Journée #80

Mercredi Cyber

Mercredi, 07 Janvier 2026
11h
Salle de Conférence, PC HELIOS

THÈME 80 : ETAT DE L'ART DES APPLICATIONS DE L'IA PAR LES FORCES ARMEES

- *Géopolitique de l'IA militaire*
- *Systèmes de Combat Aérien Collaboratif et Autonomie Avancée*
- *Guerre Navale et Drones de Surface Autonomes*
- *Guerre Cognitive et l'IA Générative*
- *Enjeux Éthiques*

Projet HELIOS
NB: Cet évènement intervient dans le cadre des actions de sensibilisation aux questions liées à la cybersécurité/cyberdéfense.
https://heliosc4i.github.io/cyberwednesday/

Journée #80

PRESENTE PAR: Hadrien Gayap, Msc. Ing

Projet HELIOS
NB: Cet évènement intervient dans le cadre des actions de sensibilisation aux questions liées à la cybersécurité/cyberdéfense.
https://heliosc4i.github.io/cyberwednesday/

Etat de l’art des Applications de l’IA par les Forces Armées

HELIOS - CAMEROUN

Présenté par : Hadrien Gayap, Msc. Ing.

AGENDA

Plan de la Présentation

01

Intelligence Artificielle

Définitions fondamentales et composantes technologiques de l'IA militaire moderne

02

Géopolitique de l'IA

Doctrines stratégiques des grandes puissances et acteurs émergents

03

Combat Aérien

Systèmes collaboratifs et autonomie avancée dans le domaine aérien

04

Guerre Navale

Drones de surface autonomes et révolution maritime

05

Guerre Terrestre

Robotique, systèmes intégrés et automatisation du champ de bataille

06

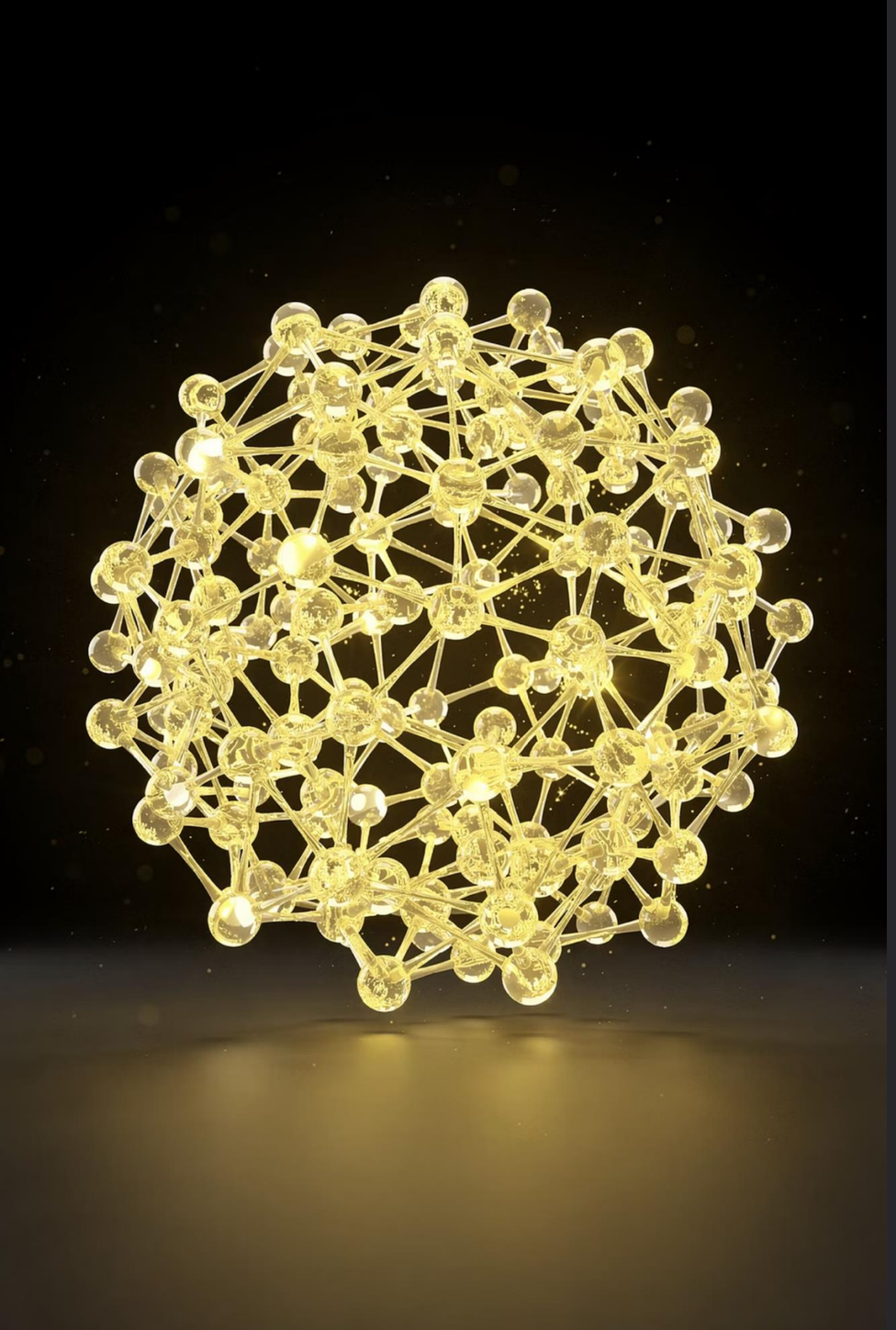
Guerre Cognitive

IA générative et manipulation de l'espace informationnel

07

Enjeux Éthiques

Controverses du ciblage automatisé et cadres réglementaires



CHAPITRE 1

Intelligence Artificielle : Définitions

Définitions et Fondements

Qu'est-ce que l'Intelligence Artificielle ?

L'Intelligence Artificielle (IA) désigne l'ensemble des théories et techniques mises en œuvre pour créer des machines capables de simuler l'intelligence humaine.

L'année 2025 marque une rupture fondamentale où l'IA transite du statut de catalyseur expérimental à celui de colonne vertébrale opérationnelle des conflits modernes.

Les théâtres d'opérations contemporains servent de laboratoires validant des concepts doctrinaux tels que la "guerre intelligentisée" chinoise ou l'approche de "masse attritable" américaine.

> *"La domination de la décision"* - la capacité de percevoir, comprendre et agir plus vite que l'adversaire grâce à des architectures cognitives automatisées.

Les Composantes Fondamentales de l'IA Militaire

Perception & Vision

Traitement d'images et vidéos pour la reconnaissance automatique de cibles (ATR), surveillance ISR, navigation autonome et détection d'anomalies en temps réel

Apprentissage Machine

Algorithmes supervisés, non-supervisés et par renforcement permettant l'amélioration continue des performances sans programmation explicite

Traitement Langage

Grands Modèles de Langage (LLM) pour l'analyse de renseignement, traduction automatique, génération de rapports et aide à la décision

Réseaux Neuronaux

Architectures profondes (Deep Learning) mimant le fonctionnement du cerveau pour résoudre des problèmes complexes de classification et prédiction

Technologies Clés et Architecture

Edge Computing Militaire

Le traitement en périphérie (edge computing) permet l'exécution d'algorithmes d'IA directement sur les plateformes tactiques (drones, véhicules, capteurs) sans dépendance aux communications satellites. Cette approche est critique dans les environnements contestés où les liaisons peuvent être brouillées ou coupées.

- Processeurs embarqués (Jetson Nano, TPU)
- Modèles optimisés légers (YOLO, MobileNet)
- Fonctionnement en mode déconnecté
- Latence réduite pour décisions temps-réel

Cloud Brain & Fusion de Données

Les architectures cloud centralisées permettent la fusion de données multi-sources (satellites, drones, capteurs sol) pour créer une image opérationnelle commune. Ces "cerveaux cloud" effectuent l'analyse stratégique et la planification de missions complexes.

- Fusion multi-capteurs temps-réel
- Analyse prédictive logistique
- Commandement et contrôle distribué
- Maintenance prédictive des flottes

Niveaux d'Autonomie des Systèmes Militaires

Niveau 1 : Contrôle Humain Direct

Systèmes télé-opérés nécessitant un pilotage constant. Exemple : drones FPV ukrainiens guidés manuellement jusqu'à l'impact.

Niveau 2 : Assistance Automatique

Systèmes effectuant des tâches spécifiques (maintien d'altitude, évitement d'obstacles) sous supervision humaine.

Niveau 3 : Autonomie Conditionnelle

Systèmes exécutant des missions complètes avec intervention humaine en cas de situations imprévues. Exemple : drones de patrouille ISR.

Niveau 4 : Haute Autonomie

Systèmes prenant des décisions tactiques autonomes dans un cadre opérationnel prédéfini. Exemple : défense anti-missile automatisée.

Niveau 5 : Autonomie Complète

Systèmes d'armes létaux autonomes (LAWS) capables de sélectionner et engager des cibles sans intervention humaine - hautement controversés.

Algorithmes et Techniques Dominants

Réseaux Convolutifs (CNN) (CNN)

Architecture dominante pour la vision par ordinateur. Les CNN analysent les images par couches successives, extrayant des caractéristiques de plus en plus abstraites pour identifier chars, avions ou combattants.

Apprentissage par Renforcement

Technique où l'IA apprend par essai-erreur dans des simulations. Utilisée pour entraîner des agents autonomes au combat aérien, comme démontré avec le X-62 VISTA battant des pilotes humains.

Transformers & LLM

Architecture révolutionnaire derrière les grands modèles de langage (GPT, BERT). Applications militaires : analyse de renseignement, traduction tactique, génération de rapports automatisés.

Réseaux Antagonistes (GAN) (GAN)

Deux réseaux neuronaux en compétition créent des contenus synthétiques ultra-réalistes. Utilisés pour les deepfakes, l'entraînement en simulation et la génération de scénarios tactiques.

CHAPITRE 2

Géopolitique de l'IA Militaire

La restructuration des forces armées mondiales autour de l'IA reflète des divergences doctrinales profondes, influencées par les contraintes économiques, les cultures stratégiques et les impératifs géopolitiques immédiats. Trois superpuissances technologiques dominent cette course : les États-Unis, la Chine et la Russie, chacune développant une vision distincte de la guerre algorithmique.

États-Unis : Domination par la Déréglementation

La stratégie américaine en 2025, cristallisée dans la nouvelle National Security Strategy et l'Executive Order 14179, opère un virage radical vers la dérégulation pour maintenir l'hégémonie technologique face à la Chine. L'administration a explicitement révoqué les cadres éthiques antérieurs jugés trop restrictifs, privilégiant une approche agressive visant la "domination globale de l'IA" pour la sécurité nationale.

Stratégie de "Jeu Défensif" Technologique

- **Contrôles d'exportation draconiens** sur puces avancées (NVIDIA H100, A100)
- **Restriction des "poids de modèles fermés"** - innovation 2025 empêchant adversaires d'accéder aux paramétrages internes
- **Coalition des Démocraties Technologiques** avec alliés OTAN, Japon, Corée du Sud
- **Sanctions sur chaînes d'approvisionnement** ciblant fournisseurs chinois de composants IA

Initiative Replicator

Programme phare du Pentagone visant à contrer la masse numérique de l'APL chinoise par des milliers de systèmes autonomes sacrifiables (attributables) à bas coût, avec production rapide à l'échelle industrielle.

Initiatives Technologiques Américaines Majeures

Third Offset Strategy

Doctrine visant à maintenir la supériorité militaire non par la masse, mais par l'avantage technologique. Focus sur systèmes autonomes, réseaux de capteurs distribués et combat collaboratif homme-machine.

JADC2 (Joint All-Domain C2)

Architecture de commandement unifiant tous les domaines de guerre. L'IA fusionne données air-terre-mer-espace-cyber pour accélérer la boucle décisionnelle (OODA Loop) et permettre "kill chains" de quelques secondes.

Project Maven

Programme pionnier utilisant l'IA pour analyser automatiquement les gigaoctets de vidéos de drones ISR. Détection et suivi automatique de personnes et véhicules, libérant les analystes pour interprétation de haut niveau.

DARPA ACE & Air Combat

Programmes développant pilotes IA pour combat aérien autonome. Tests X-62 VISTA ont démontré victoires contre pilotes humains experts, validant l'approche pour CCA (Collaborative Combat Aircraft).

Le secteur privé américain (Silicon Valley) demeure le moteur d'innovation avec entreprises comme Anduril, Palantir, Shield AI et Scale AI fournissant technologies de pointe au DoD via processus d'acquisition accélérés.

Chine : La Guerre Intelligentisée et Fusion Fusion Civil-Militaire

La République Populaire de Chine poursuit une trajectoire distincte, conceptualisée sous le terme de "guerre intelligentisée" (intelligentized warfare).

Contrairement à l'approche occidentale focalisée sur des plateformes spécifiques, la Chine vise une intégration systémique où l'IA coordonne l'ensemble des domaines de guerre (terre, air, mer, espace, cyber, cognitif) dans une vision holistique du conflit moderne.

Doctrine Chinoise : Intégration Totale

Stratégie de Fusion Civil-Militaire (MCF)

Le modèle chinois mobilise les géants technologiques (Baidu, Alibaba, Tencent, Huawei) pour soutenir directement les projets de l'Armée Populaire de Libération. Cette synergie permet un transfert bidirectionnel de technologies entre secteurs civil et militaire, accélérant l'innovation.

- Baidu : LLM ERNIE pour analyse renseignement
- Tencent : Reconnaissance faciale tactique
- Alibaba : Logistique prédictive Cloud Brain
- DJI : Drones commerciaux militarisés
- Huawei : Infrastructure 5G pour C4ISR

Réduction de l'Écart Technologique

Le rapport 2025 du Département de la Défense américain au Congrès souligne que la Chine a considérablement réduit l'écart, notamment dans les Grands Modèles de Langage et le raisonnement algorithmique, malgré les restrictions d'exportation sur semiconducteurs avancés.

> La doctrine chinoise envisage une "guerre totale nationale", où l'IA sert à mobiliser les ressources économiques et industrielles en temps réel pour soutenir l'effort de guerre.

Capacités Chinoises en Développement

1

2023-2024 : Essaims de Drones

Démonstrations publiques d'essaims de plus de 1000 drones coordonnés par IA pour saturation défenses adverses. Technologies commerciales DJI adaptées pour applications militaires SWARM.

2

2024-2025 : LLM Militaires

Développement de modèles de langage spécialisés (ERNIE Military, PLA-GPT) pour assistance commandement, analyse de renseignement multilingue et planification opérationnelle automatisée.

3

2025 : Logistique Intelligente

Déploiement système "Cloud Brain" logistique avec visibilité totale stocks, dispatching dynamique par IA et intégration logistique civile (JD Logistics) pour mobilisation nationale rapide.

4

2025-2026 : Combat Naval Autonome

Tests de véhicules de surface sans pilote (USV) et sous-marins autonomes (UUV) pour missions anti-navire et mouillage de mines intelligent en Mer de Chine méridionale.

Russie : Pragmatisme de Survie et Alliance CRINK

L'approche russe est dictée par les nécessités existentielles de la guerre en Ukraine.

Loin des concepts futuristes, Moscou intègre l'IA pour résoudre des problèmes tactiques immédiats : pénurie de main-d'œuvre qualifiée, besoin de précision d'artillerie améliorée et supériorité en guerre électronique face aux systèmes OTAN.

En 2025, la Russie s'appuie fortement sur une coalition de facto désignée par les analystes comme l'axe **"CRINK"** (Chine, Russie, Iran, Corée du Nord). Cette alliance technologique informelle permet à la Russie d'accéder à composants et logiciels IA chinois pour ses drones Orlan et Lancet, technologies de guerre électronique iraniennes pour USV Shahed maritimes, et munitions nord-coréennes pour saturation.

Les rapports de renseignement US révèlent que 70% des composants électroniques russes de nouveaux systèmes d'armes proviennent de contournement sanctions via pays tiers.

Innovations Russes : Guerre Électronique Cognitive

Système Bylina (RB-109A)

Innovation majeure : système de guerre électronique utilisant l'apprentissage automatique pour analyser le spectre électromagnétique en temps réel. L'IA détecte, classifie et priorise automatiquement les cibles (radars HIMARS, drones Switchblade, communications Starlink) et optimise le brouillage pour éviter interférences fratricides. Son efficacité augmente les capacités de GE russes de 30-40%, causant pertes significatives de drones ukrainiens dans zones contestées.

Drones Lancet-3 avec IA

Munitions rôdeuses équipées de vision par ordinateur pour reconnaissance automatique de cibles (ATR).

Peuvent identifier et engager véhicules blindés ukrainiens de manière autonome même en environnement de brouillage GPS, utilisant navigation inertielle et verrouillage optique terminal.

Robot UGV Marker

Véhicule terrestre sans pilote déployé en petit nombre dans le Donbass comme banc d'essai. Utilise vision par ordinateur pour navigation autonome en terrain complexe et engagement de cibles. Sert à développer algorithmes d'essaimage et coopération drone-robot pour futures opérations de masse.

Automatisation Systèmes Hérités

Modernisation de plateformes soviétiques (chars T-72, artillerie 2S19) avec kits IA pour visée assistée, acquisition automatique de cibles et intégration aux réseaux de commandement numériques, compensant obsolescence matérielle par supériorité logicielle.

OTAN et Alliés : Interopérabilité Responsable

L'Alliance Atlantique navigue entre l'impératif d'adoption rapide de l'IA et le respect des normes démocratiques et du droit international humanitaire. La stratégie IA révisée de l'OTAN (2024-2025) établit un cadre pour développement éthique et interopérable des capacités autonomes entre les 32 États membres.

Priorités Stratégiques de l'OTAN

Interopérabilité Technique

Défi majeur : 32 armées nationales avec systèmes hétérogènes. L'OTAN développe standards communs (STANAG AI) pour permettre partage de données et coordination IA entre plateformes américaines, européennes et autres alliés.

Centres de Test & Validation

Établissement de centres d'excellence IA (Pays-Bas, Estonie) pour tester fiabilité, robustesse et résilience des algorithmes face aux attaques adverses avant déploiement opérationnel.

Principes d'Utilisation Responsable

Cadre éthique : contrôle humain approprié, transparence des décisions IA, accountability juridique, biais algorithmiques, protection civils, conformité droit international humanitaire (DIH).

Accélérateur DIANA

Defence Innovation Accelerator for the North Atlantic : programme soutenant startups deeptech européennes développant solutions IA duales (civil-militaire) via financement et accès aux marchés OTAN.

Contrairement aux approches sino-russe autoritaires ou américaine dérégulée, l'OTAN tente une "troisième voie" conciliant innovation technologique et valeurs démocratiques, bien que certains experts questionnent si cette approche peut maintenir compétitivité face à adversaires moins contraints.

Comparatif Doctrinal : Quatre Visions de l'IA Militaire

Indicateur	États-Unis	Chine	Russie	OTAN
Concept Central	Third Offset / Replicator Mass	Intelligentized Warfare	Modernisation Adaptative	Interopérabilité Responsable
Priorité Tactique	Masse autonome & CCA	Commandement Cognitif Unifié	Guerre Électronique & UGV	Logistique & ISR
Approche Éthique	Dérégulation (EO 14179)	Contrôle Étatique Total	Non-Contrainte	Principes PRUs
Source Innovation	Silicon Valley (Anduril, Palantir)	Fusion Civil-Militaire (BAT)	Complexe Militaro-Industriel + Import	Écosystème DIANA
Budget IA 2025	~18 Mrd USD (DoD)	~25 Mrd USD (estimé)	~2 Mrd USD (public)	Fragmenté (national)
Doctrine LAWS	Opposition régulation contraignante	Développement sans limites	Déploiement pragmatique	Support régulation ONU

CHAPITRE 3

Systèmes de Combat Aérien Collaboratif

L'évolution la plus marquante dans le domaine aérien est l'abandon progressif du concept de "télépilotage" au profit de la "collaboration équipage-machine" (Manned-Unmanned Teaming - MUM-T), où l'IA agit comme un allié autonome capable de prendre des décisions tactiques indépendantes dans le cadre d'une mission coordonnée.

Programme CCA : Révolution de la Supériorité Aérienne

Le programme Collaborative Combat Aircraft (CCA) de l'US Air Force incarne la vision américaine de la supériorité aérienne future. Il ne s'agit plus de simples drones télépilotés, mais d'avions de combat autonomes dotés d'intelligence artificielle volant aux côtés des chasseurs de 5ème génération (F-35 Lightning II) et 6ème génération (NGAD - Next Generation Air Dominance) comme de véritables ailiers.

En décembre 2025, l'USAF a sélectionné neuf fournisseurs pour la phase de raffinement de l'Incrément 2, signalant une accélération massive du programme avec objectif de production à l'échelle industrielle dès 2027-2028.

Concept Opérationnel

Un chasseur F-35 piloté contrôle 2-4 CCA autonomes qui précèdent le chasseur dans les zones dangereuses, effectuent suppression défenses ennemies (SEAD), reconnaissance, et saturation des systèmes adverses.

Capacités CCA de Nouvelle Génération

- **Autonomie de Mission** : Navigation, évitement de menaces et exécution de tactiques sans commandes pilote constantes
- **Combat Air-Air** : Engagement autonome de cibles aériennes hostiles avec missiles AIM-120 ou futurs LREW
- **Suppression SEAD/DEAD** : Destruction radars et défenses sol-air avec missiles anti-radiation AGM-88
- **ISR Avancé** : Collecte renseignement en zone contestée avec capteurs EO/IR et SIGINT
- **Attrition Acceptable** : Coût unitaire 20-30M$ vs 80M$ F-35 permet engagement dans missions à haut risque

Anduril Fury : Architecture Lattice et Apprentissage

Plateforme Logicielle Lattice

Le système Anduril Fury (désignation YFQ-44A) repose sur l'architecture logicielle "Lattice", un système d'exploitation militaire modulaire et ouvert permettant une autonomie de mission sophistiquée. Lattice fusionne les données de multiples capteurs (radar, EO/IR, RF, datalinks) pour créer une image tactique unifiée et permet à l'IA de prendre des décisions en millisecondes.

L'innovation majeure réside dans l'utilisation de l'**apprentissage par renforcement** (Reinforcement Learning) pour entraîner l'IA au combat aérien. Dans des millions de simulations, l'algorithme apprend par essai-erreur à optimiser les manœuvres, la gestion de l'énergie et l'emploi des armes contre différents adversaires.

Validation X-62 VISTA

Les tests sur l'avion expérimental X-62 VISTA (Variable In-flight Simulator Test Aircraft) ont démontré la viabilité du concept. L'IA Fury a affronté des pilotes de chasse experts de l'US Air Force dans des combats tournoyants (dogfights) simulés et a remporté des victoires consistantes, validant la maturité de l'approche pour déploiement opérationnel.

> "L'IA ne se fatigue jamais, ne ressent pas le stress, et peut calculer des milliers de trajectoires possibles simultanément."

Munitions Rôdeuses Intelligentes : Switchblade 600 Block 2

Caractéristiques Techniques

- Portée : 110 km
- Endurance : 50 minutes
- Charge militaire : 15 kg (anti-blindage)
- Poids total : 23 kg (portable)
- Déploiement : 10 minutes (tube)

L'évolution des munitions rôdeuses (loitering munitions) illustre la descente de l'IA vers l'échelon tactique des petites unités. Le **Switchblade 600 Block 2** d'AeroVironment, déployé massivement en Ukraine et par les forces spéciales US en 2025, représente un saut qualitatif majeur.

Reconnaissance Automatique de Cibles (ATR)

Contrairement aux versions précédentes nécessitant un pilotage constant via liaison vidéo, le Block 2 intègre des capacités de vision par ordinateur avancées.

L'IA embarquée, fonctionnant sur processeur edge computing, peut détecter, classifier et engager des cibles statiques ou mobiles de manière autonome, même en environnement de brouillage GPS ou coupure liaison satellite.

Cette autonomie permet à l'opérateur de se concentrer sur la **validation éthique et légale de la frappe** plutôt que sur le pilotage technique, réduisant la charge cognitive et améliorant le respect du droit des conflits armés.

Technologies Clés du Combat Aérien Autonome

Fusion Multi-Capteurs

Intégration radar AESA, électro-optique infrarouge (EO/IR), détecteurs d'alerte missile (MWS) et récepteurs d'avertissement radar (RWR) dans image tactique unifiée traitée par IA pour conscience situationnelle supérieure.

Apprentissage par Renforcement

Entraînement dans millions de simulations combat aérien permettant à l'IA de découvrir tactiques optimales, gestion énergie et emploi armes contre profils adversaires variés (chasseurs russes Su-57, chinois J-20).

Communications Résilientes

Liaisons de données tactiques à faible probabilité d'interception (LPI) et résistantes au brouillage, permettant coordination essaim de CCA même en environnement électromagnétique contesté. Redondance par routage mesh.

Contre-Mesures IA Adverses

Algorithmes robustes contre attaques adversariales (adversarial attacks) où adversaire tente de tromper systèmes vision par ordinateur via patterns spécifiques ou de compromettre modèles via empoisonnement données.

CHAPITRE 4

Guerre Navale et Drones de Surface Surface Autonomes

Le conflit en Mer Noire (2022-2025) a démontré qu'une flotte de drones navals peu coûteux, pilotés par intelligence artificielle, peut neutraliser une marine conventionnelle majeure, remettant fondamentalement en cause les doctrines navales séculaires basées sur la supériorité des navires capitaux. Cette révolution maritime s'étend désormais à tous les théâtres : Mer Rouge, Détroit d'Ormuz, Indo-Pacifique.

L'Écosystème Ukrainien : De Kamikaze à Plateforme Multi-Rôle

Magura V5 (GUR) - Évolution Capacitaire

Le drone de surface Magura V5, développé par le renseignement militaire ukrainien (GUR), illustre l'évolution rapide des capacités USV.

Initialement conçu comme simple engin explosif pour attaques kamikazes contre navires russes en Mer Noire, le système a subi des améliorations radicales en 2024-2025 pour devenir une véritable plateforme de combat multi-missions.

- **Autonomie** : 800 km (opérations profondes)
- **Charge utile** : 300 kg (explosifs ou armements)
- **Vitesse** : 80 km/h (interception difficile)
- **Guidage** : GPS + inertiel + IA visuelle pour navigation terminale

An unmanned marine vehicle, Magura V5, was found by fishermen off the coast of Yoroz Port, Trabzon, Türkiye, Sept. 30, 2025. (AA Photo).

Innovation Majeure 2025

Intégration missiles R-73 (air-air soviétiques modifiés) permettant au Magura d'abattre hélicoptères russes Ka-52 effectuant patrouilles anti-USV. Première défense air-air autonome depuis plateforme surface sans équipage.

Sea Baby : Puissance de Feu et Variante Submersible

SBU attack at Novorossiysk. Screenshot from SBU video.

L'existence opérationnelle du Sub Sea Baby bouleverse les calculs de défense portuaire. Les ports, considérés comme sanctuaires sécurisés, deviennent vulnérables à des attaques asymétriques par essaims de véhicules sous-marins autonomes à bas coût (estimé 250 000 $ par unité vs milliards pour sous-marin conventionnel).

Asymétrie Houthie en Mer Rouge : Blocus Algorithmique

Le groupe Houthi (Ansar Allah) au Yémen a mis en place un blocus naval effectif en Mer Rouge et Golfe d'Aden depuis octobre 2023, utilisant une combinaison de missiles balistiques anti-navire, missiles de croisière et USV fournis par l'Iran. L'analyse technique révèle que leurs véhicules de surface, bien que souvent qualifiés d'"engins explosifs improvisés", disposent de kits de guidage terminaux sophistiqués.

Modèle "Blowfish" et Autonomie IA

Le principal USV houthi, désigné "Blowfish" par les analystes, utilise des capteurs électro-optiques pour verrouiller la silhouette d'un navire ou des récepteurs RF (radio-fréquence) pour cibler ses émissions radar/radio.

Une fois dans la zone cible (10-20 km), le système opère en mode autonome "fire-and-forget", rendant le brouillage inefficace.

Impact Stratégique

Plus de 80 attaques depuis oct. 2023, forçant réacheminement du trafic commercial via Cap de Bonne-Espérance (+40% coûts transport). Coût défense occidentale : missiles SM-6 à 4M$ pour intercepter drones à 20 000$.

Courbe de Coûts et Dilemme Défensif

$20K	$4M	200:1	80+
Coût USV Houthi	**Missile SM-6 US Navy**	**Ratio Coût-Échange**	**Attaques Documentées**
Véhicule surface explosif avec guidage terminal IA, produit localement avec composants iraniens et chinois disponibles commercialement	Intercepteur Standard Missile-6 utilisé par destroyers américains pour défense anti-aérienne et anti-surface contre menaces asymétriques	Asymétrie économique insoutenable : chaque interception coûte 200x la valeur de la menace, épuisant stocks munitions défensives occidentales	Nombre d'incidents contre navires commerciaux et militaires en Mer Rouge depuis octobre 2023, forçant réorganisation routes maritimes mondiales

Cette asymétrie économique impose une courbe de coûts insoutenable aux marines occidentales. La solution requiert des contre-mesures IA à bas coût : drones intercepteurs autonomes, lasers haute énergie guidés par IA, ou essaims de défense coordonnés par algorithmes.

Technologies de Guidage des USV Autonomes

Phase Croisière : GPS/GNSS

Navigation satellitaire pour transit longue distance. Vulnérable au brouillage et spoofing, nécessitant navigation inertielle (INS) de secours avec correction périodique.

Navigation Inertielle

Systèmes gyroscopes et accéléromètres calculant position par dead reckoning en environnement GNSS dégradé. Dérive cumulative nécessite corrections visuelles ou magnétiques.

Guidage Terminal IA

Vision par ordinateur (réseaux neuronaux convolutifs) pour reconnaissance et verrouillage optique de la cible. Fonction en mode totalement autonome "fire-and-forget".

Homing Passif RF

Détection et poursuite des émissions radio/radar du navire cible. Permet guidage sans émission active, rendant détection précoce difficile pour défenseurs.

CHAPITRE 5

Guerre Terrestre, Robotique et Systèmes Intégrés

Sur le champ de bataille terrestre, l'intelligence artificielle transforme radicalement la boucle "capteur-tireur" (sensor-to-shooter) en réduisant les délais de traitement de l'information de plusieurs minutes à quelques secondes. Cette compression temporelle, couplée à la robotisation progressive des plateformes, redéfinit les tactiques d'infanterie, d'artillerie et de manœuvre blindée.

Système Delta : Épine Dorsale Numérique Ukrainienne

Le système de gestion du champ de bataille **Delta** est l'épine dorsale numérique des forces ukrainiennes, comparable au système JADC2 américain mais développé en situation de guerre réelle avec itérations rapides.

Hébergé dans le cloud et accessible sur terminaux commerciaux (tablettes Samsung durcies, smartphones), Delta fusionne les données de milliers de capteurs hétérogènes en une image opérationnelle commune (Common Operating Picture - COP).

Sources de Données Fusionnées

- Drones tactiques (Mavic, Leleka, Beaver)
- Satellites commerciaux (Maxar, Planet Labs)
- Radars contre-batterie (AN/TPQ-36, -50)
- Capteurs acoustiques (détection artillerie)
- Renseignement humain (HUMINT) digitalisé
- Systèmes d'armes (position, munitions, statut)

Interopérabilité OTAN

En 2025, Delta a démontré lors de l'exercice CWIX (Coalition Warrior Interoperability eXploration) sa capacité à s'intégrer aux standards OTAN, prouvant que logiciel peut combler fossé entre équipements hétéroclites.

Module Avengers : IA Visuelle pour Ciblage Automatisé

L'intégration de la plateforme IA **"Avengers"** dans Delta en 2024-2025 représente un saut qualitatif majeur. Ce module analyse automatiquement les flux vidéo de centaines de drones simultanément, libérant les opérateurs humains de la tâche fastidieuse de surveillance constante.

1 Détection Automatique

Algorithmes de vision par ordinateur (YOLO, Faster R-CNN) balayent continuellement les flux vidéo pour détecter véhicules, personnels et équipements militaires avec taux de détection >90%.

2 Classification des Cibles

Réseaux neuronaux convolutifs entraînés sur milliers d'images classifient automatiquement types de véhicules russes : chars T-72/T-80/T-90, BMP, artillerie 2S19 Msta, systèmes AA Pantsir/Tor.

3 Génération Coordonnées

Conversion automatique de la position détectée en coordonnées de ciblage précises (MGRS) via géoréférencement de la vidéo drone et télémétrie GPS.

4 Distribution Réseau

Partage instantané via Starlink aux unités d'artillerie (Caesar, M777, HIMARS) et drones FPV pour engagement rapide avant déplacement cible.

Le système réduit la boucle F2T2EA (Find, Fix, Track, Target, Engage, Assess) de 20-30 minutes à moins de 2 minutes dans conditions optimales, augmentant drastiquement létalité de l'artillerie ukrainienne malgré infériorité numérique en tubes.

Israël : Combat Urbain et Drones d'Intérieur Lanius

Lanius d'Elbit Systems

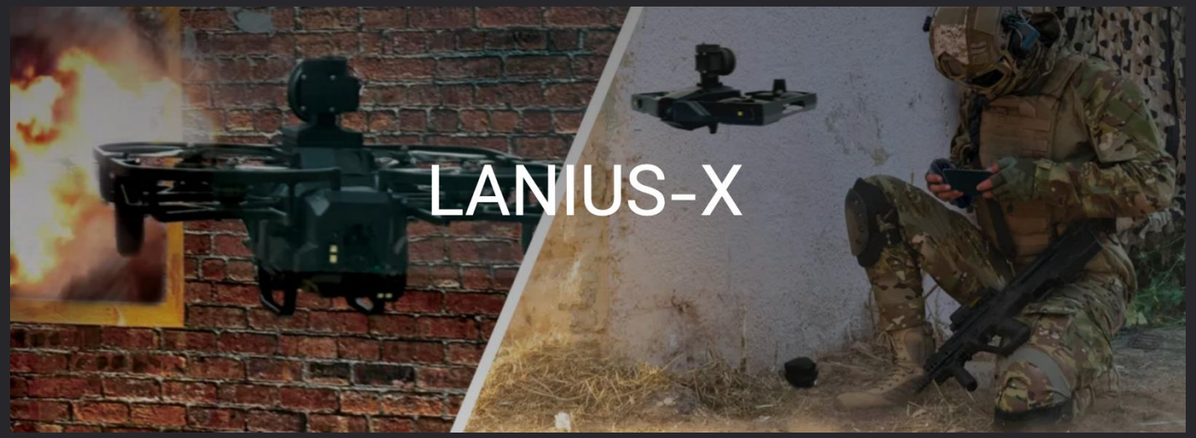
Pour répondre aux défis mortels du combat en milieu dense urbain et souterrain (Gaza), Israël a développé et déployé opérationnellement le système Lanius d'Elbit Systems. Ce micro-drone quadcoptère de course militarisé représente une innovation tactique majeure.

Navigation SLAM Autonome

Lanius utilise l'IA SLAM (Simultaneous Localization and Mapping) pour naviguer de manière autonome à l'intérieur des bâtiments multi-étages et des réseaux de tunnels sans signal GPS. Le système cartographie en temps réel son environnement via caméras stéréo et évite obstacles dynamiques.

Distinction Combattants/Civils

Elbit affirme que Lanius est capable de distinguer combattants des non-combattants via reconnaissance faciale et analyse comportementale.
Le drone peut exploser sur commande opérateur ou de manière autonome si mode activé.



Synthèse : Écosystème Terrestre IA-Enabled

Communications Résilientes

Starlink, liaisons mesh, radios logicielles pour connectivité en environnement contesté

Guerre Électronique

GE cognitive automatisée pour détection, brouillage et protection

Robotique Terrestre

UGV pour reconnaissance, logistique, déminage et combat direct

ISR Multi-Couches

Satellites commerciaux, drones tactiques, capteurs sol fusionnés par IA

Ciblage Automatisé

Vision par ordinateur pour détection, classification et génération coordonnées

Feux Précis Rapides

Artillerie guidée, munitions rôdeuses, frappes coordonnées en <2min

CHAPITRE 6

Guerre Cognitive et IA Générative Générative

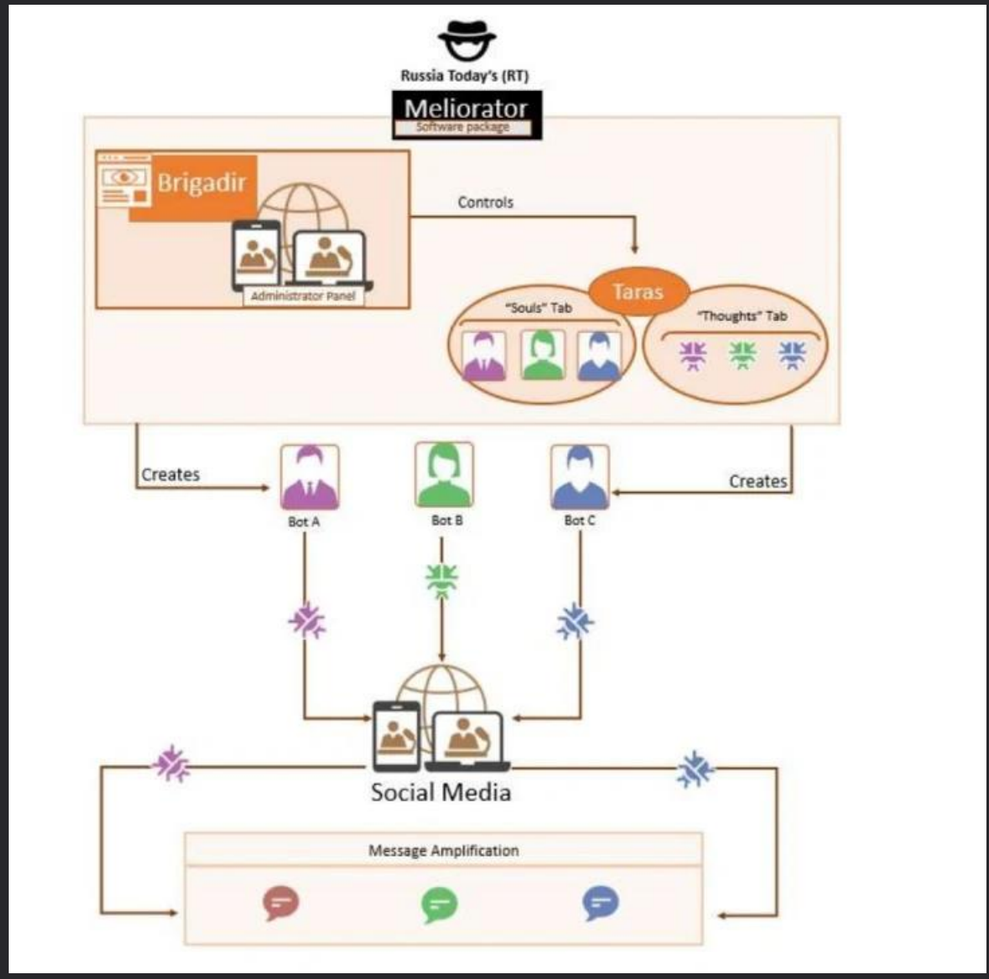
L'espace informationnel est devenu un domaine de guerre à part entière, où l'intelligence artificielle générative (GenAI) permet des opérations d'influence à l'échelle industrielle. Les modèles de langage (LLM) et de génération d'images/vidéos (deepfakes) offrent aux acteurs étatiques et non-étatiques des capacités de manipulation de l'opinion publique et de désinformation stratégique sans précédent historique.

Opération Doppelganger : Fermes de Bots Russes

Les révélations judiciaires américaines de 2024 et 2025 (Département de la Justice) ont mis à jour l'architecture technique de l'opération russe **"Doppelganger"**, une campagne d'influence massive ciblant les démocraties occidentales via réseaux sociaux. L'opération utilise des fermes de bots alimentées par IA générative pour créer l'illusion d'un débat public organique.

Mécanisme Technique

- **Génération de Personas** : LLM créent profils cohérents avec historiques, photos (GAN), styles d'écriture uniques
- **Contenu Unique** : Chaque message généré est unique pour éviter détection par filtres anti-spam
- **Adaptation Temps-Réel** : Narratifs ajustés en fonction actualité pour maximiser résonance
- **Contournement Protections** : IA résout CAPTCHAs, simule comportements humains de navigation



Échelle de l'Opération

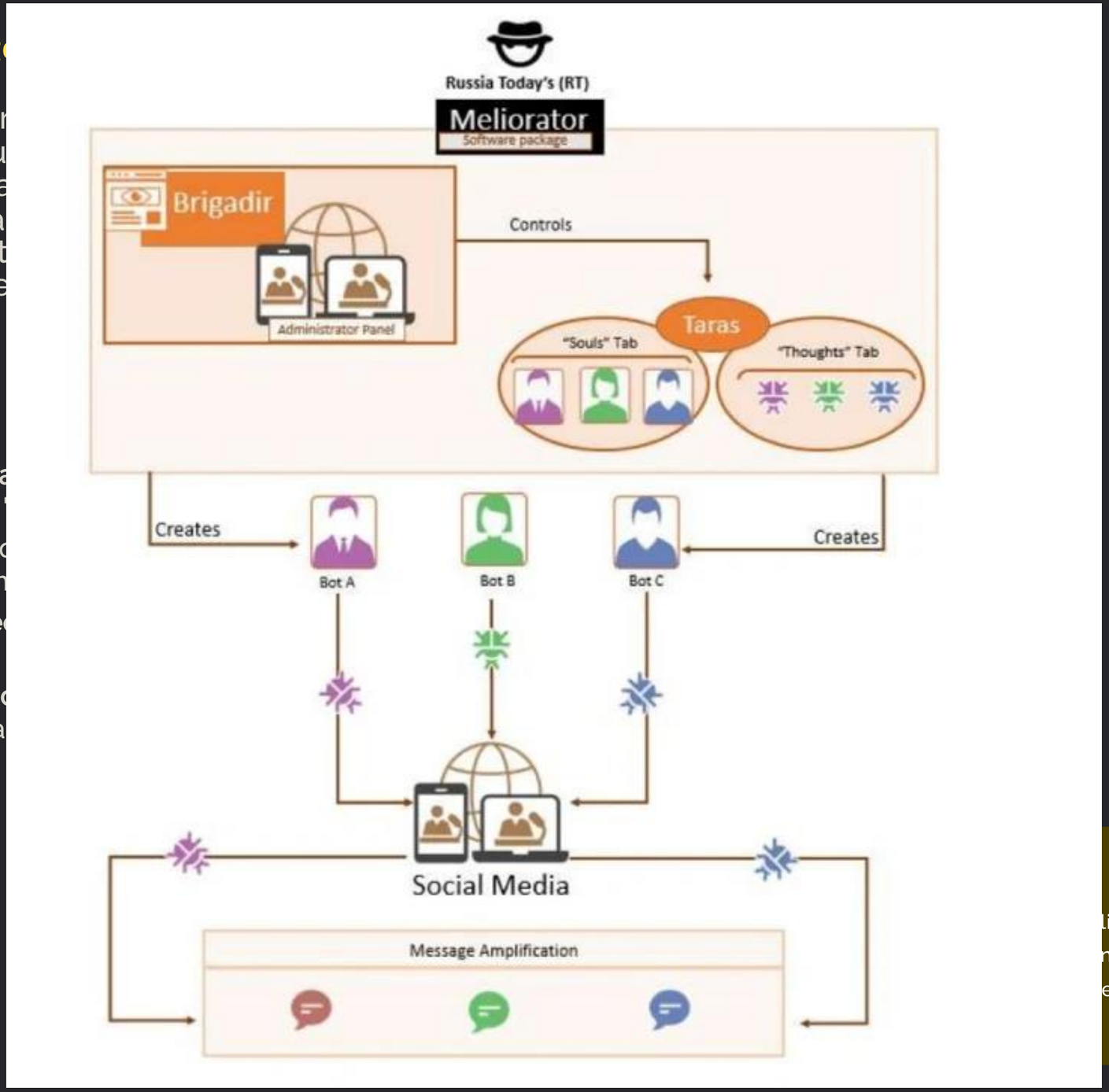
Estimations FBI : 1+ millions de comptes bots actifs sur Twitter/X, Facebook, Instagram. Coût opérationnel : 100x inférieur aux campagnes traditionnelles TV/presse pour portée équivalente.

Opération Doppelgang

Les révélations judiciair
la Justice) ont mis à jou
"Doppelganger", une ca
démocraties occidenta
fermes de bots aliment
débat public organique

Mécanisme Technique

- **Génération de Persona**
  photos (GAN), styles d'
- **Contenu Unique** : Chac
  détection par filtres an
- **Adaptation Temps-Ré**
  maximiser résonance
- **Contournement Protec**
  comportements huma



lions de comptes bots actifs sur
nstagram. Coût opérationnel : 100x
es traditionnelles TV/presse pour

Anatomie d'une Campagne IA-Générée

01

Définition Objectif Stratégique

Opérateurs humains définissent narratif cible : saper soutien aide Ukraine, amplifier divisions sociales, promouvoir candidats pro-russes dans élections occidentales.

02

Génération Personas IA

LLM créent milliers de fausses identités cohérentes avec historiques crédibles, photos de profil synthétiques (StyleGAN), biographies détaillées imitant vrais utilisateurs.

03

Production Contenu Adaptatif

Génération continue de posts, commentaires, mèmes adaptés à l'actualité. IA analyse trending topics et ajuste messages pour maximiser engagement et viralité algorithmique.

04

Amplification Coordonnée

Réseau de bots amplifie contenu via likes, shares, retweets coordonnés pour tromper algorithmes de recommandation et atteindre utilisateurs réels, créant effet boule de neige.

05

Évasion Détection

IA adapte tactiques en réponse aux contre-mesures plateformes : rotation comptes, variation horaires posting, diversification contenus pour éviter patterns détectables.

Deepfakes Tactiques : Conflit Inde-Pakistan 2025

Le bref conflit aérien entre l'Inde et le Pakistan en mai 2025 a illustré le danger mortel des deepfakes en temps de crise internationale. Des vidéos hyper-réalistes générées par IA, montrant le Premier ministre pakistanais annonçant une reddition fictive, ont circulé viralement sur réseaux sociaux et chaînes d'information.

Techniques de Deepfake Employées

- **Face Swap** : Remplacement du visage via réseaux neuronaux entraînés sur vidéos publiques du leader
- **Voice Cloning** : Synthèse vocale imitant parfaitement timbre, accent, modulations du discours cible
- **Lip Sync** : Synchronisation labiale parfaite entre fausse voix et mouvements bouche
- **Environmental Matching** : Duplication décor, éclairage bureaux officiels pour authenticité maximale

Impact Stratégique

Ce "brouillard de guerre synthétique" a compliqué la prise de décision diplomatique et militaire critique. Les états-majors ont dû consacrer ressources précieuses à la vérification de l'authenticité des déclarations officielles, créant confusion et retards dangereux dans un contexte où chaque minute compte.

Simultanément, des médias indiens ont diffusé des animations IA présentées comme images réelles de frappes aériennes, amplifiant nationalisme et rendant désescalade diplomatique plus difficile.

IA Générative : Outils Offensifs et Défensifs

Offensive : Création Deepfakes

Modèles génératifs (GANs, diffusion models) créent vidéos, audios, images synthétiques indiscernables du réel. Applications : fausses déclarations leaders, fabrication preuves, manipulation marchés financiers.

Défensive : Détection Authenticité

Algorithmes d'analyse forensique numérique détectent artefacts subtils (incohérences éclairage, anomalies pixels, asynchronisme audio-vidéo) pour authentifier contenus. Course perpétuelle attaque vs défense.

Offensive : Bots Conversationnels

Chatbots alimentés par LLM engagent conversations naturelles avec humains pour influencer opinions, récolter informations sensibles, diffuser narratifs. Indétectables dans discussions en ligne.

Défensive : Watermarking IA

Insertion de signatures numériques invisibles dans contenus IA-générés permettant traçabilité de la source. Standards émergents (C2PA) mais adoption volontaire limitée efficacité.

Contre-Mesures et Résilience Cognitive

Littératie Numérique

Éducation populations à reconnaître désinformation, vérifier sources, comprendre mécanismes viraux. Formation critique médiatique dans cursus scolaires et militaires.

Détection Automatisée

Déploiement d'IA défensive sur plateformes pour identifier bots, deepfakes, campagnes coordonnées. Mais course perpétuelle entre attaquants et défenseurs.

Législation & Régulation

Lois criminalisant deepfakes malveillants, obligations de transparence pour contenus IA-générés (labeling), sanctions contre plateformes facilitant désinformation massive.

Attribution & Dissuasion

Capacités forensiques pour attribuer campagnes d'influence aux acteurs étatiques responsables. Menace de sanctions diplomatiques/économiques comme dissuasion.

Coopération Internationale

Partage de renseignements sur campagnes, coordination réponses, standards techniques communs. Initiatives comme le EU Code of Practice on Disinformation.

CHAPITRE 7

Enjeux Éthiques et Controverses Controverses

L'utilisation opérationnelle de l'intelligence artificielle pour le ciblage létal a déclenché une crise éthique et juridique majeure au sein de la communauté internationale. Les systèmes d'armes létaux autonomes (LAWS) soulèvent des questions fondamentales sur la délégation du pouvoir de vie ou de mort à des algorithmes, la responsabilité légale en cas d'erreur, et le respect du droit international humanitaire.

Problématiques Éthiques Fondamentales

Délégation de la Décision Létale

Est-il moralement acceptable de déléguer à une machine la décision de tuer un être humain ? Le jugement humain possède des dimensions éthiques, contextuelles et émotionnelles irremplaçables par algorithmes.

Biais Algorithmiques

Les IA reproduisent et amplifient les biais présents dans leurs données d'entraînement. Risque de ciblage discriminatoire basé sur apparence, origine, comportements mal interprétés par algorithmes.

Responsabilité Juridique

Qui est légalement responsable quand une IA commet une erreur létale ? Le programmeur ? Le commandant ? Le système politique l'ayant autorisé ? Le vide juridique actuel est inacceptable.

Respect du DIH

Les IA peuvent-elles respecter les principes de distinction (combattants/civils), proportionnalité (dommages vs avantage militaire), précaution ? Capacités actuelles insuffisantes pour contextes complexes.

Course aux Armements

La prolifération de LAWS crée pression pour adoption par tous acteurs (effet domino). Risque de déstabilisation stratégique si systèmes défectueux déclenchent escalades involontaires.

Dignité Humaine

Le droit d'un être humain à ne pas être tué par une machine sans jugement humain. Principe de dignité humaine fondamental remis en cause par automatisation du champ de bataille.

Débat International sur les LAWS à l'ONU

À l'Organisation des Nations Unies, le Groupe d'Experts Gouvernementaux (GGE) sur les systèmes d'armes létaux autonomes (LAWS) discute depuis 2014 d'un possible traité d'interdiction ou de régulation. Le débat est bloqué par l'opposition des grandes puissances militaires.

Position Pro-Régulation (156 États)

La majorité des États membres de l'ONU, menés par des pays comme l'Autriche, le Brésil, l'Afrique du Sud, et soutenus par ONG (Campaign to Stop Killer Robots), plaident pour une interdiction ou régulation stricte contraignante.

- Traité d'interdiction des LAWS complètement autonomes
- Obligation de contrôle humain "significatif" et "approprié"
- Transparence des algorithmes de ciblage
- Accountability juridique claire en cas d'erreur
- Moratoire sur développement et déploiement

Opposition (USA, Russie, Israël, Chine)

Les puissances militaires majeures s'opposent à toute interdiction contraignante, arguant que les technologies IA offrent potentiel de réduction des pertes civiles (précision supérieure) et que régulation prématurée entraverait innovation bénéfique.

- Préférence pour "meilleures pratiques" volontaires
- Déclarations politiques non-contraignantes
- Focus sur "utilisation responsable" sans limites développement
- Rejet de définition précise "autonomie" pour flexibilité

Principes d'Utilisation Responsable (PRUs)

Contrôle Humain Approprié

Un opérateur humain doit conserver la capacité effective de superviser, intervenir et arrêter le système autonome. Le niveau de contrôle doit être adapté au contexte opérationnel et aux risques.

Transparence et Explicabilité

Les décisions prises par les systèmes autonomes doivent être traçables et explicables (explainable AI). Les algorithmes ne doivent pas être des "boîtes noires" opaques empêchant accountability.

Responsabilité et Accountability

Établissement clair de chaînes de responsabilité : développeurs, commandants, autorités politiques. Les systèmes ne peuvent diluer la responsabilité humaine des décisions létales.

Fiabilité et Testabilité

Les systèmes IA doivent être rigoureusement testés dans des conditions représentatives avant déploiement opérationnel. Tests adversariaux pour évaluer robustesse face à environnements imprévus et attaques.

Conformité au DIH

Les systèmes doivent être conçus et employés en strict respect du droit international humanitaire : distinction, proportionnalité, précaution. Programmation des règles d'engagement juridiques dans l'algorithme.

Cas d'Usage Éthiquement Acceptables vs Controversés

Catégorie	Application	Statut Éthique
Acceptable	Défense anti-missile (Patriot, Iron Dome)	Temps réaction humain insuffisant face menaces rapides. Cibles inanimées (missiles). Consensus large sur acceptabilité.
Acceptable	Déminage automatisé (UGV)	Sauve vies humaines. Cibles inanimées. Environnement contrôlé. Bénéfice humanitaire clair sans dilemmes éthiques majeurs.
Débattu	Drones ISR avec analyse IA	Reconnaissance et surveillance automatisées acceptables. Controverse si IA recommande cibles sans vérification humaine substantielle (biais d'automatisation).
Débattu	Sentinelles robotiques (frontières)	Surveillance acceptable. Engagement automatique controversé. SGR-A1 sud-coréen DMZ : peut tirer automatiquement mais désactivé pour raisons éthiques.
Controversé	Munitions rôdeuses autonomes (Harpy, Harop)	Sélection et engagement autonome de radars. Acceptable si cibles militaires évidentes. Inacceptable en zones peuplées (risque erreur).
Controversé	Ciblage automatisé individus (Lavender)	Décision vie/mort sur humains basée sur algorithmes opaques. Risques erreurs, biais, dommages collatéraux. Largement condamné par ONG et experts DIH.

Défis de la Régulation Internationale

Absence de Définition Consensuelle

Aucune définition internationale acceptée de "système d'arme létal autonome". Les États utilisent des définitions floues pour maintenir flexibilité et éviter contraintes juridiques sur programmes de R&D.

Vitesse Innovation > Vitesse Régulation

Le rythme de développement technologique dépasse largement la capacité des institutions internationales (ONU, GGE) à produire des normes contraignantes. Obsolescence rapide des cadres proposés.

Sécurité Nationale vs Normes Globales

Les grandes puissances militaires considèrent l'IA comme avantage stratégique vital et résistent aux limitations contraignantes perçues comme handicaps compétitifs face aux adversaires.

Prolifération Acteurs Non-Étatiques

Même si un traité interétatique existait, la disponibilité commerciale des technologies IA permet aux groupes non-étatiques de développer capacités létales autonomes. Régulation inefficace sans contrôle prolifération technologique.

Initiatives Nationales et Régionales

Déclaration Politique US (2023)

Les États-Unis ont publié une "Déclaration Politique sur l'Utilisation Militaire Responsable de l'Intelligence Artificielle et de l'Autonomie" promouvant des principes volontaires sans créer d'obligations contraignantes. Signée par 55 États alliés, elle évite toute limitation sur développement technologique.

AI Act Européen (2024)

Le règlement IA de l'UE classe les systèmes d'armes létaux comme "applications à haut risque" nécessitant évaluations de conformité strictes. Cependant, exemptions larges pour sécurité nationale limitent impact réel sur pratiques militaires.

Principes OTAN (2024)

L'OTAN a adopté des Principes d'Utilisation Responsable de l'IA (PRUs) pour ses 32 États membres, incluant : contrôle humain approprié, fiabilité, compréhensibilité, biais, et gouvernance. Engagement politique fort mais non juridiquement contraignant.

SYNTHÈSE

Dynamiques Fondamentales de l'IA Militaire

L'analyse exhaustive de l'état de l'art de l'intelligence artificielle militaire en 2025-2026 révèle trois dynamiques fondamentales qui redéfinissent irréversiblement la nature de la guerre moderne et les équilibres stratégiques mondiaux.

Implications pour les Forces Armées Africaines

L'émergence de l'IA militaire crée des opportunités et des défis spécifiques pour les forces armées du continent africain, incluant le Cameroun. La démocratisation technologique permet un "saut quantique" (leapfrogging) potentiel, mais nécessite investissements stratégiques ciblés et partenariats intelligents.

Opportunités : Partenariats Technologiques

Les nations africaines peuvent exploiter la compétition géopolitique pour négocier transferts de technologies avec multiples partenaires (USA via programmes AFRICOM, Chine via Belt & Road Initiative, Europe via accords bilatéraux, Israël pour contre-terrorisme). L'IA offre capacités de force multiplication accessibles à coûts raisonnables comparés aux plateformes conventionnelles.

Défis : Contre-Terrorisme et Insurgés IA-Enabled

Les groupes terroristes (Boko Haram, AQMI, Al-Shabaab) adoptent progressivement drones commerciaux et outils IA pour surveillance, IED guidés et opérations de propagande. Les forces africaines doivent développer capacités contre-UAS (Counter-UAS) et guerre électronique pour neutraliser ces menaces asymétriques croissantes.

Impératif : Développement Capital Humain

L'adoption efficace de l'IA militaire nécessite formation massive de personnels techniques : data scientists, ingénieurs IA, opérateurs systèmes autonomes, analystes cyber. Investissements éducation STEM (Science, Technology, Engineering, Mathematics) et création d'académies militaires spécialisées IA sont critiques pour souveraineté technologique.

Considération : Cadres Éthiques et Juridiques

Les nations africaines ont intérêt stratégique à participer activement aux négociations internationales sur régulation LAWS pour influencer normes émergentes conformes à leurs valeurs et intérêts sécuritaires. Leadership régional via Union Africaine pour positions communes.

Recommandations Stratégiques

1 **Prioriser Investissements Logiciels sur Matériels**

Plutôt que d'acquérir plateformes conventionnelles coûteuses rapidement obsolètes, privilégier développement de capacités logicielles IA duales (civil-militaire) et systèmes modulaires upgradeables. Focus sur systèmes C4ISR (Commandement, Contrôle, Communications, Ordinateurs, Renseignement, Surveillance, Reconnaissance) connectant forces existantes.

2 **Établir Centres d'Excellence IA Défense Régionaux**

Créer consortiums régionaux pour mutualiser investissements R&D, éviter duplications coûteuses, et développer masse critique d'expertise technique. Partenariats académiques avec universités leaders IA pour transfert connaissances.

3 **Développer Écosystème Startup Deeptech Local**

Soutenir émergence de startups africaines développant solutions IA sécurité/défense adaptées aux contextes opérationnels locaux (terrains, climat, menaces spécifiques). Incubateurs militaires style DARPA, financement seed, facilitation accès marchés publics pour création de base industrielle technologique souveraine.

4 **Adopter Cadres d'Utilisation Responsable Stricts**

Établir dès maintenant principes éthiques et juridiques clairs pour emploi IA militaire : contrôle humain, transparence, accountability, respect DIH. Prévenir dérives futures et positionner nations africaines comme leaders normatifs internationaux en éthique IA défense.

Conclusion : L'Impératif d'Adaptation

L'intelligence artificielle a irréversiblement transformé la nature de la guerre en 2025-2026. Les armées qui maîtriseront l'intégration de l'IA, tout en sécurisant leurs chaînes d'approvisionnement de données et de puces, domineront les conflits de la prochaine décennie. Celles qui échoueront à adapter leurs doctrines, processus d'acquisition et culture organisationnelle risquent l'**obsolescence brutale** face à des adversaires plus agiles, qu'ils soient étatiques ou insurgés.

Pour les forces armées africaines et camerounaises, le moment est critique. La fenêtre d'opportunité pour investir stratégiquement dans les capacités IA et former le capital humain nécessaire se ferme rapidement. L'alternative est la dépendance technologique permanente et la vulnérabilité face à des menaces asymétriques croissantes.

La guerre algorithmique n'est plus un concept futuriste. Elle est la réalité opérationnelle de 2025. **L'adaptation n'est plus optionnelle - elle est existentielle.**

> *"Dans le domaine militaire, ce n'est pas le plus fort qui survit, ni le plus intelligent, mais celui qui s'adapte le plus rapidement au changement."*
>
> — Principe darwinien appliqué à la guerre moderne

Merci de votre attention

HELIOS - BIR CAMEROUN 2026