UNIDIR

Funded by
the European Union

RAPPORT COMPLET

Technologies habilitantes et sécurité internationale : Compendium

Édition 2023

WENTING HE

Remerciements

L'ensemble des activités de l'UNIDIR reposent sur le soutien apporté par les principaux bailleurs de fonds de l'Institut. Cette publication a été financée par l'Union européenne dans le cadre du Programme sécurité et technologie de l'UNIDIR, soutenu par les gouvernements de l'Allemagne, de l'Italie, des Pays-Bas, de la République tchèque, de la Suisse et de la Norvège, ainsi que par Microsoft.

L'auteure exprime sa sincère gratitude à M. Giacomo Persi Paoli pour ses conseils précieux et ses contributions perspicaces tout au long du processus de rédaction. Des remerciements particuliers sont également adressés à Elia Duran-Smith pour son aide dans la recherche documentaire. En outre, l'auteure souhaite remercier James Black et Sarah Grand-Clément pour leur relecture approfondie et leurs commentaires constructifs, qui ont grandement enrichi le travail final.

À propos de l'UNIDIR

L'Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR) est un institut autonome au sein des Nations Unies financé par des contributions volontaires. L'UNIDIR est l'un des rares instituts politiques du monde à se concentrer sur le désarmement. Il génère des connaissances et encourage le dialogue et l'action en matière de désarmement et de sécurité. Basé à Genève, l'UNIDIR aide la communauté internationale à développer les idées pratiques et innovantes nécessaires pour trouver des solutions aux problèmes de sécurité les plus graves.

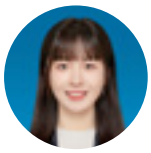
Remarque

Les désignations employées dans la présente publication et la présentation des données qui y figurent n'impliquent, de la part du Secrétariat de l'Organisation des Nations Unies, aucune prise de position quant au statut juridique de tel ou tel pays, territoire, ville ou zone, ou de ses autorités, ni quant au tracé de ses frontières ou limites. Les points de vue exprimés dans la présente publication n'engagent que leur auteure. Ils ne reflètent pas nécessairement ceux des Nations Unies, de l'UNIDIR ou de l'Union européenne, de leur personnel ou des organismes qui lui apportent leur concours.

Pour citer cette publication

He, Wenting. " Technologies habilitantes et sécurité internationale : compendium (édition 2023) ". Genève, Suisse : UNIDIR, 2024.

Author



Wenting He

Chercheuse associée, Programme sécurité et technologie

Wenting He est chercheuse associée au sein du Programme sécurité et technologie de l'UNIDIR. Elle est titulaire d'un master en affaires interna-tionales de l'Institut de hautes études internationales et du développe-ment, à Genève, et d'une licence en diplomatie de l'Université des affaires étrangères de Chine, à Pékin.

Abréviations et acronymes

5G	Réseaux de téléphonie mobile de cinquième génération
6G	Réseaux de téléphonie mobile de sixième génération
IA	Intelligence artificielle
AIAAS	Intelligence artificielle en tant que service
RA	Réalité augmentée
AWS	Amazon Web Services
CPU	Unité centrale de traitement
CSP	Fournisseur de services en nuage
DOD	Département de la Défense des États-Unis
EUV	Ultraviolet extrême
GNSS	Système global de positionnement par satellites
GPU	Unité de traitement graphique
HTS	Supraconducteurs à haute température
IAAS	Infrastructure en tant que service
CICR	Comité international de la Croix-Rouge
TIC	Technologies de l'information et des communications
IOMT	Internet des objets militaires
IOT	Internet des objets
ISR	Renseignement, surveillance et reconnaissance
JWCC	Capacité en nuage de combat interarmées
OTB	Orbite terrestre basse
IRM	Imagerie par résonance magnétique
NEMS	Nanosystèmes électromécaniques
NM	Nanomètre
NPU	Unités de traitement neuronal
PAAS	Plateforme en tant que service
PQC	Cryptographie post-quantique
QKD	Distribution quantique de clé
SAAS	Logiciel en tant que service
SOC	Système sur une puce
TPU	Unité de traitement de tenseur
TSMC	Taiwan Semiconductor Manufacturing Company
UAV	Véhicule aérien téléguidé
RV	Réalité virtuelle

Table des matières

Résumé exécutif

Les avancées technologiques dans des domaines tels que les matériaux avancés, les micropuces, les capteurs et l'infrastructure de connectivité favorisent l'innovation dans d'autres domaines technologiques, notamment les technologies de l'information et de la communication (TIC), l'intelligence artificielle (IA) et les systèmes autonomes. Ces technologies habilitantes redessinent le paysage numérique et ont des applications potentielles dans le domaine militaire. Si des progrès ont été accomplis dans la prise en compte des implications des TIC et de l'IA pour la sécurité dans le cadre de divers processus intergouvernementaux, les technologies sous-jacentes qui facilitent ou stimulent leur développement ont fait l'objet d'une attention relativement moindre. Cela souligne l'urgence d'un examen plus approfondi et plus complet des technologies habilitantes ainsi que de leurs incidences potentielles sur la sécurité internationale.

Pour combler cette lacune, ce compendium est consacré à l'identification et à l'analyse des avancées les plus marquantes en matière de technologies habilitantes, en mettant particulièrement l'accent sur celles qui en sont encore à leurs premiers stades de développement ou d'application. Le compendium explore quatre catégories de technologies habilitantes : les matériaux avancés (semi-conducteurs, supraconducteurs et nanotechnologies), les pièces et composants (micropuces et capteurs), le traitement et l'informatique (informatique en nuage, informatique en périphérie et informatique quantique), et l'infrastructure (télécommunications de cinquième et sixième générations [5G et 6G], Internet des objets, l'infrastructure en nuage et les communications par satellite).

Le compendium met en évidence plusieurs tendances et évolutions générales dans les domaines technologiques examinés. La tendance actuelle à la miniaturisation du matériel conduit à la création d'appareils de plus en plus compacts et efficaces, ce qui facilite l'intégration généralisée des technologies habilitantes dans les systèmes militaires. Ces technologies permettent d'améliorer considérablement les capacités militaires et de renforcer les efforts internationaux en matière de sécurité. Toutefois, des problèmes se posent en raison de la possibilité d'une concurrence technologique accrue entre les États et des risques et vulnérabilités en matière de cybersécurité dans la chaîne d'approvisionnement mondiale, associés aux technologies habilitantes. Si le rôle du secteur privé est crucial, la collaboration en matière de technologies à double usage peut présenter de nouveaux risques, tels que la mise en péril d'informations militaires sensibles.

Le suivi et l'analyse continus des tendances émergentes sont donc essentiels pour établir des cadres de gouvernance efficaces qui équilibrent les opportunités et les risques que présentent les technologies habilitantes.

1. Introduction

Les technologies telles que les matériaux avancés, les micropuces et les capteurs, la puissance de calcul et l'infrastructure de connectivité permettent ou stimulent l'innovation et le développement de capacités dans d'autres domaines technologiques, notamment les technologies de l'information et de la communication (TIC), l'intelligence artificielle (IA) et les systèmes autonomes. Le développement de technologies habilitantes révolutionne l'écosystème numérique, élargissant les possibilités de développement et d'application à des fins militaires.[1] À mesure que ces technologies progressent, il devient de plus en plus important de se pencher sur leurs implications pour la paix et la sécurité internationales. Une analyse prospective permanente est essentielle pour exploiter les avantages de ces technologies tout en atténuant leurs risques potentiels.

Dans le rapport 2023 intitulé " Current developments in science and technology and their potential impact on international security and disarmament efforts " (Développements actuels dans le domaine de la science et de la technologie et leur impact potentiel sur la sécurité internationale et les efforts de désarmement), le Secrétaire général des Nations Unies souligne les préoccupations persistantes selon lesquelles les progrès scientifiques et technologiques en matière de sécurité et de désarmement dépassent la capacité des cadres normatifs et de gouvernance à gérer les risques.[2] Si divers processus intergouvernementaux ont permis de progresser dans la prise en compte des implications des TIC et de l'IA en matière de sécurité, les technologies sous-jacentes qui permettent ou favorisent leur développement ont fait l'objet d'une attention relativement moindre. Cela souligne l'urgence d'un examen plus approfondi et plus complet des technologies habilitantes ainsi que de leurs incidences potentielles sur la sécurité internationale.

Afin de combler cette lacune, le présent compendium est consacré à l'identification et à l'analyse des avancées les plus marquantes en matière de technologies habilitantes. Il s'agit notamment de celles qui en sont encore aux premiers stades de leur développement ou de leur application, mais qui devraient avoir un impact important sur la paix et la sécurité internationales. Ce compendium se concentre exclusivement sur l'exploration des effets directs des technologies habilitantes sur l'écosystème numérique, en particulier en ce qui concerne la paix et la sécurité internationales. Toutefois, certains domaines technologiques peuvent avoir des implications plus larges que celles couvertes par le présent rapport.

Dans les chapitres suivants, le compendium se penche sur quatre catégories de technologies habilitantes. La catégorie I comprend les matériaux avancés, tels que les semi-conducteurs, les supraconducteurs et les nanotechnologies. La catégorie II s'intéresse aux pièces et aux composants, y compris les micropuces et les capteurs. La catégorie III couvre le traitement et l'informatique, c'est-à-dire l'informatique en nuage, l'informatique en périphérie et l'informatique quantique. La catégorie IV concerne les infrastructures, des télécommunications de cinquième et sixième génération

---

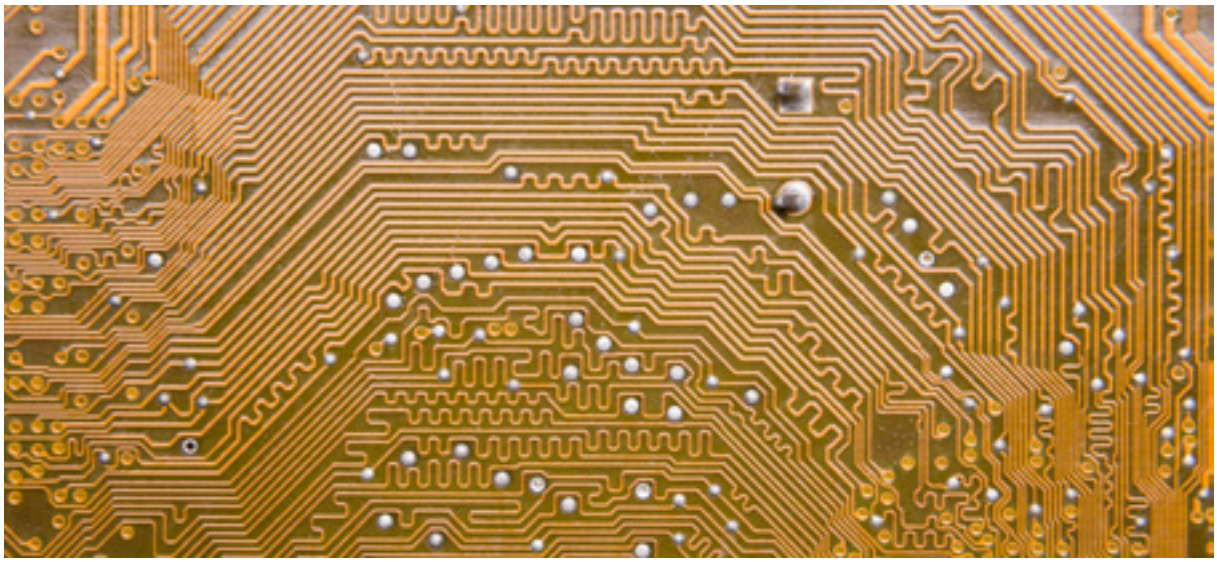
1 Aux fins du présent compendium, les technologies habilitantes sont définies comme celles qui permettent ou stimulent l'innovation et le développement de capacités dans d'autres domaines technologiques relevant du programme Sécurité et technologie de l'UNIDIR : cybernétique, IA et autonomie, ainsi que l'intégration des systèmes.

2 Assemblée générale des Nations Unies (2023).

(5G et 6G) aux communications par satellite, en passant par l'Internet des objets (IoT) et l'infrastructure en nuage. Chaque chapitre présente une analyse complète de la technologie examinée, y compris les derniers développements et les applications militaires pertinentes, suivie d'une évaluation des implications potentielles pour la sécurité internationale. Le compendium se termine par un examen général des tendances et des développements dans le domaine des technologies habilitantes.

2. Catégorie I : matériaux avancés

2.1. Semi-conducteurs



Les **semi-conducteurs** appartiennent à une catégorie de matériaux caractérisés par des propriétés de conductivité électrique qui se situent entre celles des conducteurs (par exemple, les métaux) et des isolants (par exemple, le verre). La conductivité électrique d'un semi-conducteur peut être contrôlée et modifiée, ce qui lui permet de servir d'élément de base pour les dispositifs et composants électroniques modernes, notamment les diodes, les transistors et les circuits intégrés.

Les propriétés électriques uniques des semi-conducteurs ont transformé le paysage technologique, conduisant au développement d'appareils et de systèmes électroniques de plus en plus compacts, puissants et économes en énergie. Dans l'industrie électronique, le silicium est le matériau semi-conducteur le plus couramment utilisé, mais d'autres matériaux tels que l'arséniure de gallium et le germanium sont également utilisés dans des applications spécialisées. Les plaquettes de silicium servent souvent de base à la fabrication des micropuces et jouent un rôle essentiel dans le fonctionnement des technologies numériques.

Le nœud de traitement des semi-conducteurs, désormais souvent mesuré en nanomètres (nm),[3] est un facteur critique dans la technologie des semi-conducteurs. La compression des nœuds de traitement permet de monter un plus grand nombre de transistors sur une seule puce, ce qui améliore souvent les performances et l'efficacité énergétique. La taille

[3] Un nanomètre équivaut à un millième de micromètre ou à un milliardième de mètre.

des nœuds des semi-conducteurs s'est considérablement réduite au cours des décennies, depuis la mesure initiale en micromètres (µm)[4] jusqu'au niveau actuel, le plus avancé, de la technologie à 3 nm.[5] Taiwan Semiconductor Manufacturing Company (TSMC), l'un des fabricants de semi-conducteurs les plus perfectionnés, prévoit de produire la prochaine génération de semi-conducteurs à 2 nm à partir de 2025. Cette technologie devrait permettre d'atteindre des vitesses de traitement supérieures de 10 à 15 % à celles des puces à 3 nm.[6]

La force motrice de l'évolution du nœud du processus est ce que l'on appelle la loi de Moore. Il s'agit d'une observation empirique de Gordon Moore, l'un des cofondateurs d'Intel, selon laquelle le nombre de transistors sur une puce électronique a historiquement eu tendance à doubler tous les deux ans environ. La loi prévoit donc que les performances informatiques continueront à augmenter tandis que le coût des ordinateurs diminuera. Bien que la théorie se soit largement maintenue au XXIe siècle, les ingénieurs ont commencé à atteindre les limites des matériaux semi-conducteurs traditionnels dans le cadre de la compréhension actuelle des lois de la physique. C'est pourquoi certains observateurs ont même proclamé la fin de la loi de Moore.[7] L'industrie est maintenant à la recherche de solutions innovantes pour poursuivre les améliorations futures des semi-conducteurs.

D'autres matériaux ont été identifiés comme des alternatives potentielles au silicium pour répondre à la demande croissante de puissance de calcul. Les semi-conducteurs composés, par exemple, combinent plusieurs éléments pour produire des matériaux capables de surpasser le silicium. Ces matériaux sont appelés à jouer un rôle central dans le développement des nouvelles technologies de connectivité et des véhicules autonomes.[8] L'arséniure de gallium, le deuxième matériau semi-conducteur le plus utilisé après le silicium, est un composé connu pour sa mobilité électronique supérieure, ce qui lui confère une plus grande efficacité que le silicium. Il présente également une plus grande tolérance à la surchauffe. Toutefois, la production à grande échelle d'arséniure de gallium devra relever des défis importants, notamment celui de la dépendance à l'égard de produits chimiques toxiques, ce qui soulève des inquiétudes quant à l'impact sur la santé publique et l'environnement.[9]

Les efforts de recherche en cours explorent de nouveaux matériaux qui présentent un potentiel significatif pour le développement de dispositifs de plus en plus compacts et efficaces. Des études récentes ont démontré l'efficacité d'un matériau connu sous le nom d'arséniure de bore cubique pour résoudre certains problèmes posés par les semi-conducteurs traditionnels à base de silicium, avec le potentiel de devenir " le meilleur matériau

---

4 Par exemple, le processeur 4004 d'Intel lancé en 1971 : **https://www.intel.com/content/www/us/en/history/museum-story-of-intel-4004.html**

5 À partir de septembre 2023, seules deux entreprises dans le monde sont en mesure de fabriquer des semi-conducteurs à 3 nm : TSMC (**https://www.tsmc.com/english/dedicatedFoundry/technology/logic/l_3nm**) et Samsung (**https://news.samsung.com/global/samsung-begins-chip-production-using-3nm-process-technology-with-gaa-architecture**).

6 Ryugen, Hideaki (2023).

7 Arcuri et Shivakumar (2022).

8 IEEE (s.d.-a).

9 IEEE (s.d.-b).

semi-conducteur jamais découvert ".[10] Malgré ses propriétés prometteuses, l'arséniure de bore cubique est actuellement en phase expérimentale, et ses applications réelles restent encore à déterminer. Parallèlement, d'autres matériaux semi-conducteurs émergents gagnent également du terrain, notamment le nitrure de gallium haute puissance, les matériaux à base d'antimoniure et de bismuthure, ainsi que les matériaux bidimensionnels (2D) tels que le graphène.[11] Ces matériaux présentent des propriétés physiques distinctes qui se sont avérées avantageuses dans des applications spécifiques. Néanmoins, leur utilisation généralisée est entravée par leur coût et la complexité de leur production.

L'innovation continue dans le domaine des matériaux semi-conducteurs jouera un rôle essentiel dans les futurs systèmes militaires. Les semi-conducteurs sont utilisés concrètement dans toute une série de composants essentiels des appareils électroniques, allant des capteurs, des actionneurs et des puces mémoire aux systèmes électro-optiques et aux microcontrôleurs.[12] Ces semi-conducteurs constituent le pilier des dispositifs électroniques de pointe qui occupent le premier plan dans les systèmes militaires sophistiqués, notamment les dispositifs de communication à grande vitesse, les systèmes de radars et les armes à guidage de précision. En outre, la technologie des semi-conducteurs sert de catalyseur à des innovations transformatrices telles que l'intelligence artificielle et l'Internet des objets (IoT). L'émergence de nouveaux matériaux semi-conducteurs est donc susceptible de renforcer les capacités de défense nationale, mais aussi d'ouvrir une nouvelle ère de concurrence technologique entre les États.

---

10 Chandler (2022).

11 IEEE (s.d.-b).

12 Gargeyas (2022).

En outre, les vulnérabilités de la chaîne d'approvisionnement constituent actuellement un défi majeur. La chaîne d'approvisionnement en semi-conducteurs est un réseau mondial très complexe et interconnecté qui implique plusieurs étapes de production et des entreprises de différentes régions. Elle se caractérise également par un degré élevé de spécialisation, avec, par exemple, une concentration d'installations de production de semi-conducteurs de pointe en Asie de l'Est. Toute perturbation des capacités de production dans la région, qu'elle soit due à des tensions géopolitiques ou à des catastrophes naturelles, pourrait avoir un impact négatif sur la disponibilité des semi-conducteurs et de graves conséquences pour la sécurité nationale. Toutefois, le développement de matériaux semi-conducteurs alternatifs pourrait modifier le paradigme actuel et accroître la diversification au sein de la chaîne d'approvisionnement mondiale.

Semi-conducteurs : les faits marquants en 2023

- Des progrès constants sont en cours pour créer des semi-conducteurs plus compacts et plus efficaces. Les principaux fabricants de semi-conducteurs, tels que **TSMC** et **Samsung**, poursuivent activement le développement de la technologie de semi-conducteurs à 2 nm de prochaine génération, qui devrait permettre d'augmenter les vitesses de traitement de 10 à 15 % par rapport aux semi-conducteurs à 3 nm, actuellement les plus avancés.
- Le silicium reste le matériau semi-conducteur le plus couramment utilisé, mais il approche de ses limites physiques. Les efforts de recherche en cours portent sur de nouveaux matériaux semi-conducteurs susceptibles d'améliorer les performances, notamment l'**arséniure de bore cubique** et les **matériaux 2D**.
- La chaîne d'approvisionnement en semi-conducteurs est vulnérable aux perturbations en raison de sa nature complexe et interconnectée, ce qui peut représenter un défi important pour la sécurité nationale. Cependant, l'exploration de matériaux semi-conducteurs alternatifs pourrait potentiellement renforcer la diversification de la chaîne d'approvisionnement mondiale.

2.2. Les supraconducteurs

Les **supraconducteurs** sont des matériaux qui peuvent conduire l'électricité sans résistance ni perte d'énergie et repousser les champs magnétiques lorsqu'ils sont refroidis en dessous d'une température critique spécifique. Cette propriété unique permet à un courant électrique de circuler indéfiniment à l'intérieur d'un supraconducteur.

Les caractéristiques électromagnétiques exceptionnelles des supraconducteurs peuvent améliorer divers domaines, notamment l'électronique, l'informatique quantique, la transmission et le stockage de l'énergie et la technologie d'imagerie par résonance magnétique (IRM). Toutefois, leur utilisation pratique est pour l'instant limitée par l'exigence de températures extrêmement basses, ce qui nécessite une ingénierie cryogénique coûteuse et une forte consommation d'énergie pour le processus de refroidissement. La plupart des matériaux supraconducteurs présentent des températures critiques comprises entre le zéro absolu et 10 kelvins (environ -273 à -263 degrés Celsius).[13] Par conséquent, l'application à grande échelle des supraconducteurs est actuellement hors de portée.

La recherche sur les supraconducteurs est principalement axée sur la découverte de matériaux présentant des températures critiques nettement plus élevées. Des supraconducteurs à haute température (HTS) ont

[13] NCCR (2021). La température critique est la température à laquelle la résistance électrique d'un supraconducteur tombe à zéro.

été découverts, présentant une supraconductivité à des températures plus élevées que les matériaux conventionnels. Bien qu'ils soient appelés " haute température ", les HTS font référence à des matériaux dont la conductivité est supérieure à 77 kelvins (-196,2 degrés Celsius), le point d'ébullition de l'azote liquide.[14] Ces dernières années, la communauté scientifique s'est de plus en plus attachée à repousser les limites en s'efforçant de développer la supraconductivité à température ambiante. Bien que ces recherches soient en cours, aucune avancée n'a été réalisée jusqu'à présent.

La recherche et le développement futurs pourraient réduire efficacement les coûts opérationnels et rendre la technologie des supraconducteurs plus accessible pour des applications pratiques. L'utilisation de supraconducteurs avancés dans le domaine militaire devrait entraîner une véritable transformation. La mise au point de matériaux supraconducteurs évolutifs à température ambiante pourrait révolutionner le domaine de l'électronique et déboucher sur des applications prometteuses telles que des puces informatiques ultrarapides et économes en énergie, des communications sans fil à large bande et à faible latence, et des réseaux électriques très efficaces.[15] En outre, les supraconducteurs peuvent être utilisés pour construire des qubits (les unités de base des processeurs quantiques), ce qui offre de vastes possibilités pour l'informatique quantique.[16] De nouveaux matériaux supraconducteurs sont en cours de développement pour générer des qubits résistants aux perturbations externes, une caractéristique qui pourrait rendre les ordinateurs quantiques beaucoup plus fiables.[17] Néanmoins, l'émergence des supraconducteurs à température ambiante pourrait alimenter une nouvelle compétition technologique entre les États, susceptible de déboucher sur des litiges internationaux concernant les brevets, les transferts de technologie et l'accès au marché.[18]

Les supraconducteurs : les faits marquants en 2023

- L'application pratique des supraconducteurs est actuellement entravée par la nécessité d'atteindre des températures extrêmement basses, ce qui implique une ingénierie cryogénique coûteuse et une forte consommation d'énergie. Les scientifiques s'efforcent de parvenir à la supraconductivité à température ambiante.
- La mise au point de supraconducteurs évolutifs à température ambiante promet de révolutionner le domaine de l'électronique, mais leur apparition risque d'entraîner des **conflits internationaux** concernant les brevets, les transferts de technologie et l'accès au marché.

---

14 Clynes (2023).

15 Pedram (2023).

16 Pour une analyse détaillée de l'informatique quantique et des derniers progrès réalisés, voir la section 4.3 ci-dessous.

17 Feldman (2023).

18 Roa (2023).

2.3. Nanotechnologies

Les **nanotechnologies** contribuent à la conception, à la fabrication et à l'application de matériaux à l'échelle nanométrique, généralement de 1 à 100 nanomètres (un nanomètre est un milliardième de mètre).

À l'échelle nanométrique, des propriétés uniques et souvent inédites apparaissent en raison des effets quantiques et du comportement de la surface.[19] Ces propriétés peuvent être exploitées pour diverses applications, notamment dans les nanomatériaux et la nanoélectronique. Dans l'électronique moderne, la tendance actuelle à la miniaturisation des dispositifs est considérablement facilitée par les progrès des nanosystèmes électromécaniques (NEMS). Ces systèmes peuvent être utilisés pour créer des capteurs, des actionneurs et d'autres dispositifs plus petits et plus efficaces, avec des applications essentielles dans les domaines de la détection, de l'informatique et des communications avancées.

Dans les applications de détection, les nanotechnologies sont utilisées pour la surveillance environnementale de la qualité de l'air et de l'eau, ainsi que pour la détection des polluants. L'intégration des nanotechnologies permet de fabriquer des capteurs plus petits et plus sensibles pour les opérations militaires sur le terrain qui peuvent, par exemple, détecter des agents de menace biologique et chimique. Par rapport aux méthodes conventionnelles de détection des menaces biologiques, les biocapteurs à base de nanomatériaux peuvent atteindre une sensibilité et une précision plus élevées, même avec un volume d'échantillon, un temps de préparation et des coûts

19 Bureau national de coordination des nanotechnologies des États-Unis (s.d.).

d'analyse réduits.[20] Les nanocapteurs peuvent être utilisés pour fournir des informations en temps réel sur les menaces potentielles pour les opérations militaires, améliorant ainsi la connaissance de la situation sur le champ de bataille. Ils pourraient également profiter aux efforts de vérification du désarmement dans les domaines des armes biologiques et chimiques.

Dans le domaine de l'informatique, les nanotechnologies ouvrent la voie à l'informatique de nouvelle génération en facilitant le développement de nanomatériaux tels que les nanotubes de carbone, le graphène et les boîtes quantiques. La technologie conventionnelle du silicium approchant de ses limites physiques, l'intérêt pour les matériaux et approches alternatifs en vue de nouveaux paradigmes informatiques s'est accru. Ces dernières années, les chercheurs ont identifié les nanotubes de carbone comme une alternative intéressante pour remplacer le silicium dans la fabrication des transistors.[21] L'utilisation de ce nanomatériau hautement conducteur peut faciliter la création de transistors plus compacts et plus efficaces, capables de surpasser les transistors à base de silicium.[22] Toutefois, leur avantage dans les applications réelles n'a pas encore été prouvé de manière concluante.[23] En outre, les boîtes quantiques (c'est-à-dire des cristaux à l'échelle nanométrique synthétisés par le processus de nanofabrication) peuvent potentiellement révolutionner le domaine de l'informatique quantique. En raison de leurs propriétés quantiques, les boîtes quantiques peuvent être utilisées comme des qubits qui constituent la base même des ordinateurs quantiques, permettant la structure d'une machine de travail évolutive, rentable et tolérante aux pannes. [24] Cependant, la technologie n'en est qu'à ses débuts et plusieurs obstacles techniques et commerciaux doivent être surmontés avant de parvenir à une production pratique et à grande échelle d'ordinateurs quantiques.[25]

En outre, les nanotechnologies peuvent faciliter les communications avancées pour les opérations militaires, en offrant de multiples avantages, notamment une moindre consommation d'énergie, des dispositifs de communication miniaturisés et une meilleure connectivité. Dans les systèmes de communication sans fil, le développement des nanotechnologies permet d'obtenir des capteurs sans fil plus petits, moins chers, moins énergivores et plus efficaces, et rend possibles les réseaux 5G.[26] Les nanomatériaux peuvent également être utilisés pour créer des antennes très efficaces qui permettent d'améliorer l'efficacité et la fiabilité du signal. Par exemple, des antennes à l'échelle nanométrique ont été mises au point par des chercheurs pour permettre le transfert de données à la vitesse de la lumière entre différents processeurs centraux avec peu de pertes.[27]

Si les nanotechnologies sont très prometteuses pour l'amélioration des systèmes d'information et de communication militaires, leur développement et leur déploiement s'accompagnent également de certains risques. Des études ont montré que les nanoparticules

---

20 Rowland et al. (2016).

21 Fadelli (2023).

22 Basheer et al. (2022).

23 Fadelli (2023).

24 Hecht (2022).

25 Pour une analyse détaillée de l'informatique quantique et des derniers progrès réalisés, voir la section 4.3 ci-dessous.

26 Hamza et Jaafar (2022).

27 Kullock et al. (2020).

peuvent présenter un large éventail de toxicité et de risques pour l'environnement, ce qui constitue une menace importante pour la santé humaine et le bien-être écologique.[28] La taille et la composition des nanoparticules leur permettent de franchir les barrières physiologiques des organismes vivants et elles peuvent provoquer des réactions biologiques nocives dans le corps humain (par exemple, des inflammations pulmonaires et des problèmes cardiaques).[29] Les nanomatériaux produits par les processus de fabrication peuvent pénétrer dans l'environnement par des rejets délibérés ou accidentels. Une fois répandus dans le sol, ils ont le potentiel de le contaminer et de migrer ensuite dans les réseaux hydrographiques.[30]

Nanotechnologies : les faits marquants en 2023

- Les progrès constants dans le domaine des nanotechnologies permettent d'améliorer constamment la détection, l'informatique et les communications. Les nanomatériaux tels que les **nanotubes de carbone** et les **boîtes quantiques** ont le potentiel de stimuler l'informatique de prochaine génération, y compris le domaine émergent de l'informatique quantique. Toutefois, des difficultés persistent pour parvenir à une production pratique et à grande échelle.
- Les nanotechnologies offrent des avantages potentiels pour les systèmes d'information et de communication militaires, mais elles présentent également des risques. **La recherche** indique que les nanoparticules peuvent être toxiques et dangereuses pour l'environnement, et qu'elles constituent une menace importante pour la santé humaine et le bien-être écologique.

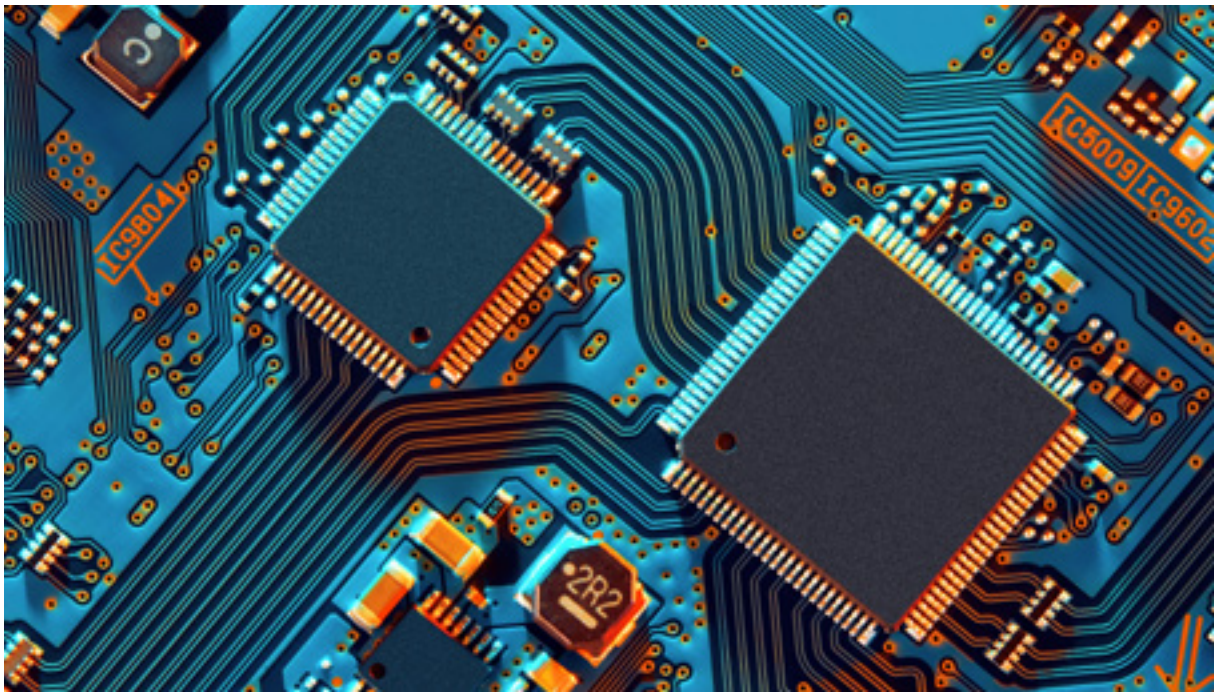
28 Kumah et al. (2023).

29 Ibid.

30 Ray, Paresh et al. (2009).

3. Catégorie II : pièces et composants

3.1. Micropuces



Les **micropuces** ou puces électroniques, également connues sous le nom de circuits intégrés, sont des assemblages compacts de composants électroniques miniaturisés, notamment des transistors, des diodes et des résistances, sur un petit morceau plat de matériau semi-conducteur, généralement une plaquette de silicium.

On ne saurait trop insister sur l'importance de la technologie des micropuces. Elle constitue la pierre angulaire des systèmes électroniques et informatiques modernes, créant des appareils non seulement plus petits, mais aussi plus puissants, plus rentables et plus économes en énergie que ceux construits à partir de composants discrets. Les micropuces peuvent remplir diverses fonctions essentielles, notamment le traitement de l'information, le stockage des données et l'exécution d'instructions, et elles peuvent être utilisées comme puces de mémoire, unités centrales de traitement (CPU) et unités de traitement graphique (GPU).

Les micropuces sont en constante évolution, les progrès réalisés dans le domaine des matériaux semi-conducteurs permettant

d'offrir de nouvelles fonctionnalités et des performances accrues à moindre coût.[31] Comme décrit ci-dessus, l'industrie des semi-conducteurs continue de repousser les limites de la miniaturisation pour développer des transistors avec des nœuds de processus plus petits. La miniaturisation permet d'intégrer davantage de transistors sur une seule puce, ce qui se traduit par une augmentation de la puissance de traitement et de l'efficacité énergétique. Toutefois, comme la technologie actuelle des semi-conducteurs à base de silicium approche progressivement de ses limites physiques, des matériaux et des approches alternatifs sont recherchés pour assurer la croissance et la transformation continues de la technologie des micropuces.

L'innovation dans ce domaine est également stimulée par l'amélioration de la conception des puces. D'autres méthodes de conception de puces ont été proposées, telles que les " systèmes multituiles " et la " conception basée sur les micropuces ".[32] Contrairement aux puces monolithiques traditionnelles, l'architecture multituiles consiste en un ensemble de puces spécialisées, telles que des puces mémoire et des unités centrales de traitement, qui peuvent être reliées pour créer un système sur une puce (SoC) complexe et intégré. La conception innovante de la puce serait capable de prendre en charge l'apprentissage automatique de l'IA à grande échelle, d'améliorer les rendements en silicium et de minimiser les déchets dans le processus de fabrication des puces.[33] Des entreprises telles qu'Apple, Google/Alphabet et Amazon Web Services (AWS) ont conçu des SoC personnalisés afin d'optimiser les performances des puces pour des applications et des charges de travail spécifiques – c'est ce que l'on appelle l'approche du " silicium personnalisé ".[34]

Des puces spécialisées sont en cours de conception pour permettre d'autres applications technologiques telles que la 5G et l'intelligence artificielle. La connectivité 5G nécessite le développement de micropuces avancées capables de répondre aux exigences de vitesse élevée et de faible latence de la technologie. Les capacités d'IA reposent également en grande partie sur la puissance de traitement des micropuces spécialisées telles que les unités de traitement de tenseur (TPU) et les unités de traitement neuronal (NPU). Les puces d'IA de pointe peuvent être des dizaines voire des milliers de fois plus rapides et plus efficaces que les puces à usage général telles que les unités centrales de traitement.[35]

En outre, la technologie de lithographie extrême ultraviolet (EUV) joue actuellement un rôle important dans la fabrication des micropuces les plus avancées au monde. Elle facilite la création de composants ultra-compacts et très précis sur des plaquettes de silicium et contribue à la miniaturisation continue des micropuces. Afin de poursuivre le processus de miniaturisation, une méthode plus complexe, connue sous le nom de lithographie EUV à haute ouverture numérique, a été identifiée par les chercheurs pour parvenir à la production de masse de la prochaine génération de technologie à nœud de 2 nm.[36] Les nouveaux systèmes de fabrication devraient être pleinement

---

31 Pour une analyse détaillée de la technologie des semi-conducteurs et des derniers progrès réalisés, voir la section 2.1 ci-dessus.

32 MIT Technology Review Insights (2023).

33 Ibid.

34 Shilov (2023).

35 Khan et Mann (2020).

36 IBM (2023).

opérationnels d'ici 2025.[37] En outre, les méthodes de mise en boîtier avancées continuent d'améliorer les performances et l'efficacité énergétique des micropuces, notamment les techniques d'empilage et de mise en boîtier en trois dimensions (3D) qui intègrent plusieurs puces dans une structure en 3D.[38]

Les nouveaux progrès de la technologie des micropuces continueront à façonner le paysage technologique dans les années à venir, avec des implications importantes pour la sécurité internationale. Le rôle omniprésent des systèmes électroniques dans la guerre moderne signifie que l'amélioration des performances des micropuces peut profiter à divers aspects des opérations militaires. Il s'agit notamment d'accroître la précision et l'efficacité des armes de pointe, de renforcer les capacités de renseignement, de surveillance et de reconnaissance (ISR), d'améliorer les systèmes de communication et de faciliter l'intégration de l'IA et de l'autonomie dans les systèmes militaires. Toutefois, cette technologie pose également de nouveaux défis en matière de sécurité. La chaîne d'approvisionnement des micropuces est extrêmement globale et complexe, depuis la conception et la fabrication des puces jusqu'à leur mise en boîtier, leur test et leur distribution. Les technologies et les capacités de production les plus avancées sont souvent concentrées dans certaines régions, ce qui crée des vulnérabilités potentielles au niveau de la chaîne d'approvisionnement. Par exemple, ASML, aux Pays-Bas, est actuellement la seule entreprise capable de fabriquer les machines de lithographie EUV utilisées pour la production à grande échelle des micropuces les plus avancées au monde.[39]

Un autre défi concerne la nature à double usage de la technologie et la prolifération potentielle. Les micropuces utilisées dans des applications civiles, telles que les smartphones et les ordinateurs portables, peuvent échapper aux règles de contrôle des exportations et donc être exploitées à des fins militaires ou intégrées dans des systèmes militaires.[40] L'utilisation des micropuces pose également des problèmes de cybersécurité. Les vulnérabilités matérielles sont difficiles à détecter en raison de la complexité de l'architecture des circuits intégrés. Les modifications physiques peuvent être efficacement dissimulées parmi la vaste gamme de composants et de fonctions valides et rester indétectables pendant longtemps.[41] Par rapport aux problèmes logiciels, les failles matérielles sont souvent beaucoup plus difficiles et coûteuses à corriger, ce qui ouvre une fenêtre de vulnérabilité et met en péril l'ensemble des systèmes numériques.[42]

---

37 ASML (s.d.).

38 Moore (2022).

39 ASML (s.d.).

40 Gilchrist (2023).

41 Levine et Pipikaite (2019).

42 Giles (2019).

Micropuces : les faits marquants en 2023

- Les progrès de la technologie des semi-conducteurs continuent d'accroître les performances et les fonctionnalités des micropuces à des coûts moindres grâce à la miniaturisation. L'exploration de matériaux et d'approches alternatifs pour les semi-conducteurs est susceptible de soutenir la croissance et la transformation de la technologie des micropuces.
- Les progrès dans ce domaine sont également dus à l'amélioration de la conception des puces et des techniques de production. Les conceptions de puces innovantes, telles que les " systèmes **multituiles** ", offrent des systèmes de puces intégrés complexes et peuvent prendre en charge l'apprentissage automatique de l'IA à grande échelle. Le développement en cours de la **lithographie EUV à haute ouverture numérique** vise à permettre la production de masse de la prochaine génération de technologies à nœuds de 2 nm d'ici 2025.
- Malgré les avantages potentiels de l'amélioration des performances des micropuces pour les opérations militaires, les défis comprennent les vulnérabilités de la chaîne d'approvisionnement, la nature à double usage de la technologie et les préoccupations en matière de cybersécurité.

3.2. Capteurs

Les **capteurs** sont des dispositifs conçus pour détecter des propriétés physiques et des conditions environnementales, puis pour convertir ces informations en signaux de sortie.

Les capteurs, qui englobent les capteurs de mouvement, les capteurs de proximité, les capteurs biométriques et les capteurs d'image, entre autres, ont un large éventail d'applications et de fonctionnalités. Ils sont devenus indispensables dans presque toutes les facettes des systèmes militaires, qu'il s'agisse de véhicules terrestres, de navires, de véhicules aériens téléguidés (UAV), de missiles ou de satellites. Les progrès de la technologie des capteurs jouent donc un rôle crucial dans la modernisation des capacités de défense, avec la possibilité d'améliorer l'efficacité globale des opérations militaires. Les applications des capteurs avancés peuvent apporter aux forces militaires une collecte de données plus précise et plus rapide, améliorer la connaissance de la situation et la protection sur le champ de bataille, perfectionner la précision du ciblage et la détection des menaces, et faciliter la prise de décision dans des environnements opérationnels dynamiques.

De nombreuses avancées ont été réalisées dans le domaine de la technologie des capteurs à des fins militaires. La fusion de capteurs représente un domaine clé de l'innovation. Les forces armées cherchent de plus en plus à combiner plusieurs sources de capteurs pour obtenir des informations plus précises et plus complètes sur le champ de bataille. Les systèmes multicapteurs intègrent et analysent des données provenant de divers types de capteurs (par exemple, des capteurs acoustiques, radars, électro-optiques et infrarouges), améliorant ainsi la connaissance de la situation à un niveau supérieur à celui qui peut normalement être atteint en analysant ces sources individuellement. Dans les véhicules militaires terrestres, la technologie de fusion de capteurs offre à l'équipage ou au

commandant une vue complète à 360 degrés de leur environnement et facilite l'échange d'informations avec d'autres systèmes.[43]

La détection quantique exploite la sensibilité inhérente des états quantiques aux perturbations, ce qui permet non seulement d'effectuer des mesures plus précises et plus sensibles, mais aussi de mesurer des phénomènes auparavant non mesurables. [44] La détection quantique a le potentiel de transformer les capacités militaires. Par exemple, des chercheurs ont mis au point des capteurs quantiques capables de détecter des objets dissimulés derrière des murs ou d'autres barrières, ce qui peut contribuer à des applications militaires telles que la reconnaissance.[45] En outre, la technologie de détection quantique pourrait améliorer la précision des systèmes de navigation inertielle utilisés dans les navires, les sous-marins et les avions. Cela permettrait d'améliorer considérablement les capacités de positionnement et de navigation dans les environnements dépourvus de GNSS.[46]

Les capteurs sont de plus en plus souvent intégrés à des technologies d'IA afin de fournir une collecte et une analyse intelligentes des données, améliorant ainsi l'efficacité de la prise de décision militaire. Les systèmes de radars cognitifs utilisent des capacités d'apprentissage automatique pour s'adapter aux changements dans l'environnement ou dans le comportement d'un adversaire.[47] En outre, des capteurs biométriques portables ont également été mis au point pour surveiller en temps réel les signes vitaux des soldats (par exemple, la fréquence cardiaque, la température corporelle et l'hydratation), ainsi que leur état mental, y compris la fatigue et le niveau de stress. L'intégration de l'IA dans les futurs systèmes sera essentielle pour accélérer le filtrage et l'interprétation des données collectées par les dispositifs portables des soldats.[48] Ce nouveau développement pourrait aider les commandants à prendre des décisions militaires et améliorer les performances du personnel militaire.

Outre le renforcement des capacités militaires, les progrès de la technologie des capteurs offrent de nouvelles possibilités pour la paix et la sécurité internationales. La technologie de la télédétection peut contribuer à la surveillance des conflits armés en cours et au respect des accords de paix.[49] L'utilisation de capteurs avancés améliore également l'efficacité de la détection des substances dangereuses, telles que les agents chimiques et biologiques, dans l'environnement. Ces applications peuvent faciliter la détection précoce des menaces, ce qui permet de réagir rapidement et de prendre des mesures d'atténuation, et elles peuvent renforcer les régimes de vérification du désarmement.

Cependant, l'utilisation de capteurs pose également un ensemble unique de défis qu'il convient de relever. Les capteurs, en particulier ceux qui participent au partage de données entre différents systèmes, reposent en grande partie sur des réseaux et sont donc susceptibles de subir des cyberattaques. Des acteurs malveillants peuvent tenter de perturber ou de manipuler les systèmes de capteurs,

---

43 Eshel (2022).

44 van Amerongen (2021).

45 Programme national britannique sur les technologies quantiques (s.d.).

46 Coggins et al. (s.d.).

47 Laboratoire des sciences et technologies de la défense du Royaume-Uni (2022).

48 Hamblen (2023).

49 Avtar et al. (2021).

compromettant ainsi l'intégrité des données et conduisant à une prise de décision erronée. Au fur et à mesure que la technologie progresse, les capteurs acquièrent la capacité de générer des volumes de données de plus en plus importants dans les systèmes, ce qui peut potentiellement entraîner des délais importants et affecter la qualité des données.[50] Cette situation peut entraver la prise de décision militaire si elle ne s'accompagne pas d'une amélioration de l'architecture du réseau. Enfin, en collectant et en stockant des informations concernant à la fois le personnel militaire et les civils, les applications de capteurs peuvent soulever des préoccupations valables concernant la vie privée et les pratiques de surveillance.

Capteurs : les faits marquants en 2023

- La fusion de capteurs, qui intègre des données provenant de diverses sources (capteurs acoustiques, radars et infrarouges, par exemple), offre une connaissance globale du champ de bataille.
- La détection quantique est prometteuse pour les applications militaires, car elle exploite la sensibilité des états quantiques aux perturbations, permet des mesures plus précises, la **détection d'objets** derrière des barrières et l'amélioration des systèmes de navigation inertielle dans des **environnements dépourvus de GNSS**. L'intégration de capteurs avec des technologies d'IA améliore la collecte et l'analyse des données, ce qui permet d'optimiser la prise de décision militaire.
- La technologie des capteurs avancés peut contribuer aux efforts de sécurité internationale, en aidant à la surveillance des **conflits armés en cours et au respect des accords de paix**, ainsi qu'à la détection précoce des substances dangereuses. Néanmoins, il est essentiel de répondre aux préoccupations en matière de cybersécurité et de relever d'autres défis, notamment les **délais potentiels** résultant de l'augmentation du volume de données.

50 Macri (2022).

4. Catégorie III : traitement et calcul

4.1. L'informatique en nuage

L'informatique en nuage facilite l'accès des utilisateurs aux ressources informatiques sans qu'il soit nécessaire de maintenir une infrastructure sur place. Elle offre la possibilité d'adapter les ressources en fonction de l'évolution des besoins.

L'informatique en nuage fonctionne avec le soutien des composants matériels et logiciels intégrés de l'infrastructure en nuage.[51] Ces dernières années, les capacités de l'informatique en nuage ont servi de catalyseur à l'innovation dans un large éventail d'applications, notamment l'analyse des mégadonnées, l'apprentissage automatique, l'informatique sans serveur, la réalité augmentée (RA), la réalité virtuelle (RV) et diverses autres technologies de pointe. Les plateformes basées sur le nuage permettent désormais l'externalisation de l'IA en tant que service (AIaaS), ce qui facilite l'accès généralisé aux capacités transformatrices de l'IA.[52] En outre, la technologie " native en nuage " est apparue comme une nouvelle approche pour créer, tester, déployer

51 Pour une analyse détaillée de l'infrastructure en nuage et des derniers progrès, voir la section 5.3 ci-dessous.

52 Marr (2023).

et gérer des applications dans des environnements d'informatique en nuage, offrant les avantages d'une efficacité, d'une réduction des coûts et d'une évolutivité accrues.[53]

L'informatique en nuage a le potentiel d'alimenter l'innovation dans le secteur militaire. Plus précisément, l'exploitation de la technologie en nuage peut accélérer les processus de conception, de développement et de test des logiciels pour les systèmes militaires.[54] Cela peut renforcer les capacités dans diverses applications militaires, allant de l'intelligence artificielle et de l'apprentissage automatique à la modernisation des logiciels et à la cybersécurité.[55] Dans le domaine de la formation militaire, les plateformes basées sur le nuage peuvent permettre au personnel d'accéder à des environnements de formation réalistes et immersifs, grâce à des technologies émergentes telles que la RV ou la RA. Depuis septembre 2022, l'armée britannique collabore avec une entreprise privée pour développer et mettre à l'échelle une simulation immersive de guerre terrestre distribuée dans le nuage, conçue pour faciliter l'entraînement collectif à grande échelle des utilisateurs physiques et virtuels dans différents lieux.[56] En outre, l'informatique en nuage fournit la puissance de calcul à grande vitesse indispensable au traitement de données à grande échelle dans le cadre d'opérations militaires. Compte tenu de la complexité et du volume des données militaires, la technologie en nuage permet de déployer des outils qui aident les forces armées à analyser les données de manière plus efficace. Cela leur permet de garder une longueur d'avance sur les menaces qui évoluent rapidement, tout en maintenant la sécurité.[57]

Néanmoins, la technologie du nuage pose des défis et des menaces potentielles. L'intégration de l'informatique en nuage dans les opérations militaires soulève des inquiétudes quant à la sécurité des données, en particulier lorsque des fournisseurs de services en nuage tiers sont impliqués.[58] En outre, les problèmes de connectivité, tels qu'une latence excessive dans des environnements éloignés ou difficiles, peuvent affecter la fiabilité des services basés sur l'informatique en nuage et avoir ainsi un impact sur l'efficacité opérationnelle et la prise de décision en temps réel. Enfin, l'intensification de la concurrence mondiale dans le domaine des technologies en nuage pourrait devenir un catalyseur potentiel de tensions internationales accrues, les États pouvant chercher à renforcer les contrôles à l'exportation sur les technologies en nuage avancées en fonction de leurs intérêts en matière de sécurité nationale.[59]

---

53 Google (s.d.) et AWS (s.d.)

54 Microsoft (2023).

55 Département de la défense des États-Unis (2023).

56 Hadean (2022).

57 Microsoft (2023).

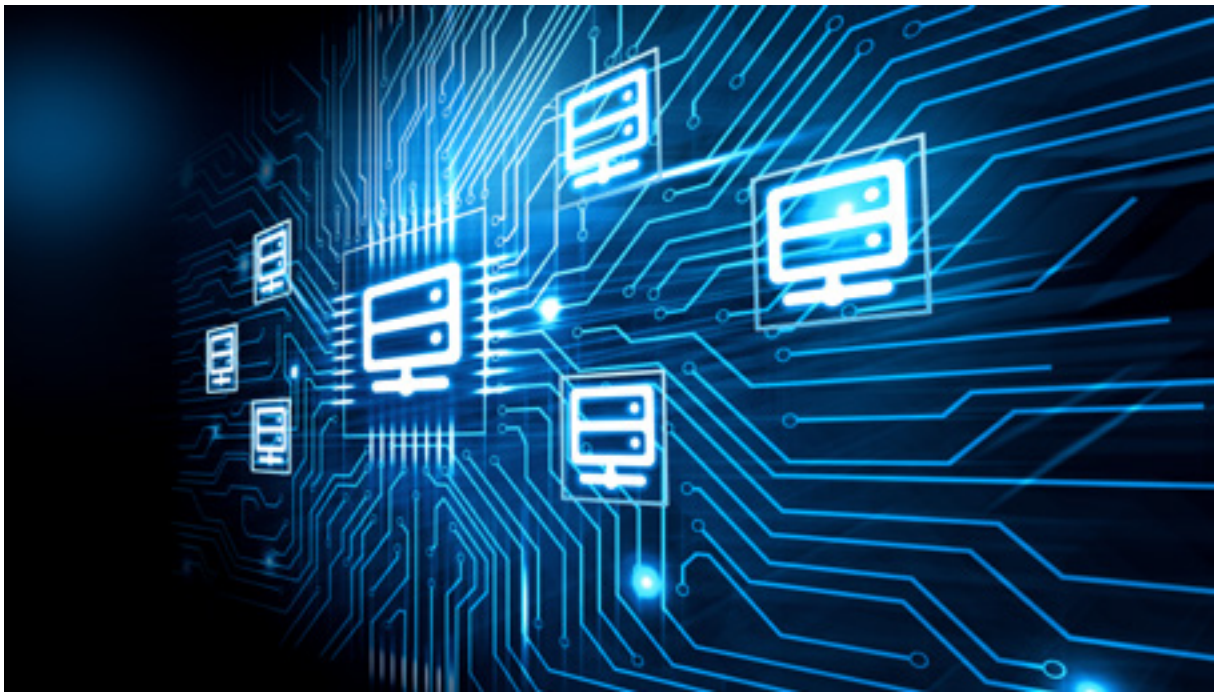
58 Pour une analyse plus approfondie des problèmes de sécurité des données liés à la technologie en nuage, voir la section 5.3 ci-dessous.

59 Hayashi et McKinnon (2023).

L’informatique en nuage : les faits marquants en 2023

- L’informatique en nuage continue d’alimenter l’innovation dans toute une série d’applications de pointe, notamment l’analyse des mégadonnées, l’apprentissage automatique, l’informatique sans serveur, la RA et la RV. Les plateformes basées sur le nuage permettent actuellement l’externalisation de l’**IA en tant que service (AIaaS)**, démocratisant l’accès aux capacités transformatrices de l’IA.
- Dans le secteur militaire, la technologie en nuage peut faciliter la création d ’**environnements d’entraînement réalistes et immersifs**, grâce à des technologies émergentes telles que la RV ou la RA. L’informatique en nuage fournit également la **puissance de calcul à grande vitesse** indispensable au traitement de données à grande échelle dans le cadre d’opérations militaires. Cependant, les problèmes de connectivité, tels que la latence excessive dans les environnements distants, peuvent avoir un impact sur la fiabilité des services basés sur l’informatique en nuage.

4.2. Informatique en périphérie



L'informatique en périphérie utilise un paradigme de l'informatique distribuée qui rapproche le stockage des données et le calcul de la source de données ou de la " périphérie " du réseau, plutôt que de s'appuyer sur un système centralisé basé sur l'informatique en nuage.

Dans l'informatique en périphérie, le traitement des données s'effectue sur un appareil ou un serveur local situé à la " périphérie " d'un réseau. Lorsque les données doivent être traitées dans le centre de données centralisé, seules les informations critiques sont transmises.[60] Par conséquent, l'informatique en périphérie réduit la latence et augmente la puissance de calcul en stockant et en traitant les données localement et en réduisant les goulets d'étranglement potentiels dans les réseaux et les centres de données en nuage. Ces avantages sont particulièrement importants pour les appareils périphériques qui nécessitent un traitement en temps réel, comme c'est le cas dans des applications telles que l'Internet des objets, les véhicules autonomes et la RA.

Le développement de l'informatique en périphérie pourrait transformer le mode de fonctionnement du secteur militaire en améliorant les capacités de communication, de traitement des données et de prise de décision.[61] Le déploiement de l'informatique en périphérie sur le terrain permet un partage instantané des données entre les forces connectées au même réseau en périphérie, ce qui

60 Microsoft Azure (s.d.).

61 Lee et al. (s.d.).

facilite la communication et la coordination en temps réel. Il apporte également des ressources informatiques à la périphérie tactique des opérations militaires et réduit la dépendance à l'égard des centres de données en nuage. Les grands ensembles de données provenant du terrain, tels que les données des capteurs et les flux vidéo pour la surveillance et la reconnaissance, peuvent être analysés localement sur des sites périphériques, ce qui accélère les temps de réponse et améliore la connaissance de la situation. L'adoption d'une architecture en périphérie sur le champ de bataille peut donc améliorer les applications de l'Internet des objets militaires (IoMT) et permettre au personnel militaire de réagir rapidement à des situations potentiellement dangereuses.[62]

L'informatique en périphérie garantit la disponibilité des ressources de données et de calcul dans des endroits éloignés où la connectivité Internet est intermittente et même dans des environnements opérationnels extrêmes. L'analyse avancée de l'IA peut fonctionner efficacement sur des plateformes en périphérie lorsqu'elles sont complètement hors ligne dans des environnements difficiles, soutenant ainsi des missions critiques telles que les opérations de recherche et de sauvetage.[63] Pourtant, les applications d'IA déployées sur des appareils militaires en périphérie tels que les UAV, les satellites et les véhicules terrestres sont souvent limitées et peuvent être inférieures aux modèles de pointe en raison des contraintes liées à la vitesse de traitement, à la mémoire de travail et à la puissance.[64] En outre, Amazon Web Services a récemment présenté AWS Snowblade, un nouveau produit d'informatique en périphérie spécialement conçu pour le contrat de Capacité en nuage de combat interarmées (JWCC) conclu avec le Département de la défense des États-Unis (DOD).[65] AWS Snowblade permet aux utilisateurs militaires du JWCC d'effectuer des opérations dans des zones périphériques qui peuvent être soumises à des températures, des vibrations ou des chocs extrêmes.

Néanmoins, l'informatique en périphérie présente certains problèmes de sécurité pour les applications militaires. Le cadre de l'informatique distribuée peut augmenter la surface d'attaque, en fournissant davantage de points terminaux pour les cyberattaques. L'informatique en périphérie est vulnérable à une série de menaces de cybersécurité, notamment les attaques par déni de service (DoS), les attaques par canaux auxiliaires, les attaques par injection de logiciels malveillants et les attaques d'authentification et d'autorisation.[66] Les installations informatiques en périphérie sont également susceptibles d'être endommagées physiquement, ce qui peut entraîner des perturbations et des violations de données dans les réseaux périphériques.[67] Pour remédier à ces vulnérabilités, des efforts constants sont déployés pour améliorer les mesures de sécurité des systèmes informatiques en périphérie. Par exemple, les périphériques AWS Snowblade intègrent une technologie de chiffrement avancée pour garantir la sécurité des données et empêcher tout accès non autorisé de la part d'adversaires potentiels.[68]

---

62 Cameron (2018).

63 Thomas (2021).

64 Miller et Lohn (2023).

65 AWS (2023).

66 Xiao et al. (2019).

67 OTAN CCDCOE (2022).

68 Konkel (2023).

Informatique en périphérie : les faits marquants en 2023

- L'informatique en périphérie peut transformer les opérations militaires en améliorant les capacités de communication, de traitement des données et de prise de décision. En outre, dans les environnements éloignés ou extrêmes, l'informatique en périphérie joue un rôle essentiel dans la sécurisation des données et la fourniture des ressources informatiques nécessaires.
- Les plateformes en périphérie permettent à l'analyse de l'IA de fonctionner efficacement hors ligne dans des environnements difficiles, à l'appui de missions essentielles telles que les **opérations de recherche et de sauvetage**. Les **limitations** en termes de vitesse de traitement, de mémoire et de puissance peuvent affecter les applications d'IA sur les appareils militaires en périphérie.
- Les défis persistants en matière de sécurité dans le domaine de l'informatique militaire en périphérie comprennent la surface élargie pour les cyberattaques et la vulnérabilité aux dommages physiques. Des efforts continus sont déployés pour améliorer les mesures de sécurité, comme le chiffrement avancé dans **AWS Snowblade.**

4.3. Informatique quantique[69]

L'informatique quantique est un domaine émergent qui s'appuie sur les principes de la mécanique quantique pour résoudre des problèmes dont la complexité dépasse les capacités des ordinateurs classiques.

La possibilité pour les ordinateurs quantiques de surpasser les ordinateurs classiques est attribuée à des phénomènes quantiques uniques, notamment la superposition et l'intrication. Les bits quantiques ou qubits, l'unité d'information fondamentale de l'informatique quantique, peuvent exister simultanément dans plusieurs états (0 et 1) grâce à la superposition. Lorsque des qubits sont intriqués, l'état d'un qubit est directement lié à celui d'un autre qubit, quelle que soit la distance physique qui les sépare. L'intrication quantique peut être exploitée pour augmenter considérablement la vitesse de calcul, ce qui permet aux ordinateurs quantiques d'effectuer des calculs spécifiques plus efficacement que leurs homologues classiques.

Le domaine de l'informatique quantique a connu des progrès considérables. Des entreprises privées comme IBM, Google/Alphabet et Microsoft ont investi massivement dans la recherche et le développement d'ordinateurs quantiques pratiques. IBM, par exemple, a régulièrement augmenté le nombre de qubits sur une seule puce. En décembre 2023, IBM a dévoilé le processeur Condor, qui compte 1 121 qubits, une avancée notable par rapport au précédent processeur Osprey de 433

---

69 Un rapport à venir de l'UNIDIR, intitulé " International Security in a Quantum New World: A Primer " (La sécurité internationale dans un nouveau monde quantique : introduction), fournira une analyse plus approfondie du domaine de l'informatique quantique et de ses implications pour la sécurité internationale.

qubits.[70] Parallèlement, l'entreprise a présenté le Heron, son processeur quantique le plus performant à ce jour, équipé de 133 qubits de haute qualité.[71] Les processeurs Heron ont notamment la capacité de se connecter directement à d'autres processeurs Heron, ce qui pourrait faciliter l'extensibilité des ordinateurs quantiques.[72]

Néanmoins, malgré ces avancées, le domaine reste confronté à des défis importants qui doivent encore être relevés. L'un des principaux problèmes est connu sous le nom de décohérence, un phénomène quantique résultant d'un isolement insuffisant d'un qubit physique par rapport à son environnement, ce qui peut introduire du bruit dans les calculs. Il est donc devenu essentiel de surmonter la décohérence et de corriger les erreurs quantiques.[73] En outre, bien que les preuves mathématiques suggèrent des avantages quantiques par rapport aux modèles classiques, les preuves empiriques font encore défaut en raison de l'indisponibilité d'ordinateurs quantiques dotés d'un nombre suffisant de qubits.[74] Par exemple, les chercheurs ont estimé que le décryptage de la cryptographie de pointe en huit heures nécessiterait 20 millions de qubits.[75]

Bien que les applications pratiques de l'informatique quantique restent encore à l'horizon, les développements futurs potentiels ont de profondes implications pour les pratiques militaires et la sécurité internationale. L'informatique quantique a le potentiel de révolutionner divers domaines technologiques, notamment en améliorant l'intelligence artificielle et l'apprentissage automatique. Le succès des algorithmes classiques d'apprentissage automatique dépend souvent de paramètres étendus et de données d'apprentissage substantielles. En revanche, l'apprentissage automatique quantique, en tirant parti des divers états disponibles pour les particules quantiques, peut potentiellement réduire le nombre de paramètres et de données requis.[76] La recherche empirique a montré que les réseaux hybrides, qui combinent les caractéristiques des ordinateurs classiques et quantiques, peuvent améliorer le traitement des modèles d'apprentissage automatique.[77] Ces avancées pourraient transformer les futures applications militaires de l'IA, notamment en développant des systèmes plus précis d'armes létales autonomes.[78]

En outre, l'informatique quantique peut remodeler le paysage de la cybersécurité, en présentant à la fois des défis et des opportunités. Les ordinateurs quantiques ont la capacité de résoudre certains problèmes mathématiques exponentiellement plus rapidement que les ordinateurs classiques, ce qui pourrait compromettre la sécurité de certains algorithmes cryptographiques couramment utilisés (par exemple, les systèmes de chiffrement RSA et ECC). Des algorithmes quantiques capables de décrypter les communications numériques, notamment l'algorithme de Shor, ont été développés et pourront être

---

70 Gambetta (2023).

71 Ibid.

72 Brooks (2023a).

73 Lidar (2023).

74 Brooks (2023b).

75 Ibid.

76 Ibid.

77 Xu (2023).

78 Service de recherche du Congrès des États-Unis (2023).

exécutés lorsque des ordinateurs quantiques pratiques seront disponibles.[79] Cela introduit de nouvelles vulnérabilités en matière de cybersécurité et peut donner lieu à des attaques de type HNDL (Harvest Now Decrypt Later), où des acteurs malveillants acquièrent des données sensibles et chiffrées dans l'intention de les décoder plus tard, à la suite d'éventuelles percées dans la technologie du décryptage. Ces attaques peuvent poser des problèmes de sécurité nationale en permettant à des adversaires d'accéder à des informations militaires sensibles.[80] En réponse aux menaces quantiques potentielles, des efforts sont actuellement déployés pour développer la cryptographie post-quantique (PQC). Il s'agit de créer des systèmes cryptographiques capables de résister aux futures attaques des ordinateurs quantiques. Les technologies quantiques émergentes, telles que la distribution quantique de clé (QKD)[81] et la génération quantique de nombres aléatoires (QRNG)[82], offrent également la possibilité d'améliorer les mécanismes de chiffrement et les communications sécurisées.

Informatique quantique : les faits marquants en 2023

- Des progrès considérables ont été réalisés dans le domaine de l'informatique quantique. IBM, par exemple, n'a cessé d'augmenter le nombre de qubits sur une seule puce, atteignant une étape importante avec l'introduction du **processeur Condor à 1 121 qubits** en 2023. Simultanément, la société a lancé le processeur Heron avec la possibilité de se connecter directement à d'autres processeurs Heron, ce qui pourrait faciliter son **extensibilité**.
- La recherche empirique a montré que les **réseaux hybrides** combinant des ordinateurs classiques et quantiques peuvent améliorer le traitement des modèles d'apprentissage automatique. Cette évolution a de profondes implications pour les applications militaires de l'IA, en particulier pour le développement de **systèmes plus précis d'armes létales autonomes**.
- Cependant, le développement de l'informatique quantique présente des défis importants en matière de cybersécurité et de sécurité de l'information, notamment le risque d'attaques de type HNDL, étant donné que les ordinateurs quantiques pratiques **peuvent** compromettre des algorithmes cryptographiques largement utilisés. Par conséquent, des efforts sont actuellement déployés pour développer la cryptographie post-quantique en réponse aux menaces quantiques émergentes.

79 van Amerongen (2021).

80 Service de recherche du Congrès des États-Unis (2023).

81 OTAN (2022).

82 Argillander et al. (2023).

5. Catégorie IV : infrastructure

5.1. 5G et 6G

5G désigne la norme technologique de cinquième génération pour les réseaux cellulaires, qui fournit des connexions à large bande avancées qui surpassent ses prédécesseurs, tels que la 4G LTE. **6G** désigne le développement en cours de la technologie cellulaire de sixième génération, conçue pour surpasser la 5G et offrir des capacités de réseau encore plus avancées.

La génération actuelle d'infrastructures de connectivité se caractérise par des progrès significatifs dans la technologie sans fil, notamment avec la mise en œuvre généralisée des réseaux cellulaires de cinquième génération (5G). La technologie 5G présente plusieurs avantages par rapport à ses prédécesseurs, grâce à de nouvelles caractéristiques telles que le découpage du réseau et la capacité de fonctionner sur le spectre des ondes millimétriques (mmWave), une bande hautes fréquences du spectre radioélectrique dans la plage des 30-300 GHz.[83] La 5G améliore considérablement la connectivité en offrant des vitesses plus rapides, en réduisant la latence, en améliorant la fiabilité du réseau et en prenant en charge la connexion simultanée d'un plus grand nombre

83 Gerwig et Goss. (2023).

d'appareils. Ces capacités innovantes de la 5G sont essentielles pour répondre aux demandes croissantes d'innovations technologiques, en particulier dans les applications basées sur l'IoT, permettant la connexion d'un plus grand nombre d'appareils et d'objets aux réseaux.

La technologie 5G peut libérer un immense potentiel pour des applications militaires transformatrices, en facilitant une communication optimisée, un transfert de données rapide et des capacités de prise de décision en temps réel sur le champ de bataille. Sa capacité de connectivité à haut débit et à faible latence peut prendre en charge des fonctions militaires essentielles, allant des communications et de la logistique à l'ISR, en passant par le commandement et le contrôle. Des recherches récentes ont mis en évidence trois applications militaires concrètes rendues possibles par la mise en œuvre de la 5G : le suivi d'éléments et d'équipements à l'aide d'étiquettes intelligentes pour optimiser les opérations, l'exploitation des réseaux 5G à large bande pour le transfert des données de grands ensembles de données de capteurs, et l'utilisation de communications 5G à distance pour le commandement et le contrôle afin d'améliorer la coordination multinationale.[84] L'utilisation du suivi des étiquettes intelligentes dans les expéditions via un réseau 5G est également prometteuse pour faire progresser les efforts de contrôle des armes en atténuant potentiellement les risques associés au détournement d'armes et de munitions conventionnelles. En outre, la 5G peut servir de puissant catalyseur pour des applications IA et IoT de pointe dans le domaine militaire, ouvrant la voie à des capacités renforcées. Les réseaux 5G à grande vitesse peuvent faciliter l'intégration de l'IA pour un traitement efficace de vastes quantités de données de capteurs sur le champ de bataille. Par exemple, les signaux adverses peuvent être transmis en temps réel via un réseau 5G sécurisé pour une analyse plus approfondie à l'aide d'algorithmes de traitement des signaux avancés.[85]

Néanmoins, l'intégration de la technologie 5G introduit de nouveaux risques, notamment dans le domaine de la cybersécurité. Avec l'augmentation des volumes de données et des dispositifs interconnectés au sein des réseaux 5G, les vulnérabilités potentielles en matière de sécurité peuvent être amplifiées, offrant aux acteurs malveillants des possibilités accrues d'exploitation et de perturbation. Les caractéristiques de la technologie 5G, notamment les interfaces ouvertes et sa nature basée sur l'informatique en nuage, créent également des menaces de sécurité supplémentaires, ce qui se traduit par un paysage de menaces étendu pour les déploiements de la 5G.[86] Un large éventail de menaces de cybersécurité peut se manifester dans les multiples sous-systèmes de la 5G, qui s'étendent de l'équipement utilisateur 5G et du réseau d'accès radio (RAN) au réseau central, aux services en nuage et à l'informatique périphérique multiaccès (MEC), parmi d'autres composants critiques.[87]

Le développement des réseaux cellulaires 6G est actuellement en cours et promet d'être encore plus prometteur que les avancées actuelles de la technologie 5G. Il devrait apporter de nouvelles améliorations en termes de vitesse, de latence et de connectivité, ainsi que la capacité de permettre un plus large éventail d'applications technologiques novatrices. Par rapport aux générations précédentes de réseaux de communication,

---

84 Lee et al. (2023).

85 Tucker (2022).

86 Śliwa et Suchański (2022).

87 OTAN CCDCOE (2022).

la recherche et le développement de la 6G mettent davantage l'accent sur l'obtention d'une couverture réseau complète " sur terre, en mer, dans l'air et dans l'espace ", en combinant les réseaux mobiles cellulaires terrestres avec des plateformes aériennes et satellitaires.[88] Cette architecture intégrée de réseau satellite-terrestre devrait offrir un potentiel important pour assurer une couverture mondiale de l'Internet et fournir un support de communication omniprésent pour l'Internet des objets.[89] Le déploiement de la technologie 6G devrait commencer aux alentours de 2030.[90]

5G et 6G : les faits marquants en 2023

- Les progrès actuels de la technologie 5G libèrent un potentiel de transformation dans les **applications militaires**, en permettant des communications optimisées, un transfert rapide des données et une prise de décision en temps réel sur le champ de bataille. La 5G peut également faciliter l'intégration d'applications de pointe en matière d'IA et d'IoT, renforçant ainsi les capacités militaires.
- Cependant, l'introduction de la technologie 5G amplifie les vulnérabilités potentielles en matière de cybersécurité en raison de l'augmentation des volumes de données et de l'interconnexion des appareils. Les interfaces ouvertes et le fait qu'elles soient basées sur l'informatique en nuage créent également **un vaste paysage de menaces** pour les déploiements de la 5G.
- Les travaux de recherche et de développement en cours sur les réseaux cellulaires 6G visent à **assurer une couverture complète** de la terre, de la mer, de l'air et de l'espace grâce à un réseau satellite-terrestre intégré, dont le déploiement est prévu d'ici à 2030.

88 Chen et al. (2023).

89 Tirmizi et al. (2022).

90 Kharpal (2023) et Chen et al. (2023).

5.2. Internet des objets

L'Internet des objets (IoT) relie un vaste réseau de dispositifs physiques, d'appareils, de véhicules et d'autres objets intégrés à des capteurs, des logiciels et une connectivité réseau, facilitant la collecte et l'échange de données entre les dispositifs et les systèmes. En permettant à ces appareils de communiquer et de collaborer entre eux via l'Internet ou d'autres réseaux de communication, l'IoT crée un écosystème interconnecté qui peut être surveillé et contrôlé à distance.

Les évolutions récentes dans le domaine de l'Internet des objets (IoT) sont liées à des innovations technologiques dans d'autres domaines, notamment l'informatique en périphérie, les réseaux 5G et l'intégration de l'intelligence artificielle.[91] L'essor de l'informatique en périphérie a favorisé une approche plus localisée du traitement et du stockage des données, réduisant efficacement la latence et améliorant les capacités de traitement en temps réel des appareils IoT.[92] Parallèlement, le déploiement des réseaux 5G a également accéléré le développement de l'IoT en offrant des vitesses de transfert de données plus élevées, une latence plus faible et une capacité de réseau accrue.[93] En outre, l'intégration des technologies d'IA, en particulier l'apprentissage automatique, peut soutenir l'analyse et l'interprétation en temps réel de la grande quantité de données générées par les

---

91 Coughlin (2023).

92 Pour une analyse détaillée de l'informatique en périphérie et des derniers progrès, voir la section 4.2 ci-dessus.

93 Pour une analyse détaillée des réseaux cellulaires 5G et des derniers progrès, voir la section 5.1 ci-dessus.

applications IoT, conduisant à une prise de décision et à une automatisation plus efficaces.

La technologie IoT est de plus en plus exploitée dans les systèmes militaires pour optimiser les opérations et améliorer l'efficacité, ce qui a facilité l'évolution vers un paysage militaire plus connecté et axé sur les données. L'Internet des objets militaires (IoMT) peut faire appel à un large éventail de capteurs déployés dans différents domaines, afin d'obtenir une connaissance globale de la situation et un contrôle efficace dans des environnements de conflit complexes et variés.[94] L'intégration de réseaux de capteurs et de systèmes non pilotés dans le cadre de l'IoMT peut considérablement accroître les capacités de surveillance et de reconnaissance, permettant aux forces militaires de suivre l'environnement du champ de bataille, de gérer les équipements et les véhicules et de surveiller l'état de santé des soldats.[95] L'exploitation de la technologie IoT/IoMT peut améliorer la précision du ciblage et minimiser le risque de pertes civiles lors des opérations militaires, car les capteurs intégrés dans un réseau IoT/IoMT peuvent guider les armes avec plus de précision vers la cible visée.[96]

En outre, les progrès de la technologie IoT/IoMT ont également permis d'améliorer considérablement les systèmes de communication militaires. L'IoT facilite le partage des données et la connectivité, améliorant ainsi la collaboration entre les forces interarmées et de coalition, et entre les différents domaines.[97] En outre, l'intégration de protocoles de communication sécurisés et l'utilisation du chiffrement et des signatures numériques dans les systèmes compatibles avec l'IoT peuvent protéger efficacement les canaux de communication, en garantissant la confidentialité, l'intégrité et la disponibilité des informations militaires sensibles.[98] Pourtant, sans protocoles de communication robustes, l'adoption généralisée de la technologie IoT peut introduire des menaces substantielles de cybersécurité pour les systèmes militaires interconnectés. Les réseaux IoMT présentent une vaste surface d'attaque comprenant les appareils IoMT, les canaux de communication reliant ces appareils, les applications dorsales spécifiques à l'IoMT, ainsi que le stockage des données dorsales.[99] Les implications des cyberopérations impliquant des dispositifs IoT peuvent s'étendre au-delà des systèmes militaires, pouvant causer des perturbations indiscriminées à d'autres systèmes connectés, y compris des installations médicales, des établissements d'enseignement et d'autres réseaux sensibles.[100]

---

94 Withrington (2023).

95 Khawaja (2023).

96 Douglass (2022).

97 Breaking Defense (2023).

98 Kannan et al. (2023).

99 Withrington (2023).

100 Renals (2021).

Internet des objets : les faits marquants en 2023

- La technologie de l'IoT est de plus en plus appliquée dans les systèmes militaires à des fins d'optimisation opérationnelle (connue sous le nom d'Internet des objets militaires). L'IoMT utilise un ensemble diversifié de capteurs dans différents domaines pour une **connaissance et un contrôle complets de la situation**. Les capteurs intégrés dans un réseau IoT/IoMT peuvent également améliorer la précision du ciblage dans les opérations militaires, avec la possibilité de **minimiser le risque de pertes civiles**.
- Toutefois, en l'absence de protocoles de communication robustes, l'adoption généralisée de l'IoT dans les systèmes militaires peut entraîner des risques de cybersécurité. Les réseaux IoMT créent une surface d'attaque importante dont les implications potentielles vont au-delà des systèmes militaires et touchent d'**autres secteurs critiques**, notamment les installations médicales, les établissements d'enseignement et d'autres réseaux sensibles.

5.3. Infrastructure en nuage

L'infrastructure en nuage consiste en des composants matériels et logiciels essentiels à la prestation de services en nuage sur l'Internet. Il s'agit de matériel tel que les serveurs, le stockage, les composants de réseau et les centres de données, ainsi que de logiciels tels que les logiciels de virtualisation.

L'infrastructure en nuage constitue la base sur laquelle les services d'informatique en nuage sont construits et fournis.[101] Les services en nuage se sont développés ces dernières années, les entreprises privées jouant un rôle essentiel en tant que fournisseurs de services en nuage (CSP). Les principaux CSP sont Amazon Web Services (AWS), Microsoft Azure, Google Cloud, Oracle Cloud et Alibaba Cloud. Ils proposent une gamme variée de services en nuage, qui peuvent être regroupés en trois catégories principales : l'infrastructure en tant que service (IaaS), la plateforme en tant que service (PaaS) et le logiciel en tant que service (SaaS). Les CSP ont continué à étendre rapidement la couverture de leur infrastructure en nuage dans le monde entier, établissant une présence sur tous les continents.[102]

La technologie en nuage est de plus en plus utilisée pour améliorer l'efficacité opérationnelle et la gestion des données dans le domaine militaire. Les forces armées ont non seulement développé leur propre infrastructure en nuage, mais elles ont également adopté

---

101 Pour une analyse détaillée de l'informatique en nuage et des derniers progrès, voir la section 4.1 ci-dessus.

102 Une carte mondiale de l'infrastructure en nuage de huit grands fournisseurs de services en nuage : **https://www.cloudinfrastructuremap.com/**

des capacités et des services commerciaux en nuage fournis par des CSP privés. À titre d'exemple, en décembre 2022, le Département de la défense des États-Unis a attribué des contrats à quatre fournisseurs de services informatiques de premier plan (AWS, Google, Microsoft et Oracle) pour soutenir la Capacité en nuage de combat interarmées du Département de la défense des États-Unis.[103] L'infrastructure en nuage permet aux forces armées de stocker et de gérer d'importants volumes de données militaires, qu'il s'agisse de données ISR, d'informations logistiques ou d'autres données essentielles à la mission. Cela peut faciliter la communication et la coordination entre le personnel militaire et les unités provenant de différents endroits.

Garantir la sécurité des données a été une considération essentielle dans le déploiement de la technologie en nuage dans les contextes militaires. L'infrastructure en nuage offre souvent une sécurité renforcée pour les informations sensibles, grâce à un chiffrement solide, à la gestion des identités et des accès, et à d'autres fonctions de sécurité avancées. En particulier, la décision proactive du gouvernement ukrainien de migrer une grande partie de ses données critiques vers le nuage a permis au pays d'être mieux préparé à faire face à des cyberattaques sans précédent.[104] Les gouvernements et les CSP ont continué à renforcer les mesures de sécurité de leur infrastructure en nuage, y compris par l'adoption d'une approche de confiance zéro dans les environnements informatiques en nuage.[105]

Néanmoins, les environnements en nuage, comme les autres plateformes numériques, restent exposés à des cyberrisques et à des vulnérabilités potentielles. Le transfert de données sensibles vers des systèmes en nuage peut aggraver les problèmes de sécurité, comme l'ont montré les précédents incidents de sécurité dans le nuage. En février 2023, un volume important de courriels militaires sensibles a été exposé en raison d'un serveur de messagerie mal configuré sur la plateforme Microsoft Azure Government Cloud. [106] Si l'utilisation des services commerciaux en nuage des principaux fournisseurs de services de télécommunications offre l'avantage de protocoles de sécurité robustes et de fortes concentrations d'expertise, elle présente également le risque que les incidents qui affectent l'infrastructure en nuage de ces fournisseurs aient des effets étendus.[107] En outre, le Comité international de la Croix-Rouge (CICR) a souligné l'implication croissante des civils dans les opérations numériques pendant les conflits armés, ce qui pourrait conduire à une utilisation accrue de l'infrastructure civile, y compris l'infrastructure en nuage, à des fins militaires.[108] Cette tendance accroît le risque que des civils et des infrastructures civiles soient pris pour cible, ce qui compromet le principe de distinction universellement reconnu.[109]

---

103 Département de la défense des États-Unis (2022).

104 Lewis (2023).

105 Département de la défense des États-Unis (2023).

106 Martin et al. (2023).

107 Maurer et Hinck (2020).

108 CICR (2023).

109 Ibid.

Infrastructure en nuage : les faits marquants en 2023

- Les forces armées ont de plus en plus recours à l'infrastructure en nuage pour améliorer l'efficacité opérationnelle et la gestion des données. Bien que des mesures de sécurité avancées, telles qu'un chiffrement solide, soient mises en œuvre, l'intégration d'environnements en nuage dans le cadre militaire reste vulnérable aux cyberrisques, comme l'ont montré les **incidents passés.**
- En outre, le **CICR** a souligné l'implication croissante des civils dans les opérations numériques pendant les conflits armés, ce qui pourrait accroître l'utilisation de l'infrastructure civile, y compris l'infrastructure en nuage, à des fins militaires. Cela augmente le risque que des civils et des infrastructures civiles soient pris pour cible, ce qui compromet le principe de distinction.

5.4. Communications par satellite

Les **communications par satellite** impliquent l'utilisation de satellites artificiels pour établir des liens de communication entre divers endroits de la Terre.

Les systèmes de communication par satellite jouent un rôle essentiel pour assurer la couverture mondiale de l'Internet, réduire la fracture numérique et accroître la résilience de l'infrastructure de connectivité, en particulier dans les zones où les réseaux de communication terrestres traditionnels sont limités ou indisponibles. Les technologies satellitaires font partie intégrante des opérations militaires et les progrès constants dans ce domaine continuent à stimuler l'innovation dans le secteur de la défense. L'augmentation actuelle des déploiements de constellations de satellites en orbite terrestre basse (LEO) est sur le point d'accroître de manière significative le nombre de satellites en orbite autour de la Terre. Par rapport aux satellites géosynchrones traditionnels, les grandes constellations de petits satellites en orbite terrestre basse peuvent réduire considérablement la latence, augmenter la capacité de la bande passante et offrir une couverture mondiale régulière. Les entités privées sont principalement à l'origine des développements dans le domaine des satellites LEO, notamment Starlink de SpaceX, OneWeb et le projet Kuiper d'Amazon.[110]

La connectivité améliorée fournie par les systèmes LEO peut être exploitée par les forces militaires pour permettre des transferts de données en temps réel, optimisant ainsi la précision et l'efficacité des opérations militaires. Comme on l'a vu dans le conflit entre la Russie et l'Ukraine, la constellation de satellites LEO Starlink de SpaceX a joué un rôle

110 Borowitz (2022).

crucial en facilitant les communications essentielles à des fins civiles et militaires en Ukraine, y compris le déploiement sur des UAV pour la surveillance et la reconnaissance.[111] Au-delà des applications de défense, les constellations LEO ont également le potentiel de combler le fossé numérique mondial, en fournissant l'Internet à haut débit dans les zones rurales ou éloignées où l'infrastructure terrestre traditionnelle est difficile à déployer.[112]

Une autre innovation notable dans le domaine des communications par satellite est l'intégration des technologies quantiques. La distribution quantique de clé (QKD) permet de sécuriser les communications par satellite en appliquant les principes de la mécanique quantique pour créer et échanger des clés de cryptage entre deux parties. En septembre 2022, l'Agence spatiale européenne a annoncé une collaboration avec la Commission européenne et plus de 20 entreprises spatiales européennes pour introduire le premier système QKD basé dans l'espace dans la région, connu sous le nom de satellite Eagle-1.[113] Ce système de connectivité par satellite ouvrira la voie à un réseau ultra-sécurisé en Europe. Parallèlement, des pays tels que la Chine[114] et Singapour[115] poursuivent également le développement de la technologie QKD afin de renforcer la sécurité des communications par satellite.

Si la technologie satellitaire ouvre de vastes perspectives en matière de connectivité mondiale et de communications sécurisées, elle pose également une série de problèmes de sécurité. L'un des défis concerne la vulnérabilité des systèmes satellitaires aux cybermenaces et aux violations potentielles de données. Les communications par satellite sont indispensables pour transmettre des informations sensibles cruciales pour les opérations militaires, et toute compromission des systèmes peut entraîner des désavantages stratégiques importants. Les systèmes militaires de communication par satellite sont devenus la cible de cyberattaques, entraînant des pannes et des interruptions de services essentiels.[116] Les déploiements de satellites en orbite, en particulier le grand nombre de satellites LEO, peuvent également poser des problèmes de sécurité tels que ceux liés au trafic spatial et à l'augmentation des débris spatiaux, qui constituent une menace pour la sécurité et la durabilité de l'espace.[117] En outre, compte tenu du rôle central joué par les entités privées dans le domaine des communications par satellite, les forces militaires continueront à exploiter les technologies commerciales à leur avantage. Néanmoins, la dépendance à l'égard d'acteurs commerciaux pour les infrastructures de communication critiques pendant les conflits a mis en évidence les pièges potentiels découlant des différences d'incitations, de principes de fonctionnement et de mécanismes de responsabilité entre les entités privées et publiques.[118]

---

111 Jayanti (2023).

112 Marquina (2022).

113 ESA (2022).

114 Laursen (2022).

115 SpeQtral (2022).

116 Menn (2023).

117 Mukherjee (2021).

118 Jayanti (2023).

Communications par satellite : les faits marquants en 2023

- Parmi les innovations importantes dans le domaine des communications par satellite, citons la multiplication des constellations de satellites en LEO, sous l'impulsion d'**entités privées** telles que Starlink de SpaceX. Celles-ci contribuent non seulement à améliorer la **connectivité mondiale**, mais jouent également un rôle essentiel dans les opérations militaires en facilitant la communication critique pendant les conflits. En outre, l'intégration de la technologie de distribution quantique de clé dans les **systèmes satellitaires** ouvre la voie à des communications plus sûres.
- Toutefois, les communications par satellite peuvent également poser des problèmes de sécurité, notamment en raison de leur vulnérabilité aux **cybermenaces** et des préoccupations liées aux **débris spatiaux**. En outre, alors que les forces militaires continuent d'exploiter les technologies satellitaires commerciales, il est essentiel de mettre en évidence les **pièges potentiels** liés aux différences d'incitations, de principes de fonctionnement et de mécanismes de responsabilité entre les entités publiques et privées.

6. Conclusion

Dans les domaines technologiques examinés ici, plusieurs tendances et évolutions générales sont apparues. En particulier, une tendance persistante dans la technologie du matériel est le processus continu de miniaturisation, qui conduit à la création d'appareils de plus en plus compacts et efficaces. Les récentes percées dans le domaine des matériaux semi-conducteurs, des nanotechnologies, des micropuces et des capteurs ont toutes joué un rôle essentiel dans cette évolution. Cette tendance facilite l'adoption généralisée de technologies habilitantes dans l'armement et les systèmes militaires, contribuant ainsi à la modernisation des équipements militaires.

L'exploitation des technologies habilitantes permettra d'accroître considérablement les différentes capacités militaires. Il s'agit notamment d'une meilleure connaissance de la situation, d'un commandement et d'un contrôle rationalisés, d'un transfert et d'un traitement accélérés des données et d'une précision accrue de l'armement avancé. Notamment, certaines technologies habilitantes, telles que les micropuces, l'informatique en nuage et l'informatique quantique, agissent comme des catalyseurs de l'innovation dans les applications militaires. Elles facilitent l'intégration de technologies transformatrices telles que l'IA et les capacités d'apprentissage automatique, ce qui amplifie encore le potentiel d'avancées dans les opérations militaires. En outre, les technologies habilitantes peuvent renforcer les efforts internationaux en matière de sécurité en consolidant les mécanismes de vérification du désarmement et de suivi des conflits. Cela peut se faire, par exemple, par l'utilisation de capteurs avancés pour détecter les agents chimiques et biologiques dans l'environnement et pour contrôler le respect des accords de paix.

Toutefois, les progrès récents des technologies habilitantes posent également des risques et des défis importants. Si les innovations dans le domaine de la technologie en nuage et de la distribution quantique de clé peuvent renforcer la sécurité des communications, du stockage des informations et du traitement des données, le déploiement à grande échelle des technologies habilitantes accroît la vulnérabilité aux risques en matière de cybersécurité. Cette expansion du paysage technologique peut élargir la surface d'attaque, ce qui pose des défis accrus en matière de protection des systèmes militaires contre les cybermenaces potentielles. L'informatique quantique, en particulier, a le potentiel de perturber les protocoles et les normes de chiffrement largement utilisés en raison de ses capacités anticipées de décryptage.

En outre, la recherche d'innovations de pointe dans les technologies habilitantes est susceptible d'aggraver les tensions internationales et d'alimenter la concurrence technologique entre les États. Les États peuvent chercher à imposer des contrôles stricts sur les exportations de technologies avancées en fonction de leurs intérêts en matière de sécurité nationale. En outre, les vulnérabilités de la chaîne d'approvisionnement constituent un défi important dans le domaine des technologies habilitantes. La chaîne d'approvisionnement des composants matériels, tels que les micropuces, est un réseau extrêmement mondial et complexe, avec une forte concentration de la spécialisation de la production dans certaines régions du globe. Les perturbations des capacités de production dans ces régions, qu'elles résultent de tensions géopolitiques ou de catastrophes naturelles, auraient un impact négatif sur la disponibilité des technologies et des implications pour la sécurité internationale.

Enfin, l'évolution de nombreux domaines

technologiques souligne le rôle essentiel joué par le secteur privé. Les entreprises privées sont à l'origine de progrès et d'innovations dans un large éventail d'applications technologiques, notamment la technologie en nuage, les communications par satellite et l'informatique quantique. Les forces armées ont depuis longtemps commencé à collaborer avec des entités privées pour tirer parti des technologies de pointe, mais cette implication n'est pas sans risques. Les incidents qui ont un impact sur l'infrastructure des entreprises privées peuvent avoir des effets étendus, avec le risque de compromettre des informations militaires sensibles. La dépendance à l'égard des acteurs privés peut également conduire à des écueils potentiels découlant des différences d'incitations, de principes de fonctionnement et de mécanismes de responsabilité entre les entités privées et publiques.

Les progrès des technologies habilitantes continueront d'avoir des répercussions importantes sur les pratiques militaires et la sécurité internationale. Cela nécessite une analyse continue des tendances nouvelles et émergentes ainsi qu'un examen plus approfondi des cadres de gouvernance potentiels afin d'exploiter les opportunités tout en atténuant les risques. Dans ses futurs projets de recherche, l'UNIDIR continuera d'identifier et d'examiner les technologies nouvelles et émergentes, ainsi que les nouvelles applications des technologies plus anciennes, et fournira des recommandations politiques orientées vers l'action afin de régir efficacement les différentes catégories de technologies.

Références

Amazon Web Services (AWS). 2023. “ Announcing AWS Snowblade for U.S. Department of Defense JWCC Customers ” (Annonce d’AWS Snowblade pour les clients JWCC du Département de la défense des États-Unis). 6 juin. Consulté le 6 décembre 2023 : https://aws.amazon.com/about-aws/whats-new/2023/06/aws-snowblade-us-defense-jwcc-customers/

Agence spatiale européenne (ESA). 2022. “ Quantum Encryption to Boost European Autonomy ” (Le chiffrement quantique au service de l’autonomie européenne). 22 septembre. Consulté le 6 décembre 2023 : https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Quantum_encryption_to_boost_European_autonomy

—.s.d. “ What is cloud native? ” (Qu’est-ce que la technologie native en nuage ?). Consulté le 6 décembre 2023 : https://aws.amazon.com/what-is/cloud-native/

Arcuri, Gregory et Sujai Shivakumar. 2022. “ Moore’s Law and Its Practical Implications ” (La loi de Moore et ses implications pratiques). Centre d’études stratégiques et internationales. 18 octobre. Consulté le 6 décembre 2023 : https://www.csis.org/analysis/moores-law-and-its-practical-implications

Argillander, Joakim et al. 2023. “ Quantum Random Number Generation Based on a Perovskite Light Emitting Diode ” (Génération quantique de nombres aléatoires basée sur une diode électroluminescente à base de pérovskite). Communications Physics 6, 157. Consulté le 6 décembre 2023 : https://doi.org/10.1038/s42005-023-01280-3

ASML. s.d. “ EUV Lithography Systems ” (Systèmes de lithographie EUV). Consulté le 6 décembre 2023 : https://www.asml.com/en/products/euv-lithography-systems

Assemblée générale des Nations Unies. 2023. “ Current Developments in Science and Technology and Their Potential Impact on International Security and Disarmament Efforts ” (Dernières évolutions scientifiques et techniques et leurs incidences éventuelles sur l’action menée en matière de sécurité internationale et de désarmement). Document des Nations Unies A/78/268, 1er août.

Avtar, Ram et al. 2021. “ Remote Sensing for International Peace and Security: Its Role and Implications ” (La télédétection au service de la paix et de la sécurité internationales : son rôle et ses implications). Remote Sensing 13, 3: 439. Consulté le 6 décembre 2023 : https://doi.org/10.3390/rs13030439

Basheer, Taha et al. 2022. “ Nanotechnology and Computer Science: Trends and Advances ” (Nanotechnologies et sciences informatiques : tendances et progrès). Memories - Materials, Devices, Circuits and Systems (Mémoires - Matériaux, dispositifs, circuits et systèmes) 2 octobre. Consulté le 6 décembre 2023 : https://doi.org/10.1016/j.memori.2022.100011

Borowitz, Mariel. 2022. “ The Military Use of Small Satellites in Orbit ” (L’utilisation militaire des petits satellites en orbite). Institut français des relations internationales. 4 mars. Consulté le 6 décembre 2023 : https://www.ifri.org/sites/default/files/atoms/files/m._borowitz_military_use_small_satellites_in_orbit_03.2022.pdf

Breaking Defense. 2023. “ When We Talk about What Will Enable JADC2, We’re Really Talking about the Internet of Warfighting Things ” (En parlant de ce qui permettra la mise en œuvre de JADC2, nous parlons en réalité de l’Internet des objets de guerre.). 22 mars. Consulté le 6 décembre 2023 : https://breakingdefense.com/2023/03/when-we-talk-about-what-will-enable-jadc2-were-really-talking-about-the-internet-of-warfighting-things/

Brooks, Michael. 2023a. “ What’s Next for Quantum Computing ” (Prochaine étape de l’informatique quantique). MIT Technology Review. 6 janvier. Consulté le 6 décembre 2023 : https://www.technologyreview.com/2023/01/06/1066317/whats-next-for-quantum-computing/

Brooks, Michael. 2023b. “ Quantum Computers: What are They Good For? ” (Ordinateurs quantiques : à quoi servent-ils ?). Nature. 24 mai. Consulté le 6 décembre 2023 : https://www.nature.com/articles/d41586-023-01692-9

Bureau national de coordination des nanotechnologies des États-Unis. s.d. “ What Is So Special about “ Nano ”? ” (Pourquoi les nanotechnologies sont-elles si spéciales ?). Consulté le 6 décembre 2023 : https://www.nano.gov/about-nanotechnology/what-is-so-special-about-nano

Cameron, Lori. 2018. “ Internet of Things Meets the Military and Battlefield: Connecting Gear and Biometric Wearables for an IoMT and IoBT ” (L’Internet des objets rencontre l’armée et le champ de bataille : connecter les équipements et les dispositifs biométriques portables pour un IoMT et un IoBT). IEEE Computer Society. 1er mars. Consulté le 6 décembre 2023 : https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt

Centre d’excellence pour la cyberdéfense en coopération (CCDCOE) de l’OTAN. 2022. “ Military Movement: Risks from 5G Networks ” (Mouvements militaires : les risques liés aux réseaux 5G). Rapport de recherche. Consulté le 6 décembre 2023 : https://ccdcoe.org/uploads/2022/06/Report_Military-Movement-Risks-from-5G-Networks.pdf

Chandler, David L. 2022. “ The Best Semiconductor of Them All? ” (Le meilleur des semi-conducteurs ?). MIT News. 21 juillet. Consulté le 6 décembre 2023 : https://news.mit.edu/2022/best-semiconductor-them-all-0721

Chen, Zhi et al. 2023. “ Experts’ Take on 6G Technology ” (Le point de vue des experts sur la technologie 6G). China Daily. 7 août. Consulté le 6 décembre 2023 : https://www.chinadaily.com.cn/a/202308/07/WS64d01ddca31035260b81a8d3_1.html

Clynes, Tom. 2023. “ 5 Big Ideas for High-Temperature Superconductors ” (5 grandes idées pour les supraconducteurs à haute température). IEEE Spectrum. 18 septembre. Consulté le 6 décembre 2023 : https://spectrum.ieee.org/high-temperature-superconductors

Coggins, Kevin et al. s.d. “ Quantum Sensing: A New Approach to Maintaining PNT in GPS-Denied Environments ” (Détection quantique : une nouvelle approche pour le maintien du PNT dans les environnements sans GPS). Institut naval des États-Unis. Consulté le 6 décembre 2023 : https://www.usni.org/magazines/proceedings/sponsored/quantum-sensing-new-approach-maintaining-pnt-gps-denied

Coughlin, Tom. 2023. “ 9 IoT Trends to Keep an Eye on in 2023 and Beyond ” (9 tendances de l’IoT à surveiller en 2023 et au-delà). TechTarget. 12 juillet. Consulté le 6 décembre 2023 : https://www.techtarget.com/iotagenda/opinion/IoT-trends-to-keep-an-eye-on

Douglass, Robert. 2022. “ Introduction: IoT for Defense and National Security ” (Introduction : l’IoT pour la défense et la sécurité nationales). In IoT for Defense and National Security (L’IoT au service de la défense et de la sécurité nationales) (éd. R. Douglass, K. Gremban, A. Swami et S. Gerali). Consulté le 6 décembre 2023 : https://doi.org/10.1002/9781119892199.fmatter

Eshel, Tamir. 2022. “ Sensor Fusion for Land Combat Vehicles ” (Fusion de capteurs pour les véhicules de combat terrestres). European Security & Defence. 26 avril. Consulté le 6 décembre 2023 : https://euro-sd.com/2022/04/articles/exclusive/25763/sensor-fusion-for-land-combat-vehicles/

Fadelli, Ingrid. 2023. “ Researchers Demonstrate Scaling of Aligned Carbon Nanotube Transistors to below Sub-10 nm Nodes ” (Des chercheurs démontrent la mise à l’échelle de transistors à nanotubes de carbone alignés en dessous de nœuds de moins de 10 nm). Phys.org. 27 juillet. Consulté le 3 janvier 2024 : https://phys.org/news/2023-07-scaling-aligned-carbon-nanotube-transistors.html

Feldman, Andrey. 2023. “ New Superconductor Could Lead to Quantum Computing Breakthrough ” (Un nouveau supraconducteur pourrait permettre une percée de l’informatique quantique). Advanced Science News. 18 juillet. Consulté le 6 décembre 2023 : https://www.advancedsciencenews.com/new-superconductor-could-lead-to-quantum-computing-breakthrough/

Gambetta, Jay. 2023. “ The Hardware and Software for the Era of Quantum Utility is Here ” (Le matériel et les logiciels pour l’ère de l’utilitaire quantique sont là). IBM. 4 décembre. Consulté le 11 janvier : https://www.ibm.com/quantum/blog/quantum-roadmap-2033

Gargeyas, Arjun. 2022. “ The Role of Semiconductors in Military and Defence Technology ” (Le rôle des semi-conducteurs dans la technologie militaire et de défense). Defence and Diplomacy Journal 11, 2 (Janvier-Mars). Consulté le 6 décembre 2023 : https://capsindia.org/wp-content/uploads/2022/07/DD-Journal-January-March-2022-Arjun-Gargeyas.pdf

Gerwig, Kate et Michaela Goss. 2023. “ The Essential 5G Glossary of Key Terms and Phrases ” (Glossaire des termes et expressions clés de la 5G). TechTarget. 19 octobre. Consulté le 6 décembre 2023 : https://www.techtarget.com/searchnetworking/feature/The-essential-5G-glossary-of-key-terms-and-phrases

Gilchrist, Karen. 2023. “ How U.S. Microchips are Fueling Russia’s Military – Despite Sanctions ” (Comment les micropuces américaines équipent l’armée russe, malgré les sanctions). CNBC. 7 août. Consulté le 6 décembre 2023 : https://www.cnbc.com/2023/08/07/how-us-microchips-are-fueling-russias-military-despite-sanctions.html

Giles, Martin. 2019. “ Cybersecurity Flaws in Chips are Still Taking Too Long to Fix ” (Les failles de cybersécurité dans les puces prennent encore trop de temps à être corrigées). MIT Technology Review. 3 juin. Consulté le 6 décembre 2023 : https://www.technologyreview.com/2019/06/03/135108/cybersecurity-flaws-in-chips-are-taking-too-long-to-fix/

Google. s.d. “ What is cloud native? ” (Qu’est-ce que la technologie native en nuage ?). Consulté le 6 décembre 2023 : https://cloud.google.com/learn/what-is-cloud-native

Hadean. 2022. “ Hadean Awarded British Army Contract to Build Simulation Pathfinder ” (Hadean remporte un contrat de l’armée britannique pour la construction d’un simulateur Pathfinder). 14 juillet.

Consulté le 6 décembre 2023 : https://hadean.com/news/hadean-awarded-british-army-contract-to-build-simulation-pathfinder/

Hamblen, Matt. 2023. “ Stephanie Brown on Sensors Worn by Soldiers for Their Vital Data ” (Stephanie Brown à propos des capteurs portés par les soldats pour suivre leurs paramètres vitaux). Fierce Electronics. 6 juin. Consulté le 6 décembre 2023 : https://www.fiercesensors.com/sensors/stephanie-brown-sensors-worn-soldiers-and-their-vital-data

Hamza, Ekhlas Kadum et Shahad Nafea Jaafar. 2022. “ Nanotechnology Application for Wireless Communication System ” (Nanotechnology Application for Wireless Communication System). Nanotechnology for Electronic Applications. Materials Horizons: From Nature to Nanomaterials. (Horizons des matériaux : de la nature aux nanomatériaux.) Springer, Singapour. Consulté le 6 décembre 2023 : https://doi.org/10.1007/978-981-16-6022-1_6

Hayashi, Yuka et John D. McKinnon. 2023. “ U.S. Looks to Restrict China’s Access to Cloud Computing to Protect Advanced Technology ” (Les États-Unis envisagent de restreindre l’accès de la Chine à l’informatique en nuage pour protéger les technologies de pointe). 4 juillet. Consulté le 6 décembre 2023 : https://www.wsj.com/articles/u-s-looks-to-restrict-chinas-access-to-cloud-computing-to-protect-advanced-technology-f771613

Hecht, Jeff. 2022. “ Nanomaterials Pave the Way for the Next Computing Generation ” (Les nanomatériaux ouvrent la voie à la prochaine génération d’ordinateurs). Nature. 10 août. Consulté le 6 décembre 2023 : https://www.nature.com/articles/d41586-022-02147-3

IBM. 2023. “ Why We Need EUV Lithography for the Future of Chips ” (Pourquoi la lithographie EUV est nécessaire à l’avenir des puces). 26 juin. Consulté le 6 décembre 2023 : https://research.ibm.com/blog/what-is-euv-lithography

Institut de l’ingénierie électrique et électronique (IEEE). s.d.-a. “ Future of Semiconductor Performance ” (L’avenir des performances des semi-conducteurs). Consulté le 6 décembre 2023 : https://irds.ieee.org/topics/future-of-semiconductor-performance

—.s.d.-b. “ Semiconductor Materials ” (Matériaux semi-conducteurs). Consulté le 6 décembre 2023 : https://irds.ieee.org/topics/semiconductor-materials

Intel. s.d. “ The Story of the Intel® 4004 ” (L’histoire du 4004 d’Intel). Consulté le 6 décembre 2023 : https://www.intel.com/content/www/us/en/history/museum-story-of-intel-4004.html

Jayanti, Amritha. 2023. “ Starlink and the Russia–Ukraine War: A Case of Commercial Technology and Public Purpose? ” (Starlink et la guerre entre la Russie et l’Ukraine : un cas de technologie commerciale et de finalité publique ?). Analysis & Opinions, Belfer Center for Science and International Affairs, Harvard Kennedy School. 9 mars. Consulté le 6 décembre 2023 : https://www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose

Kannan, B. Maruthu et al. 2023. “ Secure Communication in IoT-enabled Embedded Systems for Military Applications Using Encryption ” (Communications sécurisées dans les systèmes embarqués basés sur l’IoT pour les applications militaires à l’aide du chiffrement), 2023 2nd International Conference on Edge Computing and Applications (ICECAA), Namakkal, Inde, p. 1385–1389. Consulté le 6 décembre 2023 : https://doi.org/10.1109/ICECAA58104.2023.10212400

Khan, Saif M. et Alexander Mann. 2020. “ AI Chips: What They Are and Why They Matter ” (Puces d’IA : présentation et importance). Center for Security and Emerging Technology. Avril. Consulté le 6 décembre 2023 : https://cset.georgetown.edu/publication/ai-chips-what-they-are-and-why-they-matter/

Kharpal, Arjun. 2023. “ Next-gen Mobile Internet – 6G – will Launch in 2030, Telecom Bosses Say, Even as 5G Adoption Remains Low ” (L’Internet mobile de nouvelle génération 6G sera lancé en 2030, selon des responsables des télécommunications, même si l’adoption de la 5G reste faible). CNBC. 7 mars. Consulté le 6 décembre 2023 : https://www.cnbc.com/2023/03/08/what-is-6g-and-when-will-it-launch-telco-execs-predict.html

Khawaja, Saleem. 2023. “ How Military Uses of the IoT for Defence Applications are Expanding ” (Développement des utilisations militaires de l’IoT pour les applications de défense). Army Technology. 28 mars. Consulté le 6 décembre 2023 : https://www.army-technology.com/sponsored/how-military-uses-of-the-iot-for-defence-applications-are-expanding/

Konkel, Frank. 2023. “ AWS Unveils Edge Device for Defense Customers in Most Extreme Environments ” (AWS dévoile un dispositif de pointe pour les clients du secteur de la défense dans les environnements les plus extrêmes). Nextgov/FCW. 8 juin. Consulté le 6 décembre 2023 : https://www.nextgov.com/digital-government/2023/06/aws-unveils-edge-device-defense-customers-most-extreme-environments/387302/

Kullock, René et al. 2020. “ Electrically-driven Yagi-Uda Antennas for Light ” (Antennes Yagi-Uda à commande électrique pour la lumière). Nature Communications 11, 115. Consulté le 6 décembre 2023 : https://doi.org/10.1038/s41467-019-14011-6

Kumah, Elizabeth Adjoa et al. 2023. “ Human and Environmental Impacts of Nanoparticles: A Scoping Review of the Current Literature ” (Impacts des nanoparticules sur l’homme et l’environnement : revue générale de la bibliographie actuelle). BMC Public Health 23, 1059. Consulté le 6 décembre 2023 : https://doi.org/10.1186/s12889-023-15958-4

Laursen, Lucas. 2022. “ As China’s Quantum-Encrypting Satellites Shrink, Their Networking Abilities Grow ” (Alors que les satellites chinois à chiffrement quantique rétrécissent, leurs capacités de réseau augmentent). IEEE Spectrum. 25 août. Consulté le 6 décembre 2023 : https://spectrum.ieee.org/satellite-qkd-china

Lee, Ki et al. s.d. “ Decentralized Decision Making at the Tactical Edge ” (Prise de décision décentralisée sur le front tactique). Booz Allen. Consulté le 6 janvier 2024 : https://www.boozallen.com/s/insight/blog/decentralized-decision-making-at-the-tactical-edge.html

Lee, Mary et al. 2023. “ Opportunities and Risks of 5G Military Use in Europe ” (Opportunités et risques de l’utilisation militaire de la 5G en Europe). Santa Monica, Californie : RAND Corporation. Consulté le 6 décembre 2023 : https://www.rand.org/pubs/research_reports/RRA1351-2.html

Lee, Sukbae et al. 2023a. “ The First Room-Temperature Ambient-Pressure Superconductor ” (Le premier supraconducteur à température ambiante et à pression ambiante). arXiv. 22 juillet. Consulté le 6 décembre 2023 : https://arxiv.org/abs/2307.12008

—. 2023b. “ Superconductor Pb10-xCux(PO4)6O Showing Levitation at Room Temperature and Atmospheric Pressure and Mechanism ” (Le supraconducteur Pb10-xCux(PO4)6O montre une lévitation à température ambiante et à pression atmosphérique, et son mécanisme). arXiv. 22 juillet. Consulté le 6 décembre 2023 : https://arxiv.org/abs/2307.12037

Levine, Edlyn V. et Algirde Pipikaite. 2019. “ Hardware is a Cybersecurity Risk. Here’s What We Need to Know ” (Le matériel informatique est un risque pour la cybersécurité. Voici ce qu’il faut savoir). Forum économique mondial. 19 décembre. Consulté le 6 décembre 2023 : https://www.weforum.org/agenda/2019/12/our-hardware-is-under-cyberattack-heres-how-to-make-it-safe/

Lewis, James Andrew. 2023. “ Accelerating Federal Cloud Adoption for Modernization and Security ” (Accélérer l’adoption de l’informatique en nuage au niveau fédéral pour la modernisation et la sécurité). Centre d’études stratégiques et internationales (CSIS). 28 juillet. Consulté le 6 décembre 2023 : https://www.csis.org/analysis/accelerating-federal-cloud-adoption-modernization-and-security

Lidar, Daniel. 2023. “ A Scientist Explains an Approaching Milestone Marking the Arrival of Quantum Computers ” (Un scientifique explique l’approche d’un jalon marquant l’arrivée des ordinateurs quantiques). Phys.org. 20 novembre. Consulté le 6 décembre 2023 : https://phys.org/news/2023-11-scientist-approaching-milestone-quantum.html

Macri, Kate. 2022. “ Army is Modernizing Sensors for Data-Driven Decision-Making ” (L’armée modernise ses capteurs pour une prise de décision fondée sur les données). GovCIO Media & Research. 4 mars. Consulté le 6 décembre 2023 : https://governmentciomedia.com/army-modernizing-sensors-data-driven-decision-making

Marquina, Claudia. 2022. “ How Low-Earth Orbit Satellite Technology Can Connect the Unconnected ” (Comment la technologie des satellites en orbite basse peut connecter ce qui ne l’est pas). 18 février. Consulté le 6 décembre 2023 : https://www.weforum.org/agenda/2022/02/explainer-how-low-earth-orbit-satellite-technology-can-connect-the-unconnected/

Marr, Bernard. 2023. “ The 10 Biggest Cloud Computing Trends In 2024 Everyone Must Be Ready For Now ” (Les 10 plus grandes tendances de l’informatique en nuage en 2024 auxquelles chacun doit se préparer dès maintenant). Forbes. 9 octobre. Consulté le 6 décembre 2023 : https://www.forbes.com/sites/bernardmarr/2023/10/09/the-10-biggest-cloud-computing-trends-in-2024-everyone-must-be-ready-for-now/?sh=7ab779e66d67

Martin, Peter et al. 2023. “ Pentagon and Microsoft Are Investigating Leak of Military Emails ” (Le Pentagone et Microsoft enquêtent sur la fuite de courriels militaires). Bloomberg. 22 février. Consulté le 6 décembre 2023 : https://www.bloomberg.com/news/articles/2023-02-22/pentagon-and-microsoft-investigating-leak-of-military-emails

Maurer, Tim et Garrett Hinck. 2020. “ Cloud Security: A Primer for Policymakers ” (Sécurité dans le nuage : un guide à l’intention des décideurs politiques). Dotation Carnegie pour la paix internationale. Août. Consulté le 6 décembre 2023 : https://carnegieendowment.org/files/Maurer_Hinck_Cloud_Security-V3.pdf

Menn, Joseph. 2023. “ Cyberattack Knocks Out Satellite Communications for Russian Military ” (Une cyberattaque met hors service les communications par satellite de l’armée russe). Washington Post. 30 juin. Consulté le 6 décembre 2023 : https://www.washingtonpost.com/technology/2023/06/30/satellite-hacked-russian-military/

Microsoft. 2023. “ BAE Systems and Microsoft Join Forces to Equip Defence Programmes with Innovative Cloud Technology ” (BAE Systems et Microsoft unissent leurs forces pour doter les programmes de défense d’une technologie innovante d’informatique en nuage). 14 avril. Consulté le 6 décembre 2023 :https://news.microsoft.com/en-gb/2023/04/14/bae-systems-and-microsoft-join-forces-to-equip-defence-programmes-with-innovative-cloud-technology/

Microsoft Azure. s.d. “ What is Edge Computing? ” (Qu’est-ce que l’informatique en périphérie ?) Consulté le 6 décembre 2023 : https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-edge-computing

Miller, Kyle et Andrew Lohn. 2023. “ Onboard AI: Constraints and Limitations ” (IA embarquée : contraintes et limites). Center for Security and Emerging Technology (CSET). Août. Consulté le 6 janvier 2024 : https://cset.georgetown.edu/publication/onboard-ai-constraints-and-limitations/

MIT Technology Review Insights. 2023. “ Multi-die Systems Define the Future of Semiconductors ” (Les systèmes multituiles définissent l’avenir des semi-conducteurs). 31 mars. Consulté le 6 décembre 2023 : https://wp.technologyreview.com/wp-content/uploads/2023/03/Synopsys-Report-v6.pdf

Moore, Samuel K. 2022. “ 3 Ways 3D Chip Tech Is Upending Computing ” (3 façons dont la technologie des puces 3D bouleverse l’informatique). IEEE Spectrum. 16 mars. Consulté le 6 décembre 2023 : https://spectrum.ieee.org/amd-3d-stacking-intel-graphcore

Mukherjee, Supantha. 2021. “ Should We be Worried about Space Debris? Scientists Explain ” (Faut-il s’inquiéter des débris spatiaux ? Les scientifiques expliquent). Forum économique mondial. 24 novembre. Consulté le 6 décembre 2023 :https://www.weforum.org/agenda/2021/11/space-debris-satellite-international-space-station/

Pôle de recherche national (PRN). 2021. “ Superconductivity, High Critical Temperature Found in 2D Semimetal Tungsten Nitride ” (Supraconductivité et température critique élevée découvertes dans un semi-métal 2D, le nitrure de tungstène). Phys.org. 5 mai. Consulté le 6 décembre 2023 : https://phys.org/news/2021-05-superconductivity-high-critical-temperature-2d.html

OTAN. 2022. “ Using Quantum Technologies to Make Communications Secure ” (Utiliser les technologies quantiques pour sécuriser les communications). 27 septembre. Consulté le 6 décembre 2023 : https://www.nato.int/cps/en/natohq/news_207634.htm

Pedram, Massoud. 2023. “ Room-Temperature Superconductors Could Revolutionize Electronics – An Electrical Engineer Explains the Materials’ Potential ” (Les supraconducteurs à température ambiante pourraient révolutionner l’électronique : un ingénieur électricien explique le potentiel des matériaux). The Conversation. 28 mars. Consulté le 6 décembre 2023 : https://theconversation.com/room-temperature-superconductors-could-revolutionize-electronics-an-electrical-engineer-explains-the-materials-potential-201849

Ray, Paresh et al. 2009. “ Toxicity and Environmental Risks of Nanomaterials: Challenges and Future Needs ” (Toxicité et risques environnementaux des nanomatériaux : défis et besoins futurs). Journal of Environmental Science and Health, Part C, 27:1, 1–35. Consulté le 6 décembre 2023 : https://doi.org/10.1080/10590500802708267

Renals, Pete. 2021. “ Future Developments in Military Cyber Operations and Their Impact on the Risk of Civilian Harm ” (Évolution future des cyberopérations militaires et leur impact sur le risque de préjudices civils). Humanitarian Law & Policy du CICR. 24 juin. Consulté le 6 décembre 2023 : https://blogs.icrc.org/law-and-policy/2021/06/24/future-military-cyber-operations/

Roa, Carlos. 2023. “ Have We Created the Philosopher’s Stone? Policymakers Should Care about Room-Temperature Superconductors ” (Avons-nous créé la pierre philosophale ? Les décideurs politiques devraient se préoccuper des supraconducteurs à température ambiante). National Interest. 2 août. Consulté le 6 décembre 2023 : https://nationalinterest.org/feature/have-we-created-philosopher%E2%80%99s-stone-policymakers-should-care-about-room-temperature

Rowland, Clare E. et al. 2016. “ Nanomaterial-Based Sensors for the Detection of Biological Threat Agents ” (Capteurs à base de nanomatériaux pour la détection d’agents de menace biologique). Materials Today, 19, 8 octobre. Consulté le 6 décembre 2023 : https://doi.org/10.1016/j.mattod.2016.02.018

Ryugen, Hideaki. 2023. “ TSMC to Make Cutting-edge 2-nm Chips at New Plant in Southern Taiwan ” (TSMC va fabriquer des puces à 2 nm à la pointe de la technologie dans une nouvelle usine située dans le sud de Taïwan). Nikkei Asia. 10 août. Consulté le 6 décembre 2023 : https://asia.nikkei.com/Business/Tech/Semiconductors/TSMC-to-make-cutting-edge-2-nm-chips-at-new-plant-in-southern-Taiwan

Samsung. 2022. “ Samsung Begins Chip Production Using 3nm Process Technology with GAA Architecture ” (Samsung lance la production de puces à l’aide de la technologie de traitement à 3 nm et de l’architecture GAA). Consulté le 6 décembre 2023 : https://news.samsung.com/global/samsung-begins-chip-production-using-3nm-process-technology-with-gaa-architecture

SpeQtral. 2022. “ SpeQtral Announces SpeQtral-1 Quantum Satellite Mission for Ultra-Secure Communications ” (SpeQtral annonce la mission du satellite quantique SpeQtral-1 pour des communications ultra-sécurisées). 9 février. Consulté le 6 décembre 2023 : https://speqtralquantum.com/newsroom/speqtral-announces-speqtral-1-quantum-satellite-mission-for-ultra-secure-communications

Shilov, Anton. 2023. “ The Golden Age of Custom Silicon Draws Near ” (L’âge d’or du silicium personnalisé se rapproche). EE Times. 26 juillet. Consulté le 6 décembre 2023 : https://www.eetimes.com/the-golden-age-of-custom-silicon-draws-near/

Śliwa, Joanna and Marek Suchański. 2022. “ Security Threats and Countermeasures in Military 5G Systems ” (Menaces pour la sécurité et contre-mesures dans les systèmes 5G militaires), 2022 24th International Microwave and Radar Conference (MIKON), Gdansk, Pologne, p. 1-6. Consulté le 6 décembre 2023 : https://doi.org/10.23919/MIKON54314.2022.9924818

Taiwan Semiconductor Manufacturing Company (TSMC). s.d. “ 3nm Technology ” (Technologie 3 nm). Consulté le 6 décembre 2023 : https://www.tsmc.com/english/dedicatedFoundry/technology/logic/l_3nm

Thomas, Arthur. 2021. “ AI at the Tactical Edge for Search & Rescue Operations ” (L’IA au service de la tactique pour les opérations de recherche et de sauvetage). Microsoft. 22 juin. Consulté le 6 décembre 2023 : https://www.microsoft.com/en-us/industry/blog/government/2021/06/22/ai-at-the-tactical-edge-for-search-rescue-operations/

Tirmizi, Syed Bilal Raza et al. 2022. “ Hybrid Satellite–Terrestrial Networks toward 6G: Key Technologies and Open Issues ” (Réseaux hybrides satellite-terre vers la 6G : technologies clés et questions ouvertes). Sensors 22, no. 21 : 8544. https://doi.org/10.3390/s22218544

Tucker, P. 2022. “ How Will the Military Use 5G? A New Drone Experiment Offers Clues ” (Comment les militaires utiliseront-ils la 5G ? Une nouvelle expérience de drones donne des indices). Defense One. 28 septembre. Consulté le 6 décembre 2023 : https://www.defenseone.com/technology/2022/09/how-will-military-use-5g-new-drone-experiment-offers-clues/377745/

UK Defence Science and Technology Laboratory. 2022. “ Sensing: Defence Science and Technology Capability ” (Détection : capacités scientifique et technologique de défense). 31 mars. Consulté le 6 décembre 2023 : https://www.gov.uk/guidance/sensing-defence-science-and-technology-capability

UK National Quantum Technologies Programme. s.d. “ Look Around Corners with the Quantum Periscope ” (Contournez les angles avec le périscope quantique). Consulté le 6 décembre 2023 : https://uknqt.ukri.org/wp-content/uploads/2021/10/Look-Around-Corners-With-The-Quantum-Periscope.pdf

US Congressional Research Service. 2023. “ Defense Primer: Quantum Technology ” (Guide de défense : technologie quantique). 25 octobre. Consulté le 6 décembre 2023 : https://crsreports.congress.gov/product/pdf/IF/IF11836

Département de la défense des États-Unis. 2022. “ Department of Defense Announces Joint Warfighting Cloud Capability Procurement ” (Le Département de la défense des États-Unis annonce l’acquisition d’une Capacité en nuage de combat interarmées). 7 décembre. Consulté le 6 décembre 2023 : https://www.defense.gov/News/Releases/Release/Article/3239378/department-of-defense-announces-joint-warfighting-cloud-capability-procurement/

—. 2023. “ DOD Makes Headway on Cloud Computing ” (Le Département de la défense progresse dans le domaine de l’informatique en nuage). 29 mars. Consulté le 6 décembre 2023 : https://www.defense.gov/News/News-Stories/Article/Article/3345260/dod-makes-headway-on-cloud-computing/

van Amerongen, Michiel. 2021. “ Quantum Technologies in Defence & Security ” (Technologies quantiques dans le domaine de la défense et de la sécurité). Revue de l’OTAN. 3 juin. Consulté le 6 décembre 2023 : https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html

Withrington, Claire. 2023. “ The Internet of Military Things ” (L’Internet des objets militaires). The Cove. 24 août. Consulté le 6 décembre 2023 : **https://cove.army.gov.au/article/internet-military-things**

Xiao, Yinhao et al. 2019. “ Edge Computing Security: State of the Art and Challenges ” (Sécurité de l’informatique en périphérie : situation et défis), dans Proceedings of the IEEE 107, nº 8, p. 1608-1631, août. Consulté le 6 décembre 2023 : **https://doi,org/10.1109/JPROC.2019.2918437**

Xu, Tammy. 2023. “ Better Machine-Learning Models with Quantum Computers ” (De meilleurs modèles d’apprentissage automatique grâce aux ordinateurs quantiques). IEEE Spectrum. 15 novembre. Consulté le 6 décembre 2023 : **https://spectrum.ieee.org/quantum-machine-learning-terra-quanta**

@unidir
/unidir
/un_disarmresearch
/unidirgeneva
/unidir

Palais de Nations
1211 Geneva, Switzerland

© 2026, UNIDIR

UNIDIR.ORG