

LES NOUVELLES TECHNOLOGIES ET LA STRATÉGIE NUCLÉAIRE

INITIATIVES POUR LE DÉSARMEMENT NUCLÉAIRE



IDN
Initiatives pour le désarmement nucléaire.

Initiatives pour le désarmement nucléaire

14 rue Brochant

BAL N°17

75017 Paris

Courriel : idn@idn-france.org

Site internet : https://www.idn-france.org/

Twitter : @IDN_Nucleaire

Initiatives pour le désarmement nucléaire (IDN) est une association sans but lucratif.

← *Photo de couverture :*

Félix Anthonysamy

LES NOUVELLES TECHNOLOGIES ET LA STRATÉGIE NUCLÉAIRE

SOMMAIRE

AVANT-PROPOS

Cette étude est publiée peu après que Paul Quilès, Président-fondateur d'IDN, et Michel Drain, membre du bureau de l'association, nous ont quittés.

Elle leur est dédiée en hommage à leur action inlassable et à leur contribution inestimable à notre combat commun pour un monde plus sûr, plus juste et plus pacifique.

Malgré leur propre combat courageux contre la maladie, Paul et Michel sont à l'origine de cette étude.

Ils y ont apporté leurs connaissances, leurs convictions et leurs préoccupations pour la sécurité de l'humanité et de l'environnement, menacées par les armes nucléaires rendues encore plus dangereuses et inutiles par les nouvelles technologies.

Michel Drain avait déjà exprimé ses craintes à ce sujet dans son ouvrage corédigé avec Paul Quilès en 2018, « L'Illusion nucléaire » (Ed. L'Harmattan).

Paul Quilès a rédigé pour cette étude le chapitre sur la guerre dans l'espace, qui sera sa dernière publication.

Fort de son expérience d'ancien ministre chargé de la Défense, il y dresse un tableau inquiétant de la course aux armements dans l'espace.

En effet, la stratégie nucléaire est dépendante des systèmes spatiaux, ce qui accroît la tentation des puissances nucléaires de détruire les systèmes des adversaires, aggravant encore le risque de catastrophe nucléaire.

Espérons que la sagesse contenue dans ces analyses et recommandations sera de nature à convaincre nos dirigeants et décideurs.

L'équipe d'IDN

1. INTRODUCTION

Source : iStock

Depuis quelques années, le développement de nouvelles technologies de pointe suscite de nombreuses réflexions et interrogations concernant les changements profonds qu'elles impliquent pour nos modes de vie, dans tous leurs aspects. Une abondante littérature est ainsi apparue, consacrée aux perspectives ouvertes par ces technologies émergentes pour l'amélioration des conditions de la vie mais aussi pour l'aggravation des conditions de la sécurité humaine.

Parmi tous ces commentaires, l'idée de l'impact disruptif de ces nouvelles technologies sur la géopolitique et donc sur les politiques de sécurité a fait rapidement consensus : « *la course à la domination technologique est inextricablement liée à l'évolution de la géopolitique* » [1].

Dans un monde interconnecté où la maîtrise de l'information devient un enjeu existentiel, un monde complexe mis sous tension par une compétition internationale exacerbée, les atouts que peut procurer la suprématie technologique font de celle-ci un enjeu stratégique essentiel.

Pour cette raison, Initiatives pour le Désarmement Nucléaire - IDN - a décidé d'entreprendre une étude consacrée à l'impact des nouvelles technologies sur la stratégie nucléaire des pays dotés d'armes nucléaires et de leurs alliés. Une stratégie communément appelée « dissuasion nucléaire », mais qui en réalité n'est autre qu'une **stratégie de terreur nucléaire**.

[1] *Le Monde en 2040 vu par la CIA*, Préface de Piotr Smolar, Ed. Equateurs Document, juin 2021.

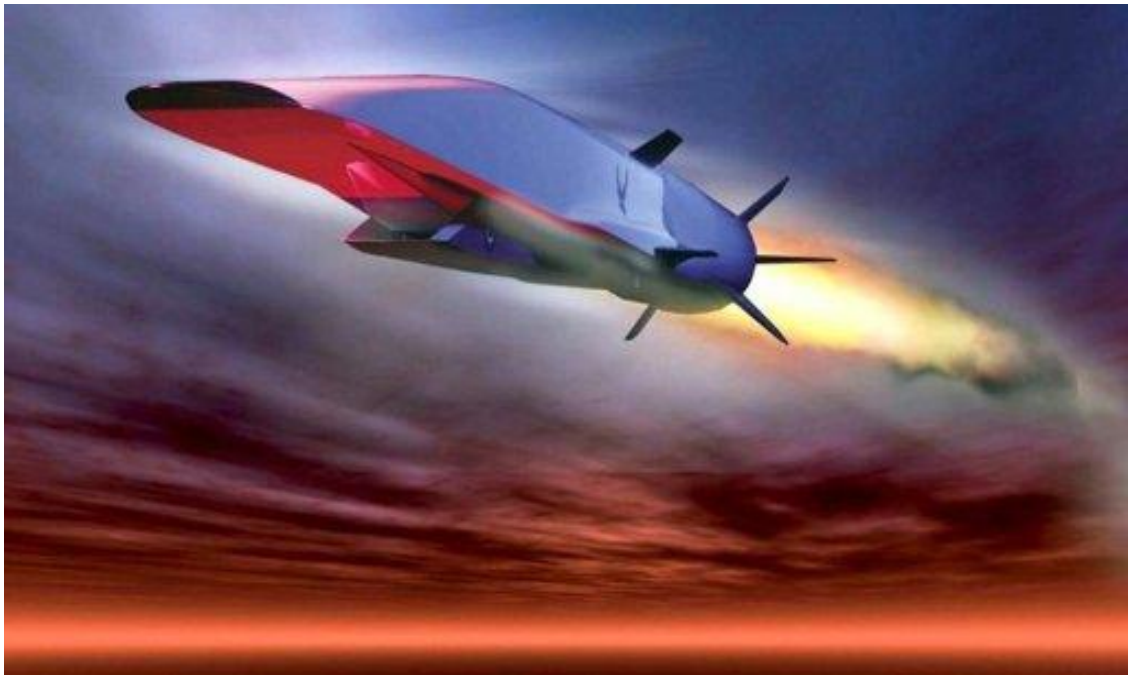
Cependant, cette étude a également mis en évidence les questions éthiques, sociétales et sécuritaires que soulèvent les nouvelles technologies. Les applications de l'intelligence artificielle combinée à d'autres technologies, les innovations biotechnologiques, la physique quantique pour ne citer que quelques-uns de ces développements, mettent en évidence la nécessité mais aussi la difficulté d'un contrôle et d'une régulation globale.

Ce travail porte sur huit technologies (missiles hypersoniques, armes à énergie dirigée, menace cyber, guerre de l'espace, intelligence artificielle, biotechnologies, nanotechnologies, et technologie quantique) qui nous ont paru essentielles par leur aspect novateur et prospectif. Il n'a pas la prétention d'être exhaustif ni d'être une étude scientifique, mais il se concentre sur un aspect qui est très rarement traité de façon synthétique, celui de l'impact des nouvelles technologiques sur la stratégie nucléaire.

2. LES MISSILES HYPERSONIQUES

Marc Finaud

Résumé : Les États-Unis font mine de s'inquiéter du futur déploiement par la Russie et la Chine de missiles hypersoniques capables de neutraliser toute défense antimissile alors même qu'ils investissent eux aussi dans cette technologie. La confiance dans la « dissuasion nucléaire » pour empêcher une première frappe était déjà passablement affaiblie par le recours à la défense antimissiles. L'escalade résultant de la course actuelle au contournement de cette défense est un pari dangereux qui ne peut qu'encourager l'offensive et conduire au cataclysme mondial.



Boeing X51-A Waverider à scramjet testé par l'armée de l'air américaine.
Source : US Air Force

2.1 Définitions et caractéristiques

Un missile (ou « véhicule ») hypersonique peut se définir par rapport à un missile balistique en fonction de plusieurs caractéristiques :

- Il décolle dans l'atmosphère comme un avion à partir d'une **plateforme** (terrestre, maritime ou aérienne) ;

- Il vole dans l'espace proche (en-dessous de 100 km d'altitude) à des **vitesses** supérieures à Mach 5 (soit cinq fois la vitesse du son ou 6 150 km/h) jusqu'à Mach 20 (24 696 km/h) voire plus ;

- Il utilise pour sa propulsion non pas un turboréacteur ou un moteur à réaction classique (compte tenu de la raréfaction de l'oxygène), mais un *superstatoréacteur* ou statoréacteur à combustion supersonique (« ***scramjet*** » en anglais) ;

- Comme un missile balistique, il est capable d'emporter une **charge** soit conventionnelle (explosif classique) soit nucléaire.

L'**hypervélocité** qui le caractérise ne suffit pas à le distinguer d'un missile balistique dont une partie de la trajectoire (phase finale) peut aussi intervenir à une vitesse supersonique. Le missile hypersonique peut lui aussi voler à une vitesse supérieure à la vitesse du son dans une partie de sa trajectoire seulement (phase de décollage ou propulsion, phase intermédiaire, ou phase finale). La principale différence réside dans sa **manœuvrabilité**, comparable à celle d'un missile de croisière dont la trajectoire, contrairement à celle d'un missile balistique, n'est pas prévisible.

Toutefois, la combinaison de l'**hypervélocité** et de la **manœuvrabilité** réduit ou rend plus difficile la **précision** pour atteindre la cible, ce qui amène à réduire la vitesse de l'engin en phase finale, d'où le recours à la technologie du **planeur** (« *glide vehicle* ») pour un guidage plus efficace.

La **portée** du missile hypersonique dépend, elle, de plusieurs facteurs : le type de plateforme de lancement, la vitesse de lancement, le nombre de manœuvres effectuées, l'altitude de vol, la durée du passage dans l'atmosphère, le poids de la charge, etc.

Outre le superstatoréacteur à combustion, un missile hypersonique, par comparaison avec un missile balistique, exige une **technologie avancée** :

- Un aérodynamisme spécifique ;
- Des matériaux résistant à de fortes chaleurs en vue de la protection aérothermique ;
- Des systèmes de navigation et de stabilisation perfectionnés, etc.

Les défis technologiques rencontrés depuis le lancement des premiers programmes de recherche sur les missiles hypersoniques dans les années 1990 ne manquent pas :

- La combustion du superstatoréacteur ne peut fonctionner efficacement en-dessous de Mach 1, ce qui oblige à le combiner avec un autre système de propulsion (turboréacteur ou lancement d'avion) pour ses phases de vol sonique ou subsonique ;
- Les systèmes de guidage tels que la navigation inertielle (INS) perdent de leur précision à grande distance et le GPS est vulnérable au piratage informatique ;
- L'aérodynamisme exige une enveloppe fine qui est sensible aux températures élevées ;
- La stabilisation dans les différentes phases de vol reste difficile à maîtriser.

CATÉGORIE	VITESSE FINALE	PROPULSION	EXEMPLE
Supersonique	Mach 1 à Mach 3	Propulseur, turboréacteur, statoréacteur	Missile de croisière antinavires BrahMos (Russie-Inde), avion sans pilote X-51 WaveRider (États-Unis)
Missile de croisière hypersonique	Mach 5	Statoréacteur, superstatoréacteur	Missile aérobalistique air-sol à haute précision Kinjal Kh-47M2 (Russie), missile de croisière hypersonique Zircon 3M22 (Russie)
Planeur hypersonique	Mach 20	Propulseur et planeur	Missile balistique de rentrée manœuvrable (MARV), planeur hypersonique

			Avangard (Russie), planeur hypersonique DF-17 (Chine), planeur hypersonique Falcon HTV-2 (États-Unis).
Missile balistique intercontinental / lancé depuis un sous-marin	Mach 27	Propulseur, véhicule de rentrée à charges indépendantes (MIRV)	Missile balistique Minuteman III ou Trident I D-5 (États-Unis), SS-19 (Russie), etc.

Tableau de catégorisation des missiles nucléaires. © IDN 2021.

2.2 Impact sur la « *dissuasion nucléaire* »

Le concept de « *dissuasion nucléaire* » tel qu'il avait été forgé au cours de la guerre froide reposait sur l'équilibre de la terreur et la destruction mutuelle assurée (MAD, ou « fou » en anglais) : la capacité de riposte en cas d'attaque (première frappe) devait être tellement dévastatrice qu'aucun agresseur rationnel ne pourrait prendre le risque d'être anéanti, et qu'il serait donc dissuadé d'attaquer. Mais toute l'histoire de la guerre froide et de la période actuelle est aussi celle de la course effrénée entre armes offensives et défensives.

Dans les années 1960, tant les États-Unis que l'Union soviétique ont développé et déployé des missiles défensifs capables d'intercepter les missiles intercontinentaux offensifs de leur adversaire. Conséquence : afin de contrecarrer ces défenses, les missiles offensifs furent équipés dès les années 1970 d'ogives nucléaires multiples (MIRV) et de contre-mesures, rendant inabordable ou inefficace tout système défensif. Jusqu'au jour où les deux superpuissances décidèrent de négocier parallèlement la limitation de leurs arsenaux stratégiques offensifs (Traité SALT de 1972) et de leurs systèmes antimissiles (Traité ABM de 1972). Introduire une défense antimissile contre une frappe nucléaire revenait à reconnaître la faiblesse intrinsèque de la dissuasion, puisque, dans ce scénario, elle n'aurait pas empêché une première frappe. Tout au plus les systèmes défensifs prévoyaient-ils de limiter les destructions d'une première frappe et de préserver des capacités de riposte.

Mais la course n'en a pas été stoppée pour autant : le président Reagan, sceptique à l'égard du concept de dissuasion, a lancé au début des années 1980 sa fameuse « *Guerre des étoiles* » ou Initiative de Défense stratégique (IDS), qui visait à rendre les armes nucléaires obsolètes en assurant une protection totale du territoire américain contre une attaque

soviétique. Exagérément ambitieux et techniquement et financièrement irréalisable, ce projet a été abandonné au profit de programmes de défense antimissiles plus limités, notamment, du point de vue américain, pour se protéger non plus contre des missiles intercontinentaux mais contre des missiles tirés par des « *États voyous* » tels que l'Iran ou la Corée du Nord, argument utilisé par le président Bush (fils) pour retirer en 2002 les États-Unis du Traité ABM. La réponse russe ne s'est pas fait attendre : Moscou a alors dénoncé le Traité START II qui avait inclus l'interdiction des MIRV, relançant ainsi la course des armes offensives contre les armes défensives.

Le déploiement d'un système de défense antimissiles en Europe (EPAA), lancé par le président Obama en 2009, n'a pu empêcher, malgré les démentis réguliers de Washington et de l'OTAN, d'être perçu par la Russie comme une menace à ce qu'un doux euphémisme qualifie de « *stabilité stratégique* » : sa capacité de riposte en cas d'attaque de la part des États-Unis ou de l'OTAN. Il n'est donc pas étonnant que le président Poutine ait réagi en annonçant à grand renfort de publicité le 1er mars 2018 le lancement de nouveaux programmes offensifs, parmi lesquels le missile intercontinental de croisière Sarmat à portée « *illimitée* », équipé non seulement de MIRV et de contre-mesures mais pouvant aussi lancer à son tour des véhicules *hypersoniques* (« *Boost-glide vehicles* ») du nom de Vangard capables de déjouer toute défense antimissiles. Comme clairement proclamé par Poutine, cet investissement massif répondait au retrait américain du Traité ABM, mais aussi au projet du Pentagone de déployer un missile de précision à longue distance conventionnel (« *Prompt Global Strike* »), perçu par Moscou comme une menace contre ses sites de missiles nucléaires.

Les États-Unis, en réaction, ont qualifié ces annonces d'« *irresponsables* » en soulignant que l'ambition de la défense antimissiles américaine était limitée à une protection contre l'Iran et la Corée du Nord. Ils n'en poursuivent pas moins, de leur côté, un programme de développement de missiles hypersoniques (Mach 5) destiné à répondre non seulement aux projets russes, mais à ceux de la Chine, considérés comme très avancés. Tout comme l'Inde, la France n'est pas en reste puisqu'elle développe le missile hypervéloce aéroporté ASN4G (air-sol nucléaire de 4ème génération) destiné à succéder au missile ASMP-A. Principal reproche adressé à ces choix technologiques : les missiles en question sont susceptibles de servir de vecteurs à des armes tant conventionnelles que nucléaires et risquent donc par méprise de provoquer une riposte nucléaire à une frappe conventionnelle.

En effet, le risque de guerre nucléaire est même aggravé par la **nature duale des missiles hypersoniques** : une attaque conventionnelle, par exemple contre des centres de commandement et contrôle, des systèmes d'alerte avancée terrestres ou spatiaux, des silos

de missiles ou des sous-marins en surface, des réseaux de communication, ou des porte-avions, pourrait entraîner une escalade vers la guerre nucléaire.

C'est précisément pour contourner la défense antimissile « classique » que la Russie et la Chine ont investi dans les missiles hypersoniques, censés déjouer toute neutralisation et renforçant ainsi l'intérêt d'une frappe en premier. Sauf que, pour anéantir toute capacité de riposte de l'adversaire, il faudrait pouvoir détruire non seulement tous ses sites terrestres (y compris de commandement et contrôle) mais aussi ses capacités sous-marines, ce qui reste encore impossible. En résumé, **ni les armes offensives ni les armes défensives ne sont capables d'éviter une guerre nucléaire**.

Même si les investissements russes et chinois dans les missiles hypersoniques sont énormes, à ce stade, ils semblent plutôt destinés à envoyer un message aux États-Unis : « *abandonnez votre défense antimissiles pour permettre à notre dissuasion ("seconde frappe") de fonctionner ou nous menaçons votre propre dissuasion par nos capacités de première frappe* ». Un jeu de poker dangereux qui ne peut que conduire à l'escalade.

Au-delà de toute considération sur l'absurdité et l'inefficacité de la « *dissuasion nucléaire* », il est donc grand temps, puisque la mise au point et le déploiement de ces systèmes exigent une longue durée, de briser ce cercle vicieux et de lancer la course au désarmement. La meilleure assurance que les armes nucléaires ne seront jamais utilisées reste sans conteste leur élimination. Mais on sait que celle-ci n'est pas pour demain.

En attendant, pour empêcher le déclenchement – fût-il accidentel ou involontaire – du cataclysme nucléaire, il est crucial de revenir aux mécanismes qui ont permis l'équilibre et la stabilité :

- Limiter les systèmes antimissiles ;
- Interdire les têtes nucléaires multiples (MIRV) ;
- Renforcer la transparence des activités balistiques et spatiales ;
- Négocier l'interdiction du déploiement d'ogives nucléaires sur des vecteurs hypersoniques, afin de confiner cette technologie au domaine de la défense conventionnelle et prévenir une redoutable dérive.

2.3 Bibliographie

- BAROTTE, Nicolas, « Les grandes puissances dans la course aux missiles hypersoniques », *Le Figaro*, 20 août 2020, https://www.lefigaro.fr/international/les-grandes-puissances-dans-la-course-aux-missiles-hypersoniques-20200820

- BORRIE, John, PORRAS, Daniel, « *The Implications of Hypersonic Missiles for International Stability and Arms Control* », UNIDIR, octobre 2019, https://unidir.org/sites/default/files/2019-10/Hypersonic%20Weapons%20Tabletop%20Exercise%20Report.pdf

- FINAUD, Marc, « Missiles hypersoniques et dissuasion nucléaire : un jeu de poker dangereux », *IDN*, 1er août 2018, https://www.idn-france.org/États-unis/missiles-hypersoniques-et-dissuasion-nucleaire-un-jeu-de-poker-dangereux/

- GUDRUB, Mark, « Going Too Fast: Time to Ban Hypersonic Missile Test? », *The Bulletin of the Atomic Scientists*, septembre 2015, https://thebulletin.org/2015/09/going-too-fast-time-to-ban-hypersonic-missile-tests-a-us-response/

- McWHINNEY, Mark, *The Risks of Hypersonic Weapons,* Canada, Ploughshares Spotlight, avril 2020, https://ploughshares.ca/wp-content/uploads/2020/12/Spotlight_Hypersonic-Weapons.pdf

- STEFANOVITCH, Dmitry, *Hypersonic weapons and arms control*, Russian International Affairs Council, décembre 2020, https://russiancouncil.ru/en/analytics-and-comments/analytics /hypersonic-weapons-and-arms-control/

- TRACY, Cameron L, WRIGHT, David « Modelling the Performance of Hypersonic Boost Glide-Missiles », *Science & Global Security*, vol. 28, n°3, avril 2020, p. 137-170, http://scienceandglobalsecurity.org/archive/2020/12/modelling_the_performance.html

3. LES ARMES À ÉNERGIE DIRIGÉE

Jacques Fath

Résumé : Les armes à énergie dirigée (armes laser ou armes à impulsion électromagnétique) s'inscrivent dans les technologies de la guerre électronique. Elles offrent des capacités multiples, notamment antimissiles ou de paralysie des systèmes de communication ou de commandement. Ces armes présentent des potentialités stratégiques fortes avec, par exemple, la neutralisation du fonctionnement ou la destruction des systèmes d'armement et de défense les plus sophistiqués, jusqu'aux aéronefs ou aux satellites dans leurs missions nucléaires. Elles rendent possible ce que l'on peut appeler des chaos stratégiques localisés (zones ou bases militaires) par l'interruption du fonctionnement des ordinateurs, de l'ensemble des systèmes informatiques ou de la distribution de l'électricité et par l'incapacité qu'elles peuvent imposer à contrôler ses propres forces. Contrairement à certaines thèses, les armes à énergie dirigée ne constituent pas une « alternative à la dissuasion », mais elles sont susceptibles d'en modifier les termes, d'en affecter singulièrement la logique et la pertinence en conférant à ceux qui les détiennent une capacité supérieure de neutralisation adverse et de première frappe nucléaire.

Le système laser AN/SEQ3 de la Marine américaine.
Source : J. F. Williams / US Navy

3.1 Définitions utiles

Une arme à énergie dirigée ou à rayonnement est une arme pouvant projeter vers une cible, à la vitesse de la lumière, un faisceau d'ondes laser ou micro-ondes, éventuellement (pour le laser) avec une forte directivité. De telles armes comportent plusieurs avantages : fulgurance, puissance modulable, précision, économie (pas de munitions). Elles peuvent atteindre des cibles très éloignées. Elles peuvent aveugler ou neutraliser des systèmes d'armes terrestres, aéroportées ou navales, ou encore des systèmes d'information et de communication.

3.1.1 Les armes à rayonnement

Les armes à rayonnement sont développées par les pays disposant des capacités de recherche et développement nécessaires, en particulier les plus grandes puissances (États-Unis, Chine, Russie, France…) qui sont, dans ce domaine comme dans bien d'autres, engagées dans une rapide et intense course aux armements. Cependant, le coût de ces armes, relativement peu élevé comparativement aux armements conventionnels sophistiqués actuels, pourrait intéresser nombre de pays désireux de disposer de systèmes aussi évolués et présentant des performances considérées comme dissuasives.

Ces armes entrent aujourd'hui dans l'expérimentation ou dans les phases d'intégration dans les armées. Elles ouvrent les champs de la guerre électronique.

3.1.2 Les armes laser

Les armes laser[2] agissent par concentration d'un faisceau sur une surface, par exemple la surface d'un missile. L'effet thermique peut permettre jusqu'à la perforation de cette surface. Plus le niveau de l'énergie dégagée est élevé, plus les cibles à traiter peuvent être importantes. L'efficacité de ces armes est cependant fonction des variations de l'environnement : brouillard, humidité, tempête de sable… Elles présentent un certain nombre de difficultés techniques, notamment la nécessité d'une production d'énergie considérable pour le tir. En conséquence, le système peut présenter un poids et un encombrement peu compatibles avec certains vecteurs aériens ou autres. Les applications militaires du laser sont très nombreuses : télémétrie, aide à la conduite du tir, éclairage des cibles, éblouissement de

[2] LASER est l'acronyme anglais de « light amplification by stimulated emission of radiation » signifiant « amplification de la lumière par émission stimulée de radiation ».

capteurs électroniques, télécommunications sécurisées, simulation nucléaire expérimentale (laser mégajoule).

3.1.3 Les armes à micro-ondes

Les armes à micro-ondes fonctionnent par l'émission de faisceaux ou d'impulsions d'ondes à haute fréquence, ou hyperfréquences. L'impulsion électromagnétique a le potentiel de dégrader voire de paralyser des circuits électroniques, des systèmes informatiques et des ordinateurs, des satellites, des systèmes de communication et de commandement et des infrastructures civiles ou militaires critiques (vitales), théoriquement sans dommages collatéraux, mais susceptibles d'affecter des civils.

3.2 Sur les armes laser et leur rapport au nucléaire

La technologie laser a de multiples vocations militaires, notamment celle de pouvoir être utilisée en milieu spatial (communications entre satellites), ou bien pour les liaisons terrestres avec les satellites, par exemple pour transmettre des données d'observation terrestre, ce qui montre le potentiel stratégique de cette technologie. Le laser est aussi (depuis au moins une dizaine d'années) en expérimentation pour les communications entre sous-marins, et entre des véhicules de surface et des sous-marins. Des recherches sont en cours, notamment afin de dépasser les limites inhérentes aux turbulences du milieu marin. L'utilisation du laser pour ce type de communications est susceptible de fournir une communication fiable, à haut débit et sûre, ce qui peut représenter un avantage stratégique. Dans ces deux configurations (milieu spatial et milieu marin), l'intérêt d'une telle technologie semble évident, par exemple pour contribuer à la maîtrise des forces nucléaires (forces aériennes stratégiques et sous-marins lanceurs d'engins – SNLE – concernant la France).

Des lasers antimissiles seraient susceptibles d'assurer la protection des aéronefs de soutien (avions ravitailleurs et de renseignement) au cours d'opérations aériennes effectuées dans des contextes conflictuels. L'utilisation de tels lasers pourrait être ainsi liée à des exercices ou des opérations stratégiques de dimension nucléaire.

Avec la possibilité de pointer un faisceau laser de haute puissance sur un missile de croisière ou un missile balistique, le laser pourrait acquérir une capacité d'élimination des menaces aériennes ou une capacité de défense antimissile adaptée à toutes sortes d'armes conventionnelles, hypersoniques, voire nucléaires. Mais on en est encore au niveau de l'expérimentation ou de la spéculation.

3.3 Sur les armes à impulsion électromagnétique et leur rapport au nucléaire

L'efficacité potentielle de ces armes sur les infrastructures (bases militaires stratégiques par exemple) ou sur certains armements se précise puisque les systèmes existants sont de plus en plus dépendants de leurs dispositifs électroniques, des moyens de transmission. Les armes à impulsion électromagnétique ont donc la capacité stratégique d'entraver, voire de neutraliser le fonctionnement des systèmes d'armement et de défense les plus sophistiqués jusqu'aux aéronefs, aux satellites, y compris dans leur possibles missions nucléaires. Des avions à mission nucléaire – le Rafale, le SCAF[3] demain… – pourraient voir leurs capacités mises en échec du fait d'une vulnérabilité aux armes électromagnétiques.

Avec les armes à micro-ondes ou hyperfréquences, il est possible de créer un chaos stratégique localisé par l'interruption des communications, du fonctionnement des systèmes informatiques, de la distribution d'électricité, par la paralysie des systèmes de commandement, par l'incapacité à contrôler ses propres forces. D'où la tentation de concevoir des dispositifs offensifs suffisamment puissants qui soient capables de démultiplier les effets d'impulsion électromagnétique. Contrairement à certaines thèses, les armes à énergie dirigée ne constituent pas une « alternative à la dissuasion nucléaire », mais elles sont susceptibles d'en modifier les termes, d'en affecter singulièrement la logique en conférant à ceux qui les détiennent une capacité supérieure de neutralisation adverse, et ainsi une possibilité d'initiative de première frappe.

3.4 Qu'est-ce qui change avec les armes à énergie dirigée ?

Les hautes technologies, comme multiplicateurs de force et révolution dans les capacités, permettent la mise au point de nouvelles catégories d'armements capables (hors nucléaire) de porter des frappes et de produire des dommages qualitativement supérieurs à ce qui était possible auparavant. On entre dans une autre dimension. Cependant, il ne s'agit

[3] Système de Combat Aérien du Futur : il s'agit d'un projet d'avion européen très complexe censé devenir opérationnel en 2040, et devant être construit par des groupes industriels de défense de France, d'Allemagne et d'Espagne.

pas d'armes de dissuasion au sens stratégique habituel, mais de nouveaux moyens de guerre, ici de guerre électronique.

Il faut rappeler qu'évidemment, par définition, les armes nucléaires et les armes conventionnelles relèvent de deux ordres militaires et stratégiques différents, mais il existe des continuums structurants dans les systèmes de défense et dans les stratégies. Aujourd'hui, les armes à rayonnement, comme d'autres armements de hautes technologies, pourraient faire bouger sensiblement ce constat de base. Les hautes technologies, et notamment les armes à rayonnement, vont introduire à la fois des vulnérabilités nouvelles et des moyens spécifiques inédits de protection et d'efficacité pour les infrastructures, pour les vecteurs, pour les dispositifs de commandement, notamment pour le nucléaire. Les hautes technologies poussent donc à une intégration plus forte dans les systèmes de défense.

Alors que l'on assiste à un certain renouveau de l'intérêt pour des armes nucléaires tactiques, davantage susceptibles d'un emploi effectif, une plus grande intégration entre conventionnel, nucléaire et hautes technologies dans les systèmes de défense, pourrait signifier une perte de pertinence (supplémentaire) de la dissuasion au sens strict ou traditionnel, au profit d'une nouvelle conception de la guerre, intégrant l'ensemble des moyens dans tous les domaines. On peut craindre un risque nucléaire ainsi amplifié.

L'impact des armes à énergie dirigée sur le nucléaire s'annonce donc réel, comme l'est celui de l'hypersonique, de l'intelligence artificielle ou de la cyberdéfense. Ce n'est pas une forme de « dépassement » du nucléaire militaire par les hautes technologies. Mais cela induit de grandes transformations dans les formes de la guerre.

Les nouveaux systèmes d'armes reposent sur des technologies de très haut niveau impliquant vitesse, puissance, précision, adaptabilité, autonomie. Dans le nouveau contexte stratégique, de grandes guerres, des conflits dits de haute intensité... redeviennent d'autant plus envisageables (voire probables ?) que le numérique, l'intelligence artificielle, la confrontation croissante dans le cyberespace et dans l'espace extra-atmosphérique, la robotisation... risquent de nourrir, dans le processus de dématérialisation en cours, la dangereuse illusion d'une « *mise à distance* » de la guerre et des chocs futurs, et l'illusion d'un reflux des risques pour la vie humaine, la vie des soldats en particulier. Au risque bien réel d'escalades permettant les guerres d'aujourd'hui et de demain, avec éventuellement des dimensions nucléaires.

On peut tenter de différencier l'impact des hautes technologies en fonction de leurs caractéristiques et de leurs fonctions réelles ou potentielles. Comme l'IA, le cyber et

l'informatique quantique auront certainement un impact transversal, voire global sur des systèmes de défense fortement intégrés. Quant à l'hypersonique, il pourrait s'inscrire comme un « *game changer* » au sens d'une forte potentialité de rupture stratégique.

Il est en réalité assez compliqué, et peut-être pas forcément nécessaire (mais cela aide à l'analyse) d'établir des hiérarchies ou des calibrages fonctionnels entre technologies. En réalité, c'est la configuration novatrice des opérations dites multi-domaines (ou du combat collaboratif) qui se concrétise ainsi grâce aux technologies qui permettent et qui accélèrent cette forme très intégrée des opérations de guerre : une guerre « *globale* » rendue possible notamment par les technologies qui en fournissent les instruments sophistiqués d'une très grande diversité. Dans cette guerre globale, c'est surtout l'intégration et la complémentarité de toutes les composantes de défense qui détermineront les nouvelles normes de la puissance militaire. La « *performance* » technologique et militaire sera globale. La supériorité dépendra de la capacité à maîtriser cette intégration et synchronisation des opérations de guerre.

Manifestement, on est seulement au début de cette guerre du futur dont les technologies ne constituent qu'un aspect. Cette guerre du futur, c'est le produit, à la fois, des mutations technologiques et de la transformation radicale du contexte géopolitique mondial.

Nous entrons dans une phase de compétitions et de confrontations exacerbées dominées par les principales puissances (États-Unis, Chine, Russie...), avec un effondrement périlleux de l'architecture internationale de sécurité existante (notamment l'« *arms control* ») et du multilatéralisme. La guerre du futur qui se dessine signifie un changement de période, des risques nouveaux, des enjeux de sécurité internationale transformés dans le contexte de la fin de l'ordre international installé sous hégémonie américaine après 1945.

3.5 Interpeller les autorités françaises

La France est très engagée sur les hautes technologies militaires depuis des années. En 2018, elle a mis en place l'Agence de l'innovation défense. En 2019, elle a installé la Red Team chargée, avec l'aide d'experts, d'auteurs et de scénaristes de science-fiction, de dégager des idées « *disruptives* » et une vision prospective. En 2020, elle a créé le Comité d'éthique de la défense lié en particulier aux conséquences de l'émergence des nouvelles technologies dans la défense. Concernant les armes à énergie dirigée, elle teste, notamment pour la Marine nationale, une tourelle laser « *Helma-P* », dont la vocation est de suivre et d'abattre des cibles en vol, comme des drones.

Pourtant, les Livres blancs sur la défense et la sécurité nationale (LBDSN) de 2008 et 2013, mais aussi la Revue stratégique de 2017, ne font guère de commentaires sur les projets français et sur l'intérêt du pouvoir politique pour les hautes technologies militaires en général. Dans ses discours officiels concernant la défense, le président Emmanuel Macron n'en dit pas un mot. La ministre des Armées Florence Parly ne s'attarde jamais sur le fond du problème.

Quant à l'Union européenne, elle a mis au point un projet de « *capacité de guerre électronique* », adopté le 19 novembre 2018 dans le cadre de la Coopération structurée permanente (CSP), en vue de la création d'une « *unité de guerre électronique commune* ». Les pays participants à ce projet sont l'Allemagne et la République tchèque comme chefs de file[4].

La signification de l'émergence des hautes technologies militaires dans l'ordre international et leur intégration aujourd'hui nettement plus volontariste qu'hier dans la politique de défense de la France ne peuvent pas être traitées dans la quasi- ou semi-confidentialité qui aujourd'hui domine le discours, ou plutôt le non-discours officiel. Comme si le pouvoir politique français voulait masquer la nature et la portée de ses choix… et de ses difficultés.

3.6 Bibliographie

Livres et documents généraux

- ASSOCIATION DES AUDITEURS ET CADRES DES HAUTES ETUDES DE L'ARMEMENT (AACHEAR), *Géostratégie et armements au XXIe siècle*, La Documentation française, Collection armements et sécurité, 2014, 570 p.

- BOUTHERIN, Grégory, « Un nouveau phénomène conceptuel made in USA : le combat multidomaine », *Areion24News*, 9 janvier 2017, https://www.areion24.news/2017/01/09/nouveau-phenomene-conceptuel-made-in-usa-combat-multidomaine/

- DEPARTEMENT AMERICAIN DE LA DEFENSE, « *Directed Energy Futures 2060. Visions for the next 40 years of U.S. Department of Defense Directed Energy technologies* »,

[4] Voir « Défense européenne : le défi de l'autonomie stratégique », Rapport d'information n° 626 (2018-2019) de Ronan Le Gleut et Hélène Conway-Mouret au nom de la Commission des affaires étrangères, de la défense et des forces armées du Sénat, 3 juillet 2019. Annexe 2, projets CSP (https://bit.ly/3gmxWVN).

https://www.afrl.af.mil/Portals/90/Documents/RD/Directed_Energy_Futures_2060_Final29June21_with_clearance_number.pdf

– FATH, Jacques, « Les très hautes technologies dans une nouvelle course aux armements », dans FATH Jacques, *Chaos. La crise de l'ordre international libéral. La France et l'Europe dans l'ordre américain*, Éditions du Croquant, 2020, pp. 101-136.

– FAURY Etienne, « Les opérations multidomaines : une révolution militaire », « 2020 : chocs stratégiques », regards du CHEM - 69e session, *Revue Défense nationale*, 2020, https://www.defnat.com/e-RDN/vue-article-cahier.php?carticle=235

– FONTAINE, Bernard, (préf. PARRAUD, PAUL), *Les armes à énergie dirigée : mythe ou réalité ?*, L'Harmattan, octobre 2011.

– LAURENT, Boris, « De la bataille aux opérations multidomaines : se préparer pour la guerre du futur », *Areion24News*, 22 juillet 2020, https://www.areion24.news/2020/07/22/de-la-bataille-aux-operations-multidomaines-se-preparer-pour-la-guerre-du-futur/

– LELE, Ajay, *Quantum Technologies and Military Strategy*, Springer, 2021.

– MISSIROLI, Antonio, « Game of drones ? Ou comment les nouvelles technologies influent sur la dissuasion, la défense et la sécurité », *NATO Review*, 5 mai 2020, https://www.nato.int/docu/review/fr/articles/2020/05/05/game-of-drones-ou-comment-les-nouvelles-technologies-influent-sur-la-dissuasion-la-defense-et-la-securite/index.html.

– SECRETARIAT GENERAL DE LA DEFENSE ET DE LA SECURITE NATIONALE (SGDSN), «*Chocs futurs - Étude prospective à l'horizon 2030 : impacts des transformations et ruptures technologiques sur notre environnement stratégique et de sécurité »*, 2017, http://www.sgdsn.gouv.fr/rapport_thematique/chocs-futurs/

Sources de l'industrie de défense

– CAILABS, « AED Armes laser à énergie dirigée », https://www.cailabs.com/application/armes-laser-a-energie-dirigee/

– CAILABS, « Communications laser sous-marines : Tilba fiabilise les communications laser sous-marines en compensant la turbulence », https://www.cailabs.com/application/communications-laser-sous-marines/

– LOCKHEED MARTIN, « New age threats require new age defenses: Directed Energy Technology has advanced from the lab and is now ready for the field », https://www.lockheedmartin.com/en-us/capabilities/directed-energy.html

– LOCKHEED MARTIN, « Tactical airborne laser pods are coming », https://www.lockheedmartin.com/en-us/news/features/2020/tactical-airborne-laser-pods-are-coming.html

– THALES DEFENSE ET SECURITE, « Systèmes optroniques pour les forces aériennes », https://www.thalesgroup.com/fr/activites/defense/air-forces/systemes-optroniques-forces-aeriennes

Articles et thèmes particuliers

– ARMEE DE L'AIR ET DE L'ESPACE, « Chammal : première mission opérationnelle du pod Talios », 7 décembre 2020, https://www.defense.gouv.fr/air/actus-air/chammal-premiere-mission-operationnelle-du-pod-talios

– BOURDON, Pierre, *Technologies laser pour applications militaires*, thèse (optique/photonique), Université Paris-Sud, Faculté des Sciences d'Orsay», 2016, 183 p., https://hal.archives-ouvertes.fr/tel-01371573/document

– COHEN, Rachel S, « Some Directed-Energy Weapons Show Promise While Others Slow », *Air Force Magazine*, 7 juillet 2020, https://www.airforcemag.com/some-directed-energy-weapons-show-promise-while-others-slow/

– « Les armes laser : vers une entrée timide dans l'arène du combat naval à l'orée de la prochaine décennie », *Défense et industrie*, n°12, (octobre 2018), https://www.frstrategie.org/sites/default/files/documents/publications/defense-et-industries/2018/12-5.pdf

– FENG, John, « China Developing Unique Laser Gun for Faster Hypersonic Missiles and Planes », *Newsweek*, 27 juillet 2021, https://www.newsweek.com/china-developing-unique-laser-gun-faster-hypersonic-missiles-planes-1613374

– KELLER John, « Air Force asks industry for laser weapons and high-power micro-wave to defend against cruise missiles.», *Military & Aerospace Electronics*, 10 septembre 2019, https://www.militaryaerospace.com/power/article/14039601/laser-weapons-cruise-missiles-highpower-microwaves

– « Les armes laser : vers une entrée timide dans l'arène du combat naval à l'orée de la prochaine décennie », *Défense et industrie*, n°12, octobre 2018, https://www.frstrategie.org/sites/default/files/documents/publications/defense-et-industries/2018/12-5.pdf

– KELLER, John, « Wanted: high power RF and microwave amplifiers for electronics-killing electronic warfare (EW) systems », *Military & Aerospace Electronics*, 11 mars 2021, https://www.militaryaerospace.com/rf-analog/article/14199141/rf-and-microwave-amplifiers-electronic-warfare-ew

– PARDE, Nathan, « Lincoln Laboratory advances undersea optical communications: Researchers are applying narrow-beam laser technology to greatly improve communications between underwater vehicles », *MIT Lincoln Laboratory News*, 1er août 2018.

– VERGUN, David, « DoD Officials Discuss Framework for Advancing Directed Energy Weapons », *DoD News*, 11 août 2020, https://www.defense.gov/Explore/News/Article/Article/2309408/dod-officials-discuss-framework-for-advancing-directed-energy-weapons/

– VERGUN, David, « Ready, Aim, Fire: Hypersonics, Directed Energy, Lasers », *DoD News*, 25 avril 2019, https://www.defense.gov/Explore/News/Article/Article/1824471/ready-aim-fire-hypersonics-directed-energy-lasers/

– WILSON, J.R, « The new era of high-power electromagnetic weapons », *Military & Aerospace Electronics*, 19 novembre 2019, https://www.crows.org/news/478754/The-new-era-of-high-power-electromagnetic-weapons.htm

– WOLF, Fabrice, « La vulnérabilité des avions ravitailleurs inquiète l'US Air Force », *Meta Défense*, 24 septembre 2020, https://www.meta-defense.fr/2020/09/24/la-vulnerabilite-des-avions-ravitailleurs-inquiete-lus-air-force/

– WOLF, Fabrice, « Les armées françaises se préparent à tester leurs premières armes laser de la PME orléanaise CILAS », *Meta Défense*, 3 mars 2020, https://www.meta-defense.fr/2020/03/03/les-armees-francaises-se-preparent-a-tester-leurs-premieres-armes-laser-de-la-pme-orleanaise-cilas/

4. LA MENACE CYBER

Solène Vizier

Résumé : L'avènement de l'ère du numérique augmente les risques quant aux vulnérabilités préexistantes au sein des systèmes d'armes nucléaires, et crée de nouvelles menaces. Les systèmes de communication et de contrôle peuvent être piratés, tandis que les systèmes de communication, les données télémétriques des missiles, les installations d'assemblage ou encore les systèmes autonomes robotisés dans l'infrastructure stratégique sont vulnérables. Le développement d'armes intelligentes, comme les défenses antimissiles balistiques ou les armes satellites, aura un impact sur les pensées et les stratégies nucléaires. Ces nouvelles technologies peuvent offrir des possibilités de « dissuasion par déni » : conçues pour intercepter les missiles ou les ogives après le lancement, elles sont aussi utilisées pour empêcher les systèmes d'armes nucléaires de fonctionner comme prévu. Bref, c'est toute la stratégie nucléaire qui est remise en question.

Officiers de cyberguerre.
Source : ASPI Strategist

Introduit dans le lexique de la sécurité nationale au début des années 1990, le terme "cyber", préfixe de cybernétique, est devenu une expression générique utilisée pour signifier la dimension numérique de la notion qu'il accompagne (cyberdéfense, cyberdiplomatie, cyberterrorisme…). **La notion de "*cyber*" peut être définie à la fois comme l'émergence d'un nouveau contexte numérique et comme un nouvel ensemble d'outils, de dynamiques et d'armes.**

L'avènement de l'ère du numérique augmente désormais les risques quant aux vulnérabilités préexistantes, et crée de nouvelles menaces. La fiabilité et l'intégrité des systèmes d'armes nucléaires dans toutes leurs actions sont aujourd'hui interrogées. **Leur piratage, qui semblait hier impossible, est aujourd'hui devenu un risque réel.** La menace est d'autant plus grande que les armes nucléaires ont été créées à une époque où l'informatique en était à ses balbutiements et que le risque cybernétique n'a pas été pris en compte dans l'architecture des systèmes et stratégies nucléaires actuelles. Et si les armes nucléaires sont censées être des ordonnances politiques plutôt que militaires, supposées maintenir la paix sans jamais être utilisées, les obstacles à leur utilisation s'érodent peu à peu.

Le cyber-défi touche au commandement et au contrôle de toutes les technologies de l'information impliquée dans la gestion des armes nucléaires. Il opère dans les quatre domaines de l'environnement de l'information :

- Physique / mécanique : les infrastructures physiques et le matériel,
- Logique : les commandes indiquant au matériel quoi faire et les logiciels permettant la transmission, - l'interprétation et le partage de l'information–,
- Informationnel : les informations et les données que le système collecte, stocke, génère et utilise pour fonctionner,
- Humain / cognitif : les êtres humains et leurs interactions avec le matériel, les logiciels et l'information.

4.1 Les cybermenaces

Les cybermenaces englobent un spectre large d'activités, du simple piratage aux attaques de déni de service, de l'espionnage au sabotage. Les risques cybernétiques ont introduit de nouvelles vulnérabilités – entendues comme des faiblesses au niveau d'un élément

d'un système industriel ou d'information – dans les systèmes d'armes nucléaires. Dans son rapport « *Cybersecurity of Nuclear Weapons Systems Threats, Vulnerabilities and Consequences* », le Département de sécurité internationale de Chatham House a identifié **13 zones vulnérables aux cyber-risques**, parmi lesquelles les différents systèmes de communication, les données télémétriques des missiles, les cyber-technologies dans les laboratoires et les installations d'assemblage, les informations météorologiques et de ciblage provenant de systèmes spatiaux ou de stations au sol, ou encore les systèmes autonomes robotisés dans l'infrastructure stratégique. Ces zones vulnérables possèdent toutes des vecteurs d'attaques par lesquels un acteur malveillant peut accéder à une information sensible ou créer de fausses informations.

4.1.1 Le cyberespionnage.

Souvent considéré comme la deuxième profession la plus ancienne au monde, l'espionnage n'est pas un défi nouveau pour les systèmes d'armes nucléaires et a contribué à la prolifération nucléaire au XX^{e} siècle. Le second âge nucléaire (depuis 1991) présente deux ensembles de défis. Pour Andrew Futter, un premier développement clé pour l'espionnage nucléaire est le recours croissant aux ordinateurs numériques pour le stockage des données. Du matériel scientifique et technique sur les essais nucléaires, des données de recherche et développement, des conceptions d'armes, des structures militaires, des doctrines sont stockées sur des réseaux. Cela rend l'accès à l'information plus aisé, même si ces ordinateurs sont séparés de l'Internet et des réseaux non-sécurisés. Une part importante des opérations d'espionnage nucléaire a impliqué des initiés ayant accès à des systèmes mal sécurisés en raison de manquements importants en termes de cybersécurité et de cyber-hygiène. Le deuxième développement clé tient à la capacité d'accéder et de cibler les secrets nucléaires à distance – comme dans le cadre de l'attaque **SolarWinds** qui a notamment touché début 2020 la *National Nuclear Security Administration* des États-Unis.

4.1.2 Manipulation de l'information et cyber-handicap.

La cybermenace affecte les risques nucléaires principalement de deux façons : **elle compromet les systèmes d'information et d'alerte liés aux armes nucléaires, mais aussi les systèmes de commandement et de contrôle des armes nucléaires**. L'expert Andrew Futter souligne ainsi que le premier défi majeur aux systèmes d'armes nucléaires est la contamination et la manipulation (*spoofing*) de l'information sur laquelle les décisions

nucléaires sont fondées. Les capteurs et les systèmes pourraient être trompés – et l'ont déjà été – soit par un faux positif, soit par un faux négatif. Les pirates pourraient, en outre, accéder directement aux systèmes de d'alerte ou de communication pour manipuler, contaminer, corrompre l'information au sein des réseaux, induisant des erreurs de compréhension en temps de crise nucléaire. Il existe enfin des vulnérabilités concernant l'accès des systèmes à bord des satellites. Les informations sur lesquelles s'appuient les systèmes nucléaires et leurs opérateurs représentent le vecteur de menace le plus direct, en temps de crise comme en temps de paix. En réalité, le seul fait de **savoir que les systèmes nucléaires sensibles pourraient être compromis remet en cause la confiance en ces mêmes systèmes**, indépendamment de l'ampleur ou de la nature de l'attaque.

Le deuxième défi, qui n'est pas nouveau, concerne **le risque de cyber-handicap et de destruction pour les systèmes d'armes nucléaires**. Les capacités cybernétiques pourraient être utilisées pour les désactiver, les perturber ou les détruire, à travers des logiciels malveillants, des bombes logiques, des codages trafiqués, des chevaux de Troie introduits dans les logiciels, les systèmes ou les composants des armes nucléaires. La chaîne d'approvisionnement est particulièrement vulnérable. Selon le rapport de Beyza Unal et Patricia Lewis pour Chatham House, plusieurs aspects du développement des armes nucléaires – dont la production d'ogives – et la gestion des systèmes sont privatisés, et il y a donc un risque important d'introduction de vulnérabilités lors de la fabrication compromettant l'intégrité globale des systèmes d'armes nucléaires nationaux.

4.2 Vers un troisième âge nucléaire et la fin du principe de « *dissuasion* ».

Les capacités cybernétiques des États modifient la composition des systèmes d'armes conventionnelles et nucléaires, et mettent à mal les principes de la « *dissuasion nucléaire* ».

Si les nouvelles technologies sont une aide à la fonctionnalité des systèmes, à la prise de décision en temps réel et au traitement des données, **les nouveaux ordinateurs et codes complexes rendent également les systèmes moins sûrs, plus difficiles à protéger et donc plus faciles à compromettre**. Un recours accru à des systèmes d'informations de plus en plus complexes pour les opérations nucléaires augmente la possibilité d'erreurs, de défaillances et d'accidents. De même, le recours croissant à des technologies

commerciales crée d'importants risques. Par exemple, plusieurs États dotés de l'arme nucléaire comptent en effet sur des technologies commerciales et des composants achetés à l'étranger pour des opérations nucléaires sensibles, car ils sont incapables fabriquer des composants de haute technologie et des puces informatiques.

Le développement des capacités cybernétiques a aussi **un effet transformateur sur les autres systèmes d'armes**. Le développement d'armes intelligentes, comme les défenses antimissiles balistiques ou les armes satellites, aura un impact sur les pensées et les stratégies nucléaires. Ces nouvelles technologies peuvent offrir des possibilités de « *dissuasion par déni* » : conçues pour intercepter les missiles ou les ogives après le lancement, elles sont aussi utilisées pour empêcher les systèmes d'armes nucléaires de fonctionner comme prévu. Cela amène des questions importantes pour la sécurité, la réflexion et la stratégie nucléaire : capacité des États à viser des cibles adverses vulnérables face aux boucliers antimissiles, rôle de contre-force non-nucléaire des technologies avancées, risques des technologies à double usage, intelligence artificielle… Si cette dernière peut aider à la décision, la RAND Corporation souligne son fort potentiel déstabilisateur. **L'intelligence artificielle va renforcer les capacités de renseignement des États les plus avancés, affaiblissant la « *dissuasion nucléaire* », et accélérant la prise de décision dans les crises nucléaires.**

Ainsi, **la nouvelle menace cyber fait peser des risques importants sur le principe même de « dissuasion nucléaire »**. Élément clé des futurs conflits, les cyber-capacités offensives, dont l'avantage est à l'attaquant plutôt qu'au défenseur, auront pour effet d'augmenter les tensions en temps de crise, et cela pourrait avoir des conséquences importantes pour la stabilité stratégique, **nécessitant de repenser les concepts nucléaires établis.**

Les risques qui pèsent sur les systèmes de commandement et de contrôle nucléaire, ainsi que sur les systèmes d'information et d'alerte précoce pourraient **rendre inopérant l'ordre nucléaire** en cas de crise. Dans le cas de l'intelligence artificielle comme des cyberattaques, la seule existence de tels moyens d'attaque pourrait saper la confiance entretenue envers les systèmes d'armes nucléaires et **remettre en question la capacité nucléaire de seconde frappe**. Craignant de ne plus avoir la possibilité de mener des représailles, **les États pourraient se sentir si vulnérables qu'ils mèneraient des actions préemptives.** Les risques sont d'autant plus grands que plusieurs des États dotés de l'arme nucléaire maintiennent leurs forces nucléaires en état d'alerte permanent, et que les

temps de lancement sont de plus en plus réduits. Le développement de capacités cybernétiques offensives pourrait alors bouleverser l'échelle traditionnelle de l'escalade : les États pouvant être rendus vulnérables à tout moment par leurs ennemis, étatiques ou non, on entre alors dans un « *état permanent de rivalité* ».

Selon Futter, ces évolutions pourraient avoir de graves conséquences sur la dissuasion nucléaire fondée sur la capacité de seconde frappe et sur la peur de destruction mutuelle assurée. La potentielle utilisation des capacités cybernétiques comme précurseurs pour retarder les systèmes avant de mener une attaque stratégique introduit le risque que les systèmes puissent être compromis et donc ne fonctionnent pas comme prévu. **Les États réintroduiraient alors la possibilité d'effectuer des frappes préventives contre les armes nucléaires ou les systèmes associés.**

Cela aura aussi **un impact sur la probabilité d'un futur accord de réduction des armements nucléaires, ainsi que sur la prolifération nucléaire**, car toute réduction des armements pourrait accroître l'influence des cybermenaces. Les armes cybernétiques représentent donc un risque de contre-pouvoir sérieux et croissant, avec l'avènement d'un dilemme de sécurité cyber, où les États dotés de l'arme nucléaire doivent supposer que leurs infrastructures de sécurité nationale sont ciblées. Cela entraîne une incitation croissante des États nucléaires à adapter leurs politiques nucléaires vers une « *dissuasion préventive* » fondée sur la « *dissuasion par déni* » plutôt que la « *dissuasion par punition* ». **Le caractère sacré des normes nucléaires est en passe d'être entièrement réévalué, et laisse craindre un abaissement du seuil nucléaire.**

4.3 Bibliographie

- ARQUILLA, John, RONFELD, David, *Cyberwar is Coming*, RAND Corporation, 1993

- BLAIR, Bruce, « Could U.S.-Russia Tensions Go Nuclear? » *Politico*, 27 novembre 2015, https://www.politico.com/magazine/story/2015/11/russia-us-tensions-nuclear-cold-war-213395/

- BORRIE, John, CAUGHLEY, Tim, WAN, Wilfred (dir.), *Understanding Nuclear Weapon Risks*, UNIDIR, 2017.

– CIMBALA, Stephen J., « Nuclear Deterrence and Cyber: The Quest for Concept », *Air & Space Power Journal*, mars-avril 2014.

– CLECH, Jérôme « L'hybridité : nouvelles menaces, inflexion stratégique ? » *Revue Défense Nationale*, 3(3), (2016), p. 12-18, https://www.cairn.info/revue-defense-nationale-2016-3-page-12.htm

– DEJEAN, Philippe, & SARTRE, Patrice, « La cyber-vulnérabilité ». *Études*, (juillet-août 2015), p. 21-31.

– DEPARTMENT OF DEFENSE OF THE UNITED STATES, DEFENSE SCIENCE BOARD, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, janvier 2013.

– DEPARTMENT OF DEFENSE OF THE UNITED STATES, *Nuclear Posture Review*, 5 février 2018.

– DOUZET, Frédérick, « Le cyberespace, un champ d'affrontement géopolitique », in GIBLIN, Béatrice (dir.), *Les conflits dans le monde : Approche géopolitique* (327-343). Paris : Armand Colin, 2016

– DUNN, Will, « Can Nuclear Weapons be Hacked?" *New Statesman* », 7 mai 2018, https://www.newstatesman.com/spotlight-america/cyber/2018/05/can-nuclear-weapons-be-hacked

– FUTTER, Andrew, *Hacking the Bomb: Cyber Threats and Nuclear Weapons,* Georgetown University Press, Washington DC, 2018.

– GEIST, Edward, Lohn Andrew J., « How Might Artificial Intelligence Affect the Risk of Nuclear War? », *Security 2040*, RAND Corporation, 2018.

– GROLL, Elias, « How AI Could Destabilize Nuclear Deterrence », *Foreign Policy*, 24 avril 2018, https://foreignpolicy.com/2018/04/24/how-ai-could-destabilize-nuclear-deterrence/

– HEALY, Jason, « Beyond Attribution: Seeking National Responsibility for Cyber Attacks », *Issue Brief*, Conseil Atlantique, Washington, DC, 2011.

– HOLLANDE, François, « Discours sur la dissuasion nucléaire », Istres, 19 février 2015.

- IASELLO, Emilio, « Is Cyber Deterrence an Illusory Course of Action? », *Journal of Strategic Security*, Henley-Putnam University, n° 1, 2013.

- « Ile Longue. Les incroyables failles dans la sécurité », *Le Télégramme*, (11 juin 2013), https://www.letelegramme.fr/ig/generales/fait-du-jour/ile-longue-des-failles-dans-la-securite-11-06-2013-2132250.php#7LdM2xQTcRHTzk4R.99

- MAZAAR, Michael J., « Rivalry's new face », *Survival*, n°54, vol. 4, 2012.

- MINISTERE FRANÇAIS DE L'INTERIEUR, DELEGATION MINISTERIELLE AUX INDUSTRIES DE SECURITE ET A LA LUTTE CONTRE LES CYBERMENACES, *État de la menace liée au numérique en 2017*, janvier 2017.

- NTI, *The 2016 NTI Nuclear Security Index: Theft and Sabotage - Building a Framework for Assurance, Accountability, and Action,* in, 3e édition, janvier 2016.

- OFFICE OF THE PRESIDENT OF THE UNITED STATES, *International Strategy for Cyberspace*, 2011.

- PINTAT, Xavier, LORGEOUX, Jeanny, TRILLARD, André, ALLIZARD, Pascal, HAUT Claude, « La nécessaire modernisation de la dissuasion nucléaire », *Rapport d'information n°560 au nom de la Commission des Affaires étrangères, de la Défense et des Forces armées du Sénat*, 23 mai 2017.

- SANGER, David E., BROAD William J., « Pentagon Suggests Countering Devastating Cyberattacks with Nuclear Arms », *New York Times*, 16 janvier 2018, https://www.nytimes.com/2018/01/16/us/politics/pentagon-nuclear-review-cyberattack-trump.html

- STEWART Phil, « Deep in the Pentagon, a secret program to find hidden nuclear missiles », *Reuters*, 5 juin 2018, https://www.reuters.com/article/us-usa-pentagon-missiles-ai-insight-idUSKCN1J114J

- STOUTLAND, Page, "Growing Threat: Cyber and Nuclear Weapons Systems", *Bulletin of Atomic Scientists*, 18 octobre 2017, https://thebulletin.org/2017/10/growing-threat-cyber-and-nuclear-weapons-systems/

- STOUTLAND, Page, PITTS-KIEFFER, Samantha, *Nuclear Weapons in the Cyber Age: Report of the Cyber-Nuclear Weapons Study Group*, NTI, septembre 2018.

– UNAL, Beyza, LEWIS Patricia, *Cybersecurity of Nuclear Weapons Systems Threats, Vulnerabilities and Consequences*, International Security Department, Chatham House, janvier 2018.

– US HOUSE OF REPRESENTATIVES, « *The Report of the Select Committee on US National Security and Military/Commercial Concerns with the People's Republic of China* », 1999.

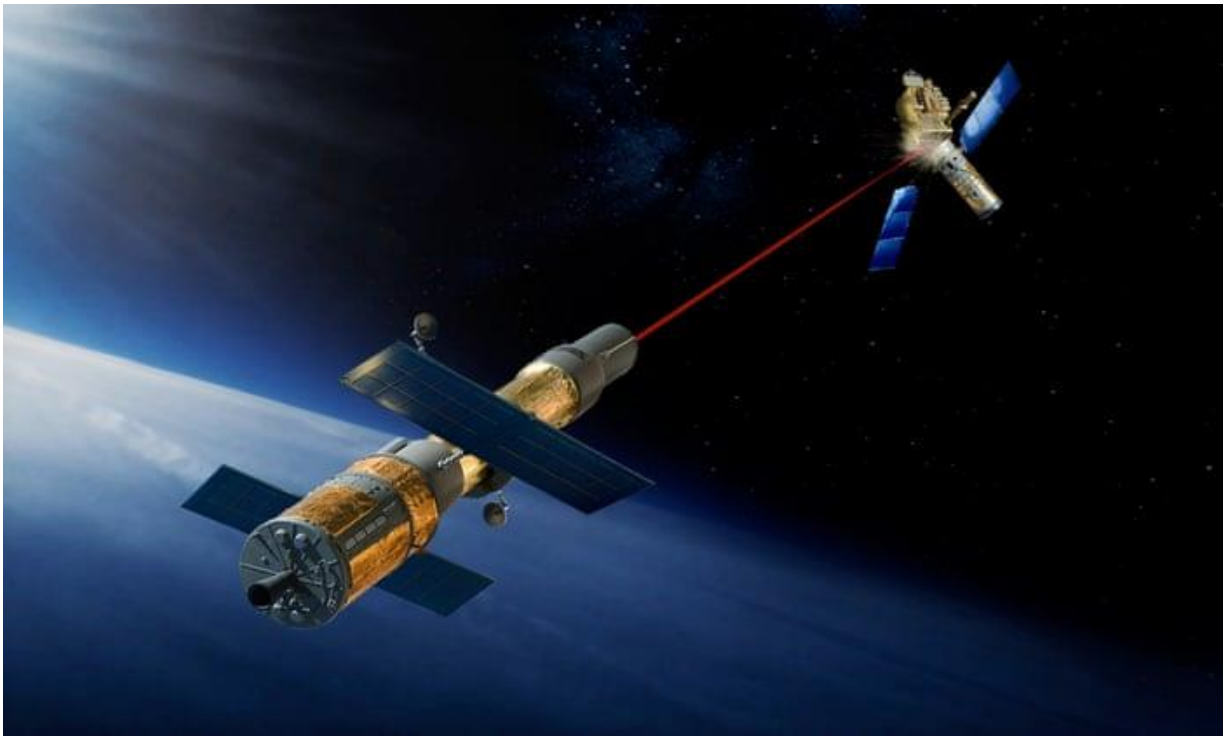
– VIZIER, Solène, *« SolarWinds, une cyberattaque qui remet en cause la dissuasion nucléaire », IDN*, janvier 2021, https://www.idn-france.org/nos-publications/actualites/solarwinds-cyberattaque-remet-en-cause-dissuasion-nucleaire/

– WIENER Norbert, *Cybernetics or control and communication in the animal and the machine* (2nd edition), the M.I.T press, Cambridge, 1948.

5. LA GUERRE ET L'ESPACE

Paul Quilès

Résumé : L'espace est devenu indispensable à la vie économique et sociale sur Terre. Mais en même temps, l'espace est devenu un nouveau champ de confrontation. Historiquement contenu dans les trois domaines – Air-Terre-Mer – l'affrontement stratégique s'étend à de nouveaux champs : cyber, espace, cognitif. L'exacerbation de la compétition internationale conjuguée à l'émergence de nouvelles technologies rend la perspective d'une véritable guerre de l'espace, une nouvelle « guerre des étoiles », de moins en moins hypothétique.



Reconstitution d'une attaque par laser contre un satellite.
Source : Erik Simonsen/Photographers Choice/Getty Images

Dans une récente interview au *Figaro*[5] le général James Dickinson, commandant de l'Espace des États-Unis, déclarait : « *l'espace jouera un grand rôle dans le prochain conflit* » et le général Michel Friedling, commandant de l'Espace au ministère français des Armées, ajoutait : « *l'espace est un lieu de menaces émergentes* ».

5.1 Quelques chiffres :

- 30 États ont au moins un satellite en orbite ;
- Il existe 22 000 objets en orbite, dont 2 000 satellites en fonction ;
- 400 satellites militaires sont en orbite dont 13 de la France ;
- On distingue 3 orbites : géostationnaire (36 000 km) pour les satellites de télécommunications, basse (entre 160 et 2 000 km) pour les satellites d'observation (civile et militaire) et moyenne (entre 2 000 et 35 786 km) pour la géolocalisation (GPS, Galileo) ;
- Le projet *Starlink* (SpaceX) prévoit la mise en orbite de 12 000 satellites ;
- 70 % du renseignement américain provient de l'espace ;
- Les budgets pour l'espace atteignent 50 milliards de dollars pour les États-Unis et 10 milliards de dollars pour la Chine ;
- Les revenus mondiaux du spatial devraient passer (selon Morgan Stanley) de 350 milliards de dollars aujourd'hui à 1 000 milliards de dollars en 2040.

L'Inde, qui a mis au point son premier missile antisatellite, et le Japon commencent à développer des activités militaires spatiales.

En résumé, l'espace est devenu indispensable à notre vie. En particulier l'information sur laquelle reposent maintenant tous les flux intellectuels, commerciaux, culturels, sociaux et de santé transite pour une grande part par l'espace.

[5] *Le Figaro*, 2 juillet 2021, propos recueillis par Nicolas Barotte.

5.2 Peut-on « réguler » l'espace ?

Le Traité sur l'Espace de 1967, élaboré dans le cadre de l'ONU (« sur les principes régissant les activités des États en matière d'exploration et d'utilisation de l'espace extra-atmosphérique, y compris la Lune et les autres corps célestes »), proscrit entre autres les armes de destruction massive en orbite. Cependant, il n'interdit pas la militarisation de l'espace, ni la légitime défense et il ne définit pas ce que signifie un **usage pacifique de l'espace.**

À l'ONU et à la Conférence du désarmement, Chine et Russie proposent le non-déploiement d'armes dans l'espace. En particulier, la Russie s'est officiellement prononcée, par la voix de son ministre des Affaires étrangères Sergueï Lavrov[6], pour un accord international juridiquement contraignant contre le déploiement d'armes dans l'espace, mais les États-Unis refusent car un tel traité n'inclurait pas les armes antisatellites au sol de ses rivaux. Dans ces conditions, on assiste actuellement à une véritable « arsenalisation » de l'espace.

En même temps, des discussions lancées par l'Union européenne sont en cours entre les États-Unis, la Grande-Bretagne, le Canada, l'Australie, la Nouvelle-Zélande et l'Allemagne pour établir un **code de bonne conduite** visant à définir des normes de comportement responsable. C'est l'action la plus susceptible d'apporter des réponses crédibles et réalistes aux dangers que peut représenter une éventuelle « guerre de l'espace »

5.3 Les risques

Dans ce nouvel environnement stratégique et technologique, tous les États, compte tenu de leur dépendance des systèmes spatiaux et de la vulnérabilité de ceux-ci, mais aussi de la possibilité d'acquérir la suprématie dans le cadre d'une rivalité géopolitique, développent des **armes défensives et offensives** qui font de l'espace un nouveau champ conflictuel et la source de menaces existentielles.

[6] Déclaration du 12 avril 2021 à l'occasion du soixantième anniversaire du vol de Youri Gagarine.

La Russie et la Chine ont très vite saisi toute l'importance de cet enjeu pour rétablir un équilibre stratégique avec les États- Unis et plus encore pour la Chine qui, en se dotant, d'une puissante industrie spatiale, menace directement l'hégémonie américaine.

5.3.1 Armes offensives

La Chine développe et teste depuis le début des années 2000 un arsenal important d'**armes antisatellites** :

- Des **capacités cinétiques** antisatellites (ASAT) par missiles depuis la surface ou les airs, avec l'inconvénient qu'un tir cinétique contre un satellite en orbite basse provoque des milliers de débris (actuellement 90 % des objets dans l'espace proche sont des débris) ;
- Des **armes à énergie dirigée** incluant des lasers basés à terre, des missiles antisatellites et des robots orbitaux antisatellites ;
- Des **satellites brouilleurs** de communications et de signaux GPS,
- Des **satellites espions** et des moyens électroniques et cyber visant à mettre hors service les systèmes spatiaux adverses.

La Chine prépare également le lancement d'un premier **robot de minage** de l'espace. Mais la Chine n'a pas le monopole des systèmes offensifs : les **États-Unis** et tous les États « spatiaux » comme l'**Inde** et le **Japon** par exemple, se dotent également de missiles antisatellites et de moyens de destruction ou de neutralisation des constellations de satellites dont dépendent la plupart des États dans le monde.

5.3.2 Armes défensives

Il s'agit de développer une « défense active » pour assurer la préservation des moyens spatiaux » de communication, de navigation, d'observation, de renseignement et de ciblage. Le rôle de l'espace va devenir encore plus vital au moment où tous les systèmes de combat seront mis en réseau et où l'espace jouera un rôle essentiel pour la collecte et la distribution de l'information en temps réel.

Ainsi **les États-Unis** développent le projet de la mise en orbite progressive d'une constellation de plusieurs centaines de satellites dont le rôle sera de détecter et transmettre pour ciblage, de manière « instantanée », toutes les informations concernant une menace de quelque nature que ce soit et en même temps de renforcer la résilience de leurs satellites en

cas d'attaques antisatellites. Ce projet a pour conséquence d'instaurer un état de guerre instantanée qui ne peut que favoriser la mise en œuvre de systèmes d'armes autonomes.

S'agissant de **la France**, le comportement en 2017 du satellite russe *Luch-Olymp* s'approchant un peu trop près du satellite de communications militaires franco-italien *Athena-Fidus* a été à l'origine d'une prise de conscience de la vulnérabilité de nos capacités spatiales. C'est pourquoi la France a entrepris le développement d'un système spatial *Yoda* (des Yeux en Orbite pour un Démonstrateur Agile), une sorte de satellite patrouilleur chargé de veiller sur les satellites militaires français et un système précurseur de l'arrivée de nanosatellites brouilleurs.

L'espace est aussi un lieu de transit des nouveaux missiles hypervéloces, des missiles intercontinentaux.

5.4 Impact sur la « *dissuasion nucléaire* »

Cette révolution en cours, la révolution du « New Space », ouvre un nouveau champ de compétition géopolitique dans le cadre d'une stratégie de puissance qui n'est plus dorénavant l'apanage des seules grandes puissances traditionnelles.

Le développement technologique accéléré des systèmes spatiaux offre de nouveaux horizons en matière de circulation et de traitement des données mais simultanément il accroît la vulnérabilité de ces systèmes. La stratégie de la terreur nucléaire, c'est-à-dire la « dissuasion nucléaire », dont la crédibilité repose maintenant en grande partie sur les satellites pour ses moyens de commandement et de contrôle, ses moyens d'observation et de navigation notamment, devient à la fois inutile et vulnérable donc dangereuse.

Cette vulnérabilité conceptuelle et opérationnelle tient à plusieurs facteurs :

- Tout d'abord la **dualité civile-militaire et public-privé**, inhérente au milieu spatial. Celui-ci est à la fois un enjeu commercial et un enjeu militaire ; de plus, les briques technologiques utilisées sont à usage dual. Ainsi les dimensions civiles et militaires ne sont pas toujours séparées. Cette imbrication du civil et du militaire du public et du privé provoque sur ce marché, qui devient aussi un espace de confrontation, l'émergence incontrôlée de **nouveaux acteurs** étatiques et privés.

– Cette nouvelle dimension qu'est dorénavant l'espace devient une dimension « grise » où il devient très **difficile d'attribuer des actions inamicales ou hostiles** conduites dans l'espace et d'élaborer une riposte proportionnée. Or la stratégie nucléaire est incompatible avec cette incertitude sur la connaissance claire de l'adversaire. Elle ne peut pas s'exercer dans ce « brouillard » spatial. Elle devient inutile.

– **La dépendance de la stratégie nucléaire** au rôle croissant de l'espace dans la circulation et le traitement des données pour ses réseaux de commandement et ses capacités de renseignement et d'observation indispensables à l'exécution des frappes **la rend extrêmement vulnérable** soit à une neutralisation de ses systèmes spatiaux la rendant inopérante soit à une autonomisation de tir ou à un tir préemptif par crainte d'une attaque sur ses satellites devenus très vulnérables.

– Le lancement de milliers de satellites et d'essaims de nanosatellites et leur rôle croissant dans la conduite des opérations militaires où la vélocité et l'immédiateté deviennent des facteurs déterminants, donnent naissance au **concept de « guerre instantanée** », c'est-à-dire la capacité de déclencher une guerre sans aucun préavis ni signal faible d'alerte. Cette guerre instantanée peut être un substitut à la politique de terreur nucléaire qu'est la dissuasion, mais elle peut être aussi provoquer une attaque nucléaire instantanée.

5.5 Conclusion

L'espace est désormais un milieu de manœuvre et de confrontation, un facteur structurant de puissance. Il est devenu un véritable domaine de confrontation stratégique. Plus généralement, il est un domaine indispensable à l'ensemble des activités humaines. Aussi, une neutralisation sous une forme ou une autre, sélective ou non, des systèmes spatiaux aurait des conséquences dramatiques pour une partie ou l'ensemble de l'humanité sans que pour autant l'origine d'un acte hostile puisse être clairement identifiée. C'est dire l'importance de la stratégie spatiale qui sape les fondements de toute stratégie nucléaire et rend celle-ci obsolète et inutile.

Cependant, dans le même temps, la stratégie spatiale offre à la stratégie nucléaire la possibilité de devenir encore plus prégnante et menaçante.

Une stratégie spatiale dans le cadre d'une stratégie globale conventionnelle plaide donc pour un **abandon de la stratégie nucléaire et une élimination des armes nucléaires**.

Mais les perspectives parfois très inquiétantes ouvertes par les technologies émergentes, et notamment les technologies spatiales, plaident également pour une régulation et un contrôle de ces nouveaux systèmes d'armes à l'instar de ce qui a été fait pour le contrôle des armes de destruction massive.

5.6 Bibliographie

- « Spatial militaire et guerre instantanée », *Air et Cosmos*, 1er mai 2020.
- DUFFORT Chloé, *« Espace, armement et conflit : le droit international en orbite »,* Open Diplomacy Institute, 3 août 2020 (https://bit.ly/3xPgQ8J).
- PASCO Xavier, *« Des initiatives européennes pour la sécurité dans l'espace »,* Centre Thucydide, 2015, https://www.afri-ct.org/wp-content/uploads/2015/03/69-_Article_Pasco.pdf
- TESTE Jean-Daniel, « La militarisation de l'espace : quels enjeux pour aujourd'hui et demain ? », *Areion24.news*, 8 avril 2021 https://www.areion24.news/2021/04/08/la-militarisation-de-lespace-quels-enjeux-pour-aujourdhui-et-demain/

6. L'INTELLIGENCE ARTIFICIELLE

Bernard Norlain

Résumé : L'intelligence artificielle (IA) ouvre des perspectives révolutionnaires dans tous les champs de l'activité humaine. Mais si elle est un multiplicateur de progrès, elle est aussi un multiplicateur de force. De ce fait elle devient un enjeu de défense prioritaire pour les puissances du XXIe siècle. Par essence duale, l'IA favorise la fusion du civil et du militaire et l'apparition de nouveaux acteurs et de nouveaux usages. Elle joue un rôle essentiel dans la lutte informationnelle et permet une robotisation et une autonomisation des décisions et des processus. Ses impacts sur la stratégie nucléaire sont donc systémiques à la fois parce qu'elle rend cette stratégie obsolète, mais aussi parce qu'elle accroît le risque du déclenchement d'un conflit nucléaire. Au-delà, l'IA et ses applications constituent une véritable révolution pour la conduite et la maîtrise des conflits à venir. Facteur déterminant de supériorité, elle est un véritable défi à la stabilité stratégique.

Représentation artistique des applications militaires de l'IA.
Source : K_E_N / Shutterstock

Vladimir Poutine : « *Celui qui deviendra leader en ce domaine sera le maître du monde.* »

6.1 L'intelligence artificielle : une rupture stratégique

Définir l'intelligence artificielle se révèle une tâche difficile tant le sujet est complexe et multiforme. Schématiquement, l'intelligence artificielle vise à reproduire le cerveau humain. Elle désigne alors un programme autour d'un objectif ambitieux : comprendre comment fonctionne le cerveau humain et le reproduire, c'est-à-dire créer des processus cognitifs comparables à ceux de l'être humain. Le champ est donc extrêmement vaste tant en ce qui concerne les procédures techniques utilisées que les disciplines convoquées : mathématiques, informatiques, sciences cognitives.

Plus concrètement, l'intelligence artificielle (IA) résulte de la convergence entre des algorithmes, la disponibilité de données en grand nombre et les progrès de l'accessibilité des capacités de calcul. C'est le résultat de la convergence calcul-données-algorithmes. L'IA reproduit les processus cognitifs au moyen d'algorithmes et de traitement automatisé du « Big Data » Son développement actuel est dû à l'essor de l'apprentissage automatique (*machine learning*).

Le Commissariat à l'énergie atomique et aux énergies alternatives (CEA), pour sa part, complète cette définition en précisant que l'IA est *« un ensemble d'algorithmes conférant à une machine les capacités d'analyse et de décision lui permettant de s'adapter intelligemment aux situations en faisant des prédictions à partir de données déjà acquises* ». Et Stuart Russel, professeur en IA, ajoute que l'IA est « *l'étude des méthodes permettant aux ordinateurs de se comporter intelligemment* ». Le mot « intelligence » mériterait à ce stade d'être lui aussi précisé, mais la définition lapidaire de Yann Le Cun (« *la capacité à prédire constitue l'essence même de l'intelligence* ») suffit à le caractériser.

Il s'agit alors de produire des machines intelligentes, ce qui ouvre des perspectives révolutionnaires à la fois aux plans scientifique, technologique, sociétal et humain. Ainsi, depuis plusieurs années, de très nombreuses publications s'attachent à décrire les perspectives révolutionnaires qu'ouvre l'intelligence artificielle et si, selon Elon Musk, l'IA est plus dangereuse que l'arme nucléaire, d'autres sont plus optimistes, estimant que les opportunités l'emportent sur les risques. Pour ceux-là, l'IA est l'outil le plus puissant qui puisse bénéficier à

l'humanité et tous s'accordent pour dire que l'IA dans toutes ses applications va bouleverser nos modes de vie. On pourrait reprendre à cet égard la phrase de Thomas Edison à propos de l'électricité : « *c'est le champ des champs. Elle contient les secrets qui vont réorganiser la vie du monde* ».

Mais si, en paraphrasant le mot d'Artur Rimbaud, l'IA constitue « un multiplicateur de progrès », elle devient en même temps un « multiplicateur de force » et de ce fait jouera un rôle considérable dans les conflits futurs. Les technologies d'IA combinées aux progrès de la robotique, des biotechnologies, de l'informatique, révolutionnent de nombreux domaines, à commencer par celui de la défense. La palette des applications de l'IA dans la défense est extrêmement large, des applications de gestion aux systèmes de combat autonomes. Elle permet de traiter, dans le domaine de la défense et de la sécurité, des masses de données pour des fonctions de protection, d'observation et d'analyse, mais elle permet aussi une automatisation de la prise de décision, y compris pour le ciblage et l'usage létal.

Le champ d'application est donc vaste. Il va des fausses informations (*deep fakes*) aux drones létaux. Selon le rapport de l'OTAN sur les tendances technologiques 2020-2040, « *l'utilisation de l'IA intégrée dans d'autres technologies associées telles que la réalité virtuelle ou augmentée, l'informatique quantique, l'autonomie, la modélisation et la simulation, l'espace, la recherche sur les matériaux, la logistique, l'analyse des données, aura des effets transformateurs sur les technologies nucléaires, aérospatiales, cybernétiques, les matériaux et les biotechnologies* ».

Le rapport poursuit en affirmant que ces transformations seront du même ordre que « l'introduction des armes nucléaires ». **L'IA se pose désormais en concurrent des technologies nucléaires et, paradoxalement, si elle rend la dissuasion nucléaire de plus en plus inutile, elle la rend de plus en plus dangereuse**.

Dans notre monde numérique, l'IA va accélérer la rupture numérique. Elle sera donc l'une des clés du monde à venir, génératrice de ruptures technologiques et de ruptures stratégiques. Les doctrines militaires subiront de profondes mutations provoquées par la montée en puissance de l'IA. À moyen terme, tous les espaces militaires seront investis par des unités robotisées plus ou moins autonomes.

Ainsi l'IA devient un **enjeu de défense prioritaire pour les puissances militaires** du XXI^{e} siècle. Mais plus encore, elle provoque une transformation des dynamiques politico-

militaires et un **changement dans la nature même de la guerre**. Elle prend ainsi une importance géostratégique. En permettant l'émergence de nouvelles technologies à l'origine d'armes déstabilisantes, elle constitue un véritable défi à la stabilité stratégique.

6.2 Les domaines de l'intelligence artificielle

L'IA irrigue les très nombreuses technologies émergentes qui sont en train de révolutionner l'art de la guerre. Ces applications technologiques de l'IA, encore immatures pour beaucoup, mais dont le développement est caractérisé par sa vitesse, présentent des aspects communs qui peuvent être regroupées autour de trois grands pôles.

6.2.1 Dualité civil/militaire-public/privé :

Actuellement, dans le domaine des technologies de défense, l'une des grandes nouveautés réside dans le fait que la composante civile tire la composante militaire ; l'intelligence artificielle issue de la convergence calcul-algorithmes-données en est le meilleur exemple. Les briques technologiques nécessaires à la constitution d'armes ne relèvent plus du domaine militaire mais du domaine civil. On assiste ainsi à une véritable fusion civilo-militaire. Les conséquences en sont :

- Une **diversité public-privé des acteurs**, en particulier dans le domaine de la recherche. Les Google-Apple-Facebook-Amazon-Microsoft (GAFAM) et Baidu-Alibaba-Tencent-Xiaomi (BATX) investissent des dizaines de milliards de dollars dans la recherche pour l'IA. Mais aussi une multiplication des acteurs, étatiques, non-étatiques, car tout acteur initié à l'IA peut créer des armes autonomes. Cette diversité des acteurs provoque mécaniquement une prolifération des technologies de défense ;

- Une **diversité des usages**, car les applications civiles sont transposables dans le domaine militaire. De plus, les nouveaux systèmes d'armes comme les missiles hypervéloces, les planeurs hypersoniques qui peuvent emporter des têtes nucléaires ou conventionnelles et sont donc des armes duales, augmentent le risque d'un tir préemptif nucléaire afin de garantir la capacité de riposte sur laquelle repose toute dissuasion nucléaire.

En définitive, cette dualité qui comporte trois facettes (public/privé-civil/militaire-conventionnel/nucléaire) contribue à créer un vaste espace conflictuel où les frontières,

qu'elles soient technologiques, sociétales ou étatiques, se dissolvent et augmentent le « *brouillard de la guerre* ».

6.2.2 La lutte informationnelle : la guerre de l'information

La révolution numérique nous a fait entrer dans le monde de l'information et l'IA est la science du traitement de l'information. L'information dans un espace numérique devient la valeur essentielle et son traitement par l'IA permet toutes les applications et manipulations. Création de fausses informations, de visages fictifs mais réalistes, transformation à la volée d'une voix par une autre, sont quelques-unes des applications qui témoignent de la guerre de l'information dans laquelle le monde est plongé et pour laquelle l'IA joue un rôle primordial. L'observation, le renseignement, le commandement et le contrôle des opérations de combat, qui ont pour objet de recueillir et d'analyser l'information, deviennent un champ d'application majeur de l'IA et conduit notamment à l'élaboration de stratégies de combat numérique temps réel. Le cyber espace, dans ses aspects offensifs et défensifs, est un domaine immense où l'IA peut se développer et apporter de nouvelles opportunités : virus informatiques polyformes, automatisation des cyberattaques, brouillage des satellites, usurpation de données de satellite, etc. Conjuguée, en particulier, à la physique quantique, l'**IA empêchera que tout système de cryptologie soit inviolable**. En revanche, l'IA, système numérique, sera susceptible d'être attaquée par d'autres systèmes numériques.

6.2.3 Robotisation-autonomisation des décisions et des processus

Incontestablement, la question de l'autonomie, qui est au cœur de l'IA, est la plus emblématique de ses capacités et de ses enjeux. Si l'autonomie, dans son acception littérale, c'est-à-dire la reproduction du cerveau, reste encore du domaine de l'utopie et de la science-fiction, il existe un continuum entre ce qui est autonome et ce qui ne l'est pas et donc des degrés divers de l'autonomie, des échelles de l'autonomie. Grâce à l'apprentissage profond, les algorithmes ouvrent des perspectives révolutionnaires comme la robotisation du champ de bataille et donc l'éloignement de l'homme du risque létal, mais en même temps soulèvent des questions légales, éthiques et stratégiques concernant l'usage autonome de la force létale. Dans ce domaine, ce sont les **systèmes d'armes létales autonomes** (SALA ou LAWS en anglais) qui portent la charge symbolique la plus forte. Les États développent des SALA qui, une fois activés, peuvent choisir leurs cibles, les traquer et utiliser la violence sans supervision humaine. Ils sont considérés comme les facteurs d'une rupture militaire en étant des

multiplicateurs de force : un petit nombre de contrôleurs humains opérant des essaims d'armes, de drones dans tous les milieux. Le développement des SALA dans un contexte d'accélération de la course aux armements internationale a pour conséquences :

- Un abaissement du seuil des conflits armés résultant de l'augmentation de robots diminuant le risque de pertes humaines et donc l'inhibition au conflit ;
- Une prolifération incontrôlable des SALA ;
- Un affrontement de systèmes automatisés conduisant à des déclenchements non souhaités de conflits ;
- Une automatisation dans la prise de décision, particulièrement de l'engagement nucléaire, compte tenu de l'immédiateté des décisions à prendre dans le cas par exemple de l'utilisation de missiles hypersoniques ;
- Une autonomisation complète de l'utilisation de la force létale ;
- Une violation facilitée du droit international humanitaire, qui exige notamment la distinction entre cibles militaires autorisées et cibles civiles ou non-combattantes interdites et prévoit la responsabilité pénale ou disciplinaire des auteurs de frappes illégales.

En définitive, l'autonomie qu'apporte l'IA conduit peu ou prou à l'exclusion de l'homme de la boucle de décision. Cette évolution dangereuse est inhérente au développement des technologies émergentes orchestrées par l'IA. Le meilleur opérateur humain ne peut rien dans un conflit l'opposant à de multiples machines effectuant des milliers de calculs et de manœuvres par seconde.

6.3 Impacts de l'IA sur la « dissuasion nucléaire »

Ce passage en revue rapide et non exhaustif des applications de l'IA conduit inévitablement à questionner le concept de « dissuasion nucléaire » dans ce nouveau cadre stratégique. En effet, on constate :

- Une augmentation de l'efficacité des armements conventionnels en termes notamment de précision, de robotisation, de vitesse d'exécution des opérations et des décisions, d'efficacité des missiles de défense, qui permet de disposer d'une dissuasion conventionnelle crédible ;

- Une dualité qui augmente le « brouillard de la guerre », difficilement compatible avec la clarté qu'exigent l'arme nucléaire et la dissuasion nucléaire ;

- Un risque d'automatisation de la décision d'engagement nucléaire ;

- Une dualité conventionnelle-nucléaire des nouveaux systèmes d'armes dont les performances peuvent provoquer une frappe nucléaire préemptive dans l'incertitude d'une capacité de deuxième frappe ;

- Une relance de la course aux armements nucléaires afin de restaurer cette capacité de deuxième frappe ;

- Une grande vulnérabilité aux cyber attaques des systèmes de commandement et contrôle des armes nucléaires ;

- Une diminution de la prévisibilité de la capacité d'analyse de la menace et donc une vulnérabilité de la « dissuasion nucléaire », mais en même temps un risque de tir préemptif ;

- Une prolifération nucléaire relancée et

- Une désinhibition à l'usage de l'arme atomique, donc un abaissement du seuil d'emploi nucléaire.

Paradoxalement, les conséquences de l'impact des applications de l'IA sur la « dissuasion nucléaire » conduisent à un constat de contournement conventionnel de celle-ci et donc à son inutilité, mais en même temps au constat d'une augmentation du risque de conflit nucléaire provoqué par une course aux armements internationale, l'apparition d'acteurs non-étatiques, une automatisation des systèmes, une vulnérabilité nouvelle des systèmes d'armes nucléaires et un risque de mauvaise interprétation et de mauvaise perception de la menace.

Ce constat plaiderait alors pour l'abandon de la « dissuasion nucléaire » ou à défaut par l'instauration d'une dissuasion globale faite d'une « dissuasion nucléaire » minimale et d'une forte dissuasion conventionnelle. Cependant, l'émergence de ces technologies rendues disruptives par l'IA pose, au-delà de la remise en cause de l'arme nucléaire, la question d'une stabilité stratégique à réinventer, qui prenne en compte les nouvelles perspectives souvent inquiétantes ouvertes par ces développements scientifiques.

6.4 La guerre du futur

L'IA et ses applications dans les nouvelles technologies, si elles dessinent un nouveau paysage stratégique dans lequel l'arme nucléaire se trouve dévalorisée, pour ne pas dire rendue obsolète, n'en prépare pas moins un monde où les domaines de conflictualité seront non seulement étendus en termes quantitatifs avec le cyberespace et l'espace exo-atmosphérique et d'autres encore à venir, mais aussi étendus en termes qualitatifs par les nouvelles possibilités offertes par ces disciplines scientifiques parfois naissantes. À cette extension du domaine de la lutte s'ajoute une dimension temporelle qui fait de l'accélération du rythme des développements technologiques, de la vitesse sous toutes ses facettes, le maître du temps de la réorganisation stratégique.

Dans ces conditions, la prospective devient difficile voire impossible et la mise en place de systèmes de régulation – dont on pressent déjà l'absolue nécessité – un exercice improbable. Néanmoins, on peut, à partir des connaissances déjà acquises, présenter quelques caractéristiques de ce nouveau monde conflictuel :

- Un **effacement des frontières** : paix-guerre, civil-militaire, public-privé, conventionnel-nucléaire, ami-ennemi, réel-virtuel, intérieur-extérieur. L'espace conflictuel devient un espace flou où le conflit est partout et nulle part. C'est un monde nouveau sur lequel les classifications, les concepts anciens n'ont plus de prise. La stabilité stratégique, la sécurité internationale doivent être repensées de façon globale ;

- Une **présence de plus en plus forte des machines intelligentes et des réseaux neuronaux** : l'être humain, en attendant qu'il devienne un objet non-identifié, est éloigné de l'action et de la décision, pour le bien et pour le mal, tout l'enjeu étant de lui préserver son rôle de contrôle et de décideur ultime ;

- Un **pouvoir égalisateur des nouvelles technologies** : avec pour conséquence une augmentation du nombre d'acteurs étatiques et non-étatiques, donc un monde encore plus complexe, interconnecté et interdépendant ;

- Une **révolution de l'information sous toutes ses formes** : fausse, vraie, réelle, virtuelle, augmentée, qui en fait un enjeu stratégique majeur ;

- Un « **brouillard de la guerre » qui réduit considérablement le champ d'action du concept de coercition**, de l'usage de la force brute et particulièrement de la force nucléaire.

6.5 Conclusion

L'IA constitue une véritable révolution pour la conduite et la maîtrise des conflits à venir. Elle est un facteur déterminant de supériorité et un véritable défi à la stabilité stratégique. La combinaison des nouvelles technologies et de l'IA a pour première conséquence paradoxale de **rendre obsolète l'arme nucléaire, mais en même temps d'accroître le risque de déclenchement d'un conflit nucléaire**. Cette nouvelle situation plaide, dans un premier temps, pour un rééquilibrage entre « dissuasion nucléaire » et dissuasion conventionnelle, une dissuasion nucléaire minimale et une dissuasion conventionnelle s'appuyant sur des technologies disruptives. Cependant, ce nouvel équilibre stratégique pose des questions de maîtrise afin qu'une course aux armements incontrôlée ne se déclenche pas et qu'une instabilité stratégique ne se crée pas dans la durée.

6.6 Bibliographie

- CHAMAYOU, Grégoire, *Théorie du drone*, Ed. La Fabrique, avril 2013.
- ERÄSTÖ, Tytti, *New technologies and Nuclear Disarmament: Outlining a Way Forward*, SIPRI, mai 2021, https://www.sipri.org/sites/default/files/202105/2105_new_technologies_and_nuclear_disarmament_0.pdf
- FAVARO, Marina, *Weapons of mass distortion: A new approach to emerging technologies, risk reduction, and the global nuclear order*, Centre for Science and Security Studies, King's College London, 2021.
- FUTTER, Andrew, *Explaining the nuclear challenges posed by emerging and disruptive technology: a primer for European policymakers and professionals*, EU Non-Proliferation and Disarmament Consortium, mars 2021, https://www.nonproliferation.eu/wp-content/uploads/2021/03/EUNPDC_no-73_FINAL-1.pdf

– KUBIAK Katarzyna et al., « New technologies, complexity, nuclear decision making and arms control : Workshop Report », European Leadership Network, 22-23 mars 2021, https://www.europeanleadershipnetwork.org/report/new-technologies-complexity-nuclear-decision-making-and-arms-control-workshop-report/

– LE CUN, Yann, *Quand la machine apprend*, Ed. Odile Jacob, octobre 2019.

– USA, NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE, *Final Report*, 2021, https://www.nscai.gov/2021-final-report/

– NOËL, Jean-Christophe, « Intelligence artificielle : vers une nouvelle révolution militaire ? », *Focus stratégique (Etudes de l'IFRI)*, n°84, octobre 2018, https://www.ifri.org/fr/publications/etudes-de-lifri/focus-strategique/intelligence-artificielle-vers-une-nouvelle

– « L'intelligence artificielle et ses enjeux pour la défense », *Revue Défense Nationale*, n° 820, mai 2019, https://www.defnat.com/sommaires/sommaire.php?cidrevue=820

– PATIRANA, P, « What is Artificial Intelligence? », *Medium.com*, 6 août 2021, https://medium.com/@primeshs.17

– RUSSEL, STUART, NORVIG, PETER, *Intelligence Artificielle*, Pearson France, 2010.

– SHARKEY, Noel, « Algorithms delegated with life and death decisions », *Revue Défense Nationale*, n°820, mai 2019, https://www.cairn.info/revue-defense-nationale-2019-5-page-173.htm?contenu=resume

– UK CABINET OFFICE, *Global Britain in a Competitive Age - The Integrated Review of Security, Defence Development and Foreign Policy*, 2021, https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy

– VILLANI, Cédric, *Donner un sens à l'intelligence artificielle : Pour une stratégie nationale et européenne*, Rapport de mission parlementaire, 2017-2018, https://www.vie-publique.fr/rapport/37225-donner-un-sens-lintelligence-artificielle-pour-une-strategie-nation

7. LES BIOTECHNOLOGIES

Pablo Chaillat

Résumé : Cela fait plus de quarante ans que les États tentent de réguler l'application militaire des processus biologiques. Si les armes biologiques sont restées pendant longtemps inutilisables ou inaccessibles, les innovations technologiques actuelles renforcent significativement l'applicabilité de la biologie au contexte de guerre. Les biotechnologies ont le potentiel de façonner le visage de la guerre moderne, en la rendant moins visible, plus diffuse et plus destructrice. Une prise en compte collective de ces nouveaux dangers s'impose.

Les armes biologiques sont considérées comme des armes de destruction massive au même titre que les armes nucléaires et les armes chimiques
Source : Fastfission

7.1 Définitions et cadrage

La biotechnologie est un domaine des sciences dont le but est la manipulation des processus biologiques par la technologie à des fins industrielles ou médicales. Les progrès scientifiques des dernières décennies ont permis un développement majeur de notre compréhension des systèmes génétiques et biologiques, tout en rendant plus aisée leur manipulation. La technique CRISPR (pour *Clustered Regularly Interspaced Short Palindromic Repeats*), dite des « ciseaux moléculaires », rend ainsi possible la modification facile et rapide des génomes des cellules animales ou végétales. Ces développements scientifiques sont très prometteurs sur le plan médical ou industriel, par une prévention et un traitement des maladies beaucoup plus efficaces, mais soulèvent aussi des questions éthiques.

Par ailleurs, **les techniques de manipulation génétique présentent des risques d'application militaire**. Un pathogène porteur de maladie peut ainsi être modifié pour augmenter sa virulence, sa contagiosité ou encore sa résistance aux vaccins et autres interventions thérapeutiques. De même, les progrès scientifiques rendent théoriquement possible la création d'une arme biologique nouvelle et destructrice, au travers par exemple :

- Du développement de pathogènes de synthèse (en laboratoire) déjà éteints ou entièrement nouveaux ;
- De la modification du système immunitaire, du système nerveux, du génome ou du microbiome (gènes du microbiote) ;
- De l'utilisation du système de guidage génétique (gene drive en anglais) afin de disséminer rapidement et économiquement des gènes nocifs via les animaux ou les plantes ;
- De la dissémination de pathogènes et de systèmes biologiques par de nouveaux moyens.

Les principales tendances de la biotechnologie et leurs implications pour la sécurité

Tendances clés de la biotechnologie :

- Des investissements substantiels sont nécessaires, mais une fois les découvertes effectuées, elles peuvent être reproduites presque immédiatement et à coût réduit ;
- L'accès est facilité aux connaissances, aux instruments et aux composants nécessaires à la création d'organismes vivants ;
- Des amateurs, des scientifiques autodidactes et d'autres nouveaux acteurs pénètrent le champ des biosciences ;
- La « boîte à outils » nécessaire à la manipulation des gènes et des organismes (p. ex. CRISPR) évolue rapidement ;
- On assiste à une convergence entre la biologie et les autres sciences et technologies (chimie, ingénierie, informatique) ;
- Les expériences, la production et les données biologiques sont de plus en plus numérisées et automatisées.

Implications pour la sécurité

- De nouvelles armes biologiques ;
- Possibilité accrue d'un détournement de la science pour un nombre plus élevé d'acteurs ;
- Potentiel accru de détournement de la science à cause de la convergence avec les technologies émergentes ;
- Espace potentiel d'attaque et vulnérabilités accrus susceptibles d'être exploités pour causer des dommages* ;
- Zone grise élargie entre activités défensives licites et activités offensives illicites ;
- Difficulté accrue de détecter et d'attribuer une attaque par armes biologiques.

* J. Kirkpatrick et al., Editing Biosecurity: Needs and Strategies for Governing Genome Editing, Institute for Philosophy and Policy et al., décembre 2018

Source : F. Lentzos, « 2019. Capturing Technology. Rethinking Arms Control », Conférence, Berlin, 15 mars 2019.

Cependant, les progrès scientifiques en matière de biologie et de manipulation du tissu génétique sont difficilement transmutables dans le domaine militaire en eux-mêmes. Aussi, **la révolution fondamentale en matière d'application militaire des biotechnologies réside dans le croisement des progrès scientifiques en biologie et des développements technologiques les plus récents dans des domaines connexes**. Les innovations technologiques dans l'intelligence artificielle (IA), la (nano)robotique et l'impression 3D (ou fabrication additive), entre autres, permettent en effet d'augmenter significativement l'**applicabilité** des techniques de manipulation génétique et des organismes au contexte de guerre, c'est-à-dire à aux **impératifs de prévisibilité d'une arme et de ses effets sur l'adversaire et plus largement sur le rapport de force.**

7.2 L'arme biologique : un développement compliqué suivi d'une prohibition internationale

Historiquement, l'utilisation des armes biologiques s'est confrontée à trois obstacles majeurs :

- Premièrement, à la difficulté de contrôler les effets de la contagion biologique et donc au risque d'un **effet boomerang** ;
- Deuxièmement, à l'**absence** de **précision et à l'immédiateté** de ces armes, la dispersion et dissémination des pathogènes par l'air étant très dépendantes des conditions météorologiques d'une part, et la contamination par le pathogène prenant souvent plusieurs jours et étant assez aléatoire d'autre part ;
- Finalement, à la découverte potentielle d'un **antidote ou vaccin** par l'adversaire qui annulerait les effets de l'attaque (biodéfense).

Confrontés à ces difficultés, la quasi-totalité des États ont fait le choix (officiellement) de renoncer à développer une arme biologique, décision qui a été actée par l'entrée en vigueur en 1975 de la Convention sur l'interdiction de la mise au point, de la fabrication et du stockage des armes bactériologiques (biologiques) ou à toxines et sur leur destruction ou **Convention sur l'interdiction des armes biologiques** (CIAB) ou *Biological Weapons Convention* (BWC) en anglais, qui **rend illégales les armes biologiques**.

Définir une arme biologique

En général, une arme biologique consiste en un agent biologique militarisé et en un vecteur. Transformer un agent, c'est-à-dire le sélectionner, le concevoir, le développer et le manipuler à des fins spécifiques, principalement militaires est différent du simple emploi de matières biologiques, y compris des pathogènes ou des agents toxiques à des fins hostiles*. La transformation d'un agent en arme cherche à garantir l'efficacité d'une arme biologique grâce à l'obtention d'un pathogène adéquat capable d'infecter la cible et provoquer une maladie ou la mort par dissémination sans être affecté par les conditions environnementales ou considérablement atténué par un traitement médical ou des mesures défensives.

Le vecteur d'une arme biologique est un système qui facilite une dissémination et une dispersion adéquate de l'agent de telle sorte qu'il rende la cible vulnérable à ses effets. Des exemples de dissémination incluent le recours à un réservoir de pulvérisation sur un aéronef pour rendre une zone inaccessible, l'injection d'un agent dans une capsule ou une pastille ou l'emploi manuel d'un aérosol pour assassinat ciblé. Dans le cas de la dispersion par aérosol, l'efficacité dépend de la dimension adéquate des particules de l'agent pour son absorption par le système respiratoire de la cible.

Il est souvent plus utile d'examiner les capacités en matière d'armes biologiques – c'est-à-dire si un État est capable de menacer ou de lancer une attaque biologique – que de connaître la possession effective ou les stocks de telles armes**. Il est crucial de distinguer entre un acteur possédant des armes biologiques et un acteur ayant accès à des technologies militaires permettant de développer un programme d'armes biologiques pour effectuer une analyse de risque et déployer des efforts de contrôle. Ces capacités peuvent être obtenues non seulement par la mise en œuvre d'un programme militaire offensif, mais aussi par des activités licites de défense, de recherche en sciences de la vie et la mise au point industrielle ou la formulation d'agents biologiques : les processus et les connaissances requis pour de telles activités sont souvent difficiles à distinguer.

* J.-P. Zanders, « Assessing the risk of chemical and biological weapons proliferation to terrorists », *Nonproliferation Review*, vol. 6, no. 4 (automne 1999), pp. 17-34, pp. 18-19.

** E. Bohm et F. Lentzos, « Technical briefing note on developments in science and technology and governance in relation to biological weapons », *document de travail*, SIPRI, novembre 2018.

7.3 Au croisement des nouvelles technologies et de la biologie

Comme le soulignent de nombreux rapports cités dans cette synthèse [7], les développements technologiques récents rendent beaucoup plus aisée et prévisible la manipulation des processus biologiques à des fins militaires ou terroristes, fragilisant par là-même le consensus sur l'interdiction des armes biologiques. Surtout, les développements dans les domaines de l'impression 3D, de l'IA ou de la robotique rendent plus floue la frontière entre applications militaires et applications civiles – autrement dit, **ces technologies sont intrinsèquement duales et donc plus difficiles à contrôler.**

7.3.1 L'impression 3D (additive manufacturing) et la biologie

L'impression 3D peut servir par exemple à construire sur demande des outils médicaux souvent nécessaires sur les terrains militaires, ce qui est plutôt positif, mais elle risque aussi de faciliter la prolifération d'armes de destruction massive, en permettant de contourner les contrôles à l'exportation opérés par les États sur certains produits sensibles. Ainsi, **l'usage de l'impression 3D pour la fabrication de drones armés pourrait renforcer les capacités de certains groupes non-étatiques à lancer une attaque biologique par les airs, avec précision et discrétion**. De plus, la numérisation des techniques d'impression 3D les rend vulnérables aux cyberattaques et donc au vol de données sensibles. En même temps, l'impression en 3D de pièces militaires souvent hautement sophistiquées requiert un niveau d'expertise qui est hors de portée de la plupart des groupes non-étatiques, réduisant ainsi le risque de prolifération militaire.

7.3.2. L'intelligence artificielle et la biologie

L'IA, qui vise à rendre les robots plus « intelligents » ou « autonomes », en particulier au travers de la transmission massive de données extraites du monde réel (*machine learning* en anglais), ouvre de nouvelles perspectives d'augmentation des capacités humaines (*human enhancement* en anglais). L'utilisation du *machine learning* pour des analyses d'ADN et des prédictions génomiques pourrait ainsi permettre de mieux identifier les individus réceptifs aux

[7] Pour une étude approfondie, voir en particulier: BROCKMANN, Kolja et al., « Bio Plus X: Arms Control and the Convergence of Biology and Emerging Technologies », SIPRI, 2019

procédures d'augmentation des capacités humaines, en particulier à travers la manipulation génomique. Ces avancées sont significatives dans le domaine militaire, puisque l'IA pourrait permettre d'identifier les besoins d'un soldat à un instant T, de créer des vaccins ou médicaments personnalisés pour chaque soldat en fonction de son patrimoine génétique, ou encore d'augmenter la résistance des soldats à un pathogène spécifique, voire à une arme biologique. Cependant, les développements de l'IA sont particulièrement inquiétants pour les raisons suivantes :

- L'IA pourrait permettre de viser de façon discriminative un groupe d'individus (en fonction de certaines caractéristiques génomiques, d'exposition à un vaccin particulier, ou d'une vulnérabilité spécifique de leur système immunitaire), et ouvre donc la possibilité d'une **guerre biologique « chirurgicale » voire raciste** ;

- L'IA pourrait rendre beaucoup plus facile le développement d'**agents biologiques avancés**, en renforçant la **virulence** ou la **transmissibilité** d'un virus notamment. Cependant, ces processus demandent un niveau de sophistication scientifique élevé, ainsi qu'un laboratoire, et restent donc inaccessibles aux acteurs non-étatiques, et extrêmement complexe pour les États également ;

- L'accumulation de données qu'implique l'IA renforce la vulnérabilité de certaines données hautement sensibles aux **cyberattaques** pouvant émaner d'un État ou groupe non-étatique. Ces données pourraient ensuite être utilisées pour planifier une attaque biologique « chirurgicale ».

7.3.3 La robotique et la biologie

Au travers de l'automatisation des tâches, la robotisation permet de renforcer l'efficacité et la reproductibilité des expérimentations scientifiques, ainsi que d'augmenter la productivité en laboratoire (les robots peuvent potentiellement reproduire des expériences sans interruption). De plus, la robotisation permet aussi aux chercheurs d'effectuer des expériences à distance, en indiquant aux machines les étapes à exécuter. Si la robotique ouvre des perspectives certainement prometteuses dans un cadre médical (prévention et traitement rapide des maladies, production et livraison de vaccins, etc.), elle renferme aussi le potentiel de **rendre le développement d'armes biologiques plus facile, plus rapide et possiblement accessible à un plus grand nombre d'acteurs**. Cependant, ici encore, le degré de sophistication nécessaire pour des attaques de précision est encore hors de portée

de la plupart des groupes non-étatiques, et des avancées telles que la nanorobotique en sont encore à une phase expérimentale.

7.3.4 Bilan des risques issus de la convergence des nouvelles technologies et de la biologie

- Dans leur ensemble, les nouvelles technologies facilitent le développement ou la production d'armes biologiques ainsi que de leurs systèmes de diffusion.

- De plus, elles permettent d'augmenter significativement la précision des armes biologiques, fragilisant le consensus autour de leur non-utilisation.

- La numérisation croissante qui accompagne les nouvelles technologies augmente les risques de cyberattaques.

- La plupart des nouvelles technologies échappent au contrôle direct des gouvernements, ce qui renforce les possibilités de prolifération. Du reste, la cadence importante des innovations technologiques rend plus difficile la définition sur la durée de paramètres techniques de contrôle des exportations et de mesures de transparence.

7.4 Quelles conséquences pour la « dissuasion nucléaire » ?

Comme souligné précédemment, les effets de l'utilisation d'armes biologiques ont traditionnellement été considérés comme particulièrement aléatoires (absence de précision et immédiateté), voire contre-productifs (effet boomerang, découverte d'un antidote par l'adversaire). Dès lors, les programmes de développement d'armes biologiques ont été abandonnés dans leur immense majorité par les États, et sont restés hors de portée des groupes non-étatiques, privilégiant des méthodes plus conservatrices. Cependant, les avancées majeures de la biotechnologie ces dernières années, au croisement de la biologie et des nouvelles technologies, apportent des solutions à la plupart de ces problèmes anciens, en renforçant la capacité des acteurs à contrôler les effets d'une attaque biologique – et donc à augmenter la prévisibilité de ces armes.

Si cette « nouvelle donne » biotechnologique n'a pas nécessairement un effet direct sur les armes nucléaires, autrement qu'en **renforçant encore un peu plus la possibilité d'une « première frappe » nucléaire** en réponse à une attaque biologique, elle peut

néanmoins inciter les États à percevoir les armes biologiques comme une **nouvelle arme de dissuasion**. Les progrès de la biotechnologie rendent en effet théoriquement possible pour un État d'infecter une population de façon ciblée avec un virus dormant, lequel pourrait être activé au moment désiré. En faisant jouer l'impact psychologique qu'une telle annonce entraînerait (panique de la population dans son ensemble, chaos), un État serait ainsi en mesure d'espérer appliquer une stratégie de dissuasion crédible.

Plus généralement, **les biotechnologies ont le potentiel de façonner le visage de la guerre moderne, en la rendant moins visible, plus diffuse et plus destructrice**. Surtout, en fragilisant le contrôle des États sur les industries stratégiques, les **biotechnologies alimentent une dualité dans leur usage qui met en péril le cadre de non-prolifération ainsi que la doctrine de « dissuasion nucléaire », laquelle repose sur une identification des menaces et une stabilité du paysage interétatique**.

7.5 Conclusion

La question du contrôle et de l'interdiction des armes biologiques a traditionnellement été abordée sous un prisme biologique, et insuffisamment sous un prisme technologique. Ainsi, la plupart des traités internationaux ne sont pas à jour des évolutions technologiques récentes. De façon significative, la question de la dualité, qui est au centre des innovations technologiques et de leur croisement avec la biologie, est largement absente de la Convention d'interdiction des armes biologiques (CIAB) de 1972, laquelle se focalise sur le développement des armes elles-mêmes.

Ces lacunes sont profondément inquiétantes, car les biotechnologies ouvrent la voie à de **nouvelles formes de dissuasion, plus diffuses, qu'il importe de saisir**. Dès lors, et au regard de la complexification du paysage stratégique, ne serait-il pas sage de renoncer à la dissuasion nucléaire traditionnelle, qui apparaît obsolète ?

7.6 Bibliographie

- BEN OUARGHRAM-GORMLEY, « Gene Drives: The good, the Bad, and the Hype », *Bulletin of the Atomic Scientists*, 2016, https://thebulletin.org/2016/10/gene-drives-the-good-the-bad-and-the-hype/

- BROCKMANN, Kolja et al., *Bio Plus X: Arms Control and the Convergence of Biology and Emerging Technologies*, SIPRI, 2019 https://www.sipri.org/publications/2019/other-publications/bio-plus-x-arms-control-and-convergence-biology-and-emerging-technologies

- CROSS, Glenn, "Wrestling with imponderables: assessing perceptions of biological-weapons utility", *The Nonproliferation Review*, 2021

- FEARS, Robin, TER MEULEN, Volker « Assessing the Security Implications of Genome Editing Technology: Report of an international workshop », *Frontiers in Bioengineering and Biotechnology,* Allemagne, 2017, https://www.interacademies.org/publication/assessing-security-implications-genome-editing-technology-report-international-workshop

- FINAUD Marc et al., *Global Biosecurity: Towards a New Governance Paradigm*, Slatkine, 2008.

- GALAMAS Francisco, « Biological Weapons, Nuclear Weapons and Deterrence: The Biotechnology Revolution », *Comparative Strategy*, 27:4, 2008, p 315-323.

- GALAMAS, Francisco, « Biotechnology and Biological Weapons: Challenges to the U.S. Regional Stability Strategy », *Comparative Strategy*, 2009, 28:2, 164-169, DOI: 10.1080/01495930902799756

- GALANOPOULO, L., « Quelle éthique pour les ciseaux génétiques ? », *CNRS – Le Journal*, 2016, https://lejournal.cnrs.fr/articles/quelle-ethique-pour-les-ciseaux-genetiques

- INTERACADEMY PARTNERSHIP, *The Biological and Toxin Weapons Convention: Implications of advances in science and technology,* 2015, https://www.interacademies.org/publication/biological-and-toxin-weapons-convention-implications-advances-science-and-technology

– KOBLENTZ, Gregory D, « The De Novo Synthesis of Horsepox Virus: Implications for Biosecurity and Recommendations for Preventing the Re-emergence of Smallpox », *Journal of Health Security*, Vol. 15, no. 6, 2018, p. 620–28.

– KIRKPATRICK, Jessica et al., *Editing Biosecurity: Needs and Strategies for Governing Genome Editing*, George Mason University, 2018.

– LENTZOS, Filippa, « Ignore Bill Gates: Where Bioweapons Focus Really Belongs », *Bulletin of the Atomic Scientists*, 2017, https://thebulletin.org/2017/07/ignore-bill-gates-where-bioweapons-focus-really-belongs/

– LENTZOS, Filippa, INVERNIZZI, Cédric, « DNA Origami: unfolding risk? » *Bulletin of the Atomic Scientists*, 2018, https://thebulletin.org/2018/01/dna-origami-unfolding-risk/

– NATIONAL ACADEMIES OF SCIENCE, *Biodefense in the Age of Synthetic Biology* Washington DC, 2018.

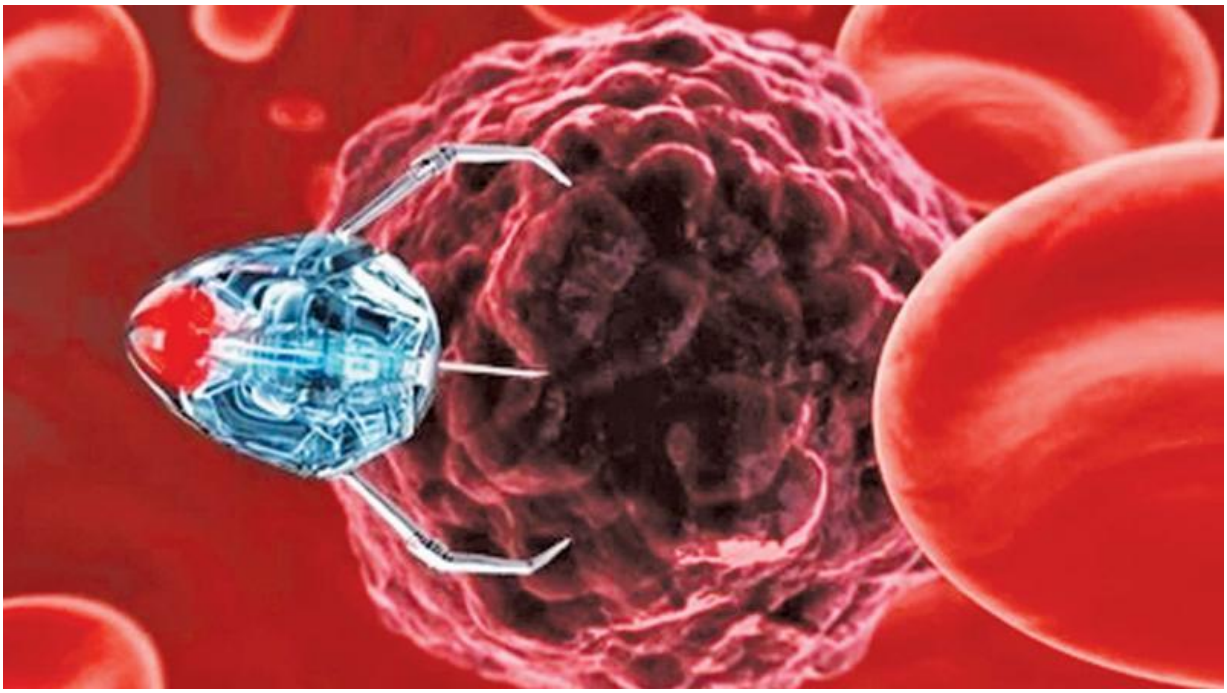
– ROYAL SOCIETY, « Trends In Synthetic Biology And Gain Of Function And Regulatory Implications», *Sackler Forum*, 2015, https://royalsociety.org/topics-policy/publications/2016/sackler-forum-report/

– THIBERGE, C., « Des insectes pour disséminer des virus, arme incontrôlable ? », *Le Monde*, 2018, https://www.lemonde.fr/planete/article/2018/10/04/des-insectes-pour-disseminer-des-virus-une-arme-incontrolable_5364811_3244.html

8. LES NANOTECHNOLOGIES

Anaïs Cren-Larvor

Résumé : Les nanotechnologies, en travaillant les matériaux et l'électronique à très petite échelle, permettent la miniaturisation et la dissémination d'armes très sophistiquées, y compris nucléaires. Offrant en outre des capacités de détection inégalées, elles peuvent mettre à mal toute stratégie de « dissuasion » nucléaire, tout en augmentant le risque d'explosion incontrôlée, accidentelle ou terroriste.



Les nanotechnologies permettent de fabriquer des nanorobots capables de guérir comme de tuer. Source : OnlyMyHealth

8.1 Description des nanotechnologies / nanosciences

8.1.1 Que sont les nanotechnologies / nanosciences ?

Les nanosciences sont l'ensemble des études scientifiques qui s'intéressent à l'échelle nanométrique (10^{-9} m, soit un milliardième de mètre ou un millième de micromètre ; on est presque à l'échelle atomique, la taille d'une molécule d'eau par exemple étant de l'ordre de 0,1 nanomètre).

Les nanotechnologies regroupent l'étude, la fabrication et la manipulation de structures, de dispositifs et de systèmes matériels à l'échelle de moins d'une quarantaine de nanomètres. Elles peuvent adapter les structures des matériaux à des échelles extrêmement petites pour obtenir des propriétés spécifiques. Ainsi, les matériaux peuvent être rendus plus résistants, plus légers, plus durables, plus réactifs, ou de meilleurs conducteurs électriques, entre autres caractéristiques.

C'est pourquoi les nanotechnologies contribuent à améliorer considérablement, voire à révolutionner, de nombreux secteurs technologiques et industriels : technologies de l'information, sécurité intérieure, médecine, transports, énergie, sécurité alimentaire, sciences environnementales… et armement, tant conventionnel que nucléaire.

Quoique ce dernier domaine d'application soit rarement cité en raison du secret-défense, il est clair que les nanotechnologies, menant à des systèmes plus résistants, plus rapides et plus portatifs, pouvant gérer et stocker des quantités d'information de plus en plus grandes, sont fortement exploitées par l'armée. Il est nécessaire de disposer de mécanismes d'armement et de déclenchement extrêmement robustes et sûrs pour les armes nucléaires, comme les obus d'artillerie atomique. Dans ces ogives, l'explosif nucléaire et son déclencheur subissent une accélération extrême, d'où la nécessité que les composants essentiels de la détente soient les plus résistants et les plus petits possibles.

Les nanotechnologies possèdent donc un très fort potentiel destructeur. Mais leur caractère dual (civil et militaire) rend leur réglementation très complexe.

8.1.2 Quel impact militaire ?

Les nanotechnologies permettent :

- De stocker et d'analyser plus efficacement les informations, ce qui optimise la surveillance et les informations des services de renseignement ;
- D'avoir de meilleurs dispositifs de surveillance et de détection (ex : essaims de nanocapteurs) ;
- D'améliorer la prise de décision tactique (en lien avec l'IA) ;
- D'améliorer drastiquement les systèmes d'armes existants ;
- De créer des armes et des munitions « intelligentes » et de nouveaux systèmes d'armes ;
- D'augmenter l'autonomie des systèmes ;
- D'avoir un impact logistique et financier (véhicules plus résistants, moins chers, avec une précision extrême de tir ; meilleure rentabilité des chaînes de production).

8.2 Impact des nanotechnologies sur les armes nucléaires

Les nanotechnologies permettent une amélioration drastique des armes nucléaires :

- Elles permettent la création d'une bombe de 4ème génération à micro-fusion, grâce à :
    - Un nouveau système d'armes nucléaires un peu moins puissantes (passer sous les 1 000 tonnes de TNT) qui brouillent la frontière entre arme conventionnelle et arme de destruction massive ;
    - Une augmentation très conséquente de la puissance de feu d'un État ;
    - La création d'une arme dite « propre » avec moins de retombées radioactives ;
    - Au contournement des systèmes de surveillance internationaux car l'arme ne franchit pas vraiment le seuil d'utilisation d'une arme nucléaire.
- Elles permettent la création d'armes nucléaires miniatures :

- Plus difficiles à détecter (voire invisibles grâce aux nanosciences),
- Déclenchées par un super-laser,
- Plus petites, plus gérables, plus faciles à transporter et à dissimuler,
- Offrant une meilleure précision, une meilleure information (via des nano-ordinateurs) ;
- Comportant un danger supplémentaire : ces mini-bombes pourraient plus facilement faire l'objet d'un trafic illicite et finir dans des pays inattendus (voire aux mains de groupes terroristes).

– Elles entraîneraient une augmentation rapide des arsenaux nucléaires grâce à une fabrication plus rapide et moins chère.

8.3 L'impact des nanotechnologies sur la stratégie nucléaire

Un nano-armement nucléaire pourrait mettre à mal l'équilibre géostratégique mondial de deux façons :

– En offrant à un plus grand nombre d'acteurs des moyens de destruction sans commune mesure avec les arsenaux existants,

– En conférant à ces mêmes protagonistes des capacités de résistance inégalées face à des risques d'attaque de toute provenance et de toute nature.

Les nanotechnologies offrent une plus grande capacité de détection : on serait capable de repérer une tête nucléaire beaucoup plus rapidement, et potentiellement de la détruire ou de l'intercepter grâce aux armes hypersoniques dans lesquelles les nanotechnologies ont un rôle à jouer.

En dehors des armes nucléaires, les nanotechnologies permettent la création d'un nouveau système d'armes autonomes plus destructeurs encore que l'arme atomique, si bien qu'on parle de « dissuasion nanotechnologique » :

– Des systèmes de très petite taille et de capacités proches de celles du vivant en termes d'autonomie peuvent acquérir la capacité de se reproduire, ce qui ouvrirait la porte à de nombreuses armes d'un type nouveau ;

– Une attaque (accidentelle, terroriste ou militaire) de nanorobots, de structures moléculaires et autres pathogènes autorépliquants peuvent détruire la biomasse et la civilisation en seulement quelques jours ou semaines ;

– La capacité de répliquer la vie au niveau moléculaire peut faciliter le développement de nouvelles armes biologiques plus meurtrières par des acteurs indépendants.

Une guerre nanotechnologique aurait une rapidité foudroyante et serait extrêmement destructive, provoquant la déstabilisation des équilibres géostratégiques et menaçant de faire passer la bombe atomique d'une arme de « dissuasion » à une arme d'emploi.

Un nouvel équilibre de la terreur pourrait naître : il est possible que la course aux armements nanotechnologiques entraîne une prolifération nucléaire effrénée et l'expansion des principaux arsenaux nucléaires jusqu'à des centaines de milliers ou des millions d'ogives.

8.4 Les conséquences géopolitiques

Dans un futur conflit nanotechnologique, si les deux parties (ou plus) sont équipées de telles armes, les pertes pourront se chiffrer en millions de vies. Comme ces armes seraient moins chères et plus faciles à produire, le risque est que tous les États et entités non-étatiques puissent en acquérir. Une telle évolution remettrait en cause les équilibres militaires et géopolitiques de la planète : les cinq États « dotés » d'armes nucléaires (EDAN) n'auront plus l'avantage, leur stratégie de « dissuasion » s'effondrera. Non seulement cette stratégie sera obsolète, mais il existe un risque d'utilisation préemptive de l'arme nucléaire contre un État qui possède des armes nanotechnologiques.

Les nanotechnologies menacent donc de saper le pouvoir de la « dissuasion nucléaire », si souvent invoqué par les EDAN, tout en augmentant le risque d'utilisation des armes nucléaires. Là comme pour d'autres technologies de rupture, **il faudra trouver un nouveau cadre réglementaire international qui préserve le développement des nanotechnologies mais encadre plus drastiquement leur utilisation dans le domaine militaire.**

8.5 Bibliographie

- DANIELS Jeff, « Mini-nukes and Mosquito-like Robot Weapons Being Primed for Future Warfare », *CNBC*, 17 mars 2017, https://www.cnbc.com/2017/03/17/mini-nukes-and-inspect-bot-weapons-being-primed-for-future-warfare.html

- FONDATION SCIENCES CITOYENNES, *Nanotechnologies et applications militaires,* 5 février 2011, https://sciencescitoyennes.org/wp-content/uploads/2012/12/nano-et-militaire.pdf

- « Après la dissuasion nucléaire, la dissuasion nanotechnologique ? », *Futura Sciences*, 14 avril 2006, https://www.futura-sciences.com/tech/actualites/tech-apres-dissuasion-nucleaire-dissuasion-nanotechnologique-8657/

- GSPONER André, « La nanotechnologie va permettre l'avènement d'armes nucléaires de quatrième génération », *Imagine Magazine*, septembre-octobre 2003, 17 p, http://isri.ch/wiki/_media/publications:isri-03-07.pdf

- SANDBERG Anders BOSTROM Nick, « Global Catastrophic Risks Survey », *Technical Report* , Future of Humanity Institute (Oxford University), janvier 2008 p. 1-5 https://www.fhi.ox.ac.uk/reports/2008-1.pdf

9. LA TECHNOLOGIE QUANTIQUE

Pablo Chaillat

Résumé : La technologie quantique promet de rendre obsolètes les systèmes de communication et de localisation actuels. Les impératifs de confidentialité et de furtivité au cœur des stratégies de la « dissuasion nucléaire » sont ainsi profondément fragilisés. En compressant le temps et l'espace, la technologie quantique augmente drastiquement les risques d'escalade nucléaire.

Ordinateur quantique IBM Q System One installé près de Stuttgart.
Source : IBM

9.1 Définitions et cadrage

La physique est la science qui tente de comprendre, modéliser et expliquer les phénomènes naturels de l'univers. Pour l'homme de la rue, la compréhension des « lois naturelles » est avant tout un travail d'observation du monde qui nous entoure, tel Isaac

Newton découvrant la loi de la gravité au travers d'une pomme tombant d'un arbre. Seulement, cette acception commune, qui est de l'ordre de la « **mécanique classique** », ne s'applique pas aux domaines atomiques et subatomiques de la « **mécanique quantique** », dont les lois diffèrent voire s'opposent à celles du monde des milieux solides, liquides et gazeux qui nous est observable.

Deux phénomènes quantiques (superposition et intrication) présentent de fortes potentialités technologiques (ordinateur quantique, communications, radars, capteurs…) avec des conséquences probables pour les stratégies nucléaires.

9.2 Superposition, informatique quantique et cryptologie

Le phénomène de **superposition**, d'une part, explique qu'en mécanique quantique, contrairement à la mécanique classique, les particules élémentaires (protons, électrons, photons…) sont susceptibles de se trouver dans *plusieurs états en même temps*. En effet, une particule élémentaire peut être définie avec certaines valeurs, par exemple sa vitesse, sa position dans l'espace, une rotation. À un moment donné, si l'on prépare la particule élémentaire d'une certaine manière, alors elle pourra posséder plusieurs valeurs d'états en même temps : par exemple, un photon pourrait être à la fois orienté vers le haut et vers le bas, simultanément.

9.2.1 L'informatique quantique

Cette singularité quantique ouvre des potentialités immenses, en particulier dans l'**informatique quantique** et le **traitement ultra-rapide de larges quantités de données**. À la différence des ordinateurs classiques pour lesquels l'information s'affiche en valeur 0 ou 1, l'ordinateur quantique s'appuie sur des qubits (particules quantiques) qui utilisent la superposition pour adopter différents états en même temps[8]. En d'autres termes, là où pour résoudre un problème complexe, un ordinateur classique doit traiter les solutions possibles les unes après les autres, **un ordinateur quantique peut fouiller**

[8] Certains articles journalistiques avancent l'idée que l'ordinateur quantique ouvre la possibilité d'être *aussi bien* 0 que 1 (0+1) – et non plus seulement 0 *ou* 1. Cependant, le phénomène quantique semble plus compliqué que cela et cette comparaison n'est pas nécessairement adaptée. On préfèrera la formulation « différents états en même temps ».

simultanément dans toutes les informations disponibles à la recherche de propriétés communes et déceler une constante dans ces données.

9.2.2 *L'informatique quantique et la cryptologie*

En permettant de trier de façon rapide et efficace de très larges quantités de données, l'informatique quantique promet de révolutionner des secteurs comme la livraison de marchandises (calcul du meilleur itinéraire), la médecine (compréhension de l'origine des maladies et définition des meilleurs traitements en fonction d'une très large base de données des patients) ou encore l'analyse financière et météorologique. En même temps, les possibilités ouvertes par l'informatique quantique présentent aussi des risques certains, en particulier en **cryptologie**. Les systèmes actuels de cryptage les plus utilisés fonctionnent selon la méthode de chiffrement RSA (du nom de ses fondateurs, Ronald Rivest, Adi Shamir et Leonard Adleman), qui repose sur l'incapacité d'un ordinateur classique à explorer chaque solution l'une après l'autre *dans un temps acceptable*. Cette opération est bien sûr quasi-instantanée pour un ordinateur classique dans le cas d'un petit nombre, mais pour un nombre à plusieurs dizaines ou centaines de chiffres, un ordinateur classique pourrait mettre des années avant de trouver la solution, là où le système de superposition de l'ordinateur quantique lui permet d'effectuer la même opération en quelques minutes voire secondes. Toutefois, les codes nucléaires reposent sans doute sur des combinaisons plus complexes tels que AES (pour *Advanced Encryption Standard*) qui sont à ce jour « quantum-resistant »[9], mais peut-être plus pour très longtemps…

9.3 Intrication, cryptologie et capteurs quantiques

Le phénomène de **l'intrication** est la seconde caractéristique importante de la mécanique quantique, qui la distingue de la mécanique classique. À savoir que, dans l'infiniment petit, deux particules peuvent être liées par leur état (i.e. *intriquées*) quelle que soit la distance qui les sépare : un changement dans l'une des particules aura une conséquence *immédiate* sur l'état de l'autre particule.

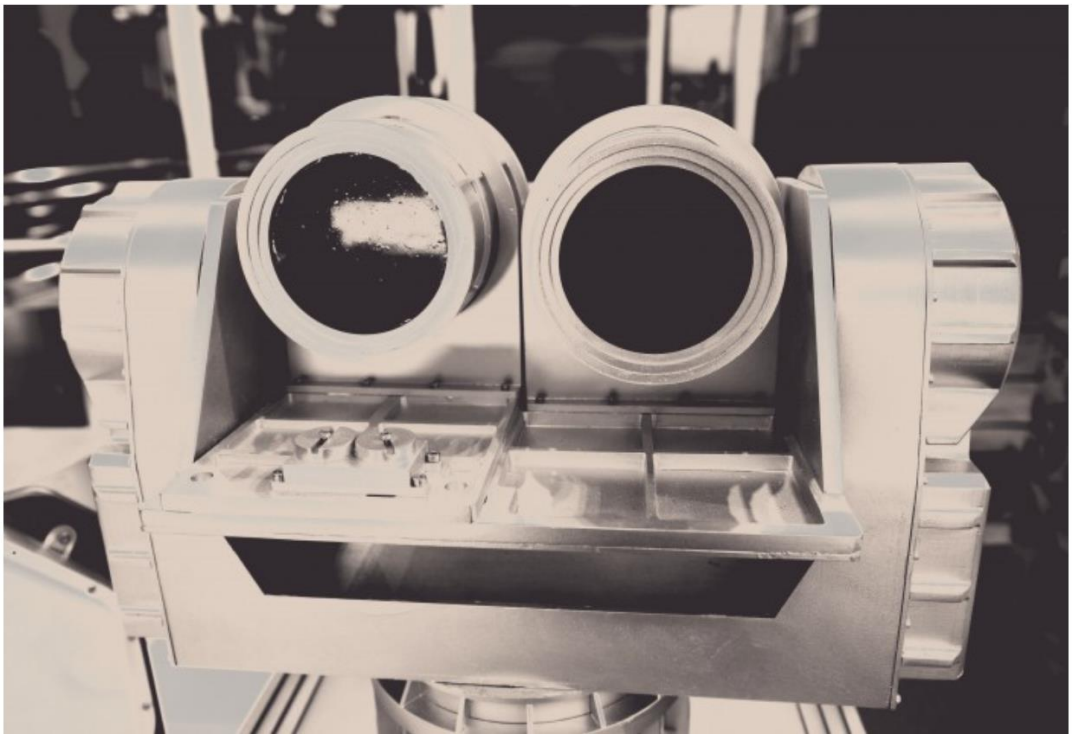
[9] Lane Wagner, « Is AES-256 Quantum Resistant? », qvault.io, 10 septembre 2020 (https://qvault.io/cryptography/is-aes-256-quantum-resistant/).

9.3.1 L'intrication et les systèmes de communication

Les applications technologiques de l'intrication sont immenses, en particulier dans les communications et les capteurs. Les systèmes de communication quantiques fonctionnent ainsi au travers d'une machine qui lie deux photons entre eux (l'un est diffusé à l'extérieur et l'autre reste dans la machine), ce qui permet de créer une « clé quantique », laquelle est ensuite *inviolable* dans la mesure où l'intervention d'un acteur indiscret sur une partie du système aurait automatiquement des conséquences sur l'ensemble du système, selon la logique de l'intrication, et serait donc automatiquement détectée. **La communication quantique rend ainsi beaucoup plus sûrs les systèmes de lancement des armes nucléaires face aux risques de cyberattaque**, présentés au chapitre 4.

9.3.2 Les capteurs quantiques : radars et gravimètres

Le phénomène de l'intrication est aussi très prometteur pour l'amélioration des capteurs quantiques, qui peuvent permettre de détecter aussi bien les avions furtifs que les sous-marins nucléaires. Dans le cas d'un radar traditionnel, celui-ci fonctionne selon un processus de rebondissement : des photons (ou ondes radios) sont envoyés dans l'espace, et lorsqu'un avion se trouve sur cette voie, les photons concernés sont renvoyés à l'émetteur, révélant ainsi la position de l'objet recherché. C'est pourquoi les avions furtifs sont conçus avec une forme et une peinture particulières, permettant de dévier ces photons dans tous les sens, et ainsi d'éviter leur retour à l'émetteur. Cependant, les capteurs quantiques rendent caduc cette technologie, puisque ceux-ci fonctionnent selon le phénomène de l'intrication : un photon est envoyé dans l'espace, tandis que l'autre reste dans le radar — l'état de l'un influe sur l'état de l'autre. Dès lors, si l'un des photons est absorbé par la peinture d'un avion furtif, cela aura une conséquence directe sur l'état de son jumeau intriqué. **Le phénomène de l'intrication permet ainsi de mettre au point des radars ultra-performants capables de détecter au mètre près des objets furtifs.**



Équipement d'un prototype de radar quantique fabriqué par la société China Electronics Technology Group
Source : Imaginechina via AP Images

Dans le cas des sous-marins, c'est la technologie des gravimètres, hautement améliorée en version quantique, qui pourrait permettre d'espionner leurs trajectoires confidentielles. En effet, si les gravimètres traditionnels permettent d'évaluer les fluctuations de la gravité terrestre en fonction de la matière située sous nos pieds, un gravimètre quantique pourrait aller jusqu'à détecter des mouvements souterrains de matière, pour en déduire les mouvements d'objets furtifs.

9.4 Autres applications : le magnétomètre, compas quantique et détection des sous-marins

En utilisant des **magnétomètres** traditionnellement utilisés pour mesurer les anomalies magnétiques, mais augmentés de la technologie quantique, il devient possible a) de détecter de larges objets métalliques comme des sous-marins, b) pour ces mêmes sous-marins de naviguer « à vue », ou plutôt sans l'aide d'un GPS classique, relié à un satellite. Le

« compas quantique » pourrait permettre aux sous-marins nucléaires de ne plus dépendre des communications satellites classiques, qui sont vulnérables aux cyberattaques et rendent plus difficile l'obligation de furtivité[10].

9.5 Conséquences pour la « dissuasion nucléaire »

La capacité de l'informatique quantique à casser les **codes informatiques** pose de sérieux problèmes pour la « dissuasion nucléaire », notamment en ce qui concerne la confidentialité des codes nucléaires ou encore de la localisation des bases ou sous-marins nucléaires. Dans un monde où les États nucléaires ne seraient plus en mesure de garder secrète la localisation de leurs sites de lancement, l'incitation à frapper en premier (en sachant que l'on peut espérer complètement détruire la capacité de réponse nucléaire de son adversaire) serait fortement renforcée. De même, les États pourraient engager un réarmement massif, selon la logique qu'une multiplication des armes nucléaires rend plus difficile pour un adversaire l'élimination des capacités de représailles en une seule frappe.

Les conséquences potentielles des **capteurs quantiques** pour la stratégie de « dissuasion nucléaire » sont également immenses, en particulier en ce qui concerne l'obligation de furtivité qui est associée aux « triades » nucléaires (air, sol, mer). Dans la mesure où la dissuasion est basée principalement sur la capacité *perçue* d'infliger un dommage inacceptable en cas d'attaque, ces nouveaux capteurs pourraient réduire la confiance des décideurs dans leur capacité militaire à effectuer une « seconde frappe » avec succès, en l'absence d'effet de surprise. Inversement, au même titre que pour la cryptologie, l'impossibilité de cacher la localisation des sous-marins nucléaires pourrait inciter un État à frapper en premier.

9.6 Et la France ?

La France est consciente de la course quantique en cours. De nombreux pays, au premier rang desquels la Chine, investissent massivement dans la recherche quantique, dans l'espoir d'applications technologiques révolutionnaires. L'Europe a aussi investi de façon conséquente dans la recherche quantique et bénéficie en la matière du prestige de ses

[10] Project Q, Peace & Security in a Quantum Age (https://projectqsydney.com/).

universités. Le ministère des Armées français a déjà prévu d'investir 30 millions d'euros entre 2019 et 2025 sur les recherches dans la technologie quantique. Le président Macron a lui annoncé un investissement global de 1,8 milliard d'euros de la part de la France. L'Agence de l'Innovation de Défense (AID) justifie son investissement de la façon suivante : « *L'exploration de telles technologies émergentes, et plus largement l'identification précoce de ruptures potentielles, fait l'objet de recherches exploratoires pour préparer le futur au-delà du 'besoin militaire prévisible'* ».

Cependant, si l'application de la mécanique quantique présente des potentialités intéressantes en matière technologique, elle augmente en même temps la fragilité de la dissuasion nucléaire, qui repose sur la confidentialité des canaux de communication et des sites de lancement nucléaires. Du reste, en raccourcissant drastiquement le temps de réponse à une attaque, la technologie quantique risque de rendre le scénario d'une escalade nucléaire plus probable qu'auparavant. Les recherches au croisement de la technologie quantique et de la dissuasion sont encore balbutiantes et c'est pourquoi le rapport d'IDN apportera certainement une contribution intéressante. Le **Project Q,** lancé par James Der Derian, professeur à l'université de Sydney, semble l'initiative la plus prometteuse en la matière aujourd'hui.

9.7 Bibliographie

- DER DERIAN James & WENDT A., « 'Quantizing international relations': The case for quantum approaches to international theory and security practice », *Security Dialogue*
- DER DERIAN, James, itw. par CASTRO Vic, « Drones, radars, nucléaires : comment le quantique va changer la guerre », *Numérama*, 22 février 2020, https://www.numerama.com/politique/606950-drones-radars-nucleaire-comment-le-quantique-va-changer-la-guerre.html.
- DUFOUR, A., « Comprendre (un peu mieux) l'ordinateur quantique », *La Croix*, 2021, https://www.la-croix.com/JournalV2/Comprendre-peu-mieux-lordinateur-quantique-2021-05-04-1101153951
- GAMBERINI, S.J & RUBIN L., « Quantum Sensing's Potential Impacts on Strategic Deterrence and Modern Warfare », *Foreign Policy Research Institute,* 51(5), 399-413, 2021

- GILES Martin, « The US and China are in a quantum arms race that will transform warfare », *MIT Technology Review*, 3 janvier 2019, https://www.technologyreview.com/2019/01/03/137969/us-china-quantum-armsrace/#Echobox=1580145311

- HAYES Peter, « Nuclear Command and Control in the Quantum Era », *Nautilus*, (29 mars 2018), https://nautilus.org/napsnet/nuclear-command-and-control-in-the-quantum-era/

- KUBIAK Katarzyna, *Quantum Technology and Submarine Near-invulnerability*, European Leadership Network, 11 décembre 2020,

- KUBIAK Katarzyna et al. « Nuclear Weapons Decision-making under Technological Complexity », European Leadership Network, 25 mars 2021 (https://bit.ly/2VfLxXh).

- OWEN, T. & GORWA, R., « Quantum Leap: China's Satellite and the New Arm Race », *Foreign Affairs*, 2016

- ROBLIN, S, « No More 'Stealth' Submarines: Could Quantum 'Radar' Make Submarines Easy to Track (And Kill)? », *The National Interest*, 2019, https://nationalinterest.org/blog/buzz/no-more-stealth-submarines-could-quantum-radar-make-submarines-easy-track-and-kill-54547

- SOKOVA, Elena, *Disruptive Technologies and Nuclear Weapons*, Vienna Center for Disarmament and Non-Proliferation, 17 juillet 2020, https://vcdnp.org/disruptive-technologies-and-nuclear-weapons/).

- WADHWA, Vivek, « Quantum Computers may be more of an imminent threat than AI », *The Washington Post*, 2018, https://www.washingtonpost.com/news/innovations/wp/2018/02/05/quantum-computers-may-be-more-of-an-imminent-threat-than-ai/

10. CONCLUSIONS

Résumé : Alors que la menace nucléaire pèse déjà sur l'humanité, de nouvelles technologies émergent et conduisent, à brève échéance, à la fois à aggraver encore le risque de catastrophe nucléaire et à rendre carrément obsolète cette stratégie déjà condamnée pour son illégalité internationale. C'est ce que la présente étude s'est efforcée de démontrer.

Essai nucléaire français en Polynésie en 1971
Source : Banque d'images de l'OTICE

La stratégie dite de « *dissuasion nucléaire* » adoptée par la France consiste à menacer tout État qui s'en prendrait à ses « *intérêts vitaux* » de « *dommages absolument inacceptables sur ses centres de pouvoir, c'est-à-dire sur ses centres névralgiques, politiques, économiques, militaires*[11] ». On ne le dira jamais assez, cette stratégie est contraire au droit international :

[11] Discours du président Emmanuel Macron devant l'Ecole de guerre (7 février 2020).

celui-ci exige, notamment, que la légitime défense soit nécessaire et proportionnée, que les civils soient épargnés, faute de quoi elle s'apparente à un crime de guerre voire à un crime contre l'humanité, et que soit négocié « de bonne foi » le désarmement nucléaire. C'est pourquoi les autorités françaises se sont attachées à en gommer les conséquences : elles ne parlent plus de « *stratégie anti-cités* » et affirment, sans certitude possible, que le pouvoir destructeur de la force nucléaire dissuadera l'agresseur et donc évitera la guerre.

Le terme même de « dissuasion » est un euphémisme choisi à dessein par les concepteurs de la doctrine française. Il implique chez l'adversaire un calcul rationnel, qui n'est d'ailleurs nullement garanti. Il se distingue, sur le plan sémantique, du terme anglais *deterrence* dont la racine est la même que « terreur » ou « terrorisme ». Plus honnêtement, les autres puissances nucléaires admettent que leur but est de semer la terreur chez les adversaires potentiels, mais aussi dans leurs populations. Mais au fond, la stratégie est la même. C'est en fait toute l'humanité qui est soumise à ce chantage compte tenu des conséquences humanitaires mondiales de toute guerre nucléaire, fût-elle régionale.

Cette **capacité de terroriser les populations** repose évidemment sur une technologie, l'explosion nucléaire dont les effets ont été démontrés à Hiroshima et Nagasaki, mais aussi par les quelque 2 121 essais nucléaires dont 520 dans l'atmosphère (soit l'équivalent, pour ces derniers, de 29 000 bombes d'Hiroshima). Cette technologie a été découverte il y a plus de 80 ans et c'est pour empêcher Hitler de se doter de la bombe atomique que le colossal projet Manhattan a été lancé par les États-Unis dès 1942. Malgré les évolutions et les modernisations intervenues depuis lors, la technologie demeure quasiment identique.

Parallèlement, le monde a vu naître **de nouvelles technologies qui rendent la stratégie de menace nucléaire vulnérable et, à terme, obsolète**. Les partisans de l'arme nucléaire répondent à ceux qui entendent l'éliminer qu'il est impossible de la « désinventer ». Mais l'histoire abonde en technologies, y compris de défense, qui ont été dépassées par de nouvelles découvertes et abandonnées : de l'arc et du mousquet à poudre à la marine à voile.

Ainsi, l'**intelligence artificielle**, si fascinante pour tout un chacun, séduit aussi les militaires, préoccupés de limiter les pertes en personnel au combat et intéressés par les **systèmes d'armes autonomes** ou les aéronefs sans pilote. Introduire une telle autonomie dans des systèmes de commandement et contrôle d'armes nucléaires ne permettrait plus

d'éviter les fausses alertes détectées par des humains grâce à qui le monde a plusieurs fois échappé à la catastrophe.

La stratégie de menace nucléaire repose sur la capacité de riposte en cas de première frappe, principalement au moyen de missiles tirés de sous-marins prétendument indétectables et donc invulnérables. Or les progrès combinés de l'**intelligence artificielle** et de l'**informatique quantique** permettront, tôt ou tard, de calculer les trajectoires de sous-marins et donc de les cibler tout aussi facilement que des bases aériennes ou des silos de missiles terrestres. De quoi faire réfléchir face à l'assurance de la ministre des Armées qui affirmait récemment que les sous-marins français lanceurs d'engins de troisième génération navigueraient jusqu'en 2090 !

Les **capacités numériques** conjuguées à l'**intelligence artificielle** pourraient tout aussi facilement pirater les systèmes d'authentification et d'autorisation de tirs d'armes nucléaires, une fois détectée la menace. Ainsi, la technologie des « **deep fakes** » permettrait d'imiter une communication ou un enregistrement vidéo du dirigeant confirmant son approbation du tir, provoquant une attaque involontaire.

Les systèmes nucléaires offensifs ou défensifs (antimissiles) dépendent également de réseaux de communications cryptés et déployés sur des satellites en orbite. Or le cryptage de ces réseaux est devenu vulnérable aux **attaques cyber** renforcées par l'**informatique quantique,** et les satellites eux-mêmes peuvent facilement faire l'objet d'attaques par **collision kinétique** d'apparence accidentelle ou par **armes à énergie dirigée** (lasers puissants). Les attaques cyber, elles-mêmes quasi impossibles à attribuer, pourraient aussi se concentrer sur les centres de commandement et de contrôle et soit désactiver des systèmes de détection ou de lancement, soit au contraire provoquer des tirs non autorisés susceptibles d'entraîner une riposte nucléaire.

La technologie de l'hypervélocité (**missiles hypersoniques**) est aussi devenue attrayante pour celles des puissances nucléaires qui redoutent une première frappe décapitante encouragée par des systèmes antimissiles capables de repousser toute riposte. En investissant massivement dans des missiles plus rapides et surtout plus manœuvrables que les missiles balistiques ou même de croisière, ces puissances nucléaires sont incitées à se lancer dans des frappes préventives et donc contribuent à abaisser le seuil de recours aux armes nucléaires. D'arme dite dissuasive, l'arme nucléaire redevient sans retenue une arme de combat.

Une autre technologie est déjà liée à la menace nucléaire, celle de l'**impulsion électromagnétique**, capable, au moyen d'armes nucléaires ou combinée avec des armes à micro-ondes ou hyperfréquences, de créer un chaos stratégique : interruption des communications, des systèmes informatiques et de la distribution d'électricité, paralysie des systèmes de commandement, incapacité à contrôler les forces militaires. Ce scénario est celui de « *l'ultime avertissement* » prévu par la France en cas d'échec de la dissuasion (donc admis comme une possibilité) et de nature à déclencher l'escalade nucléaire. En effet, le seuil du nucléaire serait franchi et, de surcroît, il serait impossible de ne cibler que des objectifs militaires, toutes les infrastructures critiques (contrôle aérien, hôpitaux, centrales nucléaires civiles, système bancaire, etc.) étant potentiellement paralysées.

À terme, même si cela paraît encore de la science-fiction, on peut imaginer des **nanorobots** saturant des systèmes de commandement et de contrôle ou toute infrastructure militaire apparemment protégée contre des attaques cinétiques, et anéantissant toute capacité offensive ou défensive. Et plus près de nous, que penser de la capacité de drones équipés d'IA à transpercer les dômes de protection même sophistiqués tels que le système Patriot israélien ?

Ainsi, les risques que font peser ces nouvelles technologies sur la stratégie de menace nucléaire ne peuvent qu'aggraver encore la probabilité de déflagrations nucléaires intentionnelles, par méprise, par accident ou action terroriste. En soi, cette aggravation devrait suffire à convaincre les dirigeants des puissances nucléaires de renoncer à cette stratégie dont le danger est devenu inacceptable.

En outre, **ces nouvelles technologies pourraient à brève échéance rendre la prétendue « *dissuasion nucléaire* » complètement obsolète et inefficace**. Une raison de plus pour y mettre fin, tout en veillant à ce que les potentiels offerts par ces nouvelles technologies, en particulier les armes autonomes et les cyberattaques, ne soient pas pires que le mal, c'est-à-dire ne menacent encore davantage les infrastructures sensibles ou les populations civiles. Du travail en perspective pour les diplomates, les juristes, les experts militaires et la société civile, d'autant que si l'arme nucléaire reste encore entre les mains des États, les armes cyber sont largement entre les mains de groupes criminels ou terroristes plus difficiles à contrôler ou à atteindre, voire impossibles à attirer à une table de négociation.

10.1 Bibliographie

- BRUSTLEIN, Corentin « La réduction des risques stratégiques entre puissances nucléaires », Proliferation Papers (IFRI), n°63, janvier 2021, https://www.france24.com/fr/20190509-ia-intelligence-artificielle-nucleaire-menace-atomique-sipri-russie

- ERÄSTÖ, Tytti, *New Technologies and Nuclear Disarmament*, SIPRI, 7 mai 2021, https://www.sipri.org/publications/2021/other-publications/new-technologies-and-nuclear-disarmament-outlining-way-forward

- FAVARO, Marina, « Emerging Technologies and Nuclear Stability », *European Leadership Network*, 19 juillet 2021, https://www.europeanleadershipnetwork.org/commentary/emerging-technologies-and-nuclear-stability/

- GNESOTTO, Nicole, « Révolutions technologiques : pour le meilleur ou pour la guerre ? », *Forum mondial Normandie pour la Paix*, 2019, https://normandiepourlapaix.fr/ressources/nicole-gnesotto-revolutions-technologiques-pour-le-meilleur-ou-pour-la-guerre

- JOHNSON, James, KRABILL, Eleanor, « AI, Cyberspace and Nuclear Weapons », *War on the Rocks,* 31 janvier 2020, https://warontherocks.com/2020/01/ai-cyberspace-and-nuclear-weapons/

- MAITRE Emmanuelle, « Phébé – La dissuasion nucléaire à l'épreuve de la technologie », *Le Point*, 3 juillet 2018, https://www.lepoint.fr/phebe/phebe-ces-technologies-qui-menacent-la-dissuasion-nucleaire-03-07-2018-2232655_3590.php

- SEIBT, Sébastien, « De la Bombe A à la Bombe IA », *France24*, 9 mai 2019, https://www.france24.com/fr/20190509-ia-intelligence-artificielle-nucleaire-menace-atomique-sipri-russie

- SU, Fei et al., *Artificial Intelligence, Strategic Stability and Nuclear Risk*, SIPRI, juin 2020, https://www.sipri.org/publications/2020/other-publications/artificial-intelligence-strategic-stability-and-nuclear-risk

À PROPOS DES AUTEURS

REMERCIEMENTS

ANAÏS CREN-LARVOR

Anaïs Cren-Larvor est diplômée d'un Master 2 de droit international public et spécialisée dans le domaine de la non-prolifération des armes nucléaires et de la protection physique des matières et installations nucléaires.

Elle a effectué un stage à IDN et est actuellement Chargée de projet coopération internationale chez Astove Conseil.

BERNARD NORLAIN

Président d'IDN

Général d'armée aérienne (2S) et président d'IDN depuis octobre 2021, Bernard Norlain est titulaire du diplôme d'Ingénieur de l'Ecole de l'air et ancien pilote de chasse. Il a occupé les fonctions de Chef du Cabinet militaire des Premiers ministres Jacques Chirac et Michel Rocard.

Il a dirigé l'Institut des Hautes Etudes de Défense nationale (1994-1996), a été Vice-Président de Deloitte & Touche France puis Président-Directeur général de SOFEMA Group. Il est aujourd'hui Président d'honneur du Comité d'études de la Revue Défense nationale. Il est Commandeur de la Légion d'Honneur et a reçu la Médaille d'Or Mahatma Gandhi de l'Unesco. Il est co-auteur de « Arrêtez la bombe ! » (2013) avec Paul Quilès et Jean-Marie-Collin.

JACQUES FATH

Bureau d'IDN

Membre du bureau d'IDN depuis octobre 2021, Jacques Fath est un chercheur indépendant, spécialiste des relations internationales, des enjeux de la sécurité et de la paix. Son approche est résolument critique des politiques et des courants de pensée aujourd'hui médiatiquement dominants.

Il est diplômé de l'Institut d'Études Politiques (Grenoble) et licencié en sociologie. Il est l'auteur de : « Penser l'après… Essai sur la sécurité, la puissance et la paix dans le nouvel état du monde » (2015), « Terrorisme. Réalités, causes et mystifications idéologiques » (2019) et de « Chaos. La crise de l'ordre international libéral. La France et l'Europe dans l'ordre américain » (2020).

MARC FINAUD

Vice-président d'IDN

Ancien diplomate de carrière, Marc Finaud travaille comme formateur pour jeunes diplomates et officiers au sein du Centre de Politique de Sécurité de Genève (GCSP) dans tous les domaines de la sécurité internationale. Au cours de sa carrière diplomatique, il a été affecté à plusieurs postes bilatéraux (URSS, Pologne, Israël, Australie) ainsi qu'à des missions multilatérales (CSCE, Conférence du Désarmement, ONU), et a été Collaborateur scientifique de l'Institut des Nations unies pour la Recherche sur le Désarmement (UNIDIR) (Programme sur les Armes de destruction massive).

Vice-président d'IDN, il a la responsabilité d'assurer les relations internationales et diplomatiques de l'association. Il est l'auteur de « L'arme nucléaire : éliminons-la avant qu'elle nous élimine » (2020).

PABLO CHAILLAT

Bureau d'IDN

Pablo Chaillat est diplômé d'un Master 2 en Sécurité internationale de l'Université de Warwick (Royaume-Uni). Il détient également une double Licence en Histoire et Philosophie, obtenue dans le cadre de trois années de Classe préparatoire aux grandes écoles à Paris.

Il travaille comme *Junior Professional Officer* au sein du Centre de Politique de Sécurité de Genève (GCSP). Passionné par les enjeux de prévention des conflits et de construction de la paix, il se spécialise sur la géopolitique du Proche et Moyen-Orient. Il contribue aux pôles Recherche et Relations Extérieures.

PAUL QUILÈS

Ancien président d'IDN

Récemment décédé, Paul Quilès a exercé plusieurs fonctions d'élus et ministérielles. Ministre de la Défense, il a également été vice-président de la Commission de la Défense et des Forces Armées de l'Assemblée nationale. Ancien Maire de Cordes sur Ciel (Tarn), il était impliqué de longue date dans la lutte pour le désarmement nucléaire. Membre fondateur d'IDN, il en a assumé la présidence jusqu'à son décès. Il était l'auteur de « Face aux désordres du monde » (2006), « Nucléaire, un mensonge français » (2012), « L'Illusion nucléaire avec » (2012) et « Arrêtez la bombe ! » (2013).

SOLÈNE VIZIER

Bureau d'IDN

Passionnée de géopolitique, Solène Vizier est titulaire d'un double Master 2 en Études stratégiques à l'Université Paris 13 et en cybersécurité, cyberterrorisme et cyberguerre à l'INISEG (Espagne). Elle est actuellement analyste au sein d'un cabinet spécialisé en stratégie digitale.

Elle est membre du groupe de travail Cyber de l'Institut EGA. Au sein d'IDN, elle est chargée du Pôle Recherche.

Remerciements à **Annick Suzor-Weiner**, vice-présidente d'IDN et de Pugwash France, **Blaise Imbert**, Trésorier d'IDN, **Thierry Lorho**, concepteur du système d'intelligence artificielle Mileva, et **Félix Anthonysamy**, stagiaire, pour leur aimable et substantielle contribution.

Concept de couverture : **Félix Anthonysamy** © IDN 2021.