wǎngluò Qiángguó*. Retrieved from New America: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/lexicon-wangluo-qiangguo/

Cronin, P. M., & Neuhard, R. (2020, January 8). *Total Competition: China's Challenge in the South China Sea*. Retrieved from CNAS: https://www.cnas.org/publications/reports/total-competition

CRS. (2013, March 20). *Understanding China's Political System*. Retrieved from Congressional Research Service: https://crsreports.congress.gov/product/pdf/R/R41007

CRS. (2019, June` 25). *China's Economic Rise: History, Trends, Challenges, and Implications for the United States*. Retrieved from Congressional Research Service: https://crsreports.congress.gov/product/pdf/RL/RL33534

CSIS. (2019, October 10). *How much trade transits the South China Sea?* Retrieved from ChinaPower CSIS: https://chinapower.csis.org/much-trade-transits-south-china-sea/

CSIS. (2019, October 18). *How will the Belt and Road Initiative advance China's interests?* Retrieved from ChinaPower CSIS: https://chinapower.csis.org/china-belt-and-road-initiative/

CSIS. (2020, January 27). *Does China dominate global investment?* Retrieved from ChinaPower CSIS: https://chinapower.csis.org/china-foreign-direct-investment/

CSIS. (2020). *What does China really spend on its military?* Retrieved from China Power CSIS: https://chinapower.csis.org/military-spending/

De Maio, G. (2020). *brookings.edu*. Retrieved 29 janvier, 2021, from www.brookings.edu/research/natos-response-to-covid-19-lessons-for-resilience-and-readiness/

DIA. (2019). *China Military Power*. Retrieved from Defense Intelligence Agency: 2019 DIA China Military Power Modernizing a Force to Fight and Win

DoD. (2012, May 2). *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*. Retrieved from DoD: https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf

Elmer, K. (2019, September 18). *China, Russia set to double trade to US$200 billion by 2024 with help of soybeans*. Retrieved from South China Morning Post: https://www.scmp.com/news/china/diplomacy/article/3027932/china-russia-set-double-trade-us200-billion-2024-help-soybeans

European Commission. (2020, January 29). *Secure 5G networks: Questions and Answers on the EU toolbox*. Retrieved from European Commission: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127

European Commission. (2020). *Trade: Policy: Countries and regions: China*. Retrieved from European Commission: https://ec.europa.eu/trade/policy/countries-and-regions/countries/china/

European Parliament. (2020, May). *A New EU International Procurement Instrument (IPI)*. Retrieved from European Parliament: https://www.europarl.europa.eu/legislative-

train/api/stages/report/current/theme/international-trade-inta/file/international-procurement-instrument-(ipi)

FBI. (2020, May 13). *People's Republic of China (PRC) Targeting of COVID-19 Research Organizations*. Retrieved from FBI: https://www.fbi.gov/news/pressrel/press-releases/peoples-republic-of-china-prc-targeting-of-covid-19-research-organizations

Flanagan, S. J., Osburg, J., Binnendijk, A., Kepe, M., & Radin, A. (2019). *rand.org*. Retrieved 29 janvier, 2021, from www.rand.org/pubs/research_reports/RR2779.html.

French, H. W. (2017). *Everything Under the Heavens.* Knopf.

Gady, F.-S. (2019, April 29). *China, Russia Kick Off Bilateral Naval Exercise 'Joint Sea'*. Retrieved from The Diplomat: https://thediplomat.com/2019/04/china-russia-kick-off-bilateral-naval-exercise-joint-sea/

Gjørv, G. H. (2020). *nato.int*. Retrieved 29 janvier, 2021, from www.nato.int/docu/review/articles/2020/05/20/coronavirus-invisible-threats-and-preparing-for-resilience/index.html

Godement, F. (2020, March 23). *Fighting the Coronavirus Pandemic: China's Influence at the World Health Organization*. Retrieved from Institut Montaigne: 2020 https://www.institutmontaigne.org/en/blog/fighting-coronavirus-pandemic-chinas-influence-world-health-organization

Goldstein, L. J. (2020, January 25). *The Fate of the China-Russia Alliance*. Retrieved from The National Interest: https://nationalinterest.org/feature/fate-china-russia-alliance-117231

Grand, C., & Gillis, M. (2020). Alliance capabilities at 70: achieving agility for an uncertain future. In T. (. Tardy, *NATO at 70: No Time To Retire* (pp. 81-87). NDC.

Griffiths, J. (2019, March 27). *China is the big winner from Europe's Brexit chaos*. Retrieved from CNN: https://edition.cnn.com/2019/03/27/europe/china-europe-brexit-italy-bri-intl-gbr/index.html

Groupe d'experts. (2020). *nato.int*. Retrieved 29 janvier, 2021, from www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf

Hanemann, T., Huotari, M., & Kratz, A. (2019, March 6). *Chinese FDI in Europe: 2018 trends and impact of new screening policies*. Retrieved from Mercator Institute for China Studies: https://www.merics.org/en/papers-on-china/chinese-fdi-in-europe-2018

Harris, J. (2018, November 15). *Weapons of the weak: Russia and AI-driven asymmetric warfare*. Retrieved from Brookings: https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/#cancel

Hart, M., & Johnson, B. (2019, February 28). *Mapping China's Global Governance Ambitions*. Retrieved from Center for American Progress: https://www.americanprogress.org/issues/security/reports/2019/02/28/466768/mapping-chinas-global-governance-ambitions/

Hass, R. (2020, February). *U.S.-China relations: The search for a new equilibrium*. Retrieved from Brookings: https://www.brookings.edu/research/u-s-china-relations-the-search-for-a-new-equilibrium/

Havnes, H., & Seland, J. M. (2019, July 16). *The Increasing Security Focus in China's Arctic Policy*. Retrieved from The Arctic Institute: https://www.thearcticinstitute.org/increasing-security-focus-china-arctic-policy/?cn-reloaded=1

He, A. (2019, September). *The Belt and Road Initiative: Motivations, Financing, Expansion and Challenges of Xi's Ever-expanding Strategy*. Retrieved from CIGI Papers: 2019 CIGI Papers No. 225 The Belt and Road Initiative

Heydarian, R. (2019, June 14). *Beijing's Inchoate Hegemony: The Brewing Backlash in Asia to China's Resurgence*. Retrieved from Carnegie Endowment for International Peace: https://carnegieendowment.org/2019/06/24/beijing-s-inchoate-hegemony-brewing-backlash-in-asia-to-china-s-resurgence-pub-79302

Heydarian, R. (2020, February 4). *A Divided Resistance: The Philippines and its Neighbors Diverge on China*. Retrieved from CSIS Asia Maritime Transparency Initiative: https://amti.csis.org/a-divided-resistance-the-philippines-and-its-neighbors-diverge-on-china/

Hill, ., & Martinez-Diaz, L. (2020). *foreignaffairs.com*. Retrieved 29 janvier, 2021, from reader.foreignaffairs.com/2020/01/23/adapt-or-perish-2/content.html

HRW. (2019, April 1). *UN: China Responds to Rights Review with Threats*. Retrieved from Human Rights Watch: https://www.hrw.org/news/2019/04/01/un-china-responds-rights-review-threats

Hu, W. (July 2018). Xi Jinping's 'Major Country Diplomacy': The Role of Leadership in Foreign Policy Transformation. *Journal of Contemporary China*, 1-14.

IISS. (2019, May). *China's cyber power in a new era*. Retrieved from Asia Pacific Regional Security Assessment 2019: https://www.iiss.org/publications/strategic-dossiers/asiapacific-regional-security-assessment-2019/rsa19-07-chapter-5

IISS. (2019, February). *Quantum computing and defence*. Retrieved from The Military Balance: 2019 IISS Military Balance: Quantum computing and defence

Jones, B. (2020, February). *China and the return of great power strategic competition*. Retrieved from Brookings: https://www.brookings.edu/research/china-and-the-return-of-great-power-strategic-competition/

Kaska, K., Beckvard, H., & Minárik, T. (2019, March). *Huawei, 5G, and China as a Security Threat*. Retrieved from NATO Cooperative Cyber Defence Centre of Excellence: https://ccdcoe.org/library/publications/huawei-5g-and-china-as-a-security-threat/

Kawashima, S. (January 2019). Xi Jinping's Diplomatic Philosophy and Vision for International Order: Continuity and Change from the Hu Jintao Era. *Asia Pacific Review*, 121-145.

Kempe, F. (2019, December 7). *NATO's China challenge*. Retrieved from Atlantic Council: https://www.atlanticcouncil.org/content-series/inflection-points/natos-china-challenge/

Kitson, A., & Liew, K. (2019, November 14). *China Doubles Down on Its Digital Silk Road*. Retrieved from Reconnecting Asia CSIS: https://reconnectingasia.csis.org/analysis/entries/china-doubles-down-its-digital-silk-road/

Kohler, K. (2020). *css.ethz.ch*. Retrieved 29 janvier, 2021, from css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Estonia.pdf

Kuchler, H., & Murphy, H. (2020). *ft.com*. Retrieved 29 janvier, 2021, from https://www.ft.com/content/9c303207-8f4a-42b7-b0e4-cf421f036b2f?accessToken=zwAAAXZq78xIkdOcMDIHj0pCt9Ow5M9CHwNrLw.MEUCIDt9595iGse_C05tTG8J4tl3wZSRGn9Gzm6vaMHOUHaWAiEA6lYx-kThkt6OwU9IvKJBjvBjVgfQWxXFWX5MskMMtHU&sharetype=gift?token=59e3ba00-e807-41ea-9bb9

Kumar, S. (June 2019). China's South Asia Policy in the 'New Era'. *India Quarterly: A Journal of International Affairs*, 137-154.

Kuok, L. (2019, November). *How China's actions in the South China Sea undermine the rule of law*. Retrieved from Brookings: https://www.brookings.edu/research/how-chinas-actions-in-the-south-china-sea-undermine-the-rule-of-law/

Le Corre, P. (2018). Retrieved 29 janvier, 2021, from carnegieendowment.org: carnegieendowment.org/files/RethinkingtheSilkRoad.pdf

Lee, K. (2019, September 16). *Coming Soon to the United Nations: Chinese Leadership and Authoritarian Values*. Retrieved from Foreign Affairs: https://www.foreignaffairs.com/articles/china/2019-09-16/coming-soon-united-nations-chinese-leadership-and-authoritarian-values

Leng, A., & Rajah, R. (2019, December` 18). *Chart of the week: Global trade through a US-China lens*. Retrieved from The Interpreter: https://www.lowyinstitute.org/the-interpreter/chart-week-global-trade-through-us-china-lens

Lidarev, I. (2020, January 4). *2019: Reviewing a Passable Year in China-India Relations*. Retrieved from The Diplomat: https://thediplomat.com/2020/01/2019-reviewing-a-passable-year-in-china-india-relations/

Lin, Z. (July 2018). Xi Jinping's 'Major Country Diplomacy': The Impacts of China's Growing Capacity. *Journal of Contemporary China*, 1-16.

Liu, M. (2020, February 24). *How Do You Keep China's Economy Running With 750 Million in Quarantine?* Retrieved from Foreign Policy: https://foreignpolicy.com/2020/02/24/xi-jinping-coronavirus-china-covid-19-quarantine/

Maizland, L. (2019, July 19). *Is China Undermining Human Rights at the United Nations?* Retrieved from Council on Foreign Relations: https://www.cfr.org/in-brief/china-undermining-human-rights-united-nations

Ministère de l'intérieur de la Finlande. (2018). *ec.europa.eu*. Retrieved 29 janvier, 2021, from ec.europa.eu/echo/sites/echo-site/files/national_risk_assessment_2018.pdf

Ministère estonien des affaires économiques et des communications. (2019). *mkm.ee*. Retrieved 29 janvier, 2021, from www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Nakashima, E., & Aratani, L.. *DHS to issue first cybersecurity regulations for pipelines after Colonial hack,* Retrieved from Washington Post, https://www.washingtonpost.com/business/2021/05/25/colonial-hack-pipeline-dhs-cybersecurity/

OCDE. (2019). *oecd-ilibrary.org*. Retrieved 29 janvier, 2021, from www.oecd-ilibrary.org/sites/9789264311602-8-en/index.html?itemId=/content/component/9789264311602-8-en

Oppenheimer, M. (2020). *foreignaffairs.com*. Retrieved 29 janvier, 2021, from reader.foreignaffairs.com/2020/10/13/as-the-world-burns/content.html

OTAN. (2018). *Résilience et article 3* www.nato.int/cps/en/natohq/topics_132722.htm?selectedLocale=fr

OTAN. (5 juin 2018). *NATO and China resume military staff to staff talks*. [*non disponible en français*]: https://www.nato.int/cps/en/natohq/news_155840.htm

OTAN. (12 novembre 2019). *Speech by NATO Secretary General Jens Stoltenberg on receiving the "Diplomat of the Year" award by Foreign Policy magazine*. [*non disponible en français*] https://www.nato.int/cps/en/natohq/opinions_170714.htm?selectedLocale=ru

OTAN. (14 november 2019). *Keynote address by NATO Secretary General Jens Stoltenberg at the NATO Industry Forum*. [*non disponible en français*]: https://www.nato.int/cps/ru/natohq/opinions_170786.htm

OTAN. (2019). *Rapport 2019 du secrétaire général de l'OTAN* https://www.nato.int/cps/fr/natohq/opinions_174406.htm

OTAN. (24 mars 2020). *La République tchèque reçoit des fournitures médicales d'urgence grâce aux moyens de transport aérien des Alliés*. https://www.nato.int/cps/en/natohq/news_174494.htm?selectedLocale=fr

OTAN. (2020). *La préparation du secteur civil*. Dossiers de l'OTAN www.nato.int/cps/fr/natohq/topics_49158.htm#:~:text=La%20pr%C3%A9paration%20du%20secteur%20civil%20est%20un%20%C3%A9l%C3%A9ment%20central%20de,pr%C3%A9paration%20de%20leur%20secteur%20civil.

Pavel, B., & Brzezinsky, I. (2019, August 21). *It's Time for a NATO-China Council*. Retrieved from DefenceOne: https://www.defenseone.com/ideas/2019/08/its-time-nato-china-council/159326/

Perlroth, N., Scott, M., & Frenkel, S. (2017). *nytimes.com*. Retrieved 29 janvier, 2021, from https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html

Perlroth, N. Scott, & Satariano, A. (2021). *nytimes.com*. Retrieved 25 juin 2021, from https://www.nytimes.com/2021/05/20/technology/ransomware-attack-ireland-hospitals.html

Perović, J., & Zogg, B. (2019, October). *Russia and China: The Potential of Their Partnership*. Retrieved from CSS Analyses in Security Policy: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse250-EN.pdf

Plantan, E. (2017, August 10). *Comparing Recent NGO Laws in Russia and China*. Retrieved from China file - the China NGO Project: https://www.chinafile.com/ngo/analysis/comparing-recent-ngo-laws-russia-and-china

Poling, G. (2020, January 10). *The Conventional Wisdom on China's Island Bases is Dangerously Wrong*. Retrieved from War on the Rocks: https://warontherocks.com/2020/01/the-conventional-wisdom-on-chinas-island-bases-is-dangerously-wrong/

Pothier, F. (2019, September 12). *How should NATO respond to China's growing power?* Retrieved from IISS: https://www.iiss.org/blogs/analysis/2019/09/nato-respond-china-power

Revere, E. J. (2019, November). *Lips and teeth: Repairing China-North Korea relations*. Retrieved from Brookings: https://www.brookings.edu/research/lips-and-teeth-repairing-china-north-korea-relations/

RFE/RL. (2020, April 23). *U.S. Aid To Greenland Looks To Counter Russian, Chinese Influence In Arctic*. Retrieved from RFE/RL: https://www.rferl.org/a/us-aid-looks-to-counter-russian-chines-influence-in-arctic/30573145.html

Ringsmose, J., & Rynning, S. (2020, February 5). *China Brought NATO Closer Together*. Retrieved from War on the Rocks: https://warontherocks.com/2020/02/china-brought-nato-closer-together/

Roberts, K. (2020, February 5). *It's Official: Mexico Is No. 1 U.S. Trade Partner For First Time, Despite Overall U.S. Trade Decline*. Retrieved from Forbes: https://www.forbes.com/sites/kenroberts/2020/02/05/its-official-mexico-is-no-1-us-trade-partner-for-first-time-despite-overall-us-trade-decline/#43672d433eab

Sabbagh, D., & Roth, A. (2020). *theguardian.com*. Retrieved 29 janvier, 2021, from www.theguardian.com/world/2020/jul/16/russian-state-sponsored-hackers-target-covid-19-vaccine-researchers?CMP=Share_AndroidApp_Outlook

Salonius-Pasternak, C. (2018). *fiia.fi*. Retrieved 29 janvier, 2021, from www.fiia.fi/wp-content/uploads/2018/06/bp240_the-defence-of-finland-and-sweden.pdf

Saunders, P. C., & Wuthnow, J. (2019). *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms*. Retrieved from National Defense University Press: https://ndupress.ndu.edu/Publications/Books/Chairman-Xi-Remakes-the-PLA/

Schaake, M. (2020). *foreignaffairs.com*. Retrieved 29 janvier, 2021, from https://reader.foreignaffairs.com/2020/10/13/the-lawless-realm/content.html

Silver, L., Devlin, K., & Huang, C. (2019, December 5). *People around the globe are divided in their opinions of China*. Retrieved from Pew Research Center: https://www.pewresearch.org/fact-tank/2019/12/05/people-around-the-globe-are-divided-in-their-opinions-of-china/

SIPRI. (2019, March). *Trends in International Arms Transfers, 2018*. Retrieved from SIPRI: https://www.sipri.org/sites/default/files/2019-03/fs_1903_at_2018.pdf

Smith, N. R., & Fallon, T. (2019, January 16). *China's soft-power play: what will it take to get it just right and hit the Goldilocks zone?* Retrieved from South China Morning Post: https://www.scmp.com/comment/insight-opinion/united-states/article/2182196/chinas-soft-power-play-what-will-it-take-get

SoftPower30. (2019). *The Soft Power 30* . Retrieved from Portland Communications and the USC Center on Public Diplomacy: https://softpower30.com/wp-content/uploads/2019/10/The-Soft-Power-30-Report-2019-1.pdf

Sørensen, C. T. (2019, November 5). *Hybrid CoE Strategic Analysis 19: The ice dragon – Chinese interests in the Arctic*. Retrieved from Hybrid CoE: https://www.hybridcoe.fi/publications/strategic-analysis-5-2019-the-ice-dragon-chinese-interests-in-the-arctic/

Stanzel, A. (2019, October 11). *China and Russia: Brothers-In-Arms*. Retrieved from Institut Montaigne: https://www.institutmontaigne.org/en/blog/china-trends-3-china-and-russia-brothers-arms

Stent, A. (2020, February). *Russia and China: Axis of revisionists?* Retrieved from Brookings: https://www.brookings.edu/research/russia-and-china-axis-of-revisionists/

Swanson, A., & McCabe, D. (2020, February 20). *Trump Effort to Keep U.S. Tech Out of China Alarms American Firms*. Retrieved from The New York Times: https://www.nytimes.com/2020/02/16/business/economy/us-china-technology.html

Szczudlik, J. (2019, April). *Seven Years of The 16+1: An Assessment of China's 'Multilateral Bilateralism' in Central Europe*. Retrieved from IFRI:

https://www.ifri.org/en/publications/notes-de-lifri/asie-visions/seven-years-161-assessment-chinas-multilateral-bilateralism

Tamkin, E. (2017). *foreignpolicy.com*. Retrieved 29 janvier, 2021, from foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/

Tanas, O., Shiryaevskaya, A., & Murtaugh, D. (2019, November 25). *How Russia-China Gas Pipeline Changes Energy Calculus*. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2019-11-25/how-russia-china-gas-pipeline-changes-energy-calculus-quicktake

Tharoor, I. (2019, December 3). *Is China NATO's new adversary?* Retrieved from The New York Times: https://www.washingtonpost.com/world/2019/12/03/is-china-natos-new-adversary/

The Economist. (2020). *economist.com*. Retrieved 29 janvier, 2021, from www.economist.com/asia/2020/12/12/the-japanese-authorities-understood-covid-19-better-than-most?frsc=dg%7Ce%3cspan%20id=%22ms-outlook-android-cursor%22%3e!~OMSelectionMarkerEnd~

Thomas, G., Williams, P., & Dyakova, Y. (2020). *nato.int*. Retrieved 29 janvier, 2021, from www.nato.int/docu/review/fr/articles/2020/06/16/exercice-defender-europe-20-la-facilitation-et-la-resilience-en-action/index.html

UNOCT. (2019). *un.org*. Retrieved 29 janvier, 2021, from www.un.org/counterterrorism/events/unoct-and-nato-launch-project-prevent-and-counter-chemical-biological-radiological-and

USCC. (2019, March 21). *Hearing on an Emerging China-Russia Axis? Implications for the United States in teh Era of Strategic Competition*. Retrieved from United States-China Economic and Security Review Commission: https://www.uscc.gov/sites/default/files/2019-10/March%2021,%202019%20Hearing%20Transcript.pdf

USIP. (2019, May 6). *China's Role in North Korea Nuclear and Peace Negotiations*. Retrieved from USIP: https://www.usip.org/publications/2019/05/chinas-role-north-korea-nuclear-and-peace-negotiations

USTR. (2020). *The People's Republic of China: U.S.-China Trade Facts*. Retrieved from Office of the US Trade Representative: https://ustr.gov/countries-regions/china-mongolia-taiwan/peoples-republic-china

von Sydow, B. (2018). *Resilience: Planning for Sweden's "Total Defence"*. Retrieved from NATO Review: https://www.nato.int/docu/review/articles/2018/04/04/resilience-planning-for-swedens-total-defence/index.html

Wambach, J. (2012). *reliefweb.int*. Retrieved 29 janvier, 2021, from reliefweb.int/sites/reliefweb.int/files/resources/Liaison2012_Web.pdf

Wertz, D. (2019, November). *China-North Korea Relations*. Retrieved from NCNK: https://www.ncnk.org/resources/briefing-papers/all-briefing-papers/china-north-korea-relations

Westcott, B. (2020, March` 5). *China's military is going from strength to strength under Xi Jinping*. Retrieved from CNN: https://edition.cnn.com/2019/03/04/asia/china-military-xi-jinping-intl/index.html

Whalen, J. (2019, August 19). *The quantum revolution is coming, and Chinese scientists are at the forefront*. Retrieved from The Washington Post: https://www.washingtonpost.com/business/2019/08/18/quantum-revolution-is-coming-chinese-scientists-are-forefront/

Wither, James Kenneth. (2020). *Back to the future? Nordic total defence concepts*. Retrieved from Defence Studies: https://www.tandfonline.com/doi/abs/10.1080/14702436.2020.1718498

Xinhua. (2020, February 17). *China appreciates NATO's remarks of not seeing China as an adversary: spokesperson*. Retrieved from Xinhua: China appreciates NATO's remarks of not seeing China as an adversary: spokesperson

Zhang, W. (2018). *Neither friend nor big brother: China's role in North Korean foreign policy strategy*. Retrieved from Palgrave Communications: https://www.nature.com/articles/s41599-018-0071-2.pdf