Institut EGA

La Revue Diplomatique

NATO OTAN

En partenariat avec la Division Diplomatie Publique de l'OTAN

SOUS LA DIRECTION DE ROMAIN BERTOLINO, MANON GOUREAU ET ALEXANDRE NEGRUS

Revue trimestrielle - Avril 2022

N°17 - 9.80 €

OTAN 2030 : QUELLES ORIENTATIONS DU NOUVEAU CONCEPT STRATÉGIQUE ?

Pierre ANDRIEU • Xavier AURÉGAN • Magomed BELTOUEV • Cécile DOUTRIAUX

Hugues EUDELINE • Alexandra GOUJON • Manon GOUREAU • Karl HADDAD

Emilio IASIELLO • Agnès LEVALLOIS • Nato TARDIEU • Daniel VENTRE

www.institut-ega.org

ATLAS GÉOPOLITIQUE
du monde contemporain

PODCASTS & VIDÉOS

Romain **Bertolino**
Alexandre **Negrus**
Nato **Tardieu**
Préface de Michel Foucher
Postface de Anne-Cécile Robert

À commander depuis ce lien

ellipses

AVERTISSEMENT

OTAN 2030 : quelles orientations du nouveau concept stratégique ?

Les propos exprimés par chaque contributeur n'engagent ni l'Institut d'études de géopolitique appliquée, ni les rédacteurs entre eux, ni le comité de relecture.

Aucune personne physique ou morale citée dans le texte d'un contributeur n'a pour objectif d'identifier l'Institut d'études de géopolitique appliquée ou les autres contributeurs.

Comment citer cette publication :

OTAN 2030 : quelles orientations du nouveau concept stratégique ?, (dir. Romain Bertolino, Manon Goureau, Alexandre Negrus), *Institut d'études de géopolitique appliquée*, *Revue Diplomatique*, n°17, Paris, 2022.

ISSN : 2739-2341

Institut d'études de géopolitique appliquée
31 Rue de Poissy, 75005 Paris
Courriel : contact@institut-ega.org
Site internet : www.institut-ega.org

Institut
EGA

SOMMAIRE

OTAN 2030 : quelles orientations du nouveau concept stratégique ?

Institut EGA

L'OTAN entre ruptures et continuité[1]

Camille GRAND
Secrétaire général adjoint de l'OTAN pour les investissements de défense

En 2022, l'Organisation du traité de l'Atlantique Nord (OTAN) est en pleine transformation. Si le traité de Washington date de 1949, l'OTAN comme organisation visible et permanente n'a vu le jour qu'en 1952. Un secrétaire général, Lord Ismay, s'installe alors à Paris, au palais de Chaillot. Soixante-dix ans plus tard, le quartier général de Bruxelles réunit au quotidien les diplomates et les militaires de trente délégations. Leurs chefs d'État et de gouvernement se préparent à adopter, en juin 2022, à Madrid, un nouveau concept stratégique qui sera la traduction pratique du traité de 1949 et permettra de mener à bien les trois tâches fondamentales de l'organisation, à savoir la défense collective, la gestion de crise et la sécurité coopérative. Parler de l'OTAN aujourd'hui, c'est donc expliquer le rôle d'une institution restée essentielle pour la sécurité de la France et de l'ensemble du continent européen.

Où en est l'OTAN ?

Pour répondre à cette question, on peut dire que l'OTAN est en phase avec l'époque actuelle qui rebat les cartes dans de nombreux domaines. Pour commenter la représentation cartographique de l'OTAN, suggérons d'abord l'idée qu'elle ne peut rendre compte visuellement de tout ce que l'OTAN fait aujourd'hui. Si la carte met en évidence une activité foisonnante dans les domaines terrestre, aérien et maritime, l'espace, le cyber ou la lutte contre la désinformation sont invisibles et ne connaissent pas de frontières. Les sujets sont nombreux qui redéfinissent la gamme des menaces et orientent vers de nouveaux partenariats – les nouvelles technologies, la mobilité militaire, la défense antimissile, la dissuasion, la sécurité des espaces communs, l'impact du changement climatique sur la sécurité, la résilience des infrastructures critiques, les manipulations de l'information qui ressemblent parfois à une sorte de guerre de l'espace cognitif, etc.

La géographie aide l'œil à cerner l'ampleur des défis. Elle est un point de départ incontournable. Les pays partenaires de l'OTAN comme ses adversaires potentiels se penchent, eux aussi, sur les vérités cachées dans les replis des cartes. L'Alliance a tout d'abord, par sa géographie, mené à la fois une alliance terrestre et maritime. Vingt-cinq des trente pays alliés ont un accès à la mer et douze sont ouverts sur deux mers ou océans. Et pourtant, l'architecture de sécurité de l'Europe reste marquée par la présence de la puissance russe dont le comportement constitue une menace persistante. Les rivalités dans l'espace géopolitique expliquent l'attention portée par l'OTAN aux partenariats, d'une part, et aux nouvelles géographies issues de la crise climatique, d'autre part.

Des alliés, mais aussi des partenaires

Il n'est pas anodin que la carte de l'OTAN soit à l'échelle du monde et non plus du seul rideau de fer qui a séparé l'Europe en deux, avec une partie orientale et une autre occidentale, durant quatre décennies. En 2022, l'OTAN veille sur la sécurité de presque un milliard d'habitants. Depuis ses débuts, elle a fait du dialogue une marque de fabrique de son action et une condition de son succès. Ce dialogue se formalise dans les nombreux partenariats de l'OTAN, qui illustrent l'élargissement, non plus seulement de ses membres, mais du regard qu'elle porte sur l'environnement de sécurité. C'est le sens de la démarche OTAN 2030 lancée par le secrétaire général Jens Stoltenberg, en 2020. L'OTAN a

[1] Cette contribution est extraite de l'Atlas géopolitique du monde contemporain (Romain Bertolino, Alexandre Negrus, Nato Tardieu) paru aux éditions Ellipses en mars 2022 : https://www.editions-ellipses.fr/accueil/14144-atlas-geopolitique-du-monde-contemporain-9782340065666.html

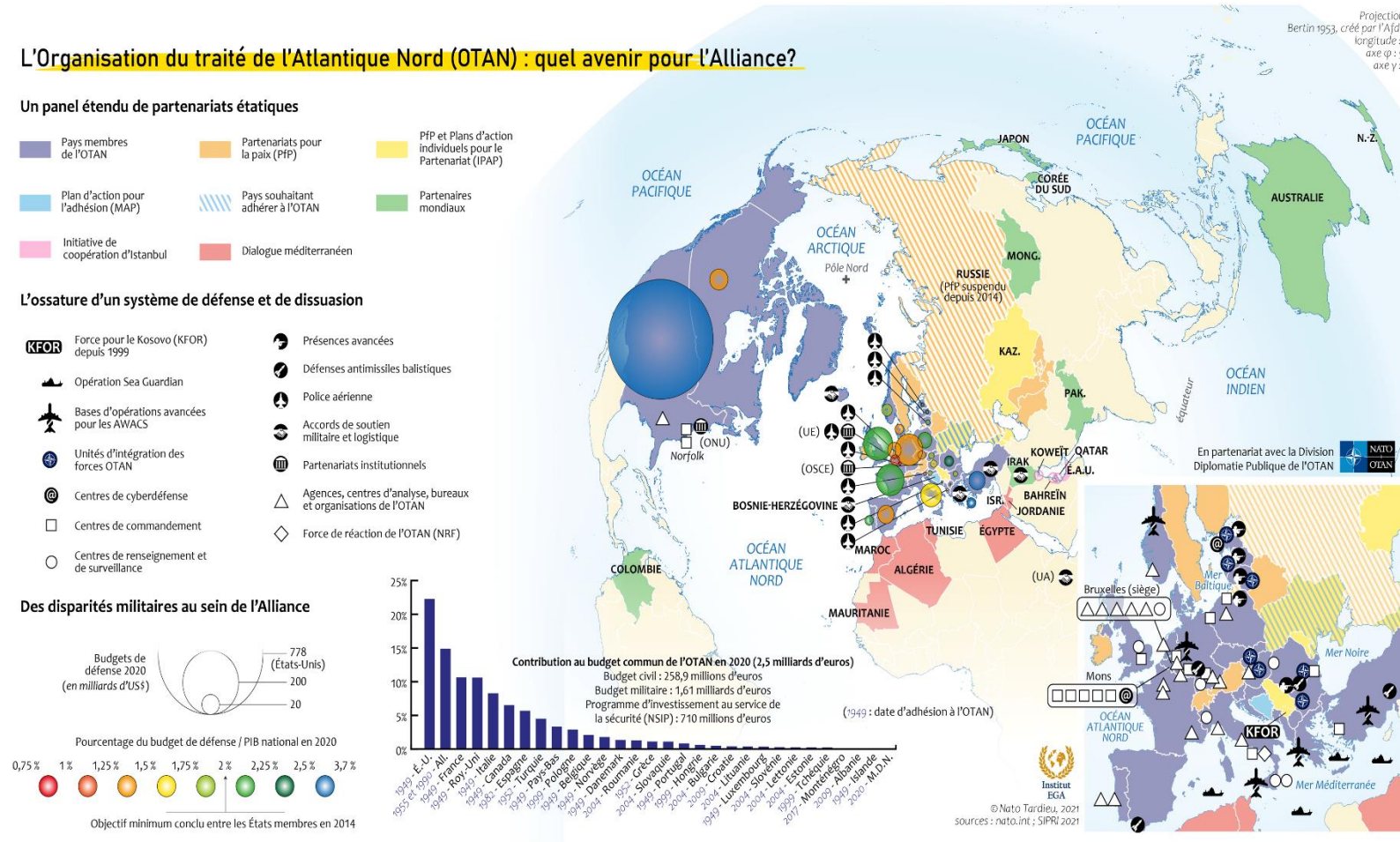
conscience que les menaces qui l'entourent peuvent être diffuses et parfois moins territorialisées. Elle recherche des partenariats afin que, dans un cadre établi, les alliés puissent nouer des accords de coopération avec des pays amis, là où des intérêts convergents le nécessitent.

À l'évidence, se sont succédé plusieurs phases de développement des partenariats depuis la fin du monde bipolaire. D'abord après la guerre froide, l'OTAN s'est ouverte à la Russie, à l'Europe centrale et orientale et aux pays du Caucase et d'Asie centrale. Puis, elle a forgé des relations avec sept pays du pourtour méditerranéen et quatre du golfe Arabo-Persique. Un centre de coopération a ainsi vu le jour, en janvier 2017, dans la ville capitale du Koweït. Plus récemment, l'OTAN a noué des partenariats avec plusieurs pays plus éloignés de l'Europe. Les partenaires « de par le monde » comptent la Nouvelle-Zélande, l'Australie, la Corée du Sud, le Japon, l'Irak, l'Afghanistan, la Colombie, la Mongolie et le Pakistan. En tout, les trente alliés ont donc des relations suivies avec une quarantaine de pays partenaires des cinq continents. Ces partenariats comprennent des activités de formation, des déploiements dans des opérations conduites par l'OTAN, des efforts d'aide au contrôle civil des forces armées, etc.

L'Atlantique Nord ouverte sur l'Arctique

La carte livre enfin une autre clé de lecture sur l'OTAN de demain. En effet, il faut souligner la perspective d'une ouverture progressive de l'océan Arctique à la navigation commerciale, ce qui ne sera pas sans implications stratégiques. Il ne s'agit là que d'un exemple de l'impact du changement climatique sur la sécurité euro-atlantique.

Si l'OTAN demeure l'expression la plus achevée de la solidarité transatlantique et de l'engagement des États-Unis et du Canada, l'évolution de la géographie des menaces et des défis de sécurité a modifié la géographie de l'Alliance, de ses opérations et de ses missions comme de ses partenariats. Dans un environnement stratégique dégradé et incertain, la capacité de l'Alliance atlantique à évoluer et à se transformer est, sans aucun doute, sa plus grande force.



Carte réalisée par Nato Tardieu, pour le compte de l'IEGA en partenariat avec la Division diplomatie publique de l'OTAN, à retrouver dans l'*Atlas géopolitique du monde contemporain* (mars 2022, Editions Ellipses). Cliquer ici

Pourquoi l'OTAN perçoit la Chine comme une menace ?

Arnaud LEVEAU
Docteur en science politique de l'Ecole normale supérieure de Lyon

L'Organisation du Traité de l'Atlantique Nord peine à se réinventer et à garder une raison d'être depuis la dissolution du pacte de Varsovie en 1991. La guerre déclenchée par la Russie en Ukraine replace l'organisation au cœur de l'architecture de défense sur le continent européen et lui confère une nouvelle attractivité pour des nombreux pays, y compris pour certains en dehors de l'alliance. Toutefois, pour assurer sa pérennité, l'Alliance cherche depuis quelques temps à élargir son spectre, notamment en direction de l'Asie et c'est la Chine qui est dans sa nouvelle ligne de mire.

À l'occasion d'un discours prononcé le 8 juin 2020 pour le lancement d'une réflexion sur le renforcement de l'OTAN[2] dans le monde à l'horizon 2030, le secrétaire général de l'Organisation, Jens Stoltenberg, a évoqué l'idée d'une organisation ayant une approche plus globale et, pour faire face à la montée en puissance de la Chine, d'un rapprochement avec certains pays d'Asie Pacifique partageant des vues proches de celles des pays de l'alliance. Il a cité l'Australie, le Japon, la Nouvelle-Zélande et la Corée du Sud.

Un changement des équilibres mondiaux

Dans son intervention Jens Stoltenberg a souligné que l'Organisation ne voyait pas en la Chine un adversaire ou un ennemi mais que la montée en puissance de cette dernière changeait fondamentalement l'équilibre mondial des pouvoirs. Le rapport OTAN 2030 publié en novembre 2020 soulignait que si la Chine ne représentait pas sur le plan militaire pour la zone euro-atlantique une menace aussi immédiate ni de la même ampleur que la Russie, elle pouvait être considérée comme « un rival systémique opérant tous azimuts plutôt qu'un compétiteur purement économique ou un acteur de la sécurité braqué sur la seule Asie ». Le rapport rappelle également que la Chine devrait devenir prochainement la première économie mondiale et qu'elle a déjà le second budget de la défense au monde après les États-Unis. Dans la continuité, le rapport insiste sur le fait que la Chine investit fortement dans la modernisation de ses capacités militaires y compris dans le développement de missiles à longue-portée capables de frapper l'ensemble des pays membres de l'alliance. Le rapport pointe également que la Chine construit des aéronefs à long rayon d'action, des porte-avions et des sous-marins nucléaires d'attaque déployables partout dans le monde, qu'elle renforce considérablement ses capacités spatiales et étoffe son arsenal nucléaire. Le rapport poursuit en soulignant que la Chine est aussi en pointe dans de nombreuses technologies notamment en matière d'intelligence artificielle et d'informatique quantique.

De même, les « nouvelles routes de la soie » terrestres et maritimes, la route de la soie polaire et la route de la soie numérique se développent rapidement. La Chine est déjà présente en Afrique et en Arctique et se rapproche des intérêts vitaux des membres de l'Alliance, notamment en investissant dans des infrastructures critiques de certains pays. Le rapprochement économique, commercial et militaire avec la Russie, notamment en participant à des exercices russes dans la zone euro-atlantique, tout comme le fait que la Chine acquière des infrastructures un peu partout en Europe ce qui à

[2] Le lancement de cette réflexion s'est fait dans le cadre d'une conversation transatlantique organisé par l'Atlantic Council, le German Marshall Fund of the United States en partenariat avec a division Diplomatie publique de l'OTAN. Les analyses et les recommandations du groupe de travail sont disponible sur : https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Fre.pdf

terme pourrait entraîner des conséquences sur les communications et l'interopérabilité entre les alliés.

Enfin, toujours selon ce rapport un certains alliés ont récemment attribué des cyberattaques à des acteurs ayant la Chine comme port d'attache. Ils ont constaté que des informations protégées par la propriété intellectuelle, qui étaient importantes du point de vue de la défense, avaient été volées, et ont subi des campagnes de désinformation orchestrées depuis la Chine, surtout depuis le début de la pandémie de Covid-19.

Un changement de paradigme stratégique

Dans son intervention de juin 2020, Jens Stoltenberg soulignait que ni l'Europe, ni l'Amérique du Nord n'étaient capables de gérer seuls ce changement de paradigme stratégique. Pour lui, la réponse à apporter doit aller vers un renforcement des capacités politiques de l'alliance et un développement plus étroit des liens avec certains des pays d'Asie Pacifique ayant des vues similaires. Il a appelé à une plus grande cohésion entre les membres de l'alliance et à résister à la tentation des solutions nationales.

Les recommandations formulées dans le rapport OTAN 2030 pourraient laisser supposer que la Chine serait progressivement en train de remplacer la Russie comme adversaire potentiel prioritaire des États-Unis et de l'OTAN. Ce sentiment s'est renforcé depuis l'élection de Joe Biden à la présidence des États-Unis. Très rapidement après sa prise de fonction en janvier 2021, l'administration américaine a fait passer le message au quartier général de l'OTAN que l'Alliance devait dorénavant considérer au même niveau les menaces russes et chinoises.

Depuis, les choses se sont accélérées. Lors du sommet de l'OTAN qui s'est tenu à Bruxelles en juin 2021, les États-Unis ont réussi à faire avancer leur vision. Certes il y a eu quelques réticences. Ainsi, la chancelière allemande de l'époque, Angela Merkel, s'est montrée prudente et a manifesté le souhait de garder une position équilibrée à l'égard de la Chine, à l'image de la stratégie allemande en Indopacifique publiée en septembre 2020[3]. De son côté le président français Emmanuel Macron a demandé lors de sa conférence de presse finale à ce que l'OTAN ne se détourne pas de ses missions essentielles afin de ne pas « biaiser » la relation avec la Chine. Il a ainsi rappelé que L'OTAN était une organisation militaire, que le sujet du rapport à la Chine était bien plus large et qu'il ne se limitait pas aux questions militaires[4]. Toutefois au terme du sommet, les chefs d'État et de gouvernement participant à la réunion ont affirmé dans leur déclaration finale que « les ambitions déclarées de la Chine et son assertivité » présentaient « des défis systémiques pour l'ordre international »[5] et la sécurité de l'Alliance Atlantique reprenant ainsi l'essentiel des déclarations du secrétaire général de Jens Stoltenberg, un an plus tôt.

Les relations entre d'un côté les pays occidentaux, dont nombre d'entre eux sont membres de l'OTAN et de l'autre la Chine et la Russie n'ont depuis cessé de se dégrader (débat sur l'origine de la Covid-19, Xinjiang, Hong Kong, Taiwan, Ukraine, etc.)

En février 2022, peu de temps avant le début de l'invasion de l'Ukraine par la Russie, la Chine et la Russie dans une déclaration commune sur l' « entrée des relations internationales dans une nouvelle ère [6]» ont dénoncé l'influence américaine et le rôle des alliances militaires occidentales, notamment de l'OTAN et de l'AUKUS[7], les jugeant déstabilisatrices. Dans le même document, les deux pays se sont dit

[3] Le texte de la stratégie allemande en Indo-Pacifique est disponible sur : https://www.auswaertiges-amt.de/fr/newsroom-/-/2381772

[4] La conférence de presse du président français est disponible sur : https://www.elysee.fr/emmanuel-macron/2021/06/14/sommet-de-lotan-a-bruxelles

[5] Le communiqué du sommet de Bruxelles est disponible sur : https://www.nato.int/cps/fr/natohq/news_185000.htm

[6] Le texte de la déclaration commune est disponible sur : Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development • President of Russia (kremlin.ru)

[7] AUKUS pour Australia, United Kingdom et United States est une alliance militaire tripartite formée par l'Australie, les États-Unis et le Royaume-Uni. Présentée le 15 septembre 2021, le jour où l'Union Européenne rendait publique sa stratégie pour la coopération dans la région Indo-Pacifique. L'AUKUS entend approfondir la coopération en matière de sécurité, de diplomatie et de défense entre les trois pays membres dans la région Indo-Pacifique. Elle comprend aucun membre de l'Union

opposés à tout « élargissement futur de l'OTAN ». Sur un ton rappelant une autre époque, la Chine et la Russie ont par ailleurs appelé l'OTAN « *à renoncer à ses approches idéologisées datant de la guerre froide* » et ont adopté ensemble le concept d'« indivisibilité de la sécurité ». La Russie s'appuie depuis longtemps sur ce concept pour réclamer le départ de l'OTAN de son voisinage proche arguant du fait que la sécurité des uns ne peut se faire aux dépens de celle d'autres, en dépit du droit selon lequel chaque État est libre de choisir ses alliances. Parallèlement la Chine et la Russie se sont dit préoccupés par la création de l'AUKUS estimant qu'elle aurait des effets négatifs pour la paix et la stabilité en Asie. Toutefois, le comportement de Chine dans le cadre de l'offensive russe en Ukraine semble dénoter une divergence d'approche entre les deux pays sur la manière de régler les conflits territoriaux régionaux et sur la posture à tenir à l'égard des États-Unis et de leurs alliés.

Un centre de gravité qui se déplace à l'Est

Alors que les zones de tensions s'accroissent dans le monde et que la dimension stratégique de la région Indopacifique ne cesse de croitre, il semble logique que l'OTAN, toujours largement pilotée par les États-Unis, porte son attention vers cette région bien que l'est du continent européen demeure une zone stratégique et à observer dans les mois et années qui viennent. On peut s'interroger sur la manière dont cette organisation, créée autour de la défense de l'Europe de l'Ouest face à la menace soviétique pourrait être en mesure de projeter ses capacités vers l'Indopacifique tout en maintenant des moyens suffisants sur le vieux continent, notamment en réponse au conflit engagé par la Russie en Ukraine.

Il ne serait toutefois pas surprenant de voir se mettre en place un renforcement des accords bilatéraux de défense entre certains pays membres de l'OTAN (États-Unis, France, Royaume-Uni, Canada) avec quelques pays de la région Indo/Asie Pacifique (Australie, Inde, Japon, Nouvelle Zélande, Corée du Sud, Singapour voire Vietnam).

Nous pourrions également assister à l'élaboration de mini-accords multilatéraux à l'image de l'AUKUS ou des tentatives de relances du QUAD[8] auquel pourraient participer à différents degrés et individuellement des membres de l'Alliance atlantique, notamment le Royaume-Uni et la France. Un format QUAD+ existe déjà, incluant la Nouvelle-Zélande, le Vietnam et la Corée du Sud.

Déjà, l'Australie, la Corée du Sud, le Japon et la Nouvelle-Zélande participent depuis 2014 à la plateforme d'interopérabilité qui rassemble les membres de l'Alliance et 24 pays partenaires. En 2018, l'Australie et le Japon ont participé à l'exercice cyberdéfense *Locked Shields* piloté par le Centre d'excellence de cyberdéfense coopérative de l'OTAN, accrédité par l'OTAN et dont la Corée du Sud et le Japon participent déjà au financement[9].

Des échanges plus fréquents et plus étroits entre l'OTAN et certains pays de la zone Indopacifique pourraient donc continuer de se développer à un rythme soutenu, illustrant ainsi le rapide basculement du centre stratégique mondial vers l'Est.

Européenne. Elle exclue aussi la Nouvelle-Zélande, pays qui refuse l'accès des navires nucléaires dans ses eaux territoriales. La création de cette alliance a eu pour première conséquence la rupture par l'Australie d'un contrat passé avec la France pour la fourniture de douze sous-marins conventionnels. Cette nouvelle alliance est perçue comme un moyen pour tenter de contrer l'expansionnisme chinois en Indopacifique.
Le communiqué officiel de la création de cette nouvelle alliance est disponible sur le lien suivant : https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/15/joint-leaders-statement-on-aukus/

[8] QUAD pour Quadrilateral Security Dialogue (Dialogue Quadrilatéral pour la Sécurité). Créé à l'initiative du Premier ministre japonais en 2007 le QUAD est un dialogue stratégique informel comprenant l'Australie, les Etats-Unis, l'Inde et le Japon. Le dialogue a pris fin en 2010 après le retrait de l'Australie avant d'être relancé en 2017.

[9] Voir le site du CCDCOE ; https://ccdcoe.org/about-us/

La puissance maritime chinoise en mer de Chine méridionale

Hugues EUDELINE
Ancien officier de marine, docteur en Histoire militaire, chercheur associé à l'Institut Thomas More

La République populaire de Chine (RPC) est l'acteur, voire le perturbateur principal dans le théâtre Indopacifique, en particulier dans ses approches maritimes, indispensables à son émergence économique.

Ce pays a des modes d'action politique, diplomatique, militaire et scientifique très différents de ceux des démocraties occidentales. Il maîtrise tout d'abord le temps long en pratiquant l'analyse fine du retour d'expérience historique, la planification à long terme et le respect de la continuité dans la réalisation des projets.

Première puissance économique mondiale au début du XIXe siècle, la Chine s'est appauvrie progressivement jusqu'en 1976. Ce siècle « d'humiliation » est en partie imputable aux étrangers, pour la plupart venus de la mer, mais il est surtout la conséquence des nombreuses révoltes et luttes intestines qui ont toujours marqué son histoire plurimillénaire. Si ces révoltes et luttes sont toujours occultées par les Chinois, l'ingérence étrangère nourrit un ultranationalisme exacerbé dans la population. À la mort de Mao, la part du PIB mondial de la Chine avait chuté vertigineusement, passant de 32,4% en 1820 à 4,9%.

À partir de 1978, Deng Xiaoping ouvre cette île géopolitique à l'économie mondiale par le commerce maritime qui alimente les zones économiques spéciales créées le long des côtes. L'émergence économique est fulgurante et, aujourd'hui, la Chine nourrit un « rêve chinois » qui doit en faire la première puissance mondiale en 2049, centenaire de la conquête du pouvoir par les communistes.

Le succès de l'Initiative de la route et de la ceinture[10] (IRC) repose avant tout sur l'accroissement des flux maritimes qui irriguent son industrie et écoulent ses productions manufacturées devenues indispensables à la population mondiale. La RPC applique en cela le précepte de Sir Walter Raleigh, marin britannique qui écrivait à l'aube du XVIIe siècle : « Celui qui commande la mer commande le commerce ; celui qui commande le commerce commande la richesse du monde et par conséquent, le monde lui-même. »

Pour protéger ses approches maritimes, la Chine doit prioritairement commander[11] les eaux qui baignent ses côtes, celles des mers de Chine et de la mer Jaune. Elles baignent également celles de quatre autres puissances économiques majeures, le Japon, la Corée du Sud, Taïwan (République de Chine — RDC) et Singapour dont les échanges sont très majoritairement maritimes.

Donnant accès à l'océan Indien par les détroits indonésiens, clés des routes maritimes vers l'Afrique, l'Asie du Sud, le Moyen-Orient et l'Europe, c'est la mer de Chine méridionale qui est aujourd'hui la principale approche maritime de la Chine.

Délimité à l'est par une ligne d'îles dont aucune ne lui appartient, au nord par l'île de Taïwan qui refuse son autorité et au sud par le détroit de Malacca qu'elle ne contrôle pas, cet espace maritime constitue le talon d'Achille de l'économie de la Chine, et par conséquent de sa stabilité sociale et politique.

Pour bien marquer que la fermeture du détroit du même nom constituerait une menace existentielle pour la Chine, le président Hu Jintao l'a qualifiée de

[10] L'IRC, lancée par Xi Jinping en 2013, est composée de la route maritime de la soie du XXIe siècle et de la ceinture économique de la soie (terrestre).

[11] L'acception donnée au terme commander est ici celle de disposer d'une puissance dominatrice sur mer qui permet de chasser le pavillon ennemi ou ne lui permettre d'apparaître que fugitivement.

« dilemme de Malacca » en 2003. Pour contrer la menace induite par cette tyrannie de la géographie, ses successeurs n'ont eu de cesse de développer des moyens maritimes à une échelle et à une cadence encore jamais connues, avec pour objectif de faire de la mer de Chine méridionale un lac chinois.

Les forces maritimes chinoises

Pour commander cet espace maritime, la RPC se dote du corps de garde-côtes (GCC), le plus important au monde (plus de 250 unités). Il est soutenu par une milice maritime de plusieurs centaines de navires. Ces forces paramilitaires peuvent s'appuyer autant que de besoin sur une énorme marine de guerre (l'Armée populaire de libération — Marine — APL-M) en croissance rapide. Bien équilibrée, mais n'ayant pas encore atteint la taille voulue ni la condition opérationnelle nécessaire, elle sera à terme capable de conduire tous les types de lutte et d'intervenir partout dans le monde. Le nombre de ses bâtiments de guerre dépasse aujourd'hui celui des États-Unis, sans pour autant atteindre leur tonnage cumulé. Soigneusement planifiée, la cadence accélérée de production est destinée à amener l'APL-M au premier rang mondial en 2035.

Le fait de disposer dans les approches de la Chine de ces trois forces maritimes (Milice maritime, garde-côtes et Marine de guerre), toutes placées sous un même contrôle opérationnel, lui permet de coordonner leurs actions pour maîtriser le niveau de conflictualité, tout en lui permettant, à terme, d'atteindre ses objectifs stratégiques.

Les garde-côtes chinois, outre leur supériorité numérique sur ceux des autres pays riverains, disposent de plusieurs bâtiments d'un tonnage supérieur à 10 000 tonnes dont la coque renforcée leur permettrait d'épauler ou d'éperonner des bâtiments contrevenants sans qu'il leur soit nécessaire d'utiliser leurs armes.

La Chine vient encore de durcir sa position en adoptant le 22 janvier 2021 une loi autorisant les garde-côtes à utiliser des armes légères si les circonstances d'une infraction l'exigent ou, dans les cas plus graves, d'utiliser leurs canons. Elle leur permet explicitement d'intervenir pour arrêter la construction ou détruire des structures érigées sur des îles revendiquées par la Chine. Elle donne également à la GCC un large pouvoir discrétionnaire pour créer des zones d'exclusion temporaires, arraisonner et inspecter les navires étrangers dans les eaux revendiquées par la Chine, en contradiction avec la Convention des Nations unies sur le droit de la mer, c'est-à-dire à l'intérieur de la « ligne en 10 traits », cette zone qui recouvre près de 70% de la surface de la mer de Chine méridionale.

La troisième grande force maritime — qui n'existe qu'en Chine et au Vietnam où elle est de moindre ampleur — est la Milice maritime. Elle est composée de navires de pêche à coques en acier, armés par des marins civils ayant reçu une formation militaire et une éducation politique. La Milice maritime de Chine méridionale opère à partir de dix ports situés dans les provinces chinoises du Guangdong et de Hainan. Environ 300 de ses navires opèrent simultanément et à tout moment dans les îles Spratly, ce qui permet d'estimer leur nombre total à environ 400 compte tenu des impératifs de maintenance. Auxquels il faut ajouter les pêcheurs qui les rejoignent par intérêt ou opportunisme.

Protégée par la puissance de ses forces militaires, la RPC peut pratiquer une politique efficace des petits pas sans jamais reculer sous la pression internationale. Quand apparaît une résistance comme ce fut le cas lors de la plainte déposée par les Philippines, elle préfère attendre que le temps fasse son œuvre et que la situation évolue en sa faveur. Le temps politique est court dans les démocraties dont les responsables politiques se succèdent à une cadence plus rapide qu'en Chine où, de plus, les dirigeants gardent toujours un même cap géopolitique.

Outre les objectifs purement économiques, cette stratégie de commandement des approches maritimes répond à un besoin purement militaire, celui de la constitution d'un bastion pour la protection des sous-marins lanceurs d'engins de la force de dissuasion chinoise. Encore trop bruyants, ils ne peuvent s'aventurer seuls dans l'immensité océanique. La plus grande partie de la zone délimitée par la « ligne en dix traits » est constituée de grands fonds qui sont rapidement accessibles par

les sous-marins basés dans l'île Hainan où une base souterraine a été creusée à leur usage. Une demi-heure après avoir appareillé ils ont suffisamment d'eau sous la quille pour pouvoir plonger et entamer leur patrouille dans une bulle sécurisée par des moyens navals et aériens importants.

Des bases avancées et des points d'appuis logistiques sont nécessaires pour mener à bien cette stratégie. Ils ont été aménagés sur des îles ou des hauts fonds remblayés dans les archipels des Paracel (pris au Vietnam en 1974) et des Spratly dont la prise de contrôle se poursuit méthodiquement en appliquant la stratégie du saucisson, c'est-à-dire la lente accumulation de petites actions (les tranches) dont aucune ne peut constituer de *casus belli*, mais qui, par leur accumulation au fil du temps, conduisent à un changement stratégique majeur.

Les sept hauts fonds qui ont été remblayés en un temps record en mer de Chine méridionale disposent de ports protégés permettant le soutien logistique des forces maritimes qui y patrouillent.

Trois ont été pourvus de pistes d'aviation d'une longueur de 3000 m environ (*Fiery Cross reef, Subi reef* et *Mischief shoal*). Situés entre 100 et 150 milles nautiques (MN) les uns des autres ils se soutiennent mutuellement. Ils sont de plus situés presque à mi-distance de l'île de Hainan, le point le plus au sud de la Chine et du détroit de Malacca (respectivement 570 MN et 730 MN), c'est-à-dire à portée d'intervention aérienne sans ravitaillement en vol. Cette menace que l'aviation navale chinoise fait peser sur les détroits constitue une réponse efficace au « dilemme de Malacca. »

Le rôle de la marine de guerre est à présent volontairement restreint dans les mers de Chine aux seules démonstrations de puissance navale. Il s'agit de limiter autant que possible le risque qu'une rencontre entre des bâtiments de guerre dégénère dans le cadre d'une simple action de police. Du fait des différends maritimes engendrés par les revendications chinoises, des confrontations violentes opposent fréquemment des nuées des pêcheurs de différents pays. Le 30 janvier 2013, une de ces rencontres s'est déroulée en mer de Chine orientale entre pêcheurs japonais et chinois. Des bâtiments de guerre de chaque pays étaient sur zone quand une unité de la marine chinoise a illuminé une frégate japonaise avec son radar de conduite de tir. L'équipage de celui-ci aurait pu faire usage de ses missiles pour anticiper une attaque et déclencher une escalade incontrôlée de la violence.

À la suite de cet événement, des mesures ont été prises de part et d'autre pour éviter tout dérapage. Le 9 mars 2013, le Premier ministre japonais a ordonné à sa marine d'adopter une attitude non provocante en restant hors de vue des forces de l'APL-M. De leur côté, les Chinois ont réorganisé leurs forces maritimes, lesquelles, en plus de la marine de guerre, comprenaient alors cinq corps paramilitaires qui armaient de très nombreux bâtiments de petit ou moyen tonnage. Le 9 juillet 2013, le nouveau corps des garde-côtes (CCG) est créé. Il en regroupe quatre (tous sauf l'Administration de la sécurité maritime [MSA] du ministère des Transports.) Il dépend dans un premier temps du ministère civil de la terre et des ressources, avant d'être rattaché en 2018 aux forces armées.

Le cas de Taïwan

Depuis que Mao a pris le contrôle de la Chine continentale en 1949, trois opérations militaires majeures ont été menées par la RPC contre Taïwan et les quelques îles de moindre importance où s'étaient réfugiés les membres du Kuomintang. Les « crises de Taïwan » de 1954-55, 1958 et 1995-96, ont échoué en raison de l'intervention de groupes aéronavals américains, plus puissants que les forces chinoises. La Chine a tiré les leçons de ces échecs cuisants et n'entamera pas d'hostilités sans disposer localement — et pendant le temps nécessaire — d'une supériorité numérique et technique indiscutable dans tous les domaines de lutte. Une inconnue demeure : la compétence opérationnelle des équipages et des états-majors de l'APL-M. Faute d'avoir été engagée dans des opérations réelles de grande envergure, elle n'a pu être évaluée.

Le 14 mars 2005, la République populaire de Chine promulguait une loi anti-sécession dont l'article 8 stipule : « Dans le cas où les forces sécessionnistes "indépendantistes de Taïwan" agiraient (…) pour provoquer la sécession de Taïwan de la Chine (…) l'État emploiera des moyens non pacifiques (…) pour

protéger la souveraineté et l'intégrité territoriale de la Chine. »

La Chine propose une réunification suivant le principe « un pays, deux systèmes », mais la reprise en main brutale de Hong Kong en 2020 a montré le manque de crédibilité de la parole politique chinoise.

Le maintien du *statu quo*, sous réserve que Taïwan ne déclare pas son indépendance, permettrait le maintien de la paix sans nuire aux économies très imbriquées des deux États. Il ne saurait cependant convenir durablement à Xi Jinping qui a fait inscrire, dans un livre blanc publié le 6 septembre 2011, que la réunification du pays fait partie des intérêts vitaux (*core interest*) de la Chine. C'est bien sûr Taïwan — principal verrou de la ligne d'îles qui sépare les mers de Chine de l'océan Pacifique — qui est principalement visée, ainsi que la zone circonscrite par la « ligne en dix traits » et les hauts fonds qui s'y trouvent.

Pourtant, la situation économique de la RPC et celle, politique de son président, se sont dégradées. La crise sanitaire de la Covid, largement imputée à la Chine par la communauté internationale, le rejet par de nombreux pays de la norme de télécommunication 5G de Huawei et les différents embargos américains ainsi que les pénuries énergétiques résultant des sanctions qu'elle a imposées à l'Australie pourraient induire un mécontentement de la population chinoise et du parti communiste, ce que Xi Jinping ne saurait tolérer.

Prenant avantage des très importants moyens militaires dont il a doté l'Armée populaire de libération (APL) et en particulier sa Marine, il pourrait être tenté de canaliser le ressentiment populaire et de désarmer ses opposants politiques en exacerbant le nationalisme et en précipitant une attaque de Taïwan par ses forces armées. Cette dernière, à défaut de pouvoir vaincre militairement un agresseur beaucoup plus puissant, lui opposerait une défense active. Infliger des pertes suffisamment importantes pourrait suffire à déconsidérer Xi Jinping et à gagner le temps nécessaire à la constitution d'un soutien international sous l'égide des États-Unis.

***

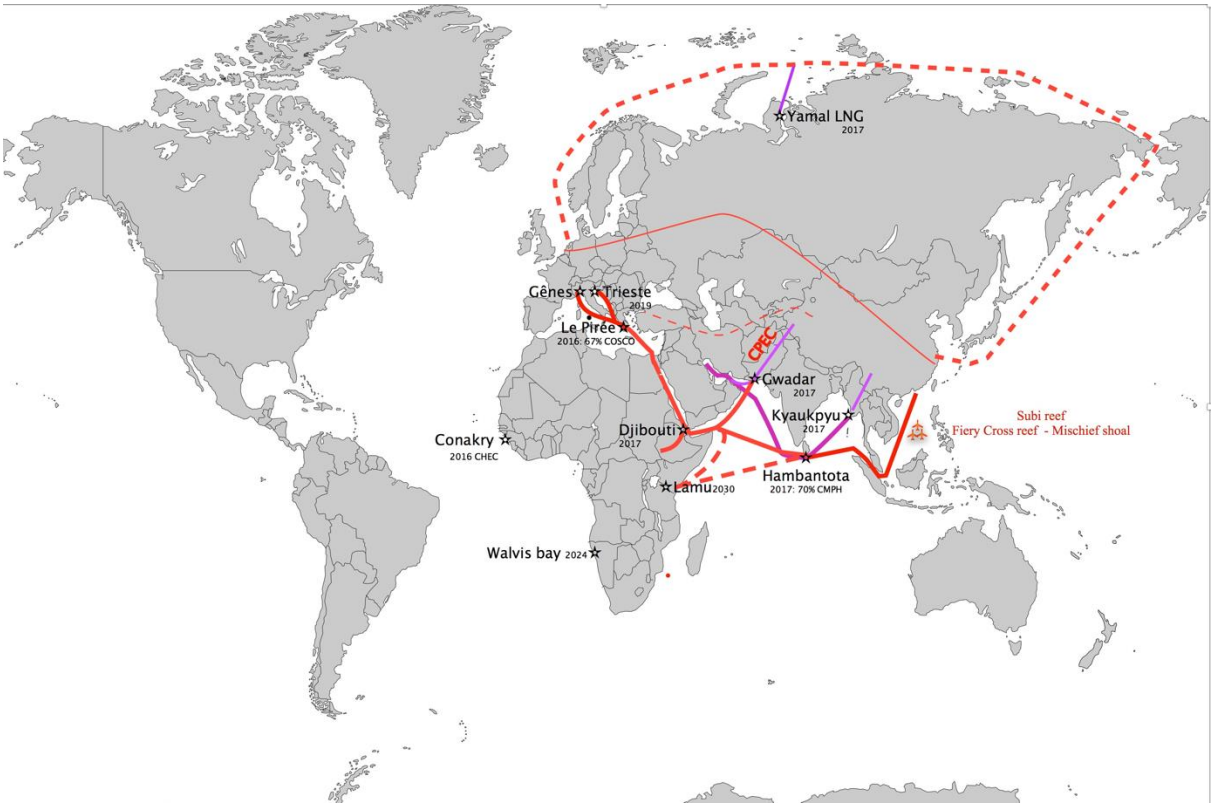
Commander la mer de Chine méridionale est vital pour l'économie chinoise et donc pour le régime. Jusqu'à présent, la Chine l'a fait en menant une stratégie des petits pas qui privilégie l'emploi de forces paramilitaires très nombreuses sous l'égide d'une marine de guerre puissante, mais toujours en plein essor et en formation. L'Empire du Milieu continue de prendre progressivement le contrôle d'îlots en submergeant leurs approches par des centaines de navires « civils ». Il ne négocie que de façon bilatérale avec les autres pays côtiers — beaucoup plus faibles — et rejette les décisions d'organisations internationales comme autant d'ingérence dans ses affaires internes. Cette diplomatie navale qui s'inscrit dans le temps est efficace parce qu'elle privilégie l'usage de la menace et du blocage prolongé des situations sans recours massif aux armes dans un conflit auquel elle n'est pas encore prête.

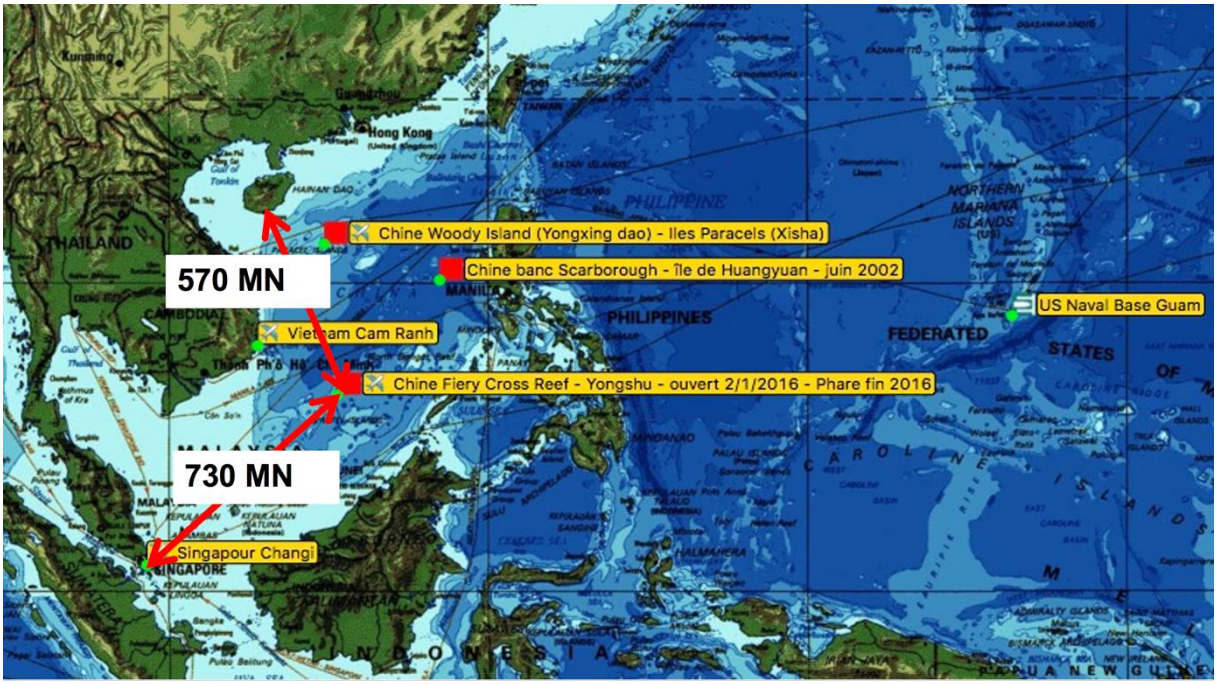
Dans un futur proche, la situation géostratégique va changer sous l'effet du réchauffement climatique avec l'ouverture progressive de la route maritime Arctique à tous les navires de commerce. Le pivot des échanges entre l'Asie et l'Europe va basculer de l'océan Indien à l'océan Arctique raccourcissant de 30% les distances. Si la Chine ne veut pas être confrontée à un « dilemme de Taïwan » — pendant de celui de Malacca à l'autre extrémité de la mer de Chine méridionale —, elle sera dans l'obligation de prendre le contrôle de la RDC. Il est peu probable que l'unification des deux Chine se fasse pacifiquement après l'exemple de la reprise en main de Hong Kong et l'instauration à Taïwan d'une véritable démocratie à laquelle les citoyens adhèrent. Les alliances et les partenariats contre la Chine communiste se concrétisent petit à petit autour des États-Unis. Bien que ceux-ci maintiennent une ambiguïté de façade quant à leurs intentions, le partage des mêmes systèmes d'armes américains de haute technologie (Chasseurs F-35B, porte-aéronefs, systèmes antimissiles AEGIS, avions de patrouille maritime P-8, torpilles Mk-48…) avec les principales puissances militaires de la zone Indopacifique (Corée du Sud, Japon, Australie) et les partenariats avec d'autres — moins proches — comme l'Inde (Quad), signent la mise en place d'une logistique de combat unifiée. Taïwan, avec ou sans

les États-Unis et leurs Alliés, sera alors confrontée à l'ensemble d'une Marine de guerre chinoise, assistée par le corps de garde-côtes et la Milice maritime les plus nombreux au monde, combattant à proximité de ses bases et sous la couverture de la Force de missiles et de l'Armée de l'air. À moins que les États-Unis ne reculent où que la situation intérieure chinoise se dégrade au point de déstabiliser le régime comme il y a tant d'exemples dans l'histoire de l'Empire du Milieu.

Les routes maritimes de la soie du XXIe siècle

Cartes : Hugues Eudeline





Les nouvelles routes de la soie en Afrique et en Amérique latine

Xavier AUREGAN
Maître de conférence à l'Université catholique de Lille, chercheur associé à l'IFG Lab' (Institut français de géopolitique, Paris 8, France) et au Conseil québécois d'études géopolitiques (CQEG, Université Laval, Québec, Canada)

Depuis l'arrivée au pouvoir de Xi Jinping et du lancement concomitant du projet des nouvelles routes de la soie en 2013, les présences chinoises dans le monde, pluriformes, ont été amplement analysées et décomposées, parfois critiquées, parfois encensées, plus rarement neutralisées, mais toujours commentées. En Amérique du Nord, en Europe ou en Océanie, ces présences et l'État chinois, assimilés à tort, sont peu souvent perçus d'une manière bienveillante. En est-il autrement dans les pays en développement, où, du fait de l'histoire ou d'évènements plus récents, un sentiment anti-occidental – mais non pas toujours associé à l'altermondialisme ou à l'anticapitalisme – se développe et se diffuse ? Peut-on seulement les appréhender ? Nous proposons *infra* quelques éléments de réponse permettant d'aborder les enjeux, les risques et les représentations de territoires et populations dits du « Sud » vis-à-vis de la Chine du XXIe siècle et de son projet des nouvelles routes de la soie. Dans ce cadre, deux régions et leurs 87 pays et territoires peuvent être mobilisés : l'Afrique et l'Amérique latine et Caraïbe (ALC).

La Chine des nouvelles routes de la soie en Afrique et en ALC : enjeu(x) et risque(s)

Stato-centré comme les relations bilatérales entre la Chine et ses « partenaires », le projet des nouvelles routes de la soie est avant tout sino-centré. En dépit du cinquième objectif annoncé par les autorités chinoises, soit « people-to-people bonds », il doit effectivement permettre de soutenir la croissance domestique en offrant de nouveaux marchés (*market-seeking investment*), tout en pourvoyant à sécuriser les routes énergétiques et par suite, l'approvisionnement en matières premières (*resource-seeking investment*). C'est en cela que les deux régions susnommées s'avèrent stratégiques. D'une part, elles sont richement dotées en ressources naturelles renouvelables ou non. D'autre part, elles font l'objet d'un – relatif – désintérêt occidental depuis la décennie 1990.

Bien qu'elles ne puissent être reliées au projet des nouvelles routes de la soie via le volet terrestre (*the Silk Road Economic Belt*), les régions Afrique et ALC vont opportunément l'être par la voie maritime (*the 21st Century Maritime Silk Road*), permettant aux autorités d'intégrer 68 membres sur 145 au total. Pourquoi rejoindre ce programme ? « L'attrait de la Chine est à la fois porteur d'opportunités (à saisir) et de défis (à relever). Exportatrices de matières premières peu transformées et fortement dépendantes des puissances traditionnelles, ces deux régions du monde regroupent de nombreux États attachant historiquement de l'importance aux questions de souveraineté et d'autodétermination que promeut opportunément le partenariat proposé par Pékin. La puissance économique et financière de la Chine leur offre de surcroît une nouvelle marge de manœuvre potentielle » (Aurégan et Wintgens, 2020). Effectivement, ces régions et territoires doivent développer leurs propres plans ou programmes de développement dans lesquels les infrastructures (sociales, de production et de communication) occupent une place considérable. Ce faisant, ils sont à la recherche de capitaux que les institutions financières internationales ou les bailleurs « traditionnels » leurs refusent régulièrement.

Dans le cas africain (Aurégan, 2022), ces infrastructures ont été financées par la Chine à hauteur de 30,5 % entre 2006 et 2018. C'est dire l'importance que revêtent les engagements chinois dans la dotation, ici africaine, d'infrastructures qui concernent le maritime (ports et aménagements), le terrestre (routes, autoroutes et ferroviaire), l'énergie (barrages, lignes électriques), les

télécommunications, l'aéroportuaire ou encore les canalisations en eau. Paradoxalement, la pandémie de la Covid-19 (Aurégan, 2021) n'a pas freiné ces prêts chinois estampillés « nouvelles routes de la soie », mais a réamorcé ces financements qui stagnaient depuis 2017.

Les infrastructures financées, construites et parfois gérées par des acteurs économiques chinois en Afrique et en ALC sont donc autant des opportunités, que des sources de risques pour les différentes parties. Côté chinois, les chantiers domestiques ayant tendance à être saturés, les entreprises recherchent de nouveaux marchés à l'étranger, et l'Afrique (32,6 %) et l'ALC (7,9 %) comptent pour plus de 40% des contrats gagnés à l'international sur la période 1998-2018 (42 % depuis 2013). En cela, ces deux régions incarnent des relais de croissance extraterritoriaux. Toutefois, comme tout chantier à l'étranger, ces infrastructures ne sont pas exemptes de risques : incapacités des États clients à rembourser, difficultés techniques, grèves et conflits, enlèvements, violences allant jusqu'au meurtre ou atteintes à la réputation des entreprises et à l'image de la Chine. Le cas du projet avorté du canal inter-océanique du Nicaragua est symptomatique d'effets d'annonce non-suivis d'effets concrets. Côté africain et latino-américain, au-delà de l'apport nécessaire en infrastructures modernes permettant d'intégrer et d'interconnecter les territoires, parfois enclavés, les simples présences et financements chinois permettent de mettre en concurrence « anciens » et « nouveaux » partenaires intéressés par les territoires, ressources et marchés. Compte tenu des sommes afférentes aux infrastructures, les risques sont nombreux. Parmi eux, la possibilité d'alimenter l'extraversion de pays tournés vers l'Asie *a minima*, et d'affaiblir les relations ou échanges intra-régionaux. Très capitalistiques, les prêts – et subsidiairement les investissements – chinois ont tendance à accroître la désindustrialisation et surtout la reprimarisation des économies, en plus de l'augmentation des dettes extérieures, de formes de dépendances en matière de normes, de main d'œuvre, de techniques et savoir-faire, et naturellement, d'une « diplomatie de club » (Aurégan et Wintgens, 2019 : 6). Selon les États, les représentations à l'égard de la Chine et de son projet sont *de facto* hétérogènes, mais qu'en est-il des populations ?

De la difficile appréhension des représentations

La Chine et son projet sont difficilement dissociables, comme l'indiquent les sondages d'opinion réalisés par certains centres de recherche et entreprises originaires des États-Unis. En l'espèce, *Gallup* (2019a) estime que l'Afrique est la région approuvant le plus le leadership chinois à l'échelle internationale avec 53% d'opinions positives en 2018. Les États africains figurent parmi les pays les mieux classés avec le Pakistan et la Mongolie, concentrant 8 des 10 premiers d'entre eux. Faute de différencier l'Amérique du Nord de la latine, il est complexe d'appréhender les résultats portant sur cette région. En tout état de cause, la Chine semble maintenant dépasser les États-Unis en Afrique (53% contre 52% en 2019) et talonner Washington sur le continent américain, Canada inclus (30% contre 31%) (Gallup, 2019). Plus que l'approbation en termes de leadership, il convient certainement d'observer les désapprobations : en Amérique, les sondés indiquent s'opposer au leadership états-unien à 53%, mais seulement à 33% pour la Chine. En Afrique, seuls 19% (États-Unis) et 16% (Chine) contestent cette forme de pouvoir (ou capacité). Bien que la méthodologie soit contestable (sondages téléphoniques et limités en valeurs absolues), ces perceptions peuvent apporter une image, datée et limitée, des représentations régionales à l'égard de ces deux puissances.

Le *Pew Research Center* (2019) peut à son tour contribuer à évaluer ces cartes mentales. Ses résultats sont peu ou prou identiques à *Gallup*, si ce n'est que les questions sont à la fois plus nombreuses et plus précises : droits de l'homme et son respect en Chine ; comparaisons entre les chefs d'État, y compris asiatiques ; confiance en la politique étrangère de Xi Jinping ; montée en puissance militaire chinoise ; investissements chinois, etc. La synthèse se rapprocherait donc de *Gallup*, avec des opinions très favorables en Afrique, mitigées en Amérique latine, faibles en Asie et dans l'Océanie, hostiles dans les pays occidentaux et au Japon.

Finalement, quelques recherches scientifiques ont été menées sur ces perceptions internationales inhérentes aux nouvelles routes de la soie, telle que

celle d'Alicia Garcia-Herrero et Jianwei Xu (2019) qui s'appuie en réalité sur une base de données, la *Global Database of Events, Language and Tone* (GDELT). Premier enseignement, peu de différences semble-t-il entre les pays membres et non-membres du projet. De nouveau, l'Afrique (avec l'Asie centrale) est présentée comme la région possédant le meilleur *a priori* du projet chinois, alors que l'ALC est avant-dernière, entre l'Amérique du Nord et l'Asie du Sud.

***

La conclusion à laquelle nous parvenons aisément est la suivante : ces sondages réalisés par des États-uniens, souvent depuis les États-Unis et au sein d'organismes éponymes ne permettent pas réellement d'analyser les perceptions populaires ayant trait à la Chine et à son projet. Selon ce postulat, seules les études de terrain et la démarche géopolitique pourvoient à apporter des réponses croisées, structurées, qui ne schématisent ni les présences chinoises liées aux nouvelles routes de la soie, ni les représentations enclines à les (dé)valoriser. Au sein des régions abordées, les projets d'infrastructures financés et bâtis par des acteurs chinois peuvent être contestés en raison d'atteintes à l'environnement, de conflits d'usage, d'endettement ou finalement du fait de leur viabilité/légitimité. De telle manière qu'il semble nécessaire de rappeler que les financements chinois sont avant tout adossés à des projets africains ou latino-américains, d'échelles locale, nationale comme régionale, et que les prêts ou contrats afférents ne sont que le résultat de négociations ou de rapports – déséquilibrés certes – entre ces capitales et Pékin. De fait, il est ainsi tout autant nécessaire d'affirmer que la Chine et ses acteurs économiques n'imposent rien *a priori*, mais proposent et sont choisis par les acteurs politiques locaux, ce qui permet de déconstruire toute essentialisation des présences chinoises sur le continent, et à l'avenant tout « modèle » ou « voie » de développement chinois proposés – imposés pour certains – à l'Afrique et à l'Amérique latine.

Références

Aurégan, X. (2022). Les contributions de la Chine au financement et à la réalisation des infrastructures en Afrique, *Mondes en développement*, vol. 50, n° 197.

Aurégan, X. (2021). L'Afrique au temps du Covid-19 et de la route sanitaire de la soie : un relai géopolitique extraterritorial pour la Chine, *Hérodote*, vol. 4(*183*), pp. 99-116.

Aurégan, X. et S. Wintgens (2020). Les dynamiques de la Chine en Afrique et en Amérique latine. *Démocratie*, 5, 10-12. Repéré à http://www.revue-democratie.be/images/articles-en-pdf/numeros_complets/DEMO05_COMPLET.pdf

Aurégan, X. et S. Wintgens (dir.). (2019). *Les dynamiques de la Chine en Afrique et en Amérique latine – Enjeux, défis et perspectives*. Louvain-la-Neuve : Academia.

Gallup (2019a). *China's Leadership Gains Global Admirers*. Repéré à https://news.gallup.com/poll/247196/china-leadership-gains-global-admirers.aspx

Gallup (2019b). *Rating World Leaders – The U.S. vs. Germany, China and Russia*. Repéré à https://www.gallup.com/analytics/247040/rating-world-leaders-2019.aspx?thank-you-report-form=1

Garcia-Herrero, A. et J. Xu (2019). *Countries' Perceptions of China's Belt and Road initiative: A Big Data Analysis*, Working Paper, n° 1, Bruegel. Repéré à https://www.bruegel.org/wp-content/uploads/2019/02/WP-2019-01final.pdf

Pew Research Center (2019). People around the globe are divided in their opinions of China. Repéré à https://www.pewresearch.org/fact-tank/2019/12/05/people-around-the-globe-are-divided-in-their-opinions-of-china/

Kaliningrad, bastion militaire russe face à l'OTAN

Frank TETART
Docteur en géopolitique et diplômé en relations internationales, enseignant dans le secondaire et à l'Université Paris 1 ainsi qu'à l'ENSTA Bretagne. Il est co-auteur de l'émission « Le Dessous des Cartes » et de l'*Atlas du Dessous des Cartes, le monde mis à nu* (éditions Tallandier)

Avec le déclenchement de la guerre en Ukraine par la Russie, l'enclave russe de Kaliningrad voit son rôle de bastion militaire qu'elle jouait pendant la guerre froide renforcé. Elle est même au cœur de la « guerre hybride », outil de défense que la Russie utilise désormais face à l'OTAN.

Une enclave stratégique

Dès son origine en 1946, Kaliningrad est un bastion militaire. De fait, si Staline a demandé dès 1943, lors de la conférence de Téhéran avec les alliés, l'annexion de la partie nord de la Prusse-Orientale par l'URSS, c'est parce qu'il connaît l'atout stratégique que représentent les ports de Königsberg et Pillau (l'actuel Baltiisk) : ils sont libres de glaces toute l'année, à la différence de Leningrad et de Kronstadt. L'ancien territoire allemand, d'une superficie de 15 000 km2, est alors immédiatement transformé en une zone militaire renommée en juillet 1946 Kaliningrad, tout comme sa capitale Königsberg, en l'honneur de Mikhaël Kalinine, président du Soviet suprême décédé quelques semaines auparavant. Il est dès lors interdit aux étrangers. Les populations allemandes demeurées après l'assaut soviétique de 1945 sont expulsées en totalité à l'automne 1948.

L'objectif stratégique assigné à Kaliningrad est alors le contrôle de la nouvelle zone de domination soviétique en Europe centrale, en particulier la Pologne et les États baltes, réintégrés de force dans l'Empire soviétique à la faveur de la guerre. Avec la guerre froide, la mer Baltique devient un lieu de rivalité Est/Ouest et Kaliningrad se transforme en avant-poste soviétique. Prenant dès lors un rôle défensif face à une éventuelle attaque des forces de l'OTAN, le territoire dans son entier est organisé à cette fin. Dans le cadre de la spécialisation économique de l'URSS, Kaliningrad développe en priorité les secteurs militaires, le complexe militaro-industriel et la construction navale. Même si la population majoritaire à Kaliningrad reste « civile », ses liens familiaux, professionnels avec les militaires contribuent à l'émergence d'une mentalité militaire dans l'ensemble de la région.

Avec l'éclatement de l'Union soviétique fin 1991, Kaliningrad demeure le quartier général de la Flotte de la Baltique. Toutefois, la concentration sur ce petit territoire de cet important potentiel militaire suscite des inquiétudes chez les voisins directs de l'enclave et du pourtour de la Baltique. La définition par la Russie en 1992 d'un « étranger proche », une zone d'intérêts vitaux couvrant l'ancien espace soviétique, complique les négociations autour du retrait des troupes russo-soviétiques d'Estonie et de Lettonie, et ce d'autant que d'importantes minorités russes, représentant en 1991 respectivement 38% et 48% de la population totale de ces deux États y vivent[12]. On craint alors en effet que cette présence russe, en particulier dans les régions frontalières, ne serve d'instrument d'aspirations séparatistes et aiguise les tensions avec Moscou.

Le retrait de l'Armée rouge qui est définitif en 1993 pour la Lituanie et à l'été 1994 pour les deux autres pays baltes entraîne deux conséquences pour la région de Kaliningrad. D'une part, l'enclave prend la relève de toutes les bases perdues dans la région. D'autre part, elle sert de zone d'accueil aux forces armées qui se retirent de l'ancienne zone d'influence soviétique en Europe centrale et orientale (Allemagne de l'Est, Pologne et pays baltes).

Pour la Pologne, l'accroissement de la présence militaire à Kaliningrad est perçu comme une menace, alors qu'elle est confrontée à de grosses difficultés pour compenser, avec la dissolution du Pacte de Varsovie, la perte d'un système de défense aérienne

[12] Susanne Nies, Les Etats baltes, une longue dissidence, Payot, 2004.

intégré. Le nombre de soldats stationnés à Kaliningrad est presque équivalent aux effectifs de l'armée polonaise (220 000 hommes). La Pologne demeure extrêmement méfiante à l'égard de la Russie et cette frontière « surmilitarisée » longue de près de 200 kilomètres. De leur côté, les pays baltes ont le sentiment d'être pris en tenaille entre d'un côté Kaliningrad et de l'autre la Biélorussie, qui est intégrée militairement à la Russie depuis 1994.

En 1997, le ministre de la Défense russe, Igor Sergeev, annonce une réduction unilatérale des forces terrestres et navales dans le district Nord-Ouest de la Russie, en évoquant une amélioration de la sécurité dans la région, et le district militaire de Kaliningrad est placé sous l'autorité du district de Leningrad[13]. Les forces militaires déployées à Kaliningrad passent à 30 000 à la fin des années 1990 pour atteindre en 2002, quelque 10 000 hommes[14]. Pour Moscou, le rôle de Kaliningrad reste avant tout défensif, mais répond aussi à des objectifs économiques, comme l'énonce la doctrine de la Fédération de Russie pour la Marine jusqu'à 2010, approuvée par le Président Poutine en juillet 2001. Cette doctrine met en effet l'accent sur les intérêts économiques et civils dans la « mer mondiale », et érige en priorités, bien avant les missions militaires, le développement des infrastructures portuaires et la modernisation de la flotte de commerce, la coopération économique avec les États riverains de la Baltique ainsi que le marquage de la souveraineté maritime. La forte militarisation de la région est de moins en moins conciliable avec le projet destiné à transformer Kaliningrad en un « Hong-Kong de la Baltique », la première étape du projet passant par la mise en place en 1993 de la zone économique spéciale Yantar[15].

Kaliningrad, un levier russe face à l'expansion de l'OTAN

Or au début des années 2000, les perspectives d'élargissement de l'Union européenne et de l'OTAN, notamment aux trois États baltes, avalisent un recul de l'influence russe dans la région baltique. Pour Moscou, voir ces anciennes républiques de l'Union soviétique rejoindre l'ancien bloc ennemi affecte le prestige et la puissance de la Russie. Elle fait craindre même à l'armée russe, en raison de leur proximité avec des territoires russes considérés comme stratégiques, que l'OTAN n'y installe des points d'appui militaires, voire n'y stationne des armes nucléaires, sans même évoquer la crainte de voir Kaliningrad encerclé par des pays membres de l'OTAN.

Moscou joue dès lors la « carte Kaliningrad »[16]. En 1999, Kaliningrad devient ainsi le terrain de la plus importante manœuvre militaire russe organisée depuis la chute de l'URSS, appelée, de manière très explicite, « Zapad 99 », c'est-à-dire « Ouest 99 ». Le scénario des exercices repose sur l'attaque militaire de Kaliningrad par l'OTAN, sans que les États riverains en soient informés.

L'annonce en 2007 de l'installation par les Américains d'éléments de leur bouclier antimissile en Europe centrale, à savoir un radar de détection en République Tchèque et dix intercepteurs de missiles en Pologne, suscite ensuite l'*ire* de Moscou. Le Kremlin réagit immédiatement en déclarant que ces deux pays pourraient devenir la cible des forces armées russes[17]. Puis le président Poutine annonce le déploiement des nouveaux missiles russes Iskander (SS26), vecteur possible de tête nucléaire, dans l'enclave russe de Kaliningrad, c'est-à-dire aux frontières de la Pologne.

Toutefois, Moscou ne met à exécution sa menace qu'au profit de la crise ukrainienne de 2013-2014. En Europe, les objectifs de la Russie sont d'abord de nature géopolitique, puisqu'ils visent à réaffirmer son rôle central dans les affaires du continent. Moscou cherche ainsi à peser sur la gouvernance politique comme sécuritaire et donc à se voir reconnaître un droit de regard sur son voisinage occidental. Or depuis la chute du mur de Berlin en 1989, les Russes ont le sentiment que « les Européens de l'Est n'ont fait que déplacer le rideau de fer »[18] avec l'adhésion des ex-pays de l'Est à partir de 2004 à l'Union européenne et surtout à l'OTAN. Or l'OTAN, alliance ennemie pendant la guerre froide, aurait dû, selon les

[13] Alors que Leningrad est redevenue Saint-Pétersbourg, la région attenante a conservé la référence à Lénine (*Leningradskaïa Oblast*), tout comme le district militaire dont dépend Saint-Pétersbourg.

[14] Chiffres publiés dans leur publication annuelle *The Military Balance* (1993 à 2002).

[15] Yantar signifie en russe ambre, dont Kaliningrad détient 90 % des réserves mondiales.

[16] L'expression est de Richard Krickus, *op. cit*.

[17] « Europe's space wars », *The Economist*, 23 février 2007.

[18] *Hélène Carrère* d'*Encausse*, *La Russie entre deux mondes*, Fayard, Paris, 2011.

décideurs russes, disparaître en même temps que le Pacte de Varsovie, dissout en 1991.

L'intégration en 2007 des pays baltes a porté l'OTAN aux frontières russes, ravivant un sentiment d'encerclement contre lequel la Russie a historiquement constamment lutté, notamment par la mise en place d'un glacis tant à l'époque des tsars que de l'Union soviétique. En août 2008, la Russie réagit par les armes à ce qu'elle perçoit comme une menace à ses frontières en Géorgie. Cette opération a été ordonnée deux mois après la décision de l'OTAN d'intégrer l'Ukraine et la Géorgie. Même si la mise en œuvre du processus d'adhésion avait été repoussée *sine die*, cet élargissement de l'Alliance atlantique avait été perçu par Moscou comme un verrouillage de sa frontière sud.

À partir de 2009, une lutte d'influence s'engage entre Bruxelles et Moscou dans l'isthme Baltique-mer Noire. D'un côté, l'Union européenne propose un Partenariat oriental aux pays de cette zone, de l'autre, la Russie leur offre l'adhésion ou l'association à l'Union eurasiatique, une zone de libre-échange en gestation. L'Ukraine devient en 2013 l'enjeu principal de cette rivalité. Dans ce contexte de montée des tensions, l'heure n'est plus à la coopération avec l'Europe au sujet de Kaliningrad, mais à la confrontation. De fait, l'OTAN procède à des déploiements de forces dans les pays baltes, en réponse à une présence de plus en plus forte des forces russes en Baltique, puis au déploiement des missiles russes Iskander à Kaliningrad en octobre 2016.

Selon les autorités russes, ces missiles sont censés remplacer les missiles balistiques tactiques à courte portée Tochka (SS21 selon la terminologie de l'OTAN). Toutefois, avec une portée doublée (500 km environ), ces nouveaux missiles sont par conséquent susceptibles de menacer l'ensemble des pays voisins du pourtour baltique. Ce déploiement est complété par le positionnement à Kaliningrad de missiles S-400, un système de défense antiaérienne et antimissile qui couvre la Lituanie et une bonne partie de la Pologne et de la Lettonie[19]. Sont également positionnées à Kaliningrad des batteries côtières dotées de missiles SSC-5 Bastion, supersoniques, de 300 km de portée, et des missiles SSC-1 Sepal, de 450 km de portée. Au total, les effectifs militaires déployés dans l'enclave sont estimés à 30 000 hommes[20]. Ce déploiement permet de sanctuariser le territoire de Kaliningrad selon une logique A2/AD (Anti Access/Area Denial) ayant pour objectif de tenir l'OTAN à distance de la région de la mer Baltique.

Ce déploiement contribue à provoquer un vent de panique chez les pays voisins de l'oblast et à élever le sentiment d'insécurité et le niveau d'instabilité régionale. Ce sentiment est encore renforcé par l'exercice militaire russe Zapad-2017 qui mobilise selon les autorités russes 12 700 soldats (selon l'OTAN près de 40 000) pour tester les capacités militaires A2/AD, y compris par un blocus maritime. Ces manœuvres démontrent la détermination russe à intensifier son potentiel militaire sur son flanc ouest, rendu possible par l'abrogation par la Russie du Traité sur les forces conventionnelles en Europe.

Dans ce contexte, Kaliningrad revient au centre des tensions régionales de l'espace baltique. Depuis l'annexion de la Crimée, les États baltes craignent en effet que Moscou ne lance à leur encontre une stratégie de déstabilisation sur le même modèle qu'en Ukraine, s'appuyant sur la manipulation de leurs minorités russophones, avant de les envahir depuis l'enclave de Kaliningrad. Une série de jeu de guerre simulant une invasion des États baltes par la Russie par des chercheurs de la Rand Corporation[21] a montré que Riga ou Tallinn seraient encerclées par les forces russes en moins de 60 heures.

Kaliningrad, instrument stratégique de guerre hybride ?

Depuis le troisième mandat de Vladimir Poutine (2012-2018) et l'affichage de nouvelles ambitions sur la scène internationale, la Russie a un recours limité à l'usage de sa force militaire, à l'exception de la Syrie, privilégiant les outils de la guerre hybride, comme la propagande et la guerre de l'information,

[19] Philippe Langoit, « La *joint forcible entry frace* à la trouée de Suwalki », *DSI hors-série, n°48, juin-juillet 2014*, www.defense24.news/2018/07/04/la-joint-forcible-entry-face-a-la-trouee-de-suwalki/

[20] Estimation de l'auteur, basée sur les chiffres d'Ingmar Oldberg, chercheur au Swedish Institute of International Affairs, prenant en compte l'ensemble des forces de sécurité et les annonces faites par Moscou de renforcer sa présence militaire à Kaliningrad.

[21] https://www.rand.org/pubs/research_reports/RR1253.html

le cyberespace, des fins de sabotage et de déstabilisation. Cette notion de « guerre hybride » (*hybrid warfare*) popularisée au milieu des années 2000 par deux officiers du corps des *Marines* – le général James Mattis et le colonel Frank Hoffman – décrit un type de guerre alliant guerres conventionnelle et non conventionnelle, guerres régulière et irrégulière, et surtout guerre de l'information et cyberguerre. Dans la pratique, une menace peut être considérée comme hybride dès lors qu'elle s'inscrit dans plusieurs dimensions et types de guerre différents[22]. Dans ce contexte, la sanctuarisation de Kaliningrad par sa militarisation accrue apparaît comme un moyen de pression contre ses voisins et partenaires européens, et plus généralement occidentaux, notamment à travers les instances euroatlantiques de l'Union européenne et de l'Otan.

Depuis l'annexion de la Crimée en 2014, l'enclave remilitarisée est devenue un pion stratégique dans la guerre hybride que mène Moscou avec les pays de l'OTAN. Elle accroît à la fois le sentiment de vulnérabilité des pays voisins confrontés à un nouveau rapport de force défavorable et favorise l'escalade des tensions par une guerre de l'information et de la propagande.

Depuis les exercices Zapad-2017, la trouée de Suwalki, cette bande terrestre longue de 65 km, qui forme la frontière entre la Pologne et la Lituanie et donc le lien entre les pays baltes et le reste des membres de l'OTAN, est perçue par l'Alliance comme particulièrement vulnérable[23]. Baltes comme Polonais considèrent dès lors la Russie comme la principale menace à la sécurité régionale.

La remilitarisation de l'oblast de Kaliningrad s'accompagne à l'échelle de la Russie d'une modernisation de l'appareil militaire[24]. Depuis son élection de 2008, le président Poutine s'est attaché à restaurer la crédibilité de la puissance militaire russe sur la scène internationale. Celle-ci passe par un effort budgétaire important, qui a permis un rééquipement massif des forces armées, une modernisation de l'arsenal nucléaire, une restructuration profonde des forces conventionnelles et une professionnalisation des personnels. Au niveau de la doctrine maritime, celle de 2015 fait de la prévention de l'élargissement à l'Est de l'OTAN une priorité absolue. Kaliningrad est redevenue non seulement le siège de la Flotte de la Baltique mais également une composante significative de la défense anti-missile balistique russe. Quelque 10 000 hommes sont déployés au sein de trois brigades de combat entièrement équipées : une brigade d'infanterie de marine d'élite et deux brigades motorisées.

En temps de paix comme de crise, l'enclave sert d'avant-poste de surveillance et de recueil de renseignements. Elle participe à la sécurité des routes maritimes, des gazoducs et câbles sous-marins, tout en jouant le rôle de plateforme de dissuasion stratégique, de coercition et d'endiguement, grâce au déploiement depuis 2016 de drones et de missiles de différents types.

En cas de conflit, les forces armées basées à Kaliningrad interviendraient pour la défense aérienne avancée du territoire russe et la désactivation des infrastructures menaçantes de l'OTAN, par exemple le site de défense antimissile basé en Pologne. Elles pourraient en outre empêcher l'accès de la mer Baltique aux forces des pays membres de l'OTAN. Selon certaines sources, Kaliningrad hébergerait même des groupes de *hackers* capables de lancer une guerre de l'information ou procéder à des sabotages de réseaux.

Alors que la fin de la guerre froide laissait accroire que le sort de Kaliningrad serait celui d'un territoire prospère et profitant de la dynamique de l'élargissement de l'Union européenne à l'Est, force est de constater que l'enclave russe est redevenue un avant-poste militaire, élément incontournable de la sécurité et de la stratégie militaire russes en Baltique et face à la poussée de l'OTAN vers l'Est.

[22] « La guerre hybride existe-elle déjà ? », *Revue de l'Otan magazine*, 2015, consulté en juillet 2019, www.nato.int/docu/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/FR/index.htm

[23] Céline Bayou, « Tensions sécuritaires dans la région baltique : que reste-t-il de l'équilibre nordique ? », *Questions internationales*, n°90, mars-avril 2018.

[24] Isabelle Facon, « La nouvelle *armée russe* », Questions internationales, n°101, janvier-février 2020.

La guerre du Haut-Karabagh et la remise en question des alliances régionales

Pierre ANDRIEU
Ancien ambassadeur, ancien co-président français du Groupe de Minsk de l'Organisation pour la sécurité et la coopération en Europe (OSCE), enseigne la politique étrangère russe à Sciences Po

L'arrière-plan historique

Le Caucase, massif montagneux le plus élevé en Europe (le mont Elbrouz culmine à 5642 m), est un kaléidoscope ethnique, linguistique et religieux. Il a été également un important obstacle naturel que la Russie a franchi dès le XVIIè siècle pour conquérir les territoires stratégiques en Transcaucasie, relevant alors de l'Empire perse, afin d'accéder aux « mers chaudes » et le Golfe persique.

Par les traités de Golestan en 1813 et de Tourmanchaï en 1828, la Perse a abandonné à la Russie toutes ses possessions au nord de l'Araxe, notamment les khanats situés le long et dans l'arrière-pays de la Caspienne, dont les khanats de Bakou, de Karabagh, de Nakhichevan et de Erevan, vassaux de la dynastie Kadjar. Ceux-ci ont été annexés par l'Empire russe et redécoupés en *gubernia,* dont certains ont été repeuplées d'Arméniens chrétiens.

L'instauration du pouvoir soviétique dans les années 20 du siècle dernier a bouleversé à nouveau la situation dans le Sud-Caucase. En application de la « politique soviétique des nationalités », théorisée par Staline dès 1913, toute nationalité devait être dotée d'un territoire et d'une langue distincts. Dans cette région, l'URSS a créé les trois Républiques socialistes soviétiques (RSS) de Géorgie, d'Arménie et d'Azerbaïdjan. Comme pour d'autres républiques soviétiques, y ont été intégrées des régions autonomes, dont l'ethnie était différente de l'ethnie majoritaire. Ainsi la région autonome du Haut-Karabagh, bien que peuplée en majorité d'Arméniens, a été englobée dans la RSS d'Azerbaïdjan[25].

Dès la fin de l'URSS, les limites administratives qui divisaient ces entités soviétiques sont devenues des frontières internationales, très vite contestées par les pays devenus indépendants. En septembre 1991, trois mois avant la dissolution de l'URSS, le Haut-Karabagh a proclamé son indépendance et sorti unilatéralement de l'Azerbaïdjan. La guerre qui s'en est suivie entre ce pays et l'Arménie s'est conclue par une victoire de celle-ci, dont les armées ont occupé, outre le Haut-Karabagh, sept districts azerbaïdjanais le ceinturant. La disposition des forces a été figée par le cessez-le-feu de mai 1994 signé à Moscou.

D'un *statu quo* à l'autre, ou comment l'instabilité a perduré

Le *statu quo* était inadmissible pour l'Azerbaïdjan, qui était décidé à le remettre en question par tous les moyens. Vaincu mais revanchiste, ce pays a engagé un vaste programme de modernisation de son outil militaire. Disposant d'un budget de défense supérieur, à lui seul, au budget total de l'État arménien, Bakou aurait dépensé plus de 24 milliards de dollars entre 2009 et 2018 pour financer son réarmement et améliorer la formation de ses armées, avec l'assistance de la Turquie.

Les Arméniens, au contraire, forts de leur victoire en 1994 et se pensant inexpugnables, ont refusé toute concession sur les plans politique et territorial et, sur le plan militaire, n'ont modernisé ni leur tactique ni leurs armements.

Profitant de circonstances internationales favorables (élections américaines, pandémie et crise économique en Europe), l'Azerbaïdjan a lancé le 27 septembre 2020 son offensive, surpris les Arméniens en les contournant par le sud, le long de la frontière avec l'Iran, pour ensuite les déloger de leurs réduits montagneux. La Turquie, qui a toujours soutenu « ses frères d'arme azerbaïdjanais », notamment sur le plan militaire (fourniture des drones qui ont fait la différence sur le terrain, formation et envoi de mercenaires de Syrie), a joué un rôle crucial dans cette victoire.

[25] « La guerre Arménie-Azerbaïdjan » selon P. Andrieu, EuroAsia Prospective 04/10/2020.

L'écrasante victoire militaire de l'Azerbaïdjan a également signifié une défaite de la diplomatie déployée pendant plusieurs années par le groupe de Minsk, co-présidé par la Russie, la France et les États-Unis. Se heurtant à la mauvaise volonté des deux parties, les co-présidents n'ont jamais pu surmonter leurs divergences inconciliables tout au long des négociations.

Sifflant « la fin de la partie », les Russes ont stoppé les Azerbaïdjanais, qui auraient pu sans peine atteindre le territoire arménien lui-même, et ont imposé aux deux protagonistes la signature, le 10 novembre 2020, d'un cessez-le-feu, en écartant le groupe de Minsk. Ce texte a entériné la reconquête par les Azerbaïdjanais des sept districts occupés par les Arméniens mais aussi l'occupation des deux tiers du territoire du Haut-Karabagh, dont la ville de Choucha, emblématique pour les deux pays.
Le cessez-le-feu a permis le déploiement de près de 2000 soldats russes chargés de garantir son application. Prenant acte du rôle important de la Turquie dans le conflit, les Russes ont concédé à ce pays la présence de quelques soldats au sein d'un « Centre de contrôle du cessez-le-feu » dont les inspections sont censées se dérouler uniquement par drones, à l'exclusion de toute présence sur le terrain[26].

Ce conflit a coûté très cher en termes humain et matériel. Le nombre de victimes des deux côtés atteindrait 6500 tués dont 150 civils. S'agissant des pertes matérielles, elles auraient été six fois plus importantes pour l'Arménie que pour l'Azerbaïdjan. L'armée de ce pays aurait détruit pour 4,8Mds$ d'équipements arméniens, dont une partie a été exhibée à Bakou à l'occasion de « la parade de la victoire » en présence des présidents azerbaïdjanais et turc.

Mais le nouveau *statu quo* issu du cessez-le-feu du 10 novembre 2020 ne paraît pas plus stable que celui de 1994. Les questions politiques, notamment le statut de ce qui reste du Haut-Karabagh et les délimitations frontalières, ne sont pas réglées. Et, contrairement à la situation précédente, la Russie se trouve directement engagée sur le terrain, en contact avec les protagonistes, ce qui lui ferait porter la responsabilité des risques éventuels.

Les alliances de 1994 n'ont qu'imparfaitement fonctionné en 2020

Comme en 1994, la Russie est apparue comme le grand vainqueur diplomatique de cette guerre. Renforçant son alliance avec l'Arménie, dont elle continue à assurer la sécurité en dernier ressort, elle conserve ses bonnes relations avec l'Azerbaïdjan, qu'elle approvisionne toujours en armements et dont le régime continue à bénéficier du soutien du Kremlin. Le cessez-le-feu a également renforcé sa présence militaire dans la région, ses 2000 soldats déployés dans le Haut-Karabagh, en application du cessez-le-feu, venant s'ajouter à ceux stationnés dans sa base militaire à Gyumri en Arménie, à ses gardes-frontières qui veillent sur les frontières extérieures de ce pays, ainsi qu'à ses troupes en Géorgie (Abkhazie et Ossétie du Sud).

Dans leur politique d'équilibre subtil entre l'Arménie et l'Azerbaïdjan, les Russes avantagent tantôt l'une tantôt l'autre pays, au gré de leurs intérêts. À l'exemple de ce qui s'est passé pendant la guerre d'avril 2016, le soupçon a affleuré à Erevan que Moscou n'aurait pas su, ou voulu, prévenir l'offensive azerbaïdjanaise de septembre dernier afin de donner une « leçon » au premier ministre libéral Pachinian et lui rappeler que la sécurité de son pays continuait de dépendre exclusivement de la Russie.

Ainsi, l'OSTC (Organisation du Traité de sécurité collective), cette alliance militaire créée en 2002 qui rassemble autour de la Russie, l'Arménie, la Biélorussie, le Kazakhstan, le Kirghizstan et le Tadjikistan, a-t-elle refusé de faire jouer la clause de sécurité collective, comme l'avait demandé Erevan. Elle a argué de manière quelque peu fallacieuse que c'était le Haut-Karabagh, et non le territoire national de l'Arménie, qui était attaqué.

Nouvelle configuration géostratégique et évolution des alliances

La « guerre des Quarante-quatre jours » a bouleversé la situation géostratégique dans le Caucase du Sud tout en faisant bouger les alliances existantes.

Prenat acte de l'entrée fracassante de la Turquie ans le Sud-Caucase, la Russie a réussi à l'encadrer dans son « partenariat conflictuel » avec ce pays. Moscou

[26] « Les bouleversements géostratégiques dans le Sud-Caucase » P. Andrieu, Télos 16 avril 2021.

et Ankara s'entendent pour « gérer » le conflit du Haut-Karabagh sans interférence des Occidentaux, sur le « modèle » syrien du « processus d'Astana » signé en 2017 entre la Russie, la Turquie et l'Iran.

Mais Ankara a d'autres agendas importants dans la région : diplomatiques, avec le renforcement de son alliance avec Bakou, par la signature le 15 juin 2021 de la « Déclaration de Choucha »; connectivité, avec la réouverture des voies de transport fermées depuis 1991, notamment celle qui relie l'Azerbaïdjan à son exclave de Nakhitchevan et, au-delà, à la Turquie et à la Russie, en traversant le territoire arménien de Syunik (Zanguezour), que Bakou a du reste a menacé d'annexer [27]. Le président Erdogan a même proposé de créer une plateforme à six (les trois pays du Sud-Caucase et ses trois voisins : Iran, Russie et Iran)[28] pour discuter de cette question, ce qui aurait pour effet de renouer le dialogue avec l'Arménie. Projet de transport du gaz turkmène à travers la mer Caspienne et l'Azerbaïdjan, pour ensuite l'acheminer en Europe[29]. Enfin, début de réalisation du rêve pantouranien visant à établir des contacts directs avec l'Asie centrale turcique.

L'Iran, enfin, semble être le grand perdant de cette guerre et s'est avéré incapable de retrouver son influence dans une région où pourtant il était dominant jusqu'au début du XIXè siècle[30].

En outre, ce pays apprécie peu le renforcement de la Turquie en Azerbaïdjan alors que la présence dans sa partie septentrionale d'une très forte communauté azérie renforce la méfiance et les soupçons de séparatisme que Téhéran nourrit à l'égard de Bakou. Par ailleurs, la réouverture des voies de communication pourrait empêcher l'accès de l'Iran vers son allié arménien et, au-delà, vers le Nord. Enfin, sur le plan géostratégique, Israël, son ennemi juré, qui a également fourni quantité de drones à l'Azerbaïdjan, voit ses positions considérablement renforcées le long de sa frontière avec l'Azerbaïdjan.

Pourtant, si l'Iran a perdu une bataille, il n'a pas perdu la guerre. En réponse à des manœuvres organisées le 12 septembre 2021 par l'Azerbaïdjan, la Turquie et le Pakistan, l'Iran a mené en miroir des manœuvres importantes à titre d'avertissement, qui semble avoir été entendu à Bakou[31].

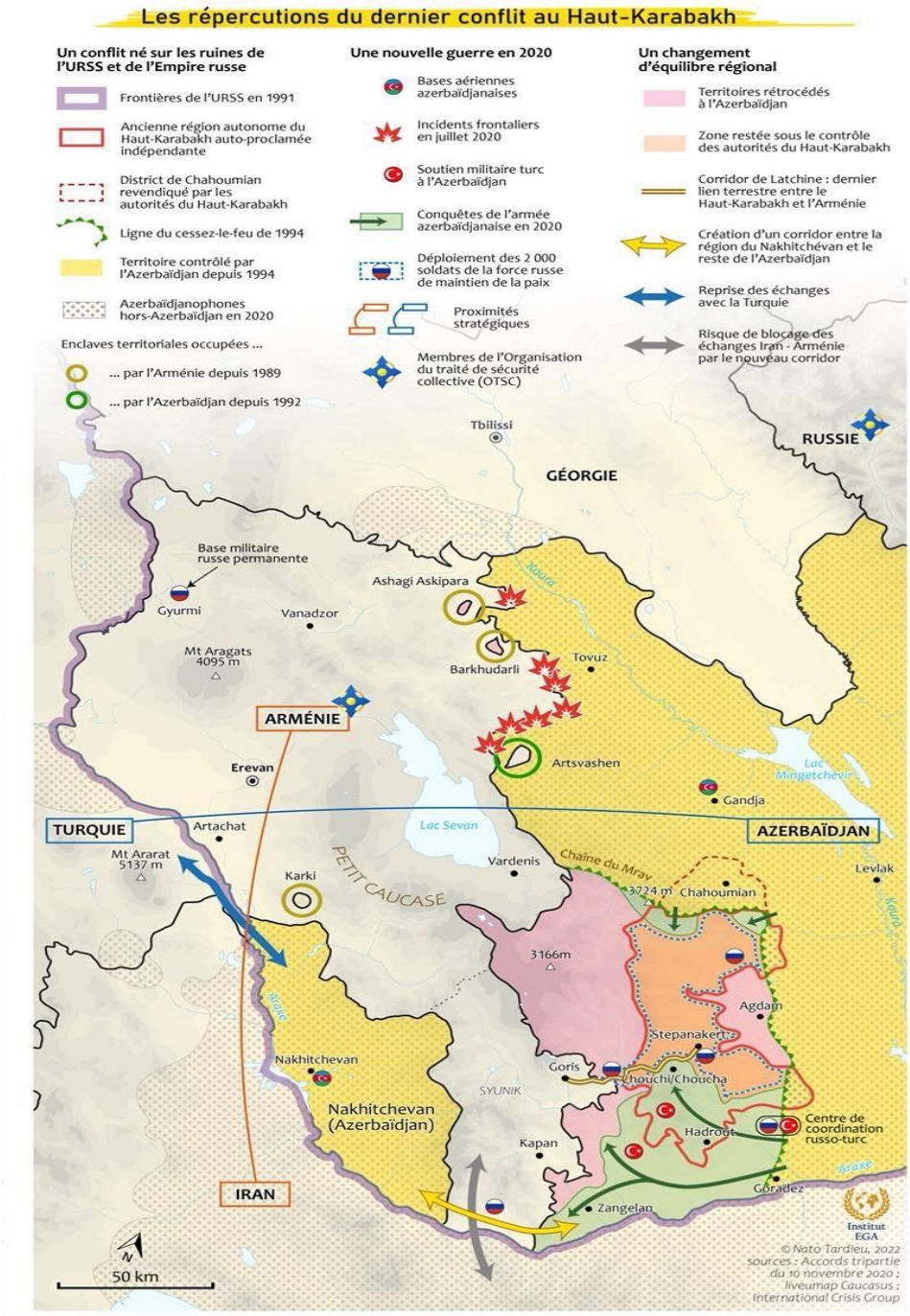
***

La Russie a puissamment « réinvesti » le Sud-Caucase à l'occasion de la « guerre des quarante-quatre jours ». Mais, là comme dans d'autres parties de l'espace ex-soviétique, Moscou a été obligé « recalibrer » sa posture[32]. N'ayant plus les moyens d'assumer sa position hégémonique, elle se voit obligée de prendre de plus en plus en compte la situation intérieure dans les trois républiques sud-caucasiennes, sur laquelle elle n'a plus vraiment la main, ainsi que la présence en Transcaucasie d'autres puissances, comme la Turquie et sans doute l'Iran, voire la Chine en fonction de la progression de son projet de la « Belt and Road Initiative (BRI) »[33].

S'agissant des Occidentaux, les États-Unis de Biden ont certes exprimé leur volonté de revenir dans la région mais ne semblent pas encore prêts à y mettre les moyens, mobilisés par leur obsession chinoise. Quant à l'UE, sa volonté exprimée de devenir une puissance « géostratégique » dans une zone qu'elle a intégrée dans sa politique de Partenariat oriental l'amène tout naturellement à tenter d'y renforcer sa présence pour participer au règlement politique et contribuer à la reconstruction après-guerre. Un Sommet entre Charles Michel, le Président du Conseil européen, et les deux dirigeants arménien et azerbaïdjanais, a été organisé le 15 décembre 2021 à Bruxelles en marge du Sommet du Partenariat

[27] "In the South Caucasus, Can New Trade Routes Help Overcome a Geography of Conflict?" Thomas de Waal, Carnegie Europe, Novembre 2021.
[28] « Caucase du Sud : le grand chantier de l'ouverture des voies de communication », Benoît Filou, « Les clés du Moyen-Orient », 30 janvier 2022.
[29] « Iran-Azerbaïdjan : que se cache-t-il derrière les dernières tensions ? », Middle East Eye, octobre 2021.
[30] « Haut-Karabakh : un échec pour la République islamique d'Iran ? » Mohammad-Reza Djalili, Clément Therme, Centre de recherches internationales (CERI) à Sciences-Po Paris.
[31] « Turkey, Nagorno-Karabakh and the Central Asian Nexus" Eugene Chausovsky, 19 mars 2021.
[32] "Russia Is Worried About Challenges in the Caucasus, The Nagorno-Karabakh war's aftermath is still impacting Moscow's plans", Eugene Chausovsky, Foreign Affairs, 14 janvier 2022.
[33] Pierre Andrieu, « L'impact de la pandémie sur les équilibres internationaux au sein de l'Eurasie », in A. de Tinguy (dir.), Regards sur l'Eurasie. L'année politique 2020/Les Etudes du CERI, n° 254-255, février 2021 [en ligne : www.sciencespo.fr/ceri/fr/papier/etude].

oriental. Bien que cette réunion ait reçu l'assentiment de Moscou et de Bakou, l'UE ne semble pas encore en mesure de jouer le rôle qui lui revient dans cette région.



Vers une hausse d'activité de l'OTAN au Moyen-Orient ?

Agnès LEVALLOIS
Maîtresse de recherche à la Fondation pour la recherche stratégique (FRS)

Si lors de sa création, la première préoccupation de l'Alliance en matière de sécurité était la stabilisation de l'Europe centrale et orientale, celle-ci doit, depuis les années 1990, relever les défis en provenance de la rive sud de la Méditerranée. Cela s'est traduit par un nouveau concept stratégique approuvé au sommet de Rome en 1991 et révisé lors du sommet de Washington en 1999 d'élargissement et d'engagement dans la gestion des crises hors de son territoire traditionnel en menant une politique de coopération au Moyen-Orient avec plusieurs pays non-membres. Depuis sa création, l'OTAN a noué des relations avec les forces armées du Moyen-Orient, la Turquie occupant une place particulière et incontournable car elle en est membre depuis 1952.

À partir de 1994, l'Alliance met en place un dispositif en Méditerranée connu sous l'appellation de « Dialogue méditerranéen » (DM). Il instaure une coopération avec sept pays de la rive sud Méditerranée entre 1995 et 2000. Les objectifs sont de renforcer la sécurité et la stabilité régionale par une confiance mutuelle – notamment le regain de la légitimité occidentale au Moyen-Orient. Les pays sont les mêmes que pour le *MPCs* – Partenaires méditerranéens pour la coopération[34]-, la Mauritanie en plus. Ce Dialogue n'a pas eu les résultats espérés car l'Alliance est une institution peu connue par les pays de la région sans parler d'une suspicion à son égard liée à l'absence de mécanismes de dialogue et de coopération et de l'impasse dans lequel se trouve le conflit israélo-palestinien entre autres. En outre, les pays de la région préfèrent avoir des relations bilatérales avec l'Alliance ce qui rend par exemple l'organisation d'exercices militaires collectifs difficile.

Les gouvernements de la région Moyen-Orient/Afrique du Nord (particulièrement en Afrique du Nord) nourrissent toujours une grande méfiance à l'égard des activités de sécurité et de défense des pays du Nord (prenons pour exemple les Forces Eurofor, Euromarfor, ou encore la Politique Européenne de Sécurité et de Défense). L'amalgame est souvent fait entre les États-Unis et l'OTAN alors que le sentiment anti-américain répandu et la question du soutien inconditionnel à Israël limitent les possibilités de coopération avec l'Alliance[35].

En 2016, l'OTAN a commencé à appliquer une nouvelle approche à ses partenariats régionaux, appelée « projection de la stabilité ». Ce concept met l'accent sur la nécessité de stabiliser les zones d'intérêt, comme le Moyen-Orient, en aidant les partenaires régionaux à renforcer leurs capacités militaires. Depuis lors, la « projection de la stabilité » est le récit dominant de l'engagement de l'OTAN au Moyen-Orient. Il faut ajouter à cela la lutte contre le terrorisme. Il existe en effet un consensus politique entre les pays de l'OTAN à propos du djihadisme mondial lequel constitue une menace réelle et vis-à-vis duquel la négociation n'est pas une option. À ce titre, les troupes des pays de l'OTAN sont engagées contre les groupes terroristes en Syrie, au Sahel et en Afghanistan et elles ont entraîné les forces irakiennes à la demande de Bagdad pour empêcher le retour de l'État islamique (EI). Le principe du transfert d'une partie des missions menées en Irak par la coalition internationale de lutte contre l'EI vers l'Alliance a été acté lors d'une réunion à Bruxelles des ministres de la Défense de l'OTAN les 12 et 13 février 2020.

Donald Trump avait évoqué, le 9 janvier 2020, l'idée d'intégrer les pays arabes à l'Alliance transatlantique pour devenir « l'OTAN-MO » (ou le « NATO-ME » en anglais). Depuis, l'organisation a accordé le statut spécifique de *Major non-NATO ally* (« allié majeur non-membre ») à certains pays de la région Proche et Moyen-Orient : Israël, Égypte, Jordanie, Bahreïn (qui est le siège de la 5e flotte de l'US Navy), Koweït et Qatar (qui est officiellement candidat depuis 2018

[34] Les partenaires méditerranéens pour la coopération, modèle multilatéral créé en dehors de l'OTAN et développé à partir du processus d'Helsinki.

[35] Mustapha Shimi, « Peurs et malentendus : la vision du Sud », J.-F. Daguzan et R. Giradet (sous la dir.), *La Méditerranée : nouveaux défis, nouveaux risques*, Paris, Publisud, 1995 pp. 62-63.

à son intégration pleine et entière dans l'OTAN). On retrouve pour le « NATO-ME » la même hypothèque que celle pesant sur le projet inabouti de « l'OTAN arabe » intitulé *The Middle East Strategic Alliance* (MESA) destiné à constituer une alliance d'États du Moyen-Orient afin de contrecarrer ce qui est perçu comme l'expansionnisme de l'Iran dans la région[36]. Pour Trump, l'élargissement de l'OTAN au Moyen-Orient était plus motivé par des considérations financières que géopolitiques : en effet, Washington y voyait la possibilité de réduire son investissement financier induit par les engagements militaires dans le monde. Plus précisément, l'ancien président américain voulait intégrer de nouveaux riches contributeurs comme les pétromonarchies considérant que ce serait un point positif pour l'Alliance[37]. Dans le même temps, l'OTAN s'est impliquée davantage dans la région en étendant la mission d'entraînement en Irak, la faisant passer graduellement de 500 à 4000 hommes tout comme elle a contribué à la sécurité maritime des navires européens en Méditerranée en raison des activités grandissantes de la Chine.

Mais la question qui se pose est celle de l'activation de l'article 5 de la charte du traité qui stipule que si un pays de l'OTAN est victime d'une attaque armée, chaque pays membre de l'Alliance devra prendre toutes les mesures nécessaires, y compris l'emploi de la force armée, pour rétablir et assurer sa sécurité. À partir de là les pays européens ne souhaitent pas intégrer les pays du Moyen-Orient pour ne pas se retrouver exposés alors qu'il s'agit d'une zone de grande conflictualité. Le seul pays de la région dont la participation à l'OTAN est une réalité est la Turquie même si la politique d'Erdogan brouille les relations avec les États-Unis. Il n'en demeure pas moins que le risque de la sortie de la Turquie de l'organisation est quasi improbable car Ankara assure la sécurité dans la région.

Quelle est la réalité de l'engagement de l'OTAN au Moyen-Orient ?

La formation et l'entraînement militaires sont la pierre angulaire de la politique régionale de l'OTAN. Les partenaires du Moyen-Orient participent à de nombreux programmes, notamment des exercices militaires ainsi qu'à des stages opérationnels à l'École de l'OTAN en Allemagne et des stages de niveau stratégique au Collège de défense de l'OTAN en Italie. Cette dernière entité dispense un stage de coopération régionale, qui a formé à ce jour plus de 600 officiers des armées de l'OTAN et du Moyen-Orient.

La Méditerranée est confrontée à une réalité géopolitique et sociale très instable (conflit israélo-palestinien, conflit libyen, crise libanaise, Sahara occidental, etc.) qui nécessite un projet adapté et accepté par l'ensemble des parties prenantes au Nord et au Sud visant à une prospérité partagée. Pour raviver un projet méditerranéen, il faudrait donc organiser un débat entre les États du bassin pour arriver à des résultats, corriger les imperfections et adapter le cadre institutionnel du projet aux besoins d'urgence.

Si l'OTAN souhaite jouer un rôle significatif en Afrique du Nord et au Sahel, elle doit réfléchir à des moyens réalistes visant à renforcer la stabilité régionale du Sahel tout en atténuant les risques de débordement en Afrique du Nord et sur le bassin méditerranéen. Cependant, il est difficile pour l'OTAN, organisation peu légitime dans la région, de négocier avec les autorités locales afin de contribuer à cette stabilité. En d'autres termes, l'OTAN possède peu de marges de manœuvre pouvant lui permettre de mener une action concrète sur le terrain et même élargir le Dialogue méditerranéen aux pays sahéliens du G5 (Mauritanie, Burkina Faso, Mali, Niger, Tchad) alors que celui-ci n'a pas rencontré le succès espéré. La solution pourrait résider plutôt dans la coopération avec d'autres organisations internationales comme l'ONU, l'Union africaine, l'Union européenne, la CEDEAO et le G5. Dans ce cas de figure, l'OTAN pourrait soutenir l'UE et l'ONU en faisant office de centre de sécurité du Sahel, en améliorant ainsi la coordination des initiatives et en identifiant les lacunes en termes de ressources et de procédures opérationnelles[38]. Rappelons que la seule réelle implication de l'Alliance est en Libye car depuis la chute du régime en 2011, la région du Sahel a gagné en importance pour l'OTAN, le chaos dans ce pays ayant accéléré l'interconnexion entre l'Afrique du Nord et les dynamiques à l'œuvre au Sahel.

[36] Pour les Américains, l'objectif était qu'ils dirigent cette instance financée par l'Arabie saoudite et les Émirats arabes unis et que l'Egypte et la Jordanie fournissent les ressources humaines.

[37] David Rigoulet-Roze, « Pourquoi Trump veut intégrer ses alliés arabes à l'OTAN », Institut des relations internationales et stratégiques (IRIS), 25 janvier 2020.

[38] Chloé Berger, « What role for NATO in the Sahel? », NATO Defense College, 22 décembre 2021.

Le semi-échec en Afghanistan (depuis le retrait d'août 2021) pose la question du rôle de l'Alliance aujourd'hui. D'une part, depuis le sommet du Pays de Galles en 2014, l'OTAN a eu tendance à se concentrer à nouveau sur ses missions principales, tout en incluant le cyberespace dans le matériel de l'article 5. D'autre part, les tensions entre la Chine et Taïwan en 2021 ont commencé à poser la question du rôle possible de l'OTAN, le Conseil de l'Atlantique Nord ayant qualifié la Chine de « menace systémique » en juin 2021. Cependant, la région du Moyen-Orient ne semble pas être au premier plan des objectifs de l'Alliance (comprenons ici les États-Unis). Plus que jamais, les différences politiques entre les Alliés sur la vocation de l'OTAN restent la principale pierre d'achoppement à ce jour[39].

***

L'arrivée au pouvoir de Joe Biden a permis de relancer la relation transatlantique après le mandat de Trump qui n'a cessé d'inquiéter ses partenaires. La décision a rapidement été prise d'étendre la mission de l'Alliance en Irak. Mais l'opportunité de relancer le partenariat, en général et le Dialogue méditerranéen de l'OTAN en particulier, dépend de la cohérence entre les intentions réelles de l'OTAN, l'engagement des pays partenaires et les jeux de pouvoir régionaux et extra-méditerranéens, dans un contexte empreint d'incertitude et d'inquiétude. Une chose est sûre, les pays des deux rives de la Méditerranée doivent renforcer le dialogue, les échanges grâce à l'implication systématique d'universitaires et de représentants de la société civile, pour mieux se comprendre et dissiper les perceptions négatives. La mise en avant des seuls risques sécuritaires venant des pays de la rive sud de la Méditerranée ne contribue pas à l'instauration d'un dialogue constructif permettant des coopérations au service de l'ensemble des pays concernés.

[39] Delphine Deschaux-Dutard, « Afghanistan in context: a « globalization » of NATO? », Fondation pour la recherche stratégique, 23 novembre 2021.

La question de l'imputabilité de la faute et la nécessité d'un cadre juridique dans le cyberespace

Maître Cécile DOUTRIAUX
Avocate, fondatrice du cabinet Juris Défense Avocats

Aujourd'hui, l'utilisation de l'arme cyber confère des bénéfices stratégiques et opérationnels considérables pour les États les mieux dotés. L'émergence du terrain de confrontation cyber a conduit les armées à repenser profondément leur manière d'aborder les modalités de la guerre, tant au niveau technique (robotisation du champ de bataille) que juridique (règlementation et doctrine d'emploi).

La réflexion juridique entamée au niveau international a conduit à l'adoption de nombreux textes de loi et à l'élaboration de doctrines d'emploi pour la lutte informatique défensive et offensive. Il semble bien loin le temps où le cyberespace était considéré comme une « zone de non droit » dont les frontières seraient floues.

Mais ce déploiement de force, intellectuel et opérationnel, est-il suffisant pour permettre l'identification des auteurs et l'imputabilité de la faute à l'auteur des cyberattaques ? Quels sont les freins existants et quelles sont les solutions qui pourraient être apportées pour obtenir enfin la réduction, voire l'anéantissement de ces cyberattaques ?

Cadre légal existant

S'il est souvent reproché aux juristes de ne pas être suffisamment rapides et réactifs face aux évolutions sociétales et techniques, il n'en reste pas moins que de nombreux textes sont intervenus pour réprimer les cyberattaques, aussi bien sur le terrain guerrier que civil.

Sur champ de bataille : Manuel Tallin et doctrine d'emploi (LIO/LID)

Les États ont très rapidement compris que la détention et l'utilisation de cyberarmes leur permettait de disposer de moyens importants pour mener une guerre à la fois silencieuse et bruyante. En effet, à ce jour encore, l'attribution de l'attaque informatique à son ou ses auteurs et l'imputabilité de la faute pouvant donner naissance à la responsabilité des États, reste une difficulté souvent insurmontable.

Mais avant même de régler cette épineuse question, il a fallu réglementer la répression des attaques informatiques. En effet, ce préambule était indispensable et à ce titre, l'Estonie a été la première à engager une profonde réflexion juridique sur la répression de la guerre informatique menée par et entre les États. Elle a été accompagnée dans cette démarche par l'OTAN qui a installé son Centre d'excellence de coopération pour la cyberdéfense à Tallinn[40].

La question primordiale était alors de savoir si le droit des conflits armés et le droit international humanitaire pouvaient s'appliquer aux cyberarmes dans le cadre d'un conflit international entre États.

Les experts[41], dont les travaux ont abouti à la rédaction du Manuel de Tallinn, publié en 2013 et revisité en 2017, ont ainsi posé des règles reprenant ou développant le droit existant pour adapter le *jus ad bellum* (droit de faire la guerre) et le *jus in bello* (droit dans la guerre).

[40] Le Centre d'excellence de cyberdéfense coopérative de l'OTAN (NATO CCD COE) a été créé à Tallinn en Estonie par la signature le 14 mai 2008 d'un protocole d'accord entre l'Allemagne, l'Espagne, l'Estonie, l'Italie, la Lettonie, la Lituanie et la Slovaquie.

[41] Le comité était présidé par Michael N.Schmitt, président et professeur au département juridique de l'United States Naval War College. Une vingtaine d'experts indépendants ont élaboré le manuel, assistés par d'autres organismes tels que le Comité international de la Croix-Rouge (CICR), l'Allied Command Transformation (ACT) et l'US Cyber command.

Ainsi, il a été décidé que les attaques informatiques sont susceptibles de relever de l'usage de la force au sens de l'article 2§4 de la Charte des Nations unies[42], ce qui revient à admettre que le principe de souveraineté s'applique au cyberespace, devenu un terrain conflictuel comme un autre. Ce principe est également établi en droit coutumier par l'arrêt de la Cour internationale de Justice du 27 juin 1986 dans l'affaire des Activités militaires et paramilitaires au Nicaragua contre les États-Unis d'Amérique. Le manuel de Tallinn, dans sa règle 13, admet qu'une cyber opération constitue une attaque armée si les effets de ces attaques sont comparables, en termes de létalité et de destruction, à ceux d'attaques conventionnelles ou nucléaires, biologiques ou chimiques. Ainsi, selon l'article 30 du Manuel de Tallinn, les attaques informatiques doivent provoquer des destructions matérielles, des blessures ou des décès, pour être considérées comme une agression et justifier une riposte.

C'est sur cette base que de nombreux États ont adopté leur doctrine d'emploi défensive et offensive en matière informatique, les États-Unis ayant été les premiers à se positionner dans un rapport publié en avril 2010 par le Congrès américain. D'autres États ont suivi ce mouvement par la suite et en France, la politique ministérielle en matière de lutte informatique défensive a été établie par une instruction ministérielle, nr.101000/MINARM du 1er décembre 2018. Pour mieux anticiper les menaces informatiques, un classement des attaques informatiques a été établi selon plusieurs critères tels que l'intentionnalité, la dangerosité selon l'atteinte, l'attribution, la massivité et la récurrence, ce qui peut, selon les hypothèses les plus graves, autoriser l'État attaqué à riposter, sur le fondement de la légitime défense, prévue à l'article 51 de la Charte des Nations unies.

Enfin, certains États, dont la France, disposent désormais d'une doctrine de lutte informatique d'influence dans un contexte de guerre de l'information, ce qui recouvre toute la couche informationnelle du cyberespace, qui comprend aussi bien les équipements et systèmes informatiques (couche physique) que les données numériques, les logiciels (couche logique) et les informations, les interactions sociales et l'identité numérique (couche cognitive ou sémantique).

Les cyberattaques sont soumises ici encore la Charte des Nations unies et au principe de non-ingérence qui suppose l'absence d'intervention dans un processus électoral à l'étranger, par exemple. Lors d'un conflit armé, elles respectent également les règles du droit international humanitaire (DIH), comme les principes de distinction, de précaution et de proportionnalité dans l'attaque notamment.

La conduite des hostilités et la protection des civils victimes de cyberattaques

Il a été admis, au niveau international, que toute cyber opération menée dans un contexte de conflit armé, en lien avec celui-ci et constitutif d'un acte de violence, offensif ou défensif, contre une autre partie au conflit, est une attaque au sens de l'article 49 du Protocole additionnel I aux Conventions de Genève.

Les règles régissant la conduite des hostilités sont particulièrement pertinentes dans le cyberespace. Elles ont pour objet de protéger la population civile contre les effets des hostilités. Ainsi, les belligérants doivent respecter le principe de distinction qui interdit de cibler les personnes et les biens civils pour se concentrer sur les combattants et les objectifs militaires, tels que les équipements et les données informatiques, tâche ardue en matière de cyberattaque puisque les réseaux sont interconnectés.

L'objectif du droit international humanitaire est de limiter les effets du conflit au strict minimum nécessaire et l'A.57 du 1er PA indique « dans la conduite des opérations militaires, des soins constants doivent être pris pour épargner la population, les personnes et les biens civils ». Ainsi, le principe d'humanité repose sur la volonté d'éviter, dans la mesure du possible, la souffrance excessive engendrée par le recours à la force et les biens connectés, indispensables à la survie de la population civile, ne doivent pas être attaqués, détruits ou être mis hors d'usage (54 1er PI).

Les cyberarmes, de nature à frapper sans discrimination, sont interdites. Il faut ainsi prendre en

[42] L'article 2§4 de la Charte des Nations unies qui énonce : « Les membres des Nations Unies s'abstiennent dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies. »

considération la nature des biens et viser les postes informatiques des forces armées, les réseaux de commandement militaire, depuis lesquels sont menées les cyberattaques, leur destination ou leur utilisation à des fins militaires notamment.

À l'opposé, tous les biens qui ne sont pas des objectifs militaires sont considérés comme des biens civils, ce qui peut concerner les systèmes informatiques des écoles, des établissements médicaux[43], les biens indispensables à la suivie de la nation[44], les installations contenant des forces dangereuses[45] comme les centrales nucléaires, les entreprises hydro-électriques, les usines fabriquant des produits chimiques ou toxiques, et les biens culturels notamment. Ils ne doivent pas être visés.

Les cyberattaques disproportionnées, c'est-à-dire celles dont on peut attendre qu'elles causent incidemment des pertes en vies humaines dans la population civile, des blessures aux personnes civiles, des dommages aux biens de caractère civil, ou une combinaison de ces pertes et dommages qui seraient excessifs par rapport à l'avantage militaire concret et direct attendu, sont également interdites.

La difficulté est que certaines cyberarmes ont été conçues pour affecter, sans discrimination, des systèmes informatiques utilisés à grande échelle. L'interconnectivité qui est le propre du cyberespace signifie que tout dispositif qui se connecte à Internet peut être ciblé de n'importe quel lieu dans le monde. Qui plus est, une attaque contre un système spécifique peut entraîner des conséquences pour d'autres systèmes et causer des effets sans discrimination.

Dès lors, il existe un risque réel de voir les cyberattaques utilisées en violation du DIH, de manière délibérée ou accidentelle. De plus, si la distinction peut sembler relativement simple en matière de biens matériels, elle s'avère particulièrement ardue en matière de combattants et de civils. En effet, la physionomie des conflits a évolué, puisqu'il est souvent difficile de déterminer quel rôle joue un individu dans les cyber opérations.

Dans ces conditions, comment qualifier ces nouveaux guerriers cybernétiques ? Faut-il les considérer comme des combattants ? Des civils ? Des combattants illégaux et leur refuser toute protection ?

Ces questions sont cruciales car elles déterminent l'imputabilité de la faute et l'engagement de la responsabilité des auteurs cyberattaques, mais aussi la faculté de riposter dans le cadre de la lutte informatique défensive et offensive.

L'imputabilité de la faute et la responsabilité des auteurs de cyberattaques

Poursuivre les acteurs des cyber conflits et les sanctionner n'est possible que s'ils ont été clairement identifiés et qu'il n'existe aucun doute sur leur responsabilité dans les opérations.

Or, le cyberespace offre diverses possibilités techniques permettant aux acteurs de dissimuler ou de falsifier leur identité, ce qui rend l'attribution complexe. Ensuite, la physionomie des conflits a évolué, puisque de nouveaux acteurs sont présents sur le théâtre des opérations cybernétiques.

Cette caractéristique est une source de grandes difficultés car si l'attribution de la cyberattaque est impossible, ces cyberattaquants n'auront aucune limite et aucun scrupule à enfreindre le droit international en les utilisant.

L'imputabilité et l'identification des auteurs des cyberattaques

Distinguer clairement les acteurs présents lors des cyber conflits est complexe. En effet, de nouveaux acteurs non étatiques prennent désormais une part active à des cyberattaques, sans que l'on sache exactement s'ils appartiennent à la catégorie des combattants ou des civils[46].

[43] Articles 19.7, 24, 25, 35 et 36 de la première Convention de Genève de 1949, articles 22 alinéa 1,36 et 39 de la deuxième Convention de Genève notamment.
[44] Articles 54 alinéa 2 du PA I et 14 du PA II.
[45] Article 56 alinéa 2 du PA I.
[46] Le Comité international de la Croix-Rouge (CICR) a été victime le 19 janvier 2022, d'une vaste cyberattaque au cours de laquelle les pirates se sont emparés des données de plus de 515 000 personnes, dont certaines ont fui des conflits, et des prisonniers. Les auteurs cette cyberattaque massive n'ont pas été identifiés, mais la CICR a précisé que cette attaque a été perpétrée d'abord contre une société externe en Suisse avec laquelle le CICR a passé des contrats pour stocker des données.

L'attribution ne représente pas un problème pour les acteurs qui exécutent, dirigent ou supervisent les cyber opérations, dans un cadre militaire, lors d'un conflit armé, ce qui comprend les forces armées, les services de renseignement, les entreprises privées que l'État a habilitées à exercer des prérogatives de puissance publique, les milices ou groupes de pirates informatiques qui agissent sur instructions de l'État, ou sous ses directives ou son contrôle.

Il n'y aucune ambiguïté pour les guerriers cybernétiques qui sont intégrés ou rattachés aux forces armées d'un État, selon l'A.43 du 1er PA, ils ont le statut de combattant et peuvent être attaqués. Mais les États peuvent aussi utiliser, dans les opérations cybernétiques, des agents, qui ne sont pas officiellement affiliés aux forces armées de l'État. Tout d'abord, les États peuvent embaucher des entrepreneurs civils pour concevoir des cyberarmes. Un spécialiste en informatique dont le rôle se limite à la conception d'armes cybernétiques ou à la collecte des informations sur la nature de l'infrastructure de l'ennemi, pourra être considéré comme un civil. En revanche, un spécialiste informatique, qui modifie un virus pour surmonter les défenses actives de la cible ou qui recueille des informations sur les moyens de défense, afin de concrétiser une attaque, pourra être considéré comme un combattant.

En revanche, l'attribution est complexe lorsque les États ont recours à des acteurs non étatiques pour lancer des cybers opérations, car cela leur permet de dénier toute implication dans les attaques et d'éviter une riposte de l'État attaqué, dans le cadre de la légitime défense.

Nous savons que les civils peuvent participer directement aux hostilités, ce qui comprend non seulement les actes préparatoires, au temps de l'attaque, mais également ceux de la période postérieure, pendant laquelle les effets de l'arme cybernétique se manifestent encore. Ensuite, la participation directe d'un civil aux hostilités doit entraîner un préjudice direct et d'une gravité suffisante. Bien sûr, les attaques dirigées contre les réseaux informatiques de l'armée sont suffisamment graves pour constituer une participation directe aux hostilités. À l'inverse, les attaques dirigées contre des réseaux et des systèmes informatiques civils, dans le but de porter atteinte aux intérêts économiques d'un État ennemi ne constitueraient pas un préjudice suffisamment grave, à l'exception des opérateurs d'importance vitale, nécessaires à la survie de la nation.

Toutes les incertitudes ne sont cependant pas levées pour certains acteurs non-étatiques, engagés dans des cyberattaques. Il s'agit par exemple de terroristes ou encore des hacktivistes affiliés à aucune des parties au conflit armé et qui entreprennent des cyberattaques par sympathie personnelle avec un belligérant.

A priori, ils ne peuvent pas être qualifiés de combattants légitimes puisqu'ils n'appartiennent pas à un État partie au conflit et ne sont pas sous son « contrôle effectif ». Ainsi, les hacktivistes qui commettent des cyberattaques, sans intention réelle d'aider les belligérants et qui souhaitent avant tout garantir la liberté d'expression des opposants, en rétablissant la connexion Internet ou en aidant les opposants à utiliser les réseaux sociaux de manière anonyme, conservent leur immunité civile et ne peuvent pas être attaqués. Mais pour les hacktivistes qui aident réellement leur pays en guerre, en procédant à des intrusions informatiques destinées à détruire des systèmes ou en procédant à des attaques par déni de service, du fait de leur participation directe aux hostilités, peuvent être qualifiés de combattants et être attaqués.

Enfin, des civils peuvent prendre massivement des cyberarmes pour protéger leur pays en réponse à une cyberattaque et peuvent être reconnus comme des combattants légitimes au titre de l'A.4 & 6 3ème CG du 12 août 1949, à condition qu'ils respectent les lois et les coutumes de guerre et qu'ils portent ouvertement les armes ou un signe distinctif fixe. Mais ces personnes doivent également « mener des hostilités au nom et avec l'accord de l'État Partie » qui doit faire preuve de « contrôle effectif » sur un tel groupe, ce qui suppose une relation de « dépendance et d'allégeance » selon le TPI dans l'arrêt Tadić du 2 octobre 1995.

Or, il peut être difficile d'établir qu'un tel groupe agit sous le « contrôle effectif » de l'État et l'application de ces exigences aux cybers guerriers est délicate car ils ne portent pas d'uniforme, ils opèrent à distance et peuvent utiliser une fausse adresse IP ou

https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/la-croix-rouge-victime-d-une-vaste-cyberattaque_4922939.htm (page consultée le 25/01/2022).

un réseau de machines infectées, tels que les botnets, et ainsi ne pas répondre à l'exigence de porter un signe distinctif.

La responsabilité juridique

Si certaines règles juridiques posées semblent claires, sur le terrain des conflits, de nombreuses questions se posent encore pour l'attribution des attaques et la mise en cause de la responsabilité de ou des auteurs des cyberattaques. En effet, il n'existe aucune obligation en droit international, pour un État réagissant à l'acte internationalement illicite d'un autre État, d'apporter publiquement la preuve de l'imputabilité de l'acte en question à l'État responsable.

Néanmoins, la production de preuve est de plus en plus encouragée, afin de justifier les actions et les ripostes induites par la légitime défense. Ainsi, la production de preuve est de plus en plus encouragée afin de justifier les actions entreprises dans le domaine numérique, car les accusations d'organiser et d'exécuter des actes illicites portées contre des États devaient être étayées »[47]. Selon la règle 14, la responsabilité internationale d'un État dépend de deux critères cumulatifs : premièrement, que l'acte lui soit attribuable ; deuxièmement, que cet acte constitue une violation d'une obligation internationale de l'État. L'État sera donc responsable uniquement si la cyberattaque lui est attribuable et si elle constitue une violation d'une obligation internationale et ce, peu importe s'il en résulte un dommage ou non.

À l'inverse, l'État ne sera pas responsable s'il s'agit d'un acte purement privé. Les cyber opérations conduites par l'organe d'un État mis à la disposition d'un autre État sont attribuables à ce dernier lorsque l'organe exerce des prérogatives de puissance publique de l'État à la disposition duquel il se trouve, selon la règle 16.

Pourtant, la question de la preuve et de l'identification des attaquants reste délicate puisque l'anonymat et l'usurpation d'identité numérique règnent en maître dans le cyberespace et ce, d'autant plus que la localisation d'une adresse IP ne peut faire office de preuve suffisante pour acter la responsabilité d'un État, en raison du recours à des botnets. Dans le droit cyber, encore en construction sur ce point, la preuve numérique est très fragile et il faut alors se contenter de recouper différents éléments, pour structurer un faisceau d'indices et mettre en cause un État.

***

Le cadre légal, tel qu'il existe aujourd'hui, pour contrer les cyberattaques est amplement suffisant. La question de l'identification des auteurs de ces attaques informatiques reste toutefois problématique, pour des raisons techniques en raison de l'utilisation de botnets ou de logiciel espion, mais aussi humaines en raison du difficile rattachement des attaquants à des États bien identifiés. La solution sera essentiellement technique et non pas juridique, ce que les États ont fort bien compris depuis plusieurs années, en renforçant la cybersécurité des biens militaires et civils et en responsabilisant les opérateurs d'importance vitale et en engageant depuis juin 2019, des négociations internationales notamment entre l'Union européenne et les États-Unis sur l'accès transfrontalier aux preuves électroniques et ce, afin de faciliter l'identification des auteurs des attaques informatiques.

[47] Selon le paragraphe 28(f) du rapport de 2015 du Groupe d'experts gouvernementaux des Nations unies (Chapitre 4, section 1 – règles 14 à 19) 3.2.4.1.1

Cyber-coopération au sein de l'OTAN

Daniel VENTRE
CNRS, Laboratoire CESDIP (UMR 8183)

Au début des années 2000, l'OTAN a investi le champ de la cyberdéfense, décidant dès lors d'en faire l'un des piliers de sa stratégie. Au cours des deux dernières décennies l'OTAN a progressivement élaboré sa politique de cyberdéfense, en proposant et réaffirmant les grands principes au fil de ses divers Sommets. La mise en œuvre de la cyberdéfense au sein de l'Alliance a pris forme en partie grâce aux actions de coopération engagées entre les membres, mais aussi à l'extérieur. Plusieurs modalités de coopération ont pris forme, en garantissant la dynamique. Mais elle se heurte aussi parfois à certains écueils ou difficultés.

Chronologie de la construction d'une politique de cyberdéfense collective

Lors du Sommet qui se tient à Prague en 2002, l'OTAN intègre un volet « cyber » dans sa politique de défense. L'objectif est alors de protéger l'OTAN contre les cyberattaques. À l'issue du Sommet, ses représentants déclarent : « nous avons décidé de renforcer nos capacités de défense contre les cyber-attaques »[48]. Deux facteurs expliquent cette évolution : la prise de conscience de la vulnérabilité des systèmes, suite aux attaques de hackers subies en 1999 lors des opérations menées au Kosovo ; et la transformation plus large de l'organisation qu'imposent les attaques du 11 septembre 2001 à New York, afin de faire face aux nouveaux défis. Cette dimension cybernétique du conflit n'est pas tout à fait nouvelle, elle a fait au cours de la décennie précédente (1990-2000) l'objet de nombreuses publications médiatisées, principalement américaines d'ailleurs[49]. Mais cette appropriation du terme « cyber » par l'OTAN contribuera selon nous à en généraliser l'usage dans l'espace doctrinal militaire de l'ensemble des pays de l'Alliance, et bien au-delà.

Les Sommets qui se sont succédés depuis 2002 ont été l'occasion de réaffirmer à maintes reprises l'importance de la cyberdéfense dans la stratégie de l'OTAN, d'en définir le périmètre et de poser les jalons de son organisation. Les cyberattaques qui ont touché l'Estonie en 2007 ont confirmé la nécessité de poursuivre la construction de la cyberdéfense.

Ainsi, lors du sommet de Bucarest (2008) est-il question du renforcement des systèmes d'information clefs de l'Alliance. La protection des systèmes d'information essentiels est une responsabilité qui incombe à la fois aux États et à l'Alliance. Il est également essentiel de pouvoir apporter aux alliés assistance pour contrer les cyberattaques. C'est dans ce contexte qu'est créé la même année le CCDCOE, *Cooperative Cyber Defence Centre of Excellence*, qui s'installe à Tallinn.

Lors du sommet de Lisbonne (2010) l'accent est mis sur la nécessité de développer au sein de l'OTAN les capacités de prévention, détection des cyberattaques, et de défense. Il est prévu d'accélérer le développement du NCIRC (*NATO Computer Incident Response Capability*), dont la mission est de centraliser la protection cyber de toutes les entités de l'OTAN.

En 2011, l'OTAN adopte sa « politique de cyber défense »[50], qui est un jalon essentiel de cette longue construction. Face à l'ampleur de la tâche, la cyberdéfense ne peut être assurée ni au seul niveau des États, ni même de l'Alliance. Il est donc essentiel, c'est l'un des messages centraux de cette politique, de développer des collaborations à la fois avec des partenaires industriels, académiques, des États, et des organisations internationales. Mais la première fonction de la cyberdéfense de l'OTAN est la protection de ses propres réseaux et celle des systèmes des pays alliés sur lesquels repose le

[48] https://www.nato.int/cps/en/natohq/official_texts_19552.htm

[49] M. Libicki, What is Information Warfare?, National Defense University, 110 pages, 1995, https://apps.dtic.mil/sti/pdfs/ADA367662.pdf ; John Arquilla, David Ronfeldt, Cyberwar Is Coming!, Comparative Strategy, 12 (1993), 141-165.

[50] https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf

fonctionnement de l'Alliance, sa capacité opérationnelle. Cette ligne stratégique est rappelée lors du Sommet du Pays de Galle en 2014[51].

Le Sommet de Chicago (2012) fut l'occasion de réitérer les grands principes de cette politique de cyberdéfense, notamment la nécessité de développer des coopérations internationales (comme l'UE, le Conseil de l'Europe, l'ONU, l'OSCE)[52], sur laquelle revint le sommet de 2014 (appelant à de la coopération bilatérale et multilatérale).

En 2016, lors du sommet de Varsovie, l'OTAN déclare que le droit international est applicable dans le cyberespace et que ce dernier est un milieu opérationnel dans lequel l'alliance doit se défendre de la même manière qu'elle le fait sur terre, sur mer et dans les airs[53].

Enfin, plus récemment, lors du sommet de Bruxelles (2021) la nouvelle politique de cyberdéfense globale est entérinée, visant à renforcer la posture de défense, de dissuasion et la résilience de l'OTAN, l'enjeu étant de préserver ses capacités de défense collective, gestion de crise et sécurité coopérative[54]. Ce n'est qu'au cas par cas que l'invocation par les États attaqués de l'article 5 peut être considérée. L'OTAN veut être une plate-forme de dialogue au niveau politique sur la nature et l'ampleur des cyberattaques, sur les approches et réponses nationales, et les possibles réponses collectives[55].

L'OTAN a publié en janvier 2020 une doctrine pour les opérations dans le cyberespace[56]. Il est également question de la dimension militaire du cyberespace dans l' « *Allied Joint Doctrine for Joint Targeting* » (NATO Standard AJP 3.9, Novembre 2021)[57], où il est inscrit que les alliés acceptent d'intégrer leurs capacités cyber nationales dans les opérations de l'OTAN.

Les instruments de la coopération

La coopération, qui est l'un des piliers de la politique de cyberdéfense de l'OTAN, prend aujourd'hui plusieurs formes : partage d'information, exercices de cyberdéfense, réflexions au sein du Centre d'Excellence, partenariats industriels, accords de coopération.

Le partage d'informations peut concerner des données techniques, relatives aux cyber-incidents. À titre d'exemple citons le programme MN CD2 créé en 2013 à l'initiative du Canada, du Danemark, des Pays-Bas, de la Norvège et de la Roumanie, conçu dans le cadre de la *Smart Defence Initiative* de l'OTAN, ouvert à tous les États membres de l'alliance, qui visait à proposer des outils de partage d'information technique sur les cybermenaces et les attaques. D'autres projets, comme la *Malware Information Sharing Platform* (MISP) *Smart Defence Initiative*, ou encore la *Cyber Defence Education and Training* (CD E&T) *Initiative* s'inscrivent dans cette même démarche.

Les nombreux exercices de cyberdéfense fournissent un autre cadre de coopération, de partage d'information et de création de compétences. Ces exercices internationaux ont pour nom *Baltic Ghost*, *Coalition Warrior Interoperability eXercise* (CWIX), *Trident Juncture*, *Trident Jaguar*, *Cyber Coalition*, *Crisis Management Exercise* (CMX), *Locked Shields* ou encore *Crossed Swords*. Les CDX (*cyber defense exercises*) peuvent impliquer plusieurs centaines de participants et observateurs de plusieurs dizaines de pays.

La coopération est également favorisée par l'existence du CCDCOE (*Cooperative Cyber Defence Centre of Excellence*)[58], créé en mai 2008 à l'initiative de huit pays membres de l'alliance (Estonie, Allemagne, Italie, Lettonie, Lituanie,

51 https://www.nato.int/cps/en/natohq/official_texts_112964.htm

52 https://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en

53 https://www.nato.int/cps/en/natohq/official_texts_133169.htm

54 https://www.nato.int/cps/fr/natohq/topics_78170.htm

55 https://www.nato.int/cps/en/natohq/news_185000.htm

56 Allied Joint Doctrine for Cyberspace Operations » (NATO Standard AJP 3-20, Janvier 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

57 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1033306/AJP-3.9_EDB_V1_E.pdf

58 https://ccdcoe.org/organisations/nato/

République de Slovaquie, Espagne), accrédité par l'OTAN en octobre de la même année[59]. L'une des activités principales du Centre d'excellence consiste en l'organisation de colloques (l'*International Conference on Cyber Conflict* – CyCon - fait désormais référence, attirant des chercheurs du monde entier), de débats et la publication de travaux de recherche, qui portent entre autres sur la dimension juridique du cyberconflit et de la cyberdéfense, sur les stratégies et politiques de cyberdéfense. L'une des productions majeures de cette coopération internationale réside dans le Manuel de Tallinn. Le Centre organise également des formations et des exercices de cyberdéfense.

Les entreprises jouant un rôle essentiel dans la structuration du cyberespace, l'OTAN a créé en 2014 un programme spécifique de collaboration, le *NATO Industry Cyber Partnership* (NICP). L'industrie est perçue comme « la première ligne de défense »[60].
Enfin, le cyberespace n'étant pas circonscrit aux seuls espaces des territoires nationaux, l'organisation de la défense face aux cybermenaces impose des actions plus larges, coordonnées et concertées. Des accords de coopérations[61] viennent renforcer la construction de la cyberdéfense car ils créent un cadre légal pour la coopération en matière politique, de R&D, d'organisations d'exercices militaires conjoints, de formation et de partage d'information[62]. Ont ainsi été signés entre pays membres de l'organisation les accords États-Unis-Pologne en 2019[63] ; États-Unis-Estonie, 2020 ; États-Unis-Allemagne, 2020 ; Lettonie-Pologne, 2021…) Des accords bilatéraux ont également été signés avec des pays non membres de l'OTAN (États-Unis-Singapour, 2021 ; États-Unis-Australie, 2020 ; Turquie-Kazakhstan, 2020…) Conformément à son projet de coopération avec l'UE, l'OTAN a signé un accord technique avec elle en février 2016, afin de rapprocher leurs équipes de gestion des cyber-incidents (le NCIRC et le CERT-EU)[64].

Dans le même temps bien sûr des accords de coopération en cyberdéfense sont signés par nombre d' États dans le monde, qui sont en dehors du cadre otanien : Israël-Maroc, 2021 (dans le cadre de la politique de normalisation des relations entre Israël et des pays de la région) ; Vietnam-Japon, 2021 (dans le contexte de tensions avec la Chine) ; Chili-Brésil, 2021…).

Quelques questions théoriques et politiques

La coopération au sein de l'Alliance est-elle optimale et produit-elle les effets escomptés ? Les pays membres et l'organisation militaire sont-ils plus en sécurité et plus performants collectivement qu'ils ne le seraient individuellement ou en s'organisant autrement, en optant pour d'autres cadres de construction de leur sécurité ? Le nombre relativement élevé de modalités de la coopération au sein de l'OTAN et en dehors, atteste de l'existence d'une forte dynamique autour de la cyberdéfense. Mais alliance ne signifie pas toujours acteurs à l'unisson. La coopération peut se trouver altérée par la poursuite d'intérêts divergents et par des approches des enjeux discordantes. Les alliances sont d'ailleurs ainsi faites et l'OTAN n'y échappe probablement pas, que les partenaires cherchent à s'influencer les uns les autres, que des mécanismes de pouvoir et de contrôle se mettent en place, que la poursuite des intérêts collectifs n'est plus toujours le véritable enjeu et que l'on observe plutôt la coexistence de plusieurs intérêts nationaux. Ainsi les enjeux de souveraineté des États inhiberaient-ils en partie les actions communes de cyberdéfense au sein de l'OTAN[65]. Le partage d'informations ne peut être total. L'appartenance à l'OTAN n'empêche pas une adversité dans le cyberespace entre ses pays membres : intrusions dans les systèmes des entreprises et des gouvernements étrangers, interceptions des communications, autant de pratiques agressives dont E. Snowden avait rappelé

[59] https://ccdcoe.org/about-us/

[60] NATO Deputy Secretary General Alexander Vershbow at the 2014 NATO Industry Forum, Croatia, cite dans https://nicp.nato.int/nicp-stakeholders/index.html

[61] Les accords de coopération se distinguent des alliances en ce qu'ils ne prévoient pas de clauses de non-agression et de défense mutuelle.

[62] Kinne, B. (2018). Defense Cooperation Agreements and the Emergence of a Global Security Network. *International Organization*, *72*(4), 799-837. doi:10.1017/S0020818318000218

[63] L'accord prévoit échange d'informations de cybersécurité, formation, promotion d'une posture commune de cyberdéfense, développement de capacités communes de cyber opérations défensives https://pl.usembassy.gov/cyberspace_agreement/

[64] https://www.nato.int/cps/fr/natohq/topics_78170.htm

[65] Vincent Joubert, Jean-Loup Samaan, L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'Otan et de l'UE, revue Hérodote, 2014, n°152-153, pp. 261-275

l'existence et montré toute l'ampleur. La coopération, quand bien même s'appuie-t-elle sur un principe de répartition des tâches et des ressources, peut encore avoir pour écueil la disparité des capacités nationales de cyberdéfense. L'indice NCPI de Harvard montre ces écarts qui existent en termes de « cyber puissance » étatiques. Sur 29 pays que compte l'indice, les États-Unis sont sans surprise en première position, mais la Turquie est au 22ème rang, l'Italie au 28ème et des trente Etats que compte l'OTAN, dix-neuf n'entrent pas même dans ce classement.

La politique de cyberdéfense de l'OTAN s'est construite en fonction de deux adversaires majeurs, la Russie et la Chine. Les membres de l'OTAN, individuellement, n'adhèrent pas nécessairement tous à cette vision des rapports de force. La coopération au sein de l'OTAN soulève la question du rapport de ses membres à l'acteur américain dominant. La cyberdéfense de l'OTAN est-elle véritablement le reflet d'une co-construction consensuelle ou celui du pouvoir d'influence trop important qu'exerceraient les États-Unis sur l'Alliance ? La pensée juridique notamment, qui émane du Centre d'Excellence de Tallin, subirait une influence directe trop pesante des conceptions juridiques américaines sur la défense préemptive[66].

66 https://theatrum-belli.com/pacte-defense-cyber- gare-aux-alliances/

Cyberguerre : faire la guerre sans le dire

Manon GOUREAU
Chargée de mission, département Sécurité et Défense internationales de l'Institut d'études de géopolitique appliquée (IEGA)

L'enjeu grandissant de la cyber sécurité a pu s'illustrer de bien des façons ces dernières années. Piratage du système d'information de la présidence française en 2012 (via le compte Facebook d'un collaborateur du Président), implant de malware espion dans les GSM des décideurs politiques mondiaux (via le logiciel d'exploitation *Pegasus*), affaires *WannaCry*, *Notpeya*, *SolarWinds* ou encore *Colonial Pipeline*, la frontière entre les sphères civiles et militaires face aux assauts du numérique semble se confondre et redéfinir les notions d'ingérence, de guerre et de paix sur le plan légal et stratégique.

Pour comprendre les implications actuelles de la guerre du cyber et son caractère « *hybride* » voire asymétrique, on ne peut faire l'économie d'une rétrospective historique.

Les questions de protection de l'information et d'attaque ne sont pas nouvelles. Dès la Seconde Guerre mondiale, la France sépare le chiffrement en une mission de défense (chiffrement et déchiffrement) et une mission d'attaque (renseignement, interception et décryptement). Ces opérations sont coordonnées au niveau interministériel afin de cibler la principale menace que constitue la confidentialité des télécommunications. Pour se protéger, la France lance des programmes d'équipement de chiffrement (produits cryptographiques) dont elle confie la conception aux industriels. La France a conscience alors que ces derniers vont produire du matériel de guerre. La croissance de ces industries privées de défense est également attisée par l'OTAN au travers de concours de machine de chiffrement entre les différents alliés, poussant à leur multiplication.

Les années 80 voient l'essor de l'ère digitale, de la démocratisation de l'outil numérique et de la connectivité sociale. Emporté par les idéaux d'une structure nouvelle, empreinte de liberté d'expression, de partage et d'égalité, les artisans de l'outil numérique et notamment les industriels dans le chiffrement, le façonnent sans structure, sans régulation et sans mode d'emploi d'utilisation. Le secteur devient incontrôlé, ouvrant la porte à toute pratique malveillante. Les nouveaux géants privés n'ont pas conscience des risques liés à la vente de certaines informations et technologies, tandis que les États sont eux-mêmes dépassés par ces nouveaux enjeux s'élevant au-delà de leur espace légal.

Des pays comme la France identifient, dès le début des années 2000[67], les risques graves que font peser les cyber menaces sur les infrastructures nationales. Les années 2010-2020 vont voir les intérêts commerciaux des grandes industries fragiliser davantage l'espace informatique, avec un accroissement de la technologie numérique et de sa grande friabilité. Un produit est remplacé par un autre dans une optique de vendre toujours plus, et ce sans garde-fou ni considération pour les effets ricochets.

Dans cette configuration nous assistons à une évolution des modes opératoires, une sophistication technique des outils d'attaques utilisés, une complexification croissante en termes d'attribution des attaques, liés à l'essor des marchés de ces outils.

Les pratiques malveillantes, de plus en plus complexes (sabotage, espionnage, déstabilisation politique, coercition, enrichissement...) ainsi que l'émergence de nouveaux profils et l'hybridation d'acteurs malveillants (individuels, terroristes, États et criminels) se multiplient.

Leurs motifs évoluent également, passant d'un simple piratage opportuniste - espionner ses ennemis - à des intérêts financiers, des motivations

[67] Livre blanc sur la défense et la sécurité nationale de 2008.

politiques, voire pourquoi pas, à l'attaque de l'intégrité et l'indépendance d'un pays ?

Faire la guerre sans le dire

Depuis quelques années, les chercheurs s'interrogent : la cyberguerre rentre-t-elle dans le champ des conflits armés ? L'état de guerre désigne une situation juridique à laquelle le droit attache un régime spécifique.

Le droit international public est conçu pour réglementer la guerre cinétique, classique. Traditionnellement la guerre est réservée aux États, mais le terrorisme et l'attribution d'attaques transnationales asymétriques par des acteurs armés non-étatiques ces dernières années (comme le groupe Daech) montrent l'adaptabilité du droit à travers la coutume, aux nouvelles formes de guerres hybrides.

Dans le cas d'attaques dans un milieu virtuel et ayant un impact direct ou indirect sur notre réalité physique, une attribution est bien souvent difficile qu'elle soit étatique ou par des acteurs non-étatiques. Multiplication des intermédiaires, anonymisation ou encore fausse identité, ne sont pas les seuls atouts empêchant une identification. L'internet peut passer par de multiples juridictions rendant les poursuites compliquées, sans compter celles qui ne condamnent pas toutes les pratiques informatiques malveillantes.

De même ces attaques cyber, si récurrentes, n'atteignent pas forcément le seuil de répétition et le degré de gravité retenu la jurisprudence et la doctrine pour définir une agression et justifier une entrée en guerre.

Enfin, une attaque sous forme de désinformation peut-elle être considérée comme une attaque armée ? S'interroger sur la nature de ces attaques cyber est important, car de cette nature dépend la réponse.

Face à des individus privés qui lancent une attaque de type rançongiciel pour des raisons financières, la réponse semble davantage défensive qu'offensive. Mais face à une campagne d'attaques cyber par déni de service distribué (DDOS) contre un pays comme l'Ukraine en 2014 (lors de l'annexion de la Crimée) ou encore dès février 2022 contre les sites du gouvernement Ukrainien, la réponse à cette crise doit-elle être la seule protection des victimes ou bien doit-elle être tournée vers l'agresseur pour qu'il cesse son action malveillante et sous quelle forme ?

Les Hackers (qu'ils soient mandatés par un gouvernement ou indépendant) connaissent depuis longtemps les enjeux économiques et politiques derrière nos écrans. La plasticité opérationnelle qu'offrent les moyens cyber comme la désinformation ou les attaques DDOS est une véritable manière de faire la guerre, mais sans le dire ce qui permet ainsi d'éviter le fragile équilibre de la terreur nucléaire.

À l'image de la récente attaque cyber sur Colonel Pipeline, les conséquences économiques et sociales sur une partie d'un pays peuvent être très dommageables, au point d'impacter la souveraineté et l'indépendance d'un pays.

L'utilisation du cyberespace permet d'attaquer un État ennemi sans pénétrer sa zone géographique, ni le combattre physiquement. Néanmoins l'impact économique et social de telles cyberattaques n'en demeure pas moins dommageable à son intégrité.

Des solutions nationales ?

Les nouvelles tensions géopolitiques qui en découlent poussent à un accroissement des activités mondiales de cyber sécurité face aux enjeux de sécurité dans la société civile et économique. Les infrastructures critiques (Opérateur d'importance vitale – OIV - comme l'énergie, le nucléaire, l'eau, la santé...) détenues en grande partie par le secteur privé, font l'objet d'attaques importantes, pouvant avoir des effets dévastateurs sur un pays.

Les États vont tenter de recréer de la centralité et du contrôle sur des espaces qui semblent de moins en moins pacifiés et capable de se réguler seuls.

Sur le plan institutionnel, sous l'égide du Secrétariat général de la Défense et de la sécurité nationale

(SGDSN)[68], la France se dote dès 2008 de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) qui d'une part, propose les règles à appliquer pour la protection des systèmes d'information de l'État et d'autre part, assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques sur les OIV. En aucun cas l'ANSSI ne peut mener des missions cyber offensives. Elle n'est pas non plus un service de renseignement.

Au fil des années, tout un arsenal étatique vient se mettre en place avec la création du commandement de la cyberdéfense (COMCYBER) au sein du ministère des Armées, la délégation ministérielle aux industries de sécurité et à la lutte contre les cyber menaces (DMISC), l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), la brigade d'enquête sur les fraudes aux technologies de l'information (BEFTI) ou encore le centre de lutte contre les criminalités numériques (C3N) au sein du ministère de l'Intérieur ; le commissariat à l'intelligence stratégique et à la sécurité économique (CISSE) et la direction des entreprises (DGE) à Bercy, ou encore la direction des affaires stratégiques, de sécurité et du désarmement du ministère de l'Europe et des Affaires étrangères.

Il faut également citer le Conseil de défense et de sécurité nationale (CDNS), appuyé par le Comité de direction de la cyberdéfense (CODIR cyber) et le Comité de pilotage de la cyberdéfense (COPIL cyber) au sein duquel sont organisées les orientations nationales en matière de cyberdéfense.

Enfin il ne faut pas oublier les services de renseignement, qui sont des acteurs incontournables dans l'attribution des cyberattaques.

Sur le plan logistique, pour répondre aux attaques cyber, les États peuvent enclencher deux réponses : un dispositif étatique de gestion de crise qui sera tourné davantage vers les victimes et une réponse tournée vers l'agresseur, n'impliquant pas nécessairement de riposte.

S'agissant de la première, les acteurs français cités précédemment s'emploient à assurer la sécurité numérique au niveau national grâce à des missions de prévention, d'anticipation et de protection.

S'agissant de la deuxième réponse, La *Revue stratégique de cyberdéfense* de 2018 formalise l'idée d'une chaîne opérationnelle de cyberdéfense dédiée à la protection. Ce même document appelle « *un renforcement substantiel à la fois des moyens défensifs et offensifs de la France* » invitant les armées à planifier et conduire des opérations numériques jusqu'au niveau tactique, mais interdisant les *hackback* (riposte) par les acteurs privés. Ici la frontière entre civil et militaire reprend son sens.

L'appel à la création de capacités cyber offensives est un grand pas dans la lutte contre les cyberattaques, puisqu'elle apporte désormais une réponse à l'agresseur. Par ailleurs, dans ce document, la France reconnaît les cyberattaques majeures comme une agression armée au sens de l'article 51 de la Charte des Nations unies, s'octroyant ainsi un droit de légitime défense selon le droit international public. Elle ouvre donc la porte à la reconnaissance d'une cyberattaque comme acte de guerre, à l'application du droit des conflits armés et donc une véritable guerre cyber.

La conceptualisation d'une guerre du cyber « cinétique » semble compliquée avec des acteurs privés du numérique plus riches et puissants que certains États, des frontières intraçables et une numérisation technologique dont les moyens et les techniques échappent à une régularisation positive et créent une conflictualité stratégique en perpétuelle croissance.

Au niveau international, une défense active possible ?

Pour illustrer cette conflictualité stratégique, pensons à l'article 5 du traité de l'Atlantique Nord (TAN) qui

[68] Le Secrétariat général de la défense et de la sécurité nationale fait partie des secrétariats généraux sous le giron du Premier Ministre, qui est chargé de la politique publique de sécurité et de défense des systèmes d'information (il coordonne l'action gouvernementale en matière de cybersécurité).

détaille une clause d'assistance mutuelle des nations alliées en cas d'agression armée contre l'une d'elle.

D'une part du coté offensif, il semble que les trente États membres s'accordent à voir une cyberattaque contre l'un d'entre eux comme entraînant la possibilité d'invoquer l'article 5 du TAN (suite au sommet de Newport en 2014). Aucune précision doctrinale n'a été apportée et la seule fois où l'article a été invoqué, aucune offensive n'a été menée[69]. Pour que l'agression cesse, il faudrait une riposte immédiate cyber, or l'OTAN n'a, en théorie, pas de capacité cyberoffensive comme le *hackback*. Il faudrait donc que la réplique intervienne sur un autre domaine militaire comme le milieu terrestre. Mais alors où frapper dans la limite du droit international public ?

D'autre part du coté défensif, les commandements de l'OTAN n'interviennent que sur les réseaux communs de l'OTAN avec une cyberdéfense active. Néanmoins, il est improbable qu'un État donne un accès permanent et surtout complet à l'ensemble de son réseau pour des raisons évidentes d'espionnage cyber (l'espionnage entre alliés étant davantage la règle que l'exception.)

Finalement, trouver un consensus suffisant pour attribuer l'attaque à des personnes et entités est compliqué. Ainsi, sous l'égide de l'OTAN, de l'ONU, de l'OCDE ou de l'UE, un nombre important de documents de régulation et de coopération ont vu le jour ces dernières années, mais toujours sous le prisme de la cyberdéfense « passive ».

La guerre du cyber n'est pas déclarée, elle se joue en subreptice et redessine les moyens militaires traditionnels et le type de réponse apportée à l'agresseur. Il faut ici mentionner le cas de la Russie et la potentielle vague de cyberattaques qui pourrait être dirigée vers l'Union européenne comme l'a annoncé le 21 mars 2022 Joe Biden, suite aux sanctions économiques drastiques contre la Russie en réponse à l'invasion de l'Ukraine. La guerre n'est plus tellement fantôme lorsqu'elle est en capacité de paralyser des pays, mais davantage effrayante quand notre défense ne semble que « passive ».

La responsabilité des acteurs privés

Le cyberespace tend à devenir un véritable espace de non-droit avec l'émergence d'acteurs privés puissants financièrement qui rebattent les cartes des relations internationales et la façon de faire la guerre. Yann Salamon explique qu'aujourd'hui les technologies du numérique permettent aux grands et puissants acteurs privés de s'accaparer des fonctions traditionnellement réservées aux États *« battre monnaie (cf. les monnaies électroniques), user de la « violence légitime » (cf. le sujet du « hackback »), désigner l'adversaire (cf. l'attribution de cyberattaques par des entreprises privées de cyber threat intelligence) »*[70].

Aussi, ils subissent le même sort que les États face à des évènements incontrôlables. Le télétravail non anticipé et non maitrisé à l'occasion de la pandémie de Covid-19 a accru les vulnérabilités des entreprises et donc des actes de cybermalveillances dans la sphère économique. Cette pratique du télétravail, si elle est une importante source d'économie pour les entreprises, peut s'avérer dangereuse et pourtant demeure largement appliquée malgré la possibilité de retourner dans des locaux protégés.

Aujourd'hui les PME victimes de cyberattaque préfèrent payer le prix d'un rançongitiel eu égard au coût économique que représenterait une opération de remédiation couplée au préjudice sur l'image de la marque, mais au prix de renseignements important pour les services secrets nationaux et les accords de coopération mis en place par l'ANSSI.

De tels comportements ouvrent la porte à des attaques massives et de plus en plus récurrentes.

[69] En 2007 l'Estonie a subi une vague massive de cyberattaque et a invoqué l'article 5 TAN. Ce sont posées les questions de considérer ou non une cyber attaque comme une agression, si cette dernière rentrait dans le champ de l'article 51 de la Charte des Nations Unies ; et du type de réponse cyber à apporter entre autre. Devant ces problèmes doctrinaux aucune réponse militaire collective n'a été activé.

[70] Y. SALAMON, « Cybersécurité et cyberdéfense enjeux stratégiques », éd. Ellipses, 2020, p. 241.

D'une affaire entre États, la régulation du cyberespace doit passer par des accords de régulation avec le secteur privé. Une forte coopération mutuelle est de rigueur à tous les niveaux. Le domaine légal est également une arme importante à disposition des États.

Les industries de la télécommunication jadis et du numérique aujourd'hui, vendent leur outils et technologies pour être rentables sur des marchés qui les dépassent. Grâce à l'arrangement de Wassenaar qui permet de coordonner les politiques nationales en matière de contrôle des exportations d'armes et de biens à double usage, des pays comme la France ont pu inscrire des outils et techniques utilisés à l'occasion de cyberattaques et ainsi freiner de grands acteurs privés dans la vente de technologies numériques pouvant devenir des armes de déstabilisation.

Si la reconnaissance des responsabilités spécifiques des acteurs privés est un sujet important, installer des logiciels de sécurité sur nos infrastructures critiques et tenter de contrôler les réseaux, comme nous avons pu le voir, n'est pas suffisant. Certains chercheurs préconisent de débrancher la prise, désautomatiser certaines fonctions ou réintroduire les humains dans le processus[71]. D'autres pourront défendre qu'il faut porter le combat chez l'ennemi à défaut d'arrêter les attaquants, mais là encore nous avons pu voir que ce n'est pas aisé.

La guerre du cyber est bien réelle. Elle n'est plus le seul apanage des États, mais de qui la veut. Des groupes privés comme Anonymous portent déjà les armes, avec par exemple leur récente attaque sur des chaines de télévision russes pour dénoncer l'invasion en Ukraine. La guerre du cyber ne tue pas des civils, mais des économies, des sociétés et de façon plus discrète, la démocratie.

Selon Sébastien Picard, chef de la branche « *opérations de cyber défense* » du NATO HQ LANDCOM, « *il est à espérer que proche est le moment où Arthur considèrera le cyber non comme merlin, mais comme Excalibur à son poing* [72]».

[71] S.BERINATO, « La réponse à la manoeuvre : défense active et *hackback* », *in* La fin de la cybersécurité : réagir aux menaces, *Harvard Business Review*, Avril-mai 2019.

[72] S.PICARD, « Intégrer les opérations cyber à la guerre moderne », *Revue Conflits*, 15 octobre 2021.

Deterrence in Cyberspace Remains an Academic Exercise

Emilio IASIELLO
Strategic cyber intelligence analyst supporting US government civilian and military intelligence organizations, as well as the private sector

Hostilities in cyberspace are not only increasing, but they are fast becoming the norm that risks instilling apathy in the global civilian population the longer governments fail to reduce their volume and impact. Cyber crime, cyber espionage, disruptive attacks, and soft-power information campaigns are leveraged by both state and nonstate actors and are directly connected to some of the most news-garnering events over the past couple of years. Election meddling, the professionalization of ransomware, and attacks against critical infrastructure reaffirm the fact that governments are constantly in the state of reaction. This December 2021 emergence of Log4j vulnerability has underscored this reality, showing how hostile actors quickly capitalize on zero-days and newly publicized flaws before organizations can properly mitigate and remediate them. Given the sheer expanse of this vulnerability in hundreds of millions of devices worldwide, this is a boon for any malicious actor looking to exploit them for a variety of purposes.[73] Proof to point, one cybersecurity firm recorded approximately 900 thousand attacks exploiting Log4j during the first four days of its release, a staggering amount by any measure.[74] Unsurprisingly, cybersecurity firms quickly identified nation state actors taking advantage of this discovery. Researchers discovered that suspected state actors from China, Iran, North Korea, and Turkey actively engaged in exploiting the vulnerability.[75] State cyber activity has been linked to many of the more notable recent cyber attacks including the 2020 SolarWinds supply chain compromise, as well as state influence over nonstate ransomware attacks against Colonial Pipeline and JBS meat supplier that impacted consumer supply. Due to the direct impacts these types of attacks have against civilian populations, governments continue to search for cyber deterrence models to curb this activity, a task that has proven Sisyphean at best. Despite some noteworthy efforts mostly initiated by the United States, cyber deterrence remains more of a thought exercise than a practical strategy, as the current cyber environment continues to favor actors being able to operate freely in cyberspace without suffering any noteworthy repercussions for their activities.

Deterrence Needs to Affect Decision-Making

Cyber deterrence has its roots in previous deterrent strategies such as nuclear, terrorism, and rogue states.[76] In the context of cyberspace, cyber deterrence is a strategy that seeks to alter an adversary's behavior by influencing the decision-making calculus. This is achieved by punishment or denial in which the potential consequence of a series of punitive actions is enough to influence an adversary to change his intended course of action. Deterrence by punishment in cyberspace could range in actions and severity from disrupting or destroying specific targets, operational infrastructure, arrest and conviction of cyber actors, or stringent political and/or economic sanctions, to

[73] Liam Tung, "US Warns Log4j Flaw Puts Hundreds of Millions of Devices at Risk," *ZDNet*, December 14, 2021, https://www.zdnet.com/article/log4j-flaw-puts-hundreds-of-millions-of-devices-at-risk-says-us-cybersecurity-agency/.

[74] "Log4j Vulnerability Causes Nearly 900K Cyberattacks in Four Days," *PYMNTS*, December 14, 2021, https://www.pymnts.com/news/security-and-risk/2021/log4j-vulnerability-causes-nearly-900000-cyberattacks-four-days/.

[75] "Guidance For Preventing, Detecting, and Hunting for CVE-2021-44228 Log4j Exploitation," *Microsoft*, December 11, 2021, https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/.

[75] Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?," *Journal of Strategic Studies*, 7, no. 1 (2013): 54-6.

[76] Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?," *Journal of Strategic Studies*, 7, no. 1 (2013): 54-6.

name a few alternatives. Deterrence by denial in cyberspace can assume different forms such as the implementation of robust security mechanisms and denying hostile actors the ability to access or operate in cyberspace to include impacting infrastructure, financial sources, or communication channels.

The nebulousness of what transpires in cyberspace, the difficulty in attributing activities to state actors, and the inability to monitor state cyber developments make adopting deterrence principles used in existing strategies like nuclear an unfeasible effort. Surveillance and intelligence collection capabilities can be applied to monitoring a state's nuclear activities where such mechanisms cannot be equally applied against a state's cyber program. So, to try to take some principles from established deterrence strategies and cobble them together for the purposes of applying them to the cyber domain seems more desperation than a thought-out and planned stratagem. There are too many variables that need to be considered, and too many situations where a rigid deterrence strategy might not apply, that it suggests that cyber deterrence may be better suited for a case-by-case scenario where different punitive and denial tools can be applied to achieve the policymaker's objective.

Arguably, the United States has led multi-pronged efforts to curb hostile state and non-state driven hostile cyber activity. The latest of these measures is the April 2021 White House-issued executive order (EO) that imposed costs on the "harmful foreign activities by the Russian government." The EO institutes punitive measures in the way of economic sanctions to impose costs to Russian entities for a variety of malfeasance ranging from election meddling to violations of international law.[77] The United States has been on the forefront of trying to curb hostile actor behavior implementing various political, economic, and cyber retaliation, depending on the specific situation. The following lists how the United States has addressed state and nonstate actor cyber hostility:

- **Cyber Retaliation**. This reflects instances where the United States has allegedly engaged in retaliatory cyber attacks in response to a state or non-state adversary's offending action. These instances have typically disrupted an adversary's ability to access or use the Internet to support their activities. Notably, after Russian ransomware gangs successfully exploited and disrupted U.S. fuel and meat supply chains, U.S. Cyber Command (CYBERCOM) shut down REvil's operations by collaborating with foreign governments to redirect traffic from the group's website.[78] This was the second time the group's operational infrastructure was targeted, having suffered an attack in July 2021 that knocked its website offline after the group's attack against Kaseya, an IT management software company.[79] Another example occurred in the aftermath of the U.S. Intelligence Community's assessment of foreign involvement in the 2016 U.S. presidential elections, CYBERCOM retaliated by targeting an identified Russian troll form known for executing disinformation campaigns.[80] The attacks was not only a retaliatory action, but it temporarily disabled the farm's operations throughout the U.S. midterm election cycle.

[77] The White House, "Executive Order on Blocking Property with Respect to Specified Harmful Foreign Activities of the Government of the Russian Federation, April 15, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/04/15/executive-order-on-blocking-property-with-respect-to-specified-harmful-foreign-activities-of-the-government-of-the-russian-federation/.

[78] Tonya Riley, "Cyber Command Boss Acknowledges U.S. Military Actions Against Ransomware Groups," *CyberScoop*, December 6, 2021, https:// www.cyberscoop.com/naksone-cyber-command-ransomware/.

[78] Maggie Miller, "Russian Hacking Group Believed to Be Behind Kaseya Cyber Attack Goes Offline," *The Hill*, July 13, 2021, https://thehill.com/policy/cybersecurity/562773-Russian-hacking-group-behind-kaseya-attack-goes-offline.

[79] Maggie Miller, "Russian Hacking Group Believed to Be Behind Kaseya Cyber Attack Goes Offline," *The Hill*, July 13, 2021, https://thehill.com/policy/cybersecurity/562773-Russian-hacking-group-behind-kaseya-attack-goes-offline.

[80] Julian E. Barnes, "Cyber Command Operation Took Down Russian Troll Farm for Midterm Elections," *The New York Times*, February 26, 2019, https://www.nytimes.com/2019/02/26/us/politics/us-cyber-command-russia.html.

[80] Alison Peters, "Unpacking U.S. Cyber Sanctions," *Third Way*, January 20, 2021, https://www.thirdway.org/memo/unpacking-us-cyber-sanctions

- **Economic Sanctions**. The imposition of economic sanctions has been a foreign policy tool frequently used by the United States to punish and/or deter entities' behaviors. The ability to impact a target government enough for this to be successful remains a topic for debate. In many instances, it has served an official "put on notice" measure, rather than one that has actually succeeded in changing behavior. With respect to cyber-related sanctions, the U.S. government has targeted primarily individuals and organizations affiliated with or connected to their respective governments of Iran, North Korea, and Russia. According to one non-profit organization, as of January 2021, 36 organizations and 75 individuals associated with Iran, seven organizations and 11 individuals associated with North Korea, and 55 entities and 103 individuals associated with Russia have been sanctioned. Seven entities and 19 individuals unaffiliated with a state have been sanctioned as well.[81]

- **Cyber Indictments**. The United States has assumed a leading role in levying indictments against individuals associated with nation states for committing cyber malfeasance. The U.S. government has levied substantial cyber indictments against state-affiliated individuals and organizations from China, Iran, North Korea, and Russia.[82] These indictments have identified foreign intelligence and security services involvement in such activities, the intimation of which is that they were directed by the leaders in their respective governments. As such, the guiding principle behind these indictments was that the governments in question could not easily hide behind plausible deniability, thereby strengthening their culpability to offensive cyber activities.

- **No Hack Pacts**. The United States made an historic "no hack pact" with China in 2015, which was quickly followed up by similar pronouncement agreed to by senior-level representatives of the G-20 that same year. Ostensibly, in principle, all agreed not to conduct cyber espionage for commercial advantage against each other.[83] Lauded at the time, supporters hailed these non-binding agreements as important steps forward into reducing the volume of harmful economic-focused cyber espionage.

By any measure, deterrence is difficult to obtain and rarely if ever can be accomplished through one channel. The complexities and interconnectivity of cyberspace further complicate the matter. Attribution, determining state responsibility, use of proxies, absence of a consensus on state norms of behavior, and the geographies where hostile actors operate underscore some of these challenges. On the surface, it would appear that the United States is implementing a comprehensive multi-pronged approach toward addressing adversary activity, using political, economic, and operational means to punish with the aim of curbing future behavior. However, there appears to be little headway made with regards to their most fervent adversaries, as the measures applied toward deterring adversary activities have not yielded significant results to deem them successful endeavors.

- **Cyber Retaliation**. The dismantling of Russian ransomware gangs' operational infrastructures has not caused them to deter their activities, though some of the more prolific groups have promised to avoid certain targets like some (not all) critical infrastructure organizations.[84] Given ransomware has been identified as a U.S. "national security" consideration is indicative of the potential threat ransomware is to U.S. economic interests.[85] There is no reason to expect ransomware to abate anytime in the near future further supporting the idea that targeted dismantling of some gangs is not enough to deter future activities. Simply, there is too much money to be made. Taking down troll farms, temporarily disrupting Russia's power grid,[86] and

[81] Alison Peters, "Unpacking U.S. Cyber Sanctions," *Third Way*, January 20, 2021, https://www.thirdway.org/memo/unpacking-us-cyber-sanctions

[82] David Hechler, "What Is the Point of These Nation-State Indictments?" *Lawfare*, February 8, 2021, https://www.lawfareblog.com/what-point-these-nation-state-indictments.

[83] Emilio Iasiello, "No-Hack Pacts: Beijing Assumes a Global Leadership Role," *The Cyber Defense Review*, January 12, 2016, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136172/no-hack-pacts-beijing-assumes-a-global-leadership-role/.

[84] Jen Ellis, "ransomware: Is Critical Infrastructure Safe?" *Rapid 7 Blog*, September 24, 2021, https://www.rapid7.com/blog/post/2021/09/24/ransomware-is-critical-infrastructure-in-the-clear/.

[85] The White House, "FACT SHEET: Ongoing Public U.S. Efforts to Counter Ransomware," October 13, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/.

[86] David E. Sanger and Nicole Perlroth, "U.S.

allegedly knocking a limited connected country like North Korea, while punitive in nature, has yet to curb these actors' online malfeasance. While it may make a government "feel better," cyber deterrence by punishment has shown little results in reducing adversary willingness to execute cyber attacks.

- **Economic Sanctions**. Similar to cyber retaliation, economic sanctions certainly can hurt a country fiscally, but there has been little evidence to suggest that sanctions even imposed over a long period of time have factored into whether an adversary will or will not conduct cyber operations. The most sanctioned countries to date remain the United States' most primary adversaries whose cyber activities continue to be tracked and reported on, despite the imposition of the sanctions. While sanctioning may seem to be a preferable alternative to a more aggressive form of deterrence like cyber retaliation or even kinetic world options, they remain a statement more than a practical solution.

- **Cyber Indictments**. There is no real expectation that the state agents that have been indicted by the United States will ever see a U.S. court of law. The host governments will not turn them over, with the only hope of extradition being in the form of arresting them in a third country with laws allowing their removal to the United States. These indictments serve as token gestures that officially put on notice adversarial governments that Washington knows what they did and was able to identify them with their surveillance and intelligence capabilities. But that is where the accountability ends as none of these indictments have changed the way these adversarial governments have approached the way they operate in cyberspace. State agent activities are directed or supervised by their states, and most states operate in their self-interests. If cyber espionage or cyber attacks fulfill this commitment, then indicting individual actors for what their governments want is a bark without a bite behind it.

- **No Hack Pacts**. Despite coming to an agreement with the United States in 2015 that it would not hack for commercial advantage, China resumed its activities after a brief hiatus.[87] In fact, in 2020, the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency updated its information on China's cyber espionage activities, disseminating a report on the tactics, techniques, and procedures used by Chinese cyber actors to commit cyber espionage and disseminated it to the private sector to enhance their cyber security postures.[88] Again, most states put their self-interests ahead of anything else, regardless what they say in diplomatic and public channels.

***

What does this mean for cyber deterrence? At this juncture, it is evident that cyber deterrence is more of an experimental thought exercise than a feasible, deployable, course of action for any state. This is largely due to the fact that states will operate first and foremost in accordance with what they perceive to be in their national interests, which may be unique to them and at odds with others. This can include harassing other states (e.g., Russia and Iran), stealing money (e.g., North Korea), or stealing intellectual property to be more competitive on the international stage (e.g., China). It stands to reason that resentment from the victim or others will not be enough to dissuade the offender from pursuing this track. Obviously, the offending state has determined a level of risk that it is willing to accept, largely based on observing the consequences suffered by other states as a result of their alleged involvements in cyber malfeasance and concluded that these penalties have lacked the teeth to leave a mark.

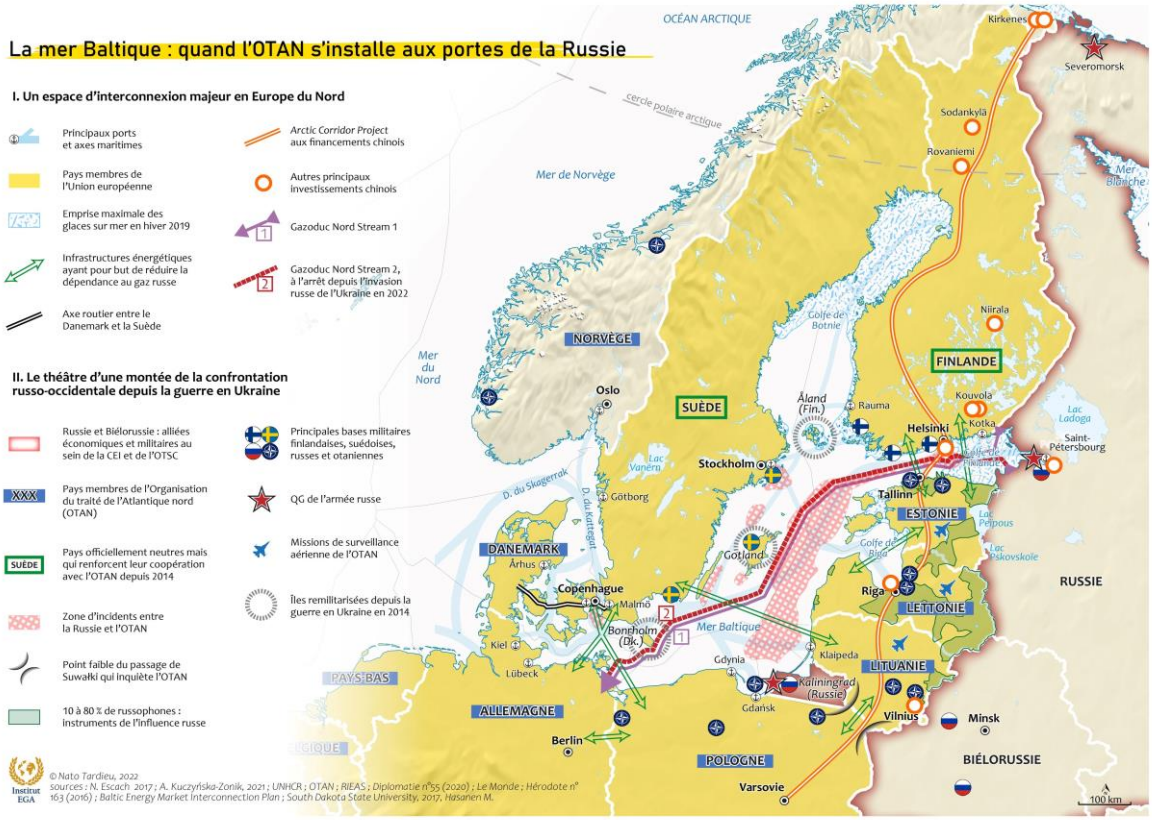
These are the things that governments like the United States need to consider when trying to create a cyber deterrence strategy. Deterrence will only succeed when a state is able to deliver political, economic, retaliatory, or any combination of these consequences that *exceeds* the level of acceptable risk offending states have determined for themselves. Thus far, states haven't figured out that balance, suggesting that cyber deterrence may not

Escalates Online Attacks on Russia's Power Grid," *The New York Times*, June 15, 2019, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html/www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

[87] Adam Segal, "The U.S.-China Cyber Espionage Deal One Year Later," *Council of Foreign Relations*, September 28, 2016, https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later.

[88] "Chinese State-Sponsored Cyber Operations: Observed TTPs," *The Department of Homeland Security, Cybersecurity & Infrastructure Security Agency*, July 19, 2021, https://www.cisa.gov/uscert/ncas/alerts/aa21-200b.

be feasible – at least not as of yet – largely because they can't figure out what that level of risk. Implementing a multi-factored approach using the various political/economic/retaliatory tools at a state's disposal appears a good approach toward determining what that threshold is, but it's one that must be applied in synchronicity and tailored to the targeted state. Imposing a sanction or delivering an indictment independent of other consequences has proven wholly ineffective, as the United States can attest. If states don't move in this direction, it is unlikely that there will be any significant progress in deterring hostile cyber activity, and thereby keeping the status quo, an environment that favors all cyber actors to operate without significant repercussion.



Carte réalisée par Nato Tardieu, pour le compte de l'IEGA, à retrouver en version commentée dans l'*Atlas géopolitique du monde contemporain* (mars 2022, Editions Ellipses). Cliquer ici

Le voisinage oriental de l'OTAN. La relation à l'Ukraine et au Bélarus

Entretien avec Alexandra GOUJON
Maîtresse de conférences à l'université de Bourgogne, spécialiste du Bélarus et de l'Ukraine, auteur de *L'Ukraine. De l'indépendance à la guerre* (Le Cavalier bleu, 2021)

Réalisé par Karl HADDAD puis transcrit par Magomed BELTOUEV,
Responsables du département Eurasie de l'Institut d'études de géopolitique appliquée

Karl HADDAD - Comment expliquer l'intérêt de l'Otan pour les anciennes républiques soviétiques telles que la Géorgie mais surtout l'Ukraine ? Pouvons-nous qualifier les conflits dans ces deux pays de rupture dans les rapports entre Moscou et l'Alliance nord atlantique ?

Alexandra GOUJON - Du fait de son maintien après la fin de la guerre froide, l'Otan a réfléchi à son positionnement en Europe et a donc développé ce programme qu'on appelle « Partenariat pour la paix ». Ce partenariat, créé en 1994, s'adresse aux pays européens qui ne sont pas membres de l'organisation. Font donc partie de ce partenariat pour la paix non seulement l'Ukraine, la Géorgie, mais également la Russie. Chacun de ces pays développe ensuite des relations spécifiques avec l'OTAN avec notamment des traités de coopération puis des structures de décision comme la Commission OTAN-Ukraine (1997), la Commission OTAN-Géorgie (2008) ou le Conseil OTAN-Russie (2002). L'idée pour l'Otan est de ne pas cloisonner l'organisation sur elle-même. La relation spécifique Otan-Ukraine ou Otan-Géorgie est liée au fait que l'Ukraine et la Géorgie sont menacées par la Russie du point de vue de leur intégrité territoriale avec le soutien russe aux entités séparatistes dans les deux pays sans parler de l'invasion russe du 24 février 2022. L'autre spécificité tient au fait qu'une partie des pays dits partenaires, et donc non-membres, souhaitent devenir membres : c'est le cas de l'Ukraine et de la Géorgie. À ce titre, l'Otan est dans une position particulière, puisqu'elle a annoncé publiquement, lors d'un sommet en 2008, qu'il existait bien une perspective d'adhésion pour l'Ukraine et la Géorgie. Mais à ce stade, les deux pays ne sont pas rentrés et ne bénéficient toujours pas du plan d'action pour l'adhésion qui est la première étape à une éventuelle intégration. Les dirigeants d'Ukraine et de Géorgie militent pour obtenir ce plan d'action. Si ce plan d'action n'est pas aujourd'hui engagé, c'est pour plusieurs raisons : il y a d'abord le fait que les 30 membres de l'Otan ne sont pas unanimes sur le sujet. C'est d'ailleurs en raison de l'absence de consensus en 2008 qu'une déclaration est prononcée sans ouverture de plans d'action. Une autre raison renvoie également aux réformes que les États candidats doivent faire notamment en termes de gouvernance. Enfin, certains États membres de l'Otan craignent également la réaction de la Russie qui exprime régulièrement, depuis 2007, son opposition à tout nouvel élargissement à l'Est.

K.H - La Géorgie et l'Ukraine sont menacées dans leur intégrité territoriale par la Russie. Que représente un pays comme l'Ukraine dans la stratégie géopolitique et sécuritaire de la Russie ?

A.G - La Russie voit depuis de nombreuses années, même avant 2014 et l'annexion de la Crimée, l'élargissement progressif de l'Otan comme une menace, ce qui peut paraître un peu paradoxal puisque cet élargissement ne menace pas l'intégrité territoriale de la Russie en tant que telle. C'est comme s'il y avait une inversion de la perception des menaces pour la Russie. La Russie est dans un processus, depuis l'arrivée de Vladimir Poutine au pouvoir, de restauration de la puissance russe au niveau international et au niveau régional, c'est-à-dire européen. L'un de ses projets est la création d'une Union économique eurasiatique dans l'espace post-soviétique qui prend forme en 2014 suite à une première Union douanière créée en 2010. Il existe également une alliance militaire, l'Organisation du traité de sécurité collective, fondée en 2002 avec pour États membres la Russie, la Biélorussie, l'Arménie, le Kirghizstan, le Tadjikistan et le Kazakhstan où cette organisation est intervenue en janvier 2022. L'objectif russe est d'arrimer à ces organisations d'autres pays dont l'Ukraine. Mais, en

Ukraine, depuis le début des années 2000, même s'il y a des gouvernements d'obédiences différentes, la politique étrangère vise un rapprochement avec l'Union européenne et l'Otan. La Russie voit l'Ukraine s'éloigner progressivement, ce qui explique en partie son intervention militaire en 2014 ; elle a clairement posé comme ligne rouge une éventuelle adhésion de l'Ukraine à l'Otan alors même que le pourcentage d'opinions favorables à l'Otan augmente en Ukraine depuis 2014. L'invasion russe en février 2022 ne vise pas uniquement à faire de l'Ukraine un pays neutre, comme le revendique les autorités russes, alors même que l'intégration à l'UE et l'OTAN est inscrite comme objectif dans la Constitution ukrainienne depuis 2019. Elle a également pour objectif de soumettre l'Ukraine aux bonnes volontés du pouvoir russe, à affaiblir l'État et sa population comme en témoignent les exactions commises par les troupes russes sur le sol ukrainien.

K.H - Nous n'avons pas observé une telle hostilité de la part de la Russie à l'adhésion des pays baltes à l'Otan, du moins pas avec la même insistance alors que la Russie réclame une neutralité stratégique pour l'Ukraine. Comment expliquer cette différence de traitement par rapport à ces deux régions ?

A.G - La Russie n'a pas pu empêcher l'adhésion des pays baltes ; elle n'était pas tout-à-fait dans la même posture en termes même de capacité d'action. Elle est plus puissante que dans les années 1990. Mais cela ne veut pas dire que l'adhésion des pays baltes a été bien perçue, côté russe ; celle-ci apparaît plutôt comme la dernière concession. Concernant l'Ukraine, l'histoire est convoquée par les autorités russes qui soulignent l'imbrication des peuples slaves. Le Bélarus ne résiste pas, pour le moment, au projet russe en raison de l'allégeance d'Alexandre Loukachenko à la Russie, renforcée après le mouvement de contestation de 2020, fortement réprimé. Mais le pays pourrait adopter une autre orientation politique, plus proche de la démocratie et des valeurs européennes, s'il y avait un changement de pouvoir d'où le soutien russe à A. Loukachenko.

Ces trois peuples slaves ont une histoire commune qui est largement instrumentalisée par Vladimir Poutine qui, en juillet 2021, publie un essai historique sur le site du Kremlin en trois langues (en anglais, en russe et en ukrainien) dans lequel il indique que les Russes et les Ukrainiens forment un même peuple. Tout l'argumentaire de cet essai vise à montrer, comme son discours du 21 février 2022, que l'État ukrainien contemporain est une sorte d'erreur historique ce qui vise in fine à nier la souveraineté ukrainienne et à justifier une invasion militaire. Il faut tout de même rappeler, qu'en 1997 l'Ukraine et la Russie signaient un traité d'amitié et de coopération et qu'aucune prétention territoriale n'existait à cette époque. Et en 1994, au moment où l'Ukraine rétrocède les armes nucléaires à la Russie, le mémorandum de Budapest est signé par les États-Unis, le Royaume-Uni et la Russie qui s'engagent à respecter l'intégrité territoriale du pays. Jusqu'en 2014 il n'y a pas de conflit entre les deux Etats en termes de frontières. Depuis les années 2000 et le développement des révolutions de couleur dont la Révolution orange en Ukraine (2004), le discours politique et médiatique russe s'est concentré sur le fait de présenter l'Ukraine comme faisant partie de l'histoire russe. Mais ce discours date de l'Empire russe où les Ukrainiens étaient présentés comme des Petits Russes mais aussi de l'Union soviétique qui s'appuyait sur une rhétorique liée à l'amitié entre les peuples. Il y a une spécificité autour de la ville de Kiev, qui est souvent présentée comme la mère des villes russes alors que la Russie, ni même la Moscovie, n'existe au moment de la création de Kiev au Xème siècle. Kiev est alors la capitale de la Rous kiévienne, qu'on a traduit parfois en français par Ruthénie et qui a disparu au XIIIème siècle mais qui est considérée en Russie comme faisant partie de l'histoire proprement russe.

K.H - Quelle était la situation dans le Donbass avant l'invasion russe de l'Ukraine le 24 février 2022 ? Pourquoi la Russie reconnaît-elle l'indépendance des républiques séparatistes de Donetsk et de Louhansk quelques jours avant ?

A.G - Après avoir été un conflit très meurtrier en 2014-2015 opposant les forces armées ukrainiennes et les groupes armés séparatistes, le conflit dans le Donbass s'est transformé en conflit de basse intensité avec des cessez-le-feu régulièrement signés mais fréquemment violés. Le conflit a fait 14 000 morts, plus de 30 000 blessés et plus de 2 millions de réfugiés. Un cessez-le-feu avait été davantage respecté entre juillet 2020 et février 2021 avant que les échanges de tirs se multiplient. La Russie a joué un double-jeu dans les négociations sur ce conflit au côté de l'Ukraine, de l'Allemagne et de la France (format de Normandie) dans le cadre des accords de Minsk signés en 2014 et 2015 ; elle se présentait comme médiatrice alors qu'elle soutenait les républiques séparatistes de Donetsk et de Louhansk militairement, politiquement et

financièrement. La reconnaissance de l'indépendance de ces républiques quelques jours avant l'invasion russe est justifiée par le fait que l'Ukraine menacerait leurs populations. Les autorités ukrainiennes ont pourtant rappelé qu'elles ne chercheraient pas à récupérer ces territoires qui représentaient, avant l'invasion du 24 février, un tiers du territoire global du Donbass sachant que les deux autres tiers des régions administratives de Donetsk et Louhansk étaient sous contrôle ukrainien. La reconnaissance des indépendances de ces entités vise à signifier que Moscou sort des accords de Minsk : l'objectif n'est donc plus la résolution du conflit dans le Donbass mais l'invasion du territoire de l'Ukraine sur plusieurs fronts (Nord, Sud et Est).

L'Ukraine n'étant pas dans l'Otan, elle ne bénéficie pas de son aide automatique. Depuis le début du conflit, l'aide militaire à l'Ukraine provient donc séparément d'États membres de l'OTAN et de l'UE.

K.H - La Russie a utilisé le cas du Kosovo comme précédent pour justifier l'annexion de la Crimée. Comme on le sait, le Kosovo a réussi à gagner son indépendance à travers les bombardements otaniens contre la Serbie en 1999. Que pensez-vous de ce parallèle ?

A.G - Ce parallèle pose de nombreux problèmes. Premièrement, il supposerait que la menace qui a pesé sur le peuple kosovar, et donc le nettoyage ethnique, serait similaire en Ukraine. Or l'annexion de la Crimée n'est précédée d'aucune menace réelle sur la population de Crimée. Deuxièmement, l'accès du Kosovo à l'indépendance n'est pas mené par une puissance étrangère soucieuse d'agrandir son territoire ; elle est proclamée en 2008 près de 9 ans après les frappes de l'Otan qui cherchent alors à mettre fin au nettoyage ethnique lancé par Slobodan Milosevic en représailles aux attaques de l'Armée de libération du Kosovo. La Crimée est annexée par la Russie en deux semaines suite à un référendum de rattachement mené dans des conditions non transparentes tout comme la proclamation de l'indépendance de la Crimée effectuée sous occupation militaire russe.

K.H - L'adhésion de l'Ukraine à l'Otan est-elle un objectif réaliste pour Kiev ?

A.G - Il paraît peu probable que l'Otan accepte un État membre tel que l'Ukraine qui ne contrôle pas l'intégrité de son territoire. L'adhésion de l'Ukraine à l'Otan conduirait à une implication directe dans le conflit ouvert par l'invasion russe du 24 février 2022. Le président ukrainien Volodymyr Zelensky a indiqué, en février-mars 2022, qu'il avait constaté les réticences des États membres de l'Otan sur cette question. Mais la perspective d'adhésion de l'Ukraine à l'UE est, elle, maintenue et promue. Une demande d'adhésion a même été déposée officiellement le 28 février 2022 auprès de l'organisation. On sait toutefois que la procédure d'acceptation d'une candidature officielle peut prendre plusieurs années. Une telle acceptation changerait l'attitude de l'UE à l'égard de l'Ukraine qui fait partie de la politique de voisinage, depuis sa création en 2004, et non de la politique d'élargissement. L'accord d'association avec l'UE, signé puis ratifié en 2014, en est une des réalisations concrètes avec l'accord de libre-échange. Dans cet accord, la perspective d'adhésion n'est pas envisagée.

Pour revenir à l'Otan, on peut aussi noter que l'invasion russe de l'Ukraine provoque des inquiétudes chez les voisins nordiques de la Russie et notamment dans les États neutres tels que la Finlande et la Suède, dont les dirigeants envisagent désormais une demande d'adhésion à l'Otan.

K.H - Les évènements au Bélarus suite à l'élection présidentielle de 2020 ont parfois suggéré des similitudes avec Maïdan. Ce parallèle est-il justifié ? Quels intérêts pour l'Otan et la Russie au Bélarus ?

A.G - Le parallèle avec la révolution Maïdan de 2013-2014 n'est pas le plus adéquat, parce que la révolution de Maïdan est une révolution qui a pour point de départ la signature d'un accord d'association avec l'Union européenne. La contestation qui se déploie au Bélarus à l'été 2020 concerne des fraudes électorales. Le parallèle avec la révolution orange de 2004 en Ukraine est donc plus pertinent puisqu'il s'agit d'une révolution de couleur qui se déroule à l'occasion d'une élection frauduleuse contestée par des citoyens et qui entraîne un changement de pouvoir. Le mouvement contestataire au Bélarus est d'ailleurs strictement national et ne s'appuie pas sur des enjeux géopolitiques ; il revendique des élections libres, la fin de la répression des manifestations et la libération des prisonniers politiques. La répression policière est telle depuis l'automne 2020 que les leaders de l'opposition qui ne sont pas emprisonnés, sont en exil dans l'Union européenne comme Svetlana Tikhanovskaïa. Mais au moment de la campagne électorale, les enjeux européens sont assez peu présents. Plusieurs

candidats dont un qui a été emprisonné sont même considérés comme « pro-russes ».

K.H - Vous pensez à Valéry Tsepkalo ?

A.G - V. Tsepkalo mais aussi Viktar Babaryka, qui avait une certaine popularité, et qui a travaillé pour la Belgazprombank, filiale bélarusse d'une banque appartenant au groupe russe Gazprom. En tous les cas, c'est bien le changement de pouvoir potentiel qui a alerté Loukachenko qui a mis en œuvre une répression sans précédent à l'égard des opposants mais également des citoyens ordinaires. Certains opposants sont accusés d'avoir essayé de prendre le contrôle de l'État. Quant à V. Babaryka, il est condamné, en juillet 2021, à 14 ans de prison pour corruption et évasion fiscale. Les relations entre le Bélarus et l'Otan sont extrêmement faibles, le Bélarus appartient à l'Organisation du traité de sécurité collective dirigée par la Russie. Il n'y a donc pas d'ambition d'adhésion à l'Otan. Depuis le mouvement de contestation de 2020, la rhétorique officielle est extrêmement virulente à l'égard de l'Otan et semble calquée sur le discours russe. A. Loukachenko explique que l'Otan se rapproche du Bélarus, veut prendre le contrôle du pays et que les opposants sont des marionnettes des Occidentaux… A. Loukachenko a toujours été un allié géopolitique de la Russie mais n'a pas toujours été aligné sur la politique russe ; il a notamment cherché à maintenir une certaine autonomie face à la Russie dont il craignait la domination économique et militaire. En 2015, les accords de résolution du conflit dans le Donbass sont signés à Minsk ; A. Loukachenko cherche alors à se présenter comme un médiateur non engagé ce qui entraîne une levée des sanctions de l'UE en 2016 après la libération de prisonniers politiques. Mais, depuis le retour des sanctions occidentales liées à l'élection frauduleuse et à la répression policière, A. Loukachenko est devenu plus dépendant de la Russie sans compter l'usage de son territoire par les troupes russes dans le cadre de l'invasion de l'Ukraine. Les relations entre l'Ukraine et le Bélarus se sont détériorées à partir du moment où le dirigeant bélarusse s'est aligné sur le discours russe concernant les menaces ukrainienne et occidentale. Quant à la Russie, elle soutient A. Loukachenko non pas tellement pour des raisons personnelles mais pour éviter un changement de pouvoir non maitrisé qui pourrait entraîner une réorientation géopolitique de ce pays, un petit peu à l'image de ce qui a pu se passer en Ukraine. La Russie souhaite éviter ce scénario par tous les moyens.

K.H - Un traité existe entre Moscou et Minsk pour la création d'une union des deux États, qui avait été signé et ratifié par Loukachenko et Boris Eltsine en 1997. Est-ce que ce traité est toujours d'actualité ? Quelle serait la perception par l'OTAN ou de l'Ukraine d'une réalisation de ce traité ?

A.G - Depuis 2020, on observe une réactivation du projet d'union des deux États. C'est un projet dont, côté bélarusse, on s'est toujours un peu méfié. A. Loukachenko ne souhaitait pas que son pays soit vassal de la Russie. Pendant un temps, certaines voix ont même indiqué que A. Loukachenko représentait une sorte de paravent à une intégration trop poussée avec la Russie, sans doute aussi par ambition personnelle. Pour lui, le projet d'union d'États pouvait être pensé comme la possibilité de devenir président de cette union, dans le cadre d'une présidence rotative qui lui reviendrait pendant quelques années. Ce projet s'appuie également sur un discours historique autour des peuples frères qui n'est pourtant pas conçu comme un effacement de la spécificité du Bélarus : la perte d'indépendance de son pays signifierait la perte de son propre pouvoir. On constate la réactivation d'un certain nombre de programmes de coopération dans plusieurs domaines ce qui ne veut pas dire que l'intégration politique est pour demain. Par ailleurs, côté russe, est-ce que l'idée serait d'annexer le Bélarus au même titre que la Crimée ? Sans doute pas. Le Bélarus participe à l'Union eurasiatique et à l'Organisation du traité de sécurité collective et ne représente pas une menace pour la Russie qui active déjà un certain nombre de leviers en utilisant le territoire bélarusse pour déployer des troupes en Ukraine. Le champ d'action russe est donc suffisamment libre sans nécessairement entamer l'indépendance du Bélarus même si la marge de manœuvre du dirigeant bélarusse semble se réduire.

K.H - Comment la rivalité Russie-Otan se concrétise-t-elle en termes de *soft power* en Ukraine et au Bélarus ?

A.G - L'Ukaine et le Bélarus sont des pays extrêmement différents. Pour le Bélarus, comme indiqué précédemment, le traitement médiatique du mouvement de contestation a repris une partie de la rhétorique utilisée dans les médias russes à propos d'une contestation qui pouvait conduire à la guerre civile à l'image de ce qui s'était passé dans les pays arabes ou en Ukraine. La contestation est donc présentée sous ces aspects violents alors que la

protestation bélarusse était pacifique. Dès l'été 2020, certains observateurs parlent de la présence de spin doctors russes dans les rédactions de la télévision d'État. À cette époque, il y avait déjà assez peu de médias indépendants ; depuis 2021, ils n'opèrent plus sur le sol bélarusse sous peine d'emprisonnement.

En Ukraine, depuis 2014, il existe un journalisme d'investigation et des sites internet tels que *StopFake* qui ont été créés pour lutter contre la désinformation russe. Il s'agit donc de résister à l'influence informationnelle russe en condamnant les fausses informations divulguées par la Russie. Cette résistance informationnelle s'est développée depuis l'invasion russe de février 2022 en utilisant, la plupart du temps, les mêmes canaux et outils que depuis 2014. Par ailleurs, depuis 2021, plusieurs médias dits pro-russes en Ukraine ont été interdits par les autorités au nom de la protection de la sécurité nationale. Certaines voix s'étaient alors élevées y compris dans les organisations de défense de la liberté d'expression pour critiquer ces mesures. Mais l'invasion russe a fait taire ces critiques puisque la population rejoint les autorités sur la défense de la patrie ukrainienne. Du côté religieux, le projet existant depuis l'indépendance de l'Ukraine de création d'une Église orthodoxe d'Ukraine est réalisé en 2018 puis reconnue par Constantinople en 2019. Cette création est également une réaction à l'influence de l'Eglise orthodoxe du patriarcat de Moscou qui était majoritaire, face à une Eglise du patriarcat de Kiev non reconnue, et qui est considérée comme ayant soutenu le séparatisme à l'est du pays. Suite à l'invasion russe de l'Ukraine, l'Eglise du patriarcat de Moscou qui est alignée sur la position du Kremlin perd des paroissiens. Le domaine du cyber est un autre instrument de pression de la Russie sur l'Ukraine. Plusieurs cyber-attaques ont régulièrement lieu sur les sites internet d'organismes gouvernementaux, d'entreprises ou de banques comme au début de l'invasion.

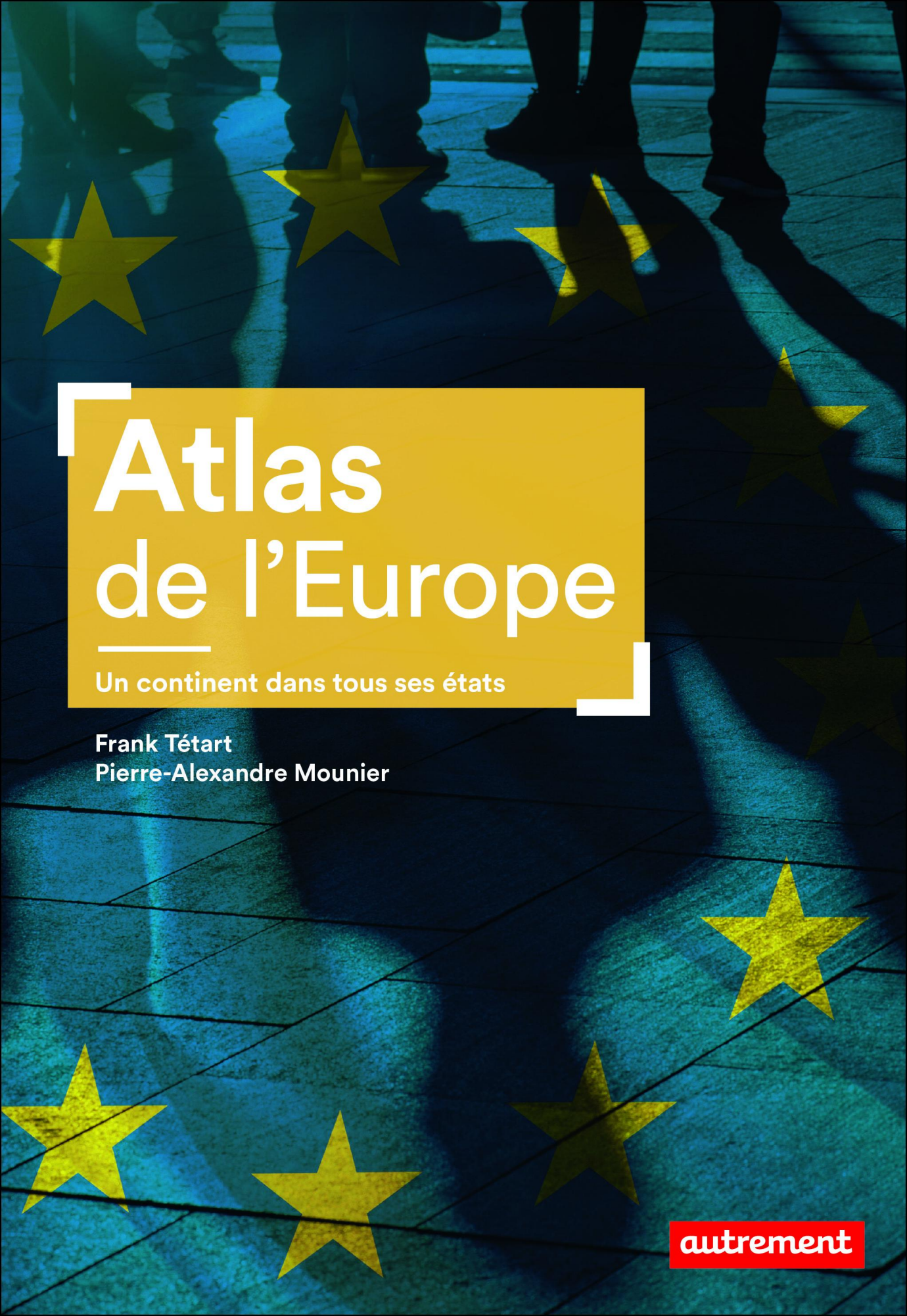
Dans le domaine politique, on évoque aussi régulièrement les « forces pro-russes » en Ukraine. Cette dénomination est trompeuse parce qu'elle ne veut pas dire que ces forces politiques souhaitent un rattachement à la Russie ou une occupation de leur territoire par ce pays. La résistance politique observée dans le Sud de l'Ukraine où l'armée russe occupe plusieurs municipalités en témoigne. La Russie trouve des alliés ici ou là mais en faible quantité sachant que la collaboration avec l'occupant est passible de 15 années d'emprisonnement selon une loi votée par le Parlement le 3 mars 2022. Dans le sillage de l'ancien Parti des régions de Viktor Ianoukovitch destitué en 2014, des forces politiques sont considérées comme étant des agents russes. C'est notamment le cas de Viktor Medvedtchouk, homme politique et homme d'affaires ukrainien, proche de Poutine, qui était assignée à résidence depuis mai 2021 après avoir été inculpé de haute trahison et de tentative de pillage de ressources naturelles en Crimée. V. Medvedchouk qui a disparu quelques jours après l'invasion avant d'être arrêté le 12 avril 2022 fait désormais l'objet de tractations avec la Russie en vue d'un échange de prisonniers.

idées reçues

Alexandra Goujon

L'Ukraine

de l'indépendance à la guerre



Atlas de l'Europe

Un continent dans tous ses états

Frank Tétart
Pierre-Alexandre Mounier

autrement

Institut EGA

La Revue Diplomatique

JE M'ABONNE EN CLIQUANT ICI

www.institut-ega.org