MINISTÈRE
DE L'ENSEIGNEMENT
SUPÉRIEUR ET UNIVERSITAIRE

IA dans les défis de la défense de la patrie par les scientifiques de l'ESU

Colloque

sur la sauvegarde de la souveraineté et de l'intégrité territoriale

Kodjo NDUKUMA ADJAYI

Professeur d'informatique juridique à l'UCC

Doyen de la Faculté de droit de l'UPC

Dr de l'Université Paris 1 Panthéon Sorbonne

SOMMAIRE

OBJECTIF D'INTERVENTION

POSTULAT : Défense et innovation technologique

PARTIE 1 : Continuum Défense, cyberespace et Souveraineté numérique

PARTIE 2 : IA appliquée la Défense nationale

RECOMMANDATIONS

Objectif d'intervention au Colloque

- Sensibiliser sur l'Intelligence artificielle dans les défis de la défense de la mère-patrie par les scientifiques de l'ESU face aux enjeux de sauvegarde de notre souveraineté et de notre intégrité territoriale

Postulat : Défense et Innovation technologique

- Dans toute l'Histoire, il a été démontré que les plus hautes **intelligences** et les grandes **inventions** ont toujours été mises **au service de la puissance des États et donc des armées**.
- Si « l'apothéose de la puissance des armes a été atteinte avec l'arme nucléaire », il y a toujours deux paradigmes entre l'Humain inventeur et la Machine inventée, entrainant **la proéminence de la valeur** :
  - soit **de l'humain** à l'ère des « armées d'archers » ;
  - Soit **de la machine** à l'ère des « **armées d'arbalètes** ».

PARTIE I :

CONTINUUM DÉFENSE, CYBERESPACE ET SOUVERAINETÉ NUMÉRIQUE

Souveraineté : Principe et exercice

- « **Caractère suprême d'une puissance** (*summa potestas*) **qui n'est soumise à aucune autre** » (G. CORNU, *Vocabulaire juridique*, 11e éd., PUF, Paris, 2016, p.9995)
- « Pouvoir perpétuel et indivisible d'un État »
- « La souveraineté nationale appartient au peuple. Tout pouvoir émane du peuple qui l'exerce directement par voie de référendum ou d'élections et indirectement par ses représentants.

  Aucune fraction du peuple ni aucun individu ne peut s'en attribuer l'exercice. » (Article 5, Constitution de la RDC du 18 février 2006)

Défense de sa souveraineté

1. **Défense nationale** : **ensemble des moyens militaires et non militaires** ayant pour objet d'assurer la **protection et la sauvegarde des intérêts fondamentaux de la nation**, en toute circonstance et contre toutes les formes d'agression et menace
2. **Défense militaire:** le **fait de s'opposer,** en tout temps et en toute circonstance, **par des moyens militaires, à toute forme d'agression dirigée contre les intérêts fondamentaux de la Nation**;
3. **Défense civile: ensemble des moyens non militaires ayant pour objet d'assurer la survie des populations, de sauvegarder les capacités de production, d'organiser la résistance en cas d'occupation et d'apporter un soutien aux Forces armées**;

(Article 5, Loi organique n° 11-012 du 11 août 2011 portant organisation et fonctionnement des Forces armées.).

Souveraineté : atouts et technologies

- L'exercice de sa souveraineté **dépend tout aussi des moyens et atouts que chaque Etat-Nation développe** en vue de (d'):
  - **Accroître sa puissance** en tant que Nation ou « être géographique »,
  - **Défendre l'intégrité de son territoire**,
  - **Assurer la sécurité et la prospérité de sa population**,
  - **Défendre sa liberté et ses valeurs fondamentales** contre tout assujettissement anti-patrie ;
  - **Faire respecter son existence et son indépendance** en tant que personne morale de Droit international **face aux autres États, en position de concurrence ou d'alliance**, dans le concert des Nations.


807e CTRS
CYBERDEFENSE

Espaces de souveraineté et cyberespace

- « L'Etat exerce une souveraineté permanente notamment sur le sol, le sous-sol, les eaux et les forêts, sur les espaces aérien, fluvial, lacustre et maritime congolais ainsi que sur la mer territoriale congolaise et sur le plateau continental. » (Article 9, Constitution, préc.)
- Il se fait que le **Cyberespace existe** indéniablement, en tant qu'espèce d'espace numérique


F9
W
F2
F12
E
R
T
F3
G
Y

Cyberespace sous prisme de la Défense

- **Espace stratégique** de déplacement des conflits et d'expression d'autres formes de puissance « soft power » participant à la souveraineté des Etats
- **Espace opérationnel**, en plus de Terre, Mer, Air et extra-Atmosphère ;
- **Espace cybernétique à effet cinétique** i.e. espace dit virtuel mais produisant des effets dans la vie réelle avec échelle des dégâts
- **Espace procédural de génie informatique mais espace d'action du génie humain** pour le bien ou le mal à échelle planétaire et transfrontière
- **Espace déterritorialisé**, d'apparence a-territoriale, mais en réalité, stato-centrée
- **Zone de guerre et de cyber-affrontement**

Numérique et défis de défense

- Si on sait qu'Internet fut conçu lui-même comme une arme avec DARPA aux USA dans les années 1940, le **Numérique** s'avère un **instrument et un espace de guerre multiforme** à l'usage et à la portée de tous les États et des groupements personnalisés ou non.
- À ce titre, la défense de la souveraineté s'y intéresse contre les emplois de la cyber guerre dans la guerre totale et multiforme :
  - **Guerre de propagande et donc de l'information ;**
  - **Guerre d'influence et donc de l'image ;**
  - **Guerre psychologique et donc des capacités d'hommes ;**
  - **Guerre informatique et donc des cyber armements ;**
  - **Guerre économique et donc des ressources stratégiques ;**
  - **Guerre de destruction des capacités de défense et donc de déstabilisation des infrastructures vitales essentielles ;**

Cyberespace, terrain et outil de guerre

Ordinateur de combat

Informatique de guerre

Défense d'une nouvelle espèce d'espace*

AUPARAVANT

- **Initialement idée opérative de la Défense :**
  - Imposition de la paix et Restauration espace de droit,
  - Opportunité de vaincre par la violence létale,
  - Sauvegarde de l'intégrité territoriale et donc des frontières nationales

ACTUELLEMENT

- **Cybersécurité-défense :** politique prudentielle des espaces, impose l'analyse des relations entre la politique et l'espace
- **Cyberdéfense** : politique de l'espace numérique (Cyberespace) dans ses aspects de « territoire stratégique » :
  - **Aspects de géopolitique :** confrontations territoriales et déterrorialisés
  - **Aspects de géoéconomie :** guerre économique
  - **Aspects d'intelligence économique** et de ***soft power***

** Espèce d'espace, terme de Georges Perec*

Outils intellectuels de cyber-guerre (2)

- **Nouveau cadre d'engagement des forces :** espace artificiel devenu « territoire » stratégique, directionnel et opérationnel, là où, de calibre, les corps des armées sont fonction de la maîtrise des contraintes physiques de l'espace naturel Terre, Mer, Air [et Espace extra-atmosphérique consécration sous Donald Trump]
- **Consubstantialité d'Internet à l'armement du futur** depuis (D)ARPA et des Télécoms au Ministère de la guerre et des armées depuis Napoléon au XVIII^{e} siècle
- **Inscription de l'espionnage** (même des alliés) dans tout modèle des puissances militaires antiques (depuis Israël de l'Exode au pays du lait et du miel) et **des technologies numériques intrusives de l'Internet**

« Souveraineté numérique »

- Le cadrage stratégique du **Numérique** en RD Congo le **définit comme** un ensemble :
  - **(i) des télécommunications**
  - **(ii) de l'informatique**, y compris : Informatique embarquée, **Intelligence artificielle** et objets connectés
  - **(iii) des technologies de l'information et de la communication**
  - **(iv) de l'Internet**.

  (Présidence de la République, Plan National du Numérique, Kinshasa, 2019, p.11)
- « *Souveraineté numérique : Droit d'autodétermination dont un pays dispose à décider de sa propre politique en matière du Numérique sur ses infrastructures, sur ses données et leurs traitements* »

  (Article 2, point 77, Ordonnance-loi n°23/010 du 13 mars 2023 portant Code du numérique)


L'INTELLIGENCE ARTIFICIELLE,
APPLIQUÉE AU MONDE
DE LA DÉFENSE
probayes

PARTIE II :

INTELLIGENCE ARTIFICIELLE APPLIQUÉE À LA DÉFENSE NATIONALE

IA par définition – applicative

- « L'intelligence artificielle, ce n'est pas une technologie en particulier, **ce n'est pas non plus quelque chose de secret ou de confidentiel**, encore moins une puissance autonome capable d'initiative.
- C'est **un ensemble de méthodes informatiques qui sont destinées à accomplir des tâches sophistiquées, et de toute discipline scientifique qui va avec, englobant des experts, des ingénieurs, des informaticiens, des mathématiciens, des experts de la donnée**.
- C'est **si multiforme que d'ici un certain temps, [l'IA] va se diffuser partout comme l'électricité** ».
- Il y a aussi dit que **les grandes plateformes numériques captent la valeur ajoutée de l'IA mondiale**.[15] (ChatGpt, OpenAI de Google ou Siri de Meta, Facebook)

(C. VILLANI, « Le pari de l'intelligence artificielle », in *L'Obs*, Cahier n ° 1, éd. n ° 272, Paris, 1er au 7 mars 2018, pp. 27-33. M. BERNARD, « Intelligence artificielle en Afrique : le risque de captation de valeur existe, décrypte Cédric Villani », *Le Monde,* 17 juin 2018.)

IA par définition – technique et méthodique

- « **Discipline informatique visant à reproduire par ordinateur le schéma de prise de connaissance et de traitement de données pratiqué par le cerveau humain, souvent d'un expert dans un certain domaine**. »
- « **Les techniques d'intelligence** artificielle visent ainsi à produire des systèmes experts simulant un comportement humain. »
- Deux méthodes et techniques d'entrainement de l'IA :
  - **Recherche : avec des hommes experts en la matière pour la reproduction des stimuli d'informations** avec lesquelles l'expert prend une décision, afin que la machine devienne elle-seule capable de décider
  - **Apprentissage : sur logiciel essayant un certain nombre de décisions,** les évalue et met en mémoire les résultats pour tenter d'aboutir à des décisions optimales, **faisant de la machine un agent autonome**.

(Jacques GUALINO, *Dictionnaire pratique Informatique, Internet et nouvelles technologies de l'information et de la communication*, Gualino éditeur, Paris, 2005, p.241.)

Intelligence artificielle

- **Baran (1940)** et **Turing (1950)** en sont les pionniers, IA devenue **discipline scientifique dès 1956**, avant sa latence d'intérêt puis le boom de sa **relance par les travaux de LeCun (1990)** sur le *deep learnig*, l'auto-apprentissage des machines entrainées

Domaine de l'IA	IA faiblef et IA forte
Reconnaissance des formes, des visages et de la vision en général	Machine capable de produire comportement intelligent, mais aussi d'avoir une compréhension de on propre raisonnement
Apprentissage automatique	Approche pragmatique d'Ingénieur
Traitement automatique des langues	Construction des systèmes autonomes
Systèmes experts	Développement et entrainement des programmes et algorithmes capables de résoudre des problèmes d'une certaine classe

6 applications concrètes de l'IA en Défense

- **1 - Oreille d'or – traiter massivement des données acoustiques en appui des oreilles d'or (EM – Naval Sous-marin de guerre)**
- **2 - DeMAIA – appuyer les équipages dans la veille optique des véhicules Griffon (EM - Armée de terre et appui à l'infanterie)**
- **3 - Rora – Identifier rapidement des pièces détachées (EM - Armée de terre)**
- **4 - IA versus deepfake - Détecter les informations mensongères contre les forces armées (EM- Rens, Ops-civilo-militaire)**
- **5 - IA FPN – Maximiser les chances de succès de la formation des pilotes (EM - Armée de l'air)**
- **6 - Resistance : traduire instantanément des langues étrangères sur son smartphone en opération (EM de renseignement Mission en territoire ennemi ou décodage**

[Source : https://www.defense.gouv.fr/actualites/ia-defense-6-cas-dusage-concrets-armees]

Autres applications de l'IA dans la Défense

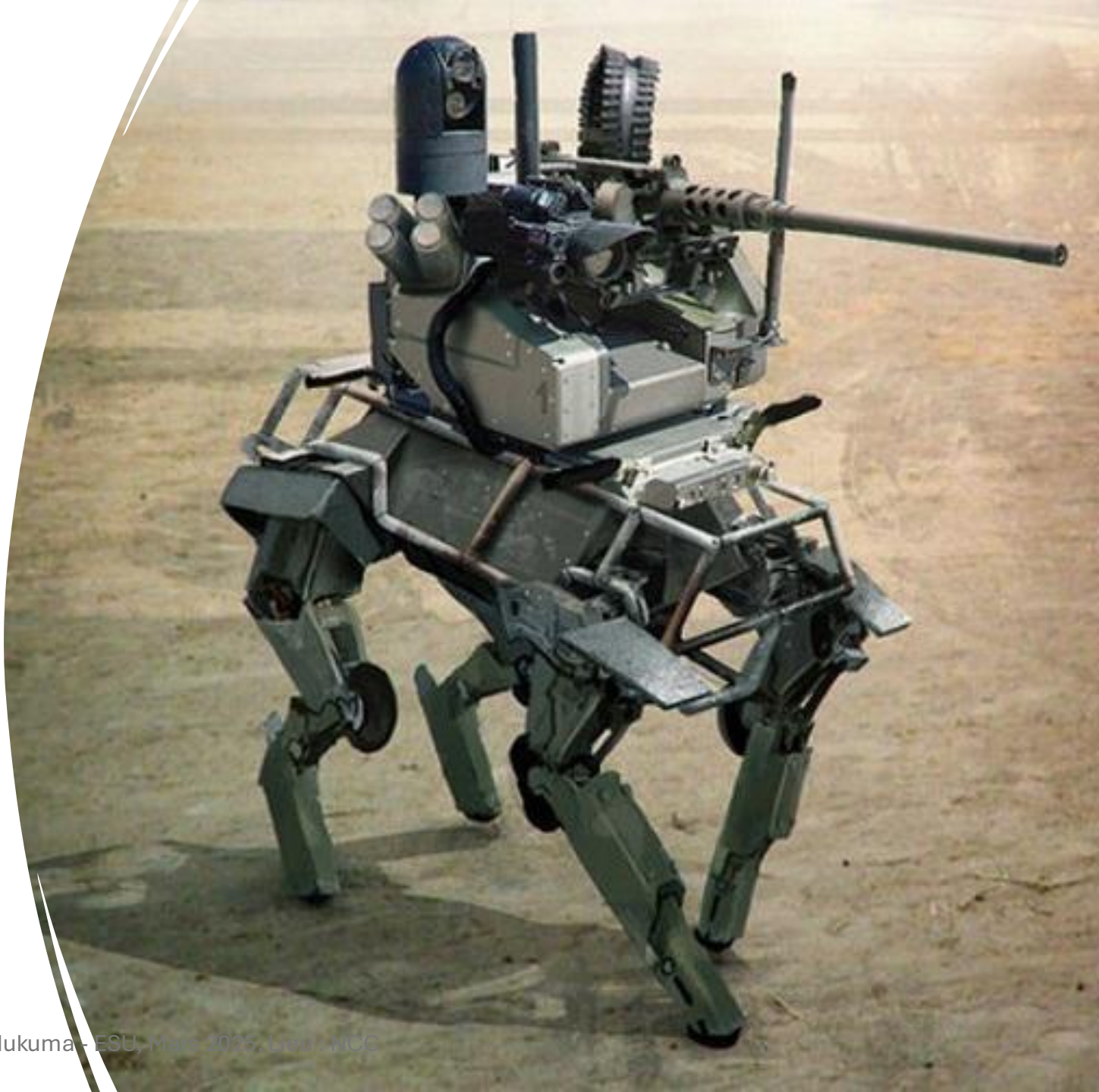
- Brouillage des fréquences de navigation des aéronefs de combat
- Cyber-renseignement et capacités décuplées d'analyse et de traitement des informations pour le renseignement opérationnel
- Téléguidage des bombes et projectiles avec coefficient de correction des erreurs
- Affinement de la géolocalisation
- Télédétection des minerais et donc orientation des zones de combat dans un contexte de guerre pour les minerais


Brouilleur BARAGE
THALES
THALES

Autres applications de l'IA dans la Défense

- Détermination intelligente des cibles humaines et matérielles de destruction
- Optimisation de l'informatique de combat
- Création des contenus de propagandes des plus réalistes pour la démoralisation des troupes engagées au front, pour la préparation des esprits à la capitulation, pour l'inculturation de la supériorité de l'ennemi
- Correcteur de visée
- Cryptage quantique des données Secret Défense

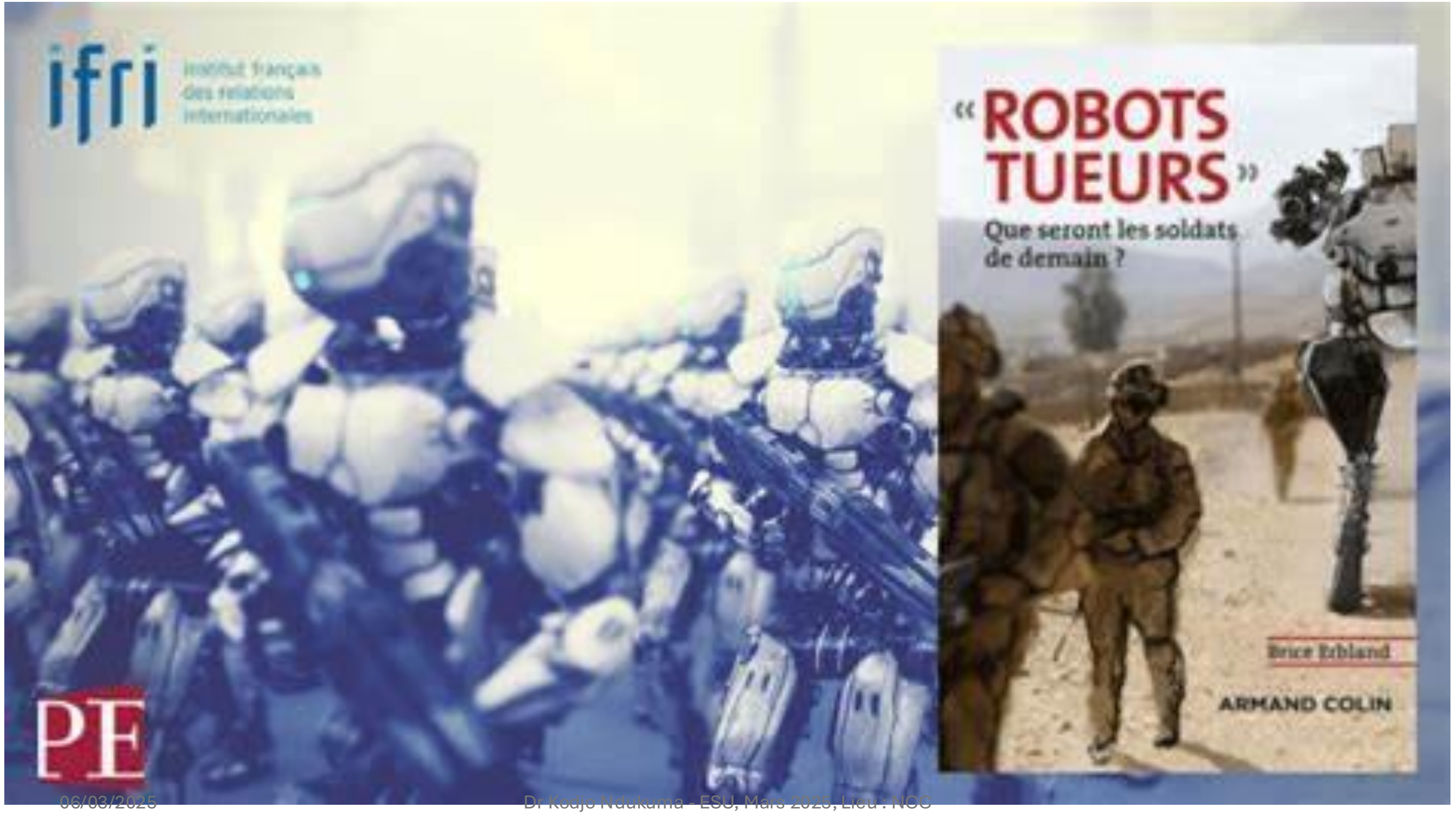
Robots soldats



IA et Robotique en général

- **Le Robot** relève en principe de la **mécanique** comme branche de la physique, les **robots intelligents** relèvent cependant de **l'informatique** spécialement sur la branche d'étude de l'IA
- La Norme ISO 8373-2012 définit :
  - le **robot** comme un « mécanismes programmables actionné sur au moins deux axes avec un degré d'autonomie, se déplaçant dans son environnement pour exécuter des tâches prévues »
  - le **robot intelligent** « robot capable d'exécuter des tâches par détection de son environnement et ou par interaction avec des sources extérieures et adaptation de son environnement »

(Yves BISMUTH, *Petit guide pratique de la Robotique*, L'Harmattan, Paris, 2018, p. 33)


ifri
institut français
des relations
internationales
« ROBOTS TUEURS »
Que seront les soldats de demain ?
Bruce Erbland
ARMAND COLIN
PE

Application de l'IA dans les « Robots tueurs »

- **SALA : *Systèmes d'Armes Létales Autonomes***
- « Systèmes d'armes qui, une fois activé, est capable de décider seul, c'est-à-dire sans intervention ni supervision humaine; du ciblage et du déclenchement de la frappe, en fonction d'un environnement changeant auquel il s'adapte »

(Jean-Baptise JEANGENE VILMER , « *Terminator Ethics : faut-il interdire les « robots tueurs » ? », in Politique étrangère Hiver, n°4, 2014,* pp. 151-167.)

- **Exemple : plateforme autodéclencheuse d'interception des missiles et des roquettes en Israël**

Drone militaire de combat lançant un missile

IA et Robots intelligents de Combat

- *SALA* sont des technologies maîtrisées par les puissances comme la Turquie, la Chine, les USA ou plus précisément Israël *lorsqu'on imagine les corrélations géopolitiques de la Guerre de l'Est du Congo, cachant mal une autre guerre par procuration, celle d'une Afrique du Sud pro-Palestine face à Israël et ses alliés traditionnels.*
- **Technologies autonomes ou téléopérée à grande distance** , à l'instar des drones dans un combat où des soldats humains s'exposent au danger sans réciprocité de danger avec les machines. (Lire : Brice ERBLAND, « *Robots tueurs » quels seront les soldats de demain?* , Albin Michel, Paris)

RECOMMANDATIONS

- Développer les stratégies de « *reverse technology* »
- Financer la veille technologique et l'intelligence économique
- Développer une industrie de la défense créative et innovante avec le génie informatique congolais
- S'approprier les inventions locales dans les emplois des Forces armées à travers des concours scienfifiques
- Financer le R&D en coopération avec les universités et centre de recherche au profit de l'industrie de la défense et de l'Armée
- Créer un Etat-major cyber avec atouts de cybersécurité, cyber-résilience, cybersoldats et de lutte informatique
- Développer une doctrine équilibrée entre modernisation (équipement) et professionnalisation (formation) des forces armées

Merci de votre attention

Kodjo NDUKUMA ADJAYI

Professeur des universités

Doyen de la Faculté de droit de l'UPC

kndukuma@hotmail.fr