



LES NOUVELLES TECHNOLOGIES ET LA STRATÉGIE NUCLÉAIRE

INITIATIVES POUR LE DÉSARMEMENT NUCLÉAIRE



IDN
Initiatives pour le
désarmement nucléaire.

LES MISSILES HYPERSONIQUES

IDN-INITIATIVES POUR LE DÉSARMEMENT NUCLÉAIRE



DARPA Falcon HTV-2

Planeur hypersonique

Mach 20



Zircon 3M22

Missile de croisière hypersonique

Mach 5

2 Ils volent dans l'espace proche, **en dessous de 100km**. L'oxygène y étant rare, ils se propulsent à l'aide d'un **superstatoréacteur à combustion supersonique**



Mach 5 (6500 km/h) à
Mach 20 (24 696 km/h)

3 Ce qui les différencie des missiles balistiques : **la manoeuvrabilité**. Leur trajectoire **peut être changée en cours de vol** à haute vitesse, les rendant **difficiles à repérer et arrêter**.



1 Les missiles hypersoniques peuvent être lancés depuis **le sol, la mer ou les airs**

4 Certains missiles ont recours à la technologie du **glide vehicle (planeur)** pour faciliter **la précision** à haute vitesse et manoeuvrabilité

5 Peuvent délivrer des charges conventionnelles ou nucléaires **N'IMPORTE OÙ DANS LE MONDE EN UNE HEURE**



Ils volent assez haut pour être hors de portée des missiles sol-air et assez bas pour échapper aux systèmes extra-atmosphériques, rendant ainsi caducs les systèmes de défense. Cela favorise une dangereuse course aux armements, centrée sur l'offensive. Leur vitesse **réduit considérablement la fenêtre de réaction et augmente les risques d'escalade**.

LES ARMES À ÉNERGIE DIRIGÉE

INITIATIVES POUR LE DÉSARMEMENT NUCLÉAIRE

Le laser : **versatile** mais encore en **expérimentation**

MEILLEURE MAÎTRISE DES FORCES NUCLÉAIRES



Un faisceau laser concentré peut perforer la surface d'un missile, d'un avion ou d'un drone



PERMET DE SIMULER DES ESSAIS NUCLÉAIRES

- ✓ Fin des essais nucléaires en conditions réelles, dangereux pour la santé et l'environnement
- ✗ assure la pérennité de la dissuasion, en permettant de continuer les essais

Les armes lasers pourraient être intégrées dans des systèmes de défense antimissile, pour neutraliser des missiles de croisière, balistiques ou hypersoniques

La technologie laser permettrait d'améliorer la communication dans des **MILIEUX TURBULENTS** (espace, profondeurs marines) et entre des véhicules de surface, des sous-marins et des satellites

- 📡 TÉLÉMÉTRIE
- 🎯 AIDE AU TIR
- 💡 ÉBLOUISSEMENT

- ⚠️ **Limites**
- 🌊 Efficacité variable selon les conditions météo
- 💡 Coût énergétique élevé

Impulsion électromagnétique et chaos stratégique



Une attaque à impulsion électromagnétique peut être déclenchée par une **explosion nucléaire à haute altitude**, une **arme à micro-ondes**, ou une **bombe électronique «propre»**



Une IEM peut griller les **circuits électroniques et le réseau électrique** sur de vastes zones, d'un champ de bataille à des régions entières



Brouillage des télécommunications = **paralyse des centres de contrôle et de commandement**



Avions à mission nucléaire et satellites inutilisables

Une attaque à impulsion électronique ne ferait pas de victimes directes mais elle n'en aurait pas moins un impact dévastateur sur des infrastructures civiles et militaires vitales



IL NE S'AGIT PAS D'UNE ALTERNATIVE À LA DISSUASION NUCLÉAIRE : ELLE EN MODIFIE LES TERMES. AVEC UNE CAPACITÉ DE NEUTRALISATION SUPÉRIEURE, UNE PREMIÈRE FRAPPE DEVIENT PLUS TENTANTE.

Les armes à énergie dirigée s'inscrivent dans le champ de la **guerre électronique**. Elles vont introduire aussi bien des **moyens supplémentaires de protection** des forces nucléaires que de **nouvelles vulnérabilités**. Cela amènerait à une intégration plus poussée du conventionnel et du nucléaire, au risque de **brouiller la dissuasion** et d'**augmenter les risques de guerre**.

LA GUERRE DE L'ESPACE

INITIATIVES POUR LE DÉARMEMENT NUCLÉAIRE

L'espace : le champ de bataille du futur ?

Satellite espion/pirate



Peut espionner des points sensibles et neutraliser les autres satellites par des attaques cyber

Satellite brouilleur



Brouille les signaux GPS et les communications des autres satellites

Armes à énergie dirigée

Laser (terrestre ou embarqué sur un satellite), armes à impulsion électromagnétique, missiles antisatellites

Nanosatellites et "bouclier"

Ces petits satellites tenant dans le creux de la main sont envoyés par centaines voire par milliers pour former un essaim de détecteurs autonomes.

Missile cinétique antisatellite

Tiré depuis la surface ou les airs

Arme irresponsable qui crée des milliers de débris spatiaux dangereux pour les autres appareils



Traité sur l'Espace de 1967 : interdit les armes de destruction massive en orbite

MAIS N'INTERDIT PAS LA MILITARISATION DE L'ESPACE

L'espace et ses défis pour la stratégie nucléaire



Course aux armements spatiaux

Extrême dépendance des systèmes de contrôle, communications et commandement nucléaires aux satellites

Les essais de "nanosats" donnent lieu à une "guerre instantanée", capacité de déclencher un conflit d'envergure sans préavis ni signal faible d'alerte

UN SUBSTITUT À LA DISSUASION ? PEUT-ÊTRE. MAIS ELLE PEUT AUSSI PROVOQUER UNE ATTAQUE NUCLÉAIRE INSTANTANÉE

Le brouillard stratégique de l'espace rend difficile l'attribution d'intentions hostiles ou pacifiques



MILITAIRE/CIVIL

La dualité des acteurs empêche le contrôle des technologies



PUBLIC/PRIVÉ

Jouant déjà un rôle crucial pour les forces militaires, l'espace orbital pourrait bien lui-même devenir un théâtre d'affrontement d'ici peu. Les Etats s'y préparent, notamment en développant des capacités militaires "adaptées". Rappelons que ce qui se joue au-dessus de nos têtes a des conséquences ici-bas, notamment pour la stratégie et la sécurité nucléaire.

LA MENACE CYBER

INITIATIVES POUR LE DÉSARMEMENT NUCLÉAIRE

Les trois grandes cybermenaces sur le nucléaire



Cyberespionnage

Les opérations de cyberespionnage nucléaire visent généralement à récupérer du matériel scientifique et technique sur les essais nucléaires, des données de recherche et développement, des conceptions d'armes, des structures militaires, des doctrines qui sont stockées sur des réseaux.



Manipulation de l'information

Le « spoofing » désigne le fait de contaminer et manipuler l'information sur laquelle les décisions nucléaires sont fondées.

Il vise les systèmes d'information et d'alerte liés aux armes nucléaires, mais aussi les systèmes de commandement et de contrôle.

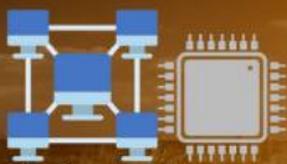
Le but est de remettre en cause la confiance dans ces systèmes, en multipliant par exemple les fausses alertes.



Cyber-handicap et destruction des systèmes d'armes nucléaires

Il s'agit de désactiver, perturber ou 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.

L'avènement du troisième âge nucléaire ?



Informatisation

Le recours à des systèmes informatiques de plus en plus complexes accroît les risques d'erreurs et d'accidents et les rend plus faciles à compromettre.

La dépendance de certains pays à des composants fabriqués à l'étranger présente également de grands risques.



Armes intelligentes et intelligence artificielle

Dissuasion par déni : recours aux capacités cybernétiques pour intercepter les missiles ou perturber les défenses antimissiles et les satellites. L'IA devrait approfondir ces vulnérabilités.

**AFFAIBLISSEMENT DE LA DISSUASION,
ÉTAT PERMANENT DE RIVALITÉ,
FAVORISE FRAPPES PRÉVENTIVES**

Recommandations



Education aux enjeux cyber, adoption de normes et seuils internationaux.



Réévaluation des doctrines avec le no-first use. Temps de décision allongé.



Garanties humaines face à l'intelligence artificielle.



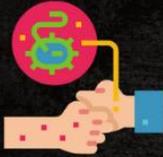
Renforcer la cyber-sécurité et la cyber-hygiène.

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. Elles pourraient mener à un "troisième âge nucléaire", en se combinant à d'autres technologies comme l'IA. Il est important d'établir des gardes-fous juridiques, doctrinaux et technologiques.

LES BIOTECHNOLOGIES

INITIATIVES POUR LE DÉSARMEMENT NUCLÉAIRE

LES CONTRAINTES LIÉES AUX ARMES BIOLOGIQUES



Contagion difficile à maîtriser, peut se retourner facilement contre l'utilisateur



Absence de précision et d'immédiateté



Peuvent être contrées par la découverte d'un vaccin ou d'un remède

FACE À CES DIFFICULTÉS, LA PLUPART DES ÉTATS ONT SIGNÉ LA CONVENTION SUR L'INTERDICTION DES ARMES BIOLOGIQUES

Les nouvelles technologies fragilisent le consensus contre les armes biologiques



Ciseaux CRISPR

Outil révolutionnaire qui rend la manipulation génétique beaucoup plus accessible et facile



Imprimante 3D

Permet de contourner les restrictions sur la vente ou l'importation de matériel médical ou militaire, en les créant sur demande



Intelligence artificielle

Pourrait permettre de mieux protéger les soldats face aux risques biologiques. Mais aussi de créer des agents biologiques plus virulents et cibler certaines parties de la population sur la base de leur patrimoine génétique



Robotique

La robotisation automatise la production et pourrait grandement favoriser la prolifération

On pourrait assister à la supplantation du risque nucléaire par le risque biologique



Guerre "chirurgicale": potentiel génocidaire

L'IA et les progrès de la génétique permettent de cibler une partie précise de la population avec un virus, pour éventuellement mener une "guerre raciste"



Prolifération et terrorisme

L'impression 3D pourrait par exemple permettre à des terroristes de créer des drones pour diffuser des agents pathogènes. Les restrictions pourraient aussi être contournées



Cybervulnérabilité

La numérisation des données sur les agents biologiques à potentiel militaire les rendent vulnérables au piratage par des acteurs malveillants



Fragilisation de la non-prolifération

La non-prolifération des armes de destruction massive repose sur le contrôle des États et une identification des menaces. Mais les progrès en biotechnologie remettent sérieusement en cause ce cadre ainsi que la dissuasion nucléaire, en permettant à des acteurs privés d'y avoir recours



Nouvelle arme de dissuasion ?

La fragilisation du consensus contre les armes biologiques et les progrès scientifiques risquent d'en faire les nouvelles armes de dissuasion

Un virus "dormant" pourrait être ainsi diffusé dans une population avant d'être "réveillé", pour déclencher le chaos dans le pays ciblé.

LES NANOTECHNOLOGIES

INITIATIVES POUR LE DÉSARMEMENT NUCLÉAIRE

Les multiples applications militaires des nanotechnologies



Un nanorobot se rapproche par sa taille de l'échelle atomique



Ils peuvent adapter les structures des matériaux à des échelles extrêmement petites pour obtenir des propriétés spécifiques (résistance, conductivité, légèreté, réactivité)



Meilleur stockage et analyse des data



Amélioration drastique des systèmes de détection et de surveillance



Amélioration des systèmes d'armes



Facilitent la création d'armes autonomes et intelligentes



Aide à la prise de décision tactique conjointement avec l'IA



Rentabilité

Les nanotechnologies pourraient bien révolutionner les armes nucléaires...



Bombe atomique de 4ème génération à micro-fusion

- Un peu moins puissante
- Moins de retombées radioactives
- Brouille la frontière entre nucléaire et conventionnel
- Ne franchit pas vraiment le seuil nucléaire, est plus dure à détecter
- Augmentation de la puissance de feu des États



Mini-bombes nucléaires

- Plus difficile à repérer (voire invisibles grâce aux nanosciences)
- Plus faciles à transporter et cacher
- Déclenchées grâce à un super laser
- Plus précises et offrent une meilleur information
- Danger : plus susceptibles au trafic
- Favoriserait la course aux armements (fabrication rapide et pas chère)



Les accélérateurs et détonateurs des armes nucléaires ont besoin de composants à la fois petits et résistants. Les nanotechnologies offrent une solution de choix.



Capacité de détection accrue

Nanobots 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

...mais aussi les rendre obsolètes et les dépasser en termes de capacités de destruction



Destruction de la biomasse

Des nano-systèmes ayant acquis la faculté de se répliquer pourraient produire une réaction en chaîne catastrophique. La biomasse et la civilisation seraient détruites en seulement quelques jours



Combinaison mortelle avec les biotechnologies

Des nano-armes ayant acquis la faculté de répliquer la vie au niveau moléculaire pourraient faciliter le développement de nouvelles armes biologiques plus meurtrières par des acteurs indépendants



Course aux armements exponentielle

Le pouvoir apocalyptique des nano-armes bouleverserait l'équilibre géostratégique dominé par les puissances nucléaires. On aurait une expansion de l'ordre de milliers, voir de millions de têtes pour y faire face

LA DISSUASION DEVIENDRAIT OBSOLÈTE ET UNE FRAPPE PRÉVENTIVE POURRAIT AVOIR LIEU CONTRE UN ETAT DÉVELOPPANT DE TELLES ARMES



Nécessité d'un traité d'encadrement

On ne peut pas demander l'interdiction des nanotechnologies puisqu'elles jouent déjà un rôle révolutionnaire et important dans plusieurs sphères civiles.

IL EST EN REVANCHE POSSIBLE - ET URGENT - D'ENCADRER STRICTEMENT LEUR USAGE MILITAIRE

LA MENACE CYBER

INITIATIVES POUR LE DÉSARMEMENT NUCLÉAIRE

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.

Cyberespionnage, "spoofing", sabotage : les trois grandes cybermenaces sur le nucléaire



Cyberespionnage

Les opérations de cyberespionnage nucléaire visent généralement à récupérer du matériel scientifique et technique sur les essais nucléaires, des données de recherche et développement, des conceptions d'armes, des structures militaires, des doctrines qui sont stockées sur des réseaux.



Manipulation de l'information

Le « spoofing » désigne le fait de contaminer et manipuler l'information sur laquelle les décisions nucléaires sont fondées

Il vise les systèmes d'information et d'alerte liés aux armes nucléaires, mais aussi les systèmes de commandement et de contrôle.

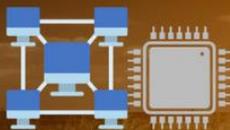
Le but est de remettre en cause la confiance dans ces systèmes, en multipliant par exemple les fausses alertes.



Cyber-handicap et destruction des systèmes d'armes nucléaires

Il s'agit de désactiver, perturber ou 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

Cybermenaces et "troisième âge nucléaire" : comment s'y préparer



Informatisation

Le recours à des systèmes informatiques de plus en plus complexes accroît les risques d'erreurs et d'accidents et les rend plus faciles à compromettre

La dépendance de certains pays à des composants fabriqués à l'étranger présente également de grands risques



Armes intelligentes et intelligence artificielle

Dissuasion par déni : recours aux capacités cybernétiques pour intercepter les missiles ou perturber les défenses antimissiles et les satellites. L'IA devrait approfondir ces vulnérabilités.

AFFAIBLISSEMENT DE LA DISSUASION, ÉTAT PERMANENT DE RIVALITÉ, FAVORISE FRAPPES PRÉVENTIVES

Recommandations



Education aux enjeux cyber, adoption de normes et seuils internationaux



Réévaluation des doctrines avec le no-first use. Temps de décision allongé



Garanties humaines face à l'intelligence artificielle.



Renforcer la cyber-sécurité et la cyber-hygiène

LA TECHNOLOGIE QUANTIQUE

INITIATIVES POUR LE DÉSARMEMENT NUCLÉAIRE

LA MÉCANIQUE QUANTIQUE : DEUX GRANDS PRINCIPES

SUPERPOSITION



Ordinateur quantique

Utilise des qubits (particules élémentaires) pour traiter plusieurs éléments **en même temps** grâce à la SUPERPOSITION = traitement ultra-rapide de larges quantités de données



Ordinateur classique

Doit traiter les solutions **les une à la suite des autres** jusqu'à ce qu'il trouve la bonne. Cela prends **beaucoup plus de temps** qu'avec le traitement quantique

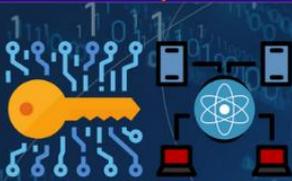
INTRICATION



Deux particules « intriquées » sont liées par leur état, quelque soit la distance qui les sépare. Tout changement d'état dans l'une entraîne un changement immédiat dans l'autre

Nombreuses applications en **cyberdéfense et surveillance**

La technologie quantique : un changement de paradigme dans la stratégie nucléaire...



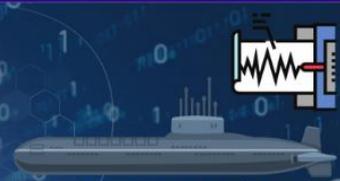
Clé quantique

Recours à l'intrication pour protéger les systèmes de communication notamment ceux impliqués dans le **lancement des armes nucléaires**. Une intrusion dans une partie du système se répercuterait à son ensemble. **Détection immédiate PROTECTION INVOLABLE**



Radars et détection d'avions furtifs

Les radars normaux **envoient des photons dans le ciel** pour détecter des avions. Les avions furtifs les réfléchissent pour rester invisibles. Cependant, les radars quantiques changent la donne. Ils utilisent eux aussi des photons, l'un dans l'appareil, l'autre dans le ciel. Si un avion furtif absorbe ce dernier, **il se retrouve ancré au radar** par intrication



Gravimètres, magnétomètres et sous-marins

Les gravimètres quantiques détectent les mouvements souterrains de matière, (ex : magma). Mais ils pourraient également détecter les sous-marins nucléaires **tapis au fond des océans et dont les trajectoires sont secret-défense**. Des magnétomètres peuvent de leur côté aider les sous-marins à naviguer sans GPS, grâce à un « **compas quantique** » embarqué, réduisant ainsi la vulnérabilité cyber

...qui pourrait précipiter un conflit par son efficacité



Cryptologie

L'informatique quantique pourrait dans le futur rendre caducs les systèmes protégeant la confidentialité des codes nucléaires et de la localisation des armes nucléaires



LES AVANCÉES DANS LE DOMAINE QUANTIQUE RISQUENT DE METTRE À NU **LES SECRETS NUCLÉAIRES**, VITAUX DANS LA LOGIQUE DE DISSUASION. UNE **PREMIÈRE FRAPPE** POURRAIT ALORS DEVENIR **PLUS TENTANTE**.



Capteurs quantiques

L'amélioration des capteurs par le quantique risque de rendre impossible la furtivité nécessaire des forces liées à la triade nucléaire (air, sol, mer). Remet en question la capacité de seconde frappe

L'INTELLIGENCE ARTIFICIELLE

IDN-INITIATIVES POUR LE DÉSARMEMENT NUCLÉAIRE

Les champs d'application multiples de l'IA créent un «brouillard de la guerre» égalisateur, qui efface les frontières



MILITAIRE/CIVIL



CONVENTIONNEL/NUCLÉAIRE



PUBLIC/PRIVÉ

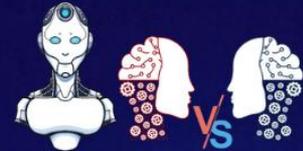
«Robots tueurs», automatisation, guerre de l'information : l'IA transforme la guerre...



AUTOMATISATION DU RECOURS À LA FORCE LÉTALE



DÉSINFORMATION PAR USURPATION D'IDENTITÉ (EX : DEEPPAKE)



AFFRONTEMENT DE SYSTÈMES AUTOMATISÉS + ROBOTISATION DES ARMÉES = ABAISSEMENT DU SEUIL DE CONFLIT.



RESPONSABILITÉ PLUS DIFFICILE À ÉTABLIR EN CAS D'ATTAQUES SUR DES CIVILS



PIRATAGE FACILITÉ



PROLIFÉRATION INCONTRÔLABLE DES ARMES LÉTHALES AUTONOMES

...et risque d'aggraver les risques liés au nucléaire



Efficacité accrue des armes conventionnelles = REMET EN CAUSE LA CAPACITÉ DE SECONDE FRAPPE NUCLÉAIRE



**EXCLUSION DE L'HOMME =
DÉSINHIBITION ET
AUTOMATISATION
DE L'ENGAGEMENT
NUCLÉAIRE**



IA augmente la vulnérabilité de la chaîne de commandement et de contrôle face aux cyberattaques



Relance de la course aux armements pour retrouver la capacité de seconde frappe



Imprévisibilité de la menace affaiblit la dissuasion nucléaire MAIS AUGMENTE LE RISQUE DE TIR PRÉVENTIF