# Souveraineté numérique : Conférence sur les fondements et frontières de la souveraineté numérique

Category: 2020-2030,Actualités,Alain Juillet,Souveraineté
1 janvier 2025

Le monde est en train de changer en passant de la domination des occidentaux à celle des BRICS. Parallèlement après avoir cru à la mondialisation depuis 1990 nous rentrons dans la multipolarité dans laquelle chaque groupe de pays veut affirmer sa spécificité et recouvrer une souveraineté mise à mal par le système occidental.

La souveraineté c'est le droit absolu d'exercer une autorité législative, judiciaire ou exécutive sur une région, un pays ou un peuple. Comme l'a défini le général De Gaulle : Tout système qui consisterait à transmettre notre souveraineté à des aéropages internationaux serait incompatible avec les droits et devoirs de la république française.

Au niveau d'un pays elle peut être politique, territoriale, économique, militaire et, pour ce qui nous intéresse, numérique.

A ce stade il faut rappeler la définition du numérique : c'est une information qui se présente sous forme de nombres, associés à une indication de la grandeur physique à laquelle ils s'appliquent, permettant les calculs, les statistiques, et la vérification des modèles.

La souveraineté numérique c'est donc tout ce qui permet à un état ou une organisation d'établir son autorité, pour exercer ses pouvoirs dans le cyberespace, en couvrant des domaines comme le contrôle des données personnelles ou la dépendance technologique.

Pour aller plus loin il faut se souvenir qu'elle est de deux ordres :

- La souveraineté numérique proprement dite concerne la propriété et fait référence à la capacité de gouverner l'infrastructure numérique. Elle permet de donner confiance aux citoyens, aux entreprises et aux administrations en contribuant à la protection de leurs données personnelles, professionnelles ou étatiques. On la mesure en identifiant au niveau des fournisseurs, des technologies, et des personnes, les endroits où un effet de verrouillage ou d'autres problèmes affectent ou peuvent affecter la souveraineté numérique

- La souveraineté des données concerne le contrôle. Elle fait référence aux lois et à la gouvernance entourant la collecte et le stockage des données. Elle repose sur l'autorité permettant de détenir des données et sert en droit générique au service des nombreux aspects liés au traitement des données numériques entre protection chiffrement transmission et stockage.

En France la RGPD établit ce qui est acceptableen matière de collecte de traitement et de stockage des données personnelles. On attend des entreprises qu'elles respectent la vie privée, qu'elles soient transparentes sur la manière de collecter et d'utiliser les données, et qu'elles leurs fournissent les outils dont elles ont besoin pour gérer leurs données.

Au niveau de l'UE dans le cadre du *Digital Cyber Act* mis en marche le 6 mars 2024, le commissaire européen Thierry Breton a fait adopter 3 textes : le *Digital Operational Resilience Act* (DORA) pour les financiers, le *Digital Service Act* (DSA) pour les contenus illégaux , et le *Digital Market Act* (DMA) pour protéger les utilisateurs européens et leurs données.

Cette souveraineté des données de l'UE est garantie par l'application de ces réglementations assurant leur protection quel que soit leur lieu de traitement ou de stockage.

Elle développe la concurrence sur les marchés numériques avec les géants du secteur. Sa mise en œuvre au niveau des enquêtes qui démarrent va permettre des sanctions réelles : ainsi Apple risque 6% d'amendes sur son CA mondial pour abus de monopole. Mais les capacités de remplacement des GAFAM par des acteurs européens est loin d'être évidente d'autant que la commission se mobilise peu pour y contribuer comme on l'a vu par exemple pour Nokia.

En complément de la souveraineté numérique et des données, il faut évoquer l'IA souveraine qui est la capacité d'une nation à développer l'IA avec des talents locaux à différents niveaux, en fonction de sa stratégie nationale en matière d'IA. Elle fait référence au contrôle exercé par un gouvernement ou une organisation sur les technologies d'IA et les données pour l'adapter à ses besoins locaux en vue de préserver ses valeurs et sa surveillance réglementaire.

Comme l'a dit Joseph Wehbe au *World Economic Forum* de Davos : Tous les gouvernements devraient travailler à lancer et développer des ecosystèmes d'IA locaux pour piloter la compétitivité économique et préserver leurs propres valeurs.

Selon la définition de Francois Jolain, la souveraineté numérique repose sur 3 piliers :

– l'électronique que l'on fabrique (hardware)
– les logiciels qui tournent (software),
– les logiciels qui offrent un service en ligne sur internet (cloud)

**Le Hardware :**

C'est la filière des infrastructures commençant par les serveurs dans les datacenters reliés par des câbles de fibres optiques à travers le monde et se terminant en périphérie par tous les appareils connectés.

Les GAFAM et les BATX investissent dans les infrastructures. Les câbles sont surveillés et interceptés non seulement par les pays traversés mais aussi sur leur parcours sous-marins.

L'ensemble repose sur l'utilisation massive de semi-conducteurs. Il y a quelques années Intel contrôlait la chaine avec un quasi-monopole. Aujourd'hui c'est très fragmenté mais la majeure partie de la fabrication se concentre sur l'Asie, principalement à Taiwan avec TSMC, Foxcom, et Mediatel mais il y en a aussi en Corée, au Japon, et en Chine avec Huawei.

La clé du process est dans la réalisation des puces. Les schémas de base sont vendus par ARM ou RISC-V en open source. La fabrication passe par un producteur sélectionné pour sa capacité selon l'épaisseur en nanomètre sachant que plus les transistors du circuit électronique sont fins plus on peut densifier le circuit et dissiper la chaleur. La plupart des producteurs font des puces de 7nm, soit environ 10.000 fois moins que l'épaisseur d'un cheveu, qui répondent à des besoins courants.

Les Hollandais d'ASML sont les seuls à faire des machines de gravure de 5nm. En position quasi monopolistique puisqu'elle est la seule capable de fabriquer des puces de 5nm, TSMC est localisée dans la zone conflictuelle de Taiwan. Pour préserver la souveraineté numérique des occidentaux, les Américains ont obtenu la création de deux usines dans l'Arizona qui seront opérationnelles fin 2026. l'UE a également obtenu qu'une usine soit construite en Allemagne. Parallèlement on est obligé de constater que, depuis l'interdiction d'achat de puces taiwanaises et de machines ASML imposée par les Américains, la Chine rattrape son retard plus vite que prévu grâce à de très gros investissement dans la recherche avec l'aide de l'espionnage technologique.

Dépendre de puissances étrangères pour le *hardware* ouvre la porte à la surveillance et aux interceptions. On l'a vu avec Cisco pour la 4G et Huawei pour la 5G. Pour limiter le risque il faut avoir des entreprises capables de concevoir et de produire en France, comme ST Micro appuyé par des labos de recherche comme le CEA Tech à Grenoble qui intéresse nos concurrents.

**Le Software :**

Il existe autant de logiciels tournant sur le *hardware* que d'usage, les plus critiques étant les systèmes d'exploitation (OS). Chacun crée une sorte de monopole car leurs applications sont conçues pour cet OS. De surcroit, plus il y a d'utilisateurs plus il y a d'applications ce qui attire plus d'utilisateurs. Le meilleur exemple est Microsoft qui propose un OS avec son ensemble d'applications permettant de répondre à tous les besoins.

Tout OS permet d'espionner son utilisateur directement ou par des *back doors*. C'est dans le *software* qu'apparaissent chaque semaine 5 000 virus nouveaux qui peuvent piller, détourner, copier ou détruire les données, ou encore organiser des demandes de rançons. Leur capacité peut aller jusqu'aux destructions massives avec des virus type *Scada* comme *Stuxnet* et *Olympic Games* qui peuvent détruire des usines iraniennes ou couper des sources d'énergies comme la lumière de villes ukrainiennes.

D'un autre côté l'exploitation des failles des OS et des applications ouvre des possibilités qui justifient les travaux de recherche pour les détecter et les éliminer. L'open source qui réduit une partie du danger et de la dépendance est devenue la norme la plus utilisée. La Gendarmerie française qui utilise un OS, basé en open source, sur Linux en est un bon exemple.

**Le Cloud**

Les Américains ont été les premiers à créer des *clouds* pour stocker des datas et créer nombre de services et logiciels en ligne. Le problème est venu des lois extraterritoriales des Etats-Unis qui permettent aux Services et administrations de pouvoir consulter et copier tout ce qui passe à travers ou utilise un élément américain.

De surcroit les différences de conception de la donnée, protégée en Europe mais commercialisée aux USA fait que des opérateurs comme, par exemple, Facebook, Tik tok ou Waze aspirent les données quand on les utilise.

Au-delà de son utilité indiscutable, le *cloud* est donc un endroit dangereux pour la sécurité des données si l'on n'y prend pas garde. Il faut toujours vérifier où sont localisés les *datacenters* et connaitre l'origine et les fonds du propriétaire du *cloud*. Ce risque réel a provoqué la création de *clouds* souverains européens et nationaux aux résultats variables car la concurrence est rude avec ceux d'outre atlantique qui sont en général moins coûteux et plus performants.

En réalité, si l'on veut vraiment sécuriser ses données, la solution passe par une évaluation hiérarchisée des données mises dans le *cloud*. On peut confier à un *cloud* américain ou international celles dont la diffusion ne représente aucun risque, à un *cloud* national celles qui sont très importantes ou essentielles, et à un *cloud* européen celles qui sont entre les deux.

La pratique montre que nous en sommes loin pour deux raisons ;

- Après l'échec du projet *Andromède,* la France ne dispose que d'un nombre très restreint de *clouds* souverains performants. De plus on est obligé de constater que les tentatives d'entrées en bourse d'OVH pour se renforcer ont été perturbées selon un processus que l'on a déjà connu chaque fois que cela pouvait pénaliser des entreprises américaines.
- En dépit des alertes et sensibilisations l'Etat et de nombreuses grandes entreprises

continuent à traiter avec des *clouds* et des sociétés américaines dans des domaines variés comme la santé les impôts ou les énergies.

Au-delà du législatif, incluant la certification et les réglementations en vigueur, de l'optimisation de la chaine opérationnelle, et de la protection des données, le maintien de la souveraineté numérique implique l'utilisation de la cyberdéfense défensive et offensive face aux prédateurs de toute sortes et de toutes origines. Face à une évolution continue des technologies et des modes d'actions utilisés par les Etats, certaines entreprises et les groupes criminels, c'est un complément indispensable pour sécuriser sa position, qui utilise des outils conçus pour cette mission.

L'efficacité de la cybersécurité suppose une définition des objectifs à atteindre, un cadrage du périmètre et une identification préalable des vulnérabilités de l'entreprise. A ce stade il faut viser large en commençant par les modes de travail, les outils et leur utilisation, les bonnes pratiques, sans oublier les actions de prévention. Il ne faut jamais oublier que sans une politique de prévention on subit. Ajoutons que le développement de la mobilité et des outils nomades renforce l'importance des communications sécurisées et les risques d'interceptions.

Vouloir une souveraineté numérique demande non seulement d'anticiper mais aussi de répondre aux attaques qui se multiplient. Ainsi en 2023 :

- 69% des attaques ciblaient des entreprises
- 20% des collectivités territoriales
- 11% des établissements de santé

Sommes-nous numériquement souverains quand :

– en janvier 2024 l'hôpital Simone Veil de Cannes est attaqué par un ransomware et le groupe Ramsay santé subit une attaque conjointe dans deux établissements

– en février France Travail subit un malware infiltré ses systèmes informatiques

– en avril Saint-Nazaire subit une attaque qui paralyse les systèmes d'information et les services municipaux tandis qu'à Pont-à-Mousson la communauté de communes doit faire face à un cryptovirus

– en mai Engie subit une cyberattaque du groupe Lapsus tandis qu'Intersport se fait voler 52 Go de données sensibles.

– et pendant tout ce temps la SNCF et la Société générale affrontent des actions de pishing sur les clients qui continuent encore aujourd'hui

Les fondements et les frontières de la souveraineté numérique concernent aussi bien la data que la régulation, l'innovation que la cyberdéfense, sans oublier la puissance numérique dans tous les domaines que nous venons d'évoquer. Leur énumération et les problèmes rencontrés

démontre qu'il est impossible pour un pays comme la France mais également pour l'Europe de contrôler toute la chaine. Notre souveraineté ne peut donc être totale. Elle ne peut être que partielle et sélective car certaines composantes doivent être partagées ou transférées. C'est à travers la liberté de choisir ce qui est transférable que s'exerce la véritable souveraineté. Le but ultime étant la protection du pays et la capacité d'assurer les fonctions essentielles à son bon fonctionnement. Cette option est donc réalisable en se focalisant sur certains niveaux et certains domaines comme les logiciels dans le *software* et dans le *cloud* ou sur des secteurs stratégiques.

Mais n'oublions pas l'évolution permanente des techniques et outils. L'arrivée du quantique risque de remettre en cause toute une partie de notre analyse et des éléments potentiels de souveraineté. Pouvant gérer d'énormes ensembles de données beaucoup plus efficacement, il va changer notre futur technologique dans de nombreux secteurs. De surcroit, il faut être conscient que ces innovations et leurs applications variées vont être amplifiée par l'intelligence artificielle.

**Alain JUILLET**
*Conférence prononcée par le président de l'AASSDN*
*Producteur de la chaine Open Box TV*
http://openboxtv.fr/emissions/

---

# Vidéo : Analyse de l'implosion syrienne après la chute du régime de Bachar al-Assad

Category: 2020-2030,Actualités,Alain Juillet
1 janvier 2025


Dans cette nouvelle émission, Alain Juillet et Claude Médori reviennent sur les événements en Syrie, notamment le départ de Bachar el-Assad et l'arrivée des islamistes à Damas. Alain Juillet nous éclaire sur les raisons de la chute de la maison Assad et ses incidences régionales et internationales sur l'échiquier géopolitique mondial.

Titre : "***L'implosion Syrienne : les analyses d'Alain Juillet***"
Durée : **00:42:08**
Date de mise en ligne : **20 décembre 2024**
Réalisé par : **Open Box TV**
Mis en ligne sur le compte YouTube d'**Open Box TV**

Vous pouvez accéder au compte YouTube d'Open Box TV en cliquant ICI

Source photo : Commons Wikimedia

## Résumé de la vidéo

La Syrie, prospère avant 2011, a été confrontée à une migration massive des populations rurales pauvres vers les villes, créant des tensions sociales. Ce phénomène a alimenté les mouvements insurrectionnels dès les premières révoltes, soutenus par des puissances étrangères. La guerre civile a opposé le régime d'Assad, appuyé par les minorités (chrétiens, Kurdes, alaouites), à des factions sunnites influencées par des courants islamistes.

**Les acteurs majeurs et la guerre civile**

1. **Occidentaux et opposition syrienne**
    - Les États-Unis et l'Europe ont soutenu des factions comme l'Armée syrienne libre. Cependant, ces groupes ont rapidement été surpassés par des mouvements

extrémistes comme Al-Qaïda et le Front Al-Nosra.
    - Des armes ont été fournies aux islamistes, entraînant des conséquences imprévues, dont l'installation de groupes djihadistes dans la région.

2. **Assad et ses alliés**
    - Le régime syrien a résisté grâce à l'appui des **Russes**, des **Iraniens** (via les Gardiens de la Révolution) et du **Hezbollah**.
    - Les Russes ont assuré une supériorité aérienne et maintenu leur influence avec des bases stratégiques (Tartous et Lattaquié).

3. **Les Kurdes et la Turquie**
    - Les Kurdes ont tenté de consolider un territoire autonome (Rojava), mais se sont heurtés à la Turquie et aux djihadistes.
    - La Turquie a joué un rôle ambigu en soutenant des groupes islamistes tout en contrôlant la zone frontalière d'Idlib.

**Conséquences de la guerre en Ukraine**

- La Russie, accaparée par le conflit en Ukraine, a réduit son soutien en Syrie, affaiblissant le régime d'Assad.
- L'absence de soutien militaire aérien a permis à des groupes islamistes, réorganisés sous la bannière de Hayat Tahrir al-Cham, de progresser.

**Réactions internationales et redistribution des forces**

- **Israël** a intensifié ses frappes sur les infrastructures militaires syriennes et a annexé des zones stratégiques, anticipant une montée en puissance des groupes djihadistes en Syrie.
- Les **États-Unis**, présents pour exploiter les ressources pétrolières syriennes, se désintéressent du conflit global.
- **Les pays du Golfe** ont renoué avec le régime syrien pour contrer l'influence iranienne.

**Futur incertain**

- La Syrie est en voie de morcellement entre différentes zones d'influence (Kurdes, alaouites, djihadistes).
- Les minorités, notamment chrétiennes, risquent de fuir en raison de l'application accrue de la charia dans les territoires islamistes.
- La chute d'Assad pourrait engendrer un vide politique, ouvrant la voie à un régime islamiste théocratique, rappelant les expériences libyenne et afghane.

**Enjeux globaux**

- La complexité du conflit illustre les limites des interventions étrangères et les conséquences imprévues de la déstabilisation des régimes autoritaires.
- La région demeure un terrain de confrontation pour des puissances comme la Turquie, l'Iran, la Russie, et les États-Unis, tandis qu'Israël prépare sa défense face à une menace djihadiste croissante.

---

# Intégration. Au 1er janvier 2025, l'espace Schengen intègre deux nouveaux pays : la Bulgarie et la Roumanie.

Category: 2020-2030,Actualités,Union Européenne
1 janvier 2025


Les frontières de Schengen s'agrandissent puisque deux pays intègrent le programme au 1er janvier 2025 : la Roumanie et la Bulgarie. Pour les touristes, c'est l'assurance de pouvoir voyager plus facilement et d'en découvrir les richesses artistiques. Mais cela place également les frontières de Schengen au niveau de la mer Noire, espace crucial des circulations et des trafics illicites. Schengen aura également une frontière commune avec la Moldavie et étend sa frontière avec l'Ukraine, Odessa n'étant qu'à 540 km de Constanta, la station balnéaire

roumaine des rives de la mer Noire. Schengen étant réputé pour laisser passer les trafics et les migrants illégaux, une telle extension de l'espace européen peut donc légitimement inquiéter. Plus que jamais, la mer Noire est l'un des épicentres de la conflictualité en Europe. Un enjeu crucial pour les années à venir.

***Pour lire l'article dans son intégralité, rendez-vous sur le site de la revue Conflits [en cliquant ICI]***

Revue Conflits avec AFP
30/12/2024

---

# Géopolitique. Entre Turquie et Azerbaïdjan, le corridor de Zangezur : un enjeu géopolitique ignoré en Europe

Category: 2020-2030,Actualités,Europe de l'Ouest,Maghreb - Moyen Orient
1 janvier 2025


***Le corridor de Zangezur est un espace crucial à l'échelle de toute l'Eurasie. C'est par lui que doivent transiter les routes de l'énergie reliant le Moyen-Orient à l'Europe. Il attise de nombreuses convoitises mais demeure sous-estimé en Europe.***

*« Il jouait du piano debout, c'est peut-être un détail pour vous, mais pour moi ça veut dire beaucoup »* chantait France Gall.

De même le corridor de Zangezur entre Arménie et Azerbaïdjan, dont nul ou presque, dans l'Union européenne et ses principaux pays-membres, ne sait grand-chose.

Pourtant, ce corridor veut dire autant pour l'avenir de la cruciale charnière intercontinentale Asie-Europe débouchant sur la mer Noire, que la guerre Russie-Ukraine, sur laquelle toute l'Europe, tout le monde atlantique, s'obnubilent à présent.

S'il est achevé, ce corridor de Zangezur reliera Kars en Turquie orientale à Bakou en Azerbaïdjan, passant par une bande de territoire arménien, le long de la frontière de l'Iran, à travers la province azérie-exclave du Nakhitchevan, que ce corridor arménien sépare justement du pays lui-même.

Corridor de Dantzig dans l'entre-deux-guerres mondiale… Corridor de Zangezur à présent… Toujours, des terres stratégiques. Un résultat inévitable : une situation de conflit émerge et s'aggrave. Dans le cas présent, d'autant plus que les enjeux sont majeurs :

**Pour R. T. Erdogan**, ouvrir ce corridor est un impératif du panturquisme ; aller droit par l'autoroute et le train, sans obstacle (chrétien, en plus), d'Ankara à Bakou, c'est l'accès direct aux « Stans » d'Asie centrale, tous turcophones (sauf le Tadjikistan) ; l'émergence d'un « Turkestan » demain rassemblé, des limites de l'Europe à celles de la Chine

**Pour l'Azerbaïdjan**, perspective immense, ce corridor réalisé l'installe au carrefour des deux cruciales connexions économiques eurasiatiques : Nord-Sud et Est-Ouest. À terme, la voie ferrée directe + autoroute Kars-Bakou en ouvre une autre, plus stratégique encore, unissant la Russie à l'Inde ; bien plus courte, donc moins cher, que toute autre à travers l'Asie centrale. La circulation directe des conteneurs Russie-Azerbaïdjan ; de là jusqu'à Mumbai (Bombay) via l'océan Indien est le rêve des pays en cause.

**La Chine** aussi surveille la situation : que Zangezur s'ouvre, raccourcirait et accélèrerait ses « Routes de la Soie ».

**Obstacle majeur cependant, l'Iran**, que le corridor de Zangezur couperait de l'Arménie. Quelle importance, diront les âmes simples. L'Azerbaïdjan, antique terre zoroastrienne (Azer = feu en Perse) – Azerbaïdjan, pays du feu et ses temples où brûle l'éternelle flamme du naphte de son sous-sol ? Pays musulman, à 60% chi'ite ? Un allié évident pour l'Iran ? Non justement : l'Azerbaïdjan est pleinement dans l'orbite turque ; et de toujours, le chi'isme perse vit dans la révérence du christianisme arménien. Pour les chi'ites perses, sans exagérer, les Arméniens chrétiens sont un peuple-Christ aussi révéré que les Juifs pour les protestants américains.

Or là, déchirement pour Téhéran : le dernier tronçon du corridor Mourmansk – Moscou – Bakou – Mumbai, doit traverser tout l'Iran, de la Caspienne à l'océan Indien, jusqu'à son port de Chabahar. La voie ferrée Iran-Azerbaïdjan (Qazvin-Rasht-Astara) est la clé du corridor international de transport Nord-Sud (INSTC), raccordant Téhéran à l'immense grille commerciale de l'UEE (Union Économique eurasienne), suscitant maints bienfaits économiques, dont des exportations massives vers l'Asie centrale et la Russie.

Là cependant sont les soucis et espoirs de demain. Aujourd'hui, la guerre menace. Depuis novembre, l'état-major de Bakou et ses drones *« Bayraktar-TB2 »* turcs reprennent la surveillance des positions arméniennes, au-dessus du Karabagh, au long des frontières

arménienne et iranienne ; survolant bien sûr le corridor de Zangezur et le Nakhitchevan.

Des intérêts économiques immenses. Un étroit corridor au fin fond d'une Arménie fragilisée. Un Azerbaïdjan qui renforce sans cesse un arsenal turc, que son pétrole lui permet d'acheter. Des chefs d'État comme V. Poutine et R.T. Erdogan, adeptes de la géopolitique au long cours. L'OTAN et l'UE happées par l'Ukraine et désormais, par la Syrie. Une conjugaison bien tentante, quand même.

**Xavier RAUFER**
Revue CONFLITS
16/12/2024

*Légende et source de la carte : L'Arménie et l'Azerbaïdjan (c) Wikipédia*

---

# Un héros silencieux (poème)

Category: 2020-2030,Actualités
1 janvier 2025

**Nous partageons un poème de Jean-Baptiste TOMACHEVSKY, membre du conseil départemental pour les anciens combattants et victimes de guerre – 2ème collège (Opex) ONACVG de la Moselle, vice-président du Souvenir Français (Lorquin 57) et ancien combattant**

Gardien des silences, veilleur des nuits,

Sous le poids du devoir, solitaire tu te tiens,
Un fusil en main, un cœur en émoi,
Face à l’innocence qui brûle dans leurs mains.

Deux bougies, deux âmes, reflet d’espoir,
Dans ce monde troublé où la paix vacille,
Un enfant lève les yeux, brûlant d’histoire,
Cherchant dans tes traits l’écho d’un exil.

Tu es l’ombre, le rempart, l’invisible lumière,
Pour eux, tu es plus qu’un soldat, tu es un homme,
Un héros silencieux sous ta lourde armure,
Qui protège leur avenir quand la nuit se fait sombre.

Que les flammes vacillantes guident ton chemin,
Que leurs regards d’enfants te rappellent demain.
Car dans chaque souffle, dans chaque silence,
C’est pour eux que tu portes l’uniforme en cadence.

Jean-Baptiste TOMACHEVSKY

# Gaza : la difficile évaluation des pertes humaines

Category: 2020-2030,Actualités
1 janvier 2025

**Les conflits actuels, notamment entre Israël et Gaza, sont marqués par des pertes humaines difficiles à quantifier précisément, souvent sources de désinformation et de polémiques. Les chiffres des victimes, contestés par les différentes parties, restent sujets à spéculation, malgré les efforts des organisations internationales pour établir une évaluation crédible.**

**Commentaire AASSDN :** Les pertes humaines des pays engagés dans les conflits actuels sont sources de désinformation compte tenu de l'importance médiatique et stratégique qu'elles revêtent .
Entre la Russie et l'Ukraine, il est très difficile de connaitre avec précision le nombre de morts, de blessés, de disparus et de prisonniers de chacune des armées.
A Gaza , sur ce territoire de 350 km2 peuplé de 2 millions d'habitants, combien de soldats israéliens ont été tués et blessés ? Seul Israël le sait avec certitude; mais combien de Gazaouis et comment distinguer les pertes des forces combattantes du Hamas des victimes civiles dites

« collatérales » au sein de la population civile ? Israël conteste les chiffres donnés par le Hamas, mais n'autorise pas des organismes internationaux à venir les vérifier.
A ce jour on peut sans doute estimer à plusieurs centaines de milliers le nombre de soldats morts dans le conflit russo-ukrainien et à plusieurs dizaines de milliers le nombre de civils tués à Gaza.

**Le nombre de morts à Gaza est source d'incertitude, de spéculation et de débats houleux. Depuis qu'Israël a déchaîné sa machine de guerre sur le territoire d'où le groupe militant Hamas a lancé sa frappe meurtrière du 7 octobre 2023, nous nous appuyons sur les données fournies par le ministère de la Santé de Gaza, dont le travail de comptage des morts lors des précédents cycles de conflit est considéré comme précis, bien qu'il ne fasse pas de distinction entre combattants et civils. La plupart des organisations humanitaires, les Nations Unies elles-mêmes et les gouvernements amis d'Israël, y compris l'administration Biden, ont largement accepté les données rendues publiques comme la meilleure mesure de ce qui s'est déroulé au cours des 14 derniers mois.**

Les responsables israéliens et leurs partisans à l'étranger se moquent des chiffres des victimes signalés à Gaza comme étant le produit gonflé des propagandistes du Hamas. Ils accusent le Hamas de s'être implanté dans les quartiers densément peuplés de Gaza. Mais la dévastation indéniable de Gaza et les centaines d'événements documentés faisant de nombreuses victimes racontent une histoire différente – une histoire que de nombreux groupes de surveillance et organisations de défense des droits de l'homme tentent d'étoffer plus en détail. (…)

Extrait article de **Ishaan THAROOR** avec **Kelsey BAKE**
The Washington Post
15 décembre 2024

*Source photo : Pixabay*

---

# Les nouveaux brouilleurs de la Force spatiale américaine

Category: 2020-2030,Actualités,Contre-espionnage,Renseignement,Technologies
1 janvier 2025

**La Force spatiale américaine est sur le point de déployer son premier lot d'un nouveau brouilleur de communications par satellite au sol dans les mois à venir – conçu pour perturber les signaux des engins spatiaux ennemis.**

Le *Space Operations Command* vient d'approuver les terminaux modulaires distants pour une mise en service initiale, a déclaré un porte-parole à Defense News mercredi, ajoutant que les brouilleurs seront entre les mains d'utilisateurs militaires sous peu.

La Force spatiale prévoit de déployer 11 systèmes dans le cadre de la première version, donnant aux unités une chance d'utiliser le système avant qu'il ne soit accepté pour les opérations. Le programme dispose d'un financement pour en construire environ 160, et le service prévoit en avoir besoin jusqu'à 200 dans les années à venir.

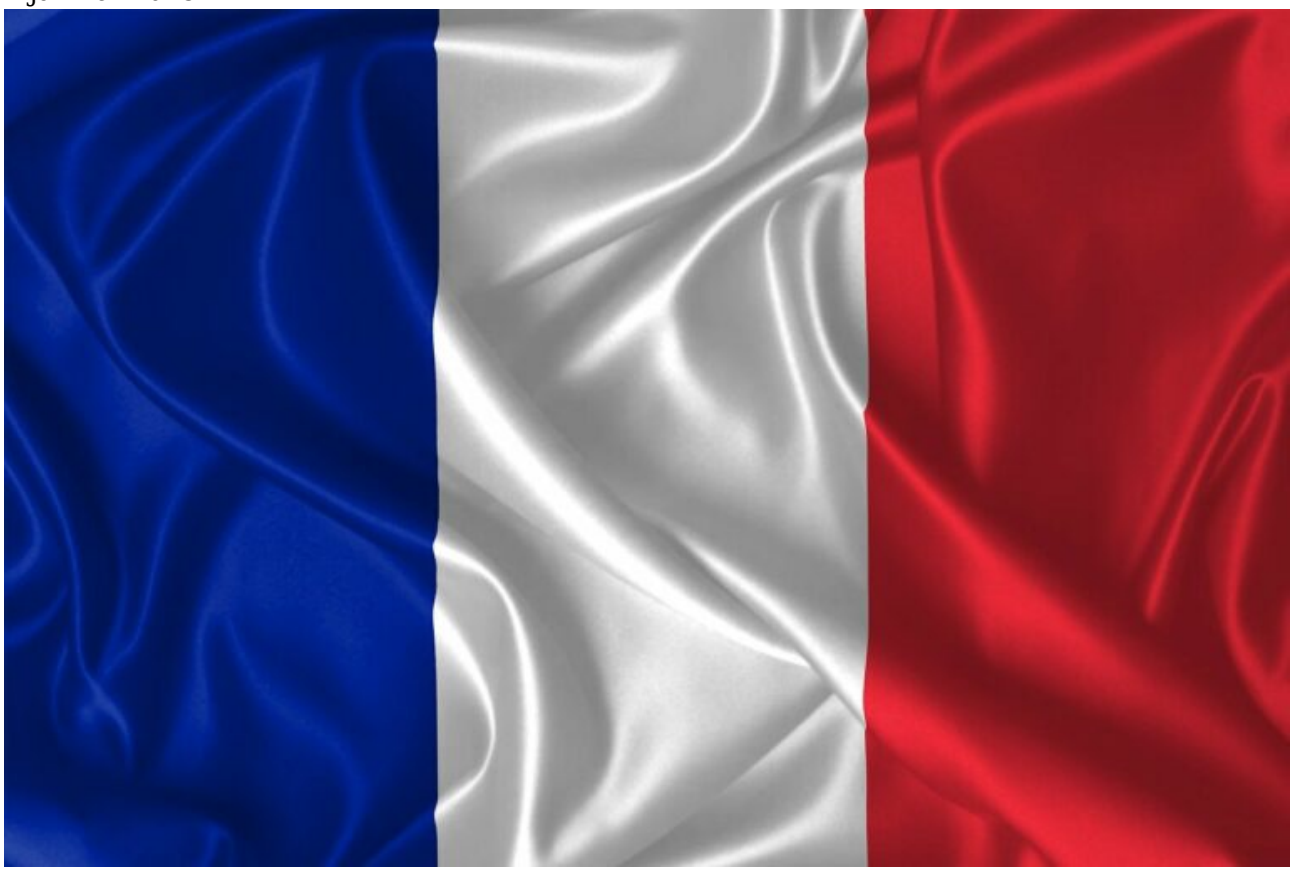
Pour lire la suite de l'article de Courtney ALBON, **cliquez ICI**

**Courtney ALBON ***
Defense News
le 19 décembre 2024,

***Courtney ALBON****
*Elle est la journaliste spécialisée dans l'espace et les technologies émergentes pour C4ISRNET. Elle couvre l'armée américaine depuis 2012, en se concentrant sur l'armée de l'air et la force spatiale. Elle a fait des reportages sur certains des défis les plus importants du ministère de la Défense en matière d'acquisition, de budget et de politique*

# Vidéo : “La France en faillite : scandale d’État”

Category: 2020-2030,Actualités
1 janvier 2025



Dans cette nouvelle émission, Alain Juillet et Claude Médori reçoivent Marc Touati, économiste reconnu, pour analyser la situation actuelle de l’économie française.

Au moment où la France traverse une crise politique sans précédent sous la Ve République, Alain Juillet et Marc Touati dressent un tableau sans concession des finances françaises et de son économie.

La France est-elle proche du défaut de paiement, de la banqueroute ? Attention, danger !

Titre : **“La France en faillite : scandale d’État”**
Durée : **00:42:04**
Date de mise en ligne : **06/12/2024**
Invité : **Marc Touati**
Publiée sur le compte YouTube : Open Box TV

# Rapport : Pour une meilleure gouvernance de l'OSINT

Category: 2020-2030,Actualités,Renseignement
1 janvier 2025

**Rapport Synopia**
**(novembre 2024)**

**En novembre 2024, Synopia, grâce au travail de son groupe d'experts de haut niveau, a publié son 2e rapport sur l'OSINT (*Open Source Intelligence*). Nous en présentons ici un résumé**.

**Commentaire AASSDN** : Le *Think tank Synopia* qui prend une place croissante dans la réflexion sociétale et stratégique vient de publier son deuxième rapport sur l'*Osint*. En quelques années le renseignement par sources ouvertes a quitté les rives des spécialistes du cyber et devenir essentiel pour les Administrations, les Services et les Entreprises. Au-delà de la technique et des outils il est réconfortant de voir que l'analyste, l'homme croisant expérience et intuition, est le maillon clé à condition qu'il ne se laisse pas submerger par l'émotion, les *a priori* et les idéologies.

Le problème est que, contrairement à beaucoup d'acteurs étrangers de tous ordres, tous n'ont pas mesuré l'utilité de ce moyen révolutionnaire qui permet de comprendre et d'anticiper. Il suffit de lire ou d'écouter les médias pour comprendre que la majorité des journalistes l'ignorent, que nos Services ont toujours du mal à intégrer une approche qui remet

en cause leurs méthodes traditionnelles, et que la plupart de nos responsables politiques ne savent pas comment utiliser cet apport essentiel pour comprendre le monde réel.

La guerre est devenue hybride, et nous n'avons pas d'amis. Dans le monde de l'information il faut savoir se battre contre les actions de toutes origines qu'elles soient d'influence de désinformation ou subversives.

L'OSINT, dont l'importance a été mise en lumière avec le conflit russo-ukrainien, consiste à utiliser une multitude d'informations accessibles en ligne pour en extraire des renseignements sur des individus, des groupes, des produits, des entreprises et des organisations militaires.

Ce processus nécessite de disposer d'**analystes qualifiés**, maîtrisant les techniques d'exploration de données et dotés d'un esprit critique pour évaluer avec précision la fiabilité et la pertinence de ces données. Mais **l'OSINT nécessite surtout de disposer de capteurs et des logiciels** qui aident les analystes à collecter, traiter et analyser plus efficacement les données de source ouverte.

Sur le plan étatique, une **vraie prise en compte de l'OSINT s'est opérée ces dernières années au sein des services de renseignement et des administrations**. Cependant, c'est au sein des entreprises privées qu'ont eu lieu les évolutions les plus importantes. En effet, au niveau commercial et entrepreneurial, **l'OSINT est devenue un instrument essentiel de l'aide à la décision**, en particulier dans le domaine de la veille concurrentielle.

En revanche, au niveau des services de l'État, l'OSINT demeure encore **un complément d'information délicat à intégrer dans la manouvre du renseignement** et parfois regardé avec méfiance, souvent par manque de formation, ou par « culture ».

La plupart du temps **utilisé de façon défensive dans notre pays**, l'information en source ouverte constitue cependant un puissant levier de la **guerre informationnelle** au travers de ses capacités d'influence, de **manipulation des esprits** (cognitif) et de **fabrication de narratifs** ou de contre-narratifs.

De nombreux pays alliés ont bien compris la **menace asymétrique** qu'il constituait et ont développé des programmes de coopération internationale, notamment pour lutter contre le terrorisme. **Mais il reste beaucoup à faire pour tirer le meilleur profit de l'OSINT**, en France comme en Europe. Le travail mené pendant deux ans par Synopia a permis de mettre en lumière la multiplicité des usages de l'OSINT, la diversité des sources d'information et la rapidité stupéfiante des évolutions technologiques.

L'application du principe de l'OSINT aux données web peut être représentée par une chaîne de valeur en six composantes, chacune assumée par des acteurs différents :

- Moteur de recherche web
- Veille web
- Alerte temps réel sur le web
- Protection du risque humain sur le web
- Influence ou contre-influence web
- Stratégie fondée sur des données web

Chaque composante peut ensuite être comprise selon trois grandes étapes de traitement des données : **le questionnement, la collecte et l'analyse**.

Des attributs transverses peuvent être associés aux solutions d'OSINT :

- Renseignement défensif et/ou offensif
- Renseignement d'origine ou d'intérêt cyber
- Enjeu de discrétion
- Enjeu de souveraineté numérique

En parallèle des enjeux techniques et opérationnels, deux autres domaines sont apparus comme essentiels :

- La formation

Il existe de multiples formations OSINT, qui consistent en l'apprentissage de techniques pour **collecter et analyser les informations publiques, et effectuer une veille stratégique**. Certaines formations apprennent également à **se prémunir des conséquences d'une analyse trop parcellaire**, partisane ou incorrectement sourcée pour une entreprise ou une institution. L'OSINT est enseigné aussi bien de manière offensive que défensive.

Notre rapport dresse un inventaire des principales formations en OSINT.

- Le cadre juridique

Les aspects juridiques, en perpétuelle évolution, sont à appréhender avec rigueur si l'on veut **rester dans le cadre légal mais aussi éthique**. Les outils de l'OSINT et l'information à laquelle ils donnent accès doivent respecter les contraintes légales et réglementaires applicables, notamment concernant la protection de la vie privée, la gestion des données, l'utilisation d'avatars et l'extra-territorialité. Là encore, **la formation des utilisateurs et des destinataires de l'OSINT est nécessaire, de même que le recours aux spécialistes** de ces enjeux très pointus (avocats, juristes et professeurs de droit). Le rapport Synopia traite ainsi des différents moyens envisageables qui permettraient d'optimiser l'utilisation de l'OSINT et **Synopia recommande qu'une impulsion politique forte structure la filière de l'OSINT**, afin de permette à l'État de mieux s'adapter aux évolutions technologiques, voire de les anticiper, et de mieux intégrer les innovations technologiques dans les processus décisionnels, en prenant garde à bien en garder le contrôle. Il en va de sa souveraineté. **Le rapport souligne aussi l'importance de préserver la liberté d'action des différentes entités** pour leur permettre de s'adapter à ce domaine si évolutif.

Pour en savoir plus, contactez Synopia : **synopia@synopia.fr**

Synopia
20, rue Georges Bizet
F-75116 Paris
www.synopia.fr

---

# Vers une stratégie durable pour la maintenance des équipements militaires

Category: 2020-2030,Actualités
1 janvier 2025

**Pour s'adapter aux bouleversements géopolitiques, la France a dévoilé une nouvelle feuille de route pour son industrie de défense. L'augmentation de la production, la refonte des normes et le développement de pôles d'excellence régionaux sont au cœur de cette stratégie.**

**Commentaire AASSDN** : L'industrie de Défense française s'articule autour de 9 grands groupes (*Thalès, Dassault, Safran, Naval Group, Airbus, KNDS*[1]*, MBDA, TechnicAtome, Arquus*), reliés à environ 4 000 sous-traitants (ETI,  PME, TPE, laboratoires et centres de recherche). Ce réseau d'entreprises est un atout majeur pour assurer à la France sa souveraineté dans le domaine de la Défense . En outre, ce réseau lui fournit  des outils lui permettant de nouer des partenariats stratégiques avec des pays qui souhaitent ne pas être

totalement dépendants de tel ou telle grande puissance (Etats-Unis ou Chine notamment ) tout en disposant de matériels de la meilleure qualité.

Par ailleurs, c'est un atout pour notre économie tant par les exportations qu'elle réalise (la France est 2e ou 3e exportateur mondial selon les années) que par le fait que l'essentiel des armements est produit en France.
Notons que les centres de recherche et les processus de fabrication de certains équipements de haute technologie, sont particulièrement visés par les Services de nos compétiteurs. C'est pourquoi la France se doit de maintenir, voire renforcer son excellence scientifique et d'assurer la meilleure protection contre les ingérences étrangères.

[1] *En 2015, les sociétés Nexter et Krauss Maffei Wegmann (KMW), respectivement systémier intégrateur du Leclerc et du Leopard, se sont regroupées au sein de KNDS afin de devenir le leader européen de la défense terrestre.*

Le 24 octobre 2024, sur le site Maîtrise NRBC de la Direction générale de l'Armement à Vert-le-Petit, le Ministre des Armées Sébastien Lecornu a dressé la feuille de route que tâchera de suivre l'industrie de défense nationale pour les années à suivre. Un mot d'ordre : relancer « *l'esprit pionnier* ». Une question se pose alors : quelles sont les forces qui motivent la transformation de la base industrielle et technologique de défense (BITD), et comment y parvenir ?

**Impulsions et transformations**

D'abord, la priorité est d'augmenter les cadences de production. Depuis février 2022, l'industrie de défense française se prépare à l'éventualité de passer en économie de guerre, avec des mesures concrètes prises par certains des principaux groupes français. Dans cette optique, *MBDA* a annoncé son intention de produire 40 missiles *Mistral-3* par mois à l'horizon 2025, ce qui revient à doubler sa production mensuelle actuelle. De son côté, la DGA apporte une nouvelle forme de support aux entreprises du secteur, avec la création de la Direction de l'industrie de Défense.

**L'Île-de-France : l'excellence terrestre, spatiale et électronique**

La région parisienne est spécialisée dans les questions spatiales, électroniques et terrestres. Le plateau de Versailles-Satory est le lieu d'implantation de plusieurs grandes entreprises à la réputation mondiale comme KNDS France (ex-*Nexter*), *Arquus* mais aussi des institutions étatiques comme la Section Technique de l'Armée de Terre. Utilisé dès l'entre-deux-guerres comme terrain d'entraînement militaire, le plateau de Satory sera de plus en plus utilisé à partir des années 1960-1970. Le plateau se transforme en 2020 avec la création de nouvelles pistes d'essais destinées aux besoins de R&D de l'Armée de terre et plus généralement de l'industrie de défense française. La région francilienne n'est pas en reste dans le domaine de l'électronique, notamment par le nombre important de clusters et des laboratoires innovants, à l'image de Paris Saclay et de l'École Polytechnique. Le secteur spatial est quant à lui représenté par *Ariane Groupe*, *Thalès*, *Airbus Defence and Space* et *Aresia*.

**L'Occitanie et la Nouvelle-Aquitaine : le cœur de l'aéronautique**

L'aéronautique est particulièrement bien développée en Occitanie et en Nouvelle-Aquitaine,

régions qui abritent de nombreux sites et entreprises majeurs, comme *Dassault Aviation* à Mérignac et Biarritz, ou encore *Safran* et *Airbus Defence & Space* à Toulouse. Cette concentration géographique est également le fruit d'une histoire riche. En effet, la création en 1915 du Centre d'Instruction des Spécialistes de l'Aviation à Bordeaux, ainsi que l'établissement de nombreuses bases aériennes dans la région, ont contribué à l'ancrage historique des industriels de l'aéronautique dans cette partie de la France.

**La région Provence-Alpes-Côte d'Azur : territoire de l'Aéronavale**

L'industrie aéronavale est très présente en PACA, avec des entreprises comme *Dassault Aviation* à Istres, *Airbus Helicopters* à Marignane et *Naval Group* à Ollioules. Cette présence s'explique par le fait que le premier hydroaéroplane a été conçu localement, créant un environnement propice au développement de ce secteur. Au cours de la Seconde Guerre mondiale, une partie des avions de chasse et des hydravions y a été produite. Post-1945, plusieurs entreprises se sont installées dans la région, notamment la *Société Nationale de Constructions Aéronautiques du Sud-Est*. Aujourd'hui, la région demeure un endroit clé dans la production et la construction d'armement et d'équipements aéronavals, tout en développant régulièrement la recherche et l'innovation.

**La Bretagne et la Normandie pour la puissance navale**

Autre pôle d'excellence, les régions bretonne et normande se sont spécialisées dans l'industrie navale, avec des implantations du géant *Naval Group* à Brest, Lorient, Nantes-Indrets et Cherbourg. L'entreprise emploie plus de 3 000 salariés en région normande, notamment sur le site de Cherbourg.

Cependant, cette territorialité se manifeste également en dehors des principaux pôles. Par exemple, on peut citer *Eurenco*, spécialiste des poudres et des explosifs, à Bergerac, ainsi que les différents sites de MBDA à Selles-Saint-Denis et à Bourges, sans oublier le site historique de production de KDNS France à Roanne. En plus de dynamiser économiquement des régions parfois en marge, cette territorialité pourrait être renforcée pour constituer une véritable force de production, notamment grâce à l'implantation d'un réseau de réservistes de la DGA.

**Des industriels étatiques en recherche d'efficacité**

Si les grands maîtres d'œuvre industriels privés sont répartis sur tout le territoire français, c'est également le cas des institutions de l'État chargées des questions d'armement et de sa maintenance. Dispersées dans toutes les régions de France, les industriels d'État sont des exemples du maillage territorial des services publics de l'armement : la Structure intégrée du maintien en condition opérationnelle des matériels terrestres, le Service de la maintenance industrielle terrestre à Versailles ainsi que les 12ème, 13ème et 14ème base de soutien du matériel, le Service de Soutien de la Flotte à Paris, Brest et Toulon, mais aussi la Direction de la Maintenance aéronautique, qui est implantée sur 17 sites différents à travers la France. La DGA est elle aussi répartie sur des centres d'expertises et d'essais dans diverses régions.

Le 2 octobre 2024 paraît le rapport d'information n°4, par la Commission des finances, à propos du maintien en condition opérationnelle des équipements militaires. Cette étude a révélé que, malgré des efforts conséquents, le maintien en condition opérationnelle ne répond pas aux besoins actuels. Les problèmes concernant la disponibilité des matériels et le coût

élevé des contrats de maintenance sont trop importants. En outre, il est question de repenser la stratégie de maintenance de l'armement français, en impliquant de façon plus directe les TPE-PME françaises. Il est par ailleurs fait mention de la possibilité de ré-internaliser une partie de la maintenance militaire, ce qui sous-entend de renforcer le maillage territorial de la maintenance. La question de l'état des recrutements a également été mentionnée, notamment la fidélisation et la formation des personnels de la maintenance militaire et du secteur de l'armement en général.

**L'humain et la formation : moteurs de développement**

Si la voie royale pour devenir ingénieur de l'armement reste Polytechnique et l'École nationale supérieure de techniques avancées, les concours restent ouverts à tous les diplômés d'écoles d'ingénieurs. En dehors des grands corps d'ingénieurs, les universités proposant des maîtrises « Défense et Sécurité » ou des cursus d'intelligence économique intéressent de plus en plus à la fois les entreprises, mais aussi les services de la DGA.

Du point de vue opérationnel, il est tout à fait possible de développer et de renforcer l'intérêt du monde ouvrier et technique pour l'industrie de défense. MBDA et *Naval Group* l'ont fait, avec respectivement 2 600 et 4 500 recrutements au cours des dernières années. Pour accélérer cette capacité à recruter, il faut également offrir plus de visibilité aux entreprises et aux institutions. Uniquement au travers de la filière de la maintenance en condition opérationnelle, 25 formations certifiantes sont ainsi proposées par le ministère des Armées et des Anciens combattants, dont plusieurs bacs professionnels et un certain nombre de BTS. En renforçant le lien Armée-Nation, voir même BITD-Nation, ainsi que la formation à tous les échelons de la BITD, la France participe à donc sa souveraineté. Ainsi, le secteur de l'armement doit se réformer, recruter et impulser si il veut retrouver son esprit « pionnier ».

**Theo MOREAU** pour le **club Défense de l'AEGE**
**22 novembre 2024**