n° 06
/2025-05

Longitudes

Monde-IHEDN Auditeurs

Association internationale des auditeurs Monde de l'IHEDN

Co-directeurs de publication
& **co-rédacteur en chef**
Catherine Bouchet-Orphelin
& Isabelle Chanel

Monde-Ihedn Siège social
École militaire Case 41
1place Joffre
Paris SP 07
75700 Paris

Comité éditorial et de lecture
Catherine Bouchet-Orphelin, Isabelle Chanel, Pierre Millan, Pierre Vauterin.

Conception maquette/édition
Catherine Bouchet-Orphelin
& Isabelle Chanel

Préfecture de Paris :
n° W751269972
ISSN : en cours
CPPAP : en cours
Parution trimestrielle plus suppléments

Contact
monde.ihedn@gmail.com

Dear Auditors, Chers Auditeurs,

News around the world moves very quickly, and it's important not to break off dialogue. Each of you can enlighten others with your own analyses and perspectives. Through your *Longitudes* newsletter, we wish to share this wealth of each of us.

In this issue No. 06, we extend special thanks to Major General (Dr.) Rambir Singh Mann of the Indian Army, as well as Dr. Swasti Rao, Professor and Associate Dean at the Jindal School of International Affairs, and of course, to our French contributors, for all their excellent articles. We hope you find them interesting and enjoyable.

L'actualité dans le monde va très vite et il est important de ne pas rompre le dialogue. Chacun d'entre vous peut éclairer les autres par ses analyses avec sa propre expérience. À travers votre *newsletter Longitudes*, c'est cette richesse de chacun que nous souhaitons partager.

Dans ce N° 06, nous remercions tout spécialement le Major General (Dr) Rambir Singh Mann, de l'Armée indienne, ainsi que Dr Swasti Rao, professeure et doyenne associée à l'école des affaires internationales Jindal, mais bien sûr également nos contributeurs français, pour tous leurs articles de haut niveau. Nous espérons que vous trouverez intérêt et plaisir à les lire.

Yours sincerely,
Catherine Bouchet-Orphelin
Chairperson of Monde-Ihedn Association

Coming soon
Zoom conference on Libya with Ms. Imen Chaanbi as speaker: « Libya: Between Internal Rivalries and Foreign Interference. »
We will notify you as soon as we have a date.

Prochainement
Conférence par Zoom sur la Libye avec Madame Imen Chaanbi comme intervenante: « La Libye entre rivalités internes et ingérences étrangères. »
Nous vous informerons dès que nous aurons une date.

Sommaire / Content

From France

From India

Notes de lecture
Reading notes

Les articles sont classés par ordre alphabétique des pays d'auteurs.
Articles are listed in alphabetical order by author's country

La Libye post-Kadhafi. Un champ d'analyse pour la géopolitique prédictive

Imen Chaanbi
IHEDN SN64

Depuis 2011, la Libye a sombré dans une instabilité chronique, marquée par la fragmentation du pouvoir, les ingérences étrangères et une économie de prédation qui se nourrissent mutuellement. Ce pays, qui incarne l'exemple d'un *failed state* structurel, met en lumière les limites des modèles traditionnels de géopolitique prédictive. La dynamique libyenne échappe en grande partie à l'analyse classique, qui a du mal à saisir l'ampleur et la profondeur des phénomènes locaux. Au-delà des scénarios classiques de guerre civile, la Libye devient un terrain d'expérimentation pour des modèles d'analyse géopolitique hybrides et plus systémiques, capables de considérer les logiques internes, les variables cachées et les acteurs externes.

Abou Mohammad al-Jolani : leader du groupe, HTS*

Aqmi : Al-Qaïda au Maghreb islamique

EI : État islamique

GNA : *Government of National Accord*, Gouvernement d'accord national

GUN : gouvernement d'unité nationale

Haftar : Khalifa Belqasim Haftar Alferjani, né en 1943 à Ajdabiya, militaire libyen, maréchal et commandant en chef de l'Armée nationale libyenne depuis 2015. Il est candidat déclaré à la prochaine élection présidentielle libyenne.

HTS : Hayat Tahrir al-Sham, en Syrie

LNA : *Libyan National Army*, Armée nationale libyenne (LNA) de Haftar

Fragmentation interne : un système chaotique d'interactions tribales et miliciennes

L'un des traits les plus marquants de la Libye post-Kadhafi est la fragmentation du pouvoir. Le pays, autrefois unifié sous le régime de Kadhafi, s'est retrouvé divisé en plusieurs zones d'influence, dominées par des factions tribales, des milices locales et des groupes criminels. La Libye ne se limite plus à un simple clivage Est-Ouest entre la Tripolitaine (à l'ouest) et la Cyrénaïque (à l'est), mais est devenue un véritable archipel de pouvoirs locaux interconnectés de manière informelle.

Les divisions tribales et ethniques – entre Touaregs, Toubous et Arabes – qui ont été exacerbées par des décennies de marginalisation sous le régime de Kadhafi, sont au cœur de cette fragmentation. Chaque groupe cherche à maximiser son pouvoir au détriment des autres, alimentant ainsi des cycles de violence qui s'entrelacent de manière difficilement prévisible. Ce n'est pas seulement une question de contrôle territorial, mais aussi de domination des ressources. Dans ce contexte, la violence devient une forme d'économie. Les milices et les groupes armés, qui sont les principaux acteurs politiques en dehors des structures formelles, tirent leurs revenus de la gestion de points stratégiques : les champs pétroliers, les routes commerciales, et les flux illégaux de migrants, d'armes et de drogues.

Le vide sécuritaire dans le Sud libyen a permis l'émergence de réseaux transnationaux qui contrôlent ces trafics. Ce phénomène a des répercussions sur la politique nationale et internationale : d'un côté, ces flux illégaux financent des acteurs non étatiques et permettent leur développement ; de l'autre, ils créent une instabilité qui fragilise les tentatives de

centralisation du pouvoir par les acteurs politiques « légitimes », qu'il s'agisse du GNA* ou de LNA* de Haftar.

La Libye devient ainsi un cas d'école du « cercle vicieux » d'une économie rentière : le pays est riche en ressources naturelles, principalement en hydrocarbures, mais cette richesse est loin de contribuer à la stabilité. Au contraire, elle alimente la rivalité entre les milices pour le contrôle des infrastructures stratégiques. Les revenus pétroliers, concentrés entre les mains de quelques factions dominantes, entretiennent des clientélismes locaux tout en exposant la Libye aux fluctuations des marchés internationaux. Cette situation est exacerbée par la concurrence féroce pour les points d'exportation, comme les terminaux pétroliers de Ras Lanouf, qui deviennent des symboles du pouvoir et de la résistance.

Ingérences étrangères : un jeu d'échecs multidimensionnel

L'interférence des puissances étrangères est un autre facteur clé qui structure l'instabilité libyenne. La Libye est devenue le théâtre de rivalités géopolitiques entre puissances régionales et mondiales, qui poursuivent chacune des objectifs contradictoires mais interconnectés. La Turquie, par exemple, a soutenu le GNA* en fournissant des drones Bayraktar TB2 et des conseillers militaires, dans l'objectif de sécuriser ses intérêts en Méditerranée orientale et de relancer des contrats d'infrastructures bloqués depuis 2011. De son côté, les Émirats arabes unis, l'Arabie saoudite, l'Égypte ont soutenu le maréchal Khalifa Haftar, dont ils perçoivent l'ascension comme un moyen de contrer l'influence de l'islam politique et des Frères musulmans, tout en cherchant à renforcer leur influence régionale.

La Russie, quant à elle, a déployé une stratégie hybride en Libye. L'entreprise militaire privée Wagner, qui opère dans le pays, sécurise les champs pétroliers au profit de Moscou, et des diplomates russes négocient l'accès à des ports méditerranéens pour la marine russe, dans une logique d'expansion géostratégique en Afrique du Nord et dans le Sahel. Ces ingérences, loin d'être coordonnées, génèrent des dépendances asymétriques, où les factions libyennes se transforment en proxy dans une rivalité géopolitique entre puissances globales.

Au-delà de ces acteurs traditionnels, la Libye attire de nouveaux joueurs sur la scène internationale, comme la Chine et le Qatar, intéressés par les ressources énergétiques et les infrastructures logistiques. Ces acteurs font évoluer les alliances locales et redéfinissent le paysage géopolitique, compliquant encore l'édification d'un État libyen unifié et stable.

Scénarios prédictifs : quel avenir pour la Libye ?

- Le premier scénario consisterait en un accord politique impliquant l'ensemble des parties prenantes. Cela pourrait mener à la formation d'un gouvernement d'unité nationale (GUN), soutenu par une coalition interne de factions modérées. Ce scénario, bien que favorisant une paix fragile, serait entravé par des tensions sous-jacentes liées au contrôle des ressources pétrolières et aux rivalités tribales. Le pays resterait vulnérable à des conflits sporadiques.

- Pour le deuxième scénario, le pays pourrait se scinder en plusieurs régions autonomes. En effet, chaque entité serait contrôlée par des milices ou des factions régionales (Tripolitaine, Cyrénaïque, Fezzan). Ce scénario de "balkanisation" verrait un conflit prolongé avec des affrontements pour le contrôle des ressources stratégiques. L'ingérence étrangère pourrait intensifier la polarisation et mener à une guerre par proxy.

- Le troisième scénario aboutirait à la prise du pouvoir par le maréchal Haftar. Fort du soutien de puissances extérieures comme l'Égypte, les Émirats arabes unis et l'Arabie saoudite, il aurait la mainmise sur la Tripolitaine. Bien que ce scénario stabilise temporairement le pays, il

ne résoudrait pas les fractures internes, et la répression violente des opposants serait probable.

Les scénarios pour l'avenir de la Libye oscillent entre des perspectives de stabilisation fragile et de fragmentation prolongée. Les défis économiques, politiques et sécuritaires, combinés à l'interférence des puissances étrangères, continueront de jouer un rôle clé dans la configuration du futur libyen. L'instabilité régionale pourrait conduire à la résurgence des groupes djihadistes tels que l'État islamique (EI) et l'Aqmi. La prise du pouvoir par Abou Mohammad al-Jolani, le leader du groupe Hayat Tahrir al-Sham (HTS) en Syrie, ainsi que la reconstitution des milices islamistes en Libye, représentent des menaces de plus en plus graves, tant pour la stabilité régionale que pour la sécurité de l'Europe. Ces dynamiques risquent de redéfinir l'équilibre des forces au Moyen-Orient et en Afrique du Nord, et les pays occidentaux, en particulier l'Union européenne, doivent surveiller ces évolutions de près.■

Imen Chaanbi : experte en géopolitique, géostratégie et veille stratégique (Afrique, Asie et Moyen-Orient). Consultante au sein des cabinets 5WE Consulting & Strategik.IA. France Libye Business Club President
Imen Chaanbi : expert in geopolitics, geostrategy and strategic monitoring (Africa, Asia and the Middle East). Consultant at 5WE Consulting & Strategik.IA. France Libya Business Club President

Post-Gaddafi Libya: A Field of Analysis for Predictive Geopolitics

Since 2011, Libya has descended into chronic instability, marked by the fragmentation of power, foreign interferences, and a predatory economy that mutually fuel each other. This country, which embodies the example of a structurally failed state, highlights the limitations of traditional predictive geopolitical models. Libya's dynamics largely elude traditional analysis, which struggles to grasp the breadth and depth of local phenomena. Beyond classic civil war scenarios, Libya is becoming a testing ground for hybrid and more systemic geopolitical analysis models capable of considering internal logics, hidden variables, and external actors.

Internal Fragmentation: A Chaotic System of Tribal and Militia Interactions.

One of the most striking features of post-Gaddafi Libya is the fragmentation of power. The country, once unified under Gaddafi, has now been divided into several zones of influence, dominated by tribal factions, local militias, and criminal groups. Libya is no longer a simple East-West divide between Tripolitania (in the west) and Cyrenaica (in the east), but has become a veritable archipelago of informally interconnected local powers.

Tribal and ethnic divisions – between Tuaregs, Tebus, and Arabs – exacerbated by decades of marginalization under Gaddafi are at the heart of this fragmentation. Each group seeks to maximize its power at the expense of the others, fueling cycles of violence that intertwine in difficult to predict ways. It's not just a question of territorial control, but also of resource domination. In this context, violence becomes a form of economics. Militias and armed groups, which are the main political actors outside of formal structures, derive their income from the management of strategic points: oil fields, trade routes, and the illegal flow of migrants, weapons, and drugs.

The security vacuum in southern Libya has allowed the emergence of transnational networks that control this trafficking. This phenomenon has repercussions for national and international politics: on the one hand, these illegal flows finance non-state actors and enable their development; on the other one, they create instability that undermines attempts to centralize power by "legitimate" political actors, whether the Government of National Accord (GNA) or Haftar's Libyan National Army (LNA).

Libya thus becomes a textbook case of the "vicious circle" of a rentier economy: the country is rich in natural resources, primarily hydrocarbons, but this wealth does not contribute to stability. On the contrary, it fuels rivalry between militias for control of strategic infrastructure. Oil revenues, concentrated in the hands of a few dominant factions, foster local patronage while exposing Libya to fluctuations in international markets. This situation is exacerbated by fierce competition for export points, such as the Ras Lanuf oil terminals, which have become symbols of power and resistance.

Foreign Interference: A Multidimensional Chess Game

The interference of foreign powers is another key factor structuring Libyan instability. Libya has become the scene of geopolitical rivalries between regional and global powers, each pursuing contradictory but interconnected objectives. Turkey, for example, has supported the GNA by providing Bayraktar TB2 drones and military advisors, with the aim of securing its interests in the Eastern Mediterranean and reviving infrastructure contracts stalled since 2011. For their part, the United Arab Emirates, Saudi Arabia, and Egypt have supported Field Marshal Khalifa Haftar, whose rise they see as a means of countering the influence of political Islam and the Muslim Brotherhood, while seeking to strengthen their regional influence. Russia, for its part, has deployed a hybrid strategy in Libya. The private military company Wagner, which operates in the country, is securing oil fields for Moscow, and Russian diplomats are negotiating access to Mediterranean ports for the Russian navy, as part of its geostrategic expansion in North Africa and the Sahel. These interferences, far from being coordinated, generate asymmetric dependencies, where Libyan factions become proxies in a geopolitical rivalry between global powers.

Beyond these traditional actors, Libya is attracting new players on the international scene, such as China and Qatar, interested in its energy resources and logistical infrastructure. These actors are shifting local alliances and redefining the geopolitical landscape, further complicating the building of a unified and stable Libyan state.

Predictive Scenarios: What Future for Libya?

- The first scenario would consist of a political agreement involving all stakeholders. This could lead to the formation of a Government of National Unity (GNU), supported by an internal coalition of moderate factions. This scenario, while conducive to a fragile peace, would be hampered by underlying tensions related to control of oil resources and tribal rivalries. The country would remain vulnerable to sporadic conflicts.

- In the second scenario, the country could split into several autonomous regions. Each entity would be controlled by militias or regional factions (Tripolitania, Cyrenaica, Fezzan). This "balkanization" scenario would see a protracted conflict with clashes over control of strategic resources. Foreign interference could intensify polarization and lead to a proxy war.

- The third scenario would result in Field Marshal Haftar seizing power. With the support of external powers such as Egypt, the United Arab Emirates, and Saudi Arabia, he would control Tripolitania. While this scenario would temporarily stabilize the country, it would not resolve internal divisions, and violent repression of opponents would be likely.

Scenarios for Libya's future oscillate between prospects of fragile stabilization and prolonged fragmentation. Economic, political, and security challenges, combined with interference from foreign powers, will continue to play a key role in shaping Libya's future. Regional instability could lead to the resurgence of jihadist groups such as the Islamic State (IS) and AQIM. The rise to power of Abu Mohammad al-Jolani, leader of Hayat Tahrir al-Sham (HTS), in Syria, and the reconstitution of Islamist militias in Libya pose increasingly serious threats to both regional stability and European security. These dynamics threaten to redefine the balance of power in the Middle East and North Africa, and Western countries, particularly the European Union, must monitor these developments closely.■

Pour aller plus loin, Imen Chaanbi vient de publier ce livre

Géopolitique prédictive : l'intelligence au service de la prospective, avril 2025
par Mathieu Guidère et Imen Chaanbi

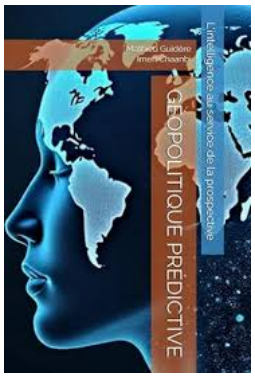
Outre les fiches détaillées de profil pays, les analyses s'appuie sur les techniques de la veille stratégique et mettent à profit les données massives (big data) pour générer, grâce a l'IA, les scénarios prédictifs les plus probables. L'entraînement de l'intelligence artificielle (IA) sur des données massives (Big Data) permet aujourd'hui de faire un saut qualitatif inédit en matière de veille stratégique et d'intelligence économique. L'intégration des technologies prédictives dans l'analyse géopolitique et la prospective participe de cette révolution et offre un éclairage innovant sur un monde en pleine mutation.

To go further, Imen Chaanbi has just published this book

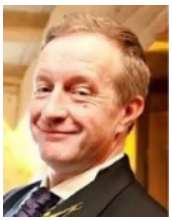
Predictive Geopolitics: Intelligence at the Service of Foresight, April 2025
by Prof. Mathieu Guidère and Imen Chaanbi

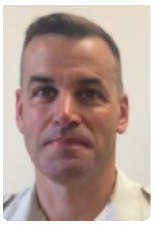
In addition to detailed country profile sheets, the analyses rely on strategic intelligence techniques and leverage big data to generate the most likely predictive scenarios using AI. Training artificial intelligence (AI) on big data now enables unprecedented qualitative leaps in strategic intelligence and business intelligence. The integration of predictive technologies into geopolitical analysis and foresight is part of this revolution and offers innovative insights into a rapidly changing world.

https://www.strategikia.com/ressources/
https://www.strategikia.com/



Anticiper les guerres cognitives : enjeux, défis et méthodologies ?


Didier Bazalgette


LCL Paul Janin

Les opérations cognitives représentent un profond changement dans la conduite des opérations : tandis que les guerres conventionnelles reposent sur des affrontements physiques et que les cyberattaques visent les systèmes numériques, elles ont pour ambition d'attaquer l'esprit humain[1]. La guerre cognitive vise à influencer, déstabiliser et manipuler les perceptions des militaires mais aussi des civils afin d'altérer leur prise de décision, leur résilience ou encore leur volonté d'agir. Dans un monde où l'information est diffusée à une vitesse de plus en plus intense et où les technologies de l'intelligence artificielle sont susceptibles d'anticiper les capacités d'information et de persuasion, la cognition devient un champ de bataille stratégique.

Les opérations cognitives cognitives portent sur trois piliers : biologique et physiologique, cognitif et comportemental et enfin socio-culturel. Pour agir sur ces piliers, quatre grands axes d'action paraissent possibles :

- la narratologie, où le message est délivré par des récits,
- l'ingénierie sociale, où l'action repose sur des modifications des normes ou de l'organisation sociale,
- la captologie, où l'informatique est utilisée pour transmettre le message,
- la neurobiologie, où les voies biologiques sont le vecteur.

Les manœuvres de désinformation et de manipulation, via l'injection de contenus manipulés ou biaisées dans l'espace informationnel, interviennent dans les deux premiers axes. On cherche à convaincre un auditoire ou à faire agir, notamment par des *fake news*[2], des *deepfake*[3] et des *info ops*[4].

Par utilisation d'algorithmes qui permettent de façonner les opinions et d'exploiter les vulnérabilités à travers les biais de confirmation, ces attaques sont en mesure de changer les perceptions et les potentielles prises de décision. La cyber psychologie et la fatigue cognitive utilisent l'exploitation du volume massif d'informations (infobésité) à des fins de confusion et de perte de repères moraux et logiques. Il s'agit également, de la conception d'interface qui génèrent des effets particuliers (confusion, captation de l'attention…). Dans le cadre des neurosciences appliquées à la guerre informationnelle, l'utilisation des connaissances sur le fonctionnement du cerveau visent l'optimisation de l'influence et des méthodes de désinformation.

Ces modes d'action donnent toute leur efficacité dès lors qu'ils sont combinés. Ces différentes dimensions de la guerre cognitive permettent de développer des stratégies qui visent à fragiliser nos institutions, à affaiblir la résistance psychologique des populations civiles et militaires et à créer des phénomènes de polarisation. La guerre cognitive est particulièrement utilisée dans les conflits contemporains. Ainsi, lors des opérations russes en Ukraine, la Russie a mené des campagnes massives de désinformation visant à influencer l'opinion publique occidentale et à saper le moral des Ukrainiens. De manière plus insidieuse, Pékin utilise *WeChat* et *TikTok* afin de diffuser des narratifs qui sont favorables au PCC pour influencer les différentes diasporas chinoises de l'étranger. Enfin des organisations

terroristes comme l'État islamique continuent à tirer parti des réseaux sociaux et des jeux vidéo pour tenter, et souvent réussir, de recruter des individus fragiles du monde entier.

Les pistes de l'anticipation des guerres cognitives

La massification des opérations cognitives et le caractère diffus et latent de ces stratégies étatiques et organisationnelles font du champ cognitif un environnement particulièrement explosif. Dès lors, les organisations militaires sont naturellement amenées à s'interroger sur les méthodes permettant d'anticiper voire de contrer les opérations cognitives. Est-ce seulement possible ? Et si cela l'est, avec quels outils et quelles méthodes ? Les conclusions des rapports du groupe de travail Cognition et Monde Virtuel du CDEC mettent l'accent sur trois grandes catégories d'anticipation des guerres cognitives :

1. La détection des signaux faibles, méthode d'analyse des tendances émergentes qui peut permettre dans le domaine de la propagande, de la manipulation informationnelle et de l'utilisation des nouvelles techniques de persuasion de développer une meilleure appréciation des menaces en train de se développer.
2. Les méthodologies de cartographie des écosystèmes informationnels et en particulier les cartographies dynamiques peuvent permettre une identification d'influences clés, des publics cibles et des vecteurs de propagation des informations.
3. Par des simulations ou des « jeux de guerre » fondés sur des scénarios réalistes, les décideurs pourraient tester des stratégies d'influence et de contremesure. Ces trois grandes catégories se trouveront naturellement renforcées par une intégration de l'intelligence artificielle dans ces processus.

La résilience face aux opérations cognitives

La question des méthodologies d'anticipation est une question complexe à laquelle le groupe du travail du CDEC a tenté de répondre. Une question encore plus complexe est celle qui concerne les méthodes de résilience face aux opérations cognitives : le groupe de travail du CDEC a utilisé une méthodologie qui combine la linguistique et l'informatique pour analyser et traiter le langage naturel de façon automatique a*d hoc* en effectuant deux séries d'entretiens en parallèle et en les confrontant. Les premiers entretiens concernaient une population d'opérationnels spécialisés dans les opérations cognitives, et une seconde série concernait des spécialistes de cette question dans le domaine de l'enseignement et de la formation.

De cette confrontation de deux points de vue et de grille de lecture, profondément différents, les auteurs retirent que « On peut considérer que la meilleure défense contre la guerre cognitive est ce que l'on pourrait nommer la résilience cognitive.

À ce titre notre analyse systématique des entretiens croisés nous permet de mettre en exergue quatre grandes approches qui pourraient être mises en place à la fois au niveau civil mais également au niveau militaire :

- la première concerne l'éducation à l'analyse de l'information et à la pensée critique pour développer des compétences analytiques permettant de discriminer l'information légitime et les tentatives de désinformation ;
- une autre est celle de la modélisation des récits des adversaires. On peut en effet utiliser de la linguistique computationnelle[5] Et des sciences comportementales pour tenter de prédire les narratifs hostiles ;
- un effort important sur le renfort de la cohésion sociale semble également une approche utile : la limitation des fractures sociétales, largement utilisées par nos adversaires dans les opérations cognitives, offrent une résistance plus forte à ces tentatives de déstabilisation ;
- la protection des systèmes d'information contre les attaques qui visent les perceptions humaines et les ingérences psychologiques constituent une « cybersécurité cognitive ». Pour conclure, il

reste indispensable de revenir sur les enjeux des menaces futures dans le domaine de la guerre cognitive afin d'amorcer le travail de construction de méthodes et d'outils de riposte Ces menaces, selon le groupe de travail du CDEC, prendront des formes de plus en plus avancées : « il apparait de plus en plus évident que les campagnes d'influence utiliseront l'IA et des réseaux de bots[6] afin d'orchestrer des campagnes de persuasion et de désinformation à la fois massives et personnalisées. Le développement des outils audiovisuels augmentés par l'intelligence artificielle permet d'envisager des phénomènes de désinformation hyperéalistes avec une probable explosion des *deepfakes,* voire des réalités augmentées à même de créer des univers alternatifs où le vrai et le faux sont difficiles à identifier. Enfin, les avancées en neurosciences font craindre la mise en place d'opérations de neuro-influence ciblées utilisant les signaux neuronaux et les interfaces cerveau/machine. » La guerre cognitive fait donc face à de nombreux défis, l'anticipation et la résilience face à ces opérations de plus en plus complexes nécessitent une connaissance avancée des mécanismes des sciences cognitives indispensable pour préserver la « souveraineté cognitive » des individus et des organisations. En ce sens, la formation des officiers supérieurs en matière de sciences cognitives ne saurait se limiter à des généralités sur les biais cognitifs et se doit, dans un moment de compétition méthodologique décisif, de faire appel aux meilleurs scientifiques et opérationnels pour construire des enseignements complets et pragmatiques.■

(1) l'esprit humain comme champ de bataille
(2) *fausses nouvelles*
(3) *fausse profondeur*
(4) *guerres de l'information*
(5) qui combine la linguistique et l'informatique pour analyser et traiter le langage naturel de façon automatique
(6) dispositifs infectés par des logiciels malveillants qui peuvent être contrôlés à distance.

Bibliographie

- Claverie, B., & du Cluzel, F. (2021). *The Cognitive Warfare Concept*. NATO Innovation Hub.
- De Boudemange, N. G., & Langlois-Berthelot, J. (2022). *Réalité augmentée. DSI (Défense et Sécurité Internationale)*, (160), 92–95.
- Karasek, R. (2022). *Enhancing Defenses Against Cognitive Warfare through Cyber Means*. LinkedIn.
- Langlois-Berthelot, J. (2021). *Appréhender et Assurer les risques Cyber au sein des Organisations: une Approche Systémique et Opérationnelle*. Thèse de doctorat, EHESS.
- Langlois-Berthelot, J., & Bazalgette, D. (2023). *Chi ese Army Cognitive Warfare: Challenges for 6 Next Generation of Operations*. HAL.
- Li, T., & Zhu, Q. (2024). *Symbiotic Game and Foundation Models for Cyber Deception Operations in Strategic Cyber Warfare. arXiv preprint* arXiv:2403.10570.
- Muhammad, Z. (2024). *Introduction à la guerre cognitive : les enjeux d'une nouvelle forme de conflictualité*. CEDIRE.
- NATO Strategic Communications Centre of Excellence. **(**2020). *Cognitive Warfare*. Tomabechi, H. (2023). *Internal Representation in Cognitive Warfare*. George Mason University.

LCL Paul Janin est Lieutenant-colonel de l'Armée de terre.
LCL Paul Janin is a Lieutenant Colonel in the French Army.

Didier Bazalgette , docteur en biologie a été expert sur le sujet guerre cognitive auprès de la DGA et de l'Agence nationale de la Recherche, il a été référent sur de nombreux projets et groupes de travail sur cette thématique
Didier Bazalgette, a doctor of biology, has been an expert on cognitive warfare for the DGA and the National Research Agency. He has been a referent on numerous projects and working groups on this topic.

Anticipating Cognitive War: Issues, Challenges, and Methodologies?

Cognitive operations represent a profound change in the conduct of operations: while conventional warfare relies on physical confrontations and cyberattacks target digital systems, their ambition is to attack the human mind [1]. Cognitive warfare aims to influence, destabilize, and manipulate the perceptions of both military personnel and civilians in order to alter their decision-making, resilience, and willingness to act. In a world where information is disseminated at an increasingly rapid pace and where artificial intelligence technologies are likely to anticipate information and persuasion capabilities, cognition is becoming a strategic battlefield.

Cognitive operations focus on three pillars: biological and physiological, cognitive and behavioral, and finally, sociocultural. To address these pillars, four main avenues of action appear possible:

- narratology, where the message is delivered through stories;
- social engineering, where action is based on changes in norms or social organization;
- captology, where information technology is used to transmit the message;
- neurobiology, where biological pathways are the vector.

Disinformation and manipulation tactics, through the injection of manipulated or biased content into the information space, are involved in the first two areas. The aim is to convince an audience or to provoke action, particularly through fake news, deepfakes, and info ops.

By using algorithms that shape opinions and exploit vulnerabilities through confirmation bias, these attacks are capable of changing perceptions and potential decision-making. Cyber psychology and cognitive fatigue exploit the massive volume of information (infobesity) to confuse and disorient moral and logical reference points. It also involves the design of interfaces that generate specific effects (confusion, attention capture, etc.). Within the framework of neuroscience applied to information warfare, the use of knowledge about how the brain works aims to optimize influence and disinformation methods.

These methods of action are most effective when combined. These different dimensions of cognitive warfare allow the development of strategies aimed at weakening our institutions, weakening the psychological resilience of civilian and military populations, and creating polarization. Cognitive warfare is particularly used in contemporary conflicts. For example, during the Russian operations in Ukraine, Russia conducted massive disinformation campaigns aimed at influencing Western public opinion and undermining Ukrainian morale. More insidiously, Beijing uses WeChat and TikTok to spread narratives favorable to the CCP and influence the various Chinese diasporas abroad. Finally, terrorist organizations like the Islamic State continue to leverage social media and video games to attempt, and often succeed, in recruiting vulnerable individuals from around the world.

Avenues for Anticipating Cognitive War

The widespread use of cognitive operations and the diffuse and latent nature of these state and organizational strategies make the cognitive field a particularly explosive environment. Military organizations are therefore naturally led to question the methods for anticipating or even countering cognitive operations. Is this even possible? And if so, with what tools and methods? The conclusions of the reports of the CDEC's Cognition and Virtual World working group emphasize three main categories for anticipating cognitive warfare:

- Weak signal detection, a method for analyzing emerging trends that can help develop a better understanding of developing threats in the fields of propaganda, information manipulation, and the use of new persuasion techniques.
- Information ecosystem mapping methodologies, particularly dynamic mapping, can help identify key influences, target audiences, and information propagation vectors.
- Through simulations or "war games" based on realistic scenarios, decision-makers could test influence and countermeasure strategies. These three main categories will naturally be reinforced by the integration of artificial intelligence into these processes.

Resilience in the face of cognitive operations

The issue of anticipation methodologies is a complex one that the CDEC working group attempted to address. An even more complex question concerns methods of resilience against cognitive operations: the CDEC working group used a methodology that combines linguistics and computer science to automatically analyze and process natural language ad hoc by conducting two series of interviews in parallel and comparing them. The first interviews involved a population of operational professionals specializing in cognitive operations, and a second series involved specialists in this field in the field of education and training.

From this comparison of two profoundly different perspectives and frameworks, the authors conclude that "We can consider that the best defense against cognitive warfare is what we might call cognitive resilience." In this regard, our systematic analysis of cross-interviews allows us to highlight four main approaches that could be implemented at both the civilian and military levels:

- The first concerns education in information analysis and critical thinking to develop analytical skills to distinguish between legitimate information and disinformation attempts;
- Another is modeling adversary narratives. Indeed, computational linguistics5 and behavioral sciences can be used to attempt to predict hostile narratives;
- A significant effort to strengthen social cohesion also seems a useful approach: limiting societal fractures, widely used by our adversaries in cognitive operations, offers stronger resistance to these destabilization attempts;
- Protecting information systems against attacks targeting human perceptions and psychological interference constitutes "cognitive cybersecurity."

To conclude, it remains essential to revisit the challenges of future threats in the field of cognitive warfare in order to begin the work of building response methods and tools. These threats, according to the CDEC working group, will take increasingly advanced forms: "it appears increasingly evident that influence campaigns will use AI and bot networks6 to orchestrate persuasion and

disinformation campaigns that are both massive and personalized. The development of audiovisual tools augmented by artificial intelligence makes it possible to envisage hyper-realistic disinformation phenomena with a probable explosion of deepfakes, or even augmented realities capable of creating alternative universes where truth and falsehood are difficult to identify. Finally, advances in neuroscience raise fears of the implementation of targeted neuro-influence operations using neural signals and brain/machine interfaces. » Cognitive warfare therefore faces many challenges; anticipation and resilience in the face of these increasingly complex operations require advanced knowledge of the mechanisms of cognitive science, which is essential for preserving the "cognitive sovereignty" of individuals and organizations. In this sense, the training of senior officers in cognitive science cannot be limited to generalities on cognitive biases and must, in a moment of decisive methodological competition, call upon the best scientists and operational experts to construct comprehensive and pragmatic courses.■

(1) The human mind as a battlefield
(2) Fake news
(3) False depth
(4) Information warfare
(5) Combining linguistics and computer science to automatically analyze and process natural language
(6) Devices infected with malware that can be remotely controlled.

Bibliography

- Claverie, B., & du Cluzel, F. (2021). The Cognitive Warfare Concept. NATO Innovation Hub.
- De Boudemange, N. G., & Langlois-Berthelot, J. (2022). Augmented Reality. DSI (Defense and International Security), (160), 92–95.
- Karasek, R. (2022). Enhancing Defenses Against Cognitive Warfare through Cyber Means. LinkedIn.
- Langlois-Berthelot, J. (2021). Understanding and Insuring Cyber Risks within Organizations: A Systemic and Operational Approach. Doctoral Dissertation, EHESS.
- Langlois-Berthelot, J., & Bazalgette, D. (2023). Chinese Army Cognitive Warfare: Challenges for 6 Next Generation of Operations. HAL.
- Li, T., & Zhu, Q. (2024). Symbiotic Game and Foundation Models for Cyber Deception Operations in Strategic Cyber Warfare. arXiv preprint arXiv:2403.10570.
- Muhammad, Z. (2024). Introduction to Cognitive Warfare: The Challenges of a New Form of Conflict. CEDIRE.
- NATO Strategic Communications Centre of Excellence. (2020). Cognitive Warfare. Tomabechi, H. (2023). Internal Representation in Cognitive Warfare. George Mason University.

Guerre cognitive et cyber : un mariage de raison ?

Christophe Gaie

La guerre cyber et la guerre cognitive relèvent de cadres analytiques bien distincts. Néanmoins ces deux types de conflits sont de plus en plus interconnectés. La guerre cyber repose sur la défense et l'attaque des infrastructures numériques, tandis que la guerre cognitive vise à perturber les processus cognitifs des individus et sociétés. Dès lors que c'est l'information qui devient le « nerf de la guerre », le cyber espace devient le terrain privilégié de la guerre cognitive. Par l'utilisation des algorithmes pour orienter les perceptions et orienter les failles cognitives, dans un environnement hyperconnecté les domaines cognitifs et cyber sont imbriqués de manière croissante.

Pour des raisons de champs disciplinaires la guerre cognitive et la guerre cyber sont souvent étudiées de manière séparée. Dans quelle mesure leur rapprochement peut-il susciter un débat stratégique ? S'agit-il d'un simple chevauchement d'outils et de méthodes ? D'une simple complémentarité ou d'une interpénétration croissante qui risque de déterminer les mécanismes opérationnels et leurs implications pour la sécurité internationale ?

Pendant longtemps les opérations psychologiques ainsi que les opérations d'influence « classiques » s'appuyaient sur les médias traditionnels. Le cyberespace est aujourd'hui l'environnement principal par lequel s'exerce les stratégies de guerre cognitive. Les attaques cognitives qui sont menées via le cyber espace peuvent prendre plusieurs formes. La désorganisation cognitive provoquée par la saturation informationnelle est un processus qui vise à engendrer de la confusion, la lassitude et la perte de confiance dans les sources officielle. On a pu voir les effets de cette approche lors de la pandémie de Covid-19 lorsque de nombreuses campagnes de désinformation ont permis de promouvoir des théories inexactes et ont cherché à discréditer des autorités scientifiques et sanitaires.

L'exploitation des biais cognitifs est rendue possible par la montée en puissance de la désinformation algorithmique. L'utilisation croissante de bots et des campagnes de microciblage permettent la propagation de faux récits et la polarisation des opinions publiques comme on a pu le voir lors de campagnes électorales aux Etats-Unis ou lors des opérations d'influence russes en Ukraine. Enfin, l'intelligence artificielle grâce à des modèles de machine Learning permet d'identifier les vulnérabilités psychologiques de certains individus pour personnaliser les opérations d'influence. L'objectif de ces systèmes d'IA est d'optimiser les effets des contenus manipulatoires en fonction des comportements des utilisateurs.

Dans quelle mesure les opérations cyber sont-elles vectrices d'opération cognitives ?

Le cyberespace comme champ de bataille cognitif

Si le cyberespace est un environnement particulièrement propice à la guerre cognitive on peut noter également que les opérations cyber peuvent être l'objet d'instrumentalisation afin d'altérer la perception de la réalité. Il peut en effet être développé des cyberattaques qui visent à modifier des informations et des données cruciales afin d'influencer des décisions stratégiques. On peut penser dans le domaine militaire, à des attaquants qui manipuleraient des renseignements pour orienter une mauvaise prise de décision.

Les attaques perpétrées contre des infrastructures critiques semblent, en première impression, éloignées de la guerre cognitive. Néanmoins ce type d'attaque peut jouer un rôle déterminant en biais cognitif dès lors qu'il permet un climat d'incertitude et de peur, on pensera aux nombreux exemples de cyberattaques contre les hôpitaux qui ont en Europe provoqué des sentiments de vulnérabilité et des effets de phobies massives qui vont bien au-delà des dommages matériels.

Le troisième axe de convergence est la guerre psychologique utilisant la cyber psychologie. Les attaquants peuvent en effet utiliser les connaissances en neuroscience et en psychologie comportementale pour mieux comprendre les mécanismes de protection de leurs adversaires et mieux pénétrer et attaquer les systèmes informationnels.

Les nombreuses implications pour la sécurité internationale et les contremesures potentielles

Le phénomène d'imbrication croissante entre cognition et cyber pose des défis majeurs pour les organisations internationales et les États. Tout d'abord, cette imbrication complique les attributions des attaques, alors qu'une cyberattaque pouvait être attribuée à un acteur particulier, une attaque cognitive se dissout souvent dans une complexité, qui rend les acteurs pluriels. Cette ambiguïté stratégique est largement exploitée par les acteurs qui mènent des campagnes prolongées avec un risque plus faible de représailles directes.

Par ailleurs, les mesures de protection classique de la cyber sécurité ne peuvent suffire à contrer les attaques combinant le cognitif et le cyber. En ce sens les réponses doivent être transdisciplinaires et associer cyber sécurité, résilience psychologique et politique. Le rapprochement entre la guerre cognitive et la guerre cyber pose un certain nombre de défis mais offre également une opportunité en matière de formation. Dès lors que les institutions légitimes appréhendent ce phénomène d'hybridation durable comme une transformation profonde des logiques de conflictualité qui ne sauraient se limiter à une simple addition de menaces. Alors ce changement rend possible un certain nombre d'innovations en matière de pédagogie. L'un des axes que nous souhaitons mettre en avant est celui détecté par le groupe de travail du CDEC Cognition et Mondes Virtuels : « bien loin d'être des domaines distincts le cyber et le cognitif forment en quelle sorte, un continuum où le contrôle des infrastructures numériques et celui des perceptions s'entrelacent pour façonner des environnements de plus en plus difficiles à appréhender. Cette hybridation croissante impose une réflexion profonde sur les doctrines et les approches, et nécessite de développer des formations associant des connaissances diverses, parfois très spécialisées, à des cas d'études et à des simulations réalistes. »■

Bibliographie

- Huang, L., & Zhu, Q. (2023). An Introduction of System-Scientific Approaches to Cognitive Security. arXiv
- Karasek, R. (2022). Enhancing Defenses Against Cognitive Warfare through Cyber Means.
- Langlois, J. (2021). Evaluating and Insuring Cyber Risks within Organizations (Doctoral dissertation, EHESS).
- Langlois-Berthelot, J., & Barthelmess, B. (2020). How Information Technologies are Changing Forensic Finance in Africa. Africa Trends.
- Li, T., & Zhu, Q. (2024). Symbiotic Game and Foundation Models for Cyber Deception Operations in Strategic Cyber Warfare. arXiv
- Meghraoui, L., & Belkhamza, Z. (2025). Cognitive Warfare and Cybersecurity: Strategic Implications for Global Security.
- NATO Review. (2021). Countering Cognitive Warfare: Awareness and Resilience. NATO.
- NATO Strategic Communications Centre of Excellence. (2020). Cognitive Warfare. NATO ACT.
- Orun, A., Orun, E., & Kurugollu, F. (2023). Recognition of Cyber-Intrusion Patterns in User Cognitive Behavioural Characteristics for Remote Identification.
- Papadaki, M. (2024). The Role of Cyber Security in Cognitive Warfare. TDHJ.
- Tomabechi, H. (2023). Internal Representation in Cognitive Warfare. George Mason University.

Christophe Gaie : chef de division ingénierie et innovation numérique au sein des services du Premier ministre. Sous la coordination du Lieutenant Colonel Langlois-Berthelot, il travaille avec le CEMST au développement des compétences et des pratiques de la transformation numérique.

Christophe Gaie : Head of the Engineering and Digital Innovation Division within the Prime Minister's Office. Under the coordination of Lieutenant Colonel Langlois-Berthelot, he works with the CEMST to develop digital transformation skills and practices.

Cognitive Warfare and Cyber: A Marriage of Convenience?

Cyber warfare and cognitive warfare fall within very distinct analytical frameworks. However, these two types of conflict are increasingly interconnected. Cyber warfare is based on the defense and attack of digital infrastructures, while cognitive warfare aims to disrupt the cognitive processes of individuals and societies. Since information becomes the "sinews of war," cyberspace becomes the preferred terrain for cognitive warfare. Through the use of algorithms to steer perceptions and exploit cognitive weaknesses, in a hyperconnected environment, cognitive and cyber domains are increasingly intertwined.

For disciplinary fields reasons, cognitive warfare and cyber warfare are often studied separately. To what extent can their convergence spark a strategic debate? Is this simply an overlap of tools and methods? A simple complementarity, or a growing interpenetration that risks determining operational mechanisms and their implications for international security?

For a long time, psychological operations and "classic" influence operations relied on traditional media. Cyberspace is now the primary environment through which cognitive warfare strategies are carried out. Cognitive attacks carried out via cyberspace can take several forms. The cognitive disorganization caused by information saturation is a process that aims to generate confusion, fatigue, and a loss of trust in official sources. The effects of this approach were seen during the Covid-19 pandemic, when numerous disinformation campaigns promoted inaccurate theories and sought to discredit scientific and health authorities.

The exploitation of cognitive biases is made possible by the rise of algorithmic disinformation. The increasing use of bots and microtargeting campaigns enable the spread of false narratives and the polarization of public opinion, as seen during election campaigns in the United States and Russian influence operations in Ukraine. Finally, artificial intelligence, using machine learning models, can identify the psychological vulnerabilities of certain individuals to personalize influence operations. The goal of these AI systems is to optimize the effects of manipulative content based on user behavior.
To what extent do cyber operations drive cognitive operations?

Cyberspace as a cognitive battlefield

While cyberspace is a particularly conducive environment for cognitive warfare, it should also be noted that cyber operations can be exploited to alter perceptions of reality. Cyberattacks can indeed be developed that aim to modify crucial information and data in order to influence strategic decisions. In the military field, we can think of attackers manipulating intelligence to influence poor decision-making.

Attacks against critical infrastructure may seem, at first glance, far removed from cognitive warfare. However, this type of attack can play a decisive role in cognitive biases when it fosters a climate of uncertainty and fear. One might think of the numerous examples of cyberattacks against hospitals in Europe, which have provoked feelings of vulnerability and massive phobias that go far beyond material damage.

The third area of convergence is psychological warfare using cyber psychology. Attackers can use knowledge in neuroscience and behavioral psychology to better understand their adversaries' defense mechanisms and more effectively penetrate and attack information systems.

The Many Implications for International Security and Potential Countermeasures

The growing intertwining of cognition and cyber poses major challenges for international organizations and states. First, this intertwining complicates attack attribution. While a cyberattack could be attributed to a specific actor, a cognitive attack often dissolves into a complexity that creates multiple actors. This strategic ambiguity is widely exploited by actors conducting protracted campaigns with a lower risk of direct retaliation.

Furthermore, traditional cybersecurity protection measures are insufficient to counter attacks that combine cognitive and cyber aspects. Therefore, responses must be transdisciplinary and combine cybersecurity with psychological and political resilience. The convergence of cognitive warfare and cyberwarfare poses several challenges but also offers a training opportunity. As soon as legitimate institutions understand this phenomenon of lasting hybridization as a profound transformation of the logic of conflict that cannot be limited to a simple addition of threats, this change makes possible a number of innovations in pedagogy. One of the areas we wish to highlight is that identified by the CDEC Cognition and Virtual Worlds working group: "Far from being distinct domains, cyber and cognitive form a continuum where the control of digital infrastructures and that of perceptions intertwine to shape environments that are increasingly difficult to understand. This growing hybridization requires in-depth reflection on doctrines and approaches and necessitates the development of training courses that combine diverse, sometimes highly specialized, knowledge with case studies and realistic simulations."■

Bibliography: cf. page 16

Europe's security crossroads: navigating U.S. policy shifts and rearming challenges

Maj Gen (DR)
Rambir Mann
SIAMO-IHEDN

Prologue

The European security landscape in 2025 is undergoing a profound transformation, driven by shifts in U.S. foreign policy, the evolving role of NATO and Europe's accelerating re-arming efforts in response to persistent threats, most notably from Russia following its 2022 invasion of Ukraine. The United States, under a renewed "America First" doctrine following Donald Trump's re-election in 2024, has recalibrated its strategic priorities characterized by a transactional approach to alliances, scepticism of multilateral commitments, and a focus on reducing U.S. overseas military burdens emphasizing burden-sharing within NATO and redirecting resources toward the Indo-Pacific to counter China. This shift has compelled Europe to reassess its defense posture, prompting a wave of rearmament initiatives across the continent. However, this process is fraught with challenges—military, political, industrial, and economic—that must be addressed to ensure a credible and cohesive defense framework. This essay examines the key problems and aspects to consider in this context and proposes strategies for Europe to organize itself effectively, balancing NATO's collective defense with the European Union's (EU) aspirations for strategic autonomy.

Historical Context

To understand the current predicament, one must first consider the historical reliance of Europe on U.S. military power within NATO. Founded in 1949, NATO was designed as a transatlantic security pact to deter Soviet aggression, with the U.S. providing the lion's share of military capability, including nuclear deterrence and troop deployments. During the Cold War, U.S. forces in Europe peaked at over 300,000, a figure that dwindled to approximately 65,000 by 2025 following post-Cold War drawdowns and strategic pivots towards the Indo Pacific. Europe, meanwhile, enjoyed a "peace dividend" in the 1990s and 2000s, reducing defense budgets and allowing military capabilities to atrophy. Germany's Bundeswehr, for instance, saw its tank fleet shrink from over 2,000 in 1990 to fewer than 300 operational units by 2020, while France and the UK maintained expeditionary forces but lacked the scale for continental defense.

The 2014 Russian annexation of Crimea marked a turning point, exposing Europe's vulnerabilities and prompting NATO to reinforce its eastern flank with Enhanced Forward Presence battlegroups. Yet, U.S. leadership remained pivotal, with American troops forming the backbone of these deployments. The 2022 Ukraine war further underscored this dependence, as Europe struggled to supply Ukraine with sufficient munitions, relying heavily on U.S. stockpiles. By 2025, with U.S. policy shifting under Trump's administration demanding that NATO allies contribute more or face reduced American commitment, Europe finds itself at crossroads, compelled to re-arm while navigating internal divisions and external pressures. Whether this policy persists beyond Trump's term depends on several factors such as political succession, structural U.S. interests and

European responses. It however must be noted that the U.S. strategic pivot to the Indo-Pacific predates Trump, rooted in China's rise as a peer competitor. This bipartisan consensus, evident in the 2018 National Defense Strategy, means that post-Trump administrations are unlikely to fully reverse the reallocation of resources away from Europe, even if they soften the approach. The US policy's longevity hinges on Europe's ability to adapt and on the 2028 U.S. election outcome, with a hybrid scenario (partial continuity) being the most probable.

Projected Security Threats 2050

Europe's security environment is poised for significant evolution by 2050, shaped by a confluence of traditional military threats, emerging technological risks and non-traditional challenges like climate change and societal instability. As of 2025, Russia's war in Ukraine, U.S. strategic reorientation and internal European divisions set the stage for a complex threat landscape. Russia will continue to pose the most prominent threat. Its invasion of Ukraine, has revitalized its military-industrial complex, with annual production of 3 million artillery shells and a mobilized force exceeding 1 million personnel. Its hybrid tactics such as cyberattacks, disinformation and energy coercion target NATO's eastern flank, particularly the Baltic states and Poland. By 2050, Russia could sustain a standing army of 1.5–2 million, bolstered by conscription and technological upgrades. A stabilized Ukraine conflict might redirect Russian focus toward NATO borders, exploiting perceived Western disunity. Advances in AI-driven disinformation could amplify Russian influence operations and cyberattacks on critical European infrastructure. Further, Russia's militarization of the Arctic could dominate resource-rich zones by 2050, challenging Norway and NATO's northern flank. Europe thus faces a persistent conventional and hybrid threat, requiring fortified eastern defenses, cyber resilience, and energy independence. In this endeavour, Russia is likely to be covertly supported by China. Though Beijing avoids direct European confrontation, but it leverages trade, critical supply chains (rare earths, semiconductors) and tech dependencies. Chinese 6G networks and quantum computing, projected to lead globally by 2040, could infiltrate European systems, enabling espionage or sabotage. The threat of anti-satellite weapons, disrupting Europe's Galileo system, crippling navigation and military coordination, would also be a serious concern.

Challenges and Limitations

The oft repeated target of 2 % of GDP to be committed by all NATO members towards defence of Europe has resulted in 23 of NATO's 31 members meeting this target. However qualitative disparities persist. Poland, spends 4.1% of GDP, boasts a modernizing army of 200,000, whereas Germany, at 2%, fields a Bundeswehr plagued by shortages: only 20% of its Puma infantry fighting vehicles are combat-ready, and its navy lacks operational submarines. This uneven burden-sharing undermines NATO's deterrence credibility.

An additional challenge is the overlapping yet divergent roles of NATO and the EU. The EU's European Defence Industrial Strategy (EDIS), launched in March 2024, aims to bolster the continent's defense industry, targeting €100 billion in joint investments by 2030, to reduce reliance on U.S. arms (which account for 63% of EU purchases). Initiatives like the Permanent Structured Cooperation (PESCO) and the European Defence Fund (EDF) have spurred projects such as next-generation tanks and drones. However, these efforts risk duplicating NATO structures, straining budgets, and alienating non-EU NATO members like the UK, Turkey, and Norway, whose exclusion could fracture alliance cohesion.

Similarly, Political fragmentation within the EU compounds this issue. Hungary and Slovakia, wary of antagonizing Russia, have resisted sanctions and arms deliveries to Ukraine, clashing

with hawks like Poland and the Baltic states. This lack of unity hampers the EU's ability to present a credible deterrent, especially as NATO relies on consensus for major decisions. The UK's post-Brexit role adds further complexity: its 2025 defense review prioritizes naval power and AUKUS, potentially diverging from continental needs.

Besides this, Europe's re-arming efforts face significant industrial bottlenecks. Decades of underinvestment have left the defense sector fragmented, with national champions like France's Nexter and Germany's Rheinmetall operating in silos rather than at scale. Producing a single Leopard 2 tank takes 18 months, compared to Russia's ability to churn out refurbished T-90s in weeks. The EU's goal of doubling artillery shell production to 1 million annually by 2026 is ambitious but lags behind NATO's collective needs, estimated at 3-4 million to match Russian output. Workforce shortages, exacerbated by an aging population and raw material dependencies (e.g., titanium from Russia) further constrain capacity. Logistically also Europe's infrastructure is ill-suited for rapid mobilization. The Baltic states' Soviet-era rail gauges differ from Western standards, delaying troop and equipment transfers undermining the "military mobility" pillar of NATO's deterrence strategy.

Funding rearmament poses a formidable challenge. Analysts estimate that Europe requires €250 billion annually and additional troops to achieve strategic autonomy. A tall order amid economic stagnation and inflation hovering at 3-4% in 2025. Political resistance is acute in southern states like Italy and Spain, where debt-to-GDP ratios exceed 100%, limiting fiscal flexibility. Support for Ukraine adds further strain. Europe has pledged €85 billion in aid, depleting stockpiles and diverting funds from domestic rearmament. Balancing these commitments risks creating a "guns versus butter" dilemma.

Securing Europe : Options and Strategies

To navigate these challenges, Europe must adopt a multi-pronged strategy that reinforces NATO's collective defense, advances EU-led capabilities, and fosters industrial and political cohesion. NATO remains Europe's primary security framework and its cohesion must be preserved. The alliance should refine its Defence Planning Process (NDPP) to shift from spending targets to capability-based goals, assigning roles based on national strengths: Germany could focus on armoured brigades, France on air defense and Poland on rapid-response forces. The EU must complement NATO by focusing on enablers rather than rival structures. EDIS should prioritize joint procurement, targeting high-demand systems like Patriot-equivalent missile defenses and MQ-9 Reaper-style drones, reducing costs through economies of scale. Standardizing equipment would enhance interoperability. Industrial capacity can be boosted by repurposing civilian sectors. Germany's automotive plants, facing declining car sales, could shift to producing military vehicles, mirroring U.S. World War II conversions. Financing this transformation demands creative solutions. Joint EU defense bonds, proposed by Macron in 2024, could raise €200 billion over a decade. National contributions could be tiered: wealthier states like the Netherlands can fund more than poorer ones like Bulgaria. Tax incentives for defense firms and public-private partnerships would spur investment.

Politically, leaders must build consensus through a "European Security Pact," endorsed at a EU-NATO summit. This pact would commit members to a 10-year rearmament plan, with annual progress reviews to maintain accountability. Public support could be galvanized via campaigns highlighting jobs and security benefits, drawing on Poland's successful "Strong Nation" narrative, which boosted

approval for defense spending from 60% to 75% between 2022 and 2025.

Europe must avoid isolating key partners and the UK, with its 83,000-strong army and nuclear deterrent, should be integrated via a NATO-EU "Associate Framework," co-funding projects like cyber defense. Turkey's 400,000 troops and drone expertise warrant a similar arrangement, despite political tensions. Norway's Arctic expertise could bolster NATO's northern flank. The U.S. remains indispensable and Europe must reinforce transatlantic ties. A "New Atlantic Charter" is needed with Europe taking the lead on conventional forces, the U.S. on nuclear and naval power ensuring mutual investment.

Poland offers a model for rapid rearmament. Since 2022, it has doubled its military to 200,000, acquiring 1,000 K2 tanks from South Korea and 32 F-35 jets from the U.S., funded by a 4% GDP budget. Its focus on deterrence by deploying HIMARS systems near Kaliningrad, shows how targeted investments can shift regional balances. Similarly France exemplifies strategic autonomy within NATO. Its 2025 Force de Frappe upgrade, including hypersonic missiles and leadership in PESCO projects like the Future Combat Air System (FCAS) demonstrate how national ambition can align with collective goals. Scaling FCAS to include Germany and Spain would accelerate deployment and operational readiness.

Allies Can Boost Europe's Rearmament.

As Europe intensifies its re-arming efforts in 2025 amid heightened security threats, particularly from Russia, leveraging the military industrial capacity of friendly nations outside the European Union (EU) and NATO's immediate sphere offers a strategic pathway to bolster its defense capabilities. Internal European industrial constraints limit rapid scaling however partnerships with allies such as the United Kingdom, Canada, South Korea, Japan, Australia and India can accelerate production, diversify supply chains, and enhance technological innovation. Towards this end Joint Procurement Agreements can be formalised and Europe can pool orders through NATO or EU frameworks with these nations, negotiating bulk purchases to reduce costs and expedite delivery, co-production and technology transfer agreements. Establishing joint manufacturing ventures can localize production while tapping foreign expertise.

Exploiting these nations' capacities offers Europe multiple advantages such as supply chain diversification, speed and scale, cost efficiency, diversifying suppliers mitigates risks from export curbs, ensuring steady production even under sanctions pressure. Europe can thus transform these alliances into a force multiplier, ensuring security in an uncertain era.

Conclusion

Europe stands at a pivotal moment in 2025. U.S. policy shifts, NATO's evolving role, and Russia's aggression demand a robust response. By strengthening NATO's capabilities, advancing EU autonomy, fostering industrial and political unity, and tapping friendly nations, Europe can transform challenges into opportunities. A decade-long plan, blending deterrence with diplomacy, could yield a continent capable of defending itself and contributing to global stability. The path is arduous, but with resolve and coordination, Europe can secure its future by 2035, ensuring that its re-arming efforts today lay the foundation for peace tomorrow.■

Major General (Dr) Rambir Singh Mann served nearly four decades in key operational, logistics, administrative, and procurement roles in the Indian Army. His career includes counter-insurgency operations and commanding mechanized formations as well as an Infantry Division. Diplomatic assignments included United Nations Peace Keeping in Angola and coordinating tri-services foreign cooperation with the UK and France. He played a key role in defence procurement and associated policy making, enabling indigenous production, Joint ventures and defence offsets. Additionally, he also steered major projects like the Tactical Communication System and Futuristic Infantry Combat Vehicles. Having attended many strategic training courses including at IHEDN, Paris, he is academically accomplished and holds a doctorate from Indian Institute of Technology, Delhi on Defence Industrial Policy and Defence Offsets, and diplomas in Management and Transformation. A recipient of multiple Indian and UN military honors and awards, he currently advises the Ministry of Defence on technology and offsets matters. He writes for various Defence and Security magazines and his articles can be accessed on his LinkedIn profile https://www.linkedin.com/in/rambir-mann-8333a912/

Le général de division (Dr) Rambir Singh Mann a occupé près de quarante ans des fonctions clés dans les domaines opérationnel, logistique, administratif et des achats au sein de l'armée indienne. Sa carrière comprend des opérations de contre-insurrection et le commandement de formations mécanisées, ainsi que d'une division d'infanterie. Parmi ses missions diplomatiques, on compte la mission de maintien de la paix des Nations unies en Angola et la coordination de la coopération interarmées avec le Royaume-Uni et la France. Il a joué un rôle clé dans les achats de défense et l'élaboration des politiques associées, favorisant la production locale, les coentreprises et les compensations de défense. Il a également piloté des projets majeurs tels que le système de communication tactique et les véhicules de combat d'infanterie futuristes. Fort de nombreuses formations stratégiques, notamment à l'IHEDN de Paris, il est un universitaire accompli et titulaire d'un doctorat de l'Indian Institute of Technology de Delhi sur la politique industrielle de défense et les compensations de défense, ainsi que de diplômes en gestion et transformation. Lauréat de plusieurs distinctions et distinctions militaires indiennes et onusiennes, il conseille actuellement le ministère de la Défense sur les questions de technologies et de compensations. Il écrit pour divers magazines de défense et de sécurité et ses articles sont accessibles sur son profil LinkedIn : https://www.linkedin.com/in/rambir-mann-8333a912/

À la croisée des chemins de l'Europe en matière de sécurité : gérer les changements de politique américaine et les défis du réarmement

Prologue

Le paysage sécuritaire européen connaît en 2025 une profonde transformation, portée par les changements de politique étrangère américaine, l'évolution du rôle de l'OTAN et l'accélération des efforts de réarmement de l'Europe face aux menaces persistantes, notamment celles de la Russie suite à son invasion de l'Ukraine en 2022. Les États-Unis, s'appuyant sur une doctrine renouvelée de « l'Amérique d'abord » suite à la réélection de Donald Trump en 2024, ont recalibré leurs priorités stratégiques, caractérisées par une approche transactionnelle des alliances, un scepticisme à l'égard des engagements multilatéraux et une priorité donnée à la réduction du fardeau militaire américain à l'étranger, en privilégiant le partage des charges au sein de l'OTAN et en réorientant les ressources vers la région indopacifique pour contrer la Chine. Cette évolution a contraint l'Europe à réévaluer sa stratégie de défense, déclenchant une vague d'initiatives de réarmement sur tout le continent. Cependant, ce processus est confronté à de nombreux défis – militaires, politiques, industrielles et économiques – qu'il faut relever pour garantir un cadre de défense crédible et cohérent. Cet essai examine les principaux problèmes et aspects à prendre en compte dans ce contexte et propose des stratégies permettant à l'Europe de s'organiser efficacement, en équilibrant la défense collective de

l'OTAN et les aspirations de l'Union européenne (UE) à l'autonomie stratégique.

Contexte historique

Pour comprendre la situation difficile actuelle, il faut d'abord considérer la dépendance historique de l'Europe à la puissance militaire américaine au sein de l'OTAN. Fondée en 1949, l'OTAN a été conçue comme un pacte de sécurité transatlantique visant à dissuader l'agression soviétique, les États-Unis fournissant la majeure partie des capacités militaires, notamment la dissuasion nucléaire et le déploiement de troupes. Pendant la Guerre froide, les forces américaines en Europe ont culminé à plus de 300 000 hommes, un chiffre qui a chuté à environ 65 000 en 2025 suite aux réductions d'effectifs post-Guerre froide et aux réorientations stratégiques vers la région indo-pacifique. L'Europe, quant à elle, a bénéficié des « dividendes de la paix » dans les années 1990 et 2000, réduisant ses budgets de défense et laissant ses capacités militaires s'atrophier. La Bundeswehr allemande, par exemple, a vu sa flotte de chars passer de plus de 2 000 en 1990 à moins de 300 unités opérationnelles en 2020, tandis que la France et le Royaume-Uni maintenaient des forces expéditionnaires, mais sans l'envergure nécessaire pour assurer une défense continentale.

L'annexion de la Crimée par la Russie en 2014 a marqué un tournant, révélant les vulnérabilités de l'Europe et incitant l'OTAN à renforcer son flanc oriental avec des groupements tactiques de présence avancée renforcée. Pourtant, le leadership américain est resté essentiel, les troupes américaines constituant l'épine dorsale de ces déploiements. La guerre de 2022 en Ukraine a encore accentué cette dépendance, l'Europe peinant à approvisionner l'Ukraine en munitions en quantité suffisante, s'appuyant fortement sur les stocks américains. D'ici 2025, face à l'évolution de la politique américaine sous l'administration Trump, exigeant des alliés de l'OTAN une contribution accrue sous peine de voir leur engagement américain réduit, l'Europe se trouve à la croisée des chemins, contrainte de se réarmer tout en naviguant entre divisions internes et pressions externes. La pérennité de cette politique au-delà du mandat de Trump dépend de plusieurs facteurs, tels que les successions politiques, les intérêts structurels des États-Unis et les réponses européennes. Il convient toutefois de noter que le pivot stratégique des États-Unis vers l'Indo-Pacifique est antérieur à Trump et trouve son origine dans l'émergence de la Chine comme concurrent de sa taille. Ce consensus bipartisan, manifeste dans la Stratégie de défense nationale de 2018, signifie que les administrations post-Trump sont peu susceptibles d'inverser complètement la réaffectation des ressources hors d'Europe, même si elles assouplissent leur approche. La pérennité de la politique américaine dépend de la capacité d'adaptation de l'Europe et de l'issue des élections américaines de 2028, un scénario hybride (continuité partielle) étant le plus probable.

Menaces sécuritaires projetées à l'horizon 2050

L'environnement sécuritaire européen est appelé à évoluer considérablement d'ici 2050, façonné par la confluence de menaces militaires traditionnelles, de risques technologiques émergents et de défis non traditionnels tels que le changement climatique et l'instabilité sociétale. À partir de 2025, la guerre menée par la Russie en Ukraine, la réorientation stratégique des États-Unis et les divisions internes européennes ouvrent la voie à un paysage de menaces complexe. La Russie restera la menace la plus importante. Son invasion de l'Ukraine a revitalisé son complexe militaro-industriel, avec une production annuelle de 3 millions d'obus d'artillerie et une force mobilisée de plus d'un million de personnes. Ses tactiques hybrides, telles que les cyberattaques, la désinformation et la coercition énergétique, ciblent le flanc oriental de l'OTAN, en particulier les États baltes et la Pologne. D'ici 2050, la Russie pourrait maintenir une armée permanente de 1,5 à 2 millions de soldats, renforcée par la conscription et les améliorations technologiques. Une stabilisation du conflit ukrainien pourrait rediriger l'attention russe vers les frontières de l'OTAN, exploitant ainsi la désunion perçue de l'Occident. Les progrès de la désinformation basée sur l'IA pourraient amplifier les opérations d'influence russes et les cyberattaques contre les infrastructures européennes critiques.De plus, la militarisation de l'Arctique par la Russie pourrait dominer des zones riches en ressources d'ici 2050, mettant en péril la Norvège et le flanc nord de l'OTAN. L'Europe est ainsi confrontée à une menace conventionnelle et hybride persistante, nécessitant des défenses orientales fortifiées, une cyber-résilience et une indépendance énergétique. Dans cette entreprise, la Russie est susceptible d'être secrètement soutenue par la Chine. Bien que Pékin évite toute confrontation directe avec l'Europe, elle exploite les échanges commerciaux, les chaînes d'approvisionnement

critiques (terres rares, semi-conducteurs) et les dépendances technologiques. Les réseaux 6G et l'informatique quantique chinois, qui devraient dominer le marché mondial d'ici 2040, pourraient infiltrer les systèmes européens et permettre l'espionnage ou le sabotage. La menace des armes antisatellites, perturbant le système européen Galileo et paralysant la navigation et la coordination militaire, constituerait également une préoccupation majeure.

Défis et limites

L'objectif souvent répété de 2 % du PIB que tous les membres de l'OTAN doivent consacrer à la défense de l'Europe a permis à 23 des 31 membres de l'OTAN d'atteindre cet objectif. Cependant, des disparités qualitatives persistent. La Pologne, qui dépense 4,1 % de son PIB, peut se targuer d'une armée de 200 000 hommes en cours de modernisation, tandis que l'Allemagne, avec 2 %, déploie une Bundeswehr minée par les pénuries : seulement 20 % de ses véhicules de combat d'infanterie Puma sont prêts au combat et sa marine manque de sous-marins opérationnels. Ce partage inégal des charges compromet la crédibilité de l'OTAN en matière de dissuasion.

Un défi supplémentaire réside dans les rôles à la fois chevauchants et divergents de l'OTAN et de l'UE. La Stratégie industrielle européenne de défense (SEID) de l'UE, lancée en mars 2024, vise à renforcer l'industrie de défense du continent, en ciblant 100 milliards d'euros d'investissements conjoints d'ici 2030, afin de réduire la dépendance à l'égard de l'armement américain (qui représente 63 % des achats de l'UE). Des initiatives telles que la Coopération structurée permanente (CSP) et le Fonds européen de la défense (FED) ont stimulé des projets tels que les chars et les drones de nouvelle génération. Cependant, ces efforts risquent de dupliquer les structures de l'OTAN, de grever les budgets et d'aliéner les membres de l'OTAN non membres de l'UE comme le Royaume-Uni, la Turquie et la Norvège, dont l'exclusion pourrait briser la cohésion de l'alliance.

De même, la fragmentation politique au sein de l'UE aggrave ce problème. La Hongrie et la Slovaquie, soucieuses de ne pas contrarier la Russie, ont résisté aux sanctions et aux livraisons d'armes à l'Ukraine, se heurtant à des faucons comme la Pologne et les États baltes. Ce manque d'unité entrave la capacité de l'UE à présenter une dissuasion crédible, d'autant plus que l'OTAN s'appuie sur le consensus pour les décisions majeures. Le rôle du Royaume-Uni après le Brexit ajoute à la complexité : sa revue de défense de 2025 donne la priorité à la puissance navale et à l'AUKUS, ce qui pourrait diverger des besoins continentaux.

Par ailleurs, les efforts de réarmement de l'Europe se heurtent à d'importants goulots ~~goulets~~ d'étranglement industriels. Des décennies de sous-investissement ont fragmenté le secteur de la défense, des champions nationaux comme Nexter en France et Rheinmetall en Allemagne opérant en silos plutôt qu'à grande échelle. La production d'un seul char Leopard 2 prend 18 mois, alors que la Russie est capable de produire des T-90 remis à neuf en quelques semaines. L'objectif de l'UE de doubler sa production d'obus d'artillerie pour atteindre 1 million par an d'ici 2026 est ambitieux, mais reste en deçà des besoins collectifs de l'OTAN, estimés à 3 à 4 millions pour égaler la production russe. La pénurie de main-d'œuvre, exacerbée par le vieillissement de la population et la dépendance aux matières premières (par exemple, le titane russe), limite encore davantage les capacités. Sur le plan logistique également, les infrastructures européennes sont inadaptées à une mobilisation rapide. L'écartement des voies ferrées des États baltes, datant de l'ère soviétique, diffère des normes occidentales, ce qui retarde les transferts de troupes et d'équipements, compromettant ainsi le pilier « mobilité militaire » de la stratégie de dissuasion de l'OTAN.

Le financement du réarmement représente un défi de taille. Les analystes estiment que l'Europe a besoin de 250 milliards d'euros par an et de troupes supplémentaires pour parvenir à l'autonomie stratégique. Un défi de taille dans un contexte de stagnation économique et d'inflation oscillant entre 3 et 4 % en 2025. La résistance politique est vive dans les États du sud comme l'Italie et l'Espagne, où les ratios dette/PIB dépassent 100 %, limitant la flexibilité budgétaire. Le soutien à l'Ukraine ajoute une pression supplémentaire. L'Europe a promis 85 milliards d'euros d'aide, épuisant les stocks et détournant des fonds du réarmement national. Équilibrer ces engagements risque de créer un dilemme entre les armes et le beurre.

Sécuriser l'Europe : Options et stratégies

Pour relever ces défis, l'Europe doit adopter une stratégie à plusieurs volets qui renforce la défense collective de l'OTAN, développe les capacités dirigées par l'UE et favorise la cohésion industrielle et politique. L'OTAN demeure le principal cadre de sécurité de l'Europe et sa cohésion doit être préservée. L'Alliance devrait affiner son processus de planification de la défense (NDPP) afin de passer d'objectifs de dépenses à des objectifs capacitaires,

en attribuant les rôles en fonction des atouts nationaux : l'Allemagne pourrait se concentrer sur les brigades blindées, la France sur la défense aérienne et la Pologne sur les forces de réaction rapide. L'UE doit compléter l'OTAN en se concentrant sur les facilitateurs plutôt que sur les structures rivales. L'EDIS devrait privilégier les achats conjoints, en ciblant les systèmes à forte demande comme les systèmes de défense antimissile équivalents au Patriot et les drones de type MQ-9 Reaper, réduisant ainsi les coûts grâce aux économies d'échelle.

Les alliés peuvent stimuler le réarmement de l'Europe.

Alors que l'Europe intensifie ses efforts de réarmement en 2025 face à des menaces sécuritaires accrues, notamment de la part de la Russie, s'appuyer sur les capacités militaro-industrielles des pays amis extérieurs à l'Union européenne (UE) et à la sphère immédiate de l'OTAN offre une voie stratégique pour renforcer ses capacités de défense. Les contraintes industrielles internes à l'Europe limitent une mise à l'échelle rapide, mais des partenariats avec des alliés tels que le Royaume-Uni, le Canada, la Corée du Sud, le Japon, l'Australie et l'Inde peuvent accélérer la production, diversifier les chaînes d'approvisionnement et renforcer l'innovation technologique. À cette fin, des accords d'approvisionnement conjoints peuvent être formalisés et l'Europe peut centraliser les commandes avec ces pays dans le cadre de l'OTAN ou de l'UE, en négociant des achats groupés afin de réduire les coûts et d'accélérer les accords de livraison, de coproduction et de transfert de technologie. La création de coentreprises de production permet de localiser la production tout en exploitant l'expertise étrangère.

Exploiter les capacités de ces pays offre à l'Europe de multiples avantages, tels que la diversification de la chaîne d'approvisionnement, la rapidité et l'échelle, la maîtrise des coûts, la diversification des fournisseurs, l'atténuation des risques liés aux restrictions à l'exportation et la garantie d'une production stable, même sous la pression des sanctions. L'Europe peut ainsi transformer ces alliances en un multiplicateur de force, garantissant ainsi la sécurité dans une période d'incertitude.

Conclusion

L'Europe se trouve à un tournant en 2025. Les changements de politique américaine, l'évolution du rôle de l'OTAN et l'agression russe exigent une réponse vigoureuse. En renforçant les capacités de l'OTAN, en favorisant l'autonomie de l'UE, en favorisant l'unité industrielle et politique et en s'appuyant sur les nations amies, l'Europe peut transformer les défis en opportunités. Un plan décennal, alliant dissuasion et diplomatie, pourrait donner naissance à un continent capable de se défendre et de contribuer à la stabilité mondiale. Le chemin est ardu, mais avec détermination et coordination, l'Europe peut assurer son avenir d'ici 2035, en veillant à ce que ses efforts de réarmement d'aujourd'hui posent les bases de la paix de demain.■

Operation Sindoor: India's war on terror

Dr. Swasti Rao
IHEDN SIIP 2023

Begining of May has been momentous in India's national security narrative. Operation Sindoor, as it unfolds , is re-writing the fundamentals of India's policy towards terrorism. Apart from shelling and air raids currently underway, a brutal war of narratives is being played up across social media platforms from both sides. The fog of war is intensifying will continue to do so.

Aftermath

In the aftermath of the brutal terrorist attack in Pahalgam, where 26 Indian Hindu civilians were massacred in broad daylight, the mood across the country and its strategic community has been palpably tense, desperate to avenge the horror. As the news reverberated across the globe, familiar questions returned to the forefront: How would India respond? Would it retaliate? And if so, when and how? And how far is India willing to go?

The prevailing consensus was that New Delhi would respond with limited, precision strikes—an act of calibrated retaliation. But the element of surprise that marked India's 2019 Balakot airstrikes appeared to be absent this time. Pakistan was not only on high alert but, in many ways, seemed to be baiting India into a conflict. The diplomatic response from the international community was rather neutral. While international partners condemned the Pahalgam massacre and expressed solidarity with India, they concurrently urged both sides to exercise restraint and de-escalate. Players such as China and Turkey, unsurprisingly, leaned towards Islamabad, echoing its narrative and amplifying calls to de-escalate.

Strategic Surprise

Meanwhile, the Indian government projected an image of composure. Even as it asserted that a fitting response would follow, it appeared preoccupied with other priorities—finalizing a long-awaited free trade agreement with the United Kingdom, and announcing a caste-based census, among other pressing agendas. To many, this pause signaled a strategic choice for searching for the right timing. Meanwhile it seemed that India preferred de-hyphenating from an overriding entanglement with Pakistan in South Asia and priotitize its growth story.

As part of the official Indian delegation to DEFEA 2025, a major international defense expo in Athens, I witnessed firsthand the interest global defense and strategic community had in India's likely response and the possibility of another war. Conversations with analysts, defense officials, and industry leaders consistently circled back to India's options. What was heartening was the understanding among international experts—not just about India's military capabilities and defence industry eco-system, but also the political and strategic calculations that might influence its actions.
The consensus was sobering--India would find it difficult to catch Pakistan off guard, and any escalation would be tightly controlled.

And then, against all odds, India managed to pull off exactly that -- strategic surprise.

Operation Sindoor commenced. The name itself – evocative, symbolic, and steeped in cultural poignancy – spoke volumes. In one coordinated operation, Indian forces carried out 24 precision strikes across nine locations in Pakistan and Pakistan-occupied Kashmir. The scale and depth of these strikes, the deepest since the 1971 war, were unprecedented. In an official statement, India emphasized that the strikes had

deliberately avoided military targets, reiterating that the aim was not escalation but action against terror camps.
Initial reactions ranged from awe to skepticism. Critics were quick to point out the limited utility of attacking only terror infrastructure while leaving the primary enabler of terrorism—the Pakistani military—untouched. Their argument was not without merit. As long as Pakistan's army retains its capacity to harbor, train, and export extremist proxies, the cycle of terrorism is unlikely to be broken. Any long term strategy for countering terror from Pakistan must be multi pronged, offensive enough and capable of keeping the pressure up.

But these misgivings were soon overtaken by events on the ground.

Pakistan retaliated—predictably. The tattered country's military leadership, under pressure to assert relevance and authority, escalated the conflict. This reaction, however, only served to validate India's strategic messaging. Far from provoking an uncontrolled spiral, Operation Sindoor appears to have been a sophisticated effort to seize the narrative, demonstrate strength, and call Pakistan's long-standing nuclear bluff.
In retrospect, it was a masterstroke of strategy and timing. By appearing indifferent to immediate retaliation, the Indian leadership deftly managed domestic and international expectations. And then, by launching a comprehensive strike without much ado, it demonstrated that India retains both the political will and operational capability to act decisively. The message was unmistakable: India will not tolerate cross-border terrorism, and any future acts will invite swift and proportionate retribution.
This marks a significant shift in India's strategic posture. For decades, New Delhi operated under a policy of "strategic restraint"—an approach defined by diplomatic maneuvering, international pressure, and calculated inaction in the face of provocation. Operation Sindoor represents a departure from that philosophy. It signals the arrival of a more assertive, self-assured India—one that recognizes deterrence as a dynamic, not static, principle.

Nuclear Bluff
Perhaps the most profound implication of this shift is the diminishing potency of Pakistan's nuclear threat. For years, Islamabad has relied on its nuclear arsenal as a shield for its sub-conventional warfare strategy. That deterrent calculus will no longer work.

Operation Sindoor has showed that nuclear weapons do not confer immunity to those who export terrorism. Rather, they raise the grey zone stakes—on both sides.

The consequences are already manifesting. In the days following the strikes, cross-border shelling has intensified, leading to civilian casualties on both sides. Reports of drone incursions, air defense engagements, and downed aircraft have flooded both traditional and social media. Some reports suggest that Chinese-supplied air defense systems in Pakistan were used to down Indian fighter jets, with French and American sources now acknowledging the probable loss of at least two Indian Rafale jets. These claims are not verified by Indian sources though.

Reportedly, India has destroyed some elements-most likely a radar-- of the Chinese Air Defence installations in Pakistan using drones.

For the Indian Airforce, the entire AD spectrum that is integrated with the smallest unit on ground has been put on an ever vigilant mode.
The most likely scenario in the short term appears to be continuation of non- contact warfare using drones and missiles unless one side ups the ante.

Will Pakistan do it ? If its army decides to risk it all.

These developments underscore a vital truth about contemporary warfare: the battlefield is no longer linear. In an era of drones, cyber capabilities, and real-time surveillance, the lines

between escalation and restraint are increasingly blurred. Making analysis more complicated is the fog of misinformation and unverified claims all over social media.

Military hardware is merely a tool. Strategy, timing, narrative and political will would define any tangible outcome.

Mediation efforts

Meanwhile, diplomatic backchannels are abuzz. Saudi Arabia is reportedly mediating between New Delhi and Islamabad. Saudi officials are expected in Islamabad shortly in a bid to de-escalate tensions. Iran, backer of Pakistan, but also India's friend has dispatched its foreign affairs minister to India—ostensibly to calm tensions. Even the Taliban, in an unusual move, has called for restraint, highlighting the regional stakes.

China continues to amplify anti-India narratives through its state-controlled media, further complicating an already fraught information environment.

And yet, beneath this unfolding saga, deeper questions persist. Has the threshold for conflict irreversibly shifted? What role will international actors play in shaping the endgame? And most crucially, is the world witnessing the emergence of a new equilibrium? Is this really the era for war?

What is certain is that Operation Sindoor will be remembered as a watershed moment in India's national security strategy. It reflects not only a tactical success but a psychological one – affirming that India will not be held hostage by old paradigms or hollow bluffs.

While there is much to analyse, the subcontinent is entering a new era – one defined not by reaction, but by resolve.■

Dr. Swasti Rao is a Geopolitical Expert, Commentator and Author. She is currently Associate Professor and Associate Dean, Global Initiatives, Jindal School of International Affairs, O.P. Jindal Global University. Additionally, she is *Non- Resident Fellow* at *Eastern Circles*, Paris and a Consulting Editor to ThePrint for strategic and foreign affairs.
Dr. Rao is also **a Defence Consultant** to the **Uttar Pradesh Government** on developing the "***UP Defence Industrial Corridor***" a key undertaking of the Ministry of Defence, Govt. of India.

She has worked at the prestigious Manohar Parrikar Institute for Defence Studies and Analyses(MP-IDSA), India's premier think tank under the aegis of Ministry of Defence. At MP-IDSA, Swasti had worked on projects for Ministry for External Affairs and Ministry of Defence on European geopolitics and geo-economics. Her research project at MP-IDSA has been on **Conflicts in Europe amidst Shifting Power Structures and Europe's Indo Pacific outreach**.

Recognized as a "Geopolitical Expert" by the Government of Uttar Pradesh, India, for the G20 Summit in 2023, Dr. Rao was also honored as one of the **under-40 Young Leaders** by EICBI for substantiating India-Europe relations.

A regular commentator on IR across national and international media platforms, she writes a weekly expert's column that discusses key aspects of the geopolitical security from an Indian perspective. She hosts "WorldView with Swasti", a reputed show on strategic affairs for The Print.

She is proficient in **English**, **Hindi**, **Urdu** and **Japanese** and is currently learning **French**.

She resides in New Delhi, India, and can be reached at swastiraojnu@gmail.com. She posts at @swasrao

Opération Sindoor : la guerre de l'Inde contre le terrorisme

Début mai 2025 a été décisif pour la sécurité nationale indienne. L'opération Sindoor, telle qu'elle se déroule, réécrit les fondamentaux de la politique indienne face au terrorisme. Outre les bombardements et les raids aériens en cours, une guerre brutale de discours est alimentée sur les réseaux sociaux par les deux camps. Le brouillard de la guerre s'intensifie et continuera de s'intensifier.

Conséquences

Au lendemain de l'attentat terroriste brutal de Pahalgam, où 26 civils hindous indiens ont été massacrés en plein jour, l'atmosphère était palpable à travers le pays et sa communauté stratégique, désespérée de venger l'horreur. Alors que la nouvelle se propageait dans le monde entier, des questions familières sont revenues au premier plan : comment l'Inde réagirait-elle ? Riposterait-elle ? Et si oui, quand et comment ? Et jusqu'où l'Inde est-elle prête à aller ?

Le consensus dominant était que New Delhi riposterait par des frappes limitées et précises – une riposte calibrée. Mais l'effet de surprise qui avait marqué les frappes aériennes indiennes de Balakot en 2019 semblait absent cette fois-ci. Le Pakistan était non seulement en état d'alerte maximale, mais, à bien des égards, semblait même vouloir entraîner l'Inde dans un conflit. La réponse diplomatique de la communauté internationale a été plutôt neutre. Si les partenaires internationaux ont condamné le massacre de Pahalgam et exprimé leur solidarité avec l'Inde, ils ont simultanément exhorté les deux parties à la retenue et à la désescalade. Sans surprise, des acteurs comme la Chine et la Turquie ont penché en faveur d'Islamabad, reprenant son discours et amplifiant les appels à la désescalade.

Surprise stratégique

Pendant ce temps, le gouvernement indien affichait une image de sang-froid. Tout en affirmant qu'une réponse appropriée suivrait, il semblait préoccupé par d'autres priorités : la finalisation d'un accord de libre-échange tant attendu avec le Royaume-Uni et l'annonce d'un recensement des castes, entre autres dossiers urgents. Pour beaucoup, cette pause signalait un choix stratégique pour trouver le bon timing. Parallèlement, l'Inde semblait préférer se défaire de son implication prédominante avec le Pakistan en Asie du Sud et privilégier sa croissance.

En tant que membre de la délégation indienne officielle à DEFEA 2025, un grand salon international de la défense à Athènes, j'ai pu constater de visu l'intérêt que la communauté internationale de la défense et de la stratégie portait à la réponse probable de l'Inde et à la possibilité d'une nouvelle guerre. Les conversations avec les analystes, les responsables de la défense et les dirigeants de l'industrie revenaient systématiquement sur les options de l'Inde. Ce qui était encourageant, c'était la compréhension des experts internationaux, non seulement quant aux capacités militaires et à l'écosystème industriel de la défense de l'Inde, mais aussi quant aux calculs politiques et stratégiques susceptibles d'influencer ses actions.

Le consensus était inquiétant : l'Inde aurait du mal à prendre le Pakistan au dépourvu, et toute escalade serait rigoureusement contrôlée.

Et puis, contre toute attente, l'Inde a réussi précisément cela : la surprise stratégique.

L'opération Sindoor a débuté. Le nom lui-même – évocateur, symbolique et chargé de sens culturel – en disait long. Au cours d'une opération coordonnée, les forces indiennes ont mené 24 frappes de précision sur neuf sites au Pakistan et au Cachemire occupé par le Pakistan. L'ampleur et la profondeur de ces frappes, les plus importantes depuis la guerre de 1971, étaient sans précédent. Dans une déclaration officielle, l'Inde a souligné que les frappes avaient délibérément évité des cibles militaires, réitérant que l'objectif n'était pas l'escalade, mais une action contre les camps terroristes.
Les premières réactions ont oscillé entre la stupeur et le scepticisme. Les critiques ont rapidement souligné l'utilité limitée de s'attaquer uniquement aux infrastructures terroristes tout en laissant intact le principal moteur du terrorisme – l'armée pakistanaise. Leur argument n'était pas dénué de fondement. Tant que l'armée pakistanaise conservera sa capacité à héberger, former et exporter des intermédiaires extrémistes, le cycle du terrorisme a peu de chances d'être brisé. Toute stratégie à long terme pour contrer le terrorisme pakistanais doit être multidimensionnelle, suffisamment offensive et capable de maintenir la pression.

Mais ces appréhensions ont rapidement été dépassées par les événements sur le terrain.

Le Pakistan a riposté – comme prévu. Les dirigeants militaires du pays, sous pression pour affirmer leur pertinence et leur autorité, ont intensifié le conflit. Cette réaction, cependant, n'a fait que valider le message stratégique de l'Inde. Loin de provoquer une spirale incontrôlée, l'opération Sindoor semble avoir été une tentative sophistiquée pour s'emparer du récit, démontrer sa force et déjouer le bluff nucléaire de longue date du Pakistan.

Rétrospectivement, ce fut un coup de maître en termes de stratégie et de timing. En paraissant indifférents à des représailles immédiates, les dirigeants indiens ont habilement géré les attentes nationales et internationales. Puis, en lançant une frappe d'envergure sans trop de cérémonie, ils ont démontré que l'Inde conservait la volonté politique et la capacité opérationnelle nécessaires pour agir avec détermination. Le message était sans équivoque : l'Inde ne tolérera pas le terrorisme transfrontalier, et tout acte futur entraînera des représailles rapides et proportionnées.

Cela marque un changement significatif dans la posture stratégique de l'Inde. Pendant des décennies, New Delhi a appliqué une politique de « retenue stratégique », une approche définie par des manœuvres diplomatiques, des pressions internationales et une inaction calculée face aux provocations. L'opération Sindoor marque une rupture avec cette philosophie. Elle marque l'avènement d'une Inde plus affirmée et plus sûre d'elle-même, qui reconnaît la dissuasion comme un principe dynamique et non statique.

Bluff nucléair

L'implication la plus profonde de ce changement est peut-être la diminution de la menace nucléaire pakistanaise. Pendant des années, Islamabad s'est appuyé sur son arsenal nucléaire comme bouclier pour sa stratégie de guerre sous-conventionnelle. Ce calcul dissuasif ne fonctionnera plus.

L'opération Sindoor a démontré que les armes nucléaires ne confèrent pas l'immunité à ceux qui exportent le terrorisme. Au contraire, elles aggravent les enjeux de la zone grise, des deux côtés.

Les conséquences se font déjà sentir. Dans les jours qui ont suivi les frappes, les bombardements transfrontaliers se sont intensifiés, faisant des victimes civiles des deux côtés. Des informations faisant état d'incursions de drones, d'engagements de défense aérienne et d'avions abattus ont inondé les médias traditionnels et les réseaux sociaux. Certains rapports suggèrent que des systèmes de défense aérienne fournis par la Chine au Pakistan ont été utilisés pour abattre des avions de chasse indiens, des sources françaises et américaines reconnaissant désormais la perte probable d'au moins deux Rafale indiens. Ces affirmations ne sont cependant pas vérifiées par des sources indiennes.

Selon certaines informations, l'Inde aurait détruit certains éléments – probablement un radar – des installations de défense aérienne chinoises au Pakistan à l'aide de drones. Pour l'armée de l'air indienne, l'ensemble du spectre antiaérien, intégré à la plus petite unité terrestre, est placé en état de vigilance permanente. Le scénario le plus probable à court terme semble être la poursuite d'une guerre sans contact utilisant drones et missiles, à moins qu'un camp ne monte la barre.

Le Pakistan le fera-t-il ? Si son armée décide de tout risquer.

Ces développements soulignent une vérité essentielle de la guerre contemporaine : le champ de bataille n'est plus linéaire. À l'ère des drones, des cybercapacités et de la surveillance en temps réel, la frontière entre escalade et retenue est de plus en plus floue. Le brouillard de désinformation et d'affirmations non vérifiées qui circulent sur les réseaux sociaux complique l'analyse.

Le matériel militaire n'est qu'un outil. La stratégie, le timing, le discours et la volonté politique définiront tout résultat tangible.

Efforts de médiation

Pendant ce temps, les coulisses diplomatiques s'animent. L'Arabie saoudite jouerait un rôle de médiateur entre New Delhi et Islamabad. Des responsables saoudiens sont attendus prochainement à Islamabad afin de désamorcer les tensions. L'Iran, soutien du Pakistan mais aussi ami de l'Inde, a dépêché son ministre des Affaires étrangères en Inde, soi-disant pour apaiser les tensions. Même les talibans, dans un geste inhabituel, ont appelé à la retenue, soulignant les enjeux régionaux.

La Chine continue d'amplifier les discours anti-indiens par le biais de ses médias contrôlés par l'État, complexifiant encore un environnement informationnel déjà tendu.

Pourtant, derrière cette saga en cours, des questions plus profondes persistent. Le seuil du conflit a-t-il changé de manière irréversible ? Quel rôle joueront les acteurs internationaux dans la définition de l'issue finale ? Et surtout, le monde assiste-t-il à l'émergence d'un nouvel équilibre ? L'ère de la guerre est-elle vraiment arrivée ?

Ce qui est certain, c'est que l'opération Sindoor restera dans les mémoires comme un tournant dans la stratégie de sécurité nationale de l'Inde. Cela reflète non seulement un succès tactique, mais aussi psychologique, affirmant que l'Inde ne se laissera pas prendre en otage par de vieux paradigmes ou des bluffs creux.

S'il y a beaucoup à analyser, le sous-continent entre dans une nouvelle ère, définie non pas par la réaction, mais par la détermination.■

Note de lecture - *Reading Note*

L'Asie-Pacifique Nouveau centre du monde

Sophie Boisseau du Rocher et Christian Lechervy, 2025

Pierre Millan
IHEDN SN 42

L'Asie-Pacifique est composée de l'Asie du Nord-Est et de l'Asie du Sud-Est , comprenant 17 États et se situant au carrefour de deux océans, l'océan Pacifique et l'océan Indien.

Cette région est passée de la périphérie au centre de l'économie du monde et est devenue un modèle asiatique de développement, illustrant « le recentrage asiatique ». Pour les auteurs, cette région se trouve à l'origine de la désoccidentalisation du monde. Elle indique clairement que ce processus n'est pas seulement provoqué par l'émergence de la Chine mais qu'il se nourrit aussi de dynamiques anciennes, précoloniales et réactivées par les divers États de la région. Avec 60 % du PIB mondial et 60 % de la croissance mondiale, les puissances de l'avenir, et pas seulement la Chine, s'y trouvent. Elles retrouvent en fait la place qu'elles occupaient dans le monde avant l'arrivée des Européens.

Avec presque 800 millions de consommateurs confiants dans l'avenir,la région Asie-Pacifique est la plus dynamique du monde. Une bonne partie du trafic maritime mondial traverse l'Asie-Pacifique qui maîtrise le trafic de conteneurs. La Chine, le Japon et la Corée du Sud sont de grands constructeurs navals. Près de 54 % de la flotte mondiale s'y trouve.

Le dynamisme se traduit aussi par l'urbanisation. Parmi les 30 plus grandes villes mondiales, 21 s'y trouvent avec les *smart cities*, villes intelligentes recourant aux technologies de pointe dans les domaines les plus divers (déchets, eau, mobilité, santé, sécurité…)
Malgré le réchauffement climatique, les pays d'Asie orientale produisent de plus en plus pour leurs propres marchés, avec leurs normes, concurrençant les entreprises occidentales.

L'Asie- Pacifique dépend de moins en moins de l'Occident dans le domaine de l'innovation. Elle excelle dans le numérique. La Chine innove dans l'IA, la robotique, l'énergie, l'espace et les biotechnologies. Taïwan produit des semi-conducteurs dont 60 % partent en Chine. Les pays d'Asie du Sud-Est se distinguent dans le commerce électronique, la technologie financière, la technologie de la santé et l'IA. Des coopérations existent entre la Chine et les pays d'Asie du Sud-Est. Les pays d'Asie-Pacifique figurent parmi les plus gros exportateurs de haute technologie, la Chine étant largement en tête.

L'Asie- pacifique pourrait représenter 60 % de la croissance mondiale en 2030. Le facteur culturel explique leur réussite. Le succès repose sur l'importance de l'éducation, le respect de l'autorité et la loyauté, des caractéristiques communes à une « civilisation sinisée ». Le culte de la performance et l'ultra compétitivité sont omniprésents, avec un corollaire négatif, le suicide des jeunes à Hong Kong, en Corée du Sud, au Japon et à Singapour. Grâce aux rôles

des États, partout en Asie-Pacifique, des réformes agraires expliquent l'absence de problèmes alimentaires majeurs. L'industrialisation a fait l'objet d'impulsions gouvernementales. Les subventions aux exportations en Corée du Sud, à Taïwan et en Chine ont généré de la croissance, permettant de soutenir le processus d'exportation sur les marchés mondiaux. Partout, les interactions entre le secteur public et le secteur privé ont facilité les innovations. Les pays d'Asie-Pacifique ont fait le choix de l'ouverture régionale. À l'origine de la régionalisation se trouvent des acteurs privés, soutenus ensuite par les États. L'Union européenne renonçant aux souverainetés nationales n'a pas servi de modèle. L'harmonisation des procédures se fait sans atteinte aux souverainetés des États.

La Chine s'efforce de convaincre ses partenaires régionaux à dédollariser les transactions. Hong Kong s'implique dans la création de nouveaux instruments financiers. L'usage du yuan gagne du terrain. La Chine est un bailleur régional dans le cadre des routes de la soie.

Aspects sécuritaires : la Chine récuse la présence américaine et affirme que la sécurité de la région doit être assurée par les Asiatiques eux-mêmes. Elle revendique des territoires de l'Inde à la Russie.

Montée en puissance de la Chine dans le domaine de la défense : ayant échoué dans sa guerre contre le Vietnam en 1979, la Chine a modernisé ses forces armées, plus qu'aucun autre pays. Elle pourrait prendre l'ascendant dans le Pacifique dès 2027, grâce notamment à un programme de construction de porte-avions et de sous-marins. Avec ses missiles à longue portée, la Chine pourrait frapper le territoire américain depuis les mers qui la bordent sur 14 000 km. La coordination interarmées a progressé. Mais l'accès de la marine chinoise vers le grand large reste problématique à cause de la barrière que constitue le détroit de Bashi entre Taïwan et les Philippines.

Sur le plan diplomatique : la Chine a élaboré des partenariats stratégiques avec l'Indonésie en 2013, avec la Thaïlande en 2015, avec les Philippines en 2018. Le Cambodge entretient des relations étroites avec la Chine et lui accorde des facilités portuaires. La base de Ream pourrait recevoir des militaires chinois, comme celle de Djibouti. Quant à la Thaïlande, elle ne considère pas la Chine comme une menace et achète des armements chinois.

La marine américaine garde un avantage technologique face à la Chine mais l'a perdu sur le plan quantitatif. Elle rend visible sa présence avec des exercices et des patrouilles pour assurer la liberté de circulation.

L'Europe ne possède aucune troupe en Asie orientale. Ses États membres cherchent à vendre leurs armements. Les pays asiatiques, ne voulant pas choisir entre les États-Unis et la Chine, souhaitent une présence européenne. Néanmoins, l'Europe dispose de peu de moyens sur zone. Les pays asiatiques en sont conscients.

Trois zones conflictuelles en Asie orientale : Taïwan, Corée du Nord et mer de Chine méridionale. Mais la Chine adopte les principes de Sun Tzu, estimant que le combat doit être le dernier recours. Les pays de l'ASEAN s'accommodent en commerçant avec la Chine et en ayant des relations de sécurité avec les États-Unis. Ils ne sous-estiment pas la menace chinoise et s'efforcent de l'amortir. Une tâche difficile car la Chine agit avec dextérité sur deux tableaux, la force militaire et la diplomatie.
La désoccidentalisation s'exprime aussi dans le domaine politique. La greffe occidentale n'a pas prise. Bien que les sociétés refusent les régimes autoritaires, les procédures démocratiques n'ont pas été copiées. Si Taïwan, la Corée du Sud, le Japon et l'Indonésie adoptent certains principes démocratiques occidentaux, la démocratie n'apparaît pas comme nécessaire à la modernité. Elle est souvent perçue comme étant corrompue et instable, comme l'affirment la Chine et d'autres

pays. Elle est de plus coûteuse. À Singapour, la restriction des libertés publiques se justifie pour maintenir l'ordre et la croissance. En Chine et ailleurs, la croissance constitue la priorité.

L'Asie-Pacifique a cessé d'admirer l'Occident et le rejette de manière argumentée. Les colonisations européennes puis américaines ont produit des chocs violents et influencé les regards que les Asiatiques portent sur eux-mêmes et sur le monde. Selon la Chine, la démocratie ne garantit nullement un avenir meilleur. Les résultats qu'elle a obtenus pour sortir de la misère des millions de gens, pour l'éducation, pour la sécurité, prouvent la supériorité de son système.

L'Europe s'intéresse à l'Asie-Pacifique mais elle manque de confiance. La désoccidentalisation de cette région ne doit pas conduire à son effacement. Les pays de l'Asie orientale considèrent que l'Europe leur est utile car elle fait preuve de modération et contribue ainsi à assagir les États-Unis. Ils concluent : les Américains et les Européens ont longtemps nié leur déclin. La modernisation de l'Asie-Pacifique se fait sans occidentalisation.■

Cet article est un résumé de la recension de l'ouvrage faite par le général (2S) Alain Lamballe (Amo-IHEDN).

Asia-Pacific. New Center of the World
By Sophie Boisseau du Rocher and Christian Lechervy, 2025

Asia-Pacific is composed of Northeast Asia and Southeast Asia, comprising 17 states and located at the crossroads of two oceans, the Pacific and the Indian Oceans.

This region has moved from the periphery to the center of the world economy and has become an Asian model of development, illustrating "Asian recentering." For the authors, this region is at the origin of the de-Westernization of the world. It clearly indicates that this process is not only driven by the emergence of China but also draws on ancient, pre-colonial dynamics reactivated by the various states in the region. With 60% of global GDP and 60% of global growth, the powers of the future, and not just China, are located here. In fact, they are regaining the position they occupied in the world before the arrival of the Europeans.

With nearly 800 million consumers confident in the future, the Asia-Pacific region is the most dynamic in the world. A large portion of global maritime traffic passes through the Asia-Pacific region, which dominates container traffic. China, Japan, and South Korea are major shipbuilders. Nearly 54% of the global fleet is located there.

This dynamism is also reflected in urbanization. Among the 30 largest cities in the world, 21 are located there with smart cities, intelligent cities using cutting-edge technologies in a wide variety of fields (waste, water, mobility, health, security, etc.).

Despite global warming, East Asian countries are increasingly producing for their own markets, with their own standards, competing with Western companies.

The Asia-Pacific region is becoming less and less dependent on the West for innovation. It excels in digital technology. China innovates in AI, robotics, energy, space, and biotechnology. Taiwan produces semiconductors, 60% of which are exported to China. Southeast Asian countries stand out in e-commerce, financial technology, health technology, and AI. Cooperation exists between China and Southeast Asian countries. Asia-Pacific countries are among the largest exporters of high technology, with China leading the way.

The Asia-Pacific region could account for 60% of global growth in 2030. The cultural factor explains their success. This success is based on the importance of education, respect for authority, and loyalty—characteristics common to a "Sinicized civilization." The cult of performance and ultra-competitiveness are omnipresent, with a negative corollary: youth suicide in Hong Kong, South Korea, Japan, and Singapore. Thanks to the role of states throughout Asia-Pacific, agrarian reforms explain the absence of major food problems. Industrialization has been driven by government incentives. Export subsidies in South Korea, Taiwan, and China have generated growth, supporting the export process on global markets. Everywhere, interactions between the public and private

sectors have facilitated innovation. Asia-Pacific countries have opted for regional openness. Private actors, then supported by states, are behind regionalization. The European Union, byrenouncing national sovereignty, has not served as a model. The harmonization of procedures is carried out without compromising state sovereignty.

China is working to convince its regional partners to de-dollarize transactions. Hong Kong is involved in the creation of new financial instruments. The use of the yuan is gaining ground. China is a regional donor as part of the Silk Road Initiative.

Security aspects: China rejects the American presence and asserts that regional security must be ensured by Asians themselves. It claims territories from India to Russia.

China's rise in defense power: Having failed in its war against Vietnam in 1979, China has modernized its armed forces more than any other country. It could gain the upper hand in the Pacific as early as 2027, thanks in particular to an aircraft carrier and submarine construction program. With its long-range missiles, China could strike the US mainland from the seas bordering it for 14,000 km. Joint coordination has progressed. But the Chinese navy's access to the open sea remains problematic due to the barrier posed by the Bashi Strait between Taiwan and the Philippines.

On the diplomatic front: China developed strategic partnerships with Indonesia in 2013, with Thailand in 2015, and with the Philippines in 2018. Cambodia maintains close relations with China and provides it with port facilities. The Ream base could host Chinese troops, like the one in Djibouti. As for Thailand, it does not consider China a threat and purchases Chinese weapons.

The US Navy maintains a technological advantage over China but has lost it quantitatively. It makes its presence visible through exercises and patrols to ensure freedom of movement.
Europe has no troops in East Asia. Its member states are seeking to sell their weapons. Asian countries, unwilling to choose between the United States and China, want a European presence. Nevertheless, Europe has limited resources in the region. Asian countries are aware of this.

Three conflict zones in East Asia: Taiwan, North Korea, and the South China Sea. But China adopts Sun Tzu's principles, believing that combat should be a last resort. ASEAN countries accommodate themselves by trading with China and maintaining security relations with the United States. They do not underestimate the Chinese threat and strive to mitigate it. This is a difficult task, as China acts deftly on two fronts: military force and diplomacy.
De-Westernization is also expressed in the political sphere. The Western graft has not taken hold. Although societies reject authoritarian regimes, democratic procedures have not been copied. While Taiwan, South Korea, Japan, and Indonesia adopt certain Western democratic principles, democracy does not appear necessary for modernity. It is often perceived as corrupt and unstable, as China and other countries claim. It is also costly. In Singapore, restricting civil liberties is justified to maintain order and growth. In China and elsewhere, growth is the priority.

The Asia-Pacific region has ceased to admire the West and now rejects it with reasoned arguments. European and then American colonizations produced violent shocks and influenced the way Asians view themselves and the world. According to China, democracy in no way guarantees a better future. The results it has achieved in lifting millions of people out of poverty, in education, and in security, prove the superiority of its system.
Europe is interested in the Asia-Pacific region, but it lacks confidence. The de-Westernization of this region must not lead to its erasure. East Asian countries consider Europe useful to them because it demonstrates moderation and thus helps to temper the United States. They conclude: Americans and Europeans have long denied their decline. The modernization of Asia-Pacific is taking place without Westernization.■

This article is a summary of the book review by General (2S) Alain Lamballe (Amo-IHEDN).

Last minute
Below we recommend a presentation by Nathalie Sambhi (IHEDN SIIP 2024)

Dernière minute
Nous vous recommandons ci-dessous une intervention de Nathalie Sambhi (IHEDN SIIP 2024)

Nathalie Sambhi, Founder and Executive Director, Verve Research on CNA (Chanel Asia News), May 14th, 2025

https://youtu.be/iGGTJ7qJLJ8?si=b7heZm15R8IT1C7y&t=1455